Telnet Session Hijack

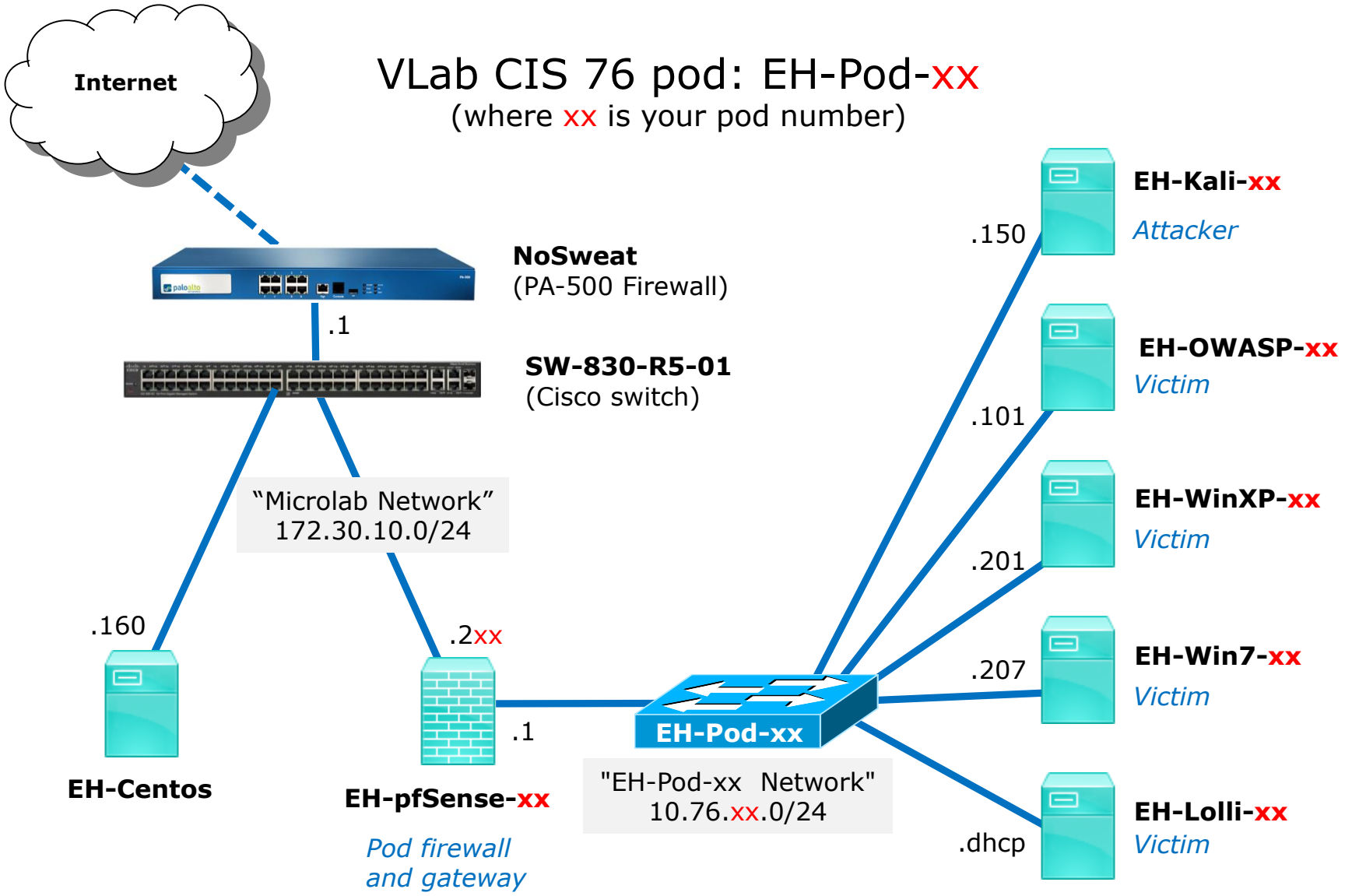
Last updated 9/13/2017

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.


Internet
VLab CIS 76 pod: EH-Pod-xx
(where xx is your pod number)
NoSweat
(PA-500 Firewall)
.1
SW-830-R5-01
(Cisco switch)
"Microlab Network"
172.30.10.0/24
.160
EH-Centos
.2xx
.1
EH-pfSense-xx
Pod firewall
and gateway
EH-Pod-xx
"EH-Pod-xx Network"
10.76.xx.0/24
.150
EH-Kali-xx
Attacker
.101
EH-OWASP-xx
Victim
.201
EH-WinXP-xx
Victim
.207
EH-Win7-xx
Victim
.dhcp
EH-Lolli-xx
Victim

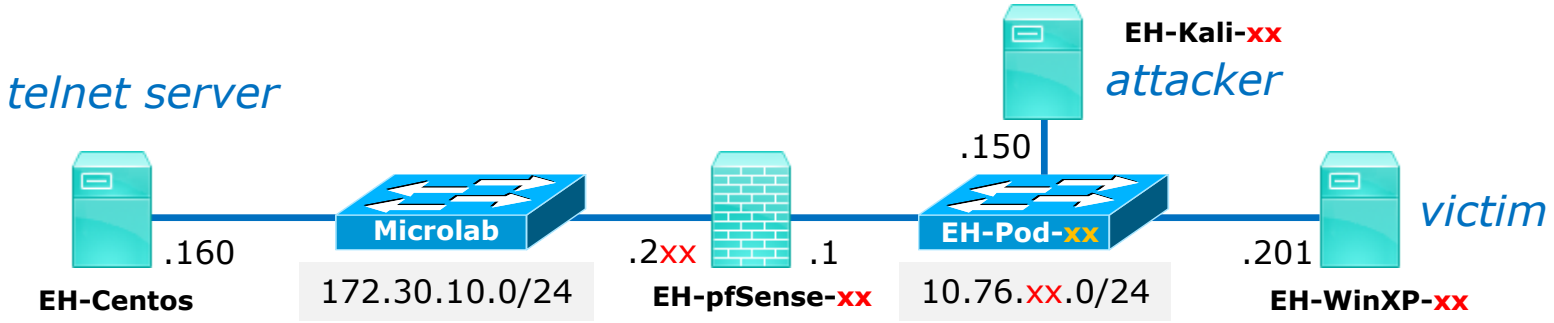
Initial Preparation

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

CIS 76 Telnet Session Hijack



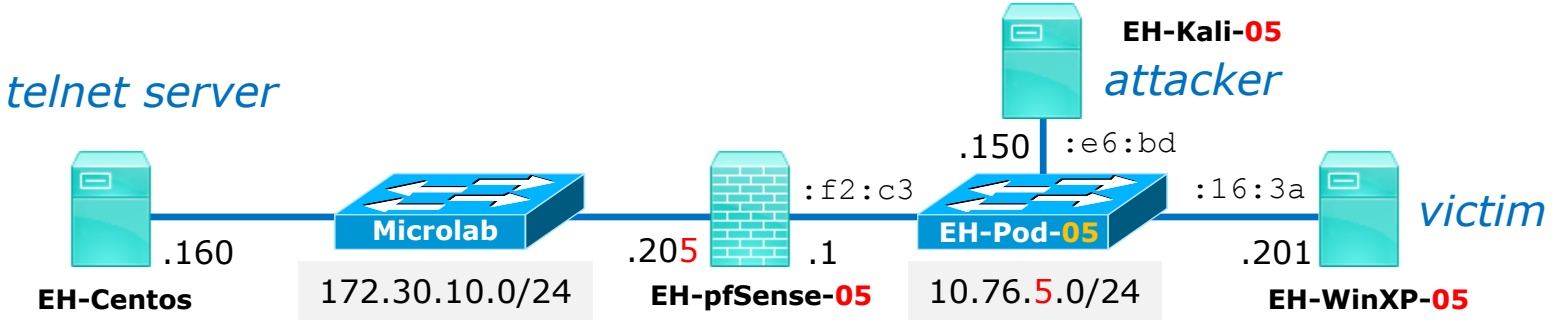
Scenario: The victim on EH-WinXP will be using telnet to log into the EH-Centos server.

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.

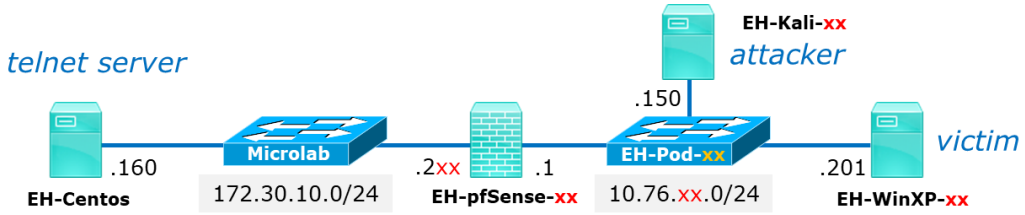
Optional Best Practice: Make a custom network map for yourself. Label each interface with the actual IP addresses. In addition, add the last portion of the MAC address to your pfSense, Kali and WinXP interfaces which will help illustrate the ARP poisoning.



