Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Συγκριτική Αξιολόγηση Λογισμικού Ανίχνευσης Τρωσιμότητας

Χριστόδουλος Παρπούλης

Επιβλέπων Καθηγητής
Πέτρος Νικοπολιτίδης

Ιούνιος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Συγκριτική Αξιολόγηση Λογισμικού Ανίχνευσης Τρωσιμότητας

Χριστόδουλος Παρπούλης

Επιβλέπων Καθηγητής
Πέτρος Νικοπολιτίδης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Ιούνιος 2017

Περίληψη

Σκοπός της παρούσας μεταπτυχιακής διατριβής ήταν η εγκατάσταση και εκμάθηση αριθμού εργαλείων λογισμικού ανίχνευσης ευπαθειών, καθώς και η χρήση τους για την διερεύνηση ενός ηθελημένα ευπαθούς περιβάλλοντος και την εξαγωγή καταστάσεων των ανευρεθέντων ευπαθειών.

Με βάση τις συστάσεις των εργαλείων, αλλά και με βιβλιογραφική ανασκόπηση, έχουν γίνει οι σχετικές τροποποιήσεις, σε ένα αριθμό ευπαθειών, στο υπό εξέταση περιβάλλον (Metasploitable 2) και στην συνέχεια έχει αντεξεταστεί από τα εργαλεία ανίχνευσης ευπαθειών, ώστε να επιβεβαιωθεί η αύξηση του επιπέδου της ασφάλειας του.

Τα αποτελέσματα της διατριβής περιλαμβάνουν την διαδικασία εγκατάστασης, τροποποίησης και διεξαγωγής ανίχνευσης τρωσιμότητας, για κάθε εργαλείο που έχει χρησιμοποιηθεί ξεχωριστά, καθώς και τις ενέργειες που ακολουθούνται για την απαλοιφή αριθμού ανευρεθέντων ευπαθειών. Επίσης περιλαμβάνεται μια αξιολόγηση των εργαλείων ανίχνευσης τρωσιμότητας που έχουν χρησιμοποιηθεί, με έμφαση στην αποδοτικότητα και ευκολία χρήσης των εργαλείων κατά την διαδικασία εγκατάστασης, παραμετροποίησης, διεξαγωγής εκτίμησης τρωσιμότητας και εξαγωγής αποτελεσμάτων.

Summary

The purpose of the current M.Sc. dissertation is the installation and the study of a number of vulnerability assessment tools and also the usage of those tools for performing an investigation audit of a purposely vulnerable system.

The outcome of the investigation was a number of vulnerability assessment reports which have been used, in addition to a further documentation research, as a guide, for the assessment of a number of vulnerabilities of the assessed system (Metasploitable 2). After the vulnerability assessment, a second investigation audit has been performed in order to identify whether the vulnerable system has become more secure or those vulnerabilities still exist.

The results of the dissertation include the process of installing, modifying and conducting a vulnerability assessment, for each vulnerability assessment tool used along with the actions taken to eradicate a number of detected vulnerabilities. Also included is an evaluation of the vulnerability assessment tools based on the data of the dissertation. The evaluation will emphasize on the efficiency and ease of use during the process of setting up, parameterizing, contacting vulnerability assessment tests and the export of assessment results.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον υπεύθυνο και επιβλέποντα καθηγητή μου, κύριο Πέτρο Νικοπολιτίδη, για την συνεχή καθοδήγηση και υπομονή που επέδειξε μέχρι να ολοκληρωθεί η παρούσα μεταπτυχιακή διατριβή.

Επίσης με την ευκαιρία αυτή, θα ήθελα να εκφράσω τις ευχαριστίες μου στο Ανοιχτό Πανεπιστήμιο Κύπρου για την ευκαιρία που μου έδωσε να συμμετάσχω στο συγκεκριμένο μεταπτυχιακό πρόγραμμα, καθώς και σε όλους του καθηγητές μου για τις πολύτιμες γνώσεις που μου μετάδωσαν, καθ' όλη την διάρκεια του ταξιδιού αυτού.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου και ιδιαιτέρα την σύζυγο μου Στέλλα και την κόρη μου Μαρίνα, για τη στήριξη που μου προσέφεραν και κυρίως για την κατανόηση που επέδειξαν κατά την διάρκεια των σπουδών μου.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Λαμβάνοντας υπόψη το χρόνο, τους πόρους και το κίνητρο, ένας κράκερ μπορεί να διεισδύσει σε σχεδόν οποιοδήποτε σύστημα. Στο τέλος της ημέρας, όλες οι διαδικασίες και τεχνολογίες ασφαλείας που διατίθενται σήμερα δεν μπορούν να εγγυηθούν ότι τα υπό προστασία συστήματα είναι ασφαλή από εισβολείς. Οι δρομολογητές (Routers) βοηθούν στην διασφάλιση ασφαλής πρόσβασης στο διαδίκτυο. Το τοίχος προστασίας (Firewall), βοηθά στην εξασφάλιση της ασφάλειας στην άκρη του δικτύου. Τα εικονικά ιδιωτικά δίκτυα (VPN,Virtual Private Networks) περνούν με ασφάλεια δεδομένα σε κρυπτογραφημένη μορφή, χρησιμοποιώντας, κατά κύριο λόγο, την τηλεπικοινωνιακή υποδομή του Διαδικτύου. Τα συστήματα ανίχνευσης εισβολής (IDS,Intrusion Detection Systems) προειδοποιούν για κακόβουλη δραστηριότητα. Ωστόσο, η επιτυχία καθεμιάς από αυτές τις τεχνολογίες εξαρτάται από έναν αριθμό μεταβλητών, που περιλαμβάνουν:

1. Τη τεχνογνωσία του προσωπικού που είναι υπεύθυνο για τη διαμόρφωση, την παρακολούθηση και τη διατήρηση των τεχνολογιών.

2. Την ικανότητα να επιδιορθώσει και να ενημερώσει τις υπηρεσίες γρήγορα και αποτελεσματικά.

3. Την ικανότητα των υπευθύνων να παραμένουν σε συνεχή επαγρύπνηση διατηρώντας την ασφάλεια του δικτύου.

Με δεδομένη τη δυναμική κατάσταση των συστημάτων και τεχνολογιών, η εξασφάλιση της ασφάλειας των εταιρικών πόρων είναι αρκετά περίπλοκη. Λόγω αυτής της πολυπλοκότητας, είναι συχνά δύσκολο να βρεθεί εξειδικευμένο προσωπικό για το σύνολο των συστημάτων ενός οργανισμού. Ενώ είναι δυνατόν να υπάρχει προσωπικό καταρτισμένο σε πολλούς τομείς της ασφάλειας των πληροφοριών σε συγκεκριμένες περιοχές, είναι δύσκολο για ένα οργανισμό να διατηρήσει το προσωπικό που είναι ειδικό σε περισσότερο από μερικές θεματικές περιοχές. Αυτό είναι κυρίως επειδή κάθε θεματική περιοχή της ασφάλειας των πληροφοριών απαιτεί συνεχή προσοχή και εστίαση. Η ασφάλεια των πληροφοριών βρίσκετε συνεχώς σε μια ρευστή κατάσταση.

Τα εργαλεία ανίχνευσης επισφαλών σημείων (Vulnerability Assessment Tools) των συστημάτων ενός οργανισμού, έρχονται να καλύψουν σε μεγάλο ποσοστό αυτή την ανάγκη παρουσίας και χρήσης των διάφορων εμπειρογνωμόνων ασφαλείας. Τα συστήματα αυτά έχουν την δυνατότητα να εκτιμήσουν την τρωσιμότητα του δικτύου και των διαφόρων συστημάτων του οργανισμού και μέσω των αποτελεσμάτων τους, να διαφανεί κατά πόσο η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των υπό έλεγχο πόρων βρίσκεται εκτεθειμένη.

1.1 Δομή Μεταπτυχιακής Διατριβής

Η δομή της εν λόγω μεταπτυχιακής διατριβής είναι ως ακολούθως:

Στο **Κεφάλαιο 2** γίνεται αναφορά στην έννοια της Ασφάλειας, στις Πηγές Ευπαθειών αλλά και στις Στρατηγικές που ακολουθούνται για διασφάλιση της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των Πληροφοριακών Συστημάτων.

Στο **Κεφάλαιο 3** γίνεται αναφορά στο τι εστί Ηλεκτρονικό Έγκλημα και οι τύποι αυτού. Επίσης γίνεται εκτενή αναφορά στις διάφορες κατηγορίες Κυβερνοεγκληματιών και στις μεθοδολογίες και τεχνικές που χρησιμοποιούν.

Στο **Κεφάλαιο 4** καταγράφονται οι λόγοι ύπαρξης των Ευπαθειών και η σημαντικότητα διεξαγωγής Εκτίμησης Τρωσιμότητας, καθώς και τα είδη εκτιμήσεων αυτής.

Στο **Κεφάλαιο 5** γίνεται παρουσίαση του περιβάλλοντος αξιολόγησης καθώς και του τρόπου λειτουργίας των εργαλείων εκτίμησης τρωσιμότητας που έχουν χρησιμοποιηθεί για την ανεύρεση των ευπαθειών.

Στο **Κεφάλαιο 6** καταγράφονται οι ευπάθειες του υπό εξέταση συστήματος, επιλέγεται αριθμός ευπαθειών για εξέταση και γίνεται καταγραφή των αποτελεσμάτων των εργαλείων εκτίμησης τρωσιμότητας. Επιπρόσθετα γίνεται προσπάθεια απαλοιφής των υπό εξέταση ευπαθειών και ακολούθως διενεργείται επανάληψη εκτίμησης τρωσιμότητας για επιβεβαίωση ή μη ευόδωσης των προσπαθειών αυτών. Στην συνέχεια γίνεται αξιολόγηση των εργαλείων εκτίμησης τρωσιμότητας και παρατίθεται μια λίστα χαρακτηριστικών που θα πρέπει να διαθέτει το ιδανικό σύστημα εκτίμησης τρωσιμότητας.

Στο **Κεφάλαιο 7,** καταγράφονται τα συμπεράσματα της παρούσας μεταπτυχιακής διατριβής σχετικά με την χρήση των εργαλείων εκτίμησης τρωσιμότητας και την αναγκαιότητα τους στην απαλοιφή των ευπαθειών στα πληροφορικά συστήματα, καθώς επίσης παραδοχές για την πρόληψη εμφάνισης ευπαθειών

Κεφάλαιο 2
Ασφάλεια Πληροφορικών Συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα γνωστικό πεδίο της επιστήμης της πληροφορικής και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Συγγενικά γνωστικά πεδία είναι η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία. [27]

Σύμφωνα με το εγχειρίδιο ασφαλείας υπολογιστών NIST (NIST95) [03], ως όρος ασφάλειας πληροφοριακών συστημάτων ορίζεται: "Η προστασία που παρέχεται σε ένα αυτοματοποιημένο πληροφοριακό σύστημα, προκειμένου να επιτευχθούν οι ισχύοντες στόχοι, για την διατήρηση της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των πόρων του συστήματος πληροφοριών (περιλαμβανομένου του υλικού υπολογιστών, λογισμικού, μόνιμου προγράμματος λογισμικού της ROM, πληροφοριών/δεδομένων και των τηλεπικοινωνιών)".

Ένας αριθμός απαιτήσεων ελέγχου και προστασίας θεωρείται θεμελιώδης για την ασφάλεια πληροφοριών σε κάθε οργανισμό. Οι απαιτήσεις αυτές, είτε βασίζονται σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική σε θέματα ασφάλειας. Απαιτήσεις απαραίτητες σε έναν οργανισμό, που βασίζονται στη νομοθεσία, είναι η διαφύλαξη των προσωπικών δεδομένων, η διαφύλαξη των δεδομένων του οργανισμού και τα δικαιώματα πνευματικής ιδιοκτησίας. Απαιτήσεις που έχουν καθιερωθεί ως κοινή πρακτική είναι η εκπόνηση πολιτικής ασφάλειας, ο καταμερισμός καθηκόντων σχετικών με την ασφάλεια, η εκπαίδευση σε θέματα ασφάλειας, η αναφορά συμβάντων και η διαχείριση της επιχειρησιακής συνέχειας. [01]

2.1 Πηγές Ευπαθειών

Εύλογα κάποιος μπορεί να αναρωτηθεί, ποίος είναι ο λόγος για τον οποίο οι υπολογιστές εξακολουθούν ακόμη και σήμερα να μην είναι ασφαλείς; Τα περαστικά εκμετάλλευσης ευπαθειών από εισβολείς δεν είναι πρόσφατα, υπάρχουν εδώ και πολύ καιρό γιατί δεν έχουν ακόμη αντιμετωπιστεί;

2.1.1 Το Πρόβλημα της Ασφάλειας των Πληροφοριακών Συστημάτων

Το πρόβλημα της ασφάλειας πληροφοριακών συστημάτων, αποτελεί γενικό όρο των προβλημάτων τα οποία ανακύπτουν όταν προσπαθούμε να επιτύχουμε ένα σύνολο λειτουργικών στόχων. Το σύνολο των στόχων αυτών αποτελείται από έξι μέρη, τα οποία είναι [04]:

1. Τα πληροφοριακά συστήματα πρέπει να κάνουν ακριβώς αυτό για το οποίο σχεδιάστηκαν.

2. Τα πληροφοριακά συστήματα πρέπει να λειτουργούν στο χρόνο που επιβάλλει ο σχεδιασμός τους.

3. Τα πληροφοριακά συστήματα πρέπει να χρησιμοποιούνται από εξουσιοδοτημένο προσωπικό.

4. Τα πληροφοριακά συστήματα δεν πρέπει ποτέ να κάνουν κάτι για το οποίο δεν έχουν σχεδιαστεί.

5. Τα πληροφοριακά συστήματα δεν πρέπει ποτέ να λειτουργούν εκτός του χρόνου για τον οποίο σχεδιάστηκαν να λειτουργούν.

6. Τα πληροφοριακά συστήματα δεν πρέπει ποτέ να χρησιμοποιούνται από μη εξουσιοδοτημένο προσωπικό.

Επομένως ο στόχος προστασίας των πληροφοριακών συστημάτων δεν εδράζεται απλά στην προστασία του δικτύου, με την χρήση συμβατικών λύσεων, τύπου τοίχου προστασίας. Ούτε είναι αρκετό να ακολουθήσει κανείς οδηγίες ή να πιστοποιηθεί. Η πραγματική αιτία του προβλήματος πηγάζει από την κακή σχεδίαση λογισμικού, την ατελή υλοποίηση και κυρίως τη μαζική ανάπτυξη κρίσιμων εφαρμογών σε εγγενώς ανασφαλείς πλατφόρμες.

Το πρόβλημα της ασφάλειας πληροφοριακών συστημάτων δεν σχετίζεται με εργαλεία λογισμικού ή σχεδιασμό δικτύων αλλά εδράζεται στα ερωτήματα:

- Πως σχεδιάζουμε λογισμικό;

- Ποιοι σχεδιάζουν λογισμικό;

- Πως επιλέγουμε λογισμικό;

- Πως εγκαθιστούμε λογισμικό;

Η συντριπτική πλειοψηφία των περιστατικών εκμετάλλευσης ευπαθειών από εισβολείς, συμβαίνουν εξαιτίας ενός από τα ακόλουθα βασικά προβλήματα:

- Η επίτευξη ασφάλειας είναι μια ενόχληση: Οι διαχειριστές συχνά αποτυγχάνουν να εφαρμόσουν λειτουργίες ασφάλειας στα λειτουργικά συστήματα, επειδή κάποιες φορές δημιουργούν προβλήματα στους χρήστες . Οι χρήστες από την άλλη, παρακάμπτουν την ασφάλεια, επιλέγοντας εύκολους στη χρήση τους και στην απομνημόνευση, κωδικούς πρόσβασης, όπως το "123456", που ποτέ δεν τους αλλάζουν, πιθανότατα γνωστοποιώντας αυτούς τους κωδικούς στους συναδέλφους τους ή ακόμη χρησιμοποιώντας κοινούς λογαριασμούς πρόσβασης.

- Οι κατασκευαστές λογισμικού διανέμουν τα προϊόντα τους έχοντας προεπιλέξει τα χαρακτηριστικά που θα εγκατασταθούν, απενεργοποιώντας στις πλείστες των

περιπτώσεων, τα χαρακτηριστικά ασφάλειας. Ο λόγος που γίνεται αυτό είναι για να αποφεύγονται τα προβλήματα στους τελικούς χρήστες, οι οποίοι δεν διαθέτουν τις ικανότητες και τις γνώσεις, για να κατανοήσουν και να ρυθμίσουν σωστά τα χαρακτηριστικά ασφάλειας.

Το γεγονός ότι η ισχυρή ασφάλεια δεν είναι φιλική στο χρήστη και το ότι απαιτεί εξειδικευμένες γνώσεις για να ρυθμιστεί και να λειτουργήσει σωστά, αποτελεί το πιο συνηθισμένο λόγο για τον οποίο η ασφάλεια αποτυγχάνει.

- Προώθηση ανασφαλών χαρακτηριστικών λογισμικού στην αγορά. Οι κατασκευαστές λογισμικού επικεντρώνουν τις προσπάθειές τους στην προσθήκη χαρακτηριστικών τα οποία θα καθιστούν τα προϊόντα τους περισσότερο εύχρηστα, δίνοντας λίγη σημασία στην ασφάλειά. Ως παράδειγμα μπορούμε να δούμε την προσθήκη της scripting γλώσσας στο Microsoft Outlook και στο Outlook Express.

  Λόγο του μεγάλου ανταγωνισμού, για το ποια εταιρεία θα διαθέσει πρώτη τα προϊόντα της και σε χαμηλότερο κόστος, για να αποκτήσει μεγαλύτερο μερίδιο αγοράς, οι κατασκευαστές λογισμικού που επενδύουν στην ασφάλεια επισκιάζονται από αυτούς που δεν το πράττουν. Το τελικό αποτέλεσμα είναι: Τα λιγότερο ασφαλή προϊόντα προωθούνται στην αγορά πρώτα και γίνονται πρότυπα!

- Οι υπολογιστές και το λογισμικό εξελίσσονται πολύ γρήγορα. Οι υπολογιστές και η τεχνολογία δικτύων εξελίσσονται πολύ πιο γρήγορα από ότι οι εταιρείες μπορούν να προβλέψουν τα πιθανά προβλήματα που αυτά μπορούν να δημιουργήσουν. Όπως αναφέρει και ο νόμος του Moore, ο οποίος παραμένει ακριβής από το 1965, το υλικό υπολογιστών θα διπλασιάζει την δύναμη/ταχύτητά του κάθε δύο χρόνια.

- Οι προγραμματιστές δεν μπορούν να προβλέψουν με ακρίβεια τις ατέλειες. Οι προγραμματιστές σπάνια θεωρούν ότι η κατάσταση των συναρτήσεών τους μπορεί να αλλάξει εξωτερικά από κάποια τιμή, ενώ εκτελείται ο κώδικας οπότε ελέγχουν μόνο για τιμές που στέλνουν οι ίδιοι στις συναρτήσεις. Όταν ο κώδικας περάσει τους τυπικούς ελέγχους εντοπισμού σφαλμάτων, διανέμεται χωρίς να ελεγχθεί προηγουμένως με διάφορα τυχαία δεδομένα. Ακόμη και αν οι προγραμματιστές συγκεκριμένου λογισμικού προσπαθήσουν να προβλέψουν τις πιθανές ευπάθειες του, δεν θα μπορούσαν να

δοκιμάσουν όλα τα είδη και τύπους των επιθέσεων, που θα επιχειρήσουν να δοκιμάσουν οι εκατομμύρια των εισβολέων.

- Υπάρχει μικρή διαφορετικότητα στην αγορά λογισμικού. Το δυοπώλιο των λειτουργικών συστημάτων Windows και Unix, που αποτελεί περισσότερο του 90% των λειτουργικών συστημάτων που χρησιμοποιούνται από τους ηλεκτρονικούς υπολογιστές, έχουν μειώσει τους στόχους των εισβολέων στις μικρές παραλλαγές αυτών των συστημάτων. Στις περισσότερες εφαρμογές, μόνο ένα ή δύο προϊόντα αποτελούν την μερίδα του λέοντος της αγοράς, έτσι οι εισβολείς έχουν να "σπάσουν" μόνο ένα προϊόν, στο οποίο θα αποκτήσει ευρεία πρόσβαση ένας μεγάλος αριθμός ανθρώπων.

- Οι κατασκευαστές λογισμικού δεν έχουν κίνητρο στο να αποκαλύψουν τις ευπάθειες των προϊόντων τους. Για την αποφυγή επιχειρηματικού φιάσκου οι κατασκευαστές λογισμικού προσπαθούν να αποκρύψουν από δημόσια προβολή, προβλήματα σχετικά με το λογισμικό τους, με αποτέλεσμα να αποθαρρύνουν τυχών συζήτηση αναφορικά με τα ελαττώματά τους. Στην αντίπερα όχθη, οι εισβολείς δημοσιοποιούν αμέσως τις ατέλειες που ανακαλύπτουν, μέσο του Διαδικτύου, σε όλο τον κόσμο. Αυτή η διαφορά των δύο πλευρών, σημαίνει ότι οι ευπάθειες του λογισμικού διαδίδονται ευρέως, σε αντίθεση από τις λύσεις τους.

- Οι διορθώσεις των ευπαθειών δεν κοινοποιούνται ευρέως και μπορούν να προκαλέσουν προβλήματα όταν εγκαθίστανται. Όταν ανακαλύπτονται προβλήματα ασφάλειας σε κάποιο λογισμικό, ο κατασκευαστής διορθώνει το πρόβλημα, δημοσιεύει τη διόρθωση στο Διαδίκτυο και αποστέλλει μια ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείου στους εγγεγραμμένους πελάτες του. Δυστυχώς, δεν παίρνουν όλοι οι πελάτες την ειδοποίηση ή εγκαθιστούν τη διόρθωση – στην πραγματικότητα, οι περισσότεροι χρήστες δεν εγκαθιστούν ποτέ διορθώσεις ασφάλειας για το λογισμικό, μέχρι να δεχτούν κάποια επίθεση. Ακόμη χειρότερα, σε κάποιες περιπτώσεις, οι κατασκευαστές στέλνουν εσπευσμένα διορθώσεις στους πελάτες τους για ευπάθειες οι οποίες δεν έχουν γίνει ακόμη αντιληπτές, με αποτέλεσμα η εγκατάστασή τους να δημιουργεί περισσότερα προβλήματα στις μηχανές των πελατών τους. Στη καλύτερη περίπτωση απαιτείται πρόσθετη επεξεργασία για να εντοπιστεί η αδυναμία, με αποτέλεσμα να επιβραδύνετε έτσι στο σύστημα. Σε ορισμένες περιπτώσεις, η θεραπεία είναι χειρότερη από την ασθένεια. [22]

2.1.2 Η Στρατηγική Ασφάλειας των Πληροφοριακών Συστημάτων

Σύμφωνα με τον ορισμό του NIST95 [03], εισάγονται τρείς βασικοί στόχοι, οι οποίοι βρίσκονται στο επίκεντρο της ασφάλειας των πληροφορικών συστημάτων. Ο στόχος της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας.

- **Εμπιστευτικότητα (Confidentiality)**. Ο όρος αυτός καλύπτει δύο συναφείς έννοιες:

    - **Εμπιστευτικότητα των Δεδομένων (Data confidentiality):** Διαβεβαιώνει ότι οι ιδιωτικές ή εμπιστευτικές πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

    - **Προστασία των Προσωπικών Δεδομένων (Privacy):** Εξασφαλίζει ότι τα άτομα ελέγχουν ή επηρεάζουν ποιες πληροφορίες που σχετίζονται με αυτά, μπορεί να συλλεχθούν και να αποθηκευτούν και από ποιον και σε ποιον μπορούν να αποκαλυφθούν.

- **Ακεραιότητα (Integrity)**. Ο όρος αυτός καλύπτει δύο συναφείς έννοιες:

    - **Ακεραιότητα των Δεδομένων (Data Integrity):** Εξασφαλίζει ότι οι πληροφορίες και τα προγράμματα μπορούν να τροποποιηθούν μόνο με συγκεκριμένο και εξουσιοδοτημένο τρόπο.

    - **Ακεραιότητα του Συστήματος (System Integrity):** Εξασφαλίζει ότι ένα σύστημα εκτελεί μια προβλεπόμενη λειτουργία, άριστα, χωρίς σκόπιμο ή ακούσιο μη εξουσιοδοτημένο χειρισμό.

- **Διαθεσιμότητα (Availability).** Εξασφαλίζει ότι τα συστήματα λειτουργούν απρόσκοπτα και ότι η υπηρεσία πρόσβασης δεν αρνείται την πρόσβαση στους εξουσιοδοτημένους χρήστες.

Η επίτευξη των στόχων αυτών προϋποθέτει την υιοθέτηση μιας ολοκληρωμένης στρατηγικής για την ασφάλεια των πληροφοριακών συστημάτων. Μια ολοκληρωμένη στρατηγική ασφάλειας περιλαμβάνει τρείς πτυχές [03]:

- Προδιαγραφή/ Πολιτική (Specification/policy): Τι αναμένεται από το σύστημα ασφαλείας να κάνει;

- Υλοποίηση/Μηχανισμοί (Implementation/mechanisms): Πως θα εφαρμοστεί;

- Αξιολόγηση/Διαβεβαίωση (Correctness/assurance): Λειτουργεί πραγματικά;

Προδιαγραφή/ Πολιτική

Το πρώτο βήμα στην εφαρμογή των υπηρεσιών και των μηχανισμών ασφαλείας είναι να αναπτυχθεί μια πολιτική ασφαλείας. Όσοι ενασχολούνται με την ασφάλεια πληροφοριακών συστημάτων χρησιμοποιούν τον όρο "πολιτική ασφαλείας" με διάφορους τρόπους. Στο ελάχιστο, μια πολιτική ασφαλείας, είναι μια άτυπη περιγραφή επιθυμητής συμπεριφοράς του συστήματος. Τέτοιου τύπου άτυπες πολιτικές μπορούν να παραπέμπουν στις απαιτήσεις για εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Πιο ωφέλιμα, μια πολιτική ασφαλείας, είναι ένα επίσημο έγγραφο από κανόνες και πρακτικές, που διευκρινίζουν ή ρυθμίζουν πώς ένα σύστημα ή ένας οργανισμός, παρέχει υπηρεσίες ασφαλείας για να προστατεύσει τους ευαίσθητους και κρίσιμους πόρους συστημάτων. Μια τέτοια επίσημη πολιτική ασφαλείας μπορεί να εφαρμοστεί τόσο από τεχνικής πλευράς στα συστήματα του οργανισμού, όσο και από διοικητικής πλευράς.

Κατά την ανάπτυξη της πολιτικής ασφαλείας, ο διευθυντής ασφάλειας πρέπει να λάβει υπόψη του, τους εξής παράγοντες:

- Την αξία των περιουσιακών στοιχείων τα οποία χρήζουν προστασίας.

- Τις ευπάθειες του συστήματος.

- Τις πιθανές απειλές και την πιθανότητα επίθεσης.

Επιπρόσθετα ο διευθυντής θα πρέπει να εξισορροπήσει μεταξύ των πιο κάτω παραγόντων:

- **Ευκολία χρήσης Vs Ασφάλεια**: Στην πλειοψηφία τους τα μέτρα ασφάλειας επηρεάζουν αρνητικά την ευκολία χρήσης. Λόγου χάρη, ο μηχανισμός ελέγχου προσπέλασης (User Authentication Mechanism), όπου απαιτεί από τους χρήστες να θυμούνται τους κωδικούς πρόσβασης και πιθανός να απαιτούν την εκτέλεση επιπρόσθετων μέτρων

πρόσβασης. Οι τοίχοι προστασίας, καθώς και άλλα μέτρα ασφαλείας δικτύων μπορούν να μειώσουν τη διαθέσιμη ικανότητα μετάδοσης δεδομένων ή να εμφανίσουν πρόβλημα αυξημένου χρόνου ανταπόκρισης. Ακόμη τα αντιικά προγράμματα (Antivirus Software) μειώνουν την υπολογιστική ισχύ του συστήματος και δημιουργούνται οι συνθήκες κατάρρευσης ή δυσλειτουργίας του, λόγω της μη αναμενόμενης αλληλεπίδρασης μεταξύ του λογισμικού ασφαλείας και του λειτουργικού συστήματος

- **Κόστος Ασφάλειας Vs Κόστος αποτυχίας και αποκατάστασης:** Εκτός από την ευκολία χρήσης και το κόστος απόδοσης, υπάρχουν άμεσες χρηματικές δαπάνες όσο αφορά την εφαρμογή και διατήρηση των μέτρων ασφαλείας. Οι δαπάνες αυτές πρέπει να ισορροπηθούν με το πιθανό κόστος αποτυχίας της ασφάλειας και της επιχειρησιακής αποκατάστασης, εάν κάποια συγκεκριμένα μέτρα ασφαλείας δεν εφαρμόζονται. Το κόστος της αποτυχίας και αποκατάστασης πρέπει να λάβει υπόψη όχι μόνο το κόστος των περιουσιακών στοιχείων που χρήζουν προστασίας και των ζημιών που μπορεί να προκύψουν από την παραβίαση της ασφάλειας, αλλά και το ρίσκο, που ορίζεται ως η πιθανότητα όπου μια συγκεκριμένη απειλή, να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια, με ένα συγκεκριμένο επιβλαβές αποτέλεσμα.

Η εφαρμογή πολιτικής ασφάλειας είναι απερίφραστα μια επιχειρηματική απόφαση που επηρεάζεται ενδεχομένως και από νομικές απαιτήσεις.

Υλοποίηση/ Μηχανισμοί

Η εφαρμογή της ασφάλειας περιλαμβάνει τέσσερα συμπληρωματικά σχέδια δράσης:

- **Πρόληψη (Prevention):** Ένα ιδανικό σύστημα ασφάλειας είναι ένα στο οποίο καμία επίθεση δεν είναι επιτυχής. Αν και αυτό δεν είναι πρακτικό σε όλες τις περιπτώσεις, υπάρχει ένα ευρύ φάσμα απειλών στο οποίο η πρόληψη είναι ένας λογικός στόχος. Για παράδειγμα, ας αναλογιστούμε την διαβίβαση κρυπτογραφημένων δεδομένων. Εάν χρησιμοποιείται ένας ασφαλής αλγόριθμος κρυπτογράφησης και αν υπάρχουν ισχύοντα μέτρα για αποφυγή αναρμόδιας πρόσβασης στα κλειδιά κρυπτογράφησης, τότε οι επιθέσεις οι οποίες έχουν στόχο την εμπιστευτικότητα των δεδομένων, μπορούν να αποτραπούν.

- **Ανίχνευση (Detection):** Σε ένα αριθμό περιπτώσεων, η απόλυτη προστασία, δεν είναι εφικτή, αλλά κρίνετε πρακτικό και αναγκαίο να ανιχνευθούν οι τυχόν επιθέσεις ασφαλείας. Για παράδειγμα υπάρχουν συστήματα ανίχνευσης παρείσφρησης (IDS) τα οποία είναι σχεδιασμένα να ανιχνεύουν τη παρουσία αναρμόδιων ατόμων τα οποία έχουν καταφέρει να συνδεθούν με το υπό επίβλεψη πληροφοριακό σύστημα. Ένα άλλο παράδειγμα είναι η ανίχνευση επίθεσης που στόχο έχει την άρνηση των υπηρεσιών (DoS attack), κατά την οποία οι πόροι των επικοινωνιών ή της επεξεργασίας καταναλώνονται έτσι ώστε να μην είναι διαθέσιμοι στους νόμιμους χρήστες.

- **Απάντηση (Response):** Στην περίπτωση που οι μηχανισμοί ασφαλείας ανιχνεύσουν μια τρέχουσα επίθεση, όπως λόγου χάρη μια επίθεση άρνησης υπηρεσιών, το σύστημα μπορεί να είναι σε θέση να αποκριθεί με τέτοιο τρόπο ώστε να σταματήσει την επίθεση και να αποτραπεί περαιτέρω ζημιά.

- **Αποκατάσταση (Recovery):** Ένα παράδειγμα αποκατάστασης είναι η χρήση εφεδρικών συστημάτων, έτσι εάν η ακεραιότητα των δεδομένων εκτεθεί, ένα προηγούμενο, αντίγραφο των δεδομένων, μπορεί να ξαναφορτωθεί.

Αξιολόγηση/ Διαβεβαίωση

Οι καταναλωτές των υπηρεσιών και μηχανισμών ασφαλείας (διευθυντές συστημάτων, προμηθευτές, πελάτες και τελικοί χρήστες) τρέφουν την πεποίθηση ότι τα μέτρα ασφαλείας τα οποία είναι σε ισχύ, λειτουργούν όπως αναμένεται να λειτουργούν. Οι καταναλωτές συστημάτων ασφαλείας θέλουν να είναι βέβαιοι ότι η υποδομή ασφαλείας των συστημάτων τους, καλύπτει τις απαιτήσεις ασφάλειας και επιβάλλει τις πολιτικές ασφάλειας που έχουν υιοθετήσει.

Οι εκτιμήσεις αυτές μας φέρνουν στις έννοιες της διαβεβαίωσης και της αξιολόγησης. Στο εγχειρίδιο ασφαλείας υπολογιστών του NIST (NIST95) [03], καθορίζεται ως διαβεβαίωση, ο βαθμός εμπιστοσύνης που κάποιος έχει, ότι τα μέτρα ασφαλείας, τεχνικά και λειτουργικά, εργάζονται όπως προβλέπεται, για την προστασία του συστήματος και των πληροφοριών που επεξεργάζεται. Αυτό περιλαμβάνει το σχέδιο των συστημάτων καθώς και την εφαρμογή τους. Κατά συνέπεια, η διαβεβαίωση, διαχειρίζεται τα ερωτήματα, " Το σχέδιο ασφαλείας των συστημάτων καλύπτει τις απαιτήσεις του;" και " Η εφαρμογή ασφαλείας των συστημάτων ανταποκρίνεται στις προδιαγραφές τις;". Σημείωση ότι η διαβεβαίωση εκφράζεται ως βαθμός

εμπιστοσύνης, όχι όμως από την άποψη μιας επίσημης απόδειξης ότι το σχέδιο ή η εφαρμογή είναι ορθό/ή.

Στη παρούσα κατάσταση, είναι πολύ δύσκολο εάν όχι αδύνατο να κινηθεί πέρα από ένα βαθμό εμπιστοσύνης προς την ολοκληρωτική απόδειξη. Έχει γίνει αρκετή δουλειά στην ανάπτυξη επίσημων προτύπων που καθορίζουν τις απαιτήσεις και τα χαρακτηριστικά των σχεδίων και των εφαρμογών, μαζί με την χρήση λογικών και μαθηματικών τεχνικών που αφορούν τα ζητήματα αυτά. Η διαβεβαίωση όμως εξακολουθεί να είναι ακόμη θέμα βαθμού εμπιστοσύνης.

Η αξιολόγηση, είναι η διαδικασία εξέτασης ενός υπολογιστικού προϊόντος ή συστήματος λαμβάνοντας υπόψη συγκεκριμένα κριτήρια. Η αξιολόγηση περιλαμβάνει τη δοκιμή καθώς επίσης ενδέχεται να περιλαμβάνει επίσημες μαθηματικές ή αναλυτικές τεχνικές. Η κύρια ώθηση των εργασιών σε αυτό τον τομέα, είναι η ανάπτυξη των κριτηρίων αξιολόγησης που θα μπορούν να εφαρμοστούν σε οποιοδήποτε σύστημα ασφαλείας (καλύπτοντας τις υπηρεσίες και τους μηχανισμούς ασφαλείας). Αυτό υποστηρίζεται ευρέως, γιατί τα κριτήρια αυτά θα μπορούν να χρησιμοποιηθούν στην σύγκριση παρεμφερή προϊόντων.

Κεφάλαιο 3
Ηλεκτρονικό Έγκλημα και Χάκερς

Η μεγαλύτερη απειλή της ασφάλειας, της μυστικότητας και της αξιοπιστίας των δικτύων ηλεκτρονικών υπολογιστών και άλλων σχετικών συστημάτων ηλεκτρονικής διαχείρισης πληροφοριών γενικότερα, είναι το ηλεκτρονικό έγκλημα που διαπράττεται από εγκληματίες και πιο συγκεκριμένα από χάκερς. Αυτό διαφαίνεται από τις ζημίες που έχουν προκληθεί στο παρελθόν από τέτοιου είδους εγκληματικές ενέργειες τόσο κατά επιχειρήσεων, κυβερνητικών οργανισμών αλλά και ατόμων, με αποτέλεσμα τη δυσχέρεια, την απώλεια παραγωγικότητας και της αξιοπιστίας. Αυτό δημιουργεί μια αυξανόμενη ανάγκη στην αγορά προς τις εταιρείες λογισμικού και υλιστικού προϊόντος, για την δημιουργία ασφαλέστερων προϊόντων που να μπορούν να χρησιμοποιηθούν για να προσδιορίσουν απειλές και ευπάθειες, να διορθώσουν τυχόν προβλήματα και για να παραδώσουν λύσεις ασφαλείας.

Η συνεχιζόμενη άνοδος του hacking, η πρωτοφανής εξάπλωση του Διαδικτύου, οι πρόσφατες εξελίξεις της παγκοσμιοποίησης, η σμίκρυνση του τεχνικού εξοπλισμού, η ασύρματη και κινητή τεχνολογία, η συνεχώς αυξανόμενη τάση των συνδεδεμένων δικτύων ηλεκτρονικών

υπολογιστών και η συνεχώς αυξανόμενη εξάρτηση της κοινωνίας στους ηλεκτρονικούς υπολογιστές, έχουν αυξήσει των αριθμό των απειλών και των χάκερς, με αποτέλεσμα την αύξηση του ηλεκτρονικού εγκλήματος σε παγκόσμιο επίπεδο. Η αύξηση των χάκερς και του ηλεκτρονικού εγκλήματος δημιουργούν σοβαρά κοινωνικά, ηθικά, νομικά, πολιτικά και πολιτιστικά προβλήματα. Αυτά τα προβλήματα περιλαμβάνουν μεταξύ άλλων, κλοπή ταυτότητας, ηλεκτρονική απάτη, κλοπή πνευματικής ιδιοκτησίας και επιθέσεις σε κρατικές υποδομές, με αποτέλεσμα τις έντονες αντιπαραθέσεις για την εξεύρεση αποτελεσματικών τρόπων διαχείρισής τους, αν όχι μόνιμου τερματισμού τους.

Οι επιχειρήσεις και οι κυβερνήσεις ανά των κόσμο, αποκρίνονται σε αυτές τις απειλές μέσω ποικίλων προσεγγίσεων και συνεργασιών όπως:

- Ο σχηματισμός διαφόρων οργανισμών όπως ο ISAC (Information Sharing and Analysis Center), ενός μη κερδοσκοπικού οργανισμού, ο οποίος παρέχει μια κεντρική υπηρεσία συγκέντρωσης πληροφοριών, όσον αφορά τις απειλές για κρίσιμες υποδομές και την παροχή διανομής πληροφοριών μεταξύ του ιδιωτικού και δημόσιου τομέα.

- Η δημιουργία πυλών επικοινωνίας μεταξύ επιχειρήσεων και παρόχων διαδικτύου, για το πώς μπορούν να αντιμετωπιστούν επιθέσεις κατανεμημένης άρνησης υπηρεσιών (DDOS), καθώς και της δημιουργίας ομάδων ανταπόκρισης έκτακτης ανάγκης (CERTs, Computer Emergency Response Teams).

- Η αύξηση της χρήσης ειδικευμένων εργαλείων και υπηρεσιών από τις εταιρείες για την ανεύρεση ευπαθειών στα δίκτυα ηλεκτρονικών υπολογιστών. Τέτοια εργαλεία περιλαμβάνουν το σχηματισμό ιδιωτικών οργανώσεων στο τομέα της ασφαλείας (PSSOs, Private Sector Security Organizations), όπως είναι το SecurityFocus, Bugtraq και το International Chamber of Commerce's Cybercrime Unit.

- Ο καθορισμός εθνικής στρατηγικής για διαφύλαξη του κυβερνοχώρου.

3.1 Ηλεκτρονικό Έγκλημα

Το 1994 οι Forester και Morrison όρισαν το Ηλεκτρονικό Έγκλημα (Computer Crime) σαν «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της». [06]

Αν θέλαμε να ορίσουμε περεταίρω το «Ηλεκτρονικό Έγκλημα» θα μπορούσαμε να πούμε ότι γενικότερα είναι κάθε παράνομη δραστηριότητα αξιόποινων εγκληματικών πράξεων, που για την διάπραξη αλλά και για την αντιμετώπισή τους, απαιτείται η τεχνολογική γνώση και τιμωρείται με συγκεκριμένες ποινές, από την εκάστοτε νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (Computer Crime) και σε Κυβερνοεγκλήματα (Cyber Crime), εάν τελέστηκαν μέσω του Διαδικτύου. Ο ορισμός του ηλεκτρονικού εγκλήματος έχει να κάνει με την οπτική γωνία από την οποία εξετάζεται. Αυτή η πολυμορφία του εγκλήματος είναι που δυσχεραίνει και τον νομοθέτη, ο όποιος αποφεύγει να του προσδώσει έναν ορισμό και είτε αφήνει αυτήν την αρμοδιότητα στα δικαστήρια και στην παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Τόσο η Διεθνής όσο και η Ευρωπαϊκή Συνθήκη σχετικά με τα Κυβερνοεγκλήματα έχουν συντάξει ένα κατάλογο των εγκλημάτων αυτών που περιλαμβάνει τα ακόλουθα:

- Παράνομη πρόσβαση σε πληροφορίες.
- Παράνομη παρεμπόδιση μεταφοράς των πληροφοριών.
- Παραποίηση πληροφοριών.
- Παράνομη χρήση εξοπλισμού τηλεπικοινωνιών.
- Παρεισφρήσεις στο δημόσιο δίκτυο μεταγωγέων και πακέτων δεδομένων.
- Παραβιάσεις ακεραιότητας δικτύων.
- Παραβιάσεις μυστικότητας.

- Βιομηχανική κατασκοπεία.
- Χρήση/διανομή πειρατικού λογισμικού υπολογιστών.
- Διενέργεια απάτης.
- Κατάχρηση Διαδικτύου/ηλεκτρονικού μηνύματος.
- Χρήση ηλεκτρονικών υπολογιστών ή της τεχνολογίας υπολογιστών για την διάπραξη φόνου, τρομοκρατικής ενέργειας, πορνογραφικού υλικού και χάκινγκ.

3.1.1 Κυβερνοεγκλήματα (Cyber Crime)

Για να μπορεί κάποιο έγκλημα να ορίζεται ως κυβερνοέγκλημα, θα πρέπει να πραγματοποιηθεί με την βοήθεια κάποιου ηλεκτρονικού υπολογιστή. Τα κυβερνοεγκλήματα εκτελούνται με δυο τρόπους, είτε με επιθέσεις διείσδυσης, είτε με επιθέσεις άρνησης υπηρεσιών.

Επιθέσεις διείσδυσης (Penetration)

Ως επίθεση διείσδυσης ορίζεται η επιτυχής αναρμόδια πρόσβαση σε ένα προστατευμένο σύστημα ή η επιτυχής αναρμόδια πρόσβαση σε ένα αυτοματοποιημένο σύστημα ή η επιτυχής πράξη παράκαμψης των μηχανισμών ασφαλείας ενός συστήματος ηλεκτρονικού υπολογιστή [17]. Γενικότερα μια επίθεση μπορεί να θεωρηθεί ως επίθεση διείσδυσης, εάν παραβιάζει την ακεραιότητα και την εμπιστευτικότητα του ιδιοκτήτη ενός συστήματος ηλεκτρονικού υπολογιστή.

Μια επίθεση διείσδυσης χρησιμοποιεί γνωστές αδυναμίες στην ασφάλεια του υπό στόχου συστήματος, με σκοπό την απόκτηση πρόσβασης στους πόρους αυτού. Με μια πλήρη διείσδυση, ένας εισβολέας αποκτά πλήρη πρόσβαση σε όλους τους πόρους του συστήματος, δίνοντας του έτσι το δικαίωμα να διαγράψει ή να τροποποιήσει αρχεία, να εγκαταστήσει ιούς ή και δούρειους ίππους (Trojan Horse). Επίσης υπάρχει η δυνατότητα, εάν το σύστημα είναι συνδεδεμένο σε ένα δίκτυο ηλεκτρονικών υπολογιστών, να το χρησιμοποιήσει ως σταθμό επίθεσης σε άλλους δικτυακούς πόρους.

Μια επίθεση διείσδυσης μπορεί να είναι τοπική, όπου ο εισβολέας αποκτά πρόσβαση στον υπολογιστή ή εξυπηρετητή του δικτύου όπου είναι εγκατεστημένο το σύστημα ή εξ αποστάσεως, μέσο διαδικτύου, όπου ο επιτιθέμενος μπορεί να βρίσκεται χιλιάδες χιλιόμετρα μακριά από το θύμα.

Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDOS)

Η άρνηση υπηρεσίας ορίζεται ως οποιαδήποτε ενέργεια ή σειρά ενεργειών που αποτρέπει οποιοδήποτε μέρος του συστήματος να εργαστεί σύμφωνα με τον προκαθορισμένο τρόπο λειτουργίας του. Αυτό περιλαμβάνει οποιαδήποτε δράση που προκαλεί την αναρμόδια καταστροφή, τροποποίηση ή καθυστέρηση της υπηρεσίας. Η άρνηση υπηρεσίας μπορεί επίσης να προκληθεί από τη σκόπιμη υποβάθμιση ή παρεμπόδιση της ορθής λειτουργίας των υπολογιστικών πόρων. [17]

Οι επιθέσεις άρνησης υπηρεσιών, γνωστές και ως επιθέσεις κατανεμημένης άρνησης υπηρεσιών, στοχεύουν υπολογιστές οι οποίοι είναι συνδεδεμένοι με το διαδίκτυο. Δεν αποτελούν επιθέσεις διείσδυσης και επομένως δεν αλλάζουν, καταστρέφουν ή τροποποιούν τους πόρους των συστημάτων. Εντούτοις έχουν επιπτώσεις στο σύστημα, μέσω της μείωσης της δυνατότητας του συστήματος να λειτουργήσει κανονικά και ως εκ τούτου να υποχρεώσουν το σύστημα να καταρρεύσει, χωρίς ωστόσο να καταστραφούν οι πόροι του.

Όπως οι επιθέσεις διείσδυσης, έτσι και οι επιθέσεις άρνησης υπηρεσιών, μπορούν να είναι τοπικές ή εξ αποστάσεως. Οι επιθέσεις στην κατηγορία αυτή περιλαμβάνουν ανάμεσα σε άλλες και τα εξής:

- **IP spoofing:** Αποτελεί μια τεχνική απόκτησης παράνομης πρόσβασης σε υπολογιστές, με τη δημιουργία πακέτων TCP/IP, χρησιμοποιώντας τη διεύθυνση και τα στοιχεία κάποιας άλλης αξιόπιστης οντότητας. Οι δρομολογητές (Routers) χρησιμοποιούν την διεύθυνση της IP προορισμού ώστε να διαδώσουν τα πακέτα μέσω διαδικτύου, αγνοώντας - αλλάζοντας εικονικά την διεύθυνση της IP πηγής. Αυτή η διεύθυνση χρησιμοποιείται μόνο από το μηχάνημα προορισμού όταν απαντά πίσω στη πηγή.

- **SYN flooding:** Ο επιτιθέμενος αποστέλλει στον διακομιστή-θύμα (Server) πολλαπλά πακέτα TCP SYN. Ο διακομιστής θεωρεί ότι τα πακέτα αυτά

προέρχονται από κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει. Λόγω του ότι για κάθε ημιτελή σύνδεση TCP, ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όρια του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρηστές.

- **Smurf attack:** Ο επιτιθέμενος στέλνει μια πληθώρα πακέτων ping ICMP Echo Request σε διευθύνσεις IP broadcast διαφόρων δικτύων. Τα πακέτα αυτά έχουν εκ των προτέρων τροποποιηθεί κατάλληλα ούτως ώστε το πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Δεδομένου ότι τα πακέτα αυτά στάλθηκαν στην διεύθυνση IP Broadcast των διαφόρων δικτύων, τα λαμβάνουν όλοι οι υπολογιστές που ανήκουν σε αυτά. Αυτό έχει ως αποτέλεσμα, όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν διεύθυνση προορισμού την διεύθυνση IP του θύματος. Το θύμα τελικός πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση.

- **Ping of Death:** Το πακέτο ping κανονικά έχει μέγεθος 64 bytes. Υπάρχουν πολλοί τύποι ηλεκτρονικών υπολογιστών που δεν μπορούν να διαχειριστούν πακέτα ping που έχουν μέγεθος μεγαλύτερο από 65535 bytes, το μέγιστο επιτρεπτό από το πρωτόκολλο IP. Ως αποτέλεσμα, η επίθεση Ping of Death περιλαμβάνει την συνεχή αποστολή μεγάλων πακέτων ping σε κάποιο υπολογιστή μέχρι αυτός να τεθεί εκτός λειτουργίας.

- **Buffer Overflow:** Στη επίθεση με υπερχείλιση μνήμης, ο εισβολέας υπερχειλίζει επιλεκτικά μια συγκεκριμένη παράμετρο εισόδου, όπως λόγου χάρη την παράμετρο της διεύθυνσης, με περισσότερους χαρακτήρες από αυτούς που μπορεί να διαχειριστεί. Οι χαρακτήρες αυτοί στις περιπτώσεις που επιδιώκεται μια κακόβουλη ενέργεια, είναι στην πραγματικότητα εκτελέσιμος κώδικας, τον οποίο ο επιτιθέμενος μπορεί να εκτελέσει για να προκαλέσει δολιοφθορά στο σύστημα. Ο συγκεκριμένος τύπος επίθεσης έχει καταστεί μια από τις σοβαρότερες απειλές ασφαλείας, λόγω του ότι ο οποιοσδήποτε με ελάχιστη γνώση το συστήματος, μπορεί να προβεί σε αυτού του είδους την επίθεση.

- **Sequence number sniffing:** Ο εισβολέας εκμεταλλεύεται την προβλεψιμότητα των αριθμών ακολουθίας που χρησιμοποιούνται από το TCP για να παρεμποδίσει μια σύνδεση.

Οι επιθέσεις DDOS, σε αντίθεση με τις επιθέσεις διείσδυσης, όπου ο επιτιθέμενος αναμένεται να κερδίσει κάτι από την επίθεση, έχουν σκοπό την παρενόχληση του συστήματος. Για το λόγο αυτό αυτού του τύπου επιθέσεις εκτελούνται με ένα συγκεκριμένο στόχο:

- να αχρηστευόσουν, λόγου χάρη, την ηλεκτρονική αλληλογραφία ενός οργανισμού,

- να στηθεί για παράδειγμα ένας μηχανισμός, ο οποίος θα αποστέλλει ηλεκτρονικά μηνύματα ταχυδρομείου, γεμίζοντας το ηλεκτρονικό γραμματοκιβώτιο ενός ή περισσοτέρων ατόμων με άχρηστα μηνύματα, καθιστώντας αδύνατη την παραλαβή και ακόμη και την αποστολή εταιρικών μηνυμάτων.

3.1.2 Κυβερνοεγληματίες (Cyber Criminals)

Οι κυβερνοεγκληματίες είναι συνηθισμένοι χρήστες του κυβερνοχώρου οι οποίοι έχουν σκοπό και στόχο. Καθώς υπάρχει ραγδαία αύξηση των χρηστών υπάρχει και παράλληλη αύξηση των κυβερνοεγκληματιών. Οι απειλές για τον παράνομο έλεγχο των συστημάτων μπορούν να προέλθουν από πολυάριθμες πηγές, όπως λόγου χάρη, από ανταγωνιστικές πηγές, όπως είναι οι εχθρικές κυβερνήσεις, οι τρομοκρατικές ομάδες, οι βιομηχανικοί κατάσκοποι, οι δυσαρεστημένοι υπάλληλοι, οι κακόβουλοι εισβολείς, καθώς επίσης και από φυσικές πηγές, όπως από την περιπλοκότητα των συστημάτων, ανθρώπινα λάθη και ατυχήματα, αστοχία υλικού και φυσικές καταστροφές.

Οι ομάδες απειλής, οι οποίες ευθύνονται για την πλειοψηφία των κυβερνοεγκλημάτων, είναι οι ακόλουθες:

- **Εισβολείς (Attackers):** Οι εισβολείς επιδιώκουν και αποκτούν παράνομη πρόσβαση σε δίκτυα ηλεκτρονικών υπολογιστών για την συγκίνηση της πρόκλησης ή για να καυχιούνται στην κοινότητα των εισβολέων. Παλαιότερα η απομακρυσμένη παράνομη πρόσβαση απαιτούσε αρκετές και εξειδικευμένες γνώσεις πληροφορικής, στην σημερινή εποχή οι εισβολείς μπορούν να "κατεβάσουν" από το διαδίκτυο συγκεκριμένα προγράμματα και να τα εκτελέσουν κατά του θύματος. Καθώς τα εργαλεία επιθέσεις

γίνονται πιο εξειδικευμένα και περίπλοκα, η χρήση τους γίνεται παράλληλα πιο εύκολη. Παρόλο που πολλοί εισβολείς δεν έχουν την κατάλληλη τεχνογνωσία να απειλήσουν δύσκολους στόχους, εντούτοις ο παγκόσμιος πληθυσμός των εισβολέων αποτελεί υψηλό κίνδυνο και προκαλεί σοβαρές ζημιές. [05]

- **Διαχειριστές δικτύων Bot (Bot-network operators):** Οι διαχειριστές αυτοί είναι εισβολείς, εντούτοις αντί να αποκτήσουν πρόσβαση στα συστήματα για την συγκίνηση της πρόκλησης ή της καυχησιολογίας, συντονίζουν τις επιθέσεις και αποκτούν πρόσβαση σε πολλά συστήματα. Επίσης συντονίζουν επιχειρήσεις ηλεκτρονικού ψαρέματος (Phishing), ανεπιθύμητης αλληλογραφίας και επιθέσεις κακόβουλου λογισμικού. Οι υπηρεσίες τους αυτές κάποτε γίνονται διαθέσιμες προς πώληση στην αγορά, όπου δρουν εγκληματικά στοιχεία. [05]

- **Εγκληματικές Ομάδες (Criminal groups):** Οι ομάδες αυτές επιδιώκουν να επιτεθούν στα συστήματα με στόχο το χρηματικό κέρδος. Συγκεκριμένα, οι ομάδες οργανωμένου εγκλήματος, χρησιμοποιούν σαν εργαλεία τους, την αποστολή ανεπιθύμητης αλληλογραφίας και τις επιθέσεις κακόβουλου λογισμικού, για να διαπράξουν την κλοπή ταυτότητας και την διεξαγωγή απευθείας διαδικτυακής απάτης. Οι διεθνείς εταιρικοί κατάσκοποι και οι οργανισμοί οργανωμένου εγκλήματος, μέσω της δυνατότητας τους να διαχειρίζονται την βιομηχανική κατασκοπεία και της μεγάλης κλίμακας οικονομική απάτη, αποτελούν μεγάλη απειλή για τους οργανισμούς και τις κυβερνήσεις ευρύτερα. Μερικές εγκληματικές ομάδες μπορεί να προβούν σε απειλές διεξαγωγής κυβερνοεπίθεσης σε κάποιο οργανισμό, με απώτερο σκοπό την απόσπαση χρημάτων. [05]

- **Χάκερς (Hackers):** Χάκερ ονομάζεται το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ένας χάκερ έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής, έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (Hacking-groups) είτε μόνοι τους. [26]

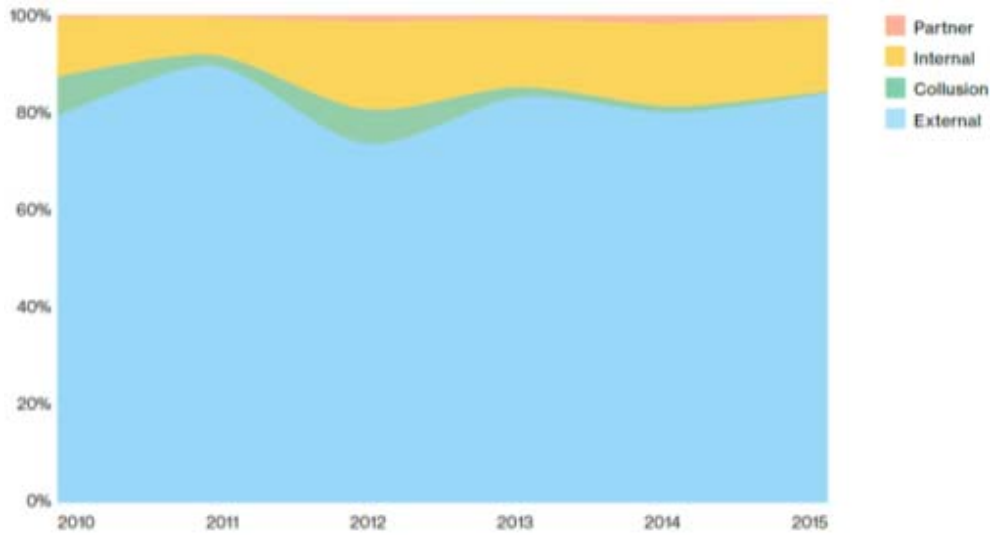
- **Δυσαρεστημένοι πρώην υπάλληλοι (Disgruntled ex-employees):** Μελέτες έχουν δείξει ότι οι δυσαρεστημένοι πρώην υπάλληλοι αποτελούν σοβαρή απειλή για τους

οργανισμούς ως πηγές στοχοθέτησης κυβερνοεγκλημάτων. Οι λόγοι αφορούν συνήθως διαφορές μεταξύ εργοδότη-υπαλλήλου, που οδήγησαν στην απόλυση του εργαζομένου. Σε ορισμένες περιπτώσεις, οι πρώην υπάλληλοι χρησιμοποιούν την γνώση που κατέχουν για τα συστήματα του οργανισμού, για να προβούν σε κάποιου είδους επίθεση με καθαρά τα οικονομικά οφέλη. [08]

- **Οικονομική κατασκοπεία (Economic espionage spies):** Η αύξηση του κυβερνοχώρου και του ηλεκτρονικού εμπορίου, καθώς και η παγκοσμιοποίηση, έχουν δημιουργήσει νέα συνδικάτα εγκλήματος. Οι οργανωμένοι οικονομικοί κατάσκοποι οργώνουν το Διαδίκτυο και ψάχνουν για μυστικά επιχειρήσεων. Καθώς ο ανταγωνισμός των επιχειρήσεων είναι έντονος και σκληρός, οι επιχειρήσεις είναι έτοιμες να καταβάλουν οποιοδήποτε ποσό για κλεμμένα εμπορικά, μάρκετινγκ και βιομηχανικά μυστικά. [08]

- **Script Kiddies:** Οι script kiddies είναι ως επί το πλείστων νεαροί σε ηλικία και βρίσκονται σε κάποια βαθμίδα της εκπαίδευσης οι οποίοι χρησιμοποιούν πολλές φορές τους υπολογιστικούς πόρους του ιδρύματος που φοιτούν και διενεργούν επιθέσεις, με κύριο σκοπό να εντυπωσιάσουν τους φίλους τους, χωρίς να γίνουν αντιληπτοί. Χρησιμοποιούν έτοιμα εργαλεία και το κίνητρο τους είναι η διασκέδαση. Δεν διαθέτουν ιδιαίτερες τεχνικές γνώσεις και στις πλείστες των περιπτώσεων δεν γνωρίζουν ακριβώς τι κάνουν.

Στην Εικόνα 3.1 διαφαίνεται το ποσοστό των παραβιάσεων για τους κυριότερους παράγοντες απειλών. Το μεγαλύτερο ποσοστό, όπως ήταν αναμενόμενο, οφείλετε σε εξωγενείς παράγοντες .



Εικόνα 3.1: Ποσοστό παραβιάσεων για τους κυριότερους παράγοντες απειλών. [25]

3.2 Χάκερς

Στην καθομιλουμένη, όταν αναφερόμαστε στον όρο Χάκερ, εννοούμε αυτούς που προβαίνουν σε κακόβουλες ενέργειες μέσω διαδικτύου. Στην πραγματικότητα όμως υπάρχει ένας αριθμός υποκατηγοριών βάση της φιλοσοφίας που ασπάζεται και ακολουθείται από την κάθε ομάδα.

Οι χάκερς

Είναι αυτοί που ενδιαφέρονται σε μεγάλο βαθμό για τις τυχόν μυστικές και κρυφές λειτουργίες ενός λειτουργικού συστήματος ηλεκτρονικού υπολογιστή. Στην πλειοψηφία τους είναι προγραμματιστές με εκτενή γνώση των λειτουργικών συστημάτων και διαφόρων γλωσσών προγραμματισμού. Η προσπάθειά τους είναι να ανακαλύψουν τυχόν "κενά" στα συστήματα υπολογιστών καθώς και το λόγο ύπαρξης αυτών των κενών. Οι χάκερς δεν καταστρέφουν σκόπιμα δεδομένα, αναζητούν επισταμένα πρόσθετη γνώση και μοιράζονται ελεύθερα ότι έχουν ανακαλύψει. Στην σημερινή εποχή οι χάκερς δεν θεωρούνται πλέον τόσο επικίνδυνοι όσο παλαιότερα . Αντίθετα προσλαμβάνονται από κυβερνητικούς οργανισμούς και επιχειρήσεις για την υπεράσπιση κρίσιμων δικτύων και συστημάτων, καθώς και την απάλειψη των επισφαλών τους σημείων.

Οι κράκερς

Είναι αυτοί οι οποίοι παραβιάζουν την ακεραιότητα του συστήματος απομακρυσμένων μηχανημάτων, με σκοπό την κακόβουλη ενέργεια. Αποκτώντας παράνομη πρόσβαση καταστρέφουν σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση νόμιμων χρηστών ή και προξενούν σοβαρά προβλήματα στα θύματά τους.

Οι χακτιβιστές (Χάκερ + Ακτιβιστής, Hacktivist)

Είναι αυτοί οι οποίοι χρησιμοποιούν με ανατρεπτικό τρόπο τους υπολογιστές για την προώθηση μιας πολιτικής ατζέντας. Έχοντας ρίζες στην κοινότητα των χάκερς και στην ηθική αυτών, οι ενέργειες τους σχετίζονται συχνά με την ελευθερία του λόγου, τα ανθρώπινα δικαιώματα ή το δικαίωμα ελευθερίας στην πληροφόρηση. Λόγο της ποικιλίας των ορισμών που προκύπτουν από τα δύο συνθετικά της λέξης "χακτιβιστής", υπάρχει μεγάλη διαφωνία αναφορικά με το είδος των ενεργειών και των σκοπών που επιτελούν. Κάποιοι ορισμοί μιλούν για κυβερνοεγκλήματα και κάποιοι άλλοι για πράξεις που προάγουν την κοινωνική αλλαγή.

Τα συνήθη εργαλεία και τακτικές που χρησιμοποιούν, είναι:

- Αυτόματα συστήματα μαζικής αποστολής ηλεκτρονικών μηνυμάτων.

- Επιθέσεις σε εξυπηρετητές φιλοξενίας ιστοσελίδων (Web Servers), όπου ανταλλάζουν το περιεχόμενο συγκεκριμένων σελίδων με τα μηνύματα που θέλουν να περάσουν στο ευρύ κοινό που τις επισκέπτεται.

- Εικονική καθιστική διαμαρτυρία, όπου επιτυγχάνεται άρνηση ή παρεμπόδιση πρόσβασης σε συγκεκριμένη ιστοσελίδα.

- Ιοί και ηλεκτρονικά σκουλήκια (Worms), ίσως η πιο προσφιλής μέθοδος που χρησιμοποιούν οι χακτιβιστές για την προώθηση των μηνυμάτων τους.

3.2.1 Χάκερς και Δίοδοι Πρόσβασης

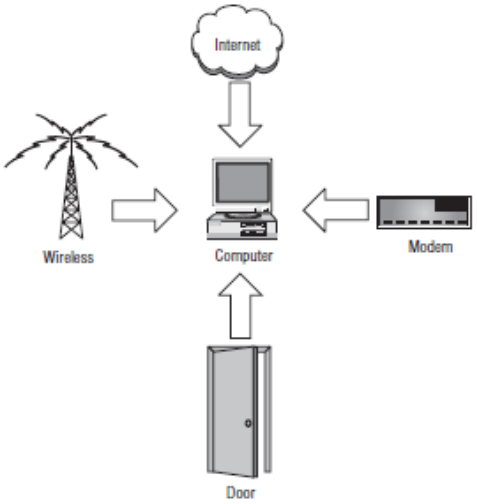
Όπως παρουσιάζεται στην Εικόνα 3.2, υπάρχουν μόνο τέσσερεις τρόποι για να αποκτήσει πρόσβαση ένας χάκερ σε κάποιο δίκτυο ηλεκτρονικών υπολογιστών [22]:

- Μέσω Διαδικτυακής σύνδεσης.

- Μέσω χρήσης ηλεκτρονικού υπολογιστή ο οποίος είναι συνδεδεμένος απευθείας με το δίκτυο του θύματος.

- Μέσω τηλεφωνικής σύνδεσης από απομακρυσμένο σημείο, χρησιμοποιώντας την υπηρεσία απομακρυσμένη σύνδεσης, που πιθανώς να έχει ενεργοποιημένη το θύμα.

- Μέσω ασύρματης μη ασφαλούς σύνδεσης.



Εικόνα 3.2: Δίοδοι πρόσβασης ενός χάκερ.

Επίθεση Δια ζώσης

Οι χάκερς εκμεταλλευόμενοι το μεγάλο αριθμό των εργαζομένων που δουλεύουν σε μεγάλους οργανισμούς, την μη χρήση μέτρων ελέγχου πρόσβασης (φρουρούς ασφαλείας, κάρτες πρόσβασης κτλ) και το γεγονός ότι είναι σχεδόν αδύνατο να γνωρίζονται όλοι οι εργαζόμενοι μεταξύ τους εξ όψεως, εισχωρούν σε αυτούς παριστάνοντας ότι εργάζονται εκεί, περνώντας απαρατήρητοι. Στη συνέχεια κάθονται σε κάποιο υπολογιστή, ο οποίος είναι συνδεδεμένος με το δίκτυο και θέτουν τις βάσεις για περεταίρω διείσδυση, η οποία θα μπορεί να γίνει αργότερα εξ αποστάσεως.

Κάποιος επίσης μπορεί να προσποιηθεί ότι εργάζεται στην τηλεφωνική εταιρεία του θύματος και να ζητήσει πρόσβαση στο δωμάτιο των εξυπηρετητών για να επαλειφθεί κάποιου υποτιθέμενου προβλήματος στις τηλεφωνικές γραμμές. Αν παραμείνει ανεπιτήρητος μπορεί πολύ απλά να δημιουργήσει ένα λογαριασμό διαχείρισης σε συγκεκριμένο εξυπηρετητή ή να τοποθετήσει ένα μικρό διαποδιαμορφωτή (Modem) ή ένα ασύρματο σημείο πρόσβασης (Wireless Router) για απομακρυσμένη πρόσβαση σε μεταγενέστερη χρονική στιγμή.

