ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ ΕΛΕΓΧΩΝ ΔΙΕΙΣΔΥΣΗΣ

ΔΗΜΗΤΡΙΟΣ ΓΙΑΝΝΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ

ΠΕΙΡΑΙΑΣ 2011

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΜΕΛΕΤΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ ΕΛΕΓΧΩΝ ΔΙΕΙΣΔΥΣΗΣ

Δημήτριος Γιάννης

Επιβλέπων καθηγητής: Σωκράτης Κάτσικας

Η εργασία υποβάλλεται για την μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του Μεταπτυχιακού Διπλώματος Σπουδών στη Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα.

ΠΕΙΡΑΙΑΣ 2011

Αφιερώνεται στους γονείς μου.

Περίληψη

Στην παρούσα διπλωματική εργασία, καταγράφεται η εμπεριστατωμένη μελέτη και έρευνα των ελέγχων και δοκιμών διεισδυτικότητας, που δύνανται να διενεργηθούν στα πλαίσια των ελέγχων ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού. Εξετάζονται οι τεχνικές και οι μεθοδολογίες που αποτελούν βέλτιστη πρακτική για την εκτέλεση του ελέγχου, καθώς επίσης γίνεται μελέτη του βέλτιστου δυνατού συνδυασμού αυτών για την αποδοτικότερη και αποτελεσματικότερη διενέργεια τους.

Ο αντικειμενικός σκοπός της εργασίας αυτής είναι να καλύψει το πεδίο των ελέγχων και των δοκιμών διεισδυτικότητας τόσο από την σκοπιά της διαχείρισης και της ανάλυσης ασφάλειας, όσο και από την σκοπιά των τεχνολογικών απαιτήσεων ασφάλειας ενός οργανισμού. Η προσπάθεια για πλήρη καταγραφή και μελέτη τόσο των υπαρχόντων διαδικασιών και των μεθοδολογιών, όσο και των υφιστάμενων τεχνικών του ελέγχου, ανταποκρίνεται αντίστοιχα τόσο στις επιχειρησιακές ανάγκες του διοικητικού προσωπικού ενός οργανισμού που ασχολούνται με την ασφάλεια αυτού, όπως για παράδειγμα του Υπεύθυνου Ασφάλειας Πληροφοριών αυτού και των ελεγκτών πληροφοριακών συστημάτων όσο και στις τεχνολογικές απαιτήσεις του διαχειριστή ασφάλειας πληροφοριακών συστημάτων των μηχανικών ασφάλειας και των διαχειριστών συστημάτων και δικτύων

Λέξεις Κλειδιά: Έλεγχος Διεισδυτικότητας, Ευπάθειες, Ρήξη ασφάλειας, Αποτίμηση Ευπαθειών

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή του Πανεπιστημίου Πειραιά κ. Σωκράτη Κ. Κάτσικα για την αμέριστη συμπαράσταση, επιστημονική αρωγή και διάθεση που επέδειξε κατά τη διάρκεια της φοίτησής μου στο μεταπτυχιακό πρόγραμμα του τμήματος Διδακτικής της Τεχνολογίας και Ψηφιακά Συστήματα.

Επίσης θα ήθελα να ευχαριστήσω τους προϊσταμένους μου στο χώρο εργασίας μου, για τις πληροφορίες τις οποίες μου παρείχαν καθώς και τη συμπαράσταση τους καθόλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας μου.

Τέλος, εκφράζω την ευγνωμοσύνη μου στην οικογένεια μου και ειδικά στους γονείς μου οι οποίοι με νουθέτησαν διαχρονικά με αξίες και ιδανικά ώστε εν' τέλει να ανταποκριθώ στο επίπονο έργο του μεταπτυχιακού προγράμματος σπουδών.

Περιεχόμενα

Εισαγωγή

Γενικά

Σήμερα, οι συνεχείς και αυξανόμενες απαιτήσεις διαχείρισης πληροφοριών σε κάθε τομέα της κοινωνικής ζωής του σύγχρονου ανθρώπου, οδηγούν στην ανάπτυξη ολοένα και πολυπλοκότερων υπολογιστικών συστημάτων και δικτύων. Η επιστήμη της πληροφορικής καθώς και τα συστήματα που την υποστηρίζουν έχουν πλέον αλλάξει ρόλο. Την δεκαετία του ΄90 ο ρόλος τους ήταν κυρίως υποστηρικτικός, ενώ πλέον η χρήση πληροφοριακών συστημάτων συμβάλει σε μεγάλο ποσοστό στην ανάληψη κρίσιμων αποφάσεων ενώ ταυτόχρονα διατηρεί και τον υποστηρικτικό ρόλο που ήδη είχε επωμιστεί.

Πλέον, η πληροφορική αποτελεί βασικό -εάν όχι το πιο βασικό- κομμάτι της διαχείρισης κρίσιμων πληροφοριών και υποδομών, με αποτέλεσμα η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών και των συστημάτων να αποτελούν προτεραιότητα για το δυναμικό που τα διαχειρίζεται. Η συνεχώς αυξανόμενη πολυπλοκότητα των συστημάτων πληροφορικής έχει την τάση να διαβάλλει τις παραπάνω τρεις θεμελιώδεις αρχές της ασφάλειας των πληροφοριών και των συστημάτων που τις υποστηρίζουν. Επιπλέον, η χρήση πληροφοριακών συστημάτων στον τομέα των κρίσιμων υποδομών όπως για παράδειγμα τα δίκτυα ύδρευσης, ηλεκτρισμού, τηλεπικοινωνιών και συγκοινωνιών, τα καθιστούν ως στόχο κακόβουλων ενεργειών από ομάδες ατόμων, επιχειρήσεων, ακόμα και κυβερνήσεων που επωφελούνται από την κατάρρευση τους. Κυβερνοεπιθέσεις σε κρατικά συστήματα πληροφοριών, σε συστήματα διαχείρισης ερευνητικών έργων μεγάλης κλίμακας, αλλά και σε βιομηχανικά συστήματα έχουν δημοσιευτεί στο παρελθόν και συνεχίζουν και αναφέρονται.

Επιτακτική είναι επίσης και η ανάγκη για την ύπαρξη ασφάλειας πληροφοριακών συστημάτων στο περιβάλλον των χρηματοπιστωτικών ιδρυμάτων και οργανισμών, η οποία αποτελεί στην περίπτωση της Ελλάδας, κανονισμό της Τραπέζης της Ελλάδος. Στις μέρες μας, κοινή πρακτική αποτελεί πλέον η πλειονότητα των τραπεζικών ιδρυμάτων να εντάσσει στις προσφερόμενες της υπηρεσίες, υπηρεσίες ηλεκτρονικής τραπεζικής (e-banking services). Στο

παρελθόν, έχουν καταγραφεί πολλές επιθέσεις στα πληροφοριακά συστήματα των τραπεζών που εξυπηρετούν συναλλαγές μέσω του παγκόσμιου ιστού. Όπως είναι κατανοητό, τέτοιου είδους επιθέσεις δύναται να εκθέσουν μια τράπεζα σε όλους τους κινδύνους που τη διατρέχουν όπως αυτοί περιγράφονται από τον πρώτο πυλώνα του Σύμφωνου της Βασιλείας ΙΙ και να εγείρουν ζητήματα κανονιστικής συμμόρφωσης με τους διαφόρους ελεγκτικούς και εποπτικούς φορείς. Παράλληλα με τω ανωτέρω, υπάρχουν και οι επιπτώσεις στους πελάτες μιας τράπεζας η οποία έχει δεχτεί επίθεση στο πληροφοριακό σύστημα ηλεκτρονικής τραπεζικής. Εάν διαβληθεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα δεδομένων του συστήματος, δύναται να προκληθεί διαρροή ευαίσθητων προσωπικών δεδομένων πελατών όπως επίσης και οικονομικές απώλειες λόγω πρόσβασης σε οικονομικά στοιχεία λογαριασμών.

Έτσι, η αναγκαιότητα για την ύπαρξη ασφάλειας στα πληροφοριακά συστήματα και τις πληροφορίες, έχει οδηγήσει τα τελευταία χρόνια την επιστημονική κοινότητα στην μελέτη και ανάπτυξη μεθόδων και τεχνικών διαχείρισης ασφάλειας (security management). Ένα μέρος της διαδικασίας αυτής αποτελεί και η διαχείριση της επικινδυνότητας (risk management). Η διαχείριση της επικινδυνότητας ως έργο, αποτελείται από διαφορετικά στάδια ανάπτυξης και ολοκλήρωσης. Ένα από τα σταδία αυτά είναι και η αποτίμηση των αδυναμιών και των απειλών (threat and vulnerability assessment) οι οποίες επιδρούν στην αυξομείωση του βαθμού επικινδυνότητας ενός Πληροφοριακού Συστήματος. Σε ιδιαιτέρως κρίσιμα περιβάλλοντα, όπως για παράδειγμα τα χρηματοπιστωτικά ιδρύματα και οι οργανισμοί διαχείρισης κρίσιμων υποδομών, εφαρμόζονται μέθοδοι και τεχνικές ελέγχου ασφάλειας, οι οποίες αξιοποιούν τα αποτελέσματα που απορρέουν από ήδη υπάρχουσες αποτιμήσεις ασφάλειας και ιδιαίτερα από τις αποτιμήσεις των απειλών και των αδυναμιών ενός οργανισμού. Ένας από τους ελέγχους αυτούς είναι και ο έλεγχος – δόκιμη διεισδύσεων σε συστήματα και δίκτυα συστημάτων, εφαρμόζοντας τεχνικές και μεθόδους επιθέσεων που είναι δυνατό να χρησιμοποιήσει και όποιος κακόβουλος χρήστης ή επιτιθέμενος ο όποιος έχει ως σκοπό τη διάτρηση των δικλείδων ασφάλειας ενός οργανισμού, θέτοντας σε επισφαλή θέση την εμπιστευτικότητα, ακεραιότητα και

διαθεσιμότητα των Πληροφοριακών συστημάτων και των πληροφοριών του οργανισμού.

Σκοπός

Η παρούσα διπλωματική εργασία αποσκοπεί στην ολοκληρωμένη κάλυψη των διαδικασιών και των μεθοδολογιών που ακολουθούνται κατά την εκτέλεση ενός επαρκούς ελέγχου διείσδυσης σε ένα ολοκληρωμένο περιβάλλον υπολογιστικών συστημάτων. Για την εκτέλεση ενός ολοκληρωμένου ελέγχου διείσδυσης απαιτούνται συγκεκριμένες τεχνικές γνώσεις γύρω από την ασφάλεια όλων των επιπέδων ενός πληροφοριακού συστήματος. Έτσι, στην παρούσα εργασία επιχειρείται η ανάλυση των μεθοδολογιών και των τεχνικών που ακολουθούνται κατά τη διενέργεια ελέγχων και δοκιμών διεισδυτικότητας στα πληροφοριακά συστήματα ενός οργανισμού.

Βασικές έννοιες και ορισμοί

Στα πλαίσια της μελέτης των διαδικασιών, των μεθοδολογιών και των τεχνικών γίνεται συχνή χρήση συγκεκριμένων όρων πληροφορικής, οι όποιοι επεξηγούνται στις επόμενες παραγράφους με σκοπό την άμεση κατανόηση του κειμένου στο οποίο εμπεριέχονται.

Οι όροι αυτοί καθώς και οι βασικές έννοιες που χρησιμοποιούνται είναι οι εξής παρακάτω:

Υπολογιστικό Συγκρότημα (IT Assembly) θεωρείται η συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιείται για τη διαχείριση πληροφοριών.

Υπολογιστικό Σύστημα (IT System) θεωρείται το υπολογιστικό συγκρότημα το οποίο είναι εγκατεστημένο σε συγκεκριμένη τοποθεσία, με συγκεκριμένο λειτουργικό περιβάλλον, που ανταποκρίνεται σε συγκεκριμένο σκοπό.

Πληροφοριακό Σύστημα (Information System) ένα οργανωμένο σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείρισης πληροφορίας, για την υποστήριξη των ανθρωπίνων δραστηριοτήτων, στα πλαίσια του οργανισμού.

Ασφάλεια (Security) είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατεύουν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή.

Ευπάθεια (Vulnerability) μπορεί να θεωρηθεί η κάθε αδυναμία ή ελάττωμα στο υλικό, στο λογισμικό ή στην αρχιτεκτονική ενός συστήματος, καθώς και στις διαδικασίες ασφάλειας που ακολουθούνται, που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του εν λόγω συστήματος.

Απειλή (Threat) ενός συστήματος είναι το κάθε άτομο, δραστηριότητα ή συμβάν που είναι δυνατόν να προκαλέσει παραβίαση της διαθεσιμότητας, ακεραιότητας ή εμπιστευτικότητας σε οποιοδήποτε σύστημα το οποίο χρησιμοποιείται για την παρακολουθήσει, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας. Οι απειλές μπορεί να είναι τυχαίες ή σκόπιμες και μπορεί να προέρχονται από το εσωτερικό ή το εξωτερικό ενός παρόχου διαδικτύου.

Διαχείριση Επικινδυνότητας (Risk Management) μπορεί να οριστεί η δομημένη προσέγγιση της διαχείρισης της αβεβαιότητας σε σχέση με τις απειλές, της ακολουθίας των ανθρωπίνων δραστηριοτήτων (αποτίμηση επικινδυνότητας, στρατηγικές διαχείρισης επικινδυνότητας) και του μετριασμού του κινδύνου. Όπως είναι κατανοητό, αναπόσπαστα μέρη της διαχείρισης επικινδυνότητας είναι η αναγνώριση της επικινδυνότητας και η αποτίμηση αυτής.

Έλεγχος/Δόκιμη Διείσδυσης (penetration test) μπορεί να οριστεί ως η μέθοδος αξιολόγησης της ασφάλειας των συστημάτων πληροφορικής και των δικτύων

αυτών, εξομοιώνοντας επιθέσεις στα συστήματα αυτά, με τρόπο παρόμοιο με αυτόν που θα ακολουθούσε ένας κακόβουλος χρήστης

Ιστορική Αναδρομή

Το penetration testing είναι μια από τις παλαιότερες μεθόδους αξιολόγησης της ασφάλειας ενός πληροφοριακού συστήματος. Χαρακτηριστικά, στις αρχές της δεκαετίας του 70 το penetration testing χρησιμοποιούταν με σκοπό την επίδειξη απουσίας ασφάλειας στα πληροφοριακά συστήματα και αποτελούσε μέσο πίεσης προς το υπουργείο άμυνας των Ηνωμένων Πολιτειών να αναπτύξει προγράμματα έρευνας με σκοπό τη δημιουργία ασφαλέστερων λειτουργικών συστημάτων. Τελικά, το penetration testing ως μεθοδολογία ενσωματώθηκε στο Trusted Product Evaluation Program (TPEP), τα αποτελέσματα του οποίου αξιολογούνται από το Εθνικό Κέντρο Ασφάλειας Υπολογιστικών Συστημάτων (National Computer Security Center- NCSC), οργανικής μονάδας της Υπηρεσίας Εθνικής Ασφάλειας των Η.Π.Α (National Security Agency - NSA).

Παρούσα Χρήση

Ο έλεγχος διεισδυτικότητας χρησιμοποιείται από οργανισμούς οι οποίοι ανήκουν σε όλους τους τομείς της κοινωνικής και επιχειρησιακής δραστηριότητας του ανθρώπου στις μέρες μας. Πολλές επιχειρήσεις και οργανισμοί αξιοποιούν το συγκεκριμένο έλεγχο λόγω της ιδιαιτερότητας του -δηλαδή τον έλεγχο από την σκοπιά του επιτιθέμενου- με σκοπό να αποτιμήσουν και αξιολογήσουν τις δικλείδες ασφάλειας τους. Πολλές φορές μάλιστα η ύπαρξη των συγκεκριμένων ελέγχων αποτελεί αντικείμενο κανονιστικής συμμόρφωσης διαφόρων εποπτικών φορέων επιχειρήσεων και οργανισμών, που δραστηριοποιούνται στην Τραπεζική, στην Υγεία και την Ασφάλεια κρίσιμων υποδομών.

Για παράδειγμα, στο χώρο των χρηματοπιστωτικών ιδρυμάτων και συγκεκριμένα στην ελληνική επικράτεια, η Τράπεζα της Ελλάδος επιβάλει στα χρηματοπιστωτικά ιδρύματα περιοδικό έλεγχο του δικτύου της από εξωτερικές εταιρείες οι οποίες εξειδικεύονται στο αντικείμενο των ελέγχων ασφάλειας.

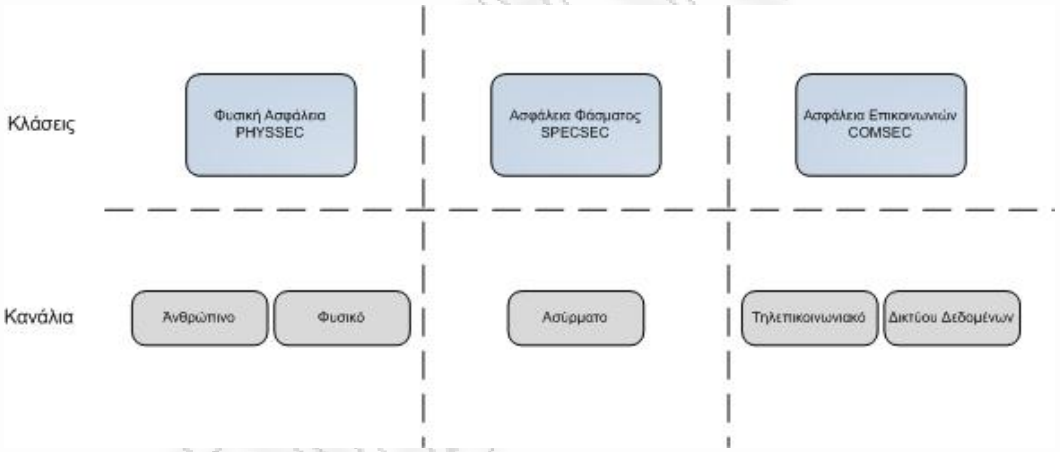
Παράλληλα, ο έλεγχος διεισδυτικότητας υποστηρίζεται ότι μπορεί να προσφέρει περεταίρω συμμόρφωση του εθνικού συστήματος υγείας της Μεγάλης Βρετανίας με το πρότυπο HIPAA οπότε και αξιοποιείται για τον σκοπό αυτό.

ΚΕΦΑΛΑΙΟ 1^{ο}

Χαρακτηριστικά Ελέγχων Διείσδυσης

1.1. Εύρος Δοκιμών

Ως εύρος δοκιμών θεωρείται το συνολικό επιχειρησιακό περιβάλλον ασφάλειας των πληροφοριακών πόρων. Το περιβάλλον αυτό οριοθετείται σε τρείς διαφορετικές κλάσεις οι οποίες αποτελούνται από πέντε διακριτά κανάλια. Τα κανάλια χαρακτηρίζουν τον τρόπο αλληλεπίδρασης του περιβάλλοντος των πόρων με αυτούς. Ο διαχωρισμός αυτός υφίσταται ώστε να κατηγοριοποιηθούν οι απαιτήσεις για τις δοκιμές ασφάλειας τόσο σε ανθρώπινο δυναμικό και την εξειδίκευσή που αυτό πρέπει να φέρει, καθώς και στον υλικοτεχνικό εξοπλισμό που πρέπει να χρησιμοποιηθεί σε κάθε περίπτωση δοκιμής. Συνοπτικά, οι κλάσεις και τα κανάλια αλληλεπίδρασής με τους πόρους παρουσιάζονται στην παρακάτω εικόνα.



Εικόνα 1

Ανθρώπινο κανάλι. Το συγκεκριμένο κανάλι αποτελεί την ανθρώπινη διεπαφή επικοινωνίας με τους πόρους και το περιβάλλον αυτών και περιλαμβάνει τους άμεσους (π.χ. φυσική) ή έμμεσους τρόπους (π.χ. ψυχολογική) αλληλεπίδρασης που μπορεί να έχει ο ανθρώπινος παράγοντας με αυτά.

Φυσικό κανάλι. Στο φυσικό κανάλι περιλαμβάνονται οι τρόποι αλληλεπίδρασης που έχει το φυσικό περιβάλλον με το σύστημα.

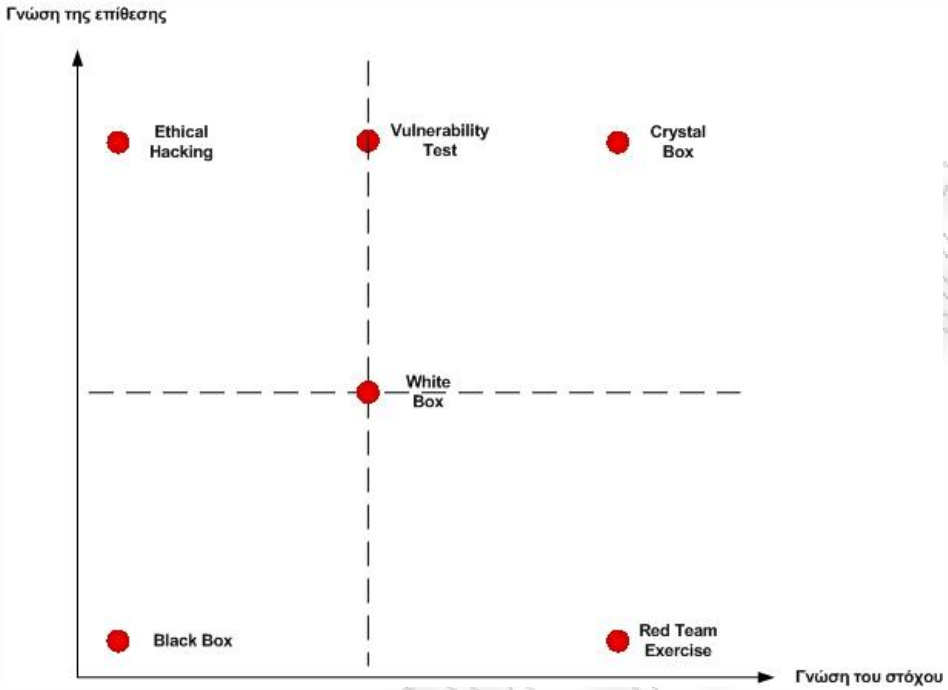
Ασύρματο κανάλι. Το ασύρματο κανάλι περιλαμβάνει το σύνολο των επικοινωνιών που μπορούν να επιτευγχθούν με το σύστημα στο ηλεκτρομαγνητικό φάσμα.

Τηλεπικοινωνιακό κανάλι. Στο συγκεκριμένο κανάλι περιλαμβάνεται το σύνολο των επικοινωνιών όπου μπορούν να επιτευγχθούν με το σύστημα μέσω τηλεφωνικών ή άλλων παρόμοιων συνδέσεων.

Κανάλι Δικτύου δεδομένων. Το κανάλι δικτύου δεδομένων περιλαμβάνει όλα τα συστήματα και τα δίκτυα διαμέσου ενσύρματων τηλεπικοινωνιακών γραμμών.