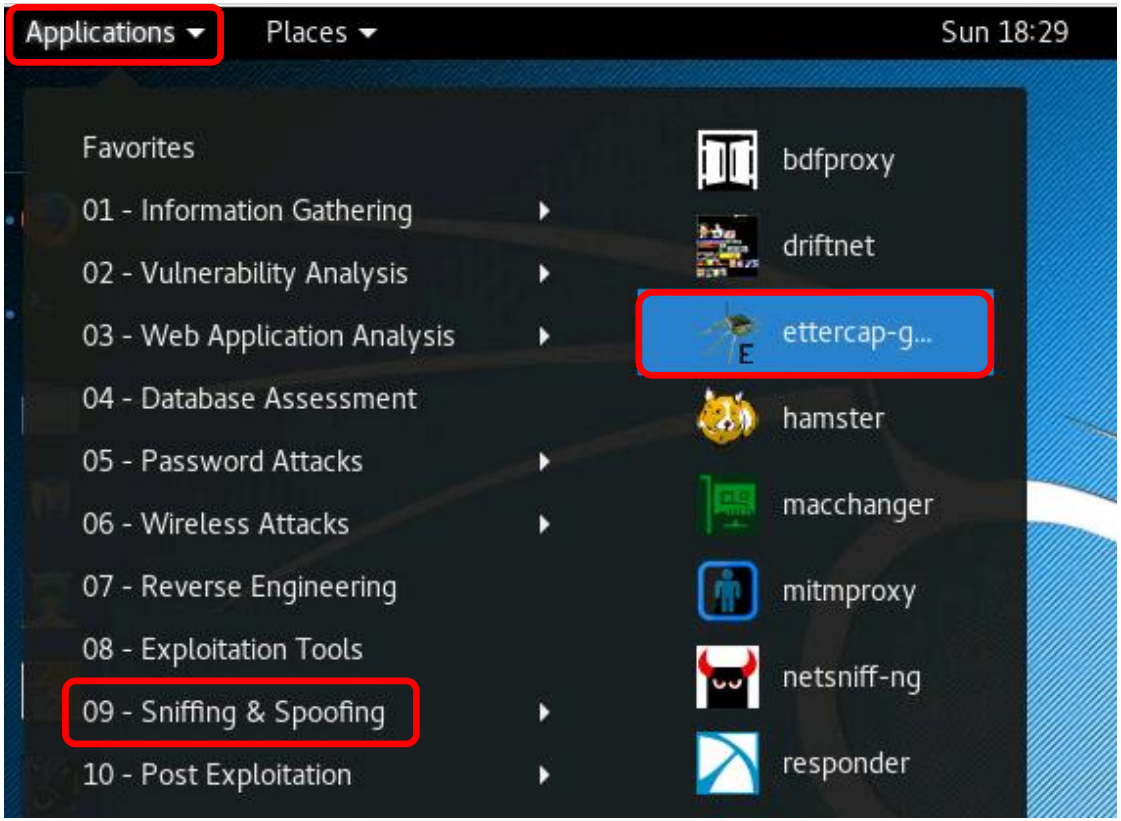
Pod 5 (Fa16)

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.

