Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων

ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Έλεγχος Ασφάλειας στο Active Directory

Σπυρόπουλος Γεώργιος
Α.Μ: mte1930

Επιβλέποντες:
Καθηγητής Λαμπρινουδάκης Κωνσταντίνος
Αξιωματικός ΚΕΠΥΕΣ Βάσιος Γεώργιος

Αθήνα 2021

ΠΕΡΙΛΗΨΗ

Το Active Directory είναι μια υπηρεσία καταλόγου ανεπτυγμένη απο την Microsoft για χρήση σε δίκτυα με συστήματα Windows. Η χρήση του είναι ευρεία και συναντάται στις υποδομές μικρών και μεγάλων εταιρειών καθώς και οργανισμών σε όλο τον κόσμο. Αυτή η ευρεία χρήση του έχει οδηγήσει στο να γίνει στόχος επιθέσεων από εξωτερικούς αλλά και εσωτερικούς παράγοντες. Αυτό συμβαίνει γιατί συχνά στα συστήματα που συμμετέχουν στο Active Directory περιέχονται πληροφορίες υψηλής αξίας όπως για παράδειγμα αποτελέσματα έρευνας, σχέδια προϊόντων, εμπορικά μυστικά και άλλα, επίσης η μερική ή ολοκληρωτική καταστροφή του βλάπτει σοβαρά τον εκάστοτε οργανισμό. Λόγω λοιπόν της σημαντικότητας των πληροφοριών που περιέχονται, της ανάγκης για διαθεσιμότητα της Active Directory υποδομής αλλα και της συχνής στοχοποίησης της, οι οργανισμοί που το χρησιμοποιούν πρέπει να μεριμνούν για την ασφάλεια του και να το διατηρούν στη το δυνατόν ασφαλέστερη κατάσταση που επιτρέπουν οι εκάστοτε συνθήκες. Ωστόσο ένα περιβάλλον Active Directory μπορεί να έχει μεγάλο μέγεθος, συνήθως είναι ανάλογο με το μέγεθος του οργανισμού, και να φιλοξενεί πολλές διαφορετικές υπηρεσίες, καθιστώντας την προστασία του ένα αρκετά πολύπλοκο πρόβλημα, ειδικά αν ληφθούν υπόψη οι συχνές αλλαγές που μπορεί να γίνονται σε αυτό. Στη παρούσα εργασία παραθέτονται οι βέλτιστες πρακτικές για την ασφάλιση του Active Directory σύμφωνα με την Microsoft και τελικά παράγεται ένα εργαλείο που αυτοματοποιει τον έλεγχο για την πρακτική εφαρμογή τους.

Λέξεις κλειδιά: Active Directory, Security Assessment, PowerShell

ΚΑΘΟΡΙΣΜΟΣ ΠΡΟΒΛΗΜΑΤΟΣ

Ο έλεγχος, η αναγνώριση και η επιδιόρθωση των σημείων και ρυθμίσεων που μπορούν να οδηγήσουν στη παραβίαση ενός περιβάλλοντος Active Directory είναι αποτελεί χρονοβόρα διαδικασία, λαμβάνοντας υπόψη τη πολύπλοκη δομή και το μέγεθος που μπορεί να έχει ένα τέτοιο περιβάλλον, καθώς και ένα σύνθετο πρόβλημα που διαρκώς αλλάζει, με την επέκταση των υπηρεσιών που προσφέρονται, την αλλαγή πρωτοκόλλων και τη συνεχή εξέλιξη της τεχνολογίας. Το πρόβλημα το οποίο καλείται να επιλύσει η συγκεκριμένη εργασία είναι η αυτοματοποίηση του ελέγχου ασφαλείας σε γνωστά τρωτά σημεία του Active Directory και η αναγνώριση ρυθμίσεων που μπορούν να οδηγήσουν σε παραβίαση ενός Active Directory περιβάλλοντος. Περιλαμβάνει ελέγχους σε πολλαπλά σημεία και συστήματα, κάτι το οποίο ανάλογα με το μέγεθος του Active Directory περιβάλλοντος μπορεί να αποδειχθεί σύνθετη και χρονοβόρα διαδικασία. Οι έλεγχοι στους οποίους καταλήγει και τελικά εφαρμόζονται είναι βασισμένοι στις οδηγίες της Microsoft για την καλύτερη ασφάλιση του Active Directory καθώς και σε πρακτική εμπειρία από την εκτίμηση της ασφάλειας στο συγκεκριμένο περιβάλλον. Τελικά παρουσιάζεται ένα εργαλείο γραμμένο σε Powershell που δημιουργήθηκε με σκοπό την εκτίμηση της ασφάλειας του εκάστοτε Active Directory. Η γλώσσα Powershell επιλέχθηκε ώστε να υπάρχουν το δυνατόν λιγότερες εξωτερικές εξαρτήσεις και να μπορεί να εκτελεστεί σε οποιοδήποτε Microsoft Windows σύστημα χωρίς την ανάγκη προσθήκης περεταίρω πακέτων και προγραμμάτων. Πιο συγκεκριμένα, αφού οριστούν κάποιες απαραίτητες παράμετροι για το εκάστοτε Active Directory περιβάλλον, το εργαλείο εκτελεί αυτοματοποιημένους ελέγχους στα κυριότερα τρωτά σημεία καθώς και σε παραμετροποιήσεις που μπορούν να οδηγήσουν στην παραβίαση του.

ΔΟΜΗ ΕΡΓΑΣΙΑΣ

Η προσέγγιση του προβλήματος στη παρούσα εργασία πραγματοποιείται ακολουθώντας την παρακάτω δομή:

Αρχικά αναλύεται το περιβάλλον Active Directory ως προς το τι είναι, από ποιά μέλη αποτελείται αλλά και τι υπηρεσίες προσφέρει. Το ενδιαφέρον εστιάζεται στην αρχιτεκτονική και την λογική δομή του ενός τέτοιου περιβάλλοντος, ώστε να γίνονται κατανοητές στη συνέχεια οι βέλτιστες πρακτικές που παρουσιάζονται καθως και οι επιπτώσεις της μη υλοποίησης τους.

Στη συνέχεια παρουσιάζονται αναλυτικά οι βέλτιστες πρακτικές για την ασφάλεια ενός Active Directory περιβάλλοντος σύμφωνα με την Microsoft αλλά και πρακτική εμπειρία στην εκτίμηση της ασφάλειας αυτών των υποδομών.

Ακολούθως επιλέγεται ένας αριθμός ελέγχων που όταν γίνονται και επαληθεύονται μειώνεται σημαντικά η επιφάνεια επίθεσης ενός Active Directory και το ρίσκο παραβίασης του, ενώ αυξάνεται η δυσκολία και η πολυπλοκότητα των επιθέσεων που μπορούν να εφαρμοστούν σε αυτό.

Τέλος, καταλήγει στη δημιουργία ενός εργαλείου χρησιμοποιώντας τη γλώσσα Powershell που εκτελεί τους προαναφερθέντες ελέγχους και παραθέτει τα αποτελέσματα στον χρήστη ώστε να στη συνέχεια προχωρήσει στις κατάλληλες ενέργειες.

1. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ACTIVE DIRECTORY

1.1 Τι είναι το Active Directory

Το Active Directory (AD) είναι μια υπηρεσία καταλόγου (Directory Access) που δημιουργήθηκε από την Microsoft και χρησιμεύει στο να πιστοποιεί (authentication) και να εξουσιοδοτεί (authorization) τους χρήστες ενός δικτύου υπολογιστών με λειτουργικό σύστημα Microsoft Windows. Ενώ το AD παρείχε μόνο υπηρεσίες καταλόγου όταν δημοσιεύτηκε για πρώτη φορά, πλέον προσφέρει μια μεγάλη γκάμα από υπηρεσίες περιλαμβάνοντας μέσα σε αυτές Certificate Services (AD CS), Federation Services (AD FS) και Rights Management Services (AD RMS).

1.2 Ανάλυση υπηρεσιών του Active Directory

Το Active Directory περιλαμβάνει διάφορες υπηρεσίες που προκύπτουν από την βασική υπηρεσία του, αυτή του καταλόγου. Αυτές οι υπηρεσίες περιλαμβάνουν:

1.2.1 AD Domain Services (AD DS)

Η συγκεκριμένη υπηρεσία ήταν η πρώτη που προσέφερε το Active Directory και αυθεντικοποιεί τους χρήστες ενός οργανισμού καθώς και την πρόσβαση που έχει ο κάθε χρήστης σε κάθε σύστημα. Για παράδειγμα, όταν ένας χρήστης συνδέεται με το user name του στο δίκτυο, το Active Directory καθορίζει τι τύπου χρήστης είναι, απλός χρήστης (user) ή διαχειριστής (administrator), αν μπορεί να εγκαταστήσει προγράμματα ή όχι, σε ποιους πόρους του δικτύου μπορεί να έχει πρόσβαση (π.χ. κοινόχρηστα και μη αρχεία, εκτυπωτές) κ.α. Ο διακομιστής (server) που έχει εγκατεστημένο το Active Directory και επιτελεί αυτές τις λειτουργίες έχει το ρόλο του Domain Controller στο δίκτυο.

1.2.2 Active Directory Certificate Services (AD CS)

Αυτός είναι ένας ρόλος server που επιτρέπει να δημιουργηθεί μια υποδομή δημοσίων κλειδιών (Public Key Infrastructure – PKI) και να προσφέρει ο σερβερ ψηφιακά πιστοποιητικά για τον οργανισμό στον οποίο ανήκει. Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν για τη κρυπτογράφηση δικτυακής κίνησης, επικοινωνίας μεταξύ εφαρμογών, για την αυθεντικοποίηση των χρηστών και συστημάτων.

1.2.3 Active Directory Federation Services (AD FS)

Τα federation service επιτρέπουν τη χρήση καθολικής σύνδεσης (single sign on) σε εξωτερικά συστήματα όπως σελίδες και εφαρμογές. Το Office 365 είναι μια από τις συχνότερα χρησιμοποιούμενες εφαρμογές με τις οποίες χρησιμοποιείται το single sign on των federation services. Όταν ένας χρήστης συνδέεται στο Office 365 το username και το password του μεταφέρονται από τον federation server και ελέγχονται ως προς την εγκυρότητα στο τοπικό Active Directory. Αυτό επιτρέπει την αυθεντικοποίηση σε

εξωτερικά συστήματα με τη χρήση «τοπικών» αναγνωριστικών (username και password).

1.2.4 Active Directory Lightweight Directory Services (AD LDS)

This service provides directory services using the LDAP protocol without the need to deploy domain controllers. This is primarily used to provide directory service functionally to directory enabled applications. This does not replace AD DS.

1.2.5 Active Directory Rights Management Services (AD RMS)

Αυτή η υπηρεσία παρέχει δυνατότητες προστασίας πληροφοριών σε ηλεκτρονικά έγγραφα. Επιτρέπει τον ακριβή ορισμό δικαιωμάτων όπως, ποιος μπορεί να διαβάσει/ανοίξει, να προωθήσει, να εκτυπώσει ή να εκτελέσει οποιαδήποτε άλλη ενέργεια σε ένα αρχείο. Μπορεί επίσης να χρησιμοποιήσει certificates για την κρυπτογράφηση των αρχεία για περισσότερη ασφάλεια.

1.3 Λογική Δομή στο Active Directory

Τα κύρια λογικά εξαρτήματα (components) του Active Directory είναι τα Objects, τα Forests/Trees/Domains και τα Organization Units (OUs).

1.3.1 Objects

Το Active Directory αποτελείται από δομές πληροφοριών σχετικών με αντικείμενα (objects) μέσα σε ένα δίκτυο. Τα αντικείμενα μπορεί να είναι είτε πόροι (resources), όπως εκτυπωτές, είτε αρχές ασφαλείας (security principals), όπως για παράδειγμα χρήστες και ομάδες χρηστών. Κάθε object έχει τα attributes του, δηλαδή τα μέλη από τα οποία αποτελείται. Αν για παράδειγμα ένα object είναι ενός χρήστη, θα έχει στα attributes το όνομα του χρήστη, το συνθηματικό του και άλλες πληροφορίες. Ένα object μπορεί να έχει εμφωλευμένα άλλα objects, όπως για παράδειγμα ένα OU (Organizational Unit). Επίσης υπάρχει το schema object το οποίο είναι ένα στοιχείο του Active Directory που περιέχει κανόνες για τη δημιουργία αντικειμένων (objects) μέσα σε ένα Active Directory forest. Το Active Directory schema είναι μια λίστα ορισμών σχετικά με τα αντικειμένων του Active Directory και πληροφοριών σχετικά με αυτά τα αντικείμενα που είναι αποθηκευμένα στην Domain Service του Active Directory. Το schema είναι το προσχέδιο του Active Directory και επίσης το schema ορίζει ποια είδη αντικειμένων μπορούν να υπάρχουν στη βάση δεδομένων του Active Directory και τα χαρακτηριστικά αυτών των αντικειμένων.

1.3.2 Domains, Trees και Forests

Τα objects ενός Active Directory μπορούν να οριστούν με παραπάνω από ένα επίπεδα. Τα Forests, Trees και Domains είναι όλα λογικές διαιρέσεις ενός δικτύου Active Directory.

1.3.3 Domains

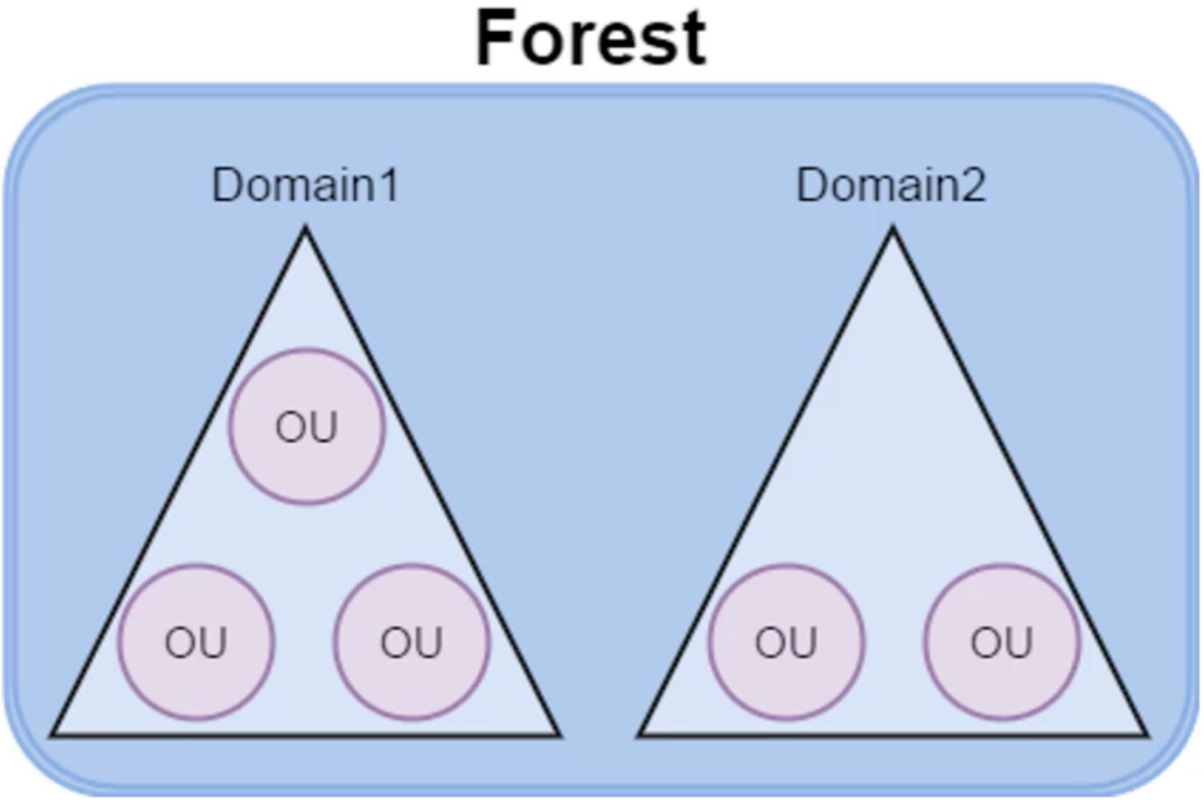
Μέσα σε ένα deployment Active Directory τα objects είναι οργανωμένα σε Domains. Κάθε Domain διαχωρίζεται με βάση το namespace τους, δηλαδή τη διαφορετική δομή των ονομάτων των στοιχείων του. Ένα Domain ορίζεται ως ένα σύνολο από δικτυωμένα στοιχεία (network objects), υπολογιστών, χρηστών και συσκευών, που υπάρχουν/μοιράζονται την ίδια βάση Active Directory.

1.3.4 Trees

Ένα Tree είναι μια συλλογή από ένα ή περισσότερα Domains με παραπλήσιο namespace που συνδέονται με μια «μεταβατική» ιεραρχία εμπιστοσύνης (trust hierarchy)

1.3.5 Forests

Στο ανώτερο επίπεδο της δομής ενός Active Directory είναι το Forest. Είναι μια συλλογή από Trees που μοιράζονται έναν κοινό global catalog, directory schema, λογική δομή και ρυθμίσεις καταλόγου. Σύμφωνα με την Microsoft το Forest αποτελεί όριο ασφαλείας και εσωτερικά αυτού οι χρήστες, οι υπολογιστές, οι συσκευές, οι ομάδες χρηστών και άλλα Active Directory objects είναι προσβάσιμα.



1.3.6 Organizational Units

Ένα Organizational Unit, είναι μια υποδιαίρεση εντός του Active Directory στην οποία μπορούν να τοποθετηθούν χρήστες, ομάδες, υπολογιστές και άλλες οργανικές μονάδες. Μπορούν να δημιουργηθούν OUs για να αντικατοπτρίζουν τη λειτουργική ή

επιχειρηματική δομή ενός οργανισμού. Κάθε domain μπορεί να εφαρμόσει τη δική του ιεραρχία OUs. Εάν ένας οργανισμός περιέχει πολλά domains, μπορούν να δημιουργηθούν δομές OUs σε κάθε domain που είναι ανεξάρτητες από τα OUs στους άλλους domains.

