2ο Εργαστήριο

Στόχος Α

Εισαγωγή στο επίπεδο εφαρμογής του μοντέλου πρωτοκόλλων του TCP/IP. Μελέτη των πρωτοκόλλων επιπέδου εφαρμογής TELNET και SSH

Α1) Wireshark - TELNET διαδικασία

Το TELNET (TELetype NETwork Protocol) είναι πρωτόκολλο αρχιτεκτονικής πελάτη/εξυπηρετητή (client/server) για το επίπεδο εφαρμογής (L5). Χρησιμοποιείται για απομακρυσμένη σύνδεση (remote connection) στην γραμμή εντολών του λειτουργικού συστήματος ενός υπολογιστή (host). Στο πρώιμο internet χρησιμοποιούταν για την σύνδεση σε τερματικά (terminal), σταθμούς εργασίας που αποτελούταν μόνο από οθόνη και πληκτρολόγιο. Έτσι διεκπεραιώνει μια μεταφορά απλού κειμένου από και προς τον host.

- Χρησιμοποιείστε την IP διεύθυνση του server που σας δόθηκε για το εργαστήριο {IP} και έχετε ήδη βρει ή κάντε ping την {Διεύθυνση} του για να την δείτε. Εφαρμόστε το παρακάτω φίλτρο στο wireshark ως εξής:
  `telnet and (ip.src == {IP} or ip.dst == {IP})` ↵
- Θα πρέπει να μην εμφανίζεται καμία γραμμή στο πρώτο μέρος της διεπαφής του Wireshark. Επιλέξτε εκκίνηση καταγραφής κίνησης.
- Ανοίξτε ένα τερματικό και πληκτρολογήστε **`telnet {Διεύθυνση}`**. Η εφαρμογή αυτή είναι ένας πελάτης telnet για την γραμμή του λειτουργικού συστήματος
- Στην προτροπή Login πληκτρολογήστε το **`user1`**
- Στην προτροπή Password πληκτρολογήστε **`n3tl@b`**
- Θα σας εμφανιστεί ένα μήνυμα καλωσορίσματος και θα σας δοθεί μια προτροπή (prompt) για να πληκτρολογήσετε τις εντολές σας. Βρίσκεστε στην γραμμή εντολών του λειτουργικού συστήματος ενός remote host.
- Ανάλογα με το αν το απομακρυσμένο μηχάνημα είναι Windows ή Unix μπορείτε να τρέξετε εντολές όπως εμφάνιση περιεχομένων του καταλόγου με **`dir`** (Windows) και **`ls -al`** (Linux).
- Πληκτρολογήστε την εντολή **`exit`** για να αποσυνδεθείτε από τον host.
- Σταματήστε την καταγραφή στο Wireshark.

Ερωτήσεις Wireshark - TELNET διαδικασία

E2.1 Τι κάνει το φίλτρο που εφαρμόσατε στο Wireshark;
E2.2 Για κάθε επίπεδο του μοντέλου πρωτοκόλλων του TCP/IP καταγράψτε όσα χρησιμοποιούνται κατά την επικοινωνία του TELNET client με τον TELNET server.
E2.3 Καταγράψτε τα source IP/port και τα destination IP/port της επικοινωνίας, που χρησιμοποιήθηκαν κατά την συνεδρία (session) με TELNET. Διαχωρίστε τα αιτήματα (requests) από τις αποκρίσεις (replies).
E2.5 Ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς (L4) που χρησιμοποιεί το πρωτόκολλο επιπέδου εφαρμογής (L5) TELNET;
E2.6 Σε ποιον αριθμό port αναμένει requests ένας TELNET server;

E2.7 Καταγράψτε τα source και destination port που χρησιμοποιήθηκαν για να στείλει ο TELNET server τα replies στον TELNET client
E2.8 Στο μεσαίο panel του Wireshark πατήστε το ▸ Telnet ώστε να επεκταθούν τα δεδομένα του μηνύματος TELNET. Διατρέξτε την λίστα του άνω panel της διεπαφής του Wireshark. Τα πρώτα μηνύματα που ανταλλάσσουν τα δύο μέρη της επικοινωνίας, client και server, αφορούν στις ρυθμίσεις που θα χρησιμοποιηθούν. Μπορείτε να βρείτε και να διαβάσετε το μήνυμα υποδοχής του server;
E2.8 Τι παρατηρείτε αν συνεχίσετε να διαβάζετε το κείμενο στα επόμενα μηνύματα μετά την αποστολή της λέξης «password» από τον server;
E2.9 Αν σκεφτούμε το μοντέλο OSI των 7 επιπέδων και την διαπίστωση που κάνατε στο E2.8, ποια είναι η λύση στο πρόβλημα και σε ποιο επίπεδο θα την τοποθετούσατε.