CIS 76 Telnet Session Hijack

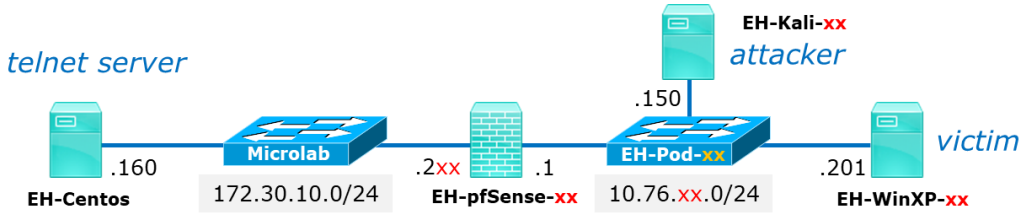


EH-Kali

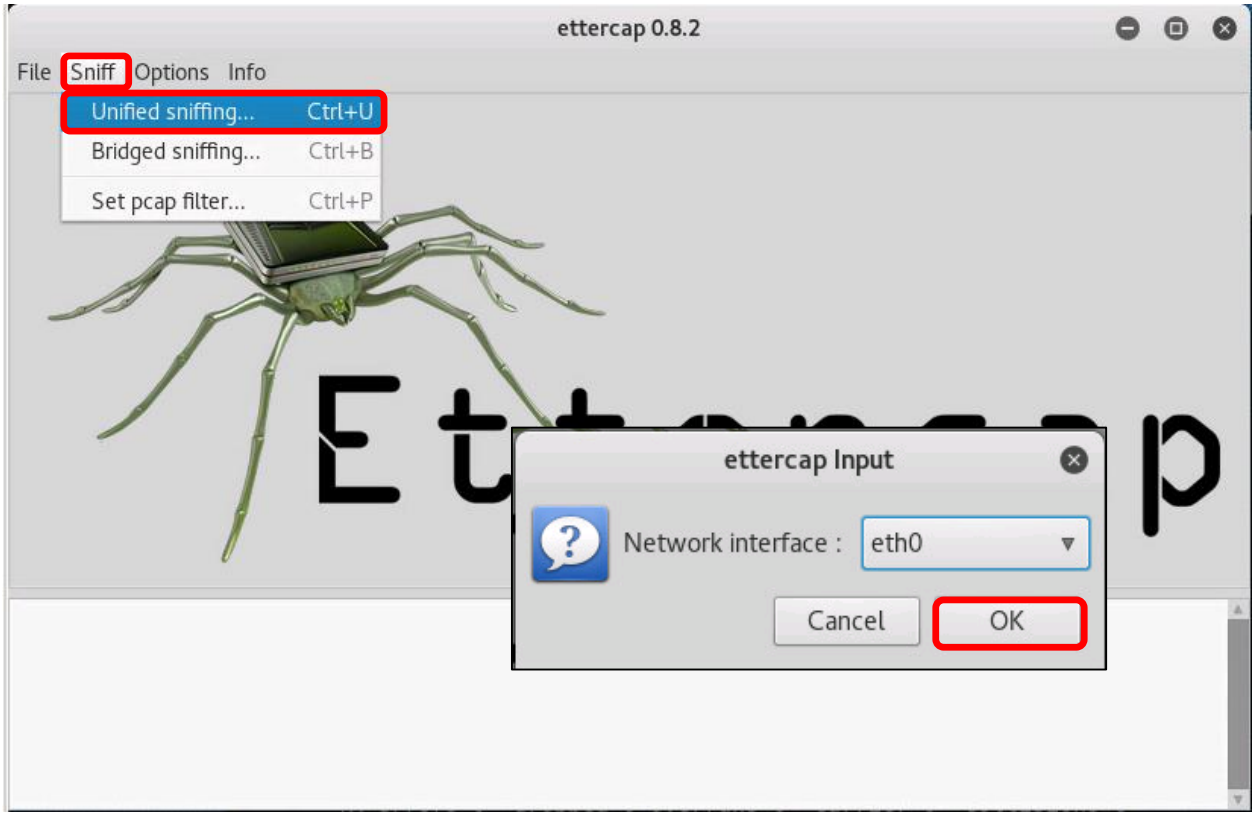


- Run Ettercap on EH-Kali

CIS 76 Telnet Session Hijack

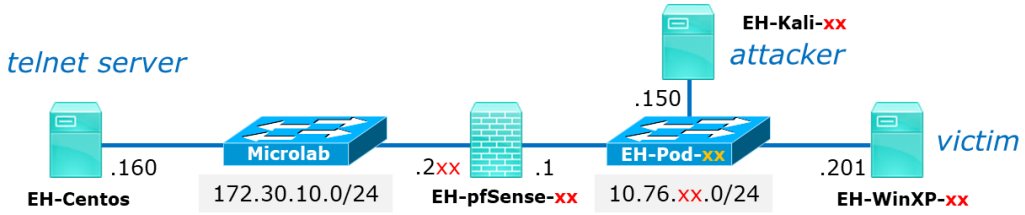


EH-Kali

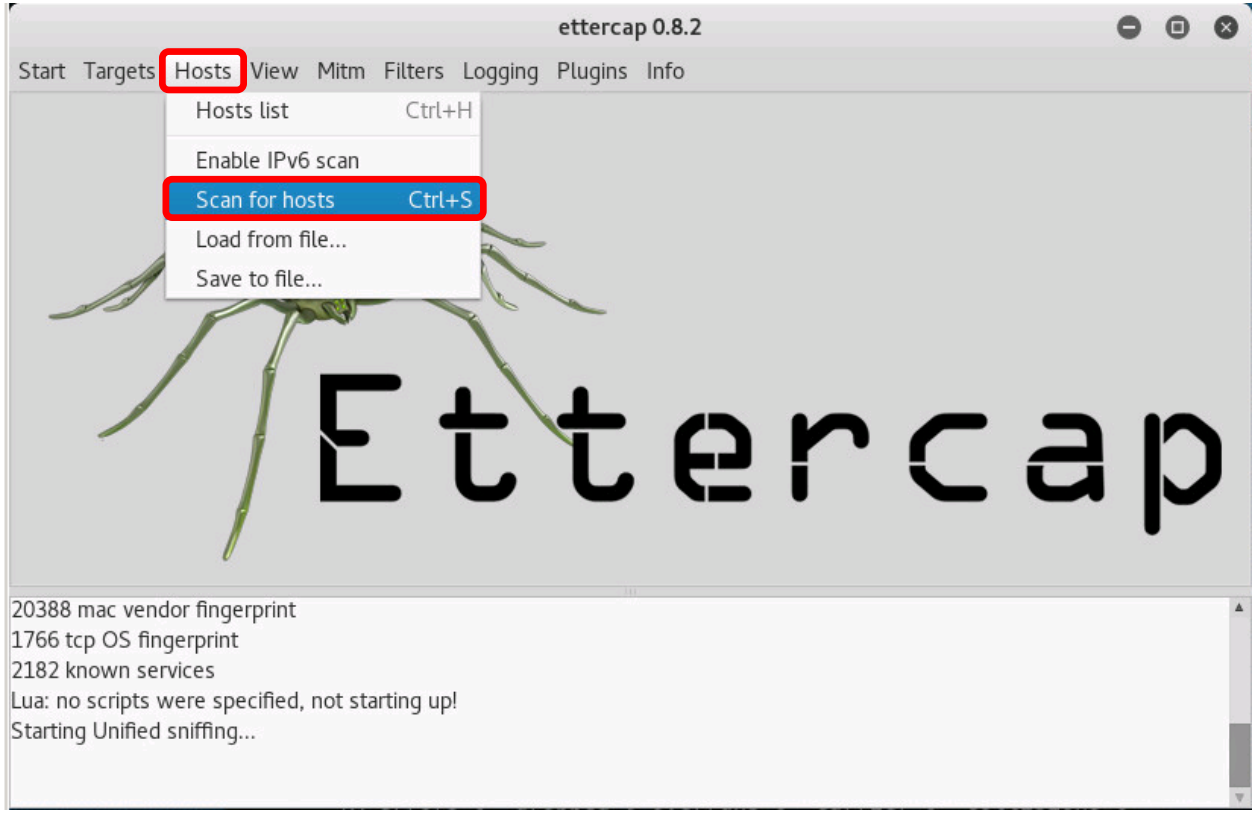


- Perform Unified sniffing on eth0

CIS 76 Telnet Session Hijack

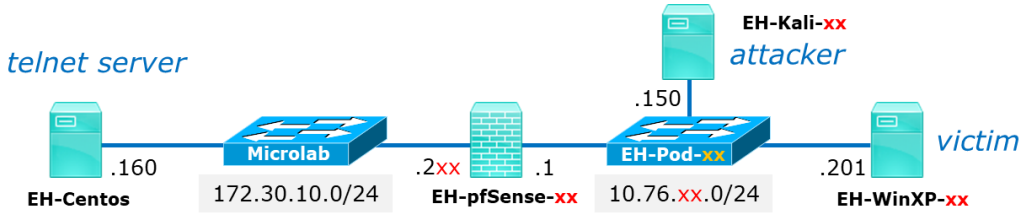


EH-Kali

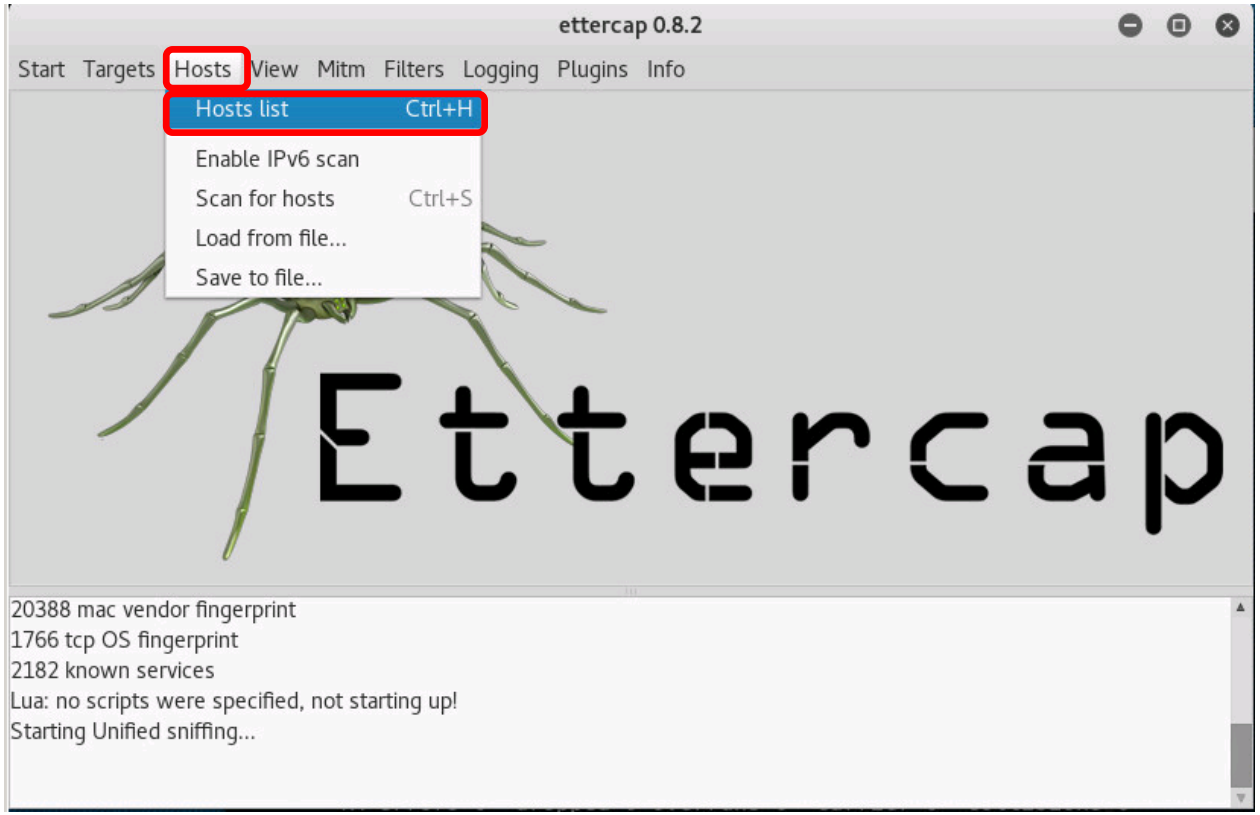


- Scan subnet to discover all online hosts

CIS 76 Telnet Session Hijack

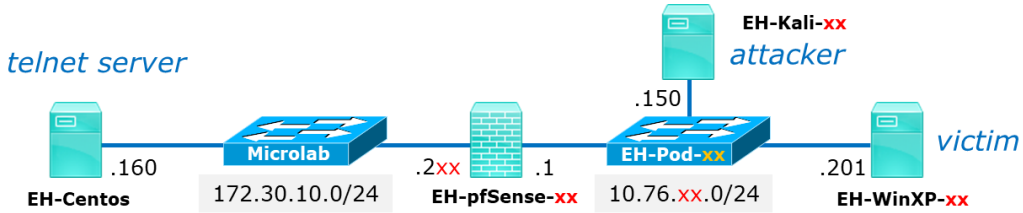


EH-Kali

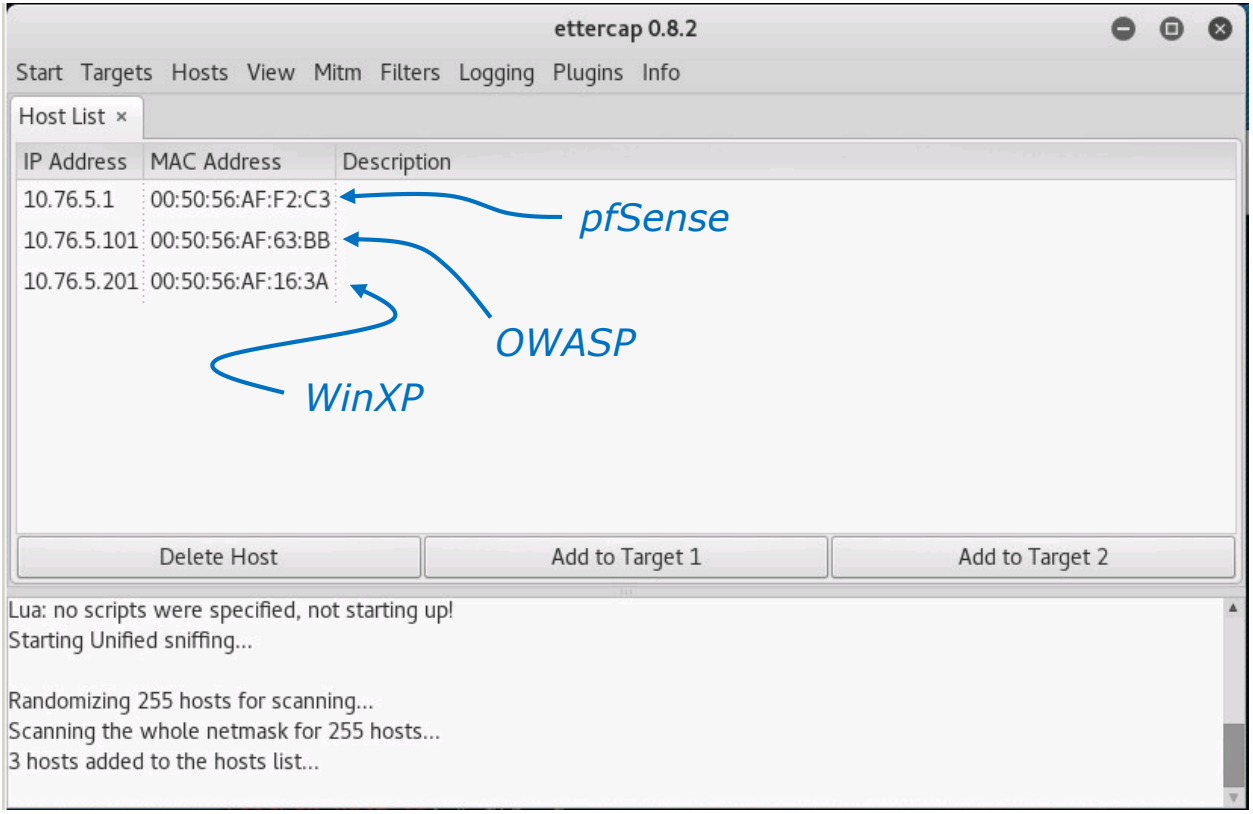


- Show the list of discovered hosts

CIS 76 Telnet Session Hijack

