

MITM ARP Poison Attack

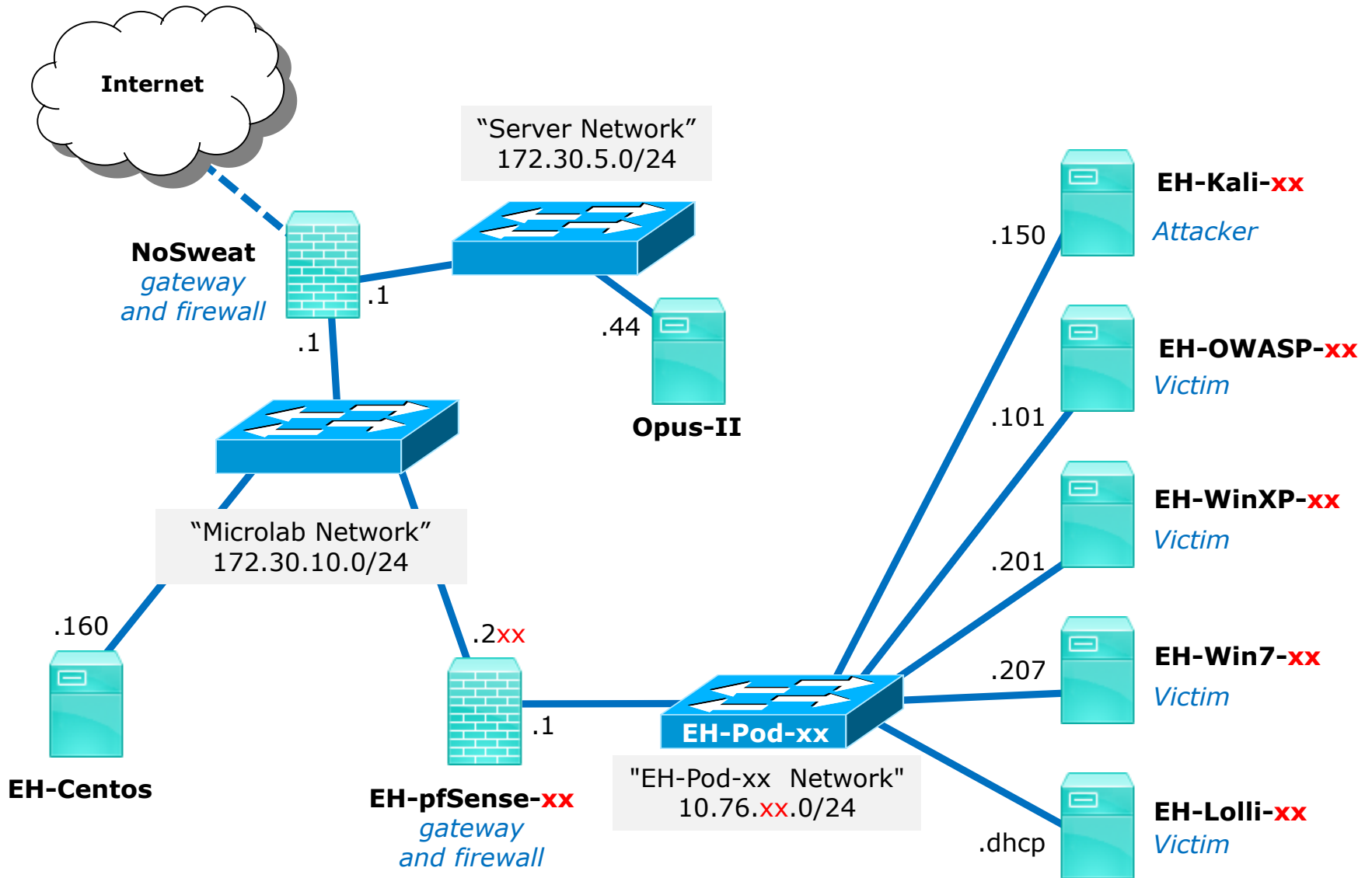
DRAFT
Last updated 9/4/2017

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.

