Admonition

Unauthorized hacking is a crime.

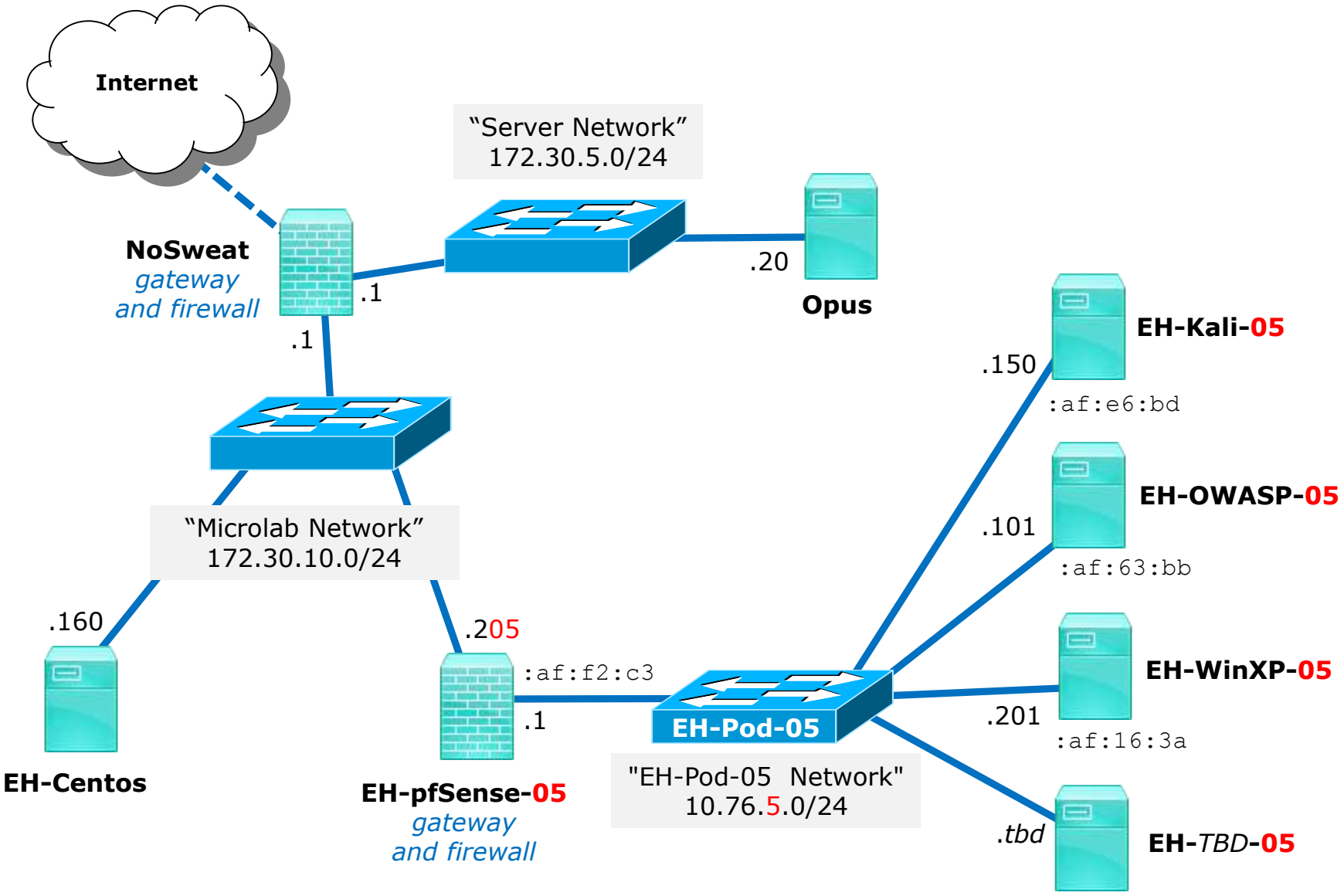
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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.

MITM ARP Poison Attack

DRAFT
Last updated 9/6/2016

CIS 76 MITM via ARP Poisoning



Requirements

1. EH-Centos VM running with vsftp installed on Microlab network.
2. OWASP VM at Baseline snapshot.
3. WinXP at Baseline snapshot.
4. pfSense VM at Baseline snapshot.
5. Cain and Abel software for WinXP VM
6. Older release of Wireshark for WinXP VM.

Tools

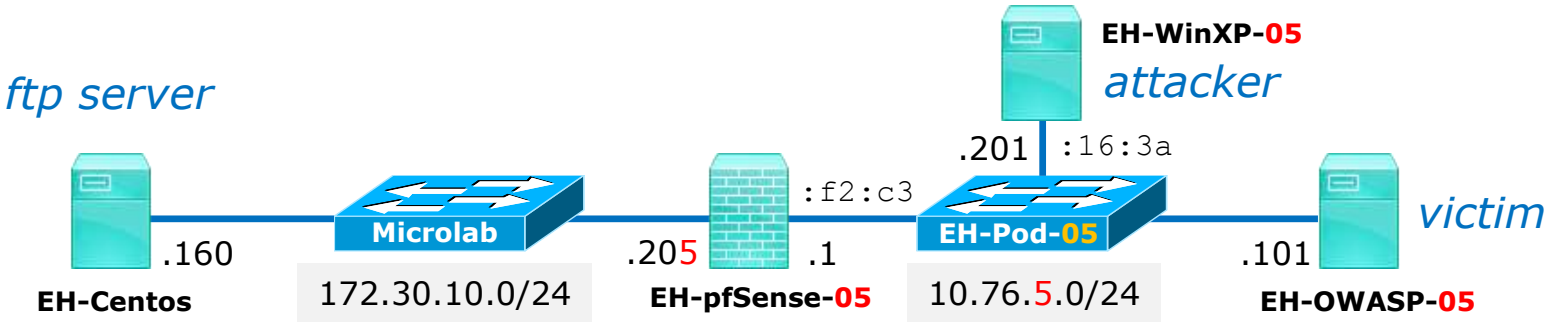
Cain and Abel site

http://www.oxid.it/index.html

Wireshark site

https://www.wireshark.org/download.html

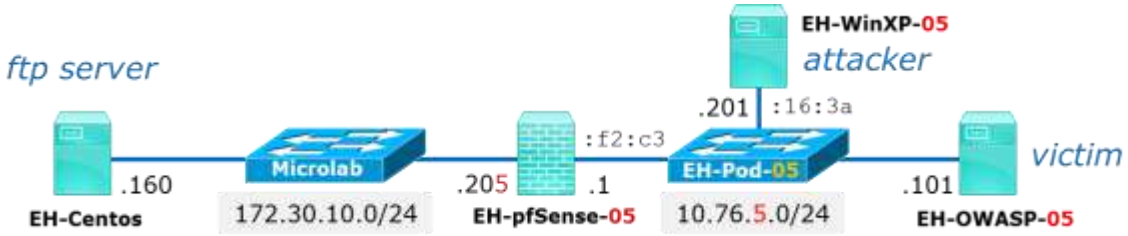
Man in the Middle Attack via ARP poisoning



In this scenario the WinXP victim will use Cain to poison the ARP caches on the pfSense firewall and the OWASP VM. The WinXP VM will intercept and sniff traffic between the OWASP and Centos VM.

Wireshark will be loaded on the WinXP VM to see how the ARP poisoning is accomplished.

CIS 76 MITM via ARP Poisoning



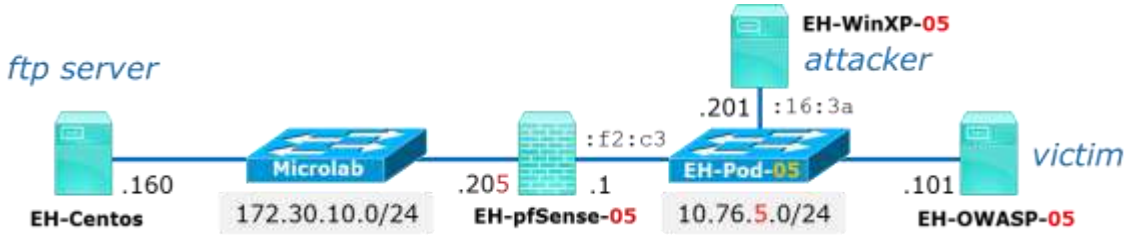
OWASP VM

```
root@owaspbwa:~# ping -c1 172.30.10.160
PING 172.30.10.160 (172.30.10.160) 56(84) bytes of data.
64 bytes from 172.30.10.160: icmp_seq=1 ttl=63 time=2.24 ms

--- 172.30.10.160 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.246/2.246/2.246/0.000 ms
root@owaspbwa:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.76.5.1                ether   00:50:56:af:f2:c3   C                     eth0
root@owaspbwa:~# _
```

Ping EH-Centos from your OWASP VM to test connectivity.

Check the arp cache to show the MAC address of your router.

CIS 76 MITM via ARP Poisoning



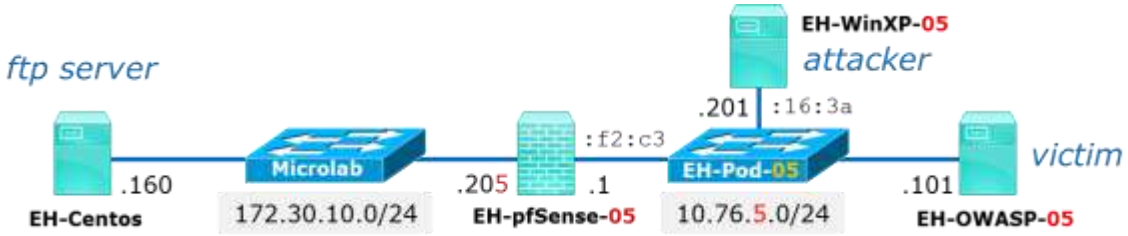
OWASP VM

```
root@owaspbwa:~# ftp 172.30.10.160
Connected to 172.30.10.160.
220 Welcome to CIS 76 FTP service.
Name (172.30.10.160:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls
227 Entering Passive Mode (172,30,10,160,82,12).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Sep 05 01:01 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (172,30,10,160,221,147).
150 Here comes the directory listing.
-rw-r--r--    1 0        0             205 Sep 05 01:01 admonition
226 Directory send OK.
ftp> _
```

ftp to EH-Centos and login as anonymous with any password.

Change to passive mode, descend and list the contents of the pub directory.

CIS 76 MITM via ARP Poisoning

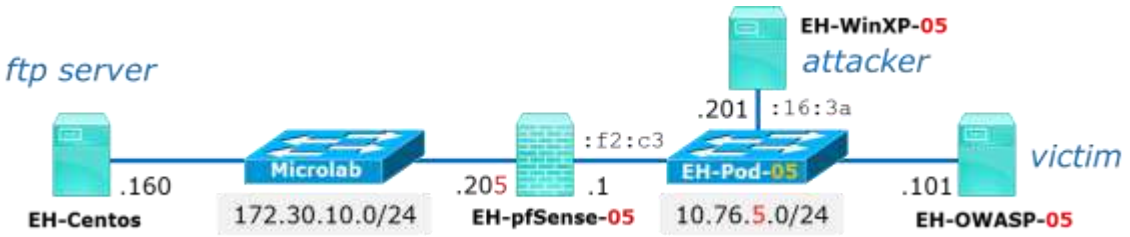


OWASP VM

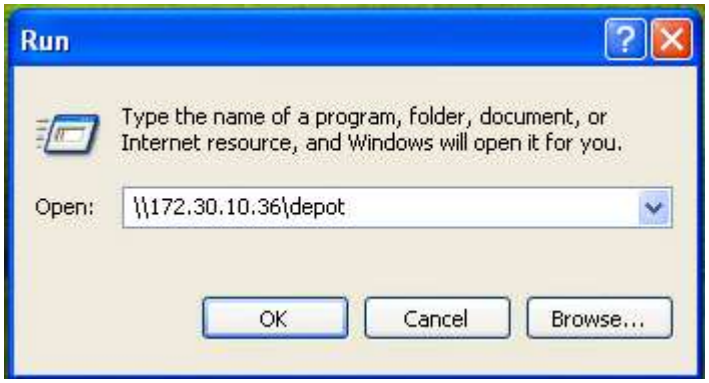
```
ftp> get admonition
local: admonition remote: admonition
227 Entering Passive Mode (172,30,10,160,37,183).
150 Opening BINARY mode data connection for admonition (205 bytes).
226 Transfer complete.
205 bytes received in 0.00 secs (1551.9 kB/s)
ftp> exit
221 Goodbye.
root@owaspbwa:~# cat admonition
Remember ...

Unauthorized hacking is a crime!

An ethical hacker will only perform penetration testing with
the explicit end-to-end authorization from the owners of the
networks and systems being tested.
root@owaspbwa:~#
```

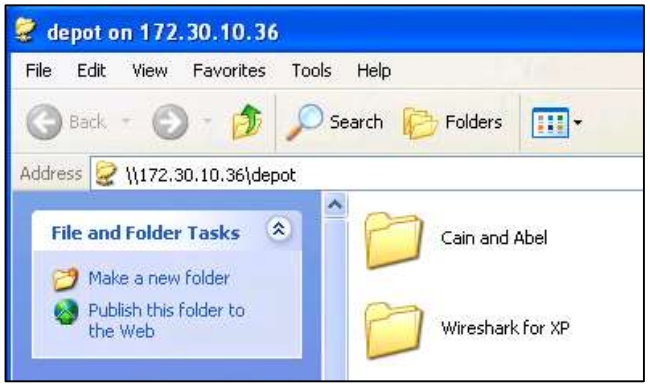
Confirm you can download the admonition file.

