



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	4-iptables
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	27-03-2019



A) Να υλοποιήσετε μία πολιτική ασφάλειας δικτύου με τη χρήση κανόνων iptables, η οποία να είναι προσανατολισμένη στις ανάγκες ασφάλειας ενός σταθμού εργασίας (Workstation). Την υλοποίηση μπορείτε να την εφαρμόσετε σε ένα virtual machine που θα έχει το ρόλο του σταθμού εργασίας. Οι κανόνες που θα πρέπει κατά ελάχιστο να υλοποιήσετε είναι οι εξής:

- Επιτρέπεται η κίνηση στο loopback interface
- Επιτρέπεται η εξερχόμενη σύνδεση μόνο στις υπηρεσίες dns, http, https και smtp.
- Επιτρέπεται η αποστολή πακέτων ping.
- Επιτρέπεται η λήψη πακέτων ping, με όριο 5 πακέτα/λεπτό
- Οποιαδήποτε σύνδεση έχει επιτραπεί από προηγούμενο κανόνα, επιτρέπεται μέχρι των τερματισμό της σχετικής σύνδεσης (stateful inspection).
- Οποιαδήποτε κίνηση δεν έχει επιτραπεί ρητώς, απορρίπτεται.
- Καταγράφεται οποιαδήποτε κίνηση πριν την απόρριψή της.

Να δημιουργήσετε τους σχετικούς κανόνες σε αρχείο και να διαμορφώσετε το σύστημα ώστε οι παραπάνω κανόνες να εφαρμόζονται κάθε φορά κατά την εκκίνηση του συστήματος. Η διαμόρφωσή σας μπορεί να περιλαμβάνει και άλλους κανόνες, εφόσον απαιτείται.

Για τις επιτρεπόμενες υπηρεσίες να δημιουργήσετε μία καινούρια αλυσίδα κανόνων με το όνομα WHITELIST. Για την καταγραφή και απόρριψη των πακέτων να δημιουργήσετε μία νέα αλυσίδα με το όνομα LOGNDROPLIST. Να γίνει διαμόρφωση του συστήματος ώστε οι κανόνες να εφαρμόζονται κάθε φορά κατά την εκκίνηση του συστήματος. Το αρχείο των κανόνων να περιλαμβάνει και τη σχετική τεκμηρίωση.



Αρχικά διαγράφουμε όλους τους κανόνες που υπήρχαν.



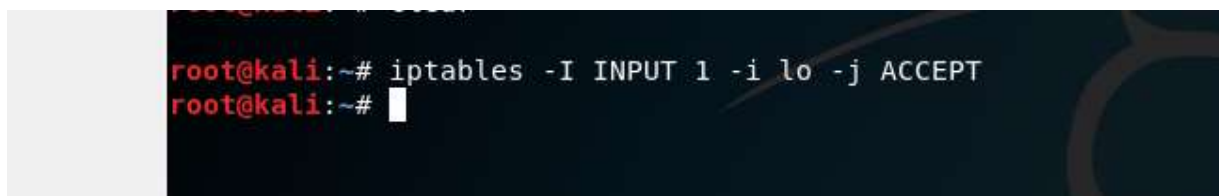
```
root@kali:~# iptables -F
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@kali:~#
```

Διαγράφουμε όλες τις εντολές με την εντολή:
Iptables -F

Επιτρέπεται η κίνηση στο loopback interface

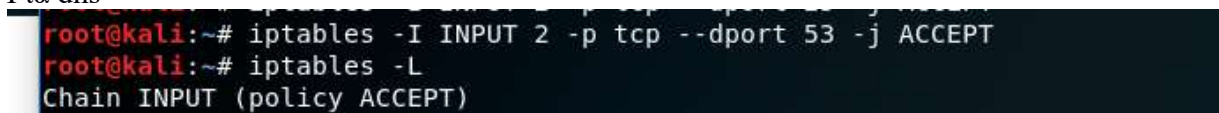


```
root@kali:~# iptables -I INPUT 1 -i lo -j ACCEPT
root@kali:~#
```

iptables -I INPUT 1 -i lo -j ACCEPT

Επιτρέπεται η εξερχόμενη σύνδεση μόνο στις υπηρεσίες dns, http, https και smtp.