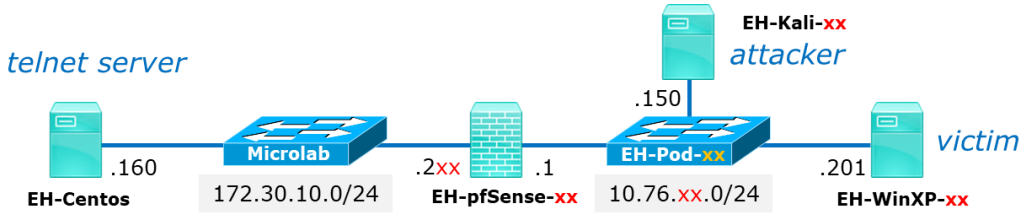


EH-Kali

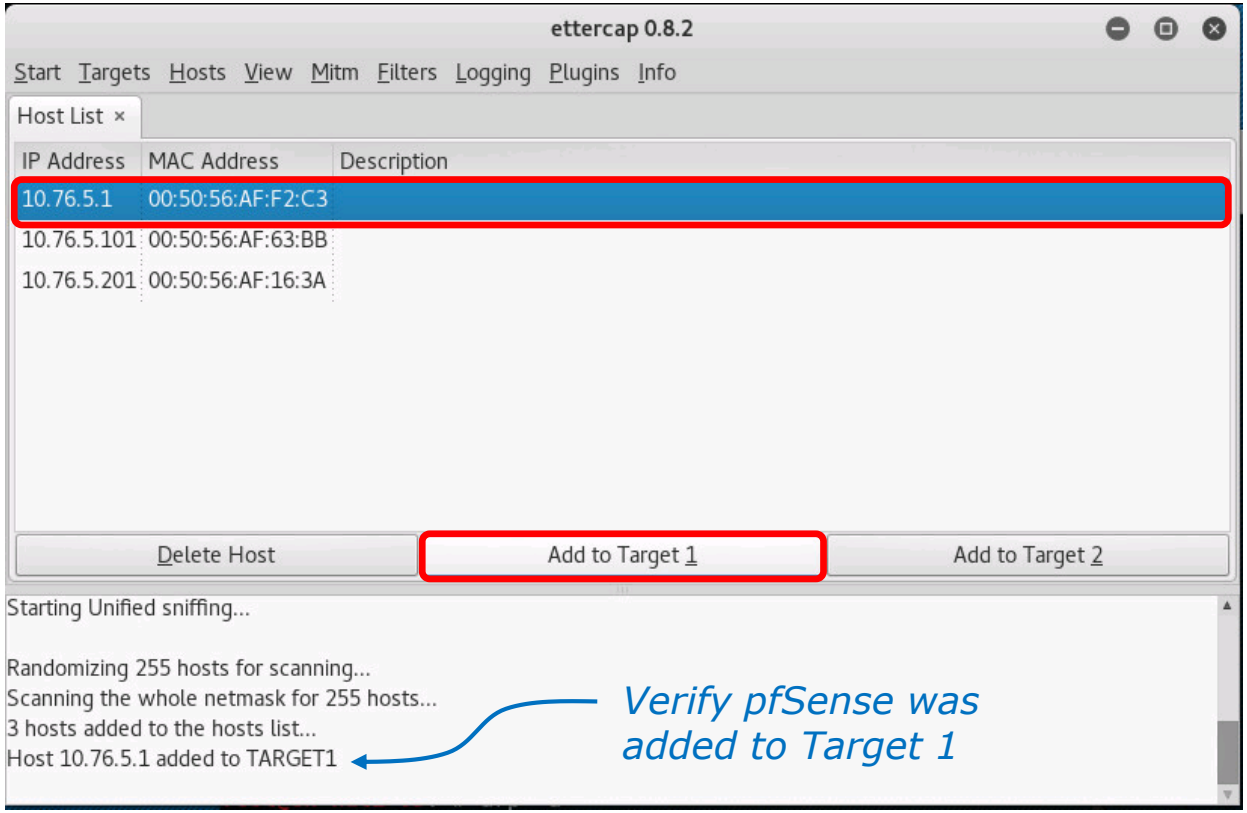


- Use the network map at the beginning of this document to identify the hosts discovered.

CIS 76 Telnet Session Hijack

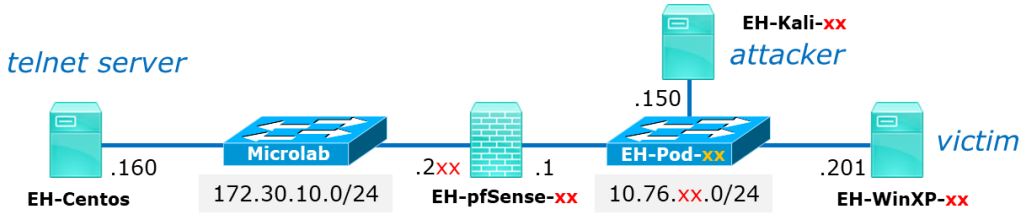


EH-Kali

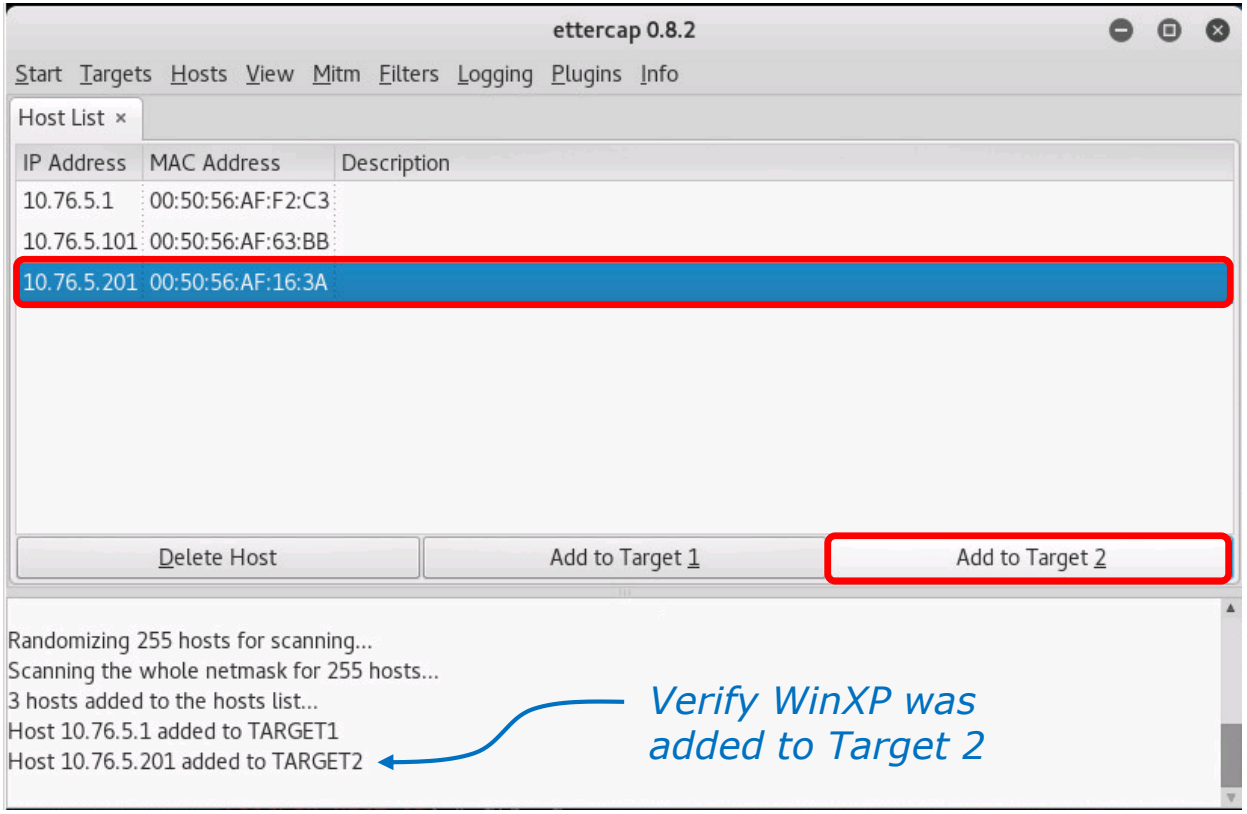


- Select your pfSense firewall (10.76.xx.1) and click the "Add it to Target 1" button.
- Verify it was successfully added.

CIS 76 Telnet Session Hijack

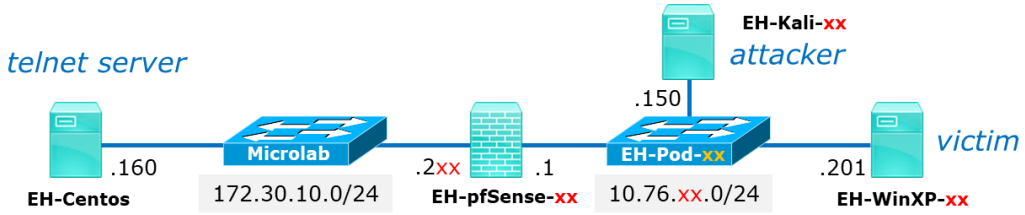


EH-Kali

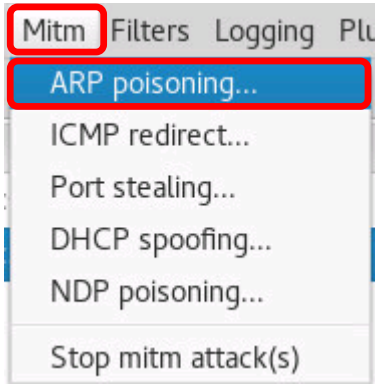


- Select your WinXP VM (10.76.xx.201) and click the "Add it to Target 2" button.
- Verify it was successfully added.

