Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. " Ασφάλεια Ψηφιακών Συστημάτων "

Δημιουργία πρακτόρων για αυτόματη αναφορά ευπαθειών

Γεώργιος Γεραμάνης

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Φεβρουάριος 2021

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος Εικόνων

Περίληψη

Μελετήσαμε σε βάθος κάποια από τα υπάρχοντα εργαλεία ανίχνευσης ευπαθειών, δίνοντας έμφαση σε αυτά που είναι ανοικτού κώδικα, και είδαμε τα αποτελέσματα αλλά και τις επιπλέον λειτουργικότητες που παρέχει το καθένα από αυτά. Παρατηρήσαμε πως διαφορετικά εργαλεία έχουν και διαφορετικές επιδόσεις τόσο στον εντοπισμό των ευπαθειών όσο και σε άλλες λειτουργικότητες ως προς τη διαχείριση των ευπαθειών. Έτσι οδηγηθήκαμε στη δημιουργία ενός εργαλείου που συμβάλλει στη διαχείριση των ευπαθειών μιας υποδομής μέσω της σύγκρισης διαδοχικών σαρώσεων αλλά και της παροχής αυτόματων ειδοποιήσεων / αναφορών.

1. Εισαγωγή

Η ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων αποτελεί στις μέρες μας παράγοντα κομβικής σημασίας για κράτη, οργανισμούς και άτομα. Καθημερινά όμως προκύπτουν ευπάθειες που μπορούν να αξιοποιηθούν κακόβουλα, προκαλώντας από τις πιο μικρές μέχρι και τις πιο συντριπτικές συνέπειες. Η ανίχνευση ευπαθειών έχει υιοθετηθεί ευρέως ως μια διαδικασία που μπορεί να εντοπίσει ευπάθειες σε πολλαπλά επίπεδα.

Το οικοσύστημα των ευπαθειών έχει ωριμάσει τα τελευταία χρόνια. Έχει επενδυθεί μεγάλη προσπάθεια για τη συστηματική καταγραφή, την ταξινόμηση αλλά και την επικοινώνηση των ευπαθειών με όρους κρισιμότητας, επιπτώσεων και πολυπλοκότητας της σχετικής απειλής. Η τυποποίηση στην περιγραφή των ευπαθειών συμβάλλει παράλληλα, όχι μόνο σε αποτελεσματικό διαμοιρασμό πληροφορίας για απειλές, αλλά ενδεχομένως και σε μια πιο αποτελεσματική διαχείριση των απειλών.

Μελετήσαμε σε βάθος κάποια από τα υπάρχοντα εργαλεία, δίνοντας έμφαση σε αυτά που είναι ανοικτού κώδικα, για την ανίχνευση ευπαθειών και είδαμε τα αποτελέσματα αλλά και τις επιπλέον λειτουργικότητες που παρέχει το καθένα από αυτά. Συγκεκριμένα πραγματοποιήσαμε σαρώσεις με το Nessus, το Nexpose, το OpenVAS, το Flan Scan καθώς και με το Nmap κάνοντας χρήση των NSE scripts.

Στη μελέτη μας παρατηρήσαμε πως διαφορετικά εργαλεία έχουν και διαφορετικές επιδόσεις τόσο στον εντοπισμό των ευπαθειών (false positives/negatives, διενέργεια διαφορετικών ελέγχων από τον εκάστοτε σαρωτή κ.ο.κ), όσο και σε άλλες λειτουργικότητες. Αυτό έχει ως αποτέλεσμα να μη μπορεί να προκύψει μια συνολική εικόνα για το κατα πόσο μια υποδομή είναι ευπαθής ή όχι όταν έχει σαρωθεί με ένα μόνο εργαλείο. Για το λόγο αυτό, σε πολλές περιπτώσεις χρειάζεται να διεξάγεται εκτίμηση ευπαθειών με παραπάνω από μία από τις υπάρχουσες λύσεις. Το παραπάνω οδηγεί όμως σε πολλαπλές αναφορές από τους πολλαπλούς σαρωτές κάτι που δεν είναι πρακτικό και αυξάνει την πολυπλοκότητα στη διαχείριση ευπαθειών, ιδιαίτερα όταν πρόκειται για υποδομές που περιλαμβάνουν μεγάλο αριθμό οντοτήτων (πολλαπλούς σταθμούς εργασίας, εξυπηρετητές κλπ).

Προκύπτει λοιπόν η αναγκαιότητα της σύγκρισης μεταξύ των αποτελεσμάτων από τα διαφορετικά εργαλεία ώστε ο διεξάγων την εκτίμηση ευπαθειών, να έχει κάθε φορά να μελετήσει μια μόνο αναφορά. Η αναφορά αυτή πρέπει να περιλαμβάνει το σύνολο των ευπαθειών που προέκυψαν από τα διαφορετικά εργαλεία χωρίς κάποιες από τις ευπάθειες να υπάρχουν παραπάνω από μια φορά.

Ο λόγος για τον οποίο διεξάγεται η εκτίμηση ευπαθειών, είναι η έγκαιρη και έγκυρη εξάλειψη τους από το σύστημα το οποίο μας αφορά. Παρατηρήσαμε πως δεν υπάρχει - τουλάχιστον στις λύσεις που δοκιμάσαμε - η δυνατότητα αυτόματων ειδοποιήσεων και αναφορών (σε επίπεδο λειτουργικού και χωρίς να χρειάζεται ο εκάστοτε διαχειριστής να συνδεθεί στην κονσόλα διαχείρισης), ανεξαρτήτως λειτουργικού συστήματος. Διαπιστώσαμε επίσης, στα εργαλεία ανοικτού κώδικα με τα οποία πειραματιστήκαμε πως δεν παρέχεται η δυνατότητα αυτόματης σύγκρισης των αποτελεσμάτων ανάμεσα σε διαδοχικές σαρώσεις. Η παραπάνω λειτουργικότητα, θα έκανε πολύ πιο εύκολη την διαχείριση των ευπαθειών καθώς ο διαχειριστής θα είχε εικόνα για τις νέες ευπάθειες που εντοπίστηκαν στο σύστημα / υποδομή, τις ευπάθειες που εκκρεμεί ακόμη το να εξαλειφθούν από την προηγούμενη σάρωση καθώς και τις ευπάθειες που έχουν πάψει να υπάρχουν από την προηγούμενη σάρωση.

Οι παραπάνω διαπιστώσεις μας οδήγησαν στη δημιουργία ενός εργαλείου που συμβάλλει στη διαχείριση των ευπαθειών μιας υποδομής. Το εργαλείο αυτό, μπορεί να συνδεθεί με κάποιες από τις υπάρχουσες λύσεις και να παραμετροποιηθεί κατάλληλα ώστε να σαρώνει συστήματα με την καθεμία ανά επιθυμητά χρονικά διαστήματα. Στη συνέχεια, αναλύει και συγκρίνει τα αποτελέσματα που προκύπτουν από την κάθε σάρωση με τα προηγούμενα και τέλος μας τροφοδοτεί δικτυακά με τις κατάλληλες ειδοποιήσεις. Επιπλέον, επιχειρήσαμε χρησιμοποιώντας ως πρόσθετα δυο διαφορετικά εργαλεία, και πραγματοποιώντας διαδοχικές σαρώσεις κάνοντας χρήση πρώτα του OpenVAS και στη συνέχεια του Flan Scan να συγκρίνουμε τα αποτελέσματα που προκύπτουν για το ίδιο σύστημα από το καθένα από αυτά.

1.1 Εισαγωγικές έννοιες

1.1.1 Ευπάθειες

Στην ασφάλεια πληροφοριών ως ευπάθειες ορίζονται οι αδυναμίες που μπορεί να προκαλέσουν επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα.[1] Πρόκειται για αδυναμίες τις οποίες αν τις εκμεταλλευτεί ένας παράγοντας απειλής - όπως ένας επιτιθέμενος - μπορεί να ξεπεράσει τα όρια προνομίων σε ένα υπολογιστικό σύστημα. Για την εκμετάλλευση μιας ευπάθειας, ένας επιτιθέμενος πρέπει να διαθέτει τουλάχιστον μία τεχνική ή ένα εργαλείο που να μπορεί να συνδεθεί στην αδυναμία του συστήματος.[2] Σε αυτό το πλαίσιο, οι αδυναμίες είναι επίσης γνωστές και ως επιφάνεια επιθέσεων.

1.1.2 CVE

Το σύστημα CVE (Common Vulnerabilities and Exposure system) μας παρέχει μία μέθοδο αναφοράς για δημοσίως γνωστές ευπάθειες και εκθέσεις ασφάλειας πληροφοριών.[3] Το FFRDC εθνικής ασφάλειας στον κυβερνοχώρο των ΗΠΑ, το οποίο λειτουργεί από την εταιρεία Mitre, διατηρεί το σύστημα και χρηματοδοτείται από το τμήμα εθνικής ασφάλεια στον κυβερνοχώρο. Το σύστημα ξεκίνησε να λειτουργεί επισήμως το 1999.[4] Επιπλέον το Πρωτόκολλο Αυτοματοποίησης Ασφάλειας περιεχομένου χρησιμοποιεί το CVE, όπως επίσης και η Εθνική Βάση Ευπαθειών των ΗΠΑ.

1.1.3 Αναγνωριστικά CVE

Το εγχειρίδιο της εταιρείας MITRE ορίζει τα αναγνωριστικά CVE (που επίσης ονομάζονται ονόματα των CVE, αριθμοί των CVE, CVE-IDs και CVEs) ως μοναδικά, κοινά αναγνωριστικά για δημοσίως γνωστές ευπάθειες ασφάλειας πληροφοριών, δημοσιευμένες σε πακέτα λογισμικού. Ιστορικά, τα αναγνωριστικά CVE αρχικά

[1] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
[2] https://nvd.nist.gov/vuln
[3] https://cve.mitre.org/cve/cna/rules.html#section_7-1_what_is_a_vulnerability
[4] https://cve.mitre.org/about/history.html

βρίσκονται σε κατάσταση υποψηφίων (“CAN-”) και στη συνέχεια μπορούσαν να προαχθούν σε CVE, ωστόσο αυτή η πρακτική έπαψε και πλέον σε όλα τα αναγνωριστικά ανατίθεται το CVE. Η ανάθεση ενός αριθμού CVE δεν είναι σίγουρο πως θα το εισάγει ως επίσημο CVE (π.χ. Ένα CVE μπορεί να έχει οριστεί ως τέτοιο ακατάλληλα είτε για ένα θέμα το οποίο δεν αφορά ευπάθεια ασφάλειας είτε γιατί υπάρχει ήδη αντίστοιχο).

Τα CVEs ανατίθενται από μια Αρχή Αρίθμησης CVE (CNA)[5], υπάρχουν τρία είδη ανάθεσης αριθμού CVE. Η MItre Corporation λειτουργεί ως εκδότρια και πρωταρχική CNA. Υπάρχουν κάποιες CNAs, οι οποίες αναθέτουν αριθμούς CVE για τα δικά τους προϊόντα όπως η Microsoft, η Oracle, η Red Hat, η HP και άλλες. Ένας συντονιστής τρίτων μερών όπως το CERT Coordination Center, δύναται να αναθέσει αριθμούς CVE σε προϊόντα που δεν καλύπτονται από άλλες CNAs. Όταν ερευνάται μια ευπάθεια ή μία πιθανή ευπάθεια, βοηθά αποκτά έναν αριθμό CVE από νωρίς. Οι αριθμοί CVE ενδέχεται να μην εμφανιστούν στις βάσεις δεδομένων της MITRE ή τις NVD CVE για ένα χρονικό διάστημα (ημερών, εβδομάδων, μηνών ίσως και χρόνων) είτε για λόγους απαγόρευσης (στην περίπτωση που έχει ανατεθεί ο αριθμός αλλά το συγκεκριμένο θέμα δεν έχει δημοσιευθεί) είτε σε περιπτώσεις όπου η εισαγωγή δεν έχει διερευνηθεί και περιγραφεί προς δημοσίευση από τη MITRE εξαιτίας προβλημάτων σχετικών με πόρους. Το όφελος της έγκαιρης υποψηφιότητας για ανάθεση αριθμού CVE, είναι πως όλη η μελλοντική επικοινωνία θα μπορεί να αναφέρεται στον αριθμό CVE. Η πληροφόρηση για την ανάθεση αναγνωριστικών CVE σε θέματα που αφορούν λογισμικό ανοικτού κώδικα είναι διαθέσιμη από τη Red Hat.

Τα CVEs είναι για λογισμικό το οποίο έχει δημοσιευθεί, σε αυτό περιλαμβάνονται εκδόσεις beta ή πρόοιμες εκδόσεις αν αυτές χρησιμοποιούνται ευρέως. Το εμπορικό λογισμικό περιλαμβάνεται και αυτό στην παραπάνω κατηγορία. Επιπλέον σε υπηρεσίες όπως ένας Web-based πάροχος email, δεν ανατίθενται CVEs για τις ευπάθειες που ανιχνεύονται σε αυτές (π.χ. Ευπάθεια σε XSS) εκτός αν η ευπάθεια υπάρχει σε κάποιο υποβόσκον προϊόν λογισμικού που διατίθεται δημόσια.

1.1.4 Σύστημα Βαθμολόγησης Κοινών Ευπαθειών

Το CVSS (Common Vulnerability Scoring System) είναι ένα ελεύθερο και ανοικτό βιομηχανικό πρότυπο για την εκτίμηση της σοβαρότητας των ευπαθειών ασφαλείας

[5] https://cve.mitre.org/cve/cna/

υπολογιστικών συστημάτων.[6] Το CVSS επιχειρεί να αναθέσει βαθμούς σοβαρότητας σε ευπάθειες, δίνοντας τη δυνατότητα προτεραιοποίησης της αντίδρασης αλλά και των πόρων με βάση την απειλή. Η βαθμολογία υπολογίζεται με βάση έναν τύπο που βασίζεται σε κάποια μετρικά τα οποία προσεγγίζουν την ευκολία και τις επιπτώσεις της εκμετάλλευσης μια ευπάθειας. Η βαθμολογία κυμαίνεται από το 0 μέχρι το 10, με το 10 να είναι το πιο σοβαρό.

Μολονότι χρησιμοποιείται ευρέως ως βασική βαθμολόγηση (το CVSS) για τον καθορισμό της κρισιμότητας, υπάρχουν παράλληλα χρονικές και περιβαλλοντικές βαθμολογήσεις, για να συμπεριλάβουν τη διαθεσιμότητα των μετριασμών και το πόσο εκτεταμένα είναι τα ευπαθή συστήματα μέσα σε μια υποδομή.