1.2. Τύποι Δοκιμών

Οι δοκιμές και οι έλεγχοι ασφάλειας σε μια πληροφοριακή υποδομή κατατάσσονται σε κατηγορίες ανάλογα με τις πληροφορίες που επιθυμεί να εξάγει κάθε φορά ο ελεγκτής. Οι κατηγορίες αυτές μπορούν να εκφραστούν και ως τύποι οι οποίοι δεν είναι πάντοτε περιοριστικοί, καθώς μπορούν να χρησιμοποιηθούν παραλλαγές αλλά και συνδυασμοί αυτών, ώστε να ανταποκριθούν με τον καλύτερο δυνατό τρόπο στις απαιτήσεις ενός έλεγχου. Τα χαρακτηριστικά τα οποία διαφοροποιούν τους τύπους μεταξύ τους, είναι η γνώση του επιτιθέμενου για την υποδομή στόχο και η γνώση του στόχου για τη διεξαγωγή των δοκιμών.



Εικόνα 2

Ο πρώτος τύπος ο οποίος καθορίζεται είναι ο λεγόμενος *τυφλός (blind)*. Ο ελεγκτής αλληλεπιδρά με τον στόχο δίχως την πρωτύτερη γνώση των πόρων του, των μηχανισμών έλεγχου και ασφάλειας καθώς και των καναλιών επικοινωνίας που αυτός διαθέτει. Από την αμυνόμενη πλευρά ο στόχος είναι προετοιμασμένος για τον έλεγχο που θα διενεργηθεί και γνωρίζει όλες τις λεπτομέρειες του έλεγχου. Ο σκοπός των τυφλών ελέγχων είναι πρωτίστως η δοκιμή των ικανοτήτων του ελεγκτή. Το βάθος και η αξία των ευρημάτων του έλεγχου είναι ανάλογα τόσο με τις γνώσεις όσο και με την επάρκεια του ελεγκτή που διενεργεί τις δοκιμές ασφάλειας.

Ο δεύτερος τύπος των δοκιμών ασφάλειας είναι ο *Διπλά Τυφλός (Double Blind).* Ο τύπος αυτός είναι ευρύτερα γνωστός με την ονομασία black box testing. Το σύστημα – στόχος αντιμετωπίζεται ως ένα μαύρο κουτί από τον ελεγκτή για το οποίο δεν υπάρχει πρωτύτερη γνώση των πόρων του, των μηχανισμών ασφαλείας και των καναλιών επικοινωνίας που αυτό διαθέτει. Παράλληλα, ο στόχος δεν γνωρίζει το εύρος του έλεγχου, τα κανάλια επικοινωνίας που θα ελεγχτούν όπως επίσης και τις παραμέτρους του έλεγχου. Ο σκοπός των δοκιμών αυτών είναι η αξιολόγηση αφενός των ικανοτήτων και τις επάρκειας του ελεγκτή, αφετέρου του

επιπέδου ετοιμότητας του συστήματος σε μια ενδεχόμενη επίθεση. Το βάθος του έλεγχου εξαρτώνται από την επάρκεια και τις τεχνικές δεξιότητες και ικανότητες του ελεγκτή του συστήματος.

Ο τρίτος τύπος ελέγχων – δοκιμών ονομάζεται *Gray Box* . Για τη διενέργεια των ελέγχων αυτών ο ελεγκτής έχει περιορισμένη γνώση των αμυντικών μηχανισμών και των πόρων του στόχου, ενώ γνωρίζει πλήρως τα κανάλια επικοινωνίας με αυτόν. Από την άλλη μεριά, ο στόχος έχει πλήρη επίγνωση του εύρους και των λεπτομερειών του υπό διενέργεια έλεγχου. Ο σκοπός του έλεγχου είναι αφενός η αξιολόγηση της ετοιμότητας και της επάρκειας των μηχανισμών άμυνας που διαθέτει το ελεγχόμενο σύστημα σε μη αναμενόμενες συνθήκες επίθεσης σε αυτό, αφετέρου είναι η αξιολόγηση της επάρκειας του ελεγκτή υπό συγκεκριμένες συνθήκες.

Ο τέταρτος τύπος δοκιμών ονομάζεται *Double Gray Box* ή όπως είναι ευρύτερα γνωστός White Box. Οι παράμετροι του έλεγχου για τον ελεγκτή είναι οι ίδιες με τον Gray Box τύπο, δηλαδή υπάρχει περιορισμένη γνώση των πόρων και των μηχανισμών ασφάλειας του στόχου και πλήρης επίγνωση των καναλιών επικοινωνίας. Η διαφοροποίηση έγκειται στο γεγονός ότι στον Double Gray έλεγχο ο ελεγχόμενος γνωρίζει το εύρος του έλεγχου καθώς και το χρονοδιάγραμμα αυτού, αλλά δεν γνωρίζει τα κανάλια επικοινωνίας τα οποία θα ελεγχτούν. Ο σκοπός του έλεγχου είναι η καλύτερη αξιολόγηση της ετοιμότητας και της επάρκειας του συστήματος σε μη αναμενόμενες συνθήκες και όπως και στους υπόλοιπους τύπους έλεγχου η αξιολόγηση ης επάρκειας του ελεγκτή.

Ο επόμενος τύπος ελέγχου έχει την ονομασία *Tandem.* Ο συγκεκριμένος έλεγχος είναι γνωστός και ως Crystal Box Audit. Στην περίπτωση των ελέγχων αυτών ο ελεγκτής γνωρίζει λεπτομερώς το περιβάλλον του συστήματος – στόχου και το σύστημα έχει επίγνωση όλων των λεπτομερειών του έλεγχου. Στον έλεγχο αυτό δοκιμάζονται όλα τα μέτρα προστασίας και άμυνας του συστήματος. Το μειονέκτημα των ελέγχων αυτών είναι ότι δεν ελέγχεται η ετοιμότητα και η ακολουθουμένη αντίδραση του συστήματος στόχου σε απρόβλεπτες συνθήκες και καταστάσεις. Το βάθος και τα αποτελέσματα του έλεγχου εξαρτώνται άμεσα

από την ποιότητα των πληροφοριών προ του έλεγχου και στην ικανότητα και την επάρκεια του ελεγκτή.

Ο τελευταίος τύπος ελέγχων ονομάζεται *Reversal* τύπος. Η διαφοροποίηση του σε σχέση με τον Tandem τύπο έλεγχου έγκειται στο γεγονός ότι ο ελεγχόμενος δεν γνωρίζει απολύτως καμιά παράμετρο του έλεγχου, δηλαδή το πώς, το ποτέ και το τι θα ελέγξει από το σύστημα στόχο. Αντιθέτως όπως και στον προηγούμενο τύπο ελέγχων ο ελεγκτής έχει πλήρη γνώση του περιβάλλοντος έλεγχου.

Συνοπτικά, στο παρακάτω πινάκα παρουσιάζονται οι παράμετροι που χαρακτηρίζουν και διαφοροποιούν τους ελέγχους.

	Blind	**Double Blind**	**Gray Box**	**Double Gray Box**	**Tandem**	**Reversal**
Πλήρης γνώση περιβάλλοντος					✓	✓
Περιορισμένη γνώση περιβάλλοντος			✓	✓		
Μηδενική γνώση περιβάλλοντος	✓	✓				
Πλήρης γνώση έλεγχου	✓		✓		✓	
Περιορισμένη γνώση ελέγχου				✓		
Μηδενική γνώση έλεγχου		✓				✓

Πίνακας 1

ΚΕΦΑΛΑΙΟ 2^{ο}

Μεθοδολογίες Ελέγχων Διείσδυσης Δικτύων

2.1. ISECOM-Εγχειρίδιο Ελέγχου Ασφάλειας Ανοικτού Κώδικα (OSSTMM)

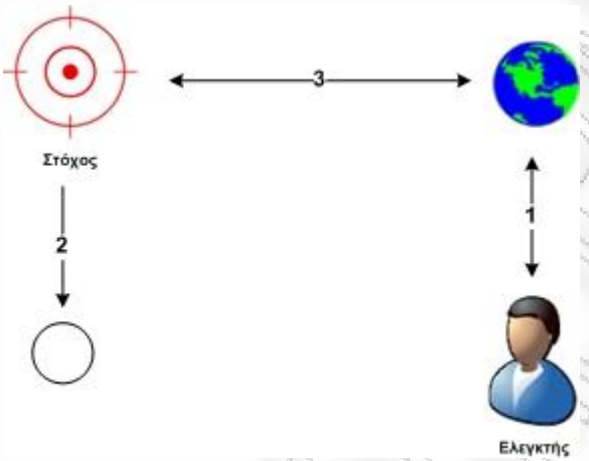
Το OSSTMM αποτελεί ένα πρακτικό εγχειρίδιο ελέγχου ασφάλειας το οποίο εκδίδεται από τον ISECOM (Institute for Security and Open Methodologies), έναν μη κερδοσκοπικό οργανισμό με έδρα τις Ηνωμένες Πολιτείες και την Ισπανία.

Το συγκεκριμένο εγχειρίδιο αποτελεί τη σύνθεση της γνώσης η οποία πηγάζει από την εκτενή μελέτη και τα έτη εμπειρίας των ανθρώπων του οργανισμού πάνω στην ασφάλεια και τον έλεγχο των πληροφοριακών συστημάτων. Η δημιουργία του κινήθηκε με γνώμονα τη συμμόρφωση με νομοθετικά και κανονιστικά πλαίσια (πχ Sarbanes-Oxley Act) όπως επίσης και με πολιτικές και πρότυπα ασφάλειας τα οποία εφαρμόζονται σε διεθνές επίπεδο (πχ ISO 27001-2005).

2.1.1. Σκοπός

Ο σκοπός του OSSTMM είναι η παροχή μιας επιστημονικής μεθοδολογίας, η οποία θα αξιοποιηθεί για τον ακριβή χαρακτηρισμό της επιχειρησιακής ασφάλειας ενός οργανισμού, διαμέσω της εξέτασης και της συσχέτισης των αποτελεσμάτων των δοκιμών που θα πραγματοποιηθούν. Το συγκεκριμένο εγχειρίδιο δύναται να αξιοποιηθεί στο σύνολο σχεδόν των ελέγχων ασφάλειας σε έναν οργανισμό, συμπεριλαμβάνοντας τις αποτιμήσεις ασφάλειας, τις αποτιμήσεις ευπαθειών καθώς και τους ελέγχους διεισδυτικότητας. Ο αναλυτικός και ολοκληρωμένος έλεγχος ασφάλειας, η συγκεκριμενοποίηση μετρικών ασφάλειας και οι κανόνες εμπλοκής που περιγράφονται στο εν λόγω εγχειρίδιο αποσκοπούν στην ορθότητα, επάρκεια και νομιμότητα των ελέγχων που εκτελούνται εντός ενός οργανισμού ανεξάρτητα του εύρους και του μεγέθους του.

2.1.2. Διαδικασία Δοκιμών



Εικόνα 3

Το OSSTMM εισάγει την έννοια της διαδικασίας των τεσσάρων σημείων η οποία διέπει τη διεξαγωγή ενός ελέγχου ασφάλειας. Με την εισαγωγή αυτή, το εγχειρίδιο διακριτοποιεί τις φάσεις του ελέγχου από την έναρξη έως και την ολοκλήρωση αυτού. Τα σημεία τα οποία χαρακτηρίζουν τη διαδικασία του ελέγχου είναι τα παρακάτω:

Εισαγωγή. Είναι το σημείο κατά το οποίο διερευνώνται οι βασικές αρχές που διέπουν το σύστημα-στόχο και αποτελούν χαρακτηριστικά του περιβάλλοντος που το περιβάλλει.

Έρευνα. Στο σημείο αυτό διερευνώνται τα ίχνη του συστήματος και τυχόν απόρροιες αυτού κατά τη εκτέλεση διαφόρων λειτουργικών διαδικασιών.

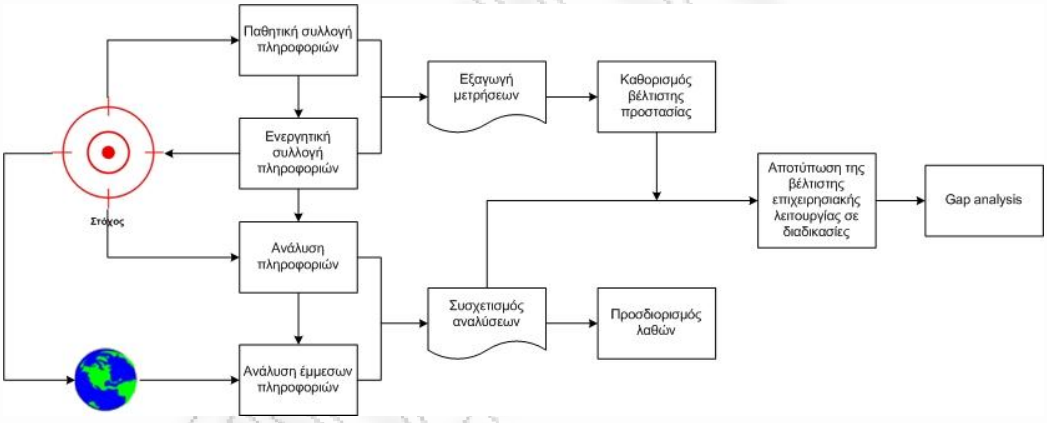
Αλληλεπίδραση. Στο σημείο αυτό, ο ελεγκτής εκτελεί διάφορες ερωτήσεις στο σύστημα με σκοπό να μελετήσει την αντίδραση του συστήματος.

Παρέμβαση. Το επόμενο σημείο είναι αυτό της παρέμβασης, κατά το οποίο ο ελεγκτής θα επέμβει μεταξύ του συστήματος και του περιβάλλοντος του, με σκοπό να διερευνήσει τις ακραίες καταστάσεις στις οποίες θα προκληθεί αστάθεια κατά την εκτέλεση των λειτουργικών διαδικασιών.

Για την ολοκλήρωση της διαδικασίας ελέγχου και συνεπώς της διαδικασίας δοκιμών παρείσδυσης, το εγχειρίδιο καθορίζει τις λειτουργικές απαιτήσεις που πρέπει να διέπουν έναν έλεγχο. Οι απαιτήσεις αυτές τίθενται υπό την μορφή ερωτημάτων που πρέπει να απαντηθούν και συγκεκριμένα:

- Πως δουλεύουν οι υπάρχουσες λειτουργίες του συστήματος;
- Λειτουργούν διαφορετικά σε σχέση με το πώς έπρεπε να λειτουργούν;
- Πώς πρέπει να λειτουργούν;

Συνδυάζοντας τη διαδικασία των τεσσάρων σημείων και τις απαιτήσεις των δοκιμών, το OSSTMM καθορίζει τα βήματα που πρέπει να ακολουθηθούν και τα οποία περιγράφονται στην παρακάτω εικόνα.



Εικόνα 4

Βήμα 1^{ο} Παθητική συλλογή πληροφοριών. Στο βήμα αυτό επιχειρείται η συλλογή πληροφοριών δίχως την επίτευξη άμεσων αλληλεπιδράσεων με το σύστημα στόχο.

Βήμα 2^{ο} Ενεργητική συλλογή πληροφοριών. Στο βήμα αυτό επιχειρείται η συλλογή πληροφοριών μέσω δοκιμών που αποκλίνουν από τις συνήθεις λειτουργίες του συστήματος.

Βήμα 3^{ο} Ανάλυση πληροφοριών. Στο βήμα αυτό αναλύονται τα δεδομένα τα οποία προέρχονται απευθείας από το σύστημα στόχο.

Βήμα 4ο Ανάλυση έμμεσων πληροφοριών. Στο βήμα αυτό αναλύονται τα δεδομένα τα οποία προέρχονται από τρίτες πηγές.

Βήμα 5ο Συσχετισμός αναλύσεων. Στο βήμα αυτό επιτυγχάνεται ο συσχετισμός των πληροφοριών που προκύπτουν από την ανάλυση των δεδομένων που πραγματοποιήθηκε στα βήματα 4 και 5, ώστε να καθοριστούν οι λειτουργικές διαδικασίες ασφάλειας του συστήματος.

Βήμα 6ο Προσδιορισμός λαθών. Στο βήμα αυτό προσδιορίζονται τα λάθη τα οποία έχουν ενδεχομένως προκύψει από το συσχετισμό των αναλύσεων του προηγούμενου βήματος.

Βήμα 7ο Εξαγωγή μετρήσεων. Στο βήμα αυτό αντλούνται οι μετρικές οι οποίες προέρχονται από τη συλλογή πληροφοριών που επιτεύχθηκε στα βήματα 1 και 2.

Βήμα 8ο Καθορισμός βέλτιστης προστασίας. Στο βήμα αυτό αξιολογούνται τα αποτελέσματα του βήματος 7 και καθορίζονται οι βέλτιστες δικλείδες ασφάλειας που απαιτούνται για την αναβάθμιση του επιπέδου ασφάλειας.

Βήμα 9ο Αποτύπωση της βέλτιστης επιχειρησιακής λειτουργίας σε διαδικασίες. Στο βήμα αυτό αποτυπώνεται η βέλτιστη κατάσταση των λειτουργιών με τις λειτουργικές διαδικασίες ασφάλειας

Βήμα 10ο GAP Analysis. Στο βήμα αυτό επιχειρείται η ανάλυση της διαφοροποίησης από την βέλτιστη κατάσταση ώστε να αποτυπωθούν οι αναγκαίοι μηχανισμοί οι οποίοι πρέπει να υλοποιηθούν για την επίτευξη της βέλτιστης επιχειρησιακής κατάστασης.

2.1.3. Φάσεις Δοκιμών

Το εγχειρίδιο OSSTMM διακριτοποιεί τους ελέγχους ασφάλειας σε τέσσερεις φάσεις και οι οποίες λαμβάνουν χώρα σε κάθε έλεγχο ασφάλειας είτε αυτός πρόκειται για έλεγχο εφαρμογών ιστού, είτε για έλεγχο δικτύου δεδομένων.

Σε κάθε φάση γίνεται έλεγχος διαφορετικού βάθους χωρίς ωστόσο αυτό να σημαίνει ότι μία φάση είναι υψηλότερης σημασίας από κάποια άλλη, οπότε και πρέπει να δοθεί ίση βαρύτητα και στις τέσσερεις.

Κάθε φάση διαιρείται σε τμήματα (modules) τα οποία καθορίζουν τα βήματα που θα ακολουθηθούν κατά τη διενέργεια των ελέγχων.

2.2.3.1. Εισαγωγική φάση

Στην παρούσα φάση γίνεται η προσπάθεια της κατανόησης των απαιτήσεων του ελέγχου, του εύρους και των περιορισμών που διέπουν τον έλεγχο ασφάλειας. Η φάση αυτή είναι καταλυτική ώστε να αποφασιστεί ο τύπος του ελέγχου που θα διενεργηθεί. Τα τμήματα αυτά είναι τα παρακάτω:

Επιθεώρηση θέσης

Στο παρόν βήμα επιθεωρούνται οι κανονισμοί, η νομοθεσία, και οι πολιτικές οι οποίες τυχόν διέπουν τον στόχο και αποτελεί σημαντικό για την ορθή εκτέλεση της φάσης αναζήτησης και ερευνών που περιγράφεται στη συνέχεια.

Λεπτομέρειες στόχου

Στο παρόν βήμα επιχειρείται η μέτρηση των τυχόν περιορισμών που υφίστανται στην αλληλεπίδραση με τον στόχο. Τέτοιος περιορισμός ενδέχεται να είναι για παράδειγμα η απόσταση του στόχου και αποτελεί κρίσιμο βήμα ώστε να διευθυνσιοδοτηθούν οι περιορισμοί του ελέγχου.

Επαλήθευση αντιδράσεων

Στο συγκεκριμένο βήμα επαληθεύονται οι πρακτικές και η ευρύτητα των δυνατοτήτων αλληλεπίδρασης και αντίδρασης από και προς τον στόχο. Το συγκεκριμένο βήμα είναι χρήσιμο κατά τις φάσεις αλληλεπίδρασης και παρέμβασης.

2.2.3.2. Φάση αλληλεπιδράσεων

Με την ολοκλήρωση της παρούσας φάσης θα έχει καθοριστεί επακριβώς το εύρος του ελέγχου, καθώς σκοπός της φάσης αυτής είναι ο προσδιορισμός του

εύρους σε σχέση με τις αλληλεπιδράσεις που διατηρούν οι στόχοι με τους πληροφοριακούς πόρους.

Έλεγχος ορατότητας

Στο συγκεκριμένο βήμα καθορίζονται οι στόχοι οι οποίοι θα ελεγχθούν εντός του εύρους του ελέγχου. Με τον όρο ορατότητα εννοείται η φυσική υπόσταση των στόχων και όχι η δυνατότητα αλληλεπίδρασης μαζί τους. Έτσι, το βήμα αυτό προσβλέπει στην λεπτομερέστερη καταγραφή του εύρους του ελέγχου.

Επαλήθευση πρόσβασης

Το επόμενο βήμα που ακολουθείται είναι η μέτρηση και καταγραφή των ενδεχόμενων σημείων εισόδου στο σύστημα καθώς επίσης και των μηχανισμών αυθεντικοποίησης που ενδεχομένως υφίστανται.

Επαλήθευση σχέσεων εμπιστοσύνης

Σο βήμα αυτό επιχειρείται ο καθορισμός τυχόν σχέσεων εμπιστοσύνης που υφίστανται μεταξύ των στόχων. Σημειώνεται ότι σχέσεις εμπιστοσύνης υπάρχουν όταν ένας στόχος επιτρέπει αλληλεπιδράσεις με αυτόν.

Επαλήθευση μηχανισμών ελέγχου

Στη συνέχεια, το επόμενο βήμα είναι η μέτρηση της αποδοτικότητας διαδικασιοστρεφών μηχανισμών ελέγχων οι οποίοι διασφαλίζουν την μη αποποίηση, την εμπιστευτικότητα, την ιδιωτικότητα και την ακεραιότητα των πληροφοριών.

2.2.3.3. Φάση ερευνών-αναζητήσεων

Στην παρούσα φάση επιχειρείται η αποκάλυψη των ελλείψεων στην διαχείριση των πληροφοριών. Η φάση αυτή καθορίζει τα παρακάτω βήματα.

Επαλήθευση διαδικασιών

Στο βήμα αυτό επιχειρείται ο προσδιορισμός της ύπαρξης και της αποδοτικότητας καταγεγραμμένων επιπέδων ασφάλειας, επιχειρώντας την αντιπαραβολή των καταγεγραμμένων διαδικασιών με το πραγματικό επίπεδο ασφάλειας που παρέχεται από την εφαρμογή τους.

Επαλήθευση παραμετροποίησης

Η έρευνα της λειτουργίας των συστημάτων στόχων μέσω της διερεύνηση της υφιστάμενης παραμετροποίησης τους αποτελεί το επόμενο βήμα της φάσης ερευνών. Επιχειρείται στο βήμα αυτό να προσδιοριστούν οι προκαθορισμένες συνθήκες υπό τις οποίες λειτουργεί το σύστημα.