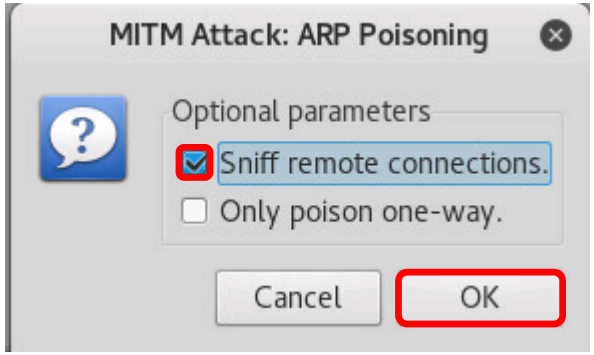
CIS 76 Telnet Session Hijack



EH-Kali

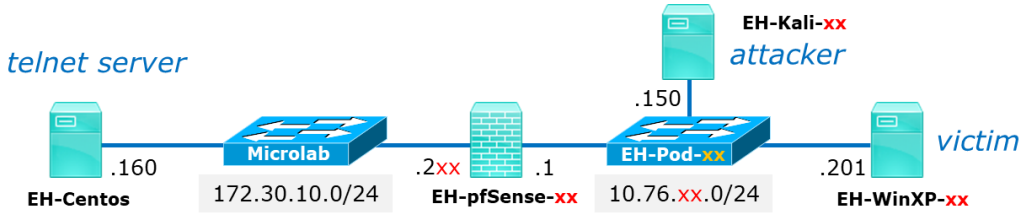


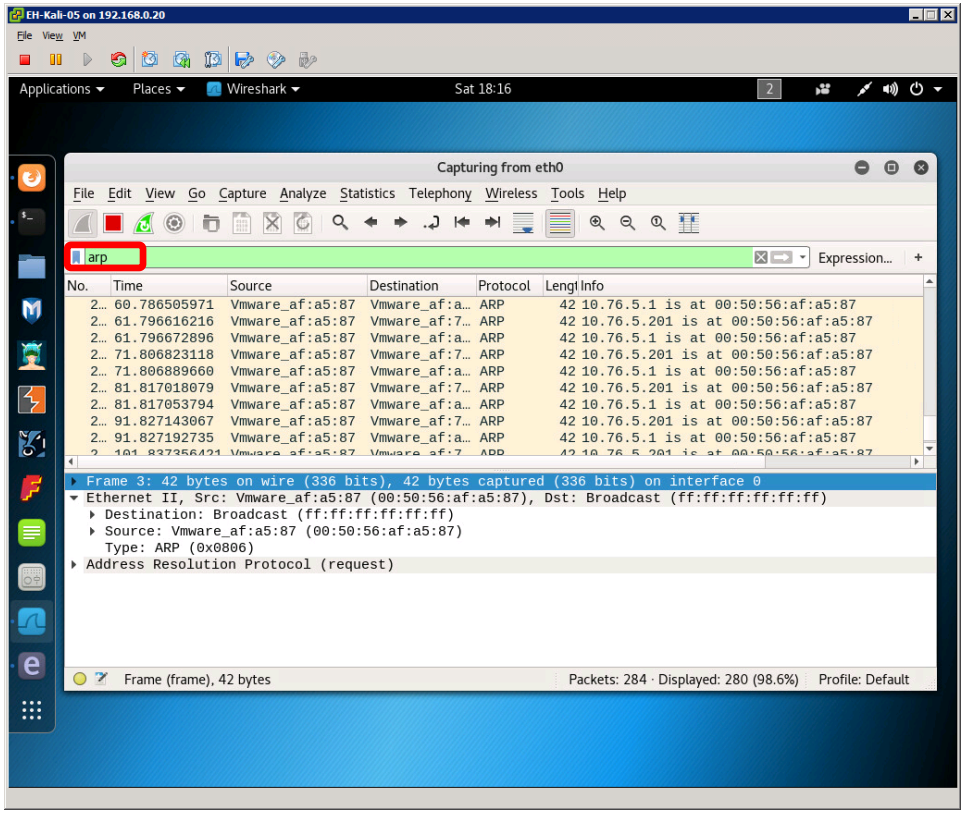
- Under the Mitm menu select ARP poisoning...



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

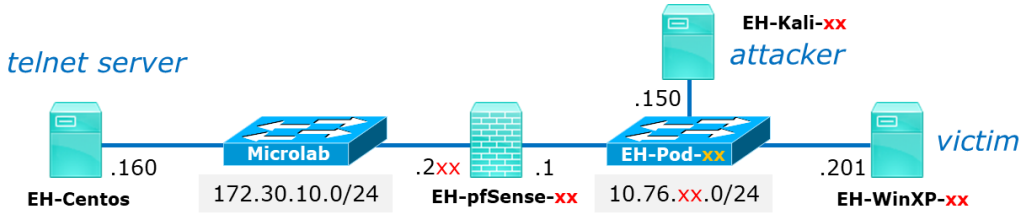
CIS 76 Telnet Session Hijack





- 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!

CIS 76 Telnet Session Hijack



EH-WinXP

Alternative binary files

The installer packages above will provide all of these (except PuTTYtel), but you ca

(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 FTP

32-bit:	psftp.exe	(or by FTP)
64-bit:	psftp.exe	(or by FTP)

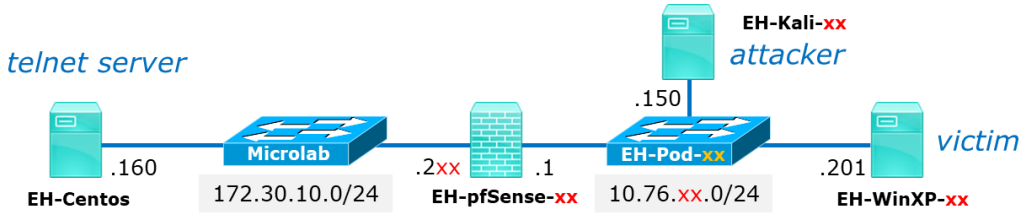
On Win XP log in as cis76 user and install Putty:

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

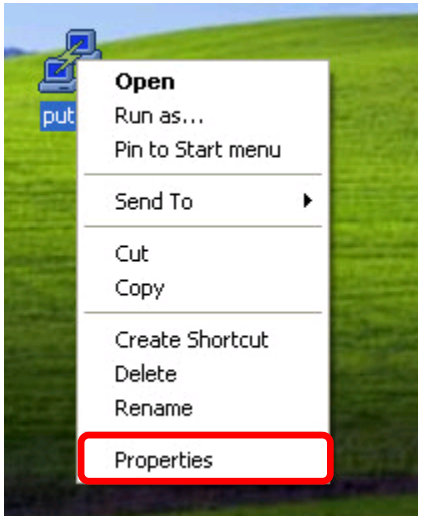
  https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

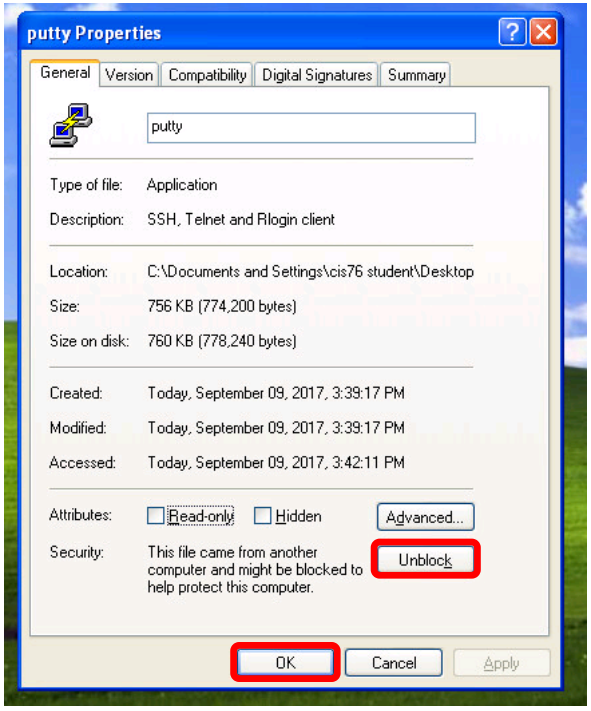
- Download the 32-bit alternative putty.exe binary to the desktop.