Με την υιοθέτηση μέτρων φυσικής ασφάλειας και την μεταχείριση οποιουδήποτε καλωδίου ή σύνδεσης που εισέρχεται στο κτήριο ως πρόβλημα ασφαλείας, το θέμα επίθεσης δια ζώσης, μπορεί να αντιμετωπιστεί. Προϋπόθεση είναι η χρήση τείχους προστασίας για έλεγχο οποιασδήποτε σύνδεσης φεύγει από το κτήριο.

Επίθεση μέσω τηλεφωνικής σύνδεσης

Η επίθεση μέσω τηλεφωνικής σύνδεσης αποτελούσε τον μόνο τρόπο επίθεσης που υπήρχε μέχρι την στιγμή της εμφάνισης της ευρυζωνικής πρόσβασης στο Διαδίκτυο, όπου πέρασε σε δεύτερη μοίρα.

Αυτό φυσικά δεν σημαίνει ότι η επίθεση μέσω τηλεφωνικής σύνδεσης έχει εκλείψει. Ο χάκερ ο οποίος έχει συγκεκριμένο στόχο, θα χρησιμοποιήσει κάθε διαθέσιμο μέσο για να επιτύχει την επιθυμητή πρόσβαση.

Οποιαδήποτε σύνδεση μέσω διαποδιαμορφωτή (Modem), ο οποίος έχει ρυθμιστεί να απαντά σε κλήσεις, με σκοπό την απομακρυσμένη σύνδεση για πρόσβαση σε φιλοξενούμενες υπηρεσίας εντός του οργανισμού ή για την εξ αποστάσεως διαχείριση συστημάτων, αποτελεί πρόβλημα ασφαλείας.

Με την υιοθέτηση τείχους προστασίας και την υποχρεωτική αυθεντικοποίηση όλων των νόμιμων χρηστών που επιχειρούν απομακρυσμένη πρόσβαση στο σύστημα και την αποτροπή ανταπόκρισης οποιασδήποτε τηλεφωνικής γραμμής, αν δεν έχει πρώτα περάσει από την αυθεντικοποίηση του τείχους προστασίας, περιορίζεται το συγκεκριμένο ρίσκο.

Επίθεση μέσω Διαδικτύου

Η επίθεση μέσω διαδικτύου, αποτελεί την πιο διαθέσιμη, την πιο εύκολα εκμεταλλεύσιμη και τη πιο προβληματική παράμετρο παρείσφρησης στο δίκτυο ενός οργανισμού.

Η χρήση κρυπτογραφίας, συστημάτων ανίχνευσης/αντιμετώπισης παρείσφρησης, τείχους προστασίας, εργαλεία ανίχνευσης τρωσιμότητας, αποτελούν κάποια από τα μέτρα που ένας οργανισμός μπορεί να εφαρμόσει για να περιορίσει το ρίσκο αυτό.

Επίθεση μέσω ασύρματων δικτύων

Ένα ασύρματο δίκτυο τοπικής περιοχής (WLAN) είναι μια ομάδα ασύρματων συσκευών δικτύωσης σε μια περιορισμένη γεωγραφική περιοχή, όπως ένα κτίριο γραφείων, όπου γίνεται η ανταλλαγή των δεδομένων μέσω ραδιοεπικοινωνιών. Οι τεχνολογίες WLAN είναι βασισμένες στο πρωτόκολλο IEEE 802.11 και στις τροποποιήσεις αυτού. Σε ένα WLAN συνδέονται συσκευές πελατών και εργαζομένων, όπως φορητοί ηλεκτρονικοί υπολογιστές, έξυπνα κινητά

τηλέφωνα (Smart Phones) καθώς και σημεία πρόσβασης (Access Points) όπου συνδέουν τις συσκευές αυτές, συνήθως, με το ευρύτερο ενσύρματο δίκτυο του οργανισμού.

Η ασφάλεια του WLAN εξαρτάται από πόσο καλά είναι ασφαλείς οι συνδεδεμένες σε αυτό συσκευές. Δυστυχώς τα WLAN, για διάφορους λόγους, είναι λιγότερο ασφαλή σε σχέση με τα αντίστοιχα ενσύρματα δίκτυα. Η ευκολία πρόσβασης και η ελλιπής ρύθμιση (για χάρη της ευκολίας χρήσης παραλείπετε η ασφάλεια) είναι μερικοί από αυτούς τους λόγους.

Τα πιο κάτω μπορούν να συμβάλουν στη διαμόρφωση πιο ασφαλών WLANs [20]:

- Η χρήση τυποποιημένων ρυθμίσεων ασφαλείας σε όλα τα τμήματα του WLAN (συσκευές πελατών, σημείων πρόσβασης, κτλ) με σκοπό την μείωση των ευπαθειών και ελάττωση των επιτυχημένων επιθέσεων. Οι ρυθμίσεις αυτές θα πρέπει να ελέγχονται περιοδικά και να διασφαλίζεται, όσο είναι εφικτό, η αποτελεσματικότητα τους σε νέες προκλήσεις.

- Ένας οργανισμός θα πρέπει να έχει ξεχωριστό WLAN για επισκέπτες και ξεχωριστό για τους εργαζομένους. Επίσης οι συσκευές οι οποίες θα είναι συνδεδεμένες στο WLAN των επισκεπτών δεν θα πρέπει να μπορούν να συνδέονται με συσκευές που είναι συνδεδεμένες στο WLAN των εργαζομένων και αντίστροφα.

- Η χρήση πολιτικών που θα δηλώνουν σαφώς ποιες συσκευές θα μπορούν να συνδέονται και στο WLAN και στο ενσύρματο δίκτυο, ταυτόχρονα. Η εφαρμογή των πολιτικών αυτών θα πρέπει να μπουν σε εφαρμογή με την ανάλογες ρυθμίσεις ασφαλείας. Εάν ένας επιτιθέμενος καταφέρει να κερδίσει, μέσω ασύρματης σύνδεσης, αναρμόδια πρόσβαση σε μια συσκευή η οποία έχει δικαίωμα ταυτόχρονης διπλής πρόσβασης, τότε μπορεί να αποκτήσει πρόσβαση στο ενσύρματο δίκτυο του οργανισμού.

- Η χρήση εργαλείων ανίχνευσης επιθέσεων και ανεύρεσης ευπαθειών. Όπως όλα τα μέρη ενός δικτύου ελέγχονται για ευπάθειες ή τυχών παραβιάσεις, έτσι θα πρέπει να ελέγχονται και τα ασύρματα δίκτυα. Σε περίπτωση αναγνώρισης ευπαθειών, θα πρέπει να προγραμματίζεται η εγκατάσταση αρχείων επιδιόρθωσης, όπως θα προγραμματίζετο για οποιοδήποτε άλλο σύστημα.

- Θα πρέπει να γίνονται περιοδικές τεχνικές αξιολόγησης της ασφάλειας των WLANs. Οι αξιολογήσεις αυτές θα πρέπει να γίνονται τουλάχιστον ετήσια.

3.2.2 Μεθοδολογία και Τεχνικές

Οι επιθέσεις των Χάκερς διεξάγονται με την χρήση διαφόρων εργαλείων και τεχνικών. Μια επίθεση περιλαμβάνει διάφορα στάδια [22]:

- Την επιλογή του στόχου
- Την συλλογή πληροφοριών
- Την επίθεση

Ο χάκερ θα προσπαθήσει να μαζέψει όσο γίνεται περισσότερες πληροφορίες αναφορικά με το δίκτυο του θύματος, μετά από κάθε επιτυχημένη ή αποτυχημένη επίθεση, ανατροφοδοτώντας παράλληλα την πιο πάνω διαδικασία.

Επιλογή στόχου

Η επιλογή στόχου αποτελεί το πρώτο βήμα στο οποίο ο χάκερ αναγνωρίζει ένα συγκεκριμένο υπολογιστή στον οποίο θα επιχειρήσει επίθεση. Ο υπολογιστής αυτός έχει εντοπιστεί μέσο διερευνητικής διαδικασίας.

Χρησιμοποιώντας τεχνικές ανεύρεσης (DNS Lookup, Network Address Scanning) διαθέσιμων υπολογιστών, αναγνωρίζουν υπολογιστές οι οποίοι είναι εν ενεργεία. Στην συνέχεια με τεχνικές, Σάρωσης Θυρών (Port Scanning), θα προσπαθήσουν να αναγνωρίσουν το λειτουργικό σύστημα το οποίο "τρέχει" στον υποψήφιο υπολογιστή θύμα και ποιες υπηρεσίες έχει ενεργοποιημένες και διαθέσιμες στο δίκτυο. Με το Port Scanning, ο χάκερ μπορεί να εντοπίσει ποιες θύρες είναι ενεργές και ποιες όχι και εντοπίζοντας τις υπηρεσίες που "τρέχουν" σε αυτές τις θύρες, να εκμεταλλευτεί τυχών ευπάθειες των υπηρεσιών αυτών.

Το Port Scanning, θα πρέπει να λαμβάνεται σοβαρά υπόψη και να διερευνάται, αφού αποτελεί απτή απόδειξη ότι κάποιος έχει θέσει ως στόχο το δίκτυο του οργανισμού.

Εκτός από το Port Scan υπάρχει και το Service Scan. Το Service Scan διενεργείται αυτόματα με την χρήση διαδικτυακών σκουληκιών (Internet Worms) τα οποία εγκαθίστανται μέσο προγραμμάτων, στους υπολογιστές-θύματα. Το Service Scan ψάχνει για συγκεκριμένη ευπάθεια σε συγκεκριμένη θύρα του υπολογιστή. Για τον λόγο αυτό δεν μπορεί να αναγνωριστεί ως Port Scan.

Συλλογή Πληροφοριών

Η συλλογή πληροφοριών, αποτελεί το στάδιο κατά το οποίο ο χάκερ θα καταγράψει τα χαρακτηριστικά του στόχου πριν την διενέργεια επίθεσης. Η συλλογή πληροφοριών μπορεί να γίνει μέσο διαφόρων διαθέσιμων, στο ευρύ κοινό πηγών (μέσα κοινωνικής δικτύωσης) ή με την εφαρμογή μη διεισδυτικών τεχνικών.

SNMP

Ένα εργαλείο, μη διεισδυτικού τύπου, το οποίο χρησιμοποιείται ευρέως από τους διαχειριστές συστημάτων και από τους χάκερς ομοίως, για τον έλεγχο και την υποστήριξη του δικτυακού εξοπλισμού εξ αποστάσεως, είναι το SNMP (Simple Network Management Protocol). Το πρωτόκολλο αυτό έχει σχεδιαστεί έτσι ώστε να παρέχει αυτόματα τις ρυθμιστικές λεπτομέρειες του συνδεδεμένου δικτυακού εξοπλισμού. Έτσι συσκευές οι οποίες είναι ορατές στο διαδίκτυο, μπορούν να παρέχουν πληροφορίες για το εσωτερικό δίκτυο του οργανισμού. Σχεδόν κάθε συσκευή δικτύου, δρομολογητές, μεταγωγείς, τείχη προστασίας, μπορούν να διαμορφωθούν έτσι ώστε να παρέχουν SNMP πληροφορίες. Η μη ορθολογιστική επίβλεψη και διαμόρφωση του SNMP δίνει την δυνατότητα συλλογής πληροφοριών ή ακόμη και απομακρυσμένου ελέγχου σε χάκερς.

Architecture Probes

Ένας άλλος τρόπος συλλογής πληροφοριών, είναι η χρησιμοποίηση αυτοματοποιημένων εργαλείων (Architecture Probes), τα οποία έχουν μια βάση δεδομένων με γνωστές απαντήσεις κατά την αποστολή ενός πακέτου δεδομένων. Τα εργαλεία αποστέλλουν πακέτα δεδομένων στο θύμα με σκοπό την απάντηση αυτού. Την απάντηση που θα αποκομίσουν θα την ελέγξουν με την βάση δεδομένων τους και θα αποφανθούν ποιο λειτουργικό σύστημα μπορεί να δώσει αυτού του τύπου απάντηση. Ο λόγος είναι ότι, κάθε λειτουργικό σύστημα απαντά με συγκεκριμένο τρόπο που δεν ομοιάζει πλήρως με κάποιο άλλο λειτουργικό σύστημα.

Directory Services Lookups

Μια ακόμη υπηρεσία η οποία μπορεί να δώσει πληροφορίες σε κάποιο χάκερ, χωρίς αυτός να διεισδύσει στο σύστημα, είναι το Lightweight Directory Access Protocol (LDAP). Το LDAP παρέχει μια πληθώρα πληροφοριών, οι οποίες δίνουν στο επίδοξο χάκερ στοιχεία για το δίκτυο και τους χρήστες του οργανισμού.

Sniffing

Το sniffing για να επιτευχθεί, ο χάκερ, χρειάζεται είτε να αποκτήσει φυσική πρόσβαση στο δίκτυο του οργανισμού-θύματος, είτε να αποκτήσει πρόσβαση εξ αποστάσεως, σε κάποιο υπολογιστή ο οποίος είναι συνδεδεμένος με το δίκτυο. Ουσιαστικά, το sniffing, γίνεται με την χρήση ειδικευμένων εργαλείων, τα οποία καταγράφουν όλα τα πακέτα δεδομένων που δρομολογούνται εντός του δικτύου και αξιολογούν τις πληροφορίες τις οποίες διανέμουν. Αν τα πακέτα είναι κρυπτογραφημένα, τότε είναι δύσκολο να αποκρυπτογραφηθούν, εκτός και αν ο εισβολέας διαθέτει κάποιο μέσο αποκρυπτογράφησης τους.

Social Engineering

Ο Kevin Mitnick, πρώην εγκληματίας ηλεκτρονικών υπολογιστών και μετέπειτα σύμβουλος ασφαλείας πληροφοριακών συστημάτων είχε πει, ότι είναι πολύ πιο εύκολο να ξεγελάσεις κάποιον να σου δώσει ένα κωδικό πρόσβασης για κάποιο σύστημα, από το να προσπαθήσεις να τον "σπάσεις". [11]

Σαν όρος έχει πλέον καθιερωθεί ότι το social engineering είναι ουσιαστικά η προφορική χειραγώγηση ατόμων με σκοπό την απόσπαση πληροφοριών. Ο πιο συνήθης τρόπος επικοινωνίας είναι μέσο τηλεφώνου ή ηλεκτρονικού ταχυδρομείου, όπου ο επιτιθέμενος ισχυρίζεται ότι είναι κάποιο τρίτο πρόσωπο (τεχνικός ηλεκτρονικών υπολογιστών, υπάλληλος τράπεζας, σύζυγος κάποιου εργαζομένου στον οργανισμό κτλ) με σκοπό την απόσπαση πληροφοριών. Οι πληροφορίες αυτές μπορεί να έχουν να κάνουν είτε με άλλα άτομα που εργάζονται σε θέσεις κλειδιά στον οργανισμό, είτε με απόσπαση των κωδικών πρόσβασης σε συστήματα του οργανισμού.

Για να αντιμετωπιστούν αυτού του τύπου οι επιθέσεις, απαιτείται συνεχής εκπαίδευση του προσωπικού ενός οργανισμού και εφαρμογή πολιτικών ασφαλείας. Θα πρέπει να γίνεται

διακρίβωση στοιχείων, προτού δοθούν οποιεσδήποτε πληροφορίες σε τρίτους και να ενημερώνεται πάντα το τμήμα ασφαλείας του οργανισμού ή το τμήμα διεύθυνσης εάν παρατηρηθούν αυτού του τύπου ενέργειες.

Επίθεση

Οι χάκερς χρησιμοποιούν ένα ευρύ φάσμα επιθέσεων κατά των συστημάτων. Οι περισσότερες από αυτές είναι φτιαγμένες για την εκμετάλλευση των ευπαθειών των διαφόρων υπηρεσιών που τρέχουν στο συγκεκριμένο δίκτυο-στόχο.

Οι πιο διαδεδομένες επιθέσεις παρατίθενται πιο κάτω:

- **Επιθέσεις Άρνησης Εξυπηρέτησης (Denial of Service).** Οι υπολογιστές χρησιμοποιούν συγκεκριμένα πρωτόκολλα επικοινωνίας για την μεταφορά των δεδομένων. Αν τα πρωτόκολλα αυτά δεν εφαρμοστούν σωστά και αν δεν έχουν τους κατάλληλους μηχανισμούς ελέγχου λαθών, τότε είναι επιρρεπής σε επιθέσεις άρνησης εξυπηρέτησης.

  Ο υπολογιστής ο οποίος δέχεται την επίθεση. είτε θα καταρρεύσει, είτε θα σταματήσει να ανταποκρίνεται σωστά. Σε κάποιες περιπτώσεις η υπηρεσία που δέχεται την επίθεση μπορεί να καταρρεύσει, αλλά ο υπολογιστής θα συνεχίσει να εργάζεται κανονικά.

  Όσο πιο περίπλοκη είναι μια υπηρεσία, τόσο πιθανότερο είναι να είναι ευπαθείς σε επιθέσεις άρνησης εξυπηρέτησης.

  Οι επιθέσεις αυτές είναι σχετικά εύκολο να υλοποιηθούν από τους χάκερς, αλλά λόγω του ότι δεν αποφέρουν χρήσιμες πληροφορίες προς εκμετάλλευση, χρησιμοποιούνται μόνο όταν θέλουν να προξενήσουν πρόβλημα στο θύμα.

- **Πλαστοί λογαριασμοί ηλεκτρονικού ταχυδρομείου (Forged E-mail).** Οι χάκερς μπορούν να δημιουργήσουν ψεύτικους λογαριασμούς ηλεκτρονικού ταχυδρομείου και να παρουσιάζεται ότι τα μηνύματα προέρχονται από όποια νόμιμη οντότητα αυτοί επιθυμούν. Με τον τρόπο αυτό μπορούν να ξεγελάσουν τον παραλήπτη και να του αποσπάσουν εμπιστευτικές πληροφορίες. Στα ηλεκτρονικά μηνύματα τα οποία αποστέλλουν στο θύμα, μπορούν να επισυνάψουν αρχεία τύπου, παραδείγματος χάρη, δούρειου ίππου ή να επικολλήσουν κάποια διεύθυνση κακόβουλης ιστοσελίδας.

- **Αυτοματοποιημένη διερεύνηση για ανεύρεση κωδικών πρόσβασης (Automated Password guessing).** Μετά την ανεύρεση του στόχου-θύματος και του ευπαθούς λογαριασμού ή υπηρεσίας αυτού, ένας χάκερ θα χρειαστεί κάποιο κωδικό πρόσβασης για να μπορέσει να έχει το πλήρη έλεγχο του συστήματος. Ο επιτιθέμενος έχει στην διάθεση του διάφορα αυτοματοποιημένα εργαλεία τα οποία μπορεί να χρησιμοποιήσει για ανεύρεση του κωδικού αυτού. Τα εργαλεία αυτά τροφοδοτούνται από λίστες με τους πιο συχνά χρησιμοποιημένους κωδικούς πρόσβασης. Οι λίστες αυτές προκύπτουν από την στατιστική ανάλυση άλλων, ήδη κλαπέντων κωδικών πρόσβασης, τρίτων συστημάτων. Οι λίστες αυτές είναι διαθέσιμες σε κάποιον χάκερ για χρήση, είτε δωρεάν, είτε επί πληρωμή από άλλους χάκερς. Η χρησιμοποίηση των λιστών κάνει την ανεύρεση κάποιου κωδικού πρόσβασης πιο εύκολη, αν αυτός ο κωδικός αποτελεί μέρος της λίστας.

- **Ηλεκτρονικό Ψάρεμα (Phishing).** Ο επιτιθέμενος με την χρήση των ψηφιακών εργαλείων και την δυνατότητα απόκρυψης της πραγματικής του ταυτότητας, υποδύεται μια αξιόπιστη οντότητα και εκμεταλλεύεται την άγνοια του θύματος με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων. Ο όρος αυτός έχει προκύψει από το γεγονός ότι, ο τρόπος με τον οποίο ο επιτιθέμενος προσπαθεί να προσελκύσει το θύμα, θυμίζει την διαδικασία του δολώματος στο ψάρεμα.

  Ο επιτιθέμενος μπορεί να αποστείλει ένα ηλεκτρονικό μήνυμα και υποδυόμενος, λόγου χάρη την εταιρεία Amazon, να ζητήσει από τον παραλήπτη να συνδεθεί με τον λογαριασμό του, για να διορθώσει κάποια προσωπικά του στοιχεία που υποτίθεται είναι λανθασμένα. Στο ηλεκτρονικό αυτό μήνυμα τοποθετείται και ένας παραπλανητικός σύνδεσμος προς την σελίδα της Amazon. Στην ουσία ο σύνδεσμος αυτός θα οδηγήσει σε μια σελίδα, η οποία είναι πανομοιότυπη με την σελίδα πρόσβασης χρήστη της Amazon. Το θύμα εάν ξεγελαστεί και βάλει των κωδικό πρόσβασής του για να συνδεθεί με τον λογαριασμό του, τότε ο κωδικός του αυτός αποστέλλεται στον χάκερ. Το θύμα φυσικά δεν θα μπορέσει να συνδεθεί στο λογαριασμό του και πιθανός να πάρει κάποιο μήνυμα ότι η ιστοσελίδα έχει αντιμετωπίσει κάποιο προσωρινό πρόβλημα και να δοκιμάσει αργότερα. Αυτό πιθανός δεν θα προξενήσει οποιαδήποτε υποψία στο θύμα, με αποτέλεσμα να ανακαλύψει τι έχει γίνει σε μελλοντικό χρόνο, όταν θα είναι πλέον αργά.

  Έχει παρατηρηθεί μια έξαρση με αυτού του τύπου μηνύματα ηλεκτρονικού ταχυδρομείου με υποτιθέμενους αποστολείς υπαλλήλους τραπεζών.

Εικόνα 3.3: Ηλεκτρονικό ψάρεμα (Phishing) μέσω ηλ. ταχυδρομείου.

Στο παράδειγμα ηλ. ταχυδρομείου της Εικόνας 3.3, επιχειρείται η κλοπή του κωδικού πρόσβασης του ηλεκτρονικό λογαριασμό που διατηρεί ο παραλήπτης στην συγκεκριμένη τράπεζα. Εάν επιχειρήσει να πατήσει τον σύνδεσμο, όπως τον προτρέπει να κάνει το μήνυμα, θα παραπεμφθεί σε μια ιστοσελίδα που οπτικά θα προσομοιάζει με την αυθεντική ιστοσελίδα της τράπεζάς του, με σκοπό την καταχώριση και δήθεν επαλήθευση των κριτηρίων πρόσβασης του λογαριασμού του.

- **Δούρειος Ίππος (Trojan Horse).** Τα προγράμματα τύπου Δούρειος Ίππος είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης για να εκμεταλλευτεί το θύμα του. Λογισμικά αυτού του είδους παρουσιάζονται ως χρήσιμα λογισμικά αλλά στην πραγματικότητα μέσα από αυτά κάποιος εγκληματίας μπορεί να υποκλέψει σημαντικά αρχεία ή και να αποκτήσει τον έλεγχο του συστήματος. Τα προγράμματα αυτά μπορεί να τα εγκαταστήσει, είτε ο ίδιος ο επιτιθέμενος στον υπολογιστή του θύματος, είτε να τα εγκαταστήσει το ίδιο το θύμα κατεβάζοντάς τα από κάποια ιστοσελίδα ή λαμβάνοντάς τα σε κάποιο ηλεκτρονικό μήνυμα σαν επισυναπτόμενο αρχείο.

- **Source Routing.** Σε ένα δίκτυο υπολογιστών, όπου γίνεται χρήση του πρωτοκόλλου TCP/IP, υπάρχει η δυνατότητα χρησιμοποίησης της λειτουργίας source routing, η οποία εμπερικλείεται στο TCP/IP πακέτο. Η λειτουργία αυτή επιτρέπει στον αποστολέα ενός πακέτου δεδομένων, να καθορίζει την πορεία του μέσα στο δίκτυο. Στα δίκτυα τα οποία η λειτουργία αυτή δεν είναι διαθέσιμη/ενεργοποιημένη, αναλαμβάνουν οι δρομολογητές του δικτύου, αυτό το έργο.

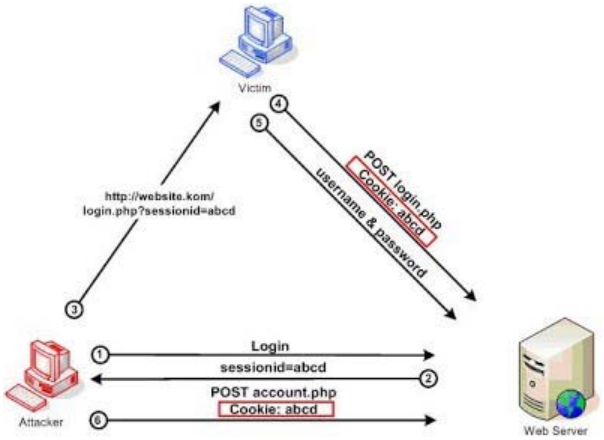
Στην περίπτωση που η λειτουργία αυτή είναι ενεργοποιημένη, ένας εισβολέας μπορεί να αποστείλει ένα πακέτο, προσποιούμενος κάποιον άλλο νόμιμο χρήστη, που είναι ήδη συνδεδεμένος με το δίκτυο και να προσθέσει επιπρόσθετες πληροφορίες τις οποίες θα μπορεί να αποστείλει, λόγου χάρη σε ένα εξυπηρετητή. Για παράδειγμα, θα μπορεί να στείλει ένα πακέτο στο οποίο θα προσποιείται ότι είναι ο διαχειριστής του εξυπηρετητή και να ζητήσει την αλλαγή του κωδικού πρόσβασης, αποκλείοντας έτσι τον νόμιμο διαχειριστή από του να έχει πρόσβαση στον εξυπηρετητή και αποκτώντας ο ίδιος πρόσβαση διαχειριστή.

- **Session Hijacking.** Session hijacking είναι τεχνική απόκτησης ελέγχου ενός session κάποιου χρήστη, αφού ανακτηθεί ή δημιουργηθεί επιτυχώς πιστοποιημένο session ID. Στο session hijacking ο επιτιθέμενος χρησιμοποιεί τεχνικές capture, brute force ή reverse-engineere για να πάρει το έλεγχο ενός "νόμιμου" Web application session χρήστη ενώ αυτό βρίσκεται σε εξέλιξη. [21]

  Το TCP session hijacking συμβαίνει όταν ο επιτιθέμενος αποκτά το TCP session μεταξύ δύο υπολογιστών. Από τη στιγμή που η επικύρωση (Athentication) λαμβάνει χώρα κατά την έναρξη του TCP session, αυτό επιτρέπει στον επιτιθέμενο να αποκτήσει έλεγχο στον υπολογιστή.

  Οι βασικές τεχνικές του session hijacking είναι οι εξής:

  - **Session Fixation.** Το session hijacking υποκλέπτει το εγκατεστημένο session μεταξύ του client και του Web Server αφού ο χρήστης κάνει log in. Το Session Fixation από την άλλη παίρνει το session από τον browser του θύματος, πριν ο χρήστης κάνει log in (Εικόνα 3.4).



Εικόνα 3.4: Session Fixation.

- **Session Sidejacking.** Ο επιτιθέμενος χρησιμοποιεί packet sniffing για να διαβάσει την κυκλοφορία δικτύου μεταξύ των δύο μερών και να κλέψει το session cookie. Πολλές ιστοσελίδες χρησιμοποιούν κρυπτογράφηση SSL κατά την διαδικασία του login, ώστε να αποτρέψουν τους εισβολείς από το να δουν τον κωδικό πρόσβασης, αλλά δεν χρησιμοποιούν κρυπτογράφηση για το υπόλοιπο site μόλις επικυρωθεί. Αυτό επιτρέπει στον επιτιθέμενο, να διαβάσει την κίνηση του δικτύου και να υποκλέψει όλα τα δεδομένα που υποβάλλονται στον server ή από τις ιστοσελίδες που προβλήθηκαν στον client.

    1. Πρώτα ο εισβολέας χρησιμοποιεί network sniffer για να συλλάβει ένα έγκυρο Session ID (Εικόνα 3.5).

Εικόνα 3.5: Υποκλοπή Session ID με την χρήση network sniffer.

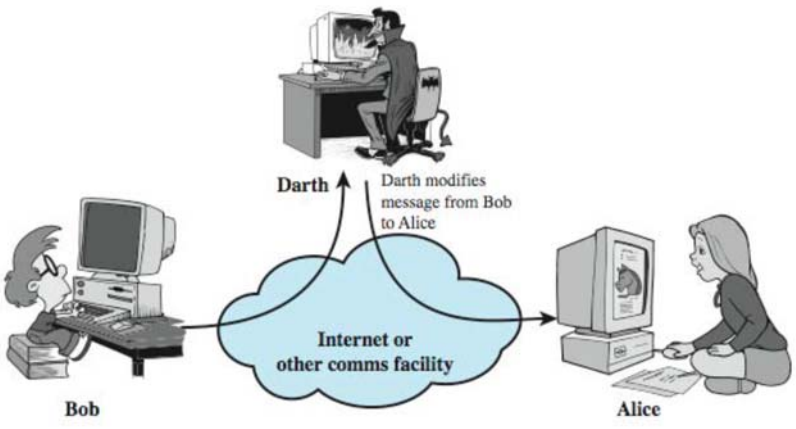
    2. Τώρα μπορεί να χειριστεί το token session για να αποκτήσει πρόσβαση στο Web Server (Εικόνα 3.6).

Εικόνα 3.6: Απόκτηση πρόσβασης στο Web server μετά από υποκλοπή ενός Session ID.

- **Cross-Site Scripting.** Ο εισβολέας μπορεί να θέσει σε κίνδυνο το session token με τη χρήση κακόβουλου κώδικα ή προγραμμάτων που εκτελούνται στην πλευρά του πελάτη. Εάν ο επιτιθέμενος στείλει ένα link στο θύμα με κακόβουλο κώδικα π.χ. JavaScript, όταν το θύμα κάνει κλικ στο link, το JavaScript θα εκτελεστεί.

- **Επίθεση Man-in-the-Middle.** Η συγκεκριμένου τύπου επίθεση είναι δύσκολο να πραγματοποιηθεί, είναι όμως πολύ αποτελεσματική όταν επιτευχθεί. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών (π.χ υπολογιστή-εξυπηρετητή) και στη συνέχεια ελέγχει τη ροή επικοινωνίας όπου μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.

  Όπως φαίνεται στην Εικόνα 3.7, ο Darth παρεμβαίνει μεταξύ της επικοινωνίας του Bob και της Alice υποκλέπτοντας αρχικά τα πακέτα δεδομένων του Bob, τα τροποποιεί και τα αποστέλλει στον αρχικό τους προορισμό, την Alice. Η Alice αγνοεί το γεγονός ότι τα πακέτα έχουν τροποποιηθεί και ότι προέρχονται από τον Darth.



Εικόνα 3.7: Επίθεση man-in-the-middle.

Για αποφυγή των επιθέσεων Man-in-theMiddle και για την διασφάλιση της εμπιστευτικότητας στην επικοινωνία μεταξύ μερών, η χρήση της κρυπτογραφίας ή/και της αυθεντικοποίησης είναι επιβεβλημένη. [1,4]

Κεφάλαιο 4
Αξιολόγηση Επισφαλών Σημείων

Το σύγχρονο διαδικτυακό περιβάλλον μπορεί να χαρακτηριστεί ως μια εμπόλεμη ζώνη, όπου ο έλεγχος κάθε δικτυωμένου συστήματος, χωρίς την βοήθεια αυτοματοποιημένων εργαλείων δεν είναι πλέον εφικτός. Τα λειτουργικά συστήματα, τα λογισμικά καθώς και τα πρωτόκολλα επικοινωνίας, έχουν εξελιχθεί σε περίπλοκες οντότητες, την τελευταία δεκαετία, όπου η ενασχόληση για την διατήρηση της ασφάλειας τους, αποτελεί μια πλήρη εργασία για ένα άτομο ή ομάδα ατόμων.

Για την καταπολέμηση των επιθέσεων, ο διαχειριστής δικτύου χρειάζεται τα κατάλληλα εργαλεία και την γνώση για να προσδιορίσει τα τρωτά σημεία, στα διάφορα συστήματα και να επιλύσει τα προβλήματα ασφαλείας τους, προτού μπορέσουν να χρησιμοποιηθούν από κάποιο εισβολέα. Ένα από τα ισχυρότερα εργαλεία το οποίο είναι διαθέσιμο σήμερα είναι η **Αξιολόγηση Ευπαθειών** ή αλλιώς η **Εκτίμηση Τρωσιμότητας**.

Η Αξιολόγηση Ευπαθειών (Vulnerability Assesment) είναι η διαδικασία κατά την οποία γίνεται αναγνώριση, ποσολόγηση και προτεραιοποίηση των ευπαθειών ενός συστήματος. Παρόλο που υπάρχουν πολυάριθμα εργαλεία τα οποία μπορούν να αξιοποιηθούν για το σκοπό αυτό και τα

οποία μπορεί να χρησιμοποιούν διαφορετικές μεθόδους για τον εντοπισμό των ευπαθειών, εντούτοις όλα δίνουν το ίδιο αποτέλεσμα, μια έκθεση ευπαθειών. Η έκθεση αυτή παρέχει ένα στιγμιότυπο όλων των προσδιορισμένων ευπαθειών ενός δικτύου την δεδομένη στιγμή. Τα συστατικά της έκθεσης περιλαμβάνουν συνήθως ένα κατάλογο ο οποίος απαριθμεί κάθε ανευρεθέν ευπάθεια, πού έχει εντοπιστεί αυτή η ευπάθεια, πιο πιθανό κίνδυνο εμπεριέχει η μη αντιμετώπισή της και πως μπορεί να επιλυθεί.

4.1 Προβλήματα Ασφαλείας

Η συχνότητα των επιθέσεων τα τελευταία χρόνια, καθώς και η ταχύτητα και η εξάπλωση τους καταδεικνύουν την ύπαρξη σοβαρών ευπαθειών στα δίκτυα ηλεκτρονικών υπολογιστών. Δεν υπάρχει κάποιος οριστικός κατάλογος όλων των ευπαθειών των συστημάτων αυτών. Πολλοί μελετητές και γραφεία αναφοράς συμβάντων ασφαλείας, έχουν στρέψει την προσοχή τους όχι σε ένα αλλά σε περισσότερους παράγοντες οι οποίοι συμβάλλουν σε αυτά τα προβλήματα ασφαλείας και θέτουν εμπόδια στις λύσεις ασφάλειας.

Ανάμεσα στις πιο συχνά αναφερθέντες πηγές των προβλημάτων ασφαλείας στα δίκτυα ηλεκτρονικών υπολογιστών είναι τα σχεδιαστικά λάθη, η ελλιπής διαχείριση της ασφάλειας, η μη ορθή και ελλιπής εφαρμογή, οι ευπάθειες των τεχνολογιών διαδικτύου, η φύση της δραστηριότητας των εισβολέων, η αδυναμία διόρθωσης των ευπαθών συστημάτων, η ανεπάρκεια της αποτελεσματικότητας των λύσεων αντιμετώπισης και η προφορική χειραγώγηση ατόμων (Social Engineering).

- **Σχεδιαστικά λάθη.** Τα δύο κύρια συστατικά ενός ηλεκτρονικού υπολογιστή, το λογισμικό και το υλικό, παρουσιάζουν αρκετά συχνά σχεδιαστικά λάθη. Συγκρίνοντας αυτά τα δύο συστατικά μέρη, θα μπορούσαμε να πούμε ότι το υλικό παρουσιάζει λιγότερα σχεδιαστικά λάθη σε αντίθεση με το λογισμικό αντίστοιχο του μέρος, μιας και παρουσιάζει λιγότερη πολυπλοκότητα. Αυτή τους η διαφορά καθιστά το υλικό μέρος πιο εύκολο στον έλεγχο. Επίσης ο έλεγχος είναι πιο εύκολος από το λογισμικό μέρος λόγου του περιορισμένου αριθμού εισόδων και αναμενόμενων εξόδων, καθώς και η μακρά ιστορία υλοποίησης μηχανικού εξοπλισμού. Παρόλα όμως τα θετικά στοιχεία του υλικού μέρους, εντούτοις, λόγο της πολυπλοκότητας των σημερινών υπολογιστικών συστημάτων, τα σχεδιαστικά λάθη είναι κάτι το συνηθισμένο.

Το μεγαλύτερο όμως πρόβλημα στην ασφάλεια των συστημάτων αποτελούν τα σχεδιαστικά λάθη στο λογισμικό συστατικό. Υπάρχουν τρείς κύριοι παράγοντες οι οποίοι έχουν την μερίδα το λέοντος στα σχεδιαστικά αυτά λάθη: ο ανθρώπινος παράγοντας, η πολυπλοκότητα του λογισμικού και οι αξιόπιστες πηγές λογισμικού.

- **Ανθρώπινος Παράγοντας.** Η απροσεξία, η συνεχής πίεση για παράδοση έτοιμου προϊόντος, η υπερ-βεβαιότητα και η χρήση κώδικα ο οποίος δεν έχει προηγουμένως ελεγχθεί, οι κακόβουλοι προγραμματιστές, οι οποίοι εισάγουν κακόβουλο κώδικα σε νόμιμα προγράμματα, καθώς και η παράβλεψη συγκεκριμένων ελέγχων, αποτελούν τον ανθρώπινο παράγοντα στην κατηγορία των προβλημάτων ασφαλείας που έγκειται στα σχεδιαστικά λάθη.

- **Πολυπλοκότητα Λογισμικού.** Σε αντίθεση με τον προγραμματισμό του υλικού μέρους ενός συστήματος, στο λογισμικό μέρος δεν μπορείς να είσαι ποτέ βέβαιος ποιο θα είναι το αποτέλεσμα σε μια πιθανή είσοδο πληροφοριών. Επιπρόσθετα δεν θα είναι ποτέ δυνατό να εντοπιστούν όλα τα λάθη σε κάποιο λογισμικό, μιας και τα δεδομένα ελέγχου δεν θα είναι ποτέ αρκετά.

  Η ευκολία με την οποία κάποιος μπορεί να προγραμματίσει σήμερα χωρίς πολλές γνώσεις, ενθαρρύνει αρκετό κόσμο με ελάχιστη εκπαίδευση στον τομέα αυτό, να ασχοληθεί με τον προγραμματισμό. Οι πλειοψηφία όμως αυτών των εν δυνάμει προγραμματιστών, δεν γνωρίζουν για τις ορθές πρακτικές οι οποίες θα πρέπει να ακολουθούνται κατά τον σχεδιασμό και την υλοποίηση ενός λογισμικού.

- **Λογισμικό από αξιόπιστες πηγές.** Είναι ελάχιστες οι πηγές λογισμικού μου μπορούν να θεωρούνται αξιόπιστες. Υπάρχει ένας μεγάλος αριθμός εταιρειών οι οποίες ανοίγουν και σε λίγα χρόνια κλείνουν αφήνοντας έτσι εκτεθειμένους τους πελάτες που τους έχουν επιστεφτεί. Οι πλειοψηφία των πελατών, από την άλλη, δεν ψάχνουν να δουν την ποιότητα του λογισμικού που αγοράζουν, ούτε τους ενδιαφέρει η αξιοπιστία της εταιρείας με την οποία θα συνεργαστούν, φτάνει το λογισμικό να κάνει αυτά που ζητούν.

  Έχει επίσης παρατηρηθεί το φαινόμενο ότι όσο ένα λογισμικό γίνεται αναγνωρίσιμο, τόσο οι μελλοντικές του εκδόσεις υστερούν σε έλεγχο, μεταφέροντας έτσι προβλήματα προηγούμενων εκδόσεων του.

Η αύξηση του λογισμικού ανοικτού κώδικα, τα τελευταία χρόνια, ως αντιστάθμισμα στις υψηλές τιμές αντίστοιχων λογισμικών και η στροφή των καταναλωτών προς αυτή την κατεύθυνση, έχει εγείρει αρκετά ερωτήματα ως προς την αξιοπιστία και την ασφάλειά τους. Έχει παρατηρηθεί μια αύξηση της προσθήκης δούρειων ίππων σε λογισμικά ανοικτού κώδικα, που δεν αφήνουν ανεπηρέαστα ούτε τα δημοφιλή και αξιόπιστα Unix, Linux και Mac OSX στα οποία τρέχουν συνήθως αυτού του τύπου λογισμικά.

- **Ελλιπής διαχείριση της ασφάλειας.** Η διαχείριση της ασφάλειας είναι τόσο τεχνική όσο και διοικητική διαδικασία, η οποία περιλαμβάνει τις πολιτικές ασφαλείας και τους ελέγχους που ένας οργανισμός αποφασίζει να βάλει σε ισχύ, για να παρέχει το απαραίτητο επίπεδο προστασίας . Επιπλέον περιλαμβάνει τον έλεγχο ασφάλειας και την αξιολόγηση της αποτελεσματικότητας των πολιτικών αυτών. Ο αποτελεσματικότερος τρόπος για να επιτευχθούν αυτοί οι στόχοι είναι η εφαρμογή αξιολόγησης του ρίσκου ασφαλείας, μέσω της ανάλογης πολιτικής ασφαλείας και να εξασφαλιστεί η πρόσβαση στους πόρους του δικτύου, μέσο της χρήσης τοίχων προστασίας (Firewall) και ισχυρού συστήματος κρυπτογραφίας.

  Η ελλιπής διαχείριση της ασφάλειας είναι αποτέλεσμα ελλιπούς ελέγχου της εφαρμογής, διοίκησης και επίβλεψης αυτής. Για να είναι αποτελεσματική η εφαρμογή της ασφάλειας σε ένα οργανισμό, η οποία θα του επιτρέψει να προστατεύσει όσο το δυνατό καλύτερα τους πόρους του, θα πρέπει να έχει σε ισχύ τα παρακάτω:

  - **Ανάλυση Κινδύνου.** Η ανάλυση κινδύνου θα αναγνωρίσει τους πόρους και τις απειλές αυτών και θα υπολογίσει το κόστος της ζημίας, εάν μια τέτοια απειλή πραγματοποιηθεί. Τα αποτελέσματα της ανάλυσης αυτής θα βοηθήσουν την διεύθυνση του οργανισμού στη σύσταση του προϋπολογισμού για την προστασία αυτών των πόρων, καθώς και την δημιουργία και εφαρμογή πολιτικών ασφαλείας.

  - **Πολιτικές Ασφαλείας.** Οι πολιτικές και διαδικασίες ασφαλείας οι οποίες δημιουργούν, εφαρμόζουν και επιβάλλουν τα θέματα ασφαλείας στους τεχνολογικούς και στους ανθρώπινους πόρους.

- **Πρότυπα και οδηγίες.** Τα πρότυπα και οι οδηγίες θα οδηγήσουν στην ανεύρεση εκείνων των τρόπων, αυτοματοποιημένων και μη, που θα επιβάλουν την δημιουργία, την ενημέρωση και την συμμόρφωση στις πολιτικές ασφαλείας σε όλο τον οργανισμό.

- **Ταξινόμηση Πληροφοριών.** Η ταξινόμηση πληροφοριών θα βοηθήσει στην διαχείριση της ανεύρεσης, του προσδιορισμού και της μείωσης των ευπαθειών των συστημάτων με την καθιέρωση της διαμόρφωσης της ασφάλειας.

- **Έλεγχος Ασφάλειας.** Ο έλεγχος ασφάλειας θα πρέπει να διεξάγεται για την αποτροπή και ανίχνευση τυχών παρείσφρησης . Επίσης θα πρέπει να διεξάγεται έλεγχος των αρχείων καταγραφής συμβάντων, καθώς επίσης και η φύλαξη αυτών για μελλοντική ανάλυσή της τάσης συγκεκριμένων γεγονότων. Θα πρέπει να γίνεται έλεγχος τρεχόντων συμβάντων ασφαλείας, καθώς επίσης και έλεγχος των διαφόρων συστημάτων καταγραφής γεγονότων τα οποία είναι συνδεδεμένα με τείχους προστασίας.

- **Εκπαίδευση.** Η εκπαίδευση κάνει το κάθε υπάλληλο του οργανισμού να αντιληφθεί πόσο σημαντική είναι η ασφάλεια και να του διδάξει την δική του ευθύνη στην διατήρηση αυτής.

- **Μη ορθή και ελλιπής εφαρμογή.** Αρκετά προβλήματα ασφαλείας προκύπτουν από την μη ορθή ή/και ελλιπή εφαρμογή τόσο του υλικού όσο και του λογισμικού συστήματος, επηρεάζοντας έτσι την αξιοπιστία τους.

  Το πρόβλημα αυτό προκύπτει συνήθως από τις αλλαγές οι οποίες γίνονται στις διεπαφές (Interface) των συστημάτων, που μπορούν να οδηγήσουν σε ασυμβατότητα και στο τέλος σε μη ορθή και ελλιπής εφαρμογή. Εάν λόγου χάρη, γίνει μια απλή συνηθισμένη αλλαγή στον κώδικα ενός συστήματος, αυτή μπορεί να έχει ως αποτέλεσμα την μην ορθή λειτουργία της διεπαφής του συστήματος αυτού. Η λανθασμένη λειτουργία της διεπαφής αυτής, μπορεί να προκαλέσει προβλήματα στην επικοινωνία του συστήματος με άλλα συστήματα, που μέχρι εκείνη τη δεδομένη στιγμή ήταν απερίσπαστη.

  Τα προβλήματα επικοινωνίας και μη συμβατότητας των διεπαφών μπορεί να προκύψουν για ένα ή περισσότερους από τους πιο κάτω λόγους:

- Προϋπάρχουσα κακή επικοινωνία κατά τον σχεδιασμό.
- Επιλογή λογισμικού ή υλικού παράγοντα διεπαφής, χωρίς πρώτα να γίνει κατανοητή η διαδικασία εισαγωγής δεδομένων στο λογισμικό αποδοχής.
- Η άγνοια σε ζητήματα συνεργασίας συστημάτων.
- Λάθη κατά την χειροκίνητη καταχώρηση δεδομένων.
- Η μη πλήρης κατανόηση των ζητούμενων.
- Η υπερβολική λεπτομέρεια.

- **Ευπάθειες των τεχνολογιών διαδικτύου.** Η ραγδαία ανάπτυξη της τεχνολογίας υλικού και επικοινωνιών και η ευρεία αποδοχή τους από τον κόσμο έχει επιστήσει την προσοχή, στους ειδικούς για θέματα ασφαλείας, για τις παρενέργειας αυτής της ανάπτυξης. Η τεχνολογία του διαδικτύου εξακολουθεί να έχει ευπάθειες τόσο στο υλικό όσο και στο λογισμικό της μέρος.

  Η χρήση των τεχνολογιών αυτών γίνεται από πολλούς, που στην πλειοψηφία τους έχουν άγνοια περί ασφάλειας. Έτσι εάν μια αδυναμία γίνει αντιληπτή λόγω αυτής της άγνοιας, δεν θα μπορούν να την αναγνωρίσουν και να την κατατάξουν ως αδυναμία και αν την αναγνωρίσουν, το πιο πιθανό είναι ότι δεν θα ξέρουν σε ποιον θα πρέπει να την αναφέρουν.

  Κανένας δεν μπορεί να πει πόσες ευπάθειες υπάρχουν, τόσο σε υλικό όσο και σε λογισμό επίπεδο. Μια εκτίμηση θα μπορούσε να πει ότι υπάρχουν χιλιάδες, όπου καθημερινά ανακαλύπτονται από τους χάκερς.

  Παρόλο που οι ευπάθειες εντοπίζονται τόσο στο υλικό όσο και στο λογισμικό μέρος, οι πλειοψηφία αυτών εντοπίζεται στο λογισμικό . Τις ευπάθειες του λογισμικού μέρους μπορούμε να τις ταξινομήσουμε σε τέσσερεις κατηγορίες:

  - **Ευπάθειες λειτουργικού συστήματος.** Αποτελούν την πλειοψηφία των ανευρεθέν ευπαθειών.

- **Ευπάθειες θυρών (Ports).** Βρίσκονται στην δεύτερη θέση στην κατηγορία των ευπαθειών. Το "κλείσιμο" των ευπαθών θυρών δικτύου και των θυρών οι οποίες δεν χρησιμοποιούνται, με την χρήση τείχους προστασίας, αποτελεί ένα επιπλέων μέτρο στην επιβολή της ασφάλειας στο δίκτυο. Θα πρέπει όμως να γίνεται έλεγχος τόσο των ανοικτών όσο και των κλειστών θυρών, καθώς οι εισβολείς μπορούν να βρουν κάποιο άλλο τρόπο και να παρακάμψουν αυτό το μέτρο ασφαλείας.

- **Σφάλματα λογισμικού**.

- **Ευπάθειες στα πρωτόκολλα επικοινωνίας λογισμικού.** Όπως λόγου χάρη ευπάθειες στα πρωτόκολλα επικοινωνίας μεταξύ εξυπηρετητή και πελάτη μέσο ενός προγράμματος περιήγησης (Web Browser).

- **Φύση της δραστηριότητας των εισβολέων.** Όσο εξελίσσεται η τεχνολογία προσφέροντας περισσότερες εμπειρίες στον τελικό χρήστη, άλλο τόσο εξελίσσονται και τα εργαλεία τα οποία χρησιμοποιούν οι εισβολείς. Υπάρχουν μάλιστα φορές, που η τεχνολογία των εισβολέων, φαίνεται να εξελίσσεται πιο γρήγορα από την τεχνολογία της αγοράς.

  Παλαιότερα χρειαζόταν ευφυΐα, αποφασιστικότητα, ενθουσιασμό και επιμονή για να γίνει κάποιος χάκερ. Στην σημερινή εποχή το μόνο που χρειάζεται είναι μια καλή μηχανή αναζήτησης, χρόνο, μια κάποια γνώση για το τι προτίθεται να κάνει και η κατοχή ενός υπολογιστή ή μιας κινητής συσκευής με πρόσβαση στο διαδίκτυο. Υπάρχουν χιλιάδες σελίδες χάκερ με εργαλεία και οδηγούς, από το πώς μπορεί κάποιος να πραγματοποιήσει μια επίθεση εκμεταλλευόμενος κάποια ευπάθεια ενός συστήματος, μέχρι το πώς να δημιουργήσει ένα ιό.

  Η ταχύτητα εξάπλωσης των ιών, από την στιγμή που θα σταλούν μέσο διαδικτύου, μέχρι την στιγμή που θα εγκατασταθούν σε κάποιο ευπαθή σύστημα, έχει αυξηθεί δραματικά. Μειώνοντας έτσι παράλληλα και τον χρόνο ανταπόκρισης των υπεύθυνων ασφαλείας, στην λήψη μέτρων. Μέχρι να παρθούν τα μέτρα (δημιουργία και εγκατάσταση επιδιορθώσεων) η ζημία έχε ήδη γίνει και εξαπλώνεται.

- **Αδυναμία διόρθωσης των ευπαθών συστημάτων.** Η αδυναμία αυτή προκύπτει από τον αυξανόμενο αριθμό των ευπαθειών των συστημάτων και τη αδυναμία των διαχειριστών να ανταποκριθούν στην διαχείριση των επιδιορθώσεων (Patches) όλων αυτών των συστημάτων τα οποία έχουν υπό την επίβλεψή τους. Οι επιδιορθώσεις αυτές κάποιες φορές είναι δύσκολο να εφαρμοστούν και κάποτε δημιουργούν προβλήματα συμβατότητας με απρόβλεπτες συνέπειες.

  Επιπρόσθετα, η επικοινωνία μεταξύ του προμηθευτή και του διαχειριστή του συστήματος το οποίο χρήζει επιδιορθώσης, μπορεί να μην είναι η ιδανική. Κάποιοι προμηθευτές διαθέτουν τις επιδιορθώσεις τους στην ιστοσελίδα τους, άλλοι στέλλουν ειδοποιήσεις μέσο ηλεκτρονικού ταχυδρομείου. Λόγο φόρτου εργασίας και μειωμένου ή ακόμη ανύπαρκτου εξειδικευμένου προσωπικού ασφαλείας, οι επιδιορθώσεις αυτές μπορεί να γίνουν μετά από μέρες, μήνες ή χρόνια ή ακόμη να μην γίνουν και ποτέ.

- **Ανεπάρκεια της αποτελεσματικότητας των λύσεων αντιμετώπισης.** Ο μεγάλος αριθμός των ευπαθειών που παρουσιάζουν στα λογισμικά προγράμματα έχει καταστήσει την ανεύρεση και διαχείρισή τους ένα εξαιρετικά δύσκολο έργο, που μόνο οι καλά στελεχωμένοι οργανισμοί μπορούν να διαχειρισθούν τις επιδιορθώσεις τους.

  Οι περισσότερες επιθέσεις γίνονται πλέον αυτοματοποιημένα μειώνοντας έτσι το χρόνο ανταπόκρισης και αντιμετώπισης τους. Επιπλέον η εξάρτηση των χρηστών αλλά και των εργαλείων που χρησιμοποιούν με το διαδίκτυο, μπορούν από μια μικρού μεγέθους επίθεση, να επηρεαστούν και να υποστούν μεγάλες και κάποιες φορές ανεπανόρθωτες ζημιές.

  Παρόλο που έχουν επινοηθεί και εφαρμοστεί διάφορες λύσεις, άλλες καλές και άλλες όχι και τόσο καλές, για την αντιμετώπιση των επιθέσεών και την ανεύρεση των διαφόρων λογισμικών και υλικών ευπαθειών, εντούτοις το πρόβλημα παραμένει μεγάλο και άλυτο. Για την ακρίβεια ένα μεγάλο πρόβλημα ασφαλείας είναι να εντοπιστεί και να εφαρμοστεί η κατάλληλη λύση μεταξύ χιλιάδων λύσεων, για τις εξειδικευμένες ανάγκες του περιβάλλοντος ενός οργανισμού ή μιας εταιρείας.

- **Προφορική χειραγώγηση ατόμων (Social Engineering).** Είναι ίσως η δυσκολότερα αντιμετωπίσιμη ευπάθεια, αφού στηρίζεται κυρίως στην ανθρώπινη περιέργεια, στην

άγνοια και στην ελλιπή εκπαίδευση. Συνήθως αυτός που την εφαρμόζει δεν βρίσκεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά.

4.2 Εκτίμηση Τρωσιμότητας

Η εκτίμηση τρωσιμότητας αποτελεί την διαδικασία εντοπισμού και αναφοράς ευπαθειών ενός συστήματος (λογισμικού ή/και υλικού). Μια από τις συνήθεις χρήσεις της εκτίμησης τρωσιμότητας είναι η ικανότητά της να επικυρώσει τα μέτρα ασφαλείας που έχουν ληφθεί. Εάν για παράδειγμα έχει γίνει πρόσφατα η εγκατάσταση ενός καινούργιου συστήματος ανίχνευσης προσπέλασης (IDS), η εκτίμηση τρωσιμότητας θα εκτιμήσει πόσο καλά δουλεύει το σύστημα αυτό.

Η εκτίμηση τρωσιμότητας έχει γίνει ένα χρήσιμο συστατικό των υποδομών ασφαλείας πολλών οργανισμών και επιχειρήσεων. Με την ανεύρεση μιας καινούργιας ευπάθειας ο διαχειριστής μπορεί να προβεί σε μια εκτίμηση τρωσιμότητας για να αξιολογήσει την κατάσταση των υπό διαχείριση συστημάτων, να ανακαλύψει πια από αυτά είναι τρωτά και να αρχίσει την διαδικασία επιδιόρθωσης. Μετά την εγκατάσταση του αρχείου επιδιόρθωσης μπορεί να επαναλάβει την διαδικασία εκτίμησης τρωσιμότητας για να επιβεβαιωθεί ότι η ευπάθεια δεν υφίσταται πλέον.

Η διαδικασία **εκτίμηση τρωσιμότητας ->επιδιόρθωση->επανεκτίμηση τρωσιμότητας**, έχει γίνει κοινή πρακτική για πολλούς οργανισμούς, όσο αφορά την διαχείριση των θεμάτων ασφαλείας τους. Πολλοί οργανισμοί έχουν επίσης εντάξει την διαδικασία αυτή κατά την εισαγωγή καινούργιων συστημάτων ή εξυπηρετητών. Πριν την εγκατάσταση ενός καινούργιου εξυπηρετητή θα πρέπει πρώτα να αξιολογηθεί από το σύστημα εκτίμησης τρωσιμότητας και στην συνέχεια, εάν δεν έχει εντοπιστεί οτιδήποτε, προχωρεί η διαδικασία εγκατάστασης του στο δίκτυο του οργανισμού. Εάν εντοπιστεί κάποια ευπάθεια, τότε η διαδικασία εκτίμηση τρωσιμότητας ->επιδιόρθωση->επανεκτίμηση τρωσιμότητας, λαμβάνει χώρα μέχρι ο εξυπηρετητής να πάρει το πράσινο φως.

Επιπρόσθετα ένα εργαλείο εκτίμησης τρωσιμότητας μπορεί να χρησιμοποιηθεί και σαν εργαλείο δημιουργίας καταλόγου των συστημάτων και των υπηρεσιών που βρίσκονται στο δίκτυο ενός οργανισμού. Γνωρίζοντας, λόγου χάρη, πόσοι και ποιού τύπου εκτυπωτές υπάρχουν διαθέσιμοι στο δίκτυο, μπορεί να βοηθήσει στον προγραμματισμό των πόρων. Επίσης γνωρίζοντας πόσα Windows XP είναι ακόμη διαθέσιμα, μπορεί να γίνει ο προγραμματισμός για αναβάθμισή τους.

Τα εργαλεία εκτίμησης τρωσιμότητας είναι επίσης σε θέση να ανιχνεύσουν παραβιάσεις εταιρικών πολιτικών. Πολλά από αυτά τα εργαλεία θα ανιχνεύσουν και θα παρουσιάσουν την ύπαρξη παράνομων αρχείων, τα οποία παραβιάζουν τα πνευματικά δικαιώματα και τα οποία μοιράζονται σε δικτυακούς κοινόχρηστους φακέλους, επίσης μπορεί να ανιχνεύσει την ύπαρξη μην εγκεκριμένων εργαλείων εξ' αποστάσεως πρόσβασης. Στην περίπτωση που κάποιος διαχειριστής συστημάτων φύγει από τον οργανισμό μπορεί να διεξαχθεί μια εκτίμηση τρωσιμότητας για να διαφανεί εάν έχει αφεθεί κάποια κερκόπορτα ανοιχτή στον τοίχο προστασίας. Εάν ακόμη υπάρξει μια ξαφνική μείωση στην ταχύτητα της γραμμής διαδικτύου, το εργαλείο εκτίμησης τρωσιμότητας θα μπορεί να ανιχνεύσει εάν κάποιος/οι υπολογιστές έχουν εγκαταστήσει παράνομα κάποιο λογισμικό διανομής αρχείων.

Μια από τις σημαντικότερες χρήσεις των εργαλείων εκτίμησης τρωσιμότητας είναι όταν στην περίπτωση που προκύψει παρείσφρηση, ο διαχειριστής έχοντας μια πρόσφατη κατάσταση των τρωτών σημείων των συστημάτων, μπορεί να συμπεράνει πως έχει γίνει αυτή η παρείσφρηση και ποία άλλα περιουσιακά στοιχεία έχουν επίσης πιθανός επηρεαστεί.

4.2.1 Είδη Εκτιμήσεων Τρωσιμότητας

Υπάρχουν διαφορετικοί τύποι εκτίμησης της τρωσιμότητας ενός συστήματος. Η μονομερής εκτίμηση τρωσιμότητας ενός συστήματος (Host Assessment) προϋποθέτει την χρήση ειδικευμένων εργαλείων και ένα λογαριασμό χρήστη με δικαιώματα διαχειριστή στο συγκεκριμένο σύστημα. Από την άλλη πλευρά η εκτίμηση τρωσιμότητας δικτύου (Network Assessment) χρησιμοποιείται για να ελεγχθεί η ασφάλεια των δικτυακών συστημάτων ως σύνολο. [02]

1. **Εκτίμηση τρωσιμότητας Τερματικού συστήματος - Host Assessment.** Τα εργαλεία εκτίμησης τρωιμότητας τερματικού συστήματος προϋποθέτουν την εγκατάσταση του συστήματος ελέγχου σε κάθε σύστημα το οποίο θα αξιολογηθεί. Το σύστημα ελέγχου, ανάλογος του είδους του, θα μπορεί να εκτιμήσει την τρωσιμότητα για ένα μόνο σύστημα ή να συνδεθεί με ένα κεντρικό σύστημα όπου θα συγκεντρωθούν όλες οι εκτιμήσεις των συστημάτων ενός δικτύου.

   Τα συστήματα αυτά ψάχνουν για ευπάθειες, όπως την απουσία συγκεκριμένων αρχείων επιδιόρθωσης (Patches), την μη τήρηση πολιτικών ασφαλείας, την ύπαρξη αρχείων με

λανθασμένα καταχωρημένα δικαιώματα πρόσβασης, την πιθανή ύπαρξη κερκόπορτας, καθώς και την ύπαρξη αρχείων τύπου δούρειος ίππος.

Η εις βάθος εκτίμηση που διεξάγεται από αυτού του τύπου τα εργαλεία τα καθιστούν ως την συνιστώμενη μέθοδο εκτίμησης τρωσιμότητας κρίσιμων συστημάτων. Το μειονέκτημα των συστημάτων αυτών είναι ότι απαιτούν την χρήση εξειδικευμένων εργαλείων, τόσο για το λειτουργικό σύστημα, όσο και για τα λογισμικά τα οποία βρίσκονται εγκατεστημένα στο υπό εξέταση τερματικό σύστημα. Επιπρόσθετα ο χρόνος τον οποίο χρειάζονται για να διεξάγουν την εκτίμηση, καθώς επίσης και η περιορισμένη τους εξελιξιμότητα, καθιστούν την χρήση των εργαλείων εκτίμησης τρωσιμότητας τερματικού συστήματος διαθέσιμη μόνο για ορισμένα κρίσιμα συστήματα.

Λόγο της ανάγκης εξελιξιμότητας των συστημάτων αυτών, για την εφαρμογή τους σε μεγάλα δίκτυα υπολογιστών με όσο το δυνατό λιγότερα διαχειριστικά κόστη, έχουν μεταλλάξει τα συστήματα από τερματικά σε συστήματα παράγοντα (Agent-Based Systems), τα οποία χρησιμοποιούν ένα κρατικοποιημένο σύστημα διαχείρισης και εξαγωγής καταστάσεων εκτίμησης.

2. **Εκτίμηση τρωσιμότητας Δικτύου - Network Assessment.** Η εκτίμηση τρωσιμότητας δικτύου ανιχνεύει όλα τα ενεργά συστήματα ενός δικτύου και ποιες υπηρεσίες χρησιμοποιούν και στην συνέχεια αναλύει αυτές τις υπηρεσίες για εύρεση πιθανών ευπαθειών.

   Σε αντίθεση με την εκτίμηση τρωσιμότητας τερματικού συστήματος, η διαδικασία αυτή δεν προϋποθέτει οποιεσδήποτε αλλαγές διαμόρφωσης στο σύστημα το οποίο υπόκειται τον έλεγχο. Η εκτίμηση τρωσιμότητας δικτύου μπορεί να είναι εξελικτική αλλά και αποδοτική από διαχειριστικής απόψεως και είναι η μόνη εφικτή μέθοδος διαχείρισης της ασφάλειας μεγάλων και σύνθετων δικτύων τα οποία αποτελούνται από διάφορα ετερογενή συστήματα.

   Τα συστήματα εκτίμησης τρωσιμότητας δικτύου είναι αρκετά αποτελεσματικά όσο αφορά την ανεύρεση ευπαθειών, ωστόσο έχουν κάποιες συγκεκριμένες αδυναμίες. Οι αδυναμίες αυτές συμπεριλαμβάνουν τις εξής: δεν μπορούν να ανιχνεύσουν συγκεκριμένου τύπου κερκόπορτες, συχνά δημιουργούνται περιπλοκές με τοίχους προστασίας, δεν μπορούν να ελέγξουν συγκεκριμένου τύπου ευπάθειες για το λόγο ότι

και η ίδια η διαδικασία του ελέγχου θεωρείτε επικίνδυνη. Τα εν λόγω συστήματα ελέγχου μπορεί να δημιουργήσουν προβλήματα στην ομαλή λειτουργία των συστημάτων ενός οργανισμού, να παρεμποδίσουν την λειτουργία σε συγκεκριμένου τύπου συσκευές, όπως λόγου χάρη τους εκτυπωτές, χρησιμοποιούν ένα μεγάλο ποσοστό του εύρους ζώνης και δημιουργούν μεγάλα αρχεία καταγραφής ενεργειών τα οποία καταναλώνουν την χωρητικότητα των δίσκων αποθήκευσης των υπό αξιολόγηση συστημάτων.

Κεφάλαιο 5
Εργαλεία Ανίχνευσης Ευπαθειών

Στο κεφάλαιο αυτό θα γίνει παρουσίαση, ανάλυση του τρόπου λειτουργίας και των χαρακτηριστικών των εργαλείων, τα οποία έχουν χρησιμοποιηθεί για την ανεύρεση των ευπαθειών στο υπό εξέταση σύστημα.

Στην συνέχεια θα καταγραφούν τα βήματα εγκατάστασης, τροποποίησης και χρήσης των εργαλείων μέχρι το τελικό στάδιο, την εξαγωγή της κατάστασης των ευπαθειών του υπό διερεύνηση συστήματος

5.1 Περιβάλλον Αξιολόγησης

Το περιβάλλον το οποίο έχει χρησιμοποιηθεί για την διεξαγωγή των ελέγχων αποτελείται από τρεις συμβατικούς υπολογιστές και ένα εικονικό.

Οι συμβατικοί υπολογιστές είναι οι εξής :

1. Kali Linux 2016.2 (Intel i5 2.5Ghz, 8GB RAM).

2. Windows 10 64bit (Intel i5 3.1Ghz, 12GB RAM).

3. Windows 7 64bit (Intel i5 3.1Ghz, 16GB RAM).

Ο εικονικός υπολογιστής ο οποίος έχει χρησιμοποιηθεί είναι το γνωστό Metasploitable της εταιρείας Rapid 7 [10]. Η εικονική αυτή μηχανή είναι μια ηθελημένα ευπαθής μηχανή με λειτουργικό Ubuntu Linux v8.0.4 Hardy και ο σκοπός δημιουργίας της από την εταιρεία Rapid 7 είναι ο έλεγχος αποδοτικότητας των διαφόρων συστημάτων ασφαλείας, καθώς και η επίδειξη κάποιον κοινών ευπαθειών. Η μηχανή που θα χρησιμοποιηθεί στη παρούσα μεταπτυχιακή διατριβή, είναι το **Metasploitable 2**, το οποίο περιέχει μεγαλύτερο αριθμό ευπαθειών από τη προηγούμενη πρώτη έκδοσή του.