Επαλήθευση περιουσιακής κατάστασης

Στο παρόν βήμα γίνεται ο έλεγχος της κατοχής και της χρήσης πόρων, όπως για παράδειγμα είναι οι εφαρμογές λογισμικού για τις οποίες δεν υφίσταται νόμιμη άδεια χρήσης.

Επισκόπηση διαχωρισμού

Στο παρόν βήμα επιχειρείται ο προσδιορισμός του επιπέδου διαχωρισμού των δικαιωμάτων πρόσβασης σε πληροφοριακούς πόρους καθώς και εάν οι πληροφορίες είναι ταξινομημένες βάσει του καταγεγραμμένου διαχωρισμού των δικαιωμάτων.

Επαλήθευση αποκάλυψης

Στο παρόν βήμα επιχειρείται ο προσδιορισμός του βαθμού αποκάλυψης πληροφοριών δημοσίως και στις οποίες υφίστανται πληροφορίες οι οποίες αποκαλύπτουν την έμμεση ορατότητα του στόχου δημοσίως.

Ανταγωνιστική νοημοσύνη

Στο παρόν βήμα επιχειρείται ο προσδιορισμός δημόσιας πληροφορίας η οποία μπορεί να πλήξει εμμέσως τον στόχο. Για παράδειγμα είναι δυνατό η γνώση των επιχειρησιακών τακτικών και των διαδικασιών του στόχου να επιφέρει

μεγαλύτερο πλήγμα στον στόχο από ότι η άμεση επίθεση στους πληροφοριακούς του πόρους.

2.2.3.4. Φάση παρεμβάσεων

Επαλήθευση καραντίνας

Στο παρόν βήμα επιχειρείται ο προσδιορισμός και η μέτρηση της αποδοτικότητας των μηχανισμών αυθεντικοποίησης και της «καραντίνας» προσβάσεων σε πόρους.

Έλεγχος δικαιωμάτων

Στο παρόν βήμα γίνεται η μέτρηση και η αποτύπωση των επιπτώσεων της ελλιπους παραμετροποίησης των μηχανισμων εξουσιοδότησης που ακολουθούν ύστερα από τη διαδικασία αυθεντικοποίησης σε ένα σύστημα.

Συνέχεια εργασιών

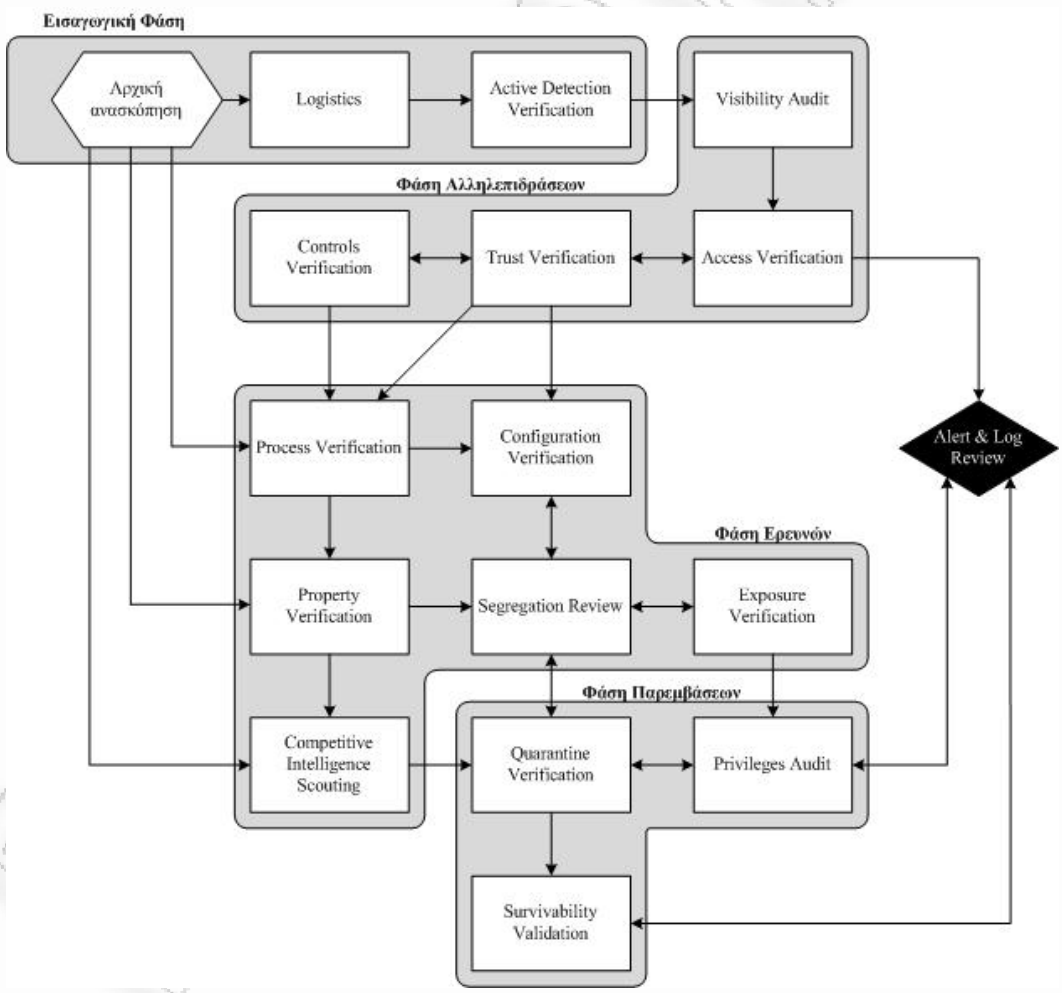
Στο παρόν βήμα προσδιορίζεται και μετράται η προσαρμοστικότητα του στόχου σε γεγονότα αλλαγών ή αστοχιών. Πιο συγκεκριμένα προσμετρείται η προσαρμοστικότητα των μηχανισμών διασφάλισης της συνέχειας υπηρεσιών σε συνθήκες (π.χ. επιθέσεις) άρνησης υπηρεσιών και άρνησης αλληλεπίδρασης του στόχου με το περιβάλλον του.

Ανασκόπηση συναγερμών

Το συγκεκριμένο βήμα αποτελεί το τελευταίο βήμα ενός ελέγχου ασφάλειας κατά το οποίο ο ελεγκτής αναλώνεται στην επισκόπηση των μηχανισμών αρχείων καταγραφής και των μηχανισμών μηνυμάτων κινδύνου (συναγερμών) που έχουν παραμετροποιηθεί σε ένα σύστημα στόχο.

2.2.4. Σύνοψη της μεθοδολογίας

Η μεθοδολογία η οποία προβλέπεται από το εγχειρίδιο OSSTMM και η οποία εκφράζεται από τη διαδικασία και τις φάσεις ελέγχου περιγράφεται στην εικόνα που ακολουθεί. Η μεθοδολογία όπως αυτή απεικονίζεται δύναται να ακολουθηθεί σε κάθε έλεγχο ασφάλειας είτε αυτός αφορά έλεγχό φυσικής ασφάλειας είτε αφορά έλεγχο διεισδυτικότητας σε πληροφοριακά συστήματα. Λόγω του γεγονότος του ότι η μεθοδολογία καλύπτει το σύνολο των τύπων ελέγχου διεισδυτικότητας που μπορεί να πραγματοποιηθούν, υφίσταται διαφορετική εμβάθυνση σε κάθε βήμα του ελέγχου ανάλογα με τον τύπο του ελέγχου ασφάλειας που θα διενεργηθεί.



Εικόνα 5

2.2. NIST-Η μεθοδολογία του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας

Το NIST (National Institute of Standards and Technology) αποτελεί το εθνικό ινστιτούτο προτύπων και τεχνολογίας των Ηνωμένων Πολιτειών της Αμερικής το οποίο είναι μη ρυθμιστική αρχή η οποία υπάγεται στο ομοσπονδιακό υπουργείο εμπορίου. Το ινστιτούτο αυτό αποτελείται από διακριτές διευθύνσεις οι οποίες ασχολούνται με καθορισμένα επιστημονικά πεδία. Η διεύθυνση ασφάλειας υπολογιστών (Computer Security Division) και συγκεκριμένα το κέντρο πηγών ασφάλειας υπολογιστών είναι αρμόδιο για τη δημοσίευση οδηγιών (guidelines) περί της ασφάλειας των πληροφοριών.

Έχουν δημοσιευτεί λοιπόν, τρεις διαφορετικές οδηγίες οι οποίες διέπουν τις δόκιμες διεισδυτικότητας και αφορούν γενικότερα τις δοκιμές ασφάλειας πληροφοριακών συστημάτων.

2.2.1. Μεθοδολογία αποτίμησης ασφάλειας πληροφοριών

Η μεθοδολογία της αποτίμησης της ασφάλειας των πληροφοριών (συμπεριλαμβανομένης και της δοκιμής διεισδυτικότητας) αποτελείται από τρείς κατ' ελάχιστον διακριτές φάσεις. Οι φάσεις αυτές είναι ο σχεδιασμός, η εκτέλεση και οι τελικές ενέργειες των ελέγχων και των δοκιμών.

Εικόνα 6

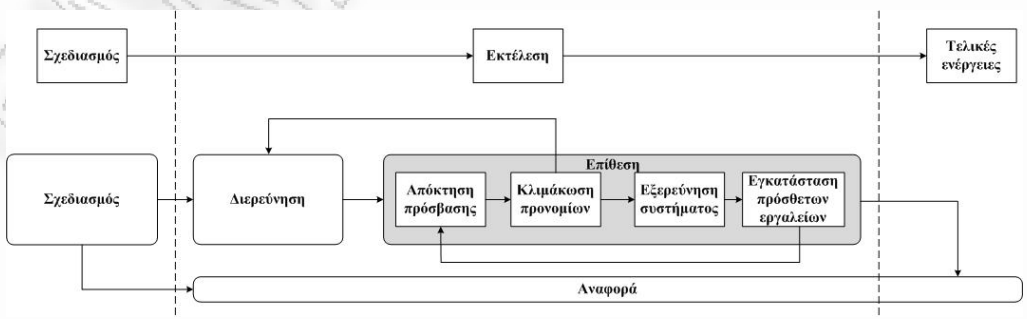
Στη φάση του σχεδιασμού συγκεντρώνονται όλες οι απαραίτητες πληροφορίες για την εκτέλεση της αποτίμησης της ασφάλειας. Τέτοιες πληροφορίες είναι οι ακριβείς πόροι για τους οποίους θα πραγματοποιηθεί ο έλεγχος, οι συνήθεις ευπάθειες που τους διέπουν και οι δικλείδες ασφάλειας που συνήθως τους προστατεύουν. Παράλληλα, προετοιμάζεται το πλάνο των δοκιμών και καθορίζονται οι διαδικασίες οι οποίες θα ακολουθηθούν κατά τη φάση εκτέλεσης. Επίσης, στη φάση του σχεδιασμού περιλαμβάνονται και όλες οι

απαιτήσεις που διέπουν τη διαχείριση ενός έργου. Τέτοιες απαιτήσεις είναι ο σκοπός των δοκιμών, το εύρος, οι λειτουργικές απαιτήσεις, οι ρόλοι και οι αρμοδιότητες των ελεγκτών, οι περιορισμοί και οι θεωρήσεις που διέπουν τους ελέγχους καθώς και το χρονικό πρόγραμμα εργασιών και τα παραδοτέα του ελέγχου. Τέλος, αφού έχουν καθοριστεί και προσδιοριστεί τα παραπάνω, οριστικοποιείται το πλάνο των δοκιμών, εγκρίνεται αρμοδίως από τον οργανισμό, και δίνεται ξεκινά η φάση της εκτέλεσης των δοκιμών.

Στη φάση της εκτέλεσης πραγματοποιούνται οι αναγκαίες ενέργειες με σκοπό τον προσδιορισμό και την επικύρωση των αδυναμιών των συστημάτων και τέλος, στις τελικές ενέργειες συγκαταλέγεται η ανάλυση των αδυναμιών ώστε να βρεθούν οι αιτίες αυτών, γίνονται προτάσεις για να περιοριστούν οι κίνδυνοι από αυτές και συντάσσεται η τελική αναφορά του ελέγχου.

2.2.2. Μεθοδολογία Penetration Testing

Όπως αναφέρθηκε και σε προγενέστερη παράγραφο, οι έλεγχοι και οι δοκιμές διεισδυτικότητας αποτελούν ένα είδος αποτίμησης της ασφάλειας των πληροφοριών. Έτσι, ο NIST εξειδικεύει τη μεθοδολογία εκτέλεσης των δοκιμών σε τέσσερεις διακριτές φάσεις. Οι φάσεις αυτές είναι ο σχεδιασμός, η φάση της διερεύνησης, η φάση της επίθεσης και τέλος η φάση της αναφοράς. Στο παρακάτω σχήμα συσχετίζονται οι φάσεις των δοκιμών διεισδυτικότητας με τις γενικές φάσεις αποτίμησης της ασφάλειας των πληροφοριών.



Εικόνα 7

2.3.2.1. Φάση σχεδιασμού

Όπως και κατά τη διάρκεια της φάσης σχεδιασμού στην αποτίμηση της ασφάλειας των πληροφοριών, έτσι και κατά τη φάση του σχεδιασμού στους ελέγχους διεισδυτικότητας οριστικοποιούνται οι κανόνες και η διαδικασία των ελέγχων, οριστικοποιείται και καταγράφεται η έγκριση της διοίκησης και τίθεται ο σκοπός του ελέγχου.

2.3.2.2. Φάση διερεύνησης

Η συγκεκριμένη φάση αποτελείται από δυο μέρη. Το πρώτο μέρος είναι η συγκέντρωση πληροφοριών για το σύστημα στόχο καθώς και η ανίχνευση. Τόσο για τη συγκέντρωση πληροφοριών, όσο και για το στάδιο της ανίχνευσης χρησιμοποιούνται τεχνικές οι οποίες περιγράφονται σε επόμενο κεφάλαιο. Το δεύτερο μέρος της φάσης αυτής, είναι η ανάλυση των ευπαθειών, κατά το οποίο γίνεται η ανάλυση των υπηρεσιών, των εφαρμογών και των λειτουργικών συστημάτων ενάντια σε δημοσιευμένες ευπάθειες καθώς και ευπάθειες γνωστές στον ελεγκτή.

2.3.2.3. Φάση επίθεσης

Η φάση της επίθεσης διαφοροποιεί τις δοκιμές διεισδυτικότητας από την αποτίμηση των ευπαθειών ενός συστήματος, προσφέροντας την απτή επικύρωση των αδυναμιών που ανακαλύπτονται σε ένα σύστημα. Η φάση αυτή αποτελείται από τέσσερα επαναλαμβανόμενα στάδια κατά τα οποία ο ελεγκτής αφού έχει εντοπίσει συγκεκριμένες αδυναμίες κατά τη διάρκεια της φάσης διερεύνησης, αποκτά πρόσβαση στο σύστημα και προσπαθεί να αποκτήσει προνόμια διαχειριστή συστήματος, ώστε στη συνέχεια να εξερευνήσει περεταίρω το σύστημα και να διερευνήσει τα υποσυστήματα του ώστε εν τέλει να εγκαταστήσει επιπλέον εργαλεία τα οποία θα του επιτρέψουν να επαναλάβει τη φάση της επίθεσης.

2.3.2.4. Φάση αναφοράς

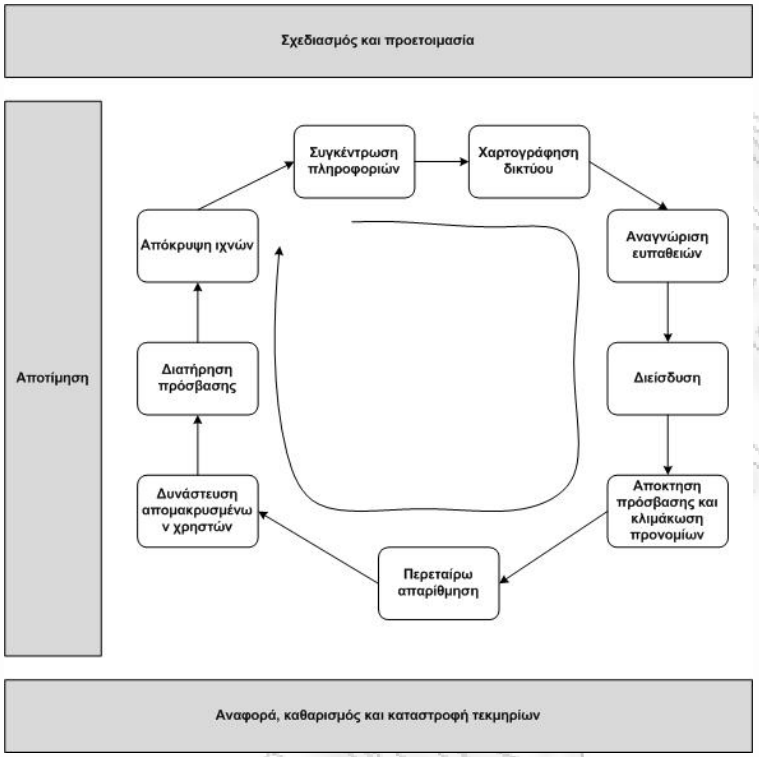
Η φάση της αναφοράς διαρκεί καθόλη τη χρονική διάρκεια διεξαγωγής των ελέγχων. Στη φάση της σχεδίασης καταγράφεται και τεκμηριώνεται το πλάνο της αποτίμησης, στη φάση της διερεύνησης και στη φάση της επίθεσης διατηρούνται τα αρχεία καταγραφής και ανάλογα με τον τύπο του ελέγχου αναφέρονται στους διαχειριστές των συστημάτων. Τέλος, συντάσσεται η τελική αναφορά-παραδοτέο στο οποίο περιγράφονται οι αναγνωρισμένες αδυναμίες και το επίπεδο κινδύνου που αυτές χαρακτηρίζουν καθώς επίσης αναγράφονται και οι συστάσεις των ελεγκτών για τον περιορισμό του κινδύνου που διέπει το σύστημα.

2.3. OISSG–Το Πλαίσιο Αποτίμησης Ασφάλειας Συστημάτων (ISSAF)

Το ISSAF αποτελεί ένα πλαίσιο εργασίας το οποίο έχει ως σκοπό την αποτίμηση της ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού και θεωρείται ως η ναυαρχίδα των πλαισίων εργασίας του Open Information Systems Security Group (OISSG). Το OISSG είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος αποσκοπεί στην ενημέρωση περί της ασφάλειας των πληροφοριακών συστημάτων.

2.4.1 Γενικά

Το ISSAF διαχωρίζει τη μεθοδολογία των ελέγχων διεισδυτικότητας σε τρεις φάσεις εκ των οποίων η κύρια φάση αποτελείται από εννέα διακριτά βήματα. Στην παρακάτω εικόνα απεικονίζονται οι φάσεις και τα βήματα που ακολουθούνται κατά τη διάρκεια των ελέγχων. Οι φάσεις που ακολουθούνται είναι αυτή του σχεδιασμού και της προετοιμασίας, η φάση της αποτίμησης και τέλος η φάση της αναφοράς, του καθαρισμού και της καταστροφής των τεκμηρίων.



Εικόνα 8

2.4.2 Φάση Σχεδιασμού και Προετοιμασίας

Στη φάση αυτή ακολουθούνται τα απαραίτητα βήματα για την ανταλλαγή πληροφοριών μεταξύ ελεγχόμενου και ελεγκτή, το σχεδιασμό και την προετοιμασία των δοκιμών και των ελέγχων διεισδυτικότητας. Πριν τη διεξαγωγή των δοκιμών θεωρείται απαραίτητη η σύναψη και υπογραφή της συμφωνίας διεξαγωγής της αποτίμησης στην οποία παρέχεται το δικαίωμα του ελέγχου (right to audit) καθώς και η αμοιβαία νομική συμφωνία για τη διεξαγωγή των δοκιμών. Επίσης, κατά τη διάρκεια της φάσης αυτής, καθορίζονται τα μέλη του ελεγκτικού κλιμακίου, η διαδικασία κλιμάκωσης της ενημέρωσης.

2.4.3. Φάση της Αποτίμησης.

Η φάση αυτή αποτελεί το κύριο μέρος των ελέγχων. Όπως φαίνεται και στην εικόνα 8, αποτελείται από εννέα διακριτά βήματα τα οποία αποτελούν τη διαδικασία των δοκιμών. Τα βήματα αυτά είναι τα παρακάτω:

2.4.3.1. Συγκέντρωση πληροφοριών

Το βήμα αυτό αποτελεί την αρχή της διεξαγωγής των ελέγχων κατά τη διάρκεια της οποία συλλέγονται πληροφορίες οι οποίες αφορούν το σύστημα στόχο. Για παράδειγμα συλλέγονται πληροφορίες για τον οργανισμό που φιλοξενεί το σύστημα, το προσωπικό αυτού καθώς και πληροφορίες που αφορούν τις τεχνολογικές του υποδομές. Για τη συλλογή των πληροφοριών χρησιμοποιούνται τόσο τεχνικές όσο και μη τεχνικές μέθοδοι οι οποίες βοηθούν τον ελεγκτή να κατανοήσει το περιβάλλον ελέγχου και το σύστημα στόχο.

Στο βήμα αυτό δεν είναι απαραίτητη η άμεση και εμφανής αλληλεπίδραση με το σύστημα, καθώς οι πληροφορίες συλλέγονται από δημόσιες πήγες όπως το διαδίκτυο και υπηρεσίες που διατηρούν πληροφορίες για τον οργανισμό. Σημειώνεται ότι η συγκέντρωση των πληροφοριών δεν απαιτεί μεγάλα χρονικά διαστήματα, χωρίς ωστόσο αυτό να σημαίνει ότι υποβαθμίζεται η σημασία της.

Ο σκοπός της συλλογής πληροφοριών είναι η διερεύνηση κάθε πιθανού σημείου εισόδου στο δίκτυο που φιλοξενεί το σύστημα στόχο. Τα αναμενόμενα αποτελέσματα μετά το πέρας του συγκεκριμένου βήματος είναι τα παρακάτω:

- Πληροφορίες προσωπικού (ονόματα, τηλεφωνικοί αριθμοί, θέσεις ευθύνης κλπ)
- Συνεργάτες τεχνολογίας (π.χ. χρησιμοποιούμενες τεχνολογίες και πλατφόρμες)
- Επιχειρηματικές συνεργασίες (επίπεδο συνεργασίας και εμπιστοσύνης κλπ.)
- Επιχειρηματικά και οικονομικά δεδομένα.
- Παρουσία στο διαδίκτυο (domain names, hosting providers κ.λ.π)
- Φυσική παρουσία (τοποθεσίες εγκαταστάσεων)

Το βήμα της συλλογής πληροφοριών αποτελείται από δυο μέρη. Αυτό της παθητικής συλλογής πληροφοριών και αυτό της ενεργητικής συλλογής πληροφοριών. Κατά τη διάρκεια της παθητικής συλλογής πληροφοριών το σύστημα στόχος δεν αξιοποιείται για την ανεύρεση πολύτιμων πληροφοριών, αλλά οι πληροφορίες προέρχονται από τρίτες με αυτό πήγες όπως για παράδειγμα

είναι οι ιστοσελίδες κοινωνικής δικτύωσης και οι μηχανές αναζήτησης. Κατά τη διάρκεια της ενεργητικής συλλογής πληροφοριών εκτελούνται κατά βάση ερωτήματα στα συστήματα τα οποία έχουν πρόσβαση στο διαδίκτυο και από τα οποία ενδέχεται να προκύψουν πληροφορίες χρήσιμες για την περαιτέρω χαρτογράφηση του δικτύου. Τέτοια συστήματα συνήθως είναι οι διακομιστές αλληλογραφίας (SMTP servers) και οι διακομιστές ονοματοδοσίας (DNS servers).