CIS 76 MITM via ARP Poisoning



WinXP VM

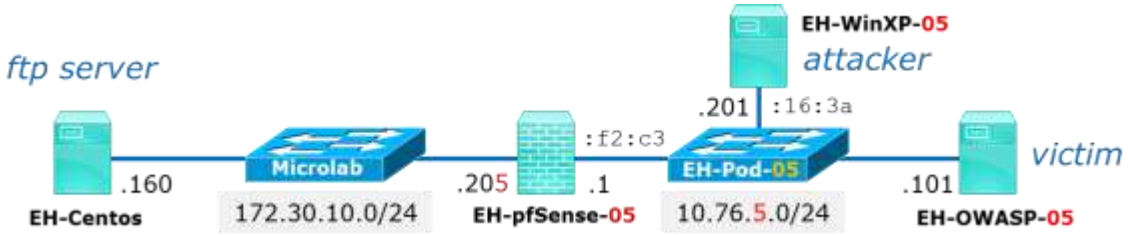




1) From your WinXP VM connect to the file share named depot on 172.30.10.36.

2) Open the "Cain and Abel" and "Wireshark for XP" folders and drag their contents to your desktop. desktop

CIS 76 MITM via ARP Poisoning

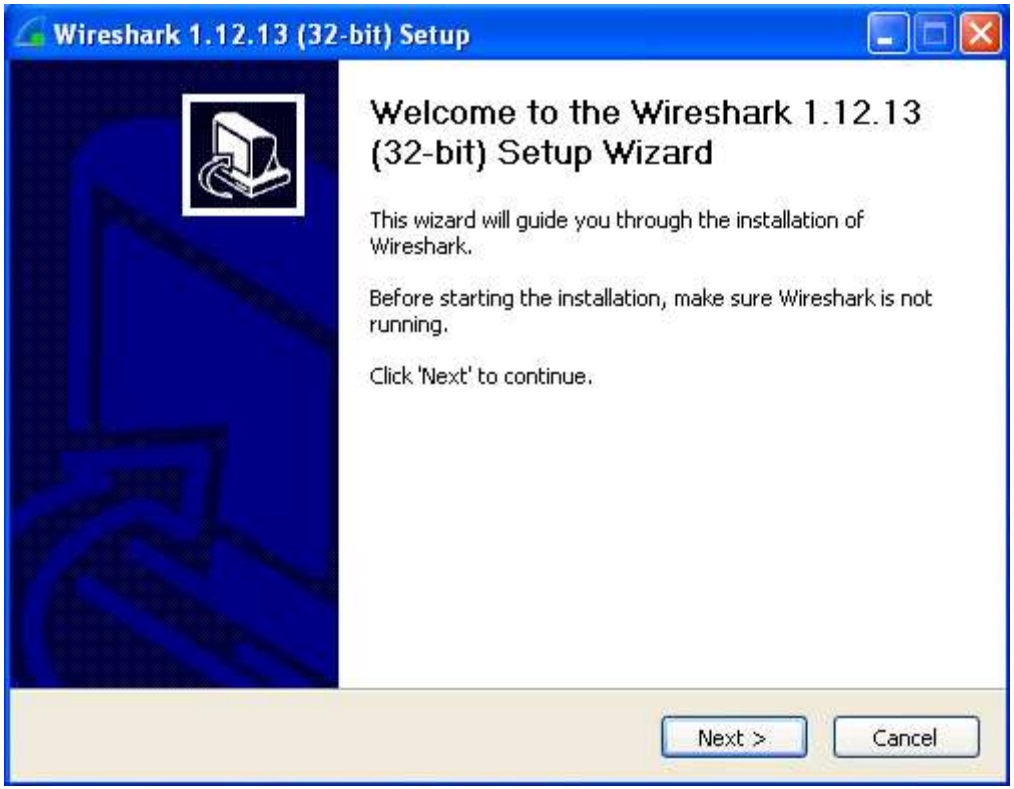


WinXP VM

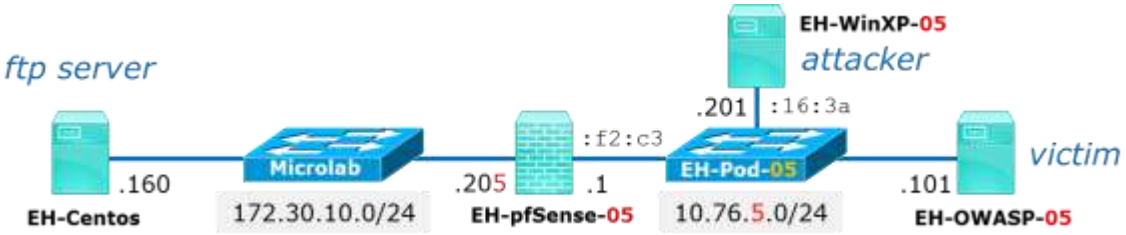
Open the Wireshark-win32-1.12.13 file on your desktop and install Wireshark.

You can ignore the XP warning.

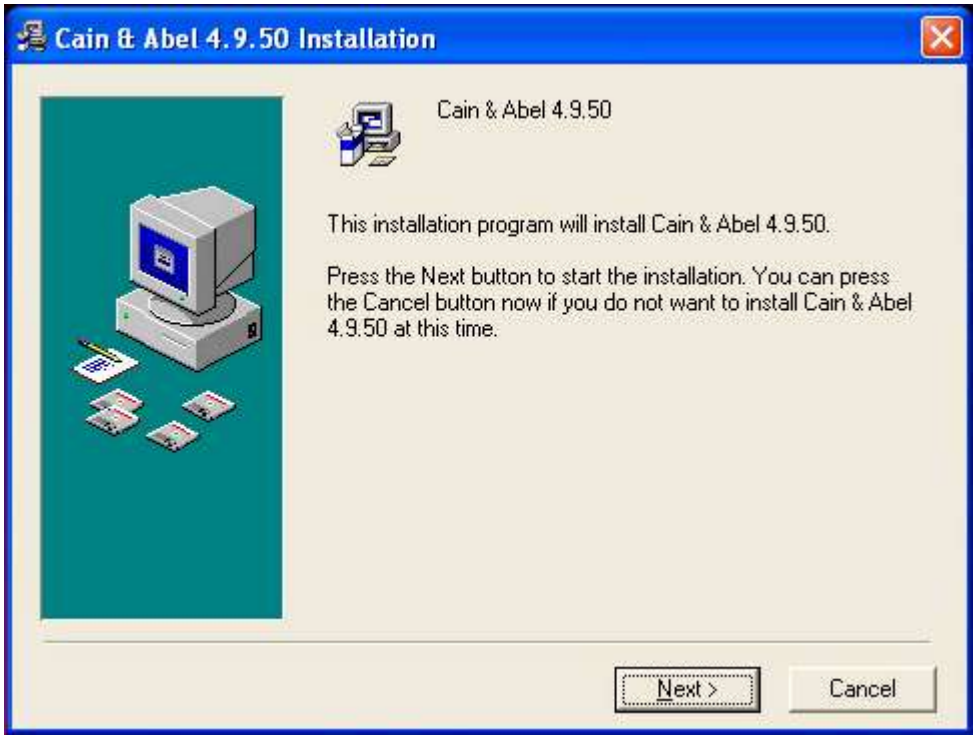
Take the setup defaults.



CIS 76 MITM via ARP Poisoning



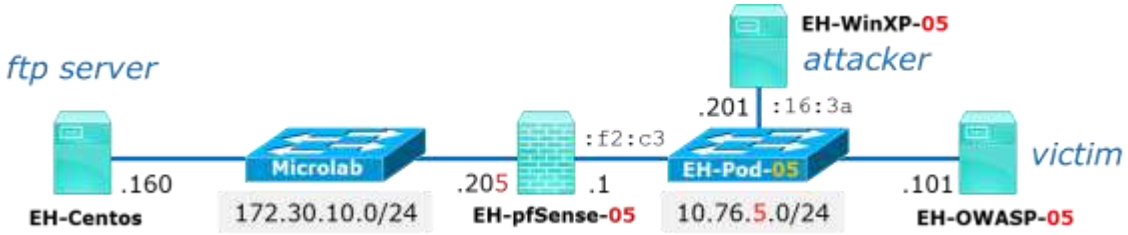
WinXP VM



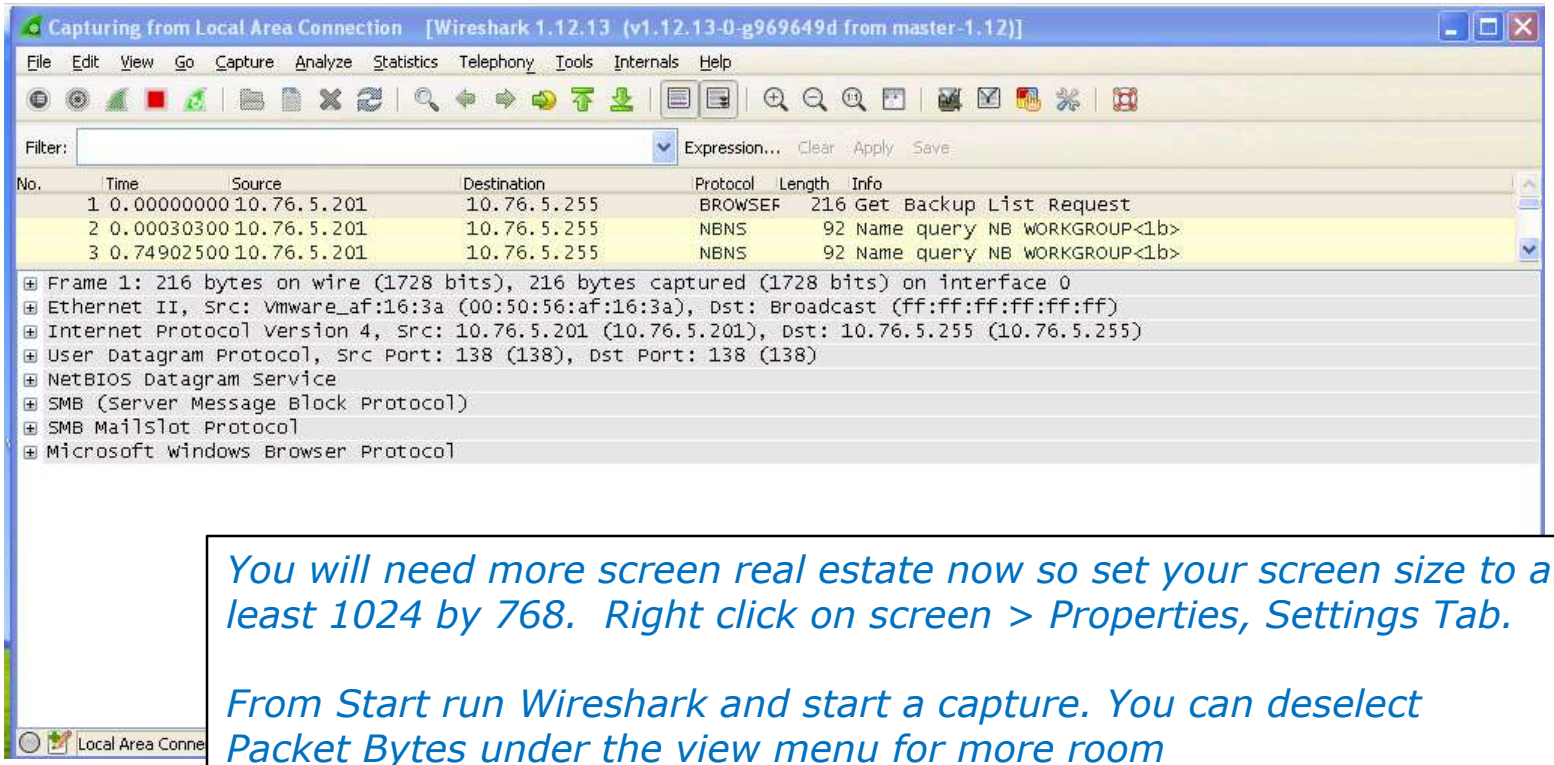
Open the ca_setup file on your desktop and install Cain and Abel.