Τα κριτήρια με βάση τα οποία έχει επιλεγεί το Metasploitable 2 ως η μηχανή η οποία θα υπόκειται τον έλεγχο είναι:

1. Για να αξιολογηθεί η ικανότητα εντοπισμού γνωστών, επιβεβαιωμένων ευπαθειών από τα εργαλεία ελέγχουν τρωσιμότητας.

2. Για να αποτελεί σημείο αναφοράς για την επιβεβαίωση ή μη των αποτελεσμάτων της παρούσας μεταπτυχιακής διατριβής.

Έχουν χρησιμοποιηθεί πέντε εργαλεία εντοπισμού ευπαθειών, τα οποία είναι τα εξής:

1. Zenmap/Nmap 7.25 BETA2.

2. OpenVas 8.

3. Nexpose Enterprise Edition.

4. Qualys Vulnerability Management, Cloud based.

5. SAINT 8 VM.

Τα κριτήρια με βάση τα οποία έχουν επιλεγεί τα συγκεκριμένα εργαλεία εντοπισμού ευπαθειών είναι:

- Μπορούν να προβούν σε έλεγχο εντοπισμού ευπαθειών τους περιβάλλοντος Metasploitable 2.

- Δεν υπάρχουν ιδιαίτερα απαιτητικές ανάγκες σε μηχανογραφικούς πόρους κατά την διαδικασία εγκατάστασης και λειτουργίας τους.

- Έχουν χρησιμοποιηθεί εργαλεία ανοικτού κώδικα (Nmap, OpenVas) για τα οποία υπάρχει εκτενής βιβλιογραφία και τεκμηρίωση για τον τρόπο χρήσης τους.

- Χρησιμοποιήθηκαν εμπορικά εργαλεία (Nexpose, SAINT 8 VM, Qualys) για τα οποία ήταν σχετικά εύκολη η απόκτηση άδειας χρήσης τους για περιορισμένο χρονικό διάστημα (Trial) χωρίς κάποιους λειτουργικούς περιορισμούς στα εργαλεία, που θα καθιστούσε μη αποδοτική την χρήση τους . Επιπρόσθετα η άδεια αυτή μπορούσε να παραχωρηθεί για ακαδημαϊκούς λόγους και η επέκτασή της για περισσότερο χρόνο από την περίοδο παραχώρησης της δεν αποτελούσε πρόβλημα.

Το εργαλείο OpenVas 8 έχει εγκατασταθεί στην μηχανή Kali Linux. Στην μηχανή Windows 7 έχουν εγκατασταθεί και τρέξει τα εργαλεία Zenmap/Nmap 7.25 BETA2 και Nexpose Enterprise Edition, ενώ στην μηχανή Windows 10 έχει εγκατασταθεί το εργαλείο Oracle VM Virtual Box 5.1.8 στο οποίο έχουν τρέξει οι εικονικές μηχανές Metasploitable 2, QualysGuard Virtual Scanner Appliance και SAINT 8 VM.

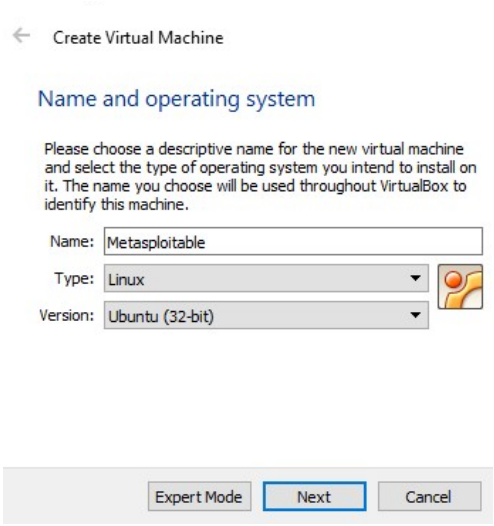
5.1.1 Εγκατάσταση Metasploitable 2

Αρχικά πριν την έναρξη της διαδικασίας εγκατάστασης του Metasploitable 2, θα προηγηθεί η διαδικασία εγκατάστασης του εργαλείου Oracle VM Virtual Box, το οποίο είναι διαθέσιμο δωρεάν από την ιστοσελίδα https://www.virtualbox.org.

Στην συνέχεια θα ακολουθήσει το κατέβασμα του Metasploitable 2 από την ιστοσελίδα https://information.rapid7.com/metasploitable-download.html, το οποίο διατίθεται επίσης δωρεάν και αφού πρώτα αποσυμπιεστεί, ακολούθως θα γίνει η φόρτωση αυτού στο Oracle VM.

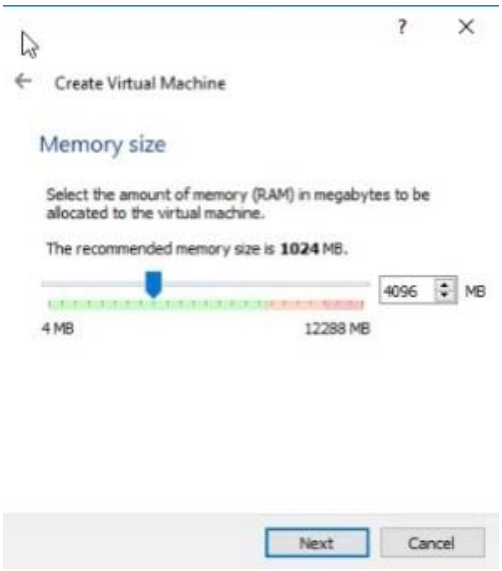
Διαδικασία Εγκατάστασης Metasploitable 2

1. Ανοίγοντας το Oracle VM, επιλέγεται το “New” όπου εδώ καταχωρούνται το όνομα της μηχανής (Metasploitable), ο τύπος του λειτουργικού συστήματος (Linux) και η έκδοση του λειτουργικού συστήματος (Ubuntu 32bit), Εικόνα 5.1.



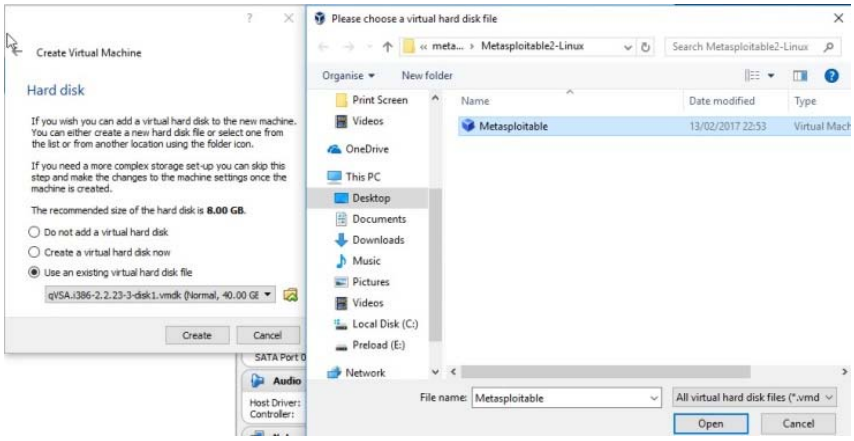
Εικόνα 5.1: Δημιουργία εικονικής μηχανής.

2. Στην συνέχεια επιλέγεται το μέγεθος της μνήμης (RAM) που επιθυμείται για την μηχανή αυτή. Η μνήμη ορίζεται στα 4096 MB, όπου θεωρείτε ικανοποιητική για το σκοπό που προορίζεται να επιτελέσει η συγκεκριμένη εικονική μηχανή, Εικόνα 5.2.



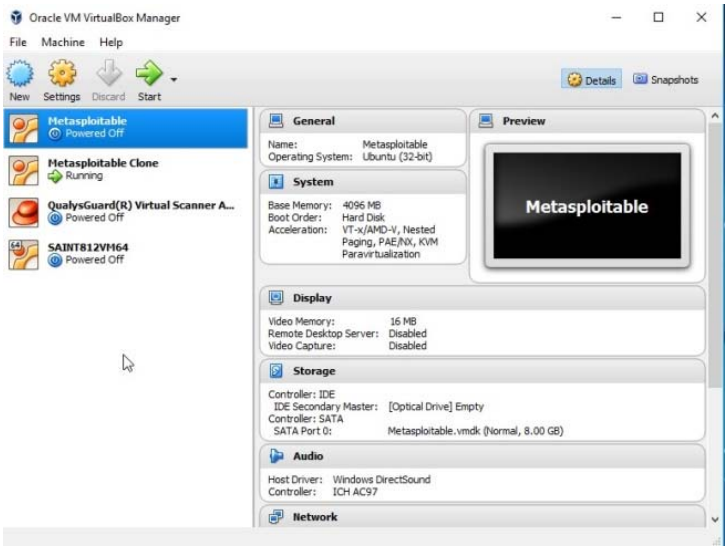
Εικόνα 5.2: Επιλογή μνήμης (RAM) για εικονική μηχανή.

3. Ακολούθως επιλέγεται ο εικονικός σκληρός δίσκος της μηχανής. Εδώ θα γίνει η επιλογή του αρχείου Metasploitable που έχει προηγούμενος αποσυμπιεστεί. Αφού πρώτα γίνει η επιλογή "Use an existing virtual hard disk file" ακολούθως επιλέγεται το εικονίδιο και στην συνέχεια το αρχείο του Metasploitable, Εικόνα 5.3.



Εικόνα 5.3: Επιλογή εικονικού δίσκου Metasploitable.

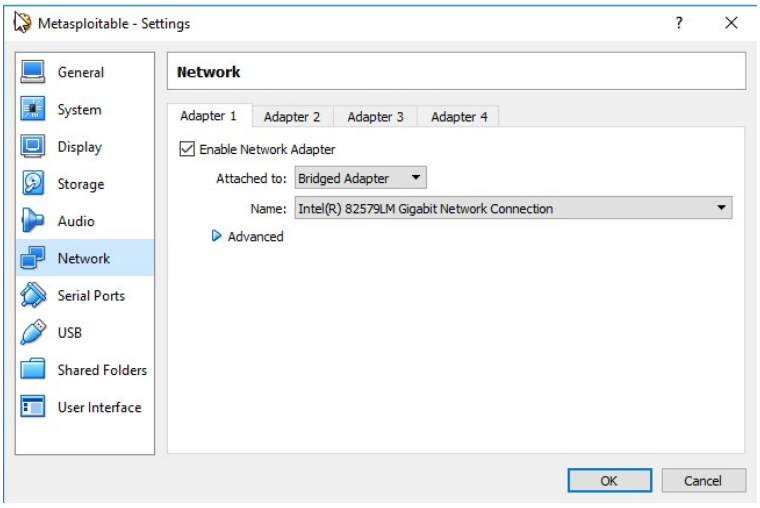
4. Η μηχανή Metasploitable έχει "φορτωθεί" στο Oracle VM, Εικόνα 5.4. Στην συνέχεια θα γίνει τροποποίηση της κάρτας δικτύου της εικονικής μηχανής . Επιλέγεται η μηχανή Metasploitable που μόλις έχει δημιουργηθεί και στη συνέχεια επιλέγεται η επιλογή "Settings".



Εικόνα 5.4: Επιλογή εικονικού δίσκου Metasploitable 2.

5. Ακολούθως επιλέγεται η επιλογή "Network". Συνίσταται η επιλογή της κάρτας να είναι "Host-only Adapter", ούτος ώστε η εικονική μηχανή να είναι απομονωμένη σε ένα

εικονικό δίκτυο προς αποφυγή πρόκλησης μη ηθελημένης ζημιάς στον υπολογιστή που την φιλοξενεί. Στην προκειμένη περίπτωση, λόγω του ότι επιθυμείται το Metasploitable να είναι διαθέσιμο στο τοπικό δίκτυο, η κάρτα επιλέγεται να είναι "Bridged Adapter", Εικόνα 5.5.



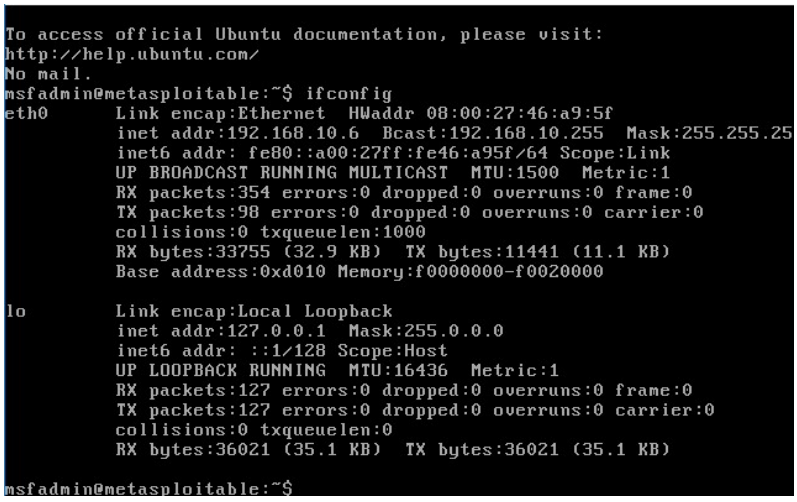
Εικόνα 5.5: Διαμόρφωση κάρτας δικτύου Metasploitable 2.

6. Μετά την τροποποίηση της κάρτας δικτύου του Metasploitable, διενεργείται η διαδικασία εκκίνησης της μηχανής και η καταχώρηση των στοιχείων αυθεντικοποίησης, Εικόνα 5.6. Τα στοιχεία αυθεντικοποίησης του διαχειριστή της εικονικής μηχανής είναι όνομα χρήστη και κωδικός πρόσβασης το "msfadmin".

Εικόνα 5.6: Αρχική οθόνη Metasploitable 2.

7. Για την ανάκτηση της IP της εικονικής μηχανής γίνεται αυθεντικοποίηση και στην συνέχεια εκτελείται η εντολή "ifconfig". Το IP που έχει η μηχανή θα χρησιμοποιείται κατά την τροποποίηση των εργαλείων ανίχνευσης ευπαθειών. Το IP αυτό ενδεχομένως να

αλλάζει κατά την χρονική στιγμή που θα χρησιμοποιείται το κάθε εργαλείο. Την δεδομένη στιγμή διαφαίνεται ότι το IP είναι το 192.168.10.6, Εικόνα 5.7.



Εικόνα 5.7: Επισκόπηση διεύθυνσης IP για Metasploitable 2.

5.2 Επισκόπηση και Χρήση Εργαλείων

Στην ενότητα αυτή θα γίνει η παρουσίαση των εργαλείων τα οποία θα χρησιμοποιηθούν καθώς και η καταγραφή των βημάτων εγκατάστασης και χρήσης τους.

5.2.1 Nmap/Zenmap

Το Nmap ή αλλιώς Network Mapper, είναι ένα δωρεάν και ανοιχτού κώδικα λογισμικό το οποίο χρησιμοποιείται για την εξερεύνηση δικτύων και για ανιχνεύσεις ασφαλείας. Έχει ως βασικό στόχο την ανίχνευση δικτυακών συσκευών και συστημάτων και τον έλεγχό τους με διάφορους και διαφορετικούς τρόπους ως προς το λογισμικό που διαθέτουν, τις παρεχόμενος υπηρεσίες και τις ανοιχτές πόρτες στις οποίες μπορούν να συνδεθούν απομακρυσμένα νόμιμοι αλλά και κακόβουλοι χρήστες. Αρκετοί διαχειριστές συστημάτων και δικτύων το χρησιμοποιούν επίσης για την απογραφή του δικτύου, την διαχείριση των προγραμμάτων αναβάθμισης των υπηρεσιών και την παρακολούθηση της κατάστασης ενός υπολογιστή/εξυπηρετητή ή μιας συγκεκριμένης υπηρεσίας.

Το Nmap χρησιμοποιεί ακατέργαστα IP πακέτα για να καθορίσει ποιοι κεντρικοί υπολογιστές (Hosts) είναι διαθέσιμοι στο δίκτυο, ποιες υπηρεσίες (το όνομα της εφαρμογής και την έκδοση) αυτοί οι hosts προσφέρουν, τι λειτουργικά συστήματα (OS και εκδόσεις) τρέχουν, το είδος του

πακέτου και φίλτρων/firewalls που είναι σε χρήση και δεκάδες άλλα χαρακτηριστικά. Για την επίτευξη του στόχου του, το Nmap στέλνει ειδικά δημιουργημένα πακέτα στον κεντρικό υπολογιστή "στόχο" και στη συνέχεια αναλύει τις απαντήσεις. Σε αντίθεση με πολλά απλά Port scanners, που στέλνουν μόνο πακέτα σε κάποιο προκαθορισμένο σταθερό ρυθμό, το Nmap παρακολουθεί τις συνθήκες του δικτύου (διακυμάνσεις λανθάνουσας κατάστασης, συμφόρηση του δικτύου ή παρέμβαση με στόχο τη σάρωση) κατά τη διεξαγωγή του.

Η έξοδος από το Nmap είναι μια λίστα από σαρωμένους στόχους, με συμπληρωματικές πληροφορίες όπου η κάθε μια εξαρτάται από τις επιλογές που χρησιμοποιήθηκαν. Μεταξύ των βασικών πληροφοριών είναι ο σημαντικός πινάκας των ports (Interesting Ports Table). Αυτός ο πίνακας παραθέτει τον αριθμό θύρας και το πρωτόκολλο, το όνομα υπηρεσίας, και την κατάσταση. Η κατάσταση είναι είτε ανοικτή, φιλτραρισμένη, κλειστή ή αφιλτράριστη. Ανοικτή, σημαίνει ότι μια εφαρμογή στον υπολογιστή-στόχο εντοπίζει για συνδέσεις/πακέτα της συγκεκριμένης θύρας. Φιλτραρισμένο, σημαίνει ότι ένα τείχος προστασίας, ένα φίλτρο, ή άλλο εμπόδιο του δικτύου μπλοκάρει τη θύρα έτσι ώστε το Nmap δεν μπορεί να πει αν είναι ανοιχτή ή κλειστή. Κλειστό, σημαίνει οι θύρες δεν έχουν εφαρμογή στο να εντοπίζει συνδέσεις και πακέτα, αν και θα μπορούσαν να ανοίξουν σε οποιαδήποτε στιγμή. Οι θύρες είναι ταξινομημένες ως αφιλτράριστες όταν ανταποκρίνονται στους ανιχνευτές Nmap, αλλά το Nmap δεν μπορεί να προσδιορίσει εάν είναι ανοικτές ή κλειστές. Το Nmap αναφέρει τους συνδυασμούς κατάστασης ανοιχτές/φιλτραρισμένες και κλειστές/φιλτραρισμένες όταν δεν μπορεί να προσδιορίσει ποιες από τις δύο καταστάσεις περιγράφουν μια θύρα. Ο πινάκας της θύρας μπορεί επίσης να περιλαμβάνει λεπτομέρειες έκδοσης του λογισμικού όταν έχει ζητηθεί έκδοση ανίχνευσης. Όταν ένα πρωτόκολλο σάρωσης IP έχει ζητηθεί (-sO), το Nmap παρέχει πληροφορίες σχετικά με τα υποστηριζόμενα πρωτόκολλα IP παρά για ανιχνεύσιμες θύρες.

Εκτός από τους σημαντικούς πίνακες των θυρών, το Nmap μπορεί να παρέχει περαιτέρω πληροφορίες σχετικά με τους στόχους, συμπεριλαμβανομένης της αντιστροφής ονομάτων DNS, εικασίες το είδος του λειτουργικού συστήματος, εικασίες τύπου των συσκευών και τις διευθύνσεις MAC.

Το Nmap χαρακτηρίζεται από ευελιξία καθώς υποστηρίζει πολλές εξειδικευμένες τεχνικές για τη χαρτογράφηση ενός δικτύου το οποίο μπορεί να έχει διάφορα “εμπόδια”, όπως τοίχους προστασίας και δρομολογητές. Έχει την δυνατότητα “σάρωσης” μεγάλων δικτύων που αποτελούνται από χιλιάδες μηχανήματα, είναι ευέλικτο καθώς υποστηρίζονται τα περισσότερα λειτουργικά συστήματα, είναι εύκολο στη χρήση προσφέροντας μια πληθώρα

δυνατοτήτων για τους προχωρημένους χρήστες, είναι δωρεάν και είναι καλά τεκμηριωμένο με συνεχώς ενημερωμένα εγχειρίδια, με online οδηγούς χρήσης που είναι διαθέσιμα σε διάφορες γλώσσες. Το Nmap υποστηρίζεται από μια μεγάλη κοινότητα χρηστών και προγραμματιστών, έχει κερδίσει αρκετά βραβεία και έχει εμφανιστεί σε εκατοντάδες άρθρα, βιβλία και ακόμη και σε ταινίες . [13,14]

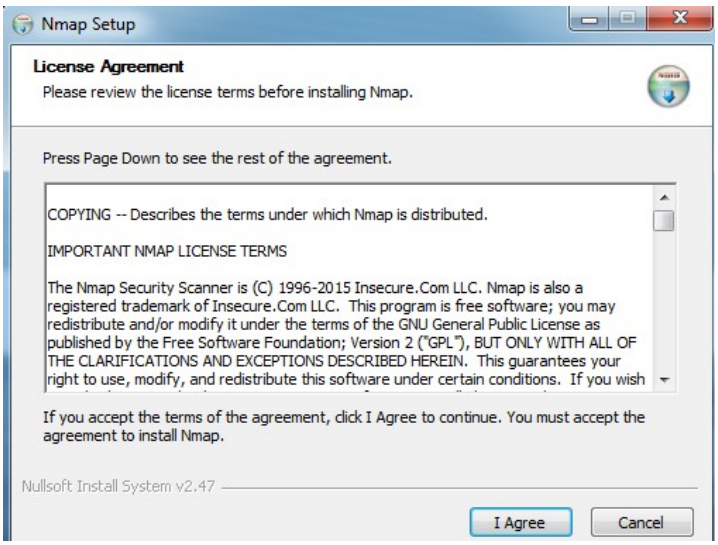
Εγκατάσταση και χρήση εργαλείου Nmap/Zenmap

Το Zenmap αποτελεί το γραφικό περιβάλλον του εργαλείου Nmap και το οποίο μπορεί να εγκατασταθεί και σε περιβάλλον Windows. Το εργαλείο είναι διαθέσιμο στην ιστοσελίδα του Nmap, https://Nmap.org/download.html.

Εγκατάσταση

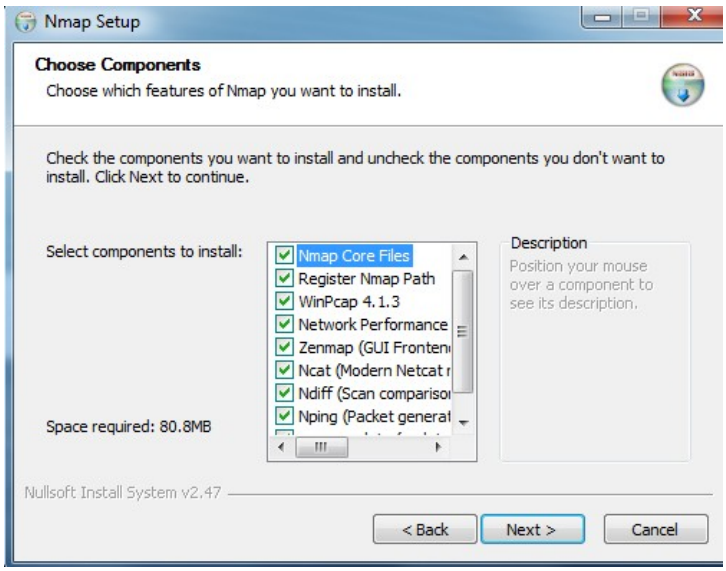
Μετά το κατέβασμα του αρχείου για περιβάλλον Windows, θα διεξαχθεί η διαδικασία εγκατάστασης του εργαλείου.

1. Αφού εκτελεστεί το αρχείο εγκατάστασης, εμφανίζεται η οθόνη με τους όρους της άδειας χρήσης, όπου και γίνεται η αποδοχή αυτών, Εικόνα 5.8.



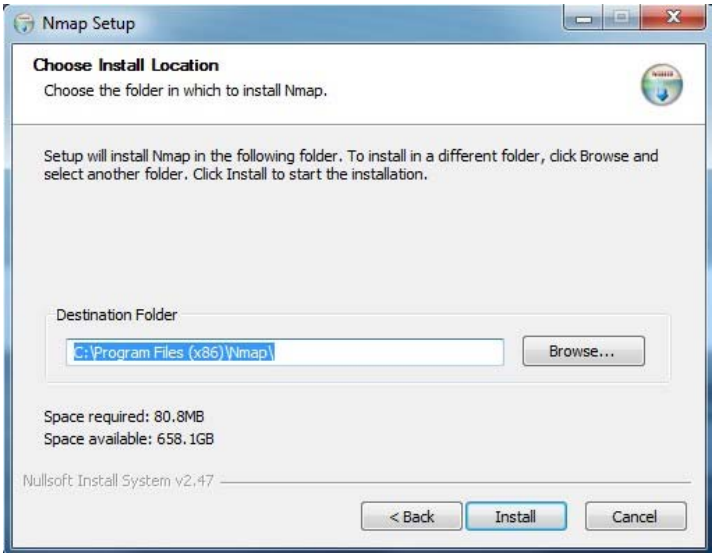
Εικόνα 5.8: Άδεια χρήσης εργαλείου Nmap/Zenmap.

2. Ακολούθως επιλέγονται τα εργαλεία του Nmap που θέλουμε να εγκαταστήσουμε και γίνεται επιβεβαίωση ότι το Zenmap είναι επιλεγμένο, Εικόνα 5.9.



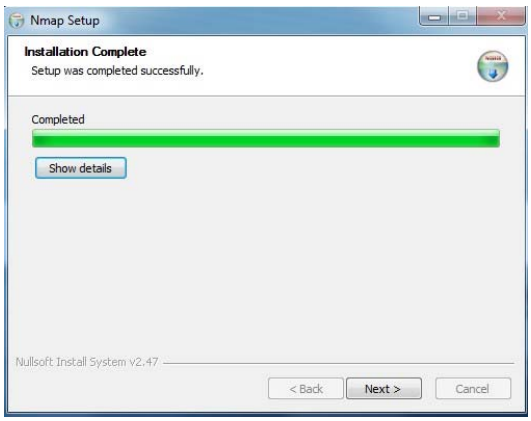
Εικόνα 5.9: Επιλογή εργαλείων Nmap/Zenmap για εγκατάσταση.

3. Στη συνέχεια επιλέγεται η τοποθεσία όπου θα γίνει η εγκατάσταση του εργαλείου και ακολούθως επιλέγεται η επιλογή "Install", Εικόνα 5.10.



Εικόνα 5.10: Επιλογή τοποθεσίας εγκατάστασης Nmap/Zenmap.

4. Μετά από πάροδο μικρού χρονικού διαστήματος πραγματοποιείται η εγκατάσταση του εργαλείου, Εικόνα 5.11.



Εικόνα 5.11: Επιβεβαίωση εγκατάστασης εργαλείων Nmap/Zenmap.

5. Το εικονίδιο του Zenmap παρουσιάζεται στην επιφάνεια εργασίας του υπολογιστή, Εικόνα 5.12. Ακολούθως γίνεται η εκκίνηση του εργαλείου και εκτελούνται οι ενέργειες διερεύνησης του Metaspolitable.

Εικόνα 5.12: Εικονίδιο εκκίνησης εργαλείου Nmap/Zenmap.

Χρήση

1. Για τον εντοπισμό των υπολογιστών που βρίσκονται στο δίκτυο τρέχουμε την εντολή στο Zenmap:

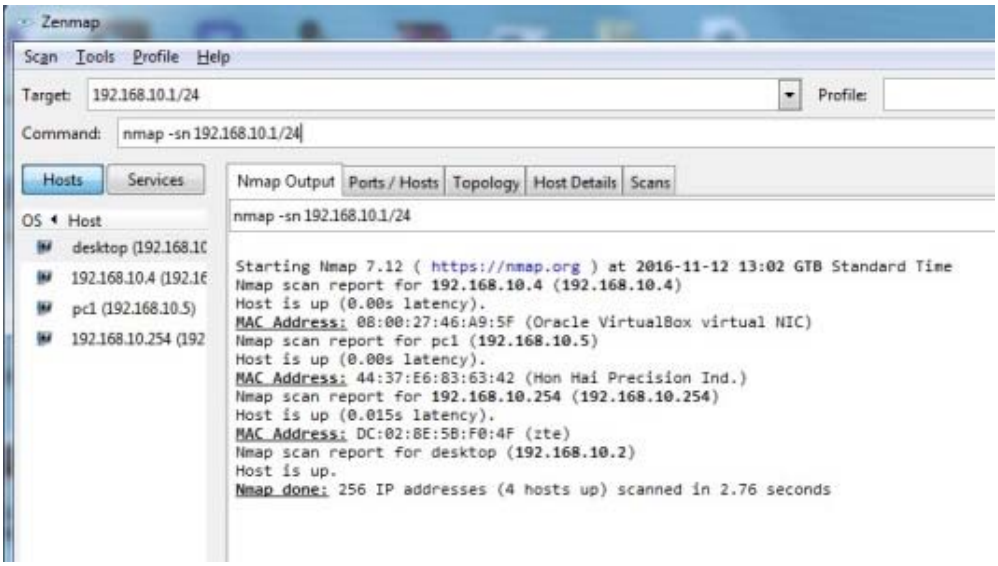
Nmap –sn 192.168.10.1/24

Όπου:

- **-sn:** Με την επιλογή αυτή τον Nmap δεν πραγματοποιεί έλεγχο των ανοιχτών θυρών στους ανευρεθέντες υπολογιστές πάρα μόνο τους καταγράφει. Αποστέλλει πακέτα ICMP, TCP SYN στην θύρα 443 και TCP ACK στην θύρα 80. Στην δεδομένη περίπτωση ο έλεγχος γίνεται χωρίς την χρήση στοιχείων διαχειριστή, έτσι στέλλονται μόνο πακέτα SYN στις θύρες 80 και 443. Εάν γινόταν έλεγχος με την χρήση στοιχείων διαχειριστή τότε θα αποστέλλονταν ARP πακέτα.

- **192.168.10.1/24:** Αποτελεί το υποδίκτυο στο οποίο διεξάγεται ο έλεγχος.

2. Από το αποτέλεσμα διαφαίνεται ότι υπάρχει κάποιος υπολογιστής ενεργός στο Oracle Virtual Box με IP 192.168.10.4, Εικόνα 5.13.



Εικόνα 5.13: Διεργασία διερεύνησης δικτύου.

Η εξαχθείσα κατάσταση με ονομασία "Nmap_Host Discovery" είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nmap" σε xml μορφή.

3. Για να διεξαχθεί ένας πιο ενδελεχής έλεγχος τρέχει η εντολή:

Nmap –sS –sV -PN –O –p 1-65535 192.168.10.4

Όπου:

- **-sS**: Θα πραγματοποιηθεί έλεγχος των ανοιχτών θυρών TCP και UDP.

- **-sV:** Θα καταγραφούν οι υπηρεσίες οι οποίες τρέχουν στις ανοιχτές θύρες και σε ποία έκδοση.

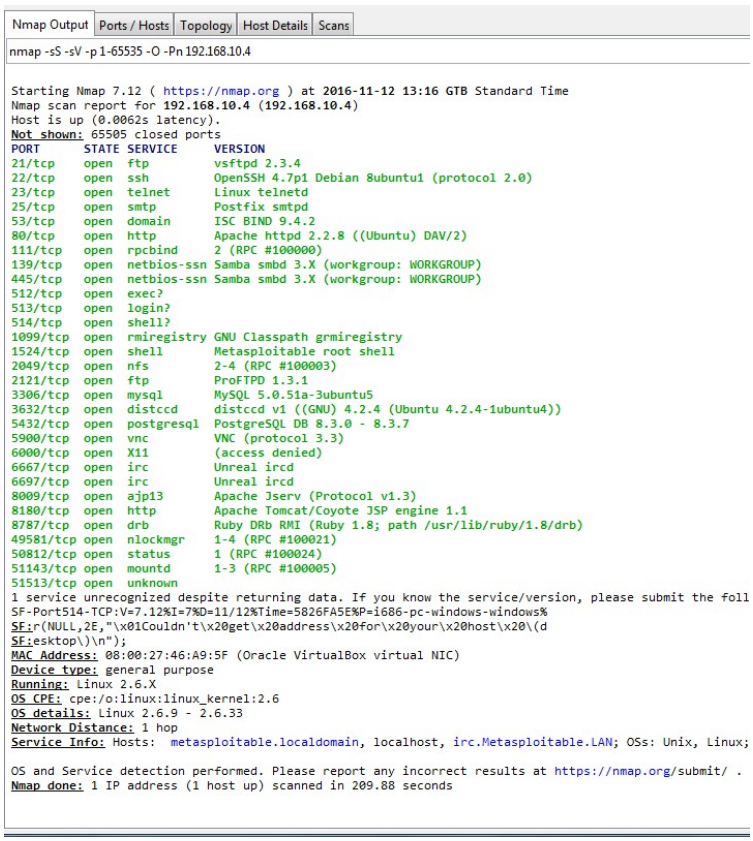
- **-PN:** Δεν θα πραγματοποιηθεί έλεγχος ping μιας και γνωρίζουμε ότι ο υπολογιστής που θα ελέγξουμε είναι διαθέσιμος. Αυτό είναι επίσης χρήσιμο όταν υπάρχει τοίχος προστασίας και εμποδίζει τα icmp πακέτα.

- **-O:** Ποιο είναι το λειτουργικό το οποίο χρησιμοποιεί ο υπό εξέταση υπολογιστής.

- **-p 1-65535:** Θα γίνει έλεγχος σε όλες τις θύρες.

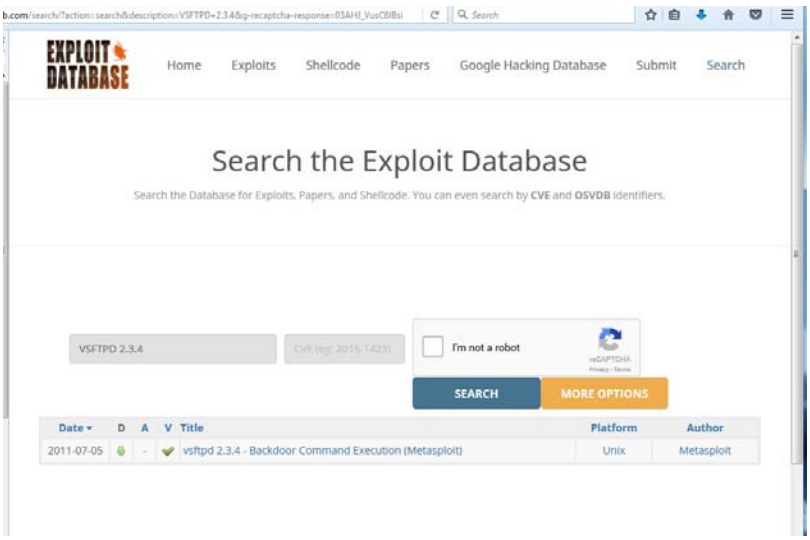
Η εξαχθείσα κατάσταση με ονομασία " Nmap_Ports_&_Services" είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nmap" σε xml μορφή.

4. Από τα αποτελέσματα βλέπουμε όλες τις υπηρεσίες που τρέχουν στον υπό έλεγχο υπολογιστή, την έκδοσή τους και σε ποια θύρα τρέχει η κάθε υπηρεσία. Επίσης ο υπολογιστής έχει λειτουργικό σύστημα LINUX έκδοσης 2.6.9 – 2.6.33. Με την ανεύρεση των υπηρεσιών και της έκδοσης αυτών μπορούμε να προβούμε σε περεταίρω ανάλυση και να βρούμε τις ευπάθειες τους, Εικόνα 5.14.



Εικόνα 5.14: Διερεύνηση υπηρεσιών και θυρών για Metasploitable 2.

Λόγου χάρη εάν ψάξουμε για ευπάθειες για την υπηρεσία VSFTPD v2.3.4 στη βάση δεδομένων της Exploit-DB (https://www.exploit-db.com/), θα πάρουμε αποτελέσματα σχετικά για την ύπαρξη κερκόπορτας στην υπηρεσία αυτή, Εικόνα 5.15.



Εικόνα 5.15: Διερεύνηση υπηρεσία VSFTPD v2.3.4 στην βάση Exploit DB για ανεύρεση ευπαθειών.

5. Ακολούθως θα προσπαθήσουμε να ανιχνεύσουμε τους χρήστες που έχουν δημιουργηθεί στο υπολογιστή. Για να το κάνουμε αυτό θα χρησιμοποιήσουμε την εντολή (στο Zenmap):

Nmap –p 445 –script smb-enum-users.nse 192.168.10.4

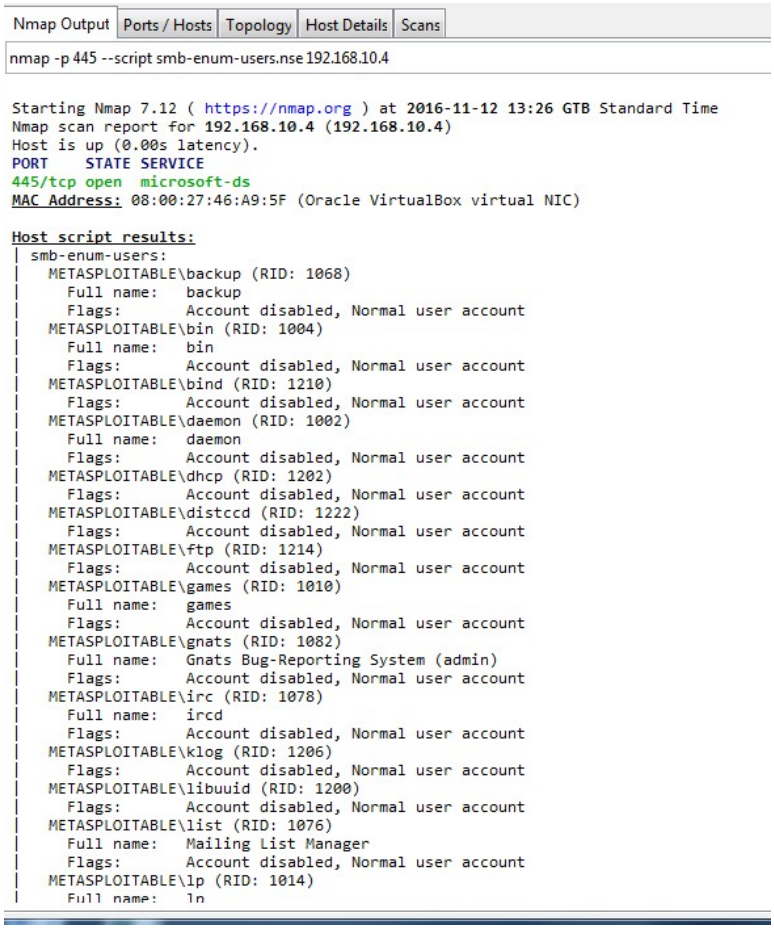
Όπου:

- **-p 445:** Η θύρα στην οποία θα προβεί ο έλεγχος.

- **-script smb-enum-users.nse:** Το πρόγραμμα (Script) το οποίο υπάρχει στην συλλογή του Nmap και θα χρησιμοποιηθεί για την ανεύρεση των χρηστών.

Από τα αποτελέσματα βλέπουμε όλους του χρήστες οι οποίοι είναι δημιουργημένοι στον υπολογιστή. Επίσης διαφαίνεται ποιοι χρήστες είναι ενεργοί και ποιοι όχι.

Η ανεύρεση και καταγραφή των χρηστών μπορεί να βοηθήσει στο να διαφανεί εάν όλοι οι χρήστες που έχουν εντοπιστεί έχουν λόγο ύπαρξης ή/και ακόμη να πραγματοποιηθεί περεταίρω έλεγχος στο κατά πόσο ο κωδικός πρόσβασης που χρησιμοποιούν είναι δύσκολος να εντοπιστεί ή όχι, Εικόνα 5.16.



Εικόνα 5.16: Διερεύνηση χρηστών στο Metasploitable 2.

Η εξαχθείσα κατάσταση με ονομασία " Nmap_Metasploitable_Users" είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nmap" σε xml μορφή.

Παρόλο που το Nmap δεν μας αποκαλύπτει τις ευπάθειες των ανευρεθέντων υπηρεσιών και χρειάζεται κάποιο περαιτέρω ψάξιμο από τρίτες πηγές, εντούτοις με την δημιουργία του NSE (Nmap Scripting Engine) έχουν δημιουργηθεί προγράμματα (Scripts) από του χρήστες του Nmap, τα οποία μπορούν να χρησιμοποιηθούν συμπληρωματικά με το Nmap και να ενισχύσουν την ικανότητα του.

Ένα από αυτά τα scripts είναι και το Vulscan [09] δημιουργία του Marc Ruef. Όπου αφού αναγνωριστούν οι υπηρεσίες που τρέχουν στον υπό διερεύνηση υπολογιστή, το VulScan χρησιμοποιεί τις ακόλουθες offline βάσεις ευπαθειών (.csv μορφή) οι οποίες έχουν προστεθεί με την εγκατάσταση του εργαλείου, όπου ψάχνει και εντοπίζει ποίες από τις υπηρεσίες αυτές έχουν καταγεγραμμένες ευπάθειες και παρουσιάζει τις ευπάθειες αυτές:

- scipvuldb.csv | http://www.scip.ch/en/?vuldb

- cve.csv | http://cve.mitre.org
- osvdb.csv | http://www.osvdb.org
- securityfocus.csv | http://www.securityfocus.com/bid/
- securitytracker.csv | http://www.securitytracker.com
- xforce.csv | http://xforce.iss.net
- expliotdb.csv | http://www.exploit-db.com
- openvas.csv | http://www.openvas.org

Συστήνεται πριν από την χρησιμοποίηση του Vulscan script να ενημερωθούν τα τοπικά αποθηκευμένα αρχεία των πιο πάνω βάσεων.

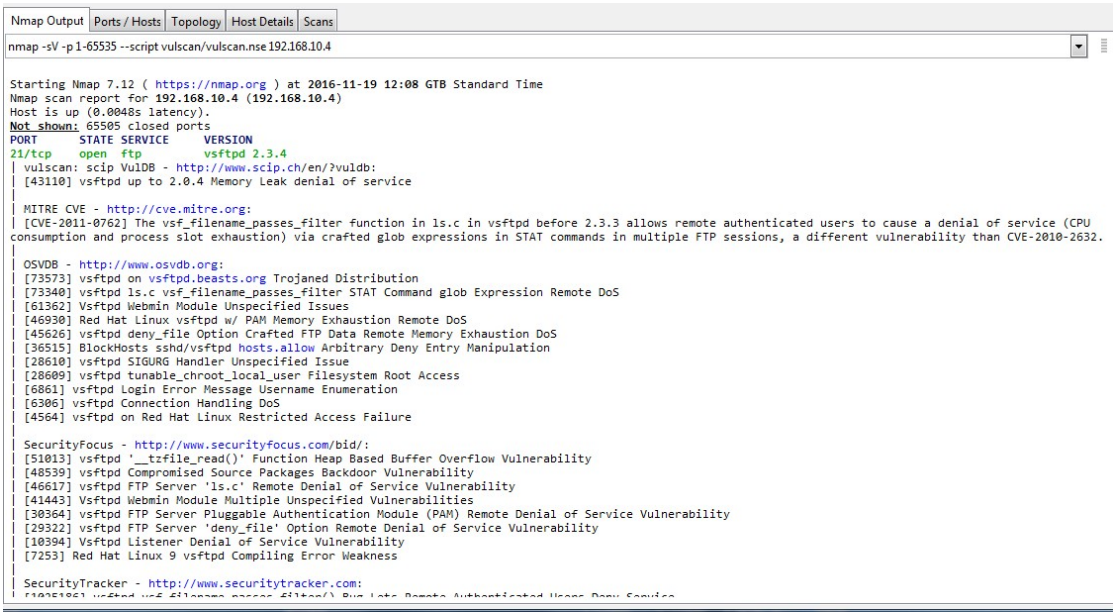
6. Μετά την εγκατάσταση του Vulscan, το script χρησιμοποιείται ως εξής (στο ZeNmap):

Nmap –sV –p 1-65535 --script vulscan/vulscan.nse 192.168.10.4

Όπου:

- **sV:** Θα καταγραφούν οι υπηρεσίες οι οποίες τρέχουν στις ανοιχτές θύρες και ποια η έκδοσή τους.
- **–p 1-65535:** Θα γίνει έλεγχος σε όλες τις θύρες.
- **--script vulscan:** Η εντολή για να εκτελεστεί το script vulscan.

Με την εκτέλεση της εντολής παρουσιάζονται η κάθε υπηρεσία, για την οποία έχουν εντοπιστεί ευπάθειες, με αύξοντα αριθμό θύρας και ακολούθως οι εγγραφές ευπάθειας για την υπηρεσία αυτή, από την κάθε βάση ευπαθειών ξεχωριστά, Εικόνα 5.17.



Εικόνα 5.17: Αποτελέσματα διερεύνησης ευπαθειών με την χρήση του Vulscan script.

Η εξαχθείσα κατάσταση με ονομασία " NMAP VulScan Metasploitable Assesment Report 1" είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nmap" σε xml μορφή.

Επιπρόσθετα μπορούν να χρησιμοποιηθούν και άλλα NSE scripts, είτε μεμονωμένα, είτε σε ομάδες, για την ανεύρεση ευπαθειών. Καλό θα ήταν πριν τη χρήση των scripts, τα οποία έχουν δημιουργηθεί από τρίτους, να έχουν πρώτα ελεγχτεί για ύποπτο ή και επιβλαβή κώδικα.

Τα NSE scripts ανήκουν σε κατηγορίες. Οι κατηγορίες που υπάρχουν αυτή την στιγμή είναι οι auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version και vuln. [15]

7. Από τις κατηγορίες αυτές έχουν επιλεγεί για χρήση οι discovery, vuln, auth, default και malware για την διεξαγωγή επιπλέον ελέγχου στο Metasploitable. Η εντολή που θα χρησιμοποιηθεί (σε ένα παράθυρο εντολών Kali) για την πραγματοποίηση του ελέγχου είναι:

Nmap –sV –p 1-65535 --script= discovery,vuln,auth,default,malware -oX NmapVul.xml 192.168.10.4

Όπου:

- **sV:** Θα καταγραφούν οι υπηρεσίες οι οποίες τρέχουν στις ανοιχτές θύρες και ποια η εκδοσή τους.

- **–p 1-65535:** Θα γίνει έλεγχος σε όλες τις θύρες.

- **--script= discovery, vuln, auth, default, malware :** Η εντολή για να εκτελεστούν όλα τα scripts των κατηγοριών αυτών.

- **-oX NmapVul.xml:** Να δημιουργηθεί ένα xml αρχείο με τα αποτελέσματα.

  Ακολούθως μπορούμε να μετατρέψουμε το αρχείο xml σε μορφή html, όπου θα είναι πιο εύκολο στην ανάγνωση, με το πρόγραμμα "xsltproc" χρησιμοποιώντας την εντολή σε ένα παράθυρο εντολών στο Kali:

  xsltproc NmapVuln.xml –o NmapVuln.html

Η εξαχθείσα κατάσταση με ονομασία " NMAP Scripts Metasploitable Assesment Report 1", είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nmap" σε html μορφή.

5.2.2 OpenVas

Το OpenVas (Open Vulnerability Assessment System) είναι μια συλλογή εργαλείων και υπηρεσιών ασφαλείας που έχουν ως πυρήνα τους τον "σαρωτή" (Scanner) του OpenVas. Ο σαρωτής αυτός είναι υπεύθυνος για την σάρωση του δικτύου και τον εντοπισμό των ευπαθειών αυτού. Ο σαρωτής αυτός τροφοδοτείται από την υπηρεσία OpenVas NVT (Network Vulnerability Test) η οποία, περιέχει περισσότερα από 47000 NVTs και συνεχίζουν να αυξάνονται σε μόνιμη βάση. Επίσης ο σαρωτής μπορεί να τροφοδοτείται και από άλλες εμπορικές υπηρεσίες.

Ο OpenVas Manager είναι η υπηρεσία η οποία προάγει την απλή ανίχνευση ευπαθειών σε μια πλήρη λύση διαχείρισης ευπαθειών. Ο OpenVas Manager διαχειρίζεται τον σαρωτή με την χρήση

του πρωτοκόλλου OTP (OpenVas Transfer protocol) και τον εαυτό του με το OMP (OpenVas Management Protocol) το οποίο έχει XML βάση. Όλες οι εργασίες διεκπεραιώνονται στο Manager ο οποίος διαχειρίζεται επίσης και μια βάση δεδομένων SQL, όπου φυλάσσονται οι ρυθμίσεις και τα αποτελέσματα της σάρωσης. Επίσης ο Manager διαχειρίζεται τους χρήστες και τους ρόλους που έχει ο καθένας στο OpenVas σύστημα. [16]

Εγκατάσταση και χρήση εργαλείου OpenVas

Εγκατάσταση

Το OpenVas αποτελεί πλέον μέρος των εργαλείων ανεύρεσης ευπαθειών του Kali Linux. Για να βεβαιωθούμε ότι το Kali Linux έχει τις τελευταίες ενημέρωσης και ότι το OpenVas είναι επίσης επικαιροποιημένο, τρέχουμε τις πιο κάτω εντολές στο Kali:

1. **root@kali:~# apt-get update**
2. **root@kali:~# apt-get dist-upgrade**
3. **root@kali:~# apt-get install openvas**
4. **root@kali:~# openvas-setup**

Όταν ολοκληρωθεί η εγκατάσταση του OpenVas τότε βεβαιωνόμαστε ότι οι υπηρεσίες OpenVas manager, scanner και GSAD είναι διαθέσιμες:

root@kali:~# netstat –antp

Ακολούθως ξεκινάμε όλες τις υπηρεσίες του OpenVas:

root@kali:~# openvas-start

Χρήση

Το GSA (Greenbone Security Assistant) v. 6.0.10 είναι το γραφικό περιβάλλον του OpenVas, το οποίο επικοινωνεί με το OpenVas μέσο του πρωτοκόλλου OMP (OpenVas Management Protocol).

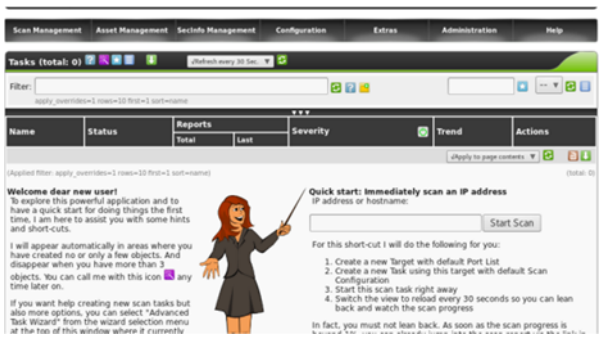
1. Για να τρέξει το GSA θα πρέπει να ανοίξουμε το φυλλομετρητή και να πληκτρολογήσουμε https://127.0.0.1:9392. Όπου θα εμφανιστεί η αρχική οθόνη του εργαλείου, Εικόνα 5.18

Εικόνα 5.18: Αρχική οθόνη εργαλείου OpenVas.

Ο χρήστης-διαχειριστής είναι ο "admin", ο αρχικός κωδικός πρόσβασης θα παρουσιαστεί κατά την εγκατάσταση του εργαλείου και θα είναι ορατός στην εγγραφή "User created with password" όπου και θα προσομοιάζει με 7b93de80-f045-4581-8c8d-d1be80172378 . Επίσης για την δημιουργία καινούργιου χρήστη-διαχειριστή μπορούμε τρέξουμε, από ένα terminal, τις εντολές:

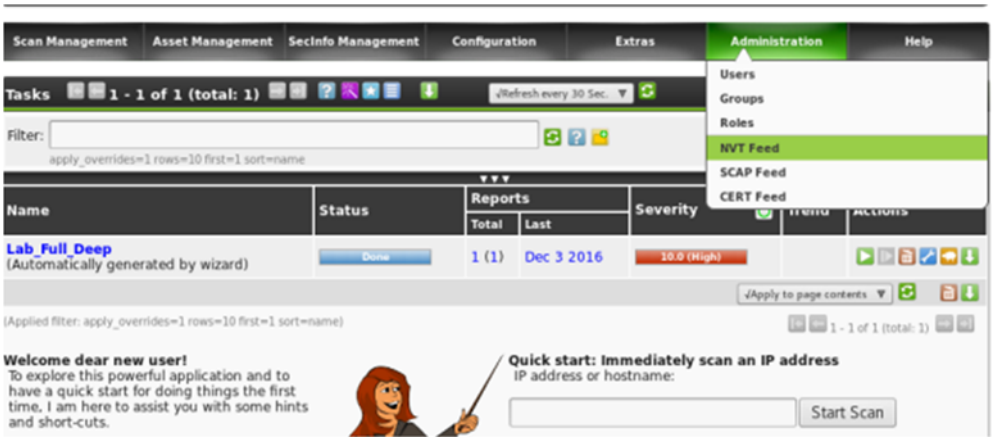
- **#openvasmd --create-user= όνομα χρήστη --role=Admin**
- **#openvasmd –user=όνομα χρήστη –new-password=ο κωδικός πρόσβασης**

2. Μετά την επιβεβαίωση των στοιχείων πρόσβασης, θα παρουσιαστεί η κύρια οθόνη (Home Screen), Εικόνα 5.19.



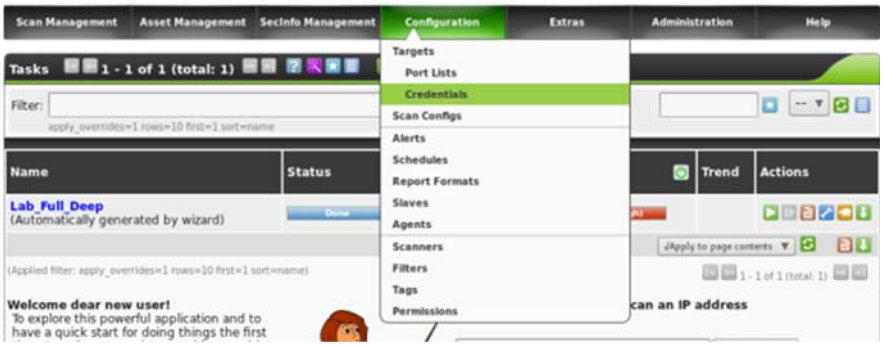
Εικόνα 5.19: Κύρια οθόνη εργαλείου OpenVas.

3. Από το μενού των διαθέσιμων επιλογών, επιλέγεται η επιλογή "Administration" και στην συνέχεια οι επιλογές "NVT Feed", "SCAP Feed" και "CERT Feed", Εικόνα 5.20, όπου θα τρέξουν οι διεργασίες ενημέρωσης της βάσης δεδομένων των ευπαθειών.



Εικόνα 5.20: Επιλογή διεργασιών ενημέρωσης.

4. Ακολούθως από την επιλογή "Configuration" επιλέγουμε "Credentials", Εικόνα 5.21, για την δημιουργία λογαριασμών πρόσβασης σε απομακρυσμένα συστήματα. Αυτό θα επιτρέψει στο OpenVas να πραγματοποιεί ελέγχους ασφαλείας σε βάθος.

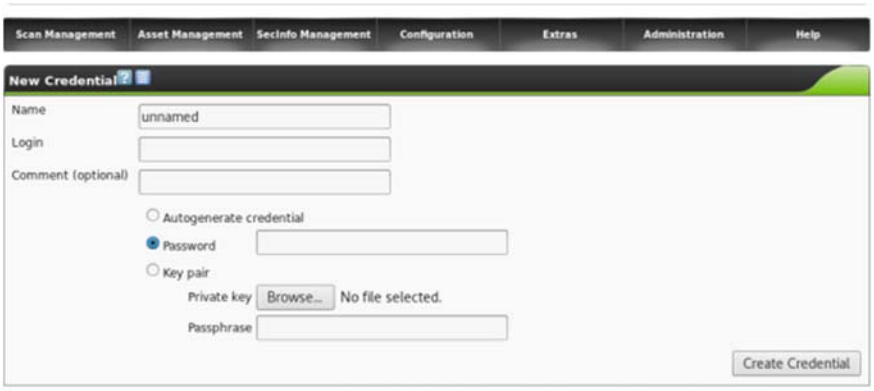


Εικόνα 5.21: Επιλογή δημιουργίας λογαριασμών πρόσβασης.

5. Από την οθόνη "Credentials" επιλέγουμε το  για την δημιουργία καινούργιου λογαριασμού πρόσβασης, Εικόνα 5.22.

Εικόνα 5.22: Επιλογή δημιουργίας νέου λογαριασμού πρόσβασης.

6. Στην οθόνη "New Credential" συμπληρώνουμε τις πληροφορίες πρόσβασης του λογαριασμό που επιθυμούμε, Εικόνα 5.23.

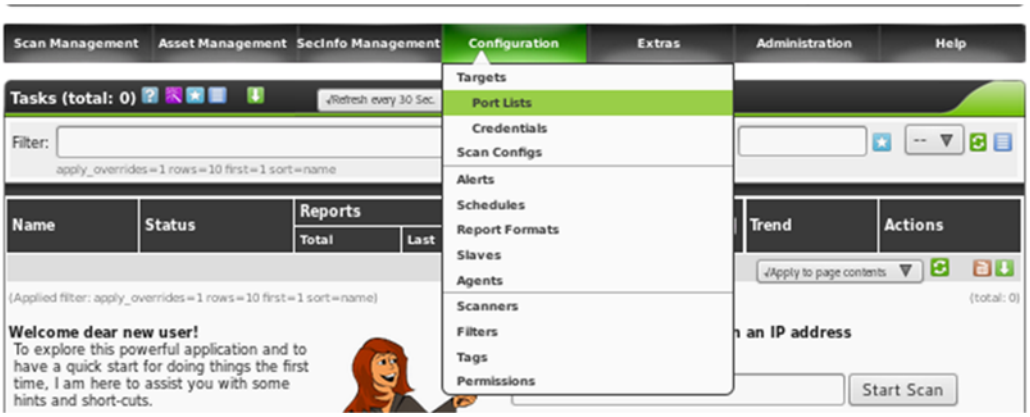


Εικόνα 5.23: Οθόνη καταχώρηση πληροφοριών λογαριασμού πρόσβασης.

7. Στην προκειμένη περίπτωση έχει δημιουργηθεί η εγγραφή "Metasploitable", Εικόνα 5.24, όπου θα χρησιμοποιηθεί για την ανίχνευση ευπαθειών στον υπό έλεγχο υπολογιστή, Metasploitable.

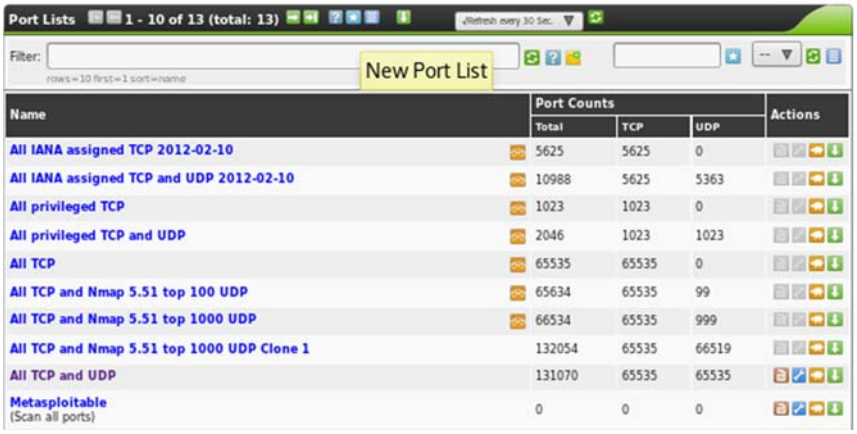
Εικόνα 5.24: Εγγραφή νεοδημιουργηθέν λογαριασμού πρόσβασης με ονομασία "Metasploitable".

8. Ακολούθως, από την κύρια οθόνη επιλέγεται η επιλογή "Configuration" και στην συνέχεια η επιλογή "Port Lists", Εικόνα 5.25, για την δημιουργία της λίστας των θυρών που θα εξεταστούν.



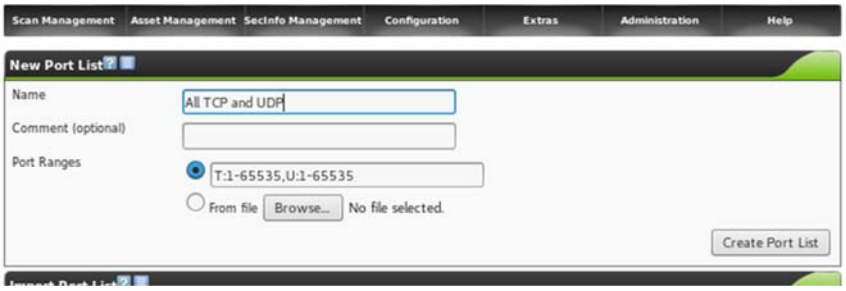
Εικόνα 5.25: Επιλογή δημιουργίας λίστας θυρών.

9. Στην συνέχεια επιλέγεται το  "New Port List", Εικόνα 5.26.



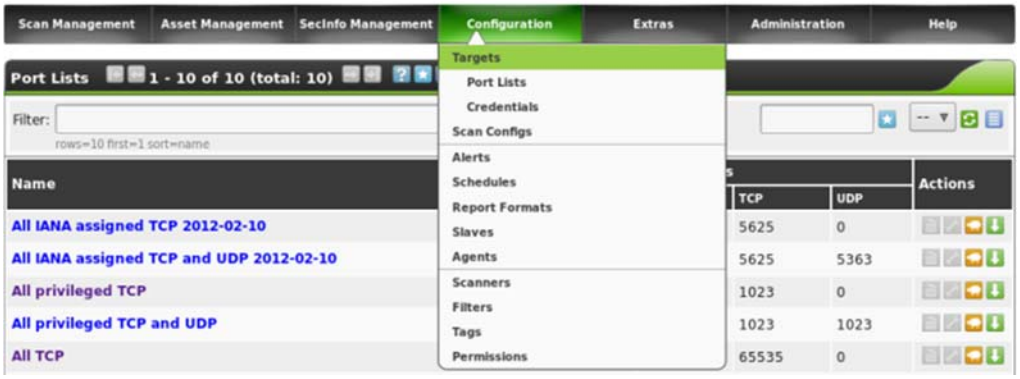
Εικόνα 5.26: Επιλογή δημιουργίας νέας λίστας θυρών.

10. Στην οθόνη "New Port List" καταχωρείται το όνομα της λίστας, "All TCP and UDP" και στην συνέχεια καταχωρούνται οι θύρες που θα εξεταστούν. Για tcp θύρες καταχωρείται το "T:" και στη συνέχεια ο αριθμός των θυρών, στην προκειμένη περίπτωση θα εξεταστούν όλες οι θύρες tcp. Με ανάλογο τρόπο καταχωρούνται και οι UDP θύρες. Στην συνέχεια επιλέγεται η επιλογή "Create Port List" για την δημιουργία της λίστας, Εικόνα 5.27.



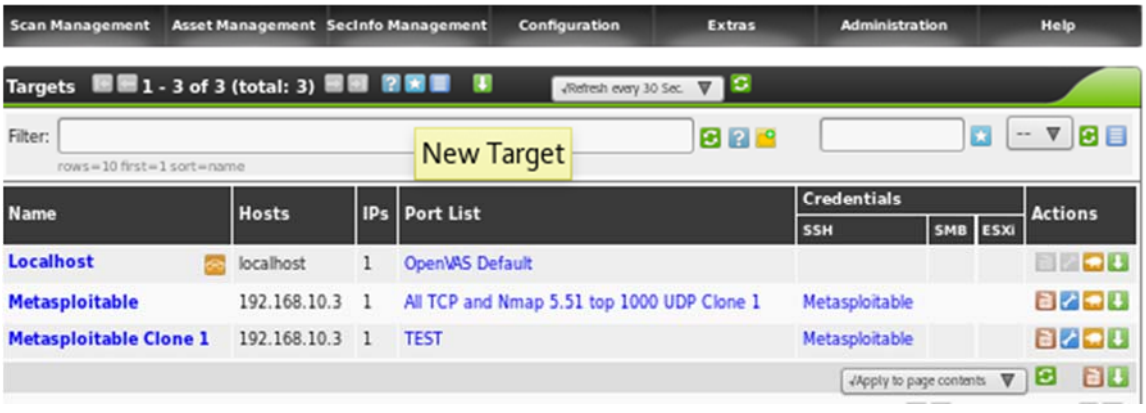
Εικόνα 5.27: Οθόνη δημιουργίας νέας λίστας θυρών.

11. Στη συνέχεια, από την κύρια οθόνη επιλέγεται η επιλογή "Configuration" και ακολούθως η επιλογή "Targets" Εικόνα 5.28, για την δημιουργία της λίστας υπολογιστών που θα ανιχνευθούν για ευπάθειες.



Εικόνα 5.28: Επιλογή δημιουργίας λίστας υπολογιστών για διερεύνηση.

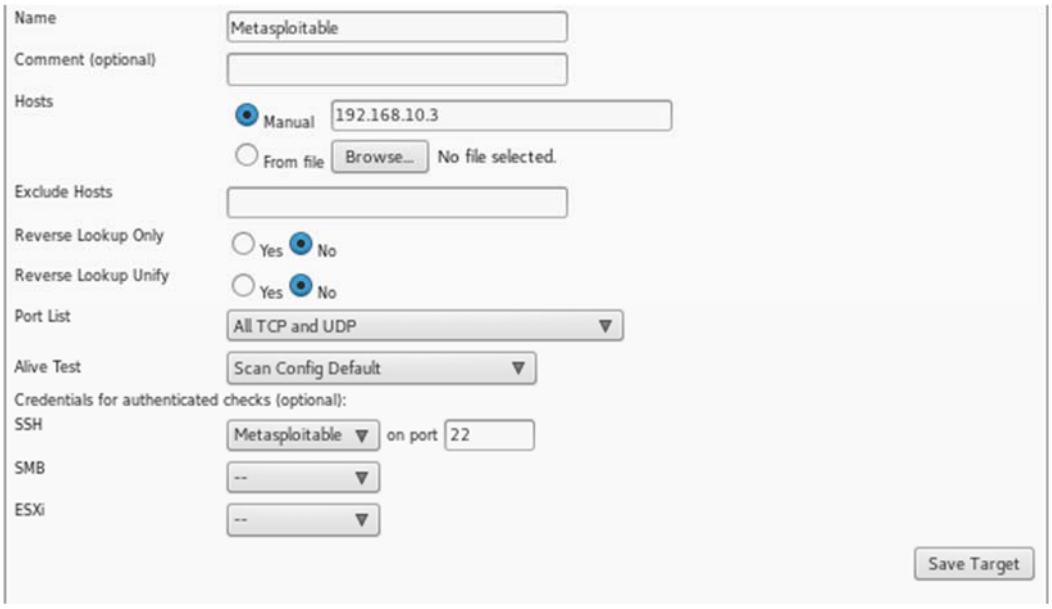
12. Ακολούθως επιλέγεται το  "New Target", Εικόνα 5.29.