1.1.5 Εκτίμηση Ευπαθειών

Ως εκτίμηση ευπαθειών ορίζουμε τη συστηματική απεικόνιση των αδυναμιών ασφαλείας σε ένα πληροφοριακό σύστημα.[7] Η διαδικασία αυτή αξιολογεί αν ένα σύστημα είναι ευάλωτο σε κάποια από τις γνωστές ευπάθειες, αναθέτει επίπεδα κρισιμότητας σε αυτές τις ευπάθειες και προτείνει τρόπους για την εξάλειψη ή τον μετριασμό τους.

Κάποια χαρακτηριστικά παραδείγματα απειλών που μπορεί να αποτραπούν μέσω της ανίχνευσης ευπαθειών είναι επιθέσεις έγχυσης κώδικα όπως SQL Injections, XSS, επιθέσεις κλιμάκωσης προνομίων που οφείλονται σε ανεπαρκείς ή λάθος παραμετροποιημένους μηχανισμούς αυθεντικοποίησης, μη ασφαλής προεπιλεγμένη ρύθμιση ή λογισμικό που εκδίδεται με αδυναμίας ή μη ασφαλείς ρυθμίσεις όπως διαχειριστικό λογαριασμό με κωδικό χωρίς καμία πολυπλοκότητα.[8]
Υπάρχει μια σειρά από τρόπους κατηγοριοποίησης της εκτίμησης ευπαθειών. Σε αυτούς περιλαμβάνονται οι παρακάτω:

- Εκτίμηση ευπαθειών σε ένα μηχάνημα - Η εκτίμηση ευπαθειών σε κρίσιμους εξυπηρετητές, που μπορεί να είναι ευπαθείς σε επιθέσεις εάν δεν έχουν ελεγχθεί επαρκώς ή δεν έχουν δημιουργηθεί από ένα δοκιμασμένο είδωλο

[6] https://www.first.org/cvss/
[7] https://www.beyondtrust.com/resources/glossary/vulnerability-assessment
[8] https://www.imperva.com

συστήματος.

- Εκτίμηση ευπαθειών σε ενσύρματο ή ασύρματο δίκτυο - Η αξιολόγηση πολιτικών και πρακτικών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ιδιωτικά ή δημόσια δίκτυα ή δικτυακώς προσβάσιμους πόρους.

- Εκτίμηση ευπαθειών σε βάσεις δεδομένων - Η αξιολόγηση βάσεων δεδομένων συστημάτων μεγάλου όγκου δεδομένων για ευπάθειες ή λάθος παραμετροποίηση, εντοπίζοντας ψεύτικες βάσεις δεδομένων και μη ασφαλή περιβάλλοντα ανάπτυξης/δοκιμών και κατηγοριοποιώντας τα ευαίσθητα δεδομένα στο εσωτερικό ενός οργανισμού.

- Σάρωση εφαρμογών - Ο εντοπισμός ευπαθειών ασφάλειας σε web εφαρμογές και στον πηγαίο τους κώδικα είτε με χρήση αυτοματοποιημένης σάρωσης στο front-end είτε με στατική ή δυναμική ανάλυση στον πηγαίο κώδικα.

1.1.6 Εκτίμηση Ευπαθειών & Εκτίμηση Επικινδυνότητας

Οι εκτιμήσεις ευπαθειών επιτρέπουν στις ομάδες ασφάλειας πληροφοριακών συστημάτων να εφαρμόσουν μια συνεπή, εκτενή και ξεκάθαρη προσέγγιση για τον εντοπισμό και τη διαχείριση των απειλών και των κινδύνων ασφάλειας.[9] Κάτι τέτοιο μπορεί να έχει μια σειρά από οφέλη για την πληροφοριακή υποδομή:

- Έγκαιρη και συνεπή ταυτοποίηση απειλών και αδυναμιών αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων.

- Δράσεις για την κάλυψη των κενών καθώς και την προστασία των ευαίσθητων συστημάτων και πληροφοριών.

- Κάλυψη των αναγκών σε επίπεδο κανονιστικού πλαισίου όσον αφορά την ασφάλεια στον κυβερνοχώρο.

- Προφύλαξη από μη εξουσιοδοτημένες προσβάσεις καθώς και παραβιάσεις δεδομένων.

[9] Arbaugh, W., Fithen, W., McHugh, J. Windows of Vulnerability: A Case Study Analysis. IEEE Computer, Vol 3, No. 12, December 2000

Μια εκτίμηση ευπαθειών ερευνά ένα ευρύ φάσμα ενδεχόμενων προβλημάτων μέσα σε πολλαπλά δίκτυα, συστήματα και άλλα μέρη ενός πληροφοριακού οικοσυστήματος. Μπορεί να ταυτοποιεί αδυναμίες που χρειάζονται διόρθωση, περιλαμβανομένων των λαθών κατα την παραμετροποίηση που με την προσθήκη των κατάλληλων ενημερώσεων ασφαλείας μπορούν να καλυφθούν σε πολλές περιπτώσεις.

Οι περισσότερες μέθοδοι εκτίμησης ευπαθειών αναθέτουν έναν βαθμό επικινδυνότητας, πραγματοποιώντας αξιολόγηση του ρίσκου για την κάθε απειλή που εντοπίζεται.[10] Στα εκάστοτε ρίσκα μπορεί να έχει ανατεθεί συγκεκριμένη προτεραιότητα, σπουδαιότητα και αντίκτυπος, κάτι που καθιστά ευκολότερο το να επικεντρωθούμε σε αυτά τα οποία μπορούν πράγματι να προκαλέσουν προβλήματα στην ύπο έλεγχο υποδομή. Αυτό είναι σημαντικό για τη διαχείριση ευπαθειών ιδιαίτερα σε μεγάλες υποδομές και όταν ο χρόνος και οι πόροι είναι περιορισμένοι, προκειμένου πάντοτε να γίνει περιορισμός μιας πιθανής καταστροφής.

Η πληροφορία που προκύπτει από μια αποτίμηση ευπαθειών βοηθά στην ιεράρχηση των ευπαθειών αλλά και τη γραφική αναπαράσταση των απαραίτητων δράσεων - που συνήθως είναι η αποκατάσταση των ευπαθειών. Σε πολλές περιπτώσεις, ωστόσο, ενδέχεται να υπάρξει αποδοχή του ρίσκου από τους υπεύθυνους του πληροφοριακού αγαθού. Για παράδειγμα, αν η ευπάθεια που έχει εντοπιστεί έχει χαμηλό αντίκτυπο ή χαμηλή πιθανότητα εμφάνισης και η αποκατάσταση της μπορεί να προκαλέσει θέματα διαθεσιμότητας για το συγκεκριμένο πληροφοριακό αγαθό ή προβλήματα σε άλλα συστήματα τα οποία είναι διασυνδεδεμένα, τότε ενδέχεται το ρίσκο της συγκεκριμένης ευπάθειας να είναι χαμηλότερο από το ρίσκο για την εξάλειψη της. Έτσι λοιπόν οι ανιχνεύσεις ευπαθειών έχουν πρωταρχικό ρόλο στο πλαίσιο της διαχείρισης επικινδυνότητας.

1.2 Μεθοδολογία εκτίμησης ευπαθειών

Η μεθοδολογία για τις ανιχνεύσεις ευπαθειών περιλαμβάνει τα παρακάτω βήματα, ασχέτως με το αν πραγματοποιείται με κάποιο από τα υπάρχοντα εργαλεία ή

[10] National Institute of Standards and Technology (September 2008). "Technical Guide to Information Security Testing and Assessment" (PDF). *NIST*

χειροκίνητα.

- *Αρχικός Σχεδιασμός*
- *Σάρωση*
- *Ανάλυση*
- *Αναφορά & αποκατάσταση*

Υπάρχουν ποικίλοι τρόποι για τη διεξαγωγή εκτίμησης ευπαθειών. Ένας από τους πιο κοινούς τρόπους είναι με τη χρήση αυτοματοποιημένων λογισμικών σάρωσης ευπαθειών. Τα εργαλεία αυτά χρησιμοποιούν βάσεις δεδομένων με γνωστές, δημοσιευμένες ευπάθειες για τον εντοπισμό πιθανών ελαττωμάτων σε δίκτυα, εφαρμογές, containers, συστήματα, δεδομένα κ.ο.κ.

Ένα εργαλείο εντοπισμού ευπαθειών σαρώνει συνολικά και διεξοδικά το σύστημα. Εφόσον ολοκληρωθεί μια σάρωση το εργαλείο δημιουργεί μια αναφορά που περιλαμβάνει τα ευρήματα που προέκυψαν και τις προτάσεις για δράσεις για την εξάλειψη των απειλών.[11] Τα εργαλεία εντοπισμού ευπαθειών με πλήρεις δυνατότητες, δύνανται να παρέχουν διορατικότητα αναφορικά με την επίδραση του λειτουργικού κόστους και του κόστους ασφάλειας της εξάλειψης ή της αποδοχής του ρίσκου αντίστοιχα. Τα δεδομένα που προκύπτουν από έναν έλεγχο ευπαθειών μπορούν επίσης να τροφοδοτούνται σε κάποιο κεντρικοποιημένο σύστημα αρχείων καταγραφής (SIEM) για την επίτευξη μιας πιο ολιστικής ανάλυσης απειλών.

Η εκτίμηση και ο έλεγχος ευπαθειών μπορούν να διεξάγονται ανά τακτά χρονικά διαστήματα δεδομένης της διαρκώς μεταβαλλόμενης κατάστασης των πληροφοριακών συστημάτων. Για παράδειγμα μια ενημέρωση λογισμικού ή η παραμετροποίηση ενός συστήματος μπορούν να δημιουργήσουν νέες ευπάθειες, ενώ ταυτόχρονα ανακαλύπτονται συνεχώς νέες απειλές. Τα παραπάνω καθιστούν απαραίτητα τον γρήγορο εντοπισμό και την γρήγορη αντιμετώπιση ενός μιας απειλής για την ασφάλεια στον κυβερνοχώρο.

Η σάρωση για ευπάθειες αποτελεί μόνο ένα μέρος της εκτίμησης ευπαθειών - άλλες διεργασίες όπως οι δοκιμές παρείσδυσης, μπορούν να εντοπίσουν διαφορετικούς τύπους απειλών σε ένα πληροφοριακό σύστημα. Οι δοκιμές παρείσδυσης συμπληρώνουν τον έλεγχο ευπαθειών και είναι χρήσιμες για τον καθορισμό του αν είναι εφικτή η επέμβαση σε μία ευπάθεια ή αν κάποια επέμβαση θα δημιουργούσε βλάβη, απώλεια δεδομένων ή άλλα προβλήματα.

[11] ENISA, Good Practice Guide for Vulnerability Disclosure: From Challenges to recommendations, 2015. Available from: https://www.enisa.europa.eu/publications/vulnerability-disclosure

Το πιο σημαντικό μέρος της εκτίμησης ευπαθειών είναι η ανίχνευση ευπαθειών και άρα τα εργαλεία σάρωσης ευπαθειών. Ένα τέτοιο εργαλείο μπορεί να πραγματοποιήσει μια σειρά από ελέγχους όπως:

- Ελέγχους με διαπιστευτήρια και ελέγχους χωρίς διαπιστευτήρια
- Εξωτερικούς ελέγχους ευπαθειών
- Εσωτερικούς ελέγχους ευπαθειών
- Περιβαλλοντικούς ελέγχους

Οι *έλεγχοι με διαπιστευτήρια* είναι οι έλεγχοι κατά τους οποίους οι δοκιμές που πραγματοποιούνται, γίνονται ως από κάποιο χρήστη με δικαιώματα πρόσβασης στο εκάστοτε σύστημα. Οι *Έλεγχοι χωρίς διαπιστευτήρια* είναι αυτοί που πραγματοποιούνται ως από κάποιο χρήστη χωρίς δικαιώματα πρόσβασης.

Οι *Εξωτερικοί έλεγχοι ευπαθειών* περιλαμβάνουν τη σάρωση οντοτήτων του πληροφοριακού οικοσυστήματος που έχουν απευθείας επικοινωνία με το διαδίκτυο και είναι προσβάσιμες απευθείας σε χρήστες εκτός του δικτύου. Για παράδειγμα δικτυακές πόρτες, δίκτυα, ιστοσελίδες και άλλα συστήματα προσβάσιμα σε εξωτερικούς χρήστες.

Οι *Εσωτερικοί έλεγχοι ευπαθειών* περιλαμβάνουν τη σάρωση οντοτήτων του πληροφοριακού οικοσυστήματος όπου η πρόσβαση γίνεται μόνο από το εσωτερικό του δικτύου. Η διαδικασία αυτή έχει ως στόχο τον εντοπισμό διάτρητων σημείων τα οποία μπορούν να προκαλέσουν σοβαρά προβλήματα στο δίκτυο.

Οι *Περιβαλλοντικοί έλεγχοι ευπαθειών* επικεντρώνονται σε συγκεκριμένες λειτουργικές τεχνολογίες όπως για παράδειγμα υπηρεσίες Cloud, συστήματα Scada, IoT και κινητές συσκευές.

Τα βασικά κριτήρια για την επιλογή ενός εργαλείου εντοπισμού ευπαθειών δίνεται έμφαση στα παρακάτω:

- Συχνότητα ενημερώσεων

- Ποιότητα και ποσότητα των ευπαθειών, περιλαμβανομένης της ελαχιστοποίησης των “false positives” και των “false negatives”

1.3 Πηγές δεδομένων για καταγεγραμμένες ευπάθειες

Βασική παράμετρος για την ανίχνευση των ευπαθειών είναι οι πηγές δεδομένων για καταγεγραμμένες ευπάθειες. Παρακάτω έχουμε συλλέξει μερικές πηγές, των τύπο των δεδομένων που παρέχουν καθώς και την περιγραφή τους.[12]

Η **NVD database** συλλέγει CVE data.[13] Είναι ο χώρος όπου αποθηκεύονται από την κυβέρνηση των ΗΠΑ δεδομένων διαχείρισης ευπαθειών που είναι βασισμένα σε κάποια τυποποίηση. Το NVD περιλαμβάνει βάσεις δεδομένων αναφορές σε λίστες αναφοράς ασφάλειας, προγραμματιστικά λάθη σε σχέση με την ασφάλεια, λάθος παραμετροποιήσεις, ονόματα προϊόντων καθώς και μετρικές επιπτώσεων.

Το **ATT&CK** περιλαμβάνει μοτίβα επιτιθέμενων (τεχνικές και τακτικές).[14] Αποτελεί μια παγκοσμίως προσβάσιμη γνωσιακή βάση με τακτικές και τεχνικές των αντιπάλων, οι οποιες βασίζονται σε παρατηρήσεις που γίνονται στον πραγματικό κόσμο.