1.3.7 Replication Service

Το Replication Service είναι ο τρόπος με τον οποίο τα δεδομένα των objects ενός Active Directory "αντιγράφονται" από έναν Domain Controller σε έναν άλλο. Έτσι κάθε αλλαγή στα δεδομένα του Directory υπάρχει σε όλους τους Domain Controllers και επιτυγχάνεται ο συγχρονισμός μεταξύ τους. Η λειτουργία του replication service γίνεται μέσω του MS-DRSR (Microsoft-Directory Replication Service Remote Protocol).

Μηχανισμός Ερωτήσεων και Ευρετηρίου: Παρέχει τη δυνατότητα αναζήτησης και δημοσίευσης των objects και των στοιχείων τους

Παγκόσμιος κατάλογος (global catalog)**:** Περιέχει πληροφορίες για κάθε αντικείμενο ενός Active Directory και υπάρχει σε κάθε Domain Controller ενός Forest/Domain.

Αναπαραγωγής (replication service): Είναι υπεύθυνη για το διαμοιρασμό των πληροφοριών ανάμεσα στους Domain Controllers.

2. ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Εκτός από την ανάπτυξη του Active Directory και τις οδηγίες για την παραμετροποίηση των προσφερόμενων λειτουργιών του, η Microsoft προσφέρει και αναλυτικές οδηγίες με τις βέλτιστες πρακτικές ασφαλείας (security best practices) για το προϊόν. Στις ακόλουθες παραγράφους αναπτύσσονται αυτές οι πρακτικές.

2.1 Συνηθέστεροι λόγοι που οδηγούν σε παραβίαση

Σε ελέγχους που έχουν πραγματοποιηθεί σε οργανισμούς μετά από κάποια καταστροφική παραβίαση έχει αποδειχθεί ότι είχαν περιορισμένη εποπτεία της IT υποδομής τους και συχνά υπάρχουν αποκλείσεις μεταξύ της καταγεγραμμένης κατάστασης και αυτής που οδήγησε στην παραβίαση[1]. Αυτές οι διαφορές συχνά δημιουργούν κενά ασφαλείας και νέα τρωτά σημεία (vulnerabilities) στο IT περιβάλλον ενώ ταυτόχρονα διατρέχουν μικρό κίνδυνο να ανιχνευτούν μέχρι οι επιτιθέμενοι να έχουν πλέον πάρει τον πλήρη έλεγχο των συστημάτων.

Αναλύοντας σε βάθος συστήματα και σημεία όπως το AD DS configuration, public key infrastructures (PKIs), τους servers, τα workstations, τις εφαρμογές (applications) και τις access control lists (ACLs) ενός οργανισμού που έχει παραβιαστεί, βρίσκονται λάθη στην παραμετροποίηση (configuration) και κενά ασφαλείας που αν είχαν αντιμετωπιστεί θα απέτρεπαν την αρχική πρόσβαση των επιτιθέμενων στον εκάστοτε οργανισμό. Αυτή η ενότητα αναλύει τους μηχανισμούς που χρησιμοποιούνται από τους επιτιθέμενους για να αποκτήσουν πρόσβαση στην υποδομή ενός Active Directory και στη συνέχεια να αποκτήσουν διαχειριστικά δικαιώματα.

2.1.1 Κενά στη χρήση Antivirus και Anti Malware λογισμικού

Οι περισσότερες παραβιάσεις της ασφάλειας πληροφοριακών συστημάτων ξεκινούν με τη παραβίαση ενός ή δύο συστημάτων κάθε φορά. Αυτά τα αρχικά συμβάντα, ή σημεία εισόδου στο δίκτυο, συχνά αξιοποιούν ευπάθειες που θα μπορούσαν να είχαν διορθωθεί, αλλά δεν είχαν.

Σε ένα περιβάλλον Active Directory οι σταθμοί των χρηστών (workstations) συνήθως διαθέτουν ενεργό, ενεργοποιημένο και ενημερωμένο Antivirus και Anti Malware λογισμικό, με εξαιρέσεις σε συσκευές που συνδέονται σπάνια στο περιβάλλον του οργανισμού ή είναι προσωπικές συσκευές των εργαζομένων και η εγκατάσταση, ενημέρωση και παραμετροποίηση του μπορεί να είναι δύσκολη. Οι διακοσμητές (servers) των οργανισμών που έχουν παραβιαστεί είναι συχνά λιγότερο σχολαστικά προστατευμένοι. Δεν είναι παράξενο το antivirus και Anti Malware λογισμικό τους να μην είναι παραμετροποιημένο με τον ίδιο(/σωστό) τρόπο, να μην είναι ενημερωμένο ή να είναι ακόμα και απενεργοποιημένο από κάποιον διαχειριστή.

[1] Microsoft documentation - Security Best Practices, Avenues To Compromise

Είναι σημαντικό να υπάρχει antivirus και Anti Malware λογισμικό εγκατεστημένο σε όλα τα συστήματα του οργανισμού, να είναι ενεργό, ενημερωμένο και να παρακολουθείται η απενεργοποίηση και η απεγκατάσταση του. Τέλος θα πρέπει να εξασφαλίζεται η ενεργοποίηση του μετά από κάθε επανεκκίνηση (reboot) ενός συστήματος.

2.1.2 Κενά στη διαχείριση ενημερώσεων και εκδόσεων των συστημάτων

Είτε μια μικρή επιχείρηση παραμετροποιεί τους υπολογιστές του Active Directory ώστε να χρησιμοποιούν το Windows Update για τη διαχείριση των ενημερώσεων του συστήματος και των εφαρμογών, είτε ένας μεγάλος οργανισμός χρησιμοποιεί λογισμικό διαχείρισης όπως το Microsoft Endpoint Configuration Manager για την εφαρμογή ενημερώσεων σύμφωνα με λεπτομερή, ιεραρχικά σχέδια, πολλοί οργανισμοί επιδιορθώνουν τις υποδομές των Windows σε σχετικά εγκαίρως.

Ωστόσο, λίγες υποδομές περιλαμβάνουν μόνο υπολογιστές Windows και εφαρμογές Microsoft, και σε παραβιασμένα περιβάλλοντα, είναι σύνηθες να διαπιστώνεται ότι η στρατηγική διαχείρισης ενημερωμένων εκδόσεων του οργανισμού περιέχει κενά. Τα συστήματα των Windows σε αυτά τα περιβάλλοντα έχουν διορθωθεί με συνέπεια. Τα λειτουργικά συστήματα που δεν ανήκουν στα Windows έχουν διορθωθεί σποραδικά, αν όχι καθόλου.

Συσκευές δικτύου συχνά παραμένουν με εργοστασιακά default credentials και χωρίς ενημερώσεις firmware (υλικολογισμικού). Εφαρμογές και λειτουργικά συστήματα που δεν υποστηρίζονται πλέον από τους προμηθευτές τους συνεχίζουν να εκτελούνται, παρά το γεγονός ότι δεν μπορούν πλέον να επιδιορθωθούν από (ευπάθειες) vulnerabilities. Κάθε ένα από αυτά τα μη ενημερωμένα συστήματα αποτελεί πιθανό σημείο εισόδου στο Active Directory.

Εκτός από την εφαρμογή των ενημερώσεων, σημαντικό ρόλο στην ασφάλεια του Active Directory παίζει και η ύπαρξη παλαιότερων ή πλέον μη υποστηριζόμενων από τον προμηθευτή συστημάτων και λογισμικού. Ένας οργανισμός θα πρέπει να διαθέτει όσο το δυνατόν λιγότερα τέτοια σύστημα καθώς ακόμα και αν ο προμηθευτής τους παρέχει ενημερώσεις ασφαλείας για αυτά, τα ίδια συχνά δεν διαθέτουν ή δεν υποστηρίζουν νεότερα πρωτόκολλα ή security features. Αποτέλεσμα αυτού είναι να αυξάνονται τα τρωτά σημεία του Active Directory.

Έτσι καταλήγουμε στο συμπέρασμα ότι πρέπει να υπάρχει ένα αποτελεσματικό σύστημα διαχείρισης των ενημερώσεων τόσο των Windows συστημάτων και εφαρμογών όσο και των συστημάτων και εφαρμογών τρίτων, σε συνδυασμό με συχνή αξιολόγηση της παραμονής παλαιότερων ή/και μη υποστηριζόμενων συστημάτων με γνώμονα τη χρησιμότητα έναντι των πιθανών κινδύνων που προσθέτουν αυτά. Στη περίπτωση που δεν είναι αναγκαία η ύπαρξη τους θα πρέπει να καταργούνται ή να αντικαθίστανται με νεότερα ή διαφορετικά συστήματα ώστε να μειωθεί η επιφάνεια επίθεσης (attack surface) του Active Directory.

2.1.3 Λανθασμένη Παραμετροποίηση (Misconfiguration)[2]

Ακόμα και σε περιβάλλοντα που διατηρούνται ενημερωμένα και χρησιμοποιούν νεότερες εκδόσεις λογισμικού συχνά εντοπίζονται κενά ασφαλείας που δημιουργούνται λόγω κακής ή λανθασμένης παραμετροποίησης (στη συνέχεια αναφέρεται ως misconfiguration) σε επίπεδο λειτουργικού συστήματος, εφαρμογής ή στο ίδιο το Active Directory. Αυτά τα misconfigurations μπορεί να εκθέτουν μόνο το τοπικό (local) σύστημα, όμως εφόσον ένας επιτιθέμενος αποκτήσει πρόσβαση σε ένα σύστημα είναι σύνηθες να συνεχίσει τις προσπάθειες του με σκοπό να παραβιάσει περισσότερα και τελικά το Active Directory του οργανισμού.

2.1.3.1 Misconfiguration στο Active Directory

Οι λογαριασμοί που στοχεύονται συχνότερα από τους επιτιθέμενους είναι αυτοί που ανήκουν σε τουλάχιστον ένα από τα administrative groups του Active Directory. Αυτά τα groups είναι, οι Domain Admins (DA), Enterprise Admins (EA) και built-in Admins (BA). Οι λογαριασμοί που είναι μέλη οποιουδήποτε από αυτά τα groups θα πρέπει να είναι μειωθούν στον δυνατόν ελάχιστο αριθμό ώστε να περιοριστεί η επιφάνεια επίθεσης του Active Directory. Η ύπαρξη περισσότερων λογαριασμών σε αυτά τα groups από όσοι είναι αναγκαίοι θεωρείται misconfiguration στα δικαιώματα των χρηστών (user privileges) και αυξάνει σημαντικά το ρίσκο και την επιφάνεια επίθεσης στο Active Directory. Είναι δυνατό, και θεμιτό να εξαλειφθεί η μόνιμη προσθήκη λογαριασμών σε αυτά τα groups και η πρόσβαση σε αυτά να γίνεται προσωρινά μόνο όταν υπάρχει ανάγκη να χρησιμοποιηθούν τα ξεχωριστά δικαιώματα (permissions) που διαθέτουν τα μέλη τους. Αποτέλεσμα της συγκεκριμένης παραμετροποίησης είναι η μείωση της επιφάνειας επίθεσης του Active Directory.

2.1.3.2 Misconfiguration στους Domain Controllers

Η παραμετροποίηση και διαχείριση των Domain Controllers με τον ίδιο τρόπο όπως οι υπόλοιποι member servers ενός Active Directory είναι συχνό λάθος στην παραμετροποίηση τους. Σε τέτοιες περιπτώσεις οι Domain Controllers βρίσκονται να έχουν εγκατεστημένες εφαρμογές και εργαλεία που υπάρχουν στους απλούς member servers, όχι επειδή χρειάζεται να υπάρχουν στους domain controllers, αλλά επειδή είναι μέρος ενός standard build που εφαρμόζει ο οργανισμός κατά την δημιουργία ενός νέου Windows server. Αυτές οι εφαρμογές είναι συνήθως περιττές ή και επικίνδυνες για τους Domain Controllers και το Active Directory συνολικά. Η εγκατάσταση τους αποτελεί misconfiguration των Domain Controllers καθώς αυτές οι εφαρμογές εκτελούνται με διαχειριστικά δικαιώματα σε κρίσιμα συστήματα για το Active Directory στα οποία θα πρέπει να εκτελούνται αποκλειστικά οι απαραίτητες εφαρμογές για τη λειτουργία του Active Directory. Ταυτόχρονα αυξάνουν την επιφάνεια επίθεσης του Active Directory αφού για να λειτουργήσουν ανοίγουν ports των domain controllers και δίνεται η δυνατότητα σύνδεσης σε χρήστες που κανονικά δεν θα έπρεπε να συνδέονται στους domain controllers παρά μόνο για την αυθεντικοποίηση τους και την εφαρμογή των

[2] Microsoft, Avenues to compromise: Misconfiguration

group policies των αντίστοιχων groups στα οποία ανήκουν. Ένα ακόμη misconfiguration είναι η πρόσβαση τους στο internet και η δυνατότητα να γίνεται download internet περιεχομένου και εφαρμογών από τους domain controllers. Αυτό μπορεί να είναι απόρροια ανάγκης κάποιας από τις περιττές εφαρμογές που αναφέρθηκαν νωρίτερα, είτε μια παραμετροποίηση που έγινε σκόπιμα από τους διαχειριστές του Active Directory. Παρότι στους Domain Controllers το Internet Explorer Enhanced Security Configuration είναι ενεργοποιημένο εξ αρχής, συχνά απενεργοποιείται από τους διαχειριστές. Το download από χρήστες με διαχειριστικά δικαιώματα είναι επικίνδυνο σε κάθε υπολογιστή, όταν αυτός είναι ένας Domain Controller τότε τίθεται σε ρίσκο ολόκληρο το Directory Service ενός Active Directory.

Οι Domain Controllers θα πρέπει να μεταχειρίζονται ως κρίσιμα συστήματα και να έχουν διαφορετική και πιο αυστηρή παραμετροποίηση από τους υπόλοιπους member servers του Active Directory. Στους Domain Controllers θα πρέπει να εκτελούνται εφαρμογές που είτε είναι απαραίτητες για τη λειτουργία των ίδιων, είτε συμβάλλουν/αυξάνουν την ασφάλεια τους. Δεν πρέπει να έχουν πρόσβαση στο Διαδίκτυο και οι ρυθμίσεις ασφαλείας πρέπει να διαμορφώνονται και να επιβάλλονται από Group Policy Objects (GPOs).

2.1.3.3 Misconfiguration στο λειτουργικό σύστημα.

Θα πρέπει να υπάρχουν διαφορετικά baseline configurations για τους διαφορετικούς τύπους servers τα οποία θα εφαρμόζονται στους νέους servers κατά την δημιουργία τους. Η ad hoc δημιουργία servers αυξάνει τη πιθανότητα να υπάρχουν διαφορές ανάμεσα στη παραμετροποίηση servers με την ίδια λειτουργία και να δημιουργεί άγνωστες ευπάθειες και δυσκολία αναγνώρισης τους από τους διαχειριστές. Ιδιαίτερη προσοχή θα πρέπει να γίνεται κατά τη δημιουργία του baseline configuration καθώς αν αυτό δημιουργεί ή αφήνει ανοιχτές ευπάθειες στους servers που εφαρμόζεται τότε η ίδια ευπάθεια δημιουργείται ή παραμένει σε όλους τους servers του συγκεκριμένου τύπου. Συχνά λάθη παραμετροποίησης σε επίπεδο λειτουργικού συστήματος είναι η απενεργοποίηση ενημερώσεων και χαρακτηριστικών ασφαλείας, η δημιουργία λογαριασμών με περισσότερα δικαιώματα από όσα χρειάζονται (κυρίως service accounts), ο ορισμός κοινών credentials παντού, η δυνατότητα εγκατάστασης εφαρμογών και εργαλείων από μη εξουσιοδοτημένους χρήστες ή η εγκατάσταση εφαρμογών άγνωστης προέλευσης (un-signed). Η ανεξέλεγκτη εγκατάσταση εφαρμογών μπορεί να δημιουργήσει νέες ευπάθειες που νωρίτερα δεν υπήρχαν.

2.1.3.3.1 Απενεργοποίηση χαρακτηριστικών ασφαλείας

Ορισμένες φορές οι οργανισμοί απενεργοποιούν το Windows Firewall με το Advanced Security (WFAS) λόγω της πεποίθησης ότι το WFAS είναι δύσκολο να παραμετροποιηθεί ή ότι η παραμετροποίηση του απαιτεί αυξημένη ενασχόληση. Ωστόσο, από τον Windows Server 2008 και στη συνέχεια, όταν οποιοσδήποτε ρόλος ή feature είναι εγκατεστημένος σε έναν server, παραμετροποιείται εξ αρχής με τα ελάχιστα δικαιώματα που απαιτούνται για τη λειτουργία του ρόλου ή feature και το Windows Firewall ρυθμίζεται αυτόματα για να υποστηρίζει τον ρόλο ή feature. Απενεργοποιώντας το

WFAS (και μη χρησιμοποιώντας άλλο host based firewall), οι οργανισμοί αυξάνουν την επιφάνεια επίθεσης σε ολόκληρο το περιβάλλον των Windows. Τα περιμετρικά firewalls παρέχουν προστασία έναντι επιθέσεων που στοχεύουν άμεσα ένα περιβάλλον από το Διαδίκτυο, αλλά δεν παρέχουν προστασία έναντι επιθέσεων που εκμεταλλεύονται άλλους φορείς επίθεσης, όπως drive-by download ή επιθέσεις που προέρχονται από άλλα παραβιασμένα συστήματα στο εσωτερικό δίκτυο.