Εικόνα 5.29: Επιλογή δημιουργίας νέας λίστας υπολογιστών για διερεύνηση.

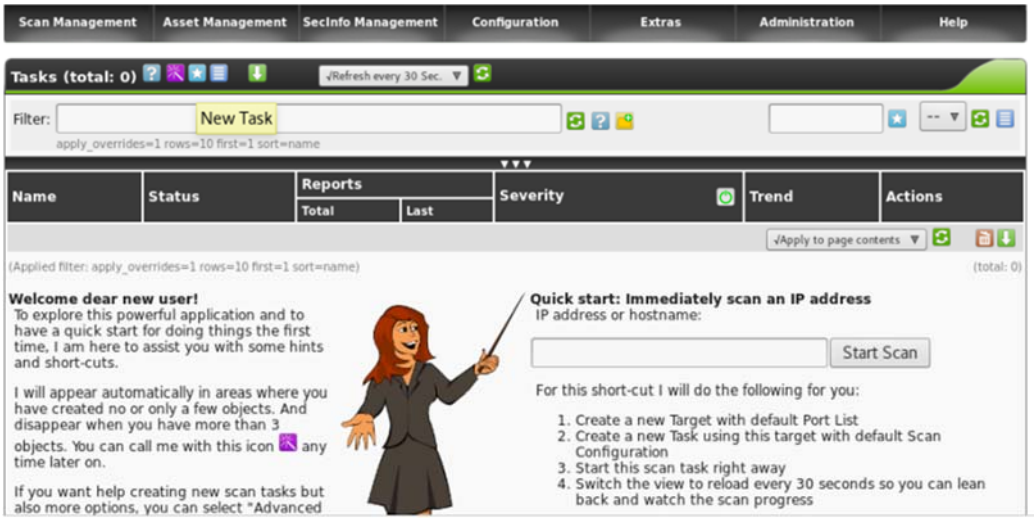
13. Στην οθόνη "New Target" καταχωρούνται η λεπτομερές των υπό διερεύνηση υπολογιστών. Στην προκειμένη περίπτωση δίνεται το όνομα "Metasploitable" και

καταχωρείται το IP του υπολογιστή, 192.168.10.3. Στην συνέχεια επιλέγεται το "Port List" που έχει προηγούμενος δημιουργηθεί στο βήμα 10, "All TCP and UDP". Ακολούθως επιλέγονται τα στοιχεία αυθεντικοποίησης "Metasploitable" που επίσης δημιουργηθήκαν προηγούμενος στο βήμα 7 και επιλέγεται το "Save Target" για φύλαξη των στοιχείων, Εικόνα 5.30.



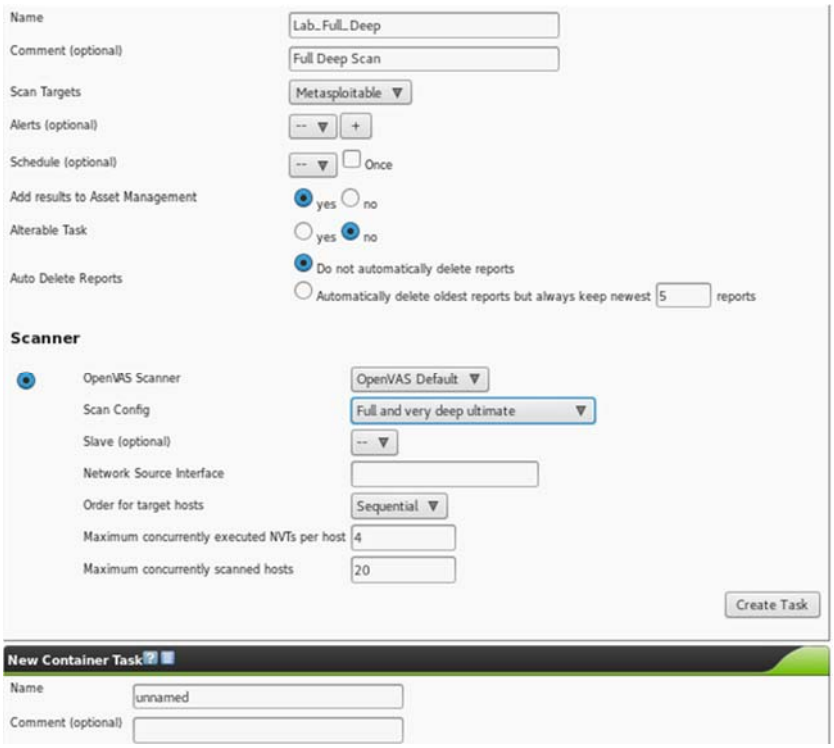
Εικόνα 5.30: Οθόνη δημιουργίας νέας λίστας υπολογιστών για διερεύνηση.

14. Από την κύρια οθόνη του εργαλείου επιλέγεται το  "New Task", Εικόνα 5.31, για την δημιουργία εργασίας ανίχνευσης.



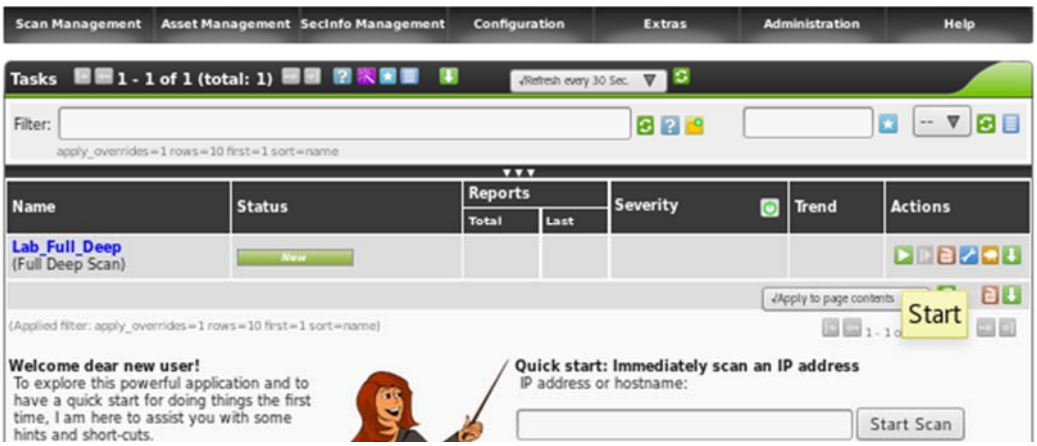
Εικόνα 5.31: Επιλογή δημιουργίας εργασίας ανίχνευσης.

15. Στην οθόνη "New Task" καταχωρούνται τα στοιχεία της εργασίας ανίχνευσης. Το όνομα της εργασίας, στην προκειμένη περίπτωση είναι "Lab_Full_Deep", στην επιλογή "Scan Targets" επιλέγεται το "Metasploitable" και στην επιλογή "Scan Config" επιλέγεται το "Full and deep ultimate", όπου αποτελεί το προφίλ το οποίο διενεργεί τους περισσότερους ελέγχους για ανεύρεση ευπαθειών. Για την φύλαξη των στοιχείων επιλέγεται το "Create Task", Εικόνα 5.32.



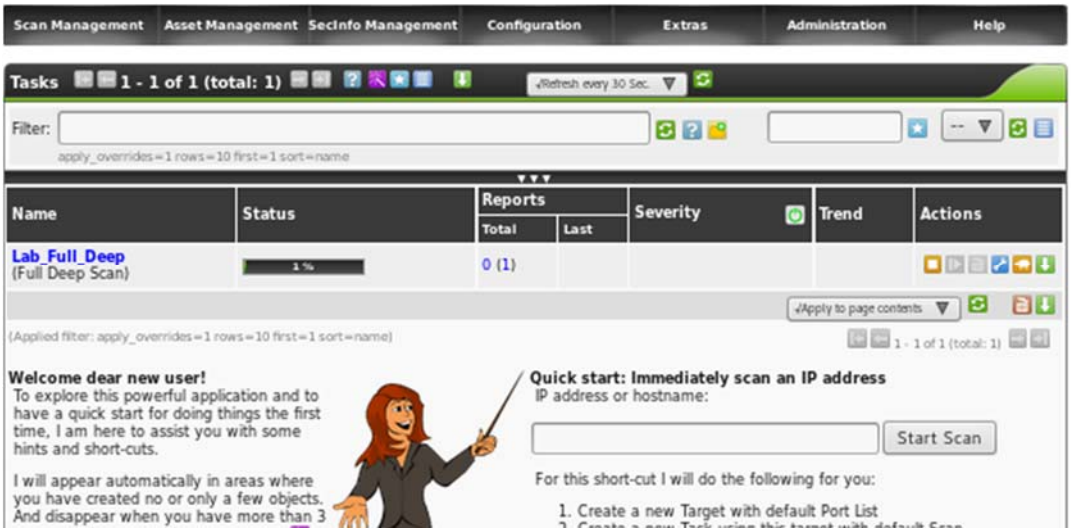
Εικόνα 5.32: Οθόνη δημιουργίας νέας εργασίας ανίχνευσης.

16. Στην κύρια οθόνη του εργαλείου εμφανίζεται η νεοδημιουργηθέν εργασία ανίχνευσης . Για την εκκίνηση της διεργασίας ανίχνευσης επιλέγεται η επιλογή "Start" , Εικόνα 5.33.



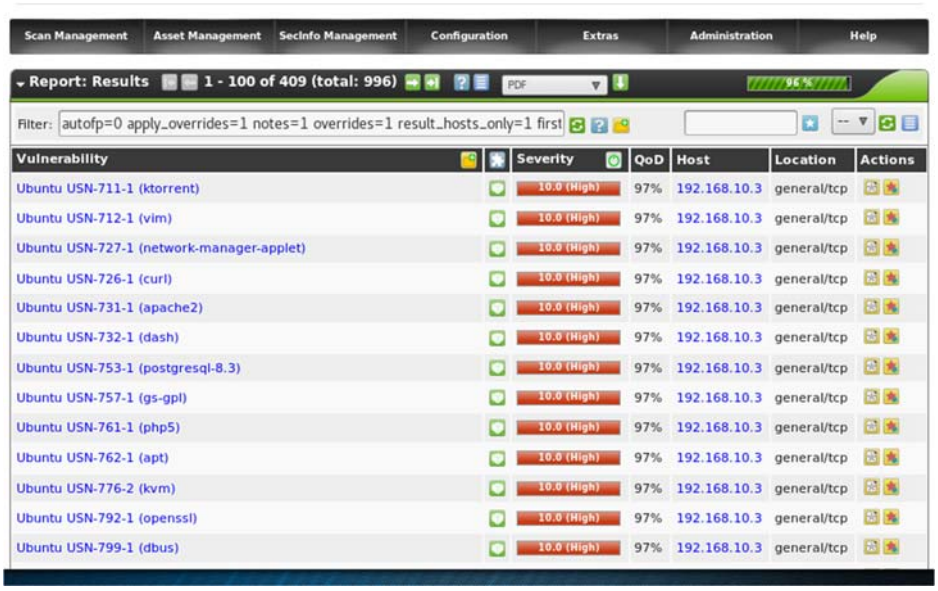
Εικόνα 5.33: Επιλογή εκκίνησης εργασίας ανίχνευσης.

17. Μετά την εκκίνηση της εργασίας διερεύνησης και οποιαδήποτε στιγμή επιθυμεί ο διαχειριστής, μπορεί να δει τι έχει εντοπιστεί μέχρι την δεδομένη στιγμή, απλά πατώντας πάνω στην τρέχουσα κατάσταση, "Status", της εργασίας ελέγχου, Εικόνα 5.34.



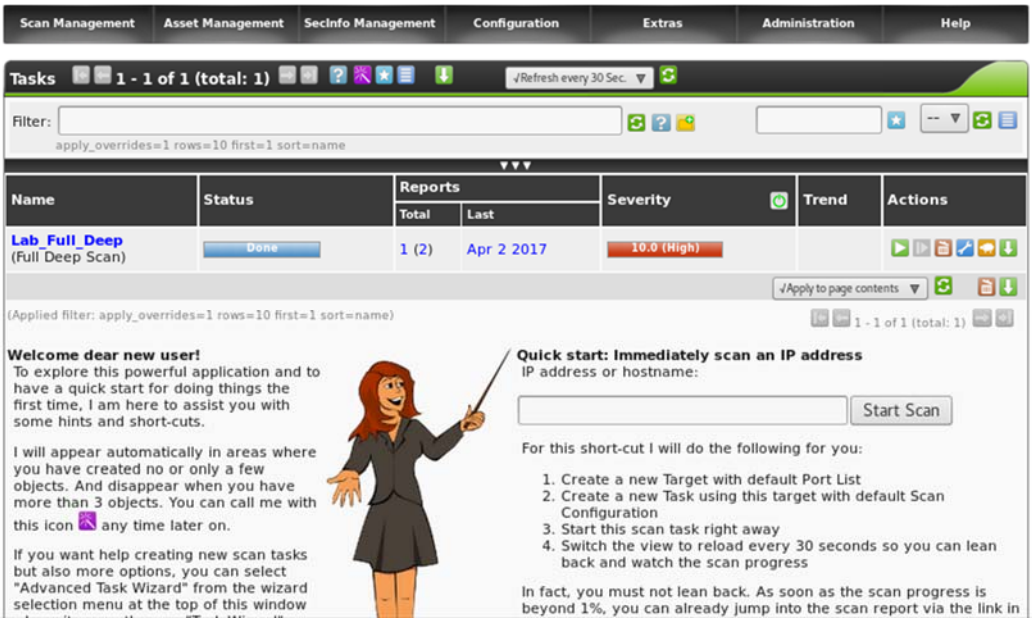
Εικόνα 5.34: Εργασίας ανίχνευσης εν ενεργεία.

Μετά την επιλογή "Status", η οθόνη με τις μέχρι τώρα ανευρεθείσες ευπάθειες θα παρουσιαστεί, Εικόνα 5.35.



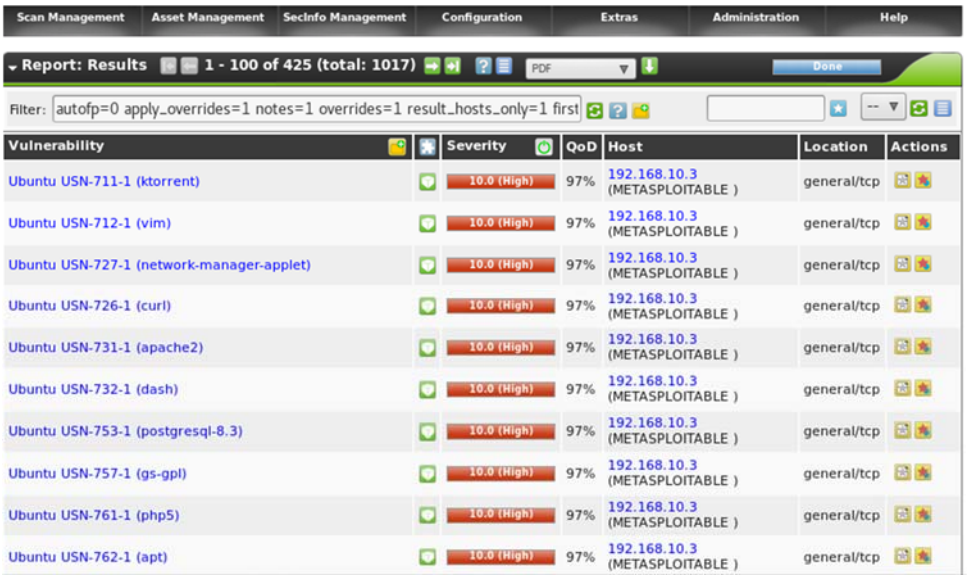
Εικόνα 5.35: Οθόνη παρουσίασης των μέχρι στιγμής ανευρεθέν ευπαθειών.

18. Με την ολοκλήρωση της εργασίας ελέγχου η κατάσταση του “Status” αλλάζει σε “Done”. Στην κατηγορία “Severity” εμφανίζεται το ρίσκο στο οποίο βρίσκεται η μηχανή Metasploitable. Στην προκειμένη περίπτωση το ρίσκο της μηχανής είναι “High”, πράγμα του σημαίνει ότι η μηχανή αυτή χρίζει άμεσης προσοχής για αντιμετώπιση των ευπαθειών, Εικόνα 5.36.



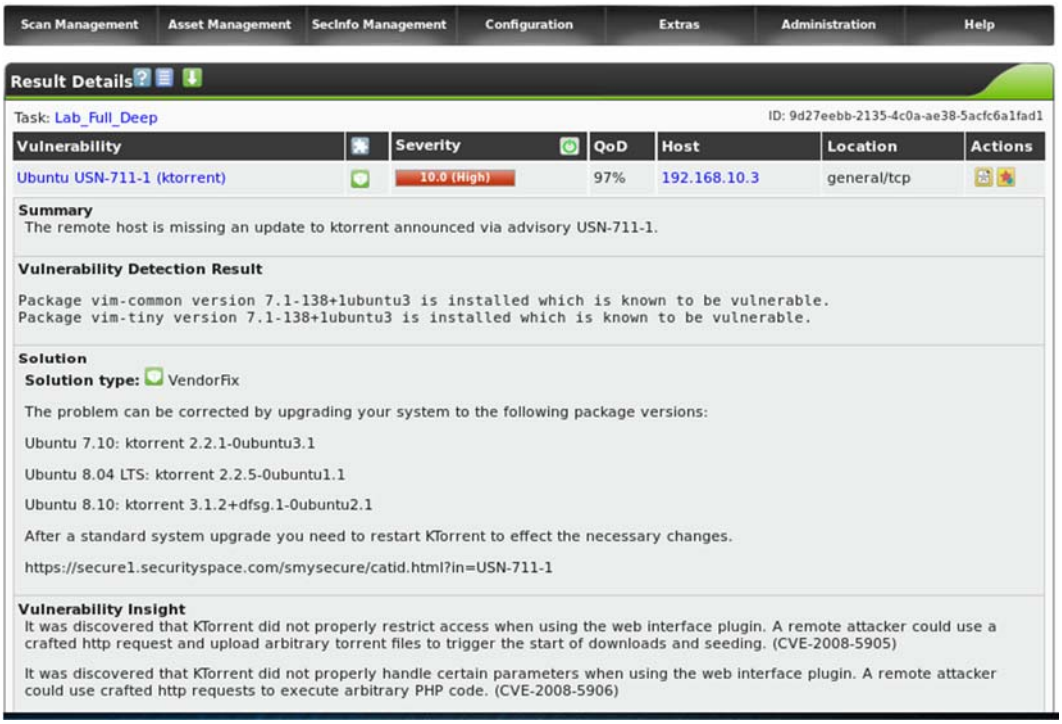
Εικόνα 5.36: Ολοκλήρωση εργασίας ανίχνευσης.

19. Κάνοντας κλικ στην κατάσταση “Done“ εμφανίζονται όλες οι ευπάθειες οι οποίες έχουν εντοπιστεί με σειρά κρισιμότητας, αρχίζοντας πρώτα από τις πιο κρίσιμες ευπάθειες (10.0 “High”), Εικόνα 5.37.



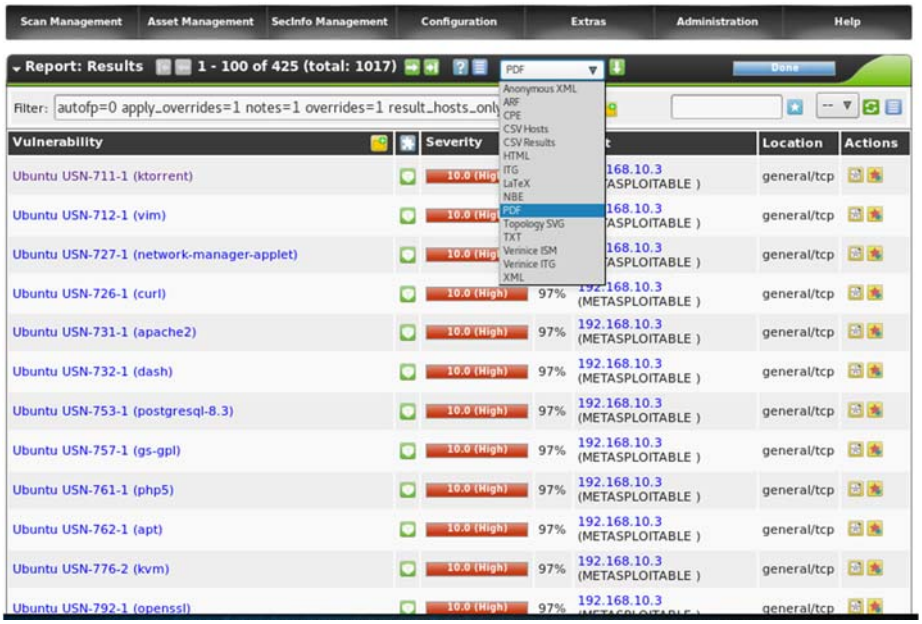
Εικόνα 5.37: Οθόνη παρουσίασης ανευρεθέντων ευπαθειών.

20. Πατώντας σε κάποια ευπάθεια εμφανίζονται οι λεπτομέρειες της συγκεκριμένης ευπάθειας. Πιο κάτω, στην Εικόνα 5.38, εμφανίζονται λεπτομέρειες της ευπάθειας “Ubuntu USN-711-1 (ktorrent)”. Περιγράφεται η ευπάθεια και πως μπορεί να εκμεταλλευτεί από ένα επιτιθέμενο. Προτείνεται επίσης και ο τρόπος επιδιόρθωσης της ευπάθειας.



Εικόνα 5.38: Λεπτομέρειες ευπάθειας "Ubuntu USN-711-1 (ktorrent)".

21. Ακολούθως μπορεί να εξαχθεί μια κατάσταση όλο των ευπαθειών και η οποία θα μπορεί να δοθεί στις αρμόδιες ομάδες για επεξεργασία. Η κατάσταση αυτή μπορεί να εξαχθεί σε διάφορες μορφές, PDF, HTML, XML, CSV κτλ, Εικόνα 5.39.



Εικόνα 5.39: Εξαγωγή κατάστασης ανευρεθέντων ευπαθειών.

Η εξαχθείσα κατάσταση με ονομασία "OpenVas Metasploitable Assesment Report 1" είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "OpenVas", σε PDF μορφή.

5.2.3 Nexpose

Το Nexpose είναι ένα εργαλείο ανεύρεσης ευπαθειών το οποίο βοηθά ένα οργανισμό να διαχειριστεί ολόκληρο το κύκλο ζωής μια ευπάθειας, από την ανίχνευση της ευπαθείας, την ταξινόμηση του κινδύνου, την ανάλυση του αντίκτυπου που θα έχει στον οργανισμό η συγκεκριμένη ευπάθεια, στην δημιουργία έκθεσης, στην επαλήθευση ευπάθειας και τέλος στο μετριασμό του κινδύνου.

Το γραφικό περιβάλλον του Nexpose διευκολύνει αρκετά τον υπεύθυνο ασφαλείας να διενεργήσει ελέγχους για γνωστές ευπάθειες, στο δίκτυο τους. Επίσης το Nexpose μπορεί να τροποποιηθεί έτσι ώστε να διενεργεί ελέγχους στις ιστοσελίδες του οργανισμού, καθώς και των εξυπηρετητών διαδικτύου (Web Servers) για ανεύρεση ευπαθειών στις εφαρμογές ιστού (Web Applications), καθώς και για να καθοριστεί το επίπεδο πολιτικής συμμόρφωσης τους.

Το Nexpose με την χρήση του Advance Exposure Analytics εντοπίζει τις ευπάθειες και τις προτεραιοποιεί με βάση ποια από αυτές είναι πιθανό να εκμεταλλευτεί πρώτη. Αυτό επιτυγχάνεται με την επί δεκαετιών ανάλυση των ενεργειών των κακόβουλων χρηστών και την ενσωμάτωση αυτή της γνώσης στη βάση δεδομένων του Nexpose, η οποία ενημερώνεται συνεχώς με καινούργια δεδομένα. Επίσης με την χρήση το Liveboards δίνετε η δυνατότητα της άμεσης ενημέρωσης για την πραγματική κατάσταση των ευπαθειών ενός οργανισμού και κατά πόσο οι ενέργειες του οργανισμού τις μειώνουν ή το αντίθετο.

Η συνεργασία του Nexpose με το Metasploit, του πιο διαδεδομένου λογισμικού δοκιμών διείσδυσης στον κόσμο, δίνει την ευχέρεια πιστοποίησης σε πραγματικό χρόνο για το ποια συστήματα είναι εκτεθειμένα και ποια μέτρα προστασίας λειτουργούν ικανοποιητικά.

Με το Nexpose η προβολή της προόδου του οργανισμού στα θέματα ασφαλείας προς τους ελεγκτές μπορεί εύκολα να γίνει με την αντιπαραβολή αυτής στο κατά πόσο πληροί τις προϋποθέσεις των PCI DSS, NERC CIP, FISMA, HIPPA, Top 20 CSC, DISA STIGS και CIS. [12]

Εγκατάσταση και χρήση εργαλείου Nexpose

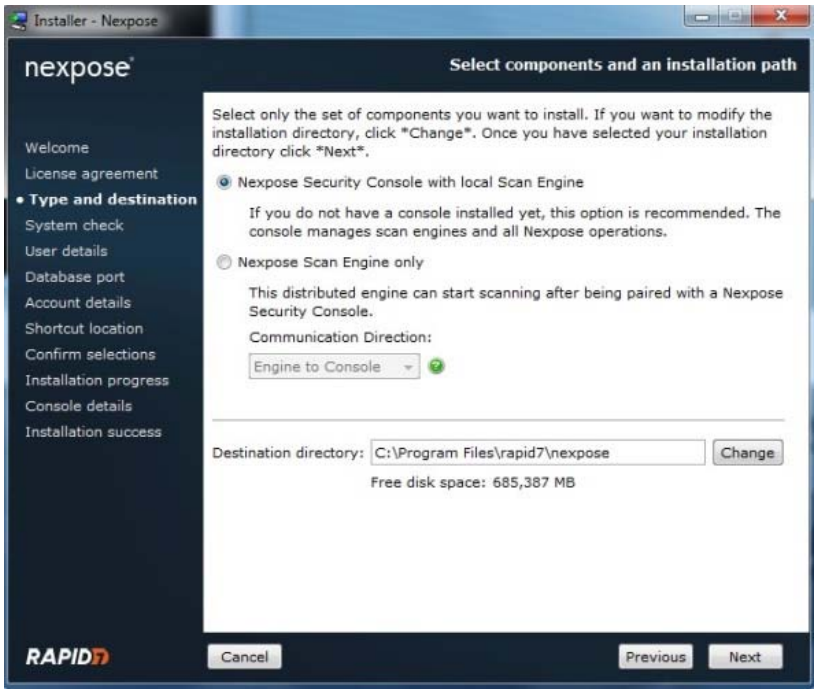
Το εργαλείο Nexpose διατίθεται για χρήση σε 4 εκδόσεις, Enterprise Community, Express και Consultant Edition, με την Enterprise να αποτελεί την πιο ολοκληρωμένη λύση.

Στην παρούσα μεταπτυχιακή διατριβή έχει χρησιμοποιηθεί το εργαλείο Nexpose Enterprise Edition (Free 14-day Trial).

Εγκατάσταση

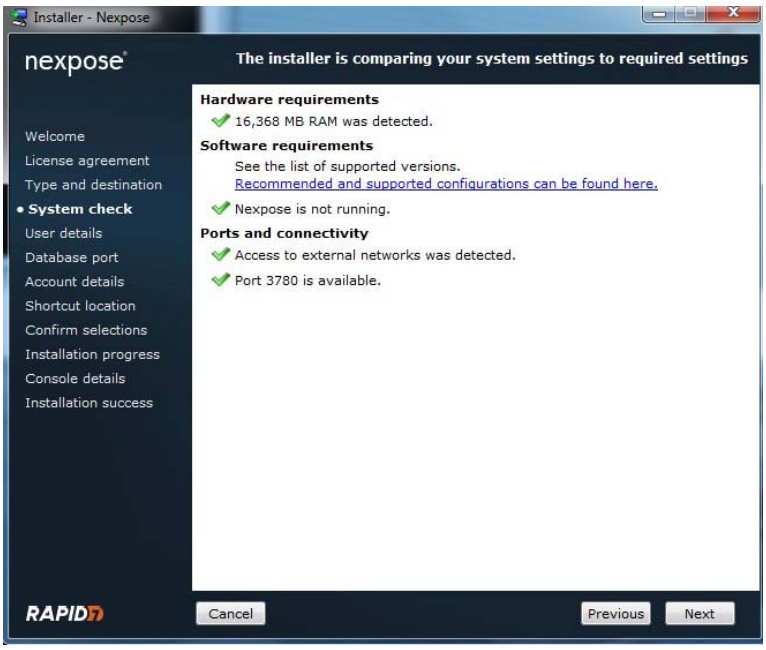
Μετά από την νενομισμένη εγγραφή στην ιστοσελίδα, το κατέβασμα και την παραλαβή του κλειδιού χρήσης (μέσω email) του εργαλείου, θα διενεργηθεί η εγκατάσταση αυτού.

1. Ξεκινώντας την εγκατάσταση, επιλέγεται το "Nexpose Security Console with local Scan Engine", Εικόνα 5.40.



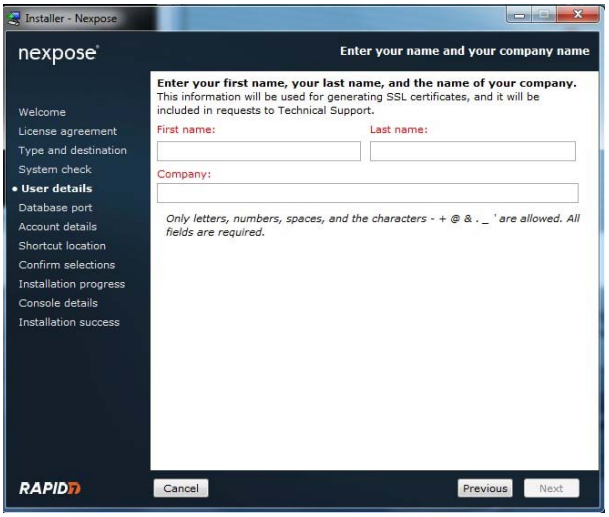
Εικόνα 5.40: Επιλογή εγκατάσταση "Nexpose Security Console with local Scan Engine".

2. Το εργαλείο διενεργεί του νενομισμένους ελέγχους και εξακριβώνει εάν το μηχάνημα στο οποίο θα εγκατασταθεί διαθέτει όλους τους πόρους, υπολογιστικό και λογισμικό υλικό, τους οποίους απαιτεί, Εικόνα 5.41.



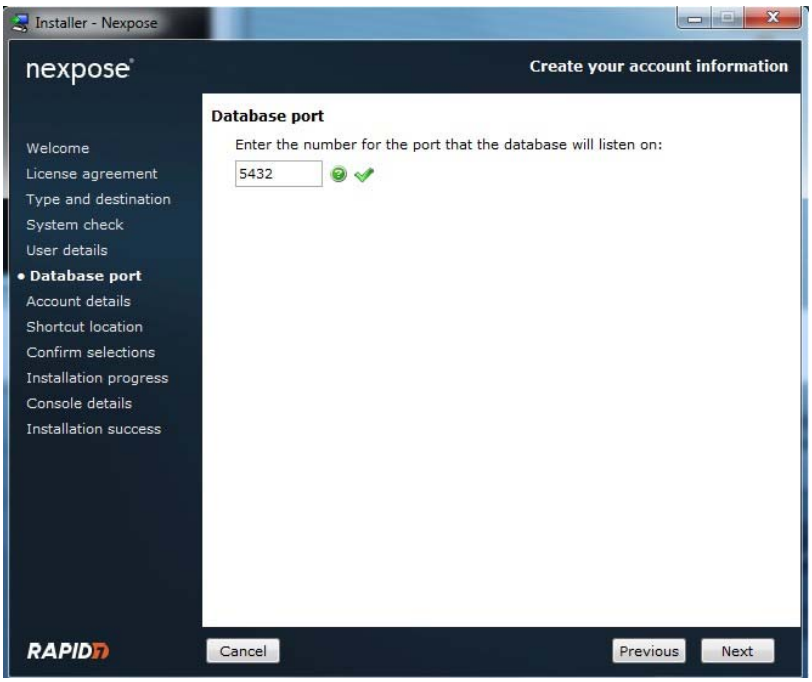
Εικόνα 5.41: Έλεγχος εξακρίβωσης διαθέσιμων πόρων για την εγκατάσταση του Nexpose.

3. Στην συνέχεια καταχωρούνται τα προσωπικά στοιχεία του χρήστη, όνομα και επίθετο, καθώς και το όνομα του οργανισμού. Τα στοιχεία αυτά θα χρησιμοποιηθούν για την δημιουργία πιστοποιητικών ασφαλείας SSL καθώς και για την επικοινωνία με την εταιρεία Rapid 7 στην περίπτωση τεχνικής υποστήριξης, Εικόνα 5.42.



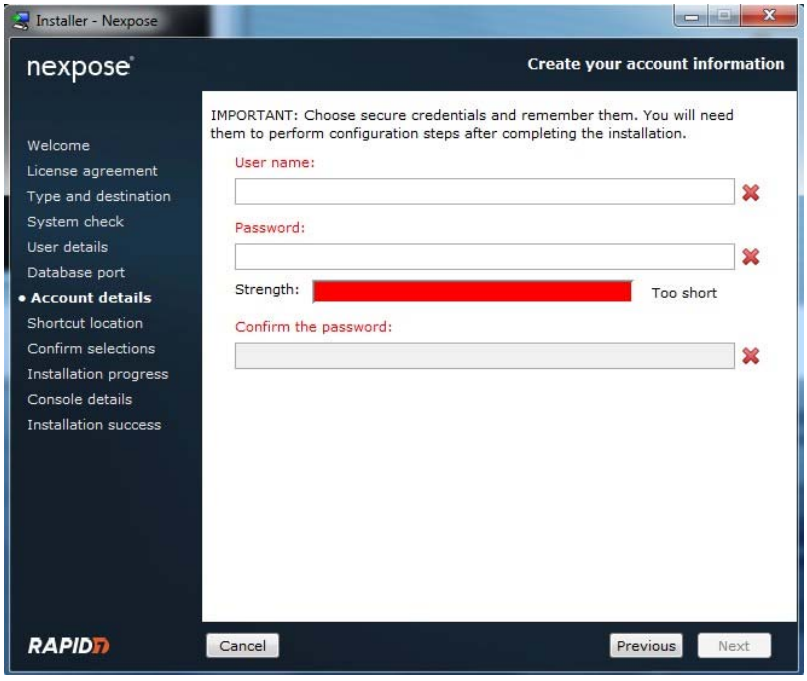
Εικόνα 5.42: Καταχώρηση προσωπικών στοιχείων διαχειριστή.

4. Ακολούθως επιλέγεται η θύρα, η οποία θα χρησιμοποιηθεί για την επικοινωνία με την βάση δεδομένων του εργαλείου. Στην προκειμένη περίπτωση έχει χρησιμοποιηθεί η προτεινόμενη θύρα “5432”, Εικόνα 5.43.



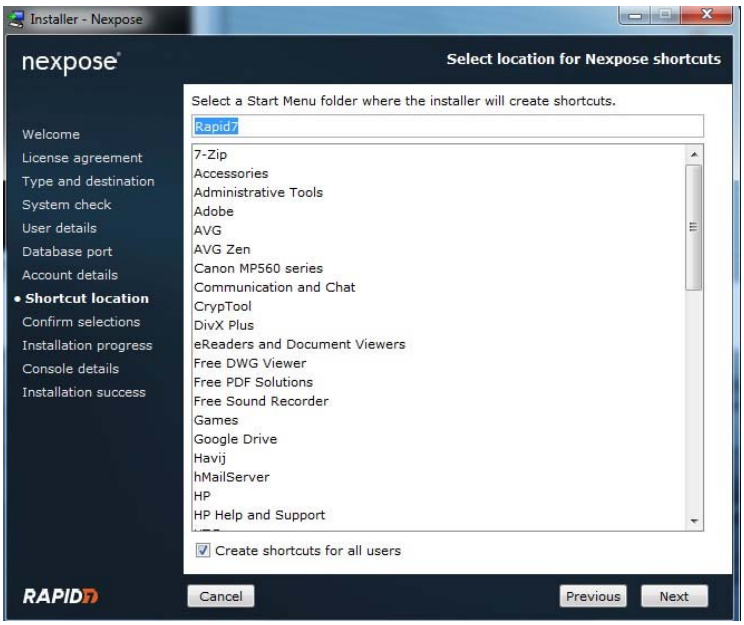
Εικόνα 5.43: Επιλογή θύρα επικοινωνίας.

5. Ακολουθεί η δημιουργία των διαπιστευτηρίων του διαχειριστή του εργαλείου, Εικόνα 5.44.



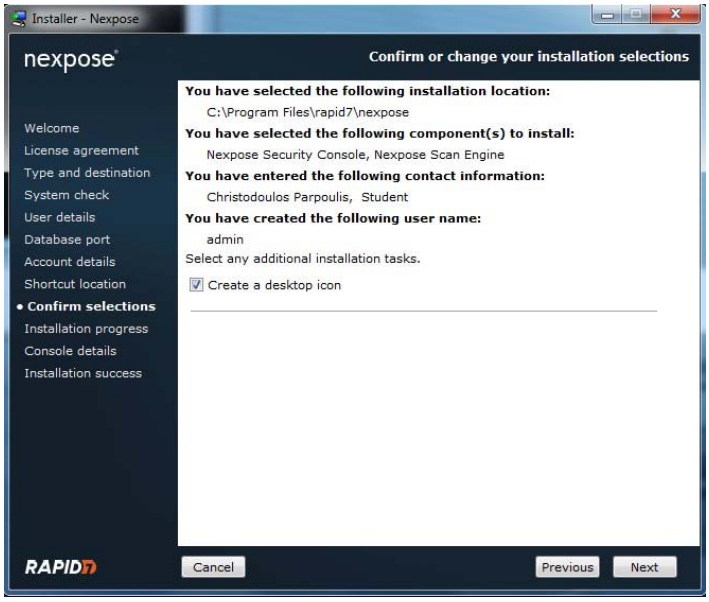
Εικόνα 5.44: Δημιουργία διαπιστευτηρίων διαχειριστή.

6. Ακολούθως επιλέγεται ο φάκελος στο Start Menu, στον οποίο θα τοποθετηθούν οι συντομεύσεις του εργαλείου, Εικόνα 5.45.



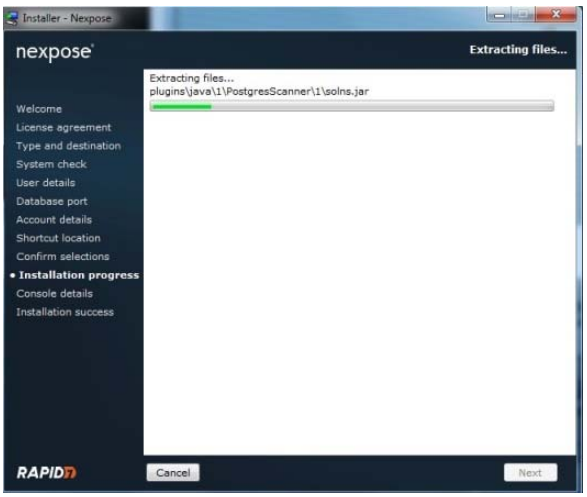
Εικόνα 5.45: Τοποθέτηση συντομεύσεων στο Start Menu.

7. Ακολούθως παρουσιάζονται όλες οι προαναφερθείσες επιλογές για επισκόπηση και επιβεβαίωση, Εικόνα 5.46.



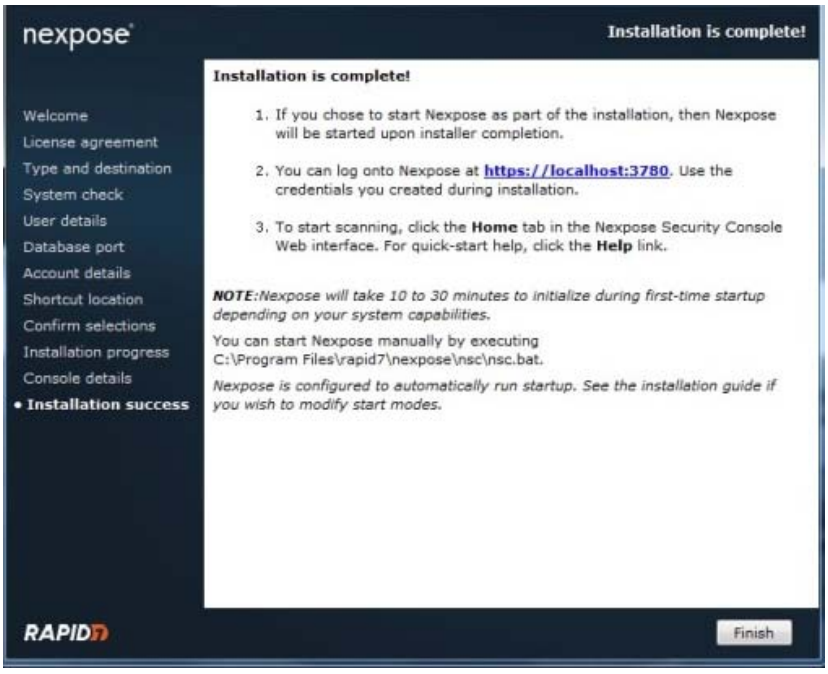
Εικόνα 5.46: Επισκόπηση επιλογών εγκατάστασης.

8. Με την επιβεβαίωση των επιλογών αρχίζει η εγκατάσταση του εργαλείου, Εικόνα 5.47.



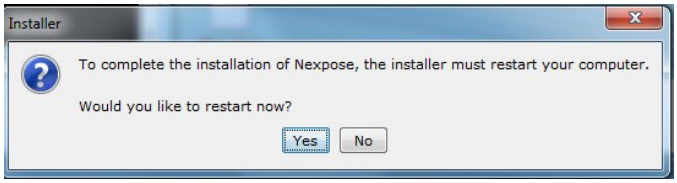
Εικόνα 5.47: Έναρξη διαδικασίας εγκατάστασης,

9. Μετά το πέρας της εγκατάστασης, παρουσιάζεται το μήνυμα επιβεβαίωσης, το οποίο περιλαμβάνει χρήσιμες πληροφορίες για την συνέχεια. Ενημερώνει τον χρήστη για τον τρόπο πρόσβασης στο εργαλείο, με την πλοήγηση στην διεύθυνση https://localhost:3780. Επίσης επιβεβαιώνει ότι οι υπηρεσίες του Nexpose έχουν ρυθμιστεί από το πρόγραμμα εγκατάστασης να εκκινούν αυτόματα, αλλά μπορούν, αν χρειαστεί να γίνουν και κατ' εντολή εκτελώντας το αρχείο **nsc.bat** το οποίο βρίσκεται στο φάκελο **C:\Program Files\rapid7\nexpose\nsc.** Επιπρόσθετα γίνεται ενημέρωση για το ότι το Nexpose, όταν εκτελεστεί για πρώτη φορά, πιθανός να χρειαστεί από 10 μέχρι 30 λεπτά για να είναι έτοιμο για χρήση, Εικόνα 5.48.



Εικόνα 5.48: Επιβεβαίωση ολοκλήρωσης διαδικασίας εγκατάστασης.

10. Για να ολοκληρωθεί η εγκατάσταση, το πρόγραμμα εγκατάστασης απαιτεί την επανεκκίνηση του συστήματος, Εικόνα 5.49.

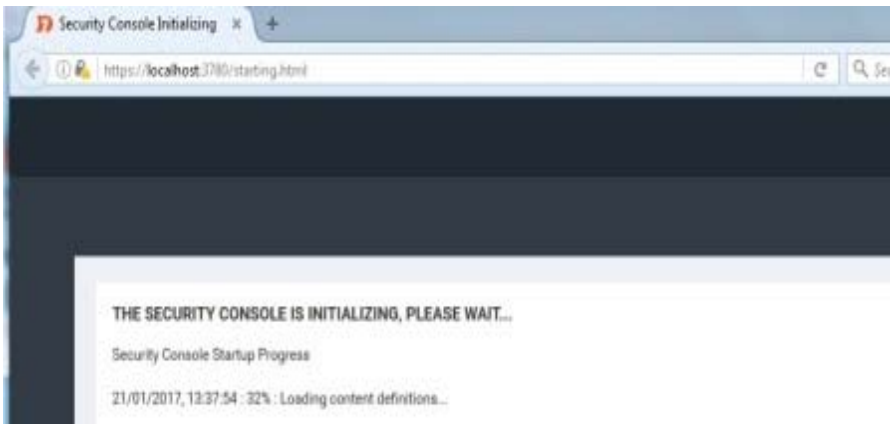


Εικόνα 5.49: Διάλογος επιβεβαίωσης για επανεκκίνηση του συστήματος.

11. Μετά την επανεκκίνηση του συστήματος το εικονίδιο του εργαλείου παρουσιάζεται στην επιφάνεια εργασίας, Εικόνα 5.50.

Εικόνα 5.50: Εικονίδιο εκκίνησης εργαλείου Nexpose.

12. Τρέχοντας το εργαλείο, ανοίγει ο φυλλομετρητής και ξεκινά η διαδικασία εκκίνησης, Εικόνα 5.51. Όπως έχει προαναφερθεί στο βήμα 9, η διαδικασία αυτή, την πρώτη φορά εκκίνησης του εργαλείου, μπορεί να χρειαστεί από 10 μέχρι 30 λεπτά. Στην προκειμένη περίπτωση χρειάστηκε 15 λεπτά για να ολοκληρωθεί.



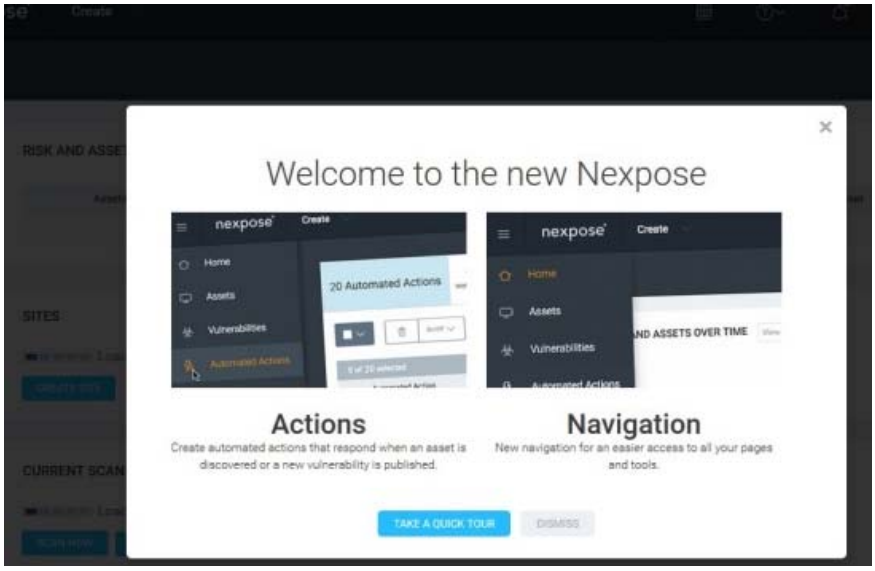
Εικόνα 5.51: Έναρξη διαδικασίας εκκίνησης.

Χρήση

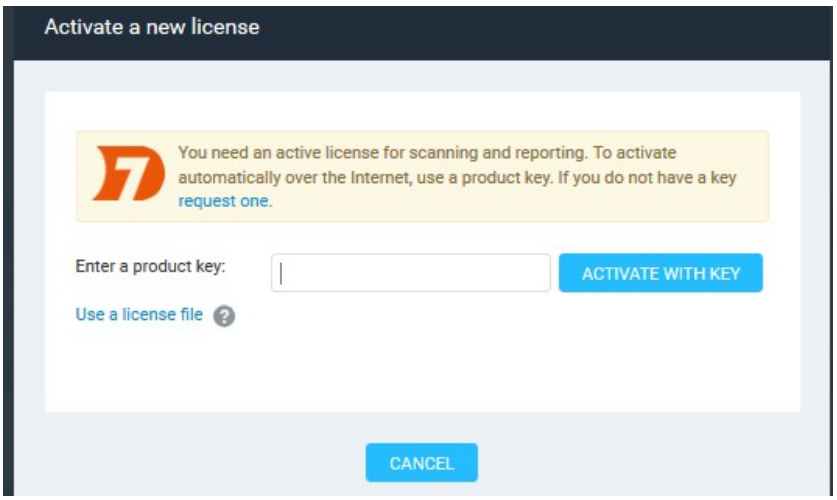
1. Με την ολοκλήρωση της διαδικασίας εκκίνησης του εργαλείου, παρουσιάζεται η οθόνη πρόσβασης, Εικόνα 5.52.

Εικόνα 5.52: Οθόνη πρόσβασης στο εργαλείο Nexpose.

2. Χρησιμοποιώντας τα στοιχεία πρόσβασης που έχουν δημιουργηθεί κατά την διαδικασία εγκατάστασης, βήμα 5, γίνεται μετάβαση στην αρχική σελίδα το εργαλείου, Εικόνα 5.53. Εδώ θα ζητηθεί και το κλειδί χρήσης, Εικόνα 5.54, του λογισμικού, που έχει σταλεί ηλεκτρονικά στο email, το οποίο έχει καταχωρηθεί κατά την διαδικασία εγγραφής, στην ιστοσελίδα του Nexpose.

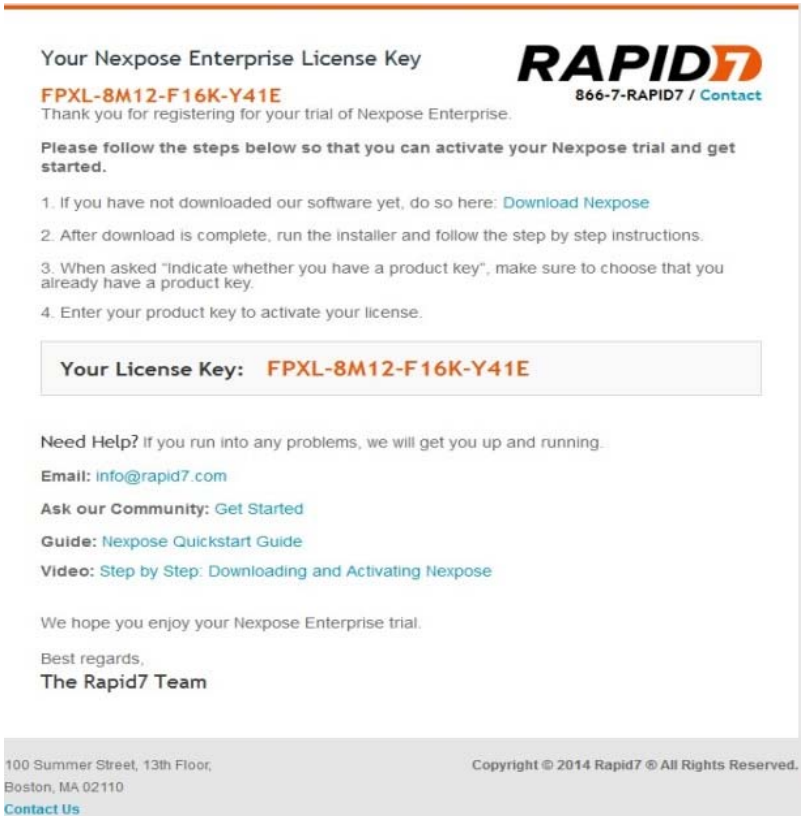


Εικόνα 5.53: Αρχική σελίδα εργαλείου Nexpose.



Εικόνα 5.54: Οθόνη καταχώρησης κωδικού άδειας χρήσης.

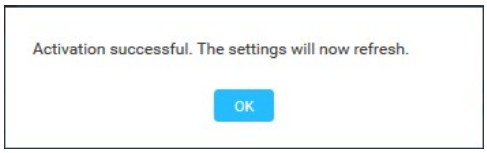
Παρατίθεται, Εικόνα 5.55, το ηλεκτρονικό μήνυμα το οποίο έχει παραλειφθεί από την Rapid 7 και το οποίο περιλαμβάνει το κλειδί άδειας χρήσης του εργαλείου Nexpose.



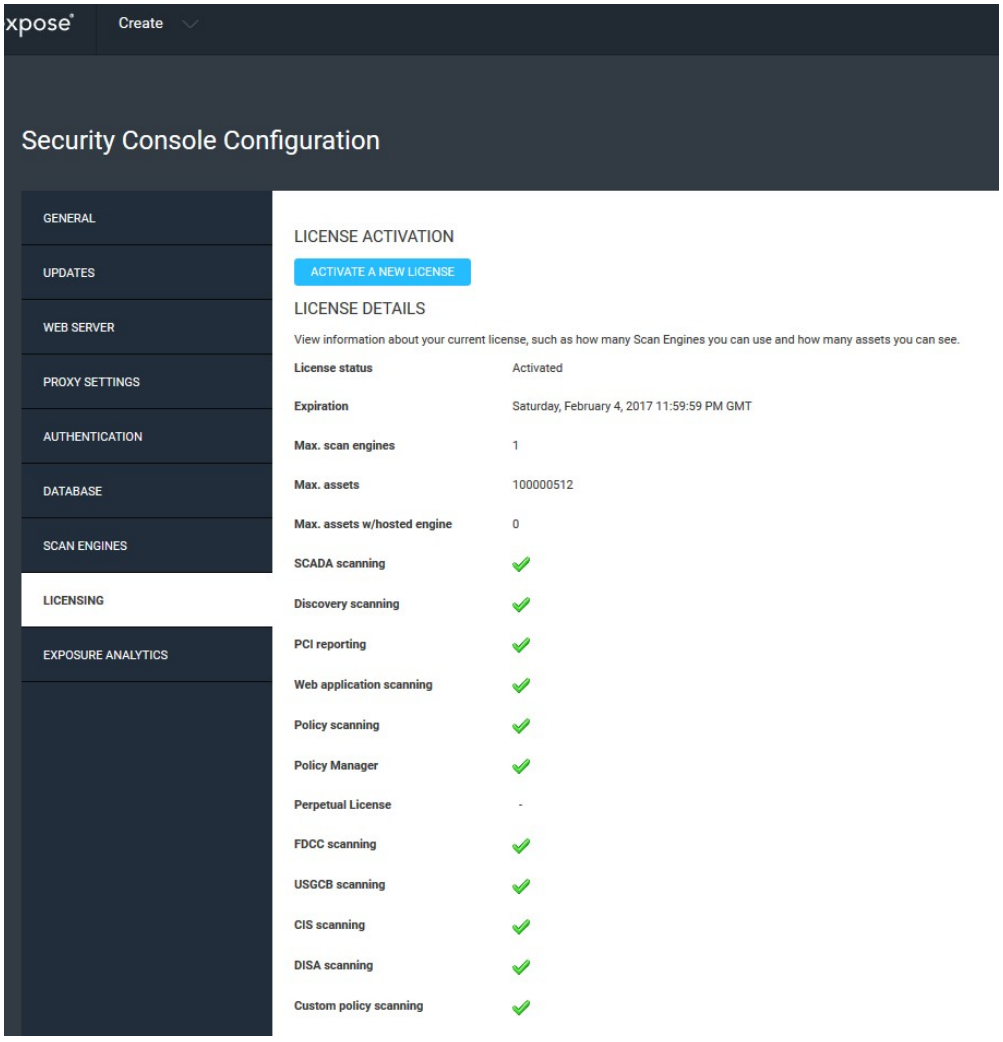
Εικόνα 5.55: Ληφθέν ηλ. μήνυμα ταχυδρομείου για το κλειδί άδειας χρήσης από Rapid 7.

3. Ακολούθως διενεργείται η διαδικασία ενεργοποίησης του εργαλείου, Εικόνα 5.56, Εικόνα 5.57 και Εικόνα 5.58.

Εικόνα 5.56: Εκκίνηση διαδικασίας ενεργοποίησης.

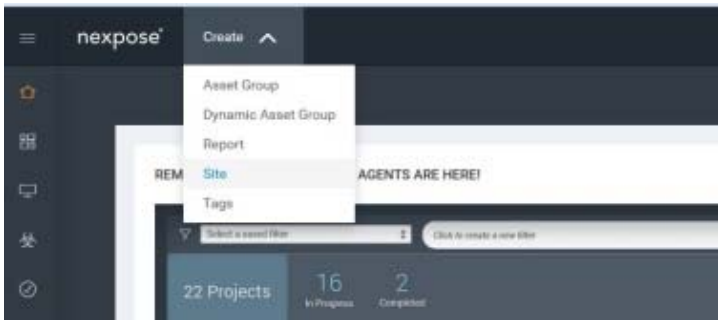


Εικόνα 5.57: Επιβεβαίωση διαδικασίας ενεργοποίησης.



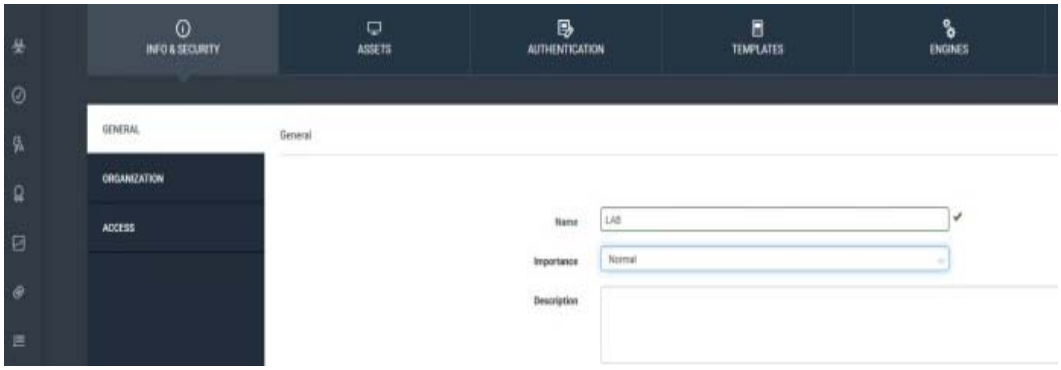
Εικόνα 5.58: Επιβεβαίωση διαδικασίας ενεργοποίησης.

4. Από την οριζόντια γραμμή εργαλείων επιλέγεται το “Create” και στην συνέχεια η επιλογή “Site”, για την δημιουργία ομάδας υπό διερεύνησης περιουσιακών στοιχείων, Εικόνα 5.59.



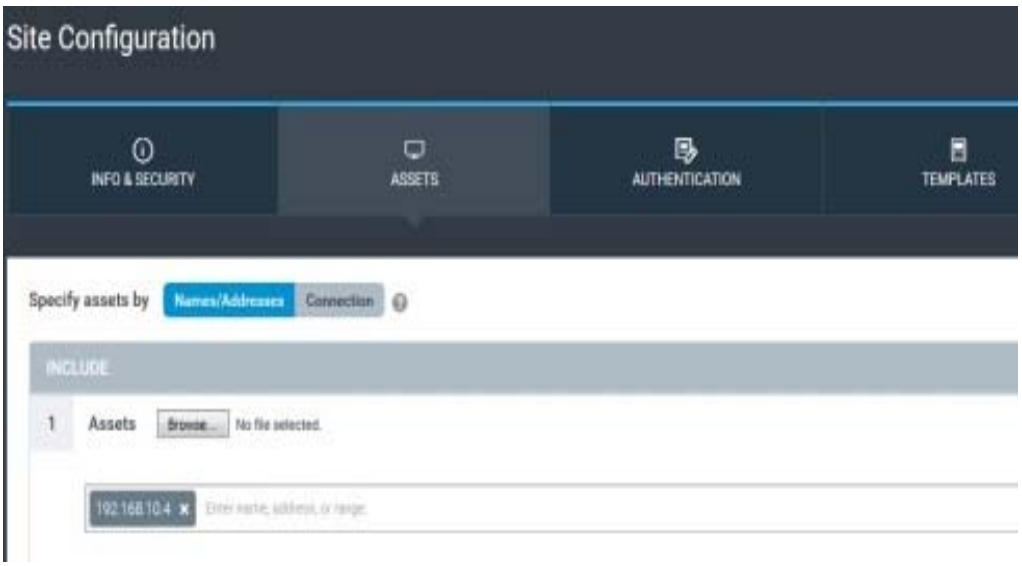
Εικόνα 5.59: Επιλογή δημιουργίας νέας ομάδας περιουσιακών στοιχείων.

5. Στην κατηγορία “Info and Security” καταχωρούνται τα στοιχεία της ομάδας. Το όνομα της ομάδας, τα στοιχεία του οργανισμού στον οποίο ανήκει η συγκεκριμένη ομάδα (ιδιαίτερα χρήσιμο σε μεγάλους πολυεθνικούς οργανισμούς), το άτομο επικοινωνίας, ακόμη και ο διαχειριστής ή οι διαχειριστές που μπορούν μέσο του Nexpose να έχουν πρόσβαση στα στοιχεία της συγκεκριμένης ομάδας, Εικόνα 5.60.



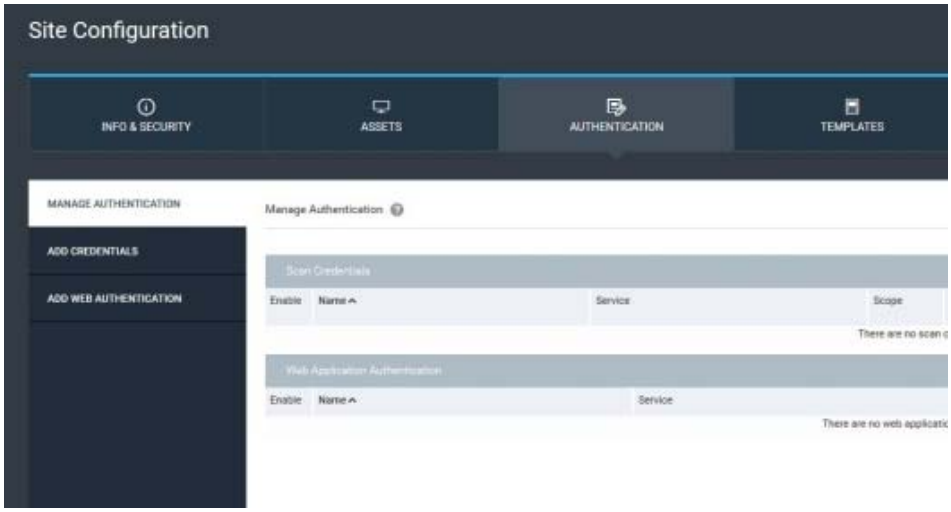
Εικόνα 5.60: Οθόνη καταχώρησης στοιχείων ομάδας περιουσιακών στοιχείων.

6. Εν συνεχεία, στην κατηγορία “Assets”, καταχωρούνται τα περιουσιακά στοιχεία της ομάδας. Μπορούν να καταχωρηθούν είτε σαν μονάδες με το IP address ή το DNS name τους, είτε σαν σύνολα στοιχείων χρησιμοποιώντας IP range ή να γίνουν upload από ένα αρχείο. Στην προκειμένη περίπτωση έχει καταχωρηθεί το IP του Metasplotable, που στην δεδομένη στιγμή είναι το 192.168.10.4, Εικόνα 5.61.



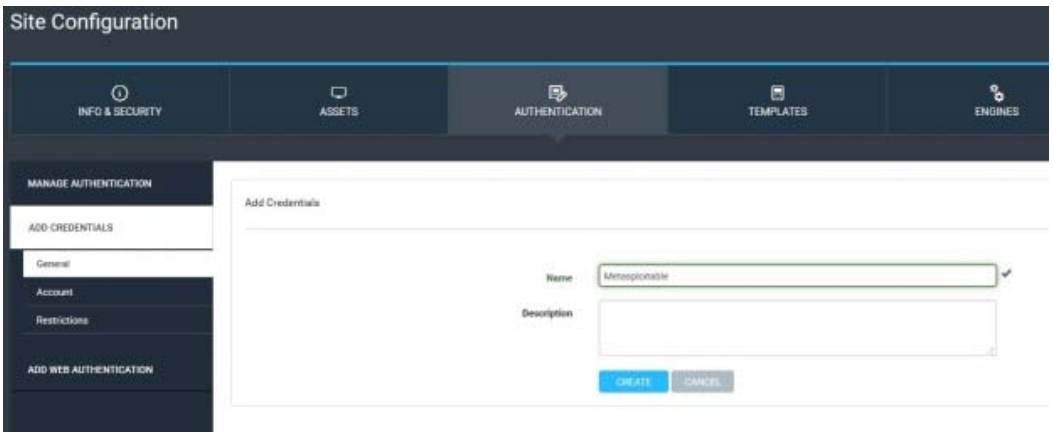
Εικόνα 5.61: Οθόνη καταχώρησης περιουσιακών στοιχείων.

7. Στην κατηγορία "Authentication", Εικόνα 5.62, εάν ο διαχειριστής επιθυμεί να έχει όσο το δυνατό περισσότερες πληροφορίες για τα υποδιεύθυνση περιουσιακά στοιχεία, μπορεί να καταχωρίσει στοιχεία πρόσβασης, διαχειριστή λόγου χάρη και να τα χρησιμοποιήσει κατά την διερεύνηση.

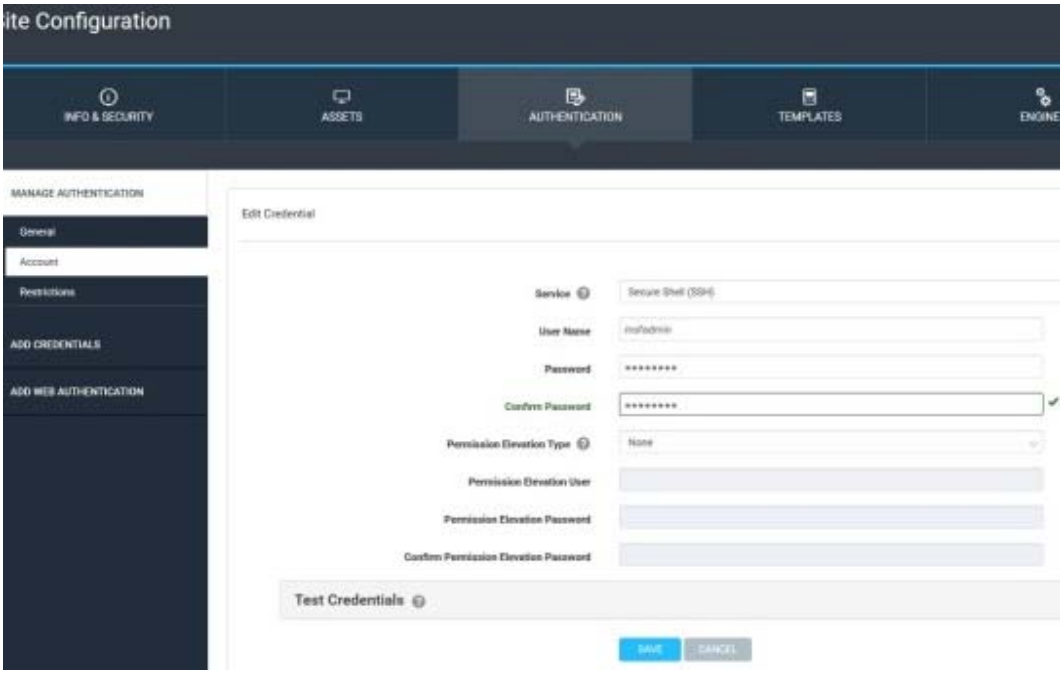


Εικόνα 5.62: Οθόνη καταχώρησης διαπιστευτηρίων διερεύνησης.