A2) Wireshark - SSH διαδικασία

Το **SSH** (**S**ecure **SH**ell) είναι πρωτόκολλο αρχιτεκτονικής πελάτη/εξυπηρετητή (client/server) για το επίπεδο εφαρμογής (L5). Και αυτό χρησιμοποιείται για απομακρυσμένη σύνδεση (remote connection) στην γραμμή εντολών του λειτουργικού συστήματος ενός υπολογιστή (host), κυρίως σε συστήματα Linux. Η ειδοποιός διαφορά είναι ότι χρησιμοποιεί κρυπτογράφηση (encryption) των δεδομένων (data encryption) που ανταλλάσσονται. Αρχίστε μια SSH σύνδεση στον εξυπηρετητή της σχολής aetos.it.teithe.gr και καταγράψτε την κίνηση με το Wireshark.

Ερωτήσεις Wireshark - SSH διαδικασία

E2.10 Για κάθε επίπεδο της στοίβας πρωτοκόλλων διαδικτύου καταγράψτε όσα χρησιμοποιούνται στην επικοινωνία του SSH client με τον SSH server.
E2.11 Καταγράψτε τα source IP/port και τα destination IP/port της επικοινωνίας, που χρησιμοποιήθηκαν κατά την συνεδρία (session) με SSH. Διαχωρίστε τα αιτήματα (requests) από τις αποκρίσεις (replies).
E2.12 Ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς (L4) που χρησιμοποιεί το πρωτόκολλο επιπέδου εφαρμογής (L5) SSH;
E2.13 Σε ποιο port number αναμένει requests ένας SSH server;
E2.14 Όταν εμφανίζονται στο μεσαίο panel δεδομένα του μηνύματος SSH μπορείτε να διαβάσετε το κείμενο; Γιατί;

A3) Wireshark - RDP διαδικασία

Το Remote Desktop Protocol (RDP) είναι πρωτόκολλο αρχιτεκτονικής πελάτη/εξυπηρετητή (client/server) της Microsoft για το επίπεδο εφαρμογής (L5). Χρησιμοποιείται για απομακρυσμένη σύνδεση (remote connection) σε γραφικό περιβάλλον Windows τόσο σε client εκδόσεις όσο και σε server. Χρησιμοποιεί κρυπτογράφηση και αλγορίθμους συμπίεσης δεδομένων για την απεικόνιση των παραθύρων και την απροβλημάτιστη λειτουργία ποντικιού.

- Πατήστε Win+R και εκτελέστε την εντολή **`mstsc.`**
- Δώστε στο παράθυρο την διεύθυνση του δοκιμαστικού server.
- Τα διαπιστευτήρια (credentials) είναι όνομα χρήστη **`user1`** και κωδικός **`n3tl@b`**.
- Στο «`Do you want to connect despite these certificate errors`” απαντήστε `Yes`

E2.15 Μελετήστε το RDP με βάση την εμπειρία που αποκτήσατε με το TELNET και το SSH.

Στόχος Β

- Προσομοίωση του διαλόγου των πρωτοκόλλων επιπέδου εφαρμογής HTTP και SMTP.
- Χρήση του dig για ερωτήματα DNS.
- Γνωριμία με εργαλεία εποπτείας δικτυακής λειτουργίας εφαρμογών.

* Σημείωση: Μπορεί να υπάρχουν μερικές διαφορές της έκδοσης που έχει χρησιμοποιηθεί για την συγγραφή του κειμένου για το εργαστήριο σε σχέση με την έκδοση του λογισμικού του Εργαστηρίου.

Β1) HTTP διάλογος

Χρησιμοποιούμε το telnet για να προσομοιώσουμε τα μηνύματα που ανταλλάσσονται στο πρωτόκολλο HTTP που είναι επιπέδου εφαρμογής (L5) και χρησιμοποιείται στο web.

- Εκτέλεση την εντολής **`telnet testbed.it.teithe.gr 80`**
- Σε λειτουργικό Windows πατήστε CTRL+] ώστε να βγει η προτροπή Microsoft Telnet>
- Εκτελέστε **`set localecho`** ↵ ↵ το δεύτερο είναι για να επιστρέψετε στον διάλογο
- Στην συνέχεια πληκτρολογήστε τα παρακάτω και στο τέλος μία κενή γραμμή
  `GET /`↵

- Θα εμφανιστεί αναγνώσιμο κείμενο που τελειώνει με `Connection to host lost.`

E2.16 Τι διαβάζετε ως απόκριση από τον web server;.