Οι ρυθμίσεις ελέγχου λογαριασμού χρήστη (UAC) μερικές φορές απενεργοποιούνται σε servers, επειδή τους διαχειριστές με σκοπό να αποφύγουν τα prompts. Παρότι δίνεται η δυνατότητα να απενεργοποιηθεί το UAC στους Windows Server, εκτός αν εκτελείται εγκατάσταση server core (όπου το UAC είναι απενεργοποιημένο by design), το UAC δεν πρέπει να απενεργοποιείται σε servers χωρίς προσεκτική εξέταση και έρευνα.
Σε άλλες περιπτώσεις, οι ρυθμίσεις των servers διαμορφώνονται σε λιγότερο ασφαλείς τιμές επειδή οι οργανισμοί εφαρμόζουν ξεπερασμένα baseline configurations σε νέα λειτουργικά συστήματα, όπως η εφαρμογή baseline configuration από Windows Server 2003 σε Windows Server 2012, Windows Server 2008 R2 ή Windows Server 2008, χωρίς αλλαγή/ενημέρωση του baseline configuration ώστε να αντικατοπτρίζουν τις αλλαγές στο λειτουργικό σύστημα. Αντί να μεταφέρονται παλαιότερα baseline configurations σε νέα λειτουργικά συστήματα, κατά την εγκατάσταση ενός νέου λειτουργικού συστήματος ή την αναβάθμιση από παλαιότερο, ελέγξτε τις αλλαγές ασφαλείας και το baseline configuration για να βεβαιωθείτε ότι οι ρυθμίσεις που εφαρμόζονται είναι εφαρμόσιμες και κατάλληλες για το νέο λειτουργικό σύστημα.

2.1.3.3.2 Παραχώρηση υπερβολικών δικαιωμάτων (Granting excessive privileges)

Η παραβίαση ενός διαχειριστικού λογαριασμού σε έναν υπολογιστή επιτρέπει στους εισβολείς να θέσουν σε κίνδυνο τους λογαριασμούς κάθε χρήστη και υπηρεσίας που συνδέεται στον υπολογιστή και να συλλέξουν και να αξιοποιήσουν credentials για να παραβιάσουν στη συνέχεια και άλλα συστήματα. Ένας εισβολέας με διαχειριστική πρόσβαση σε έναν υπολογιστή μπορεί να απενεργοποιήσει το anti malware λογισμικό, να εγκαταστήσει rootkits, να τροποποιήσει προστατευμένα αρχεία ή να εγκαταστήσει κακόβουλο λογισμικό στον υπολογιστή που αυτοματοποιεί επιθέσεις ή μετατρέπει έναν διακομιστή σε drive-by download host. Οι τακτικές που χρησιμοποιούνται για την επέκταση μιας παραβίασης σε πρόσθετα συστήματα ποικίλλουν, αλλά το κλειδί για την επιτυχία τους είναι η απόκτηση διαχειριστικής πρόσβασης. Μειώνοντας τον αριθμό των λογαριασμών με προνομιακή πρόσβαση σε οποιοδήποτε σύστημα, μειώνεται την επιφάνεια επίθεσης όχι μόνο αυτού του υπολογιστή, αλλά και η πιθανότητα ενός εισβολέα να αποκτήσει πολύτιμα credentials από τον υπολογιστή.

2.1.3.3.3 Κοινά Administrator credentials μεταξύ servers

Εάν ο τοπικός λογαριασμός διαχειριστή έχει την ίδια τιμή στους servers και ο κωδικός πρόσβασης για τον λογαριασμό έχει επίσης την ίδια τιμή, οι εισβολείς μπορούν να εξάγουν τα credentials του λογαριασμού σε έναν υπολογιστή στον οποίο αποκτήθηκε πρόσβαση σε επίπεδο διαχειριστή ή συστήματος. Ο εισβολέας δεν χρειάζεται αρχικά

να αποκτήσει πρόσβαση στον λογαριασμό διαχειριστή, αρκεί η παραβίαση ενός λογαριασμού που είναι μέλος στο group Local Administrators ή ενός service account που έχει ρυθμιστεί να λειτουργεί ως LocalSystem ή με δικαιώματα διαχειριστή. Στη συνέχεια, ο εισβολέας μπορεί να εξάγει τα credentials για το λογαριασμό διαχειριστή και να τα επαναλάβει σε άλλους υπολογιστές στο δίκτυο.
Εφόσον ένας άλλος υπολογιστής διαθέτει τοπικό λογαριασμό με το ίδιο όνομα χρήστη και κωδικό πρόσβασης (ή την hashed τιμή του) με τα credentials λογαριασμού που παρουσιάζονται, η προσπάθεια σύνδεσης επιτυγχάνει και ο εισβολέας αποκτά διαχειριστική πρόσβαση στον στοχευμένο υπολογιστή. Στις τρέχουσες εκδόσεις των Windows, ο λογαριασμός built-in Administrator είναι απενεργοποιημένος από προεπιλογή, αλλά σε παλαιότερα λειτουργικά συστήματα, ο λογαριασμός είναι ενεργοποιημένος από προεπιλογή.

2.2 Λογαριασμοί που αποτελούν στόχο[3]

Σύμφωνα με την Microsoft[4], μετά την απόκτηση διαχειριστικών δικαιωμάτων σε ένα σύστημα του οργανισμού, οι επιτιθέμενοι χρησιμοποιούν εργαλεία για να αποκτήσουν credentials από διαφορετικούς χρήστες που έχουν συνδεθεί στο συγκεκριμένο σύστημα. Αυτά τα credentials μπορεί να προέρχονται από hashes, tickets ή και plaintext passwords. Αν τα credentials στα οποία πήραν πρόσβαση ανήκουν σε χρήστες που είναι πιθανό να έχουν πρόσβαση και σε άλλα συστήματα (root σε Unix/Linux/OSX, Administrator σε Windows) τότε οι επιτιθέμενοι προσπαθούν να πάρουν πρόσβαση σε περισσότερα συστήματα με αυτά, με σκοπό να αποκτήσουν πρόσβαση ή credentials σε δύο τύπους χρηστών.
Αυτοί οι δύο τύπου λογαριασμοί χρηστών είναι οι εξής:

1. Προνομιακοί λογαριασμοί στο domain με ευρεία και βαθιά δικαιώματα (δηλαδή, λογαριασμούς με δικαιώματα διαχειριστή σε πολλούς υπολογιστές και σε Active Directory). Αυτοί οι λογαριασμοί ενδέχεται να μην ανήκουν σε κάποιο από τα groups με τα υψηλότερα δικαιώματα στο Active Directory, αλλά ενδέχεται να έχουν διαχειριστικά δικαιώματα σε πολλούς servers και workstations του forest, γεγονός που τους καθιστά παρόμοια ισχυρούς με τα μέλη διαχειριστικών groups στο Active Directory. Στις περισσότερες περιπτώσεις, οι λογαριασμοί στους οποίους έχουν παραχωρηθεί υψηλά αυτά τα υψηλά δικαιώματα σε ευρεία κλίμακα της υποδομής των Windows είναι service accounts, επομένως τα service accounts πρέπει πάντα να αξιολογούνται για το εύρος και το βάθος των προνομίων που διαθέτουν.
2. VIP (Very Important Person) domain accounts. Ένας VIP λογαριασμός είναι οποιοσδήποτε λογαριασμός έχει πρόσβαση σε πληροφορίες που θέλει ένας εισβολέας (πνευματική ιδιοκτησία και άλλες ευαίσθητες πληροφορίες) ή οποιονδήποτε λογαριασμό που μπορεί να χρησιμοποιηθεί για να παραχωρήσει στον εισβολέα πρόσβαση σε αυτές τις πληροφορίες. Παραδείγματα αυτών των λογαριασμών χρηστών περιλαμβάνουν:

[3] Microsoft, AD Security Best Practises: Attractive Accounts for Credential Theft
[4] Attractive Accounts for Credential Theft

a. Στελέχη των οποίων οι λογαριασμοί έχουν πρόσβαση σε ευαίσθητες εταιρικές πληροφορίες.
b. Λογαριασμοί για το προσωπικό του Help Desk που είναι υπεύθυνο για τη συντήρηση των υπολογιστών και των εφαρμογών που χρησιμοποιούνται από στελέχη.
c. Λογαριασμοί νομικού προσωπικού που έχουν πρόσβαση στα έγγραφα προσφοράς και σύμβασης ενός οργανισμού, είτε τα έγγραφα προορίζονται για τον δικό τους οργανισμό είτε για οργανισμούς πελατών.
d. Σχεδιαστές προϊόντων που έχουν πρόσβαση σε σχέδια και προδιαγραφές για προϊόντα που βρίσκονται αναπτύσσονται από την εταιρεία, ανεξάρτητα από τους τύπους προϊόντων που κατασκευάζει η εταιρεία.
e. Ερευνητές των οποίων οι λογαριασμοί χρησιμοποιούνται για πρόσβαση σε δεδομένα μελέτης, διατυπώσεις προϊόντων ή οποιαδήποτε άλλη έρευνα που ενδιαφέρει έναν εισβολέα.

Επειδή οι λογαριασμοί του πρώτου τύπου μπορούν στη συνέχεια να χρησιμοποιηθούν για να αποκτηθεί πρόσβαση στους VIP χρήστες και τα δεδομένα τους, οι πιο χρήσιμοι λογαριασμοί για υποκλοπή credentials είναι όσων χρηστών είναι μέλη σε ένα περισσότερα από τα διαχειριστικά groups, δηλαδή Domain Admins (DA), Enterprise Admins (EA) και οι built-in Administrators (BA). Παρότι συνήθως στόχος των εισβολέων είναι το group Domain Admins, η πρόσβαση σε οποιοδήποτε από αυτά τα groups δίνει τη δυνατότητα στους εισβολείς να παραβιάσουν ολόκληρο το AD DS (Active Directory Domain Service) μέσω κάποιου domain controller.

2.3 Ενέργειες που αυξάνουν τη πιθανότητα παραβίασης

Επειδή ο στόχος της κλοπής credentials είναι συνήθως εξαιρετικά προνομιακοί λογαριασμοί τομέα και λογαριασμοί VIP, είναι σημαντικό για τους διαχειριστές να γνωρίζουν δραστηριότητες που αυξάνουν την πιθανότητα επιτυχίας μιας επίθεσης κλοπής credentials. Παρόλο που οι εισβολείς στοχεύουν και VIP λογαριασμούς, εάν οι VIP δεν έχουν υψηλά δικαιώματα σε συστήματα ή στο (Active Directory) domain, η κλοπή των credentials τους απαιτεί άλλους τύπους επιθέσεων, όπως το social engineering του VIP για την παροχή μυστικών πληροφοριών. Ή ο εισβολέας πρέπει πρώτα να αποκτήσει προνομιακή πρόσβαση σε ένα σύστημα στο οποίο αποθηκεύονται προσωρινά (cached) τα credentials VIP. Εξαιτίας αυτού, οι δραστηριότητες που αυξάνουν την πιθανότητα κλοπής διαπιστευτηρίων που περιγράφονται εδώ εστιάζονται κυρίως στην αποτροπή της απόκτησης πολύ προνομιακών διαχειριστικών credentials. Αυτές οι δραστηριότητες είναι κοινοί μηχανισμοί με τους οποίους οι επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο τα συστήματα για να αποκτήσουν προνομιακά credentials.

2.3.1 Σύνδεση σε μη ασφαλή συστήματα με προνομιακούς λογαριασμούς

Η βασική ευπάθεια που επιτρέπει την επίτευξη επιθέσεων κλοπής credentials είναι η σύνδεση σε υπολογιστές που δεν είναι ασφαλείς με λογαριασμούς που ανήκουν στα διαχειριστικά groups και είναι ευρέως προνομιούχοι σε όλο το Active Directory. Αυτές οι συνδέσεις μπορεί να είναι το αποτέλεσμα διαφόρων λανθασμένων παραμετροποιήσεων που περιγράφονται στη συνέχεια.

2.3.2 Μη τήρηση ξεχωριστών διαχειριστικών λογαριασμών

Η χρήση ενός μόνο λογαριασμού από το προσωπικό, συνήθως του τμήματος πληροφορικής, για όλη τη δουλειά τους θέτει σε κίνδυνο όλο το Active Directory. Ο λογαριασμός είναι συχνά μέλος τουλάχιστον σε ένα από τα διαχειριστικά groups του Active Directory και είναι ο ίδιος λογαριασμός που χρησιμοποιούν οι υπάλληλοι για να συνδεθούν στους σταθμούς εργασίας τους το πρωί, να ελέγξουν το email τους, να περιηγηθούν στο Διαδίκτυο και να κατεβάσουν περιεχόμενο στο δικό τους Υπολογιστές. Όταν οι χρήστες χρησιμοποιούν λογαριασμούς στους οποίους παρέχονται δικαιώματα και δικαιώματα local Administrator, εκθέτουν τον τοπικό υπολογιστή σε κίνδυνο να παραβιαστεί πλήρως. Όταν αυτοί οι λογαριασμοί είναι επίσης μέλη των διαχειριστικών groups, εκθέτουν ολόκληρο το Active Directory σε κίνδυνο ολικής παραβίασης, καθιστώντας εύκολο για έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο του περιβάλλοντος της υπηρεσίας καταλόγου Active Directory και των Windows μηχανημάτων.
Ομοίως, η ίδια πρακτική θέτει σε κίνδυνο μη Windows συστήματα όταν εφαρμόζεται σε λογαριασμούς root ή προσθήκη στο sudo/wheel group ,κάτι που επιτρέπει στους εισβολείς να επεκτείνουν συμβιβασμούς από συστήματα UNIX ή Linux σε συστήματα Windows και το αντίστροφο.

2.3.3 Μη ασφαλείς διαχειριστικοί σταθμοί

Σε πολλούς οργανισμούς, το προσωπικό πληροφορικής χρησιμοποιεί πολλαπλούς λογαριασμούς. Ένας λογαριασμός χρησιμοποιείται για σύνδεση στο σταθμό εργασίας του υπαλλήλου και επειδή πρόκειται για προσωπικό πληροφορικής, συχνά έχουν δικαιώματα local Administrator στους σταθμούς εργασίας τους. Σε ορισμένες περιπτώσεις, το UAC (User Account Control) αφήνεται ενεργοποιημένο έτσι ώστε ο χρήστης να λαμβάνει τουλάχιστον ένα *split access token* κατά τη σύνδεση και πρέπει να κάνει elevate όταν απαιτούνται δικαιώματα. Όταν αυτοί οι χρήστες εκτελούν δραστηριότητες συντήρησης, συνήθως χρησιμοποιούν τοπικά εγκατεστημένα εργαλεία διαχείρισης και παρέχουν τα credentials για τους λογαριασμούς που διαθέτουν δικαιώματα στο domain, επιλέγοντας «Εκτέλεση ως διαχειριστής» ή παρέχοντας τα credentials όταν ζητηθούν. Αν και αυτή η παραμετροποίηση μπορεί να φαίνεται σωστή, εκθέτει το περιβάλλον σε πιθανή παραβίαση επειδή:

- Ο "κανονικός" λογαριασμός χρήστη που χρησιμοποιεί ο υπάλληλος για να συνδεθεί στο σταθμό εργασίας του έχει δικαιώματα local Administrator, ο υπολογιστής είναι ευάλωτος σε επιθέσεις, πχ. drive-by download στις οποίες ο χρήστης είναι πεπεισμένος να εγκαταστήσει κακόβουλο λογισμικό.
- Το κακόβουλο λογισμικό είναι εγκατεστημένο στο πλαίσιο ενός λογαριασμού διαχειριστή και ο εισβολέας έχει τη δυνατότητα να καταγράψει ευαίσθητες πληροφορίες όπως η είσοδος του πληκτρολογίου (key-logging), του clipboard , να τραβήξει screenshot καθώς και να αποκτήσει τα cached credentials που υπάρχουν στη μνήμη. Οποιαδήποτε από αυτές τις ενέργειες μπορεί να οδηγήσει σε απόκτηση των credentials ενός λογαριασμού με υψηλά δικαιώματα στο domain (Domain Admin, Enterprise Admin, built-in Admin).

Τα προβλήματα σε αυτό το σενάριο είναι δύο. Πρώτον, αν και χωριστοί λογαριασμοί χρησιμοποιούνται για τοπική διαχείριση και διαχείριση του domain, ο υπολογιστής δεν είναι ασφαλής και δεν προστατεύει τους λογαριασμούς από κλοπή. Δεύτερον, στον κανονικό λογαριασμό χρήστη και στον λογαριασμό διαχειριστή έχουν εκχωρηθεί υπερβολικά δικαιώματα.

2.3.4 Συνδέσεις σε παραβιασμένους σταθμούς εργασίας ή member servers με προνομιακούς λογαριασμούς

Όταν χρησιμοποιείται ένας διαχειριστικός domain λογαριασμός για σύνδεση διαδραστικά σε έναν παραβιασμένο σταθμό εργασίας ή member server, αυτός ο παραβιασμένος υπολογιστής μπορεί να συλλέξει τα credentials από οποιονδήποτε λογαριασμό συνδέεται στο σύστημα.

2.3.5 Πρόσβαση στο Internet με διαχειριστικούς λογαριασμούς

Οι χρήστες που συνδέονται σε υπολογιστές με λογαριασμούς που είναι μέλη του local Administrator group στο συγκεκριμένο σύστημα ή μέλη τουλάχιστον ενός από τα διαχειριστικά groups του Active Directory, οι οποίοι στη συνέχεια περιηγούνται στο Διαδίκτυο (ή ένα παραβιασμένο intranet) εκθέτουν τον τοπικό υπολογιστή και το domain σε κίνδυνο πιθανής παραβίασης.
Η πρόσβαση σε κακόβουλα websites με πρόγραμμα περιήγησης που λειτουργεί με δικαιώματα διαχειριστή μπορεί να επιτρέψει σε έναν εισβολέα να εκτελέσει κακόβουλο κώδικα στον τοπικό υπολογιστή στο πλαίσιο του προνομιούχου χρήστη. Εάν ο χρήστης έχει τοπικά δικαιώματα διαχειριστή στον υπολογιστή, οι εισβολείς ενδέχεται να εξαπατήσουν τον χρήστη να κατεβάσει κακόβουλο κώδικα ή να ανοίξει συνημμένα email που αξιοποιούν τις ευπάθειες εφαρμογών και αξιοποιούν τα δικαιώματα του χρήστη για εξαγωγή των τοπικά αποθηκευμένων credentials για όλους τους ενεργούς χρήστες στον υπολογιστή. Εάν ο χρήστης έχει δικαιώματα διαχειριστή στο domain όντας μέλος του group Domain Admins, Enterprise Admins ή Administrators του Active Directory, ο εισβολέας μπορεί να εξαγάγει τα domain credentials και να τα χρησιμοποιήσει για να παραβιάσει τελικά ολόκληρο τον domain ή το forest, χωρίς να χρειάζεται να παραβιάσει οποιονδήποτε άλλο υπολογιστή στο forest.

