

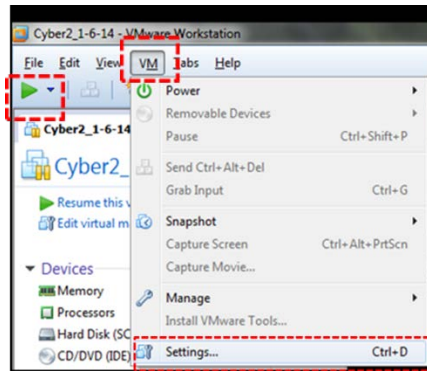
SY310 - Lab #6 Man-in-the-Middle Attack

Part 1: Set up

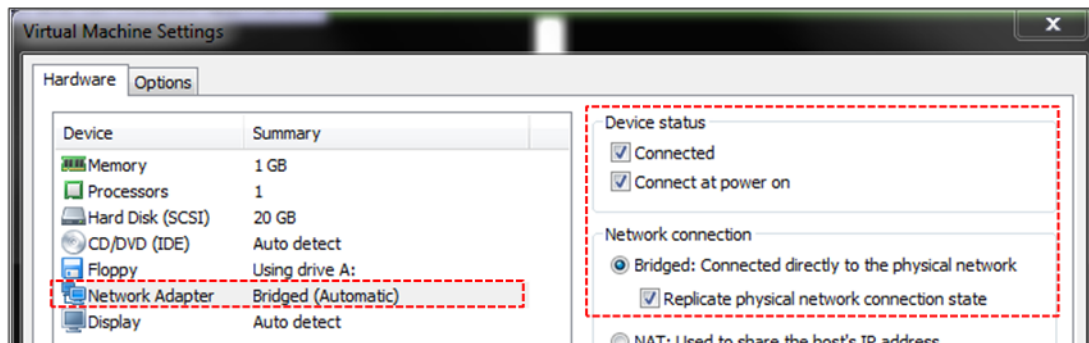
It is interesting to *hear* the theory behind a Man-In-The-Middle attack, but it is better to *experience* it yourself.

Equipment required:

- ☐ Your issued Laptop.
 - o In your laptop wireless utility, **connect** to the network named **Cyber2-XX** where XX is the room number of the lab you are currently in (i.e. Cyber2-64 if you are in Rickover 64).
- ☐ The **Lab #6 network diagram** from course website and associated **Lab #6 instructions**
 - o **Separate** the answer sheet and have it ready to fill in.
- ☐ VMware Workstation
 - o **Power on** your VM, then **click VM** and **Settings**.



- o **Select Network Adapter** and **ensure** that **Connected**, **Connected at power on**, and **Bridged: Connected directly to the physical network**, and **Replicate physical network connection state** are **selected** or **checked**, then **click OK**.



- o **Open** a terminal in your VM and **execute** the command

```
sudo dhclient
```

Once it finishes, **execute** the command

```
ifconfig
```

Your screen should look similar to Figure 1 on page 2. Interface eth1 should be assigned an IP address of 192.168.XX.YYY, where XX is your classroom number. **If not**, *notify your instructor or lab technician*.

```

midshipman@EC310:~$ ifconfig
eth1: Link encap:Ethernet HWaddr 00:0C:29:52:14:D3
      inet addr:192.168.65.110 Bcast:192.168.65.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2825 errors:82 dropped:0 overruns:0 frame:0
      TX packets:2318 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1069573 (1.0 MiB) TX bytes:271486 (265.1 KiB)
      Interrupt:16 Base address:0x2024

lo:    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:1512 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1512 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:75600 (73.8 KiB) TX bytes:75600 (73.8 KiB)

midshipman@EC310:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         0.0.0.0        0.0.0.0         U         0      0      0 eth1
192.168.65.0    0.0.0.0        255.255.255.0   U         0      0      0 eth1
169.254.0.0     0.0.0.0        255.255.0.0     U        1000    0      0 eth1
0.0.0.0         192.168.65.10 0.0.0.0         UG        0      0      0 eth1

```

Figure 1 – ifconfig executed after initial lab setup.

Part 2: The Attack

The evil instructor wants to deny you access to www.ec310.edu. He has found the IP address for the website and understands that routers work using the longest mask matching principle. He also understands the default assumption between routers in the routing algorithms they use to construct their routing tables.

Let's start by verifying the correct website.

- ☐ **use** `traceroute -n` to identify the route to www.ec310.edu.
- ☐ **access** www.ec310.edu using Firefox to verify the name of the site administrator


Question 1: What is the assumption the evil instructor understands about routers in the routing algorithms they use?

STOP! Observe Demonstration #1

- ☐ When directed, **label** part m) of your network diagram.
- ☐ When directed, **use** `traceroute` to identify the new route to www.ec310.edu.
- ☐ When directed, **access** www.ec310.edu using Firefox. If already open, **refresh** your browser using either method below.

