<CHN>CHAPTER FIVE

<CHT>Networking-Based and Web Server Attacks

<COOT>Labs included in this chapter

* <COOH1>Lab 5.1 Getting Started with Kali Linux
* Lab 5.2 IP Spoofing with Hping3
* Lab 5.3 ARP Poisoning
* Lab 5.4 Man-in-the-Middle Attack

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats and Vulnerabilities 5.1, 5.2, 5.3, 5.4

# **<H1>Lab 5**.1 Getting Started with Kali Linux

**<H2>Objectives**

<TX1>One benefit of the open-source movement is the availability of high-quality, free tools for use by systems administrators, network engineers, and information security specialists. One of these tools is Kali Linux. At the time of this writing, Version 2016.2 is the most recent edition; this is the version used in the labs that follow. Kali Linux can be installed on a hard drive but can also be used as a VMware instance, meaning that a user can load Kali Linux into VMware without having any effect on an operating system that may be installed on the computer’s hard drive. Kali Linux contains a set of penetration-testing tools that run on a version of the Linux operating system. Penetration test teams are authorized to explore a network to see if they can find vulnerabilities that can be exploited. With this information, organizations can determine how effective their security controls are and how they can improve security.

<TX2>After completing this lab, you will be able to:

* <BL>Load and configure Kali Linux in a VMware share
* Configure network connectivity on Kali Linux

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Kali Linux ISO
* Windows 10 with VirtualBox installed

**<H2>Activity**

<FE1TX1>Estimated completion time: **20–30 minutes**

[BEGIN NOTE]

<TX1>The steps in this activity use Oracle VirtualBox. If you are using VMware or other virtual machine software, your steps may differ slightly.

[END NOTE]

<TX1>In this lab, you will run Kali Linux in a VirtualBox instance and configure network connectivity.

1. <NL\_FIRST>If you do not yet have a Kali Linux ISO, open your web browser, enter <URL>www.kali.org /downloads/</URL>, and click the Kali Linux 64 bit ISO button.

[BEGIN NOTE]

<FE4TX1> It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “Kali Linux ISO.” </FE4TX1>

[END NOTE]

1. <NL\_MID>Once you have downloaded the .ISO file, use VMware to load an instance of the ISO. You can use the File/New option and navigate to the ISO stored on your computer.

[BEGIN NOTE]

<FE4TX1> If your system does not boot to the CD, you may need to alter the device boot order in the BIOS setup utility. </FE4TX1>

[END NOTE]

1. Launch Oracle VM VirtualBox software and click **New**.
2. In the Name textbox use the name **Kali Linux.**
3. Type **Linux**.
4. Version is **Linux 2.6/3.x/4.x (xx-bit).**
5. Click **Next**.
6. Leave the Memory as the default amount and click **Next**.
7. Choose **Create a virtual hard disk now** and click **Create**.
8. Select **VDI (VirtualBox Disk Image)** and click **Next**.
9. Select **Dynamically allocated** and click **Next**.
10. Set the **File location as size** to at least 25GB and click **Create**.
11. Select the **Kali Linux** and click **Start**.
12. The first time you run the VM it will ask you for a start-up disk. Navigate to the Kali Linux ISO as shown in Figure 5-1. Click **Start**.

**[Insert Figure 5-1 Here]**

1. Choose the **Graphical** **install** option as shown in Figure 5-2.

**[Insert Figure 5-2 Here]**

1. Select all defaults. When you are prompted to configure the network, enter **Test.com** and click **Continue**. Enter **admin** for an administrator password and click **Continue**.
2. When asked to partition disks, select **Yes** and click **Continue**.
3. When asked to configure the package manager, select **No** and click **Continue**.
4. When asked to install the GRUB boot loader on a hard disk, select **No** and click **Continue**. Select all defaults until the installation restarts the operating system.
5. Enter **root** for the user name and **admin** for the password.
6. When you reach the Kali Linux desktop, check your network interface by clicking the Terminal button on the panel on the left of the desktop.
7. At the command prompt, type ifconfig and press Enter. If the value for inet addr (your IP address) is 127.0.0.1, as shown in Figure 5-3, you may need to start the networking service and/or you may need to configure your IP address manually. If you have an IP address on your classroom network, skip to Step 25.

**[Insert Figure 5-3 Here]**

1. To start the networking service, at the command prompt, type /etc/init.d/networking start and press Enter. Enter ifconfig at the command line and see if you have an IP address on your classroom network. If you do, proceed to Step 25. If not, proceed to Step 24.
2. At the VirtualBox menu choose Machine/Settings/Network. Verify that VirtualBox recognizes your network adapter either with a wired connection or a wireless connection. If it is not recognized, research the FAQ of VirtualBox to identify the issue.