Το **Shodan** περιλαμβάνει μεγάλο αριθμό προγραμμάτων εκμετάλλευσης ευπαθειών.[15] Είναι ουσιαστικά μια βάση με συσκευές συνδεδεμένες στο διαδίκτυο (π.χ. Κάμερες, δρομολογητές, εξυπηρετητές) που αποκτούν δεδομένα από διάφορες δικτυακές πόρτες (HTTP/HTTPS - πόρτα 80, 443, 8080, 8443 κλπ).

Η **Exploit database** διαθέτει δεδομένα που δεν σχετίζονται με CVEs.[16] Περιλαμβάνει πληροφορίες για δημόσια προγράμματα εκμετάλλευσης ευπαθειών και το αντίστοιχο

[12] ENISA, State of Vulnerabilitites 2018/2019: Analysis of Events in the life of Vulnerabilities, December 2019
[13] https://nvd.gov/
[14] https://attack.mitre.org/
[15] https://www.shodan.io/
[16] https://www.exploit-db.com/about-exploit-db

ευπαθές λογισμικό. Η συλλογή των προγραμμάτων εκμετάλλευσης επιτυγχάνεται με άμεσες υποβολές, λίστες διαδικτυακής αλληλογραφίας και άλλες δημόσιες πηγές.

Το **CVE details** περιλαμβάνει και αυτό δεδομένα CVE.[17] Η βάση δεδομένων CVE περιλαμβάνει λεπτομέρειες για την κάθε μια δημοσιευμένη ευπάθεια ασφάλειας στον κυβερνοχώρο περιλαμβανομένου του αριθμού ταυτοποίησης, της περιγραφής και τουλάχιστον μια δημόσια αναφορά.

Το **Zero Day Initiative (ZDI)** περιλαμβάνει δεδομένα CVE αλλά και δεδομένα που δε σχετίζονται με CVEs.[18] Ο συγκεκριμένος ιστότοπος ενθαρρύνει την αναφορά ευπαθειών ημέρας μηδέν (zero-day), ιδίως σε επηρεασμενους προμηθευτές. Αυτό το επιτυγχάνουν αμοίβοντας οικονομικά ερευνητές (στην ουσία πρόκειται για πρόγραμμα επικήρυξης σφαλμάτων). Δε δημοσιεύονται τεχνικές λεπτομέρειες για κάθε μια από τις ευπάθειες παρά μόνο όταν ο εκάστοτε προμηθευτής δημοσιεύσει το κατάλληλο λογισμικό επιδιόρθωσης. Το ZDI δεν μεταπωλεί ή αναδιανέμει τις ευπάθειες.

Το **ThreatConnect** δύναται να παρέχει τον αριθμό των περιστατικών ασφάλειας που σχετίζονται με CVEs.[19] Πρόκειται ουσιαστικά για αυτοματοποιημένη παραγωγή πληροφοριών σχετικά με απειλές για συστήματα Intel.

Η **VulDB** περιλαμβάνει δεδομένα για την αξιολόγηση και τιμολόγηση προγραμμάτων εκμετάλλευσης ευπαθειών και κατηγορίες λογισμικού.[20] Είναι μια βάση δεδομένων για την καταγραφή και την επεξήγηση ευπαθειών ασφάλειας καθώς και εκμεταλλεύσεων αυτών.

Το **US CERT** διαθέτει δεδομένα για τον βιομηχανικό τομέα.[21] Το Τμήμα Ασφάλειας στον Κυβερνοχώρο και τις Υποδομές (CISA) του Υπουργείου Εσωτερική Ασφάλειας των ΗΠΑ έχει ως στόχο τη διεύρυνση της ασφάλειας, της ανθεκτικότητας και της αξιοπιστίας της ασφάλειας στον κυβερνοχώρο των ΗΠΑ καθώς και των υποδομών επικοινωνίας.

---

[17] https://cve.mitre.org
[18] https://zerodayinitiative/
[19] https://threatconnect.com/
[20] https://vulndb.com/
[21] https://www.us-cert.gov/

Το **Zerodium** μας παρέχει τιμολόγηση για επικηρυγμένα σφάλματα καθώς και για προγράμματα εκμετάλλευσης ευπαθειών.[22] Πρόκειται για μια πλατφόρμα εξέτασης ευπαθειών ημέρα μηδέν. Δημιουργήθηκε από ειδικούς στην ασφάλεια στον κυβερνοχώρο με εμπειρία στην προηγμένη ανίχνευση ευπαθειών.

2. Σαρωτές Ευπαθειών

Η εκτίμηση ευπαθειών αποτελεί τη διεργασία του εντοπισμού κινδύνων και αδυναμιών σε δίκτυα υπολογιστών, συστήματα, εξοπλισμό (φυσικό ή εικονικό), εφαρμογές και άλλα μέρη ενός πληροφοριακού οικοσυστήματος. Οι εκτιμήσεις ευπαθειών παρέχουν στις ομάδες ασφάλειας και σε άλλους ενδιαφερόμενους τις πληροφορίες που χρειάζονται ώστε να αναλύσουν και να ιεραρχήσουν ρίσκα με σκοπό τον μετριασμό τους στο κατάλληλο πλαίσιο.

Η διαδικασία αυτή είναι ένα δομικό στοιχείο της διαχείρισης των ευπαθειών καθώς και του κύκλου ζωής της διαχείρισης επικινδυνότητας σε πληροφοριακά συστήματα, δεδομένου ότι συμβάλλει επικουρικά στην προστασία συστημάτων από μη εξουσιοδοτημένες προσβάσεις καθώς και παραβιάσεις δεδομένων.

Οι εκτιμήσεις ευπαθειών συνήθως αξιοποιούν τους σαρωτές ευπαθειών ώστε να ταυτοποιήσουν απειλές και ατέλειες (όπως λάθη παραμετροποίησης) στο εσωτερικό της ύπο έλεγχο πληροφοριακής υποδομής, που ανακλούν πιθανές ευπάθειες ή έκθεση σε κίνδυνο.

Οι σαρωτές ευπαθειών είναι ίσως το πιο σημαντικό μέρος της διαχείρισης ευπαθειών. Αυτό που κάνουν είναι να σαρώνουν συστήματα για γνωστές ευπάθειες. Αναζητούν απαρχαιωμένα σημεία, σε λειτουργικά συστήματα και εφαρμογές, που είναι γνωστό πως έχουν ευπάθειες ασφάλειας. Με άλλα λόγια, ψάχνουν εκδόσεις λογισμικού που έχουν σφάλματα τα οποία έχουν δημοσιευτεί και είναι γνωστά. Σε συνάρτηση πάντα με τις προσβάσεις που έχουν δοθεί στον σαρωτή, είναι επιπλέον

[22] https://zerodium.com

εφικτός ο εντοπισμός σφαλμάτων παραμετροποίησης, όπως για παράδειγμα ο ακατάλληλος διαμοιρασμός αρχείων και παρεμφερή ζητήματα.

Υπάρχουν δικτυακοί σαρωτές ευπαθειών που σαρώνουν συστήματα τα οποία “κάθονται” σε ένα δίκτυο. Αυτοί μπορούν να εντοπίσουν ευπάθειες που είναι εκμεταλλεύσιμες από δικτυακές επιθέσεις. Υπάρχουν διαθέσιμες διαχειριζόμενες υπηρεσίες (εμπορικές και μη) που παρέχουν τη δυνατότητα για δικτυακές σαρώσεις ανά τακτά χρονικά διαστήματα. Επιπροσθέτως υπάρχουν σαρωτές ευπαθειών που δρουν σε μεμονωμένα συστήματα και μπορούν να πραγματοποιήσουν ένα επιπλέον επίπεδο ανίχνευσης προκειμένου να βρουν ευπάθειες τις οποίες μπορεί να εκμεταλλευτεί κάποιος με προσβάσεις στο σύστημα.

Οι σαρωτές ευπαθειών δικτύου ονομάζονται έτσι, προφανώς επειδή σαρώνουν ένα σύστημα μέσω του δικτύου. Αυτό το κάνουν πραγματοποιώντας ελέγχους, αρχικά αναζητώντας ανοικτές δικτυακές πόρτες και υπηρεσίες και στη συνέχεια αφού προκύψει μια λίστα με τις υπάρχουσες διαθέσιμες υπηρεσίες, διενεργούν επιπλέον έλεγχο για περισσότερες πληροφορίες που αφορούν είτε αδυναμίες παραμετροποίησης είτε γνωστές ευπάθειες.

Το εύρος των ευπαθειών που πιθανώς να εντοπιστούν μέσω αυτής της προσέγγισης είναι μεγάλο, σε γενικές γραμμές όμως περιλαμβάνει: υπηρεσίες που είναι παραμετροποιημένες με αδύναμα κρυπτογραφικά πρωτόκολλα, λογισμικό χωρίς τις κατάλληλες ενημερώσεις για γνωστές ευπάθειες ή ακόμη και υπηρεσίες που δεν θα έπρεπε να είναι ανοικτές.

2.1 Υπάρχουσες λύσεις

Γύρω από τη διαδικασία της ανίχνευσης ευπαθειών έχει δημιουργηθεί μια αγορά από κατασκευαστές που παρέχουν προϊόντα με δυνατότητες εντοπισμού, κατηγοριοποίησης και διαχείρισης ευπαθειών. Για παραπάνω από μια δεκαετία, το Nmap Project διατηρεί έναν κατάλογο με τα πιο διαδεδομένα εργαλεία ασφάλειας δικτύων.[23] Από το 2011, αυτό γίνεται με πιο δυναμικό τρόπο, προσφέροντας αξιολόγηση, ανάλυση, αναζήτηση και διαλογή μέσω της πλατφόρμας “New tool

[23] https://sectools.org/tag/vuln-scanners/

suggestion”. Σε αυτή την ιστοσελίδα, δημοσιεύονται εργαλεία ανοικτού κώδικα και εμπορικά προϊόντα οποιασδήποτε πλατφόρμας, εκτός από τα εργαλεία που διατηρεί το ίδιο το Nmap Project. Παρακάτω μπορούμε να δούμε τα πιο διαδεδομένα εργαλεία για ανίχνευση ευπαθειών που είναι είτε ανοικτού κώδικα είτε εμπορικά.

2.1 NMAP Scripting Engine (NSE)

Το Nmap Scripting Engine (NSE) αποτελεί ένα από τα πιο ισχυρά και ευέλικτα χαρακτηριστικά του Nmap.[24] Επιτρέπει στους χρήστες να γράψουν (και να μοιραστούν) απλά προγράμματα (scripts) (χρησιμοποιώντας τη γλώσσα προγραμματισμού Lua) ούτως ώστε να αυτοματοποιούν ένα ευρύ φάσμα δικτυακών διεργασιών. Αυτά τα scripts εκτελούνται παράλληλα με την ταχύτητα και την επάρκεια που αναμένεται από το Nmap. Οι χρήστες μπορούν να χρησιμοποιήσουν τα συνεχώς εξελισσόμενα και ποικιλόμορφα scripts που διανέμονται με το Nmap ή να γράψουν νέα προσαρμοσμένα στις δικές τους ανάγκες.

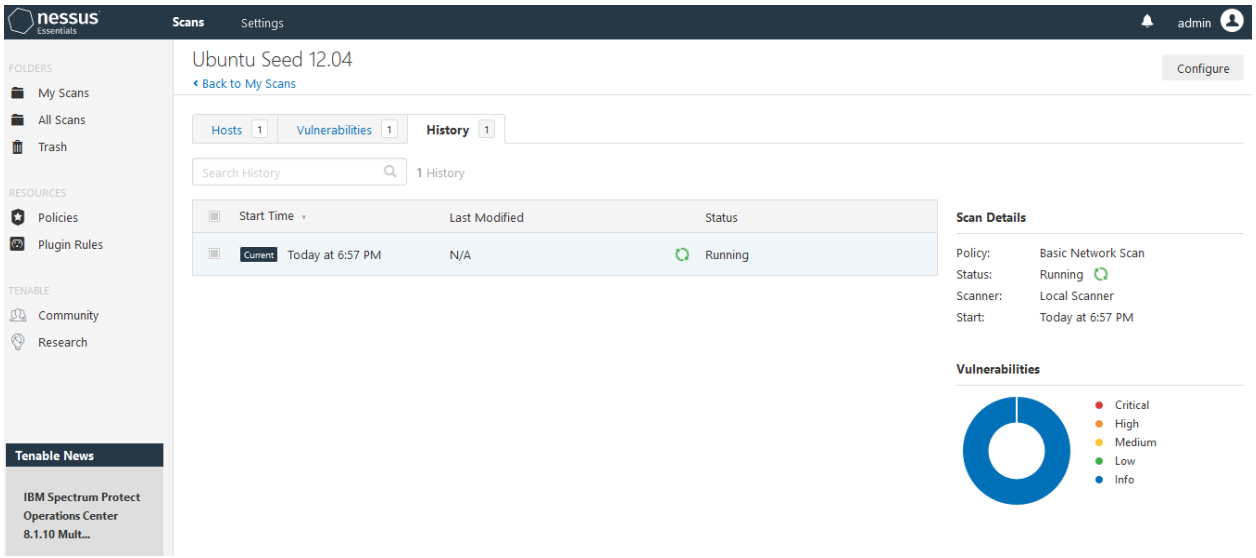
Η προφανής λειτουργικότητα που προκύπτει από τη δημιουργία του παραπάνω συστήματος, είναι μια πιο εξεζητημένη εξερεύνηση δικτύου, που να περιλαμβάνει την ανίχνευση ευπαθειών. Το NSE μπορεί ακόμη να χρησιμοποιηθεί για την εκμετάλλευση των ευπαθειών που μπορεί να υπάρχουν.

2.2 Nessus

Το Nessus[25] είναι ένα από τα πιο ικανά και διαδεδομένα εργαλεία εντοπισμού ευπαθειών, ιδιαιτέρως για συστήματα UNIX. Αρχικά ήταν ελεύθερο και ανοικτού κώδικα, αλλά από το 2005 έγινε κλειστού κώδικα και το 2008 αφαιρέθηκε ελεύθερη “Registered feed” έκδοση. Πλέον κοστίζει 2.190 δολάρια το χρόνο, διατίθεται όμως μια δωρεάν έκδοση που ονομάζεται “Nessus Home” η οποία όμως είναι αρκετά περιορισμένη και η άδεια της ισχύει μόνο για οικιακά δίκτυα.