CIS 76 Telnet Session Hijack



EH-WinXP

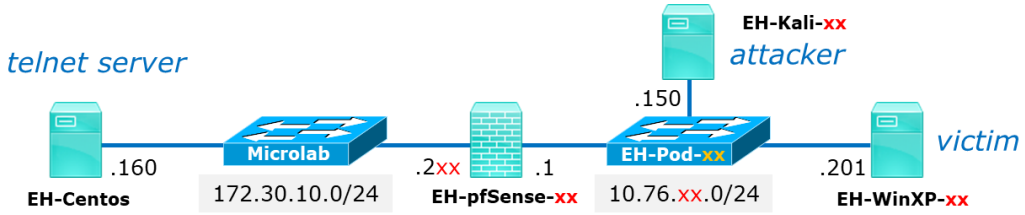




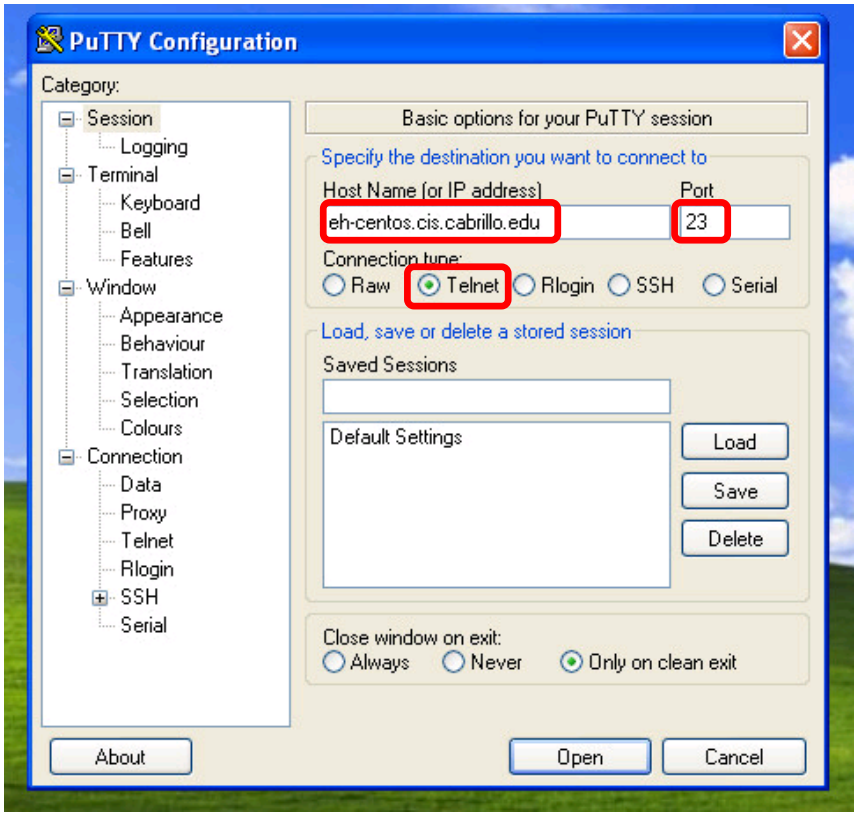
Unblock Putty so you can run it:

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

CIS 76 Telnet Session Hijack

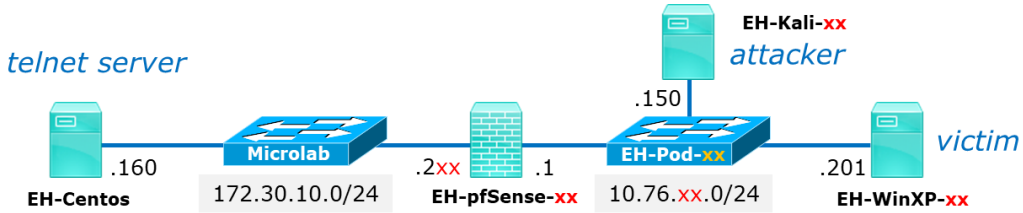


EH-WinXP

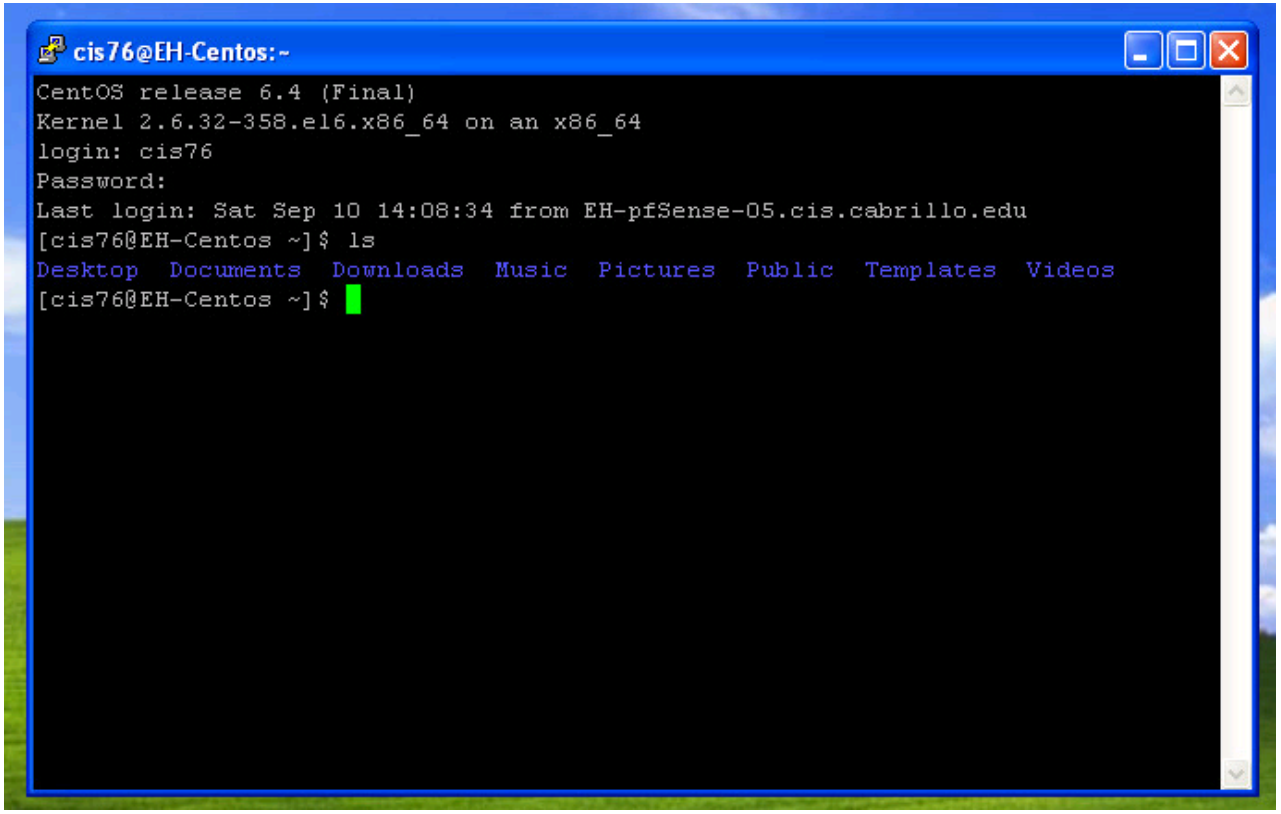


- Run Putty
- Telnet to eh-centos.cis.cabrillo.edu (port 23)

CIS 76 Telnet Session Hijack

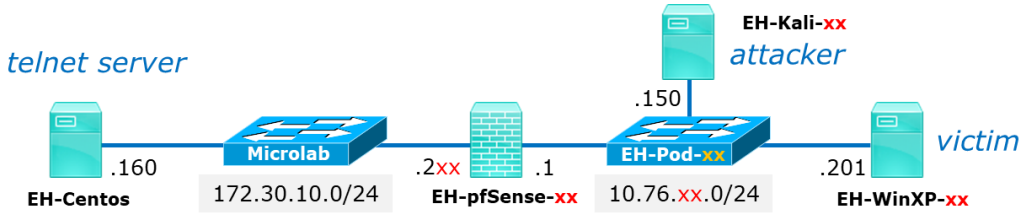


EH-WinXP

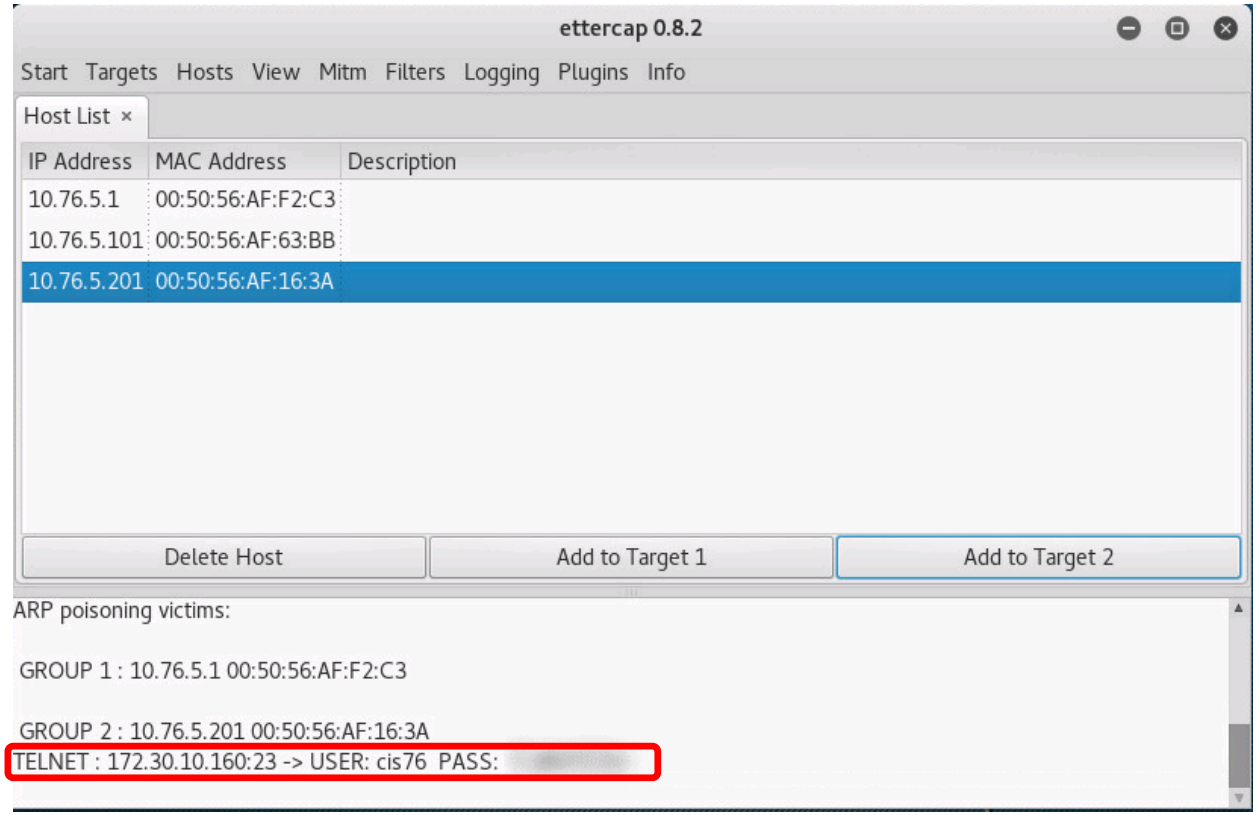


- Log into EH-Centos as the cis76 user.