2.3.6 Χρήση ίδιων credentials στους τοπικούς διαχειριστές

Η χρήση του ίδιου ονόματος και κωδικού πρόσβασης στο λογαριασμού του τοπικού διαχειριστή (local Administrator) σε πολλούς ή σε όλους τους υπολογιστές επιτρέπει τη χρήση credentials που έχουν κλαπεί από τη βάση δεδομένων SAM ενός υπολογιστή για τη παραβίαση όλων των άλλων υπολογιστών που χρησιμοποιούν τα ίδια credentials. Θα πρέπει να χρησιμοποιούνται διαφορετικούς κωδικούς πρόσβασης για λογαριασμούς τοπικού διαχειριστή σε κάθε σύστημα που συνδέεται στο domain. Οι λογαριασμοί τοπικού διαχειριστή μπορεί επίσης να ονομάζονται μοναδικά, αλλά η χρήση διαφορετικών κωδικών πρόσβασης για τους προνομιακούς τοπικούς λογαριασμούς κάθε συστήματος αρκεί για να διασφαλιστεί ότι τα credentials δεν μπορούν να χρησιμοποιηθούν σε άλλα συστήματα.

2.3.7 Υπερπληθυσμός και υπερβολική χρήση ομάδων προνομιακών τομέων

Η προσθήκη ενός χρήστη στο group EA, DA ή BA σε ένα domain δημιουργεί έναν στόχο για εισβολείς. Όσο μεγαλύτερος είναι ο αριθμός των μελών αυτών των ομάδων, τόσο μεγαλύτερη είναι η πιθανότητα ότι ένας προνομιούχος χρήστης μπορεί κατά λάθος να κάνει κατάχρηση των credentials του και να αποκτηθούν από τους εισβολείς μέσω επιθέσεων κλοπής διαπιστευτηρίων. Κάθε σταθμός εργασίας ή server στον οποίο συνδέεται ένας χρήστης με προνομιούχο domain λογαριασμό, παρουσιάζει έναν πιθανό μηχανισμό με τον οποίο τα credentials του προνομιούχου χρήστη μπορούν να συλλεχθούν και να χρησιμοποιηθούν για να θέσουν σε κίνδυνο τον Active Directory domain και το forest.

2.3.8 *Κακή προστασία των Domain controllers*

Οι domain controllers στεγάζουν ένα αντίγραφο της βάσης δεδομένων AD DS ενός domain. Στην περίπτωση των read only domain controllers, το τοπικό αντίγραφο της βάσης δεδομένων περιέχει τα credentials για μόνο ένα υποσύνολο των λογαριασμών του καταλόγου, όμως από προεπιλογή, κανένας από αυτούς δεν έχει προνομιακή πρόσβαση στο domain. Σε read-write domain controllers, κάθε domain controller διατηρεί ένα πλήρες αντίγραφο της βάσης δεδομένων AD DS, συμπεριλαμβανομένων credentials όχι μόνο για προνομιούχους χρήστες όπως οι Domain Admins, αλλά και προνομιακοί λογαριασμοί όπως λογαριασμοί ελεγκτή τομέα ή ο λογαριασμός Krbtgt του τομέα, ο οποίος είναι ο λογαριασμός που σχετίζεται με την υπηρεσία KDC σε domain controllers. Εάν οι πρόσθετες εφαρμογές που δεν είναι απαραίτητες για τη λειτουργικότητα του domain controller είναι εγκατεστημένες σε domain controller ή εάν οι domain controllers δεν έχουν εφαρμόσει τα διαθέσιμα patches και δεν έχουν ασφαλιστεί με αυστηρό τρόπο, οι εισβολείς ενδέχεται να τους θέσουν σε κίνδυνο μέσω unpatched vulnerabilities ή να αξιοποιήσουν άλλους attack vectors για να εγκαταστήσουν απευθείας κακόβουλο λογισμικό.

2.3.9 *Privilege Elevation και Propagation*[5]

Ανεξάρτητα από τις μεθόδους επίθεσης που χρησιμοποιούνται, η υπηρεσία καταλόγου Active Directory είναι πάντα στοχευμένη όταν εισβολείς επιτίθενται σε ένα περιβάλλον Windows, γιατί τελικά ελέγχει την πρόσβαση σε ότι θέλουν οι εισβολείς. Αυτό όμως δεν σημαίνει ότι στοχεύεται ολόκληρος ο κατάλογος. Συγκεκριμένοι λογαριασμοί, servers και στοιχεία υποδομής είναι συνήθως οι πρωταρχικοί στόχοι επιθέσεων κατά της υπηρεσίας καταλόγου Active Directory. Αυτοί οι λογαριασμοί περιγράφονται ως εξής.

2.3.9.1 *Λογαριασμοί με μόνιμη διαχειριστική πρόσβαση*

Η εκχώρηση δικαιωμάτων και αδειών που απαιτούνται για την εκτέλεση της καθημερινής διαχείρισης σε λιγότερο προνομιούχους λογαριασμούς μέσω της ιδιότητας μέλους σε ένα ή περισσότερα από τα groups Enterprise Admins, Domain Admins ή Administrators στην υπηρεσία καταλόγου Active Directory απαιτείται μόνο προσωρινά και σπάνια σε ένα περιβάλλον που εφαρμόζει μοντέλα least privilege στην καθημερινή διαχείριση.
Οι μόνιμοι προνομιακοί λογαριασμοί είναι λογαριασμοί που έχουν τοποθετηθεί σε προνομιακές ομάδες και τελικά αφήνονται εκεί μόνιμα. Αυτοί οι λογαριασμοί αποτελούν στόχο λόγω των μόνιμων δικαιωμάτων τους τα οποία όμως, είναι συνήθως πραγματικά αναγκαία μόνο για συγκεκριμένη διαμόρφωση σε ολόκληρο το domain και για μικρές χρονικές περιόδους.

[5] Microsoft AD Security Best Practices, Privilege Elevation and Propagation

2.3.9.2 VIP λογαριασμοί

Ένας στόχος που συχνά παραβλέπεται στις παραβιάσεις της υπηρεσίας καταλόγου Active Directory είναι οι λογαριασμοί " VIP του οργανισμού. Οι προνομιακοί λογαριασμοί στοχεύονται επειδή αυτοί οι λογαριασμοί μπορούν να παραχωρήσουν πρόσβαση σε εισβολείς, κάτι που τους επιτρέπει να παραβιάσουν ή ακόμη και να καταστρέψουν τα στοχευμένα συστήματα, όπως έχει περιγραφεί και νωρίτερα.

2.3.9.3 "Privilege-Attached" λογαριασμοί

Οι "Privilege-attached" λογαριασμοί είναι οι domain λογαριασμοί που δεν έχουν γίνει μέλη οποιασδήποτε από τις ομάδες που έχουν τα υψηλότερα επίπεδα προνομίων στο Active Directory, αλλά αντ 'αυτού έχουν παραχωρηθεί υψηλά επίπεδα προνομίων σε πολλούς servers και σταθμούς εργασίας στο περιβάλλον. Αυτοί οι λογαριασμοί είναι συνήθως λογαριασμοί βάσει τομέα που έχουν ρυθμιστεί για την εκτέλεση υπηρεσιών σε συστήματα που συνδέονται με τομέα, συνήθως για εφαρμογές που εκτελούνται σε μεγάλα τμήματα της υποδομής. Παρόλο που αυτοί οι λογαριασμοί δεν έχουν προνόμια στην υπηρεσία καταλόγου του Active Directory, εάν τους δοθεί υψηλό προνόμιο σε μεγάλο αριθμό συστημάτων, μπορούν να χρησιμοποιηθούν για να παραβιαστεί ή ακόμη και να καταστραφεί μεγάλο τμήμα της υποδομής, επιτυγχάνοντας το ίδιο αποτέλεσμα με τη παραβίαση ενός προνομιούχου λογαριασμού Active Directory.

2.4 Μείωση της επιφάνειας επίθεσης

Η μείωση της επιφάνειας επίθεσης στο Active Directory περιλαμβάνει τις εξής πληροφορίες

- Εφαρμογή του μοντέλου διαχείρισης "Least-Privilege".
- Δημιουργία ασφαλών συστημάτων ειδικά για τη χρήση από διαχειριστικούς χρήστες.
- Ασφάλιση των Domain Controllers εναντίων επιθέσεων.

Προτού αναφερθούμε στην εφαρμογή του μοντέλου "Least-Privilege" θα πρέπει να αποσαφηνιστεί η αρχική παραμετροποίηση και οι αρχικές δυνατότητες των περισσότερο προνομιούχων από τα προϋπάρχοντα groups στο Active Directory. Πριν από τη λεπτομερή αναφορά στο καθένα θα πρέπει να σημειωθεί ότι το Active Directory υποστηρίζει το μοντέλο least-privilege στο διαμοιρασμό δικαιωμάτων και αδειών. Ένας «κανονικός» χρήστης έχει δικαίωμα να διαβάσει αρκετές από τις πληροφορίες που αποθηκεύονται στο Active Directory αλλά περιορίζεται πολύ στα δεδομένα που μπορεί να αλλάξει σε αυτό. Οι χρήστες που χρειάζεται να έχουν περισσότερα δικαιώματα πρέπει να είναι μέλη σε διάφορα προνομιούχα groups για να εκτελέσουν τις εργασίες του ρόλου τους και δεν μπορούν να εκτελέσουν εργασίες που δεν εμπίπτουν στον ρόλο τους. Ένας οργανισμός μπορεί να δημιουργήσει νέα groups που δίνουν στους εργαζομένους τα ακριβώς συγκεκριμένα δικαιώματα που χρειάζονται ανάλογα με τη θέση εργασίας τους, χωρίς να έχουν πρόσβαση και δικαιώματα όπου δεν είναι αναγκαίο.

2.4.1 Active Directory groups με τα περισσότερα δικαιώματα

Τα groups με τα περισσότερα δικαιώματα στο Active Directory καθώς και τα συγκεκριμένα δικαιώματα και ιδιότητες που έχει το καθένα, είναι τα εξής:

2.4.1.1 *Enterprise Admins*

Οι Enterprise Admins (EA) είναι ένα group που υπάρχει μόνο στο root domain του Active Directory forest και από προεπιλογή είναι μέλος του Administrators group σε όλα τα domains στο σύμπλεγμα δομών. Ο built-in Administrator στο root domain του forest είναι το μόνο προεπιλεγμένο μέλος της ομάδας EA. Στους EA παραχωρούνται δικαιώματα και άδειες που τους επιτρέπουν να εφαρμόζουν αλλαγές σε ολόκληρο το forest (δηλαδή, αλλαγές που επηρεάζουν όλα τα domains του forest), όπως προσθήκη ή κατάργηση domain, δημιουργία εμπιστοσύνης μεταξύ forests ή αύξηση λειτουργικών επιπέδων του forest. Σε ένα σωστά σχεδιασμένο και εφαρμοσμένο μοντέλο ανάθεσης, η συμμετοχή στην EA απαιτείται μόνο κατά την πρώτη κατασκευή του forest ή κατά την πραγματοποίηση ορισμένων αλλαγών σε ολόκληρο το forest, όπως η δημιουργία εμπιστοσύνης προς ένα forest (outbound forest trust). Τα περισσότερα από τα δικαιώματα και τις άδειες που παρέχονται στο group EA μπορούν να ανατεθούν σε λιγότερο προνομιούχους χρήστες και groups.

2.4.1.2 Domain Admins

Κάθε domain σε ένα forest έχει το δικό του Domain Admins (DA) group, το οποίο είναι μέλος του Administrators group αυτού του domain και μέλος του local Administrators group σε κάθε υπολογιστή που είναι συνδεδεμένος στον domain. Το μόνο προεπιλεγμένο μέλος του group DA για έναν domain είναι ο built-in Administrator για αυτόν τον domain. Οι DA είναι "πανίσχυροι" στους domains τους, ενώ οι EA έχουν προνόμια σε ολόκληρο το Active Directory forest. Σε ένα σωστά σχεδιασμένο και υλοποιημένο μοντέλο ανάθεσης, η συμμετοχή στους Domain Admins θα πρέπει να απαιτείται μόνο σε σενάρια "break glass" (όπως καταστάσεις στις οποίες απαιτείται λογαριασμός με υψηλά επίπεδα προνομίων σε κάθε υπολογιστή του domain) Παρόλο που οι εγγενείς μηχανισμοί ανάθεσης του Active Directory επιτρέπουν την ανάθεση στο βαθμό που είναι δυνατή η χρήση λογαριασμών DA μόνο σε σενάρια έκτακτης ανάγκης, η κατασκευή ενός αποτελεσματικού μοντέλου ανάθεσης μπορεί να είναι χρονοβόρα και πολλοί οργανισμοί αξιοποιούν εργαλεία τρίτων για να επισπεύσουν τη διαδικασία.

2.4.1.3 Administrators

Το τρίτο group, είναι η ενσωματωμένη ομάδα τοπικών διαχειριστών *built-in local Administrators* (BA) στο οποίο είναι εμφωλευμένοι οι DA και οι EA. Σε αυτό το group παρέχονται πολλά από τα άμεσα δικαιώματα και δικαιώματα στον κατάλογο (directory) και στους domain controllers. Ωστόσο, η ομάδα διαχειριστών για έναν domain δεν έχει δικαιώματα σε member servers ή σε σταθμούς εργασίας. Με την ιδιότητα μέλους στην τοπική ομάδα διαχειριστών των υπολογιστών χορηγείται τοπικό προνόμιο.

2.4.1.4 Schema Admins

Ένα τέταρτο προνομιακή group, οι Schema Admins (SA), υπάρχει μόνο στο forest root domain και έχει μόνο τον built-in Administrator αυτού του domain ως προεπιλεγμένο μέλος, παρόμοιο με την ομάδα Enterprise Admins. Το group των Scheme Admins προορίζεται να συμπληρώνεται μόνο προσωρινά και περιστασιακά (όταν απαιτείται τροποποίηση του σχήματος AD DS).
Παρόλο που το group SA είναι το μόνο που μπορεί να τροποποιήσει το Active directory schema (δηλαδή, τις υποκείμενες δομές δεδομένων του καταλόγου, όπως αντικείμενα και χαρακτηριστικά), το πεδίο εφαρμογής των δικαιωμάτων και των δικαιωμάτων του group SA είναι πιο περιορισμένο από αυτά που περιγράφηκαν προηγουμένως. Είναι επίσης σύνηθες να διαπιστώνουμε ότι οι οργανισμοί έχουν αναπτύξει κατάλληλες πρακτικές για τη διαχείριση της συμμετοχής στο group SA, επειδή η συμμετοχή σε αυτό είναι συνήθως σπάνια απαιτείται και μόνο για σύντομα χρονικά διαστήματα. Αυτό ισχύει τεχνικά για τα groups EA, DA και BA στο Active Directory, αλλά είναι σπάνιο ένας οργανισμός να έχει εφαρμόσει παρόμοιες πρακτικές για αυτές τις ομάδες όπως και για την ομάδα SA.

2.4.2 Protected Accounts και Protected Groups

Στο Active Directory, ένα προεπιλεγμένο σύνολο προνομιακών λογαριασμών και ομάδων που ονομάζονται "προστατευμένοι" λογαριασμοί και ομάδες προστατεύονται διαφορετικά από άλλα αντικείμενα του καταλόγου. Οποιοσδήποτε λογαριασμός έχει άμεση ή μεταβατική ιδιότητα μέλους σε οποιαδήποτε προστατευμένη ομάδα (ανεξάρτητα από το αν η ιδιότητα προέρχεται από ομάδες ασφαλείας ή ομάδες διανομής) κληρονομεί αυτήν την περιορισμένη ασφάλεια. Για παράδειγμα, αν ένας χρήστης είναι μέλος ενός distribution group που, με τη σειρά του, είναι μέλος ενός protected group στο Active Directory, αυτό το αντικείμενο χρήστη επισημαίνεται ως protected account. Όταν ένας λογαριασμός επισημαίνεται ως προστατευμένος, η τιμή του χαρακτηριστικού adminCount στο αντικείμενο ορίζεται σε 1.

2.4.2.1 AdminSDHolder και SDProp

Στο System container κάθε domain του Active Directory, δημιουργείται αυτόματα ένα αντικείμενο που ονομάζεται AdminSDHolder. Ο σκοπός του αντικειμένου AdminSDHolder είναι να διασφαλίσει ότι τα δικαιώματα σε προστατευόμενους λογαριασμούς και ομάδες εφαρμόζονται με συνέπεια, ανεξάρτητα από το πού βρίσκονται οι προστατευμένες ομάδες και λογαριασμοί στον τομέα. Κάθε 60 λεπτά (από προεπιλογή), μια διαδικασία γνωστή ως Security Descriptor Propagator (SDProp) εκτελείται στον domain controller που έχει το ρόλο του PDC Emulator του domain. Το SDProp συγκρίνει τα δικαιώματα στο αντικείμενο AdminSDHolder του domain με τα δικαιώματα στους προστατευόμενους λογαριασμούς και ομάδες του domain. Εάν τα δικαιώματα σε οποιονδήποτε από τους προστατευμένους λογαριασμούς και ομάδες δεν ταιριάζουν με τα δικαιώματα στο αντικείμενο AdminSDHolder, τα δικαιώματα στους προστατευμένους λογαριασμούς και ομάδες επαναφέρονται για να ταιριάζουν με αυτά του αντικειμένου AdminSDHolder του domain.
Η μεταβίβαση δικαιωμάτων είναι απενεργοποιημένη σε προστατευμένες ομάδες και λογαριασμούς, πράγμα που σημαίνει ότι ακόμη και αν οι λογαριασμοί ή οι ομάδες μετακινηθούν σε διαφορετικές τοποθεσίες στον κατάλογο, δεν κληρονομούν δικαιώματα από τα νέα γονικά τους αντικείμενα. Η κληρονομικότητα είναι επίσης απενεργοποιημένη στο αντικείμενο AdminSDHolder, ώστε οι αλλαγές δικαιωμάτων στα γονικά αντικείμενα να μην αλλάζουν τα δικαιώματα του AdminSDHolder.

