ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διδάσκων: Επίκουρος Καθηγητής Γεώργιος Καμπουράκης
Εργαστηριακοί Συνεργάτες: Δημήτρης Παπαμαρτζιβάνος (ΥΔ), Αλέξανδρος Φακής (ΥΔ)

Ασφάλεια Δικτύων Υπολογιστών

και Τεχνολογίες Προστασίας της Ιδιωτικότητας

3η Εργαστηριακή Άσκηση

Νοέμβριος 2016

ΑΣΚΗΣΗ 2

Penetration testing, Hardening, L7 Firewalls, Hacking tournament

Περιγραφή

Σκοπός της παρούσας άσκησης είναι η γνωριμία και εξοικείωση με εργαλεία διείσδυσης και ενδυνάμωσης πληροφορικών συστημάτων, αναχώματα ασφάλειας επιπέδου εφαρμογής, καθώς και ο έλεγχος ασφάλειας δικτυακών εφαρμογών. Στο πλαίσιο της εργασίας καλείστε να επιτεθείτε σε ένα υπολογιστικό σύστημα αλλά και να ανιχνεύσετε αυτές τις επιθέσεις. Επιπλέον, καλείστε να υλοποιήσετε ένα σενάριο διαχείρισης δικτυακής κίνησης ενός «εταιρικού» δικτύου κάνοντας χρήση ενδιάμεσου εξυπηρετητή (SOCKS proxy server) και εργαλείων Deep Packet Inspection (DPI).

Η 3η εργασία χωρίζεται σε 3 φάσεις:

- Έλεγχος και ενδυνάμωση ασφάλειας πληροφορικών συστημάτων.
- Διαχείριση δικτυακής κίνησης.
- Έλεγχος ασφάλειας διαδικτυακών εφαρμογών.

1η Φάση: Έλεγχος και ενδυνάμωση ασφαλείας πληροφοριακών συστημάτων

Το Penetration Testing (PT) ή Pentesting είναι η διαδικασία δοκιμής μίας εφαρμογής ή ενός συστήματος που στοχεύει στην αποκάλυψη τυχόν ευπαθειών που θα μπορούσε να εκμεταλλευτεί ένας επιτιθέμενος για την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Πρόκειται λοιπόν για μία εκ των προτέρων σχεδιασμένη και συγχρόνως εγκεκριμένη διαδικασία, για την αξιολόγηση του επιπέδου ασφαλείας ενός συστήματος, μέσω της εκμετάλλευσης (exploitation) ευπαθειών (vulnerabilities) με ασφαλή και ελεγχόμενο τρόπο από έναν ειδικό ασφάλειας.

Η διαδικασία του PT βασίζεται στη λογική «αξιολογήστε το επίπεδο ασφάλειας του συστήματος σας, προτού το κάνουν οι Hackers για σας». Σκοπός του PT είναι να καλυφθούν κενά ασφαλείας που ενδεχομένως θα οδηγήσουν έναν οργανισμό σε διαρροή ευαίσθητων πληροφοριών ή διακοπή λειτουργίας των παρεχόμενων υπηρεσιών με αποτέλεσμα σημαντικές οικονομικές ή άλλες απώλειες. Σκοπός του PT είναι η αναγνώριση των τρωτών σημείων ενός συστήματος ώστε στη συνέχεια να παρθούν μέτρα για την προστασία και ενδυνάμωση του.

Σε αυτό το πλαίσιο, καλείστε να επιτεθείτε σε ένα υπολογιστικό σύστημα με σκοπό την εκμετάλλευση ευπαθειών που ενδέχεται να παρουσιάζει. Το σύστημα αυτό θα πρέπει να προστατεύεται από ένα σύστημα ανίχνευσης εισβολών (Intrusion Detection System) που παρακολουθεί παθητικά και καταγράφει πιθανές επιθέσεις.

Πιο συγκεκριμένα, στο πλαίσιο αυτής της φάσης καλείστε να:

- Εγκαταστήσετε ένα τοπικό δίκτυο.
- Εγκαταστήσετε ένα σύστημα στο δίκτυο με λειτουργικό σύστημα Linux (ο στόχος της επίθεσης) και ένα σύστημα Kali Linux [1]. Για το στόχο μπορείτε να χρησιμοποιήσετε οποιαδήποτε διανομή Linux επιθυμείτε.
- Εγκαταστήσετε στο στόχο υπηρεσίες όπως SSH (Secure Shell), FTP, WEB (PHP, MySQL).
- Ως επιτιθέμενοι, ελέγξετε την ασφάλεια του συστήματός σας κάνοντας χρήση των παρακάτω ειδικών ελεγκτικών εργαλείων (penetration testing tools) που βρίσκονται ήδη εγκατεστημένα στη διανομή Kali Linux.
    - Nmap: Χρησιμοποιήστε το Nmap [4] για την αναγνώριση ενεργών υπηρεσιών/θυρών στο στόχο.
    - Armitage: Αξιοποιώντας τις πληροφορίες που έχετε συλλέξει από το προηγούμενο βήμα (Nmap) επιτεθείτε στο στόχο χρησιμοποιώντας έτοιμα exploits μέσω του εργαλείου Armitage [6].
- Εγκαταστήσετε στο στόχο και ρυθμίστε το Snort IDS [2] με σκοπό την ανίχνευση των επιθέσεων που πραγματοποιείτε με το Armitage.
    - Ρυθμίστε το Snort σε mode HIDS.
    - Επιτεθείτε στο σύστημα στόχο και αξιολογήστε το αποτέλεσμα της ανίχνευσης ελέγχοντας τα αρχεία καταγραφής (log files) του Snort.
    - Εγκαταστήστε το εργαλείο PulledPork [2] και χρησιμοποιήστε το για την ενημέρωση των κανόνων ανίχνευσης (detection rules) του Snort.
    - Εγκαταστήστε ένα εργαλείο για τη γραφική απεικόνιση των αποτελεσμάτων του Snort. Επιλέξτε το Snorby ή το BASE.
    - Επιτεθείτε ξανά στο σύστημα στόχο και αξιολογήστε το αποτέλεσμα της ανίχνευσης ελέγχοντας τα αρχεία καταγραφής (log files) του Snort και τις γραφικές απεικονίσεις του Snorby [3] ή BASE [5].
- Μετά το πέρας των επιθέσεων και μελετώντας τα αρχεία καταγραφής να αποφανθείτε για την ασφάλεια του στόχου και του δικτύου σας γενικότερα.
- Περιγράψτε συνοπτικά τα εργαλεία που χρησιμοποιήσατε καταγράφοντας το σκοπό που εξυπηρετούν, τον τρόπο εγκατάστασης, τη διαδικασία παραμετροποίησης, τις δυνατότητες τους, κλπ.
- Για τις παραπάνω ενέργειες θα πρέπει να παρέχετε ενδεικτικές εικόνες εκτέλεσης (Screen shots) με την κατάλληλη περιγραφή.

Σημείωση: Κατά την εγκατάσταση των εργαλείων Snort, PulledPork και Snorby (ή Base) ενδέχεται να χρειαστεί να εγκαταστήσετε άλλα βοηθητικά εργαλεία. Δεν αποτελεί ζητούμενο της άσκησης να περιγράψετε αυτά τα εργαλεία, αλλά αιτιολογήστε συνοπτικά το σκοπό που εξυπηρετεί καθένα από αυτά.

2η Φάση: Αναχώματα ασφάλειας L7 / Διαχείριση δικτυακής κίνησης

Το Deep Packet Inspection (DPI) είναι η πρωτεύουσα και σημαντικότερη τεχνολογία όσον αφορά την κατηγοριοποίηση κίνησης δικτύου για αναχώματα ασφάλειας επόμενων γενεών. Στο DPI τα διάφορα πακέτα του δικτύου εξετάζονται με σκοπό να αποφανθεί αν αποτελούν μέρος κάποιου ιού, επίθεσης, spam ή μη αποδεκτού, με κάποιους κανόνες, πακέτου, έτσι ώστε να γίνουν αποδεκτά ή να προωθηθούν σε κάποιον άλλο προορισμό ή και να απορριφθούν. Υπάρχουν αρκετά είδη DPI εργαλείων. Όπως ήδη ειπώθηκε στη θεωρία του μαθήματος, δύο από αυτά είναι το **nDPI [7]** και το **L7-Filter [8].**
Το καθένα από αυτά, αποτελεί έναν ταξινομητή κίνησης για πακέτα επιπέδου δικτύου. Ο κύριος σκοπός τους είναι να καταστήσουν ικανή την αναγνώριση εφαρμογών οι οποίες χρησιμοποιούν απρόβλεπτες πόρτες δικτύου. Έτσι, μπορούν να ταξινομήσουν και να κατηγοριοποιήσουν πακέτα όπως HTTP, FT, BitTorrent κ.ά. ανεξαρτήτου πόρτας.

L7-Filter: Δημιουργήθηκε το 2003 ως κατηγοριοποιητής κίνησης για Linux συστήματα, και μπορεί να αναγνωρίζει κίνηση, η οποία αναφέρεται στο επίπεδο εφαρμογής. Το l7-Filter χρησιμοποιεί 3 διαφορετικές μεθόδους:

1. Αναγνώριση με βάση αριθμητικά δεδομένα, όπως αριθμό θυρών, αναγνωριστικό αριθμό πρωτοκόλλου, πλήθος μεταδιδόμενων bytes.
2. Αναγνώριση συγκεκριμένων μοτίβων, τα οποία βασίζονται σε Κανονικές Εκφράσεις (Regular Expressions).
3. Αναγνώριση βάσει συναρτήσεων.

nDPI: Πρόκειται για ένα ανοιχτού κώδικα εργαλείο, το οποίο μεταξύ άλλων υποστηρίζει και κρυπτογραφημένα πρωτόκολλα. Μέχρι στιγμής, το εν λόγω εργαλείο υποστηρίζει πάνω από 100 διαφορετικά πρωτόκολλα.