CIS 76 Telnet Session Hijack

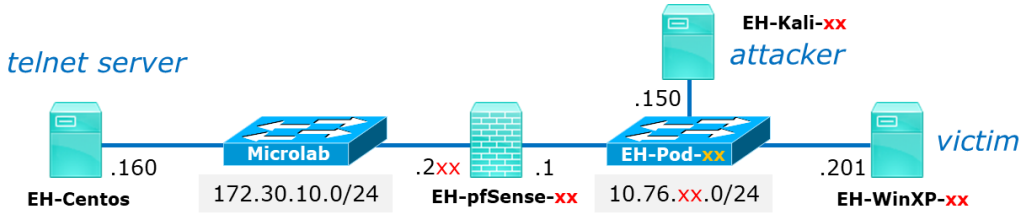


EH-Kali

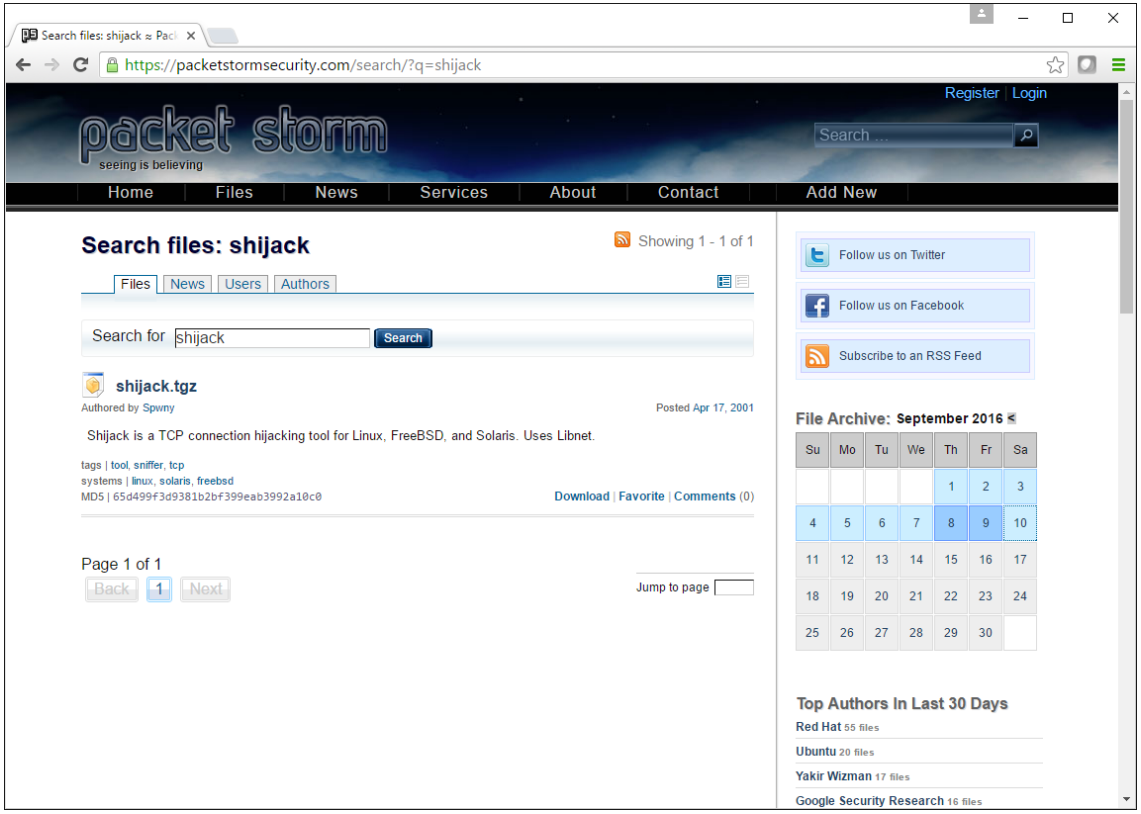


- Back on the Kali VM notice the attacker can see your username and password (blurred here)

CIS 76 Telnet Session Hijack



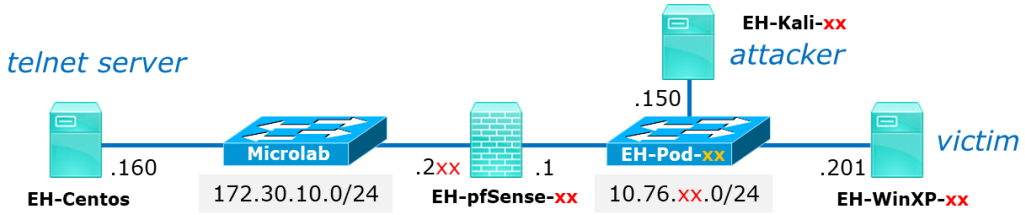
EH-Kali



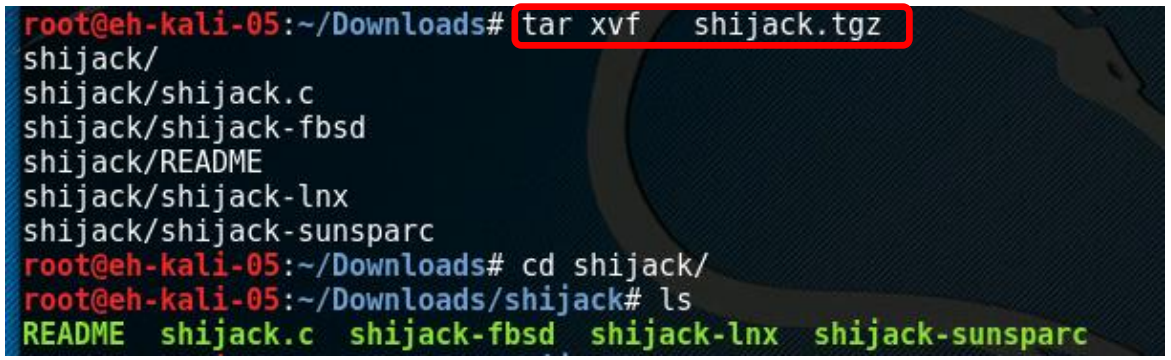
- On Kali, browse to: https://packetstormsecurity.com/
- Search for: shijack