Τρέχουμε τις εντολές αντίστοιχα:
Για dns



```
root@kali:~# iptables -I INPUT 2 -p tcp --dport 53 -j ACCEPT
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
```

Για http



```
Applications ▾ Places ▾ Terminal ▾ Sat 05:05
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iptables -I INPUT 2 -p tcp --dport 80 -j ACCEPT
```

Για https

```
File Edit View Search Terminal Help
root@kali:~# iptables -I INPUT 2 -p tcp --dport 443 -j ACCEPT
root@kali:~# iptables -L
```

Για SMTP

```
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sat 05:09
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iptables -I INPUT 2 -p tcp --dport 25 -j ACCEPT
root@kali:~#
```

```
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:domain
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:smtp
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@kali:~#
```

Επιτρέπεται η αποστολή πακέτων ping.

```
root@kali:~# iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
```

Iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT



Επιτρέπεται η λήψη πακέτων ping, με όριο 5 πακέτα/λεπτό

```
root@kali:~# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 5/s --limit-burst 10 -j ACCEPT
root@kali:~#
```

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 5/s --limit-burst 10 -j ACCEPT

```
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request limit: avg 5/sec burst 10
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:domain
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:smtp
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:https
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request
root@kali:~#
```

Οποιαδήποτε σύνδεση έχει επιτραπεί από προηγούμενο κανόνα, επιτρέπεται μέχρι των τερματισμό της σχετικής σύνδεσης (stateful inspection)

```
KaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sat 06:33
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iptables -I INPUT 2 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

iptables -I INPUT 2 -m state --state ESTABLISHED, RELATED -j ACCEPT



Καταγράφεται οποιαδήποτε κίνηση πριν την απόρριψή της

```
File Edit View Search Terminal Help
root@kali:~# iptables -I INPUT -j LOG
root@kali:~# iptables -L
```

Iptables -I INPUT -j Log

Οποιαδήποτε κίνηση δεν έχει επιτραπεί ρητώς, απορρίπτεται.

```
ACCEPT icmp -- anywhere anywhere icmp echo-request
root@kali:~# iptables -P INPUT DROP
root@kali:~#
```

Iptables -P INPUT DROP

```
bash: iptables: command not found
root@kali:~# iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
LOG       all  --  anywhere              anywhere        LOG level warning
ACCEPT    all  --  anywhere              anywhere
ACCEPT    icmp --  anywhere              anywhere        icmp echo-request limit: avg 5/sec burst 10
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:domain
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:smtp
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:https
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:http

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    icmp --  anywhere              anywhere        icmp echo-request
root@kali:~#
```

Να δημιουργήσετε τους σχετικούς κανόνες σε αρχείο και να διαμορφώσετε το σύστημα ώστε οι παραπάνω κανόνες να εφαρμόζονται κάθε φορά κατά την εκκίνηση του συστήματος

Αποθήκευση κανόνων σε αρχείο με όνομα iptables.rules

```
Applications Places Terminal Sat 06:44
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# iptables-save > /etc/iptables.rules
```

Αποθηκεύουμε τους κανόνες με όνομα iptables.rules στο φάκελο /etc

Στην συνέχεια πάμε και γράφουμε στο αρχείο interfaces με την εντολή
gedit etc/network/interfaces



```
Applications ▾ Places ▾ Text Editor ▾ Sat 06:50
Open ▾ *interfaces /etc/network Save
# 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

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp

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

Με την εντολή

`Pre-up iptables-restore < /etc/iptables.rules` έχουμε τους κανόνες συνέχεια στο σύστημα μας.

Κάνουμε Restart στο σύστημα μας και ελέγχουμε αν έχουν περαστεί οι κανόνες αυτόματα.



```
root@kali:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination          LOG level warning
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere             icmp echo-request
limit: avg 5/sec burst 10
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:smtp
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     icmp --  anywhere              anywhere             icmp echo-request
root@kali:~#
```

Για τις επιτρεπόμενες υπηρεσίες να δημιουργήσετε μία καινούρια αλυσίδα κανόνων με το όνομα WHITELIST. Για την καταγραφή και απόρριψη των πακέτων να δημιουργήσετε μία νέα αλυσίδα με το όνομα LOGNDROPLIST.