8. Στη παρούσα μεταπτυχιακή διατριβή θα χρησιμοποιηθούν τα root στοιχεία πρόσβασης του Metasploitable, Εικόνα 5.63 και Εικόνα 5.64.

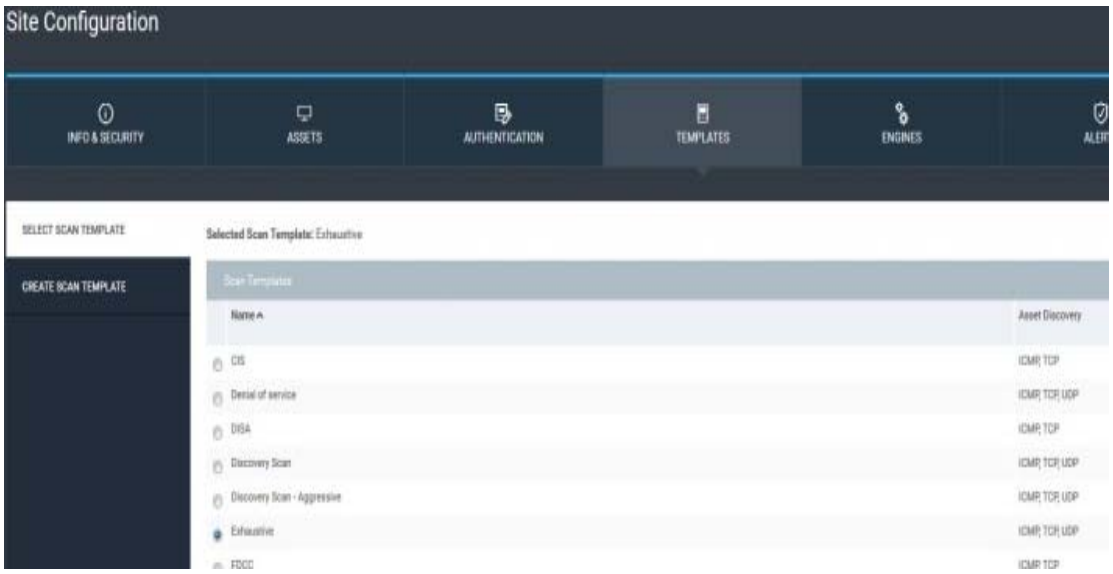


Εικόνα 5.63: Οθόνη δημιουργίας καινούργια εγγραφής διαπιστευτηρίων διερεύνησης.



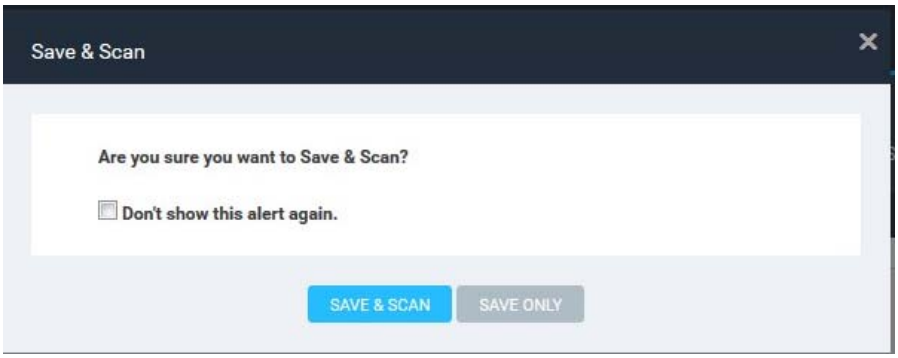
Εικόνα 5.64: Οθόνη καταχώρησης στοιχείων των διαπιστευτηρίων διερεύνησης.

9. Ακολούθως στην κατηγορία "Templates", γίνεται η επιλογή του τύπου διερεύνησης που θα χρησιμοποιηθεί. Η επιλογή "Exhaustive" έχει επιλεγεί, η οποία θα διερευνήσει το σύστημα σε βάθος και η οποία παίρνει το περισσότερο χρόνο για να ολοκληρωθεί από τις υπόλοιπες επιλογές διερεύνησης, Εικόνα 5.65.

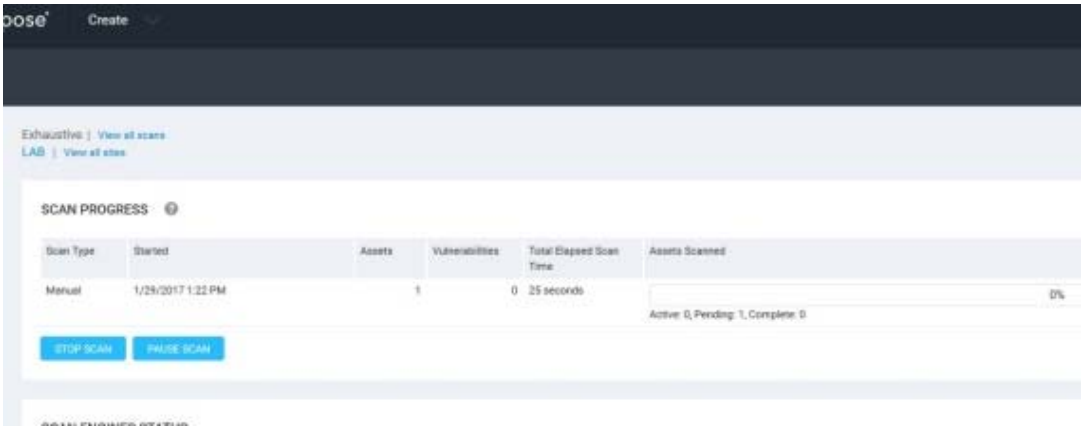


Εικόνα 5.65: Οθόνη επιλογής τύπου διερεύνησης.

10. Εν συνεχεία επιλέγεται το "Save & Scan" για να αποθηκευθούν οι επιλογές που έχουν γίνει, Εικόνα 5.66 και για να ξεκινήσει η διεργασία τις ανεύρεσης των ευπαθειών του Metasploitable, Εικόνα 5.67.



Εικόνα 5.66: Οθόνη επιβεβαίωσης φύλαξης στοιχείων και εκκίνησης διερεύνησης .

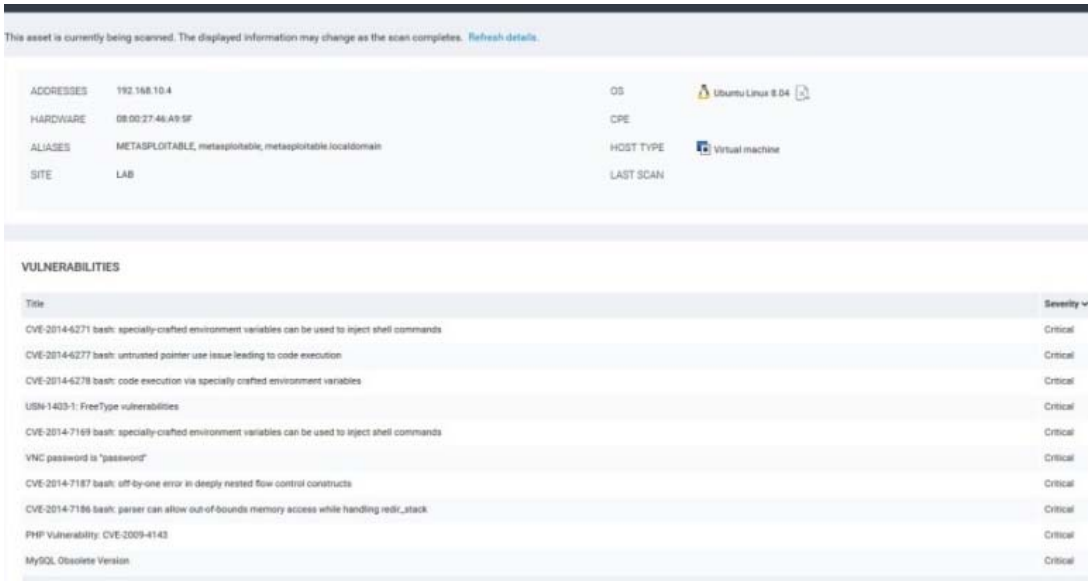


Εικόνα 5.67: Διεργασία ανίχνευσης ευπαθειών εν ενεργεία.

11. Μετά από κάποιο χρονικό διάστημα, στην προκειμένη περίπτωση, μετά την πάροδο 20 λεπτών, παρουσιάζεται το ανευρεθέν σύστημα, Εικόνα 5.68.

Εικόνα 5.68: Παρουσίαση ανευρεθέντος συστήματος (Metasploitable).

12. Κάνοντας κλικ, είτε στο IP, είτε στο όνομα του συστήματος, διαφαίνονται τα μέχρι στιγμής στοιχεία που έχουν ανευρεθεί, όπως το λειτουργικό του σύστημα, ο τύπος του συστήματος, τα εγκαταστημένα προγράμματα που έχει, ποίες υπηρεσίες τρέχουν και σε ποια θύρα, οι λογαριασμοί χρηστών που υπάρχουν δημιουργημένοι στο σύστημα κτλ. Επίσης παρουσιάζονται και οι τυχών ευπάθειες του, ταξινομημένες με το βαθμό σοβαρότητάς τους, ξεκινώντας από τις πιο κρίσιμες, Εικόνα 5.69.



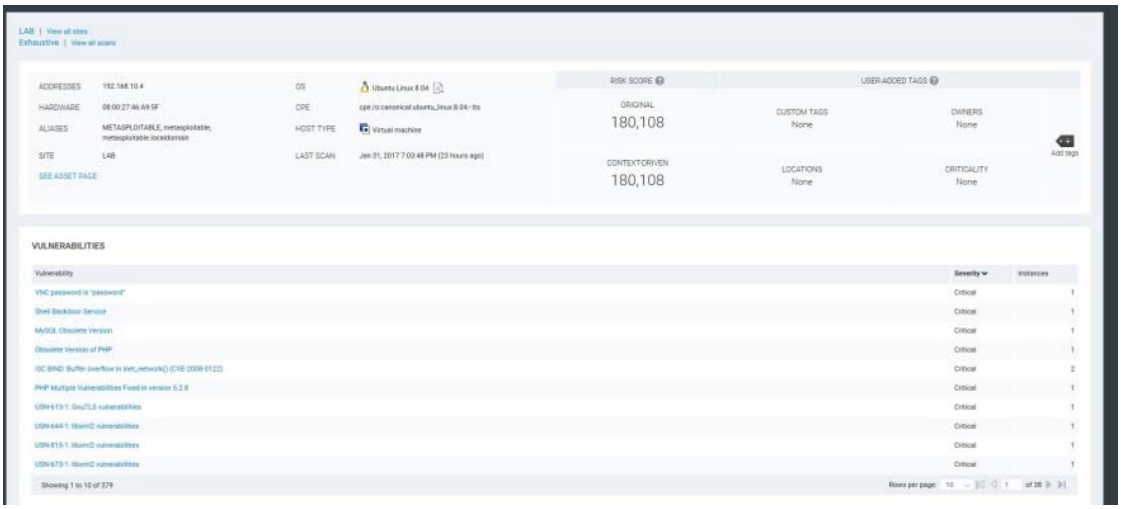
Εικόνα 5.69: Παρουσίαση αποτελεσμάτων διερεύνησης πριν από το πέρας της διεργασίας.

13. Με την ολοκλήρωση της διερεύνησης του συστήματος, παρουσιάζονται κάποιες λεπτομέρειες σε μορφή πίνακα για την διερεύνηση αυτή. Όπως το πόσες ευπάθειες

έχουν ανευρεθεί, ο χρόνος που χρειάστηκε το σύστημα να διεκπεραιώσει τη διαδικασία διερεύνησης, το εάν η διερεύνηση ολοκληρώθηκε επιτυχώς και ούτω καθεξής, Εικόνα 5.70.

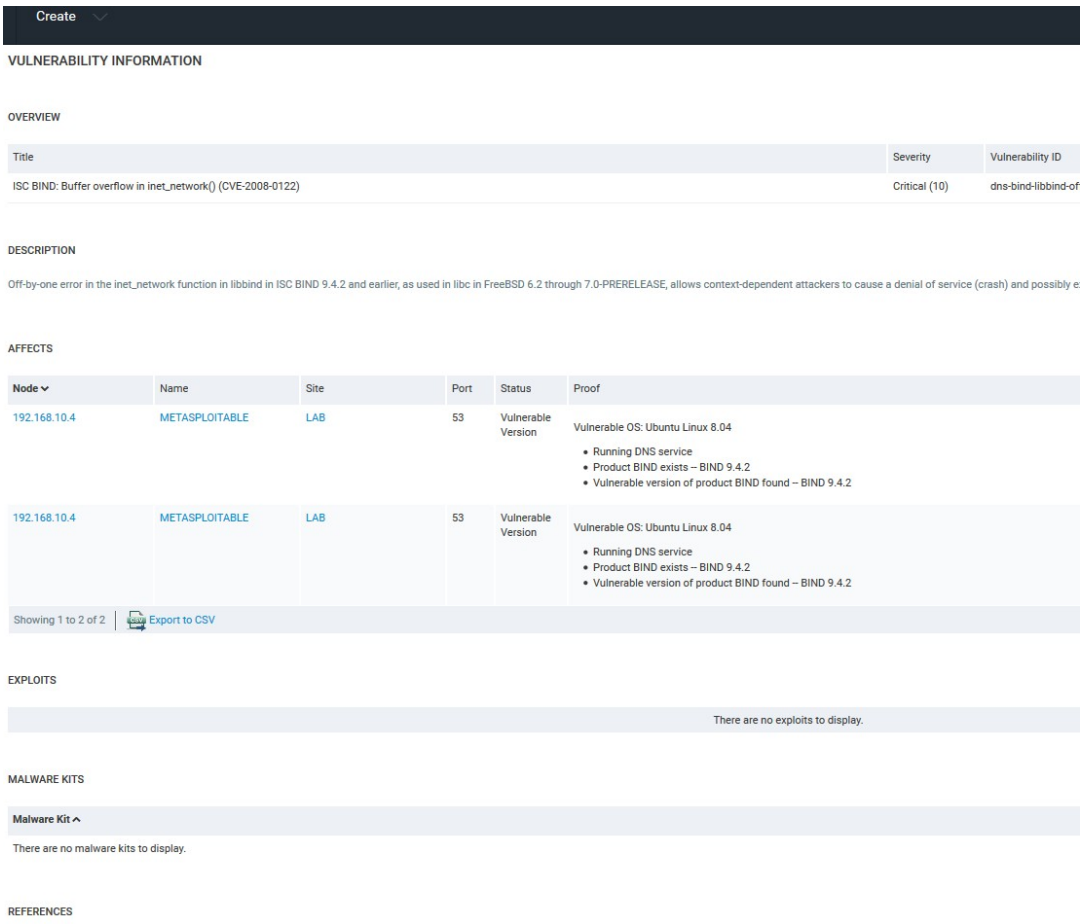
Εικόνα 5.70: Ολοκλήρωση διεργασίας διερεύνησης.

14. Κάνοντας κλικ είτε στο IP, είτε στο όνομα του συστήματος, εμφανίζεται η οθόνη με τα στοιχεία που έχουν συλλεχθεί για το υπό διερεύνηση σύστημα. Διαφαίνεται ότι το σύστημα αυτό είναι μια εικονική μηχανή (Virtual) με λειτουργικό σύστημα Ubuntu Linux 8.04 και η οποία έχει 379 ευπάθειες, Εικόνα 5.71.



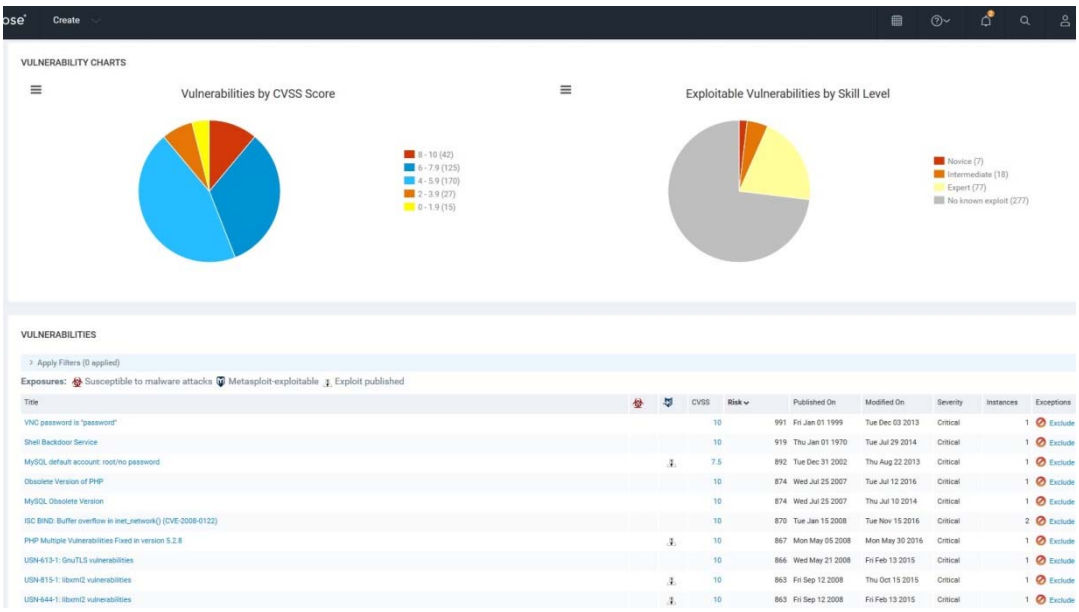
Εικόνα 5.71: Παρουσίαση αποτελεσμάτων διερεύνησης μετά το πέρας της διεργασίας.

15. Επιλέγοντας κάποια από τις ανευρεθείσες ευπάθειες, στην προκειμένη περίπτωση, την ευπάθεια με τίτλο “ISC BIND: Buffer overflow in inet_network() (CVE-2008-0122)”, αποκαλύπτονται περισσότερες πληροφορίες για αυτή. Ο διαχειριστής μπορεί να μάθει για την κρισιμότητα της ευπάθειας, ποιες υπηρεσίες του συστήματος επηρεάζονται, εάν υπάρχουν διαθέσιμα εργαλεία εκμετάλλευσης της ευπάθειας αυτής και ποια διαθέσιμη λύση υπάρχει για την αντιμετώπισή της, Εικόνα 5.72.



Εικόνα 5.72: Παρουσίαση πληροφοριών για την ευπάθεια "ISC BIND: Buffer overflow in inet_network() (CVE-2008-0122)".

16. Επιλέγοντας από το κυρίως μενού την κατηγορία "Vulnerabilities", παρουσιάζονται περισσότερες πληροφορίες για τις ανευρεθέν ευπάθειες. Παρουσιάζονται σε γράφημα με βάση την κρισιμότητα τους, όπως αυτές αξιολογούνται από το CVSS Score και σε ένα δεύτερο γράφημα με βάση το επίπεδο της γνώσης που πρέπει να διαθέτει ο επιτιθέμενος για τις εκμεταλλευτεί. Επιπρόσθετα σε ένα πίνακα ο διαχειριστής μπορεί να εντοπίσει τις ευπάθειες που έχουν δημοσιευθεί σε site ευπαθειών ή αν είναι εκμεταλλεύσιμες από το Metasploit με την χρήση του ανάλογου κώδικα (Exploitable), Εικόνα 5.73.

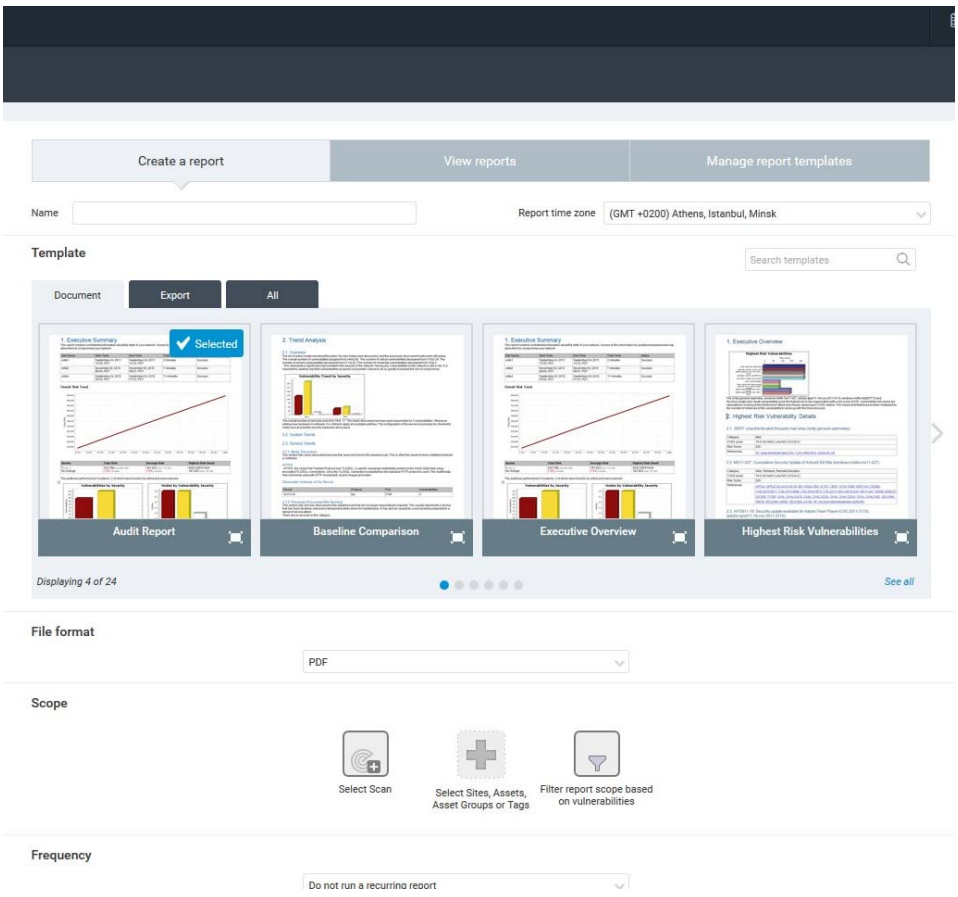


Εικόνα 5.73: Παρουσίαση ευπαθειών σε μορφή γραφήματος.

17. Στην συνέχεια ο διαχειριστής έχει την ευχέρεια δημιουργίας και εξαγωγής μιας κατάστασης των ευπαθειών με βάση την ομάδα (διευθυντική ομάδα, ομάδα ελέγχου ασφαλείας κτλ) που θα ήθελε να παρουσιάσει αυτήν την κατάσταση ή για να αντλήσει συγκεκριμένης πληροφορίες, όπως λόγου χάρη, ποία είναι τα δέκα περιουσιακά στοιχεία με τις κρισιμότερες ευπάθειες.

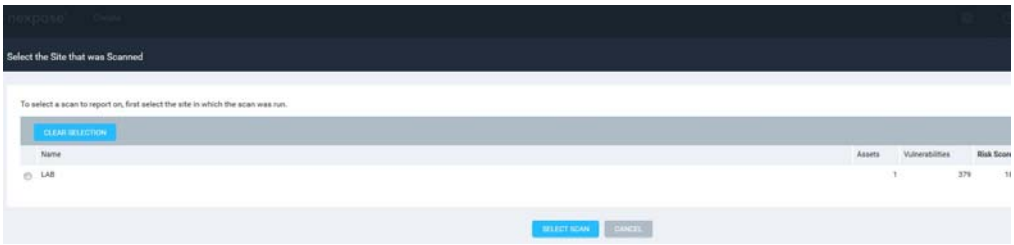
Το Nexpose διαθέτει 24 διαθέσιμα είδη έτοιμων καταστάσεων, επιπρόσθετα ο διαχειριστής μπορεί να δημιουργήσει δικές του καταστάσεις, είτε ξεκινώντας από το μηδέν, είτε τροποποιώντας κάποια από τις υφιστάμενες καταστάσεις.

Η πρόσβαση στις καταστάσεις πραγματοποιείται από το κυρίως μενού και τη κατηγορία “Reports”. Αρχικά δίδεται ένα όνομα στη κατάσταση και στη συνέχεια επιλέγεται η μορφή αυτής. Ακολούθως επιλέγεται ο τύπος του αρχείου, εάν θα είναι PDF, RTF,XML,HTML ή Text. Στην προκείμενη περίπτωση έχει επιλεγεί η κατάσταση “Audit Report” και ο τύπος του αρχείου “PDF”, Εικόνα 5.74.



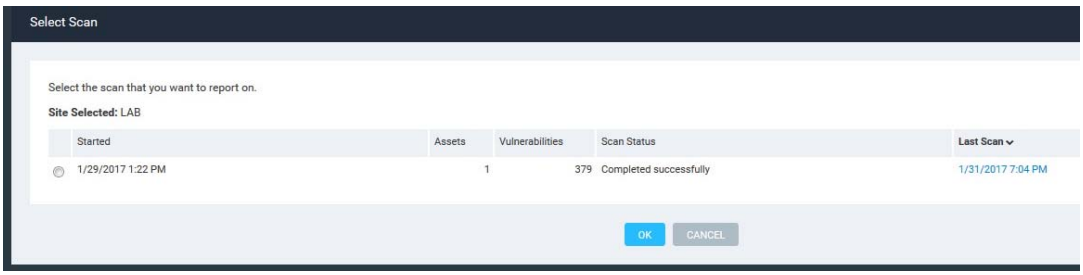
Εικόνα 5.74: Οθόνη δημιουργίας κατάστασης ανευρεθέν ευπαθειών.

18. Στην συνέχεια επιλέγεται η επιλογή "Select Scan" όπου θα επιλεγεί η διερεύνηση για την οποία ο διαχειριστής επιθυμεί να δημιουργήσει την κατάσταση. Ακολούθως επιλέγεται η επιθυμητή ομάδα των περιουσιακών στοιχείων. Στην προκειμένη περίπτωση επιλέγεται η ομάδα "LAB", Εικόνα 5.75.



Εικόνα 5.75: Οθόνη επιλογής περιουσιακών στοιχείων για την δημιουργία κατάστασης ανευρεθέν ευπαθειών.

19. Το επόμενο βήμα, είναι η επιλογή της διερεύνησης, Εικόνα 5.76.



Εικόνα 5.76: Οθόνη επιλογής διερεύνησης για την δημιουργία κατάστασης ανευρεθέν ευπαθειών.

20. Μετά την επιλογή της διερεύνησης, δημιουργείται το PDF αρχείο της κατάστασης αξιολόγησης των ευπαθειών της συγκεκριμένης ομάδας περιουσιακών στοιχείων, Εικόνα 5.77.

Εικόνα 5.77: Δημιουργία κατάστασης ανευρεθέν ευπαθειών σε pdf μορφή.

Η εξαχθείσα PDF κατάσταση με ονομασία "Nexpose Metasploitable Assesment Report 1", είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Nexpose".

5.2.4 Qualys Vulnerability Management

Το Qualys Vulnerability Management προσφέρεται ως υπηρεσία νέφους (Cloud) μειώνοντας έτσι το κόστος σε πόρους που εμπεριέχουν τα αντίστοιχα συμβατικά λογισμικά, καθώς επίσης περιορίζει και τα προβλήματα που τυχόν να προκύψουν από την εγκατάσταση ενός τέτοιου συστήματος, στο εσωτερικό δίκτυο ενός οργανισμού. Το Qualys VM μπορεί να εγκατασταθεί σε ιδιόκτητο καθώς και σε δημόσιο νέφος και να διαχειρίζεται πλήρως από την ομάδα της Qualys. Ως λύση νέφους είναι πάντα ενημερωμένη.

Προσφέρει συνεχή έλεγχο για εντοπισμό ευπαθειών, τις οποίες βάζει σε προτεραιοποίηση, βοηθώντας έτσι τον εκάστοτε οργανισμό να προστατεύσει τους μηχανογραφικούς του πόρους, τόσο εντός των κτηρίων της επιχείρησης, όσο και των απομακρυσμένων ή κινητών, αλλά και αυτών που πιθανός να βρίσκονται στο περιβάλλον νέφους της Azure ή του Amazon EC2. Επίσης αποστέλλει ειδοποιήσεις σε συγκεκριμένα επιλεγμένα άτομα της ομάδας ασφαλείας, για να προβούν σε άμεσες ενέργειες. Αυτό απαλλάσσει την ομάδα από το να περιμένει να "τρέξουν" σε συγκεκριμένο χρόνο οι έλεγχοι και στην συνέχεια να πρέπει να μελετήσει τις πιθανόν εκτενείς αναφορές για να προχωρήσει στις νενομισμένες ενέργειες.

Οι επί μέρους επικοινωνίες μεταξύ του Qualys VM και των πόρων του οργανισμού είναι κρυπτογραφημένες (End-to-End Encryption) επίσης το Qualys VM διατηρεί ισχυρούς ελέγχους πρόσβασης διασφαλίζοντας έτσι την ιδιωτικότητα των ανευρεθέν δεδομένων ασφαλείας.

Οι αναφορές για την ασφάλεια του οργανισμού μπορεί να διαμορφωθούν βάση του ρόλου του κάθε εμπλεκόμενου διαχειριστή. Επίσης μπορούν να δημιουργηθούν αναφορές οι οποίες να συνάδουν με τα ζητούμενα των ελεγκτών συμμόρφωσης. [18]

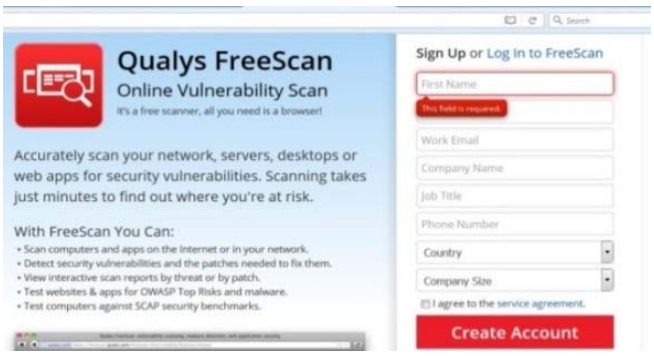
Εγκατάσταση και χρήση εργαλείου Qualys Vulnerability Management

Το Qualys Guard Express VM αποτελεί υπηρεσία νέφους η οποία μπορεί να επικοινωνεί με το εσωτερικό δίκτυο ενός οργανισμού με την χρήση εικονικών μηχανών.

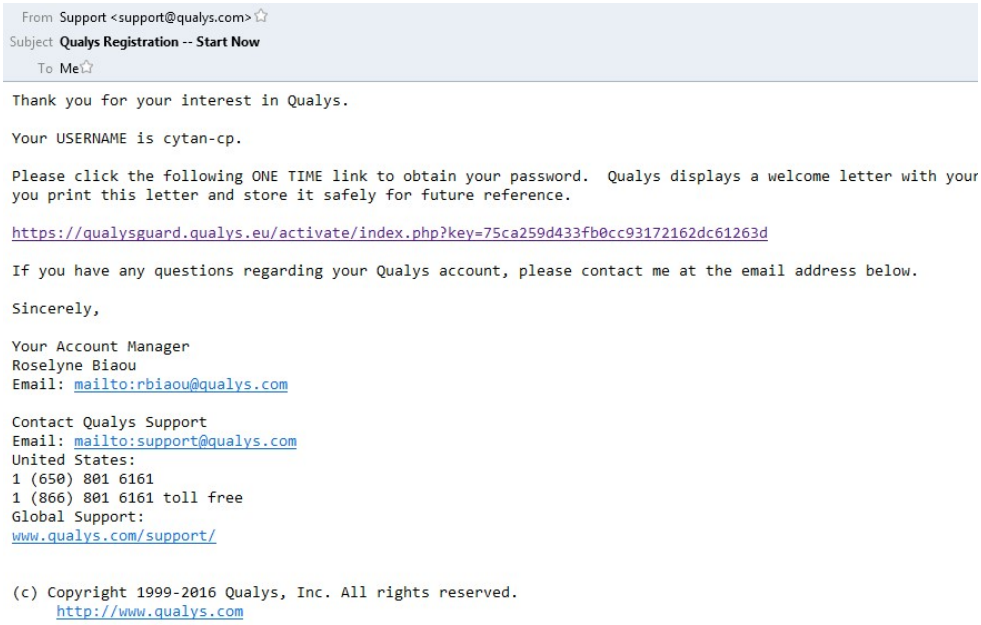
Στην παρούσα μεταπτυχιακή διατριβή έχει χρησιμοποιηθεί η εικονική μηχανή QualysGuard Virtual Scanner Appliance για χρήση με το Oracle VM VirtualBox Manager.

Εγκατάσταση

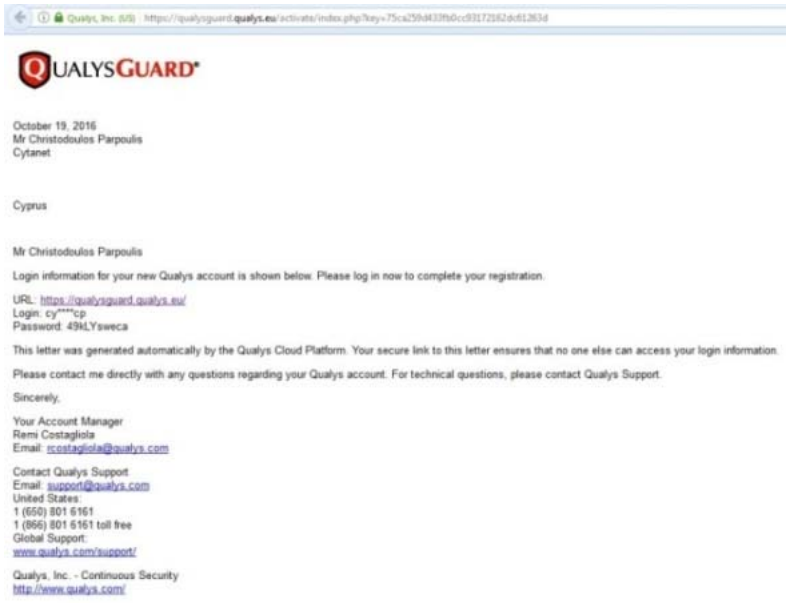
1. Μετά από την νενομισμένη εγγραφή στην ιστοσελίδα του εργαλείου για την απόκτηση άδειας χρήσης περιορισμένης διάρκειας, Εικόνα 5.78, γίνεται η παραλαβή του ηλεκτρονικού μηνύματος το οποίο περιλαμβάνει το όνομα χρήστη, Εικόνα 5.79, καθώς και πληροφορίες για την απόκτηση του κωδικού πρόσβασης, Εικόνα 5.80.



Εικόνα 5.78: Διαδικτυακή φόρμα αίτησης για την δημιουργία λογαριασμού χρήσης.



Εικόνα 5.79: Παραληφθέν ηλ. μήνυμα επιβεβαίωσης δημιουργίας λογαριασμού χρήσης.

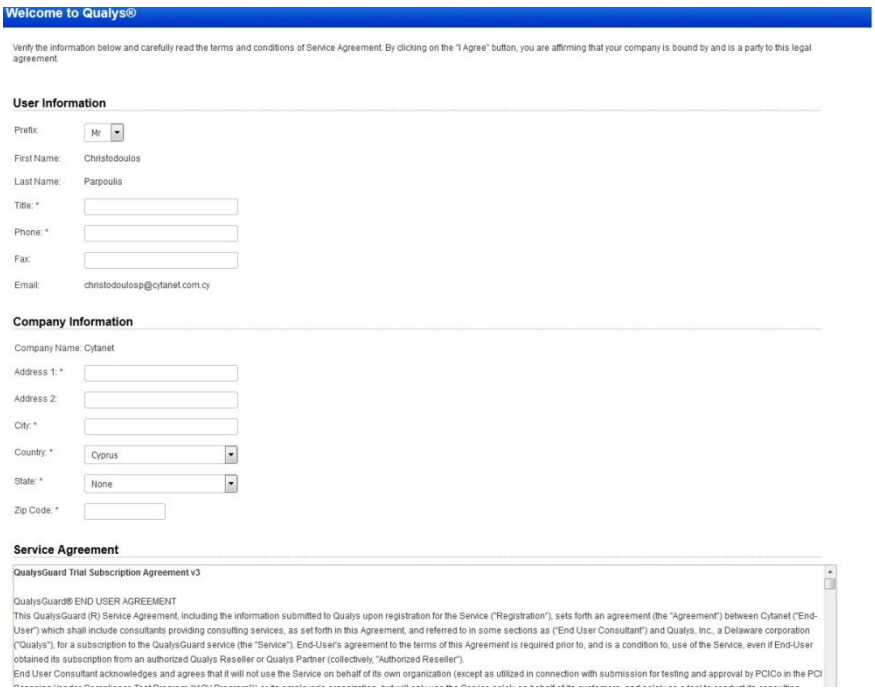


Εικόνα 5.80: Παραληφθέν ηλ. μήνυμα με κωδικό και οδηγίες πρόσβασης.

2. Μετά την πλοήγηση στην ιστοσελίδα της Qualys για την απόκτηση του κωδικού πρόσβασης, πραγματοποιείται πρόσβαση στο εργαλείο με την καταχώριση των στοιχείων αυθεντικοποίησης, Εικόνα 5.81.

Εικόνα 5.81: Διαδικτυακή οθόνη αυθεντικοποίησης του εργαλείου Qualys.

3. Ακολούθως καταχωρούνται τα προσωπικά και εταιρικά στοιχεία του χρήστη-διαχειριστή, Εικόνα 5.82.

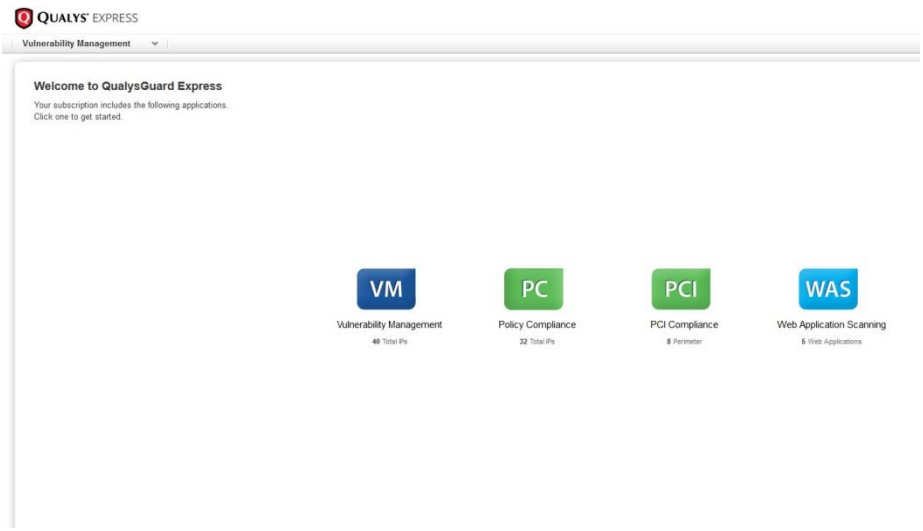


Εικόνα 5.82: Οθόνη καταχώρησης στοιχείων διαχειριστή.

4. Στην συνέχεια, για λόγους ασφαλείας, ζητείται η αλλαγή του κωδικού πρόσβασης και ακολούθως ζητείται για δεύτερη φορά η καταχώριση των στοιχείων αυθεντικοποίησης, Εικόνα 5.83.

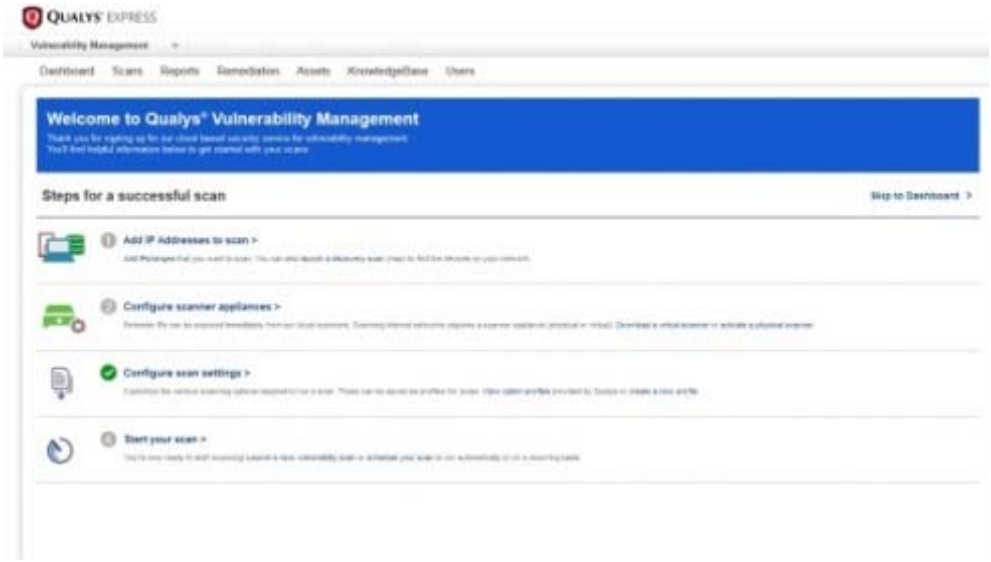
Εικόνα 5.83: Αλλαγή κωδικού πρόσβασης.

5. Μετά την αυθεντικοποίηση, εμφανίζεται η αρχική οθόνη του εργαλείου, Εικόνα 5.84. Εδώ παρουσιάζονται τα εργαλεία στα οποία έχει δοθεί άδεια χρήσης από την Qualys, για τον συγκεκριμένο λογαριασμό χρήστη. Το εργαλείο το οποίο μας ενδιαφέρει είναι το Vulnerability Management (VM).



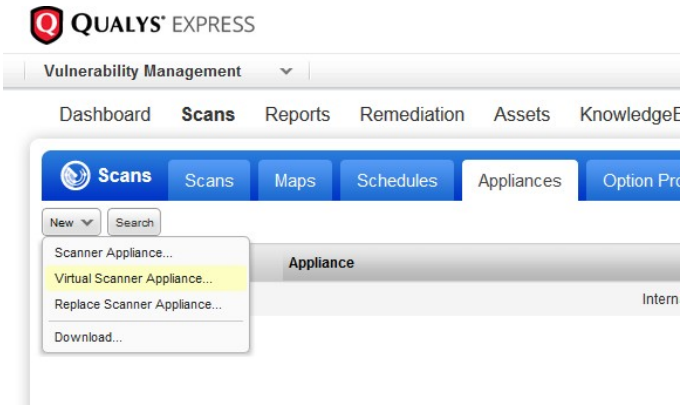
Εικόνα 5.84: Αρχική οθόνη εργαλείου Qualys.

6. Πατώντας στο εργαλείο VM παρουσιάζεται η αρχική οθόνη του Vulnerability Management, Εικόνα 5.85. Όπου από το κυρίως μενού επιλέγουμε την επιλογή "Scans".



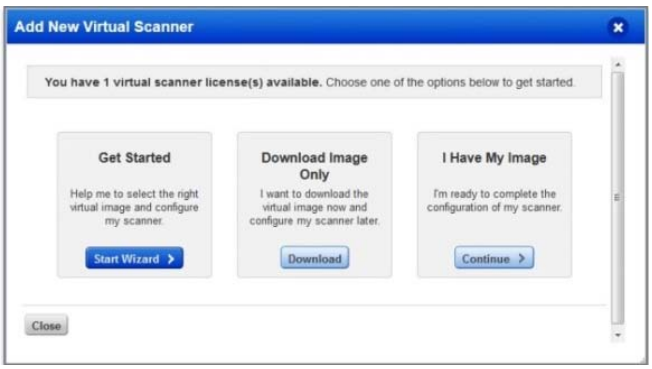
Εικόνα 5.85: Αρχική οθόνη εργαλείου Vulnerability Management.

7. Εν συνεχεία επιλέγουμε την επιλογή "Appliances" και ακολούθως την επιλογή "Virtual Scanner Appliance", Εικόνα 5.86. Στο στάδιο αυτό θα επακολουθήσει η διαδικασία εγκατάστασης και ενεργοποίησης της εικονικής μηχανής QualysGuard Virtual Scanner Appliance. Στο λογαριασμό αυτό έχει δοθεί δικαίωμα χρήσης σε μια μόνο εικονική μηχανή.



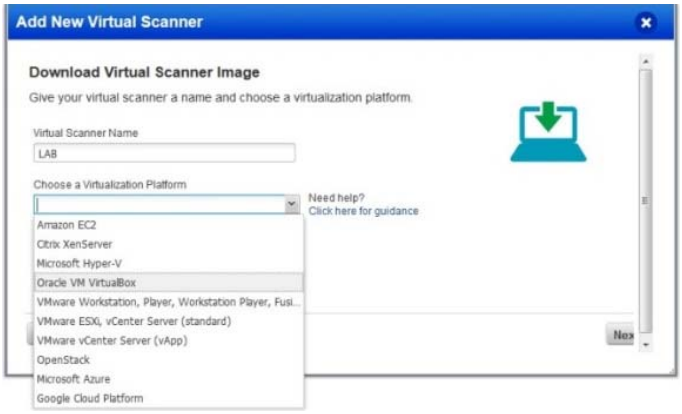
Εικόνα 5.86: Επιλογή διαδικασίας εγκατάστασης Virtual Scanner Appliance.

8. Στη οθόνη που παρουσιάζεται, Εικόνα 5.87, γίνεται η επιλογή "Start Wizard", όπου αρχίζει η διαδικασία επιλογής της κατάλληλης εικονικής μηχανής.



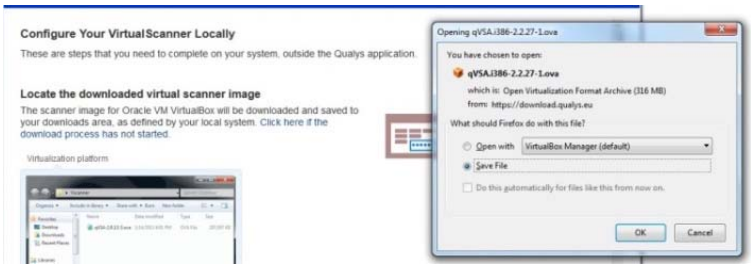
Εικόνα 5.87: Οθόνη επιλογής "κατεβάσματος" του Virtual Scanner Appliance.

9. Ακολούθως καταχωρείται ένα όνομα για την εικονική μηχανή, στην προκειμένη περίπτωση "LAB" και επιλέγεται η πλατφόρμα της εικονικής μηχανής, όπου εδώ επιλέγεται το "Oracle VM VirtualBox", Εικόνα 5.88.



Εικόνα 5.88: Επιλογή εικονικής μηχανής για κατέβασμα.

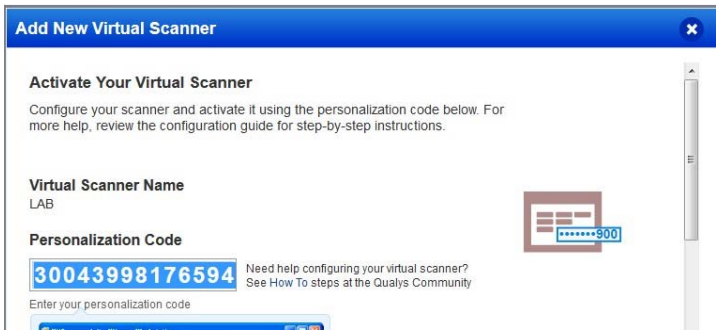
10. Στο επόμενο στάδιο διεκπεραιώνεται το κατέβασμα του αρχείου της εικονικής μηχανής, Εικόνα 5.89.



Εικόνα 5.89: Αποθήκευση αρχείου εικονικής μηχανής.

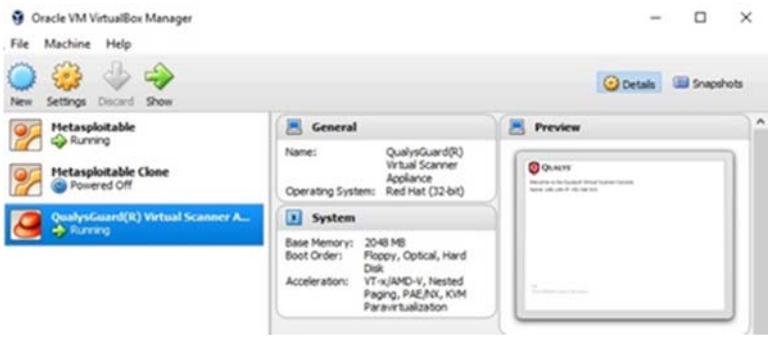
11. Εν συνεχεία η διαδικασία ενεργοποίησης της εικονικής μηχανής παρουσιάζει ένα μοναδικό κωδικό ο οποίος αντικατοπτρίζει την συγκεκριμένη εικονική μηχανή, Εικόνα

5.90. Ο κωδικός αυτός θα χρησιμοποιηθεί κατά την διαδικασία εγκατάστασης της εικονικής μηχανής.



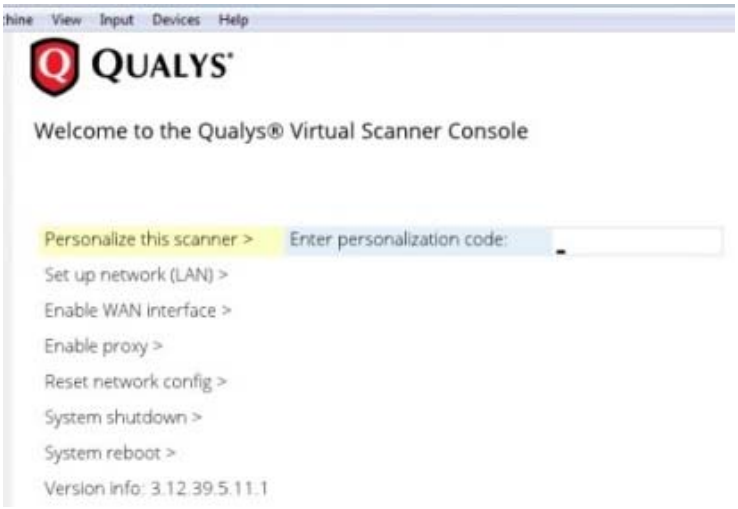
Εικόνα 5.90: Κωδικός ενεργοποίησης χρήσης εικονικής μηχανής.

12. Ακολούθως γίνεται η φόρτωση της εικονικής μηχανής "QualysGuard Virtual Scanner Appliance" στο Oracle VM VirtualBox Manager, Εικόνα 5.91. Εν συνεχεία τίθεται σε λειτουργία η εικονική μηχανή.



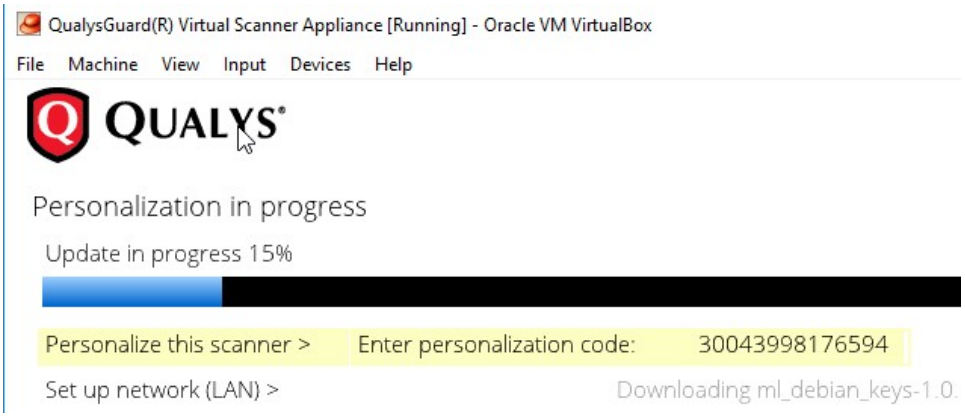
Εικόνα 5.91: Φόρτωση εικονικής μηχανής στο Oracle VirtualBox.

13. Μετά την εκκίνηση του QualysGuard Virtual Scanner Appliance, παρουσιάζεται η οθόνη των παραμέτρων του εργαλείου. Εδώ καταχωρείται ο μοναδικός κωδικός, ο οποίος έχει δοθεί στο στάδιο 11. Οι υπόλοιπες παράμετροι δεν αλλάζουν μιας και η εικονική μηχανή θα λάβει όλα τα στοιχεία του δικτύου από τον DHCP, Εικόνα 5.92.



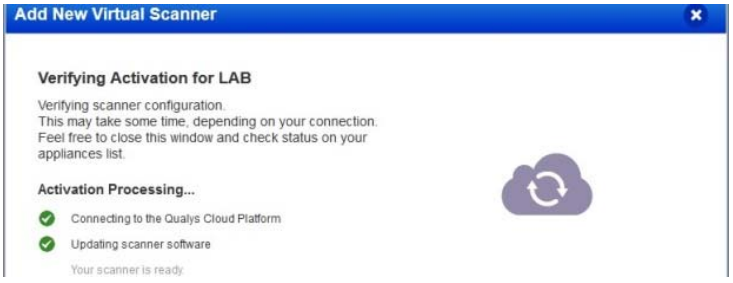
Εικόνα 5.92: Αρχική οθόνη εικονικής μηχανής Qualys Virtual Scanner.

14. Η διαδικασία ενεργοποίησης και σύνδεσης της εικονικής μηχανής με το εργαλείο νέφους VM της Qualys τίθεται σε λειτουργία, Εικόνα 5.93.



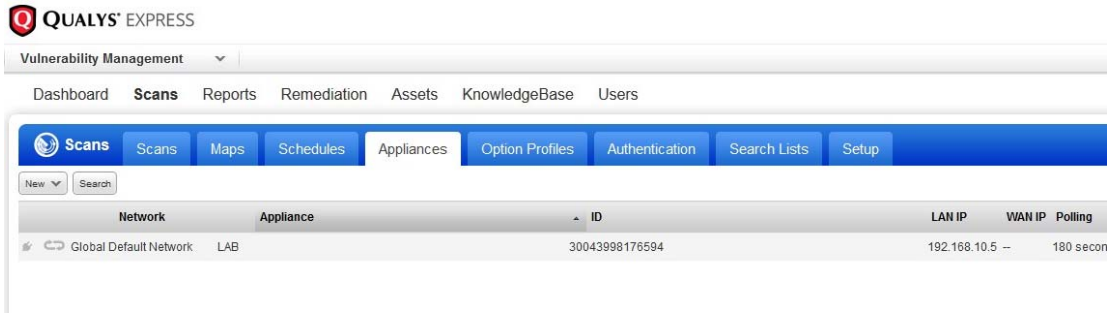
Εικόνα 5.93: Διαδικασία ενεργοποίησης σύνδεσης εικονικής μηχανής.

15. Με την ολοκλήρωση της διαδικασίας ενεργοποίησης και σύνδεσης της εικονικής μηχανής με το εργαλείο νέφους VM της Qualys, παρουσιάζεται το μήνυμα επιβεβαίωσης, Εικόνα 5.94.



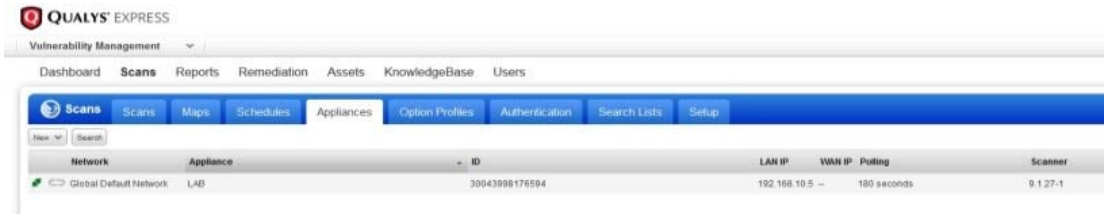
Εικόνα 5.94: Επιβεβαίωση σύνδεσης εικονικής μηχανής με το VM.

16. Επίσης παρουσιάζεται στον κατάλογο των συσκευών “Appliances”, του VM, η εικονική μηχανή, Εικόνα 5.95.



Εικόνα 5.95: Παρουσίαση εικονικής μηχανής στο κατάλογο συσκευών του VM.

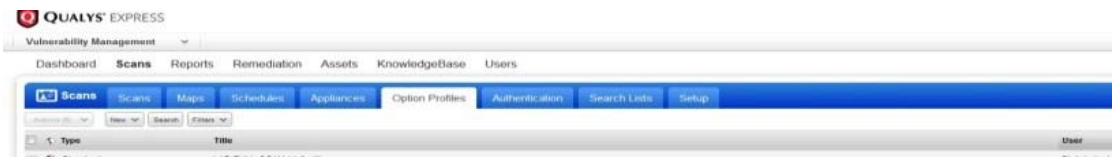
17. Μετά από πάροδο ενός ή δύο λεπτών, επιβεβαιώνεται η σύνδεση του εργαλείου με την εικονική μηχανή, παρουσιάζοντας το εικονίδιο πλησίον της εγγραφής καταχώρισης, Εικόνα 5.96.



Εικόνα 5.96: Επιβεβαίωση ενεργοποίησης σύνδεσης εικονικής μηχανής και VM.

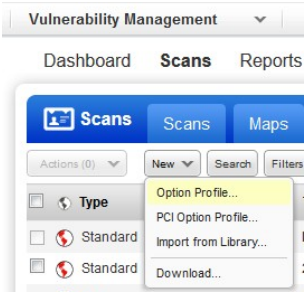
Χρήση

1. Από τον κατάλογο επιλογών τη επιλογής “Scans”, επιλέγεται η επιλογή “Option Profiles”, Εικόνα 5.97. Στο σημείο αυτό θα δημιουργηθεί το προφίλ επιλογών ανίχνευσης ευπαθειών, το οποίο θα χρησιμοποιηθεί από το εργαλείο, για την ανίχνευση των ευπαθειών του Metasploitable.



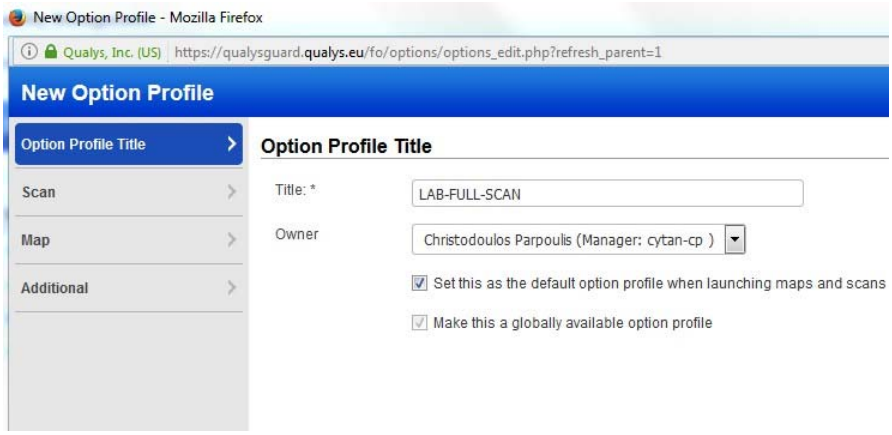
Εικόνα 5.97: Επιλογή δημιουργίας προφίλ ανίχνευσης ευπαθειών.

2. Στην συνέχεια επιλέγεται η επιλογή “New” και ακολούθως το “Option Profile”, Εικόνα 5.98.



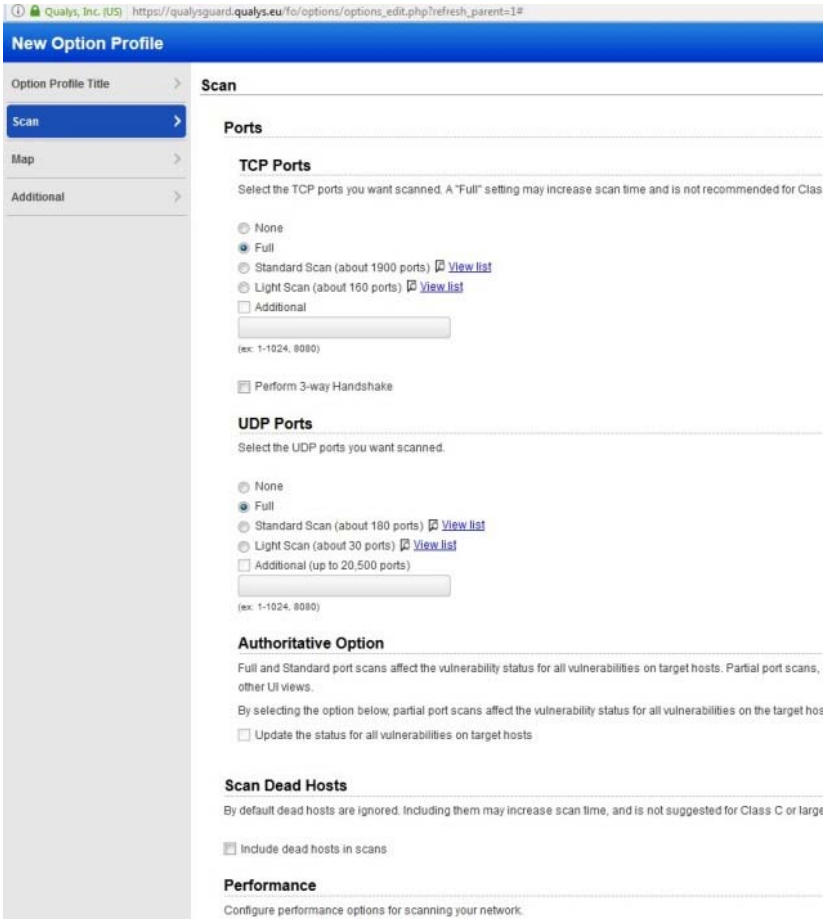
Εικόνα 5.98: Δημιουργία νέου προφίλ ανίχνευσης ευπαθειών.

3. Παρουσιάζεται η οθόνη “New Option Profile”, όπου καταχωρείται αρχικά το όνομα του προφίλ. Στην συγκεκριμένη περίπτωση το όνομα του προφίλ είναι “LAB-FULL-SCAN”, Εικόνα 5.99.



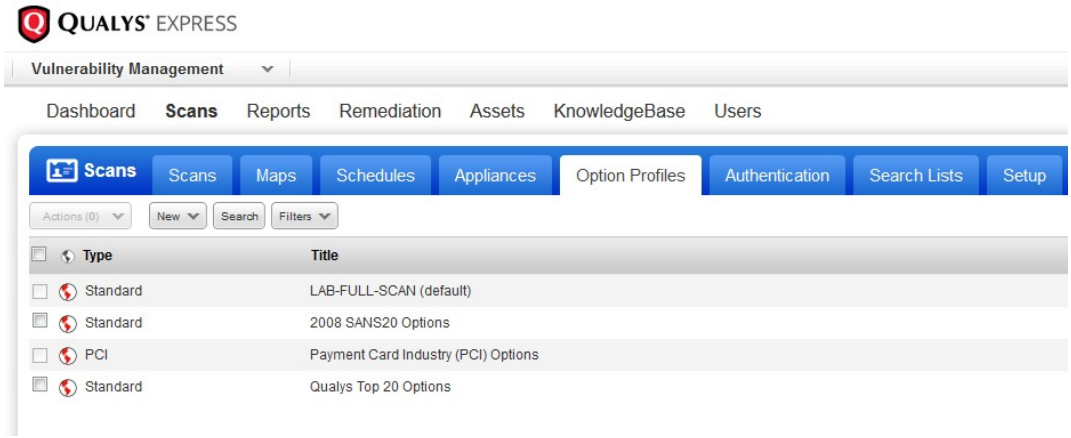
Εικόνα 5.99: Οθόνη καταχώρησης στοιχείων νέου προφίλ ανίχνευσης ευπαθειών.

4. Από το μενού στα αριστερά, επιλέγεται η επιλογή “Scan”. Εδώ καταχωρούνται όλες οι λεπτομερείς της διερεύνησης . Στη προκειμένη περίπτωση έχουν επιλεγεί όλες οι θύρες, TCP και UDP, για διερεύνηση, καθώς και η επιλογή αυθεντικοποίησης, Εικόνα 5.100. Ο λογαριασμός αυθεντικοποίησης θα δημιουργηθεί σε κατοπινό στάδιο.



Εικόνα 5.100: Οθόνη καταχώρησης λεπτομερειών διερεύνησης.

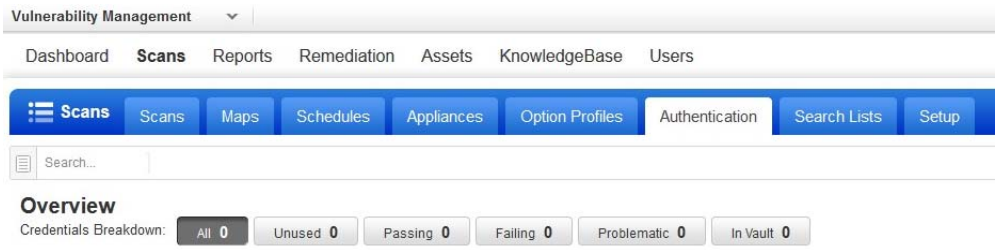
5. Το νεοδημιουργηθέν προφίλ προστίθεται στον κατάλογο των προφίλ του εργαλείου και είναι έτοιμο για επιλογή και χρήση, Εικόνα 5.101.



Εικόνα 5.101: Κατάλογος προφίλ ανίχνευσης.

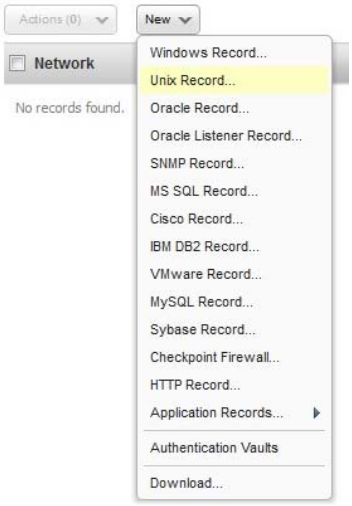
6. Από τον κατάλογο επιλογών της επιλογής "Scans", επιλέγεται η επιλογή "Authentication", Εικόνα 5.102. Στο "Authentication" θα γίνει η καταχώρηση του λογαριασμού με τα

δέοντα στοιχεία αυθεντικοποίησης, ο οποίος θα χρησιμοποιηθεί κατά την διεξαγωγή ανίχνευσης των ευπαθειών στη μηχανή Metasploitable.