2.4.2.1.1 Ιδιοκτησία AdminSDHolder

Τα περισσότερα αντικείμενα στο Active Directory ανήκουν στην ομάδα BA του domain. Ωστόσο, το αντικείμενο AdminSDHolder ανήκει, από προεπιλογή, στο group DA του domain. (Αυτή είναι μια περίπτωση κατά την οποία οι DA δεν αποκτούν τα δικαιώματα και τις άδειές τους μέσω της ιδιότητας μέλους στο group Administrators για τον domain.)
Σε εκδόσεις των Windows νωρίτερα από τον Windows Server 2008, οι κάτοχοι ενός αντικειμένου μπορούν να αλλάξουν δικαιώματα του αντικειμένου, συμπεριλαμβανομένης της εκχώρησης δικαιωμάτων που δεν είχαν αρχικά. Επομένως, τα προεπιλεγμένα δικαιώματα σε ένα αντικείμενο AdminSDHolder ενός domain εμποδίζουν τους χρήστες που είναι μέλη των groups BA ή EA να αλλάζουν τα

δικαιώματα για ένα αντικείμενο AdminSDHolder ενός τομέα. Ωστόσο, τα μέλη του Administrators group για τον domain μπορούν να αναλάβουν την ιδιοκτησία του αντικειμένου και να παραχωρήσουν πρόσθετα δικαιώματα, πράγμα που σημαίνει ότι αυτή η προστασία είναι στοιχειώδης και προστατεύει το αντικείμενο μόνο από τυχαία τροποποίηση από χρήστες που δεν είναι μέλη του group DA στο domain. Επιπλέον, τα groups BA και EA (κατά περίπτωση) έχουν άδεια να αλλάξουν τα χαρακτηριστικά του αντικειμένου AdminSDHolder στον local domain (root domain για τα μέλη του EA).

2.4.3 Εφαρμογή μοντέλων "Least-Privilege"[6]

Είναι σύνηθες σε ένα περιβάλλον Active Directory να υπάρχει μεγάλο ποσοστό λογαριασμών με δικαιώματα που ξεπερνούν κατά πολύ τα αναγκαία για τις καθημερινές εργασίες του εκάστοτε χρήστη. Πλην ελαχίστων εξαιρέσεων και ασχέτως των διαθέσιμων εργαλείων και ικανοτήτων, οι εισβολείς ακολουθούν το «μονοπάτι της λιγότερης αντίστασης». Αυτό σημαίνει ότι προσπαθούν να παραβιάσουν τα συστήματα που στοχεύουν χρησιμοποιώντας τη μικρότερη δυνατόν πολυπλοκότητα και την αυξάνουν μόνο όταν οι απλούστεροι μηχανισμοί και τεχνικές αποτύχουν. Η χορήγηση αυξημένων δικαιωμάτων δεν είναι απαραίτητα λάθος, όπως όταν για παράδειγμα οι χρήστες των υπαλλήλων που εργάζονται ως μηχανικοί στο Active Directory έχουν δικαιώματα διαχειριστή ώστε να μπορούν να εκτελούν τις απαραίτητες για την θέση τους εργασίες. Όμως η μόνιμη χορήγηση περισσότερων από τα αναγκαία δικαιώματα σε πολλαπλούς χρήστες αυξάνει κατά πολύ την πιθανή κρισιμότητα επίθεσης του Active Directory καθώς αυξάνεται η πιθανότητα ένας εισβολέας που αποκτά πρόσβαση σε ένα domain account, να καταλήξει να έχει πρόσβαση σε χρήστη με διαχειριστικά δικαιώματα και έτσι να έχει τη δυνατότητα να εισχωρήσει βαθύτερα, παραβιάζοντας περισσότερους λογαριασμούς ή και ολόκληρη την υποδομή Active Directory του οργανισμού.

2.4.3.1 Εφαρμογή στο Active Directory

Στο Active Directory είναι συχνό φαινόμενο να υπάρχουν περισσότεροι από όσους χρειάζεται χρήστες στα groups EA, DA και BA. Συνήθως στους EA υπάρχουν οι λιγότεροι χρήστες, στους DA είναι κάποιο πολλαπλάσιο των EA και οι Administrators είναι περισσότεροι από ότι το άθροισμα των χρηστών των EA και DA. Αυτό γίνεται λόγω της κοινή πεποίθησης ότι οι Administrators έχουν "λιγότερα δικαιώματα" από τους EA και DA, ενώ στην πραγματικότητα κάθε χρήστης που είναι μέλος ενός από αυτά τα group μπορεί να κάνει τον εαυτό του μέλος και των άλλων δύο. Ακολουθούν αναλυτικά μέτρα ελέγχου των δικαιωμάτων και εφαρμογής του μοντέλου least privilege σε κάθε ένα από τα groups BA, EA και DA.

[6] Implementing Least-Privilege Administrative Models

2.4.3.1.1 Built in Administrator

Κατά την δημιουργία κάθε domain δημιουργείται ένας λογαριασμός Administrator, ο οποίος είναι μέλος των Domain Admins και Administrator groups, αν το domain αποτελεί είναι ταυτόχρονα και forest root domain τότε ανήκει και στο group των Enterprise Admins. η χρήση αυτού του λογαριασμού θα πρέπει να περιορίζεται στην αρχική δημιουργία του domain και σε σενάρια disaster recovery.

Μέτρα για την προστασία του Built-in Administrator[7]

Ο σκοπός κατά την υλοποίηση αυτών των ρυθμίσεων είναι να εμποδιστεί ο συγκεκριμένος λογαριασμός απο το να είναι διαθέσιμος προς χρήση, εκτός αν τα μέτρα που έχουν υλοποιηθεί για την προστασία του έχουν αντιστραφεί. Υλοποιώντας τα παρακάτω μέτρα και παρακολουθώντας το Administrator λογαριασμό για αλλαγές, μειώνεται σημαντικά η πιθανότητα μιας επιτυχημένης επίθεσης χρησιμοποιώντας τον συγκεκριμένο λογαριασμό.
Για τον λογαριασμό Administrator κάθε Domain στο Forest θα πρέπει να εκτελεστούν οι παρακάτω ενέργειες.

- Ενεργοποίηση της επιλογής **"*Account is sensitive and cannot be delegated*"**
  Έτσι ο συγκεκριμένος λογαριασμός δεν θα μπορεί να κάνει delegate, δηλαδή δεν θα είναι δυνατό να χρησιμοποιήσει τα credentials του ώστε να συνδεθεί σε άλλο σύστημα του domain, είτε ως service είτε ως υπολογιστής. Έτσι γίνονται αδύνατες οι επιθέσεις που χρησιμοποιούν τα credentials του συγκεκριμένου λογαριασμού σε άλλα συστήματα.

- Ενεργοποίηση της επιλογής **" *Smart card is required for interactive logon*"**
  Όταν ενεργοποιείται αυτή η ρύθμιση το συνθηματικό του χρήστη αλλάζει σε ένα νέο τυχαίο 120 χαρακτήρων. Έτσι εξασφαλίζεται ότι ο κωδικός είναι όχι μόνο αρκετά σύνθετος αλλά και ταυτόχρονα άγνωστος σε όλους τους χρήστες.

Η ενεργοποίηση της χρήσης Smart card αλλάζει τον κωδικό του χρήστη αλλά δεν αποτρέπει έναν χρήστη με τα απαραίτητα δικαιώματα από το να θέσει έναν άλλο γνωστό κωδικό και στη συνέχεια χρησιμοποιώντας το username και τον νέο κωδικό να αποκτήσει πρόσβαση στον λογαριασμό Administrator και τα δικαιώματα του. Για αυτό τον λόγο θα πρέπει να υλοποιηθούν κάποια περεταίρω μέτρα. Παρότι τα συγκεκριμένα μέτρα μπορούν να αντιστραφούν, ο σκοπός τους είναι να καθυστερήσουν την πρόοδο ενός επιτηθέμενου και να περιορίσουν τη "ζημιά" που θα μπορεί να προκαλέσει ο συγκεκριμένος λογαριασμός.

[7] Microsoft, Implementing least privilege model: Securing Built-in Administrator Accounts

Με μια ή περισσότερες group policies θα πρέπει να εφαρμόζονται τα παρακάτω

- απαγορεύεται η πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
- απαγορεύεται το log on as a batch job
- απαγορεύεται το log on as a service
- απαγορεύεται το log on μέσω πρωτοκόλλου Remote Desktop (RDP)

Αυτά τα μέτρα θα πρέπει να ισχύουν σε κάθε συστημα που είναι μέλος του domain καθώς και στους domain controllers.

Επιπλέον αφου θα έχει ασφαλιστεί ο Administrator λογαριασμός και έχει απενεργοποιηθεί σε κάθε domain, θα πρέπει να παραμετροποιηθεί το auditing ώστε να παρακολουθούνται αλλαγές σε αυτόν. Οι αλλαγές αυτές μπορεί να είναι η ενεργοποίηση του, αλλαγή στο συνθηματικό του ή οποιαδήποτε άλλη αλλαγή στον λογαριασμό.

2.4.3.1.2 Enterprise Admins group[8]

Το group Enterprise Admins, που βρίσκεται στο root domain του forest, δεν θα πρέπει να περιέχει χρήστες σε καθημερινή βάση, με πιθανή εξαίρεση τον τοπικό λογαριασμό διαχειριστή του τομέα, υπό την προϋπόθεση ότι είναι ασφαλής όπως περιγράφηκε προηγουμένως. Όταν χρειάζεται πρόσβαση EA, οι χρήστες των οποίων οι λογαριασμοί απαιτούν EA δικαιώματα θα πρέπει να γίνονται προσωρινά μέλη του EA group. Με την ολοκλήρωση των αλλαγών που απαιτούν αυτά τα δικαιώματα οι χρήστες θα πρέπει να αφαιρούνται απο το EA group.

Το group Enterprise Admins είναι από προεπιλογή μέλος του built-in Adminstrators group. Η αφαίρεση του EA group από τα Administrators groups δεν αποτελεί σωστή αλλαγή καθώς τα EA δικαιώματα είναι πιθανό να χρειαστούν σε περίπτωση disaster-recovery στο Active Directory Forest. Αν το EA group έχει αφαιρεθεί από το Administrators group του forest, θα πρέπει να προστεθεί στο Administrators group του κάθε domain και τα ακόλουθα μέτρα θα πρέπει να υλοποιηθούν.

- Το Enterprise Admins group θα πρέπει να μην περιέχει κανέναν χρήστη σε καθημερινή βάση, με την εξαίρεση του λογαριασμού built-in Administrator του forest root domain, το οποίο θα πρέπει να είναι προστατευμένο με τα μέτρα που περιγράφηκαν νωρίτερα.
- Σε group policies που είναι συνδεδεμένες με OUs που περιέχουν member servers και workstations από κάθε domain, στο EA group θα πρέπει να εφαρμοστούν τα παρακάτω δικαιώματα:
    - απαγορεύεται η πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
    - απαγορεύεται το log on as a batch job
    - απαγορεύεται το log on as a service
    - απαγορεύεται το τοπικό log on
    - απαγορεύεται το log on μέσω πρωτοκόλλου Remote Desktop (RDP)

[8] Microsoft, Implementing least privilege model: Securing Enterprise Admin groups

2.4.3.1.3 Domain Admins group[9]

Όπως και με το EA group, το Domain Admins group θα πρέπει να χρειάζεται μόνο κατά την δημιουργία του domain και σε περίπτωση disaster-recovery. Δεν θα πρέπει να υπάρχουν μόνιμα μέλη αυτού του group με εξαίρεση τον Administrator σε κάθε domain, όπως έχει περιγραφεί νωρίτερα. Όταν χρειάζεται πρόσβαση με DA δικαιώματα, οι χρήστες των οποίων οι λογαριασμοί απαιτούν DA δικαιώματα θα πρέπει να γίνονται προσωρινά μέλη του DA group και με την ολοκλήρωση των αλλαγών που απαιτούν αυτά τα δικαιώματα οι χρήστες θα πρέπει να αφαιρούνται πλέον από το DA group.

Οι Domain Admins είναι από προεπιλογή μέλη του τοπικού Administrators group σε όλους τους member servers και τα workstations του εκάστοτε domain. Η συγκεκριμένη συσχέτιση μεταξύ των δύο groups δεν θα πρέπει να τροποποιείται καθώς επηρεάζει την δυνατοτητα υποστηριξης και τις επιλογές σε περίπτωση disaster recovery. Αν το Domain Admins group έχει αφαιρεθεί από τους τοπικούς Administrators στους member servers, θα πρέπει να προστεθούν στο Administrators group σε κάθε member server και workstation του domain μέσω group policy. Τα ακόλουθα μέτρα θα πρέπει να υλοποιηθούν για το domain admins group σε κάθε domain του ενός forest

1. Αφαίρεση όλων των μελών του DA group, με πιθανή εξαίρεση τον built-in Administrator του domain όπως αναφέρθηκε νωρίτερα.
2. Μέσω μιας ή περισσότερων group policies που εφαρμόζονται σε στους member servers και τα workstations κάθε domain, το DA group θα πρέπει να παραμετροποιηθεί ώστε να

    - απαγορεύεται η πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
    - απαγορεύεται το log on as a batch job
    - απαγορεύεται το log on as a service
    - απαγορεύεται το τοπικό log on
    - απαγορεύεται το log on μέσω πρωτοκόλλου Remote Desktop (RDP)

Έτσι θα αποτραπούν τα μέλη του DA group απο το να συνδεθούν σε member servers και workstations. Αν χρησιμοποιούνται jump servers για τη διαχείριση των domain controllers και το Active Directory, θα πρέπει αυτοί να είναι μέλη ενός OU το οποίο θα εξαιρείται από τα παραπάνω group policies.

3. Το auditing θα πρέπει να παραμετροποιηθεί ώστε να στέλνει ειδοποιήσεις σε περίπτωση τροποποίησης των ιδιοτήτων ή των μελών του DA group. Αυτές οι ειδοποιήσεις θα πρέπει να στέλνονται κατ' ελάχιστο στους χρήστες και τις ομάδες που είναι υπεύθυνες για τη διαχείριση των Active Directory Domain Services (AD DS), καθώς και την ομάδα incident response. Διαδικασίες θα πρέπει να δημιουργηθούν για την προσωρινή προσθήκη στο DA group περιλαμβάνοντας και διαδικασία ειδοποίησης όταν η προσθήκη στο group είναι θεμιτή.

[9] Microsoft, Implementing least privilege model: Securing Domain Admins Groups

2.4.3.1.4 Administrators group[10]

Όπως ήδη αναφέρθηκε στα EA και DA groups, τα δικαιώματα του Administrators group (BA) πρέπει να δίνονται μόνο σε σενάρια δημιουργίας του domain ή αποκατάστασης καταστροφής (disaster recovery). Δεν πρέπει να υπάρχουν λογαριασμοί ως μόνιμα μέλη του group με εξαίρεση τον τοπικό διαχειριστή του domain, εφόσον έχει ασφαλιστεί όπως περιγράφεται νωρίτερα (Built in Administrator).

Όταν χρειάζονται τα δικαιώματα του group Administrators, θα πρέπει να προσθέτονται προσωρινά μέλη στο group του domain που χρειάζεται, τα οποία θα αφαιρούνται μόλις ολοκληρωθούν.

Τα μέλη του Administrators group είναι από προεπιλογή κάτοχοι των περισσότερων αντικειμένων του AD DS στα αντίστοιχα domains. Η συμμετοχή σε αυτό το group ενδέχεται να απαιτείται σε σενάρια κατασκευής και ανάκτησης καταστροφών στα οποία απαιτείται η ιδιοκτησία ή η ικανότητα ανάληψης ιδιοκτησίας αντικειμένων. Επιπλέον, οι DA και οι EA κληρονομούν έναν αριθμό από τα δικαιώματα και τις άδειές τους λόγω της προεπιλεγμένης συμμετοχής τους στο Administrators group. Η προεπιλεγμένη ένθεση των groups για προνομιούχες ομάδες στην υπηρεσία καταλόγου Active Directory δεν θα πρέπει να τροποποιείται και κάθε Administrators group κάθε domain θα πρέπει να ασφαλίζεται όπως περιγράφεται στις οδηγίες παρακάτω.

1. Καταργήστε όλα τα μέλη από την ομάδα διαχειριστών, με πιθανή εξαίρεση τον τοπικό λογαριασμό διαχειριστή για τον τομέα, υπό την προϋπόθεση ότι έχει ασφαλιστεί όπως περιγράφεται στο Παράρτημα Δ: Ασφάλεια ενσωματωμένων λογαριασμών διαχειριστή στην υπηρεσία καταλόγου Active Directory.

2. Τα μέλη της ομάδας διαχειριστών του τομέα δεν θα πρέπει ποτέ να χρειάζεται να συνδεθούν σε member servers και workstations. Σε ένα ή περισσότερα GPO που συνδέονται με OU τα workstations και τους member servers κάθε domain, το Administrators group θα πρέπει να παραμετροποιηθεί ώστε να

   - απαγορεύεται η πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
   - απαγορεύεται το log on as a batch job
   - απαγορεύεται το log on as a service

   Αυτό θα αποτρέψει τη χρήση των μελών του group Administrators για σύνδεση σε member servers ή workstations (εκτός αν παραβιαστούν πρώτα πολλά στοιχεία ελέγχου), όπου τα διαπιστευτήριά τους θα μπορούσαν να αποθηκευτούν στην προσωρινή μνήμη και ως εκ τούτου να παραβιαστούν. Ένας προνομιακός λογαριασμός δεν πρέπει ποτέ να χρησιμοποιείται για τη

[10] Microsoft, Implementing least privilege model: Securing Administrators Groups

σύνδεση σε ένα λιγότερο προνομιούχο σύστημα και η επιβολή αυτών των ελέγχων παρέχει προστασία έναντι ενός αριθμού επιθέσεων.