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

CIS 76 Telnet Session Hijack



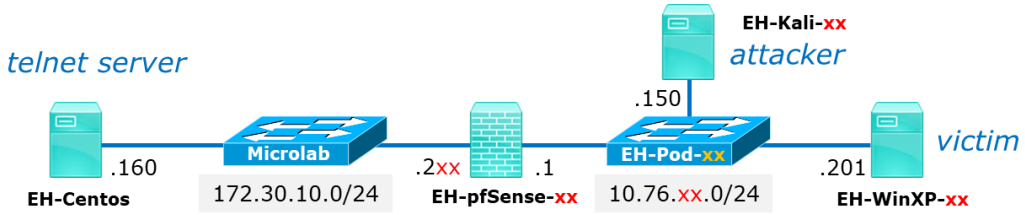
EH-Kali



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

  cd shijack
  ls

CIS 76 Telnet Session Hijack



EH-Kali

Optionally you can set a telnet display filter here

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

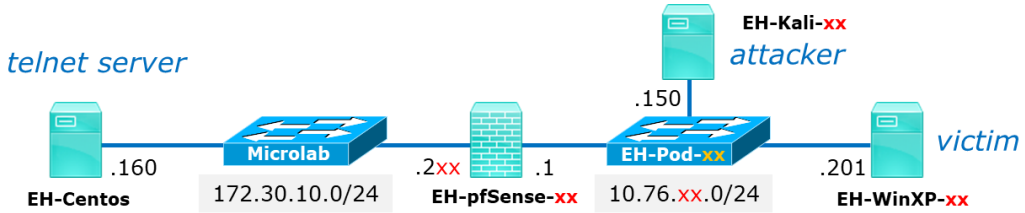
No.	Time	Source	Destination	Protocol	Length	Info
13	1.708588654	198.84.60.198	10.76.5.150	TCP	66	[TCP ACKed unseen segment] 443 ...
14	1.754981713	10.76.5.150	198.84.60.198	TCP	66	55962 → 443 [ACK] Seq=1 Ack=1 W...
15	1.772147909	198.84.60.198	10.76.5.150	TCP	66	[TCP ACKed unseen segment] 443 ...
16	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)
```

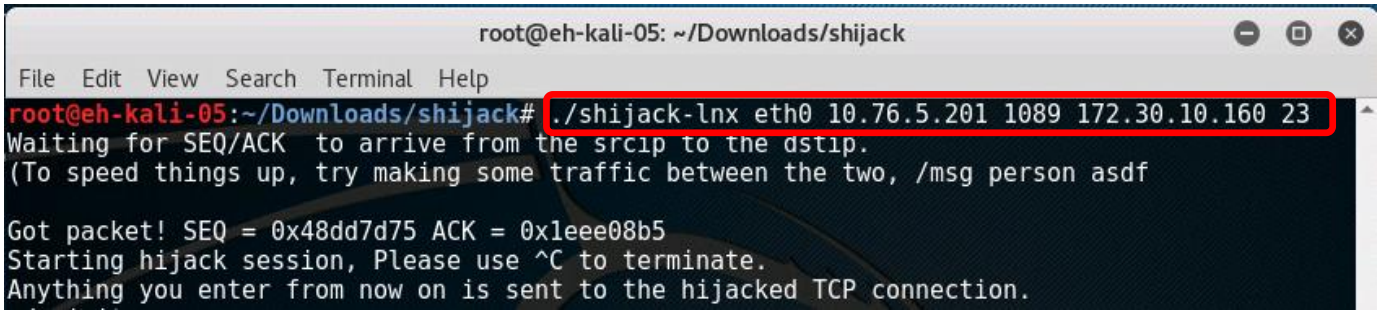
```
0000  00 50 56 af e6 bd 00 50  56 af 16 3a 08 00 45 00   .PV....P V..:..E.
0010  00 29 54 2f 40 00 80 06  df cc 0a 4c 05 c9 ac 1e   .)T/@... ...L....
0020  0a a0 04 41 00 17 48 dd  7d 5a 1e ee 08 60 50 18   ...A..H. }Z...`P.
0030  f9 e2 91 37 00 00 6c 00  00 00 00 00               ...7..l. ....
```

- 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).

CIS 76 Telnet Session Hijack

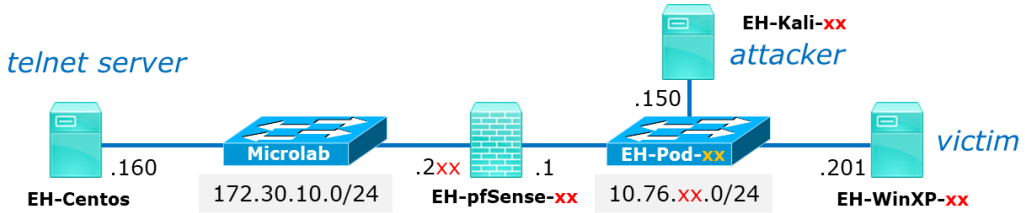


EH-Kali

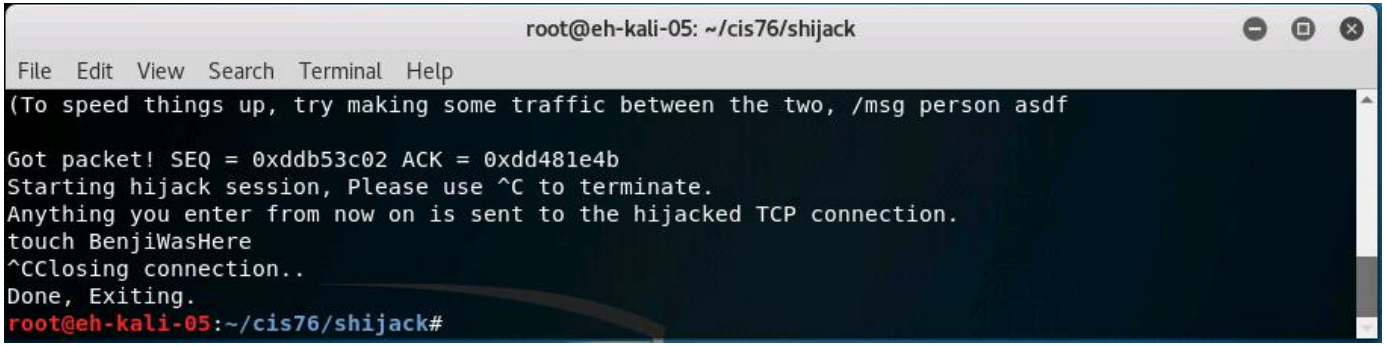


- If necessary, change into the directory with your extracted shijack files.
- Run this command:
  `./shijack-lnx eth0 10.76.`xx**`.201`** nnnn **`172.30.10.160 23`**
  where xx is your pod number and nnnn is the port your WinXP VM is using that you observed in Wireshark.
- Back on WinXP you can hit the Enter key once or twice to speed up the hijack.
- **Proceed QUICKLY to the next slide!**

CIS 76 Telnet Session Hijack

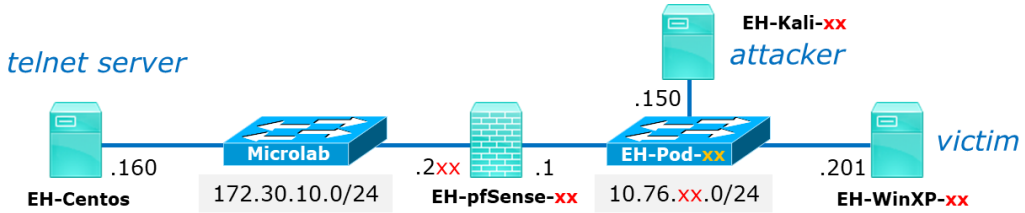


EH-Kali



- 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.

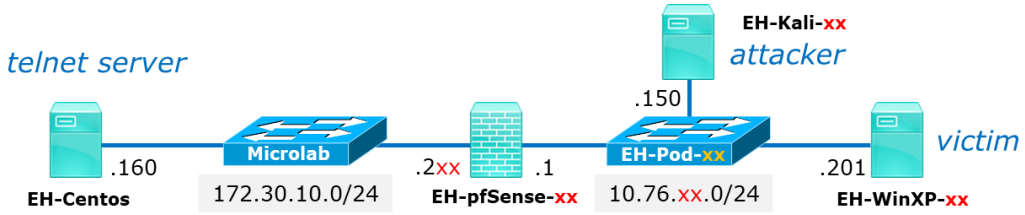
CIS 76 Telnet Session Hijack



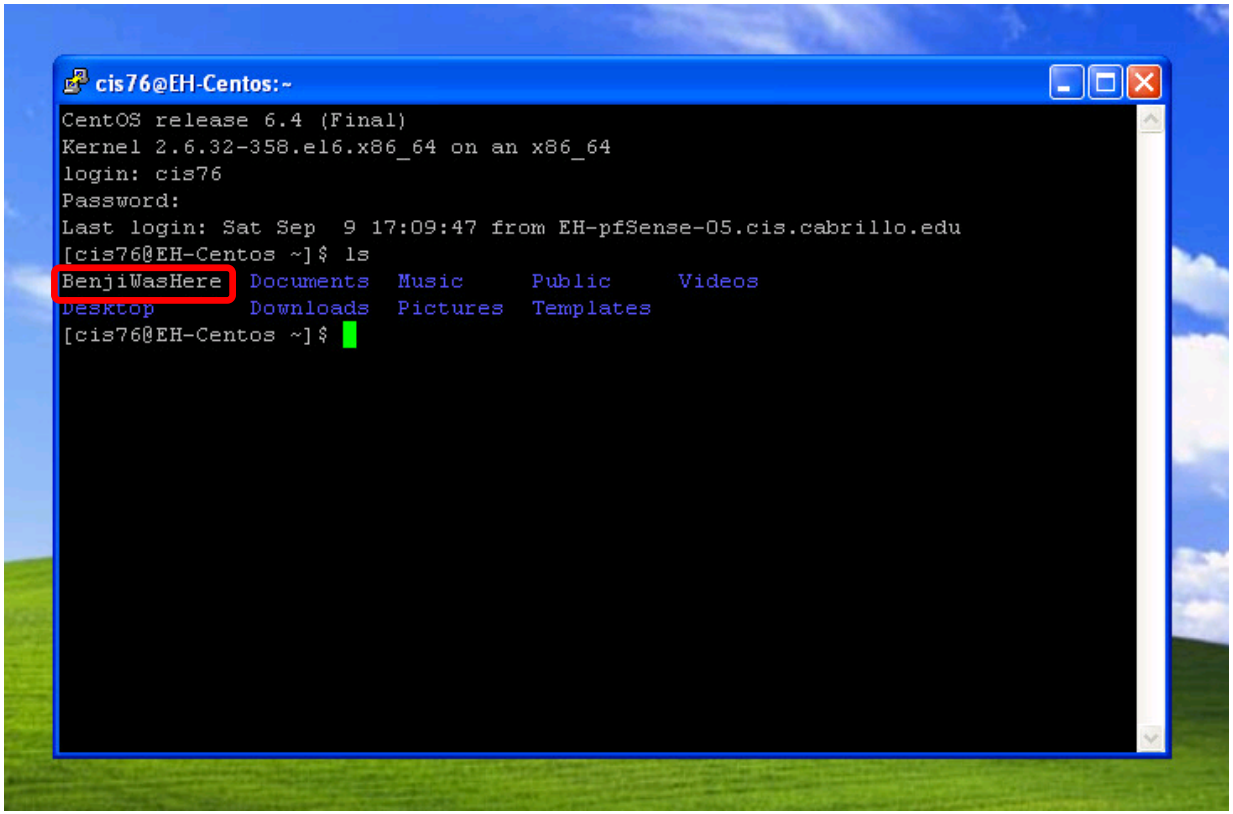
EH-WinXP

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

CIS 76 Telnet Session Hijack



EH-WinXP



- Log back in to EH-Centos from WinXP using Putty and Telnet.
- Notice the hijacker left a file!

*If you didn't type the **touch xxxWasHere** command fast enough no file will be created. You need to repeat the attack with a new telnet session.*

Credits

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