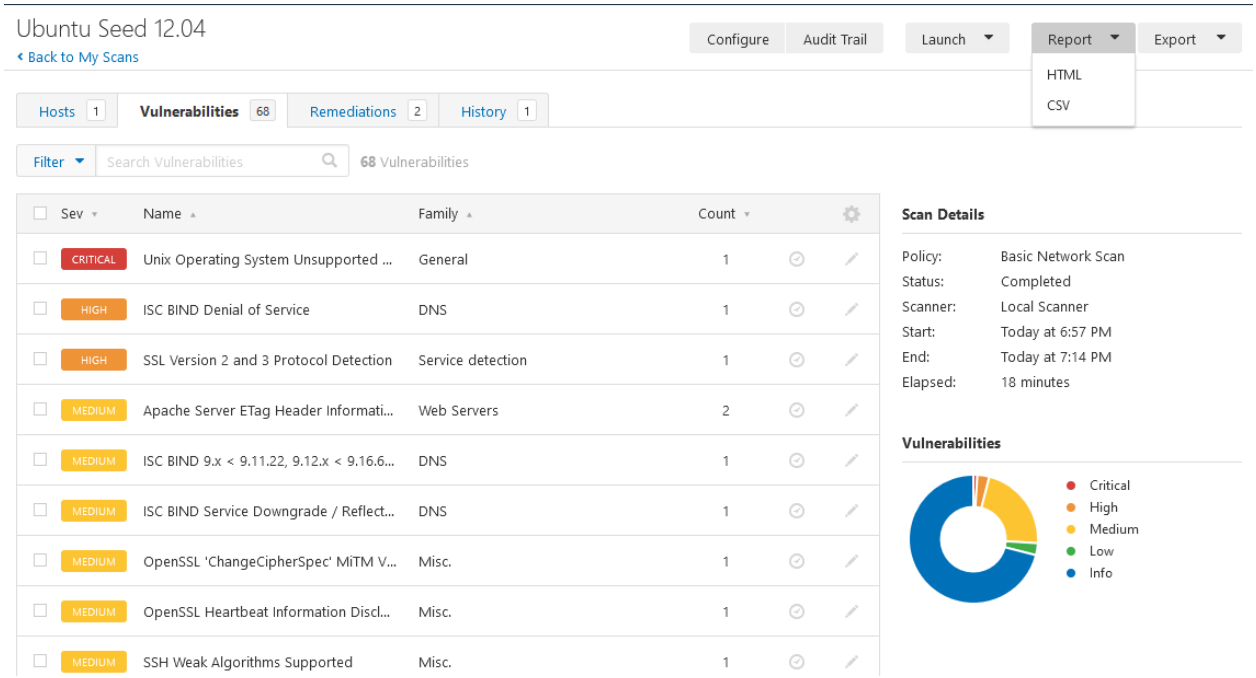
[24] https://nmap.org/book/man-nse.html
[25] **https://www.tenable.com/products/nessus**

Το Nessus ενημερώνεται διαρκώς και διαθέτει περισσότερα από 70.000 επιπρόσθετες λειτουργίες. Κάποια από τα βασικά χαρακτηριστικά του είναι πως διαθέτει απομακρυσμένους και τοπικούς (με αυθεντικοποίηση) ελέγχους ασφάλειας, μια αρχιτεκτονική βασισμένη στο μοντέλο client/server με web-based interface, καθως και μια ενσωματωμένη γλώσσα scripting ώστε ο χρήστης να μπορεί είτε να προσθέσει τα δικά του plugins, είτε να κατανοήσει περισσότερο τα ήδη υπάρχοντα.

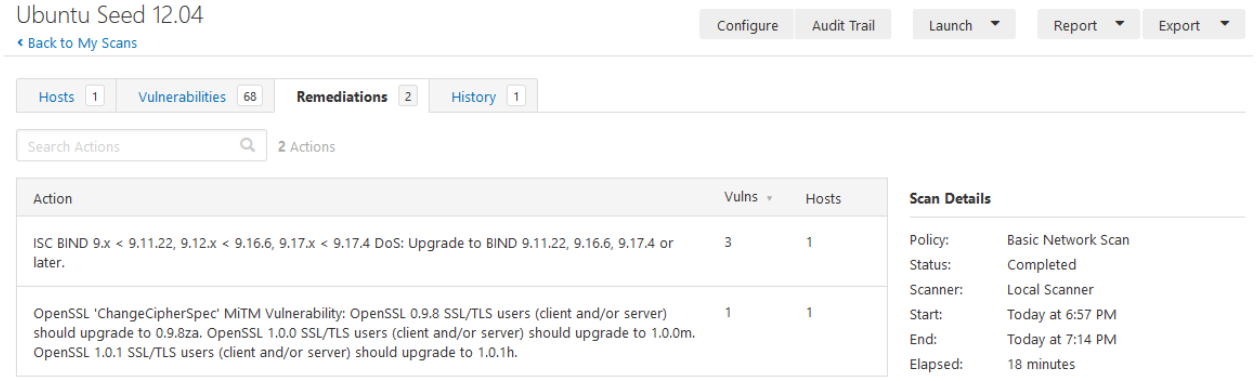


Εικόνα 1. Η διαχειριστική επιφάνεια μέσω φυλλομετρητή του Nessus κατά τη διαδικασία της σάρωσης της ευπαθούς εικονικής μηχανής με εγκατεστημένο Ubuntu Seed 12.04

Προκειμένου να ελέγξουμε τις δυνατότητες που διαθέτει το Nessus, πραγματοποιήσαμε διαδοχικούς ελέγχους στην υποδομή που δημιουργήσαμε, την οποία μπορούμε να δούμε στην εικόνα 10. Στην εικόνα 1 βλέπουμε τη διαχειριστική επιφάνεια του Nessus, μέσω φυλλομετρητή, κατά τη διαδικασία της σάρωσης της ευπαθούς εικονικής μηχανής με εγκατεστημένο Ubuntu Seed 12.04. Στην εικόνα 2 φαίνεται η αναφορά που προέκυψε μετά την ολοκλήρωση ενός Basic Network Scan καθώς και τις προτάσεις για αποκατάσταση των ευπαθειών που εντοπίστηκαν από το Nessus (εικόνα 3).



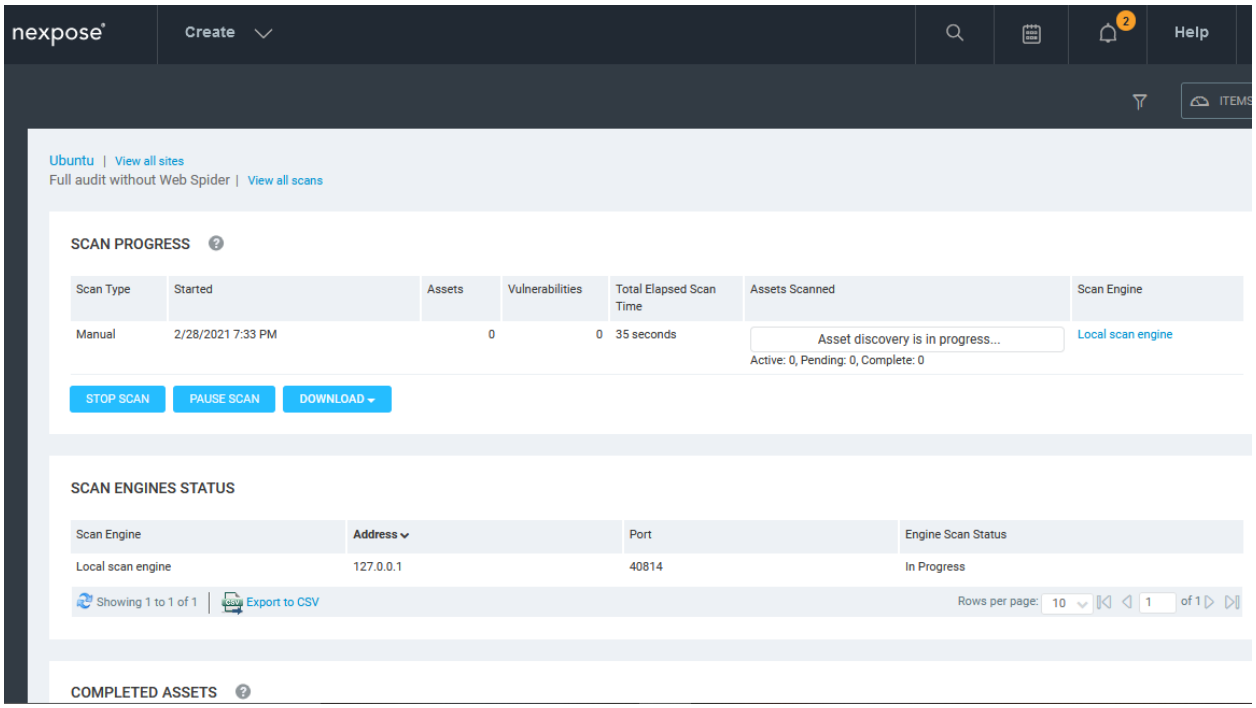
Εικόνα 2. Η αναφορά που δημιούργησε το Nessus μετά την ολοκλήρωση του Basic Network Scan



Εικόνα 3. Οι προτάσεις για αποκατάσταση των ευπαθειών που ανιχνεύθηκαν

2.3 Nexpose

Το Nexpose της Rapid7[26] είναι ένα εργαλείο εντοπισμού ευπαθειών, το οποίο έχει ως στόχο να μπορεί να υποστηρίξει όλο τον κύκλο ζωής της διαχείρισης ευπαθειών, περιλαμβάνοντας την ανίχνευση, τον εντοπισμό, την επαλήθευση, την ανάλυση αντίκτυπου, την αναφορά αλλά και τον μετριασμό των ευπαθειών. Παράλληλα μπορεί να ενοποιείται με το Metasploit της Rapid7 για την εκμετάλλευση των εκάστοτε ευπαθειών που εντοπίστηκαν. Προκειται καθαρά για εμπορικό προϊόν και πωλείται είτε ως αυτόνομο λογισμικό / εικονική μηχανή / συσκευή είτε ως διαχειριζόμενη υπηρεσία. Η διαχείριση του γίνεται μέσω web browser. Να σημειώσουμε πως υπάρχει μια δωρεάν αλλά αρκετά περιορισμένη έκδοση για την κοινότητα την οποία και χρησιμοποιήσαμε.

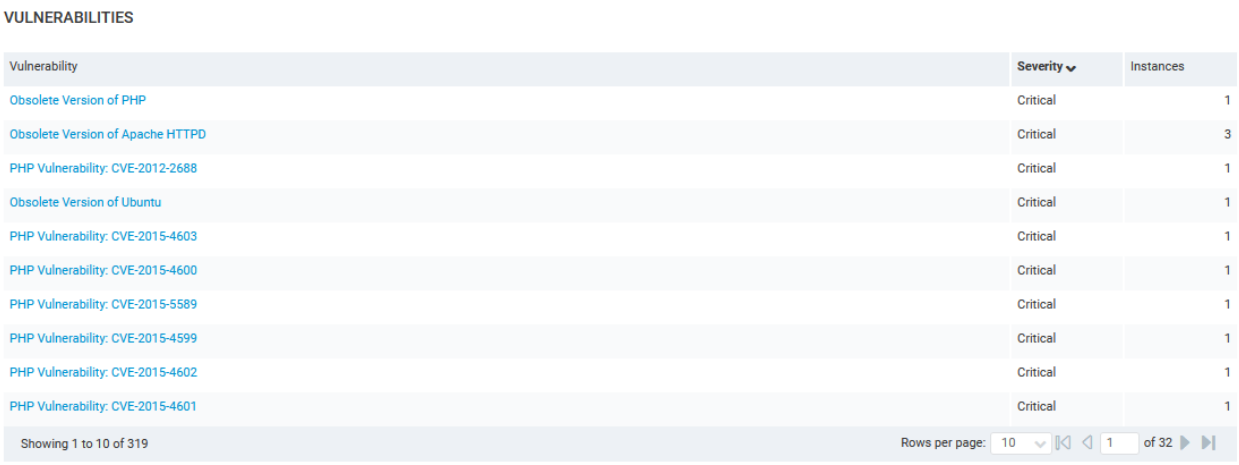


Εικόνα 4. Η διαχειριστική επιφάνεια κατά τη σάρωση του Ubuntu Seed με το Nexpose σε full audit mode

Προκειμένου να ελέγξουμε τις δυνατότητες που διαθέτει το Nexpose, πραγματοποιήσαμε διαδοχικούς ελέγχους στην υποδομή που δημιουργήσαμε, την

[26] https://www.rapid7.com/products/nexpose/

οποία μπορούμε να δούμε στην εικόνα 10. Στα στιγμιότυπα οθόνης που μπορούμε να δούμε στις εικόνες 4 και 5 περιλαμβάνεται η διαχειριστική επιφάνεια του Nexpose κατά τη σάρωση του Ubuntu Seed σε Full Audit mode καθώς και η αναφορά που προέκυψε και περιλαμβάνει όλες τις ευπάθειες που ανιχνεύθηκαν από το εργαλείο. Το Nexpose παρέχει τη δυνατότητα εξαγωγής των αναφορών σε μορφή CSV, αυτό καθιστά εφικτή τη διασύνδεση του – με χρήση του κατάλληλου προσαρμογέα – με το εργαλείο αυτομάτων ειδοποιήσεων και αναφορών που δημιουργήσαμε του οποίου τη λειτουργικότητα αναλύουμε παρακάτω.