3. Στους domain controllers OU σε κάθε domain στο forest, στο group Administrators θα πρέπει να εκχωρηθούν τα ακόλουθα δικαιώματα χρήστη (εάν δεν έχουν ήδη αυτά τα δικαιώματα), τα οποία θα επιτρέψουν στα μέλη της ομάδας Administrators να εκτελούν τις απαραίτητες λειτουργίες για Σενάριο αποκατάστασης καταστροφών σε όλο το forest:
    - Πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
    - Να επιτρέπεται η σύνδεση τοπικά
    - Να επιτρέπεται η σύνδεση μέσω των Υπηρεσιών απομακρυσμένης επιφάνειας εργασίας

4. Ο έλεγχος θα πρέπει να διαμορφωθεί έτσι ώστε να στέλνει ειδοποιήσεις εάν πραγματοποιηθούν τροποποιήσεις στις ιδιότητες ή τη συμμετοχή στην ομάδα Administrators. Αυτές οι ειδοποιήσεις θα πρέπει να αποστέλλονται, τουλάχιστον, στα μέλη της ομάδας που είναι υπεύθυνη για τη διαχείριση του AD DS. Θα πρέπει επίσης να αποστέλλονται ειδοποιήσεις στα μέλη της ομάδας ασφαλείας και θα πρέπει να καθοριστούν διαδικασίες για την τροποποίηση της ιδιότητας μέλους της ομάδας Administrators. Συγκεκριμένα, αυτές οι διεργασίες θα πρέπει να περιλαμβάνουν μια διαδικασία με την οποία η ομάδα ασφαλείας ειδοποιείται όταν πρόκειται να τροποποιηθεί η ομάδα διαχειριστών, έτσι ώστε όταν αποστέλλονται ειδοποιήσεις, να αναμένονται και να μην ακούγεται συναγερμός. Επιπλέον, θα πρέπει να εφαρμοστούν διαδικασίες για την ειδοποίηση της ομάδας ασφαλείας όταν η χρήση της ομάδας διαχειριστών έχει ολοκληρωθεί και οι λογαριασμοί που χρησιμοποιούνται έχουν αφαιρεθεί από την ομάδα.

2.4.3.1.5 Member Servers

Ανακτώντας τους λογαριασμούς που ανήκουν στους local Administrators των member servers συνήθως βρίσκονται πολλοί τοπικοί και domain λογαριασμοί και αρκετά groups, με αποτέλεσμα το πλήθος των local Administrators να είναι αυξημένο στους servers. Σε πολλές περιπτώσεις domain groups με μεγάλο αριθμό μελών είναι εμφωλευμένα μέλη των local Administrators, χωρίς να λαμβάνεται υπόψη ότι κάθε ένας από αυτούς τους χρήστες μπορεί να ασκήσει διαχειριστικό έλεγχο σε όλα τα συστήματα που ανήκουν στο group.

2.4.3.1.6 Workstations

Παρότι τα workstations έχουν κατα κανόνα σημαντικά λιγότερους χρήστες στο local administrators group σε σχέση με τους member servers, σε πολλά περιβάλλοντα οι χρήστες έχουν διαχειριστικά δικαιώματα στους προσωπικούς υπολογιστες τους. Όταν συμβαίνει αυτό, ακόμα και αν το UAC (User Account Control) είναι ενεργοποιημένο, οι χρήστες αποτελούν αυξημένο ρίσκο ώς προς την ακεραιότητα των workstations.

2.4.3.1.7 Μέτρα για την προστασία του Local Administrator[11]

Οι λογαριασμοί των Local Administrators θα πρέπει να παραμένουν απενεργοποιημένοι, αποφεύγοντας έτσι την επίθεση Pass-the-Hash και άλλες επιθέσεις που χρησιμοποιούν τα credentials του local administrator. Ταυτόχρονα θα πρέπει μέσω group policy να

- απαγορεύεται η πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου
- απαγορεύεται το log on as a batch job
- απαγορεύεται το log on as a service
- απαγορεύεται το log on μέσω πρωτοκόλλου Remote Desktop (RDP)

Με τις παραπάνω ρυθμίσεις εξασφαλίζεται ότι ο Local Administrator δεν θα μπορεί να χρησιμοποιηθεί σε άλλους υπολογιστές ακόμα και αν κατά λάθος ή επίτηδες έχει ενεργοποιηθεί.

2.4.3.1.8 Εφαρμογή στις εφαρμογές

Σε επιθέσεις που έχουν ως στόχο την πρόσβαση στη πνευματική ιδιοκτησία ενός οργανισμού, λογαριασμοί που έχουν “ισχυρα” δικαιώματα σε εφαρμογές μπορούν να στοχοποιηθούν ώστε να αποκτηθούν τα συγκεκειμένα δεδομένα. σε μορφή εγγράφων και άλλων αρχείων, οι επιτηθέμενοι στοχοποιούν λογαριασμούς ή/και groups που έχουν πρόσβαση στα συγκεκριμένα αρχεία. Για παράδειγμα αν σε έναν file server υπάρχουν αρχεία συμβολαίων και η πρόσβαση σε αυτά τα αρχεία γίνεται μέσω ενός Active Directory group, τότε ο επιτηθέμενος θα προσπαθήσει να προσθέσει σε αυτό το group κάποιο παραβιασμένο λογαριασμό ώστε να αποκτήσει πρόσβαση σε αυτά.

[11] Securing Local Administrator Accounts on Workstations and Member Servers

3. Αξιολόγηση ασφαλείας στο Active Directory

Η αξιολόγηση της ασφάλειας σε ένα περιβάλλον Active Directory γίνεται με βάση τα υπάρχοντα τρωτά σημεία που μπορεί να εκμεταλλευτεί ένας κακόβουλος εσωτερικός ή εξωτερικός χρήστης. Τα τρωτά σημεία που συναντώνται συχνότερα και οδηγούν σε παραβίαση ενός Active Directory εξετάζονται στην παρούσα εργασία και αναφέρονται αναλυτικά παρακάτω.

3.1 Δημοφιλή τρωτά σημεία στο Active Directory

Οι επιθέσεις στο Active Directory δεν περιορίζονται σε ένα σημείο. Οι επιτιθέμενοι στοχεύουν σε κενά ασφαλείας και κακές πρακτικές στο configuration ολόκληρου του οικοσυστήματος των Windows. Παλιό και πλέον μη υποστηριζόμενο λογισμικό, με γνωστές ευπάθειες, περισσότερα από όσα χρειάζονται δικαιώματα, αδύναμα passwords σε λογαριασμούς με διαχειριστικά δικαιώματα είναι τα δημοφιλέστερα τρωτά σημεία ενός Active Directory. Συχνά ένα κενό ασφαλείας δεν είναι αρκετό για να υπάρξει παραβίαση της ασφάλειας του Active Directory αλλά ο συνδυασμός πολλαπλών κενών είναι.

Η παρακάτω λίστα περιλαμβάνει ελέγχους που υλοποιήθηκαν και όταν πληρούνται, η ασφάλεια ενός περιβάλλοντος Active Directory αυξάνεται σημαντικά, χωρίς τη χρήση εξωτερικού (third party) λογισμικού. Έτσι, εξαιρώντας τη χρήση zero day vulnerabilities, οι πιθανές επιθέσεις που μπορούν να πραγματοποιηθούν μειώνεται, ενώ η πολυπλοκότητα και ο βαθμός εξειδίκευσης που απαιτείται για να πραγματοποιηθούν αυξάνονται εξίσου σημαντικά.

3.2 Έλεγχοι ασφαλείας

3.2.1 Χρήση fine grained password policy, μέσω group policy.

Με τη χρήση του fine grained password policy μπορούν να υπάρχουν πολλαπλές διαφορετικές πολιτικές για τα passwords και να κατανέμονται ανάλογα με την απαιτούμενη πολυπλοκότητα και διάρκεια εφαρμογής τους στους κατάλληλους χρήστες ανάλογα με την σημαντικότητα τους (πόσο επικίνδυνο είναι να αποκτήσει κάποιος κακόβουλος πρόσβαση). Χωρίς εφαρμοσμένη πολιτική για τη πολυπλοκότητα και τη λήξη των κωδικών μετά από κάποιο προκαθορισμένο χρονικό διάστημα επιθέσεις όπως password spraying, brute force είναι εύκολα εφαρμόσιμες.
- Normal Users: 14 characters
- Privileged Users: 18 characters
- Service accounts(with SPNs): 25 characters

3.2.2 Χρήση του LAPS (Local Administrator Password Solution)

Το LAPS είναι ένα μια ενσωματωμένη λειτουργία του Active Directory που επιτρέπει αυτοματοποιημένη αλλαγή των passwords στους local Administrator λογαριασμούς των υπολογιστών του Domain σε ένα Active Directory. Οι κωδικοί αυτοί αποθηκεύονται στο confidential attribute του αντίστοιχου υπολογιστή στο Active Directory Αυτή η

αυτοματοποιημένη λύση διευκολύνει τη διαχείριση αυτών των κωδικών και αποτρέπει τη χρήση του ίδιου password σε πολλαπλά μηχανήματα. Τέλος μειώνει σημαντικά τις επιπτώσεις μιας παραβίασης σε υπολογιστή που ανήκει στο Domain του συγκεκριμένου Active Directory.

3.2.3 Απενεργοποίηση NBT-NS, μέσω group policy

Το πρωτόκολλο NBT-NS χρησιμοποιείται από το λειτουργικό σύστημα Windows για την εύρεση της διεύθυνση IP ενός υπολογιστή γνωρίζοντας το hostname του. Λόγω της έλλειψης επαλήθευσης της προέλευσης των απαντήσεων η χρήση αυτού του πρωτοκόλλου ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί NBT-NS ερωτήματα και να μέσω της επίθεσης NBT-NS poisoning να αποκτήσει τον κωδικό πρόσβασης του χρήστη που έκανε το ερώτημα. Υπάρχουν αυτοματοποιημένα εργαλεία (responder) που κάνουν την εκτέλεση αυτής της επίθεσης απλή ακόμα και για αρχάριους χρήστες. Απενεργοποιώντας το NTB-NS μειώνεται η επιφάνεια επίθεσης στο εκάστοτε περιβάλλον Active Directory. Ο συγκεκριμένος έλεγχος επιβεβαιώνει την ύπαρξη group policy που απενεργοποιεί το NBT-NS στο domain.

3.2.4 Απενεργοποίηση του SMB v1, μέσω group policy

Το SMB (Server Message Block) είναι ένα πρωτόκολλο που χρησιμοποιείται κυρίως για file sharing, printer services και επικοινωνία μεταξύ υπολογιστών μέσα σε ένα δίκτυο. Η πρώτη έκδοση του (SMB v1 ή CIFS) είναι πλέον deprecated και δεν υπάρχει εγκατεστημένη στους Windows Servers 2016 και μεταγενέστερα. Το SMB v1 έχει πολλές ευπάθειες, που συνήθως καταλήγουν σε εκτέλεση κώδικα στο μηχάνημα του θύματος (RCE- Remote Command Execution). Για τα περισσότερα κενά ασφαλείας του SMB v1 υπάρχουν τα αντίστοιχα patches όμως αν δεν υπάρχει κάποιο legacy σύστημα στο Active Directory (πχ Windows XP) ή κάποια εφαρμογή που το χρειάζεται για να λειτουργήσει, δεν υπάρχει λόγος να είναι ενεργοποιημένο. Το γνωστό malware WannaCry βασιζόταν στην εκμετάλλευση του SMB v1 για να εξαπλωθεί μέσω του εσωτερικού δικτύου σε περισσότερα μηχανήματα. Αντίστοιχα οι επόμενες εκδόσεις του πρωτοκόλλου προσφέρουν περισσότερες δυνατότητες και έχουν αναβαθμισμένη ασφάλεια όπως η κρυπτογράφηση την επικοινωνίας από άκρη σε άκρη (end to end encryption). Ο συγκεκριμένος έλεγχος επιβεβαιώνει την ύπαρξη group policy που απενεργοποιεί το SMB στο domain.

3.2.5 Απενεργοποίηση της αυθεντικοποίησης μέσω NTLM και NTLM v1, μέσω group policy

Η χρήση των NTLM και NTLM v1 για αυθεντικοποίηση αποτελεί ρίσκο ασφάλειας και αυξάνει την επιφάνεια επίθεσης σε ένα περιβάλλον Active Directory. Καθιστά δυνατή τη χρήση NTLM relay επιθέσεων μέσω των οποίων ο επιτιθέμενος μπορεί να εκτελέσει εντολές απομακρυσμένα (remote code execution) ή να αυθεντικοποιηθεί εντός του Active Directory με τα δικαιώματα του χρήστη στον οποίο χρησιμοποίησε την εκάστοτε επίθεση. Η αυθεντικοποίηση με τα παραπάνω πρωτόκολλα θα πρέπει να είναι απενεργοποιημένη εκτός αν οι συνθήκες στο συγκεκριμένο Active Directory δεν το επιτρέπουν. Ο συγκεκριμένος έλεγχος επιβεβαιώνει την ύπαρξη group policy που απενεργοποιεί των NTLM και NTLM v1 στο domain.

3.2.6 Απενεργοποίηση των LLMNR και NBT-NS, μέσω group policy.

Το LLMNR (Link-Local Multicast Name Resolution**)** χρησιμοποιείται σε ένα Active Directory Domain για την αντιστοίχιση Hostname σε IP χωρίς τη χρήση DNS. LLMNR ερωτήματα γίνονται μετά από αποτυχημένα ερωτήματα στον ορισμένο DNS server, αν για παράδειγμα ένας χρήστης κάνει τυπογραφικό λάθος σε ένα γνωστό hostname κάποιου server τότε ο DNS server δεν μπορεί να απαντήσει και γίνεται LLMNR ερώτημα για το συγκεκριμένο λάθος γραμμένο hostname. Στην απάντηση του LLMNR δεν αυθεντικοποιείται η πηγή με αποτέλεσμα ένας κακόβουλος χρήστης να μπορεί να απαντήσει σε LLMNR ερωτήματα. Αυτό λέγεται LLMNR poison και έχει ως αποτέλεσμα το θύμα να επικοινωνεί με ένα μηχάνημα που δεν είναι αυτό με το οποίο επιθυμούσε να επικοινωνήσει αρχικά. Αυτή η επίθεση είναι ιδιαίτερα επικίνδυνη όταν το θύμα θέλει να επικοινωνήσει με κάποια υπηρεσία (service) που χρειάζεται αυθεντικοποίηση και στη συνέχεια, αφού λάβει την ψευδή απάντηση από τον επιτιθέμενο, στείλει στοιχεία αυθεντικοποιήσης (πχ NTLM v2 hash) σε μηχάνημα που ελέγχει ο επιτιθέμενος.

3.2.7 Χρήση Custom Audit Policy σε servers και Domain Controllers

Στο Audit Policy ενός Active Directory ορίζεται η πολιτική μέσω της οποίας καταγράφονται τα γεγονότα που συμβαίνουν μέσα στο περιβάλλον, όπως για παράδειγμα αυθεντικοποίηση χρηστών, πρόσβαση σε κοινόχρηστα αρχεία, προσθήκη/αφαίρεση σε Groups κ.α. Ο σκοπός αυτού του ελέγχου είναι να επιβεβαιωθεί ότι έχει οριστεί μια ελάχιστη απαραίτητη Audit Policy ώστε να καταγράφονται οι βασικότερες πληροφορίες για γεγονότα που μπορούν να επηρεάσουν την ασφάλεια και την ακεραιότητα ενός Active Directory περιβάλλοντος. Επίσης ορίζεται το χρονικό διάστημα για το οποίο θα παραμένουν οι καταγραφές (retention policy).

3.2.8 Έλεγχος για servers με μη υποστηριζόμενες εκδόσεις λειτουργικού συστήματος (Obsolete OS versions)

Οι servers με μη υποστηριζόμενες εκδόσεις λειτουργικού συστήματος αποτελούν μεγάλο κίνδυνο όταν είναι μέρος του Active Directory. Συχνά δημοσιεύονται νέες προηγουμένως άγνωστες ευπάθειες καθώς και τρόποι να τις εκμεταλλευτεί ένας κακόβουλος χρήστης. Λόγω της έλλειψης υποστήριξης όμως στις συγκεκριμένες εκδόσεις αυτές οι ευπάθειες δεν γίνονται patch και οι συγκεκριμένοι servers μένουν (μόνιμα) εκτεθειμένοι σε αυτές.

3.2.9 Έλεγχος για χρήση του Unconstrained delegation μόνο στους Domain Controllers.

Όταν ένας χρήστης αυθεντικοποιείται σε έναν υπολογιστή με ενεργοποιημένο το *unconstrained Kerberos delegation*, το TGT (ticket granting ticket) του αποθηκεύεται στη μνήμη αυτού του υπολογιστή. Η αποθήκευση του TGT στην μνήμη επιτρέπει στο σύστημα να επαληθεύσει ότι ο χρήστης έχει ήδη αυθεντικοποιηθεί χωρίς να ζητήσει εκ νέου αυθεντικοποίηση και μπορεί να υποδυθεί (impersonate) τον πιστοποιημένο χρήστη για να αποκτήσει πρόσβαση σε οποιεσδήποτε άλλες υπηρεσίες. Οι εισβολείς

μπορούν να κλέψουν αυτές τις αποθηκευμένες πληροφορίες μέσω των τεχνικών Πρόσβασης Διαπιστευτηρίων.

3.2.10 Έλεγχος του SYSVOL για ευαίσθητες πληροφορίες.