When prompted about reinstalling pcap click Cancel since this was already installed by Wireshark.

CIS 76 MITM via ARP Poisoning



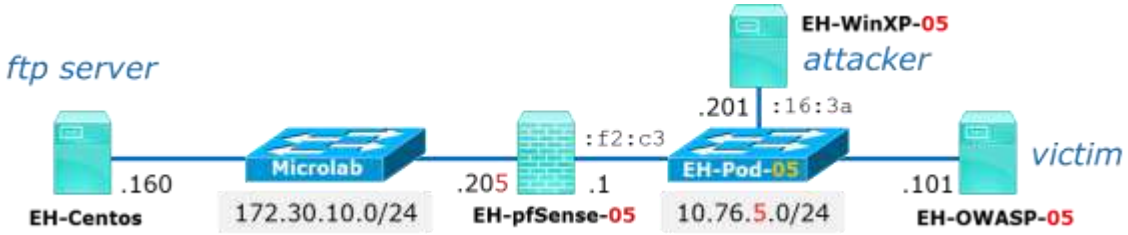
WinXP VM



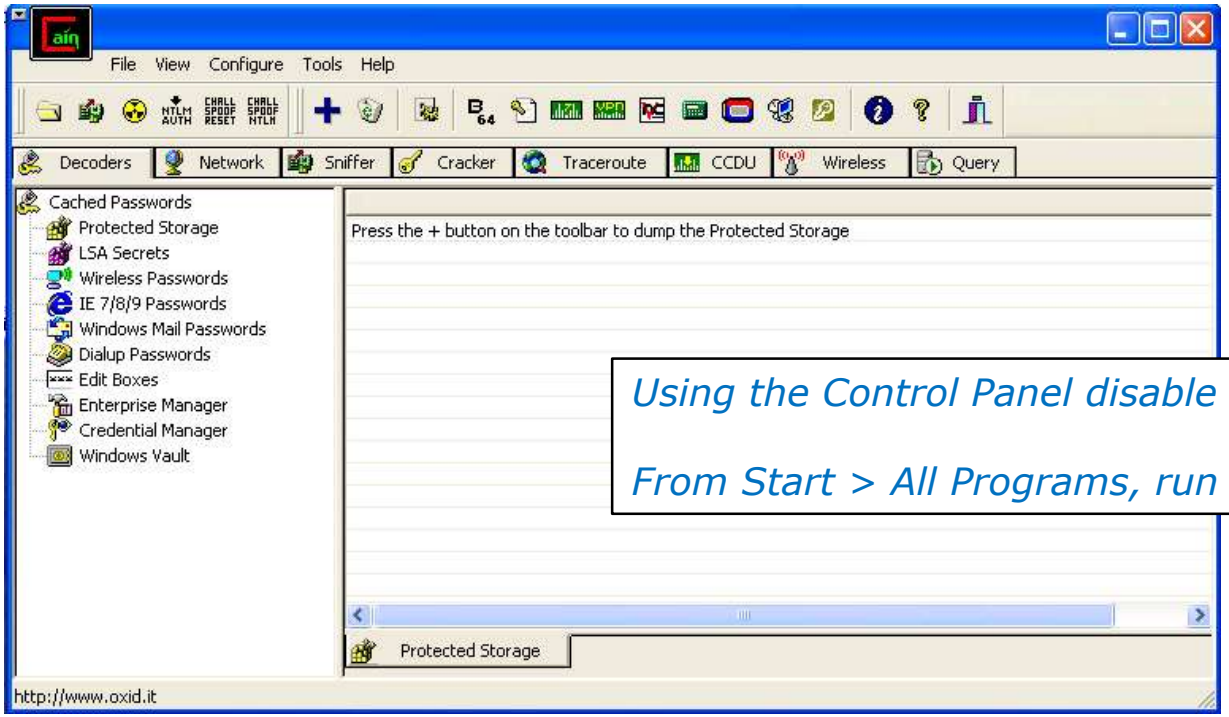
You will need more screen real estate now so set your screen size to at least 1024 by 768. Right click on screen > Properties, Settings Tab.

From Start run Wireshark and start a capture. You can deselect Packet Bytes under the view menu for more room

CIS 76 MITM via ARP Poisoning

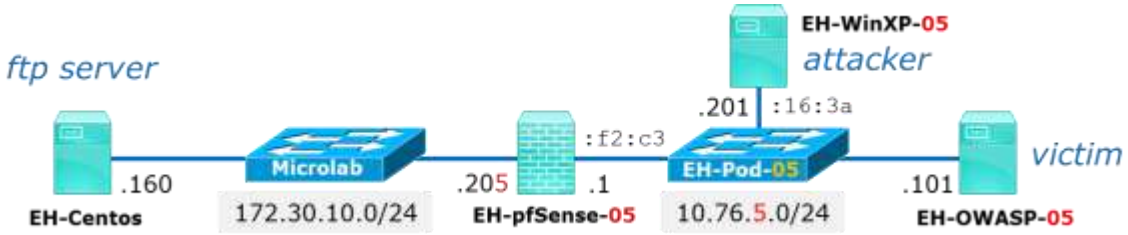


WinXP VM

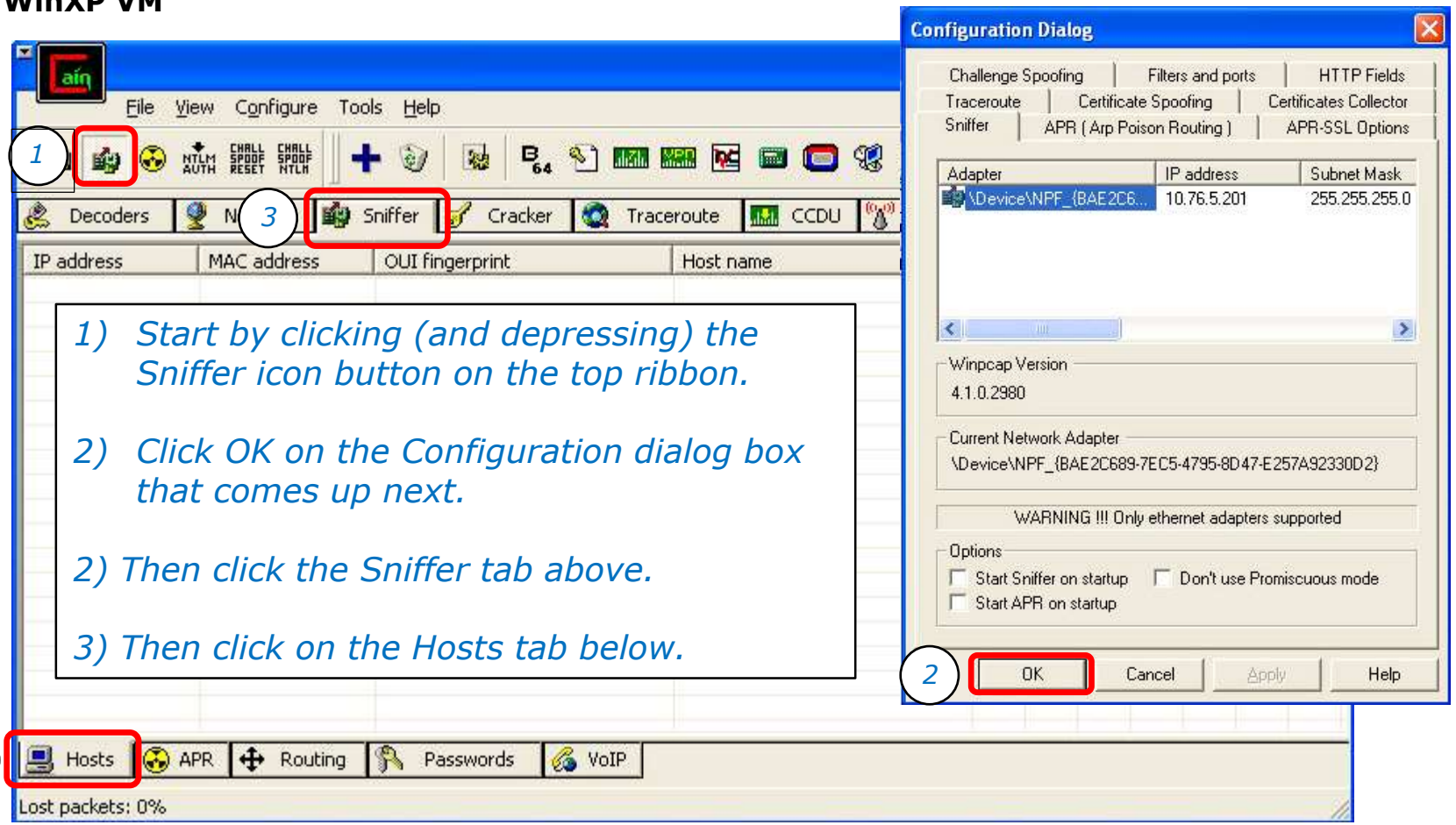


Using the Control Panel disable the Windows Firewall.

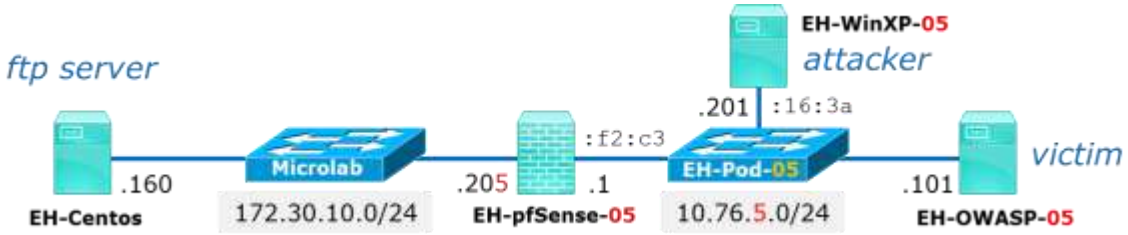
From Start > All Programs, run Cain.


ftp server
EH-WinXP-05
attacker
.201
:16:3a
:f2:c3
.160
Microlab
.205
.1
EH-Pod-05
.101
victim
EH-Centos
172.30.10.0/24
EH-pfSense-05
10.76.5.0/24
EH-OWASP-05