Εικόνα 5.102: Επιλογή δημιουργίας λογαριασμού αυθεντικοποίησης.

7. Από την επιλογή "New" επιλέγεται το "Unix Record", Εικόνα 5.103 μιας και η μηχανή Metasploitable εμπίπτει στη κατηγορία αυτή.

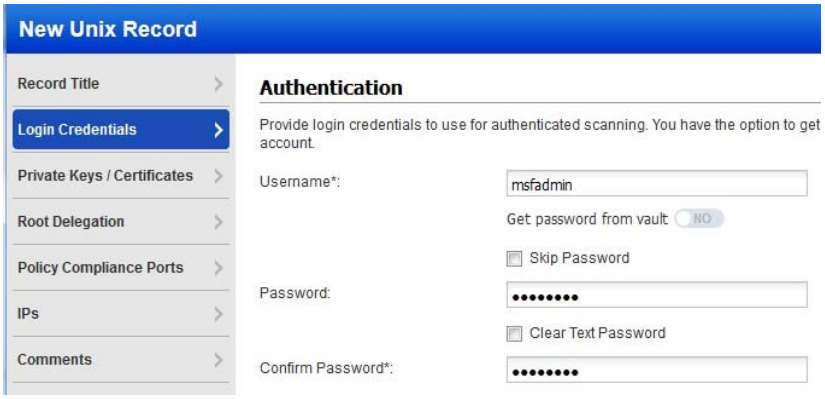


Εικόνα 5.103: Δημιουργία λογαριασμού αυθεντικοποίησης.

8. Στην φόρμα καταχώρησης του καινούργιου λογαριασμού αυθεντικοποίησης καταχωρείται το όνομα αναγνώρισης του λογαριασμού αυτού. Στην προκειμένη περίπτωση το όνομα που έχει καταχωρηθεί είναι το "Metasploitable", Εικόνα 5.104.

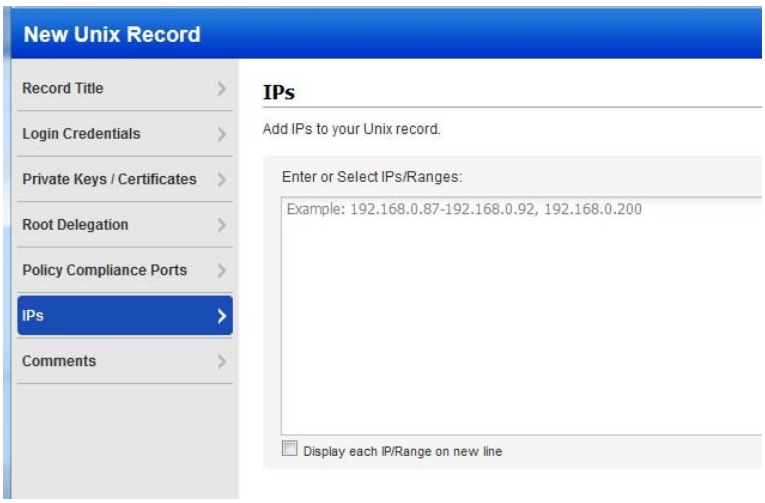
Εικόνα 5.104: Καταχώρηση ονόματος λογαριασμού αυθεντικοποίησης.

9. Ακολούθως από το μενού στα αριστερά, επιλέγεται η επιλογή "Logon Credentials", όπου καταχωρούνται τα στοιχεία αυθεντικοποίησης, το όνομα χρήστη και ο κωδικός πρόσβασης, Εικόνα 5.105.



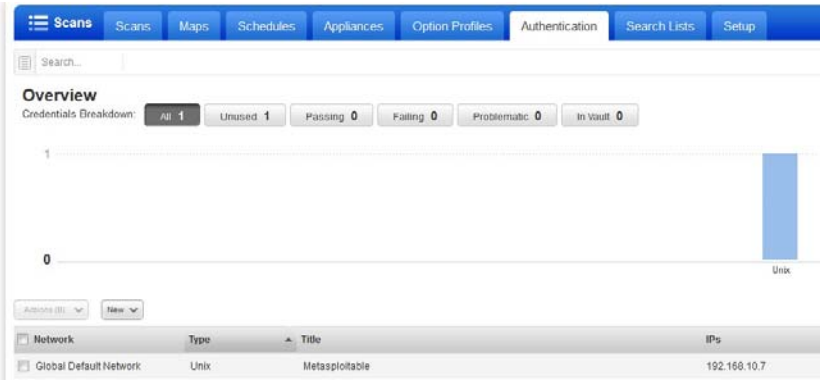
Εικόνα 5.105: Οθόνη καταχώρησης στοιχείων αυθεντικοποίησης.

10. Στην συνέχεια από το μενού επιλέγεται το "IPs", όπου καταχωρείται η διεύθυνση IP της μηχανής Metasploitable, που στην προκειμένη περίπτωση είναι η διεύθυνση "192.168.10.7", Εικόνα 5.106. Ακολούθως επιλέγεται η επιλογή "Create", για την δημιουργία του λογαριασμού πρόσβασης.



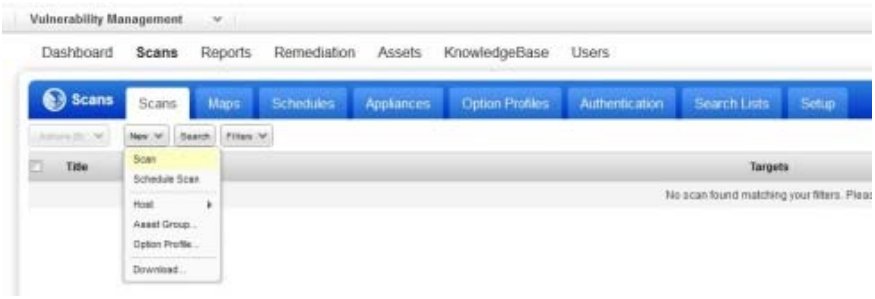
Εικόνα 5.106: Καταχώρηση IP του Metasploitable.

11. Ο νέος λογαριασμός με τα στοιχεία αυθεντικοποίησης, παρουσιάζεται στο πίνακα λογαριασμών του "Authentication", Εικόνα 5.107.



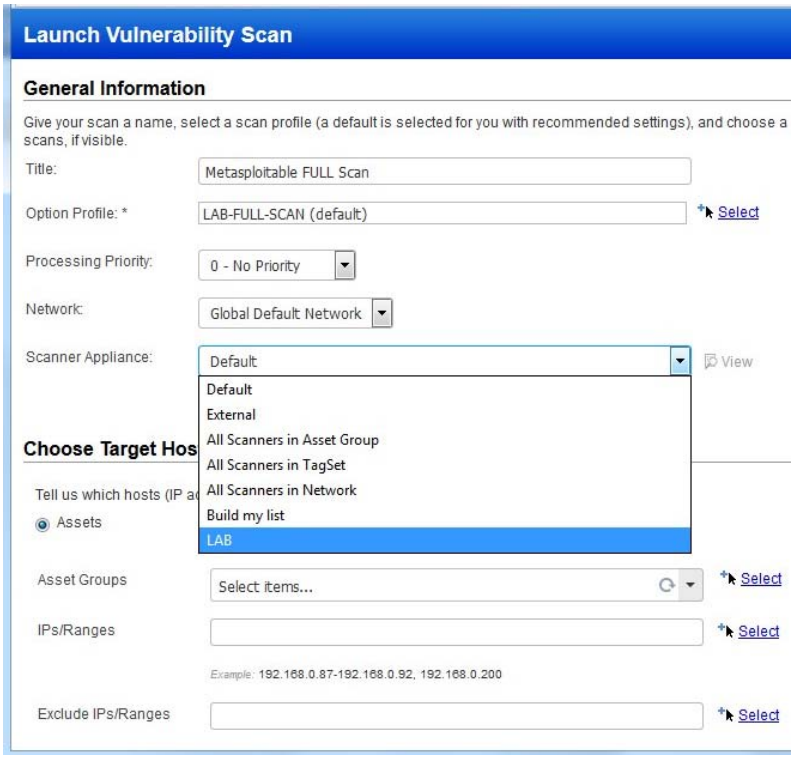
Εικόνα 5.107: Κατάλογος λογαριασμών αυθεντικοποίησης.

12. Από το κυρίως μενού επιλέγεται η επιλογή "Scans" και στην συνέχεια "New" και ακολούθως "Scan", Εικόνα 5.108. Στο στάδιο αυτό θα δημιουργηθεί το προφίλ εργασίας ανίχνευσης των ευπαθειών.



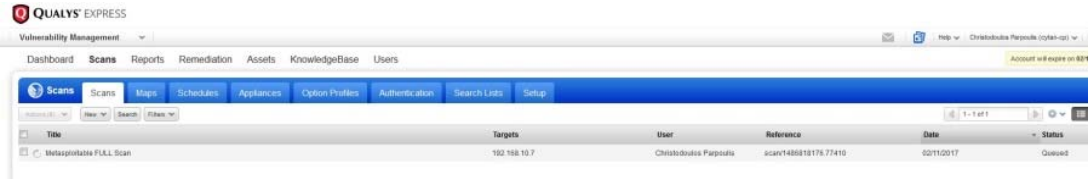
Εικόνα 5.108: Επιλογή δημιουργίας προφίλ εργασίας ανίχνευσης ευπαθειών.

13. Στην φόρμα καταχώρισης στοιχείων του προφίλ ανίχνευσης, καταχωρείται αρχικά το όνομα του προφίλ "Metasploitable FULL Scan", στην συνέχεια επιλέγεται το προφίλ επιλογών ανίχνευσης ευπαθειών "LAB-FULL-SCAN", από την επιλογή "Option Profile" και ακολούθως από την επιλογή "Scanner Appliance", η συσκευή ανίχνευσης "LAB", που αντικατοπτρίζει την εικονική μηχανή QualysGuard Virtual Scanner Appliance. Στην συνέχεια καταχωρείται η διεύθυνση IP του Metasploitable, στην επιλογή "IPs/Ranges", Εικόνα 5.109.



Εικόνα 5.109: Καταχώρηση στοιχείων εργασίας ανίχνευσης ευπαθειών.

14. Μετά την ολοκλήρωση της καταχώρησης όλων των στοιχείων, επιλέγεται η επιλογή "Launch", για την εκτέλεση της ανίχνευσης των ευπαθειών στην μηχανή Metasploitable. Η διαδικασία αρχικά βρίσκεται σε κατάσταση αναμονής "Queued", Εικόνα 5.110.

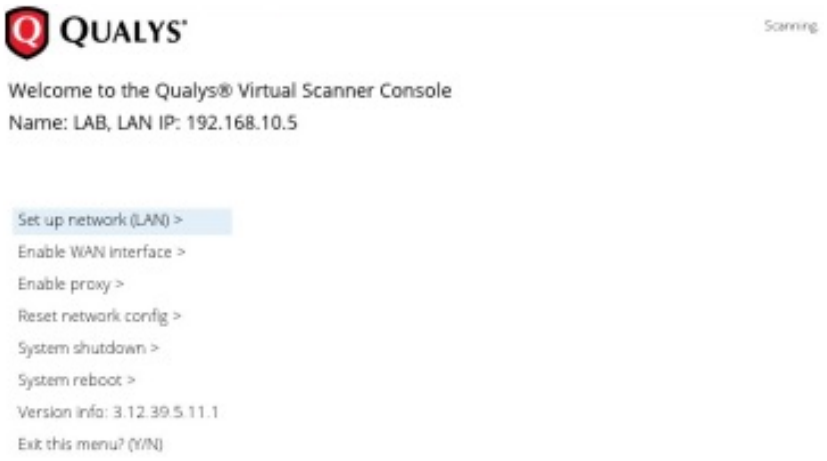


Εικόνα 5.110: Εργασία ανίχνευσης ευπαθειών σε αναμονή.

15. Στην συνέχεια η διαδικασία εκτελείται και η κατάσταση αλλάζει σε “Running”, Εικόνα 5.111.

Εικόνα 5.111: Ενεργοποίηση εργασίας ανίχνευσης ευπαθειών.

16. Κατά την διάρκεια της διαδικασίας ανίχνευσης, γίνεται εμφανής στην εικονική μηχανή QualysGuard Virtual Scanner Appliance, η ένδειξη “Scanning”, Εικόνα 5.112 επαληθεύοντας έτσι την άμεση επικοινωνία του VM εργαλείου νέφους και της εικονικής μηχανής.



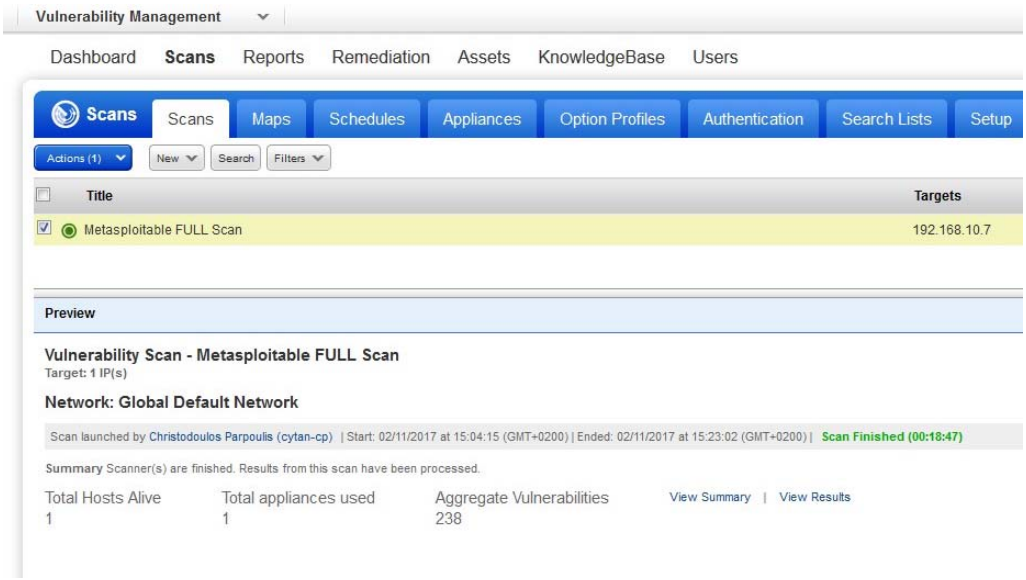
Εικόνα 5.112: Εμφάνιση ενεργής κατάστασης εργασία ανίχνευσης ευπαθειών στην εικονική μηχανή Qualys Virtual Scanner.

17. Μετά την ολοκλήρωση της διαδικασίας ανίχνευσης ευπαθειών, η κατάσταση της διαδικασίας παρουσιάζεται ως “Finished”, Εικόνα 5.113.

Εικόνα 5.113: Ολοκλήρωση εργασίας ανίχνευσης ευπαθειών.

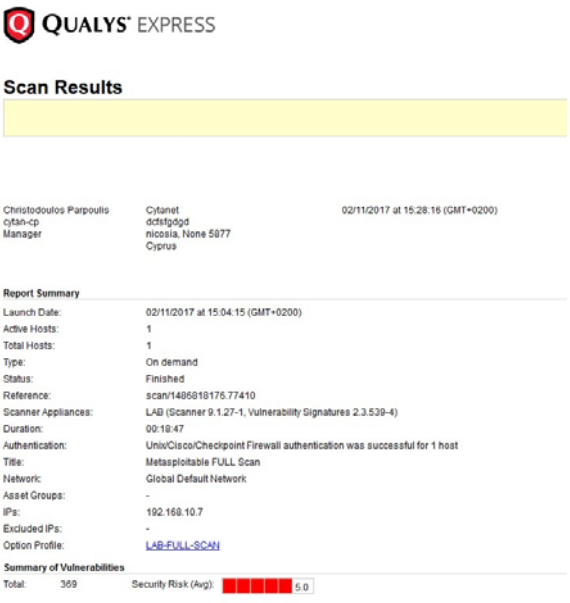
18. Επιλέγεται η ολοκληρωμένη διαδικασία ανίχνευσης και παρουσιάζεται ένας περιληπτικός πίνακας ο οποίος παρουσιάζει το σύνολο των ευπαθειών που έχουν

ανευρεθεί, Εικόνα 5.114. Για την παρουσίαση όλων των ανευρεθέν στοιχείων επιλέγεται η επιλογή "View Results".



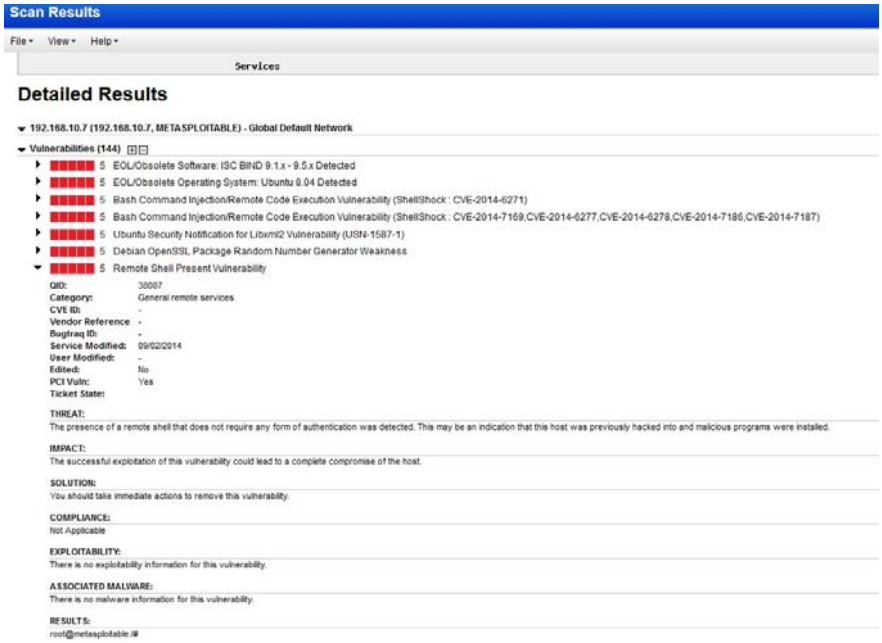
Εικόνα 5.114: Περιληπτικός πίνακας συνόλου ανευρεθέν ευπαθειών.

19. Μετά από την επιλογή "View Results", παρουσιάζεται η κατάσταση με όλα τα ανευρεθέν στοιχεία για το Metasploitable. Το Metasploitable παρουσιάζεται ως μηχάνημα υψηλού ρίσκου και συγκεκριμένα ρίσκου "5", Εικόνα 5.115. Οι ευπάθειες του υπό διερεύνηση υπολογιστή παρουσιάζονται με σειρά κρισιμότητας, ξεκινώντας με τις ευπάθειες με το μεγαλύτερο ρίσκο, "5".



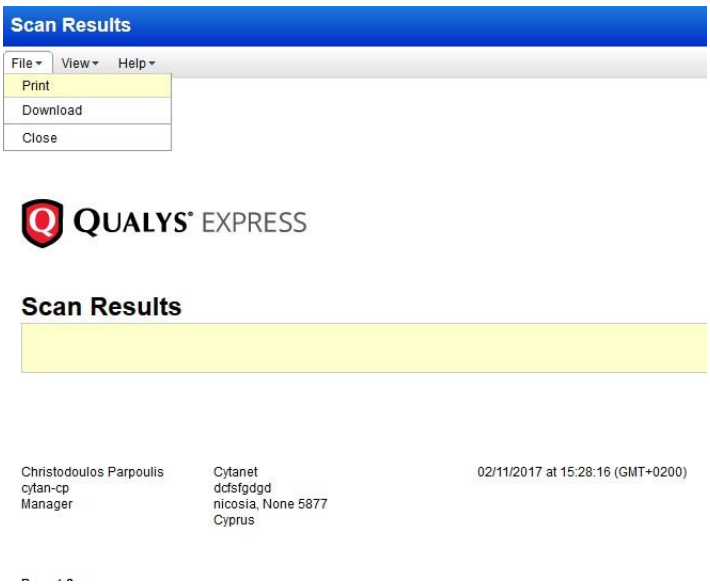
Εικόνα 5.115: Κατάσταση ανευρεθέν ευπαθειών για Metasploitable.

20. Επιλέγοντας κάποια από της ευπάθειες, ο διαχειριστής μπορεί να δει περισσότερες πληροφορίες για την συγκεκριμένη ευπάθεια. Δίνονται πληροφορίες για την κατηγορία της ευπάθειας και το τύπο της απειλής, τον αντίκτυπο που μπορεί να έχει η τυχόν εκμετάλλευσή της, η πιθανή λύση για την αντιμετώπιση της και αν υπάρχει διαθέσιμος κώδικας που μπορεί να επιτρέπει την άμεση εκμετάλλευση της, Εικόνα 5.116.



Εικόνα 5.116: Λεπτομέρειες επιλεγείσας ευπάθειας.

21. Η κατάσταση ανεύρεσης των ευπαθειών μπορεί να εξαχθεί και να αποθηκευθεί για περεταίρω διερεύνηση. Για να εξαχθεί η κατάσταση, ο διαχειριστής επιλέγει από το μενού την επιλογή “File” και στην συνέχεια “Download”, Εικόνα 5.117.



Εικόνα 5.117: Επιλογή εξαγωγής κατάστασης ευπαθειών.

22. Η κατάσταση μπορεί να εξαχθεί σε μορφή PDF, HTML,MHT, XML και CSV. Στην προκειμένη περίπτωση η κατάσταση έχει εξαχθεί σε μορφή PDF, Εικόνα 5.118.

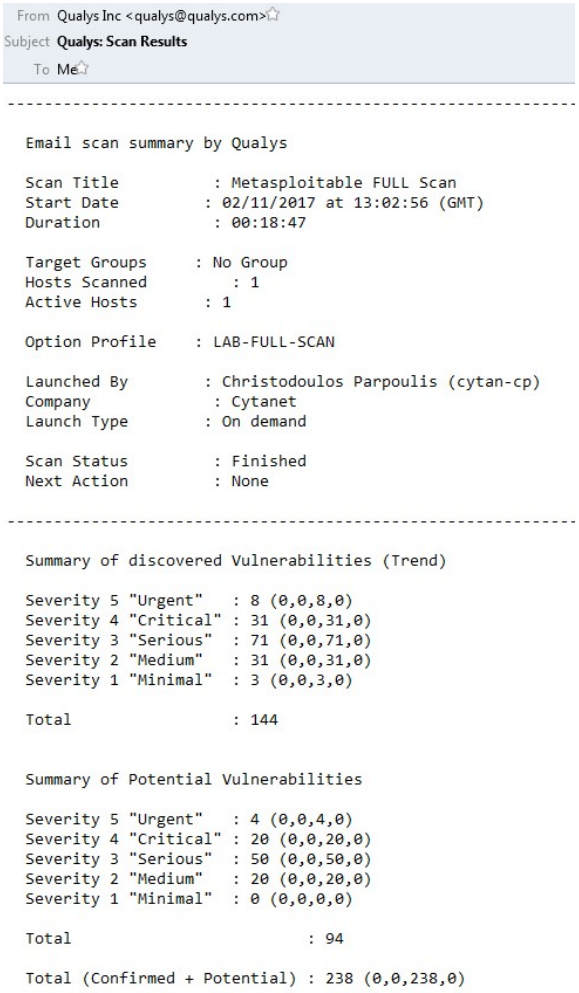
Εικόνα 5.118: Εξαγωγή κατάστασης ευπαθειών σε μορφή pdf.

23. Επιπρόσθετα το σύστημα με την ολοκλήρωση της ανίχνευσης των ευπαθειών αποστέλλει δύο ηλεκτρονικά μηνύματα στο διαχειριστή.

- Το πρώτο ηλεκτρονικό μήνυμα ενημερώνει το διαχειριστή ότι η διαδικασία διερεύνησης έχει περατωθεί, Εικόνα 5.119.

Εικόνα 5.119: Ηλ. μήνυμα περάτωσης εργασίας διερεύνησης ευπαθειών.

- Το δεύτερο ηλεκτρονικό μήνυμα περιλαμβάνει μια περίληψη των ανευρεθέν ευπαθειών, Εικόνα 5.120. Ενημερώνει το διαχειριστή πόσες ευπάθειες ανά κατηγορία ρίσκου έχουν ανευρεθεί. Για παράδειγμα, στην συγκεκριμένη περίπτωση, έχουν ανευρεθεί 8 ευπάθειες ρίσκου "5" που χρήζουν άμεσης αντιμετώπισης και 31 ευπάθειες ρίσκου 4 που εμπίπτουν στην κατηγορία των κρίσιμων ευπαθειών.



From Qualys Inc <qualys@qualys.com>
Subject **Qualys: Scan Results**
To Me

Email scan summary by Qualys

Scan Title : Metasploitable FULL Scan
Start Date : 02/11/2017 at 13:02:56 (GMT)
Duration : 00:18:47

Target Groups : No Group
Hosts Scanned : 1
Active Hosts : 1

Option Profile : LAB-FULL-SCAN

Launched By : Christodoulos Parpoulis (cytan-cp)
Company : Cytanet
Launch Type : On demand

Scan Status : Finished
Next Action : None

Summary of discovered Vulnerabilities (Trend)

Severity 5 "Urgent" : 8 (0,0,8,0)
Severity 4 "Critical" : 31 (0,0,31,0)
Severity 3 "Serious" : 71 (0,0,71,0)
Severity 2 "Medium" : 31 (0,0,31,0)
Severity 1 "Minimal" : 3 (0,0,3,0)

Total : 144

Summary of Potential Vulnerabilities

Severity 5 "Urgent" : 4 (0,0,4,0)
Severity 4 "Critical" : 20 (0,0,20,0)
Severity 3 "Serious" : 50 (0,0,50,0)
Severity 2 "Medium" : 20 (0,0,20,0)
Severity 1 "Minimal" : 0 (0,0,0,0)

Total : 94

Total (Confirmed + Potential) : 238 (0,0,238,0)

Εικόνα 5.120: Ηλ. μήνυμα περίληψης ανευρεθέν ευπαθειών.

Η εξαχθείσα PDF κατάσταση με ονομασία "Qualys Metasploitable Assesment Report 1", είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "Qualys".

5.2.5 SAINT Vulnerability Assesment

Το SAINT Vulnerability Assessment (VA) είναι προϊόν της εταιρείας SAINT, της πρώτης εταιρείας στο χώρο που πρόσφερε λύση εύρεσης ευπαθειών με ενσωματωμένο προϊόν διείσδυσης και εκμετάλλευσης των ανευρεθέντων ευπαθειών.

Το SAINT VA εντοπίζει τις ευπάθειες σε συνδεδεμένες δικτυακές συσκευές, σε λειτουργικά συστήματα, σε λογισμικά εγκατεστημένα σε υπολογιστές χρηστών, σε λογισμικά διαδικτύου, σε βάσης δεδομένων και σε πολλά άλλα. Επιπρόσθετα εντοπίζει και διορθώνει πιθανές αδυναμίες ασφαλείας στο δίκτυο πριν αυτές τύχουν εκμετάλλευσης από κακόβουλους χρήστες, καθώς και τις κοινές ευπάθειες των συστημάτων.

Με το SAINT VA επιτυγχάνεται η συμμόρφωση στους τρέχων κυβερνητικούς και επιχειρηματικούς κανονισμούς, όπως αυτοί ορίζονται από τα πρότυπα PCI DSS, NERC, FISMA, SOX, GLBA και HIPPA. Επίσης πραγματοποιεί ελέγχους με βάση τις πολιτικές που καθορίζονται από το FDCC, USGCB και DISA.

Με την ενσωμάτωση του SAINTexploit εργαλείου, δίνετε η δυνατότητα δοκιμής εκμετάλλευσης των ευπαθειών οι οποίες έχουν εντοπιστεί, επιβεβαιώνοντας έτσι την ευπάθεια και αποκαλύπτοντας το ρίσκο.

Οι έλεγχοι που πραγματοποιούνται στα λειτουργικά συστήματα, βάσης δεδομένων και λογισμικών διαδικτύου, μπορεί να γίνουν είτε με την χρήση πιστοποιημένων λογαριασμών δικτύου ή και χωρίς αυτούς. Επίσης δεν χρειάζεται η εγκατάσταση κάποιου βοηθητικού λογισμικού (Agent) στα υπό διερεύνηση υποκείμενα.

Οι έλεγχοι του SAINT VA μπορεί να επεκταθούν και στο περιεχόμενο των δεδομένων. Μπορεί δηλαδή να εντοπιστούν δεδομένα προσωπικού χαρακτήρα (PII) τα οποία είναι αποθηκευμένα σε μηχανές χρηστών ή σε εξυπηρετητές, ενώ δεν επιτρέπεται η αποθήκευση αυτού του τύπου δεδομένων.

Εμπεριέχει ένα εύχρηστο εργαλείο σχεδίασης κατά παραγγελία καταστάσεων, για τις ανευρεθέν ευπάθειες, όπου επιτρέπει την παρουσίαση των ευπαθειών αυτών, ακόμα και για μεγάλα δίκτυα, σε μια πολύ ευανάγνωστη μορφή. Ακόμη με την χρήση εκθέσεων ανάλυσης τάσεων μπορεί να διαφανεί εάν η ασφάλεια του δικτύου βελτιώνεται με την πάροδο του χρόνου.

Σε καθημερινή βάση γίνονται έλεγχοι για καινούργια αρχεία ανεύρεσης και εκμετάλλευσης ευπαθειών και αποθηκεύονται αυτόματα στην βάση δεδομένων του SAINT VA. Επίσης παρέχεται η δυνατότητα ενσωμάτωσης κατά παραγγελία ελέγχων ασφαλείας από τους διαχειριστές. [19]

Εγκατάσταση και χρήση εργαλείου SAINT Vulnerability Assesment

Το εργαλείο SAINT Vulnerability Assessment προσφέρεται σαν υπηρεσία SaaS με την ονομασία “SAINT Cloud” ή μπορεί να εγκατασταθεί στο τοπικό δίκτυο ως μια εικονική μηχανή με την ονομασία “SAINT 8”.

Στην παρούσα μεταπτυχιακή διατριβή έχει χρησιμοποιηθεί η εικονική μηχανή “SAINT 8” η οποία τρέχει σε λειτουργικό Ubuntu 16.04.

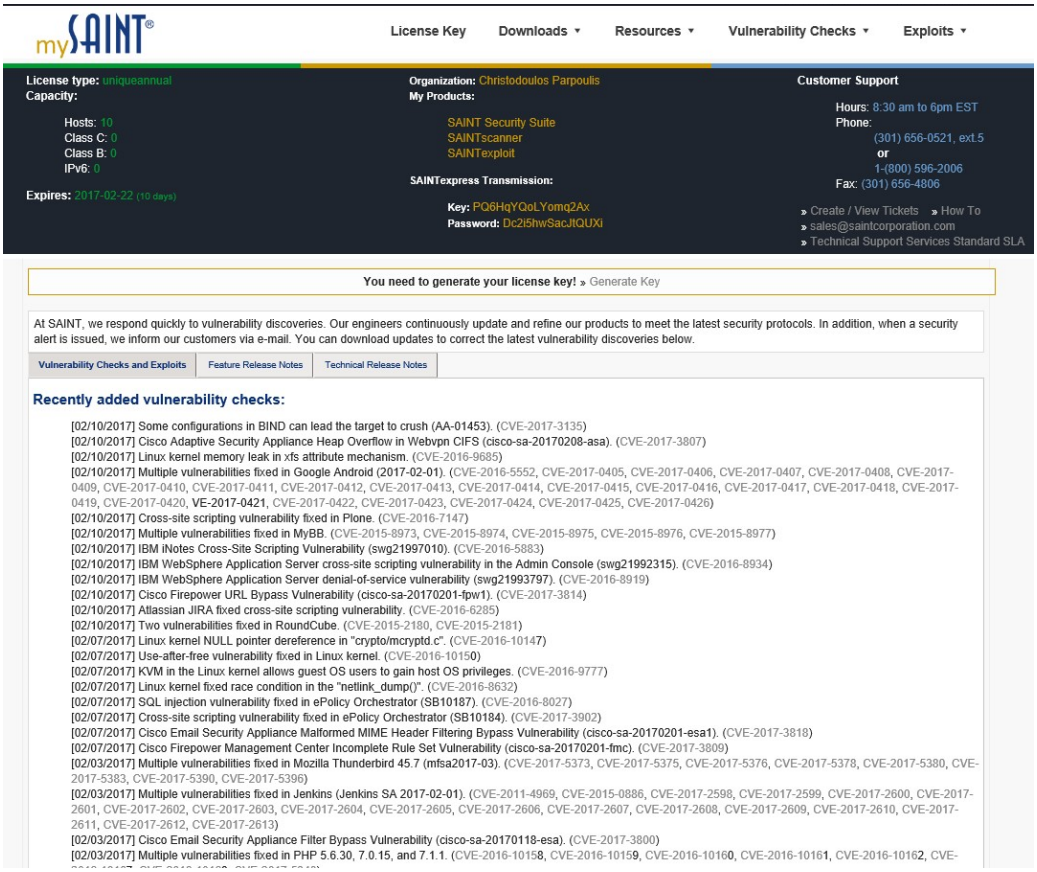
Εγκατάσταση

1. Μετά την επικοινωνία με αντιπρόσωπο της εταιρίας SAINT και αποστολής των απαιτούμενων διευκρινίσεων (λόγους απαίτησης άδειας χρήσης κ.ο.κ) γίνεται παραλαβή κωδικών πρόσβασης καθώς και οδηγιών, μέσο ηλεκτρονικού ταχυδρομείου, ούτως ώστε να γίνει δυνατή η λήψη της εικονικής μηχανής του εργαλείου.

   Ακολουθώντας τις οδηγίες του ηλεκτρονικού μηνύματος γίνεται πλοήγηση στην ιστοσελίδα από όπου θα γίνει η λήψη της εικονικής μηχανής. Αρχικά θα γίνει αυθεντικοποίηση στη πύλη mySAINT, Εικόνα 5.121.

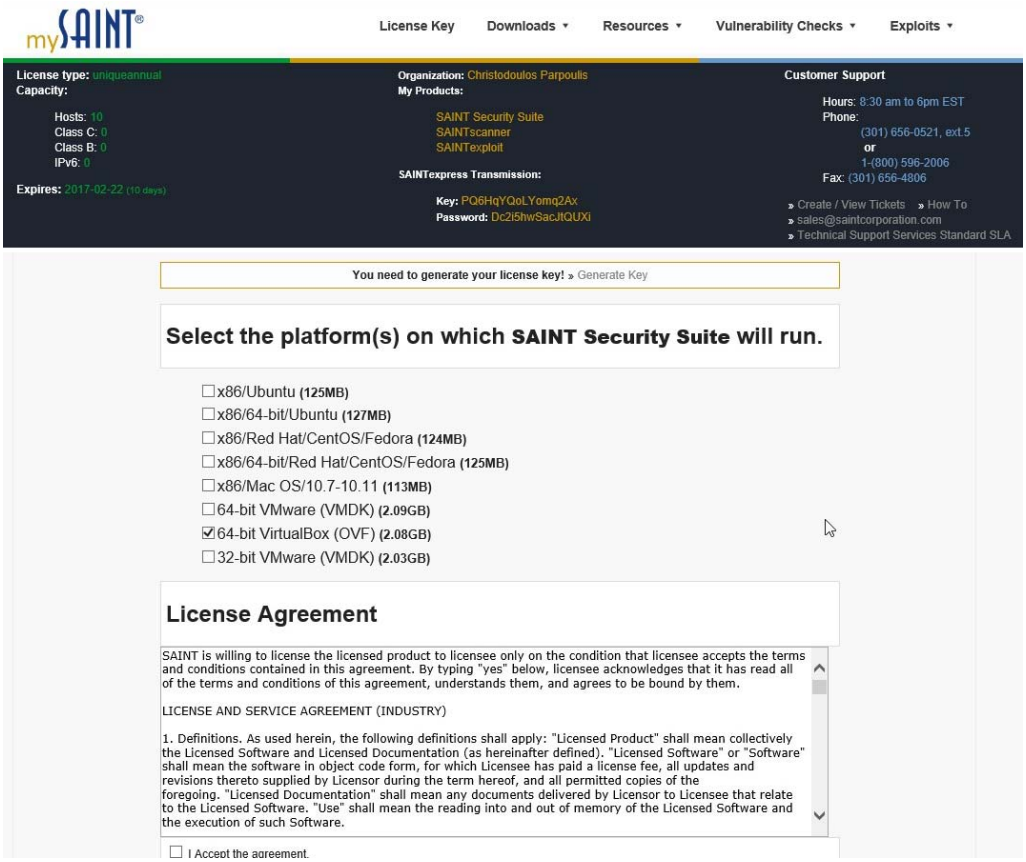
Εικόνα 5.121: Διαδικτυακή οθόνη αυθεντικοποίησης του εργαλείου SAINT.

2. Μετά την αυθεντικοποίηση επιτυγχάνεται πρόσβαση στον νεοδημιουργηθέν λογαριασμό χρήσης των εργαλείων SAINT. Διαφαίνεται ότι έχει παρασχεθεί άδεια χρήσης στα εργαλεία Saint scanner και Saint exploit, που είναι μέρος του SAINT Security Suite, Εικόνα 5.122 . Στην παρούσα μεταπτυχιακή διατριβή θα μας απασχολήσει το Saint scanner, όπου είναι το εργαλείο ανεύρεσης των ευπαθειών.



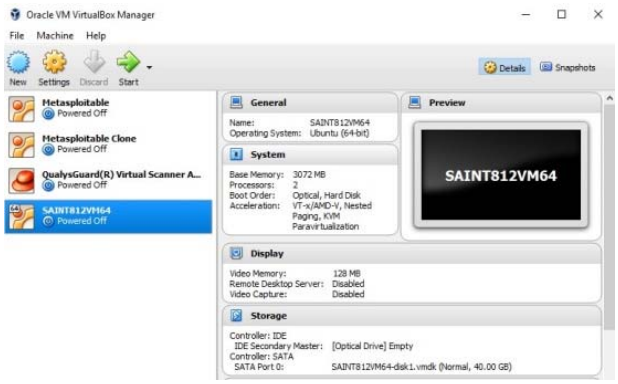
Εικόνα 5.122: Διαδικτυακή σελίδα λογαριασμού διαχειριστή των εργαλείων SAINT.

3. Από το κυρίως μενού επιλέγεται η επιλογή “Downloads” και στην συνέχεια επιλέγεται για “κατέβασμα” το πακέτο “64-bit VirtulBox “, Εικόνα 5.123, όπου αποτελεί την εικονική μηχανή του εργαλείου SAINT. Στην συνέχεια θα γίνει “φόρτωση” της εικονικής αυτής μηχανής στο Oracle VirtualBox.



Εικόνα 5.123: Επιλογή εικονικής μηχανής για "κατέβασμα".

4. Μετά το "κατέβασμα" της εικονικής μηχανής, "φορτώνεται" στο Oracle VirtualBox και είναι έτοιμη για χρήση, Εικόνα 5.124.



Εικόνα 5.124: Φόρτωση εικονικής μηχανής στο Oracle VirtualBox.

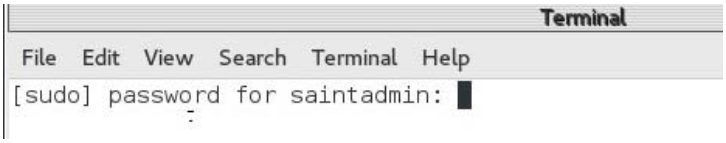
5. Αφού ολοκληρωθεί η διαδικασία εκκίνησης του λειτουργικού Ubuntu της εικονικής μηχανής, Εικόνα 5.125, στην συνέχεια θα γίνει η αυθεντικοποίηση στο Linux περιβάλλον. Ο λογαριασμός αυθεντικοποίησης έχει παραλειφθεί στο ηλεκτρονικό ταχυδρομείο κατά την διαδικασία απόκτησης άδειας χρήσης.

Εικόνα 5.125: Οθόνη αυθεντικοποίησης στην εικονική μηχανή SAINT.

6. Στην συνέχεια όταν ολοκληρωθεί η αυθεντικοποίηση, παρουσιάζεται το περιβάλλον του λειτουργικού συστήματος. Ακολούθως επιλέγεται το εικονίδιο του "SAINT 8", για να τεθεί σε λειτουργία το εργαλείο, Εικόνα 5.126.

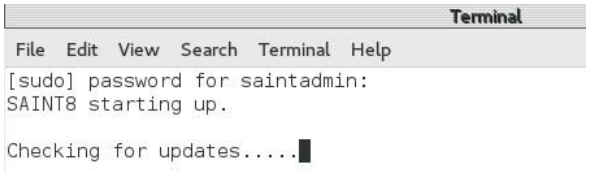
Εικόνα 5.126: Περιβάλλον λειτουργικού συστήματος της εικονικής μηχανής SAINT.

7. Στο τερματικό παράθυρο που εμφανίζεται, καταχωρούνται τα στοιχεία αυθεντικοποίησης, Εικόνα 5.127, που και πάλι έχουν παραλειφθεί με το ηλεκτρονικό ταχυδρομείο κατά την έκδοση της άδειας χρήσης.



Εικόνα 5.127: Τερματικό παράθυρο ενεργοποίησης υπηρεσιών SAINT.

8. Το εργαλείο αυτόματα διενεργεί διερεύνηση για τις τελευταίες ενημερώσεις και προχωρά στο "κατέβασμά" και στην εγκατάσταση αυτών, χωρίς κάποια επιπλέον παρέμβαση του διαχειριστή, Εικόνα 5.128.



Εικόνα 5.128: Διαδικασία "κατεβάσματος" των τελευταίων ενημερώσεων του εργαλείου.

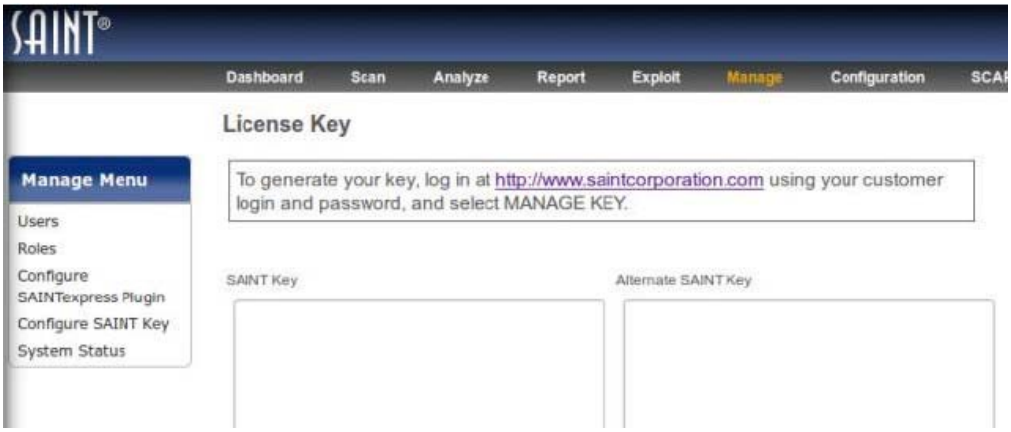
9. Μετά το πέρας της εγκατάστασης των ενημερώσεων, ανοίγει αυτόματα ένα παράθυρο στον πλοηγό διαδικτύου και παρουσιάζεται η οθόνη αυθεντικοποίησης του εργαλείου, Εικόνα 5.129. Καταχωρούνται και εδώ τα στοιχεία αυθεντικοποίησης που έχουν σταλεί με το ηλεκτρονικό ταχυδρομείο.

Εικόνα 5.129: Οθόνη αυθεντικοποίησης εργαλείου SAINT.

10. Το εργαλείο, για λόγους ασφαλείας, ζητά την αλλαγή του κωδικού πρόσβασης που έχει αποσταλεί με τον ηλεκτρονικό ταχυδρομείο, Εικόνα 5.130. Έτσι καταχωρείται ένας καινούργιος κωδικός πρόσβασης.

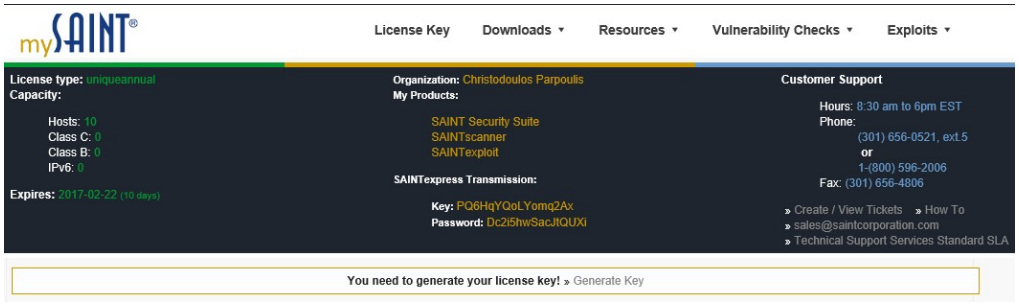
Εικόνα 5.130: Οθόνη αλλαγής κωδικού αυθεντικοποίησης.

11. Το πρώτο βήμα το οποίο θα πρέπει να ακολουθηθεί μετά την πρόσβαση στο εργαλείο, είναι η καταχώρηση του κλειδιού χρήσης . Για τον λόγο αυτό από το μενού επιλέγεται η επιλογή "Manage" και στην συνέχεια η επιλογή "Configure SAINT key", Εικόνα 5.131.

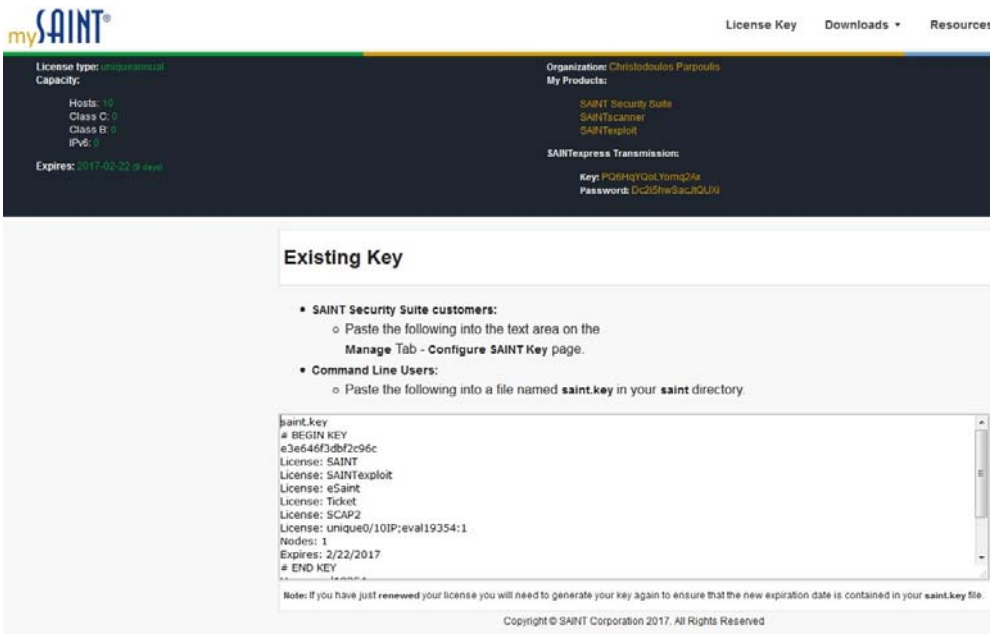


Εικόνα 5.131: Οθόνη καταχώρησης κλειδιού άδειας χρήσης.

12. Σε ένα δεύτερο παράθυρο του πλοηγού πραγματοποιείται πρόσβαση στη πύλη mySAINT (https://www.saintcorporation.com/cgi-bin/secure/customer/logon.pl) από όπου θα δημιουργηθεί και θα ανακτηθεί το κλειδί χρήσης. Μετά την αυθεντικοποίηση και πρόσβαση στη πύλη, δημιουργείται το κλειδί, με την επιλογή "Generate Key", Εικόνα 5.132 και Εικόνα 5.133.



Εικόνα 5.132: Επιλογή δημιουργίας κλειδιού άδειας χρήσης.



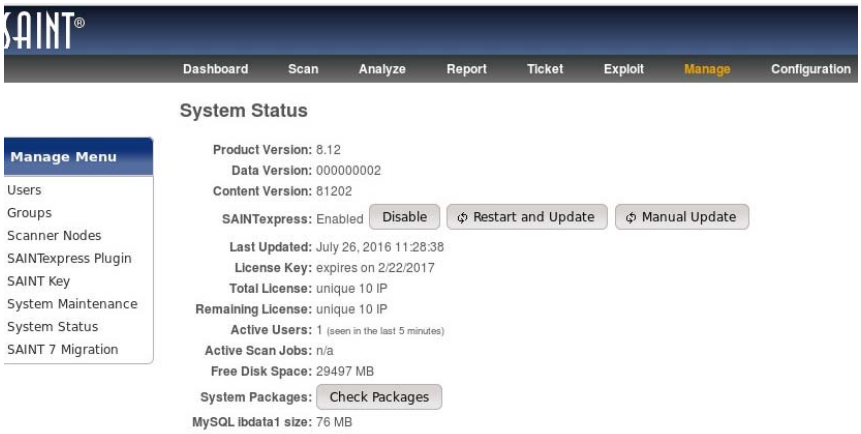
Εικόνα 5.133: Κλειδί άδειας χρήσης.

13. Ακολούθως γίνεται η αντιγραφή του κλειδιού και η επικόλλησή του στο παράθυρο του "Configure SAINT key". Στη συνέχεια επιλέγεται το "Save" για φύλαξη του κλειδιού, Εικόνα 5.134.

Εικόνα 5.134: Επικόλληση κλειδιού άδειας χρήσης.

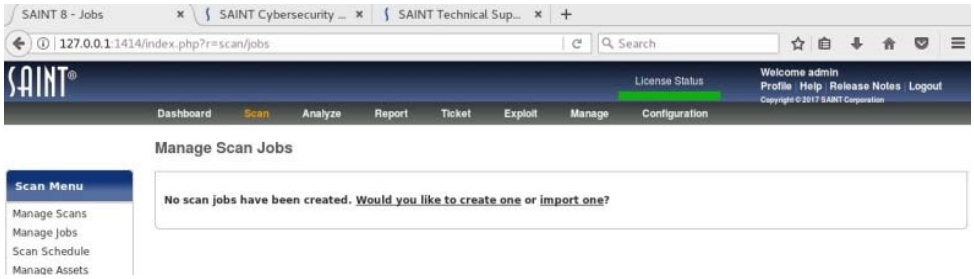
Χρήση

1. Για να διασφαλιστεί ότι το εργαλείο έχει τις τελευταίες ενημερώσεις, από το μενού επιλέγεται η επιλογή "Manage" και στην συνέχεια η επιλογή "System Status". Στη σελίδα αυτή επιλέγεται το "Restart and Update", Εικόνα 5.135. Το SAINT express εργαλείο θα κατεβάσει και θα εγκαταστήσει τις τελευταίες ενημερώσεις του εργαλείου.



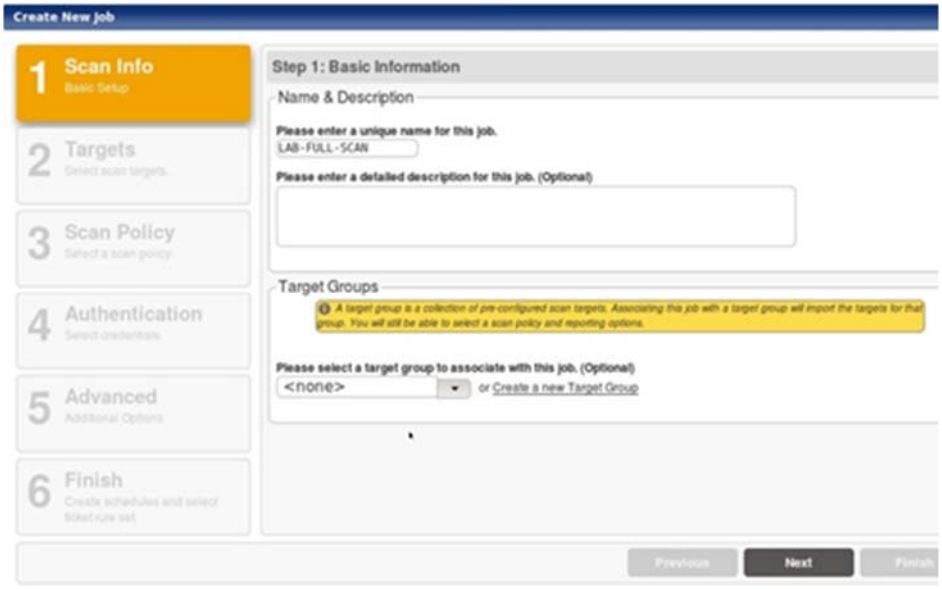
Εικόνα 5.135: Οθόνη επιλογής κατεβάσματος των τελευταίων ενημερώσεων του εργαλείου.

2. Για την διενέργεια ανίχνευσης επιλέγεται η επιλογή "Scan" από το κυρίως μενού. Στην συνέχεια επιλέγεται η επιλογή "Manage Jobs" και ακολούθως η επιλογή "Would you like to create one", για την δημιουργία μιας καινούργιας εργασίας διερεύνησης, Εικόνα 5.136.



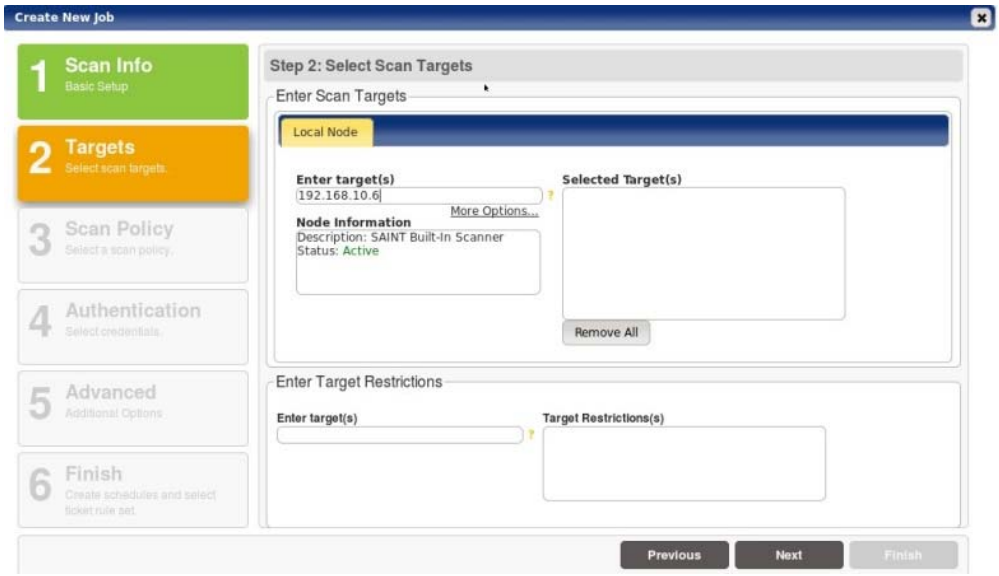
Εικόνα 5.136: Οθόνη δημιουργίας νέας εργασίας διερεύνησης.

3. Η οθόνη της δημιουργίας εργασίας διερεύνησης παρουσιάζεται και καταχωρείται αρχικά το όνομα αυτής. Στην προκειμένη περίπτωση το όνομα της εργασίας είναι το "LAB-FULL-SCAN", Εικόνα 5.137. Ακολούθως επιλέγεται η επιλογή "Next".



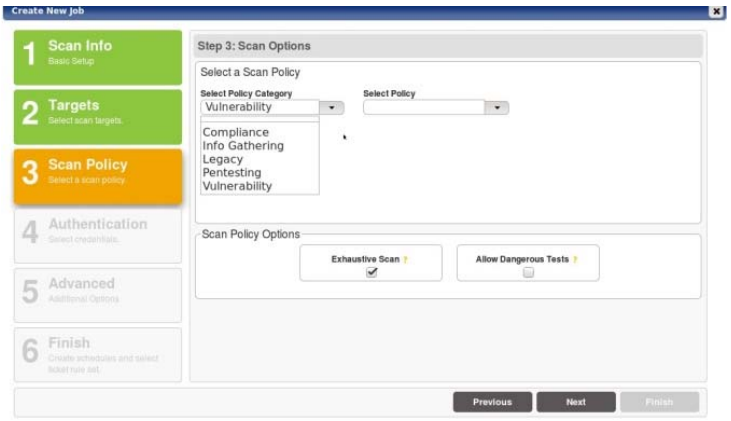
Εικόνα 5.137: Καταχώρηση ονόματος εργασίας διερεύνησης.

4. Στην επόμενη οθόνη καταχωρούνται οι υπό διερεύνηση υπολογιστές. Στο στάδιο αυτό καταχωρείται το IP του Metasploitable, που στην προκειμένη περίπτωση είναι το 192.168.10.6, Εικόνα 5.138. Ακολούθως επιλέγεται η επιλογή "Next".



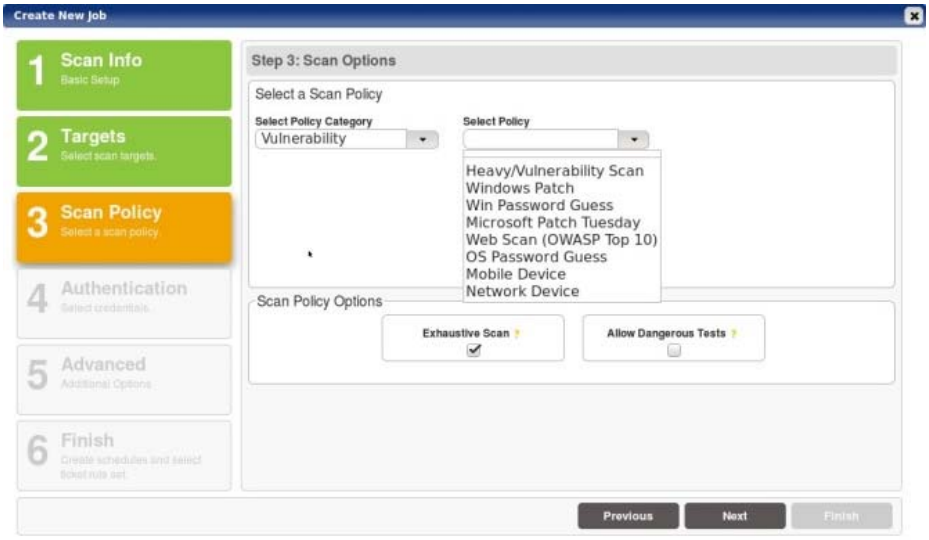
Εικόνα 5.138: Καταχώρηση IP Metasploitable.

5. Στο επόμενο στάδιο επιλέγεται η κατηγορία πολιτικής διερεύνησης. Η κατηγορία μπορεί να είναι "Compliance", "Info Gathering", "Legacy", "Pentesting" και "Vulnerability", Εικόνα 5.139. Η κατηγορία η οποία μας ενδιαφέρει είναι η "Vulnerability". Ακολούθως επιλέγεται η επιλογή "Next".



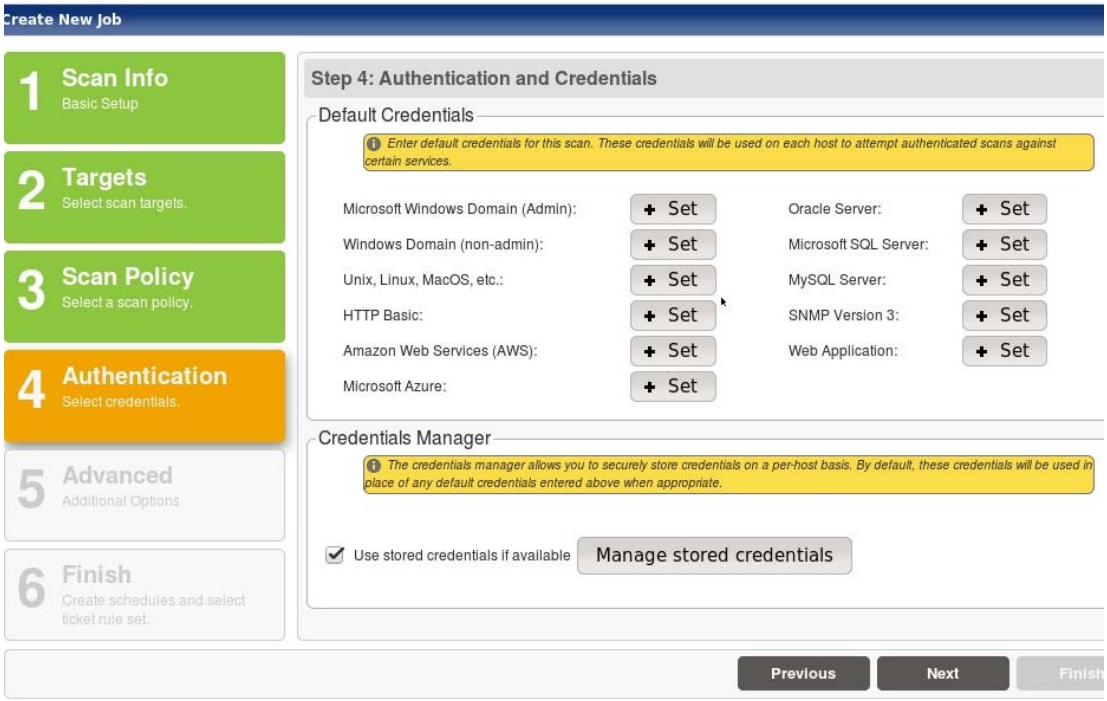
Εικόνα 5.139: Επιλογή κατηγορίας πολιτικής διερεύνησης.

6. Αφού έχει επιλεγεί η κατηγορία πολιτικής διερεύνησης, επιλέγεται στην συνέχεια η πολιτική διερεύνησης "Heavy/Vulnerability Scan", Εικόνα 5.140. Ακολούθως επιλέγεται η επιλογή "Next".



Εικόνα 5.140: Επιλογή πολιτικής διερεύνησης.

7. Στο επόμενο στάδιο θα καταχωρηθούν τα στοιχεία αυθεντικοποίησης για να μπορεί να γίνει σε βάθος η διερεύνηση στο Metasploitable. Επιλέγεται έτσι η επιλογή "Set" για "Unix,Linux,MacOS", Εικόνα 5.141, για καταχώριση των στοιχείων αυτών.

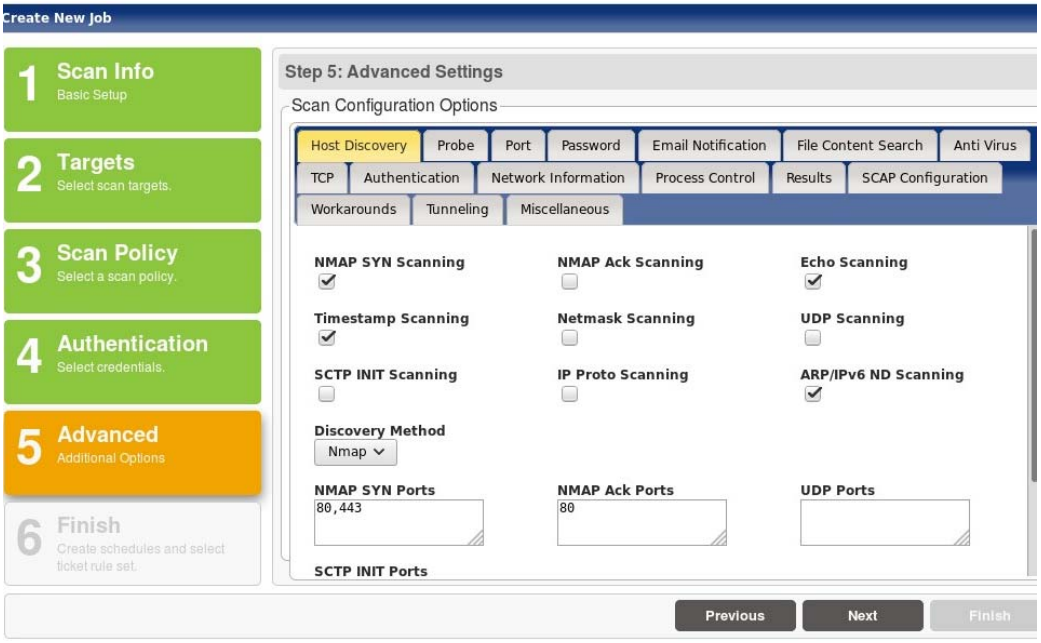


Εικόνα 5.141: Οθόνη επιλογής καταχώρησης στοιχείων αυθεντικοποίησης.

8. Καταχωρούνται τα στοιχεία αυθεντικοποίησης του Metasploitable και αποθηκεύονται, Εικόνα 5.142. Ακολούθως επιλέγεται η επιλογή "Next".

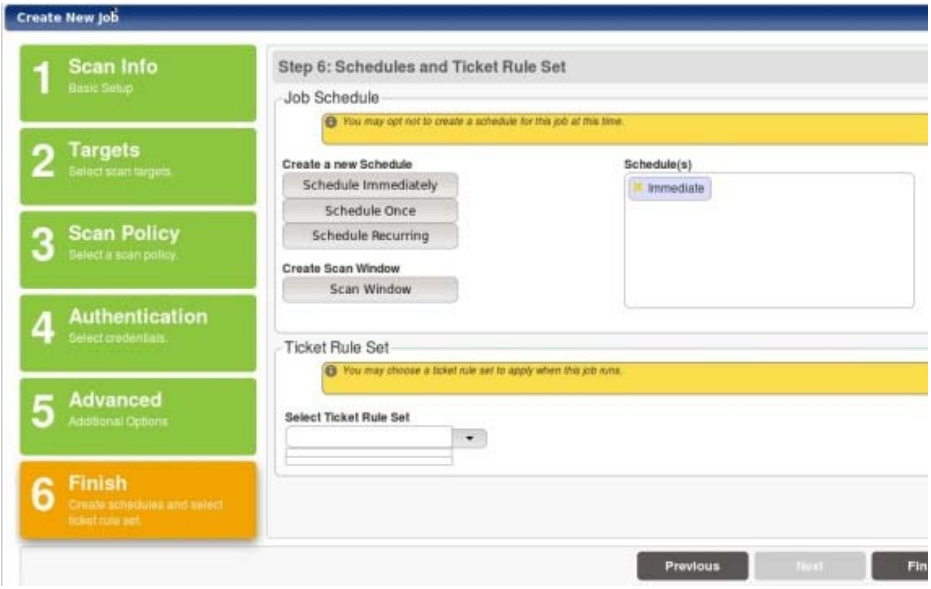
Εικόνα 5.142: Οθόνη καταχώρησης στοιχείων αυθεντικοποίησης.

