Γεώργιος Μιχούλης dai16067

ISS: Ασφάλεια πληροφοριών και Συστημάτων Εργασία 1

Θέμα 1. Θα επιλέξω το 2ο και το 3ο συνθηματικό διότι είναι πιο κοντά στους κανόνες πολυπλοκότητας, δηλαδή να περιέχουν τουλάχιστον από ένα κεφαλαίο γράμμα, ένα μικρό γράμμα, έναν αριθμό και ένα σύμβολο. Όταν τα ¾ από τα κριτήρια υπάρχουν τότε το συνθηματικό θεωρείτε αρκετά δυνατό , με την προϋπόθεση ότι και τα 2 συνθηματικά έχουνε πάνω από 8 χαρακτήρες , οπότε και οι πιθανοί συνδυασμοί φτάνουν σε μη αριθμήσιμα πλέον νούμερα. Το 1ο και το 4ο δεν θα τα επέλεγα γιατί το 1ο είναι σχεδόν ίδιο με το username ( καθώς ένα από τα κριτήρια πολυπλοκότητας είναι και το συνθηματικό να μην μοιάζει με το username) οπότε και εύκολα «μαντεύετε» και το 4ο είναι η λέξη pass$w0rd , αρκετά προβλέψιμο και εύκολο.

Θέμα 3ο. Τα πλεονεκτήματα του πρωτοκόλλου κέρβερος είναι τα εξής:

1. Γρηγορότερη αυθεντικοποίηση- ανανεώσιμη συνεδρία. Το πρωτόκολλο κέρβερος χρησιμοποιεί ένα μοναδικό “ticketing” σύστημα προ προσφέρει πιο γρήγορη αυθεντικοποίηση. Στο πλαίσιο της αμοιβαίας επαλήθευσης ταυτότητας , ο πελάτης λαμβάνει πιστοποιήσεις από το διακομιστή. Τα εισιτήρια θεωρούνται ως άδειες πρόσβασης, και μπορούν να χρησιμοποιηθούν πάνω από μια φορά από την πλευρά του πελάτη, έτσι σε μια μελλοντική συνεδρία ο διακομιστής θα αναγνωρίσει άμεσα την ταυτότητα του πελάτη.
2. Αμοιβαία πιστοποίηση ταυτότητας. Αυτό σημαίνει ότι ο πελάτης επικυρώνει την υπηρεσία που είναι υπεύθυνη για τον πόρο και ότι η υπηρεσία πιστοποιεί επίσης τον πελάτη σε περίπτωση που δεν έχει λήξη το εισιτήριο πάντα.
3. Ο Κέρβερος είναι ανοιχτού προτύπου. Η Microsoft βασίζει την εφαρμογή του Kerberos στο πρότυπο που καθορίζεται από το RFC 1510
4. Υποστήριξη την ανάθεση ταυτοποίησης και ολοκληρωμένες συνεδρίες . Όταν δύο κόμβοι αρχίζουν τις επικοινωνίες , περνούν κρυπτογραφημένα εισιτήρια μέσω ενός έμπιστου τρίτου συστήματος το οποίο ονομάζεται Κέντρο Διανομής Κλειδιών . Το σύστημα αυτό περνά ένα μυστικό εισιτήριο με ένα κλειδί αποκρυπτογράφησης στους δύο κόμβους . Οι κόμβοι στη συνέχεια περνούν κρυπτογραφημένα γραμματόσημα χρόνου ο ένας στον άλλο και χρησιμοποιούν το κλειδί για να τα αποκρυπτογραφήσουν . Αν το κάνουν με επιτυχία , επικυρώνουν τους ομολόγους τους και εμπιστεύονται ο ένας τον άλλο για όσο χρονικό διάστημα η σύνδεση παραμένει ανοιχτή .Η εξουσιοδότηση είναι χρήσιμη για αρκετές εφαρμογές όπως διαδικτυακές κ.α.
5. Υποστηρίζει την λειτουργία σύνδεσης της έξυπνης κάρτας.

Η δυνατότητα σύνδεσης με έξυπνες κάρτες παρέχει πολύ ισχυρότερη πιστοποίηση από τη λειτουργία σύνδεσης κωδικού πρόσβασης, διότι βασίζεται σε έλεγχο ταυτότητας δύο παραγόντων: α) Για να συνδεθεί, ένας χρήστης πρέπει να διαθέτει μια έξυπνη κάρτα και β) να γνωρίζει τον κωδικό PIN του. Η δυνατότητα σύνδεσης της έξυπνης κάρτας προσφέρει επίσης και άλλα πλεονεκτήματα ασφάλειας. για παράδειγμα, μπορεί να αποκλείσει τις επιθέσεις του trojan που προσπαθούν να αρπάξουν τον κωδικό πρόσβασης ενός χρήστη από τη μνήμη του συστήματος.

