



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	1- Εντολές διαχείρισης δικτύου
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	13-3-2019



A) Χρησιμοποιώντας την εντολή netstat (με κατάλληλα ορίσματα και πιθανώς σε συνδυασμό με άλλες εντολές) εκτελέστε τα παρακάτω βήματα:

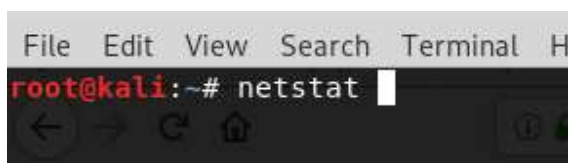
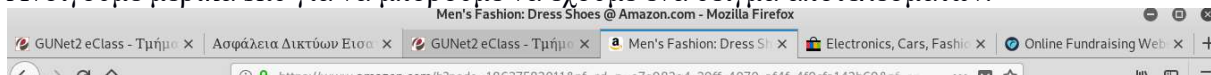
- 1) Προβολή όλων των ενεργών Internet συνδέσεων
- 2) Προβολή όλων των ενεργών Internet συνδέσεων και υπηρεσιών
- 3) Προβολή όλων των ενεργών http συνδέσεων
- 4) Το ίδιο με το βήμα 3 αλλά χωρίς τις εσωτερικές συνδέσεις (self IPs)
- 5) Το ίδιο με το βήμα 3 αλλά με προβολή μόνο IP:port
- 6) Το ίδιο με το βήμα 5 αλλά με προβολή μόνο IP
- 7) Προβολή όλων των ενεργών http συνδέσεων, ταξινομημένων και με μία εγγραφή ανά εξωτερική IP
- 8) Το ίδιο με το βήμα 7 και επιπλέον με μέτρηση συνδέσεων
- 9) Το ίδιο με το βήμα 8 αλλά επιπλέον χωρίς τις εσωτερικές IP Υπόδειξη: Δείτε τα παραδείγματα στον παρακάτω σύνδεσμο [1]



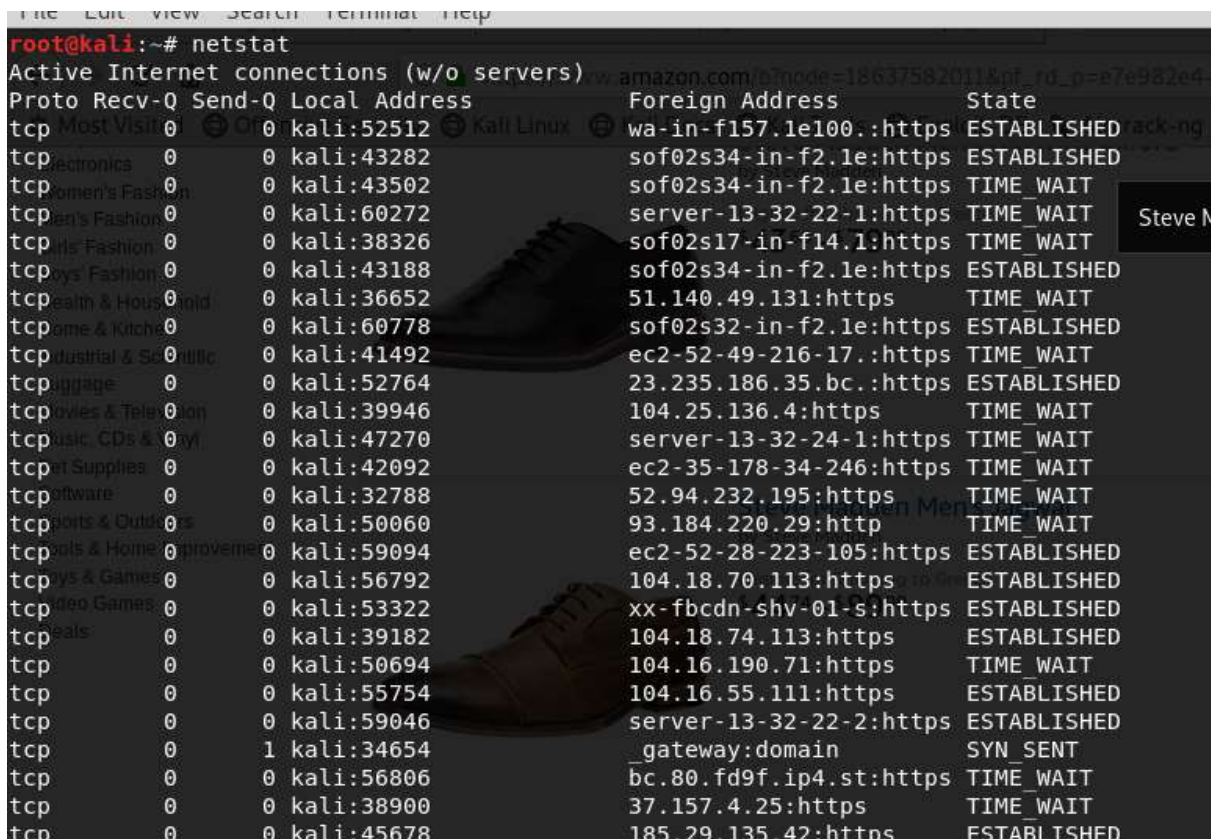
1) Προβολή όλων των ενεργών Internet συνδέσεων