2.4.3.2. Χαρτογράφηση δικτύου

Αφού έχει προηγηθεί η συλλογή των πληροφοριών στο προηγούμενο βήμα, ακολουθείται μια πιο τεχνική προσέγγιση με σκοπό να αποτυπωθεί η δικτυακή αρχιτεκτονική του συστήματος. Έτσι, χρησιμοποιώντας τις πληροφορίες για τη δικτυακή υποδομή που έχουν συλλεχθεί από το προηγούμενο βήμα, επιχειρείται η εξειδίκευση των πληροφοριών για τη δικτυακή υποδομή με απώτερο σκοπό την αποτύπωση της πλήρους δικτυακής τοπολογίας του οργανισμού και ειδικότερα του συστήματος στόχου. Η εξειδίκευση των πληροφοριών προέρχεται από την αναγνώριση των συστημάτων που βρίσκονται σε λειτουργία καθώς και των χαρακτηριστικών τους όπως είναι το λειτουργικό τους σύστημα, οι υπηρεσίες οι οποίες εκτελούνται σε αυτά, τα συστήματα που τα προστατεύουν (π.χ. firewalls).

Κατά τη διάρκεια του βήματος της χαρτογράφησης, χρησιμοποιούνται τεχνικές με τις οποίες επιτυγχάνεται η σάρωση θυρών, η αναγνώριση των λειτουργικών συστημάτων και η αναγνώριση των παρεχόμενων υπηρεσιών και οι οποίες επεξηγούνται αναλυτικότερα στο Κεφάλαιο 3.

Για την επιτυχή χαρτογράφηση του δικτύου, πρέπει να ακολουθηθεί ένα συγκεκριμένο πλάνο ελέγχων στο οποίο να γίνεται εξειδίκευση των συστημάτων που θα πραγματοποιηθούν οι δοκιμές και η αναγνώριση πιθανών ευπαθών σημείων.

2.4.3.3. Αναγνώριση ευπαθειών

Κατά την αναγνώριση ευπαθειών, ο ελεγκτής πρέπει να έχει ήδη στοχοποιήσει τα πιθανά ευπαθή σημεία του δικτύου από το προηγούμενο βήμα. Η αναγνώριση

των ευπαθειών επιτυγχάνεται κλιμακωτά, αξιοποιώντας παράλληλα τις κατάλληλες τεχνικές και ολοκληρώνεται με την αποτίμηση αυτών και την προετοιμασία για τη φάση της επίθεσης.
Έτσι, ο ελεγκτής πρέπει να προβεί στις παρακάτω ενέργειες ώστε να ολοκληρώσει επιτυχώς την αναγνώριση των ευπαθειών.

- Αναγνώριση ευπαθών υπηρεσιών
- Εκτέλεση αυτοματοποιημένης σάρωσης ευπαθειών αξιοποιώντας βάσεις δεδομένων δημοσιευμένων ευπαθειών.
- Επαλήθευση των αποτελεσμάτων.
- Απαρίθμηση των αναγνωρισμένων ευπαθειών
- Ταξινόμηση των ευπαθειών και υπολογισμός του πιθανού αντίκτυπου στα συστήματα.
- Προσδιορισμός των σεναρίων που θα ακολουθηθούν και προετοιμασία για τη φάση διείσδυσης.

Η ταξινόμηση των ευπαθειών και ο υπολογισμός του πιθανού αντίκτυπου στα συστήματα συνήθως εκτελείται αυτόματα από τα χρησιμοποιούμενα εργαλεία σάρωσης ευπαθειών. Ωστόσο, είναι σημαντικό να υπάρξει ταξινόμηση των ευπαθειών βάσει των επιπτώσεων που ενδεχομένως να έχουν στην επιχειρησιακή λειτουργία του οργανισμού και ειδικότερα του συστήματος στόχου. Για παράδειγμα δύναται να υφίσταται ευπάθεια σε ένα σύστημα, η εκμετάλλευση της οποίας να οδηγεί στη διακοπή λειτουργίας ενός υποσυστήματος. Σε αυτή την περίπτωση η διακοπή της λειτουργίας του υποσυστήματος να είναι ήσσονος σημασίας καθώς αυτό εξυπηρετεί μια μη κρίσιμη για τον οργανισμό λειτουργία. Το εγχειρίδιο λοιπόν καθορίζει τα κριτήρια ταξινόμησης των ευπαθειών βασισμένα τόσο στον επιχειρηματικό όσο και στον τεχνικό κίνδυνο και τα συνοψίζει στον Πίνακα 2. Σημειώνεται ωστόσο ότι, ιδιαίτερα για τον επιχειρηματικό κίνδυνο, οι κίνδυνοι σχετίζονται με την ανάλυση επιχειρηματικών επιπτώσεων (Business Impact Analysis) η οποία γίνεται προσεγγιστικά από την πλευρά των ελεγκτών.

	Χαμηλός επιχειρηματικός κίνδυνος	Μεσαίος επιχειρηματικός κίνδυνος	Υψηλός επιχειρηματικός κίνδυνος
Υψηλός τεχνικός κίνδυνος	ΕΥΠΑΘΕΙΕΣ ΜΕΣΑΙΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ
Μεσαίος τεχνικός κίνδυνος	ΕΥΠΑΘΕΙΕΣ ΧΑΜΗΛΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΜΕΣΑΙΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ
Χαμηλός τεχνικός κίνδυνος	ΕΥΠΑΘΕΙΕΣ ΧΑΜΗΛΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΧΑΜΗΛΟΥ ΚΙΝΔΥΝΟΥ	ΕΥΠΑΘΕΙΕΣ ΜΕΣΑΙΟΥ ΚΙΝΔΥΝΟΥ

Πίνακας 2

2.4.3.4. Διείσδυση

Στο παρόν βήμα γίνεται προσπάθεια απόκτησης μη εξουσιοδοτημένης πρόσβασης στα συστήματα, παρακάμπτοντας τις υφιστάμενες δικλείδες ασφάλειας με σκοπό την διείσδυση στο μεγαλύτερο δυνατό αριθμό συστημάτων. Το βήμα της διείσδυσης περιγράφεται από μία διαδικασία τα βήματα της οποίας είναι τα παρακάτω.

Εύρεση εργαλείου επικύρωσης αδυναμιών

Στο παρόν βήμα αναζητείται το κατάλληλο λογισμικό το οποίο θα χρησιμοποιηθεί ενάντια στον στόχο για την επικύρωση των αδυναμιών αυτού.

Δοκιμή εργαλείου επικύρωσης αδυναμιών

Στο βήμα αυτό δοκιμάζεται η αποτελεσματικότητα των διαθέσιμων εργαλείων ενάντια σε στόχους σε περιβάλλον εργαστηρίου (lab environment)

Ανάπτυξη εργαλείου επικύρωσης αδυναμιών

Στο βήμα αυτό αναπτύσσεται το κατάλληλο λογισμικό επικύρωσης αδυναμιών σε περίπτωση που δεν έχει βρεθεί κάποιο ήδη υπάρχον.

Χρήση εργαλείου επικύρωσης αδυναμιών ενάντια στον στόχο

Στο βήμα αυτό χρησιμοποιείται το κατάλληλο εργαλείο επικύρωσης των αδυναμιών με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης.

2.4.3.5. Απόκτηση Πρόσβασης και Κλιμάκωση Προνομίων

Στο βήμα αυτό, θεωρείται ότι ήδη έχει αποκτηθεί μη εξουσιοδοτημένη πρόσβαση κατά τη διάρκεια του βήματος της διείσδυσης και επιχειρείται η κλιμάκωση των προνομίων σε απόκτηση των μέγιστων προνομίων. Τα επίπεδα απόκτησης πρόσβασης είναι τα ακόλουθα:

Απόκτηση ελαχίστων προνομίων

Στο συγκεκριμένο επίπεδο αντιστοιχούν λογαριασμοί πρόσβασης με περιορισμένα ή ελάχιστα δικαιώματα. Τέτοιοι λογαριασμοί είναι συνήθως οι λογαριασμοί απλών χρηστών. Οι λογαριασμοί αυτοί αποτελούν συνήθως το μέσο για την κλιμάκωση της πρόσβασης με λογαριασμό με αυξημένα δικαιώματα.

Απόκτηση ενδιάμεσων προνομίων

Στο επίπεδο αυτό αντιστοιχούν οι λογαριασμοί με αυξημένα δικαιώματα, όπως είναι οι λογαριασμοί χρηστών αντιγράφων ασφάλειας ή οι λογαριασμοί με τα δικαιώματα των οποίων εκτελούνται ορισμένες υπηρεσίες. Οι λογαριασμοί αυτοί μπορούν να χρησιμοποιηθούν για την απόκτηση πρόσβασης στο σύστημα με πλήρη δικαιώματα και εν τέλει την τελική έκθεση του.

Πλήρης έκθεση

Ένα σύστημα έχει εκτεθεί πλήρως όταν ο ελεγκτής έχει αποκτήσει πλήρη δικαιώματα στους πόρους του συστήματος. Ως εκ τούτου, το σύστημα μπορεί να χρησιμοποιηθεί για την προσέγγιση στο τελικό σύστημα στόχο και να χρησιμοποιηθεί για την επίτευξη επιθέσεων σε αυτό.

Τελική έκθεση του στόχου

Στο επίπεδο αυτό έχει αποκτηθεί μη εξουσιοδοτημένη πρόσβαση στο σύστημα στόχο και πρόσβαση στις πληροφορίες που επιδιώκει να προστατέψει ο οργανισμός με τη διεξαγωγή των ελέγχων διεισδυτικότητας.
Σημειώνεται ότι ανάλογα το επίπεδο προνομίων που έχει αποκτηθεί επαναλαμβάνονται τα προηγούμενα βήματα ελέγχου.

2.4.3.6. Περεταίρω απαρίθμηση και κλιμάκωση προνομίων

Στο βήμα αυτό και καθόσον έχει αποκτηθεί πρόσβαση σε ένα σύστημα επιχειρείται μια σειρά από ενέργειες οι οποίες θα δώσουν τη δυνατότητα στον ελεγκτή να μεταπηδήσει σε άλλα συστήματα ώσπου να καταλήξει στο τελικό-σύστημα στόχο. Οι ενέργειες αυτές είναι οι παρακάτω:
Αποκόμιση των κωδικών σε κρυπτογραφημένη μορφή ώστε να εκτελεστεί η τεχνική του offline cracking και να αποκαλυφθεί ο πραγματικός κωδικός.

- Αποκόμιση κωδικών μέσω τεχνικών sniffing
- Αποκόμιση και ανάλυση του συνόλου των δεδομένων που διακινούνται στο δίκτυο μέσω τεχνικών sniffing.
- Συλλογή cookies και χρήση αυτών ώστε να επιτευκτούν επιθέσεις τύπου session hijacking.
- Αναγνώριση δρομολογίων και δικτύων από και προς το σύστημα στο οποίο έχει επιτευχτεί μη εξουσιοδοτημένη πρόσβαση.
- Χαρτογράφηση των εσωτερικών δικτύων.

- Επανάληψη εκτέλεσης των προηγούμενων βημάτων ελέγχου.

2.4.3.7. Δυνάστευση απομακρυσμένων χρηστών και περιοχών

Στο βήμα αυτό επιχειρείται η δυνάστευση των απομακρυσμένων χρηστών και περιοχών, δηλαδή, επιχειρείται η απόκτηση ελέγχου στους σταθμούς εργασίας χρηστών. Για παράδειγμα, η επικοινωνία των χρηστών ενός οργανισμού με το οργανισμό επιτυγχάνεται με τεχνολογίες όπως αυτή του VPN (Virtual Private Network), ώστε από κάποιον σταθμό εργασίας ο οποίος βρίσκεται σε κάποιο απομακρυσμένο σημείο, κάποιος χρήστης να αποκτήσει εξουσιοδοτημένη πρόσβαση στον οργανισμό. Η επίθεση στον σταθμό εργασίας του χρήστη και η αποκόμιση των διαπιστευτηρίων του αποτελεί σκοπό ώστε να επιτευχτεί μετέπειτα εξουσιοδοτημένη πρόσβαση στον οργανισμό από μη εξουσιοδοτημένο πρόσωπο.

2.4.3.8. Διατήρηση πρόσβασης

Στο βήμα αυτό, ακολουθούνται όλες οι απαραίτητες ενέργειες ώστε ο επιτιθέμενος να διατηρήσει πρόσβαση σε ένα σύστημα το οποίο έχει ήδη καταλάβει. Συγκεκριμένα, γίνεται προσπάθεια ώστε να δημιουργηθούν σημεία πρόσβασης ώστε μέσω της χρήσης συγκεκαλυμμένων καναλιών ο εισβολέας να αποκτά πρόσβαση στο εσωτερικό του συστήματος στόχου κατά βούληση. Τα σημεία πρόσβασης μπορούν να δημιουργηθούν με τη χρήση εξειδικευμένων λογισμικών τα οποία είναι γνωστά και ως rootkits.

2.4.3.9. Απόκρυψη ιχνών

Στο βήμα αυτό, γίνεται προσπάθεια από τον επιτιθέμενο να αποκρύψει τα ηλεκτρονικά ίχνη τα οποία έχουν δημιουργηθεί από την εισβολή του στο σύστημα στόχο. Οι τρόποι με τους όποιους ο επιτιθέμενος μπορεί να αποκρύψει ίχνη είναι η απόκρυψη αρχείων σε ασφαλή σημεία, η διαγραφή των αρχείων καταγραφής, η απενεργοποίηση ή η παραπλάνηση του λογισμικού ασφάλειας που εκτελείται σε διακομιστές και σταθμούς εργασίας.

2.4.4 Φάση αναφορών, καθαρισμού και καταστροφής τεκμηρίων

2.4.4.1. Αναφορά

Κατά τη διάρκεια του βήματος αυτού, απαιτείται η αναφορά των δοκιμών διεισδυτικότητας που εκτελέστηκαν, τα αποτελέσματα των δοκιμών και οι συστάσεις του ελεγκτικού κλιμακίου ώστε να περιοριστεί το επίπεδο κινδύνου που προκαλείται από τις υφιστάμενες ευπάθειες του συστήματος. Η δομή του εγγράφου της αναφοράς πρέπει να είναι σαφής και τα αναγραφόμενα σε αυτό επαρκώς τεκμηριωμένα. Η δομή του εγγράφου συνίσταται να είναι η παρακάτω:

- Διοικητική σύνοψη.
- Εύρος ελέγχου
- Χρησιμοποιούμενα εργαλεία
- Ημερομηνία και ώρα εκτέλεσης της κάθε δοκιμής.
- Τα αποτελέσματα κάθε πραγματοποιημένης δοκιμής
- Λίστα ευπαθειών και συστάσεις για επίλυση.
- Λίστα ενεργειών για τον περιορισμό του κινδύνου.

2.4.4.2. Καθαρισμός και καταστροφή τεκμηρίων

Απαραίτητη είναι η καταστροφή των οποιονδήποτε πληροφοριών δημιουργήθηκαν στα υπό έλεγχο συστήματα. Σε ενδεχόμενη περίπτωση αδυναμίας διαγραφής πληροφοριών πρέπει να τεκμηριωθεί και αναφερθεί στην τεχνική έκθεση του ελέγχου.

ΚΕΦΑΛΑΙΟ 3ο

Τεχνικές Ελέγχων Διείσδυσης Δικτύων

3.1.Συγκέντρωση πληροφοριών

Η συγκέντρωση πληροφοριών αποτελεί την βάση για την ορθή στοχοποίηση ενός συστήματος κατά τη μετέπειτα διαδικασία των δοκιμών διεισδυτικότητας. Οι απαραίτητες πληροφορίες μπορούν να ανακτηθούν μέσα από τεχνικά εργαλεία, από τεχνικές κοινωνικής μηχανικής και τέλος από δημοσιευμένες πληροφορίες στο διαδίκτυο όπως για παράδειγμα μπορεί να είναι η Πολιτική Ασφάλειας Συστημάτων Πληροφορικής ενός οργανισμού ή ακόμα και το οργανόγραμμα του.

3.1.1. Παθητική συγκέντρωση πληροφοριών

Με τον όρο παθητική συγκέντρωση πληροφοριών εννοείται ότι κατά την άντληση δεδομένων δεν επιτυγχάνεται καμία σύνδεση μεταξύ συστήματος ή δικτύου – στόχου και επιτιθέμενου.
Οι πήγες από τις οποίες μπορεί ο επιτιθέμενος να αντλήσει πληροφορίες είναι και οι παρακάτω:

3.1.1.1. Καταχώρηση Υπηρεσιών Διαδικτύου

Ένα πληροφοριακό σύστημα για να αποκτήσει πρόσβαση σε έναν δικτυακό πόρο στο διαδίκτυο πρέπει να έχει αποκτήσει μια IP διεύθυνση η οποία έκτος από μοναδική πρέπει να είναι και δρομολογήσιμη. Για λογούς απλοποίησης της διευθυνσιοδότησης και λογούς μνημόνευσης των πληροφοριακών συστημάτων στο διαδίκτυο, έχουν αναπτυχτεί υπηρεσίες κατά τις οποίες αντιστοιχείται μια IP διεύθυνση με ένα μοναδικό όνομα τομέα (domain name).

Τόσο οι εγγραφές των IP διευθύνσεων όσο και οι εγγραφές των domain names διαχειρίζονται και συντονίζονται σε διεθνές επίπεδο. Για τη διαχείριση των IP διευθύνσεων και των domain names , οι οργανισμοί πρέπει να παρέχουν λεπτομέρειες όπως για παράδειγμα η φυσική διεύθυνση και η τεχνική επαφή η οποία είναι υπεύθυνη για τη διαχείριση του domain name/IP διεύθυνσης. Έτσι, είναι αναγκαίο οι πληροφορίες αυτές να είναι δημόσια διαθέσιμες και αποτελούν τις πρώτες πληροφορίες τις οποίες μπορεί να αντλήσει κάποιος επιτιθέμενος.

Για τη διαχείριση λοιπόν των IP διευθύνσεων και των domain names σε παγκόσμιο επίπεδο υπάρχουν τέσσερεις υπηρεσίες οι οποίες ονομάζονται Regional Internet Registries (RIR) και οι οποίες είναι οι παρακάτω:

- APNIC (Asia-Pacific Network Information Center)
- ARIN (American Registry for Internet Numbers)
- LACNIC (Latin American and Caribbean Internet Addresses Registry)
- RIPE NCC (Réseaux IP Européens Network Coordination Centre)

Οι παραπάνω RIRs είναι υπεύθυνοι για την απόδοση IP διευθύνσεων, για αριθμούς αυτόνομων συστημάτων (Autonomous Systems Number – ASN)και τη διαχείριση του reverse domain name space.

WHOIS

Το whois μπορεί να θεωρηθεί σαν ένα σύστημα ερωταπαντήσεων από το οποίο αντλούνται πληροφορίες σχετικά με τις IP διευθύνσεις και τα domain names ενός οργανισμού. Υπάρχουν δυο διαφορετικοί τύποι whois πόρων. Ο πρώτος βασίζεται στην δικτυακή υποδομή (Network service-based) και ο δεύτερος στην ονοματοδοσίας (Name service-based). Ο πρώτος τύπος επικεντρώνεται στη καταγραφή και τη διαχείριση διακριτών IP διευθύνσεων ή blocks αυτών (net blocks) και ο δεύτερος τύπος επικεντρώνεται στην εγγραφή και διαχείριση των domain names. Όλες οι παραπάνω πληροφορίες καταγράφονται σε βάσεις δεδομένων στις οποίες μπορούν να εκτελέσουν συγκεκριμένα ερωτήματα για την άντληση πληροφοριών από κάποιον επιτιθέμενο.

Οι πληροφορίες που είναι δυνατό να αντλήσει ένας επιτιθέμενος από κάποιον RIR είναι το network space ενός οργανισμού, πληροφορίες για τη δρομολόγηση του δικτύου αυτού στο διαδίκτυο καθώς και πληροφορίες για τους διαχειριστές του δικτύου.

3.1.1.2. Σύστημα DNS

Το συγκεκριμένο σύστημα χρησιμοποιείται ώστε όταν γίνεται αναζήτηση για ένα συγκεκριμένο domain name από ένα σύστημα ή έναν χρήστη, να επιστρέφεται από τους εξυπηρετητές DNS η IP διεύθυνση η οποία αντιστοιχεί στο συγκεκριμένο domain name και κατ' επέκταση στο σύστημα που το χρησιμοποιεί. Κατά καιρούς δημοσιεύονται διάφορα κενά ασφάλειας στα προγράμματα που το αξιοποιούν (bind / MS DNS) αλλά η εκμετάλλευση αυτών δεν αποτελεί παθητική μέθοδο άντλησης πληροφοριών.

Οι ερωτήσεις που μπορούν να εκτελεστούν σε ένα σύστημα DNS προσφέρουν πληθώρα πληροφοριών τις οποίες μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Η άντληση των πληροφοριών μπορεί να γίνει είτε μέσω διαφόρων εφαρμογών ιστού (πχ www.network-tools.com), είτε μέσω διαφόρων εργαλείων όπως είναι το dig και το nslookup.

Από έναν σύστημα DNS μπορούν να αντληθούν πληροφορίες όπως είναι οι διευθύνσεις των διεπαφών του δικτύου προς το internet με σκοπό την εξυπηρέτηση υπηρεσιών ηλεκτρονικού ταχυδρομείου (mail exchangers – MX εγγραφές), πληροφορίες για την ονοματοδοσίας και διευθυνσιοδότηση συστημάτων (A, PTR, CNAME εγγραφές), πληροφορίες για τον αρμόδιο εξυπηρετητή ενός τομέα (authoritative DNS server), πληροφορίες για τον τομέα και πιθανούς υποτομείς (domains, subdomains). Είναι δυνατόν, διαμέσου των ερωτημάτων σε DNS servers και σε συνάρτηση με την ελλιπή παραμετροποίηση των διακομιστώ αυτών να ληφθούν κρίσιμες πληροφορίες όπως είναι η διευθυνσιοδότηση του εσωτερικού δικτύου ενός οργανισμού.

