

## מבדקה 4 - הרעבת שרת DHCP

ידידה בקורדזה: 332461854  
מאיר קרומבי: 214736688

במבדקה הזאת אנחנו נגידר שרת DHCP שהוא אחראי על חלוקת כתובות IP לרשת פנימית שנגידר. בנוסף נרים 2 מכונות חדשות שאחת תריש את התקופה עד לשרת DHCP יגמר כל הכתובות, והשנייה שתנסה לבקש כתובת חדשה ותראה כי לא יותר דבר.

לשם הנוחות הגדרנו שהכתובות ששרת DHCP יחולק יהיו 10, וטוחה הכתובות יהיה:  
192.168.61.100-110

נתחל את השירות DHCP במכונה ונazzi להודעות שנכנסות לפורט 67 או 68:

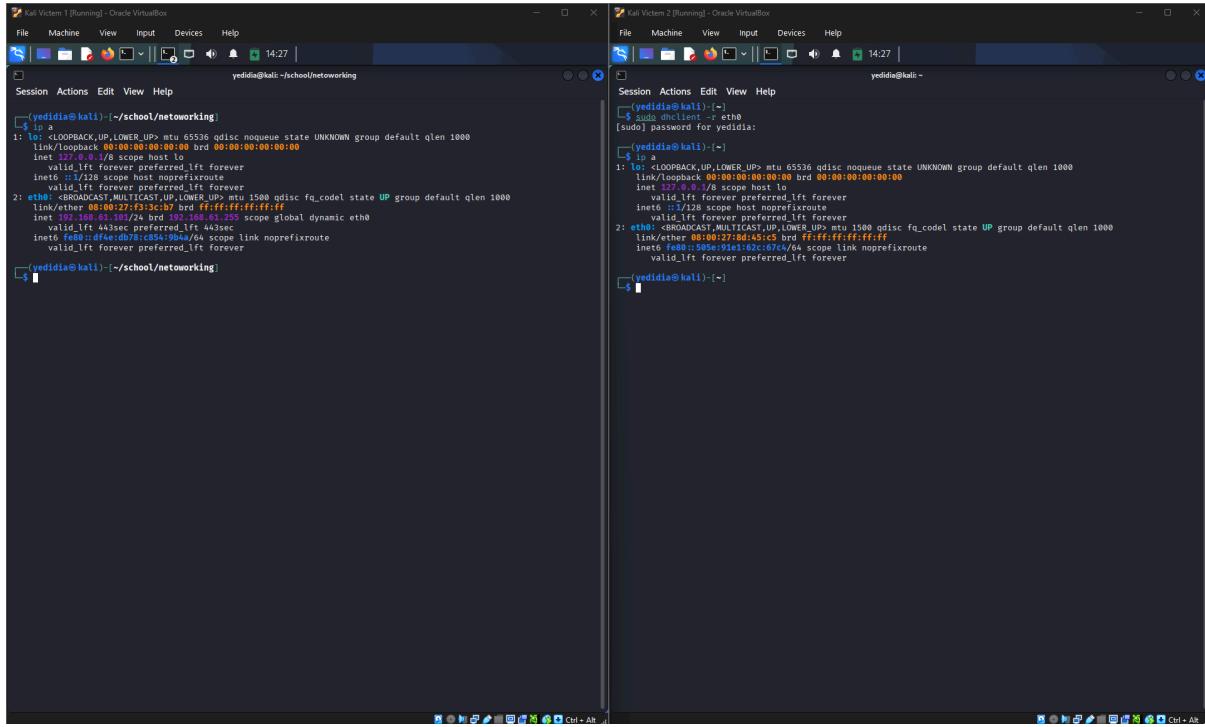
```
yedidia@kali: ~/school/networking
yedidia@kali:~/school/networking$ dhclient -v
Sess 1 [yedidia@kali] - [~/school/networking]
Tasks: 1 (limit: 5599)
Memory: 6.8M (9.4M)
CPU: 173ms
CGroup: /system.slice/isc-dhcp-server.service
        └─ 895 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf

Dec 09 14:18:06 kali dhcpd[895]: Wrote 11 leases to leases file.
Dec 09 14:18:06 kali dhcpd[895]: Server starting service.
Dec 09 14:18:06 kali dhcpd[895]: DHCPREQUEST from 192.168.61.100 to 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]: DHCPOFFER from 08:00:27:8d:45:c5 via eth0
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)

(yedidia@kali)-[~/school/networking]
yedidia@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 brd 127.255.255.255 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:feff:efb2/64 scope link proto kernel ll
            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 fd17:625c:1037:4:26a:2a52:30e4::42d/64 scope global dynamic noprefixroute
            valid_lft 86332sec preferred_lft 14332sec
            inet6 fe80::784:b45b:8077:f010/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

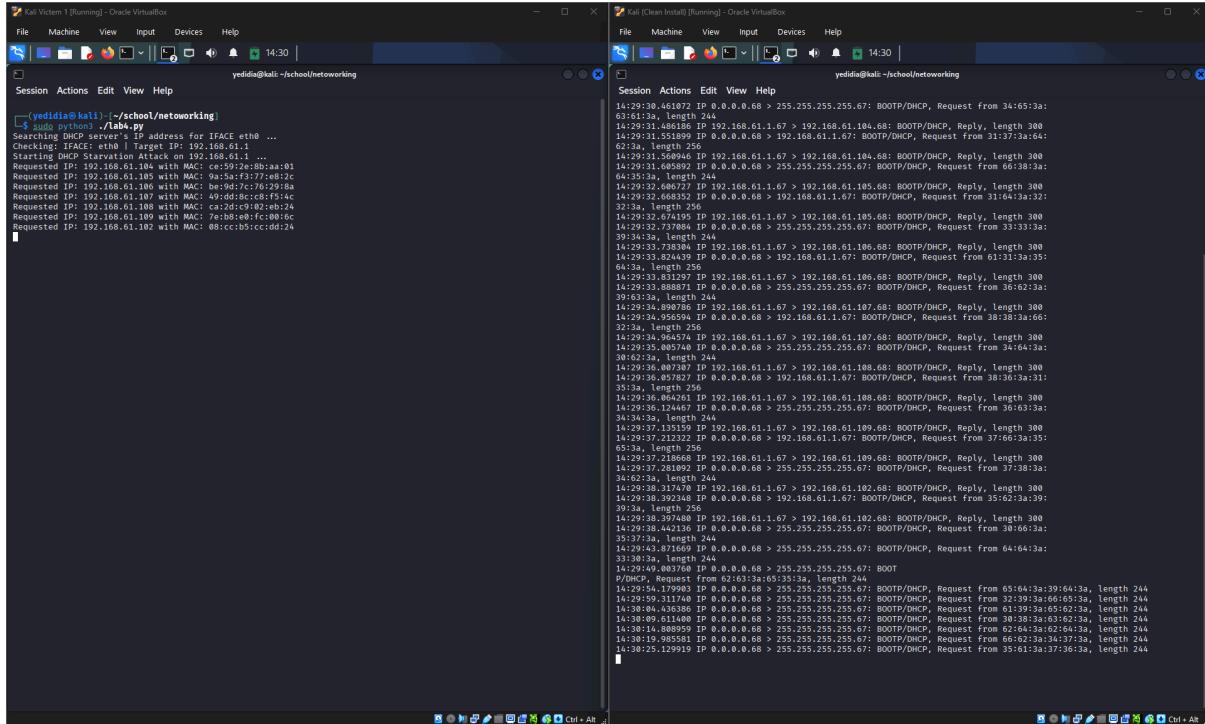
(yedidia@kali)-[~/school/networking]
```