Ανοίγουμε μια γραμμή εντολών και πληκτρολογούμε την εντολή netstat για να κάνουμε προβολή όλων των ενεργών συνδέσεων.

Ανοίγουμε μερικά site για να μπορούμε να έχουμε ένα δείγμα αποτελεσμάτων.



Βλέπουμε τις ενεργές διαδικτυακές συνδέσεις.



Αρχικά μπορούμε να δούμε το πρωτόκολλο στην αρχή υπάρχει μόνο tcp(transmission control protocol) μπορούμε να δούμε την τοπική διεύθυνση καθώς και την κατάσταση στην οποία βρίσκεται.

Στην συνέχεια μπορούμε να δούμε ότι υπάρχουν και μερικές udp (universal Datagram protocol)συνδέσεις.



tcp	0	0	kali:151978	50702917-in-1111e:https	ESTABLISHED	Steven
tcp	0	0	kali:50496	104.20.55.119:https	TIME_WAIT	
tcp	0	0	kali:33074	server-13-32-24-25:http	TIME_WAIT	
tcp	0	0	kali:45892	sof02s18-in-fl1e:https	TIME_WAIT	
tcp	0	0	kali:45314	69.173.144.151:https	TIME_WAIT	
tcp	0	0	kali:56832	a92-123-88-30.dep:https	ESTABLISHED	
udp	0	0	kali:60681	unipiweb.unipi.gr:33494	ESTABLISHED	
udp	0	0	kali:43956	unipiweb.unipi.gr:33496	ESTABLISHED	
udp	0	0	kali:52155	unipiweb.unipi.gr:33508	ESTABLISHED	
udp	0	0	kali:56285	unipiweb.unipi.gr:33505	ESTABLISHED	
udp	0	0	kali:48606	unipiweb.unipi.gr:33497	ESTABLISHED	
udp	0	0	kali:50169	unipiweb.unipi.gr:33499	ESTABLISHED	
udp	0	0	kali:40468	unipiweb.unipi.gr:33498	ESTABLISHED	
udp	0	0	kali:54295	unipiweb.unipi.gr:33500	ESTABLISHED	
udp	0	0	kali:48169	unipiweb.unipi.gr:33502	ESTABLISHED	
udp	0	0	kali:45124	unipiweb.unipi.gr:33507	ESTABLISHED	
udp	0	0	kali:38477	unipiweb.unipi.gr:33495	ESTABLISHED	
udp	0	0	kali:42087	unipiweb.unipi.gr:33506	ESTABLISHED	
udp	0	0	kali:41592	unipiweb.unipi.gr:33504	ESTABLISHED	
udp	0	0	kali:42141	unipiweb.unipi.gr:33501	ESTABLISHED	
udp	0	0	kali:33960	unipiweb.unipi.gr:33493	ESTABLISHED	
udp	0	0	kali:40142	unipiweb.unipi.gr:33503	ESTABLISHED	

