

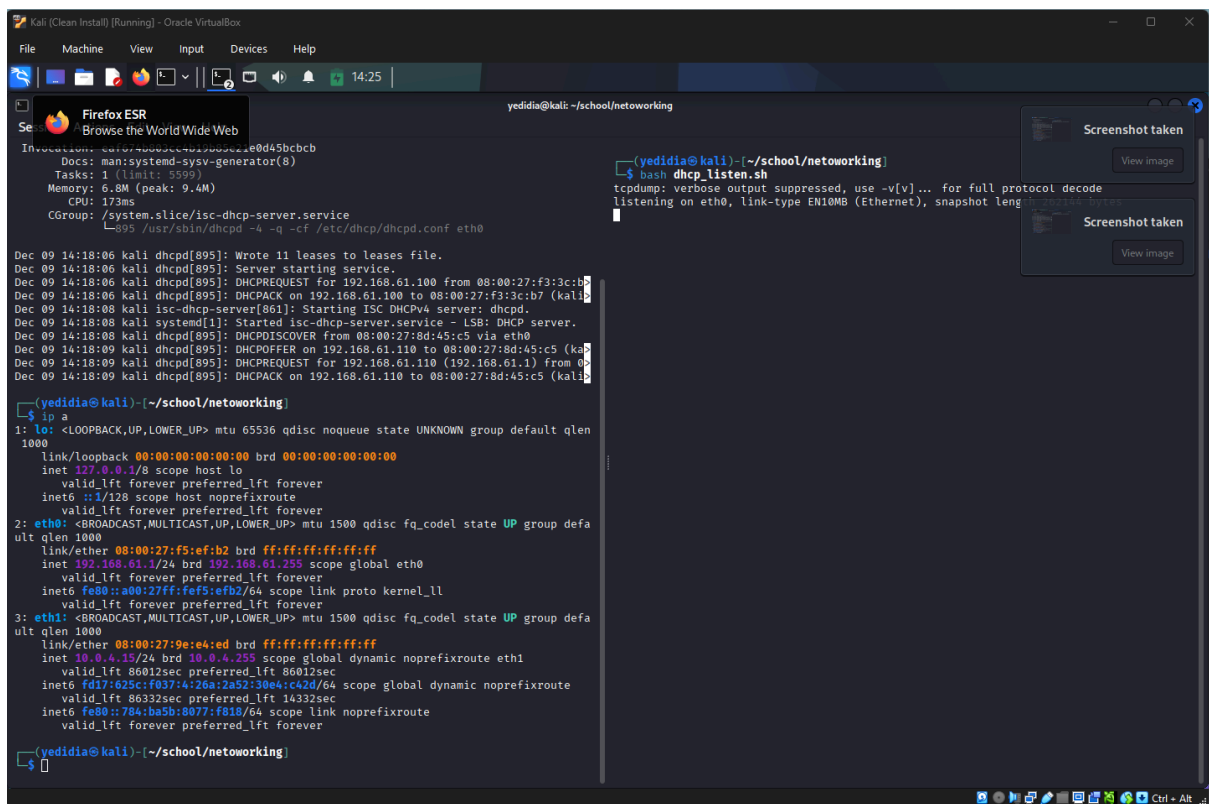
## מעבדה 4 - הרעבת שרת DHCP

ידידיה בקורדזה: 332461854  
מאיר קרומבי: 214736688

במעבדה הזאת אנחנו נגדיר שרת DHCP שיהיה אחראי על חלוקת כתובות IP לרשת פנימית שנגדיר. בנוסף נריץ 2 מכונות נוספות שאחת תריץ את ההתקפה עד שלשרת DHCP יגמרו כל הכתובות, והשניה שתנסה לבקש כתובת חדשה ותראה כי לא נותר דבר.

לשם הנוחות הגדרנו שהכתובות ששרת ה-DHCP יחלק יהיו 10, וטווח הכתובות יהיה: 192.168.61.100-110

נאתחל את השרת DHCP במכונה ונאזין להודעות שנכנסות לפורט 67 או 68:



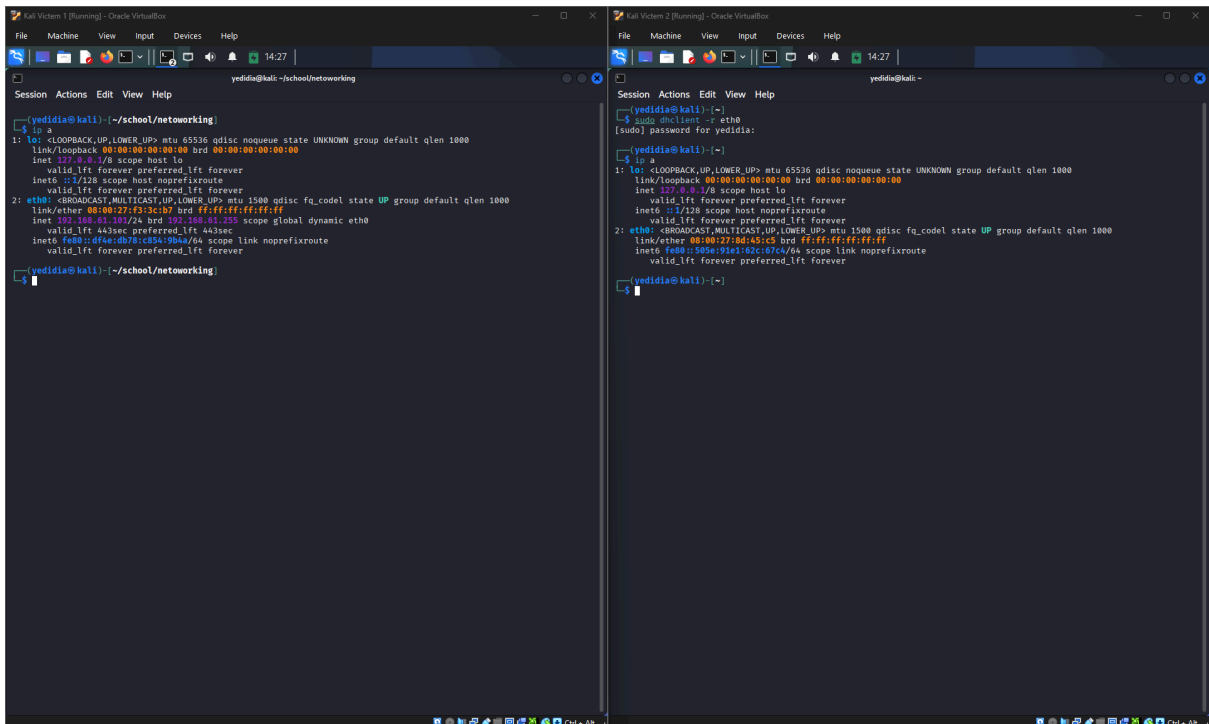
```
Kali (Clean Install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

yvedidia@kali: ~/school/networking
$ bash dhcp_listen.sh
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 1500

Dec 09 14:18:06 kali dhcpd[895]: Server starting service.
Dec 09 14:18:06 kali dhcpd[895]: DHCPREQUEST for 192.168.61.100 from 08:00:27:f3:3c:b7 (kali)
Dec 09 14:18:06 kali dhcpd[895]: DHCPACK on 192.168.61.100 to 08:00:27:f3:3c:b7 (kali)
Dec 09 14:18:08 kali isc-dhcp-server[861]: Starting ISC DHCPv4 server: dhcpd.
Dec 09 14:18:08 kali systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
Dec 09 14:18:08 kali dhcpd[895]: DHCPDISCOVER from 08:00:27:8d:45:c5 via eth0
Dec 09 14:18:09 kali dhcpd[895]: DHCPOFFER on 192.168.61.110 to 08:00:27:8d:45:c5 (kali)
Dec 09 14:18:09 kali dhcpd[895]: DHCPREQUEST for 192.168.61.110 (192.168.61.1) from 08:00:27:8d:45:c5 (kali)
Dec 09 14:18:09 kali dhcpd[895]: DHCPACK on 192.168.61.110 to 08:00:27:8d:45:c5 (kali)

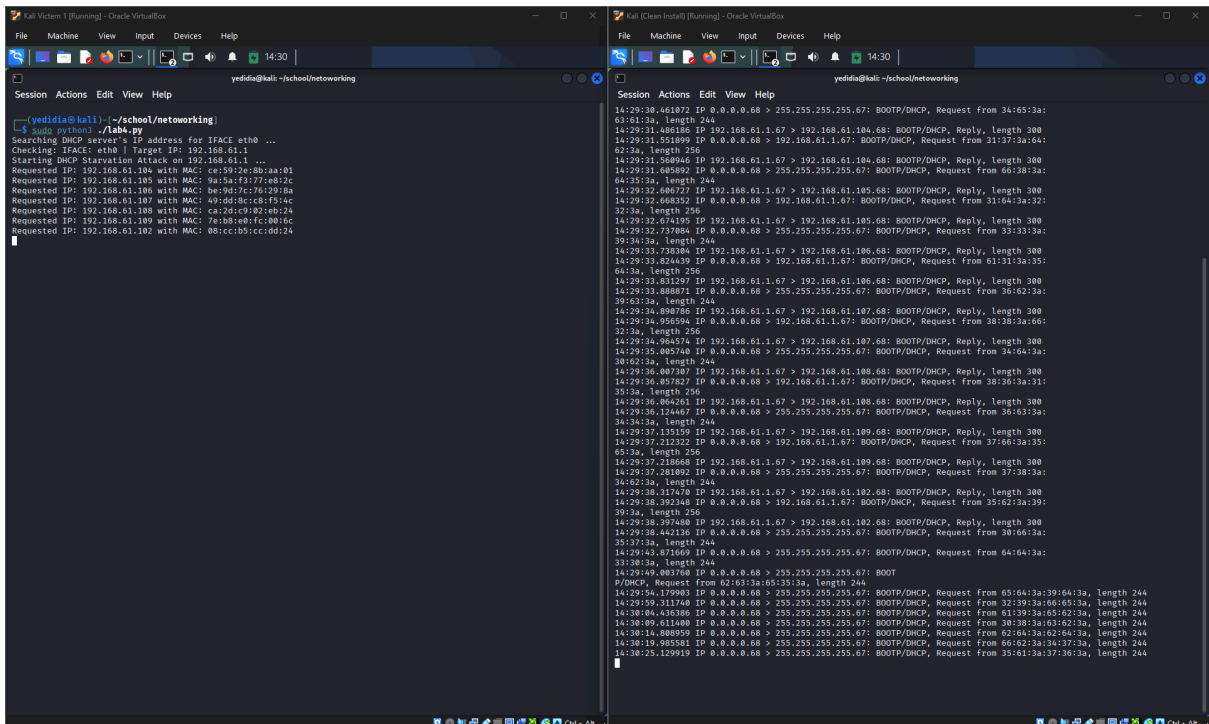
(yvedidia@kali)~[/school/networking]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f5:ef:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.61.1/24 brd 192.168.61.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe5:efb2/64 scope link proto kernel lladdr fe80::a00:27ff:fe5:efb2