Για να φτιάξουμε αυτές τις αλυσίδες θα πρέπει να ξανά περάσουμε του κανόνες με την ονομασία της αλυσίδας που θέλουμε οπότε θα κάνουμε **Append** τους κανόνες μας.

```
root@kali:~# iptables -N WHITELIST

root@kali:~# iptables -N LONGNDROPLIST
root@kali:~#
```




Αρχικά ορίζω δυο λίστες με όνομα WHITELIST, LONGNDROPLIST.

```
File Edit View Search Terminal Help
root@kali:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
LOG        all  --  anywhere               anywhere           LOG level warning
ACCEPT     all  --  anywhere               anywhere
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request limit: avg 5/sec burst 10
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:domain
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:smtp
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:https
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request

Chain LONGNDROPLIST (0 references)
target     prot opt source                destination

Chain WHITELIST (0 references)
target     prot opt source                destination
root@kali:~#
```

Περνάω με την ίδια διαδικασία του κανόνες που αφορούν τις υπηρεσίες στην αλυσίδα WHITELIST

```
root@kali:~# iptables -I WHITELIST -p tcp --dport 53 -j ACCEPT
root@kali:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
LOG        all  --  anywhere               anywhere           LOG level warning
ACCEPT     all  --  anywhere               anywhere
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request limit: avg 5/sec burst 10
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:domain
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:smtp
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:https
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     icmp --  anywhere               anywhere           icmp echo-request

Chain LONGNDROPLIST (0 references)
target     prot opt source                destination

Chain WHITELIST (0 references)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere               anywhere           tcp dpt:domain
root@kali:~#
```

Με την εντολή:

iptables -I WHITELIST -p tcp --dport 53 -j ACCEPT



```
root@kali:~# iptables -I WHITELIST -p tcp --dport 80 -j ACCEPT
root@kali:~# iptables -I WHITELIST -p tcp --dport 25 -j ACCEPT
root@kali:~# iptables -I WHITELIST -p tcp --dport 443 -j ACCEPT
root@kali:~#
```

Με την ίδια διαδικασία δηλώνω όλες τις υπηρεσίες dns,http,https,smtp

```
root@kali:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            LOG level warning
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere              icmp echo-request limit: avg 5/sec burst 10
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:domain
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:smtp
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination            icmp echo-request

Chain LONGNDROPLIST (0 references)
target     prot opt source                destination            I

Chain WHITELIST (0 references)
target     prot opt source                destination            tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:smtp
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:domain
root@kali:~#
```

Στην συνέχεια περνάω στην αλυσίδα LONGNDROP.

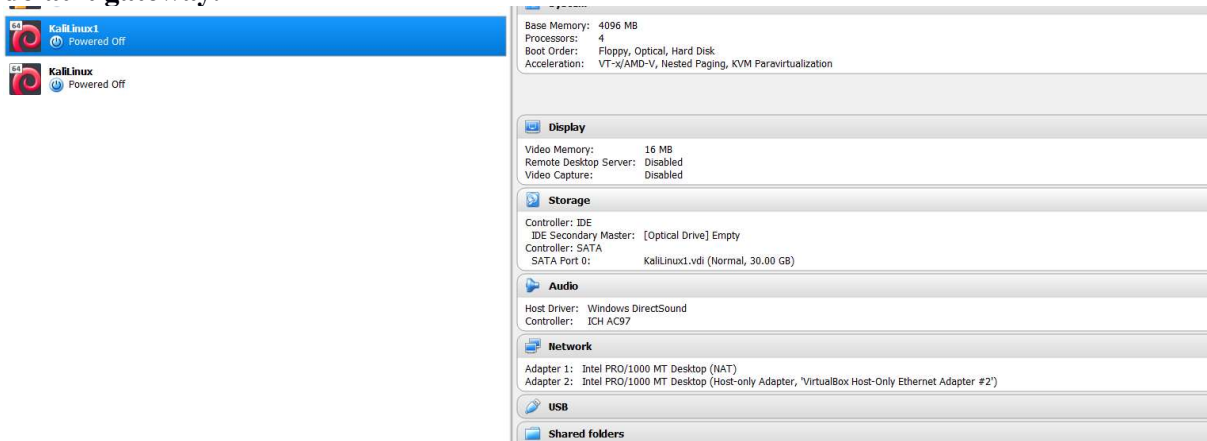
```
Applications ▾ Places ▾ Terminal ▾ Mon 05:57
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iptables -I LONGNDROPLIST -j LOG
```