2) Προβολή όλων των ενεργών Internet συνδέσεων και υπηρεσιών



```
Applications ▾ Places ▾ Terminal ▾ Tue 07:14 1
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 kali:33022             server-13-32-176-:https TIME_WAIT
tcp        0      0 kali:48232             mil04s28-in-f2.1e:https ESTABLISHED
tcp        0      0 kali:49994             wb-in-f154.1e100.:https ESTABLISHED
tcp        0      0 kali:36440             mil04s26-in-f2.1e:https ESTABLISHED
tcp        0      0 kali:45454             93.184.220.29:http      ESTABLISHED
tcp        0      0 kali:36438             mil04s26-in-f2.1e:https ESTABLISHED
tcp        0      0 kali:57778             mil04s28-in-f10.1:https ESTABLISHED
tcp        0      0 kali:39340             server-13-32-176-:https TIME_WAIT
tcp        0      0 kali:47406             104.24.108.208:https    ESTABLISHED
tcp        0      0 kali:57330             akamai-kol-7.grnet:http ESTABLISHED
tcp        0      0 kali:35834             mil04s22-in-f74.1:https ESTABLISHED
tcp        0      0 kali:44568             104.244.42.8:https      ESTABLISHED
tcp        0      0 kali:56872             server-13-32-176-:https TIME_WAIT
tcp        0      0 kali:36434             mil04s26-in-f2.1e:https ESTABLISHED
tcp        0      0 kali:36114             mil04s03-in-f14.1:https ESTABLISHED
tcp        0      0 kali:34826             mil04s28-in-f163.:https ESTABLISHED
tcp        0      0 kali:45338             93.184.220.29:http      TIME_WAIT
tcp        0      0 kali:45334             93.184.220.29:http      ESTABLISHED
tcp        0      0 kali:33680             mil04s24-in-f33.1:https ESTABLISHED
tcp        0      0 kali:40404             akamai-kol-8.grnet:http ESTABLISHED
tcp        0      0 kali:49992             mil04s24-in-f4.1e:https ESTABLISHED
tcp        0      0 kali:39606             mil04s29-in-f3.1e1:http ESTABLISHED
tcp        0      0 kali:57280             akamai-kol-7.grnet:http ESTABLISHED
tcp        0      0 kali:59796             mil04s27-in-f14.1:https ESTABLISHED
tcp        0      0 kali:54040             mil04s29-in-f3.1e:https ESTABLISHED
tcp        0      0 kali:52844             ec2-52-31-192-216:https ESTABLISHED
```

Πληκτρολογούμε `netstat -a` για να μας εμφανίσει όλες τις συνδέσεις και τις υπηρεσίες αρχικά βλέπουμε τις συνδέσεις tcp



```
Applications ▾ Places ▾ Terminal ▾ Tue 07:15 1
root@kali: ~
File Edit View Search Terminal Help
tcp 0 0 kali:51678 93.184.220.66:https ESTABLISHED
tcp → 0 0 kali:36146 mil04s03-in-f14.1:https ESTABLISHED
tcp 0 0 kali:39604 mil04s29-in-f3.1e1:http ESTABLISHED
tcp Most Visited 0 0 kali:53682 server-13-32-176-:https ESTABLISHED
tcp 0 0 kali:59254 a23-32-11-47.depl:https ESTABLISHED
tcp 0 0 kali:56470 104.16.170.82:https ESTABLISHED
tcp 0 0 kali:60552 mil04s24-in-f35.1:https ESTABLISHED
tcp 0 0 kali:41820 server-13-32-176-:https ESTABLISHED
tcp Open eclass - 0 0 kali:59258 a23-32-11-47.depl:https ESTABLISHED
tcp 0 0 kali:48118 mil04s23-in-f110.:https ESTABLISHED
tcp Η πλατφόρμα GUNet 0 0 kali:39600 mil04s29-in-f3.1e1:http TIME_WAIT
udp Διαχείριση Ηλεκτρον 0 0.0.0.0:33580 0.0.0.0:* * * *
udp και υποστήριξη την 0 0.0.0.0:bootpc 0.0.0.0:* * * *
raw6 Η πρόσβαση στην 0 0.0.0.0:bootpc 0.0.0.0:* * * *
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ACC ] STREAM LISTENING 12032 /run/systemd/journal/stdout
unix 8 [ ] DGRAM 12035 /run/systemd/journal/socket
unix 2 [ ACC ] STREAM LISTENING 24286 /tmp/.ICE-unix/1071
unix 2 [ ] DGRAM 18184 /run/user/130/systemd/notify
unix 2 [ ACC ] STREAM LISTENING 18188 /run/user/130/systemd/privat
e
unix 2 [ ACC ] STREAM LISTENING 17566 @/tmp/dbus-lkpg9n2v
unix 2 [ ACC ] STREAM LISTENING 23823 /run/user/0/keyring/control
unix 2 [ ACC ] STREAM LISTENING 18195 /run/user/130/gnupg/S.dirmng
r
unix 2 [ ACC ] STREAM LISTENING 18198 /run/user/130/gnupg/S.gpg-ag
ent.extra
unix 2 [ ACC ] STREAM LISTENING 18200 /run/user/130/gnupg/S.gpg-ag
```

Επιπλέον εμφανίζονται και οι udp συνδέσεις καθώς και οι υπηρεσίες.