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9e:e4:ed brd ff:ff:ff:ff:ff:ff
    inet 10.0.4.15/24 brd 10.0.4.255 scope global dynamic noprefixroute eth1
        valid_lft 86012sec preferred_lft 86012sec
    inet6 fd17::d25e:f037:a:26a:2a52:300e:c42d/64 scope global dynamic noprefixroute
        valid_lft 86332sec preferred_lft 14332sec
    inet6 fe80::784:ba5b:8077:f818/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

נריץ את 2 המכונות האחרות כאשר למכונה אחת נרצה לשחרר את כתובת הIP שהיא קיבלה מהשרת DHCP:

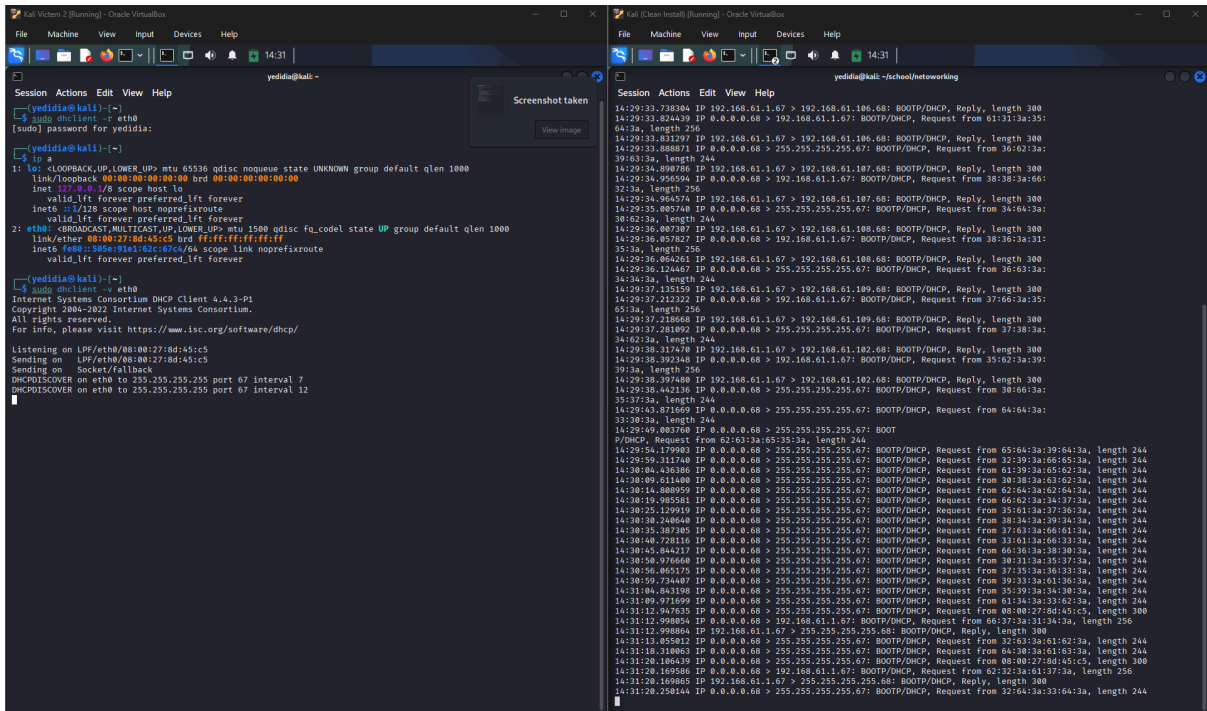


נרץ את ההתקפה מהמחשב שכן יש לו כתובת IP, ההתקפה תייצר כתובת MAC רנדמוליות ותבקש עבורם כתובת IP ותאשר אותם בהודעה חוזרת. היא תשמור במילון את כתובת ה-IP וה-MAC עבורה כך שמיד"י פעם תהליכון של המערכת יעדכן את שרת ה-DHCP שהוא עדיין משתמש בכתובת IP שהיא הקצתה לה ולכן שלא תשחרר אותה מידיה.

נרץ את ההתקפה ונראה כי אין לשרת כתובות נוספות להחזיר למתקיף



וכעת ננסה לבקש כתובת IP חדשה מהמחשב שאין לו ונראה שבקשת ה-DHCP שלו גם נשארת תלויה באוויר כי הוא לא מצליח להשיג כתובת פנויה:



בצורה הזאת גם מימשנו את הבנוס של persistent כך שההתקפה תמשיך להשפיע לאורך זמן.

הלוגים של dhcp leases:

```
server-uid "\000\001\000\0010\312\364\374\010\000\365\357\262";
```

```
lease 192.168.61.110 {
  starts 2 2025/12/09 22:51:29;
  ends 2 2025/12/09 23:01:29;
  cltt 2 2025/12/09 22:51:29;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:8d:45:c5;
  uid "\001\010\000\215E\305";
  client-hostname "kali";
}
```

```
lease 192.168.61.101 {
  starts 2 2025/12/09 22:52:07;
  ends 2 2025/12/09 23:02:07;
  cltt 2 2025/12/09 22:52:07;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:ca:f9:92;
  uid "\001\010\000\312\371\222";
  client-hostname "kali";
}
```

```
}  
lease 192.168.61.102 {  
  starts 2 2025/12/09 22:52:13;  
  ends 2 2025/12/09 23:02:13;  
  cltt 2 2025/12/09 22:52:13;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 63:38:3a:63:34:3a;  
}  
lease 192.168.61.103 {  
  starts 2 2025/12/09 22:52:30;  
  ends 2 2025/12/09 23:02:30;  
  cltt 2 2025/12/09 22:52:30;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 38:65:3a:33:61:3a;  
}  
lease 192.168.61.104 {  
  starts 2 2025/12/09 22:52:46;  
  ends 2 2025/12/09 23:02:46;  
  cltt 2 2025/12/09 22:52:46;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 38:35:3a:37:31:3a;  
}  
lease 192.168.61.105 {  
  starts 2 2025/12/09 22:53:02;  
  ends 2 2025/12/09 23:03:02;  
  cltt 2 2025/12/09 22:53:02;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 36:64:3a:34:62:3a;  
}  
lease 192.168.61.106 {  
  starts 2 2025/12/09 22:53:19;  
  ends 2 2025/12/09 23:03:19;  
  cltt 2 2025/12/09 22:53:19;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 62:34:3a:38:37:3a;  
}  
lease 192.168.61.107 {  
  starts 2 2025/12/09 22:53:35;
```

```
ends 2 2025/12/09 23:03:35;
cltt 2 2025/12/09 22:53:35;
binding state active;
next binding state free;
rewind binding state free;
hardware ethernet 66:64:3a:38:30:3a;
}
lease 192.168.61.108 {
starts 2 2025/12/09 22:53:51;
ends 2 2025/12/09 23:03:51;
cltt 2 2025/12/09 22:53:51;
binding state active;
next binding state free;
rewind binding state free;
hardware ethernet 38:62:3a:34:64:3a;
}
lease 192.168.61.109 {
starts 2 2025/12/09 22:54:07;
ends 2 2025/12/09 23:04:07;
cltt 2 2025/12/09 22:54:07;
binding state active;
next binding state free;
rewind binding state free;
hardware ethernet 36:64:3a:63:65:3a;
}
lease 192.168.61.100 {
starts 2 2025/12/09 22:54:24;
ends 2 2025/12/09 23:04:24;
cltt 2 2025/12/09 22:54:24;
binding state active;
next binding state free;
rewind binding state free;
hardware ethernet 31:65:3a:37:66:3a;
}
```