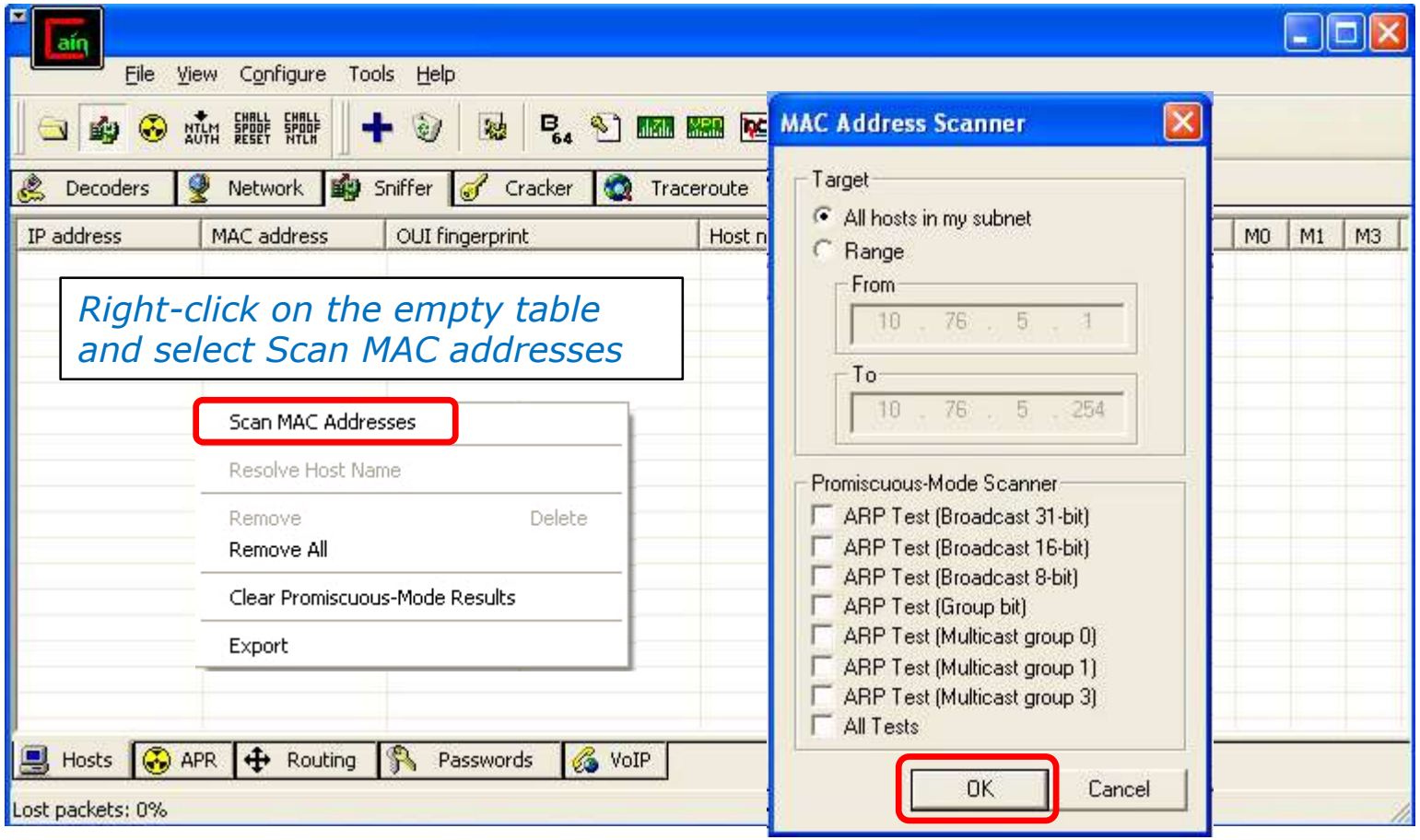
WinXP VM

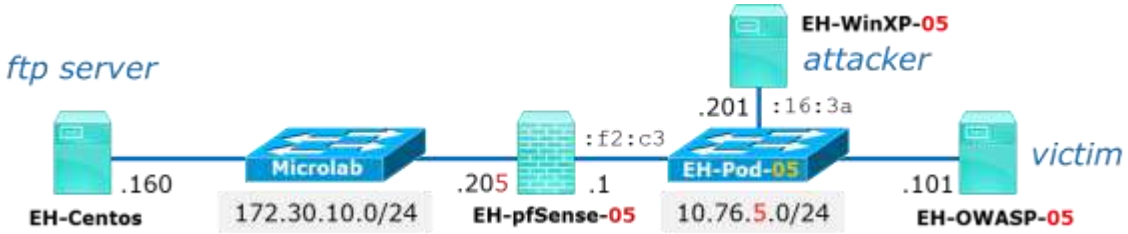

File View Configure Tools Help
1
Decoders
3
Sniffer
Cracker
Traceroute
CCDU
IP address
MAC address
OUI fingerprint
Host name
1) Start by clicking (and depressing) the Sniffer icon button on the top ribbon.
2) Click OK on the Configuration dialog box that comes up next.
2) Then click the Sniffer tab above.
3) Then click on the Hosts tab below.
Configuration Dialog
Challenge Spoofing
Filters and ports
HTTP Fields
Traceroute
Certificate Spoofing
Certificates Collector
Sniffer
APR (Arp Poison Routing)
APR-SSL Options
Adapter
IP address
Subnet Mask
\Device\NPF_{BAE2C6...
10.76.5.201
255.255.255.0
Winpcap Version
4.1.0.2980
Current Network Adapter
\Device\NPF_{BAE2C689-7EC5-4795-8D47-E257A92330D2}
WARNING !!! Only ethernet adapters supported
Options
Start Sniffer on startup
Don't use Promiscuous mode
Start APR on startup
2
OK
Cancel
Apply
Help
4
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

CIS 76 MITM via ARP Poisoning

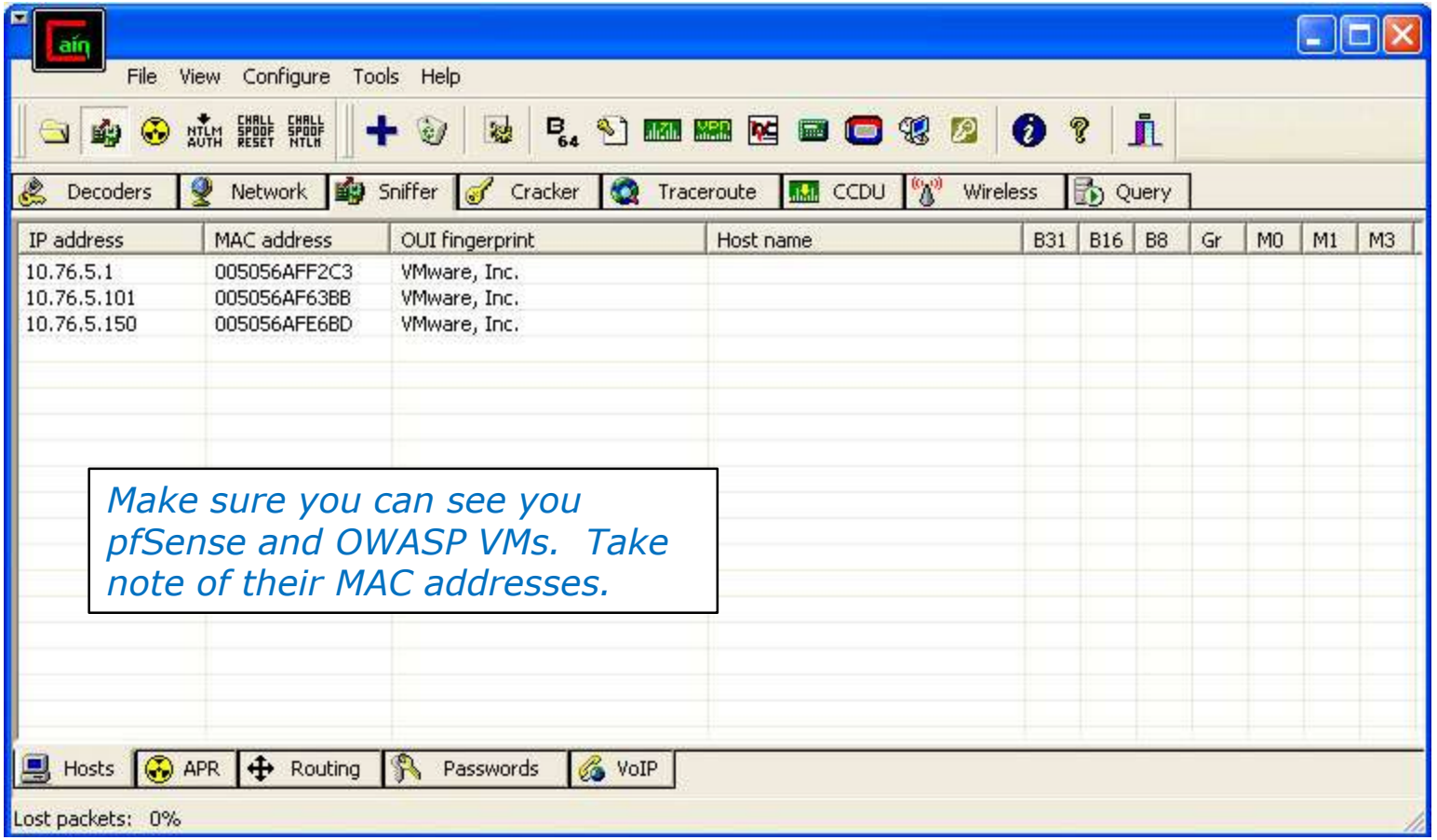


WinXP VM

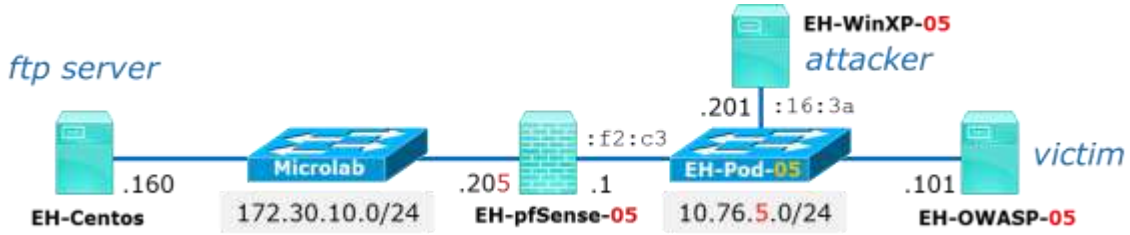



EH-WinXP-05
attacker
ftp server
.201
:16:3a
:f2:c3
victim
.160
Microlab
.205
.1
EH-Pod-05
.101
EH-Centos
172.30.10.0/24
EH-pfSense-05
10.76.5.0/24
EH-OWASP-05