3) Προβολή όλων των ενεργών http συνδέσεων.

```
Applications ▾ Places ▾ Terminal ▾ Tue 07:25 1
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -an | grep :80 | wc -l
6
root@kali:~# netstat -an | grep :80
tcp 0 0 192.168.247.129:45772 93.184.220.29:80 TIME_WAIT
tcp 0 0 192.168.247.129:45768 93.184.220.29:80 TIME_WAIT
tcp 0 0 192.168.247.129:45754 93.184.220.29:80 ESTABLISHED
tcp 0 0 192.168.247.129:54896 185.29.132.30:80 ESTABLISHED
tcp 0 0 192.168.247.129:45752 93.184.220.29:80 ESTABLISHED
tcp 0 0 192.168.247.129:45770 93.184.220.29:80 TIME_WAIT
root@kali:~#
```

Βρίσκουμε τις συνδέσεις http και τις εμφανίζουμε.

4) Το ίδιο με το βήμα 3 αλλά χωρίς τις εσωτερικές συνδέσεις (self IPs)



```
Applications ▾ Places ▾ Terminal ▾ Tue 07:35 1
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -an | grep :80 | grep -v Listen
```

Για να έχουμε κάποια αποτελέσματα κάθε φορά ανοίγουμε έναν browser.

```
File Edit View Search Terminal Help
root@kali:~# netstat -an | grep :80 | grep -v Listen
tcp 0 0 192.168.247.129:49004 185.29.135.190:80 ... ESTABLISHED
root@kali:~# netstat -an | grep :80 | grep -v Listen
tcp 0 0 192.168.247.129:36864 178.63.17.178:80 ESTABLISHED
tcp 0 0 192.168.247.129:41038 194.177.211.137:80 ESTABLISHED
tcp 0 0 192.168.247.129:36876 178.63.17.178:80 ESTABLISHED
tcp 0 0 192.168.247.129:33784 37.252.172.80:80 ESTABLISHED
tcp 0 0 192.168.247.129:59124 69.173.144.141:80 ESTABLISHED
tcp 0 0 192.168.247.129:59654 216.58.205.66:80 ESTABLISHED
tcp 0 0 192.168.247.129:43660 173.241.240.220:80 ESTABLISHED
tcp 0 0 192.168.247.129:36878 178.63.17.178:80 ESTABLISHED
tcp 0 0 192.168.247.129:36874 178.63.17.178:80 ESTABLISHED
root@kali:~#
```

5) Το ίδιο με το βήμα 3 αλλά με προβολή μόνο IP:port

```
root@kali:~# netstat -antu | grep :80 | grep -v Listen | awk '{print $5}'
178.63.17.178:80
178.63.17.178:80
194.177.211.137:80
178.63.17.178:80
69.173.144.141:80
178.63.17.178:80
216.58.198.1:80
178.63.17.178:80
173.241.240.220:80
216.58.205.162:80
185.33.223.208:80
root@kali:~#
```

6) Το ίδιο με το βήμα 5 αλλά με προβολή μόνο IP



```
File Edit View Search Terminal Help
root@kali:~# netstat -antu | grep :80 | grep -v Listen | awk '{print $5}' | cut -d: -f1
178.63.17.178
178.63.17.178
194.177.211.137
54.230.99.125
23.6.113.10
178.63.17.178
178.63.17.178
173.241.240.143
178.63.17.178
173.241.240.220
216.58.205.162
104.19.236.126
root@kali:~#
```

7) Προβολή όλων των ενεργών http συνδέσεων, ταξινομημένων και με μία εγγραφή ανά εξωτερική IP.

```
root@kali:~# netstat -antu | grep :80 | grep -v Listen | awk '{print $5}' | cut -d: -f1 | sort | uniq -c
1 173.241.240.220
5 178.63.17.178
1 185.33.223.208
1 194.177.211.137
1 216.58.198.34
1 69.173.144.141
root@kali:~#
```

8) Το ίδιο με το βήμα 7 και επιπλέον με μέτρηση συνδέσεων.

```
File Edit View Search Terminal Help
root@kali:~# netstat -antu | grep :80 | grep -v Listen | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -rn
5 178.63.17.178
1 38.67.14.240
1 31.172.81.172
1 31.172.81.160
1 216.58.198.34
1 194.177.211.137
1 173.241.240.220
1 173.241.240.143
1 104.16.92.60
root@kali:~#
```