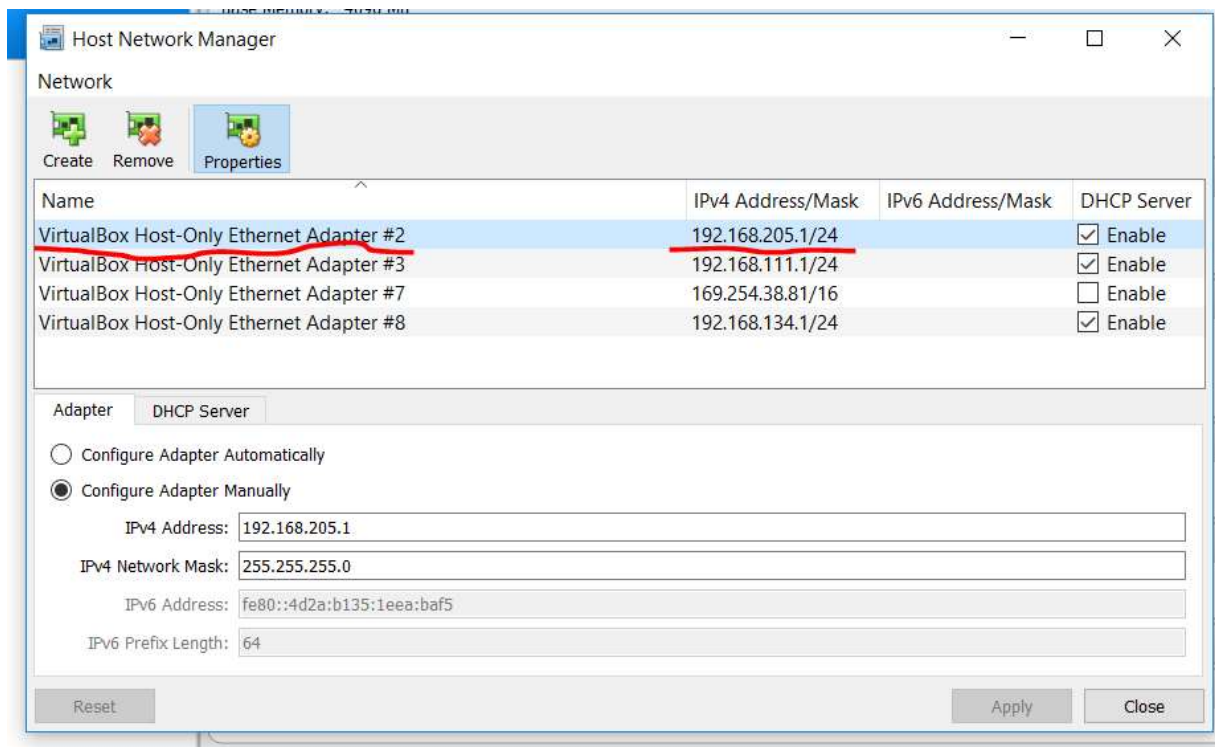
```
iptables: bad built-in chain name.  
root@kali:~# iptables -L  
Chain INPUT (policy DROP)  
target prot opt source destination LOG level warning  
LOG all -- anywhere anywhere  
ACCEPT all -- anywhere anywhere  
ACCEPT icmp -- anywhere anywhere icmp echo-request limit: avg 5/sec burst 10  
ACCEPT tcp -- anywhere anywhere tcp dpt:domain  
ACCEPT tcp -- anywhere anywhere tcp dpt:smtp  
ACCEPT tcp -- anywhere anywhere tcp dpt:https  
ACCEPT tcp -- anywhere anywhere tcp dpt:http  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
ACCEPT icmp -- anywhere anywhere icmp echo-request  
  
Chain LONGNDROPLIST (0 references)  
target prot opt source destination LOG level warning  
LOG all -- anywhere anywhere  
  
Chain WHITELIST (0 references)  
target prot opt source destination  
ACCEPT tcp -- anywhere anywhere tcp dpt:https  
ACCEPT tcp -- anywhere anywhere tcp dpt:smtp  
ACCEPT tcp -- anywhere anywhere tcp dpt:http  
ACCEPT tcp -- anywhere anywhere tcp dpt:domain  
root@kali:~#
```