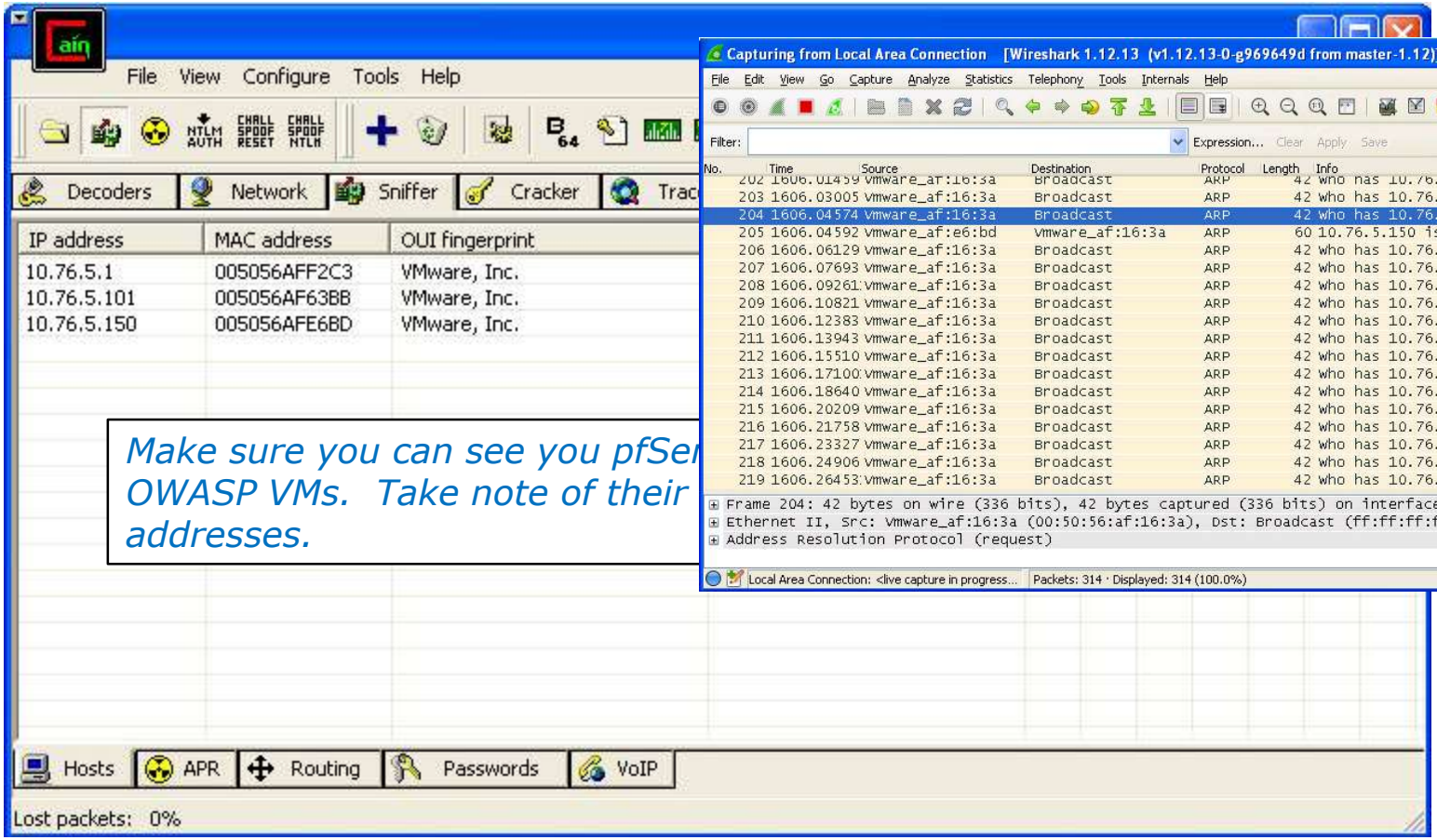
WinXP VM


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B31 B16 B8 Gr M0 M1 M3
10.76.5.1 005056AFF2C3 VMware, Inc.
10.76.5.101 005056AF63BB VMware, Inc.
10.76.5.150 005056AFE6BD VMware, Inc.
Make sure you can see you pfSense and OWASP VMs. Take note of their MAC addresses.
Hosts APR Routing Passwords VoIP
Lost packets: 0%

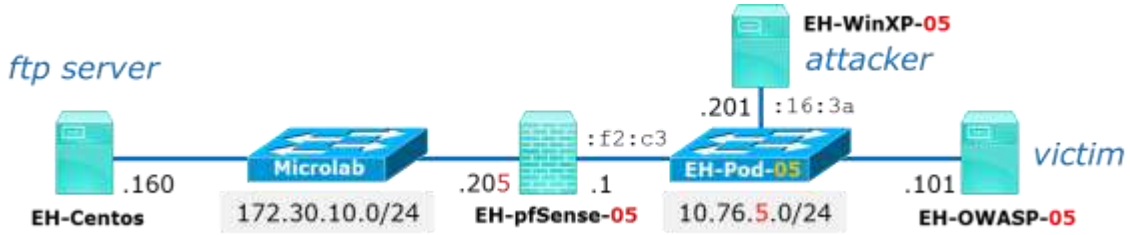
CIS 76 MITM via ARP Poisoning



WinXP VM



CIS 76 MITM via ARP Poisoning



WinXP VM

Capturing from Local Area Connection [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

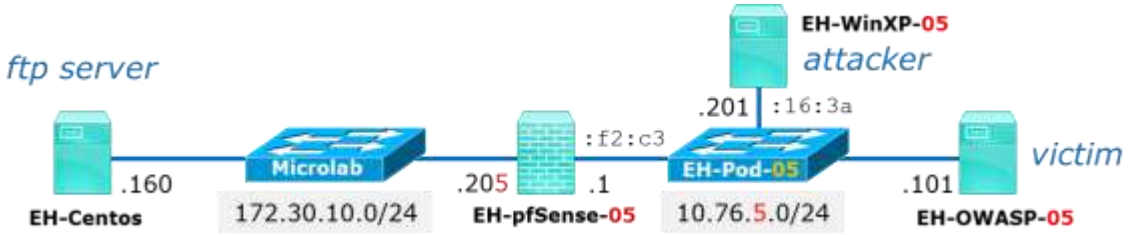
No.	Time	Source	Destination	Protocol	Length	Info
202	1606.01459	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.148? Tell 10.76.5.201
203	1606.03005	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.149? Tell 10.76.5.201
204	1606.04574	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.150? Tell 10.76.5.201
205	1606.04592	vmware_af:e6:bd	vmware_af:16:3a	ARP	60	10.76.5.150 is at 00:50:56:af:e6:bd
206	1606.06129	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.151? Tell 10.76.5.201
207	1606.07693	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.152? Tell 10.76.5.201
208	1606.09261	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.153? Tell 10.76.5.201
209	1606.10821	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.154? Tell 10.76.5.201
210	1606.12383	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.155? Tell 10.76.5.201
211	1606.13943	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.156? Tell 10.76.5.201
212	1606.15510	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.157? Tell 10.76.5.201
213	1606.17100	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.158? Tell 10.76.5.201
214	1606.18640	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.159? Tell 10.76.5.201
215	1606.20209	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.160? Tell 10.76.5.201
216	1606.21758	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.161? Tell 10.76.5.201
217	1606.23327	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.162? Tell 10.76.5.201
218	1606.24906	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.163? Tell 10.76.5.201
219	1606.26453	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.164? Tell 10.76.5.201

⊞ Frame 204: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
⊞ Ethernet II, Src: Vmware_af:16:3a (00:50:56:af:16:3a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

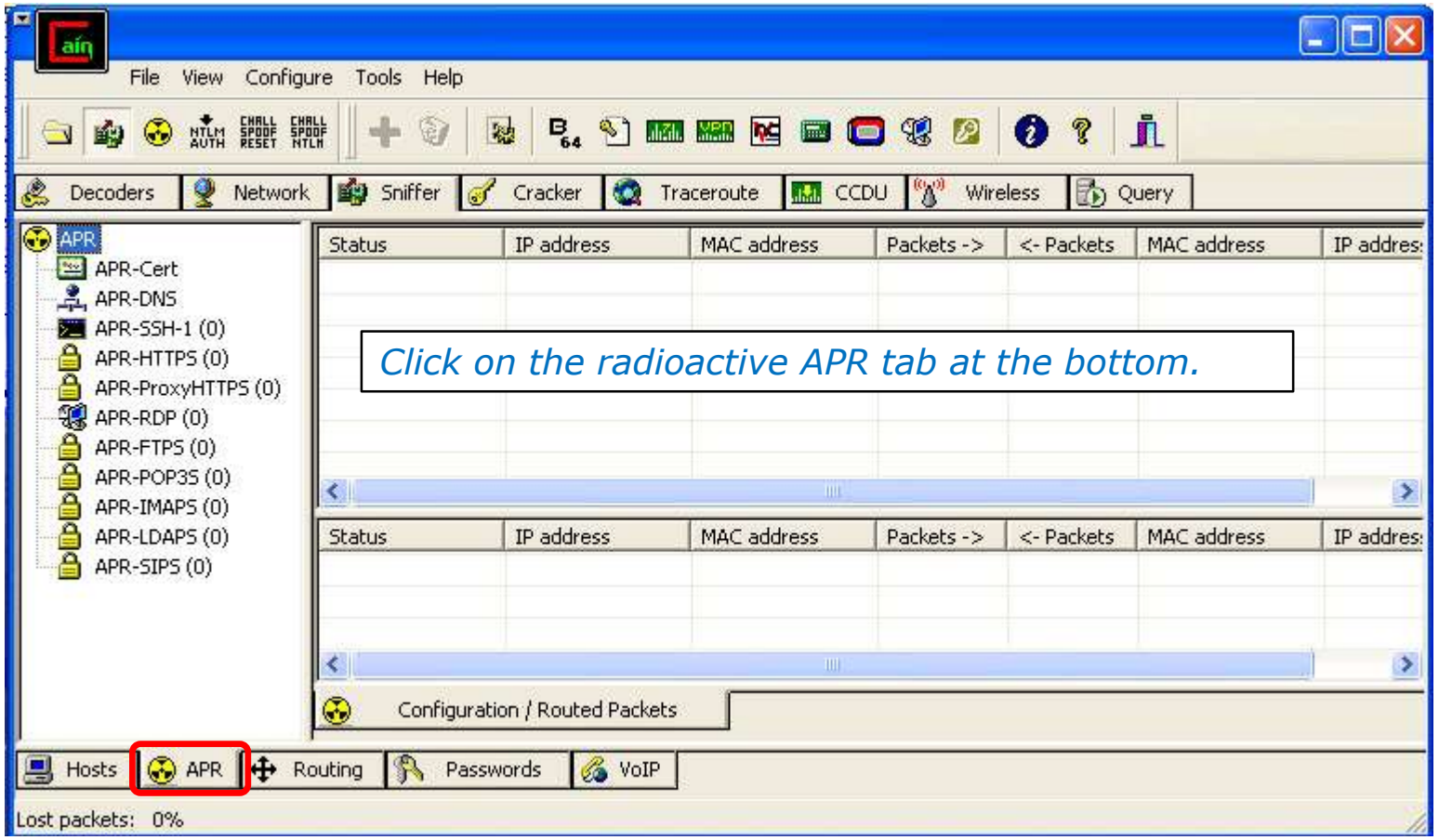
Local Area Connection: <live capture in progress... Packets: 314 · Displayed: 314 (100.0%) Profile: Default

In Wireshark you will see your WinXP VM has sent out ARP requests for every IP address on your pod subnet.

