2ο Εργαστήριο

Στόχος Α

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

** 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.*

A. Wireshark - TELNET διαδικασία

Το TELNET είναι πρωτόκολλο είναι αρχιτεκτονικής client/server για το επίπεδο εφαρμογής. Χρησιμοποιείται για να αποκτήσετε πρόσβαση στην γραμμή εντολών ενός λειτουργικού συστήματος ενός μηχανήματος, μέσω δικτύου.

Βήμα 1: Χρησιμοποιείστε την IP διεύθυνση του testbed.it.teithe.gr που βρήκατε από προηγούμενη διαδικασία (σε προηγούμενο εργαστήριο), εστω IPtestbed, και εφαρμόστε το παρακάτω φίλτρο στο wireshark ως εξής:
`telnet and (ip.src == IPtestbed or ip.dst == IPtestbed)`
Βήμα 2: Θα πρέπει να μην εμφανίζεται καμία γραμμή στο πρώτο μέρος της διεπαφής του wireshark. Επιλέξτε εκκίνηση καταγραφής κίνησης.
Βήμα 3: Ανοιξτε ένα τερματικό και πληκτρολογήστε `telnet testbed.it.teithe.gr`. Telnet είναι το όνομα του προγράμματος του λειτουργικού συστήματος που θα χρησιμοποιήσουμε ως TELNET client. Τυχαίνει να έχει το ίδιο όνομα με το πρωτόκολλο.
Βήμα 4: Στην προτροπή Login πληκτρολογήστε το `user1`
Βήμα 5: Στην προτροπή Password πληκτρολογήστε `user1`
Βήμα 6: Θα σας εμφανιστεί ένα μήνυμα καλωσορίσματος και θα σας δοθεί ένα prompt για να πληκτρολογήσετε τις εντολές σας. Βρίσκεστε στην γραμμή εντολών ενός απομακρυσμένου μηχανήματος.
Βήμα 7: Πληκτρολογήστε την εντολή `ls -al`
Βήμα 8: Πληκτρολογήστε την εντολή `exit`
Βήμα 9: Σταματήστε την καταγραφή στο wireshark

Ερωτήσεις Wireshark - TELNET διαδικασία

1. Τι κάνει το φίλτρο που εφαρμόσατε στο wireshark;
2. Για κάθε επίπεδο του μοντέλου πρωτοκόλλων του TCP/IP καταγράψτε τα πρωτόκολλα που πήραν μέρος στην επικοινωνία του TELNET client με τον TELNET server
3. Καταγράψτε την source και την destination IP διεύθυνση της επικοινωνίας.
4. Καταγράψτε το source και το destination port που χρησιμοποιήθηκαν για τα TELNET requests που εστάλησαν στον TELNET server.
5. Ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιεί το πρωτόκολλο επιπέδου εφαρμογής TELNET;
6. Σε ποιο port number αναμένει requests ένας TELNET server;

7. Καταγράψτε τα source και destination port που χρησιμοποιήθηκαν για να στείλει ο TELNET server τα replies στον TELNET client
8. Πάτε στην πρώτη εγγραφή της λίστας καταγραφής, στο πρώτο μέρος της διεπαφής του wireshark. Πατήστε το [>] που εμφανίζεται πριν από το telnet στο δεύτερο μέρος της διεπαφής του wireshark. Θα σας εμφανιστούν τα μηνύματα του πρωτοκόλλου. Τα πρώτα μηνύματα που ανταλλάσσουν τα δύο μέρη της επικοινωνίας, client και server, αφορούν στις ρυθμίσεις που θα χρησιμοποιηθούν. Κατεβείτε στην λίστα του πρώτου μέρους της διεπαφής του wireshark και εντοπίστε την γραμμή που εμφανίζει σαν μήνυμα το εξής: "**`testbed login:`**". Παρατηρήστε και καταγράψτε τα επόμενα δύο βήματα της επικοινωνίας.

B. Wireshark - SSH διαδικασία

Το SSH είναι πρωτόκολλο είναι αρχιτεκτονικής client/server για το επίπεδο εφαρμογής. Χρησιμοποιείται για να αποκτήσετε πρόσβαση στην γραμμή εντολών ενός λειτουργικού συστήματος ενός μηχανήματος, μέσω δικτύου. Χρησιμοποιεί κρυπτογράφηση των δεδομένων που ανταλλάσσονται. Αρχίστε μια SSH σύνδεση στον aetos.it.teithe.gr και καταγράψτε την κίνηση με το wireshark