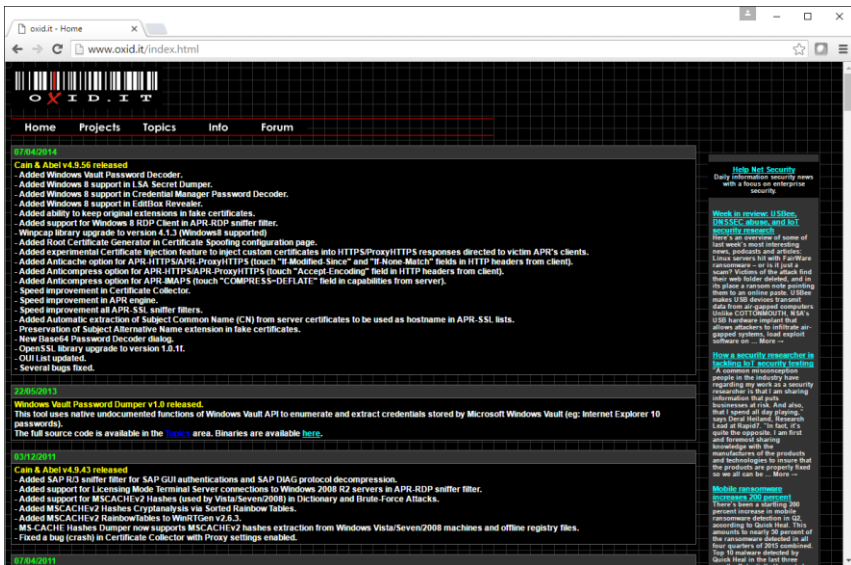


Requirements

1. EH-Centos VM running with vsftpd installed on uLab 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

Download Wireshark

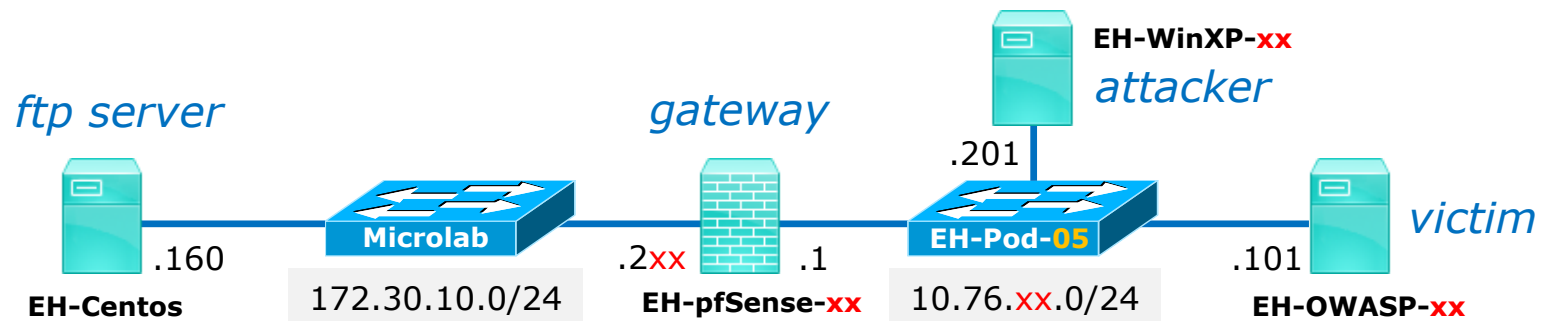
The current stable release of Wireshark is 2.0.5. It supersedes all previous releases.

Stable Release (2.0.5)	▼
Old Stable Release (1.12.13)	▲
<ul style="list-style-type: none"> Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps® (32-bit) OS X 10.6 and later Intel 64-bit .dmg OS X 10.6 and later Intel 32-bit .dmg Source Code 	
Development Release (2.2.0rc2)	▼
Documentation	▼

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

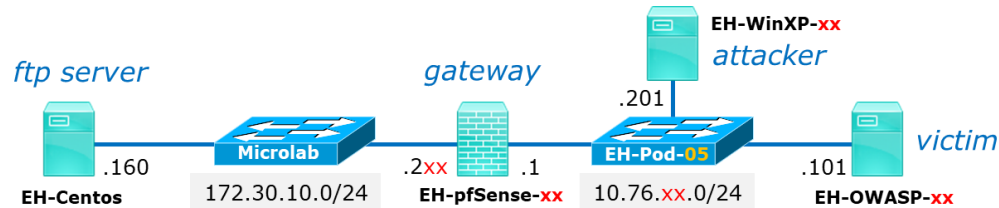
These websites are for reference only. No need to download anything from them for this exercise.

Man in the Middle Attack via ARP poisoning



In this scenario the WinXP attacker 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.



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:~# _

```

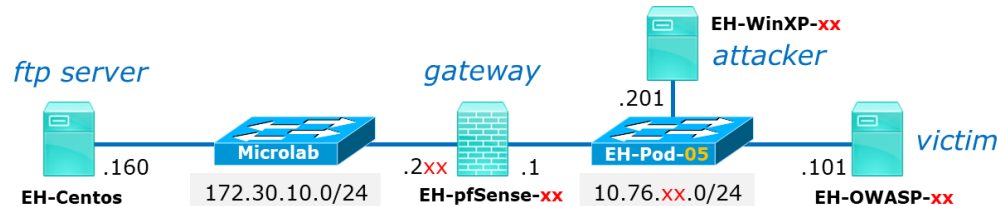
Ping EH-Centos from your OWASP VM to test connectivity.

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

```

ping -c1 172.30.10.160
arp

```

OWASP VM

```

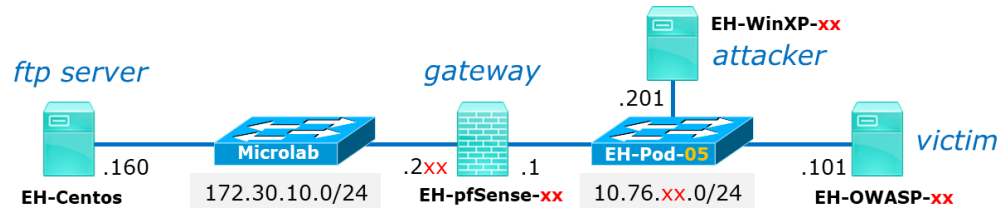
root@owaspbwa:~# ftp 172.30.10.160
Connected to 172.30.10.160.
220 Welcome to CIS 76 FTP service.
Name (172.30.10.160:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls
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.