9. Σε αυτό το στάδιο θα γίνει η επιλογή σάρωσης όλων το θυρών του υπό διερεύνηση υπολογιστή, καθώς και η χρήση όλων το μεθόδων διερεύνησης του ενσωματωμένου Nmap εργαλείου, Εικόνα 5.143. Ακολούθως επιλέγεται η επιλογή "Next".



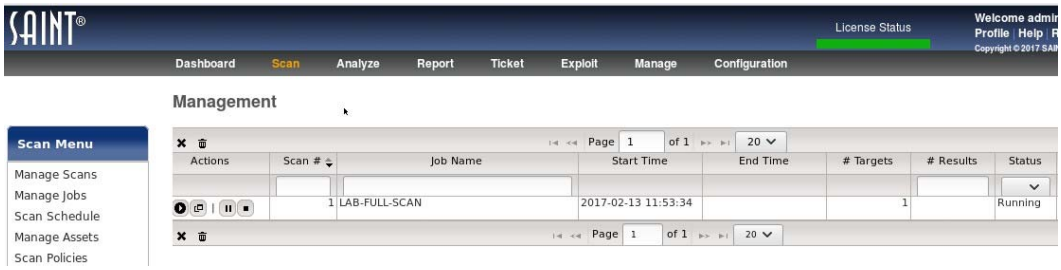
Εικόνα 5.143: Οθόνη καταχώρησης επιλογών εργασίας διερεύνησης.

10. Στην συνέχεια καταχωρείται η χρονική στιγμή που είναι επιθυμητή η διεξαγωγή της εργασίας διερεύνησης. Εδώ έχει επιλεγεί η χρονική στιγμή "Immediately", ούτος ώστε η εργασία να εκτελεστεί αμέσως μετά την αποθήκευση της, Εικόνα 5.144. Ακολούθως επιλέγεται η επιλογή "Finish".



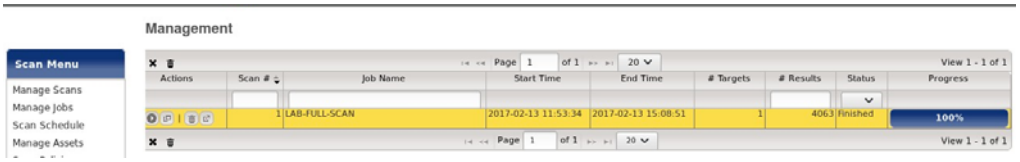
Εικόνα 5.144: Οθόνη επιλογής χρονικής στιγμής για εκτέλεση της εργασίας διερεύνησης.

11. Η εργασία διερεύνησης αποθηκεύεται και ξεκινά η διεργασία της διερεύνησης. Η κατάσταση της εργασίας τη δεδομένη στιγμή είναι "Running", Εικόνα 5.145.



Εικόνα 5.145: Ενεργοποίηση εργασίας ανίχνευσης ευπαθειών.

12. Μετά από πάροδο σχεδόν τριών ωρών η εργασία διερεύνησης ολοκληρώνεται και η κατάσταση της έχει αλλάξει σε "Finished", Εικόνα 5.146.



Εικόνα 5.146: Ολοκλήρωση εργασίας ανίχνευσης ευπαθειών.

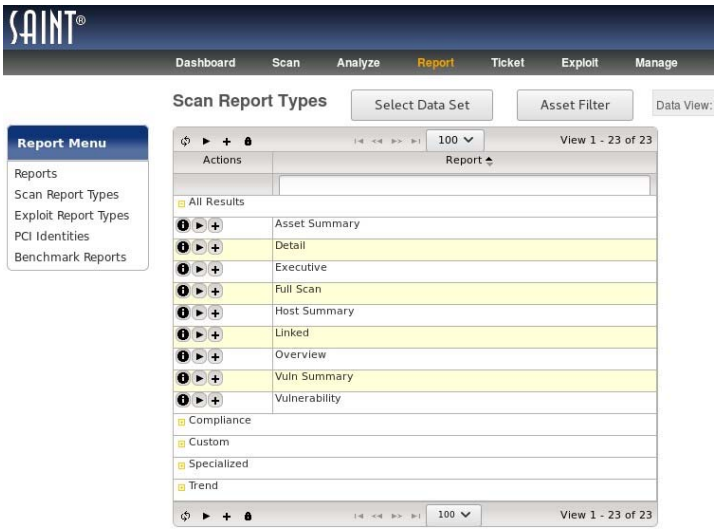
13. Για την εξαγωγή κατάστασης των αναβρεθέντων ευπαθειών επιλέγεται από το κυρίως μενού του εργαλείου η επιλογή "Report", Εικόνα 5.147.

Εικόνα 5.147: Οθόνη δημιουργίας καταστάσεων.

14. Ακολούθως επιλέγεται η επιλογή "Select Data Set". Στο σημείο αυτό θα επιλεγεί η διαδικασία διερεύνησης για τη χρονική στιγμή που επιθυμείται η δημιουργία της κατάστασης ευπαθειών, Εικόνα 5.148.

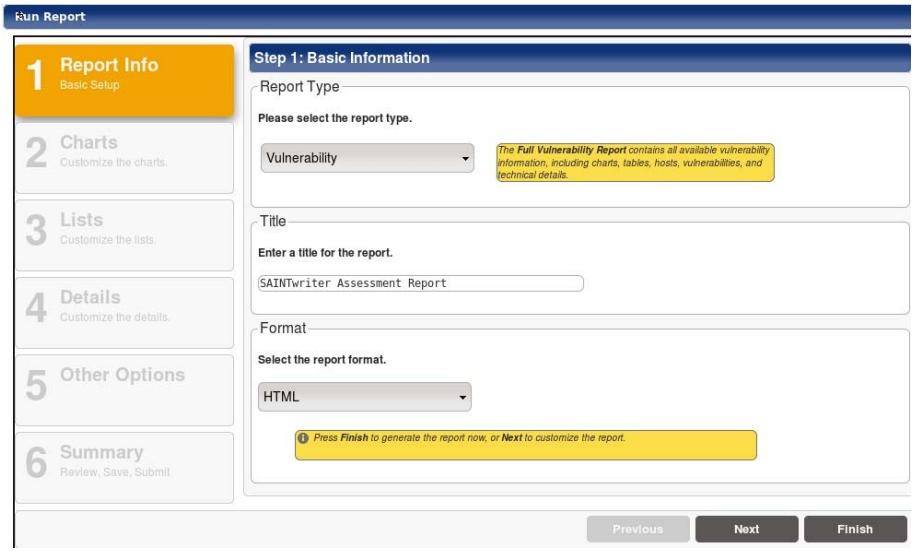
Εικόνα 5.148: Επιλογή διαδικασίας διερεύνησης για δημιουργία κατάστασης.

15. Στην συνέχεια από το "Reports Menu" επιλέγεται το "Scans Report Types" όπου θα γίνει η επιλογή για το ποιος θα είναι ο τύπος της κατάστασης που θα δημιουργηθεί. Αφού γίνει επέκταση του "All Results" επιλέγεται το  πλησίον της επιλογής "Vulnerability", Εικόνα 5.149.



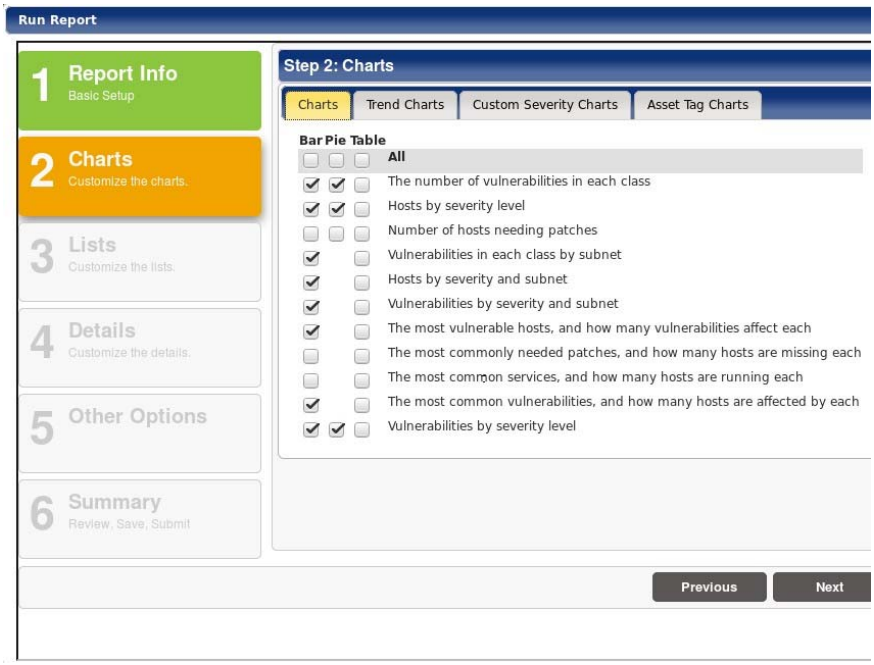
Εικόνα 5.149: Οθόνη επιλογής τύπου κατάστασης.

16. Μετά την επιλογή εκτέλεσης της συγκεκριμένης κατάστασης (Vulnerability), εμφανίζεται η οθόνη διαμόρφωσης. Αρχικά καταχωρείται το όνομα της κατάστασης, "Metasploitable Assessment Report" και επιλέγεται η μορφή της, που στη περίπτωση αυτή θα είναι σε "PDF" μορφή, Εικόνα 5.150. Ακολούθως επιλέγεται η επιλογή "Next".



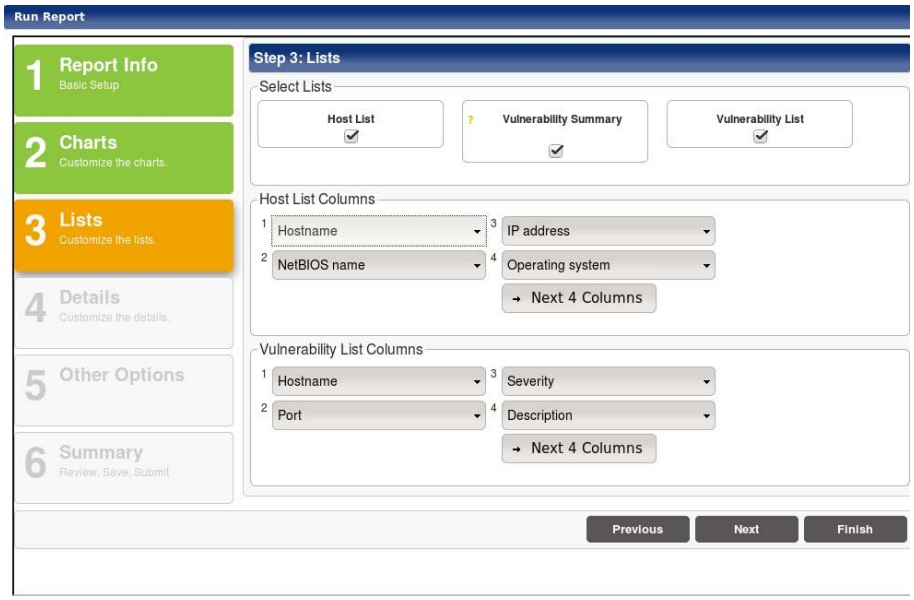
Εικόνα 5.150: Οθόνη διαμόρφωσης κατάστασης ευπαθειών.

17. Ακολούθως επιλέγονται τα περιεχόμενα των γραφικών παραστάσεων που θα συμπεριληφθούν στην κατάσταση εκτίμησης ευπαθειών, Εικόνα 5.151. Ακολούθως επιλέγεται η επιλογή "Next".



Εικόνα 5.151: Οθόνη επιλογής γραφικών παραστάσεων.

18. Στην συνέχεια επιλέγονται οι λίστες (πάγιων και ευπαθειών) αλλά και οι στήλες αυτών που θα παρουσιαστούν στην κατάσταση, Εικόνα 5.152. Ακολούθως επιλέγεται η επιλογή "Next".

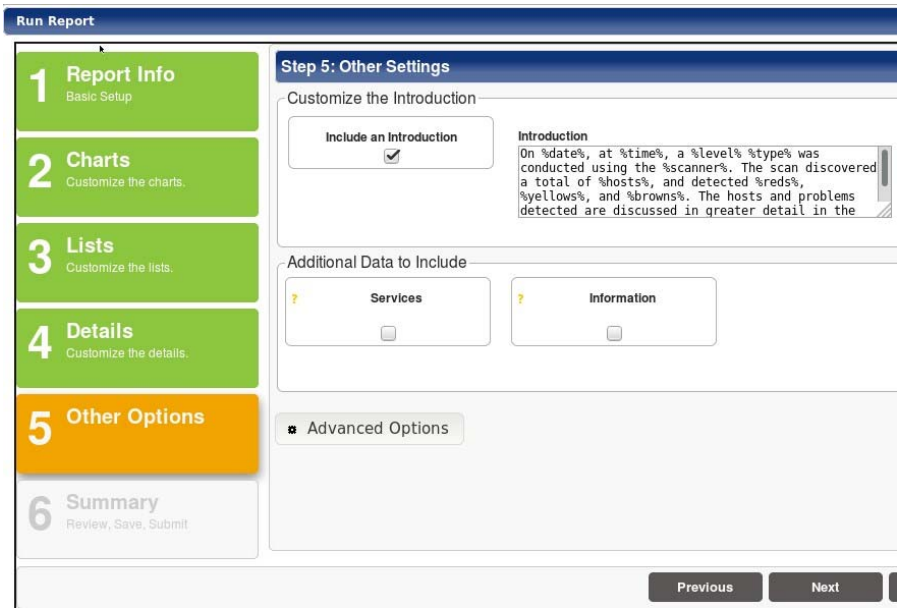


Εικόνα 5.152: Οθόνη επιλογής πάγιων, ευπαθειών και στηλών για εμφάνιση στην κατάσταση ευπαθειών.

19. Ακολούθως γίνεται επιλογή των λεπτομερειών που επιθυμεί ο διαχειριστής να είναι εμφανείς στην κατάσταση. Εδώ ο διαχειριστής μπορεί να επιλέξει να γίνεται λεπτομερής ανάλυση του προβλήματος που μια συγκεκριμένη ευπάθεια μπορεί να δημιουργήσει, η επίπτωση που μπορεί να έχει, αλλά και ποια είναι η προτεινόμενη λύση, καθώς και την ύπαρξη τυχόν περιορισμών εφαρμογής της όποιας λύσης, Εικόνα 5.153. Ακολούθως επιλέγεται η επιλογή "Next".

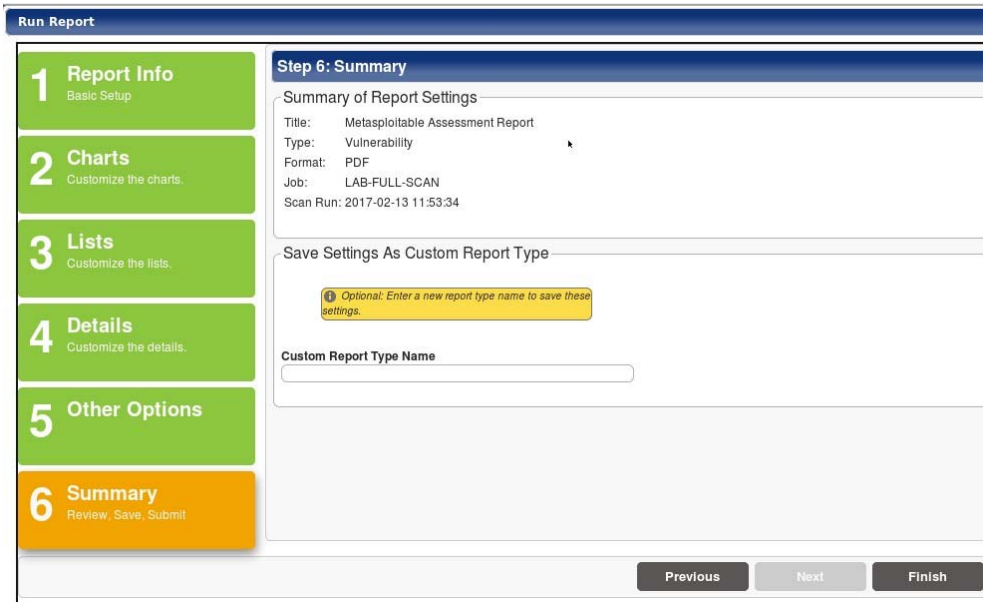
Εικόνα 5.153: Οθόνη επιλογής λεπτομερειών που θα εμφανιστούν στην κατάσταση ευπαθειών.

20. Στην συνέχεια μπορεί να γίνει επιλογή τυποποιημένης εισαγωγής η οποία θα προλογίσει την κατάσταση ευπαθειών, Εικόνα 5.154. Ακολούθως επιλέγεται η επιλογή “Next”.



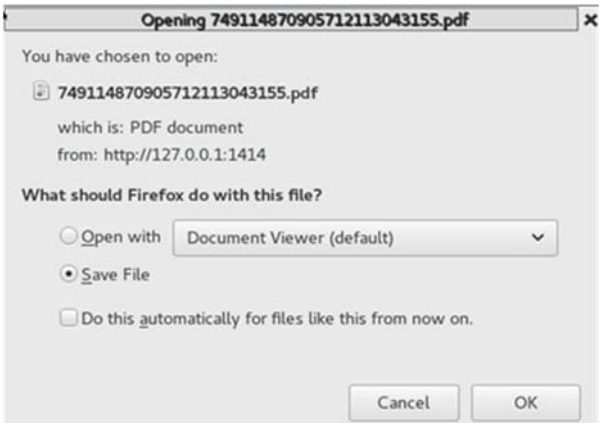
Εικόνα 5.154: Οθόνη επιλογής εμφάνισης προλόγου στην κατάσταση ευπαθειών.

21. Με την καταχώρηση όλων των πληροφοριών η κατάσταση είναι έτοιμη για εξαγωγή, Εικόνα 5.155. Επιλέγεται η επιλογή “Finish” για την δημιουργία της κατάστασης.



Εικόνα 5.155: Περίληψη επιλογών κατάστασης ευπαθειών.

22. Εμφανίζεται ο διάλογος για αρχειοθέτηση ή άμεσο άνοιγμα της νεοδημιουργηθέν κατάστασης, Εικόνα 5.156. Η κατάσταση αρχειοθετείται για μελλοντική χρήση.



Εικόνα 5.156: Οθόνη αρχειοθέτησης κατάστασης ευπαθειών σε pdf μορφή.

Η εξαχθείσα PDF κατάσταση με ονομασία "SAINT Metasploitable Assesment Report 1", είναι διαθέσιμη στο CD της εργασίας, στον φάκελο με την ονομασία "SAINT".

Κεφάλαιο 6
Ανεύρεση, Αξιολόγηση και Απαλοιφή Ευπαθειών

Στο παρόν Κεφάλαιο, που ουσιαστικά αποτελεί και το σκοπό της παρούσας μεταπτυχιακής διατριβής, θα γίνει η αξιολόγηση των αποτελεσμάτων, τα οποία έχουν εξαχθεί από τα εργαλεία ανίχνευσης ευπαθειών, που έχουν χρησιμοποιηθεί στο Κεφάλαιο 5. Στην συνέχεια θα γίνει καταγραφή και επιβεβαίωση αριθμού ευπαθειών του Metasploitable 2 και ακολούθως θα διερευνηθεί κατά πόσο αυτές οι ευπάθειες έχουν εντοπιστεί από τα εργαλεία ανίχνευσης ευπαθειών. Ακολούθως θα γίνει τροποποίηση του Metasploitable 2 με βάση τις οδηγίες των εργαλείων, για απαλοιφή των ανευρεθέντων ευπαθειών. Τέλος θα τρέξουν τα εργαλεία για δεύτερη φορά, για να διαφανεί εάν όντος οι ευπάθειες δεν υφίστανται πια.

Στο τέλος του Κεφαλαίου θα καταγραφούν τα αποτελέσματα των εργαλείων και κατά πόσο μπορούν ακόμη να εντοπίσουν τις συγκεκριμένες ευπάθειες. Επίσης θα διεξαχθεί μια αξιολόγηση των εργαλείων ανίχνευσης τρωσιμότητας που έχουν χρησιμοποιηθεί, με έμφαση στην αποδοτικότητα και ευκολία χρήσης των εργαλείων κατά την διαδικασία εγκατάστασης, παραμετροποίησης, διεξαγωγής εκτίμησης τρωσιμότητας και εξαγωγής αποτελεσμάτων. Τέλος

θα γίνει καταγραφή των χαρακτηριστικών που θα πρέπει να διαθέτει το ιδανικό εργαλείο εκτίμησης τρωσιμότητας.

6.1 Ευπάθειες Metasploitable 2

Όπως έχει αναφερθεί και στο Κεφάλαιο 5, το Metasploitable 2 είναι μια ηθελημένα ευπαθής μηχανή και ο σκοπός δημιουργίας της είναι ο έλεγχος αποδοτικότητας των συστημάτων ασφαλείας και η επίδειξη κάποιον κοινών ευπαθειών.

Στην παρούσα μεταπτυχιακή διατριβή το Metasploitable και πιο συγκεκριμένα η δεύτερη έκδοση του, έχει χρησιμοποιηθεί για την αξιολόγηση των πέντε υπό εξέταση εργαλείων ανεύρεσης ευπαθειών των Nmap, OpenVas, Nexpose, Qualys και SAINT.

Το Metasploitable διαθέτει ένα ευρύ αριθμό υπηρεσιών οι οποίες τρέχουν σε διάφορες θύρες και γίνονται εμφανείς με μια απλή διερεύνηση όλων των θυρών της μηχανής.

Σύμφωνα με την Rapid 7 [07], κατασκευαστή του Metasploitable, στο Πίνακα 6.1 διαφαίνονται όλες οι υπηρεσίες του Metasploitable 2 και σε ποια θύρα τρέχει η κάθε υπηρεσία:

Θύρα		Κατάσταση	Υπηρεσία
21	tcp	Open	Vsftpd 2.3.4
22	tcp	Open	Openssh 4.7p1
23	tcp	Open	Linux telnetd
25	tcp	Open	Postfix smtpd
53	tcp	Open	ISC BIND 9.4.2
80	tcp	Open	Apache httpd 2.2.8 Ubuntu DAV/2
111	tcp	Open	rpcbind
139	tcp	Open	Samba smbd 3.X
445	tcp	Open	Samba smbd 3.X
512	tcp	Open	exec
513	tcp	Open	login

Θύρα		Κατάσταση	Υπηρεσία
514	tcp	Open	shell
1099	tcp	Open	GNU Classpath rmiregistry
1524	tcp	Open	shell
2049	tcp	Open	nfs
2121	tcp	Open	ProFTPD 1.3.1
3306	tcp	Open	MySQL 5.0.51a-3ubuntu5
3632	tcp	Open	distccd
5432	tcp	Open	PostgreSQL DB 8.3.0 – 8.3.7
5900	tcp	Open	vnc
6000	tcp	Open	X11
6667	tcp	Open	Unreal ircd
6697	tcp	Open	unknown
8009	tcp	Open	Apache Jserv protocol 1.3
8180	tcp	Open	Apache Tomcat/Coyote JSP engine 1.1
8787	tcp	Open	Unknown
39292	tcp	Open	Unknown
43729	tcp	Open	Unknown
44813	tcp	Open	Unknown
55852	tcp	Open	unknown

Πίνακας 6.1: Ενεργές υπηρεσίες και θήρες στο Metasploitable 2.

Σχεδόν κάθε μια από τις υπηρεσίες περιέχει ευπάθειες και παρέχει σημείο απομακρυσμένης πρόσβασης στο σύστημα.

Συγκεκριμένα στο Metaspoloitable 2 υπάρχουν οι ακόλουθοι πέντε τύποι ευπαθειών:

1. **Μη σωστά διαμορφωμένες υπηρεσίες.** Πολλές από τις υπηρεσίες έχουν διαμορφωθεί με τέτοιο τρόπο ούτως ώστε να παρέχουν απευθείας πρόσβαση στο λειτουργικό σύστημα.

2. **Κερκόπορτες (backdoors).** Κάποια από τα προγράμματα και υπηρεσίες περιέχουν κερκόπορτες. Αυτές οι κερκόπορτες μπορούν να χρησιμοποιηθούν για την απόκτηση πρόσβασης στο λειτουργικό σύστημα.

3. **Αδύναμοι κωδικοί πρόσβασης.** Κωδικοί που χρησιμοποιούνται τόσο για πρόσβαση στο λειτουργικό σύστημα όσο και για την πρόσβαση σε προγράμματα λογισμικού είναι ευπαθείς σε επιθέσεις ωμής βίας. Στην εξαντλητική δηλαδή, δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα ώστε να αποκαλυφθεί το αρχικό μήνυμα.

4. **Ευπαθείς διαδικτυακές υπηρεσίες.** Κάποιες από την προ-εγκατεστημένες υπηρεσίες διαδικτύου εμπεριέχουν γνωστές ευπάθειες όπου μπορούν να εκμεταλλευτούν.

5. **Ευπάθειες διαδικτυακού λογισμικού.** Υπάρχει διαδικτυακό λογισμικό το οποίο είναι ευάλωτο και μπορεί να προσφέρει στον επιτιθέμενο πρόσβαση το λειτουργικό σύστημα του Metasploitable.

Στον Πίνακα 6.2 παρατίθενται επτά (7) από τις επιβεβαιωμένες ευπάθειες του Metasploitable 2, οι οποίες θα τύχουν περαιτέρω διερεύνησης, στην παρούσα μεταπτυχιακή διατριβή:

Α/Α	Θύρα	Υπηρεσία	Ευπάθεια
1	21	Vsftpd 2.3.4	Έχει ανακαλυφθεί ότι η έκδοση του 2.3.4, η οποία ήταν διαθέσιμη για κατέβασμα στην ιστοσελίδα διάθεσης του εργαλείου, έχει αντικατασταθεί με παραβιασμένη έκδοση του εργαλείου που εμπεριέχει κερκόπορτα.
2	6667	Unreal ircd	Στην θύρα αυτή είναι ενεργή η υπηρεσία UnrealRCD IRC daemon της οποίας η έκδοση αυτή, v. 3.2.8.1, εμπεριέχει κερκόπορτα.
3	1524	shell	Στην θύρα αυτή είναι διαθέσιμη η γνωστή κερκόπορτα “ingreslock” η οποία ήταν αρκετά δημοφιλής προ δεκαετίας για την ενεργοποίηση κερκόπορτας σε εξυπηρετητή όπου διακυβευόταν η ασφάλεια του.
4	3632	distccd	Η υπηρεσία αυτή αποτελεί εκ φύσεως κεκρόπορτα. Ένας κακόβουλος χρήστης μπορεί εύκολα να την εκμεταλλευτεί και να τρέξει οποιαδήποτε εντολή επιθυμεί στον απομακρυσμένο υπολογιστή.
5	22	Openssh 4.7p1	Χρησιμοποιούνται αδύναμοι κωδικοί αυθεντικοποίησης σαν αποτέλεσμα της ενσωματωμένης γεννήτριας αριθμών η οποία

Α/Α	Θύρα	Υπηρεσία	Ευπάθεια
			δημιουργεί εύκολα προβλέψιμους αριθμούς.
6	2049	NFS	Η υπηρεσία NFS (Network File System) επιτρέπει την πρόσβαση σε φακέλους που είναι διαθέσιμοι στο δίκτυο, από τους χρήστες. Η υπηρεσία αυτή έχει ηθελημένα διαμορφωθεί λανθασμένα.
7	80	Apache httpd 2.2.8 Ubuntu DAV/2	Ο φάκελος http://"ip-address"/doc ο οποίος περιέχει ευαίσθητες πληροφορίες είναι διαθέσιμος σε όλους.

Πίνακας 6.2: Επτά επιβεβαιωμένες ευπάθειες για το Metasploitable 2.

6.1.1 Βαθμίδες Αξιολόγησης Ευπαθειών

Χρησιμοποιώντας τις καταστάσεις ανεύρεσης ευπαθειών οι οποίες έχουν δημιουργηθεί από τα εργαλεία Nmap, OpenVas, Nexpose, Qualys και SAINT στο Κεφάλαιο 5, θα διερευνηθεί κατά πόσο έχουν εντοπιστεί και πως έχουν αξιολογηθεί οι πιο πάνω επτά ευπάθειες. Το κάθε εργαλείο διαθέτει βαθμίδες αξιολόγησης των ευπαθειών που εντοπίζει, με μόνη εξαίρεση το Nmap.

OpenVas και Nmap

Το εργαλείο OpenVas χρησιμοποιεί τις βαθμίδες αξιολόγησης του CVSS (Common Vulnerability Scoring System) το οποίο είναι ένα δωρεάν, ανοικτού τύπου πρότυπο για την εκτίμηση της σοβαρότητας των ευπαθειών ασφαλείας των συστημάτων πληροφορικής.

Όσο αφορά το Nmap, σε αριθμό ευπαθειών που εντοπίζει, παρουσιάζει και αυτό τις βαθμίδες αξιολόγησης στου CVSS, χωρίς όμως να ισχύει πάντοτε αυτό. Το Nmap μπορεί να εντοπίζει μια ευπάθεια αλλά μην παρουσιάζει τη βαθμίδα αξιολόγησης της και εναπόκειται στον διαχειριστή να πραγματοποιήσει επιπλέον έρευνα για να αξιολογήσει σωστά την ευπάθεια που έχει εντοπιστεί.

Το CVSS έχει αναπτυχθεί από το FIRST (Forum of Incident Response and Security Teams), έναν μη κερδοσκοπικό οργανισμό με έδρα της Ηνωμένες Πολιτείες Αμερικής, που έχει ως αποστολή να παρέχει βοήθεια στις ομάδες προστασίας μηχανογραφικού υλικού ανά των κόσμο . Το CVSS επιχειρεί να βαθμολογήσει την σοβαρότητα μιας ευπάθειας χρησιμοποιώντας στον αλγόριθμο αξιολόγησης μέτρησης, που έχει να κάνει με την ευκολία εκμετάλλευσής της, καθώς και με τις επιπτώσεις που θα προκύψουν εάν πραγματοποιηθεί η εκμετάλλευση αυτή. Το CVSS

αποτελείται από τρείς μετρικές ομάδες, τη Βασική (Base), τη Προσωρινή (Temporal) και την Περιβαλλοντική (Environmental).

Η Base περιλαμβάνει τις εγγενείς ιδιότητες μιας ευπάθειας οι οποίες παραμένουν αναλλοίωτες με την πάροδο του χρόνου και ανεξάρτητα από το μηχανογραφικό περιβάλλον που χρησιμοποιούν οι χρήστες. Η Temporal περιλαμβάνει τα χαρακτηριστικά της ευπάθειας που μεταβάλλονται με την πάροδο του χρόνου και η Environmental περιλαμβάνει τα χαρακτηριστικά εκείνα της ευπάθειας τα οποία είναι μοναδικά για το μηχανογραφικό περιβάλλον του χρήστη.

Σύμφωνα με την τελευταία έκδοση του CVSS,v3.0, μια ευπάθεια με βαθμολογία:

- "0.0" αξιολογείται με **"NONE"** Δεν έχει εντοπιστεί κάποια ευπάθεια.
- "0.1-3.9" αξιολογείται με **"LOW"** Έχει εντοπιστεί ευπάθεια με **χαμηλό** ρίσκο.
- "4.0-6.9" αξιολογείται με **"MEDIUM"** Έχει εντοπιστεί ευπάθεια με **μέτριο** ρίσκο.
- "7.0-8.9" αξιολογείται με **"HIGH"** Έχει εντοπιστεί ευπάθεια με **υψηλό** ρίσκο.
- "9.0-10.0" αξιολογείται με **"CRITICAL"** Έχει εντοπιστεί ευπάθεια με **κρίσιμο** ρίσκο.

Nexpose

Το Nexpose για την εκτίμηση της σοβαρότητας των ευπαθειών χρησιμοποιεί στην φόρμουλα του τις τιμές του CVSS αναφορικά με την επίπτωση και την πιθανότητα εκμετάλλευσης μιας ευπάθειας και τις συνδυάζει με την έκθεση της ευπάθειας αυτής στον αριθμό αυτοματοποιημένων εργαλείων εκμετάλλευσης της, καθώς και με τη συχνότητα εκμετάλλευσης της.

Η βαθμίδες αξιολόγησης του Nexpose είναι ως ακολούθως:

- Ευπάθειες με βαθμολογία από **8-10** θεωρούνται υψηλού ρίσκου: **CRITICAL**

- Ευπάθειες με βαθμολογία από **6-7.9** θεωρούνται μεσαίου ρίσκου: **SEVERE**

- Ευπάθειες με βαθμολογία από **4-5.9** θεωρούνται χαμηλού ρίσκου: **MODERATE**

Qualys

Το Qualys αξιολογεί την κάθε ευπάθεια που θα εντοπίσει με βάση το ρίσκο ασφαλείας το οποίο ενέχεται με την εκμετάλλευσή της. Επιπρόσθετα λαμβάνονται υπόψη παράγοντες όπως η πολυπλοκότητα της διαδικασίας εκμετάλλευσης και η πιθανότητα να πραγματοποιηθεί η εκμετάλλευση σε κανονικές συνθήκες. Ρόλο επίσης παίζουν τα δικαιώματα χρήστη που χρειάζεται ο επιτιθέμενος για να πραγματοποιήσει μια επιτυχημένη επίθεση, καθώς επίσης για το αν υπάρχουν διαθέσιμα κακόβουλα λογισμικά ή γνωστές τακτικές επίθεσης, όπου η εκμετάλλευση της ευπάθειας μπορεί να πραγματοποιηθεί με μεγαλύτερη ευκολία. Οι ευπάθειες στο Qualys διαχωρίζονται σε τρεις κατηγορίες οι οποίες είναι:

1. **Vulnerabilties:** Περιλαμβάνονται οι επιβεβαιωμένες ευπάθειες.

2. **Potential Vulnerabilties:** Περιλαμβάνονται οι ευπάθειες οι οποίες δεν μπορούν να επιβεβαιωθούν επακριβώς αλλά χρήζουν περαιτέρω προσοχής και ανάλυσης.

Οι συνέπειες που συνδέονται με την κάθε ευπάθεια αξιολογούνται με τα ακόλουθα επίπεδα σοβαρότητας και για τις δύο κατηγορίες ευπαθειών:

- **Urgent (Severity 5)** Ο επιτιθέμενος μπορεί εύκολα να αποκτήσει τον έλεγχο του υπολογιστή-στόχου, με πιθανό αποτέλεσμα την εκμετάλλευση ολόκληρου του δικτύου. Ευπάθειες αυτού του τύπου περιλαμβάνουν την απόκτηση πλήρους δικαιώματος τροποποίησης (read/write) αρχείων, εκτέλεση εντολών από απομακρυσμένο σημείο και ύπαρξη κερκόπορτας.

- **Critical (Severity 4)** Ο επιτιθέμενος υπάρχει μεγάλη πιθανότητα να αποκτήσει τον έλεγχο του υπολογιστή-στόχου ή υπάρχει μεγάλη πιθανότητα διαρροής εξαιρετικά ευαίσθητων πληροφοριών. Ευπάθειες στο επίπεδο αυτό μπορεί να περιλαμβάνουν δικαιώματα ανάγνωσης αρχείων, πιθανή ύπαρξη κερκόπορτας ή εξαγωγή της λίστας των χρηστών που χρησιμοποιούν τον συγκεκριμένο υπολογιστή.

- **Serious (Severity 3)** Ο επιτιθέμενος υπάρχει πιθανότητα να αποκτήσει πρόσβαση σε συγκεκριμένες πληροφορίες που είναι αποθηκευμένες στον υπολογιστή-στόχο, συμπεριλαμβανομένου πληροφορίες ασφαλείας. Ευπάθειες στο επίπεδο μπορούν να περιλαμβάνουν μερική πρόσβαση στο περιεχόμενο αρχείων, εμφάνιση λίστας φακέλων και περιεχομένου αυτών, να επιτραπεί επίθεση άρνησης υπηρεσίας ή μη εξουσιοδοτημένης χρήσης υπηρεσίας, όπως η αναμετάδοση ηλεκτρονικού ταχυδρομείου (Mail Relaying).

- **Medium (Severity 2)** Ο επιτιθέμενος μπορεί να περισυλλέξει πληροφορίες από τον υπολογιστή-στόχο, όπως λόγου χάρη πληροφορίες για την έκδοση που έχει ένα εγκατεστημένο λογισμικό. Τις πληροφορίες αυτές θα μπορεί να τις χρησιμοποιήσει για την ανεύρεση ευπαθειών για την συγκεκριμένη έκδοση του λογισμικού αυτού.

- **Minimal (Severity 1)** Ο επιτιθέμενος μπορεί να περισυλλέξει πληροφορίες από τον υπολογιστή-στόχο αναφορικά με της θύρες που έχει ανοιχτές και τις υπηρεσίες που τρέχουν σε αυτές. Τις πληροφορίες αυτές θα μπορεί να τις χρησιμοποιήσει για την ανεύρεση άλλων ευπαθειών.

3. **Information Gathered:** Περιλαμβάνονται πληροφορίες που μπορεί να αποκομιστούν για τον host όπως πληροφορίες traceroute, ISP κ.α ή πληροφορίες δικτύου όπως διαθέσιμα firewalls ή μια λίστα με διαθέσιμες TCP υπηρεσίες. Αξιολογείται με τα ακόλουθα τρία επίπεδα σοβαρότητας:

   - **Minimal (Severity 1)** Ο εισβολές μπορεί να αποκομίσει πληροφορίες σχετικές με τον host όπως UDP και TCP υπηρεσίες.

   - **Medium (Severity 2)** Ο εισβολές μπορεί να αποκομίσει πληροφορίες σχετικά με το λειτουργικό σύστημα του host.

   - **Serious (Severity 3)** Ο εισβολές μπορεί να αποκομίσει ευαίσθητες πληροφορίες, όπως λίστες χρηστών.

SAINT

Το SAINT εμπεριέχει τέσσερα επίπεδα σοβαρότητας ανευρεθέντων προβλημάτων Critical Problems, Areas of Concern, Potential Problems και Services.

- **Critical Problems** Ο επιτιθέμενος μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αρχεία που είναι αποθηκευμένα στον υπολογιστή-στόχο, να εκτελέσει εντολές ή να διενεργήσει επίθεση άρνησης υπηρεσίας (DoS attack).

- **Areas of Concern** Στο επίπεδο αυτό περιλαμβάνονται προβλήματα τα οποία δεν επιτρέπουν την άμεση μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή-στόχο από τον επιτιθέμενο, αλλά επιτρέπουν την εξαγωγή πληροφοριών σχετικά με τον υπολογιστή-στόχο ή ακόμα και το δίκτυο στο οποίο βρίσκεται ο υπολογιστής αυτός. Επίσης ο επιτιθέμενος, υπάρχει πιθανότητα, να μπορεί να αποκτήσει δικαιώματα περεταίρω εξουσιοδοτημένης πρόσβασης με την εξύψωση (Privilege Elevation) των δικαιωμάτων που έχει ήδη αποκτήσει.

- **Potential Problems** Υπάρχουν περιπτώσεις όπου μπορεί να υπάρχουν ευπάθειες ή μπορεί να μην υπάρχουν. Αυτό θα εξαρτάται από την έκδοση ή και τις ρυθμίσεις της ανευρεθέν υπηρεσίας. Το SAINT δεν μπορεί πάντα να αντιλαμβάνεται εάν υπάρχει ή όχι ευπάθεια. Θα πρέπει στο επίπεδο αυτό να διενεργείται επιπλέον έλεγχος από την πλευρά του διαχειριστή και να μην εκλαμβάνεται ως χαμηλού ρίσκου ο εντοπισμός αυτός.

- **Services** Καταδεικνύει, για σκοπούς πληροφόρησης, την ύπαρξη των ενεργών δικτυακών υπηρεσιών. Αυτό δεν εκλαμβάνεται ως κατάδειξη οποιασδήποτε ευπάθειας.

Με την χρήση των εξαχθεισών καταστάσεων καταγραφής ευπαθειών από τα εργαλεία, που δημιουργηθήκαν στο Κεφάλαιο 5, καταγράφεται στο Πίνακα 6.3, για κάθε μια από τις επτά ευπάθειες, από ποιο εργαλείο έχει εντοπιστεί (√), πώς έχει αξιολογηθεί και σε ποια σελίδα της κατάστασης αξιολόγησης υπάρχουν πληροφορίες για την ευπάθεια αυτή. Στην περίπτωση που κάποιο εργαλείο δεν έχει καταφέρει να εντοπίσει κάποια από τις ευπάθειες καταχωρείται "-" :

A/A	Θύρα	Υπηρεσία	NMAP	OpenVas	Nexpose	Qualys	SAINT
1	21	Vsftpd 2.3.4	√ High	√ High (σελ.116)	√ Severe (σελ.128)	√ Vulnerabilities Severity 2 (σελ.253)	√ Potential (σελ.1127)
2	6667	Unreal ircd	√ Critical	-	-	-	-
3	1524	shell	-	√ High (σελ.115)	√ Critical (σελ.14)	√ Vulnerabilities Severity 5 (σελ.14)	√ Potential (σελ.734)
4	3632	distccd	√ High	√ High (σελ.103)	-	-	-
5	22	Openssh 4.7p1	√ High	-	√ Critical (σελ.70)	-	-
6	2049	NFS	-	-	√ Severe (σελ.275)	√ Vulnerabilities Severity 3 (σελ.51)	√ Critical (σελ.677)
7	80	Apache httpd 2.2.8 Ubuntu DAV/2	√ High	-	√ Severe (σελ.244)	√ Vulnerabilities Severity 2 (σελ.229)	-

Πίνακας 6.3: Εντοπισμός των υπό εξέταση ευπαθειών από τα εργαλεία Nmap, OpenVas, Nexpose, Qualys και SAINT.

6.2 Απαλοιφή Ευπαθειών

Στο στάδιο αυτό θα καταγραφεί για κάθε μια από τις επτά ευπάθειες η προτεινόμενη λύση για την απαλοιφή της, εάν και εφόσον υπάρχει, από κάθε εργαλείο ξεχωριστά. Ακολούθως με βάση τις οδηγίες θα γίνουν οι δέοντες ενέργειες για εξάλειψη των ευπαθειών αυτών.

Όσο αφορά το εργαλείο Nmap, δεν δηλώνει ξεκάθαρα τι ευπάθεια εμπεριέχει η υπό εξέταση υπηρεσία, αλλά παραθέτει ένα αριθμό πιθανόν ευπαθειών σε σχέση με την υπηρεσία αυτή αλλά και σε σχέση με την έκδοσή της. Θα γίνει διερεύνηση κατά πόσο έχει εντοπιστεί η σωστή έκδοση της υπηρεσίας και εάν έχει στην συνέχεια παρατεθεί η σωστή ευπάθεια. Επιπρόσθετα το εργαλείο αυτό δεν παρουσιάζει λύσεις για την αντιμετώπιση των ευπαθειών, αλλά θα γίνει

προσπάθεια, στην περίπτωση που δεν δίνεται λύση από κάποιο άλλο από τα τέσσερα εργαλεία να επιδιορθωθεί η ευπάθεια.

6.2.1 Λύσεις Απαλοιφής Ευπαθειών

Ευπάθεια 1

Θύρα: 21

Υπηρεσία: vsftpd

Εντοπίστηκε από: Nmap, OpenVas, Nexpose, Qualys, SAINT

- **Nmap (NMAP VulScan Metasploitable Assesment Report 1)**

  Αξιολόγηση: High

  Περιγραφή: MITRE CVE - http://cve.mitre.org: [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.

  Προτεινόμενη Λύση: /

- **OpenVas (OpenVas Metasploitable Assesment Report 1, σελ.104)**

  Αξιολόγηση: High

  Περιγραφή: Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

  Προτεινόμενη Λύση: The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

- **Nexpose (Nexpose Metasploitable Assesment Report 1, σελ.128)**

Αξιολόγηση: Severe

Περιγραφή: The server supports authentication methods in which credentials are sent in plaintext over unencrypted channels. If an attacker were to intercept traffic between a client and this server, the credentials would be exposed.

Προτεινόμενη Λύση: Disable plaintext authentication methods or enable encryption for the FTP service. Refer to the software's documentation for specific instructions.

- **Qualys (Qualys Metasploitable Assesment Report 1, σελ.253)**

Αξιολόγηση: Vulnerabilities Severity 2

Περιγραφή: Users can access the FTP server using the "anonymous" or "ftp"account with any password. Some FTP server software is installed with Anonymous access enabled by default. Vulnerable systems include RedHat Linux installations and Microsoft IIS (Internet Information Server) installations.

Προτεινόμενη Λύση: You should first decide if you really require the FTP service on this host. If you use it to exchange files between users, you should either use a dedicated password-protected account, or, by default, an unreadable but writeable directory. The security of this last option depends on the secrecy of the filenames you upload and download from this directory. Therefore, avoid guessable filenames like "backup", "accounting" or "project".

- **SAINT (SAINT Metasploitable Assesment Report 1, σελ.1127)**

Αξιολόγηση: Potential

Περιγραφή: The vulnerabilities in the vsftpd FTP Server could lead to denial-of-service conditions, or arbitrary command execution through a backdoor.

Προτεινόμενη Λύση: Upgrade vsftpd to a version higher than 2.3.4 when available, or apply the patch from your vendor.

Ευπάθεια 2

Θύρα: 6667

Υπηρεσία: irc (unreal ircd, v3.2.8.1)

Εντοπίστηκε από: Nmap

- **Nmap (NMAP Scripts Metasploitable Assesment Report 1)**

  Αξιολόγηση: Critical

  Περιγραφή:

  Exploit-DB - http://www.exploit-db.com:

  UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow

  UnrealIRCD 3.2.8.1 Backdoor Command Execution

  Unreal IRCD 3.2.8.1 - Remote Downloader/Execute Trojan

  This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

  Προτεινόμενη Λύση: /

Ευπάθεια 3

Θύρα: 1524

Υπηρεσία: shell

Εντοπίστηκε από: OpenVas, Nexpose, Qualys, SAINT

- **OpenVas (OpenVas Metasploitable Assesment Report 1, σελ. 115)**

Αξιολόγηση: High

Περιγραφή: A backdoor is installed on the remote host. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected system.

Προτεινόμενη Λύση: /

- **Nexpose (Nexpose Metasploitable Assesment Report 1, σελ. 14)**

Αξιολόγηση: Critical

Περιγραφή: A non-standard service was found that provides a means to establish local shell access on the host over the network.

Note: The presence of a "backdoor" is a serious security concern. It indicates a high probability that this asset has been compromised and is at risk of being leveraged by malicious users.

Προτεινόμενη Λύση: Determine the mechanism used to create the backdoor and safely disable or remove it.

- **Qualys (Qualys Metasploitable Assesment Report 1, σελ. 14)**

Αξιολόγηση: Vulnerabilities Severity 5

Περιγραφή: The presence of a remote shell that does not require any form of authentication was detected. This may be an indication that this host was previously hacked into and malicious programs were installed.

Προτεινόμενη Λύση: You should take immediate actions to remove this vulnerability.

- **SAINT (SAINT Metasploitable Assesment Report 1, σελ.734)**

Αξιολόγηση: Potential

Περιγραφή: The ingreslock port (1524/TCP) is often used as a backdoor by programs which exploit vulnerable RPC (Remote Procedure Call) services. The backdoor is usually accompanied by a file called /tmp/bob which is the configuration file which opens a shell on the port.

Προτεινόμενη Λύση: Although the backdoor can be easily removed, this does not solve the problem at its root. If the vulnerability which was exploited is not corrected, there is nothing to stop the attacker from running the exploit again. The system should be taken offline and scanned for vulnerabilities. All problems should be fixed before the system is put back online.

Also note that not all vulnerability exploits create backdoors such as the ones described above. Sometimes there is no way to tell if a vulnerability has been exploited other than intrusion detection logs. Good security practices should always be followed, and systems should be scanned for vulnerabilities periodically.

You may wish to read CERT's Steps for Recovering from a UNIX or NT System Compromise. The ingreslock, 9704/TCP, and 77/TCP backdoors (i.e., on UNIX-based systems) can be removed by restoring /etc/inetd.conf, removing any unauthorized configuration files such as /tmp/bob or z, and restarting the inetd process. Only one inetd process should be running. Any extraneous processes should be killed.

Ευπάθεια 4

Θύρα: 3632

Υπηρεσία: distccd

Εντοπίστηκε από: Nmap, OpenVas

- **Nmap (NMAP Scripts Metasploitable Assesment Report 1)**

  Αξιολόγηση: High

  Περιγραφή: Allows executing of arbitrary commands on systems running distccd 3.1 and earlier. The vulnerability is the consequence of weak service configuration.

Προτεινόμενη Λύση: /

- **OpenVas (OpenVas Metasploitable Assesment Report 1, σελ. 117)**

  Αξιολόγηση: High

  Περιγραφή: Distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

  Προτεινόμενη Λύση: Vendor updates are available. Please see the references for more information.

  References: CVE: CVE-2004-2687

  Other: URL:http://distcc.samba.org/security.html

  URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687

  URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html

Ευπάθεια 5

Θύρα: 22

Υπηρεσία: ssh

Εντοπίστηκε από: Nmap, Nexpose

- **Nmap (NMAP VulScan Metasploitable Assesment Report 1)**

  Αξιολόγηση: High

  Περιγραφή: [CVE-2008-2285] The ssh-vulnkey tool on Ubuntu Linux 7.04, 7.10, and 8.04 LTS does not recognize authorized_keys lines that contain options, which makes it easier

for remote attackers to exploit CVE-2008-0166 by guessing a key that was not identified by this tool.

Προτεινόμενη Λύση: /

- **Nexpose (Nexpose Metasploitable Assesment Report 1, σελ.70)**

  Αξιολόγηση: Critical

  Περιγραφή: A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates. This vulnerability only affects operating systems which are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them

  Προτεινόμενη Λύση: Upgrade the OpenSSL package to the version recommended below to fix the random number generator and stop generating weak keys

    - For Debian 4.0 etch, upgrade to 0.9.8c-4etch3
    - For Debian testing (lenny), upgrade to 0.9.8g-9
    - For Debian unstable (sid), upgrade to 0.9.8g-9
    - For Ubuntu 7.0.4 (feisty), upgrade to 0.9.8c-4ubuntu0.3
    - For Ubuntu 7.10 (gusty), upgrade to 0.9.8e-5ubuntu3.2
    - For Ubuntu 8.0.4 (hardy), upgrade to 0.9.8g-4ubuntu3.1

  Then regenerate all cryptographic key material which has been created by vulnerable OpenSSL versions on Debian-based systems. Affected keys include SSH server and user keys, OpenVPN keys, DNSSEC keys, keys associated to X.509 certificates, etc. Optionally, Debian and Ubuntu have released updated OpenSSH, OpenSSL and OpenVPN packages to

automatically blacklist known weak keys. It is recommended to install these upgrades on all systems.

Ευπάθεια 6

Θύρα: 2049

Υπηρεσία: NFS

Εντοπίστηκε από: Nexpose, Qualys, SAINT

- **Nexpose (Nexpose Metasploitable Assesment Report 1, σελ. 275)**

  Αξιολόγηση: Severe

  Περιγραφή: An NFS volume is mountable by everyone. Although this is not necessarily a vulnerability itself, this does not exhibit "best practice" from a security standpoint; mounting privileges should be restricted only to hosts that require them.

  Προτεινόμενη Λύση: Restrict mounting privileges to only hosts that require them.

- **Qualys (Qualys Metasploitable Assesment Report 1, σελ. 51)**

  Αξιολόγηση: Vulnerabilities Severity 3

  Περιγραφή: This system is running a Network File System (NFS) server that enables a remote host to acess and share files and directories. The current configuration of this system gives both authorized and unauthorized users the list of exported disks and authorized hosts.

  Προτεινόμενη Λύση: If the NFS server is not required on this system, then shutdown and disable the "mountd" and "nfsd" RPC services. If the NFS server is required on this system, then the solution is not as simple. Since the server's clients need to be able to access the export list, this service cannot be shutdown. Access can be restricted to hosts on the local network or hosts that are authorized clients of this server. Use either a packet filter at the system level (local packet filter) or a centralized packet filter on the firewall.

Note, however, that using a firewall in front of your network will not secure the service itself, but will limit the risk to internal attacks

- **SAINT (SAINT Metasploitable Assesment Report 1, σελ.677)**

  Αξιολόγηση: Critical

  Περιγραφή: The lack of adequate NFS access restrictions allows unauthorized access to system and/or user files. Unrestricted access allows hackers to modify files on the system. An intruder could remotely compromise user or system files and then take over the machine. For example, an intruder could remotely replace a system program or configuration file. On UNIX systems, an intruder could remotely install an .rhosts file to obtain interactive access (allowing the intruder to login to the system) or remotely install a .forward file to obtain non-interactive access (the .forward file forwards a user's mail to a location specified in the file).

  Προτεινόμενη Λύση: To correct this vulnerability, make sure that all file exports specify an explicit list of clients or netgroups. Also, export all file systems as read-only where possible. It should be noted that some versions of the NFS mount daemon cannot expand large netgroups and will export to the world anyway. This problem is specific to some versions of the SunOS and is described in CERT Advisory 94.02 (link provided below). Also, be sure to check vendor patch lists. Consider blocking ports 2049 (NFS) and 111 (portmap) on routers. It should be noted that, in NIS netgroup members, empty host fields are treated as wildcards and cause the mount daemon to grant access to any host.

Ευπάθεια 7

Θύρα: 80

Υπηρεσία: Apache httpd 2.2.8 Ubuntu DAV/2

Εντοπίστηκε από: Nmap, Nexpose, Qualys

- **Nmap (NMAP Scripts Metasploitable Assesment Report 1)**

  Αξιολόγηση: High

Περιγραφή: /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'

Προτεινόμενη Λύση: /

- **Nexpose (Nexpose Metasploitable Assesment Report 1, σελ. 244)**

  Αξιολόγηση: Severe

  Περιγραφή: A web directory was found to be browsable, which means that anyone can see the contents of the directory. These directories can be found:

  - via page spidering (following hyperlinks), or
  - as part of a parent path (checking each directory along the path and searching for "Directory Listing" or similar strings), or
  - by brute forcing a list of common directories.

  Browsable directories could allow an attacker to perform a directory traversal attack by viewing "hidden" files in the web root, including CGI scripts, data files, or backup pages.

  Προτεινόμενη Λύση: Disable web directory browsing for all directories and subdirectories in your httpd.conf file, disable the "Indexes" option for the appropriate <Directory> tag by removing it from the Options line. In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

- **Qualys (Qualys Metasploitable Assesment Report 1, σελ. 229)**

  Αξιολόγηση: Vulnerabilities Severity 2

Περιγραφή: Listing of files in the /doc/ directory is allowed. For example, a default configuration of Apache on Debian Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.

Προτεινόμενη Λύση: Set a more restrictive rule on your server to prevent directory listing of the doc directory.

6.2.2 Ενέργειες Απαλοιφής Ευπαθειών

Προκαταρτικές ενέργειες

Το λειτουργικό σύστημα του Metasploitable, όπως έχει αναφερθεί και στο Κεφάλαιο 5, είναι το Ubuntu Linux 8.0.4 Hardy. Πρόκειται για ένα παλαιό λειτουργικό σύστημα για το οποίο έχουν σταματήσει να προσφέρονται αναβαθμίσεις ασφαλείας.

Για να γίνει κατορθωτή η πρόσβαση στις τελευταίες αναβαθμίσεις που προσφέρονται για το συγκεκριμένο λειτουργικό σύστημα, ούτως ώστε να επιτευχθεί η απαλοιφή κάποιων από τις ευπάθειες, θα πρέπει αρχικά να γίνουν κάποιες τροποποιήσεις στο αρχείο διαχείρισης ανεύρεσης αναβαθμίσεων. Το αρχείο αυτό είναι το **sources.list**.

Θα εκτελεστούν οι ακόλουθες οδηγίες για πρόσβαση και τροποποίηση στου αρχείου sources.list.

1. Από την γραμμή εντολών εκτελείτε η εντολή:

$sudo nano /etc/apt/sources.list

2. Αφού επιτευχθεί πρόσβαση στο αρχείο θα πρέπει να τοποθετηθεί ## σε όλες τις υφιστάμενες εντολές. Ακολούθως θα πρέπει να προστεθούν οι πιο κάτω εγγραφές-εντολές που θα παραπέμπουν στα αρχεία αναβαθμίσεων και στη συνέχεια θα γίνει αποθήκευση του τροποποιημένου αρχείου:

- **deb http://old-releases.ubuntu.com/ubuntu/ CODENAME main restricted universe multiverse**

- **deb http://old-releases.ubuntu.com/ubuntu/ CODENAME-updates main restricted universe multiverse**

- **deb http://old-releases.ubuntu.com/ubuntu/ CODENAME-security main restricted universe multiverse**

3. Έχοντας επιστρέψει στην γραμμή εντολών, θα πρέπει να γίνει η επικύρωση της λίστας των διαθέσιμων αναβαθμίσεων για τα εγκατεστημένα πακέτα που βρίσκονται στο σύστημα. Για το λόγο αυτό εκτελείται η εντολή:

$sudo apt-get upgrade

Ενέργειες για απαλοιφή ευπαθειών

Ευπάθεια 1

Θύρα: 21

Υπηρεσία: vsftpd

Περιγραφή : Έχει ανακαλυφθεί ότι η έκδοση του 2.3.4, η οποία ήταν διαθέσιμη για κατέβασμα στην ιστοσελίδα διάθεσης του εργαλείου, έχει αντικατασταθεί με παραβιασμένη έκδοση του εργαλείου που εμπεριέχει κερκόπορτα.

Τα εργαλεία προτείνουν την αναβάθμιση της έκδοση του εργαλείου. Επίσης προτείνεται η σωστή διαχείριση των χρηστών που έχουν πρόσβαση, ούτως ώστε να μην επιτρέπεται η πρόσβαση σε μη εξουσιοδοτημένα άτομα.

Για να την αναβάθμιση του vsfptd θα εκτελεστεί από την γραμμή των εντολών η πιο κάτω εντολή:

$sudo apt-get install vsftpd

Μετά την αναβάθμιση της υπηρεσίας θα πρέπει να γίνει επανεκκίνηση της, με την εντολή:

$sudo /etc/init.d/vsftpd restart

Για την ασφαλή λειτουργία του ftp server θα γίνουν κάποιες τροποποιήσεις στο αρχείο διαχείρισης του, το οποίο είναι το **vsftpd.conf**.

Από την γραμμή εντολών αποκτάται πρόσβαση στο αρχείο διαχείρισης:

$sudo nano /etc/vsftpd.conf

Στην συνέχεια εντοπίζεται η ρύθμιση: **anonymous_enable = YES** και τροποποιείται σε **anonymous_enable = NO** για να μην επιτρέπεται η πρόσβαση σε μη εξουσιοδοτημένους ανώνυμους χρήστες. Ακολούθως εντοπίζεται η ρύθμιση η οποία περιορίζει την πρόσβαση των χρηστών μόνο στο δικό τους χώρο αρχειοθέτησης στον ftp server και ενεργοποιείται:

#chroot_local_user=YES η οποία και ενεργοποιείται με την απαλοιφή του #.

Η υπηρεσία ftp είναι σχεδιασμένη χωρίς κρυπτογράφηση με αποτέλεσμα να είναι ευάλωτη σε υποκλοπές. Για τον λόγο αυτό θα γίνει ενεργοποίηση του SSL/TLS για την παροχή κρυπτογράφησης.

Από την γραμμή εντολών εκτελείται η εντολή:

$ sudo openssl req -x509 -days 365 -newkey rsa:2048 -nodes -keyout /etc/vsftpd.pem -out /etc/vsftpd.pem

Στην συνέχεια προστίθενται οι ακόλουθες παράμετροι στο αρχείο vsftpd.conf:

- **# enable TLS/SSL**

  ssl_enable=YES

- **# force client to use TLS when logging in**

  allow_anon_ssl=NO

  force_local_data_ssl=YES

  force_local_logins_ssl=YES

  ssl_tlsv1=YES

ssl_sslv2=NO

ssl_sslv3=NO

require_ssl_reuse=NO

ssl_ciphers=HIGH

- **# specify SSL certificate/private key**

  rsa_cert_file=/etc/vsftpd.pem

  rsa_private_key_file=/etc/vsftpd.pem

- **# define port range for passive mode connections**

  pasv_max_port=65535

  pasv_min_port=64000

Ακολούθως για αποφυγή επιθέσεων, τύπου DoS, θα γίνει παραμετροποίηση των επιτρεπόμενων συνδέσεων καθώς και του εύρους ζώνης. Για την επίτευξη του στόχου αυτό θα προστεθούν οι ακόλουθοι παράμετροι στο αρχείο vsftpd.conf:

- **## bandwidth allocation per anonymous session is set to roughly 30 KB/s**

  anon_max_rate=30000

- **## each local user is granted roughly 30 KB/s bandwidth**

  local_max_rate=30000

- **## client session is terminated after being idle for 300 seconds**

  idle_session_timeout=300

- **## maximum number of connections per source IP, which can help secure against DoS and DDoS attacks**

  max_per_ip=50

Τέλος αφού αποθηκευθούν όλες οι αλλαγές στο αρχείο vsftpd.conf, γίνεται επανεκκίνηση της υπηρεσίας vsftpd, με την εντολή:

$ sudo /etc/init.d/vsftpd restart

Ευπάθεια 2

Θύρα: 6667

Υπηρεσία: Unreal ircd

Περιγραφή : Στην θύρα αυτή είναι ενεργή η υπηρεσία UnrealRCD IRC daemon της οποίας η έκδοση αυτή, v. 3.2.8.1, εμπεριέχει κερκόπορτα.

Για την απαλοιφή της ευπάθειας θα πρέπει να αφαιρεθεί η εγκατεστημένη έκδοση της υπηρεσίας και να εγκατασταθεί η τρέχουσα έκδοση η οποία μπορεί να ανακτηθεί από την ιστοσελίδα https://www.unrealircd.org.

Για την αφαίρεση της υπηρεσίας Unreal ircd θα πρέπει να διαγράφουν όλοι οι φάκελοι οι οποίοι εμπεριέχουν αρχεία της υπηρεσίας. Για την ανεύρεση των φακέλων, από την γραμμή εντολών θα τρέξει η εντολή:

$ sudo find / -xdev 2>/dev/null -name unreal*

Ακολούθως για την διαγραφή των αρχείων της υπηρεσίας και κατ' επέκταση την απενεργοποίηση της θα τρέξουν οι εντολές:

$sudo rm -rf /usr/bin/unrealircd

$sudo rm -rf /etc/unreal

Σύμφωνα με τις οδηγίες του κατασκευαστή [24] η υπηρεσία UnrealRCd, για λόγους ασφαλείας θα πρέπει να εγκατασταθεί και να ενεργοποιηθεί από ένα λογαριασμό ο οποίος δεν έχει δικαιώματα διαχειριστή (root). Για το λόγο αυτό θα δημιουργηθεί ένας καινούργιος λογαριασμός χρήστη που θα αποσκοπεί στο σκοπό αυτό.

Για την δημιουργία του καινούργιου χρήστη**, unrealircd**, εκτελείται από την γραμμή εντολών η εντολή:

$sudo adduser unrealircd

Μετά την καταχώριση του κωδικού πρόσβασης και των προσωπικών στοιχείων του χρήστη, διενεργείτε διαδικασία αποσύνδεσης από τον υφιστάμενο χρήστη (msfadmin) και πραγματοποιείται επανασύνδεση με την χρήση του νεοδημιουργηθέντος λογαριασμού, unrealircd.

Στην συνέχεια θα γίνει η ανάκτηση της τρέχουσας έκδοσης της υπηρεσίας. Από την γραμμή εντολών εκτελείται η εντολή:

$wget https://www.unrealircd.org/unrealircd4/unrealircd-4.0.11.tar.gz

Μετά το πέρας της λήψης του συμπιεσμένου αρχείου, θα εκτελεστεί η εντολή αποσυμπίεσης του περιεχομένου:

$ tar zxvf unrealircd-4.0.11.tar.gz

Ακολούθως πραγματοποιείται πρόσβαση στο φάκελο unrealircd-4.0.11 που έχει δημιουργηθεί:

$cd unrealircd-4.0.11

Στο σημείο αυτό θα πραγματοποιηθεί η μεταγλώττιση του UnrealRCd. Από την γραμμή εντολής αρχικά εκτελείται η εντολή:

$./Config

Στις ερωτήσεις που εμφανίζονται δεν καταχωρείται κάποια απάντηση και επιλέγεται το “Enter” μέχρι το πέρας αυτών.

Στην συνέχεια για την μεταγλώττιση εκτελείται η εντολή:

$make

Και ακολούθως για την εγκατάσταση της υπηρεσίας εκτελείται η εντολή:

$make install

Το επόμενο στάδιο είναι η δημιουργία του αρχείου διαχείρισης της υπηρεσίας στο νεοδημιουργηθέν φάκελο **unrealircd** (/home/username/unrealircd). Η πρόσβαση στο φάκελο αυτό επιτυγχάνεται με την εντολή:

$cd ~/unrealircd

Το αρχείο το οποίο θα χρησιμοποιηθεί βρίσκεται αποθηκευμένο στο **conf/examples/examples.conf**. Θα δημιουργηθεί αντίγραφο του αρχείου **examples.conf** και θα αποθηκευτεί στο φάκελο **conf.** Χρησιμοποιείτε η πιο κάτω εντολή για την ενέργεια αυτή:

$cp conf/examples/examples.conf conf/unreal

Ακολούθως θα τροποποιηθεί το αρχείο με βάση της οδηγίες που εμφανίζονται κατά το άνοιγμα του:

$sudo nano conf/unrealircd.conf

Και τέλος θα δοθεί η πιο κάτω εντολή για την εκκίνηση της υπηρεσίας:

$ ./unrealircd start

Για την αυτόματη ενεργοποίηση της υπηρεσίας [23] μετά από κάθε εκκίνηση του υπολογιστή θα προστεθεί ένα χρονοδιάγραμμα εργασίας (job schedule) στο εργαλείο Cron, το εργαλείο διαχείρισης χρονοδιαγραμμάτων εργασίας (time based job scheduler) του λειτουργικού συστήματος.

Από την γραμμή εντολών εκτελείται η εντολή:

$crontab –e

Στο αρχείο που εμφανίζεται, προστίθενται οι δύο πιο κάτω γραμμές εντολών και τέλος αποθηκεύεται το αρχείο:

***/5 * * * * /home/yourusername/unrealircd/unrealircd croncheck**

@reboot /home/unrealircd/unrealircd/unrealircd croncheck

Ευπάθεια 3

Θύρα: 1524

Υπηρεσία: shell

Περιγραφή : Στην θύρα αυτή είναι διαθέσιμη η γνωστή κερκόπορτα "ingreslock" η οποία ήταν αρκετά δημοφιλής προ δεκαετίας για την ενεργοποίηση κερκόπορτας σε εξυπηρετητή όπου διακυβευόταν η ασφάλεια του.