Β2) SMTP διάλογος client/server

Χρησιμοποιούμε το telnet για να προσομοιώσουμε τα μηνύματα που ανταλλάσσονται στο πρωτόκολλο STMP που είναι επιπέδου εφαρμογής (L5) και χρησιμοποιείται για την αποστολή e-mail. Το πρόβλημα της ανεπιθύμητης αλληλογραφίας (spam) έχει οδηγήσει στην δημιουργία πολλών επιπλέον πεδίων στα μηνύματα του πρωτοκόλλου αλλά και επεκτάσεις στο σύστημα DNS. Ο παρακάτω απλά διάλογος έχει μόνο εκπαιδευτικό χαρακτήρα και θα ταξινομούνταν από τα περισσότερα συστήματα ως spam. Χρησιμοποιήστε εδώ μόνο το ιδρυματικό e-mail σας.

- Εκτέλεση την εντολής **`telnet smtp.it.teithe.gr 25`**
- Με μπλε είναι η απόκριση από τον SERVER. Με μαύρο το κείμενο που θα κάνετε copy-paste ή θα πληκτρολογήσετε χωρίς λάθη καθώς και τα backspace αποστέλλονται στον server.

```
220 smtp.it.teithe.gr ESMTP Sendmail 8.14.3/8.14.3/Debian-9.4; Tue, 29
Oct 2013 09:07:05 +0200; (No UCE/UBE) logging access from:
testbed.it.teithe.gr(OK)-root@testbed.it.teithe.gr [195.251.123.151]
C: HELO testbed.it.teithe.gr↵
250 smtp.it.teithe.gr Hello userX@testbed.it.teithe.gr
[195.251.123.151], pleased to meet you
C: MAIL FROM: {Το ιδρυματικό e-mail σας}↵
250 Ok
C: RCPT TO: {Το ιδρυματικό e-mail σας }↵
250 Ok
DATA↵
354 End data with <CR><LF>.<CR><LF>
Hello Alice.↵
This is a test message with 5 header fields and 4 lines in the message
body.↵
```

```
Your friend,↵
Bob↵
.
S: 250 Ok: queued as 12345
C: QUIT↵
S: 221 Bye
```

B3) DIG(1) - DNS

Το dig είναι εργαλείο για το πρωτόκολλο DNS. Με αυτό μπορείτε να απευθύνετε ερωτήσεις σε οποιονδήποτε DNS server. Υπάρχει άμεσα διαθέσιμο σε Linux.

- Για Windows κατεβάστε και αποσυμπιέστε το Bind από την διεύθυνση https://downloads.isc.org/isc/bind9/9.14.7/BIND9.14.7.x64.zip
  Ίσως χρειαστεί να κατεβάσετε και να εγκαταστήσετε το
  `Visual C++ Redistributable for Visual Studio 2012`
  από την διεύθυνση https://www.microsoft.com/en-us/download/details.aspx?id=30679
- Πηγαίνουμε σε γραμμή εργασιών στα Windows και αλλάζουμε κατάλογο σε αυτόν που αποσυμπιέσαμε το Bind.
- Εκτελούμε την εντολή **`nslookup`**
- Πληκτρολογήστε όποια διεύθυνση θέλετε και πατήστε enter. Θα δείτε ποιον DNS server χρησιμοποιεί το μηχάνημα σας και το name resolution.
- Για να δούμε τους κεντρικούς servers του διαδικτύου (DNS root servers) :
  `dig`
- Για να δούμε ποιος sever θα παραλάβει την αλληλογραφία για τον ιδρυματικό μας λογαριασμό που τελειώνει σε @it.teithe.gr:
  `dig it.teithe.gr MX`
- Για να δούμε σε ποιοι DNS servers διαχειρίζονται τις ονομασίες της σχολής:
  `dig iee.ihu.gr NS`
- Για αντίστροφο DNS (reverse DNS) δίνουμε IP address:
  `dig -x 195.251.123.232`
- Για εκτέλεση του ερωτήματος μέσω του DNS server της Google και όχι μέσω της σχολής τρέχουμε:
  `dig @8.8.8.8 www.ihu.gr`

Ερωτήσεις DIG(1) - DNS

E2.17 Προσπαθήστε να χρησιμοποιήσετε τις ίδιες εντολές με όποιους εξυπηρετητές θέλετε.
E2.18 Βρείτε τον DNS Server ο οποίο έχει δηλωμένο τον δοκιμαστικό server που σας δόθηκε στο εργαστήριο.
E2.19 Βρείτε τον MX για τον χώρο ονομάτων (domain) του ΔΙ.ΠΑ.Ε.