ftp 172.30.10.160
anonymous
 NotSoSecret
passive
ls
cd pub
ls



OWASP VM

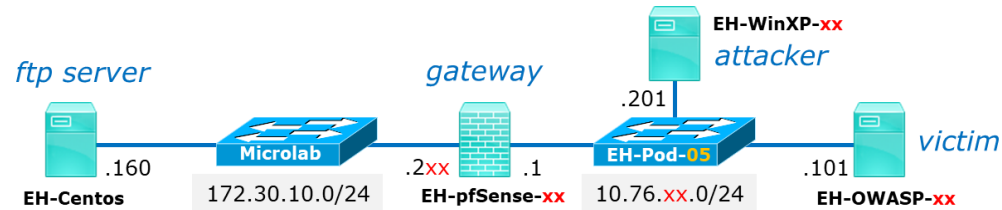
```
ftp> get admonition
local: admonition remote: admonition
227 Entering Passive Mode (172,30,10,160,37,183).
150 Opening BINARY mode data connection for admonition (205 bytes).
226 Transfer complete.
205 bytes received in 0.00 secs (1551.9 kB/s)
ftp> exit
221 Goodbye.
root@owaspbwa:~# cat admonition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

Unauthorized hacking is a crime!

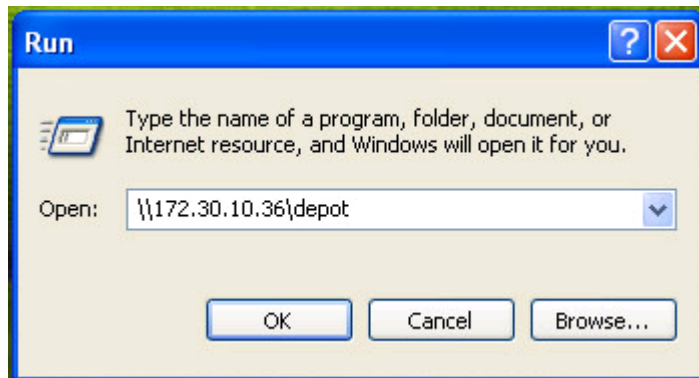
An ethical hacker will only perform penetration testing with
the explicit end-to-end authorization from the owners of the
networks and systems being tested.
root@owaspbwa:~#
```

*Confirm you can
download the admonition
file.*

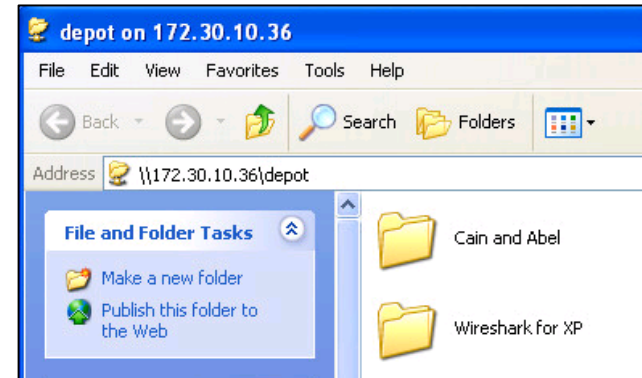
**get admonition
exit
cat admonition**



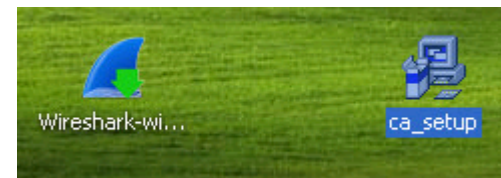
WinXP VM

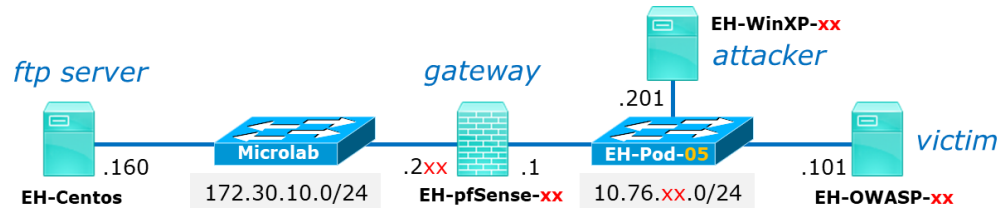


- 1) Use:
Start > Run ... > \\172.30.10.36\depot
to connect to the depot file share

