



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΑΘΗΜΑ: «ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ (8^ο ΕΞΑΜΗΝΟ)»

ΚΑΘΗΓΗΤΕΣ: ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

ΔΗΜΗΤΡΕΛΛΟΣ ΠΑΝΑΓΙΩΤΗΣ, Π17026

ΚΑΡΑΜΠΟΪΚΗΣ ΝΙΚΟΛΑΟΣ, Π17040

ΡΟΥΝΤΟΥ ΑΝΝΑ-ΦΑΝΗ, Π17113

5η Άσκηση - Υλοποίηση firewall

ΠΕΡΙΕΧΟΜΕΝΑ

1. Να υλοποιήσετε μία πολιτική ασφάλειας δικτύου με τη χρήση iptables, η οποία να είναι προσανατολισμένη στις ανάγκες ασφάλειας ενός σταθμού εργασίας.....	3
2. Στη συνέχεια, να διαμορφώσετε ένα δεύτερο σύστημα (virtual machine) το οποίο θα έχει το ρόλο του default gateway/ δικτυακού firewall για το σταθμό εργασίας.....	5
Ενέργειες στο VM1 (192.168.1.30):.....	5
Ενέργειες στο VM2:	5
Σχετικές δοκιμές:	8

1. Να υλοποιήσετε μία πολιτική ασφάλειας δικτύου με τη χρήση iptables, η οποία να είναι προσανατολισμένη στις ανάγκες ασφάλειας ενός σταθμού εργασίας.

- Rules for Firewall:

delete all rules

iptables -F

reject every traffic that is not allowed

iptables -P INPUT DROP

iptables -P OUTPUT DROP

allow the traffic from loopback interface

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

create a list for the allowed services

iptables -N WHITELIST

iptables -A OUTPUT -j WHITELIST

allow outgoing traffic only to dns,http,https,smtp

iptables -A WHITELIST -p tcp -m multiport --dports 53,80,443,25 -j ACCEPT

allow the sending ping packets

iptables -A OUTPUT -p icmp -p icmp --icmp-type echo-request -j ACCEPT

allow the ingoing ping packets with a rate 5 per minute

iptables -A INPUT -p icmp -m limit --limit 5/min -j ACCEPT

every connection which has been allowed from previous rules is allowed until the end of the connection.

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

log every traffic before being dropped

iptables -N LOGNDROPLIST

iptables -A INPUT -j LOGNDROPLIST

iptables -A LOGNDROPLIST -j LOG --log-prefix "INPUT:DROPPED: " --log-level 6

iptables -A LOGNDROPLIST -j DROP

iptables -A OUTPUT -j LOGNDROPLIST

```
iptables -A LOGNDROPLIST -j LOG --log-prefix "OUTPUT:DROP: " --log-level 6
```

```
iptables -A LOGNDROPLIST -j DROP
```

```
(panos2@kali2)-[~/Desktop]
$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- lo any anywhere
0 0 ACCEPT icmp -- any any anywhere
0 0 ACCEPT all -- any any anywhere
0 0 LOGNDROPLIST all -- any any anywhere
limit: avg 5/min burst 5
state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- any lo anywhere
0 0 WHITELIST all -- any any anywhere
0 0 ACCEPT icmp -- any any anywhere
0 0 LOGNDROPLIST all -- any any anywhere

Chain LOGNDROPLIST (2 references)
pkts bytes target prot opt in out source destination
0 0 LOG all -- any any anywhere LOG level info prefix "INPUT:DROP: "
0 0 DROP all -- any any anywhere LOG level info prefix "OUTPUT:DROP: "
0 0 LOG all -- any any anywhere
0 0 DROP all -- any any anywhere

Chain WHITELIST (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere multiport dports domain,http,https,smtp
```

Για να εφαρμόζονται οι κανόνες κατά την εκκίνηση του συστήματος κάνουμε τα εξής βήματα:

- Για αποθήκευση κανόνων:

```
iptables-save > /etc/iptables.rules
```

- Για την ενεργοποίηση των κανόνων, προσθέτουμε στο αρχείο /etc/network/interfaces την εντολή:

```
pre-up iptables-restore < /etc/iptables.rules
```

```
File Edit Search Options Help
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

pre-up iptables-restore < /etc/iptables.rules
```

2. Στη συνέχεια, να διαμορφώσετε ένα δεύτερο σύστημα (virtual machine) το οποίο θα έχει το ρόλο του default gateway/ δικτυακού firewall για το σταθμό εργασίας.