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



נريץ את ההתקפה מהמחשב שכן יש לו כתובת IP, ההתקפה תיצור כתובת MAC רנדומליות ותבקש עבורים כתובת IP ותאשר אותן בהודעה חוזרת. היא תשמור במילון את כתובת ה-IP וה-MAC-IP כר' שמייד".  
פעם תהליכין של המערכת יעדכן את שרת-DHCP שהוא עדין משתמש בכתובת IP שהיא הקצתה לה וכן שלא תשחרר אותה מידיה.

#### נריץ את ההתקפה ונראה כי אין לשרת כתובות נוספות להחזיר למקיף



וכעת ננסה לבקש כתובת IP חדשה מהמחשב שאינו לו נוראה שבקשת DHCP שלו גם נשארת תליה  
באויר כי הוא לא מצליח להציג כתובת פנוייה:

```

yedidia@kali:~$ sudo dhclient -r eth0
[sudo] password for yedidia:
(yedidia@kali)~-
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN link/nooprxroute
    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 00:0c:29:7c:0f:4f brd ff:ff:ff:ff:ff:ff state UNKNOWN link/nooprxroute
    valid_lft forever preferred_lft forever
(yedidia@kali)~-
yedidia@kali:~$ sudo dhclient -v eth0
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp

Listening on LPF/eth0:08:00:27:8d:45:c5
Sending on LPF/eth0:08:00:27:8d:45:c5
Sending on Socket/Fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 12
yedidia@kali:~$
```

```

yedidia@kali:~$ sudo dhclient -v eth0
[sudo] password for yedidia:
(yedidia@kali)~-
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN link/nooprxroute
    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 00:0c:29:7c:0f:4f brd ff:ff:ff:ff:ff:ff state UNKNOWN link/nooprxroute
    valid_lft forever preferred_lft forever
(yedidia@kali)~-
yedidia@kali:~$
```

בכזה הՁאת גם מימשו את הבונוס של `presistent` כך שההתקפה תמשיך לפחות זמן.

### הlogenim של dhcp.leases

server-duid "\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;
}
```