[BEGIN NOTE]

<FE4TX1> In VirtualBox, you can access network adapter settings by right-clicking the icon on the lower right showing two computer monitors with wire between them, and choosing Settings. You can also click Connect if it is not already connected. </FE4TX1>

[END NOTE]

1. On Kali Linux, from the command prompt, type ping **www.yahoo.com** and press Enter.
2. Once you have verified connectivity between Kali Linux and the internet, spend some time exploring the Kali Linux interface.
3. Launch the ZenMap application from the Applications/Information Gathering menu.
4. In the Target window, enter your school web address and click **Scan**.
5. Once the scan completes, explore the output. Click the **Topology** tab and see how many jumps the software had to make before it found the web address.
6. On the Nmap Output tab check for any vulnerabilities.
7. Log off all systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization
* 3.2 Given a scenario, implement secure network architecture concepts.

**<H2>Review Questions**

1. <MULT>Which of the following were previous versions of Kali Linux? (Choose all that apply.)
   1. <MULTA>Red-Hat
   2. **BackTrack**
   3. Debian
   4. Ubuntu
2. <TF>An ISO file is a stand-alone operating system that can be installed on its own. True or **False**?
3. <MULT>Which of the following programs is a Kali Linux text editor?
   1. <MULTA>KRegExpEditor
   2. **OpenWrite**
   3. KTipop
   4. GVim
4. <FIB>When a Kali Linux system runs a ping command, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ bytes are sent in each ping packet.
   1. <FIBA>16
   2. 32
   3. **64**
   4. 128
5. <FIB>On Kali Linux, from a command prompt, you can display the contents of the /etc directory by typing \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and pressing Enter.
   1. <FIBA>/etc list
   2. list /etc
   3. /etc ls
   4. ls /etc

# <H1>Lab 5.2 IP Spoofing with Hping3

**<H2>Objectives**

<TX1>One of the first stages of an attack is probing the target network to determine what services are running, what operating systems are in use, and what resources are accessible. Attackers often craft packets to evade security devices such as firewalls and intrusion detection systems. Hping3 is a tool found on Kali Linux that allows users to probe remote systems, craft packets, and spoof IP addresses.

In this lab, you use hping3 on Kali Linux to probe a remote system and spoof an IP address.

<TX2>After completing this lab, you will be able to:

* <BL>Explain some of the packet crafting options in hping3
* Use hping3 to probe a remote system
* Use hping3 to spoof an IP address

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Kali Linux ISO
* Windows 10 with VirtualBox installed
* Windows 10 ISO
* Completion of Lab 4.1

**<H2>Activity**

<FE1TX1>Estimated completion time: **30–40 minutes**

In this lab, you learn about some of the packet-crafting options available in hping3. You use hping3 to send probe packets from Kali Linux to another computer. Then you perform IP spoofing with hping3 so that the packets sent from Kali Linux to another computer appear to have been sent by a different IP address.

[BEGIN NOTE]

<FE4TX1> You could experiment with packet-crafting options on many different types of networks. To ensure that communications can happen easily, this lab starts by setting up an internal network. However, if your instructor already has a different network setup for the lab, you can skip to step 5. </FE4TX1>

[END NOTE]

1. <NL\_FIRST>In the VirtualBox Manager, click the Win Server you created in Lab 4.1. Click **Settings**, then click **Network**. In the Network Adapter 1, select **Nat Network** as seen in Figure 5-4. Click **OK**.

[Insert Figure 5-4 here]

1. <NL\_MID>Repeat the steps for the Kali Linux VM you created in Lab 5.1.
2. Launch the *Windows Server VM*. Right click the **Start** button and select **Control Panel**. In the Control Panel, open **Network and Sharing**, click **Ethernet**, and then click **Properties**. Select **Internet Protocol Version 4** and click **Properties**.
3. For the IP Address enter **192.168.0.1** with a Subnet mask of **255.255.255.0**. See Figure 5-5. Click **OK** or **Close** until you are back to the Networking and Sharing center.

[Insert Figure 5-5 here]

1. Create a new Windows 10 VM with the ISO. Accept all the defaults.
2. Launch the Windows 10 VM. Right click the **Start** button and select **Control Panel**. Click the **View by** down arrow and select **Small icons**. Click **Network and Sharing Center**.
3. Click **Change adapters settings**.
4. Right-click **Ethernet** and select **Properties**.
5. Select **Internet Protocol Version 4** and then click **Properties**. In the IP Address enter **192.168.0.2** with a Subnet mask of **255.255.255.0**. Close all windows until you are at the Windows 10 desktop.
6. Launch the Kali Linux VM. Click the **Show application** icon on the menu bar on the left-hand side of the window and then click **Settings**.
7. Click **Network**. Click the **setting wheel** icon in the lower right of the dialog. Click **IPV4**. Enter the address as **192.168.0.3** and the subnet mask as **255.255.255.0**. See Figure 5-6.
8. Click **Apply**. Close all windows until you are at the desktop.