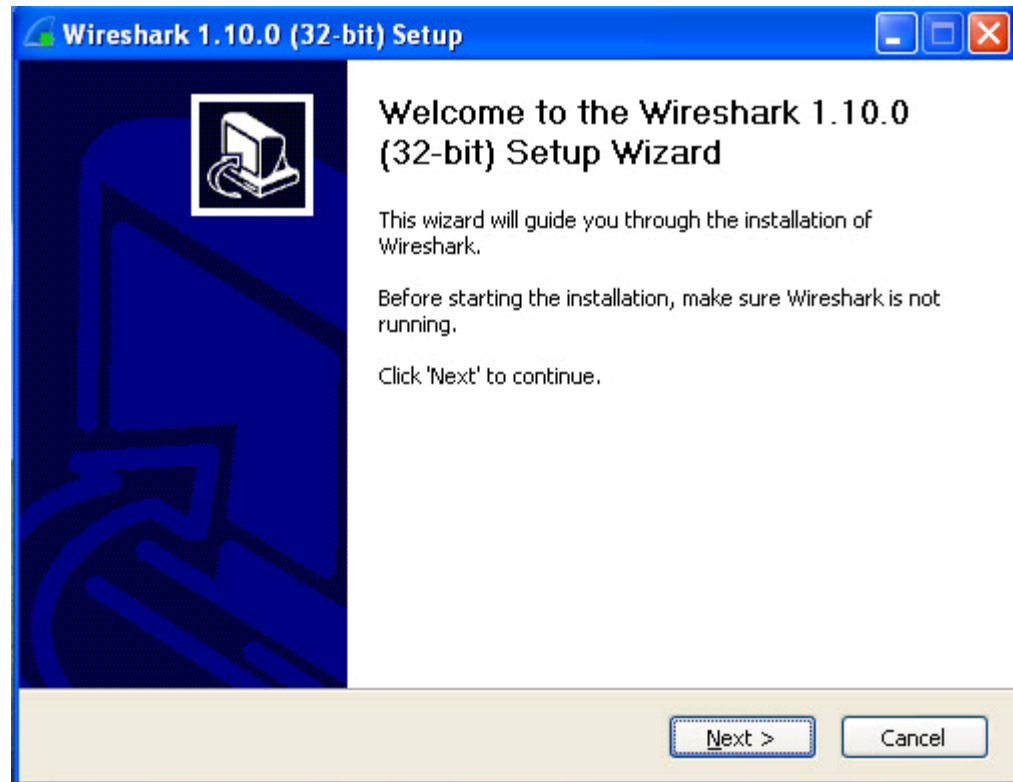


- 2) *Open the "Cain and Abel" and "Wireshark for XP" folders and drag their setup files to your desktop*





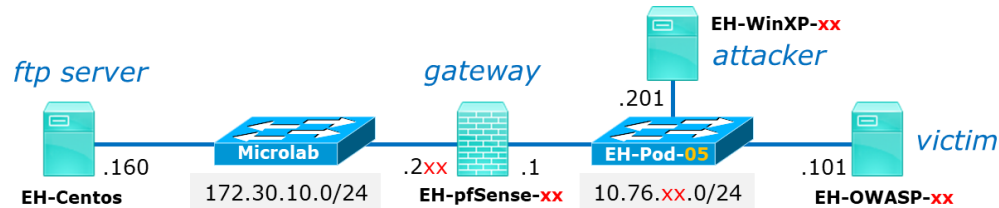
WinXP VM



*Open the
Wireshark-win32-1.10.0
file on your desktop and
install Wireshark.*

*You can ignore the XP
warning.*

Take the setup defaults.

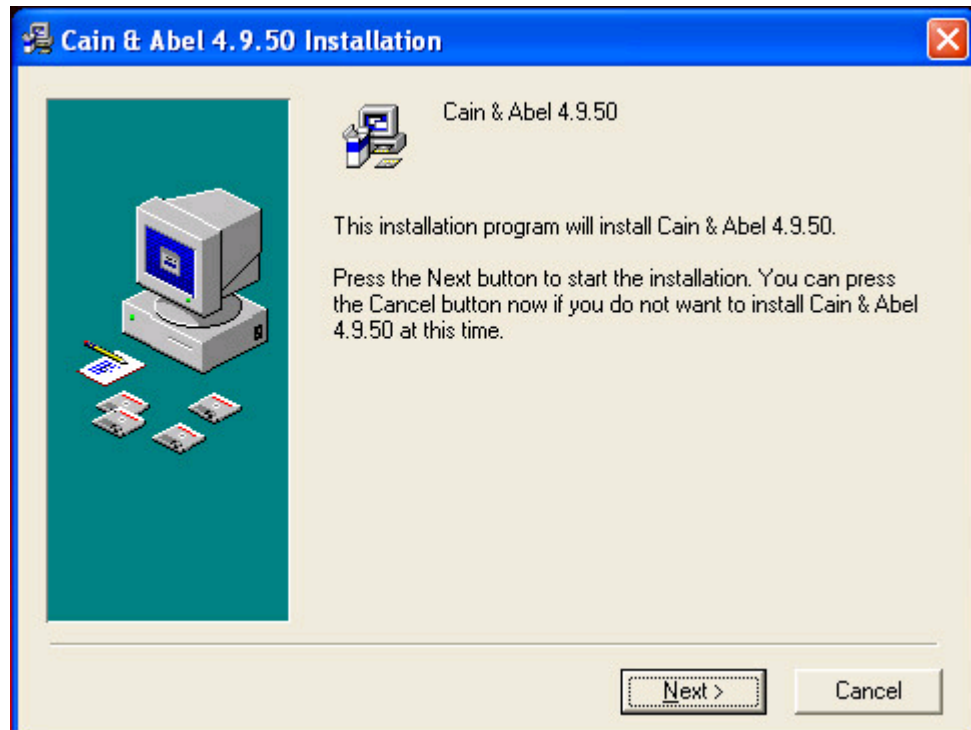


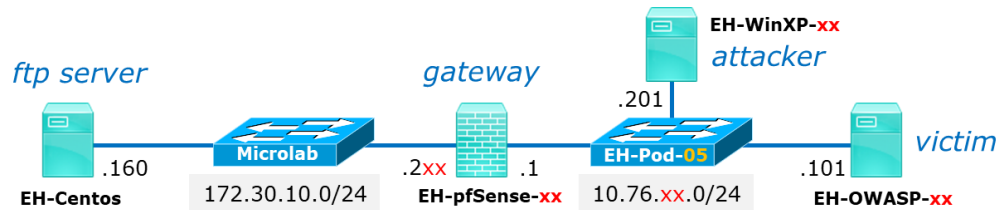
WinXP VM



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

2) When prompted about reinstalling `pcap` click **Cancel** since this was already installed by Wireshark.