Ο φάκελος System Volume (Sysvol) είναι προσπελάσιμος από κάθε χρήστη και υπάρχει σε κάθε Domain Controller ενός Active Directory. Στον Sysvol περιέχονται Group Policy templates (GPTs), Scripts, όπως τα startup scripts που ορίζονται και χρησιμοποιούνται απο τα Group Policies, καθώς και Junction points. Ο συγκεκριμένος έλεγχος, ελέγχει μέσω προκαθορισμένων regular expressions, που έχουν παραμετροποιηθεί για το περιβάλλον στο οποίο θα τρέξει το script, για την ύπαρξη ευαίσθητων πληροφοριών εντός του φακέλου sysvol.

3.2.11 Έλεγχος για λογαριασμούς χρηστών με ενεργοποιημένο το "Do not require Kerberos pre-authentication".

Αυτοί οι λογαριασμοί χρηστών είναι ευάλωτοι στην επίθεση AS-REP-ROAST. Στη συγκεκριμένη επίθεση ο κακόβουλος χρήστης έχει τη δυνατότητα να στείλει ένα dummy αίτημα για αυθεντικοποίηση από κάποιον Domain Controller και να λάβει ένα κρυπτογραφημένο TGT (Ticket Granting Ticket). Στη συνέχεια μπορεί να ανακτήσει τον κωδικό του χρήστη για τον οποίο έγινε το αίτημα και να συνδεθεί ως ο συγκεκριμένος χρήστης. Κατά την εκτέλεση του ελέγχου προκύπτει μια λίστα των λογαριασμών, εφόσον υπάρχουν, που είναι ευάλωτοι στη συγκεκριμένη επίθεση. Η λειτουργία της επίθεσης Kerberoasting περιγράφεται αναλυτικότερα στο Παράρτημα 1.

3.2.12 Έλεγχος για λογαριασμούς χρηστών με κενό password και έλεγχος για λογαριασμούς χρηστών που το password τους δεν λήγει ποτέ.

Οι συγκεκριμένοι λογαριασμοί αποτελούν κίνδυνο για ένα περιβάλλον Active Directory καθώς ένας κακόβουλος χρήστης μπορεί είτε να αποκτήσει με ευκολία πρόσβαση σε αυτούς και ταυτόχρονα να τη διατηρήσει για μεγάλο χρονικό διάστημα. Ο έλεγχος παράγει και εμφανίζει μια λίστα με τους λογαριασμούς χρηστών που πληρούν οποιοδήποτε από τα δύο κριτήρια.

3.2.13 Έλεγχος και ανασκόπηση (review) λογαριασμών χρηστών με δυνατότητα να κάνουν DC Sync.

Ο έλεγχος για την δυνατότητα replication του Active Directory. Δημιουργεί μια λίστα με τους χρήστες που έχουν τα απαραίτητα δικαιώματα ώστε να μπορούν να ξεκινήσουν ένα replication process με σκοπό να βρεθούν πιθανόν περιττά δικαιώματα σε λογαριασμους και groups. Οι χρήστες με τα περιττά δικαιώματα έχουν ως αποτέλεσμα αύξηση του ρίσκου ασφαλείας και διευρύνουν την επιφάνεια επίθεσης του Active Directory, οπότε και θα πρέπει να τους αφαιρεθούν αυτά τα δικαιώματα. Πιο αναλυτικά η επίθεση DCSync λειτουργεί όπως περιγράφεται στο Παράρτημα 2.

3.2.14 Έλεγχος για επισφαλείς αλγορίθμους κρυπτογράφησης στο Kerberos Authentication.

Αδύναμοι αλγόριθμοι κρυπτογράφησης όπως οι RC4, DES και 3DES προτιμούνται για την επίθεση Kerberoasting. Απαγορεύοντας την χρήση των επισφαλών αλγορίθμων, αυτών που μπορούν εύκολα να γίνουν reverse και να ανακτηθεί ο κωδικός πρόσβασης του λογαριασμού, μειώνεται η πιθανότητα να πετύχει η συγκεκριμένη επίθεση και ο επιτιθέμενος να αποκτήσει πρόσβαση στον λογαριασμό και Active Directory.

3.2.15 Έλεγχος για λογαριασμούς χρηστών με SPNs.

Δεν θα πρέπει να υπάρχουν χρήστες με SPNs πέρα από τους απαραίτητους, και ταυτόχρονα θα πρέπει να διασφαλίζεται ότι οι λογαριασμοί χρηστών με SPNs έχουν ασφαλή κωδικό πρόσβασης. Οι λογαριασμοί χρηστών με ορισμένα SPNs χρησιμοποιούνται για την επίθεση Kerberoast.

ΠΑΡΑΡΤΗΜΑΤΑ

A. Επίθεση Kerberoasting

Η συγκεκριμένη επίθεση έγινε δημόσια γνωστή το 2014 από τον Tim Mendin το συνέδριο DerbyCon στο Kentucky. Εμπίπτει στη κατηγορία επιθέσεων post-exploitation, που εκτελούνται δηλαδή αφού ο επιτιθέμενος έχει αποκτήσει πρόσβαση στο δίκτυο του Active Directory. Ο σκοπός της είναι η πλευρική κίνηση σε άλλους χρήστες (lateral movement) ή η απόκτηση πρόσβασης σε λογαριασμό με υψηλότερα δικαιώματα (privilege escalation) μέσω ενός, οποιουδήποτε, χρήστη του Active Directory.

Η μεθοδολογία που εφαρμόζεται βασίζεται στην μη ασφαλή αρχιτεκτονική του πρωτοκόλλου Kerberos, στο οποίο κάθε αυθεντικοποιημένος χρήστης μπορεί να ζητήσει ένα TGS ticket (Ticket-Granting-Service) για χρήστες διαφορετικούς από τον εαυτό του. Στη συνέχεια ο domain controller απαντάει με ένα TGS ticket το οποίο είναι κρυπτογραφημένο με το NTLM hash του συνθηματικού του χρήστη για τον οποίο είναι το ticket. Έχοντας αυτό το NTLM hash ο επιτιθέμενος μπορεί να τρέξει offline εργαλεία (πχ πχ Hashcat, John The Ripper, και άλλα) για να ανακτήσει το συνθηματικό του άλλου χρήστη και στη συνέχεια να συνδεθεί με το λογαριασμό του. Πλέον υπάρχουν εργαλεία που αυτοματοποιούν αυτή την επίθεση, μειώνοντας σημαντικά το τεχνικό επίπεδο που απαιτείται για την εκτέλεση της, ενώ η κρισιμότητα της παραμένει ιδιαίτερα υψηλή.

B. Επίθεση DCSync

Αναπτύχθηκε και κυκλοφόρησε το 2015, η επίθεση DCSync απλοποιεί σε μεγάλο βαθμό την πρόσβαση σε έναν domain controller του Active Directory καταργώντας την απαίτηση να παραβιαστεί ένας. Αντίθετα, το DCSync επιτρέπει σε έναν εισβολέα να χρησιμοποιήσει μόνο τα διαπιστευτήρια ενός διαχειριστικού λογαριασμού (ή ακόμα και έναν χρήστη του Active Directory domain με επαρκή προνόμια) για να παραβιάσει πλήρως ένα ολόκληρο Active Directory forest. Το DCSync επιτρέπει σε αυτόν τον εισβολέα να μιμηθεί έναν domain controller. Χρησιμοποιώντας το GetNCChanges request, ο εισβολέας ζητά από τον κύριο (primary) domain controller να αναπαράγει τα διαπιστευτήρια χρηστών πίσω στον εισβολέα χρησιμοποιώντας το πρωτόκολλο Directory Replication Service (DRS) Remote Protocol.

Εργαλεία όπως το Mimikatz[12] και το Empire[13] διευκολύνουν την υλοποίηση επιθέσεων DCSync. Για παράδειγμα, οι ενσωματωμένες δυνατότητες του Mimikatz και άλλα εργαλεία επιτρέπουν στους εισβολείς να μιμηθούν έναν domain controller και να ξεκινήσουν το αίτημα. Αυτό απαλλάσσει τον εισβολέα από την προσπέλαση και το κατέβασμα ενός αρχείου βάσης δεδομένων NTDS.DIT των Windows, μια ενέργεια που αποτελεί "κόκκινη σημαία" και σχεδόν σίγουρα θα ενεργοποιούσε ειδοποιήσεις από ένα σύστημα εντοπισμού δικτύου όπως ένα SIEM ή ένα IPS. Οι επιθέσεις DCSync μπορεί να είναι προοίμιο για επόμενες επιθέσεις Golden και Silver Ticket.

[12] https://github.com/gentilkiwi/mimikatz
[13] https://github.com/EmpireProject/Empire

Γ. Πηγαίος κώδικας Powershell

```
<#

.SYNOPSIS
 This script was developed in order to automate Windows Active Directory security assesement. It is meant to be run on a domain controller, see prerequisites section before running it.
 It should be periodically reviewed and maintained to include latest knowledge regarding the AD environment that it is executed on.

  PREREQUISITES:
  - Powershell ActiveDirectory module should be installed
  - Review/update the included OUs (will be checked for users with 'Do not require Kerberos PreAuth')
  - Review/update regular expressions that are used to audit SYSVOL for sensitive info.

.DESCRIPTION
  *** THIS SCRIPT IS PROVIDED WITHOUT WARRANTY, USE AT YOUR OWN RISK ***

   The script checks for insecure configurations that introduce vulnerabilities to the Active Directory environment.
  Some components (e.g. Obsolete OS versions array, Audit Policy config array, etc) need to be reviewed before and maintained prior to executing the script, in order to verify that are up to date.
  Otherwise the reported result might be wrong.

  The implemented security checks are the following:
  - Fine Grained Password Policy, check if is set up and used
  - LAPS, verify usage
  - SMBv1, check if disabled
  - GPO related checks:
    - Kerberos Weak Encryptions Algorithms, check if disabled
    - NBT-NS, check if disabled via GPO
    - MITM6 remediation, check if 'Prefer IPv4 over IPv6' is set
  - NTLM & NTLMv1, check if disabled
  - LLMNR, check if disabled
  - Custom Audit Policy (verify against provided minimum requirements)
  - Obsolete OS, verify usage
  - Missing Security Updates
  - Users with unconstrained delegation
  - Sysvol sensitive information
  - Users with Kerberos PreAuth (shouldn't exist)
  - Accounts with empty passwords or passwords that do not expire
  - DCSync capable users (only list them for review)



.NOTES
  Author:        George Spyropoulos (mte1930)
  Creation Date:  15/06/2021
  Last Update:    20/12/2021
  Version:        3.1

#>

# OUs to check against (for 'Do not require Kerberos PreAuth')
```

```
$kerberos_preauth_ous = "", ""

# AD audit policy config check array
$audit_policy_config_array = "Sensitive Privilege Use","Authentication Policy Change","Authorization Policy Change","MPSSVC Rule-Level Policy Change","Filtering Platform Policy Change","File System","Registry","SAM","File Share","Other Object Access Events","Detailed File Share","Removable Storage","Process Creation","DPAPI Activity","Computer Account Management","Security Group Management","Other Account Management Events","User Account Management"

# Obsolete OS check related arrays
$Obsolete_Desktop_OS_Versions = "2195","2600","3790","9200","6002","10240","10586","14393","15063","16299","17134","7601","18363"#,"19041","19042","19043",
$Obsolete_Server_OS_Versions = "18363","18362","7601","6003","3790","2195"

# Sysvol check related arrays (change/update if necessary)
$interesting_file_extentions="*.vbs","*.xml"
$patterns_of_interest="passwd","pwd"

# Script output related variables
$newline="`n"
$tab="`t"
$check_start="-"
$check_result="-"

#region Variables

########################################
# Variables
########################################
$forestInfo = Get-ADForest
$AllDomains = (Get-ADForest).Domains
$domainInfo = Get-ADDomain
$PDCEmulator = (Get-ADDomain).PDCEmulator
$DNSRoot = $domainInfo.dnsroot
$ADsiteLinks = Get-ADReplicationSiteLink -Filter *
#endregion

$domain_name = $domainInfo.Name

foreach ($word in $domain_name.split("."))
{
 write-Host $word
 if ($dc_name -eq "")
 {
  $dc_name+="DC=$($word)"
 }
 else
 {
  $dc_name+=",DC=$($word)"
 }
}

Write-Host "Forest and Domain information"
```

```powershell
#region Forest Info

#######################################
# Forest Information
#######################################
# Forest Root Domain
$RootDomain = $forestInfo.RootDomain
# Forest Functional Level
$ForestMode = $forestInfo.ForestMode
# Forest Domains
$Domains = ($forestInfo |
Select-Object -ExpandProperty Domains) -join ' | '
# AD Recycle BIN Status
$ADRecycleBIN = Get-ADOptionalFeature -filter {Name -eq 'Recycle Bin Feature'} |
Select-Object -ExpandProperty EnabledScopes

If (!$ADRecycleBIN){
 $ADRecycleBIN = 'Disabled'
} else {
 $ADRecycleBIN = 'Enabled'
}

# Forest Information Output Object
$ForestOutputObj  = New-Object -TypeName PSObject
$ForestOutputObj  | Add-Member -MemberType NoteProperty -Name ForestRootDomain -Value
$RootDomain
$ForestOutputObj  | Add-Member -MemberType NoteProperty -Name ForestFunctionalLevel -Value
$ForestMode
$ForestOutputObj | Add-Member -MemberType NoteProperty -Name ForestDomains -Value $Domains
$ForestOutputObj  | Add-Member -MemberType NoteProperty -Name ADRecycleBIN -Value
$ADRecycleBIN
$ForestOutputObjCsv = $ForestOutputObj | ConvertTo-Csv
$ForestOutputArray = $ForestOutputObjCsv.Split(",")
$ForestOutputTableTD = ""
For ($i=5; $i -lt $ForestOutputArray.Length; $i=$i+4) {
 $ForestOutputTableTD = "Forest Root Domain: "+ $ForestOutputArray[$i] + "`n`tForest Functional Level:
" + $ForestOutputArray[$i + 1] + "`n`tForest Domains: " + $ForestOutputArray[$i + 2] + "`n`tAD Recycle
BIN: " + $ForestOutputArray[$i + 3]
}
Write-Host "$($tab)$ForestOutputTableTD"

#endregion


#region Domain Info

#######################################
# Domain Information
#######################################
# Get the Domain Functional Level
$DomainMode = ($DNSRoot | foreach { Get-ADDomain -Identity $_ }  |
Select-Object -ExpandProperty DomainMode) -join ' | '
# Get the Domain NetBIOS Name
$NetBIOSName = $domainInfo.netBIOSName
```

```
# Domain Information Output Object
$DomainOutputObj  = New-Object -TypeName PSObject
$DomainOutputObj  |  Add-Member  -MemberType  NoteProperty  -Name  ForestFunctionalLevel  -Value
$DomainMode
$DomainOutputObj  |  Add-Member  -MemberType  NoteProperty  -Name  NetBIOS_Name  -Value
$NetBIOSName
$DomainOutputObjCsv = $DomainOutputObj | ConvertTo-Csv
$DomainOutputArray = $DomainOutputObjCsv.Split(",")
$DomainOutputTableTD = ""
For ($i=3; $i -lt $DomainOutputArray.Length; $i=$i+2) {
  $DomainOutputTableTD ="Domain Functional Level: " + $DomainOutputArray[$i] + "`n`tNet BIOS Name:
" + $DomainOutputArray[$i + 1]
}
Write-Output "$($tab)$DomainOutputTableTD"

#endregion

Write-Output "`nAD Security Audit checks and results`n"
######### Maestro Start #########

# Fine Grained Password Policy check (all>=14, priveleges>=20, service_accounts>=24)
# Check if the cmdlet fails or if there are at least three different objects (policies)
try{
  $count=(Get-ADFineGrainedPasswordPolicy -Filter "*" | Measure-Object).Count
  if ($count -lt 3 -or $count -eq 3)
  {
    $result_message='Fine Grained Password Policy is used and is properly configured'
    Write-Host "$($tab)$($check_result_start)$($result_message)" -f Green
  }
  else
  {
    $result_message='Fine Grained Password Policy is used but not properly configured'
    Write-Host "$($tab)$($check_result_start)$($result_message)" -f Red
  }
}catch
{
  $result_message='Fine Grained Password Policy is not used'
  Write-Host "$($tab)$($check_result_start)$($result_message)" -f Red
}


#region LAPS
#########################################
#Check if LAPS is installed

try
{
                                                                                Get-ADObject
"CN=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,$((Get-ADDomain).DistinguishedName)"
-ErrorAction Stop | Out-Null
  $lapsmessage='LAPS is installed'
    Write-Host  "$($tab)$($check_result)$($lapsmessage)" -f Green
  }catch
```

```
 {
   $lapsmessage='LAPS is NOT installed! We suggest you install LAPS!'
  Write-Host  "$($tab)$($check_result)$($lapsmessage)" -f Red
}

#endregion


#region SMBv1
#Check if server supports SMBv1

if                                                  (!(Get-ItemProperty                                                 -Path
HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters).SMB1 -eq 0)
{
 $SMBv1_status = 'SMBv1 is NOT disabled. Please disable SMBv1!'
 Write-Host  "$($tab)$($check_result)$($SMBv1_status)" -f Red
}else
{
 $SMBv1_status = 'SMBv1 is disabled. (As it should be)'
 Write-Host  "$($tab)$($check_result)$($SMBv1_status)" -f Green
}

#endregion

#region Group Policy Object related checks
########################################
$nbt_ns_correct_script=0
$mitm6_correct_script=0

$AllGPOs = Get-GPO -All | sort DisplayName;
foreach ($GPO in $AllGPOs)
{
 # Kerberos Algorithms Check
 #Check if weak encrpytion algorithms are enabled and if strong ones are disabled
 $GPOreport = Get-GPOReport -Guid $GPO.id -ReportType Xml;
 $xmlreport = [xml]$GPOreport;

                                                $permissionindex                                                =
$GPOreport.IndexOf('MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\
Parameters\SupportedEncryptionTypes');
 if($permissionindex -gt 0)
 {
  $xmlreport = [xml]$GPOreport;
                                                              $EncryptionTypes                                  =
$xmlreport.gpo.Computer.ExtensionData.Extension.SecurityOptions.Display.DisplayFields.Field;
  if(($EncryptionTypes | Where-Object {$_.name -eq 'DES_CBC_CRC'} | select -ExpandProperty value) -eq
'true')
  {
   $DES_CBC_CRC_status = 'enabled'
  }else
  {
   $DES_CBC_CRC_status = 'disabled'
  }
```

```
    if(($EncryptionTypes | Where-Object {$_.name -eq 'DES_CBC_MD5'} | select -ExpandProperty value)
-eq 'true')
    {
     $DES_CBC_MD5_status = 'enabled'
    }else
    {
     $DES_CBC_MD5_status = 'disabled'
    }

    if(($EncryptionTypes | Where-Object {$_.name -eq 'RC4_HMAC_MD5'} | select -ExpandProperty value)
-eq 'true')
    {
     $RC4_HMAC_MD5_status = 'enabled'
    }else
    {
     $RC4_HMAC_MD5_status = 'disabled'
    }

    if(($EncryptionTypes | Where-Object {$_.name -eq 'AES128_HMAC_SHA1'} | select -ExpandProperty
value) -eq 'false')
    {
     $AES128_HMAC_SHA1_status = 'disabled'
    }else
    {
     $AES128_HMAC_SHA1_status = 'enabled'
    }

    if(($EncryptionTypes | Where-Object {$_.name -eq 'AES256_HMAC_SHA1'} | select -ExpandProperty
value) -eq 'false')
    {
     $AES256_HMAC_SHA1_status = 'disabled'
    }else
    {
     $AES256_HMAC_SHA1_status = 'enabled'
    }

    if(($EncryptionTypes | Where-Object {$_.name -eq 'Future encryption types'} | select -ExpandProperty
value) -eq 'false')
    {
     $fut_encr_types_status = 'disabled'
    }else
    {
     $fut_encr_types_status = 'enabled'
    }
  }

  # NBT-NS disabled via GPO check
  # This check verifies that a certain GPO exists with a powershell script 'command'. This script checks that
the registry key at
  # 'HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\*' is set to 2. This value was
found on Microsoft documentation in the following link:
                                                                                                    #
https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-
netbt-interfaces-interface-netbiosoptions
```

```
 try
 {
  $script_path = $xmlreport.gpo.Computer.ExtensionData.Extension.Script;
  $script_content = Get-Content $script_path.Command
                                        if                    ($script_content.IndexOf("`$regkey                    =
`"HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"))
  {
           if($script_content.IndexOf("Get-ChildItem  `$regkey  |foreach  {  Set-ItemProperty  -Path
`"`$regkey\`$(`$_.pschildname)`" -Name NetbiosOptions -Value 2 -Verbose}")) {
    $nbt_ns_correct_script=1
    }
  }
 }
 catch{}

 # MITM6 mitigation GPO check
 # This check verifies that a certain GPO exists with a powershell script 'command'. This script checks that
the registry key at
      #      HKLM:SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\      has      a      key      named
'DisabledComponents' with value 32 according to Microsoft documentation at
                                                                                                        #
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-ipv6-in-windows
 try
 {
   $script_path = $xmlreport.gpo.Computer.ExtensionData.Extension.Script;
   $script_content = Get-Content $script_path.Command
   # Verify that the script contains the correct code (does what we need it to do)
                                        if                    ($script_content.IndexOf("`$regkey                    =
`"HKLM:SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\")                                    -and
$script_content.IndexOf("Set-ItemProperty        -Path        `"`$regkey\`$(`$_.pschildname)`"        -Name
DisabledComponents -Value 32 -Verbose}")) {
      $mitm6_correct_script=1
   }
 }
 catch{}
}

Write-Output "$($tab)Weak kerberos algorithm checks:"
Write-Output "$($tab)$($tab)DES_CBC_CRC: $($DES_CBC_CRC_status)"
Write-Output "$($tab)$($tab)DES_CBC_MD5: $($DES_CBC_MD5_status)"
Write-Output "$($tab)$($tab)RC4_HMAC_MD5: $($RC4_HMAC_MD5_status)"
Write-Output "$($tab)$($tab)AES128_HMAC_SHA1: $($AES128_HMAC_SHA1_status)"
Write-Output "$($tab)$($tab)AES256_HMAC_SHA1: $($AES256_HMAC_SHA1_status)"
Write-Output "$($tab)$($tab)Future encryption types: $($fut_encr_types_status)"
#endregion

# Check if NTLM & NTLMv1 are disabled
# Microsoft documentation URL:
#
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-s
ecurity-lan-manager-authentication-level

$NTLM_compatibility=(Get-ItemProperty                                                                -Path
HKLM:\System\CurrentControlSet\Control\Lsa).lmcompatibilitylevel
```

```
if ($NTLM_compatibility -eq 5 -or $NTLM_compatibility -eq 3)
{
 $NTLM_message="NTLM authentication usage is configured correctly"
 Write-host "$($tab)$($check_result)$($NTLM_message)" -f Green
}else
{
 $NTLM_message="NTLM authentication usage is not configured correctly. You need to remediate asap!"
 Write-host "$($tab)$($check_result)$($NTLM_message)" -f Red
}

#endregion


# Check if LLMNR is disabled (via GPO)

# Default Domain Policy/Computer Configuration/Administrative Templates/Network/DNS Client/Turn off
multicast name resolution

$AllGpos = Get-GPO -All
# Now retrieve every gpo report and check for the wanted name and value
foreach ($g in $AllGpos) {
   [xml]$Gpo = Get-GPOReport -ReportType Xml -Guid $g.Id
   foreach ($extension in $Gpo.GPO.Computer.ExtensionData.Extension){
      if ($extension.PSobject.Properties.name -match "Policy")
      {
         try{
            $name=($extension | select -ExpandProperty Policy).Name
            $value=($extension | select -ExpandProperty Policy).State
            if ($name -contains "Turn off multicast name resolution")
            {
             $llmnr_policy_found=1
             if ($value -contains 'Enabled')
             {
                   Write-host "$($tab)LLMNR is properly disabled. this configuration will be enforced on the
domain joined hosts after their next gpupdate" -f Green

             }elseif ($value -contains 'Not Configured' -or $value -contains 'Disabled') {
              Write-Host "$($tab)LLMNR is not disabled in the domain!" -f Red
             }
            }
         }
         catch{
            Write-Host "$($tab)LLMNR is not disabled in the domain!" -f Red
         }
      }
   }
}
#endregion


# Custom audit policy check
# Verify that the most essential security related audit is applied in the domain
```

```
# AD audit policy config check array
$domain_audit_policy =  auditpol /get /Category:* /r

$audit_policy_config=0
foreach ($policy_to_check in $audit_policy_config_array)
{
            if          (($domain_audit_policy.IndexOf($policy_to_check)          -gt          0)          -and
($domain_audit_policy.IndexOf("Success and Failure") -gt 0))
 {
  $audit_policy_config+=1
 }
}

# If the number of succesfully configured items equals the length of the 'check array' then the Audit Policy
is configured correctly
if ($audit_policy_config -eq $audit_policy_config_array.Length)
{
 $audit_policy_message="A custom audit policy is set and is properly configured"
 Write-host "$($tab)$($audit_policy_message)" -f Green
}
else
{
 $audit_policy_message="Audit policy is not properly configured"
 Write-host "$($tab)$($audit_policy_message)" -f Red
}


#endregion


# NBT-NS Check result
# Check if a GPO is present that disables NetBIOS Name Service during computer startup for all
authenticated users


if ($nbt_ns_correct_script -eq 1)
{
 Write-host "$($tab)NBT-NS is properly disabled via GPO" -f Green
}
else
{
 Write-host "$($tab)NBT-NS is not properly disabled via GPO" -f Red
}


# Check for mitm6 mitigation (prefer IPv4 over IPv6) result
if ($mitm6_correct_script -eq 1)
{
 Write-host "$($tab)mitm6 mitigation via GPO is properly configured (prefer IPv4 over IPv6)" -f Green
}
else
{
 Write-host "$($tab)mitm6 mitigation via GPO is NOT properly configured (prefer IPv4 over IPv6)" -f Red
}
```