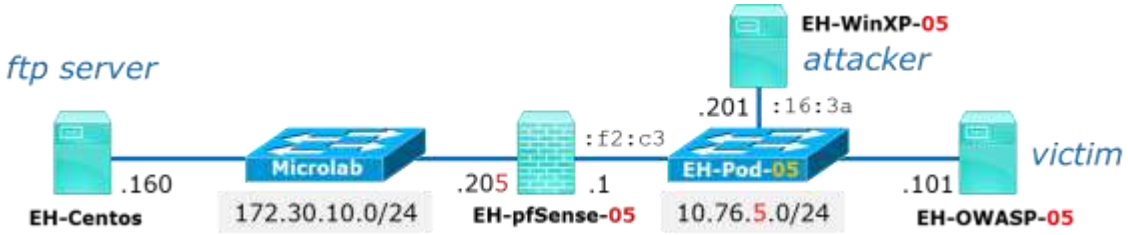
CIS 76 MITM via ARP Poisoning



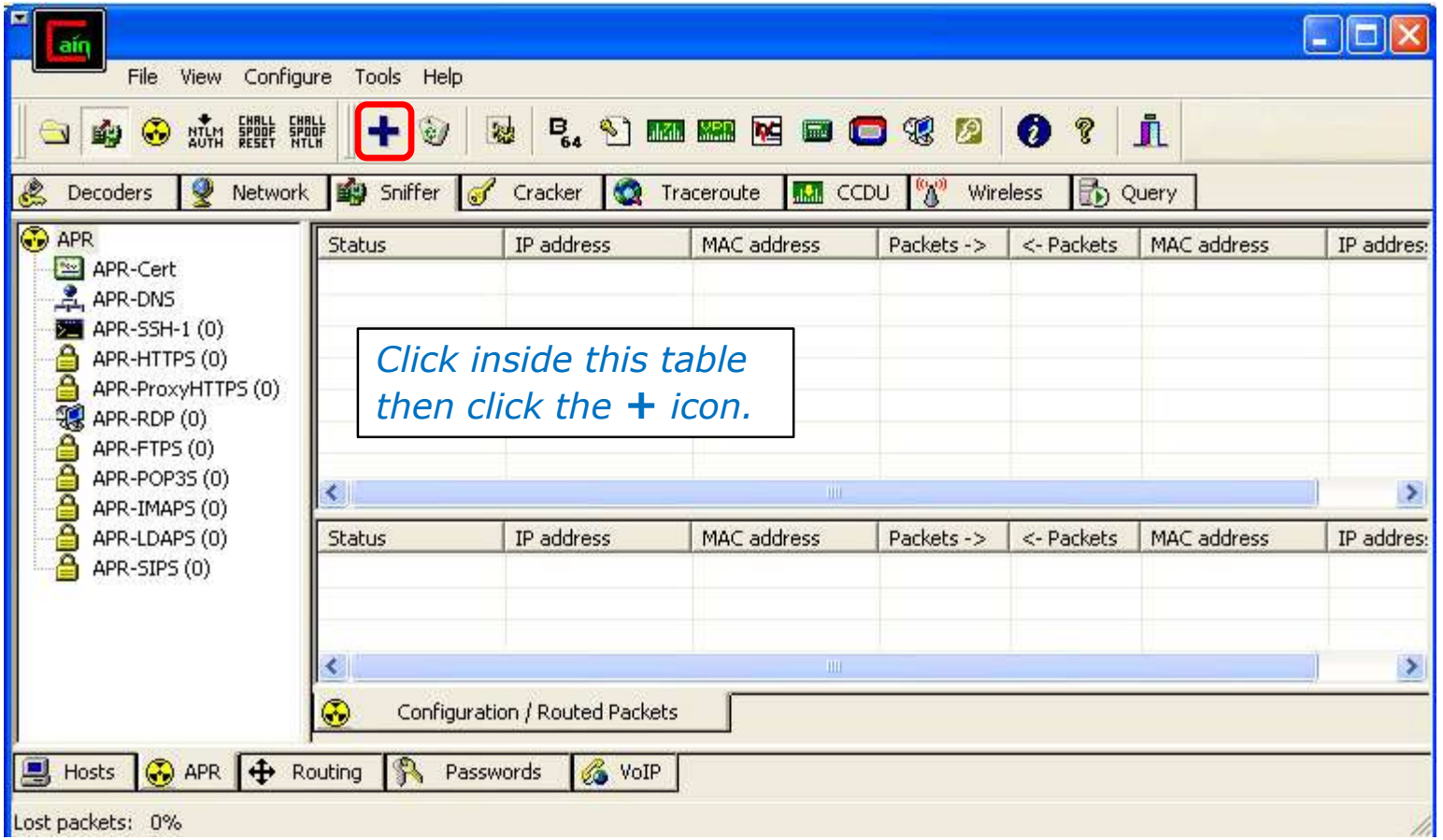
WinXP VM



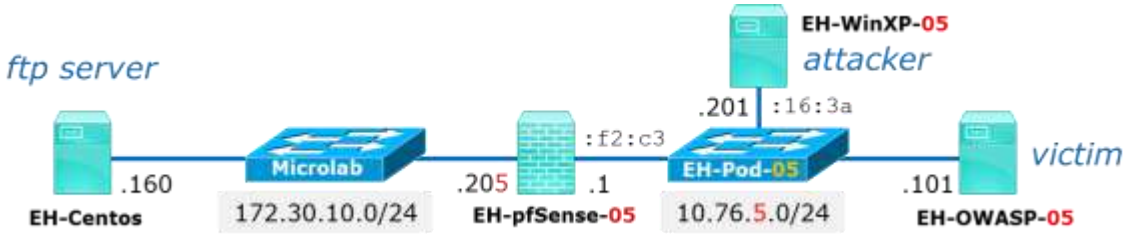
CIS 76 MITM via ARP Poisoning



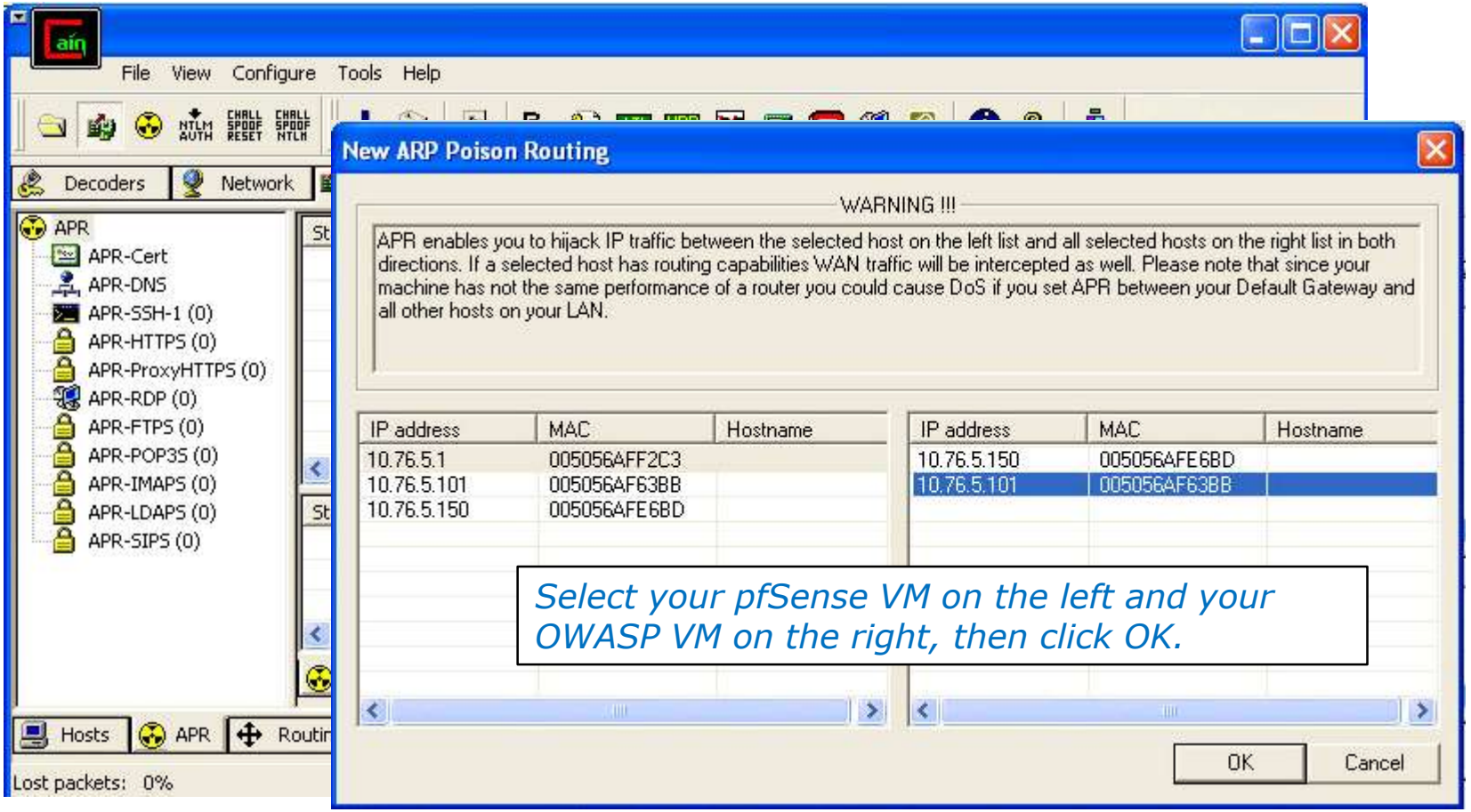
WinXP VM



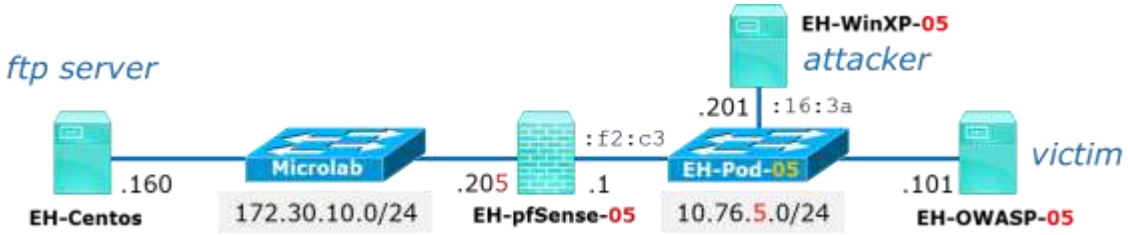
CIS 76 MITM via ARP Poisoning



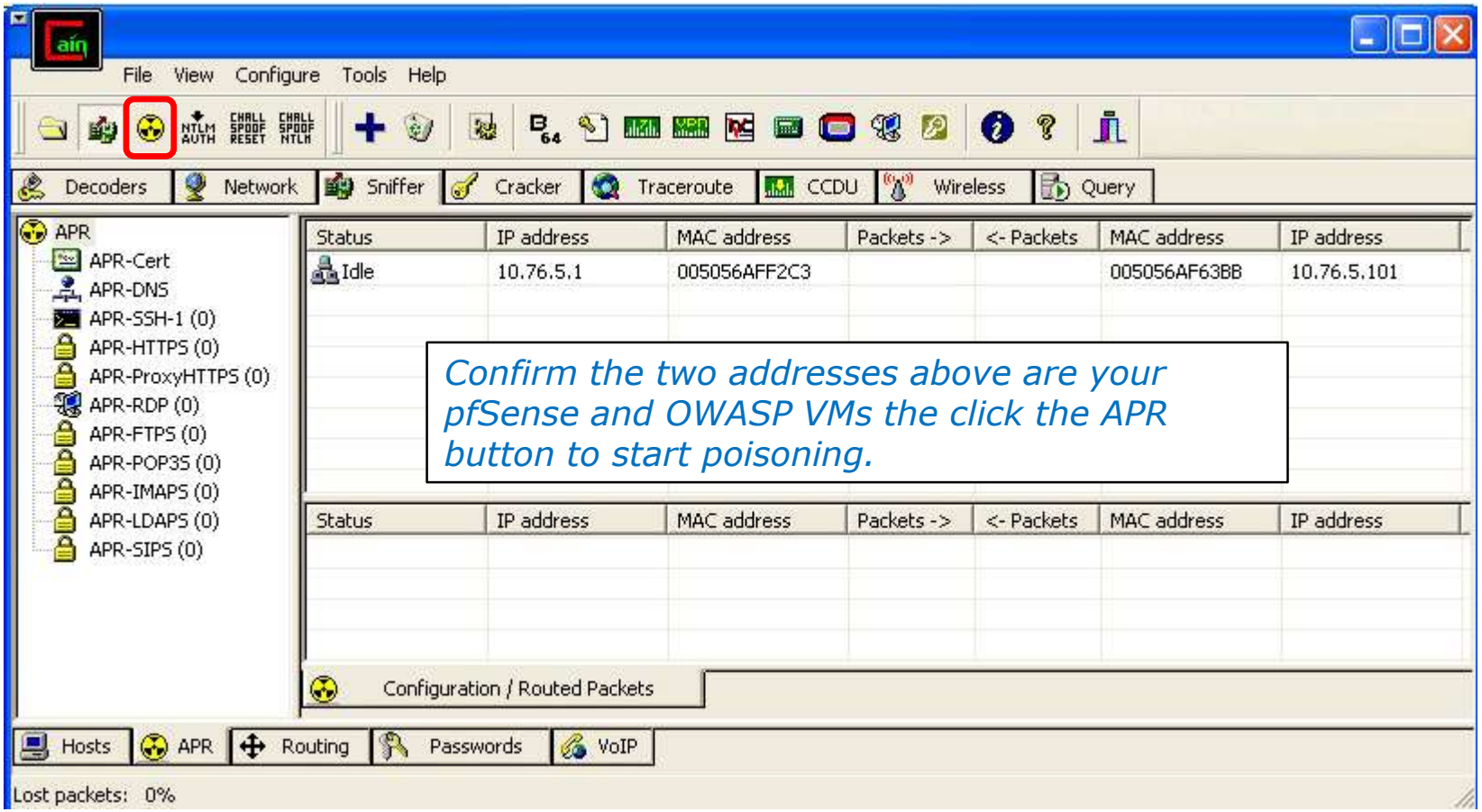
WinXP VM

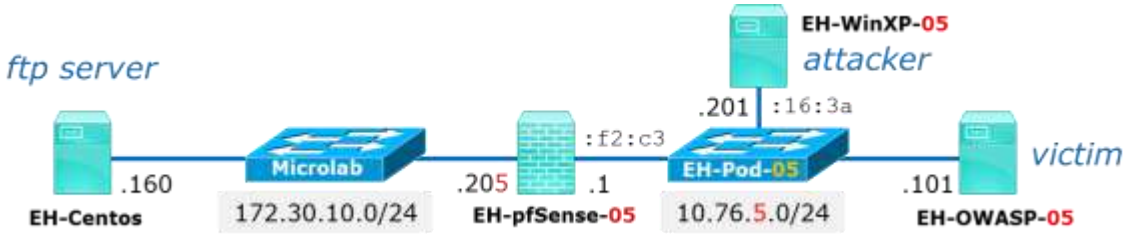


CIS 76 MITM via ARP Poisoning

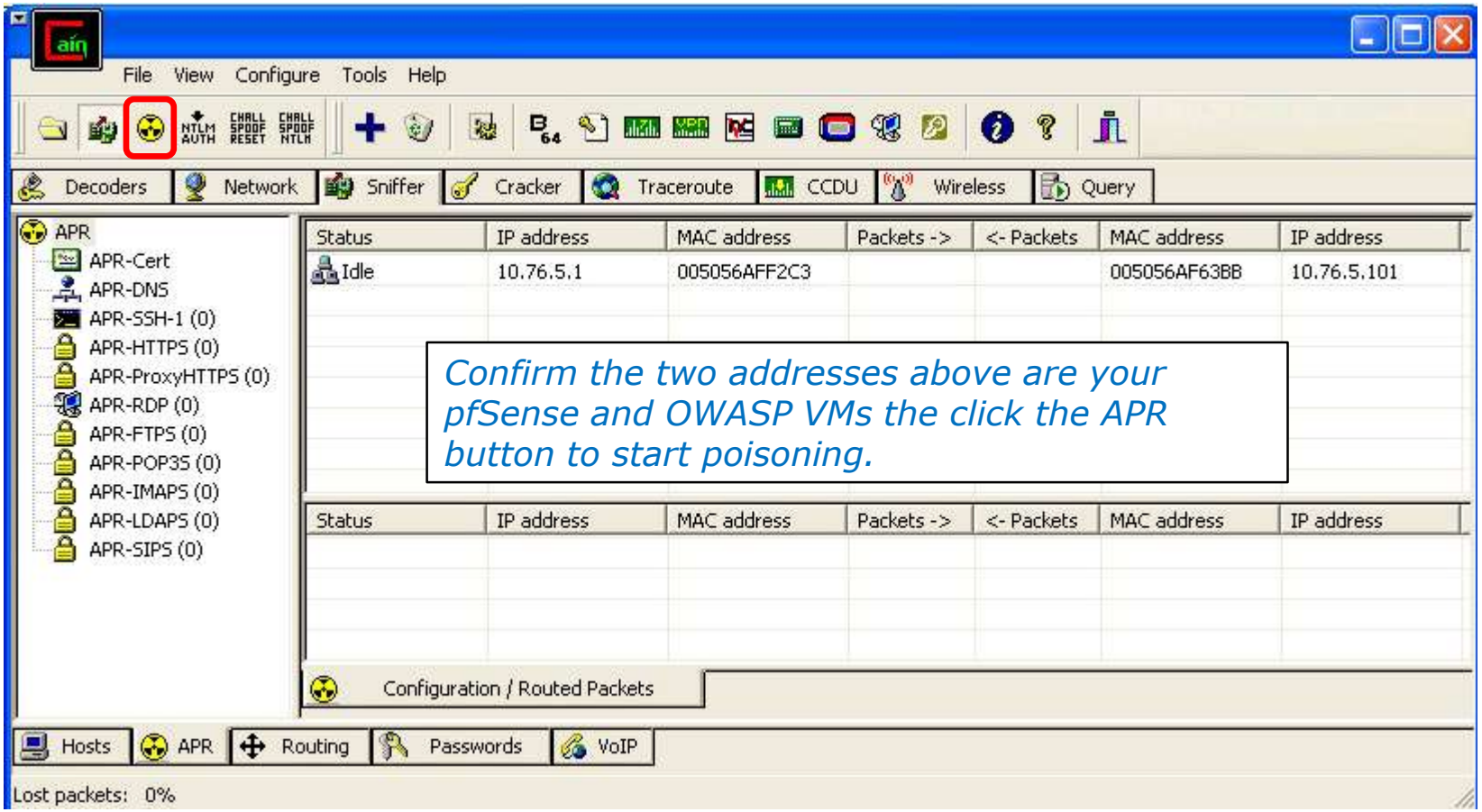


WinXP VM

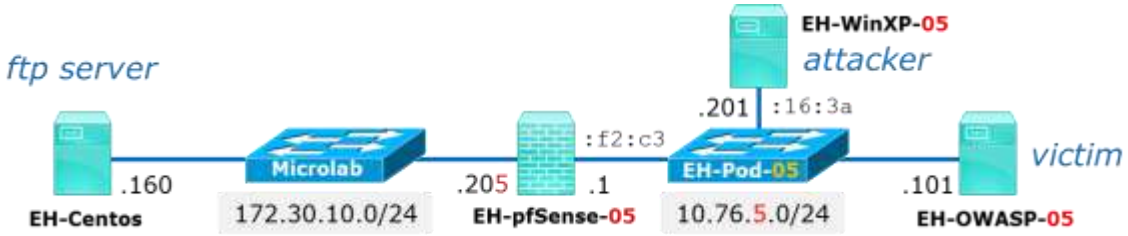



ftp server
EH-WinXP-05
attacker
.201
:16:3a
:f2:c3
.160
Microlab
.205
.1
EH-Pod-05
victim
.101
EH-Centos
172.30.10.0/24
EH-pfSense-05
10.76.5.0/24
EH-OWASP-05

WinXP VM


File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
MAC address
IP address
Idle
10.76.5.1
005056AFF2C3
005056AF63BB
10.76.5.101