Ερωτήσεις Wireshark - SSH διαδικασία

1. Για κάθε επίπεδο του μοντέλου πρωτοκόλλων του TCP/IP καταγράψτε τα πρωτόκολλα που πήραν μέρος στην επικοινωνία του SSH client με τον SSH server
2. Καταγράψτε την source και την destination IP διεύθυνση της επικοινωνίας.
3. Καταγράψτε το source και το destination port που χρησιμοποιήθηκαν για τα SSH requests που εστάλησαν στον SSH server.
4. Ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιεί το πρωτόκολλο επιπέδου εφαρμογής SSH;
5. Σε ποιο port number αναμένει requests ένας SSH server;
6. Καταγράψτε τα source και destination port που χρησιμοποιήθηκαν για να στείλει ο SSH server τα replies στον SSH client
7. Παρατηρήστε ότι τα πεδία του SSH δεν είναι αναγνώσιμα. Γιατί;

Στόχος Β

1. Προσομοίωση του διαλόγου των πρωτοκόλλων επιπέδου εφαρμογής HTTP και SMTP
2. Χρήση του dns client, dig
3. Χρήση του netstat (8) για εντοπισμό ενεργών διεργασιών

* 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.

Α HTTP διάλογος

Με την χρήση του προγράμματος telnet που είναι client για το πρωτόκολλο TELNET μπορούμε να προσομοιώνουμε τον διάλογο του HTTP ως εξής:

Σύνδεση στο CLI του ΛΣ σας και εκτέλεση της εντολής

```
telnet testbed.it.teithe.gr 80
```

Στην συνέχεια πληκτρολογήστε τα παρακάτω και στο τέλος μία κενή γραμμή

```
GET / HTTP/1.1
Host: www.it.teithe.gr
Connection: close
```

Τι παρατηρήσατε;.

B SMTP διάλογος client/server

Με την χρήση του προγράμματος telnet που είναι client για το πρωτόκολλο TELNET μπορούμε να προσομοιώνουμε τον διάλογο του SMTP ως εξής:
Σύνδεση στο CLI του testbed.it.teithe.gr και εκτέλεση της εντολής

`telnet smtp.it.teithe.gr 25`

Όπου εμφανίζεται S είναι απόκριση από τον SERVER. Οπου εμφανίζεται C πρέπει να πληκτρολογήσετε εντολή

Στην συνέχεια πληκτρολογήστε τα παρακάτω

```
S: 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
S: 250 smtp.it.teithe.gr Hello userX@testbed.it.teithe.gr
[195.251.123.151], pleased to meet you
C: MAIL FROM:ΤΟ μα ι λ του αποστολέα
S: 250 Ok
C: RCPT TO:Το μα ι λ του παραλήπτη
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the
message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

C DIG(1) - DNS

Το dig είναι client για το πρωτόκολλο DNS. Μπορείτε να απευθύνετε ερωτήσεις σε οποιονδήποτε DNS server.

1. Σύνδεση στο CLI του testbed.it.teithe.gr
2. Εκτέλεση της εντολής **`cat /etc/resolv.conf`**. Θα βρείτε τους DNS servers που χρησιμοποιεί το ΛΣ
3. dig
4. dig it.teithe.gr MX
5. dig it.telthe.gr NS
6. dig -x 195.251.123.232
7. dig grnet.gr NS
8. dig @ns0.grnet.gr www.grnet.gr

Ερωτήσεις DIG(1) - DNS

1. Καταγράψτε το είδος των ερωτήσεων που κάνατε και τις απαντήσεις που πήρατε
2. Βρείτε τον DNS server για τον χώρο ονομάτων της google

3. Βρείτε τον MX για τον χώρο ονομάτων του ΠΑΜΑΚ (uom.gr)

D Netstat(8), LSOF(8), PS(1)

Για την εύρεση πληροφοριών δικτυακών διεργασιών σε ΛΣ τύπου 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
Με την εντολή **whereis** μπορείτε να βρείτε το PATH που υπάρχει το εκτελέσιμο αρχείο μιας εφαρμογής.

Βήματα:

1. Σύνδεση στο CLI του testbed.it.teithe.gr
2. 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
3. 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)
4. 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
5. Εκτέλεση της εντολής **sudo lsof -n -P -i4UDP** με τον ίδιο τρόπο για το πρωτόκολλο μεταφοράς UDP
6. 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 Netstat(8), LSOF(8), PS(1)

1. Καταγράψτε τις δικτυακές διεργασίες που λειτουργούν στο ΛΣ για το πρωτόκολλο TCP καθώς και το PATH που βρίσκεται τα προγράμματα
2. Καταγράψτε τις δικτυακές διεργασίες που λειτουργούν στο ΛΣ για το πρωτόκολλο UDP καθώς και το PATH που βρίσκεται τα προγράμματα
3. Πόσα πρωτόκολλα επιπέδου μεταφοράς χρησιμοποιεί το πρόγραμμα server DNS