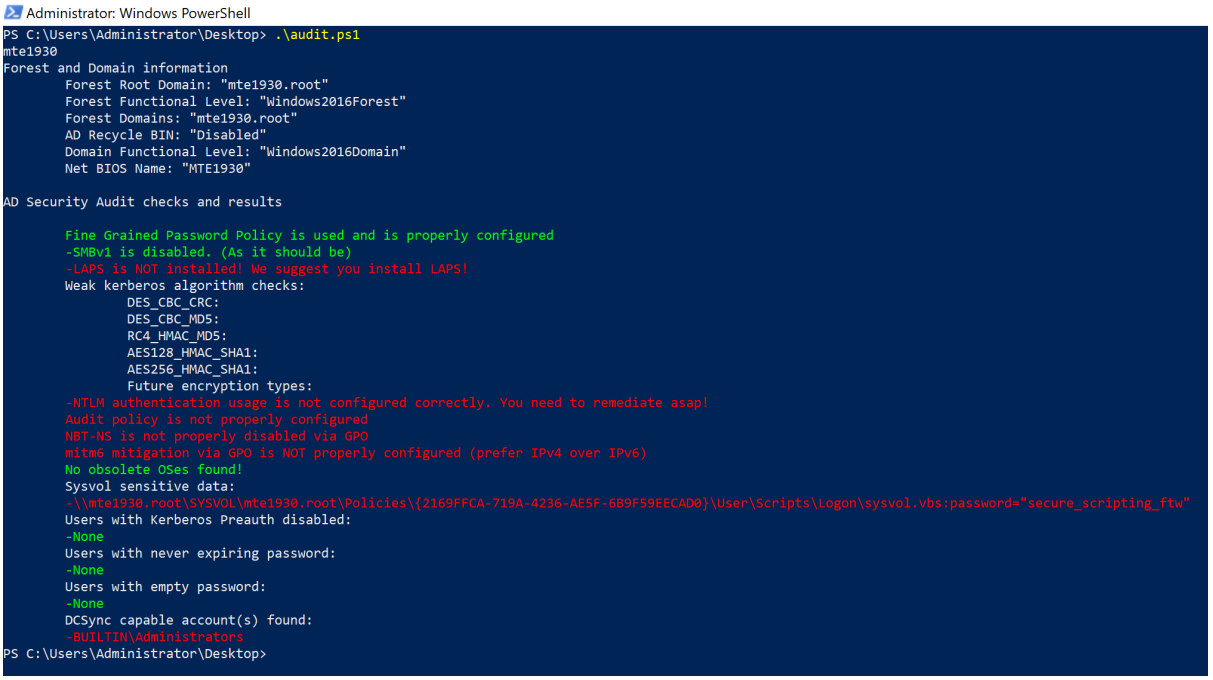
```
#endregion

# Check for Obsolete OSes (on DCs and joined pcs) against a list published by Microsoft at
# https://docs.microsoft.com/en-us/lifecycle/faq/windows
# and here https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions (verify if this get's updated over time)
# This list needs to be verified before each run in order to ensure that it is updated

$allPCs = Get-ADComputer -Filter "*" -Properties * | Select-Object *
$allDCs = Get-ADDomainController -Filter * | Select-Object ComputerObjectDN
$found_obsolete_os=0
foreach ($pc in $allPCs)
{
 #Check against Server OSes
 foreach ($obsolete_os in $Obsolete_Server_OS_Versions)
 {
  if ($pc.OperatingSystemVersion -match $obsolete_os)
  {
   $found_obsolete_os=1
   Write-Host "$($tab)Obsolete OS found on $($pc.CanonicalName)!" -f Red
   Write-Host "$($tab) $($pc.OperatingSystemVersion) "
  }
 }

 #Check against Desktop OSes
 foreach ($obsolete_os in $Obsolete_Desktop_OS_Versions)
 {
  if ($pc.OperatingSystemVersion -match $obsolete_os)
  {
   $found_obsolete_os=1
   Write-Host "$($tab)Obsolete OS found on $($pc.CanonicalName)!" -f Red
  }
 }
}

if ($found_obsolete_os -eq 0)
{
 Write-Host "$($tab)No obsolete OSes found!" -f Green
}
#endregion


# Unconstrained delegation check
# verify that no non-DCs have this enabled
$found_one = 0
# Iterate through a list of all the AD domain joined computers
foreach ($pc in $allPCs)
{
 if ($pc.TrustedForDelegation -match "True")
 {
  # Check if computer is a DC or not
  foreach ($dc in $allDCs)
  {
```

```
    if ($pc.DistinguishedName -notmatch $dc.ComputerObjectDN)
    {
      Write-Output "$($pc.Name) is trusted for delegation $($pc.TrustedForDelegation)!"
      $found_one=1
    }
   }
  }
}

#endregion


# SYSVOL sensitive info check
# will have to update searches in case of new types of sensitive patterns

$found_one = 0
Write-Host "$($tab)Sysvol sensitive data:"
foreach ($file_extension in $interesting_file_extentions)
{
 foreach ($pattern in $patterns_of_interest)
 {
  $found_one = 0
                              $result=              findstr              /S              /I              $pattern
"\\$($domainInfo.DistinguishedName)\SYSVOL\$($domainInfo.DistinguishedName)\Policies\$($file_exte
nsion)"

   # findstr returns 0 if one or more results are returned, 0 if no result is returned and 2 for wrong syntax
   if ($LASTEXITCODE -ne 1)
   {
    Write-Host "$($tab)$($check_result)$($result)" -f Red
   }
  }
}


#Kerberos PreAuth check
Write-Host "$($tab)Users with Kerberos Preauth disabled:"
# This needs to be updated in order to search on all OUs with users that must be checked and also take
the domain name from variable(s)
$no_krb_preauth = Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -searchbase "OU=Regular
Users,OU=Site1,OU=User Accounts,$($ domainInfo.DistinguishedName)" -Properties * | Select-Object
"Name"
if ($no_krb_preauth -ne $null)
{
 foreach ($user in $no_krb_preauth)
 {
  Write-Host "$($tab)$($check_result)$($user.Name)" -f Red
 }
}
else
{
 Write-Host "$($tab)$($check_result)None" -f Green
}
#endregion
```

```
# Users with Passwords set to never expire
$NeverExpire = (Get-ADUser -Filter {PasswordNeverExpires -eq $true} | Select-Object -ExpandProperty
SamAccountName)
if ($NeverExpire -eq "Guest")
{
  Write-host "$($tab)Users with never expiring password:"
  Write-host "$($tab)$($check_result)None" -f Green
}
else
{
  Write-Host "$($tab)Users with never expiring password:"
  foreach ($user in $NeverExpire)
  {
    Write-host "$($tab)$($check_result)$($user)" -f Red
  }
}

#endregion


# Users with empty password

$EmptyPass = (Get-ADUser -Filter {PasswordNotRequired -eq $true} | Select-Object -ExpandProperty
SamAccountName)
if ($EmptyPass -eq "Guest")
{
  Write-host "$($tab)Users with empty password:"
  Write-host "$($tab)$($check_result)None" -f Green
}
else
{
  Write-Host "$($tab)Users with empty password:"
  foreach ($user in $EmptyPass)
  {
    Write-host "$($tab)$($check_result)$($user)" -f Green
  }
}

#endregion


# DCSync capable users check
$domain_acl = (Get-ACL "AD:$($domainInfo.DistinguishedName)").access
$distinct_identities = @{}
$dcsync_accounts = @()
$dcsync_user_found=0

foreach ($right in $domain_acl){
   if (-not $distinct_identities.Contains($right.IdentityReference.ToString()))
   {
      $distinct_identities.add($right.IdentityReference.ToString(),@())
   }
```

```
   $distinct_identities[$right.IdentityReference.ToString()]+=@($right.ObjectType)

}

foreach ($identity in $distinct_identities.GetEnumerator())
{
  if (($identity.Value) -contains "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2" -and ($identity.Value) -contains
"1131f6aa-9c07-11d1-f79f-00c04fc2dcd2"                -and                ($identity.Value)                -contains
"89e95b76-444d-4c62-991a-0facbeda640c")
  {
   $dcsync_user_found=1
   $dcsync_accounts+=($identity.Name)
  }
}

if ($dcsync_user_found -eq 1)
{
  Write-Host "$($tab)DCSync capable account(s) found:"
  foreach ($account in $dcsync_accounts)
  {
    Write-host "$($tab)$($check_result)$($account)" -f Red
  }
}
else
{
  Write-Host "$($tab)DCSync capable account(s) found:"
  Write-Host "$($tab)$($check_result)None" -f Green
}

#endregion

######### Security Audit Code End #########
```

Δ. Ενδεικτικό αποτέλεσμα εκτέλεσης του κώδικα


Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> .\audit.ps1
mte1930
Forest and Domain information
Forest Root Domain: "mte1930.root"
Forest Functional Level: "Windows2016Forest"
Forest Domains: "mte1930.root"
AD Recycle BIN: "Disabled"
Domain Functional Level: "Windows2016Domain"
Net BIOS Name: "MTE1930"
AD Security Audit checks and results
Fine Grained Password Policy is used and is properly configured
-SMBv1 is disabled. (As it should be)
-LAPS is NOT installed! We suggest you install LAPS!
Weak kerberos algorithm checks:
DES_CBC_CRC:
DES_CBC_MD5:
RC4_HMAC_MD5:
AES128_HMAC_SHA1:
AES256_HMAC_SHA1:
Future encryption types:
-NTLM authentication usage is not configured correctly. You need to remediate asap!
Audit policy is not properly configured
NBT-NS is not properly disabled via GPO
mitm6 mitigation via GPO is NOT properly configured (prefer IPv4 over IPv6)
No obsolete OSes found!
Sysvol sensitive data:
-\\mte1930.root\SYSVOL\mte1930.root\Policies\{2169FFCA-719A-4236-AE5F-6B9F59EECAD0}\User\Scripts\Logon\sysvol.vbs:password="secure_scripting_ftw"
Users with Kerberos Preauth disabled:
-None
Users with never expiring password:
-None
Users with empty password:
-None
DCSync capable account(s) found:
-BUILTIN\Administrators
PS C:\Users\Administrator\Desktop>