WinXP VM

The screenshot shows Wireshark capturing traffic on the Local Area Connection. The packet list shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.76.5.201	10.76.5.255	BROWSEF	216	Get Backup List Request
2	0.00030300	10.76.5.201	10.76.5.255	NBNS	92	Name query NB WORKGROUP<1b>
3	0.74902500	10.76.5.201	10.76.5.255	NBNS	92	Name query NB WORKGROUP<1b>

The packet details pane for the first packet shows the following structure:

- Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 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)
- Internet Protocol Version 4, Src: 10.76.5.201 (10.76.5.201), Dst: 10.76.5.255 (10.76.5.255)
- User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
- SMB Mailslot Protocol
- Microsoft Windows Browser Protocol

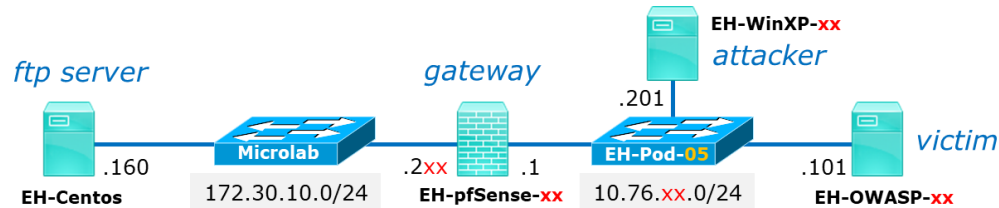
Note: If you see port 4444 traffic you have malware running from the previous lab. Revert WinXP to the Baseline snapshot.

1) Give yourself some more screen real estate:

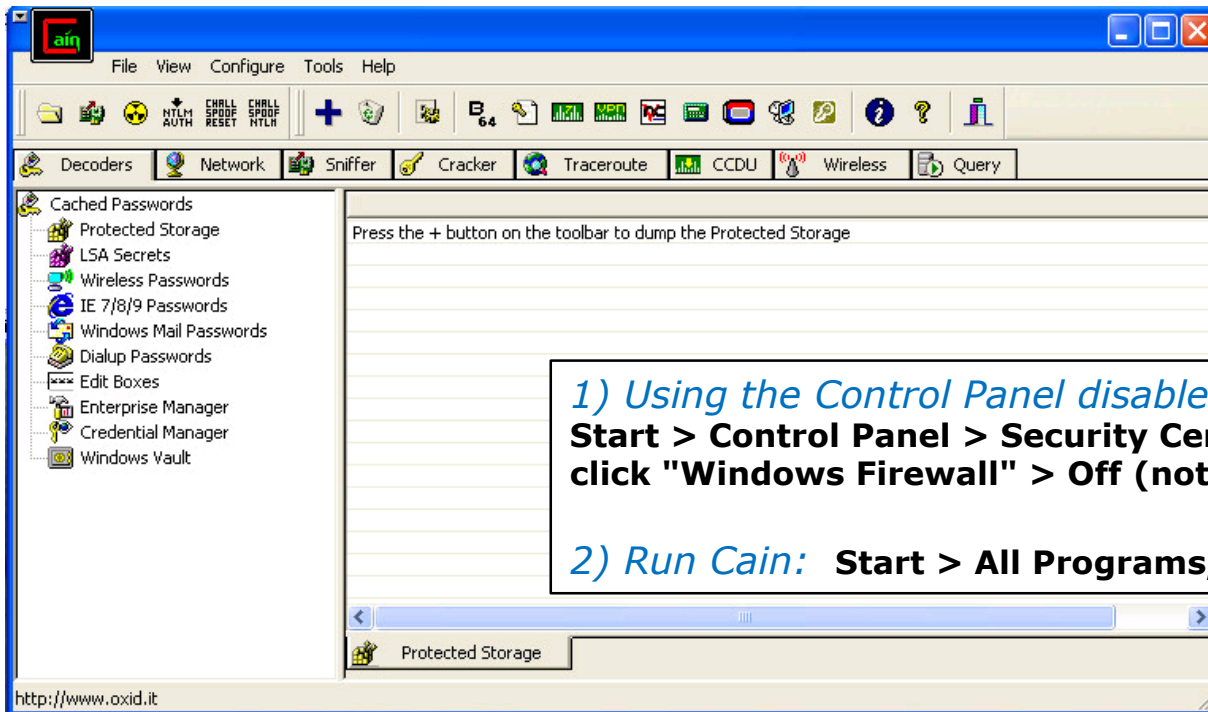
Right click on screen > select Properties > Settings Tab > slide Screen Resolution to 1024 by 768 pixels.

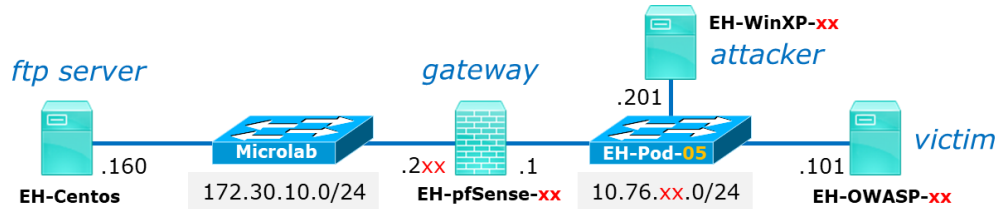
2) Run Wireshark and start a capture:

Start > All Programs > Wireshark > Click on Start (after the "green fin")
You can deselect Packet Bytes under the View menu for more room.



WinXP VM





WinXP VM

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.

3) Then click the Sniffer tab above.

