



Admonition



Unauthorized hacking is a crime.

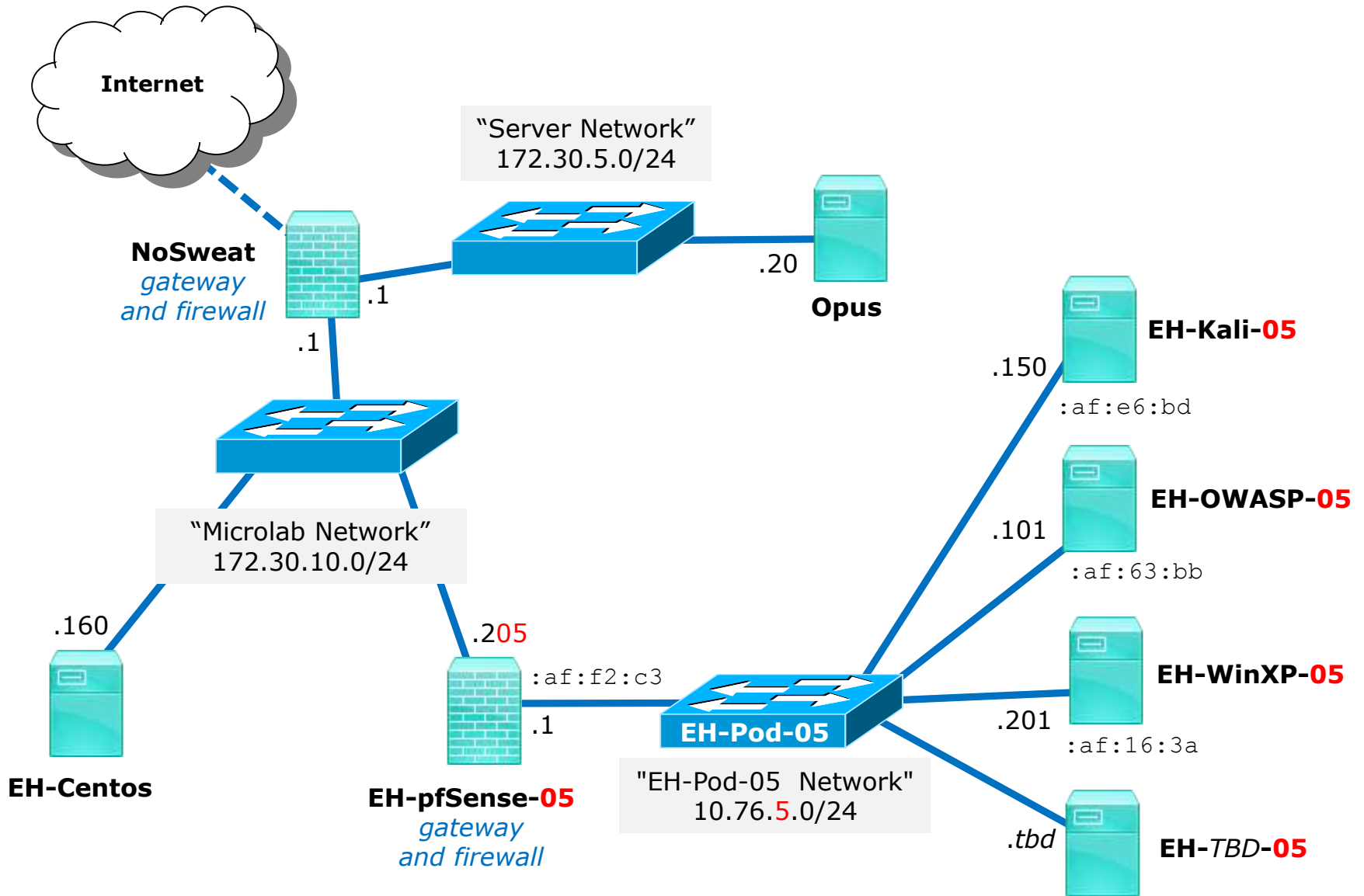
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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.



MAC Address Spoofing via macchanger

Last updated 9/4/2016



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

macchanger

```
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:~# █
```

```
ifconfig <interface> down
macchanger -A <interface>
OR macchanger -m xx:xx:xx:xx:xx:xx <interface>
ifconfig <interface> up
(use new MAC address)
ifconfig <interface> down
macchanger -p <interface>
ifconfig <interface> up
```

MAC Address Spoofing

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000000	10.76.5.150	10.76.5.1	ICMP	98	Echo (ping) request id=0x2481, seq=1/256...
← 2	0.000281338	10.76.5.1	10.76.5.150	ICMP	98	Echo (ping) reply id=0x2481, seq=1/256...


```

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Advanced_da:d1:d3 (58:1d:91:da:d1:d3), Dst: vmware_af:f2:c3 (00:50:56:af:f2:c3)
  ▶ Destination: vmware_af:f2:c3 (00:50:56:af:f2:c3)
  ▶ Source: Advanced_da:d1:d3 (58:1d:91:da:d1:d3)
    Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 10.76.5.150, Dst: 10.76.5.1
  ▶ Internet Control Message Protocol
  
```



```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# ifconfig eth0 down
root@eh-kali-05:~# macchanger -A eth0
Current MAC: 00:50:56:af:e6:bd (VMware, Inc.)
Permanent MAC: 00:50:56:af:e6:bd (VMware, Inc.)
New MAC: 58:1d:91:da:d1:d3 (Advanced Mobile Telecom co.,ltd.)
root@eh-kali-05:~# ifconfig eth0 up
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=0.302 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.302/0.302/0.302/0.000 ms
root@eh-kali-05:~#
  
```

The Kali VM now has a spoofed IP address

The -A option changes MAC to random address

MAC Address Spoofing

The image shows two windows. The top window is Wireshark, displaying a network capture. The bottom window is a terminal on a Kali VM, showing the execution of commands to spoof the MAC address.

Wireshark Capture:

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000000	10.76.5.150	10.76.5.1	ICMP	98	Echo (ping) request id=0x265a, seq=1/256...
← 2	0.000228599	10.76.5.1	10.76.5.150	ICMP	98	Echo (ping) reply id=0x265a, seq=1/256...

Terminal Output:

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# ifconfig eth0 down
root@eh-kali-05:~# macchanger -m 10:1F:74:55:66:77 eth0
Current MAC: 00:50:56:af:e6:bd (VMware, Inc.)
Permanent MAC: 00:50:56:af:e6:bd (VMware, Inc.)
New MAC: 10:1f:74:55:66:77 (Hewlett-Packard Company)
root@eh-kali-05:~# ifconfig eth0 up
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=0.256 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.256/0.256/0.256/0.000 ms
root@eh-kali-05:~#
  
```

Callout: The Kali VM now looks like an HP PC

The -m option is used to set a specific MAC address