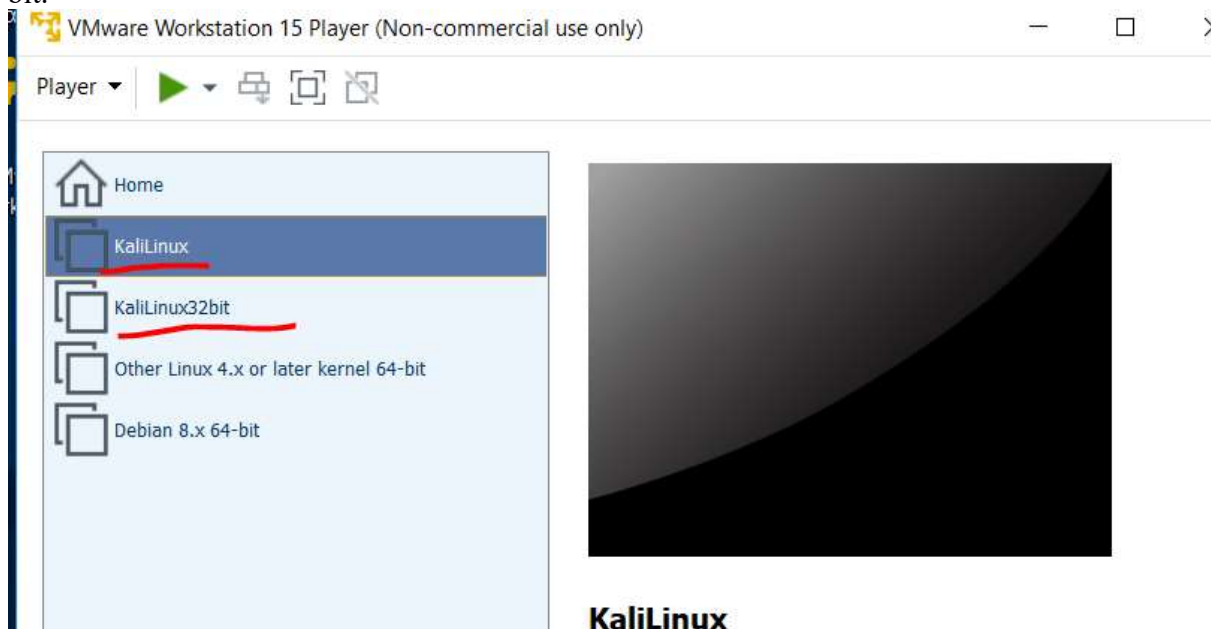
9) Το ίδιο με το βήμα 8 αλλά επιπλέον χωρίς τις εσωτερικές IP