Θέμα 4ο. Τα forests , trees and domains , είναι αντικείμενα του Active Directory και λίγο πιο συγκεκριμένα είναι λογικές υποκατηγορίες. Αυτά τα αντικείμενα ομαδοποιούνται σε τομείς. Τα αντικείμενα για έναν μόνο τομέα αποθηκεύονται σε μια ενιαία βάση δεδομένων (η οποία μπορεί να αναπαραχθεί). Οι τομείς προσδιορίζονται από τη δομή ονομάτων DNS τους, το χώρο ονομάτων.

Ο τομέας ορίζεται ως μια λογική ομάδα αντικειμένων δικτύου (υπολογιστές, χρήστες, συσκευές) που μοιράζονται την ίδια βάση δεδομένων της υπηρεσίας καταλόγου Active Directory.

Ένα tree είναι μια συλλογή ενός ή περισσοτέρων domain και domain trees σε ένα συνεχόμενο χώρο ονομάτων, που συνδέεται σε μια ιεραρχία επαγγελματικής εμπιστοσύνης.

Στην κορυφή της δομής βρίσκεται το forest. Ένα forest είναι μια συλλογή από trees που μοιράζονται έναν κοινό παγκόσμιο κατάλογο, ένα σχήμα καταλόγου, μια λογική δομή και μια διαμόρφωση καταλόγου. Το forest αντιπροσωπεύει το όριο ασφαλείας στο οποίο εχουν πρόσβαση χρήστες, υπολογιστές, ομάδες και άλλα αντικείμενα.

Το organizational unit είναι αντικείμενο μέσα στο Active directory όμως πιο συγκεκριμένα ,τα αντικείμενα που ανήκουν σε ένα domain μπορούν να ομαδοποιηθούν σε Οργανωτικές Μονάδες (OM). Οι OM μπορούν να παρέχουν ιεραρχία σε ένα domain, να διευκολύνουν τη διοίκησή του και να μοιάζουν με τη δομή του οργανισμού σε διαχειριστικό ή γεωγραφικό επίπεδο. Οι OM μπορούν να περιέχουν και άλλa domain OM, δηλαδή είναι τα δοχεία που το περιέχουν. Η Microsoft συνιστά τη χρήση δομικών μονάδων και όχι περιοχών για δομή και απλούστευση της εφαρμογής πολιτικών και διοίκησης. Οι ΟΜ είναι το επιλεγόμενο επίπεδο στο οποίο πρέπει να εφαρμόζετε τις πολιτικές ομάδας, οι οποίες είναι αντικείμενα Active Directory που ονομάζονται επίσημα αντικείμενα πολιτικής ομάδας, παρόλο που οι πολιτικές μπορούν επίσης να εφαρμοστούν σε domains ή sites.

Θέμα 5ο.  Η brute-force attack (επίθεση ωμής βίας) αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Συχνά, όμως, ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας πιο "πιθανά", κατά την άποψή, του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών. Για αυτόν τον λόγο εγώ θα επέλεγα τις εξής πολιτικές : α) Όριο κλειδώματος λογαριασμού για ένα εύλογο αριθμό δοκιμής συνθηματικών στην περίπτωση που κάποιο botaki προσπαθεί να μαντέψει το συνθηματικό, β) οι κωδικοί πρόσβασης πρέπει να τηρούν τις προϋποθέσεις πολυπλοκότητας ώστε να είναι πολύ δύσκολο κάποιος να « μαντέψει» τον κωδικό και να χρειαστεί πολύ χρόνο για να τον βρει και μέγιστη διάρκεια κωδικού πρόσβασης ώστε ανά τακτά χρονικά διαστήματα να αλλάζει και να κάνει ακόμα πιο δύσκολο την « μαντέψει» του, γ) κλείδωμα λογαριασμού για ένα χρονικό διάστημα, αυτόματα το σύστημα δηλαδή θα κλειδώσει τον λογαριασμό για ένα χρονικό διάστημα ( στην περίπτωση που κάποιος ξένος ΄ξ κάποιο botaki προσπαθεί να μπει στον λογαριασμό) ή έως ότου επιβεβαιωση με άλλους τρόπους ότι είναι όντως ο ιδιοκτήτης του κωδικού.

Θέμα 6ο. 1η μέθοδος είναι η Dictionary attack, η οποια χρησιμοποιεί ένα απλό αρχείο που περιέχει λέξεις που μπορούν να βρεθούν σε ένα λεξικό. Με άλλα λόγια αυτή η επίθεση χρησιμοποιεί ακριβώς το είδος- πλήθος των λέξεων που χρησιμοποιούν πολλοί ως κωδικό πρόσβασης.

2η μέθοδος είναι η Brute force attack την οποια περιέγραψα στο θέμα 5.

3η μέθοδος είναι η Rainbow table attack η οποια είναι ένας προκαθορισμένος πίνακας για την αντιστροφή των κρυπτογραφικών λειτουργιών κατακερματισμού, συνήθως για το σπάσιμο του κωδικού πρόσβασης με κατακερματισμού. Ουσιαστικά αυτό κατακερματίζει όλους τους πιθανούς συνδυασμούς κωδικών πρόσβασης. Ο χρόνος που χρειάζεται για να σπάσει κάποιος κωδικό πρόσβασης με ένα rainbow table μειώνεται στο χρόνο που χρειάζεται για να το αναζητήσεις στη λίστα αυτή.