3.1.1.3. Μηχανές Αναζήτησης

Η χρήση μηχανών αναζήτησης μπορεί να προσφέρει στον επιτιθέμενο αρκετές πληροφορίες ακόμα και διαβαθμισμένων πληροφοριών. Η χρήση μηχανών αναζήτησης όπως είναι το Google για παράδειγμα μπορεί να συνεισφέρει στην ανάλυση αποθηκευμένων ιστοσελίδων (cached web pages), στην άντληση πληροφοριών όπως εγχειρίδια τεχνοδιαμορφωσεων (configuration manuals),

εγχειρίδια εσωτερικού ελέγχου, αναφορές ασφάλειας κλπ. Πολλές φορές αναζήτηση για configuration files συστημάτων μπορεί να αποκαλύψει τεχνικές λεπτομέρειες για την παραμετροποίηση ενός πληροφοριακού συστήματος και να αποτελέσει κρίσιμη πληροφορία στα χεριά ενός επιτιθέμενου.

Παράλληλα με τα παραπάνω, αναζήτηση για πληροφορίες σε χώρους δημοσίων συζητήσεων (fora, newsgroups, mailing lists κλπ) μπορεί να αποκαλύψει χρήσιμες πληροφορίες για τη δομή πληροφοριακών συστημάτων και δικτυακών υποδομών. Για παράδειγμα, ο διαχειριστής συστημάτων Linux ενός οργανισμού μπορεί να έχει δημοσιεύσει σε κάποιο forum, τη λύση στο πρόβλημα εγκατάστασης ενός λογισμικού και να προτείνει την αφαίρεση από το σύστημα ενός security patch, ώστε να λειτουργήσει το αναφερόμενο λογισμικό. Ο αναγνώστης της δημοσίευσης αυτής αμέσως αντιλαμβάνεται ότι κάποιο σύστημα που διαχειρίζεται ο εν λόγω διαχειριστής είναι ευάλωτο λόγω ευπαθειών που καλύπτει το συγκεκριμένο security patch.

Τέλος, μπορούν να αποκαλυφθούν πληροφορίες οι οποίες δεν είναι χρήσιμες από τεχνικής άποψης, ωστόσο είναι πολύτιμες σε περιπτώσεις που επιτιθέμενος είναι διατεθειμένος να χρησιμοποιήσει τεχνικές κοινωνικής μηχανικής (social engineering) με σκοπό την εκμαίευση πληροφοριών. Έτσι, διαμέσου των μηχανών αναζήτησης μπορούν να αποκαλυφθούν πληροφορίες όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, τηλεφωνικοί αριθμοί, διευθύνσεις καθώς και θέσεις ευθύνης του προσωπικού ενός οργανισμού.

Εξειδικευμένες μηχανές αναζήτησης

Στο διαδίκτυο υπάρχουν μηχανές αναζήτησης οι οποίες διερευνούν συγκεκριμένα μόνο στοιχεία. Τέτοιες μηχανές αναζήτησης είναι το www.netcraft.com και το www.alexa.com.

Από τις παραπάνω μηχανές αναζήτησης μπορούν να ανεβρεθούν πολύτιμα στοιχεία για τη δικτυακή κίνηση ενός ιστότοπου, το λειτουργικό σύστημα του διακομιστή που το υποστηρίζει, το λογισμικό του διακομιστή, την τελευταία ημερομηνία που έγινε αλλαγή πάνω στον ιστότοπο καθώς επίσης και το χρονικό

διάστημα για το οποίο παραμένει χωρίς επανεκκίνηση. Χαρακτηριστικές πληροφορίες από τους δυο παραπάνω ιστότοπους παρουσιάζονται στις εικόνες που ακολουθούν.

3.1.1.4. Συστήματα ηλεκτρονικού ταχυδρομείου

Τα συστήματα τα οποία υποστηρίζουν υπηρεσίες ανταλλαγής ηλεκτρονικών μηνυμάτων (email systems) μπορούν να χαρακτηριστούν από τα ποιο κρίσιμα συστήματα για την επικοινωνία ενός οργανισμού. Πολλές φορές τα συστήματα που υποστηρίζουν την ανταλλαγή των emails είναι ελλιπώς παραμετροποιημένα με αποτέλεσμα να έχουν κρίσιμα κενά ασφάλειας.

Πολλές χρήσιμες πληροφορίες μπορεί να συγκεντρώσει ένας επιτιθέμενος από ένα μη ασφαλές σύστημα ηλεκτρονικής αλληλογραφίας. Τέτοιες πληροφορίες μπορεί να είναι η δικτυακή διασύνδεση μεταξύ συστημάτων πληροφορικής ή ακόμα και email διευθύνσεις μελών του οργανισμού, εσωτερικές IP διευθύνσεις, ονοματοδοσίας συστημάτων, η έκδοση του προγράμματος πελάτη που χρησιμοποιήθηκε κλπ.

Επικεφαλίδες SMTP

Κατά τη διαδικασία παθητικής άντλησης πληροφοριών, πολλές πληροφορίες μπορούν να αποκαλυφθούν στον επιτιθέμενο μέσα από το περιεχόμενο των επικεφαλίδων του SMTP πρωτοκόλλου που περιέχονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Εντός ενός οργανισμού μπορούν να χρησιμοποιούνται παραπάνω του ενός συστήματα πληροφορικής τα οποία υποστηρίζουν την ανταλλαγή emails. Το πρωτόκολλο SMTP χρησιμοποιεί επικεφαλίδες σε κάθε email με σκοπό την δρομολόγηση, την ασφαλή παράδοση και περιστασιακά την ασφαλή απάντηση στο ηλεκτρονικό μήνυμα.

Ετικέτες διακομιστών SMTP

Πολλά από τα λογισμικά τα οποία υποστηρίζουν την ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου κατά τη σύνδεση τους στην πόρτα 25 (SMTP Port) αποστέλλουν ένα μήνυμα το οποίο ενημερώνει τον συνδεόμενο σχετικά με την έκδοση του προγράμματος το οποίο εξυπηρετεί τη μεταφορά emails.

Έτσι, ο επιτιθέμενος γνωρίζει πλέον και το λογισμικό το οποίο εξυπηρετεί την υπηρεσία SMTP. Μέσω της σχετικής αναζήτησης μπορεί να αποκαλύψει τα διαφορά κενά ασφάλειας που αυτή έχει και να τα χρησιμοποιήσει σε ανάλογες επιθέσεις.

3.1.1.5. Ονοματολογία

Η ονοματολογία η οποία ακολουθείται στα συστήματα πληροφορικής πολλές φορές αποκαλύπτει σημαντικά στοιχεία για την τοποθεσία στην οποία βρίσκεται το υπολογιστικό σύστημα, όπως επίσης και ποιες υπηρεσίες εξυπηρετεί. Τα πλέον συνηθισμένα λάθη στην ονοματολογία των συστημάτων είναι τα παρακάτω:

- Η αναφορά φυσικής τοποθεσίας (πχ London.example.com)
- Η χρήση πληροφοριών των λειτουργικών συστημάτων (πχ win2k3.example.com)
- Η λειτουργική χρήση του συστήματος (πχ firewall.example.com)
- Η χρήση πληροφοριών του υλικού (πχ checkpoint-ng.example.com)
- Η αναφορά στη δικτυακή τοπολογία (πχ fwDMZ1.example.com)

Στην περίπτωση μικρών εταιρικών δικτύων συχνά συναντάται το σύστημα να έχει λάβει όνομα ανάλογα με τον κάτοχο του (john-pc.example.com). Το γεγονός αυτό αφενός διευκολύνει τη διαχείριση των συστημάτων, αφετέρου εγείρει την περιέργεια των χρηστών για αναζήτηση δεδομένων μέσω των πόρων του δικτύου.

3.1.2. Χαρτογράφηση Δικτύου

Οι τεχνικές οι οποίες χρησιμοποιούνται κατά τη διάρκεια της χαρτογράφησης του δικτύου, αποσκοπούν στον εντοπισμό μηχανημάτων, την ανίχνευση των ανοικτών θυρών ενός υπολογιστικού συστήματος στην ταυτοποίηση των λειτουργικών συστημάτων και των υπηρεσιών που εκτελούνται σε αυτά. Τα αποτελέσματα από τη χαρτογράφηση του δικτύου αξιοποιούνται στο επόμενο βήμα ενός ελέγχου διείσδυσης που είναι η ανάλυση και αποτίμηση των ευπαθειών των συστημάτων που έχουν χαρτογραφηθεί.

3.1.2.1. Ανίχνευση συστημάτων

Το πρώτο βήμα είναι η ανίχνευση των IP διευθύνσεων στις οποίες ανταποκρίνονται εν λειτουργία υπολογιστικά συστήματα. Στην προκειμένη περίπτωση υπάρχουν διαφορετικές τεχνικές οι οποίες μπορούν να αποδώσουν διαφορετικά αποτελέσματα αναλόγως τη παραμετροποίηση των δρομολογητών και των firewalls του δικτύου-θύματος. Ορισμένες από τις τεχνικές που μπορούν να λάβουν χώρα είναι οι παρακάτω:

ICMP ping

Χρησιμοποιώντας την τεχνική αυτή αποστέλλεται στους hosts του δικτύου ένα πακέτο ICMP echo request πακέτο. Κάθε host ο οποίος βρίσκεται σε λειτουργία θα απαντήσει στον αποστολέα με ένα ICMP echo reply πακέτο. Σημειώνεται ότι η τεχνική αυτή δεν αποφέρει τα αναμενόμενα αποτελέσματα σε περιπτώσεις όπου οι δρομολογητές και τα firewalls του δικτύου έχουν παραμετροποιηθεί έτσι ώστε να αποκόπτουν τα πακέτα του πρωτοκόλλου ICMP.

TCP SYN ping

Η τεχνική αυτή κάνει χρήση του πρωτοκόλλου TCP αντί του ICMP. Συγκεκριμένα, αποστέλλεται από τον επιτιθέμενο σε κάθε IP διεύθυνση του δικτύου ένα κενό πακέτο TCP με το SYN flag του πακέτου ίσο με 1 και TCP θύρα 80, ζητώντας να αρχικοποιήσει μια νέα σύνδεση. Εάν στην IP διεύθυνση που εστάλει το πακέτο υπάρχει κάποιος host, τότε αυτός θα απαντήσει με ένα

TCP SYN/ACK εάν η πόρτα 80 είναι ανοιχτή ή με ένα RST εάν δεν είναι. Και στις δύο περιπτώσεις ο host έχει αποστείλει απάντηση, οπότε έμμεσα έχει διαπιστωθεί η λειτουργία του. Ωστόσο, η τεχνική αυτή δεν λειτουργεί σε περιπτώσεις όπου ο host είναι κάποιο firewall ή δρομολογητής ο οποίος δεν αρχικοποιεί καμία σύνδεση στις εξωτερικές του διεπαφές παρά μόνο εάν πρόκειται για συνδέσεις προς διακομιστές που εξυπηρετούν δημοσίως διαθέσιμες υπηρεσίες (πχ web server, mail servers, ftp servers)

TCP ACK ping

Όπως αναφέρθηκε παραπάνω, υπάρχει η πιθανότητα τα τείχη ασφάλειας και οι δρομολογητές να έχουν παραμετροποιηθεί με τέτοιο τρόπο ώστε να αποκόπτουν προσπάθειες σύνδεσης σε IP διευθύνσεις ή να αγνοούν ICMP μηνύματα. Ένας τρόπος να ξεπεραστούν τέτοιου είδους εμπόδια είναι η αποστολή TCP ACK μηνυμάτων σε κάθε IP του δικτύου. Τα ACK μηνύματα αποστέλλονται για τη βεβαίωση λήψης δεδομένων σε μία σύνδεση. Όταν ένα σύστημα λάβει ένα τέτοιο μήνυμα δίχως να υπάρχει κάποια σύνδεση τότε αποστέλλει ένα μήνυμα RST στον αποστολέα του ACK πακέτου, οπότε έμμεσα αναγνωρίζεται σε λειτουργία.

UDP ping

Τα σύγχρονα firewalls έχουν τη δυνατότητα να αγνοούν κάθε μήνυμα το οποίο αναφέρεται σε TCP συνδέσεις τις οποίες δε γνωρίζουν. Έτσι μια ακόμη τεχνική η οποία ξεπερνά την παρακολούθηση των TCP συνδέσεων από τα firewalls είναι το UDP ping. Με παρόμοιο τρόπο όπως και οι υπόλοιπες τεχνικές, αποστέλλει μηνύματα στις IP διευθύνσεις ενός δικτύου, με τη διαφορά ότι αποστέλλει ένα κενό μήνυμα σε κάποια ασυνήθιστη θύρα του δικτύου η οποία κατά πάσα πιθανότητα είναι κλειστή (εάν η πόρτα είναι ανοιχτή δεν θα υπάρξει απάντηση από τον host). Σε αυτή την περίπτωση οι hosts οι οποίοι βρίσκονται σε λειτουργία απαντούν με ένα ICMP port unreachable μήνυμα.

IP ping

Στις περιπτώσεις όπου γίνεται TCP/UDP screening στα firewalls ενός δικτύου, μία λύση είναι το IP ping. Στην τεχνική αυτή, αποστέλλεται ένα κενό IP πακέτο το οποίο με παρόμοιο τρόπο με τις προηγούμενες τεχνικές έχει αποσταλεί με ένα συγκεκριμένο πεδίο σε κάποια τιμή. Το πεδίο αυτό είναι το protocol στο οποίο καθορίζεται ο τύπος των δεδομένων που θα ενθυλακώσει το IP πακέτο. Έτσι εάν ληφθεί απαντήσει από κάποιο host σχετικά με το αναφερόμενο πρωτόκολλο τότε απευθείας αναγνωρίζεται ο host σε λειτουργία.

3.1.2.2. Ανίχνευση θυρών

Το επόμενο βήμα για τη χαρτογράφηση του δικτύου είναι η αναγνώριση θυρών TCP και UDP σε κάθε διαθέσιμο υπολογιστικό σύστημα του δικτύου. Η διερεύνηση για ανοιχτές θύρες σε ένα σύστημα οδηγεί στην αναγνώριση των λογισμικών που προσφέρουν συγκεκριμένες υπηρεσίες και κατ'επέκταση οδηγούν στην αναγνώριση των ευπαθειών του συστήματος. Οι τεχνικές αυτές μπορούν να διαχωριστούν σε τέσσερις διαφορετικές κατηγορίες και οι οποίες είναι Open, Half-Open, Stealth και 3^{ου} μέρους.

TCP connect

Οι τεχνικές open scanning είναι τεχνικές οι οποίες χρησιμοποιούν ολοκληρωμένες συνδέσεις μεταξύ των hosts (επιτιθέμενου-θύματος). Χρησιμοποιούν το λεγόμενο "three-way handshaking" το οποίο λαμβάνει χώρα κατά τη διάρκεια εγκαθίδρυσης μιας TCP σύνδεσης. Το three-way handshaking καθορίζει την αποστολή ενός TCP SYN πακέτου από τον server στον client χρησιμοποιώντας την συστημική εντολή connect(). Εάν η αντίστοιχη θύρα του server είναι ανοιχτή (socket σε listening mode) τότε ο server θα απαντήσει με ένα SYN/ACK πακέτο στον client. Στη συνέχεια ο client θα απαντήσει με ένα πακέτο ACK και θα ξεκινήσει να αποστέλλει τα δεδομένα του. Εάν η θύρα του server είναι κλειστή τότε θα απαντήσει με ένα RST/ACK μήνυμα και ο client θα του απαντήσει με ένα RST μήνυμα. Η συγκεκριμένη τεχνική ονομάζεται και vanilla

scan και έχει ως πλεονέκτημα την ακρίβεια των αποτελεσμάτων της, ωστόσο είναι εύκολα ανιχνεύσιμη από firewalls και IDS.

Reverse ident

Η συγκεκριμένη τεχνική δίνει τη δυνατότητα να αξιοποιηθεί το ident service το οποίο τρέχει σε ορισμένα μηχανήματα και ακούει στην θύρα 113. Μέσω του ident ο επιτιθέμενος μπορεί να ανακαλύψει το όνομα χρήστη με δικαιώματα του οποίου έχουν αρχικοποιηθεί οι TCP συνδέσεις. Έτσι για παράδειγμα μπορεί να ανακαλύψει services τα οποία εκτελούνται με δικαιώματα root σε μηχανήματα με UNIX λειτουργικό σύστημα και να εκτελέσει επιθέσεις σε αυτά.

SYN scan

Η συγκεκριμένη τεχνική είναι γνωστή και ως half-open scan λόγω της ιδιότητας της να ξεκινά την εγκαθίδρυση σύνδεσης με το σύστημα-στόχο χωρίς ωστόσο να την ολοκληρώνει. Συγκεκριμένα, ο επιτιθέμενος αποστέλλει ένα TCP SYN πακέτο σε μια συγκεκριμένη θύρα του στόχου και αναμένει ένα πακέτο SYN/ACK εάν η συγκεκριμένη θύρα είναι ανοιχτή. Τότε ο επιτιθέμενος διακόπτει την αίτηση σύνδεσης αποστέλλοντας πίσω ένα πακέτο RST. Εάν η θύρα είναι κλειστή ο στόχος αποστέλλει ένα μήνυμα RST/ACK υποδηλώνοντας την κατάσταση της θύρας. Η συγκεκριμένη τεχνική είναι αρκετά γρήγορη και πολλές φορές παραμένει μη αντιληπτή λόγω της μη ολοκλήρωσης της σύνδεσης. Τα σύγχρονα firewalls και IDS ωστόσο αντιλαμβάνονται της προσπάθειες για half-open συνδέσεις και τις καταγράφουν.

Dump scan

Η συγκεκριμένη τεχνική αξιοποιεί το half open scan και το IP ID πεδίο του IP πακέτου (fragmentation identification number) και μπορεί να αποτελέσει και stealth scan για τον επιτιθέμενο. Στη συγκεκριμένη τεχνική παίρνουν μέρος δυο hosts ενάντια στο σύστημα στόχο. Ο ένας host είναι ο πραγματικά επιτιθέμενος και άλλος είναι ο dumb ή zombie επιτιθέμενος. Τα βήματα που την αποτελούν είναι τρία. Στο πρώτο βήμα γίνεται η ανάλυση και καταγραφή του IP ID του

dumb host με την αποστολή συνήθως ενός ICMP echo request πακέτου. Στο δεύτερο βήμα αποστέλλεται ένα παραποιημένο TCP SYN πακέτο σε μία υπό έλεγχο θύρα του συστήματος στόχου. Το πακέτο αυτό περιέχει στο source IP address πεδίο την IP διεύθυνση του dumb host. Στη συνέχεια το σύστημα στόχος αποστέλλει στο dump host είτε ένα πακέτο SYN/ACK εάν η θύρα είναι ανοιχτή ή ένα RST/ACK εάν η θύρα είναι κλειστή. Το τρίτο βήμα περιλαμβάνει τον επανέλεγχο του IP ID του dumb host από τον επιτιθέμενο. Εάν το IP ID έχει αυξηθεί το λιγότερο κατά 1 τότε η υπό έλεγχο θύρα ήταν ανοιχτή ειδάλλως η θύρα ήταν κλειστή.

Σημειώνεται ότι η συγκεκριμένη τεχνική χρησιμοποιείται για τη διερεύνηση των σχέσεων εμπιστοσύνης μεταξύ δυο hosts. Έτσι η χρήση της τεχνικής με dumb host κάποιο έμπιστο μηχάνημα (πχ router, webserver κλπ) μπορεί να αποκαλύψει τις ανοιχτές θύρες που βλέπει ο dump host και να χαρτογραφηθεί έτσι το δίκτυο με μεγαλύτερη ακρίβεια.

NULL/FIN/XMAS scans

Οι συγκεκριμένες τεχνικές βασίζονται στα flags FIN / PSH / URG οι τιμές των οποίων διαχωρίζουν και τον τύπο της σάρωσης. Εξαιρείται η περίπτωση του NULL scan κατά την οποία τα flags των TCP πακέτων δεν έχουν καμία τιμή. Το αποτέλεσμα των σαρώσεων αυτών βασίζεται στο γεγονός ότι την λήψη ενός τέτοιου πακέτου από το σύστημα-στόχο ακολουθεί η αποστολή ενός RST πακέτου στον επιτιθέμενο ώστε η θύρα του συστήματος-στόχου να θεωρηθεί ως κλειστή, ειδάλλως να θεωρηθεί κλειστή. Αξίζει να σημειωθεί ότι η συμπεριφορά ύστερα από λήψη τέτοιων πακέτων βασίζεται αποκλειστικά στην υλοποίηση του TCP stack από τον κατασκευαστή, οπότε και κάθε σύστημα αντιδρά διαφορετικά. Οι συγκεκριμένες τεχνικές αποδίδουν μόνο ενάντια σε Unix μηχανήματα και εμφανίζουν αρκετά false positives. Ωστόσο παίρνουν απαρατήρητες από αρκετά συστήματα firewall και IDS.

ACK scan

Η συγκεκριμένη τεχνική χρησιμοποιείται για την διαπίστωση εάν οι θύρες ενός συστήματος προστατεύονται από firewall ή όχι. Η τεχνική αυτή υλοποιείται με την αποστολή ενός TCP πακέτου με ορισμένο μόνο το ACK flag. Η συμπεριφορά του συστήματος στόχου είναι πάντοτε η ίδια ανεξάρτητα εάν η θύρα είναι ανοιχτή ή κλειστή. Ωστόσο εάν δεν ληφθεί από τον επιτιθέμενο κάποιο πακέτο τότε η θύρα θεωρείται ότι προστατεύεται από firewall.

3.1.2.3. Ταυτοποίηση Υπηρεσιών

Έχοντας ως στόχο την αναγνώριση των ευπαθειών ενός συστήματος, το επόμενο βήμα που ακολουθείται είναι η αναγνώριση των υπηρεσιών που προσφέρονται από ένα σύστημα. Στα προηγούμενα βήματα έγινε η αναγνώριση των συστημάτων και στη συνέχεια η αναγνώριση των θυρών των συστημάτων. Έτσι, γνωρίζοντας πλέον τα διαθέσιμα συστήματα ενός δικτύου και τις θύρες που έχουν ανοιχτές, γίνεται η προσπάθεια αναγνώρισης των υπηρεσιών που αξιοποιούν τις παραπάνω θύρες.

Banner grabbing

Η τεχνική banner grabbing βασίζεται στη συμπεριφορά πολλών υπηρεσιών ύστερα από σύνδεση στη θύρα που αξιοποιούν να αποστέλλουν ένα μήνυμα ταυτοποίησης (banner) το οποίο περιλαμβάνει συνήθως το όνομα της υπηρεσίας και την έκδοση αυτής. Υπάρχουν εργαλεία τα οποία αυτοματοποιημένα εκτελούν τη συγκεκριμένη εργασία βασισμένα σε βάσεις δεδομένων που περιέχουν signatures από banners υπηρεσιών. Έτσι, λαμβάνοντας ένα service banner από μια υπηρεσία, υπολογίζουν το signature του banner και το συγκρίνουν με τα αποθηκευμένα signatures που διατηρούν, ταυτοποιώντας με αυτόν τον τρόπο την υπηρεσία.