VULNERABILITIES

Vulnerability	Severity	Instances
Obsolete Version of PHP	Critical	1
Obsolete Version of Apache HTTPD	Critical	3
PHP Vulnerability: CVE-2012-2688	Critical	1
Obsolete Version of Ubuntu	Critical	1
PHP Vulnerability: CVE-2015-4603	Critical	1
PHP Vulnerability: CVE-2015-4600	Critical	1
PHP Vulnerability: CVE-2015-5589	Critical	1
PHP Vulnerability: CVE-2015-4599	Critical	1
PHP Vulnerability: CVE-2015-4602	Critical	1
PHP Vulnerability: CVE-2015-4601	Critical	1

Showing 1 to 10 of 319 Rows per page: 10 1 of 32

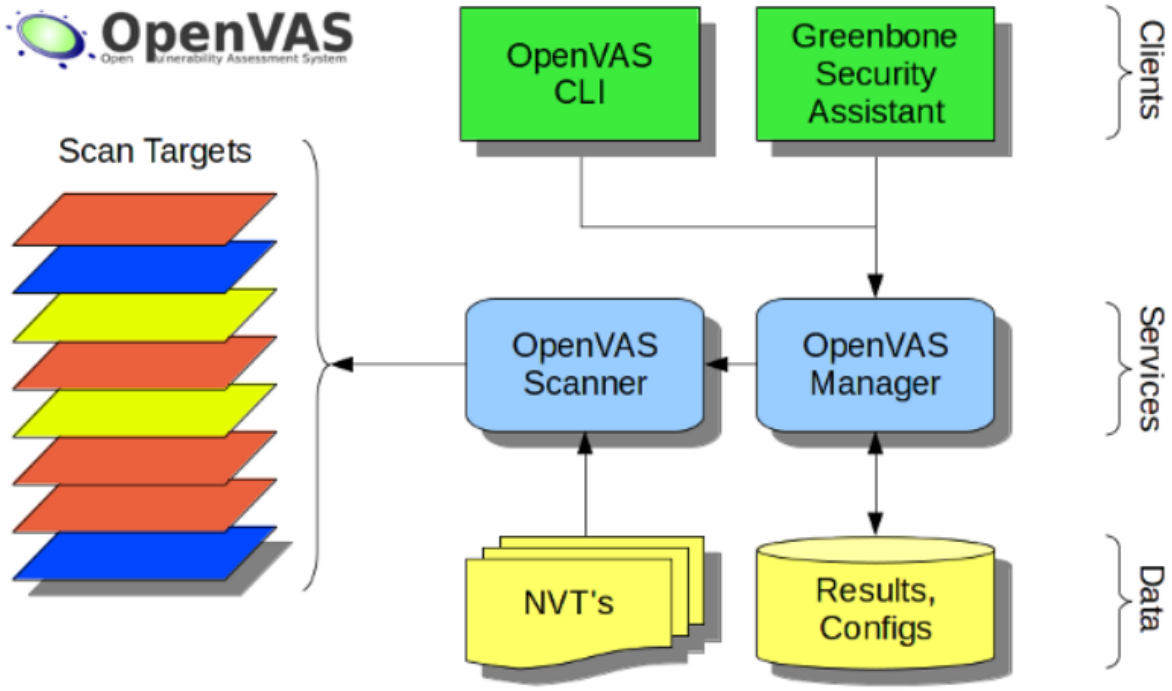
Εικόνα 5. Οι πιο κρίσιμες ευπάθειες που ανιχνεύθηκαν με τη χρήση του Nexpose

2.4 OpenVAS

Το OpenVAS (Open Vulnerability Assessment System), αρχικά γνωστό ως GNessUs)[27] είναι ένα πλαίσιο λογισμικού που παρέχει πολλαπλές υπηρεσίες και εργαλεία που προσφέρουν τη δυνατότητα για έλεγχο και διαχείριση ευπαθειών σε ένα σύστημα.

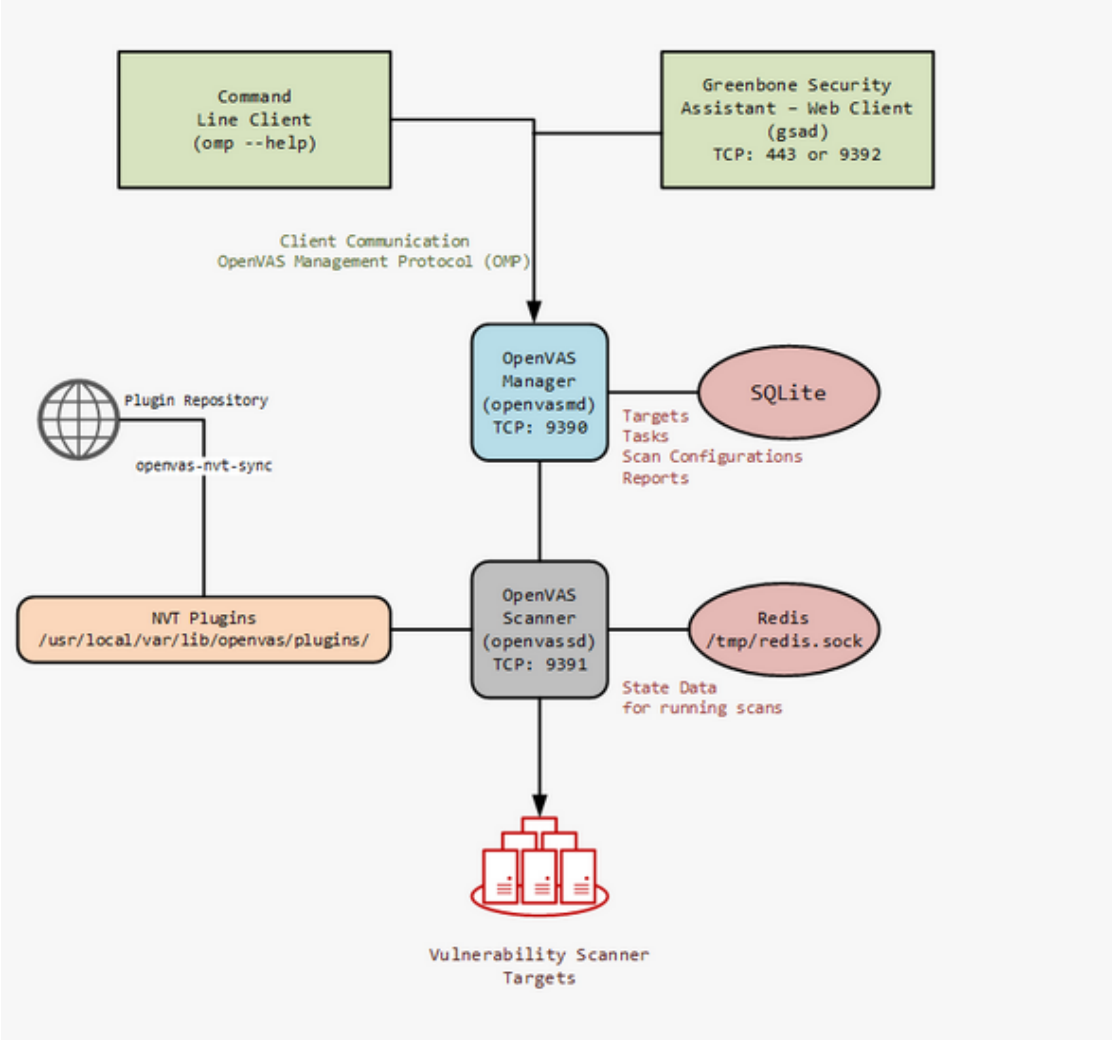
[27] https://www.openvas.org/#about

Όλα τα προϊόντα του OpenVAS είναι ελεύθερου λογισμικού και τα περισσότερα μέρη τους είναι υπό την άδεια GPL (GNU General Public License). Οι πρόσθετες λειτουργικότητες (plugins) γραμμένα σε NASL (Nessus Attack Scripting Language).



Εικόνα 6. Διάγραμμα της λειτουργικότητας του OpenVAS

Το OpenVAS ξεκίνησε υπό το όνομα GNessus, ως παρακλάδι του εργαλείου ανίχνευση ευπαθειών Nessus, το οποίο παλαιότερα ήταν open source, μέχρις ότου οι προγραμματιστές της Tenable Network Security μετέτρεψαν την ιδιότητα του σε ιδιόκτητη (κλειστού κώδικα) τον Οκτώβριο του 2005. Το OpenVas αρχικά προτάθηκε από pentesters στο SecuritySpace, συζητήθηκε στο Portcullis Computer Security και ανακοινώθηκε από τον Tim Brown στο Slashdot. Επιπλέον το OpenVAS συμμετέχει στο project “Software in the Public Interest”.

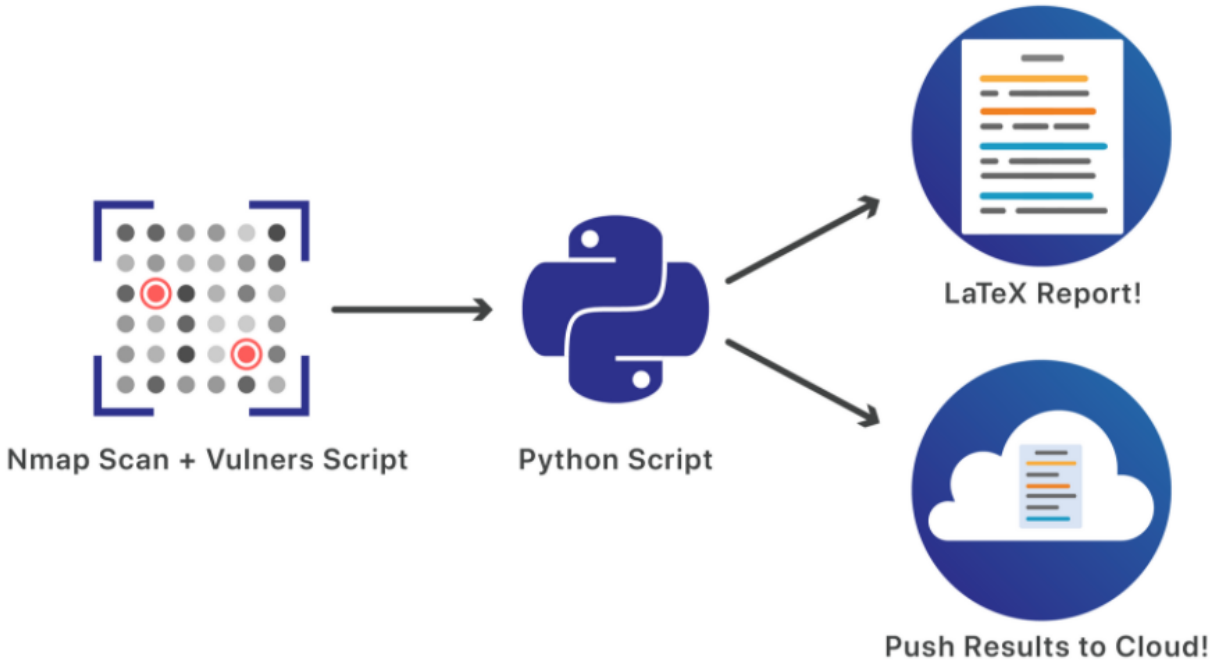


Εικόνα 7. Απεικόνιση τη διασύνδεσης μεταξύ των οντοτήτων που απαρτίζουν τη σάρωση με το OpenVAS

Στις επόμενες ενότητες αναλύουμε τον τρόπο με τον οποίο έγινε η διασύνδεση του OpenVAS με το εργαλείο μας με χρήση προσαρμογών. Πραγματοποιούμε σαρώσεις στην υποδομή της εικόνας 10 που δημιουργήσαμε και βλέπουμε τις δυνατότητες παρέχει ως προς την ανίχνευση ευπαθειών.

2.5 Flan Scan

Το Flan Scan είναι το open source εργαλείο που ανέπτυξε η Cloudflare για τον εντοπισμό ευπαθειών σε ένα δίκτυο.[28] Το Flan Scan είναι ένα ελαφρύ περιτύλιγμα γύρω από το Nmap, το οποίο το μετατρέπει σε εργαλείο εντοπισμού ευπαθειών και διαθέτει το πλεονέκτημα της ευκολίας στην υλοποίηση.



Εικόνα 8. Τα μέρη που συγκροτούν το Flan Scan

Σε αντίθεση με άλλα εργαλεία εντοπισμού ευπαθειών, το Flan Scan δίνει προτεραιότητα στην ακρίβεια σε σχέση με την ταχύτητα, επικεντρώνεται στο να εντοπίζει υπηρεσίες (services) μειώνοντας έτσι τα false positives. Όπως αναφέρθηκε στην περιγραφή των NSE, υπάρχει η δυνατότητα να εκτελεστούν scripts πάνω στα αποτελέσματα της σάρωσης ενός δικτύου. Το Flan Scan χρησιμοποιεί το script “vulners”, το οποίο διατίθεται στο NSE και το οποίο μπορεί να συσχετίσει τα ανιχνευμένα services με τα σχετικά CVEs.

[28] https://blog.cloudflare.com/introducing-flan-scan/

3. Υλοποίηση

3.1 Ποιες τεχνολογίες χρησιμοποιήσαμε

Για τη διαχείριση του σαρωτή και του ειδοποιητή καθώς και για την ανάλυση και σύγκριση των αποτελεσμάτων των σαρώσεων επιλεχθηκε η γλώσσα προγραμματισμού JavaScript. Κυρίαρχοι λόγοι για αυτή την επιλογή ήταν η event-driven αρχιτεκτονική της πλατφόρμας node.js, η οποία είναι κατάλληλη για την ανάπτυξη κατανεμημένων συστημάτων καθώς και η καλή υποστήριξη του πρωτοκόλλου Websocket που επιτρέπει την ενημέρωση πολλαπλών clients σε πραγματικό χρόνο. Ταυτόχρονα εξαλείφεται η ανάγκη ανάπτυξης native εφαρμογών για κάθε ξεχωριστό λειτουργικό σύστημα χάρη στην ενσωματωμένη υποστήριξη που υπάρχει από τους φυλλομετρητές ιστού. Το σύστημα αποτελείται από δύο οντότητες, τον σαρωτή και τον ειδοποιητή. Οι παραπάνω λειτουργούν εντελώς ανεξάρτητα μεταξύ τους. Η εφαρμογή σχεδιάστηκε γύρω από μια αρχιτεκτονική πρόσθετων, ούτως ώστε να μπορεί να υπάρξει διασύνδεση με τις υπάρχουσες λύσεις με ευκολία. Το κάθε πρόσθετο υλοποιεί την έναρξη της σάρωσης και μια μέθοδο για τη μετατροπή της εξόδου του σαρωτή στην επιθυμητή μορφή. Με αυτή τη λογική υλοποιήθηκαν προσαρμογείς για τα εργαλεια OpenVAS και Nmap - NSE scripts/Flan, τα οποία χρησιμοποιήθηκαν σε αυτήν τη μελέτη.

3.1.1 Πρόσθετα

Όπως αναφέρθηκε παραπάνω, το εργαλείο μας δέχεται ως πρόσθετα μια σειρά από υπάρχουσες λύσεις για ανίχνευση ευπαθειών. Για τις δοκιμές που κάναμε, έγινε χρήση του OpenVAS και των NSE scripts που παρέχονται από το Nmap (που χρησιμοποιούνται από το Flan).