Καλείστε να υλοποιήσετε ένα σενάριο διαχείρισης δικτυακής κίνησης ενός «εταιρικού» δικτύου κάνοντας χρήση ενδιάμεσου εξυπηρετητή (proxy server) και εργαλείων Deep Packet Inspection (DPI). Πιο συγκεκριμένα, θα πρέπει να εγκαταστήσετε και να αξιολογήσετε ως προς την απόδοση και την ευχρηστία, τα δύο προαναφερθέντα εργαλεία DPI. Θα πρέπει να εκτελέσετε και να αξιολογήσετε τα παραπάνω εργαλεία ως προς την αποτελεσματικότητά τους να αναγνωρίζουν διαφορετικού τύπου κινήσεις δικτύου. Στην συνέχεια θα πρέπει να συγκρίνετε το ποσοστό επιτυχίας τους για τον ίδιο τύπο κίνησης.
Υποθέστε ότι ο οργανισμός που εργάζεστε χρησιμοποιεί έναν SOCKS proxy. Η επικοινωνία με το διαδίκτυο επιτρέπεται μόνο μέσω του proxy. Ως διαχειριστής (admin) θα πρέπει να δημιουργήσετε κατάλληλους κανόνες στον proxy για να υλοποιήσετε συγκεκριμένη πολιτική ασφάλειας.

Κατηγορίες δικτυακής κίνησης

- Πρωτόκολλα εφαρμογών: DNS, HTTP, RTP, SIP, POP3-PLAIN, SMTP-PLAIN, SOCKS5, κ.ά.
- Εφαρμογές: Skype, League of Legends, Bit Torrent, Tor, DropBox, Spotify, World of Warcraft, Quake, eDonkey, 4Shared, Steam, κ.ά.
- Υπηρεσίες διαδικτύου: Amazon, Apple, Bing, Blogspot, Google, Facebook, Twitter, Wikipedia, Pinterest, κ.ά.

Θα πρέπει να επιλέξετε τουλάχιστον 4 τύπους δικτυακής κίνησης από κάθε κατηγορία ώστε να εξάγετε συγκεντρωτικά αποτελέσματα ως προς την αποτελεσματικότητα του κάθε εργαλείου (L7-Filter/nDPI)

στο να την αναγνωρίζει. Για την πρώτη κατηγορία (Πρωτόκολλα εφαρμογών) θα πρέπει συμπεριλάβετε υποχρεωτικά το πρωτόκολλο SOCKS5. Συνεπώς, στην κατηγορία αυτή θα εργαστείτε με το SOCKS5 και άλλα 3 πρωτόκολλα της επιλογής σας. Χρησιμοποιήστε τον Dante (Proxy Server) και προωθήστε κίνηση από firefox ή bittorrent μέσω του Dante και συγκρίνετε τα αποτελέσματα.

Τέλος, θα πρέπει να εμφανίσετε σχετικό πίνακα στον οποίο θα εμφανίζονται τα αποτελέσματά σας.

Dante

Όπως ήδη αναφέρθηκε στη θεωρία του μαθήματος, ο Dante [9] είναι ένα ελεύθερο λογισμικό, το οποίο αποτελείται από έναν SOCKS εξυπηρετητή και έναν SOCKS πελάτη. Ο SOCKS πελάτης δρομολογεί την κίνηση στον επιθυμητό προορισμό μέσω του SOCKS εξυπηρετητή.

Σενάριο

Θα πρέπει να κάνετε χρήση του Dante Proxy και να υλοποιήσετε κανόνες χάρη στους οποίους:

- Θα αποτρέπεται η πρόσβαση προς τον Proxy από μια συγκεκριμένη εξωτερική IP.
- Θα αποτρέπεται η πρόσβαση προς τον Proxy από ένα συγκεκριμένο εύρος IP του intranet.
- Θα αποτρέπεται η πρόσβαση όλων των χρηστών του Proxy σε κάποιο συγκεκριμένο εξωτερικό domain (π.χ. facebook.com).
- Bandwidth throttling: Θα πρέπει να περιορίσετε το εύρος της κίνησης ενός χρήστη και μιας υπηρεσίας αυτού του χρήστη στο δίκτυο, όπως FTP, SSH, HTTP κ.ά.

3η Φάση: Έλεγχος ασφάλειας διαδικτυακών εφαρμογών.