Service probing

Η συγκεκριμένη τεχνική μπορεί να θεωρηθεί ως λογικό επακόλουθο της banner grabbing, λόγω του ενδεχόμενου το service banner να μην περιέχει επαρκείς

πληροφορίες για την ταυτοποίηση της έκδοσης της υπηρεσίας. Έτσι με αυτόν τον τρόπο και αφού έχει ταυτοποιηθεί η υπηρεσία, αποστέλλονται σε αυτήν μηνύματα βασισμένα στο πρωτόκολλο που χρησιμοποιεί ώστε να ανταποκριθεί με μηνύματα τα οποία ενδεχομένως περιέχουν την έκδοση του λογισμικού που χρησιμοποιείται.

3.1.2.4. Ταυτοποίηση Λειτουργικών Συστημάτων

Γνωρίζοντας πλέον τις υπηρεσίες που εκτελούνται σε ένα σύστημα καθώς και τα λογισμικά που τις προσφέρουν, το επόμενο βήμα προς την αναγνώριση των ευπαθειών είναι το Operating System fingerprinting. Ως OS fingerprinting θεωρείται η διαδικασία ταυτοποίησης του λειτουργικού συστήματος το οποίο εκτελείται στο σύστημα στόχο. Για την ταυτοποίηση του λειτουργικού συστήματος υπάρχουν δυο κατηγορίες τεχνικών οι οποίες την επιτυγχάνουν και περιγράφονται παρακάτω.

Ενεργή ταυτοποίηση λειτουργικών συστημάτων

Ως ενεργή ταυτοποίηση λειτουργικών συστημάτων θεωρείται η διαδικασία κατά την οποία αποστέλλονται μηνύματα στο υπό διερεύνηση υπολογιστικό σύστημα και στη συνέχεια αναλύεται η συμπεριφορά του συστήματος καθώς και οι παράμετροι των μηνυμάτων που εστάλησαν ως απάντηση, με αποτέλεσμα βάσει της συμπεριφοράς αυτής να ταυτοποιείται το λειτουργικό σύστημα το οποίο χρησιμοποιεί.

Παθητική ταυτοποίηση λειτουργικών συστημάτων

Σε αντίθεση με την ενεργή ταυτοποίηση λειτουργικών συστημάτων, όπου απαιτείται η αποστολή δεδομένων στον στόχο ώστε να αναλυθεί η απόκριση του, στην παθητική ταυτοποίηση λειτουργικών συστημάτων γίνεται ανάλυση των πακέτων που ένα επιτιθέμενο σύστημα “ακούει”.

Τα εργαλεία τα οποία χρησιμοποιούνται για την παθητική ταυτοποίηση των λειτουργικών συστημάτων εξετάζουν τις παραμέτρους των TCP μηνυμάτων και

βασισμένα σε προδιαγεγραμμένα πρότυπα παραμέτρων (patterns) συμπεραίνουν την έκδοση του λειτουργικού συστήματος του στόχου.

3.2. Αποτίμηση ευπαθειών και Διείσδυση

Κατά τη διάρκεια της αποτίμησης των ευπαθειών με τελικό σκοπό τη διείσδυση σε κάποιο υπολογιστικό σύστημα, χρησιμοποιούνται όλες οι πληροφορίες και τα αποτελέσματα τα οποία είναι απόρροια των παραπάνω τεχνικών. Στη φάση αυτή ο ελεγκτής που διενεργεί τις δοκιμές διείσδυσης στα συστήματα αξιοποιεί τις πληροφορίες αυτές και εκτελεί παράλληλα αυτοματοποιημένη ανίχνευση ευπαθειών στα χαρτογραφημένα συστήματα.

Τα εργαλεία που χρησιμοποιούν την αυτοματοποιημένη ανίχνευση ευπαθειών δέχονται ως δεδομένα εισόδου τα αποτελέσματα των προηγούμενων βημάτων και διαπιστώνουν εάν πληρούν τις συνθήκες που χαρακτηρίζουν μια αδυναμία (π.χ. εκδόσεις των υπηρεσιών). Οι αδυναμίες συνήθως είναι δημοσιευμένες στις ιστοσελίδες των κατασκευαστών ή σε ιστοσελίδες οι οποίες επικεντρώνονται στην καταγραφή αδυναμιών συστημάτων (π.χ. www.cvedetails.com). Ωστόσο, είναι δυνατή η παραγωγή λανθασμένων αποτελεσμάτων από τα εργαλεία ανίχνευσης αδυναμιών (false positives), οπότε και απαιτείται η χειροκίνητη επαλήθευση των αποτελεσμάτων.

Έτσι, κατά τη διάρκεια τα φάσης διείσδυσης δοκιμάζονται από τον ελεγκτή προγράμματα λογισμικού που αξιοποιούν τις αδυναμίες που έχουν εντοπιστεί κατά τη διάρκεια της αποτίμησης των ευπαθειών. Τα προγράμματα αυτά συνήθως δημοσιεύονται σε παράνομους ιστοχώρους και συνήθως παρέχουν πρόσβαση με την χρήση κονσόλας στα ευάλωτα υπολογιστικά συστήματα.

Η επαρκής ενημέρωση των συστημάτων, η ύπαρξη αντιικών καθώς και η εξέλιξη των τειχών προστασίας αποτελεί συνήθως παράγοντα ο οποίος δυσχεραίνει την κατά μέτωπο επίθεση σε κάποιο υπολογιστικό σύστημα διαμέσω του διαδικτύου.

Έτσι, μια τεχνική για να προσπελαστούν τα τείχη ασφάλειας και η αδυναμία εντοπισμού σε συστήματα διακομιστώ, είναι η χρήση εξελιγμένων Trojans τα οποία όμως δεν αρχικοποιούν αυτά τις συνδέσεις προς το διαδίκτυο, αλλά χρησιμοποιούν χαρακτηριστικά και ευπάθειες κοινών εφαρμογών για να αποκτήσουν πρόσβαση στο διαδίκτυο. Με τον τρόπο αυτό, ο επιτιθέμενος στοχεύει στον αδύναμο κρίκο του δικτύου, που είναι ο κοινός χρήστης. Η διασπορά των Trojans αυτών συνήθως γίνεται είτε με την μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου στους χρήστες, είτε με την ταχυδρομική αποστολή μέσων αποθήκευσης (π.χ. CDROM) τα οποία περιέχουν το Trojan, τεχνικές οι οποίες από τη χρήση της κοινωνικής μηχανικής. Οπότε ακολουθώντας την τεχνική αυτή, ο επιτιθέμενος αποκτά πρόσβαση από απόσταση στο δίκτυο στόχο, έχοντας παρακάμψει τυχόν συστήματα ασφαλείας και έχοντας αξιοποιήσει αδυναμίες οι οποίες δε σχετίζονται άμεσα με το τελικό σύστημα στόχο.

3.3. Κλιμάκωση Προνομίων

Η κλιμάκωση προνομίων επιτυγχάνεται διαμέσω της περαιτέρω χαρτογράφησης του δικτύου, ακολουθώντας τις τεχνικές που αναφέρθηκαν παραπάνω, ώστε να επιτευχτεί διείσδυση σε μεγαλύτερο αριθμό συστημάτων. Παράλληλα, τα προνόμια που έχει αποκτήσει ήδη ένας χρήστης σε κάποιο υπολογιστικό σύστημα μπορούν να κλιμακωθούν εκτελώντας τις παρακάτω τεχνικές.

3.3.1. Καταγραφή δικτυακής κίνησης

Η τεχνική αυτή αξιοποιεί πόρους του συστήματος, με σκοπό την καταγραφή της δικτυακής κίνησης από και προς το εκτεθειμένο στον επιτιθέμενο σύστημα στόχο. Κατά τη διάρκεια της καταγραφής, συλλέγονται πληροφορίες όπως οι IP διευθύνσεις των συστημάτων με τα οποία επικοινωνεί το σύστημα στόχος, τα πρωτόκολλα επικοινωνίας τα οποία χρησιμοποιούνται, καθώς επίσης και διαπιστευτήρια εξουσιοδότησης (π.χ. ονόματα χρήστη, κωδικοί πρόσβασης) προς και από εφαρμογές που χρησιμοποιούνται στο δίκτυο.

3.3.2. Αποκάλυψη κωδικού έκτος σύνδεσης

Η τεχνική αυτή προσβλέπει στην αποκάλυψη ενός κωδικού πρόσβασης που έχει κατακερματιστεί εκτελώντας επιθέσεις κρυπτανάλυσης στο κρυπτοκείμενο (cipher text) όπως είναι αυτές με τη χρήση rainbow tables, με την χρήση λεξικών (dictionary attacks) και με τη χρήση του αλγορίθμου brute force.

Σημειώνεται ότι η πλέον αποδοτική τεχνική είναι αυτή με τη χρήση rainbow tables καθώς από τη στιγμή που είναι γνωστός ο αλγόριθμος κατακερματισμού (π.χ. MD5) οι κωδικοί πρόσβασης είναι δυνατό να αποκαλυφτούν σε μικρό χρονικό διάστημα. Ωστόσο, υφίστανται συστήματα, όπως για παράδειγμα Cisco συσκευές οι οποίες κατακερματίζουν τον κωδικό πρόσβασης εισάγοντας στον αλγόριθμο κατακερματισμού επιπλέον κείμενο παράλληλα με τον κωδικό πρόσβασης, οπότε και η εντροπία του κρυπτοκειμένου αυξάνει και καθιστά πρακτικά αδύνατη την αποκάλυψη του κωδικού πρόσβασης.

3.3.3. Αποκάλυψη κωδικού εντός σύνδεσης

Η τεχνική αυτή αποσκοπεί στην αποκάλυψη του κωδικού πρόσβασης σε κάποιο υπολογιστικό σύστημα, υποβάλλοντας στο σύστημα στόχο σε πραγματικό χρόνο συνδυασμούς διαπιστευτηρίων οι οποίοι προέρχονται από αυτοματοποιημένα εργαλεία που χρησιμοποιούν είτε λεξικά είτε τον αλγόριθμο brute force.

3.3.4. Χρήση κουπονιών εξουσιοδότησης.

Υφίστανται συστήματα τα οποία ύστερα από την επιτυχή αυθεντικοποίηση ενός χρήστη σε αυτά, προμηθεύουν το σύστημα του χρήστη με κουπόνια (π.χ. Kerberos tokens) τα οποία χρησιμοποιούνται για την μετέπειτα εξουσιοδότηση του χρήστη. Έτσι, σε ένα σύστημα το οποίο βρίσκεται υπό τον έλεγχο του επιτιθέμενου, είναι δυνατό ο επιτιθέμενος να χρησιμοποιήσει τα κουπόνια αυτά, ώστε να εκτελέσει επιθέσεις τύπου session hijacking και να αποκτήσει πρόσβαση με ανώτερα δικαιώματα σε κάποιο σύστημα.

ΚΕΦΑΛΑΙΟ 4ο

Μεθοδολογίες και Τεχνικές Ελέγχων Διείσδυσης Εφαρμογών

4.1. Γενικά

Τα τελευταία χρόνια έχει διαπιστωθεί μια ραγδαία αύξηση του αριθμού των ευπαθειών στις εφαρμογές του παγκοσμίου ιστού. Θα μπορούσε να θεωρηθεί με ασφάλεια ότι η πολυπλοκότητα των τεχνολογιών που έχουν αναπτυχτεί τα τελευταία χρόνια σε συνδυασμό με την ωριμότητα που έχει επιτευχτεί στην ασφάλεια των λειτουργικών συστημάτων και των δικτύων, έχουν συμβάλει σημαντικά στην ανάγκη για ασφάλεια των εφαρμογών ιστού.

Η ανάπτυξη των κλάδων του ηλεκτρονικού εμπορίου, της ηλεκτρονικής τραπεζικής αλλά και της ηλεκτρονικής διακυβέρνησης έχει οδηγήσει στη συνεχώς αυξανόμενη χρήση των εφαρμογών ιστού εκτός προστατευμένων ιδεατών δικτύων και πλέον είναι διαθέσιμες στην πλειονότητα των χρηστών. Όπως είναι κατανοητό, απαιτούνται αυξημένα επίπεδα ασφάλειας λόγω της φύσης των δεδομένων που διαχειρίζονται πλέον οι εφαρμογές ιστού. Η παρατήρηση της αύξησης των αδυναμιών των εφαρμογών ιστού έναντι των αδυναμιών των υπόλοιπων συστημάτων μας οδηγεί στο συμπέρασμα ότι επιβάλλεται να εφαρμοστούν ελεγκτικές μεθοδολογίες και δοκιμές της ασφάλειας των εφαρμογών αυτών.

Ενώ έως τώρα έχουν αναπτυχθεί διαφορετικές μεθοδολογίες ελέγχου και δοκιμών της ασφάλειας των δικτύων και των συστημάτων, όπως αυτές αναφέρονται στο κεφάλαιο 2, στο πεδίο της ασφάλειας των εφαρμογών έχουν αναφερθεί διαφορετικές τεχνικές ελέγχου δίχως ωστόσο να ακολουθείται μια συγκεκριμένη μεθοδολογία η οποία θα καθορίζει τη διαδικασία των ελέγχων και των δοκιμών.

Ως πρώτη ολοκληρωμένη προσπάθεια μπορεί να θεωρηθεί το OWASP Testing Guide, όπου έχει αναπτυχτεί από μία δωρεάν και ανοιχτή παγκόσμια κοινότητα με σκοπό την βελτίωση της ασφάλειας των εφαρμογών διαδικτύου, με το όνομα Open Web Application Security Project.

4.2. OWASP – Οδηγός Ελέγχου

Οι δοκιμές διεισδυτικότητας οι οποίες αναλύονται από το OWASP testing guide βασίζονται στη λογική του «black box testing». Δηλαδή σε διενέργειες ελέγχων και δοκιμών κατά τις οποίες ο ελεγκτής δε γνωρίζει τίποτα ή σχεδόν τίποτα για την εφαρμογή που θα ελέγξει και το περιβάλλον στο οποίο έχει αυτή αναπτυχθεί.

Η μεθοδολογία των ελέγχων διεισδυτικότητας η οποία περιγράφεται στο OWASP testing guide καθορίζει δυο φάσεις ελέγχου. Την παθητική και την ενεργητική. Στη διάρκεια της παθητικής φάσης ο ελεγκτής γνωρίζει στην ουσία την εφαρμογή. Προσπαθεί να κατανοήσει την λογική της και τη χρησιμοποιεί με σκοπό να κατανοήσει τη λειτουργία της τόσο από επιχειρησιακής όσο και από τεχνικής πλευράς. Η συλλογή πληροφοριών για τη λειτουργιά της εφαρμογής είναι το πρώτο βήμα του οποίου το αποτέλεσμα θα χρησιμοποιηθεί για τη διενέργεια πιο εξειδικευμένων ελέγχων και ενεργητικού πλέον χαρακτήρα.

Η δεύτερη φάση ελέγχου και δοκιμών αποτελεί και την ενεργητική φάση του ελέγχου. Αποτελείται από εννέα πεδία δοκιμών τα οποία περιλαμβάνουν συνολικά 66 ελέγχους και δοκιμές και έχουν ως σκοπό τη αξιολόγηση των μηχανισμών ασφάλειας της εφαρμογής ενάντια συγκεκριμένων απειλών.

4.2.1. Δοκιμές της Διαχείρισης Παραμετροποίησης

Ως δοκιμές της διαχείρισης παραμετροποίησης ορίζονται ο έλεγχος και οι δοκιμές διεισδυτικότητας αναλύοντας τις υποδομές και την αρχιτεκτονική της τοπολογίας. Οι δοκιμές αυτές είναι δυνατό να αποκαλύψουν λεπτομέρειες για την παραμετροποίηση του περιβάλλοντος στο οποίο υφίσταται μια εφαρμογή ιστού. Παρακάτω ακολουθούν οι τεχνικές που αξιοποιούνται για τη διενέργεια των ελέγχων.

Δοκιμή πρωτοκόλλου SSL/TLS

Περιλαμβάνει τον έλεγχο των παραμέτρων των πρωτοκόλλων SSL (Secure Sockets Layer) και TLS (Transport Layer Security). Τα πρωτόκολλα αυτά χρησιμοποιούνται συνήθως για την εγκαθίδρυση ασφαλών καναλιών

επικοινωνίας μεταξύ μιας εφαρμογής ιστού και του χρήστη, προστατεύοντας την ακεραιότητα και την εμπιστευτικότητα μεταξύ των δύο άκρων.

Δοκιμή των DB Listeners

Η παραμετροποίηση του listener ενός συστήματος διαχείρισης βάσεων δεδομένων (DBMS) εάν δεν έχουν ληφθεί υπόψη οι κανόνες ασφάλειας μπορεί να αποτελούν ευπάθεια για την εφαρμογή. Αυτό συνεπάγεται τη δυνατότητα επικοινωνίας ενός επιτιθέμενου με το σύστημα με ενδεχόμενο αποτέλεσμα την αποκάλυψη χρήσιμων παραμέτρων για την εφαρμογή και τα δεδομένα που διαχειρίζεται.

Δοκιμή της διαχείρισης παραμετροποίησης της υποδομής

Με τον όρο υποδομή γίνεται αναφορά στους διακομιστές ιστού που εξυπηρετούν την εφαρμογή. Η διασύνδεση πολλών διαφορετικών διακομιστώ ιστού σε συνδυασμό με τη συνύπαρξη διαφορετικών εφαρμογών σε αυτούς εντός του οργανισμού, καθιστά δύσκολη και συχνά ανεφάρμοστη τη διαχείριση των παραμετροποιήσεων των εφαρμογών. Είναι δυνατόν η αδυναμία μίας άλλης εφαρμογής ή ενός διακομιστή να αποτελέσει σημείο μη εξουσιοδοτημένης πρόσβασης στην εφαρμογή.

Δοκιμή της διαχείρισης παραμετροποίησης των εφαρμογών

Πολλές παράμετροι μιας εφαρμογής είναι δυνατό να αποκαλυφθούν σε μη εξουσιοδοτημένο χρήστη λόγω της αναφοράς τους και της εκ παραδρομής εμφάνισης τους μέσα στον πηγαίο κώδικα, στα αρχεία ημερολογίου (log files) καθώς και στα μηνύματα λάθους των διακομιστώ ιστού. Ο ενδελεχής έλεγχος ενάντια σε τέτοιου είδους περιπτώσεις είναι κρίσιμος ούτος ώστε να αποφεύγει η αποκάλυψη των πληροφοριών αυτών.

Δοκιμή της διαχείρισης επεκτάσεων αρχείων

Η εμφάνιση της κατάληξης των αρχείων που απαρτίζουν την εφαρμογή ιστού κάνει δυνατή την αποκάλυψη των τεχνολογιών τόσο του διακομιστή ιστού όσο

και την πλατφόρμας ανάπτυξης που χρησιμοποιήθηκε για τη δημιουργία της εφαρμογής. Η αποκάλυψη των τεχνολογιών αυτών μπορεί να χρησιμοποιηθεί από κάποιον επιτιθέμενο ώστε να αναζητήσει τυχόν αδυναμίες των συστημάτων αυτών και να τις αξιοποιήσει ώστε να αποκτήσει διαχειριστική πρόσβαση στην εφαρμογή.

Παλαιά αρχεία και αρχεία αντιγράφων ασφάλειας

Η ύπαρξη παλαιών αρχείων, backup και άλλων αρχείων που δεν αναφέρονται στις ιστοσελίδες της εφαρμογής αποτελούν ένα μείζον πρόβλημα για την ασφάλεια αυτής, καθότι στα αρχεία αυτά ενδέχεται να αναφέρονται πληροφορίες για την παραμετροποίηση της εφαρμογής τα οποία εάν αποκαλυφθούν σε μη εξουσιοδοτημένο πρόσωπο θέτουν σε κίνδυνο την εμπιστευτικότητα αυτής.

Διαχειριστικές διεπαφές υποδομής και εφαρμογών

Είναι σύνηθες το γεγονός μια εφαρμογής να έχει αναπτυχθεί από έτοιμες πλατφόρμες λογισμικού οι οποίες έχουν ένα κοινό σημείο πρόσβασης για τη διαχείριση της εφαρμογής. Γνωστά σε όλους είναι τα συστήματα CMS (Content Management Systems) τα οποία χρησιμοποιούν κάποιο συγκεκριμένο URL για τη πρόσβαση στο διαχειριστικό περιβάλλον της εφαρμογής. Εφόσον είναι γνωστό το σημείο αυτό είναι δυνατή η εκτέλεση διαφόρων τεχνικών για την παράκαμψη του μηχανισμού προσβάσεων στο σύστημα.

Δοκιμές μεθόδων του πρωτοκόλλου HTTP και XST

Ο έλεγχος προσβλέπει στην αποφυγή εκτέλεσης ενδεχόμενων HTTP εντολών από τον διακομιστή ιστού καθώς και στην εκτέλεση επιθέσεων Cross Site Tracing (XST).

4.2.2. Δοκιμές επιχειρησιακής λογικής

Το συγκεκριμένο πεδίο ελέγχου και δοκιμών έχει ως σκοπό την αποκάλυψη αδυναμιών που οφείλονται σε λογικά λάθη επιχειρησιακού σχεδιασμού. Αποτελεί ίσως και το πιο δύσκολο πεδίο ελέγχου διότι δεν βασίζεται ούτε σε

τεχνολογική αδυναμία ούτε σε λανθασμένη παραμετροποίηση αλλά σε ελλιπή επιχειρησιακό σχεδιασμό των ροών εργασίας που ακολουθεί μια εφαρμογή.

4.2.3. Δοκιμές αυθεντικοποίησης

Ως αυθεντικοποίηση ορίζεται η διαδικασία κατά την οποία πιστοποιείται η αυθεντικότητα ενός ατόμου ή υπηρεσίας έναντι ενός πληροφοριακού πόρου.

Δοκιμή μετάδοσης διαπιστευτηρίων από μη κρυπτογραφημένο κανάλι

Στη συγκεκριμένη δοκιμή εξετάζεται εάν η διαμεταγωγή των δεδομένων αυθεντικοποίησης γίνεται μέσω ασφαλούς σύνδεσης. Συγκεκριμένα, κατά τη διαδικασία σύνδεσης ενός χρήστη στην εφαρμογή γίνεται η μετάδοση στοιχείων αυθεντικοποίησης όπως username και password. Τα δεδομένα αυτά πρέπει να μεταδίδονται μέσω κρυπτογραφημένου καναλιού ώστε να αποφευχθεί ο κίνδυνος υποκλοπής τους.