B) Στη συνέχεια, να διαμορφώσετε ένα δεύτερο σύστημα (virtual machine) το οποίο θα έχει το ρόλο του default gateway/ δικτυακού firewall για το σταθμό εργασίας. Διαμορφώστε το workstation ώστε να χρησιμοποιεί το default gateway για κάθε εξωτερική επικοινωνία. Στο gateway να διαμορφώσετε μέσω iptables μία πολιτική ασφάλειας δικτυακού firewall. Το δικτυακό firewall θα πρέπει να πραγματοποιεί τους ελέγχους για όλη την κίνηση και να προωθεί (forward) από/προς το σταθμό εργασίας μόνο την κίνηση που είναι επιτρεπτή. Ενδεικτικά, να επιτρέπει στους σταθμούς εργασίας να εκκινήσουν http και https συνδέσεις ή σύνδεση σε υπηρεσία email. Η διαμόρφωσή σας μπορεί να περιλαμβάνει και άλλους κανόνες με βάση την πολιτική δικτύου για τους σταθμούς εργασίας.

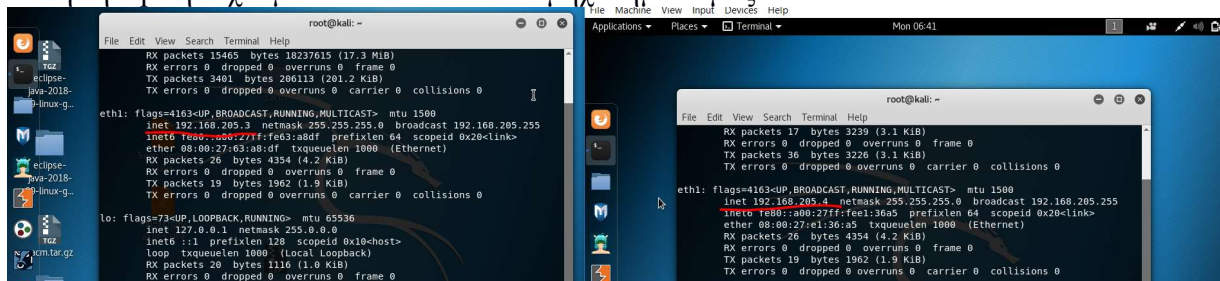
Δημιουργούμε ένα νέο Virtual machine με όνομα Kalilinux1 το οποίο θα έχει τον ρόλο του default gateway.



Έχουμε δημιουργήσει έναν virtual host manager με ip 192.168.205.1



Αυτή την ip την έχουμε δώσει και στα δύο μηχανήματα μας.



Όπως βλέπουμε το Kali Linux ένα έχει οριστεί με την ip 192.168.205.3 και αντίστοιχα 192.168.205.4.

Το default Gate Away που έχουν και τα δύο μηχανήματα είναι η Ip **192.168.205.1/24**.

Για να ορίσουμε το default gateway από το ένα μηχάνημα στο άλλο θα πρέπει να γράψουμε τις ακόλουθες τις εντολές. Θέλουμε να περνάει πρώτα η κίνηση μέσα από KaliLinux1(VM2) και στην συνέχεια να προχωράει στο KaliLinux(VM1).