Ενέργειες στο VM1 (192.168.1.30):

1. Αλλαγή του Default Gateway ώστε να έχει ως Default GW το VM2.
 - `route add default gw 192.168.1.29`

```
(root@kali2)-[/home/panos2]
# route add default gw 192.168.1.29
```

- `route del default gw 192.168.1.1`

```
(root@kali2)-[/home/panos2]
# route del default gw 192.168.1.1
```

```
(root@kali2)-[/home/panos2]
# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.29   0.0.0.0         UG    0      0      0 eth0
192.168.1.0      0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

Ενέργειες στο VM2:

1. Μετατροπή του πίνακα nat στο iptables ώστε να υποστηρίζει nat.
 - `iptables -t nat -A POSTROUTING -s 192.168.0/24 -o eth0 -j MASQUERADE`

```
(root@kali1)-[/home/panos1]
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
```

2. Ενεργοποίηση ip forwarding στον host
 - Στο αρχείο `/etc/sysctl.conf` βρίσκουμε τη γραμμή: `net.ipv4.ip_forward=1` και την ενεργοποιούμε.
 - Από shell εκτελούμε: `sysctl -p`

```
(root@kali1)-[/home/panos1]
# leafpad /etc/sysctl.conf
# sysctl -p
net.ipv4.ip_forward = 1
```

Κάνουμε traceroute στο www.unipi.gr από το VM1(192.168.1.30) για να δούμε αν περνάει από το gateway που έχουμε ορίσει το VM1(192.168.1.29).

```
root@kali2:~/home/panos2# traceroute www.unipi.gr
traceroute to www.unipi.gr (195.251.229.4), 30 hops max, 60 byte packets
 1 kali1.home (192.168.1.29)  0.396 ms  0.332 ms  0.310 ms
 2 speedport-ip (192.168.1.1)  3.238 ms  3.202 ms  3.172 ms
 3 80.106.125.100 (80.106.125.100)  11.864 ms  13.666 ms  13.640 ms
 4 79.128.224.2 (79.128.224.2)  13.615 ms  79.128.226.149 (79.128.226.149)  13.588 ms  athe-asr99a-xala-asr9ka.backbone.otenet.net (79.128.227.101)  13.506 ms
 5 79.128.227.227 (79.128.227.227)  13.468 ms  79.128.224.189 (79.128.224.189)  13.408 ms  13.339 ms
 6 grnet-2-gr-ix.gr (176.126.38.31)  15.741 ms  14.571 ms  14.524 ms
 7 eier-kolettir-AE.backbone.grnet.gr (62.217.100.63)  14.501 ms  13.999 ms  45.210 ms
 8 unipi-1.eier.access-link.grnet.gr (62.217.96.87)  13.890 ms  14.795 ms  15.784 ms
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

Όπως βλέπουμε περνάει αρχικά από το 192.168.1.29.

- Rules for Firewall of default gateway:

delete all rules

iptables -F

allow incoming connections from the internet to ports 80, 443 (http, https) and forward them to the HTTP Server.

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -p tcp --dport 443 -j ACCEPT

allow incoming connections from the internet to port 25,143(smtp, imap) and forward them to the Mail Server.

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -p tcp --dport 143 -j ACCEPT

allow outgoing connections from the HTTP Server(Workstation) to port 80,443 (http, https) and forward them to the internet.

iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 443 -j ACCEPT

allow outgoing connections from the Mail Server(Workstation) to port 25,143(smtp, imap) and forward them to the internet.

iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 143 -j ACCEPT

allow outgoing connections from the internal network to ports 20, 21 (ftp data, ftp cmd) and forward them to the internet.

iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 20 -j ACCEPT

```
iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp --dport 21 -j ACCEPT
```

#allow all incoming connections if established.

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

allow receiving ping requests with a rate of 10 per minute and forward them to the workstation.

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.30 -o eth0 -p icmp -m limit --limit 10/min -j ACCEPT
```

allow outgoing ping requests from the workstation.