Confirm the two addresses above are your pfSense and OWASP VMs the click the APR button to start poisoning.
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

CIS 76 MITM via ARP Poisoning



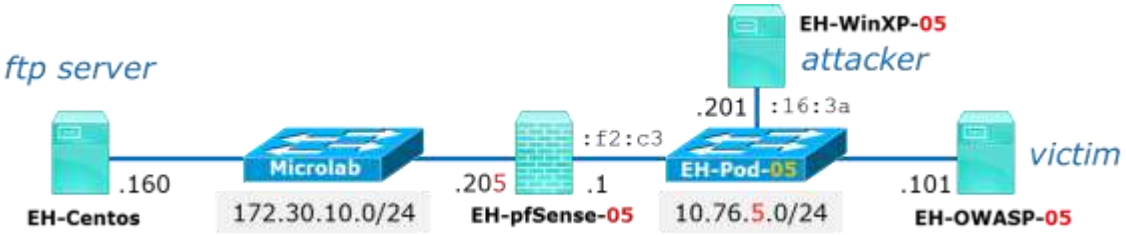
OWASP VM

```
root@owaspbwa:~# ping -c1 172.30.10.160
PING 172.30.10.160 (172.30.10.160) 56(84) bytes of data.
64 bytes from 172.30.10.160: icmp_seq=1 ttl=63 time=4.05 ms

--- 172.30.10.160 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.057/4.057/4.057/0.000 ms
root@owaspbwa:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.76.5.1                ether   00:50:56:af:16:3a   C                     eth0
root@owaspbwa:~# _
```

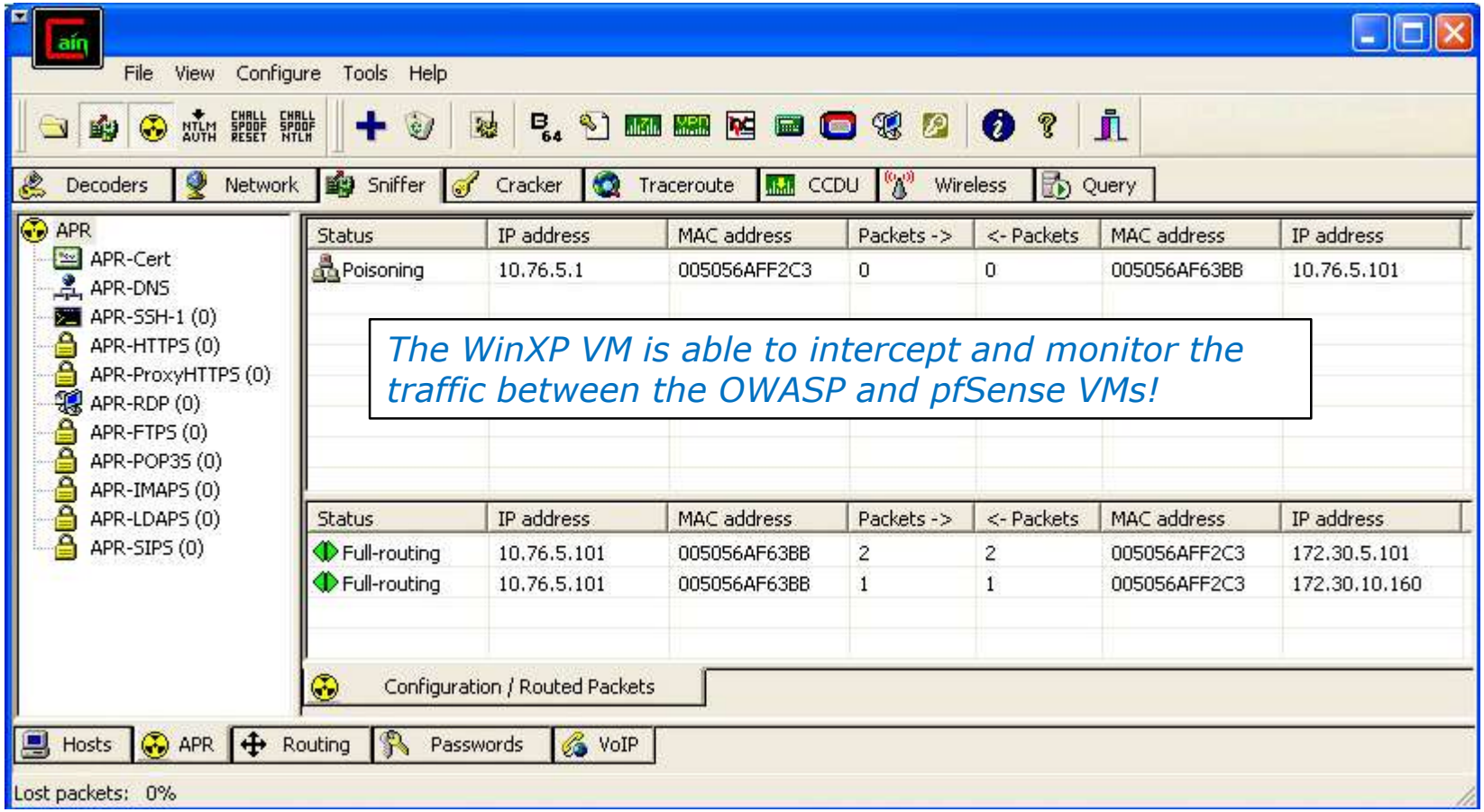
Ping EH-Centos from your OWASP VM to test connectivity.

Notice the OWASP ARP cache no longer has the real MAC address for the pfSense VM!