Ctrl + Shift + R

or

Shift + 

Question 2: After the evil instructor injected false routing information into the network, where did your traffic destined for www.ec310.edu go? Was the website still available?

Question 3: What did your evil instructor attack in order to deny you access to www.ec310.edu? Pick one.

- a) your virtual machine b) the Webserver c) a script running on the webpage d) the network


Question 4: What pillar of information assurance did this affect?

STOP! Observe Demonstration #2

- ☐ When directed, **refresh** www.ec310.edu using either method below.

Ctrl + Shift + R

or

Shift + 

- ☐ When directed, **use** `traceroute` identify the new route to www.ec310.edu.

Question 5: Who maintains the website at www.ec310.edu?


It may not seem very significant to have your homework interrupted or altered by a Man-In-The-Middle attack, but what if the website you were visiting was more important? For example, what if you needed to check on the status of your second class loan with your bank?

STOP! Observe Demonstration #3


- ☐ When directed, **refresh** www.ec310.edu using either method below.

Ctrl + Shift + R

or

Shift + 

Question 6: What fake website did your evil instructor misguide you to and what pillar of information assurance did this affect?

Recall from SY110, that the X.509 certificate system provides a mechanism to establish a secure connection with a website. It provides assurance between a website's domain name and their public key. That is, when the lock closes in our browser ( <https://>) and we establish a secure connection with a website, we know the public key that was used to transfer a symmetric encryption key was done using the public key which belongs to a particular domain name.

Question 7: If the X.509 certificate system only offers proof that a public key belongs to a specific domain name, whose responsibility is it to verify if a website is authentic?

Part 3: The Fix #1: Easy as 123456

The Open Shortest Path First (OSPF) protocol has two authentication mechanism built in to protect against the injection of false routing information. The first is a simple *plaintext-password* added to all Link State Packets (LSPs) so each router can authenticate the information it is receiving. However, by including the password in plaintext with each LSP, you can easily discover the 'secret' password by observing the LSPs with Wireshark.

Much more interesting is the second method for authentication in OSPF, *an MD5-hash of the shared secret key*. Recall from SY110, that hashing is a 'one-way' encryption technique that produces the same message digest (i.e., encrypted output) given the same input string. Additionally, while it is easy to hash the input string, it is very hard to identify the input string given only the message digest (remember the Rubik's cube?). In OSPF, routers can send the hash of the shared secret key along with their LSP to authenticate themselves with other routers. Of course, all routers must know the shared secret key in advance. This may seem trivial at first, but consider the number of routers at a place like Google or Amazon Web Services where there are literally thousands of routers.


Question 8: We have all been told to change our password regularly to increase security, but do you think it is easy to change the shared secret key in every router at a place like Google or Amazon (or even the Naval Academy)? Do you think there may be an incentive for network administrators to make the shared secret key something easy to remember?

STOP! Observe Demonstration #4

- ☐ When directed, **refresh** www.ec310.edu using either method below.

Ctrl + Shift + R

or

Shift + 

Question 9: What are some important things to consider when choosing a password?

Part 4: The Fix #2: Passive Interfaces

Consider the topology of your network diagram from a security perspective.

Question 10: Is there any reason Router B should listen to routing information being sent over interface eth2?

Most implementations of OSPF allow for creation of *passive interfaces*. Just like when your roommate starts getting on your nerves and you tune him or her out by putting your headphones on, routers can do the same thing. Once a network administrator sets up a passive interface on a router, the router will ignore all routing information being sent over that

interface. However, this requires network administrators to make smart decisions when setting up the topology of their networks and configuring their routers.

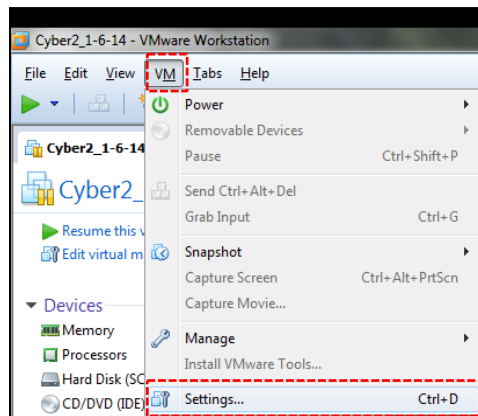
STOP! Observe Demonstration #5

Question 11: How many OSPF Hello packets did your instructor receive once the passive interface was enabled?

Question 12: As a user who do you trust by default for the safe and effective administration of your network? Do you have the ability to control the security of the network on your own?

Part 5: Clean Up

- VMware Workstation
 - In the VMware Workstation menu **click** *VM* and *Settings*.



- **Select** *Network Adapter* and **ensure** that *Connected*, *Connected at power on*, and *NAT: Used to share the host's IP address* are **not selected** or **unchecked**, then **click** *OK*.
- **Shutdown** your Cyber2 VM.