```
iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p icmp --icmp-type echo-request -j ACCEPT
```

#allow outgoing connections from the Http Server if established (for HTTP responses)

```
iptables -A FORWARD -s 192.168.1.30 -i eth0 -d 0/0 -o eth0 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT
```

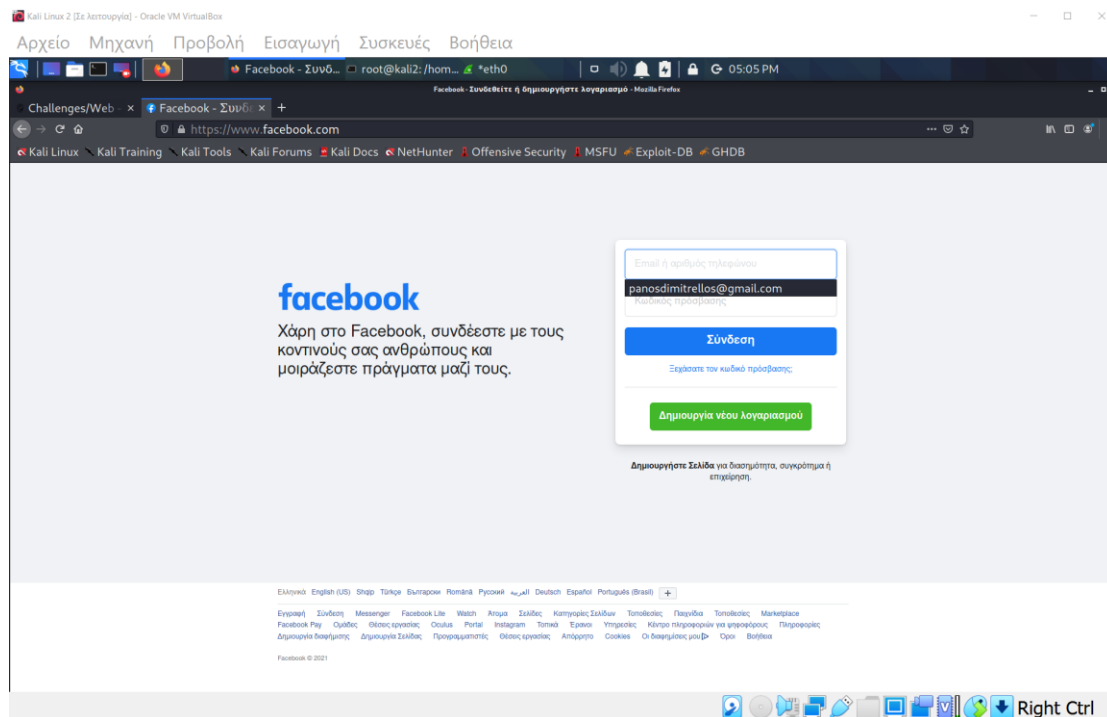
drop everything else

```
iptables -A FORWARD -j DROP
```

```
(root@kali1)-[/home/panos1/Desktop]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:http
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:https
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:smtp
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:imap2
0      0 ACCEPT      tcp  --  eth0  eth0    kali2.home     anywhere       tcp dpt:http
0      0 ACCEPT      tcp  --  eth0  eth0    kali2.home     anywhere       tcp dpt:https
0      0 ACCEPT      tcp  --  eth0  eth0    kali2.home     anywhere       tcp dpt:smtp
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:imap2
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:ftp-data
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      tcp dpt:ftp
0      0 ACCEPT      all  --  eth0  eth0    anywhere       kali2.home      state RELATED,ESTABLISHED
0      0 ACCEPT      icmp --  eth0  eth0    anywhere       kali2.home      limit: avg 10/min burst 5
0      0 ACCEPT      icmp --  eth0  eth0    anywhere       kali2.home      icmp echo-request
0      0 ACCEPT      tcp  --  eth0  eth0    anywhere       kali2.home      state RELATED,ESTABLISHED
0      0 DROP        all  --  any   any     anywhere       anywhere
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
```

Σχετικές δοκιμές:

- Για να ελέγξουμε την κίνηση ανάμεσα σε workstation και το firewall , δοκιμάζουμε να συνδεθούμε στην ιστοσελίδα του facebook από το workstation.



Περιμένουμε να δούμε κίνηση σε πακέτα http και https στο firewall του default gateway.