Η εξέλιξη του διαδικτύου έχει εισάγει πληθώρα νέων εφαρμογών (Web apps), οι οποίες βασίζονται σε τεχνολογίες όπως HTML, PHP, JavaScript, SOAP, SQL Databases. Αρκετές από αυτές εμφανίζουν ευπάθειες τις οποίες κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν με σκοπό να επιτεθούν στο σύστημα. Οι ευπάθειες αυτές μπορεί να οφείλονται είτε στη δομή των πρωτοκόλλων που χρησιμοποιούνται ή σε κάποια αδυναμία που ενδέχεται να έχει η ίδια η εφαρμογή λόγω αστοχίας του τρόπου υλοποίησης.

Οι κυριότερες μορφές από τέτοιου είδους επιθέσεις κατηγοριοποιούνται σύμφωνα με τον οργανισμό OWASP (Open Web Application Security Project) [10] ως εξής (OWASP TOP10 2013):

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

Σε αυτή τη φάση της εργασίας καλείστε να μελετήσετε τις Web επιθέσεις με χρήση της πλατφόρμας μάθησης WebGoat [11]. Η πλατφόρμα αυτή διαθέτει περισσότερα από 30 σύντομα μαθήματα, τα οποία επιδεικνύουν τις σημαντικότερες ευπάθειες. Επίσης, παρέχονται ενδεικτικά παραδείγματα του τρόπου εντοπισμού-εκμετάλλευσης αυτών των ευπαθειών.

Σκοπός αυτής της εργασίας είναι από τη μία να σας φέρει σε επαφή με την ασφάλεια διαδικτυακών εφαρμογών και από την άλλη να σας προετοιμάσει για το Hacking Tournament που θα διεξαχθεί περίπου την 1η εβδομάδα μετά τις διακοπές των Χριστουγέννων και θα διαρκέσει ένα 24ώρο (θα υπάρξει σχετική ανακοίνωση).

Χρήσιμα Εργαλεία για εκμετάλλευση ευπαθειών – έλεγχο ασφάλειας

- WebScarab
- Zed Attack Proxy (ZAP)
- Firefox Plugins
- Cookie Manager
- HackBar
- Web Developper Toolbar
- Tamper Data
- Live HTTP Headers

Παραδοτέα

Η αναφορά σας θα πρέπει να αναρτηθεί στα eclass, Gitlab σύμφωνα με τις οδηγίες που σας δόθηκαν στο εργαστήριο.

Η **αναφορά** σας ΠΡΕΠΕΙ να περιέχει τα ακόλουθα:

[1] Τεκμηρίωση για τον τρόπο εγκατάστασης, τη διαδικασία παραμετροποίησης και το σκοπό που εξυπηρετούν τα εργαλεία που χρησιμοποιήσατε.
[2] Επεξήγηση τυχόν δικών σας παραδοχών.
[3] Στιγμιότυπα εκτέλεσης προγραμμάτων (screenshots) με τον απαραίτητο σχολιασμό.
[4] Απαντήσεις στα ζητήματα που θέτουν τα σενάρια της εργασίας.
[5] Ανάλυση των αποτελεσμάτων χρήσης των αναχωμάτων ασφάλειας/εργαλείων DPI.
[6] Επεξήγηση των κανόνων που δημιουργήσατε για τη διαχείριση της δικτυακής κίνησης.
[7] Τεκμηρίωση των ευπαθειών/επιθέσεων (ύστερα από τη χρήση της πλατφόρμας WebGoat).
[8] Τεκμηρίωση και επεξήγηση του τρόπου εκμετάλλευσης των ευπαθειών.
[9] Στιγμιότυπα εκτέλεσης των επιθέσεων (screenshots).

Η εργασία πρέπει να παραδοθεί μέχρι τις **10/1/2017** μέσω της πλατφόρμας ηλεκτρονικής μάθησης **e-class**. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip (ή .rar) με όνομα:

ΑριθμόςΜητρώου1_ΑριθμόςΜητρώου2_ΑριθμόςΜητρώου3_Lab03.zip
(π.χ. icsd12001_icsd12002_icsd12003_Lab01.zip), του κάθε μέλους της ομάδας.

Συμπληρωματική Βιβλιογραφία

[1] Kali Linux - https://www.kali.org/
[2] Snort IDS - https://www.snort.org/
[3] Snorby - https://github.com/Snorby/snorby
[4] Nmap - https://nmap.org/
[5] BASE - https://sourceforge.net/projects/secureideas/
[6] Armitage - http://www.fastandeasyhacking.com/
[7] nDPI - http://www.ntop.org/products/deep-packet-inspection/ndpi/
[8] L7-Layer - http://l7-filter.sourceforge.net/
[9] Dante - https://www.inet.no/dante/
[10] OWASP - https://www.owasp.org/index.php/Main_Page
[11] WebGoat - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project