Το OpenVAS το χρησιμοποιήσαμε μέσω του Command line client. Η διαχείριση και η παραμετροποίηση των σαρώσεων με το OpenVAS έγινε μέσω των κατάλληλων flags στο OpenVAS Management Protocol και ενός xml αρχείου (το OMP πλέον θεωρείται ξεπερασμένο, αντικαταστάτης του είναι το GMP - Greenbone Management Protocol). Μέσω της διασύνδεσης του εργαλείου μας με το CLI λοιπόν, πραγματοποιήθηκε η εισαγωγή των διαπιστευτηρίων, των IP διευθύνσεων - στόχων, των δικτυακών

πορτών καθώς και το είδος της σάρωσης που θα πραγματοποιήσει το OpenVAS. Ο σαρωτής του OpenVAS είναι μια μηχανή σάρωσης πλήρης δυνατοτήτων που εκτελεί συνεχόμενους, ενημερωμένους και εκτεταμένους ελέγχους για δικτυακές ευπάθειες (Network Vulnerability Tests - NVTs). Ο τύπος της σάρωσης που επιλέξαμε για τις δοκιμές που κάναμε από τις διαθέσιμες επιλογές που παρέχονται μέσω του CLI ήταν “Full and fast ultimate” και η διάρκεια του ήταν κατα μέσο όρο 26 λεπτά.

Στην περίπτωση των NSE scripts/ Flan, γίνεται μια σάρωση εντοπισμού ανοικτών υπηρεσιών. Η σάρωση που τρέχει περιλαμβάνει ICMP ping scan ώστε να καθοριστεί το ποιες από τις δοθείσες IP διευθύνσεις είναι ενεργές και SYN scan για τη σάρωση των χιλίων κοινών δικτυακών πορτών των IP διευθύνσεων που απάντησαν ώστε να προκύψει ποιες είναι ανοικτές, κλειστές ή φιλτραρισμένες. Στη συνέχεια πραγματοποιείται η σάρωση εντοπισμού υπηρεσιών, για την ανίχνευση των υπηρεσιών που τρέχουν σε ανοικτές δικτυακές πόρτες μέσω της εκτέλεσης TCP χειραψιών και σαρώσεων “banner grabbing”. Παράλληλα, είναι διαθέσιμοι και άλλοι τύποι σαρώσεων όπως σαρώσεις UDP και σαρώσεις για IPv6 διευθύνσεις με τη χρήση των κατάλληλων flags. Επιπλέον, το Flan Scan προσθέτει και το script “vulners” ώστε στην έξοδο του να περιλαμβάνει τη λίστα με τις ευπάθειες που είναι συμβατές με τις υπηρεσίες που ανιχνεύθηκαν. Το vulners, λειτουργεί κάνοντας κλήσεις API σε μια υπηρεσία που τρέχει από το vulners.com και η οποία επιστρέφει όλες τις γνωστές ευπάθειες για την εκάστοτε δεδομένη υπηρεσία.

3.1.2 Κατανεμημένο σύστημα

Ένα κατανεμημένο σύστημα, είναι ένα σύστημα του οποίου τα μέρη είναι τοποθετημένα σε διαφορετικά μηχανήματα τα οποία είναι συνδεδεμένα δικτυακά και τα οποία επικοινωνούν και συντονίζουν τη δράση τους στέλνοντας μηνύματα το ένα στο άλλο. Τα μέρη αλληλεπιδρούν μεταξύ τους προκειμένου να πετύχουν έναν συγκεκριμένο κοινό στόχο. Η ίδια η φύση της εφαρμογής που υλοποιήσαμε απαιτεί τη χρήση ενός δικτύου επικοινωνίας το οποίο συνδέει μια σειρά από υπολογιστές και εικονικές μηχανές καθώς τα δεδομένα που παράγονται από ένα φυσικό ή εικονικό μηχάνημα απαιτούνται σε μια άλλη τοποθεσία.

3.1.3 WebSocket

Το WebSocket είναι ένα πρωτόκολλο επικοινωνίας υπολογιστών το οποίο παρέχει κανάλια αμφίδρομης επικοινωνίας μέσω μιας TCP σύνδεσης. Ως πρωτόκολλο, το WebSocket τυποποιήθηκε από τον IETF το 2011 ως RFC 6455 και το WebSocket API σε Web IDL τυποποιείται από τη W3C.

Το WebSocket είναι ξεχωριστό από το HTTP μολονότι και τα δύο πρωτόκολλα βρίσκονται στο επίπεδο 7 του προτύπου OSI και εξαρτώνται από το TCP που βρίσκεται στο επίπεδο 4 του ίδιου προτύπου. Επιπλέον το WebSocket έχει σχεδιαστεί ώστε να λειτουργεί πάνω από τις πόρτες του HTTP (80, 443) και να υποστηρίζει HTTP ενδιάμεσους κάτι που το καθιστά απολύτως συμβατό με το πρωτόκολλο HTTP. Για να επιτευχθεί αυτή η συμβατότητα, η χειραψία του WebSocket χρησιμοποιεί το HTTP Upgrade header για την αλλαγή από το πρωτόκολλο HTTP στο πρωτόκολλο WebSocket.[29] Παράλληλα, το πρωτόκολλο WebSocket παρέχει τη δυνατότητα αλληλεπίδρασης ανάμεσα σε έναν φυλλομετρητή διαδικτύου (ή άλλη εφαρμογή client) και έναν web server χωρίς το επιπλέον κόστος άλλων λύσεων, διευκολύνοντας την real-time μεταφορά δεδομένων από και προς τον server.

Το WebSocket-Node που χρησιμοποιούμε για την υλοποίηση του εργαλείου μας, περιλαμβάνει λειτουργικότητα για client και server, που είναι διαθέσιμη μέσω της χρήσης των WebSocketClient και WebSocketServer αντίστοιχα.[30] Αφού πραγματοποιηθεί η σύνδεση, το API που στέλνει τα μηνύματα είναι ίδιο είτε στην περίπτωση του client είτε του Server. Το Sockette είναι ένα μικρό (367 bytes) “περιτύλιγμα” γύρω από το WebSocket το οποίο φροντίζει για αυτόματη επανασύνδεση στην περίπτωση που χαθεί η επικοινωνία. Εκτός από την επισύναψη πρόσθετων μεθόδων API, το Sockette μας επιτρέπει να χρησιμοποιήσουμε ξανά instances, χωρίς να χρειάζεται να δηλώσουμε ξανά όλους τους event listeners.[31]

3.1.4 Ειδοποιήσεις

[29] https://developer.mozilla.org/en/WebSockets
[30] https://www.npmjs.com/package/websocket
[31] https://www.npmjs.com/package/sockette

Για την αποστολή των ειδοποιήσεων κάναμε χρήση του Node-Notifier. Ο Node-Notifier είναι συμβατός με Windows, Linux και Mac-OS κάτι που καθιστά εφικτή την αποστολή ειδοποιήσεων ανεξάρτητος του λειτουργικού που είναι εγκατεστημένο στο διαχειριστικό μηχάνημα.[32] Στην υλοποίηση μας, οι ειδοποιήσεις με τα αποτελέσματα των σαρώσεων ή της σύγκρισης μεταξύ διαδοχικών σαρώσεων αποστέλλονται δικτυακά στον client που είναι εγκατεστημένος σε Debian Linux.

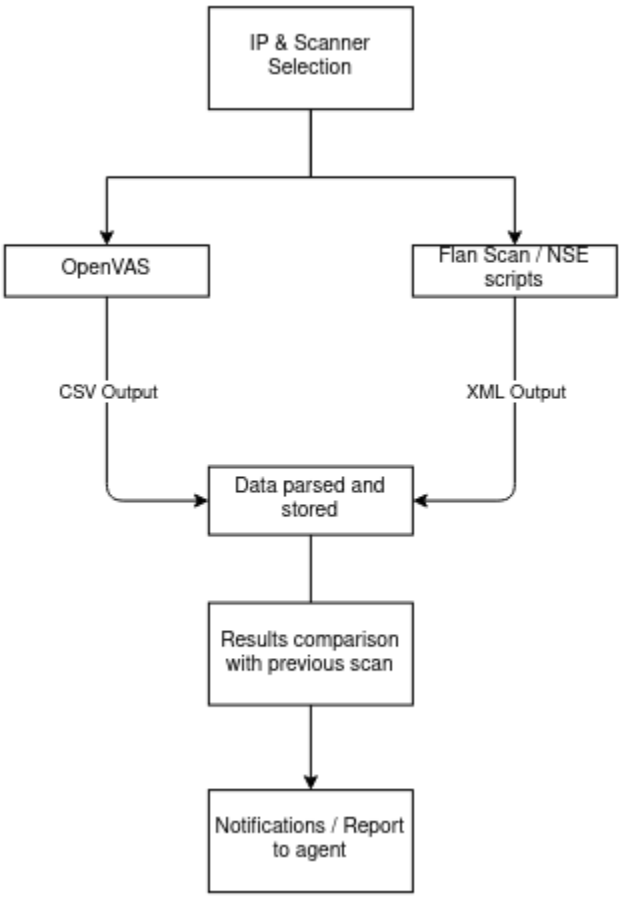
3.2 Λειτουργικότητα

Στο εργαλείο διαχείρισης ευπαθειών που έχουμε υλοποιήσει αρχικά γίνεται επιλογή των IP διευθύνσεων στις οποίες πρόκειται να γίνει σάρωση για ευπάθειες και στη συνέχεια η επιλογή του εργαλείου - σαρωτή με τον οποίο θα γίνουν οι σαρώσεις. Στην περίπτωση που η σάρωση πραγματοποιηθεί μέσω του OpenVAS, το αποτέλεσμα της σάρωση που προκύπτει είναι σε μορφή CSV, στην περίπτωση που η σάρωση πραγματοποιηθεί μέσω των Nmap NSE scripts, το αποτέλεσμα είναι σε μορφή XML.

Αφού προκύψει το αποτέλεσμα της σάρωσης, ανάλογα με τον σαρωτή που χρησιμοποιήθηκε και άρα ανάλογα με τον τύπο του αρχείου, γίνεται η κατάλληλη ανάλυση των αποτελεσμάτων και στη συνέχεια αυτά αποθηκεύονται στο σημείο που έχουμε επιλέξει σε μορφή json. Με την ολοκλήρωση αυτής της διαδικασίας αποστέλλονται δικτυακά οι ειδοποιήσεις με τα αποτελέσματα στην IP διεύθυνση που έχει οριστεί.

Μόλις πραγματοποιηθεί νέα σάρωση, ανεξάρτητα από το εργαλείο που έχουμε επιλέξει, διεξάγεται σύγκριση των αποτελεσμάτων της με αυτά της προηγούμενης και αποστέλλεται νέα ειδοποίηση που αυτή τη φορά περιλαμβάνει τα αποτελέσματα της σύγκρισης.

[32] https://www.npmjs.com/package/node-notifier



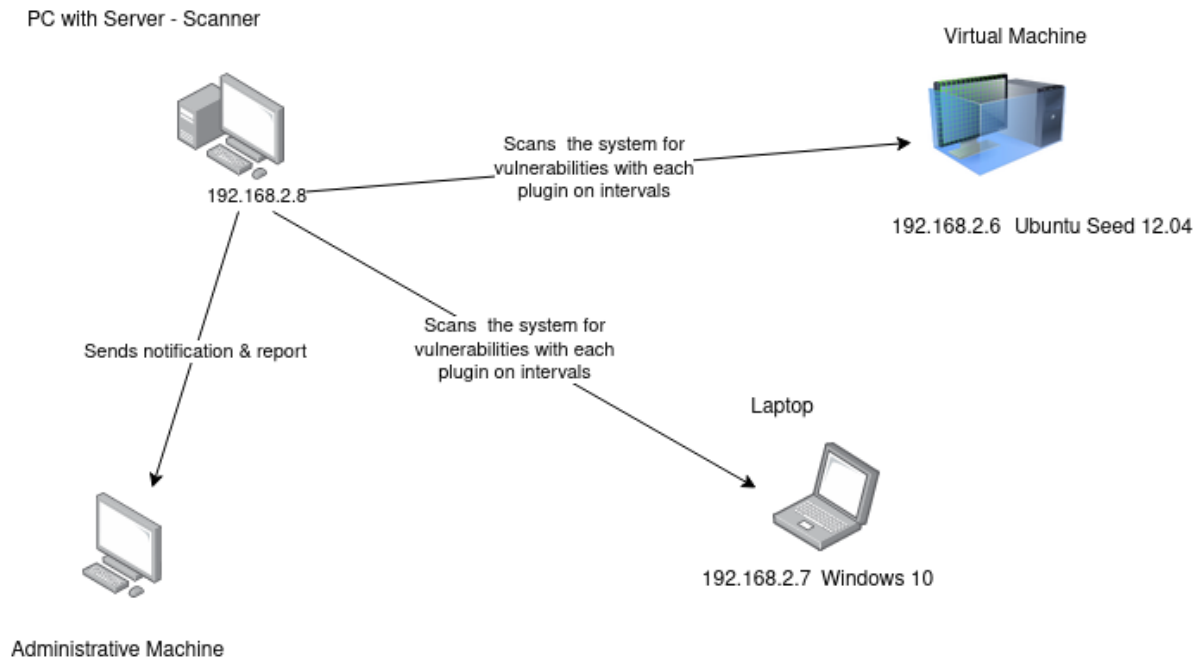
Εικόνα 9. Διάγραμμα λειτουργίας του εργαλείου διαχείρισης ευπαθειών που υλοποιήσαμε

3.3 Η υποδομή όπου έγιναν οι δοκιμές

Προκειμένου να πραγματοποιήσουμε δοκιμές ώστε να κάνουμε σύγκριση ανάμεσα στα Vulnerability scanner/ plugins στο auto reporting εργαλείο που υλοποιήσαμε, δημιουργήσαμε ένα περιβάλλον το οποίο αποτελείται από ένα φυσικό σύστημα με Debian Linux στο οποίο τρέχει το εργαλείο μας, ένα φυσικό σύστημα με Debian Linux το οποίο να δέχεται τις ειδοποιήσεις και τις αναφορές, μια σειρά από Ubuntu Seed

labs τα οποία στήσαμε σε εικονικές μηχανές στο VMware, καθώς επίσης και ένα πλήρως ενημερωμένο Windows 10 και αυτό εγκατεστημένο σε φυσικό μηχάνημα.