4) 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

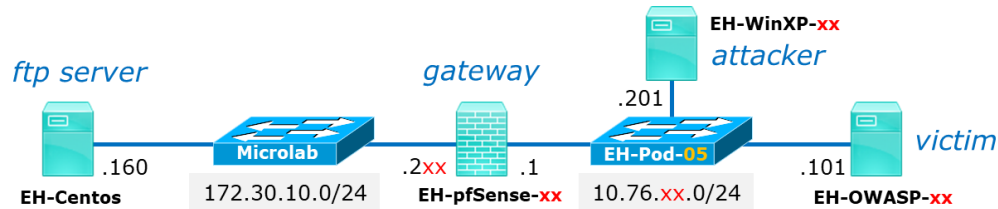
Current Network Adapter: \Device\NPF_{BAE2C689-7EC5-4795-8D47-E257A92330D2}

WARNING !!! Only ethernet adapters supported

Options:

- Start Sniffer on startup
- Don't use Promiscuous mode
- Start APR on startup

2) OK Cancel Apply Help



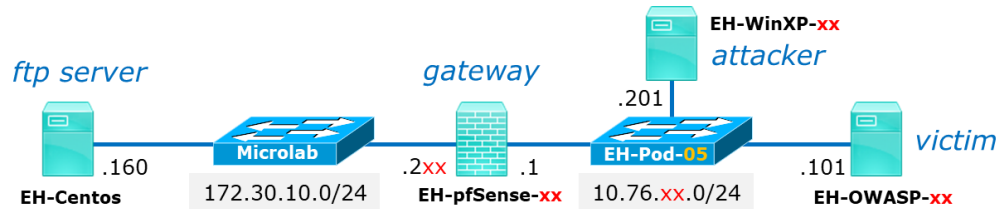
WinXP VM

The screenshot shows a WinXP VM interface with a "MAC Address Scanner" dialog box open. The dialog box has the following settings:

- Target:**
 - All hosts in my subnet
 - Range
- From:** 10 . 76 . 5 . 1
- To:** 10 . 76 . 5 . 254
- Promiscuous-Mode Scanner:**
 - ARP Test (Broadcast 31-bit)
 - ARP Test (Broadcast 16-bit)
 - ARP Test (Broadcast 8-bit)
 - ARP Test (Group bit)
 - ARP Test (Multicast group 0)
 - ARP Test (Multicast group 1)
 - ARP Test (Multicast group 3)
 - All Tests

The "OK" button is highlighted with a red box. In the background, a context menu is open over an empty table, with "Scan MAC Addresses" highlighted by a red box. A text box with blue text says: "Right-click on the empty table and select Scan MAC addresses".

IP address	MAC address	OUI fingerprint	Host n



WinXP VM

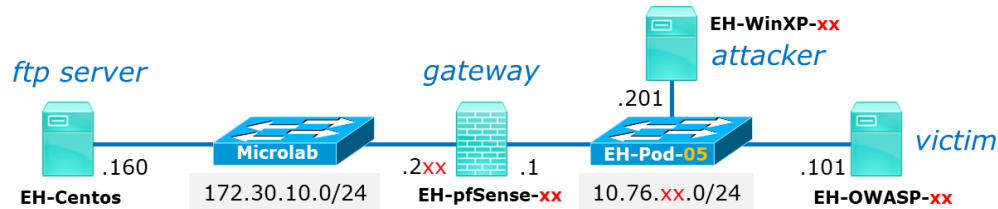
The screenshot shows a WinXP VM running a network tool. The interface includes a menu bar (File, View, Configure, Tools, Help), a toolbar with various icons, and a table of network data. A text box highlights the importance of noting MAC addresses for pfSense and OWASP VMs.

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%



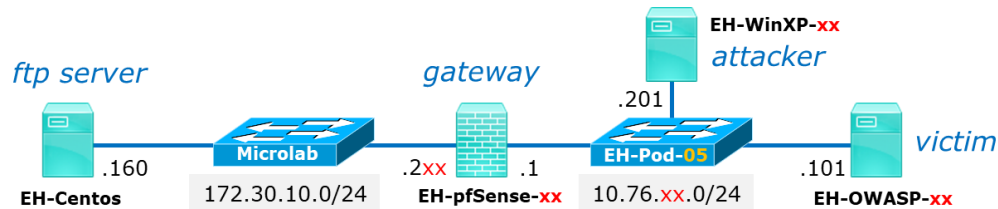
WinXP VM

The screenshot shows a WinXP VM interface with a network scanner tool and Wireshark. The scanner tool displays a list of IP addresses and MAC addresses. The IP address 10.76.5.150 and its corresponding MAC address 005056AFE6BD are highlighted with a red box. A text box below the scanner states: "The MAC addresses from the scan should show up as an ARP Response in Wireshark".

Wireshark is capturing traffic on the Local Area Connection. The packet list shows several ARP requests. The selected packet (Frame 204) is an ARP request with the following details:

- 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)

The packet details pane shows the source MAC address 00:50:56:af:e6:bd, which is highlighted with a red box in the packet list. The packet bytes pane shows the raw data of the ARP request.



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

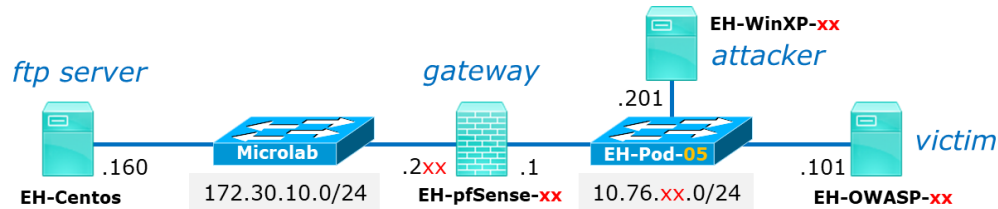
Filter: Expression... Clear Apply Save

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.