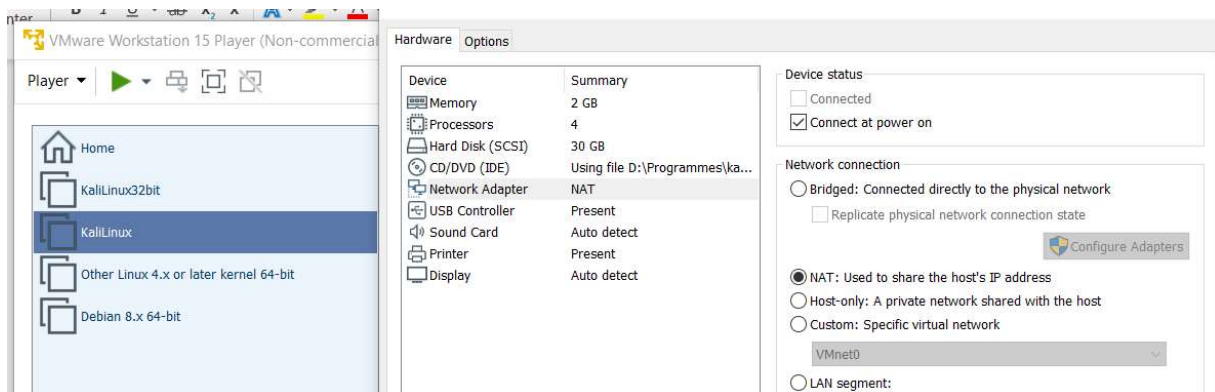
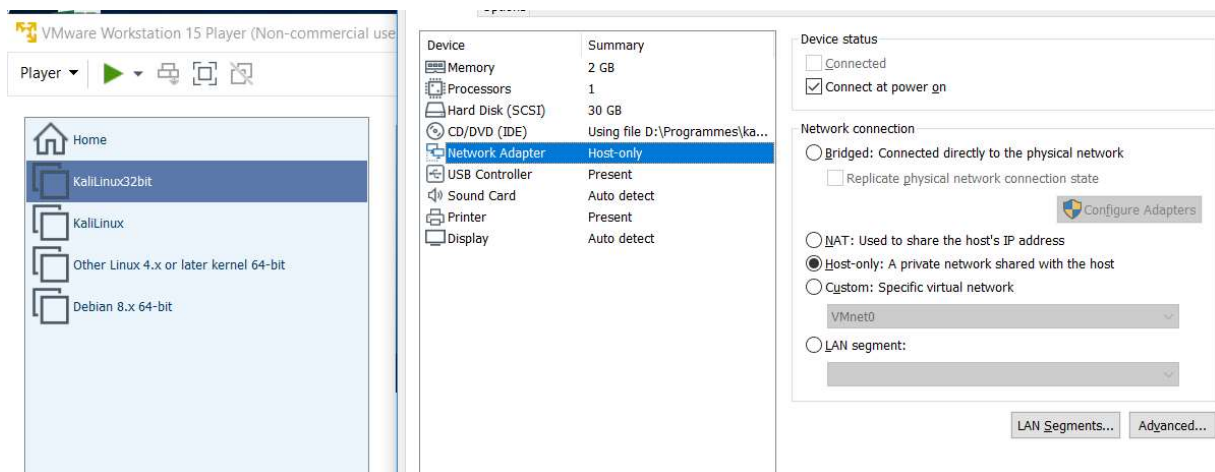
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# netstat -antv | grep :80 | grep -v Listen | awk '{print $5}' | cut -d: -f1  
| sort | uniq -c | sort -rn | grep -v 127.0.0.1  
10 178.63.17.178  
2 194.177.211.137  
2 173.241.240.220  
1 69.173.144.141  
1 38.67.14.240  
1 31.172.81.172  
1 31.172.81.160  
1 216.58.205.162  
1 216.58.198.34  
1 216.58.198.1  
1 185.33.223.218  
1 173.241.240.143  
1 104.16.92.60  
root@kali:~#
```

B) Σε εικονικό περιβάλλον με δύο εικονικές μηχανές linux τροποποιήστε τη δικτύωση ώστε η μία μηχανή να έχει ως default gateway τη δεύτερη μηχανή. Χρησιμοποιήστε την εντολή traceroute ή/και άλλες εντολές ώστε να επαληθεύσετε την επιτυχή διαμόρφωση. Υπόδειξη: Δείτε το αντίστοιχο παράδειγμα στα βοηθητικά αρχεία της ενότητας 1 στο φάκελο των εργαστηριακών μαθημάτων.