Δοκιμή απαρίθμησης λογαριασμών χρηστών

Η δοκιμή αυτή εξετάζει τη δυνατότητα απαρίθμησης των έγκυρων χρηστών που χρησιμοποιούν την εφαρμογή. Κάποιος επιτιθέμενος εάν γνωρίζει κάποιο πλήθος ονομάτων χρηστών που χρησιμοποιούν την εφαρμογή τότε μπορεί να εφαρμόσει τεχνικές επιθέσεων brute force ώστε να αποκαλύψει τους κωδικούς πρόσβασης αυτών και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στην εφαρμογή.

Δοκιμή για προκαθορισμένους ή προβλέψιμους κωδικών

Ο συγκεκριμένος έλεγχος προσβλέπει στη εύρεση ονομάτων λογαριασμών χρηστών οι όποιοι είναι είτε εύκολα προβλέψιμα είτε αποτελούν προκαθορισμένα ονόματα από τον κατασκευαστή της εφαρμογής. Συνήθως οι δόκιμες αυτές χρησιμοποιούν λεξικά και δοκιμάζουν λέξεις ή συνδυασμό λέξεων για να μαντέψουν κάποιο όνομα χρήστη.

Δοκιμή με τον αλγόριθμο Brute Force

Η συγκεκριμένη δοκιμή χρησιμοποιεί την τεχνική επίθεσης brute force κατά την οποία δοκιμάζονται συνδυασμοί γραμμάτων για την πρόβλεψη ονομάτων χρηστών και κωδικών πρόσβασης. Η συγκεκριμένη τεχνική σημειώνεται ότι είναι αρκετά χρονοβόρα και χρησιμοποιείται στις περιπτώσεις που τα dictionary attacks αποτυγχάνουν.

Δοκιμή παράκαμψης του μηχανισμού αυθεντικοποίησης

Στη δοκιμή αυτή γίνεται η προσπάθεια ανεύρεσης των πόρων εκείνων της εφαρμογής ιστού για τους οποίους λόγω προγραμματιστικής παράλειψης δεν έχει παραμετροποιηθεί η διαδικασία αυθεντικοποίησης, οπότε και μπορεί να επιτευχτεί μη εξουσιοδοτημένη πρόσβαση στον πόρο.

Δοκιμή του μηχανισμού υπενθύμισης

Στη συγκεκριμένη δοκιμή ελέγχεται ο μηχανισμός υπενθύμισης κωδικού για αδυναμίες και η δυνατότητα αποθήκευσης των κωδικών πρόσβασης στον φυλλομετρητή.

Δοκιμή μηχανισμού αποσύνδεσης

Στη συγκεκριμένη δοκιμή γίνεται έλεγχος του μηχανισμού αποσύνδεσης από την εφαρμογή και της δυνατότητας επανεισόδου στο σύστημα έπειτα από επιτυχή αποσύνδεση χρησιμοποιώντας προηγούμενη συνεδρία (session).

Δοκιμή του μηχανισμού Captcha

Ο συγκεκριμένος έλεγχος προσβλέπει στην αποκάλυψη αδυναμιών του μηχανισμού CAPTCHA. Ο μηχανισμός αυτός αποτελεί την υλοποίηση τεχνικής challenge-response κατά την οποία απαιτείται η διαδραστικότητα μεταξύ χρήστη και εφαρμογής για την αποφυγή αυτοματοποιημένων ερωτήσεων στην εφαρμογή.

Δοκιμή των μηχανισμών πολλαπλής αυθεντικοποίησης

Πολλές εφαρμογές χρησιμοποιούν μηχανισμούς με τους οποίους επιτυγχάνουν την αυθεντικοποίηση του χρήστη αξιοποιώντας μηχανισμούς με απαιτήσεις πέραν της εισαγωγής ονόματος χρήστη και κωδικού πρόσβασης από τον χρήστη. Τέτοιοι μηχανισμοί χρησιμοποιούν one-time-passwords, SMS, έξυπνες κάρτες κλπ. Στη δοκιμή αυτή ελέγχονται οι μηχανισμοί αυτοί.

Δοκιμές των race conditions

Στην δοκιμή αυτή γίνονται έλεγχοι οι όποιοι βασίζονται στη διάρκεια χρόνου που απαιτείται για να γίνουν κάποιες διεργασίες από την εφαρμογή.

4.2.4. Δοκιμές εξουσιοδότησης

Η διαδικασία της εξουσιοδότησης είναι αυτή κατά την οποία επιτρέπεται η πρόσβαση στους πόρους μόνο στα πρόσωπα και τις υπηρεσίες που έχει επιτραπεί η πρόσβαση. Η δοκιμή των μηχανισμών εξουσιοδότησης περιλαμβάνει την κατανόηση του τρόπου λειτουργίας αυτών και κατά συνέπεια τη διερεύνηση για ύπαρξη αδυναμιών που θα μπορούσαν να επιτύχουν τη μη εξουσιοδοτημένη πρόσβαση σε κάποιο πόρο. Σημειώνεται ότι η διαδικασία εξουσιοδότησης έπεται της διαδικασίας εξουσιοδότησης.

Δοκιμές χειρισμού των δρομολογίων συστήματος αρχείων

Στη δοκιμή αυτή εξετάζεται η δυνατότητα μη εξουσιοδοτημένης πρόσβασης σε αρχεία τα οποία βρίσκονται στον διακομιστή ιστού και για τα οποία δεν έχουν παραμετροποιηθεί επαρκείς μηχανισμοί εξουσιοδότησης. Είναι δυνατόν η πρόσβαση σε αρχεία να δίνει τη δυνατότητα να εκτελεστεί πηγαίος κώδικας ή συστημικές εντολές από κάποιον επιτιθέμενο.

Δοκιμές παράκαμψης μηχανισμών εξουσιοδότησης

Στον έλεγχο αυτό μελετάται ο τρόπος υλοποίησης πολιτικών εξουσιοδότησης για τους υφιστάμενους πόρους και εξετάζεται η δυνατότητα προσπέρασης των μηχανισμών εξουσιοδότησης ώστε να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε αυτούς.

Δοκιμή κλιμάκωσης προνομίων

Στην δοκιμή αυτή εξετάζεται το ενδεχόμενο κάποιος χρήστης να έχει τη δυνατότητα να μεταβάλει τα δικαιώματα που του έχουν αποδοθεί με αποτέλεσμα να αποκτήσει τη δυνατότητα πρόσβαση σε πληροφοριακούς πόρους στους οποίους δεν του επιτρέπεται η πρόσβαση.

4.2.5. Δοκιμή μηχανισμού διαχείρισης συνεδρίας

Κατά το παρελθόν, όταν προέκυψε η ανάγκη για δημιουργία εφαρμογών οι οποίες αλληλεπιδρούν με τον χρήστη διαμέσου του παγκόσμιου ιστού οι μηχανικοί λογισμικού βρέθηκαν αντιμέτωποι με το εμπόδιο της συνεχούς αυθεντικοποίησης. Όταν ο χρήστης απαιτούσε την προβολή ιστοσελίδων οι οποίες χρησιμοποιούσαν διαρκώς συγκεκριμένες παραμέτρους ανά χρήστη έπρεπε ανά σελίδα να εισάγει το όνομα χρήστη και τον προσωπικό του κωδικό. Το πρωτόκολλο HTTP ωστόσο δεν είναι ένα δυναμικό πρωτόκολλο με αποτέλεσμα να πρέπει να δημιουργηθεί κάποιος μηχανισμός ο οποίος θα διατηρεί το χρήστη διαρκώς συνδεδεμένο και η εφαρμογή να χρησιμοποιεί τις παραμέτρους για τον συγκεκριμένο χρήστη. Η λύση δόθηκε με τους μηχανισμούς διαχείρισης συνεδριών που παρέχουν διάσημες γλώσσες προγραμματισμού όπως είναι η PHP και η ASP. Ως συνεδρία (session) ορίζεται η λειτουργία της εφαρμογής με προσωποποιημένες παραμέτρους η οποία εγκαθιδρύεται όταν ο χρήστης αυθεντικοποιείται αρχικά από την εφαρμογή. Οι μηχανισμοί αυτοί χρησιμοποιούν είτε session token είτε cookies.Η δοκιμή αυτή ελέγχει την ασφάλεια διαχείρισης των εν λόγω μηχανισμών.

Δοκιμές του μηχανισμού δημιουργίας συνεδρίας

Με τον έλεγχο αυτό εξετάζονται οι μηχανισμοί δημιουργίας ενός session (πχ η δημιουργία ενός session token ή ενός cookie) και οι τρόποι αποφυγής του session ώστε να επιτευχτεί η μη εξουσιοδοτημένη πρόσβαση.

Δοκιμές των παραμέτρων των Cookies

Τα cookies γίνονται συχνά αντικείμενα επίθεσης για την ανεύρεση των κρυπτογραφικών κλειδιών των κρυπτόλεξων που αναφέρονται μέσα σε αυτά. Η δοκιμή αυτή εξετάζει τον τρόπο με τον οποίο η εφαρμογή προστατεύει τις πληροφορίες που αναφέρονται στα cookies.

Δοκιμή αλλοίωσης συνεδρίας

Στον προκείμενο έλεγχο γίνεται η προσπάθεια ανεύρεσης της αδυναμίας μη ανανέωσης ενός cookie ύστερα από την επιτυχή αυθεντικοποίηση ενός χρήστη στην εφαρμογή. Η αδυναμία αυτή κάνει δυνατή την χρήση ενός γνωστού cookie στον επιτιθέμενο από το χρήστη.

Δοκιμή για αποκάλυψη πληροφοριών των συνεδριών

Είναι δυνατό ο αλγόριθμος δημιουργίας ενός session token να βασίζεται σε προσωπικά δεδομένα όπως είναι για παράδειγμα το όνομα χρήστη που χρησιμοποιείται για την είσοδο στην εφαρμογή. Κάποιος επιτιθέμενος μπορεί να εκτελέσει επιθέσεις στο session token ώστε να κατανοήσει τον αλγόριθμο δημιουργίας του token και να μπορεί να κατασκευάζει δικά του tokens ώστε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς άλλων χρηστών.

Δοκιμές για την αδυναμία CSRF

Το CSRF (Cross Site Request Forgery) είναι μια συγκεκριμένη τεχνική επίθεσης με την οποία κάποιος επιτιθέμενος μπορεί να αναγκάσει κάποιον χρήστη να εκτελέσει συγκεκριμένες ενέργειες στην εφαρμογή στην οποία είναι ήδη αυθεντικοποιημένος. Η τεχνική αυτή ονομάζεται και session riding και ο έλεγχος

αυτός διενεργείται για τη διαπίστωση εάν η εφαρμογή είναι ευάλωτη σε αυτού του είδους τις επιθέσεις.

4.2.6. Δοκιμές επικύρωσης δεδομένων

Δοκιμές για αδυναμίες Cross Site Scripting

Στις δοκιμές αυτές ελέγχεται η εφαρμογή για αδυναμίες cross site scripting (XSS). Οι αδυναμίες αυτές δίνουν τη δυνατότητα σε κάποιον επιτιθέμενο να αλλοιώσει τη λειτουργία μιας εφαρμογής ιστού ώστε να παράγει επικίνδυνα δεδομένα εξόδου, χειραγωγώντας τις παραμέτρους εισόδου της εφαρμογής. Η αδυναμία αυτή υφίσταται σε περιπτώσεις όπου δεν πραγματοποιείται επαρκής έλεγχος των δεδομένων εισόδου δίνοντας τη δυνατότητα σε κακόβουλους χρήστες να τα χειριστούν κατά το δοκούν. Η αδυναμία αυτή οδηγεί σε πληθώρα επιθέσεων όπως είναι η εκτέλεση επικίνδυνων εφαρμογών javascript στον φυλλομετρητή των χρηστών ή στην κλοπή προσωπικών πληροφοριών.

Δοκιμές εμφύτευσης

Στις δοκιμές αυτές γίνεται προσπάθεια εντοπισμού αδυναμιών εμφύτευσης εντολών ή κώδικα στο URL ή στον HTTP κώδικα μίας εφαρμογής ιστού. Η αδυναμία αυτή δίνει τη δυνατότητα σε κάποιον κακόβουλο χρήστη να εκτελέσει για παράδειγμα ερωτήματα σε μια βάση δεδομένων (SQL injection) με σκοπό την κλοπή προσωπικών ή και άλλων δεδομένων από το σύστημα βάσεων δεδομένων που εξυπηρετεί την εφαρμογή. Εμφυτεύσεις είναι δυνατό να πραγματοποιηθούν έχοντας ως στόχο βάσεις δεδομένων (SQL injection), υπηρεσίες καταλόγου (LDAP injection), το λειτουργικό σύστημα ενός διακομιστή (OS injection) ή την παραποίηση της λειτουργίας μιας εφαρμογής (code injection).

4.2.7. Δοκιμές άρνησης υπηρεσιών

Δοκιμές SQL Wildcard επιθέσεων

Οι SQL wildcard επιθέσεις έχουν ως σκοπό την μείωση των διαθέσιμων υπολογιστικών πόρων ενός διακομιστή ο οποίος φιλοξενεί ένα σύστημα διαχείρισης βάσεων δεδομένων. Οι επιθέσεις αυτές πραγματοποιώντας ερωτήματα στη βάση δεδομένων τα οποία περιέχουν wildcard χαρακτήρες (π.χ. %).

Δοκιμές κλειδώματος λογαριασμών χρηστών

Στις δοκιμές αυτές, επιχειρείται να προσδιοριστούν οι μηχανισμοί προστασίας των λογαριασμών χρηστών, από κακόβουλους χρήστες, οι οποίοι επιδιώκουν το κλείδωμα λογαριασμών χρηστών ύστερα από πολλαπλές προσπάθειες. Ως συνέπεια των επιθέσεων αυτών είναι η άρνηση των υπηρεσιών σε αυξανόμενο αριθμό χρηστών.

Buffer Overflows

Στις δοκιμές αυτές γίνεται η προσπάθεια εντοπισμού αδυναμιών οι οποίες ενδέχεται να οδηγήσουν σε buffer overflows με αποτέλεσμα την άρνηση υπηρεσιών της εφαρμογής. Χαρακτηριστικό παράδειγμα είναι η εισαγωγή μεγάλου αριθμού χαρακτήρων σε κάποιο πεδίο εισόδου της εφαρμογής, με αποτέλεσμα την αδυναμία διαχείρισης του από τον εκάστοτε διακομιστή ιστού ή την εφαρμογή.

4.2.8. Δοκιμές υπηρεσιών ιστού

Οι εφαρμογές οι οποίες αξιοποιούν την αρχιτεκτονική SOA (Service Oriented Architecture) και κατ' επέκταση τις υπηρεσίες ιστού αποτελούν συστήματα τα οποία εφαρμόζουν την επιχειρησιακή λογική ενός οργανισμού και γνωρίζουν εξαιρετική άνθιση τα τελευταία χρόνια. Τα web services χρησιμοποιούν το πρωτόκολλο HTTP σε συνδυασμό με γλώσσες περιγραφής δεδομένων όπως είναι η XML και η WSDL και με τεχνολογίες όπως το πρωτόκολλο SOAP. Τα web

services χρησιμοποιούν το πρωτόκολλο SOAP (Simple Object Access Protocol) για την επικοινωνία μεταξύ τους, την γλώσσα WSDL με σκοπό την περιγραφή των διεπαφών ενός web service και τον μηχανισμό UDDI (Universal Description, Discovery and Integration) για την καταχώρηση και δημοσίευσης τους ώστε να είναι προσβάσιμα από πιθανούς «πελάτες», δηλαδή άλλα web services.

Το συγκεκριμένο πεδίο ελέγχου και δοκιμών επικεντρώνεται στην ασφάλεια των υπηρεσιών ιστού και στα δομικά στοιχεία αυτών. Σημειώνεται ότι οι αδυναμίες των υπηρεσιών ιστού είναι ανάλογες με αυτές των άλλων εφαρμογών ιστού ωστόσο διαφέρουν λόγω των αδυναμιών τόσο των XML parsers όσο και των πληροφοριών που εμπεριέχονται στα δεδομένα XML.

Συγκέντρωση πληροφοριών υπηρεσιών ιστού

Ο συγκεκριμένος έλεγχος επικεντρώνεται στη συλλογή πληροφοριών σχετικά με τις διεπαφές των web services και οι οποίες περιγράφονται από τη γλώσσα WSDL.

Δοκιμές WSDL

Ο έλεγχος αυτός βασίζεται στη συλλογή πληροφοριών που πραγματοποιήθηκε με τον παραπάνω έλεγχο. Συγκεκριμένα, δοκιμάζονται οι διεπαφές οι οποίες περιγράφθηκαν από την ανταλλαγή WSDL αρχείων. Δημιουργώντας πλασματικά SOAP μηνύματα και συγκεκριμένα αποστέλλοντας SOAP requests σε ένα WS γίνεται η προσπάθεια ανίχνευσης των πληροφοριών που μπορούν να εξαχθούν από τις υπό δοκιμή διεπαφές.

Δοκιμές δομής XML

Όπως αναφέρθηκε παραπάνω, οι υπηρεσίες ιστού βασίζονται στη γλώσσα XML η οποία αποτελεί γλωσσά περιγραφής δεδομένων. Τόσο για τη σύνταξη των XML αρχείων όσο και για την αξιοποίηση των δεδομένων αυτών από ένα τέτοιο αρχείο χρησιμοποιείται κάποιος μεταφραστής (parser) ο οποίος εκτελεί αυτή τη διεργασία. Ο έλεγχος αυτός επικεντρώνεται στην ανεύρεση αδυναμιών του parser

σε περιπτώσεις όπου το XML αρχείο δεν είναι σωστά δομημένο και αναγκάζει τον parser στην κατανάλωση υπολογιστικών πόρων με αποτέλεσμα την επιφόρτιση της CPU και τη μνήμης του διακομιστή στο οποίο εκτελεί η υπηρεσία ιστού.

Δοκιμές του περιεχομένου μηνυμάτων XML

Στον συγκεκριμένο έλεγχο πραγματοποιούνται δοκιμές ασφάλειας των συστημάτων που χρησιμοποιεί η υπηρεσία ιστού. Για παράδειγμα μια υπηρεσία ιστού να χρησιμοποιείται ως η διεπαφή για τη μεταφορά της λειτουργικότητας ενός παλαιού συστήματος στα πλαίσια της SOA αρχιτεκτονικής. Το παλαιό σύστημα ενδέχεται να είναι ευάλωτο σε επιθέσεις οι οποίες εν τέλει επηρεάζουν τις πληροφορίες και τη λειτουργιά της υπηρεσίας ιστού.

Δοκιμές υπηρεσιών ιστού REST

Μια κατηγορία τεχνολογίας υπηρεσιών ιστού είναι και τα REST (representational state transfer) web services. Τα συγκεκριμένα web services κάνουν χρήση των HTTP GET ερωτημάτων με σκοπό να θέσουν τις παραμέτρους σε μια μέθοδο ενός web service. Ο συγκεκριμένος έλεγχος διενεργείται με σκοπό την εύρεση αδυναμιών που επιτρέπουν τη χρήση επικίνδυνου περιεχομένου ως παράμετρος στο HTTP ερώτημα. Όπως για παράδειγμα κάποιο SQL injection ή μεγάλου μήκος δεδομένα τα οποία θα προκαλέσουν άρνηση υπηρεσιών.

Ασυνήθιστες SOAP προσαρτήσεις

Ο συγκεκριμένος έλεγχος εξετάζει τη δυνατότητα μεταφοράς δεδομένων υπό τη μορφή αρχείων με το πρωτόκολλο SOAP. Είναι δυνατό να υφίστανται αδυναμίες σχετικά με την αποστολή για παράδειγμα εκτελέσιμων αρχείων τα οποία χρησιμοποιούνται ως παράμετροι σε μια διεπαφή μιας υπηρεσίας ιστού.

Δοκιμές επαναληψιμότητας

Η συγκεκριμένη δόκιμη εξετάζει τη δυνατότητα επαναλαμβανόμενων επιθέσεων με σκοπό την πλαστοπροσωπία για τη εκτέλεση συγκεκριμένων ερωτημάτων προς τη διεπαφή ενός web service.

ΚΕΦΑΛΑΙΟ 5ο

Εργαλεία Ελέγχων Διείσδυσης

5.1.Συλλογή πληροφοριών

5.1.1. Σύστημα DNS

DnsEnum

Το DNSenum αποτελεί ένα εργαλείο το οποίο αξιοποιείται για την απαρίθμηση πληροφοριών του συστήματος DNS.

Ο σκοπός του εργαλείου είναι η συγκέντρωση πληροφοριών που βασίζονται στην παραμετροποίηση DNS servers. Το DNSenum εκτελεί ενδεικτικά τις παρακάτω λειτουργίες:

- Ανάκτηση A/NS/MX records.
- Εκτέλεση axfr ερωτημάτων (zone transfers)
- Απαρίθμηση subdomains μέσω google queries
- Brute force subdomains από αρχείο
- Υπολογισμός εύρους IP διευθύνσεων και εκτέλεση whois για αυτές
- Reverse NS lookups σε εύρος IP διευθύνσεων

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

Dns-Walk

Το Dns-Walk αποτελεί ένα εργαλείο αποσφαλμάτωσης (debugging) για την παραμετροποίηση του συστήματος DNS.

Το εργαλείο αυτό εκτελεί zone transfers για συγκεκριμένο domain και ελέγχει την παραμετροποίηση του συστήματος DNS για τη συνέχεια και την ακρίβεια του.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

5.1.2. Συλλογή λογαριασμών ηλεκτρονικού ταχυδρομείου

TheHarvester

Το εργαλείο theHarvester συγκέντρωσης λογαριασμών email, λογαριασμών χρηστών από διαφορετικές πηγές όπως μηχανές αναζήτησης, pgp servers και ιστοσελίδες κοινωνικής δικτύωσης.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.1.3. Συλλογή μεταδεδομένων

FOCA

Το FOCA αποτελεί ένα εργαλείο ανάλυσης των metadata διαφόρων τύπων εγγράφων όπως Microsoft Office Documents, PDF files, Open Office Files, Word Perfect files και EXIF Metadata. Με το συγκεκριμένο εργαλείο μπορεί να γίνει απαρίθμηση χρηστών, εκτυπωτών, λογαριασμών email καθώς και των εκδόσεων εφαρμογών δημιουργίας των αρχείων.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Windows λειτουργικών συστημάτων.

5.1.4. Διαδικτυακές υπηρεσίες

Robtex.com

Η συγκεκριμένη ιστοσελίδα προσφέρει πληθώρα υπηρεσιών αναζήτησης πληροφοριών σχετικών με IP διευθύνσεις και DNS-based πληροφοριών.

Ενδεικτικά με το robtex.com μπορούν να εκτελεστούν τα παρακάτω:

- RBL checks
- DNS information discovery
- whois lookups
- BGP announcements checks
- AS numbers checks

Network-Tools.com

Η συγκεκριμένη ιστοσελίδα προσφέρει web based υπηρεσίες όπως Pings, NS lookups, Traceroutes, whois lookups, RBLs lookups, email accounts verification.