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)

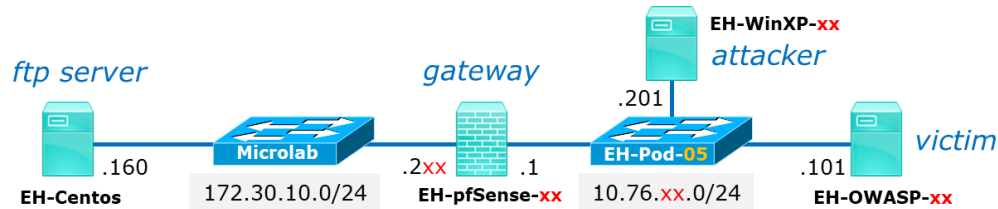
Click on the radioactive APR (ARP Poison Routing) tab at the bottom.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address:

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 0%



WinXP VM

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

APR

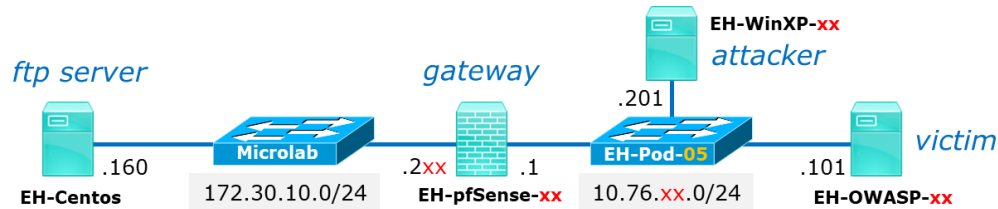
- APR-Cert
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address:

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 0%



WinXP VM

The screenshot shows the WinXP VM interface with the 'New ARP Poison Routing' dialog box open. The dialog box contains a warning message and two tables of IP addresses and MAC addresses. Red boxes highlight the selected IP addresses in both tables.

WARNING !!!

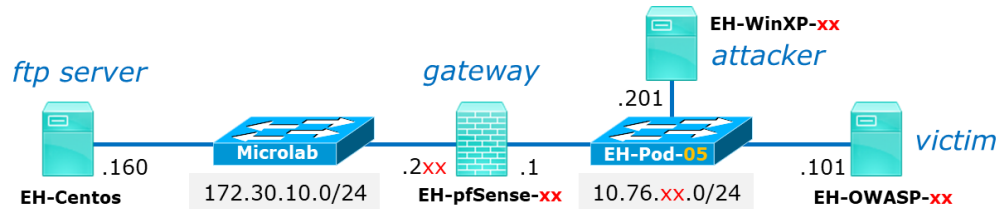
ARP enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set ARP between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname	IP address	MAC	Hostname
10.76.5.1	005056AFF2C3		10.76.5.150	005056AFE6BD	
10.76.5.101	005056AF63BB		10.76.5.101	005056AF63BB	
10.76.5.150	005056AFE6BD				

1) Select your pfSense VM on the left.

2) The select your OWASP VM on the right.

3) Then click OK.



WinXP VM

The screenshot shows the WinXP VM interface with the APR tool. The APR button is highlighted with a red box. The APR tool window shows a table with columns for Status, IP address, MAC address, Packets, and MAC address. The IP address 10.76.5.1 and the IP address 10.76.5.101 are highlighted with red boxes. A text box contains instructions for confirming the addresses and starting the poisoning process.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.76.5.1	005056AFF2C3			005056AF63BB	10.76.5.101

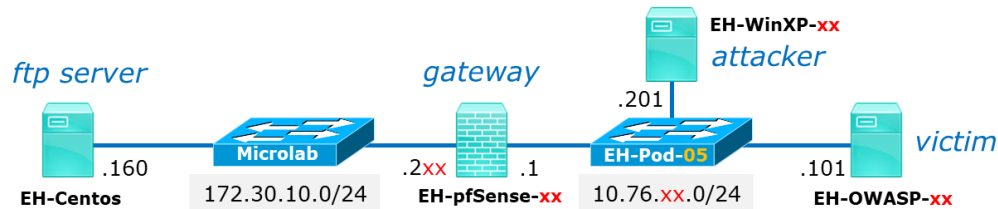
1) Confirm the two addresses above are your pfSense and OWASP VMs

2) Then click the APR button to start poisoning. The Status will change from "Idle" to "Poisoning".

