



# MAC Address Spoofing via macchanger

*Last updated 9/4/2017*



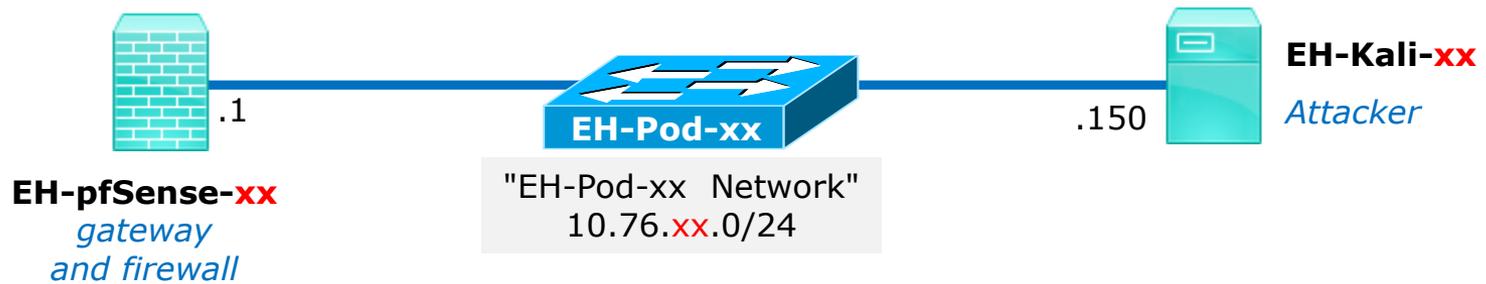
# Admonition



## **Unauthorized hacking is a crime.**

**The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.**

**Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.**



*In this example, the Kali will ping the pfSense VM using spoofed MAC addresses*



## Requirements

1. Kali VM at Baseline snapshot.

## Layer 2 - MAC Address Spoofing

Why would a hacker do this?

- Create an anonymous identity for a network device.
- Impersonate another network device.
- Gain unauthorized access to services.
- Bypass access control lists that allow and block specific MAC addresses.

[https://en.wikipedia.org/wiki/MAC\\_spoofing](https://en.wikipedia.org/wiki/MAC_spoofing)

# macchanger

## macchanger --help

```
root@eh-kali-05:~# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help                Print this help
-V, --version             Print version and exit
-s, --show                Print the MAC address and exit
-e, --ending              Don't change the vendor bytes
-a, --another             Set random vendor MAC of the same kind
-A                        Set random vendor MAC of any kind
-p, --permanent          Reset to original, permanent hardware MAC
-r, --random              Set fully random MAC
-l, --list[=keyword]     Print known vendors
-b, --bia                 Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX
    --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
root@eh-kali-05:~# █
```

*Use macchanger to change (spoof) the MAC address of an interface*

## macchanger example 1

The image shows a network traffic capture window and a terminal window. The traffic capture window displays two ICMP packets: a request from 10.76.5.150 to 10.76.5.1 and a reply from 10.76.5.1 to 10.76.5.150. The details for Frame 13 show the source MAC address as 00:50:56:af:a5:87, which is highlighted with a red box. The terminal window shows the commands used to verify the MAC address and perform the ping.

No.	Time	Source	Destination	Protocol	Length	Info
→	13 15.291734852	10.76.5.150	10.76.5.1	ICMP	98	Echo (ping) request id=0x...
←	14 15.291931717	10.76.5.1	10.76.5.150	ICMP	98	Echo (ping) reply id=0x...

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# ip link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:af:a5:87 brd ff:ff:ff:ff:ff:ff
root@eh-kali-05:~# ping -c1 10.76.5.1
PING 10.76.5.1 (10.76.5.1) 56(84) bytes of data.
64 bytes from 10.76.5.1: icmp_seq=1 ttl=64 time=0.217 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.217/0.217/0.217/0.000 ms
root@eh-kali-05:~#

```

**ip link show dev eth0**  
**ping -c1 10.76.5.1**

*Kali pings pfSense with permanent MAC address*

## macchanger example 2

The screenshot shows two windows. The top window is Wireshark, displaying a packet capture of an ICMP echo request and reply between 10.76.5.150 and 10.76.5.1. The MAC address 00:00:28:a2:78:17 is highlighted in red in the Ethernet II section of the packet details.

The bottom window is a terminal on a Kali Linux machine (root@eh-kali-05). It shows the execution of the following commands and their output:

```

root@eh-kali-05:~# macchanger -A eth0
Current MAC: 00:50:56:af:a5:87 (VMware, Inc.)
Permanent MAC: 00:50:56:af:a5:87 (VMware, Inc.)
New MAC: 00:00:28:a2:78:17 (PRODIGY SYSTEMS CORPORATION)
root@eh-kali-05:~# ip link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:00:28:a2:78:17 brd ff:ff:ff:ff:ff:ff
root@eh-kali-05:~# ping -c1 10.76.5.1
PING 10.76.5.1 (10.76.5.1) 56(84) bytes of data:
64 bytes from 10.76.5.1: icmp_seq=1 ttl=64 time=0.556 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.556/0.556/0.556/0.000 ms
root@eh-kali-05:~#

```

A white box on the right side of the terminal window contains the following commands:

```

macchanger -A eth0
ip link show dev eth0
ping -c1 10.76.5.1

```

*Kali pings pfSense with random spoofed MAC address*

## macchanger example 3

The image shows a network traffic capture window and a terminal window. The capture window displays an ICMP echo request and reply between 10.76.5.150 and 10.76.5.1. The terminal window shows the execution of the `macchanger` command to spoof the MAC address of the `eth0` interface to `10:1f:74:55:66:77`, followed by `ip link show dev eth0` and `ping -c1 10.76.5.1`. A white box highlights the terminal commands.

No.	Time	Source	Destination	Protocol	Length	Info
→	43 72.609303822	10.76.5.150	10.76.5.1	ICMP	98	Echo (ping) request id=0x...
←	44 72.609565907	10.76.5.1	10.76.5.150	ICMP	98	Echo (ping) reply id=0x...

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# macchanger -m 10:1f:74:55:66:77 eth0
Current MAC: 00:50:56:af:a5:87 (VMware, Inc.)
Permanent MAC: 00:50:56:af:a5:87 (VMware, Inc.)
New MAC: 10:1f:74:55:66:77 (Hewlett-Packard Company)
root@eh-kali-05:~# ip link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 10:1f:74:55:66:77 brd ff:ff:ff:ff:ff:ff
root@eh-kali-05:~# ping -c1 10.76.5.1
PING 10.76.5.1 (10.76.5.1) 56(84) bytes of data:
64 bytes from 10.76.5.1: icmp_seq=1 ttl=64 time=0.523 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0.523 ms
rtt min/avg/max/mdev = 0.523/0.523/0.523/0.000 ms
root@eh-kali-05:~#

```

**macchanger -m 10:1f:74:55:66:77 eth0**  
**ip link show dev eth0**  
**ping -c1 10.76.5.1**

*Kali pings pfSense pretending to be an HP PC*

## macchanger example 4

The screenshot shows two windows. The top window is Wireshark, displaying an ICMP Echo (ping) request and reply between 10.76.5.150 and 10.76.5.1. The MAC address 00:50:56:af:a5:87 is highlighted in red in the packet details. The bottom window is a terminal on a Kali Linux machine (root@eh-kali-05) showing the execution of the following commands:

```

root@eh-kali-05:~# macchanger -p eth0
Current MAC: 10:1f:74:55:66:77 (Hewlett-Packard Company)
Permanent MAC: 00:50:56:af:a5:87 (VMware, Inc.)
New MAC: 00:50:56:af:a5:87 (VMware, Inc.)
root@eh-kali-05:~# ip link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:af:a5:87 brd ff:ff:ff:ff:ff:ff
root@eh-kali-05:~# ping -c1 10.76.5.1
PING 10.76.5.1 (10.76.5.1) 56(84) bytes of data:
64 bytes from 10.76.5.1: icmp_seq=1 ttl=64 time=0.493 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.493/0.493/0.493/0.000 ms
root@eh-kali-05:~#
    
```

A white box on the right side of the terminal window contains the following commands:

```

macchanger -p eth0
ip link show dev eth0
ping -c1 10.76.5.1
    
```

*Kali pings pfSense with restored permanent MAC address*