B4) Εποπτεία (Monitoring) Δικτυακής Λειτουργίας Εφαρμογών

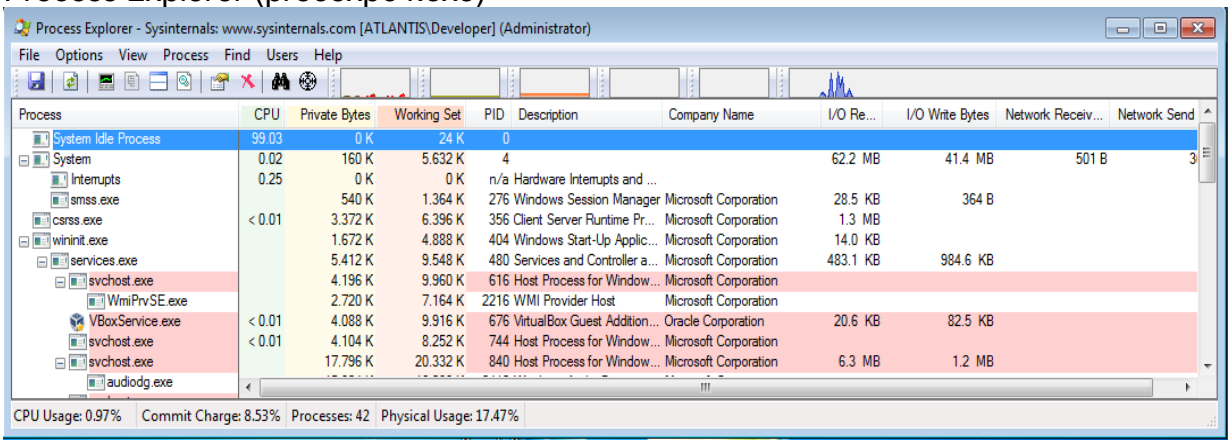
Για την εύρεση πληροφοριών δικτυακών διεργασιών σε λειτουργικά συστήματα Unix χρησιμοποιούνται οι επόμενες εντολές.

- Η εντολή **`netstat`**, μπορεί να δείχνει στον τελικό χρήστη πληροφορίες για δικτυακές διεργασίες σε εκτέλεση σε ένα λειτουργικό σύστημα. Για περισσότερες πληροφορίες `man netstat`
- Η εντολή **`lsof`**, μπορεί, μεταξύ των άλλων, να σας δείχνει τα ανοιχτά αρχεία και τις διεργασίες που έχουν ανοίξει αυτά τα αρχεία. Για περισσότερες πληροφορίες `man lsof`
- Με την εντολή **`ps -eaf`** σας εμφανίζονται οι διεργασίες του ΛΣ. Σε Ubuntu υπάρχει η **`htop.`**
- Με την εντολή **`whereis`** μπορείτε να βρείτε το PATH που υπάρχει το εκτελέσιμο αρχείο μιας εφαρμογής.

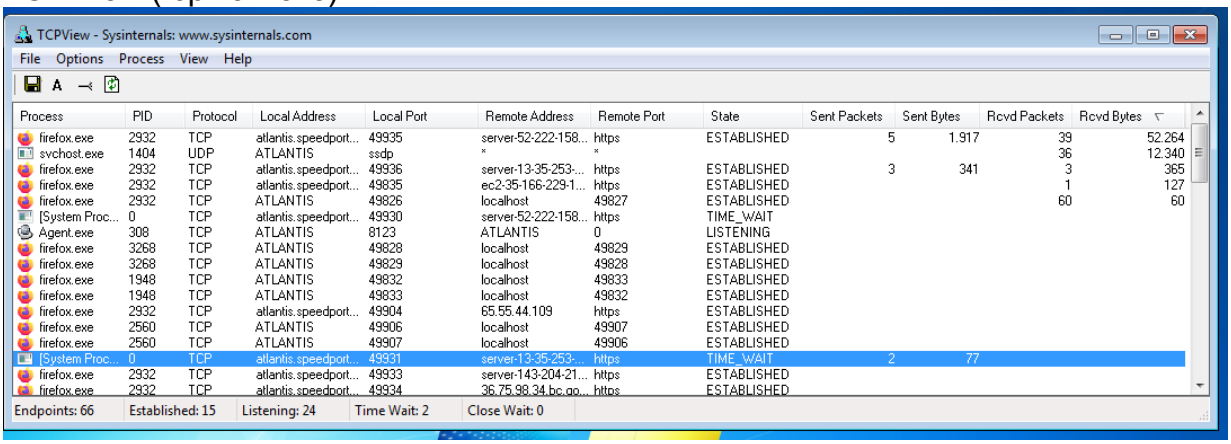
Για τις αντίστοιχες πληροφορίες σε λειτουργικά Windows τρέξτε ως administrator.