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 0%



OWASP VM

```

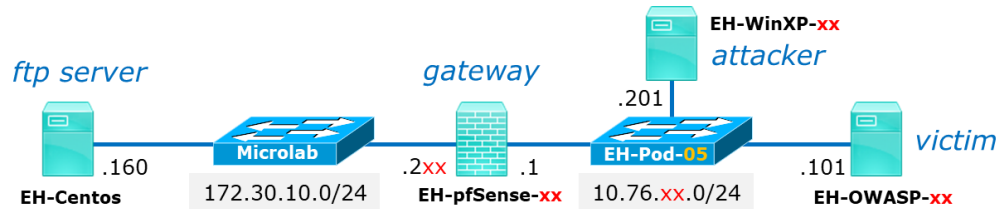
root@owaspbwa:~# ping -c1 172.30.10.160
PING 172.30.10.160 (172.30.10.160) 56(84) bytes of data.
64 bytes from 172.30.10.160: icmp_seq=1 ttl=63 time=4.05 ms

--- 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 -c1 172.30.10.160

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!



WinXP VM

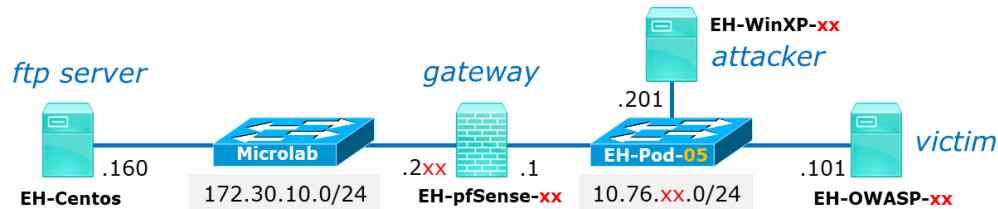
The WinXP VM is able to intercept and monitor the traffic between the OWASP and pfSense VMs!

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.76.5.1	005056AFF2C3	0	0	005056AF63BB	10.76.5.101
Full-routing	10.76.5.101	005056AF63BB	2	2	005056AFF2C3	172.30.5.101
Full-routing	10.76.5.101	005056AF63BB	1	1	005056AFF2C3	172.30.10.160

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 0%



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:~# _

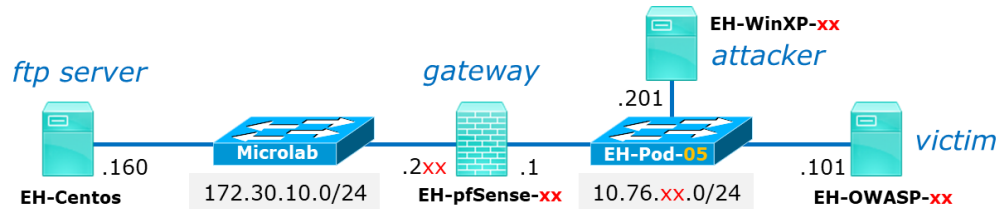
```

*Repeat downloading
a file from the ftp
server.*

```

ftp 172.30.10.160
anonymous
NotSoSecret
passive
ls
cd pub
ls
get admonition
exit

```



WinXP VM

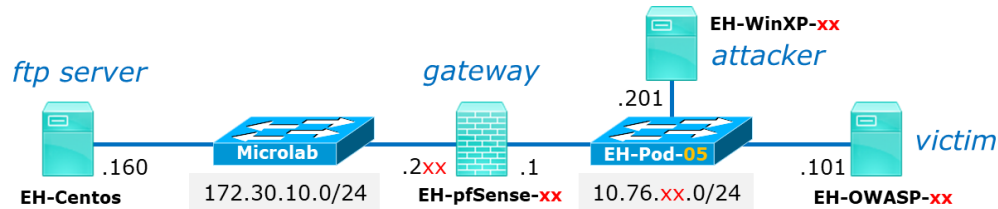
The screenshot shows the WinXP VM interface with the following elements:

- Toolbar:** The "Passwords" tab is highlighted with a red box.
- Left Sidebar:** The "FTP (1)" tab is highlighted with a red box.
- Main Window:** A table showing captured FTP credentials.

Timestamp	FTP server	Client	Username	Password
05/09/2016 - 14:33:58	172.30.10.160	10.76.5.101	anonymous	NotSoSecret

Click the password tab at the bottom and FTP on the left to show captured FTP usernames and passwords.

Lost packets: 0%



WinXP VM

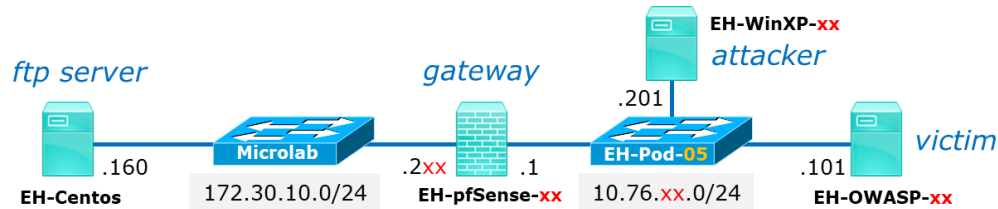
The screenshot shows the 'Follow TCP Stream' window in Wireshark, displaying the following FTP session transcript:

```

220 welcome to CIS 76 FTP service.
USER anonymous
331 Please specify the password.
PASS NotSoSecret
230 Login successful.
SYST
215 UNIX Type: L8
CWD pub
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PORT 10,76,5,101,147,191
500 Illegal PORT command.
PASV
227 Entering Passive Mode (172,30,10,160,20,147).
RETR admonition
150 Opening BINARY mode data connection for admonition (205 bytes).
226 Transfer complete.
QUIT
221 Goodbye.
  
```

Below the transcript, there are buttons for 'Find', 'Save As', 'Print', and radio buttons for 'ASCII', 'EBCDIC', 'Hex Dump', 'C Arrays', and 'Raw' (which is selected). At the bottom, there are 'Filter Out This Stream' and 'Close' buttons.

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



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
484	6335.48347	vmware_af:16:3a	vmware_af:12:c3	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
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	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
496	6515.48383	vmware_af:16:3a	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
497	6515.48392	vmware_af:16:3a	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
498	6545.48383	vmware_af:16:3a	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
499	6545.48412	vmware_af:16:3a	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56:af:16:3a
500	6575.48353	vmware_af:16:3a	vmware_af:16:3a	ARP	42	10.76.5.101 is at 00:50:56: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/>