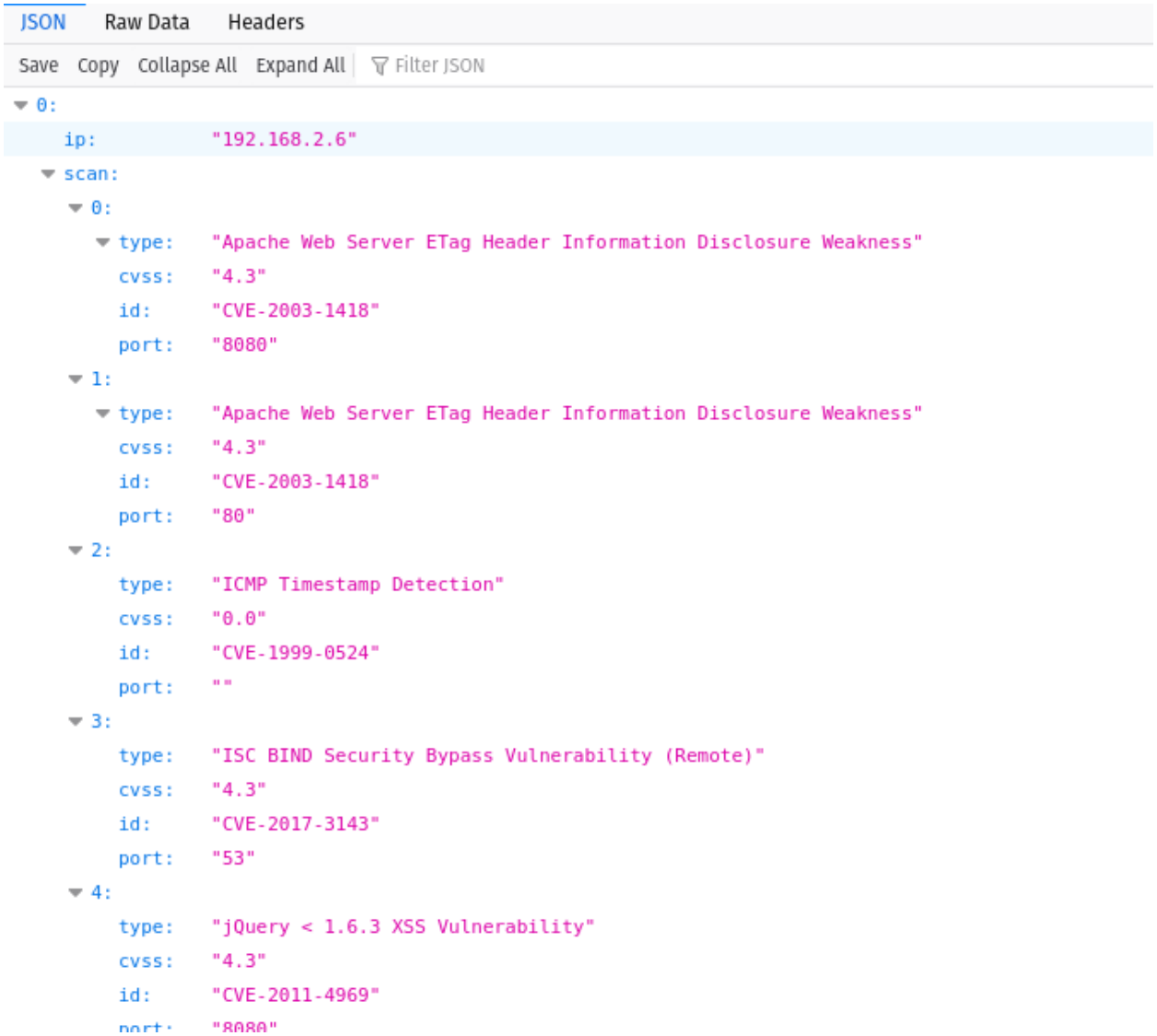
Η παραπάνω υποδομή δημιουργήθηκε ώστε να καταστεί εφικτή η σάρωση οντοτήτων οι οποίες να έχουν αρκετές ευπάθειες (π.χ. Ubuntu Seed 12.04) και η σάρωση οντοτήτων στις οποίες να έχει γίνει περιορισμός των ευπαθειών (Windows 10) ώστε να προκύψει μια συνολικότερη εικόνα για την αξιοπιστία της διαχείρισης ευπαθειών που γίνεται μέσω του εργαλείου μας.



Εικόνα 10. Η υποδομή που δημιουργήθηκε για τις δοκιμές που πραγματοποιήθηκαν

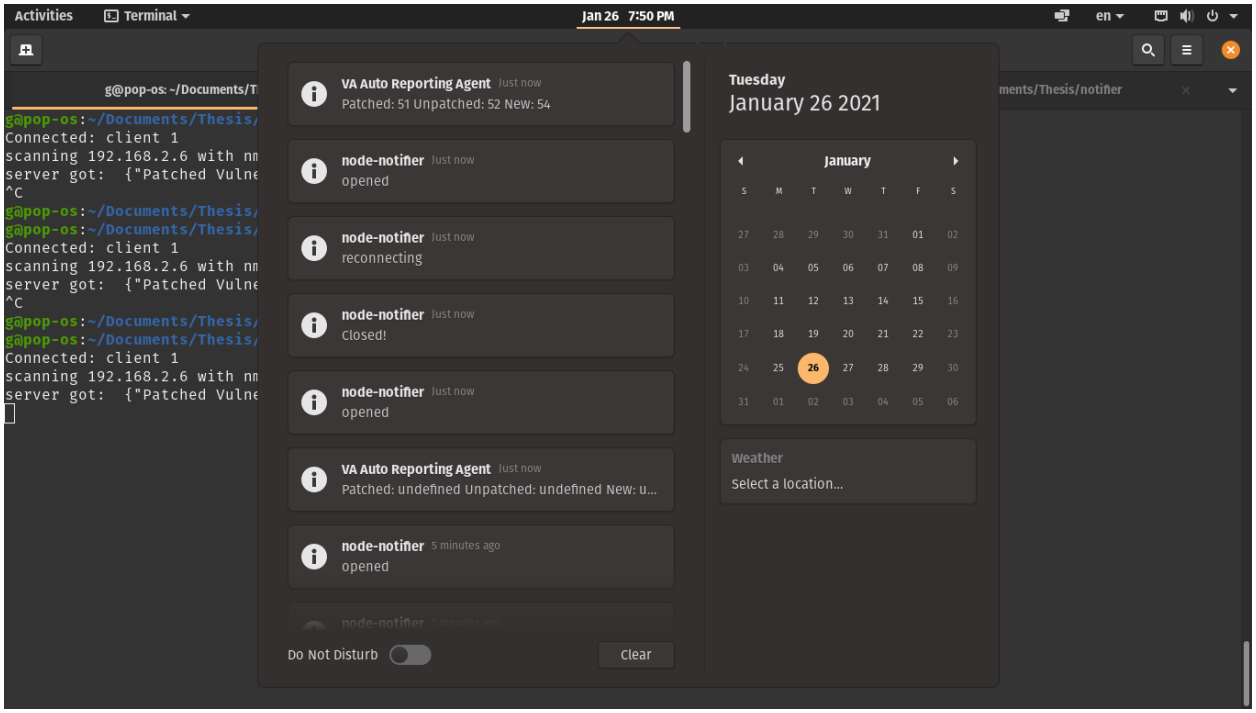
3.4 Σαρωση με το OpenVAS

Στο εργαλείο πραγματικού χρόνου που δημιουργήσαμε, το OpenVAS εισάγεται ως πρόσθετο με την κατάλληλη παραμετροποίηση. Πραγματοποιήσαμε σάρωση αρχικά του συστήματος Ubuntu Seed χρησιμοποιώντας το εργαλείο που υλοποιήσαμε αρχικά με το OpenVAS ως plug-in ώστε να προκύψει η λίστα με τις ευπάθειες του συστήματος και να σταλεί ειδοποίηση στον διαχειριστή του συστήματος προκειμένου αυτός να λάβει τα κατάλληλα μέτρα για την αντιμετώπιση τους. Μετά την ολοκλήρωση του ελέγχου δημιουργείται ένα αρχείο json το οποίο μπορεί ο διαχειριστής να δει στον φυλλομετρητή του, ανοίγοντας την ειδοποίηση - που λειτουργεί πρακτικά ως υπερσύνδεσμος - που εμφανίστηκε στο σύστημα του και η οποία του εστάλη δικτυακά.



Εικόνα 12. Το json αρχείο αναφοράς που προέκυψε από τη σάρωση με το OpenVAS και περιλαμβάνει την IP διεύθυνση - στόχο και στοιχεία για την κάθε ευπάθεια που ανιχνεύθηκε

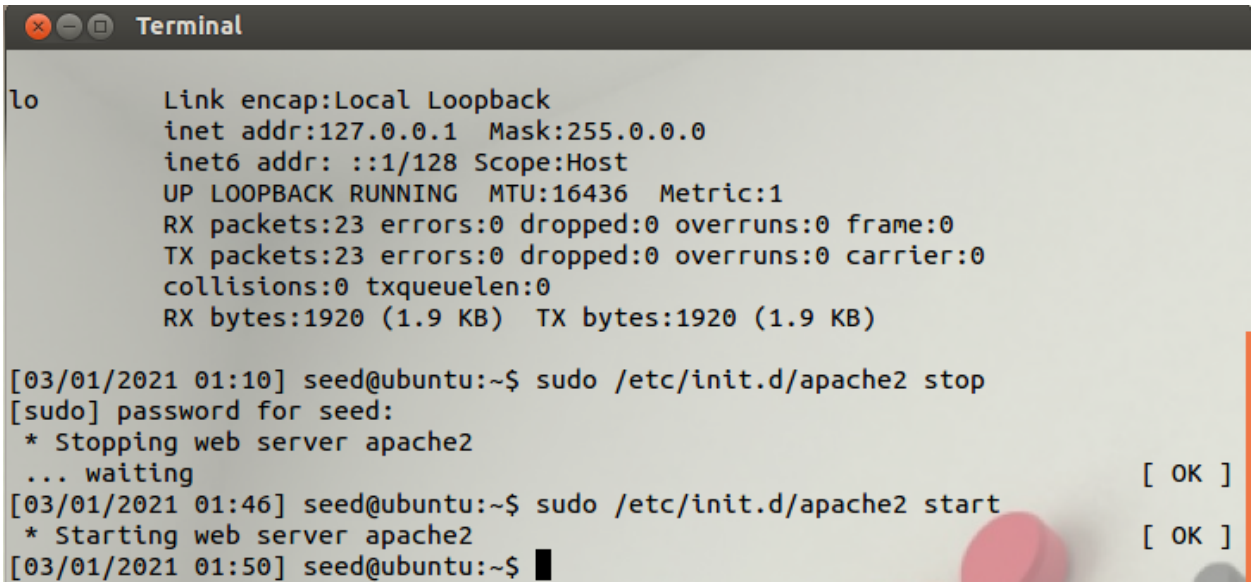
Στη συνέχεια λαμβάνει χώρα ο αμέσως επόμενα προγραμματισμένος έλεγχος ευπαθειών για το ίδιο σύστημα, ο οποίος βρίσκει το σύστημα τροποποιημένο καθώς περιορίστηκε ο αριθμός των ευπαθειών σε αυτό τερματίζοντας μια ευπαθή υπηρεσία. Προκύπτουν λοιπόν σε μορφή json η αναφορά που περιλαμβάνει τις ευπάθειες που υπάρχουν αυτή τη στιγμή στο σύστημα όπως φαίνεται στην εικόνα , αλλά και η νέα ειδοποίηση στον διαχειριστικό τερματικό σημείο με τις ευπάθειες που παραμένουν στο σύστημα, τις νέες ευπάθειες που προέκυψαν αλλά και τις ευπάθειες που έχουν πάψει να υπάρχουν από την τελευταία σάρωση του.



Εικόνα 13. Ειδοποιήσεις που περιλαμβάνουν την κατάσταση του ειδοποιητή αλλά και τις αναφορές που δημιουργήθηκαν μετά από πολλαπλές σαρώσεις

Κατά τη σάρωση του πλήρως ενημερωμένου και θωρακισμένου δικτυακά Windows 10 συστήματος δεν προέκυψαν ευπάθειες στις σχετικές αναφορές και ειδοποιήσεις. Να σημειώσουμε πως οι σαρώσεις και των δύο συστημάτων με το OpenVAS ήταν πολύ πιο χρονοβόρες σε σχέση με αυτές όπου έγινε χρήση των NSE scripts (είτε απευθείας, είτε μέσω του Flan). Κάτι που προκύπτει και από τον όγκο που έχουν οι σχετικές αναφορές σε σχέση με τις αντίστοιχες των NSE scripts. Το παραπάνω

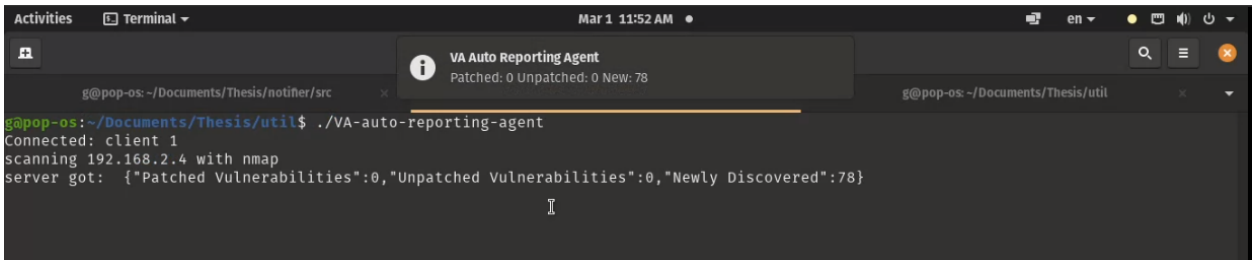
συνέβη γιατί το OpenVAS ελέγχει το κάθε σύστημα σε μεγαλύτερο βάθος διεξάγοντας περί τα 50.000 NVTs (Network Vulnerability Tests) σε σχέση με τους πιο βασικούς δικτυακούς ελέγχους που πραγματοποιούν το Flan με τα NSE scripts.