Θέμα 7ο. Η πολιτική τοπικής ασφάλειας ενός συστήματος είναι ένα σύνολο πληροφοριών σχετικά με την ασφάλεια ενός τοπικού υπολογιστή.

Οι πληροφορίες της τοπικής πολιτικής ασφαλείας περιλαμβάνουν τα εξής:

Domains που εμπιστεύονται την επαλήθευση των προσπαθειών σύνδεσης.

Αν θέλουμε οι ενέργειες ενός χρήστης να καταγράφονται στο αρχείο καταγραφής συμβάντων

Ποιοι λογαριασμοί χρηστών έχουν πρόσβαση στο σύστημα και πώς. Για παράδειγμα, διαδραστικά, μέσω δικτύου ή ως υπηρεσία.

Τα δικαιώματα και τα προνόμια που αποδίδονται στους λογαριασμούς.

Και την πολιτική ελέγχου ασφαλείας.

Θέμα 2ο. α) Kerberos. Tα M Windows Server εφαρμόζουν την 5η έκδοση πρωτόκολλου ελέγχου ταυτότητας και επεκτάσεων Kerberos για τo δημόσιo κλειδί. Ο πελάτης τύπου Kerberos υλοποιείται ως μια υπηρεσία παροχής υποστήριξης ασφαλείας και μπορεί να προσεγγιστεί μέσω της παροχής υποστήριξης ασφάλειας. Η πρώτη επαλήθευση του χρήστη είναι ενσωματωμένη με την γενική αρχιτεκτονική single sign-on . Το κέντρο διανομής κλειδιών Kerberos ενσωματώνεται και με άλλες υπηρεσίες ασφαλείας του Windows Server που εκτελούνται στον ελεγκτή τομέα . Το κέντρο διανομής κλειδιών χρησιμοποιεί την βάση δεδομένων της υπηρεσίας Active Directory ως βάση δεδομένων του λογαριασμού ασφάλειας . Το Active Directory απαιτείται για τις προεπιλεγμένες υλοποιήσεις του Kerberos.

β) NTLM. Είναι ένα πρωτόκολλο αυθεντικοποίησης πρόκλησης / απάντησης. Εκτός από τον έλεγχο ταυτότητας, το πρωτόκολλο NTLM παρέχει προαιρετικά την ασφάλεια της συνεδρίας, φροντίζοντας ειδικά την ακεραιότητα και την εμπιστευτικότητα του μηνύματος μέσω της υπογραφής και των λειτουργιών στεγανοποίησης.

γ)TLS/SSL. Αρκετές εκδόσεις πρωτοκόλλου Transport Layer Security, Secure Sockets Layer, Datagram Transport Layer Security, και η Ιδιωτική Επικοινωνιών Μεταφορών, βασίζονται στη κρυπτογραφία του δημόσιου κλειδιού . Ο πάροχος σουίτα πρωτόκολλο ελέγχου ταυτότητας Ασφαλές Κανάλι παρέχει αυτά τα πρωτόκολλα . Όλα τα πρωτόκολλα τύπου Ασφαλές Κανάλι χρησιμοποιούν ένα μοντέλο διακομιστή/πελάτη.

Θέμα 8ο. Σε όλες τις περιπτώσεις ακολουθούμε την ιδιά ακριβώς διαδρομή μιας και είναι στον ίδιο φάκελο όλες οι παραπάνω ενέργειες, δηλαδή ακολουθούμε την εξής διαδρομή [1\* Start -> Run - > secpol.msc](#ΟΚ) \*-> Account Policies -> Password Policy , και στη συνέχεια κάνουμε τα εξής :

1. Enforce password history -> Keep password history for 5 passwords remembered
2. Maximum password age -> Password will expire in 30 days
3. Minimum password age -> 2 days
4. Min password length -> 6 characters
5. Και VI. Password must meet complexity requirements Enabled

Θέμα 9ο Και εδώ ακολουθούμε την ιδιά ακριβώς διαδρομή όπως και στο θέμα 8 δηλαδή την διαδρομή [1\*\*](#ΟΚ) + Account Policies -> Account Lockout Policy

και στη συνέχεια ακολουθούμε την εξής διαδικασία: α) Account lockout duration 10 minutes -> β) Account lockout threshold 4 invalid logon attempts -> γ) Reset account lockout counter after Not Applicable

Θέμα 10ο . Πάλι και εδώ η διαδρομή [1\*\*](#ΟΚ) + Local Policies-> Audit Policy

και στη συνέχεια Ενεργοποιούμε τις λειτουργίες που εμφανίζονται στην λίστα Audit Policy -> και την καταγραφή συμβάντων ασφαλείας.

Θέμα 11ο. Η διαδρομή- διαδικασία [1\*\*](#ΟΚ) + Local Policies-> Audit Policy και στη συνέχεια ακολουθούμε τις εξής ενέργειες Ι) Audit account login events Success unchecked Failure checked, ΙΙ)Audit account management Success checked Failure checked , ΙΙΙ) Audit system events Success checked Failure unchecked