Ενέργειες στο KaliLinux (ip:192.168.205.4, VM1)

```
route add default gw 192.168.205.3  
route del default gw 192.168.205.1
```




```
Applications ▾ Places ▾ Terminal ▾ Mon 07:05
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# route add default gw 192.168.205.3
```

```
File Edit View Search Terminal Help
root@kali:~# route del default gw 10.0.2.2
```

Διαγράφουμε και με αυτόν τρόπο σταματάμε και την σύνδεση στο Internet.

```
-rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}
root@kali:~# ip r
default via 192.168.205.3 dev eth1
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15
192.168.205.0/24 dev eth1 proto kernel scope link src 192.168.205.4
root@kali:~#
```

Default via 192.168.205.3(KaliLinux)

Ενέργειες στο KaliLinux1 (ip:192.168.205.3, VM2)

1. Μετατροπή του πίνακα nat στο iptables ώστε να υποστηρίζει nat

iptables -t nat -A POSTROUTING -s 192.168.205.0/24 -o eth0 -j MASQUERADE

```
KaliLinux1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Mon 07:19
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iptables -t nat -A POSTROUTING -s 192.168.205.0/24 -o eth0 -j MASQUERADE
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
```

2.Ενεργοποίηση ip forwarding στον host

Στο αρχείο /etc/sysctl.conf βρίσκουμε τη γραμμή: net.ipv4.ip_forward=1 και την ενεργοποιούμε.



```
root@kali:/etc# nano sysctl.conf
```

```
Applications ▾ Places ▾ Terminal ▾ Mon 07:21
root@kali:/etc

File Edit View Search Terminal Help
GNU nano 2.9.5 sysctl.conf Modified

#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
# eclipse-
# kernel.domainname = example.com
#
# Uncomment the following to stop low-level messages on console
# kernel.printk = 3 4 1 3
#
#####
# Functions previously found in netbase
#
# java-2018-
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
# net.ipv4.conf.default.rp_filter=1
# net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
# net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text      ^J Justify      ^C Cur Pos      M-U Undo
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line   M-E Redo
```

Βγάζουμε το σχόλιο για να ενεργοποιήσουμε την εντολή.
Από shell εκτελούμε: `sysctl -p`.

```
root@kali:/etc# nano sysctl.conf
root@kali:/etc# sysctl -p
net.ipv4.ip_forward = 1
root@kali:/etc#
```



Το δικτυακό firewall θα πρέπει να πραγματοποιεί τους ελέγχους για όλη την κίνηση και να προωθεί (forward) από/προς το σταθμό εργασίας μόνο την κίνηση που είναι επιτρεπτή. Ενδεικτικά, να επιτρέπει στους σταθμούς εργασίας να εκκινήσουν http και https συνδέσεις ή σύνδεση σε υπηρεσία email. Η διαμόρφωσή σας μπορεί να περιλαμβάνει και άλλους κανόνες με βάση την πολιτική δικτύου για τους σταθμούς εργασίας.

```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 80 -j ACCEPT
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 443 -j ACCEPT
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- anywhere DMZ 192.168.205.4 tcp dpt:http
ACCEPT tcp -- anywhere 192.168.205.4 tcp dpt:https
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 80 -j ACCEPT
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 443 -j ACCEPT
```

Κάνω αποδοχή να επιτρέπει στους σταθμούς εργασίας να εκκινήσουν http και https

```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 25 -j ACCEPT
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 143 -j ACCEPT
root@kali:~#
```

Αποδοχή σε σύνδεση email.

```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 25 -j ACCEPT
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.205.4 -o eth1 -p TCP --dport 143 -j ACCEPT
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- anywhere DMZ 192.168.205.4 tcp dpt:http
ACCEPT tcp -- anywhere 192.168.205.4 tcp dpt:https
ACCEPT tcp -- anywhere 192.168.205.4 tcp dpt:smtp
ACCEPT tcp -- anywhere 192.168.205.4 tcp dpt:imap2
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 80 -j ACCEPT
root@kali:~# iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 443 -j ACCEPT
```