Εικόνα 14. Παύση και εκκίνηση υπηρεσιών στο Ubuntu Seed ανάμεσα στις διαδοχικές σαρώσεις για τη δημιουργία διαφορετικών αναφορών από το εκάστοτε εργαλείο

3.5 Σάρωση με χρήση των NSE scripts & Flan

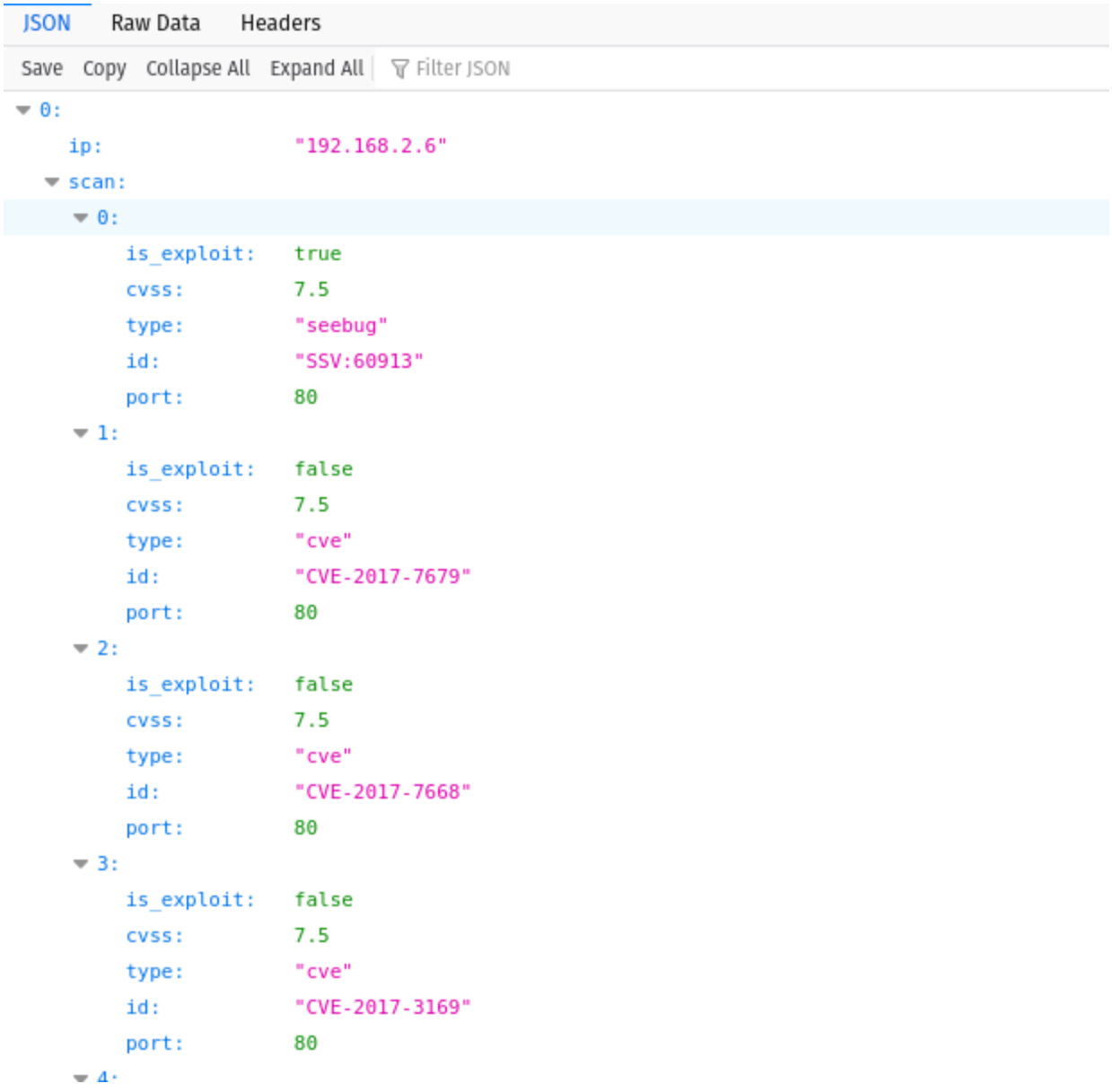
Αφού αλλάξαμε την παραμετροποίηση, πραγματοποιήσαμε σαρώσεις κάνοντας χρήση των NSE Scripts που παρέχονται από το Nmap. Οι σαρώσεις αυτές πραγματοποιήθηκαν αρκετά γρήγορα (είχαν διάρκεια μόλις λίγων λεπτών) και αυτός ήταν και ο λόγος που επιλέξαμε τη συγκεκριμένη λύση, είναι ελαφριά και γρήγορη κι έτσι μπορούμε να κάνουμε τις δοκιμές μας πολύ πιο σύντομα. Μετά την πρώτη σάρωση προέκυψε η αναφορά σε μορφή json και εστάλη ειδοποίηση στον σταθμό εργασίας που προεπιλέξαμε, η οποία ανέφερε τον αριθμό των ευπαθειών στο σύστημα.



Εικόνα 15. Η ειδοποίηση που προκύπτει μετά την ολοκλήρωση της σάρωσης με χρήση των NSE scripts. Επιλέγοντας την ειδοποίηση μπορούμε να δούμε την αναφορά που έχει δημιουργηθεί

Ακολούθως πραγματοποιήθηκε η επόμενη σάρωση, της οποίας τα αποτελέσματα αναλύθηκαν και συγκρίθηκαν με αυτά της προηγούμενης. Προέκυψε λοιπόν ένα νέο αρχείο json το οποία περιείχε τις νέες ευπάθειες που βρέθηκαν στο σύστημα (πρώτα στο Ubuntu Seed 12.04 και ύστερα στο Windows 10) και αυτές που δεν είχαν κλείσει από την προηγούμενη σάρωση. Τέλος εστάλη η νέα ειδοποίηση στον διαχειριστικό τερματικό σημείο με τις ευπάθειες που παραμένουν στο σύστημα, τις νέες ευπάθειες που προέκυψαν αλλά και τις ευπάθειες που έχουν πάψει να υπάρχουν από την τελευταία σάρωση του.

Εικόνα 11. Καταγραφή της δραστηριότητας του σαρωτή στον server, που χρησιμοποιήθηκε για εκσφαλμάτωση της πρώτης σάρωσης του Ubuntu Seed



Εικόνα 16. Το json αρχείο αναφοράς που προέκυψε από την αμέσως επόμενη σάρωση με χρήση των Nmap NSE scripts / Flan Scan όπου πραγματοποιήθηκε αποκατάσταση κάποιων ευπαθειών που βρέθηκαν στην προηγούμενη σάρωση

Να σημειώσουμε πως οι αναφορές ευπαθειών που προέκυψαν τόσο για το Ubuntu Seed, όσο και για το Windows 10 σύστημα χρησιμοποιώντας ως επιπρόσθετο το Flan ήταν ακριβώς ίδιες με αυτές που προέκυπταν με τη σάρωση μέσω των NSE scripts.

Αυτό προφανώς συμβαίνει επειδή ακριβώς η λειτουργία σάρωσης του Flan βασίζεται στα ίδια scripts που παρέχονται από το Nmap.

4. Συμπεράσματα

Σε αυτή την εργασία, μελετήσαμε το υπάρχον οικοσύστημα των ευπαθειών και πειραματιστήκαμε με μια σειρά από εργαλεία σάρωσης ευπαθειών (ανοικτού κώδικα αλλά και εμπορικά). Υλοποιήσαμε ένα εργαλείο το οποίο συμβάλλει στην διαχείριση των ευπαθειών. Μπορεί να δέχεται πολλαπλούς σαρωτές ευπαθειών ως πρόσθετα και να πραγματοποιεί με αυτούς περιοδικούς ελέγχους σε συστήματα. Αρχικά γίνεται επιλογή του σαρωτή και των IP διευθύνσεων-στόχων. Τα αποτελέσματα των εκάστοτε ελέγχων κατακερματιζονται και συγκρίνονται - κάθε φορά με τα προηγούμενα - ώστε να να προκύπτουν ουσιαστικά οι νέες ευπάθειες που βρέθηκαν στο σύστημα, καθώς επίσης και οι ευπάθειες που συνεχίζουν να υπάρχουν από την προηγούμενη σάρωση, εφόσον δεν έχει ληφθεί μέριμνα για την εξάλειψη τους.

Από τις δοκιμές που πραγματοποιήσαμε προέκυψε πως με τη χρήση των λύσεων ανοικτού λογισμικού, τα αποτελέσματα ανάμεσα στις διαφορετικές λύσεις φάνηκαν να έχουν πολλές διαφορές στις ευπάθειες που ανακάλυπταν εξαιτίας της διαφοράς τόσο στους ελέγχους όσο και στις πηγές που χρησιμοποιεί το καθένα. Το παραπάνω είχε ως αποτέλεσμα, να μη μπορεί να προκύψει μια αξιόπιστη σύγκριση μεταξύ των αποτελεσμάτων από τα διαφορετικά εργαλεία. Σε κάθε περίπτωση, το συγκεκριμένο εργαλείο βοηθά στη διαχείριση ευπαθειών καθώς μας προσφέρει τη δυνατότητα σύγκρισης μεταξύ των αποτελεσματων από το ίδιο εργαλείο.

5. Μελλοντική δουλειά

Εφόσον το εργαλείο διαχείρισης ευπαθειών που δημιουργήσαμε δέχεται σαρωτές ευπαθειών ως πρόσθετα, σκοπεύουμε να δούμε τη λειτουργικότητα του αν διασυνδεθεί και με άλλες λύσεις. Επιπροσθέτως, θα θέλαμε να υλοποιήσουμε στο

αμέσως επόμενο διάστημα ένα ασφαλές περιβάλλον χρήστη μέσω φυλλομετρητή - πέραν αυτού των ειδοποιήσεων - για τη διαχείριση του εργαλείου καθώς επίσης και την αυτόματη αντιστοίχιση των ευπαθειών που προκύπτουν από την κάθε σάρωση με ένα πλάνο αποκατάστασης τους στο οποίο ο χρήστης να μπορεί να συνδεθεί μέσα από έναν σύνδεσμο.

Το περιβάλλον χρήστη θα συμβάλλει στην πιο εύκολη παραμετροποίηση του εργαλείου και κατ’ επέκταση στην επιτάχυνση της διαδικασίας των δοκιμών με στόχο την περαιτέρω ανάπτυξη του ώστε να μας παρέχει περισσότερες λειτουργικότητες. Παράλληλα, το πλάνο αποκατάστασης θα συμβάλλει στον εύκολη πρόσβαση στη μεθοδολογία εξάλειψης των ευπαθειών από τον χρήστη και μπορεί να προστεθεί και αυτό ως πρόσθετο παρόμοια με τους σαρωτές ώστε πάλι να γίνει αξιοποίηση των υπαρχουσών λύσεων.

Ο στόχος που παραμένει, είναι η συλλογή - μέσω του εργαλείου μας - των διαφορετικών ευπαθειών που προκύπτουν από τα διαφορετικά προγράμματα σάρωσης, να μπορέσουν να ενοποιηθούν σε μια ενιαία αναφορά ώστε να υπάρχει ένας πιο ολοκληρωμένος έλεγχος για τα τρωτά σημεία της εκάστοτε υποδομής όπου γίνεται η σάρωση.

Επιπλέον σκοπεύουμε να προσθέσουμε και μια γραφική απεικόνιση, που να περιλαμβάνει στατιστικά και γραφήματα με τα ευρήματα των εκτιμήσεων επικινδυνότητας που πραγματοποιούνται.

ΑΝΑΦΟΡΕΣ

1. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
2. https://nvd.nist.gov/vuln
3. https://cve.mitre.org/cve/cna/rules.html#section_7-1_what_is_a_vulnerability
4. https://cve.mitre.org/about/history.html
5. https://cve.mitre.org/cve/cna/
6. https://www.first.org/cvss/
7. https://www.beyondtrust.com/resources/glossary/vulnerability-assessment
8. https://www.imperva.com
9. Arbaugh, W., Fithen, W., McHugh, J. Windows of Vulnerability: A Case Study Analysis. IEEE Computer, Vol 3, No. 12, December 2000
10. National Institute of Standards and Technology (September 2008). "Technical Guide to Information Security Testing and Assessment" (PDF). *NIST*
11. ENISA, Good Practice Guide for Vulnerability Disclosure: From Challenges to recommendations, 2015 https://www.enisa.europa.eu/publications/vulnerability-disclosure
12. ENISA, State of Vulnerabilitites 2018/2019: Analysis of Events in the life of Vulnerabilities, December 2019
13. https://nvd.gov/
14. https://attack.mitre.org/
15. https://www.shodan.io/
16. https://www.exploit-db.com/about-exploit-db
17. https://cve.mitre.org

18. https://zerodayinitiative/
19. https://threatconnect.com/
20. https://vulndb.com/
21. https://www.us-cert.gov/
22. https://zerodium.com
23. https://sectools.org/tag/vuln-scanners/
24. https://nmap.org/book/man-nse.html
25. https://www.tenable.com/products/nessus
26. https://www.rapid7.com/products/nexpose/
27. https://www.openvas.org/#about
28. https://blog.cloudflare.com/introducing-flan-scan/
29. https://developer.mozilla.org/en/WebSockets
30. https://www.npmjs.com/package/websocket
31. https://www.npmjs.com/package/sockette
32. https://www.npmjs.com/package/node-notifier

ΠΑΡΑΡΤΗΜΑ

Α. Βάσεις δεδομένων ελεύθερης πρόσβασης

https://exchange.xforce.ibmcloud.com/
https://www.securityfocus.com/vulnerabilities/
https://nvd.nist.gov/
https://www.cvedetails.com/
https://vuldb.com/
https://www.exploit-db.com/
https://www.rapid7.com/db/
https://snyk.io/features/vulnerability-database/
https://www.kb.cert.org/vuls/
https://www.first.org/global/sigs/vrdx/vdb-catalog
https://help.veracode.com/reader/hHHR3gv0wYc2WbCclECf_A/lQYKhC8AvpIbz5_ULOCYMw
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
https://www.cerias.purdue.edu/site/about/history/coast/projects/vdb.php
https://wpvulndb.com
https://packetstormsecurity.com/
http://cve.mitre.org/
https://0day.today/
https://www.misp-project.org/features.html
https://cert.europa.eu/cert/newsletter/en/latest_SecurityBulletins_.html
http://www.cnnvd.org.cn/
https://www.us-cert.gov/ics/advisories
https://jvn.jp/en/
https://www.kyberturvallisuuskeskus.fi/en/homepage
https://securiteam.com/
https://securitytracker.com/
https://www.zerodayinitiative.com/advisories/published/
https://www.vulnspy.com/
https://github.com/AUEB-BALab/VulinOSS
https://oval.cisecurity.org/
https://seclists.org/fulldisclosure/
https://www.seebug.org/

https://cxsecurity.com/
https://en.0day.today/
https://developer.shodan.io/api/exploits/rest
https://www.talosintelligence.com/
https://www.us-cert.gov/ncas/bulletins
https://github.com/0x4D31/awesome-threat-detection
https://www.zerodayinitiative.com/advisories/published/
https://www.zerodayinitiative.com/advisories/upcoming/

Β. Εμπορικές βάσεις δεδομένων

https://www.symantec.com/services/cyber-security-services/deepsight-intelligence
https://vulndb.cyberriskanalytics.com/
https://www.flexera.com/products/operations/software-vulnerability-management.html
https://www.accenture.com/us-en/blogs/blogs-vulnerability-intelligence
https://www.auscert.org.au/services/security-bulletins/
https://www.synopsys.com/software-integrity/security-testing/software-compositionanalysis/technology/vulnerability-reporting.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/Application_Detectors/library-vdb/fpapp-detectors-library.html
https://www.manageengine.com/vulnerability-management/help/vulnerability-database settings.html