- Η εντολή **`netstat`**, μπορεί να δείχνει στον τελικό χρήστη πληροφορίες για δικτυακές διεργασίες σε εκτέλεση σε ένα λειτουργικό σύστημα. Για περισσότερες πληροφορίες `man netstat`
- Το σύνολο εργαλείων γραμμής εντολών αλλά και GUI που λέγεται https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

Process Explorer (procexp64.exe)



TCP View (tcpview.exe)



Βήματα για Unix:

- Σύνδεση στο CLI του testbed.it.teithe.gr
- Εκτέλεση της εντολής **`netstat -4atn`**. Με αυτήν την εντολή σας παρουσιάζονται οι δικτυακές διεργασίες που χρησιμοποιούν το πρωτόκολλο μεταφοράς TCP. Παρατηρήστε την πρώτη, την τέταρτη και την πέμπτη στήλη (Proto, Local Address, Foreign Address). Στο proto φαίνεται το πρωτόκολλο μεταφοράς που χρησιμοποιείται, στο Local Address είναι ο συνδυασμός.
- Εκτέλεση της εντολής **`netstat -4aun`**. Με αυτήν την εντολή σας παρουσιάζονται οι δικτυακές διεργασίες που χρησιμοποιούν το πρωτόκολλο μεταφοράς UDP. Παρατηρήστε την πρώτη, την τέταρτη και την πέμπτη στήλη (Proto, Local Address, Foreign Address).
- Εκτέλεση της εντολής **`sudo lsof -n -P -i4TCP`**. Με αυτήν την εντολή σας παρουσιάζονται οι διεργασίες σε εκτέλεση και τα αρχεία που χρησιμοποιούν. Δηλαδή τα ονόματα των προγραμμάτων σε εκτέλεση. Οι στήλες που σας ενδιαφέρουν, COMMAND, PID, NODE και NAME. Οπου COMMAND το όνομα του προγράμματος, PID ο αριθμός διεργασίες, NODE ο τύπος του πρωτοκόλλου του επιπέδου μεταφοράς στην περίπτωσή μας και NAME ο συνδυασμός ονόματος και αριθμός θύρας.

- Εκτέλεση της εντολής **`sudo lsof -n -P -i4UDP`** με τον ίδιο τρόπο για το πρωτόκολλο μεταφοράς UDP.
- Εκτέλεση της εντολής **`ps -eaf`**. Τα πεδία που σας παρουσιάζονται είναι τα UID, PID, PPID, C, STIME, TTY, TIME και CMD. Το CMD παρουσιάζει το PATH του προγράμματος σε εκτέλεση.

Ερωτήσεις Εποπτεία (Monitoring) Δικτυακής Λειτουργίας Εφαρμογών

E2.20 Καταγράψτε με το κατάλληλο εργαλείο μέσα σε ένα αρχείο (όχι χειροκίνητα) τις δικτυακές διεργασίες που λειτουργούν στο ΛΣ για το πρωτόκολλο TCP.
E2.21 Καταγράψτε τις διεργασίες που λειτουργούν στο ΛΣ για το πρωτόκολλο UDP.
E2.22 Πόσα διαφορετικά πρωτόκολλα επιπέδου μεταφοράς (L4) εντοπίσατε;
E2.23 Στα Windows ποια είναι η ονομασία του εκτελέσιμου του κεντρικού υποσυστήματος “Host Process for Windows Services”
E2.24 Καταγράψτε τις διαφορετικές θύρες στις οποίες αναμένει ερωτήματα το “Host Process for Windows Services”.
E2.25 Με μια αναζήτηση στο διαδίκτυο βρείτε ποιες είναι οι θύρες που εμφανίζονται στο tcpview με την ονομασία των πρωτοκόλλων τους για τα netbios-ns, ws-discovery, microsoft-ds. Πως θα αναλύατε την λειτουργία τους με το Wireshark.