```
(root@kali) - [/home/panos1/Desktop]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
 0      0 ACCEPT    tcp -- eth0  eth0    anywhere         kali2.home        tcp dpt:http
 0      0 ACCEPT    tcp -- eth0  eth0    anywhere         kali2.home        tcp dpt:https
 0      0 ACCEPT    tcp -- eth0  eth0    anywhere         kali2.home        tcp dpt:smtp
 0      0 ACCEPT    tcp -- eth0  eth0    anywhere         kali2.home        tcp dpt:imap2
 2    104 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         tcp dpt:http
 46  8528 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         tcp dpt:https
 0      0 ACCEPT    tcp -- eth0  eth0    anywhere         kali2.home        tcp dpt:smtp
 0      0 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         tcp dpt:imap2
 0      0 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         tcp dpt:ftp-data
 0      0 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         tcp dpt:ftp
 42 40194 ACCEPT    all -- eth0  eth0    anywhere         kali2.home        state RELATED,ESTABLISHED
 0      0 ACCEPT    icmp -- eth0  eth0    anywhere         kali2.home        limit: avg 10/min burst 5
 0      0 ACCEPT    icmp -- eth0  eth0    anywhere         kali2.home        icmp echo-request
 0      0 ACCEPT    tcp -- eth0  eth0    kali2.home       anywhere         state RELATED,ESTABLISHED
 0      0 DROP     all -- any   any    anywhere         anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
```

Όπως σωστά αναμέναμε βλέπουμε ότι υπάρχει κίνηση στα πρωτόκολλα http, https καθώς έχει επιτραπεί και η κίνηση σε session που είναι RELATED ή ESTABLISHED.

- Ένα άλλο παράδειγμα για να ελέγξουμε την κίνηση μεταξύ του workstation και του firewall είναι η παρατήρηση των ping request.

Κάνουμε ping την σελίδα του πανεπιστημίου και βλέπουμε ότι αρχικά γίνεται κανονικά.

```
(root@kali2)-[/home/panos2]
# ping www.unipi.gr
PING unipiweb.unipi.gr (195.251.229.4) 56(84) bytes of
data.
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=1 ttl=56 time=16.4 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=2 ttl=56 time=15.3 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=3 ttl=56 time=15.1 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=4 ttl=56 time=14.8 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=5 ttl=56 time=15.6 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=6 ttl=56 time=15.2 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=7 ttl=56 time=13.4 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=8 ttl=56 time=23.0 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=9 ttl=56 time=15.3 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=10 ttl=56 time=15.9 ms
64 bytes from unipiweb.unipi.gr (195.251.229.4): icmp_
seq=11 ttl=56 time=14.9 ms
```

Στην συνέχεια παρατηρούμε ότι στο firewall του default gateway έχει καταγραφεί η κίνηση των πακέτων ping από το workstation όπως το επιτρέπει και ο κανόνας μας.

```
(root@kali2)-[/home/panos1/Desktop]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
0      0 ACCEPT      tcp -- eth0   eth0    anywhere       kali2.home      tcp dpt:http
0      0 ACCEPT      tcp -- eth0   eth0    anywhere       kali2.home      tcp dpt:https
0      0 ACCEPT      tcp -- eth0   eth0    anywhere       kali2.home      tcp dpt:smtp
0      0 ACCEPT      tcp -- eth0   eth0    anywhere       kali2.home      tcp dpt:imap2
12    624 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:http
190 37313 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:https
0      0 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:smtp
0      0 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:imap2
0      0 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:ftp-data
0      0 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       tcp dpt:ftp
165 50609 ACCEPT      all -- eth0   eth0    anywhere       kali2.home     state RELATED,ESTABLISHED
0      0 ACCEPT      icmp -- eth0   eth0    anywhere       kali2.home     limit: avg 10/min burst 5
13 1092 ACCEPT      icmp -- eth0   eth0    kali2.home     anywhere       icmp echo-request
0      0 ACCEPT      tcp -- eth0   eth0    kali2.home     anywhere       state RELATED,ESTABLISHED
0      0 DROP       all -- any    any    anywhere       anywhere
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source         destination
```