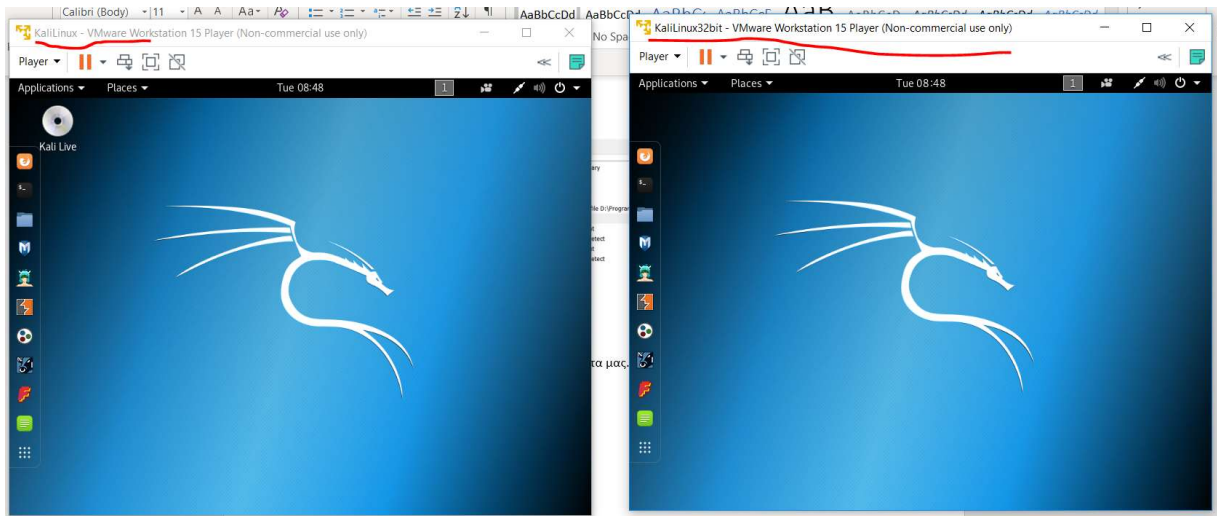
Δημιουργία στο vmWare δυο λειτουργικών συστημάτων KaliLinux το ένα 32 bit και το άλλο 64 bit.



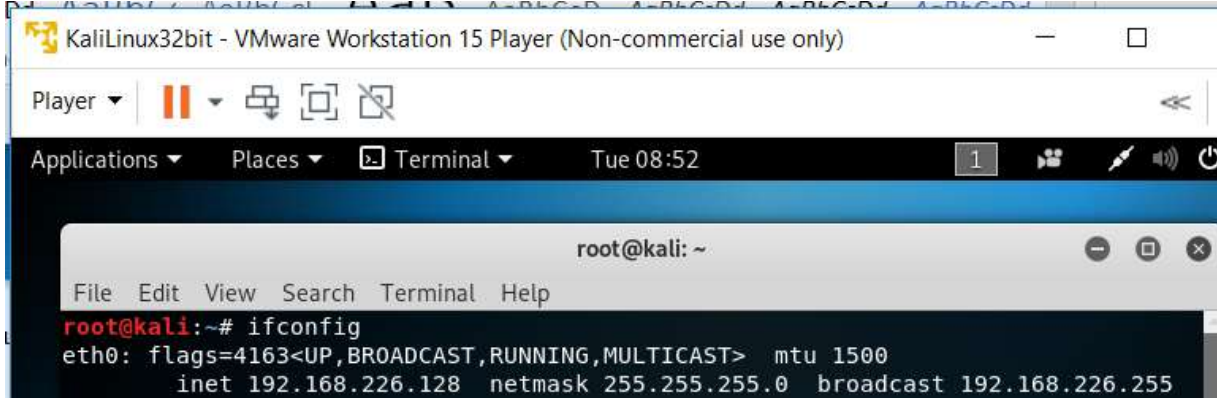
Ορισμός στις ρυθμίσεις του internet για το ένα μηχανήμα θα έχει nat σύνδεση και για το άλλο μηχανήμα θα έχει host only network.



Στην συνέχεια συνδεόμαστε και στα δύο μηχανήματα μας έτσι ώστε να είναι ενεργά.

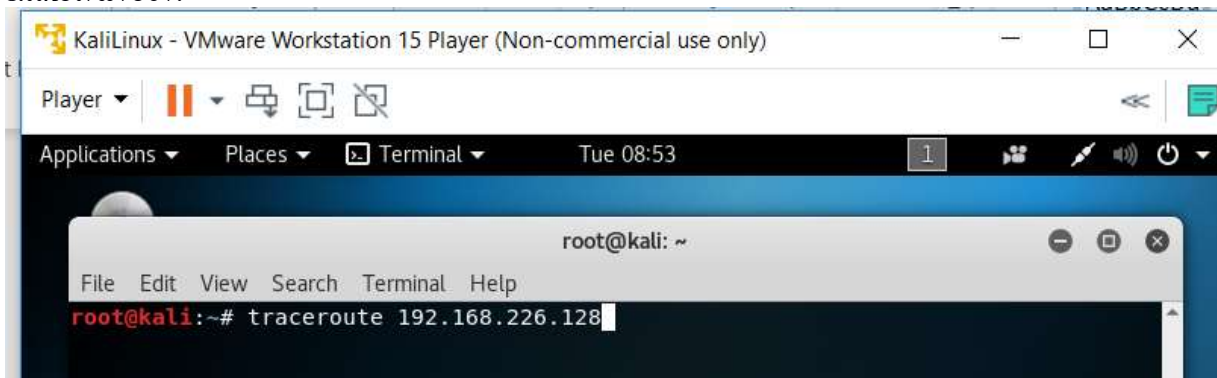


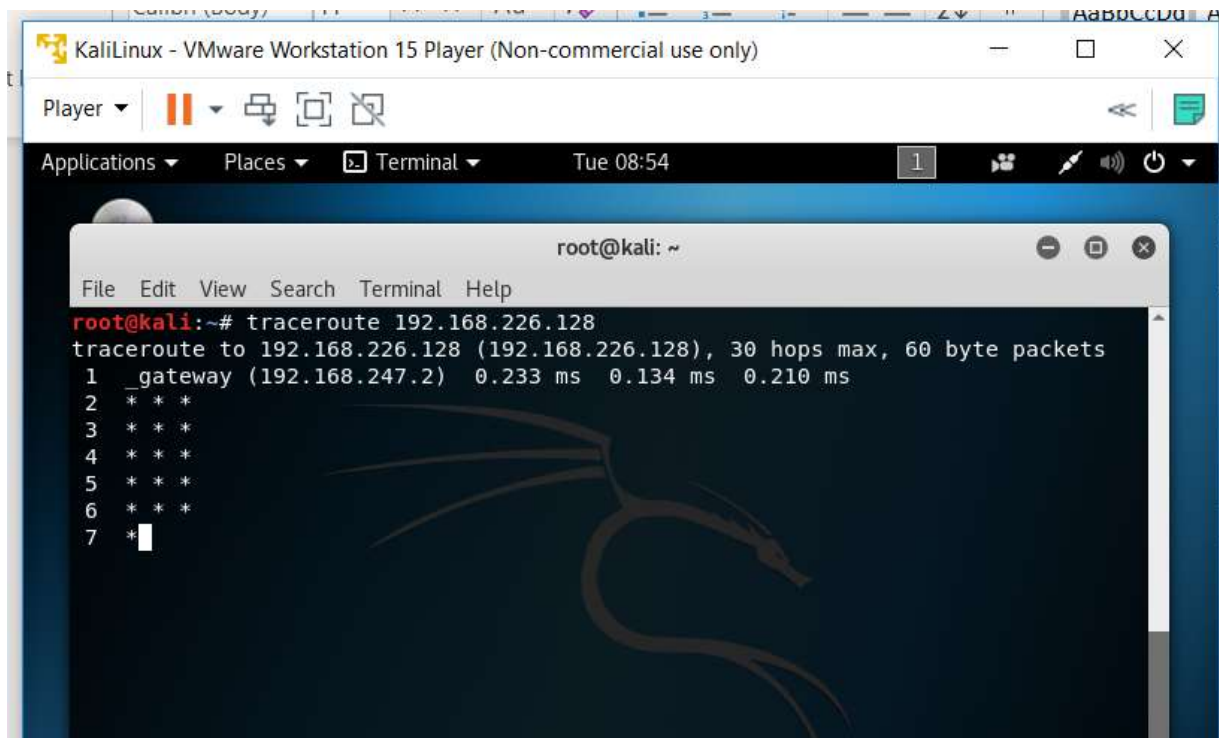
Ανοίγουμε και στα δύο μια γραμμή εντολών και ελέγχουμε αν το KaliLinux επικοινωνεί με KaliLinux32bit



Έχει ip 192.168.226.128

Πηγαίνουμε στο άλλο μηχανήμα και με την εντολή traceroute 192.168.226.128 ελέγχουμε αν επικοινωνούν.

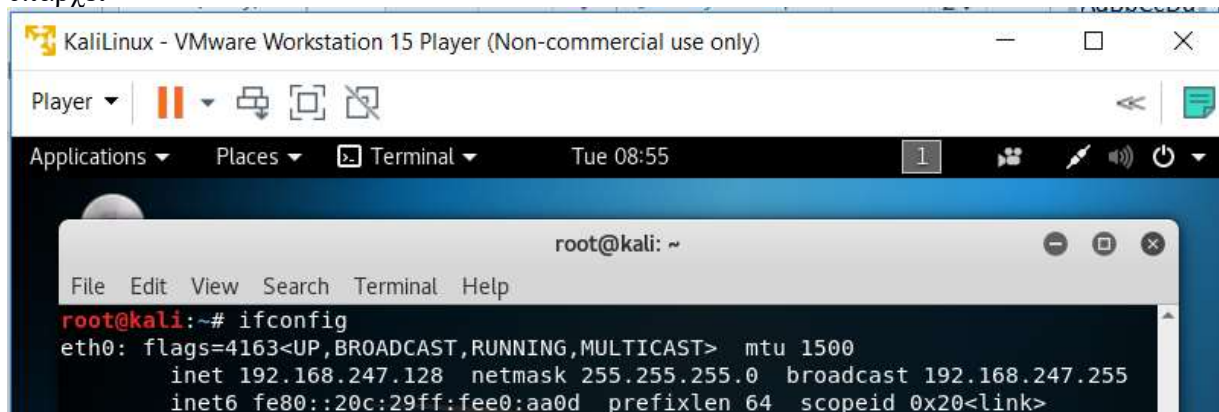




```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# traceroute 192.168.226.128  
traceroute to 192.168.226.128 (192.168.226.128), 30 hops max, 60 byte packets  
1 _gateway (192.168.247.2) 0.233 ms 0.134 ms 0.210 ms  
2 * * *  
3 * * *  
4 * * *  
5 * * *  
6 * * *  
7 * 
```

Υπάρχει επικοινωνία.

Αντίθετα τώρα αν κάνουμε ελέγχω να υπάρχει αντίστροφη επικοινωνία θα δούμε ότι δεν υπάρχει



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.247.128 netmask 255.255.255.0 broadcast 192.168.247.255  
inet6 fe80::20c:29ff:fee0:aa0d prefixlen 64 scopeid 0x20<link>
```

Ip 192.168.247.128

Τρέχουμε την εντολή traceroute



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# traceroute 192.168.247.128  
traceroute to 192.168.247.128 (192.168.247.128), 30 hops max, 60 byte packets  
connect: Network is unreachable  
root@kali:~#
```

Μας εμφανίζει ότι το δίκτυο είναι απρόσιτο δηλαδή μόνο ο host μπορεί να επικοινωνήσει.