5.1.5. Δρομολόγηση

0trace

Το 0trace είναι ένα εργαλείο αναγνώρισης με το οποίο επιτυγχάνεται hop enumeration μέσω μιας ήδη εγκαθιδρυμένης TCP σύνδεσης (SMTP, HTTP κλπ). Σημειώνεται ότι με το συγκεκριμένο εργαλείο είναι δυνατή η παράκαμψη συστημάτων τειχών ασφάλειας (firewalls) για την εκτέλεση της απαρίθμησης.

Σημειώνεται ότι, το εργαλείο δεν θα αποφέρει σημαντικά αποτελέσματα εάν στην υποδομή γίνονται drop από τα firewalls, τα firewalls εκτελούν TTL και full packet rewriting, υφίστανται load balancers. Επίσης, σημειώνεται ότι είναι πλήρως ανιχνεύσιμο από υποδομές IPS/IDS.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

Itrace

Το συγκεκριμένο πρόγραμμα εκτελεί traceroute χρησιμοποιώντας ICMP echo requests, οπότε σε υποδομές ασφάλειας εμφανίζεται ότι εκτελεί pings.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

NMBscan

Το συγκεκριμένο εργαλείο χρησιμοποιείται για την ανίχνευση κοινόχρηστων πόρων (shares) σε ένα δίκτυο χρησιμοποιώντας ta NMB/SMB/NetBIOS πρωτόκολλα.

Είναι επίσης χρήσιμο για την ανάκτηση πληροφοριών όπως:

- NMB/SMB/NetBIOS/Windows hostname
- IP address
- IP hostname
- ethernet MAC address
- Windows username
- NMB/SMB/NetBIOS/Windows domain names.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

TCPtraceroute

Το συγκεκριμένο εργαλείο είναι ένα εργαλείο tracerouting το οποίο χρησιμοποιεί TCP SYN πακέτα αντί για ICMP.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

5.1.6. Μηχανές αναζήτησης

Bing-ip2hosts

Το συγκεκριμένο εργαλείο αποτελεί εργαλείο ανεύρεσης ιστοσελίδων που γίνονται host στην ίδια IP διεύθυνση. Χρησιμοποιεί το χαρακτηριστικό αναζήτησης βάσει IP διεύθυνσης της μηχανής αναζήτησης bing.

Metagoogil

Το συγκεκριμένο εργαλείο εκτελεί εξόρυξη των metadata πληροφοριών από έγγραφα (pdf,doc,xls,ppt,odp,ods) δημοσιευμένα σε ιστοσελίδες. Εξάγει λίστες με πιθανά ονόματα λογαριασμών χρηστών, paths στα metadata, MAC διευθύνσεις από MS office έγγραφα κλπ.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

Maltego

Το maltego είναι ένα πρόγραμμα το οποίο αξιοποιεί πληροφορίες κυρίως από μηχανές αναζήτησης και με το οποίο είναι δυνατό να εξορυχτούν πληροφορίες και παραχθούν συσχετίσεις μεταξύ πληροφοριών που αφορούν:

- Domain Names
- Whois Information
- DNS Names
- Netblocks
- IP Addresses

Με το maltego είναι δυνατή η απαρίθμηση πληροφοριών ενός προσώπου (φυσικού ή νομικού) όπως Email διευθύνσεις, ιστοσελίδες και τηλεφωνικοί αριθμοί

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix kai Windows λειτουργικών συστημάτων.

5.2.Χαρτογράφηση δικτύου

5.2.1. Προσδιορισμός ενεργών μηχανημάτων

Angry IP scanner

Το angry IP scanner είναι ένας portable port scanner ο οποίος εκτελεί σάρωση θυρών, ανίχνευση ενεργών μηχανημάτων καθώς και εξόρυξη πληροφοριών μέσω netbios.

Nbtscan

Το Nbtscan είναι ένα εργαλείο το οποίο ανιχνεύει την ύπαρξη ανοιχτών NetBIOS name servers σε ένα δίκτυο.

Nmap

Το nmap είναι ένας ανιχνευτής ασφάλειας με τον οποίο μπορούν να εκτελεστούν port scans, να επιτευχτεί host enumeration, active OS και service discovery. Σημειώνεται ότι με το συγκεκριμένο εργαλείο μπορούν να εκτελεστούν και άλλες λειτουργίες μέσω NSE scripts (vulnerability assessments κλπ)

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix kai Windows λειτουργικών συστημάτων.

5.2.2. Προσδιορισμός λειτουργικών συστημάτων

Nmap

Το nmap είναι ένας ανιχνευτής ασφάλειας με τον οποίο μπορούν να εκτελεστούν port scans, να επιτευχτεί host enumeration, active OS και service discovery. Σημειώνεται ότι με το συγκεκριμένο εργαλείο μπορούν να εκτελεστούν και άλλες λειτουργίες μέσω NSE scripts (vulnerability assessments κλπ).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

P0f

Το P0f είναι ένα εργαλείο παθητικής ανίχνευσης του λειτουργικού συστήματος απομακρυσμένων συστημάτων. Επίσης έχει τη δυνατότητα ανίχνευσης firewalls καθώς και τη χρήση NAT σε ένα δίκτυο.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

Xprobe2

Το Xprobe2 αποτελεί εργαλείο ενεργής ανίχνευσης του λειτουργικού συστήματος απομακρυσμένων συστημάτων.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux και Unix λειτουργικών συστημάτων.

5.2.3. Σάρωση θυρών

Nmap

Το nmap είναι ένας ανιχνευτής ασφάλειας με τον οποίο μπορούν να εκτελεστούν port scans, να επιτευγθει host enumeration, active OS και service discovery. Σημειώνεται ότι με το συγκεκριμένο εργαλείο μπορούν να εκτελεστούν και άλλες λειτουργίες μέσω NSE scripts (vulnerability assessments κλπ).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

Angry IP scanner

Το angry IP scanner είναι ένας ανιχνευτής θυρών για τον οποίο δεν απαιτείται εγκατάσταση και ο οποίος εκτελεί σάρωση θυρών, ανίχνευση ενεργών μηχανημάτων καθώς και εξόρυξη πληροφοριών μέσω του πρωτοκόλλου netbios.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.2.4. Προσδιορισμός υπηρεσιών

Nmap

Το nmap είναι ένας ανιχνευτής ασφάλειας με τον οποίο μπορούν να εκτελεστούν port scans, να επιτευχτεί host enumeration, active OS και service discovery. Σημειώνεται ότι με το συγκεκριμένο εργαλείο μπορούν να εκτελεστούν και άλλες λειτουργίες μέσω NSE scripts (vulnerability assessments κλπ).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

Sslscan

Το συγκεκριμένο εργαλείο εκτελεί queries σε SSL services με σκοπό να διαπιστωθούν τα υποστηριζόμενα ciphers από τα συστήματα.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

SSLdigger

Το συγκεκριμένο εργαλείο εκτελεί queries σε SSL services με σκοπό να διαπιστωθούν τα υποστηριζόμενα ciphers από τα συστήματα.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Windows λειτουργικών συστημάτων.

Amap

Το amap αποτελεί ανιχνευτή πρωτοκόλλων εφαρμογών, μπορεί να ανιχνεύσει το πρωτόκολλο που χρησιμοποιείται ανεξάρτητα από τη δικτυακή θύρα που χρησιμοποιεί η υπηρεσία που προσφέρει επικοινωνία μέσω του υπό έλεγχο πρωτοκόλλου.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux λειτουργικών συστημάτων.

Httprint

Το Httprint είναι ένα εργαλείο ανίχνευσης των διακομιστώ και υπηρεσιών ιστού (fingerprinting).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.3. Αποτίμηση ευπαθειών

5.3.1. Αποτίμηση πρωτοκόλλου SMB

Keimpx

Το Keimpx είναι ένα εργαλείο για τον έλεγχο συγκεκριμένων διαπιστευτηρίων σε συστήματα με τη χρήση του πρωτοκόλλου SMB. Το συγκεκριμένο εργαλείο μπορεί να χρησιμοποιήσει διαπιστευτήρια όπως:

- Συνδυασμό user / plain-text password.
- Συνδυασμό user / NTLM hash.
- Συνδυασμό user / NTLM logon session token

Το εργαλείο στη συνέχεια δίνει τη δυνατότητα εκτέλεσης ενεργειών στα συστήματα μέσω του SMB πρωτοκόλλου.

5.3.2. Αποτίμηση πρωτοκόλλου SNMP

SnmpEnum

Το SnmpEnum αποτελεί ένα εργαλείο απαρίθμησης συσκευών που χρησιμοποιούν το πρωτόκολλο SNMP.

SnmpWalk

Το εργαλείο αυτό επιτρέπει τη συλλογή πληροφοριών συστημάτων τα οποία χρησιμοποιούν το πρωτόκολλο SNMP.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.3.3. Ανιχνευτές ευπαθειών

OpenVAS

Το openVAS αποτελεί ένα εργαλείο αποτίμησης ευπαθειών συστημάτων.

Nessus

Το Nessus αποτελεί το πλέον γνωστό εργαλείο ανίχνευσης ευπαθειών συστημάτων. Είναι αρκετά διαδεδομένο καθώς παρέχει τη δυνατότητα διασύνδεσης του με τρίτες εφαρμογές όπως είναι το nmap για port scanning, το hydra για password cracking και το metasploit για την μετέπειτα αξιοποίηση των ευρημάτων του ανιχνευτή.

5.4. Αξιοποίηση αδυναμιών

Metasploit

Το Metasploit αποτελεί ένα ολοκληρωμένο πλαίσιο ανάπτυξης εφαρμογών εκμετάλλευσης αδυναμιών και εκτέλεσης επιθέσεων σε αυτές. Είναι εξ ολοκλήρου γραμμένο στη γλώσσα ruby και αποτελεί το πιο διαδεδομένο εργαλείο στο είδος του.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.5. Κλιμάκωση προνομίων

5.5.1. Αυθεντικοποίηση Δικτύου

Ncrack

Το συγκεκριμένο εργαλείο χρησιμοποιείται για τον έλεγχο συστημάτων για αδύναμα συνθηματικά, εκτελώντας brute force attacks σε υπηρεσίες όπως είναι οι RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, και telnet. Το συγκεκριμένο εργαλείο επιτρέπει τον ταυτόχρονο έλεγχο πολλαπλών μηχανημάτων.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.5.2. Αποκάλυψη κωδικού

John

Το συγκεκριμένο εργαλείο χρησιμοποιείται για offline επιθέσεις σε κωδικούς πρόσβασης.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux λειτουργικών συστημάτων.

MDCrack

Το συγκεκριμένο εργαλείο χρησιμοποιείται για offline επιθέσεις σε κωδικούς πρόσβασης. Το MDCrack μπορεί να εκτελέσει επιθέσεις σε αλγόριθμους όπως ενδεικτικά είναι οι MD2, MD4, MD5, HMAC-MD4, HMAC-MD5, FreeBSD, Apache, NTLMv1, IOS και PIX hashes, Invision Power Board 2.x (IPB2), MD4MD4, MD4MD4S, MD5MD5, MD5MD5S, PHP, PHPS, CRC32, CRC32B, ADLER32

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

pwdump

Το συγκεκριμένο εργαλείο (πολλαπλές εκδόσεις) χρησιμοποιείται για την εξόρυξη της SAM database μηχανημάτων windows, ώστε να εκτελεστεί αργότερα με διαφορετικό εργαλείο επίθεση στα password hashes των μηχανημάτων Windows.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Windows λειτουργικών συστημάτων.

0phcrack

Το συγκεκριμένο αποτελεί bootable cd με το οποίο είναι δυνατή η ανάκτηση κωδικών πρόσβασης από μηχανήματα windows, δίχως ο χρήστης να χρειαστεί να κάνει login.

5.5.3. Καταγραφή δικτυακών δεδομένων

SSLStrip

Το συγκεκριμένο εργαλείο σε συνδυασμό με MITM attacks, μπορεί να παρέχει σε χρήστες https σελίδες σε http υποκλέπτοντας κωδικούς πρόσβασης.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux λειτουργικών συστημάτων.

Wireshark

Το Wireshark είναι ένα εργαλείο ανάλυσης των δικτυακών πακέτων που διακινούνται από και προς ένα υπολογιστικό σύστημα.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.6.Αποτίμηση βάσεων δεδομένων

5.6.1. Σύστημα βάσεων δεδομένων MS-SQL

Mssqlfp

Το συγκεκριμένο εργαλείο εκτελεί service fingerprinting ανακαλύπτοντας τις εκδόσεις συστημάτων βάσεων δεδομένων MS SQL Server 2000, 2005 και 2008.

MSSQLScan

Το εργαλείο αυτό ανιχνεύει την ύπαρξη SQL servers χρησιμοποιώντας UDP πακέτα.

Metacoretex-NG

Το εργαλείο αυτό εκτελεί ελέγχους ασφάλειας σε συστήματα βάσεων δεδομένων.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

DBPwAudit

Το DBPwAudit εκτελεί online ελέγχους των κωδικών πρόσβασης σε συστήματα βάσεων δεδομένων. Υποστηρίζει τα συστήματα βάσεων δεδομένων Microsoft SQL Server 2000/2005, Oracle 8/9/10/11, IBM DB2 Universal Database και MySQL.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.6.2. Σύστημα βάσεων δεδομένων Oracle

Oscanner

Το Oscanner αποτελεί εργαλείο αποτίμησης συστημάτων βάσεων δεδομένων Oracle. Ενδεικτικά, εκτελεί:

- Απαρίθμηση Sid

- Δοκιμές στους κωδικούς πρόσβασης
- Ταυτοποίηση την έκδοσης του RDBMS
- Απαρίθμηση των ρόλων των λογαριασμών πρόσβασης
- Απαρίθμηση των προνομίων των λογαριασμών πρόσβασης
- Απαρίθμηση των hashes των λογαριασμών πρόσβασης
- Απαρίθμηση των πληροφοριών ελέγχου
- Απαρίθμηση των πολιτικών κωδικών πρόσβασης

5.7.Ανάλυση εφαρμογών ιστού

5.7.1. Πληρεξούσιες εφαρμογές

Fiddler

Το fiddler είναι μια εφαρμογή αποσφαλμάτωσης εφαρμογών ιστού (http ή https) η οποία λειτουργεί ως ενδιάμεσο σύστημα (web debugging proxy).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Windows λειτουργικών συστημάτων.

Webscarab

Το εργαλείο αυτό είναι ένας web application proxy με τον οποίο επιτυγχάνεται ανάλυση των εφαρμογών που χρησιμοποιούν το πρωτόκολλο HTTP και HTTPs

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

Paros/Andiparos

Τα εργαλεία αυτά αποτελούν web application proxies με τα οποία επιτυγχάνεται ανάλυση των εφαρμογών που χρησιμοποιούν το πρωτόκολλο HTTP και HTTPs. Χρησιμοποιούνται για τους ελέγχους ασφάλειας web εφαρμογών.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Windows λειτουργικών συστημάτων.

5.7.2. Ανιχνευτές

W3AF

Το W3af (Web Application Attack and Audit Framework) είναι ένα εργαλείο το οποίο αυτοματοποιεί τους ελέγχους ασφάλειας σε εφαρμογές ιστού (web applications). Δίνει επίσης τη δυνατότητα εκμετάλευσης των αδυναμιών που ανιχνεύει. Το συγκεκριμένο εργαλείο περιέχει τρείς κατηγορίες plugins τα οποία χρησιμοποιούνται για ανίχνευση, έλεγχο και επιθέσεις.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

Wapiti

Το wapiti επιτρέπει τον έλεγχο ασφάλειας σε εφαρμογές ιστού. Εκτελεί black box ανιχνεύσεις, με σκοπό την ανεύρεση scripts στα οποία μπορούν να εμφυτευτούν δεδομένα. Έχει τη δυνατότητα να εκμεταλλευτεί τις αδυναμίες τις οποίες εντοπίζει ώστε να επικυρώσει τις αδυναμίες που εντοπίζει. Δε χρησιμοποιεί βάση δεδομένων με επιθέσεις, αλλά τις εντοπίζει κατά συνθήκη.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux λειτουργικών συστημάτων.

Nikto

Το nikto αποτελεί έναν ανιχνευτή ασφάλειας εφαρμογών ιστού. Εκτελεί πληθώρα ελέγχων βασισμένο σε προαποθηκευμένο αριθμό δοκιμών.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

5.8.Ανάλυση ασύρματων δικτύων

5.8.1. Αποκάλυψη κωδικών εκτός σύνδεσης

Aircrack-NG

Το Aircrack-NG είναι ένα εργαλείο offline εκτέλεσης επιθέσεων σε κλείδες κωδικών πρόσβασης σε ασύρματα δίκτυα. Εκτελεί επιθέσεις σε κλείδες των πρωτοκόλλων WEP και WPA-PSK.

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux λειτουργικών συστημάτων.

5.8.2. Ανιχνευτές

Kismet

Το kismet είναι ένα εργαλείο παθητικής ανίχνευσης ασύρματων δικτύων (802.11). Μπορεί να ανιχνεύσει κρυφά ασύρματα δίκτυα (no ssid broadcast).

Οι πλατφόρμες λειτουργικών συστημάτων που μπορεί να χρησιμοποιηθεί το εργαλείο είναι αυτές των Linux, Unix και Windows λειτουργικών συστημάτων.

Netstumbler

Το netstumbler είναι ένα εργαλείο το οποίο χρησιμοποιείται για την ανίχνευση ασύρματων δικτύων (802.11) το οποίο μπορεί να χρησιμοποιηθεί για wardriving, περιοχές χαμηλής εκπομπής σήματος, ύπαρξη μη εξουσιοδοτημένων access points

Πλατφόρμες: Windows

ΚΕΦΑΛΑΙΟ 6ο

Συμπεράσματα

Από την παρούσα μελέτη των μεθοδολογιών και των τεχνικών των ελέγχων και δοκιμών διείσδυσης προκύπτει ένας αριθμός συμπερασμάτων γύρω από το γνωστικό πεδίο των ελέγχων διεισδυτικότητας. Συγκεκριμένα:

- ✓ Το εύρος των δοκιμών διεισδυτικότητας πρέπει να είναι επαρκώς τεκμηριωμένο και συμφωνημένο με τον οργανισμό, ειδάλλως ενδέχεται να προκύψουν τεχνικά προβλήματα τα οποία μπορούν να οδηγήσουν σε νομικά κατοχυρωμένες αξιώσεις από τον ελεγχόμενο.
- ✓ Οι υφιστάμενες μεθοδολογίες χρήζουν απλοποίησης καθώς η πολυπλοκότητα τους οδηγεί σε μερική απαξίωση την υιοθέτηση τους από τους ελεγκτές δοκιμών διεισδυτικότητας.
- ✓ Οι επιτυχία των τεχνικών των δοκιμών διεισδυτικότητας σε δίκτυα δεδομένων σχετίζεται άμεσα με τη γνώση των λεπτομερών χαρακτηριστικών της λειτουργίας των πρωτοκόλλων επικοινωνιών.
- ✓ Η επίτευξη του μέγιστου βαθμού διεισδυτικότητας βασίζεται σε μεγάλο βαθμό στις εγγενείς αδυναμίες τόσο της αρχιτεκτονικής ενός συστήματος, στις αδυναμίες παραμετροποίησης αυτού, αλλά και στο επίπεδο συντήρησης του.
- ✓ Η χρήση της κοινωνικής μηχανικής σε συνδυασμό με τις υφιστάμενες τεχνικές αυξάνει σε μεγάλο βαθμό την πιθανότητα διείσδυσης σε ένα υπολογιστικό σύστημα.
- ✓ Η υιοθέτηση τεχνικών οι οποίες στοχοποιούν τους τελικούς χρήστες ενός οργανισμού αυξάνει την πιθανότητα διείσδυσης σε ένα υπολογιστικό σύστημα.
- ✓ Δεν υφίσταται οδηγός ελέγχων διεισδυτικότητας σε δίκτυα δεδομένων ο οποίος να συνδέει επαρκώς τις τεχνικές με τις μεθοδολογίες καθώς και τα εργαλεία που απαιτούνται για την εκτέλεση των δοκιμών.

Από τα παραπάνω συμπεράσματα προκύπτει ότι, οι έλεγχοι διεισδυτικότητας αποτελούν ένα ευρύ πεδίο συνεχούς μελέτης το οποίο βασίζεται σε μεγάλο βαθμό στην εκπαίδευση των ελεγκτών, στην επίγνωση της ασφάλειας των χρηστών και στην ύπαρξη ενός ολοκληρωμένου εγχειριδίου, ώστε να επιτευχτεί ο μέγιστος βαθμός επιχειρησιακής ασφάλειας ενός οργανισμού.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1.**Alisherov, Farkhod and Sattarova, Feruza.** *Methodology for Penetration Testing*. International Journal of of Grid and Distributed Computing, 2009.

2. **Klein, Amit.** *Cross Site Scripting Explained.* Sanctum Security Group, 2002.

3. **Supervision, Basel Committee on Banking.** *International Convergence of Capital Measurement and Capital Standards* . Bank for International Settlements, 2006.

4. **Downs, Deborah and Haddad, Ranwa.** *Penetration Testing – The Gold Standard for Security Rating and Ranking.* 2001.

5. **(BSI), Federal Office for Information Security.** *A Penetration Testin Model.* Bonn.

6. **OISSG.** *Information Systems Security Assessement Framework Draft 0.2.1.* 2006.

7. **Foundation, OWASP.** *Testing Guide.* OWASP Foundation, 2007.

8. **Council, Payment Card Industry Security Standards.** *Data Security Standard (DSS) - Penetration Testing.* 2008.

9. **Herzog, Pete.** *Open-Source Security Testing Methodology Manual.* ISECOM, 2006.

10. **Saindane, Manish.** *Penetration testing – A Systematic Approach.*

11. **Scarfone, Karen, και συν.** *Technical Guide to Information Security Testing and Assessment.* National Institute of Standards and Technology, 2008.

12. **Harris, Shon.** *CISSP, All in one exam guide.* McGrawHill, 2009.

13. **Gordon, Lyon.** *Nmap Network Scanning.* Insecure.Com LLC. 2009.

14. **Consortium, Web Application Security.** *Threat Classification.* Web Application Security Consortium.

15. **Spangler, Ryan.** *Analysis of Remote Active Operating System Fingerprinting Tools.* 2003

16. **Tipton, Harold and Krause Micki.** *Information security management handbook.* 2008

17**. McNab, Chris.** *Network security assessment*. 2004

18. **Symanterc corp.** Global Internet Security Threat Report Trends for 2008. 2008.

19. **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.** *Κανονισμός για τη διασφάλιση του απορρήτου των διαδικτυακών υποδομών.* Αθήνα, 2005.

20. **Κάτσικας, Σωκράτης, Γκρίτζαλης, Δημήτρης και Γκρίτζαλης, Στέφανος.** *Ασφάλεια Πληροφοριακών Συστημάτων.* 2004.

21. **Τράπεζα της Ελλάδος.** *ΠΔ/ΤΕ 2577.* Αθήνα, 2006.

22. http://nmap.org

23. http://www.ouah.org

24. http://old.honeynet.org/