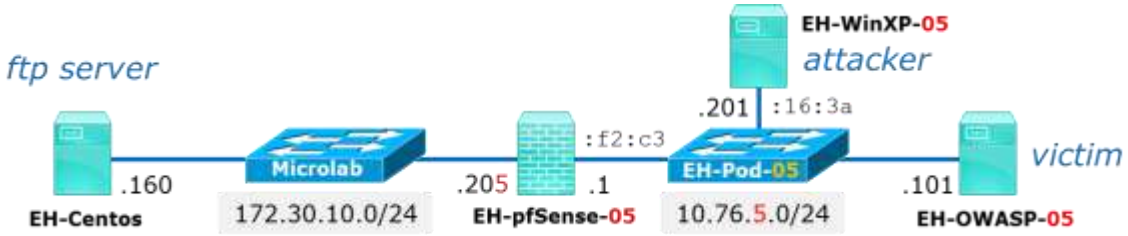
CIS 76 MITM via ARP Poisoning



WinXP VM



CIS 76 MITM via ARP Poisoning

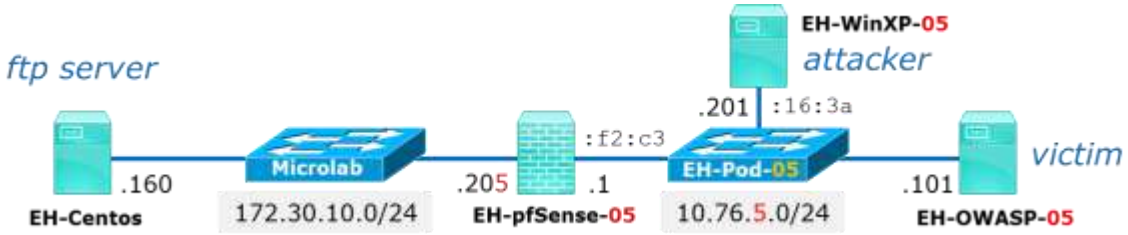


OWASP VM

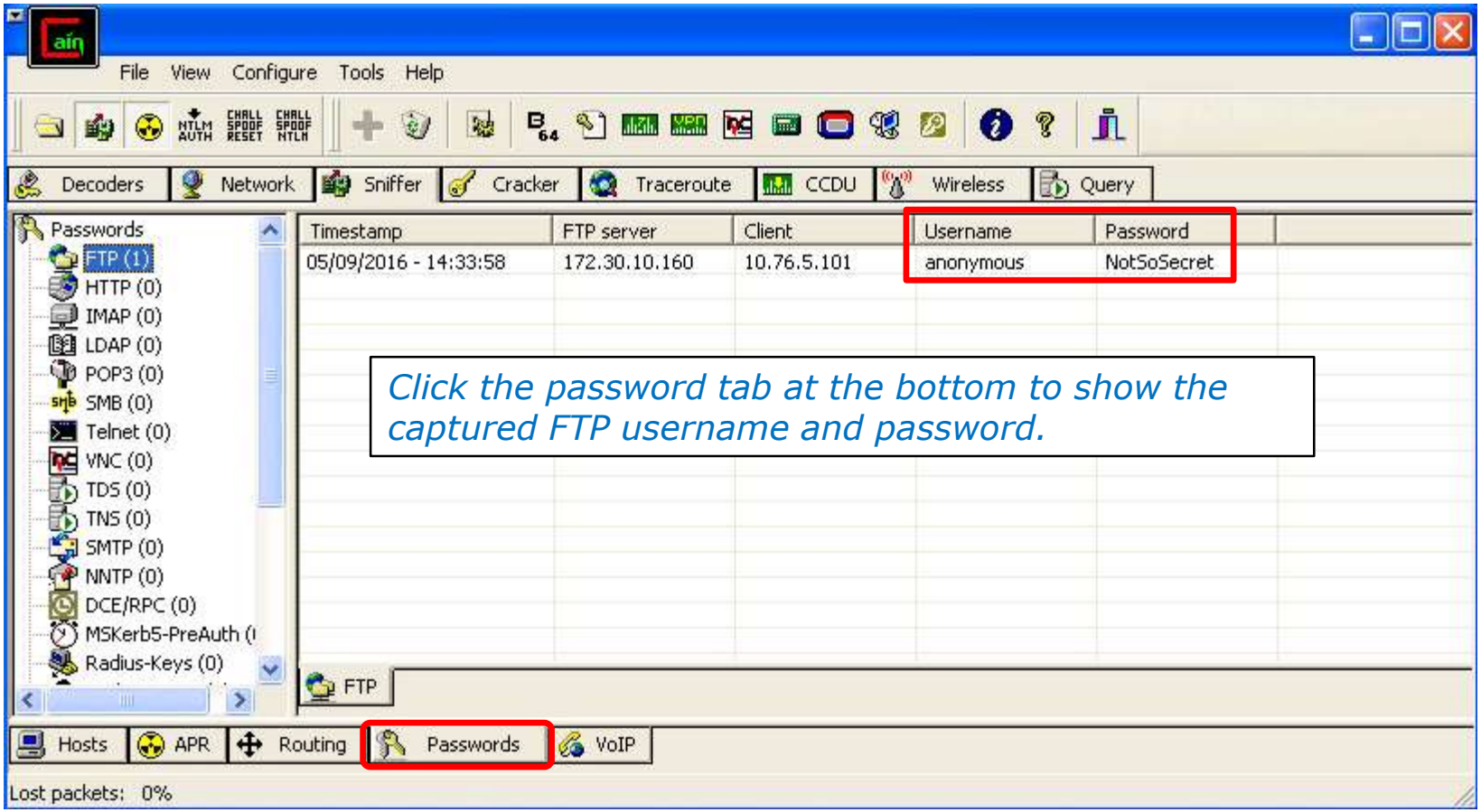
```
root@owaspbwa:~# ftp 172.30.10.160
Connected to 172.30.10.160.
220 Welcome to CIS 76 FTP service.
Name (172.30.10.160:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd pub
250 Directory successfully changed.
ftp> get admonition
local: admonition remote: admonition
500 Illegal PORT command.
ftp: bind: Address already in use
ftp> passive
Passive mode on.
ftp> get admonition
local: admonition remote: admonition
227 Entering Passive Mode (172,30,10,160,20,147).
150 Opening BINARY mode data connection for admonition (205 bytes).
226 Transfer complete.
205 bytes received in 0.00 secs (1450.7 kB/s)
ftp> exit
221 Goodbye.
root@owaspbwa:~# _
```

Repeat downloading a file from the ftp server.

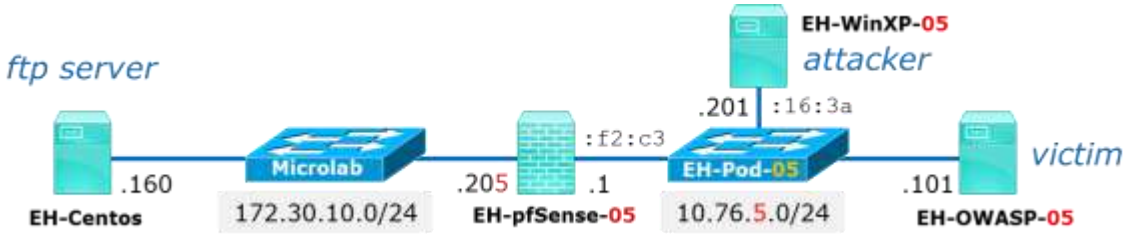
CIS 76 MITM via ARP Poisoning



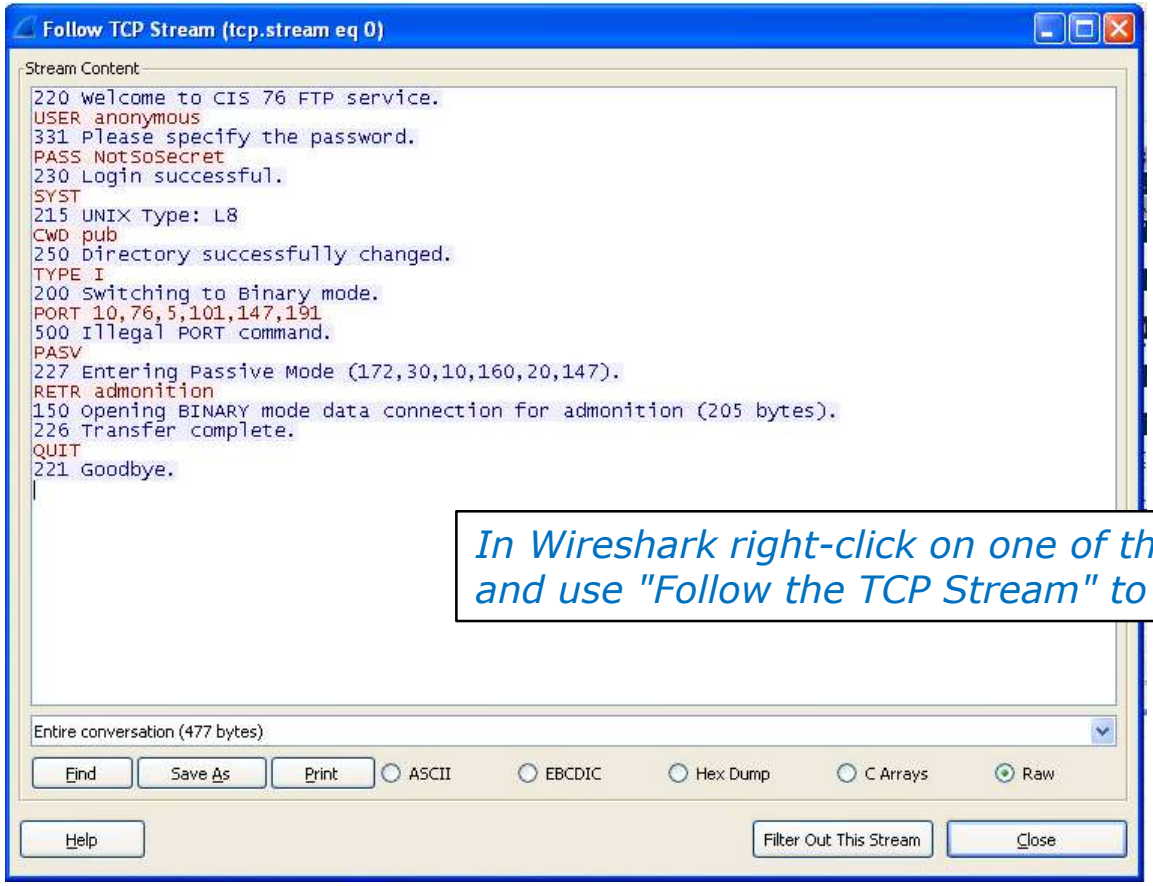
WinXP VM



CIS 76 MITM via ARP Poisoning

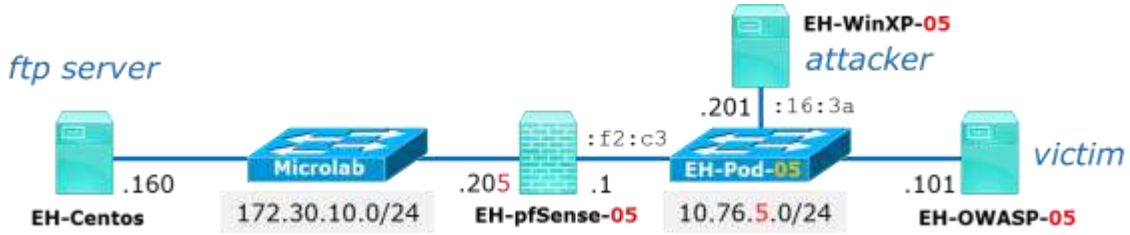


WinXP VM



In Wireshark right-click on one of the FTP packets and use "Follow the TCP Stream" to see the session.

CIS 76 MITM via ARP Poisoning



WinXP VM

Capturing from Local Area Connection [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
485	6335.48364	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a
486	6365.48349	Vmware_af:16:3a	Vmware_af:f2:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
487	6365.48365	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a
488	6395.48382	Vmware_af:16:3a	Vmware_af:f2:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
489	6395.48403	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a
490	6425.48368	Vmware_af:16:3a	Vmware_af:f2:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
491	6425.48395	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a
492	6455.48376	Vmware_af:16:3a	Vmware_af:f2:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
493	6455.48387	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a
494	6485.48386	Vmware_af:16:3a	Vmware_af:f2:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
495	6485.48396	Vmware_af:16:3a				
496	6515.48383	Vmware_af:16:3a				
497	6515.48392	Vmware_af:16:3a				
498	6545.48383	Vmware_af:16:3a				
499	6545.48412	Vmware_af:16:3a				
500	6575.48353	Vmware_af:16:3a				
501	6575.48367	Vmware_af:16:3a	Vmware_af:63:bb	ARP	42	10.76.5.1 is at 00:50:56:af:16:3a

In Wireshark notice that the poisoning is brought about by the WinXP VM flooding the subnet with ARP replies containing the fraudulent IP/MAC pairs.

Frame 381: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:16:3a (00:50:56:af:16:3a)
Internet Protocol Version 4, Src: 172.30.10.160 (172.30.10.160), Dst: 10.76.5.101 (10.76.5.101)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 43057 (43057), Seq: 1, Ack: 1, Len: 36

Local Area Connection: <live capture in progress> | Packets: 501 · Displayed: 501 (100.0%) | Profile: Default

References

- Cain
  http://www.oxid.it/cain.html
- Cain & Abel
  https://www.concise-courses.com/hacking-tools/packet-sniffers/cain-abel/