Τα εργαλεία προτείνουν την αφαίρεση της κερκόπορτας αυτής. Για να επιτευχθεί ο στόχος αυτός θα πρέπει με την χρήση του τοίχου προστασίας να κλείσει η θύρα 1524.

Από την γραμμή εντολών εκτελούνται οι πιο κάτω εντολές:

Για την δημιουργία αρχείου καταγραφής:

$/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 1524 DROP: " --log-level 7

Για την απόρριψη όλων των εισερχόμενων πακέτων:

$/sbin/iptables -A INPUT -p tcp --dport 1524 -j DROP

Λόγω του ότι η συγκεκριμένη έκδοση Ubuntu δεν διαθέτει το πακέτο **iptables-persistent** όπου θα μπορούσε να χρησιμοποιηθεί για την φύλαξη των πιο πάνω ρυθμίσεων σε μόνιμη βάση, θα χρησιμοποιηθεί μια εναλλακτική λύση.

Στην γραμμή εντολών εκτελείται η πιο κάτω εντολή για φύλαξη των ρυθμίσεων στο αρχείο **iptables.conf :**

$sudo sh -c "iptables-save > /etc/iptables.conf"

Ακολούθως καταχωρείται η πιο κάτω εντολή, στο αρχείο **/etc/network/interface** το οποίο περιλαμβάνει πληροφορίες της κάρτας δικτύου και οι οποίες φορτώνονται με την εκκίνηση του υπολογιστή. Αυτό δίνει τη ευχέρεια να φορτώνονται μαζί με τις εντολές της κάρτας δικτύου και οι εντολές του τοίχου προστασίας, iptables:

post-up iptables-restore < /etc/iptables.conf

Ευπάθεια 4

Θύρα: 3632

Υπηρεσία: distccd

Περιγραφή : Η υπηρεσία αυτή αποτελεί εκ φύσεως κερκόπορτα. Ένας κακόβουλος χρήστης μπορεί εύκολα να την εκμεταλλευτεί και να τρέξει οποιαδήποτε εντολή επιθυμεί στον απομακρυσμένο υπολογιστή.

Για απαλοιφή της συγκεκριμένης ευπάθειας θα γίνει απεγκατάσταση της υφιστάμενης έκδοσης. Λόγω του ότι δεν υπάρχει πρόσφατη έκδοση για το λειτουργικό σύστημα του Metasploitable Ubuntu 8.0.4, δεν θα γίνει επανεγκατάσταση της υπηρεσίας αυτή.

Για την απεγκατάσταση της υπηρεσίας εκτελούνται από την γραμμή εντολών οι εντολές:

$sudo apt-get remove --auto-remove distcc

$sudo apt-get remove --auto-remove distccmon-gnome

Ευπάθεια 5

Θύρα: 22

Υπηρεσία: Openssh

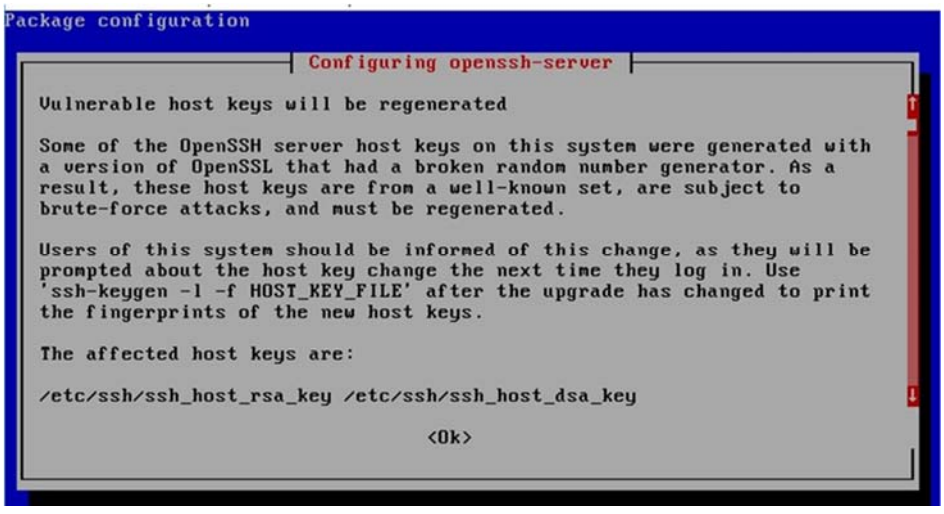
Περιγραφή : Χρησιμοποιούνται αδύναμοι κωδικοί αυθεντικοποίησης σαν αποτέλεσμα της ενσωματωμένης γεννήτριας αριθμών, η οποία δημιουργεί εύκολα προβλέψιμους αριθμούς.

Τα εργαλεία προτείνουν την αναβάθμιση της υφιστάμενη έκδοσης Openssh και την δημιουργία των κλειδιών πρόσβασης.

Σαν πρώτο βήμα θα γίνει η αναβάθμιση του Openssh εκτελώντας από την γραμμή εντολών την εντολή:

$sudo apt-get install openssh-server

Από την οθόνη, η οποία παρουσιάζεται μετά την εκτέλεση την εντολής αναβάθμισης του εργαλείου Openssh, διαφαίνεται ότι όντος τα κλειδιά πρόσβασης είχαν δημιουργηθεί από ελαττωματική γεννήτρια κλειδιών και ότι με την παρούσα αναβάθμιση θα ξαναδημιουργηθούν, Εικόνα 6.1.



Εικόνα 6.1: Εγκατάσταση εργαλείου OpenVas.

Μετά την εγκατάσταση της μη ελαττωματικής έκδοσης του Openssh εκτελείται η πιο κάτω εντολή για την επανεκκίνηση της υπηρεσίας:

$sudo /etc/init.d/ssh restart

Ευπάθεια 6

Θύρα: 2049

Υπηρεσία: NFS

Περιγραφή : Η υπηρεσία NFS (Network File System) επιτρέπει την πρόσβαση σε φακέλους που είναι διαθέσιμοι στο δίκτυο, από τους χρήστες. Η υπηρεσία αυτή έχει ηθελημένα διαμορφωθεί λανθασμένα. Έχει δοθεί πρόσβαση κοινόχρηστου φακέλου στο "/" ο οποίος είναι ο κύριος φάκελος (root) που περιλαμβάνει τα αρχεία του συστήματος.

Τα εργαλεία προτείνουν τη περιορισμένη και ελεγχόμενη πρόσβαση των χρηστών.

Για την απαλοιφή της ευπάθειας αυτής θα αφαιρεθεί η πρόσβαση από το φάκελο "/". Για να επιτευχθεί αυτό θα τροποποιηθεί το αρχείο **exports** το οποίο βρίσκεται κάτω από το φάκελο **etc**.

Το αρχείο exports είναι το αρχείο ελέγχου στο οποίο καθορίζονται ποια αρχεία του εξυπηρετητή θα γίνονται διαθέσιμα στο δίκτυο και ποια δικαιώματα θα έχει ο κάθε χρήστης ή ομάδα χρηστών σε αυτά.

Αρχικά θα πρέπει να γίνει η απενεργοποίηση της υπηρεσίας NFS. Από την γραμμή εντολής εκτελείται η εντολή:

$sudo /etc/init.d/nfs-kernel-server stop

Στη συνέχεια θα γίνει η νενομισμένη τροποποίηση στο αρχείο exports. Για την πρόσβαση στο αρχείο εκτελείται η εντολή:

$sudo nano /etc/exports

Εντοπίζεται η εγγραφή "/" και προστίθεται μπροστά από αυτή ο χαρακτήρας # για την απενεργοποίηση της.

Ακολούθως θα πρέπει να εκτελεστεί η εντολή ανάγνωσης των εγγραφών του αρχείου exports. Το περιεχόμενο του αρχείου exports εκτελείται μετά από κάθε εκκίνηση του υπολογιστή. Για την ανάγνωση και εκτέλεση των εντολών του από την γραμμή εντολών εκτελείται η πιο κάτω εντολή:

$sudo exportfs -a

Στην συνέχεια ενεργοποιείται η υπηρεσία NFS με την εκτέλεση της εντολής:

$sudo /etc/init.d/nfs-kernel-server start

Ευπάθεια 7

Θύρα: 80

Υπηρεσία: Apache httpd 2.2.8 Ubuntu DAV/2

Περιγραφή: Ο φάκελος http://"ip-address"/doc ο οποίος περιέχει ευαίσθητες πληροφορίες είναι διαθέσιμος σε όλους.

Τα εργαλεία προτείνουν την ανάκληση της προσβασιμότητας στο συγκεκριμένο φάκελο.

Για να γίνει ανάκληση της προσβασιμότητας θα πρέπει να τροποποιηθεί το αρχείο **default** το οποίο βρίσκεται αποθηκευμένο στο φάκελο **/etc/apache2/sites-available/**.

Ανοίγοντας το αρχείο default εντοπίζονται οι πιο κάτω εγγραφές:

Alias /doc/ "/usr/share/doc/"

<Directory "/usr/share/doc/">

Options Indexes MultiViews FollowSymLinks

AllowOverride None

</Directory>

Προστίθεται μπροστά από τη κάθε εγγραφή ένα # ούτως ώστε οι εγγραφές να απενεργοποιηθούν.

#Alias /doc/ "/usr/share/doc/"

#<Directory "/usr/share/doc/">

 # Options Indexes MultiViews FollowSymLinks

 # AllowOverride None

#</Directory>

Μετά από την αποθήκευση του αρχείου γίνεται επανεκκίνηση της apache υπηρεσίας με την εντολή:

$sudo /etc/init.d/apache2 restart

6.2.3 Επαλήθευση Απαλοιφής Ευπαθειών

Για να επαληθευθεί κατά πόσο οι ενέργειες που έχουν παρθεί για την απαλοιφή των ανευρεθέντων ευπαθειών, έχουν τα επιθυμητά αποτελέσματα, θα επαναληφθεί η ανίχνευση τρωσιμότητας με την χρήση των εργαλείων ανίχνευσης Nmap, OpenVas, Nexpose, Qualys και SAINT, για δεύτερη φορά.

Μετά τις νενομισμένες ενέργειες ανανέωσης της άδειας χρήσης των εργαλείων Nexpose, Qualys και SAINT, χρησιμοποιώντας τα προφίλ ή και εντολές ανίχνευσης που έχουν δημιουργηθεί και χρησιμοποιηθεί για κάθε εργαλείο στο Κεφάλαιο 5, εκτελούνται οι διεργασίας ανίχνευσης διαδοχικά από το περιβάλλον του κάθε εργαλείου.

Μετά το πέρας των διερευνήσεων και την εξέταση των καταστάσεων που έχουν εξαχθεί από το κάθε εργαλείο, επαληθεύεται ότι οι συγκεκριμένες υπό διερεύνηση ευπάθειες δεν εντοπίζονται πλέον. Εντοπίζονται όμως, σε συγκεκριμένες περιπτώσεις, άλλες ευπάθειες οι οποίες προέκυψαν μετά την εφαρμογή των βημάτων απαλοιφής.

Ένα παράδειγμα αποτελεί η Ευπάθεια 1, όπου κατά τα βήματα απαλοιφής είχε "αναβαθμιστεί" η έκδοση του εργαλείου vsftpd 2.3.4, στην τελευταία διαθέσιμη έκδοση που προσφερόταν για το λειτουργικό σύστημα Ubuntu 8.0.4 Hardy. Στην ουσία η προσφερόμενη έκδοση, 2.0.6, αναβάθμισης, ήταν παλαιότερη από την έκδοση που θα αντικαθιστούσε, η οποία όμως δεν είχε την ευπάθεια της κερκόπορτας. Επίσης είχε ενεργοποιηθεί το SSL/TLS για παροχή κρυπτογράφησης της επικοινωνίας. Τα εργαλεία κατά την δεύτερη διερεύνηση δεν είχαν εντοπίσει την ευπάθεια της κερκόπορτας αλλά είχαν εντοπίσει για την υπηρεσία vsftpd και θύρα 21 τα κάτωθι:

Nmap (NMAP Scripts Metasploitable Assesment Report 2)

Το Nmap έχει εντοπίσει την ευπάθεια **"SSL/TLS MITM vulnerability (CCS Injection)"** με ρίσκο **"High"** και περιγραφή:

> "OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability."

Σημείωση: Οι καταστάσεις επανεκτίμησης τρωσιμότητας για το εργαλείο Nmap, βρίσκονται στο CD της παρούσας μεταπτυχιακής διατριβής, στον φάκελο "NMAP" και υποφάκελο "Vulnerability Checks" με τις ονομασίες "NMAP Scripts Metasploitable Assesment Report 2", για τα Nmapscripts σε "html" μορφή και " NMAP VulScan Metasploitable Assesment Report 2", για το VulScan script σε μορφή "xml".

OpenVas (OpenVas Metasploitable Assesment Report 2)

Το OpenVas (σελ. 136-137) έχει εντοπίσει τις ευπάθειες:

1. "**OpenSSL CCS Man in the Middle Security Bypass Vulnerability"** με ρίσκο **"Medium"** και περιγραφή:

   "OpenSSL is prone to security-bypass vulnerability. Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks. Affected OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and

1.0.1 before 1.0.1h. OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability."

2. **"SSL/TLS: Certificate Signed Using A Weak Signature Algorithm"** με ρίσκο **"Medium"** και περιγραφή:

   "The remote service is using a SSL/TLS certificate chain that has been signed using a crypto-graphically weak hashing algorithm. Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates."

Σημείωση: Η εξαχθείσα κατάσταση επανεκτίμησης τρωσιμότητας για το εργαλείο OpenVas είναι διαθέσιμη στο CD της παρούσας μεταπτυχιακής διατριβής, στον φάκελο "OpenVas" με την ονομασία "OpenVas Metasploitable Assesment Report 2"σε "pdf" μορφή.

Nexpose (Nexpose Metasploitable Assesment Report 2)

Το Nexpose έχει εντοπίσει τις ευπάθειες:

1. Σελ. 295, **"Self-signed TLS/SSL certificate (ssl-self-signed-certificate)"** με ρίσκο **"Severe"** και περιγραφή:

   "The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL manin-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections."

2. Σελ. 298, **"TLS Server Supports TLS version 1.0 (tlsv1_0-enabled)"** με ρίσκο **"Severe"** και περιγραφή:

"The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2."

Σημείωση: Η εξαχθείσα κατάσταση επανεκτίμησης τρωσιμότητας για το εργαλείο Nexpose είναι διαθέσιμη στο CD της παρούσας μεταπτυχιακής διατριβής, στον φάκελο "Nexpose" με την ονομασία " Nexpose Metasploitable Assesment Report 2"σε "pdf" μορφή.

Qualys (Qualys Metasploitable Assesment Report 2)

Το Qualys έχει εντοπίσει τις ευπάθειες:

1. Σελ. 205, **"SSL/TLS Compression Algorithm Information Leakage Vulnerability"** με ρίσκο **"Vulnerabilities, Severity 3"** και περιγραφή:

   "SSL/TLS protocols support and optional compression algorithm. When used compression can ease data transfer significantly. An information leakage was discovered related to compression algorithm use in SSL/TLS protocols. The attacker needs to have ability to submit any plain text to compression and encryption process and observe the output to be able to exploit this vulnerability.

   The attack works like this:

   the attacker who has control over a web browser that is communicating to a web site that uses SSL/TLS can send a HTTP POST request that looks

   like this:

   POST /login.php HTTP/1.1

   Cookie: XYZ

   Cookie:

   The first Cookie is in the HTTP header and the second one is in the body of the request. If compression algorithm is used it will replace the second occurrence of

the string 'Cookie: ' by a reference to the first one and thus decrease the length of the string to be encrypted and eventually the output length of SSL packet. This can be observed on the network.The attacker can then prepare another request that contains a guess as to what the first character of the cookie is. That HTTP request looks like this:

POST /login.php HTTP/1.1

Cookie: XYZ

Cookie: A

If the guess was correct then the length of the output of compression + encryption will decrease more than if the guess was incorrect. Using this approach the attacker can verify their guesses and completely recover the value of the cookie.

Typically cookies are used in secure HTTP sessions as authentication tokens and as session identifications. Compromise of the cookie can lead to HTTP session hijacking and impersonation."

2. Σελ. 206, "**SSL/TLS Server supports TLSv1.0"** με ρίσκο **"Vulnerabilities, Severity 3"** και περιγραφή:

" TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade. This QID will be marked as a Fail for PCI as of November 1st, 2016 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June

30th, 2018. Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 (https://community.qualys.com/message/34120).

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications. For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages. A POODLE-type https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade."

Σημείωση: Η εξαχθείσα κατάσταση επανεκτίμησης τρωσιμότητας για το εργαλείο Qualys είναι διαθέσιμη στο CD της παρούσας μεταπτυχιακής διατριβής, στον φάκελο "Qualys" με την ονομασία " Qualys Metasploitable Assesment Report 2"σε "pdf" μορφή.

SAINT (SAINT Metasploitable Assesment Report 2)

Το SAINT έχει εντοπίσει τις ευπάθειες:

1. Σελ. 991, **"Server is susceptible to BEAST attack"** με ρίσκο **"Potential"** και περιγραφή:

   "The Browser Exploit against SSL/TLS (BEAST) may allow an attacker to perform a man-in-the-middle attack to obtain plain-text HTTP headers by conducting a blockwise chosen-boundary attack (BCBA) against an HTTPS session. This attack is an extension of two previously disclosed attacks against SSL.

   The first of these attacks was detailed by Gregory Bard in May 2004 (The Vulnerability of SSL to Chosen Plaintext Attack). This research showed that cipher block chaining mode used by SSL is vulnerable to decryption in cases where the attacker can control part of the plaintext. This attack proved to be difficult to implement against HTTPS sessions due to the attackers' inability to control the contents. This attack method was extended to support TLS 1.0 and improved in April 2006 (A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL). In September 2011, Juliano Rizzo and Thai Duong presented a modern iteration of this attack that utilized Java or HTML5 WebSockets as an

entry-point for attackers. Using this method, attackers could host a malicious website that, when visited by victims, uses Java or WebSockets to establish a connection to any secured 3rd party website of their choice. If the user has an active session to the targeted 3rd party site, any cookies he or she has saved will also be sent. Since the attacker is initiating this request, he can control the length of the requested resource, allowing him to position the cookie on a block boundary.

The attacker also knows part of the cleartext. If this can be done in a man-in-the-middle scenario, the attacker will be able to intercept this encrypted request and decrypt it off-line to obtain the cookie. If the cookie contains an authentication token, this may result in account theft.

TLS 1.1 and later have been improved to use an explicit initialization vector strategy, rendering them immune to this type of attack."

2. Σελ. 800, **"SSL certificate is signed with weak hash function: SHA1"** με ρίσκο **"Potential"** και περιγραφή:

   "The SSL/TLS certificate is signed with a weak hash function. An attacker may be able to forge a SSL/TLS certificate that would appear to be valid for the website. This may allow an attacker to perform a man-in-the-middle attack against the SSL-secured website. SAINT highly recommends that certificates signed with SHA-1 be replaced with SHA-2 signed certificates."

3. Σελ. 806-807, **"SSL/TLS server supports short block sizes (SWEET32 attack)"** με ρίσκο **"Potential"** και περιγραφή:

   "A remote attacker with the ability to sniff network traffic could decrypt long-lived TLS or SSL sessions.

   Block ciphers with small block sizes are susceptible to a class of attacks known as birthday attacks. These attacks take advantage of multiple blocks which return identical ciphertext, known as collisions. The probability of collisions occurring becomes significant after a large number of blocks have been encrypted using the

same key. The SWEET32 attack is a specific birthday attack which reveals the XOR (exclusive-OR) between a fixed

secret and known plaintext, thus allowing the secret to be determined. This attack can be launched in a browser session by javascript code which makes repeated requests containing an authentication token and predictable headers. Successful exploitation requires about 785 GB of data to be captured, and the attacker must be able to inject javascript into a web session and to sniff data from the network. ”

Σημείωση: Η εξαχθείσα κατάσταση επανεκτίμησης τρωσιμότητας για το εργαλείο SAINT είναι διαθέσιμη στο CD της παρούσας μεταπτυχιακής διατριβής, στον φάκελο “SAINT” με την ονομασία “ SAINT Metasploitable Assesment Report 2”σε “pdf” μορφή.

Με βάση τα ευρήματα των εργαλείων διαφαίνεται ότι η έκδοση της υπηρεσία **SSL/TLS** η οποία έχει ενεργοποιηθεί για χρήση από την υπηρεσία vsftpd, για την παροχή κρυπτογράφησης της επικοινωνία,, περιέχει η ίδια ευπάθειες ισάξιου ρίσκου με την ευπάθεια που έχει απαλειφθεί. Για τον λόγο αυτό κρίνεται επίσης αναγκαία, η άμεση απαλοιφή της ευπάθειας αυτής.

6.3 Αξιολόγηση Εργαλείων Εκτίμησης Τρωσιμότητας

Στο σημείο αυτό θα γίνει μια αξιολόγηση των εργαλείων εκτίμησης τρωσιμότητας τα οποία έχουν μελετηθεί και χρησιμοποιηθεί με βάση τα δεδομένα της παρούσας μεταπτυχιακής διατριβής και είναι αποτέλεσμα προσωπικών παρατηρήσεων του μελετητή. Στην αξιολόγηση δίνεται έμφαση στην αποδοτικότητα και ευκολία χρήσης τους κατά την διαδικασία εγκατάστασης, παραμετροποίησης, διεξαγωγής εκτίμησης τρωσιμότητας και εξαγωγής αποτελεσμάτων. Επίσης παρατίθεται μια λίστα με τα χαρακτηριστικά που πρέπει να διαθέτει ένα ιδανικό εργαλείο εκτίμησης τρωσιμότητας.

6.3.1 Nmap/Zenmap

Εγκατάσταση: Η διαδικασία εγκατάστασης του Nmap/Zenmap στη Windows 7 μηχανή ήταν αρκετά απλή και γρήγορη. Το μόνο που απαιτείτε είναι το κατέβασμα του κατάλληλου αρχείου εγκατάστασης, σύμφωνα με το λειτουργικό σύστημα που θα εγκατασταθεί, από την ιστοσελίδα του εργαλείου και η εκτέλεση αυτού.

Αποδοτικότητα και Ακρίβεια αποτελεσμάτων: Το Nmap/Zenmap κατά την διαδικασία ανίχνευσης ευπαθειών του Metasploitable 2 έχει καταφέρει να εντοπίσει 5 από τις 7 διερευνώμενες ευπάθειες. Οι ευπάθειες 1 και 5 έχουν εντοπιστεί με την χρήση του script Vulscan, ενώ οι ευπάθειες 2, 4 και 7 έχουν εντοπιστεί με τα NSE scripts.

Ο χρόνος που χρειάστηκε το Nmap με την χρήση του Zenmap και του script Vulscan για να ολοκληρώσει την εκτίμηση τρωσιμότητας του Metasploitable 2 ήταν περίπου 5 λεπτά. Ενώ ο χρόνος που χρειάστηκε το Nmap με την χρήση των NSE των κατηγοριών discovery, vuln, auth, default και malware και το οποίο είχε τρέξει από το Kali Linux , ήταν περίπου 10 λεπτά.

Το Nmap περιέγραψε σωστά στην ανεύρεση του και τις 5 ευπάθειες. Χρειάστηκε ωστόσο χρόνος για επιπλέον ψάξιμο (manual) για την ανεύρεση των ευπαθειών, οι οποίες είχαν εντοπιστεί με την χρήση του Vulscan, από τις εγγραφές των offline βάσεων ευπαθειών που παρουσίασε το script. Η παρουσίαση της κατάστασης ευπαθειών με την χρήση των NSE scripts ήταν σε γενικές γραμμές καλή αφού εύκολα μπορούσε να διακριθεί η θύρα, η υπηρεσία αλλά και η ανευρεθέν ευπάθεια.

Το Nmap δεν προσφέρει λύσεις για καμία από τις ευπάθειες που εντοπίζει, με αποτέλεσμα να χρειάζεται επιπλέον χρόνος για την ανεύρεση λύσεων απαλοιφής των υπό εξέταση ευπαθειών από τρίτες πηγές.

Ευκολία χρήσης: Το Nmap δεν μπορεί να χαρακτηριστεί απλό στην χρήση για όλα τα επίπεδα των διαχειριστών μιας και διαθέτει πληθώρα εντολών, που πιθανός να αποπροσανατολίσουν. Επιπρόσθετα κάποιες από τις διαθέσιμές εντολές του πιθανόν να οδηγήσουν το υπό διερεύνηση σύστημα σε κατάρρευση. Εντούτοις υπάρχουν αρκετά καλά και ενημερωμένα εγχειρίδια τα οποία μπορούν να καθοδηγήσουν τον εν δύναμη διαχειριστή να διεξάγει με ασφάλεια τους ελέγχους που επιθυμεί.

Το Nmap, προτείνεται για χρήση ως ένα συμπληρωματικό εργαλείο κατά την διαδικασία εκτίμησης τρωσιμότητας.

6.3.2 OpenVas

Εγκατάσταση: Το OpenVas αποτελεί μέρος του Kali Linux λειτουργικού συστήματος, από όπου έχει χρησιμοποιηθεί για την παρούσα μεταπτυχιακή διατριβή. Ωστόσο θα πρέπει να διεξαχθεί

διαδικασία επικαιροποίησης του συστήματος. Η διαδικασία επικαιροποίησης είναι σχετικά απλή, όπου γίνεται με την χρήση αριθμού εντολών σε ένα παράθυρο shell. Ο χρόνος που απαιτήθηκε για την επικαιροποίηση ήταν περίπου 60 λεπτά. Μετά το πέρας της επικαιροποίσης, με την χρήση και πάλι αριθμού εντολών σε ένα παράθυρο shell θα πραγματοποιηθεί η εκκίνηση των υπηρεσιών του εργαλείου. Η διαδικασία αυτή είναι καταγεγραμμένη και αρκετά επεξηγηματική στην ιστοσελίδα του Kali.

Αποδοτικότητα και Ακρίβεια αποτελεσμάτων: Το OpenVas κατά την διαδικασία ανίχνευσης ευπαθειών του Metasploitable 2 έχει καταφέρει να εντοπίσει 3 από τις 7 διερευνώμενες ευπάθειες, συγκεκριμένα έχουν εντοπιστεί οι ευπάθειες 1, 3 και 4. Ο χρόνος που χρειάστηκε το OpenVas για την εκτίμηση τρωσιμότητας ήταν περίπου 60 λεπτά.

Το OpenVas περιέγραψε σωστά στην ανεύρεση του και τις 3 ευπάθειες και έχει προτείνει λύσεις απαλοιφής για τις ευπάθειες 1 και 4, ενώ για την ευπάθεια 3 δεν έχει προτείνει κάποια λύση.

Η Greenbone διατηρεί δημόσια βάση ευπαθειών NVTs (Network Vulnerability Tests) για το OpenVas η οποία ενημερώνεται σε καθημερινή βάση και το εργαλείο μπορεί να προγραμματιστεί να ενημερώνεται αυτόματα ή να εκτελείται χειροκίνητη ενημέρωσή του από τον διαχειριστή.

Επιπρόσθετα τα αποτελέσματα του OpenVas μπορούν να χρησιμοποιηθούν από το Metasploit, ενός από τα κορυφαία εργαλεία διείσδυσης , με την χρήση του κατάλληλου OpenVas module, για την διεξαγωγή εργασιών διείσδυσης για επιβεβαίωση των ανευρεθέν ευπαθειών.

Ευκολία χρήσης: Το OpenVas με την χρήση του GUI GSA (Greenbone Security Assistant) γίνεται αρκετά φιλικό προς το χρήστη. Η καταχώρηση των στοιχείων διερεύνησης όπως των θυρών, των στοιχεία αυθεντικοποίησης, του προφίλ διερεύνησης και του υπολογιστή-στόχου (Metasploitable 2) πραγματοποιείτε με μόνο μερικά κλικ. Επίσης η διαδικασία πραγματοποίησης εργασίας διερεύνησης είναι αρκετά απλή και μπορεί προγραμματιστεί για να διεξάγεται σε τακτά χρονικά διαστήματα.

Η ευχέρεια επισκόπησης των μέχρι στιγμής ανευρεθέντων ευπαθειών, καθώς η διεργασία διερεύνησης είναι σε εξέλιξη, αποτελεί επίσης ένα σημαντικό πλεονέκτημα του OpenVas, αφού ο διαχειριστής δεν χρειάζεται να περιμένει την διαδικασία να τελειώσει και στη συνέχεια να δει τις ανευρεθέν ευπάθειες.

Η υποστήριξη ενός μεγάλου αριθμού τύπου αρχείων (PDF, HTML, XML, κτλ) για την εξαγωγή της κατάστασης ευπαθειών αποτελεί επίσης σημαντικό πλεονέκτημα του OpenVas. Η κατάσταση ευπαθειών η οποία εξάγεται από τον OpenVas παρουσιάζει τις ευπάθειες σύμφωνα με το βαθμό αξιολόγησης τους, αρχίζοντας από αυτές με το υψηλότερο βαθμό σοβαρότητας. Για κάθε ευπάθεια παρουσιάζεται μια μικρή περίληψη, όπου γίνεται επεξήγηση της ευπάθειας αυτής, τις πιθανές επιπτώσεις που μπορεί να έχει η εκμετάλλευσή της, καθώς επίσης στις πλείστες των περιπτώσεων, προτείνεται και λύση απαλοιφής της.

6.3.3 Nexpose

Εγκατάσταση: Ο διαχειριστής του Nexpose αντιλαμβάνεται αμέσως την υποστήριξη και την προσοχή που έδωσε ο κατασκευαστής του εργαλείου αυτού, στον τελικό χρήστη. Από την διαδικασία εγγραφής στην ιστοσελίδα του εργαλείου για την παροχή άδειας χρήσης, μέχρι την επιτυχή ολοκλήρωση τις εγκατάστασής του, παρέχεται λεπτομερής πληροφόρηση σε όλα τα επίπεδα χωρίς να αφήνει οποιαδήποτε περιθώρια δημιουργίας απορίων.

Η άδεια χρήσης του εργαλείου παρέχεται αμέσως, με μόνη προϋπόθεση ότι δεν θα γίνει χρήση, κατά την διαδικασία εγγραφής, email λογαριασμού από δωρεάν παρόχους (gmail, yahoo κτλ).

Ο χρόνος που απαιτήθηκε για την επιτυχή εγκατάσταση του εργαλείου ήταν περίπου 10 λεπτά. Η διαδικασία εκκίνησης του εργαλείου την πρώτη φορά διήρκησε περίπου 15 λεπτά.

Αποδοτικότητα και Ακρίβεια αποτελεσμάτων: Το Nexpose κατά την διαδικασία ανίχνευσης ευπαθειών του Metasploitable 2 έχει καταφέρει να εντοπίσει 5 από τις 7 διερευνώμενες ευπάθειες, συγκεκριμένα έχουν εντοπιστεί οι ευπάθειες 1, 3, 5, 6 και 7. Ο χρόνος που χρειάστηκε το Nexpose για την εκτίμηση τρωσιμότητας ήταν περίπου 30 λεπτά.

Το Nexpose περιέγραψε σωστά στην ανεύρεση του τις ευπάθειες 3, 5, 6 και 7 έχει προτείνει λύσεις απαλοιφής για τις ευπάθειες αυτές, ενώ όσο αφορά την ευπάθεια 1, παρόλο που δεν έχει εντοπίσει την ευπάθεια της κερκόπορτας, εντούτοις εντοπίζει ότι η υπηρεσία ftp δεν χρησιμοποιεί κρυπτογραφημένη μέθοδο αυθεντικοποίησης και προτείνει την κρυπτογράφηση της επικοινωνίας. Γενικά τα βήματα που προτείνονται από το Nexpose βοήθησαν ουσιαστικά στην διαδικασία απαλοιφής των εν λόγω ευπαθειών.

Το Nexpose ενημερώνεται αυτόματα στην περίπτωση που υπάρχει σύνδεση με το Διαδίκτυο ή με την χρήση offline αρχείου ενημέρωσης, το οποίο θα πρέπει να "κατέβει" από άλλο υπολογιστή ο οποίος να διαθέτει σύνδεση στο Διαδίκτυο και να εκτελεστεί στον υπολογιστή που φιλοξενεί το Nexpose.

Τα αποτελέσματα της διερεύνησης ευπαθειών μπορούν να αποθηκευθούν σε XML μορφή κατάλληλη για άμεση χρήση με το Metasploit, για την διεξαγωγή εργασιών διείσδυσης και επιβεβαίωσης των ανευρεθέν ευπαθειών.

Ευκολία χρήσης: Το Nexpose διαθέτει ένα καλοσχεδιασμένο περιβάλλον διαχείρισης. Η διαδικασία παραμετροποίησης ήταν αρκετή εύκολη και είχε γίνει σε σχετικά μικρό χρονικό διάστημα. Σε διάστημα 5-10 λεπτών η διαδικασία ανεύρεσης ευπαθειών είχε τεθεί σε λειτουργία. Τα αποτελέσματα της έρευνας ενημερώνονταν σε πραγματικό χρόνο δίνοντας την ευχέρεια επισκόπησης των μέχρι στιγμής ανευρεθέντων ευπαθειών, καθώς η διεργασία διερεύνησης ήταν σε εξέλιξη.

Το Nexpose κατηγοριοποιεί τις ευπάθειες όχι μόνο με την βαθμίδα αξιολόγησης CVSS αλλά και με βάση το επίπεδο της γνώσης που πρέπει να διαθέτει ο επιτιθέμενος για τις εκμεταλλευτεί. Αυτό αποτελεί ένα πολύτιμο εργαλείο για την σωστή κατηγοριοποίηση της κρισιμότητας των ευπαθειών.

Το Nexpose έχει διαθέσιμα αρκετά είδη έτοιμων καταστάσεων για τις ανάγκες διαφόρων ελέγχων συμμόρφωσης. Επιπρόσθετα ο διαχειριστής μπορεί να δημιουργήσει δικές του καταστάσεις, είτε ξεκινώντας από το μηδέν, είτε τροποποιώντας κάποια από τις υφιστάμενες καταστάσεις. Οι καταστάσεις μπορούν να εξαχθούν σε διάφορους τύπους αρχείων που να ικανοποιούν τις ανάγκες είτε των στελεχών της διεύθυνσης, είτε των διαχειριστών συστημάτων.

6.3.4 Qualys Vulnerability Management

Εγκατάσταση: Το Qualys VM αποτελεί υπηρεσίας νέφους και για αυτό τον λόγο δεν χρειάστηκε οποιαδήποτε εγκατάσταση του εργαλείου. Χρειάστηκε όμως η εγκατάσταση του QualysGuard Virtual Scanner Appliance για χρήση με το Oracle VM VirtualBox Manager, με το οποίο επικοινωνούσε το Qualys VM για την διεξαγωγή εκτίμησης τρωσιμότητας του Metasploitable 2. Αρχικά είχε γίνει εγγραφή στην ιστοσελίδα του εργαλείου για την απόκτηση άδειας χρήσης και στην συνέχεια υπήρξε επικοινωνία με εκπρόσωπο της εταιρείας για να εξηγηθεί ο λόγος και ο

σκοπός που αιτείτε αυτή η άδεια. Για την απόκτηση της άδειας χρειάστηκαν 2 μέρες. Επίσης χρειάστηκε 1 μέρα επιπλέον για να παραχωρηθεί άδεια χρήσης ενός virtual scanner appliance. Ακολούθως στάλθηκαν οι πληροφορίες πρόσβασης στο εργαλείο. Λόγω του ότι το εργαλείο αποτελεί υπηρεσία νέφους το μόνο που χρειάζεται για την παραμετροποίηση του είναι ένας υπολογιστής με πλοηγό Διαδικτύου και πρόσβαση στο Διαδίκτυο.

Μετά την πλοήγηση στην ιστοσελίδα του εργαλείου και την αυθεντικοποίηση το επόμενο βήμα ήταν το κατέβασμα του virtual scanner appliance για το VirtualBox. Η εγκατάσταση του appliance ήταν πολύ απλή και δεν χρειάστηκαν περισσότερα από 15 λεπτά για να ολοκληρωθεί η διαδικασία κατεβάσματος και εγκατάστασης του. Μετά την παραμετροποίηση των στοιχείων του δικτύου, το appliance έγινε μέρος του περιβάλλοντος αξιολόγησης. Η διαδικασία επικοινωνίας και η σύνδεσης του appliance με το Qualys VM δεν διήρκησε περισσότερο από 2 λεπτά.

Αποδοτικότητα και Ακρίβεια αποτελεσμάτων: Το Qualys κατά την διαδικασία ανίχνευσης ευπαθειών του Metasploitable 2 έχει καταφέρει να εντοπίσει 4 από τις 7 διερευνώμενες ευπάθειες, συγκεκριμένα έχουν εντοπιστεί οι ευπάθειες 1, 3, 6 και 7. Ο χρόνος που χρειάστηκε το Qualys για την εκτίμηση τρωσιμότητας ήταν περίπου 20 λεπτά.

Το Qualys περιέγραψε σωστά στην ανεύρεση του τις ευπάθειες 3,6 και 7 και έχει προτείνει λύσεις απαλοιφής για τις ευπάθειες αυτές, ενώ όσο αφορά την ευπάθεια 1, παρόλο που δεν έχει εντοπίσει την ευπάθεια της κερκόπορτας, εντούτοις εντοπίζει ότι η υπηρεσία ftp έχει ενεργοποιημένο το "anonymous login" και προτείνει την απενεργοποίηση του.

Το πλεονέκτημα του Qualys είναι ότι διαχειρίζεται πλήρως από την ομάδα της Qualys και ως λύση νέφους είναι πάντα ενημερωμένη. Προσφέρει συνεχή έλεγχο για εντοπισμό ευπαθειών, τις οποίες βάζει σε προτεραιοποίηση και έχει την δυνατότητα αποστολής ειδοποιήσεων στην ομάδας ασφαλείας, για να προβεί σε άμεσες ενέργειες.

Το εργαλείο παρέχει δυνατότητες διερεύνησης συμμόρφωσης PCI, καθώς επίσης παρέχεται η δυνατότητα δημιουργίας κατά παραγγελία πολιτικών διερεύνησης με βάση της ανάγκες ενός οργανισμού.

Ευκολία χρήσης: Με την χρήση των πηγών πληροφόρησης που στάλθηκαν κατά την διαδικασία απόκτησης άδειας χρήσης του εργαλείου και του οδηγούς οι οποίοι ήταν διαθέσιμοι

στην ιστοσελίδα του περιβάλλοντος του εργαλείου, έκαναν την διαδικασία παραμετροποίησης και χρήσης του εργαλείου εξαιρετικά απλή και εύκολη. Η διαδικασία αυτή δεν είχε διάρκεια περισσότερο από 20 λεπτά.

Το περιβάλλον διαχείρισης του Qualys, όχι ότι δεν ήταν εύχρηστο, αλλά λόγο του τρόπου μορφοποίησής του με τα πολλά αλληλεπιδρώντα μέλη που χρησιμοποιεί η πλατφόρμα, δεν διευκολύνει και τόσο τους αρχαρίους διαχειριστές να το χρησιμοποιήσουν άμεσα.

Οι καταστάσεις ευπαθειών μπορούν να εξαχθούν σε διάφορους τύπους αρχείων όπως PDF, HTML,MHT, XML και CSV. Είναι αρκετά ευανάγνωστες, παρουσιάζουν τις ευπάθειες σύμφωνα με το βαθμό αξιολόγησης τους, αρχίζοντας από αυτές με το υψηλότερο βαθμό σοβαρότητας. Για κάθε ευπάθεια παρουσιάζεται μια μικρή περίληψη, όπου γίνεται επεξήγηση της ευπάθειας αυτής, τις πιθανές επιπτώσεις που μπορεί να έχει η εκμετάλλευσή της, καθώς επίσης προτείνεται και λύση απαλοιφής της.

Η χρήση του εργαλείου αυτού αποτελεί μια εξαιρετική επιλογή για μικρούς οργανισμούς με περιορισμένο διαθέσιμο κεφάλαιο.

6.3.5 SAINT Vulnerability Assessment

Εγκατάσταση: Αρχικά είχε γίνει εγγραφή στην ιστοσελίδα του εργαλείου για την απόκτηση άδειας χρήσης και στην συνέχεια, μετά από πάροδο 1 μέρας, υπήρξε επικοινωνία με εκπρόσωπο της εταιρείας για να εξηγηθεί ο λόγος και ο σκοπός που αιτείτε αυτή η άδεια, ακριβώς όπως και στην περίπτωση του Qualys. Το εργαλείο SAINT Vulnerability Assessment προσφέρεται σαν υπηρεσία SaaS με την ονομασία “SAINT Cloud” ή εικονική μηχανή με την ονομασία “SAINT 8”, στην παρούσα μεταπτυχιακή διατριβή έχει χρησιμοποιηθεί η εικονική μηχανή.

Στην συνέχεια, μετά από πάροδο 1 μέρας από την επικοινωνία με τον εκπρόσωπο της εταιρείας και την αποστολή των πληροφοριών πρόσβασης στο εργαλείο καθώς και οδηγιών λήψης της εικονικής μηχανής του εργαλείου, πραγματοποιείται πλοήγηση στην ιστοσελίδα από όπου θα γίνει η λήψη της μηχανής για χρήση στο VirtualBox.

Η όλη διαδικασία λήψεις και εγκατάστασης της μηχανής SAINT 8 στο VirtualBox διήρκησε περίπου 15 λεπτά. Στην συνέχεια πραγματοποιήθηκε πρόσβαση το Linux περιβάλλον και στην συνέχεια έγινε εκκίνηση του εργαλείου. Το εργαλείο αρχικά διενεργεί διερεύνηση για τις

τελευταίες ενημερώσεις και προχωρά στο "κατέβασμά" και στην εγκατάσταση αυτών μέσο Διαδικτύου, η όλη διαδικασία διήρκησε περίπου 5 λεπτά. Στην συνέχεια ανοίγει αυτόματα ο πλοηγός Διαδικτύου όπου πραγματοποιείτε πρόσβαση στο εργαλείο SAINT 8. Το επόμενο βήμα είναι η καταχώριση του κλειδιού άδειας χρήσης.

Η όλη διαδικασία κατεβάσματος, εγκατάστασης και διάθεσης του εργαλείου προς χρήση δεν διήρκησε περισσότερο από 30 λεπτά.

Αποδοτικότητα και Ακρίβεια αποτελεσμάτων: Το SAINT κατά την διαδικασία ανίχνευσης ευπαθειών του Metasploitable 2 έχει καταφέρει να εντοπίσει 3 από τις 7 διερευνώμενες ευπάθειες, συγκεκριμένα έχουν εντοπιστεί οι ευπάθειες 1, 3 και 6. Ο χρόνος που χρειάστηκε το SAINT για την εκτίμηση τρωσιμότητας ήταν περίπου 3 ώρες.

Το SAINT περιέγραψε σωστά στην ανεύρεση του και τις 3 ευπάθειες και έχει προτείνει λύσεις απαλοιφής για τις ευπάθειες αυτές. Τα βήματα που προτείνονται από το SAINT για την απαλοιφή των εν λόγω ευπαθειών χαρακτηρίζονται από μεγάλη λεπτομέρεια και έχουν χρησιμοποιηθεί ουσιαστικά κατά την διαδικασία απαλοιφής. Σε σχέση με το υπόλοιπα εργαλεία το SAINT παρείχε τις περισσότερες πληροφορίες για την επιτυχή απαλοιφή των ευπαθειών που είχε εντοπίσει.

Η βάση δεδομένων του SAINT ενημερώνεται σε καθημερινή βάση με καινούργια αρχεία ανεύρεσης και εκμετάλλευσης ευπαθειών. Επίσης παρέχεται η δυνατότητα ενσωμάτωσης κατά παραγγελία ελέγχων ασφαλείας από τους διαχειριστές.

Το SAINT έχει την δυνατότητα ελέγχων συμμόρφωσης στους τρέχων κυβερνητικούς και επιχειρηματικούς κανονισμούς, όπως αυτοί ορίζονται από τα πρότυπα PCI DSS, NERC, FISMA, SOX, GLBA και HIPPA. Επίσης πραγματοποιεί ελέγχους με βάση τις πολιτικές που καθορίζονται από το FDCC, USGCB και DISA.

Επιπρόσθετα με την ενσωμάτωση του SAINTexploit εργαλείου, δίνετε η δυνατότητα δοκιμής εκμετάλλευσης των ευπαθειών οι οποίες έχουν εντοπιστεί, επιβεβαιώνοντας έτσι την ευπάθεια και αποκαλύπτοντας το ρίσκο.

Ευκολία χρήσης: Τα εγχειρίδια χρήσης στου SAINT ήταν καλογραμμένα και με σαφήνεια. Περιελάμβαναν εικόνες και λεπτομερή περιγραφή για όλα τα βήματα διαμόρφωσης του

εργαλείου κάτι που καθιστούσε την διαδικασία παραμετροποίησης του SAINT αρκετά εύκολη ακόμη και για τον ποιο αρχάριο διαχειριστή.

Το SAINT είναι εύκολο και απλό στην χρήση του. Μετά την ολοκλήρωση της αρχικής ρύθμισης του εργαλείου, σειρά είχε η παραμετροποίηση της διαδικασίας ανίχνευσης τρωσιμότητας. Η διαδικασία αυτή ήταν επίσης αρκετά απλή, αφού ελεγχόταν βήμα προς βήμα από ένα αυτοματοποιημένο οδηγό διαμόρφωσης, τύπου point and click.

Το περιβάλλον του εργαλείου ήταν γρήγορο και ανταποκρινόταν αρκετά καλά. Το SAINT επιτυγχάνει μια καλή ισορροπία μεταξύ της πληρότητας και της απλότητας γεγονός που καθιστά και τις εκθέσεις που παράγει χρήσιμες και πολύ ενημερωτικές. Οι αναφορές των ευπαθειών ήταν επίσης οπτικά καλύτερες από τα υπόλοιπα εργαλεία, αφού περιελάμβαναν αρκετά γραφήματα, διαγράμματα και άλλα οπτικά βοηθήματα. Επιπρόσθετα υπήρχε πληθώρα επιλογών για την διαμόρφωση της αναφοράς σύμφωνα με τον σκοπό τον οποίο θα εξυπηρετούσε. Ο βαθμός παραμετροποίησης των αναφορών που διαθέτει το SAINT, δεν έχει επίσης παρατηρηθεί, σε κανένα από τα υπόλοιπα υπό εξέταση εργαλεία. Οι καταστάσεις ευπαθειών μπορούν να εξαχθούν σε διάφορους τύπους αρχείων όπως PDF, HTML, XML κτλ.

6.3.6 Χαρακτηριστικά ιδανικού εργαλείου εκτίμησης τρωσιμότητας

Για να μπορέσει να επιλέξει ένας οργανισμός ανάμεσα στην πληθώρα των εργαλείων εκτίμησης τρωσιμότητας ποιο είναι το κατάλληλο για το δικό του περιβάλλον, πρέπει πρώτα να αναλογιστεί τι δυνατότητες θα πρέπει να έχει το ιδανικό εργαλείο στον τομέα αυτό. Δυνατότητες όπως η διαχείριση μηχανογραφικών περιουσιακών στοιχείων, αξιολόγηση και ιεράρχηση ευπαθειών, διαχείριση ενημερώσεων κώδικα, αποκατάσταση , δημιουργία καταστάσεων και παρακολούθησης, ακρίβεια, αρίστη υποστηρικτική ομάδα, κτλ. Αυτές θα πρέπει να είναι κάποιες από τις κύριες διερευνήσεις που θα πρέπει να κάνει ένας οργανισμός πριν καταλήξει στην χρήση ενός συστήματος εκτίμησης τρωσιμότητας.

Συγκεκριμένα:

- **Διαχείριση μηχανογραφικών περιουσιακών στοιχείων.** Διερευνάται κατά πόσο το σύστημα διαθέτει βάση δεδομένων για διαχείριση των ανευρεθέν περιουσιακών στοιχείων. Και στην περίπτωση που διαθέτει εάν μπορεί να γίνει προσθήκη επιπρόσθετων πληροφοριών για τα περιουσιακά στοιχεία. Στην περίπτωση που δεν

διατίθεται η συγκεκριμένη δυνατότητα διερευνάται κατά πόσο το σύστημα μπορεί να συνεργαστεί με άλλα συστήματα διαχείρισης περιουσιακών στοιχείων.

- **Αξιολόγηση και Ιεράρχηση ευπαθειών.** Διερευνάται κατά πόσο οι ευπάθειες οι οποίες ανιχνεύονται κατά την σάρωση αξιολογούνται και προτεραιοποιούνται με βάση την επικινδυνότητά τους.

- **Διαχείριση ενημερώσεων κώδικα.** Διερευνάται κατά πόσο το σύστημα διαθέτει ενσωματωμένο εργαλείο διαχείρισης ενημερώσεων κώδικα ή εάν μπορεί να συνεργαστεί με ένα προϋπάρχον εργαλείο διαχείρισης κώδικα. Εάν διαθέτει αυτό του τύπου το εργαλείο, διερευνάται κατά πόσο διαθέτει την δυνατότητα σωστής διαχείρισης των αποθετηρίων, τα οποία βρίσκονται σε στρατηγικά σημεία του οργανισμού και κατά πόσο μπορεί να εντοπίσει μη σωστά εγκατεστημένες ενημερώσεις και να προχωρήσει στην επανεγκατάσταση τους ή όχι.

- **Αποκατάσταση.** Διερευνάται κατά πόσο το σύστημα διαθέτει την δυνατότητα εφαρμογής τροποποιήσεων σε μη σωστά διαμορφωμένες υπηρεσίες είτε του λειτουργικού συστήματος, είτε λογισμικού, όπως είναι η απενεργοποίηση λογαριασμών χρήστη ο οποίος δεν διαθέτει κωδικό πρόσβασης ή η απενεργοποίηση και αφαίρεση αχρείαστων υπηρεσιών.

- **Δημιουργία καταστάσεων και παρακολούθησης.** Διερευνάται κατά πόσο το εργαλείο μπορεί να δημιουργήσει καταστάσεις οι οποίες να παρέχουν αρκετές λεπτομέρειες και να επιδέχονται διαμόρφωσης ανάλογα με την ομάδα (διευθυντική, διαχείρισης συστημάτων, αξιολόγησης κτλ) στην οποία απευθύνονται. Επίσης κατά πόσο παρέχεται η δυνατότητα δημιουργίας καταστάσεων για την επισκόπηση ευόδωσης ή με των μέτρων που έχουν παρθεί για την απαλοιφή των ευπαθειών.

- **Ακρίβεια.** Διερευνάται κατά πόσο το εργαλείο παρέχει ακριβή αποτελέσματα χωρίς False Positives. Τα ακριβή αποτελέσματα ενισχύουν την αποδοτικότητα των ομάδων ενός μηχανογραφικού τμήματος, προστατεύουν τον οργανισμό με το κλείσιμο ή την επιτήρηση των τρωτών του σημείων και επικυρώνεται ότι οι αρμόδιες ομάδες διαχείρισης των ευπαθειών κατάφεραν με επιτυχία να βρουν και να απαλείψουν τις ευπάθειες υψηλού κινδύνου.

- **Άριστη υποστηρικτική ομάδα.** Διερευνάται κατά πόσο η ομάδα που υποστηρίζει το εργαλείο ανταποκρίνεται άμεσα, 24/7, σε όλες τις απαιτήσεις του πελάτη. Εάν ενημερώνει το εργαλείο σε τακτά χρονικά διαστήματα προσθέτοντας σε αυτό καινούργια χαρακτηριστικά, ανταποκρινόμενη στις ανάγκες των πελατών. Εάν η βάση ευπαθειών ενημερώνεται άμεσα με καινούργιες ευπάθειες. Ένα διαθέτει ερευνητική ομάδα η οποία ασχολείται με την ανεύρεση καινούργιων ευπαθειών. Εάν διαθέτει ομάδα εκπαίδευσης και διεξαγωγής σεμιναρίων για τους πελάτες της.

- **Ευελιξία.** Διερευνάται κατά πόσο το εργαλείο μπορεί να συνεχίσει να υποστηρίζει τον οργανισμός όσο αυτός θα εξελίσσεται και θα μεγαλώνει.

- **Ευκολία εκμάθησης και χρήσης.** Διερευνάται κατά πόσο το εργαλείο είναι εύκολο στην εκμάθηση, εάν είναι καλά τεκμηριωμένο, με εύκολα στην χρήση εγχειρίδια με λεπτομερή περιγραφή για όλα τα βήματα διαμόρφωσης του εργαλείου. Εάν διαθέτει υποστηρικτικά και εκπαιδευτικά βίντεο για την ορθή χρήση του εργαλείου ή online τάξης εκμάθησης.

- **Συνεργασίας με άλλα λογισμικά.** Διερευνάται κατά πόσο το εργαλείο μπορεί να συνεργαστεί με άλλα εργαλεία διαχείρισης ασφάλειας που διαθέτει ο οργανισμός, όπως συστήματα διαχείρισης ενημερώσεων κώδικα (patch management), IDS/IPS συστήματα, συστήματα διαχείρισης μηχανογραφικών περιουσιακών στοιχείων (asset management), κτλ.

- **Συσκευή ή λογισμικό.** Διερευνάται κατά πόσο εργαλείο είναι κάποια συσκευή η οποία θα πρέπει να τοποθετηθεί σε ασφαλές μέρος (server room) ή είναι λογισμικό. Η συσκευές συνήθως διαθέτουν μεγαλύτερη ταχύτητα και είναι πιο αξιόπιστες, από την άλλη το λογισμικό μπορεί να είναι φθηνότερο και να μπορεί να εγκατασταθεί σε υφιστάμενο υλικό υπολογιστή που είναι διαθέσιμο. Επίσης μπορεί το λογισμικό να προφερθεί σαν υπηρεσία νέφους μειώνονταν έτσι ακόμη περισσότερο το κόστος.

- **Ροή εργασίας.** Διερευνάται κατά πόσο το εργαλείο διαθέτει ροή εργασίας (workflow) για την ανάθεση εργασιών και παρακολούθηση προβλημάτων και κατά πόσο αυτές οι εργασίες μπορεί να ανατεθούν με την χρήση κανόνων στις αρμόδιες ομάδες. Στην περίπτωση που δεν διαθέτη ροή εργασίας το ίδιο μπορεί να συνεργαστεί με το εργαλείο ροής εργασιών που διαθέτει ο οργανισμος.

- **Πρότυπα διαμόρφωσης ασφάλειας.** Διερευνάται κατά πόσο το εργαλείο διαθέτει έτοιμα πρότυπα διαμόρφωσης ασφάλειας τα οποία μπορούν να χρησιμοποιηθούν για διερευνηθεί κατά πόσο το περιβάλλον αξιολόγησης συνάδει με αυτά. Τέτοια πρότυπα είναι το Sarbanes-Oxley, HIPPA ,κτλ.

Κεφάλαιο 7
Επίλογος

Η ανεύρεση όλων των γνωστών τρωτών σημείων ενός συστήματος και εν συνεχεία η ορθολογιστική χρήση τεχνικών αντιμετώπισης και απαλοιφής των αδυναμιών αυτών είναι πρωτίστης σημασίας. Η μη επαρκής αντιμετώπιση των ευπαθειών, καθιστούν το σύστημα ευάλωτο σε επιθέσεις με ανυπολόγιστες συνέπειες (υλικές, ηθικές, οικονομικές κτλ).

Η χρήση αξιόπιστων εργαλείων για την έγκυρη και έγκαιρη ανίχνευση των αδυναμιών και κατ' επέκταση την διασφάλιση της ασφάλειας των πληροφοριών, αποτελεί αναγκαιότητα και όχι πολυτέλεια για ένα σύγχρονο οργανισμό, και έχει πρωταρχικό ρόλο στο να τον βοηθήσει να επιτύχει τους στόχους του.

Στην παρούσα μεταπτυχιακή διατριβή έγινε προσπάθεια παρουσίας ενός μικρού αριθμού εργαλείων ανεύρεσης ευπαθειών, τα οποία τυγχάνουν ευρείας χρήσης και αποδοχής από την επαγγελματική και επιστημονική κοινότητα . Από τα αποτελέσματα των εργαλείων διαφαίνεται ότι ένα πληροφοριακό σύστημα εμπεριέχει ευπάθειες, οι οποίες μπορεί να καταστίσουν το ίδιο ή ακόμη και το δίκτυο, στο οποίο αποτελεί μέρος του, ευάλωτο σε πολλές απειλές, εσωτερικές ή

εξωτερικές. Οι ευπάθειες οι οποίες έχουν εντοπιστεί αποτελούν μέρος κακών ρυθμίσεων, μη σωστά ενημερωμένων εκδόσεων λογισμικού ή ακόμη σε παρουσία κακόβουλου λογισμικού.

Επιπρόσθετα έχει διαφανεί ότι η μονομερής χρήση ενός μόνο εργαλείου ανεύρεσης ευπαθειών δεν αποτελεί πανάκια, αφού κανένα από τα υπό εξέταση εργαλεία δεν έχει εντοπίσει όλες τις υπό διερεύνηση ευπάθειας. Για το λόγο αυτό συνίσταται η χρήση δύο ή περισσοτέρων εργαλείων για την όσο γίνεται καλύτερη διερεύνηση των αδυναμιών ενός πληροφοριακού συστήματος.

Ο τρόπος αντιμετώπισης μιας ευπάθειας μπορεί να δημιουργήσει μια καινούργια ευπάθεια η οποία να εμπεριέχει περισσότερους κινδύνους, από την αρχική ευπάθεια. Τα βήματα που ακολουθούνται για την αντιμετώπιση των ευπαθειών θα πρέπει να καταγράφονται και να αξιολογούνται πριν, αλλά και μετά την εφαρμογή τους . Για το λόγο αυτό η διαδικασία ***εκτίμηση τρωσιμότητας ->επιδιόρθωση->επανεκτίμηση τρωσιμότητας*** θα πρέπει να αποτελεί τον ακρογωνιαίο λίθο στην ανίχνευση επισφαλών σημείων ενός οργανισμού.

Τα εργαλεία τα οποία έχουν χρησιμοποιηθεί ήταν, στην πλειοψηφία τους, εύκολα στην χρήση με καλό υποστηρικτικό υλικό. Τα αποτελέσματα των καταστάσεων των εργαλείων OpenVas, Nexpose, Qualys και SAINT έδωσαν αρκετές πληροφορίες τόσο για τις επιπτώσεις όσο και για την αντιμετώπιση των ανευρεθέν ευπαθειών. Από την άλλη το εργαλείο NMAP έδωσε και αυτό κάποιες πληροφορίες για τις ευπάθειες, αλλά χρειαζόταν περισσότερο διαδικτυακό ψάξιμο για να αποκομιστεί μια πιο ολοκληρωμένη εικόνα για την κάθε ευπάθεια και για τον τρόπο αντιμετώπισής της.

Πέρα από την χρήση των εργαλείων ανίχνευσης ευπαθειών, η πρόληψη αποτελεί το βασικότερο συστατικό στην αντιμετώπιση των επισφαλών σημείων των πληροφοριακών συστημάτων ενός οργανισμού. Κάποια μέτρα πρόληψης τα οποία συστήνονται να ακολουθούνται από τους οργανισμούς είναι:

- Η δημιουργία πολιτικών και διαδικασιών ασφαλείας.
- Η συνεχής εκπαίδευση του τεχνικού και όχι μόνο προσωπικού σε θέματα ασφαλείας.
- Η εγκατάσταση αρχείων επιδιόρθωσης τόσο για το λειτουργικό σύστημα όσο και για τα υπόλοιπα λογισμικά, όταν αυτά γίνονται διαθέσιμα, αφού έχουν πρώτα ελεγχθεί για τυχών αρνητικές επιπτώσεις στη λειτουργικότητα του συστήματος.

- Η απενεργοποίηση και αφαίρεση αχρείαστων υπηρεσιών και λογισμικού.

- Η απενεργοποίηση των πρωτοκόλλων επικοινωνίας το οποία δεν επιδέχονται κρυπτογράφηση.

- Η εφαρμογή της τακτικής διάθεσης όσο το δυνατό λιγότερων δικαιωμάτων (με βάση τα καθήκοντά τους) πρόσβασης και χρήσης, λογισμικού και δικτυακών πόρων στους χρήστες και η επανεξέταση αυτών σε τακτά χρονικά διαστήματα ή/και μετά από την αλλαγή καθηκόντων τους.

- Η καταγραφή, η διαχείριση και η συνεχής παρακολούθηση όλων των συνδέσεων του δικτύου. Η χρήση τοίχου προστασίας και η επιβολή κανόνων ούτως ώστε να επιτρέπεται μόνο η αναγκαία επικοινωνία μεταξύ των συμβαλλόντων μερών .

- Και τέλος η εγκατάσταση συστημάτων ελέγχου ασφαλείας IDS/IPS, εργαλεία ελέγχου ευπαθειών κ.ο.κ, για την επιβεβαίωση της αποδοτικότητας και αποτελεσματικότητας των μέτρων ασφαλείας που έχουν παρθεί.

Συνοψίζοντας θα λέγαμε ότι η ασφάλεια θα πρέπει να αποτελεί πλέον, μέρος της κουλτούρας ενός οργανισμού. Δε δύναται να υπάρχει οργανισμός κυβερνητικός ή μη ο οποίος να διαχειρίζεται εμπιστευτικά δεδομένα και μην έχει σε ισχύ πολιτικές ασφαλείας. Σημαντικό ρόλο στην ανάπτυξη αυτής της κουλτούρας έχουν να διαδραματίσουν τα ακαδημαϊκά ιδρύματα, από τα οποία θα εξέλθουν στην αγορά εργασίας, οι μελλοντικοί επαγγελματίες του κλάδου πληροφορικής. Η δημιουργία εξειδικευμένων κλάδων με θέμα την προαγωγή της ασφάλειας των πληροφοριακών συστημάτων, καθώς και η συνεχής εκπαίδευση και ενημέρωση τόσο του ακαδημαϊκού προσωπικού όσο και των αποφοίτων, με την διοργάνωση σεμιναρίων γύρω από τις τελευταίες εξελίξεις του τομέα είναι επιβεβλημένη.

Βιβλιογραφία

[01] Γκριτζάλης Στέφανος, Ο Δεκάλογος Για Θέματα Ασφαλείας Πληροφοριακών Συστημάτων Και Προστασίας Προσωπικών Δεδομένων Στο Ηλεκτρονικό Επιχειρείν, ebusiness forum, Ελληνική Δημοκρατία-Υπουργείο Ανάπτυξης, Αθήνα, Ιούνιος 2002 (σελ. 2), (http://84.205.229.18/securityc/d/greek/Asfaleia/dekalogos_asfaleias.pdf, τελευταία πρόσβαση στις 09/04/2017).

[02] Alder Raven, Alderson Jimmy, Johnston Andy, Theall A. George, 2004, Nessus Network Auditing, Syngress Publishing (σελ. 6-7).

[03] Brown Lawrie, Stallings William, 2012, Computer Security Principles and Practice, Second Edition, PEARSON (σελ. 10-11, 33-34).

[04] Dr. Belovish G. Steve, A brief History of IT Security & Architecture, 18 May 2010 (σελ. 02), (http://www.iqmtm.com/PDF_presentations/SecurityArticleBrief5-18-10.pdf, τελευταία πρόσβαση στις 09/04/2017).

[05] Falco Joe, Scarfone Karen, Stouffer Keith, June 2011, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Department of Commerce, U.S.A (σελ. 32).

[06] Forester Tom, Morrison Perry, 1994, Computer Ethics Cautionary Tales And Ethical Dilemmas In Computing, Second Edition, Massachusetts Institute of Technology (σελ. 29).

[07] Hdmoore, 31/05/2012, Egypt 13/12/2013, Metasploitable 2 Exploitability Guide (https://community.rapid7.com/docs/DOC-1875, τελευταία πρόσβαση στις 09/04/2017).

[08] Kizza Migga Joseph, 2013, Guide to Computer Network Security, Second Edition, Springer (σελ. 111).

[09] Marc Ruef, 2010-2017, VULSCAN.NSE(http://www.computec.ch/projekte/vulscan/, τελευταία πρόσβαση στις 09/04/2017).

[10] Metasploitable-Virtual Machine to test Metasploit, 2017, Rapid 7, (https://information.rapid7.com/metasploitable-download.html, τελευταία πρόσβαση στις 09/04/2017).

[11] Mitnick D. Kevin, Simon L. William, 2002, The Art of Deception: Controlling the Human Element of Security, Wiley (σελ. 36).

[12] Nexpose (https://www.rapid7.com/products/nexpose/features/, τελευταία πρόσβαση στις 09/04/2017).

[13] Nmap Security, (https://Nmap.org/, τελευταία πρόσβαση στις 09/04/2017).

[14] Nmap, (https://linux.die.net/man/1/Nmap, τελευταία πρόσβαση στις 09/04/2017).

[15] NSE Scripts,, Nmap (https://Nmap.org/book/nse-usage.html, τελευταία πρόσβαση στις 09/04/2017).

[16] OpenVas ,(http://www.openvas.org/software.html, τελευταία πρόσβαση στις 09/04/2017).

[17] OUSPG, Takanen Ari, Glossary of Vulnerability Testing Terminology. (http://www.ee.oulu.fi/research/ouspg/sage/glossary, τελευταία πρόσβαση στις 09/04/2017).

[18] Qualys Vulnerability Management (https://www.qualys.com/suite/vulnerability-management/, τελευταία πρόσβαση στις 09/04/2017).

[19] SAINT Vulnerability Assessment (http://www.saintcorporation.com/products/vulnerability-assessment/, τελευταία πρόσβαση στις 09/04/2017).

[20] Scarfone Karen, Souppaya Murugiah, February 2012, Guidelines for Securing Wireless Local Networks, NIST Special Publication 800-153, Department of Commerce, U.S.A.

[21] Session Hijacking (http://www.xtrmhack.com/2010/12/session-hijacking.html, τελευταία πρόσβαση στις 09/04/2017).

[22] Strebe Matthew, 2004, Network Security Foundations, Sybex (σελ. 2-4, 24-34).

[23] UnrealIRCD, 27/11/2015, Cron job (https://www.unrealircd.org/docs/Cron_job, τελευταία πρόσβαση στις 09/04/2017).

[24] UnrealIRCd, 10/11/2016, Installation from source (https://www.unrealircd.org/docs/Installing_from_source, τελευταία πρόσβαση στις 09/04/2017).

[25] Verizon 2016 Data Breach Investigations Report. (σελ. 07) (http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf, τελευταία πρόσβαση στις 09/04/2017).

[26] Wikipedia, Hacker, (https://en.wikipedia.org/wiki/Hacker, τελευταία πρόσβαση στις 09/04/2017).

[27] Wikipedia, Ασφάλεια Πληροφοριακών Συστημάτων, Ελληνική Μετάφραση, (https://en.wikipedia.org/wiki/Information_security, τελευταία πρόσβαση στις 09/04/2017).