[Insert Figure 5-6 here]

1. On the Kali Linux Virtual machine, open a terminal window, type hping3 –help and then press Enter. Examine the syntax and options available in hping3. In the sections titled IP, ICMP, and UDP/TCP, you can see options that allow you to craft packets. For example, in the UDP/TCP section, you can use the –s option to specify a port address, the –R option to set a reset flag, or the –O option to set a faked TCP data offset.
2. In the Kali Linux VM, click the Terminal button. At the command prompt, type wireshark and press Enter.
3. Wireshark displays a warning about running the program as the root user (Linux administrator). Click OK.
4. Wireshark is a protocol analyzer; it captures incoming and outgoing packets at your network interface. Before you start capturing traffic, you will start an hping3 probe of Windows Server.
5. Open a terminal window. At the command prompt, type hping3 –s ipAddress and press Enter, replacing ipAddress with the IP address of Windows Server.

[BEGIN NOTE]

<FE4TX1> You can use the IP address of any other VM or computer connected to the private network. </FE4TX1>

[END NOTE]

1. In the Capture area of the Welcome to Wireshark window, click **eth0,** then click **Capture/Start**.
2. Allow the hping3 command to run while you return to the Wireshark Capture Interfaces window. Wait 10 seconds and then, from the Capture menu, click Stop.
3. On the terminal window, where hping3 is still running, press Ctrl+c to stop hping3.
4. Next, you again will use hping3 to send packets between Kali Linux and Windows Server, but this time you will spoof the source IP address so that it appears that the packets have come from Windows 10 VM, not from Kali Linux. At the terminal window, type hping3 –S ipAddressOfWindows 10 VM -a ipAddressOfServer. Although you don’t see the same output at the terminal window as you did in Step 17, the packets are being sent.
5. Start a capture from Wireshark. Click Continue without Saving, wait 10 seconds, and then stop the capture. It should appear that Windows 10 VM (192.168.0.2) is the source of the packets being sent to Windows Server (192.168.0.1), when, in reality, the source of the packets is Kali Linux (192.168.0.3).
6. Go to the command prompt in Kali Linux and press Ctrl+c to stop hping3.

[BEGIN NOTE]

<FE4TX1> You may want to keep Kali Linux running while you answer the Review Questions. </FE4TX1>

[END NOTE]

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

**<H2>Review Questions**

1. <ESQ>In Step 22 of this lab, you captured hping3 packets that were sent to Win Server from Kali Linux. However, unlike the capture discussed in Step 18, there were no response packets from Windows Server. Why not?

[Answer: *Kali Linux* is sending the response packets to *Windows* *Server* since it is *Windows Server*’s IP address that appears to be the source of the hping3 packets.]

1. <ESQ>When you click one of the spoofed frames in Wireshark from this lab and then, in the middle frame, expand the Ethernet II node, you see a destination and source address. What types of addresses are these, and at which layer of the Open Systems Interconnection model are they processed?

[Answer: MAC addresses; Data-Link layer]

1. <FIB>While examining the frame discussed in Question 2, you determine that Wireshark has identified the packet as abnormal. You discover this by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>clicking the frame, expanding the Transmission Control Protocol node in the middle frame, and seeing that the Flags item lists (RST)
   2. clicking the frame, expanding the Internet Protocol node in the middle frame, and seeing that the source IP address is that of Server
   3. **clicking the frame, expanding the Transmission Control Protocol node in the middle frame, and seeing that the Acknowledgement number field lists Broken TCP**
   4. clicking the frame, expanding the Transmission Control Protocol node in the middle frame, and seeing that the Version field lists 7
2. <MULT>Which of the following options in hping3 splits packets into fragments?
   1. <MULTA>–**f**
   2. –o
   3. –mtu
   4. –tos
3. <MULT>Which of the following options in hping3 sets the ACK flag?
   1. <MULTA>–**A**
   2. –M
   3. –K
   4. –k

# <H1>Lab 5.3 ARP Poisoning

**<H2>Objectives**

<TX1>ARP is a broadcast protocol that resolves IP addresses to MAC addresses. Because it relies on broadcasts, it can only resolve addresses within a broadcast domain. In other words, ARP works only within an IP segment since broadcasts are not transmitted by routers. Once a host resolves an IP address to a MAC address using ARP, it stores the resolution in its ARP cache for a period. That way it doesn’t need to keep broadcasting for the resolution because the resolution is already stored on the local machine. The problem with this is that an attacker can poison a target system’s ARP cache and fool the target into sending packets to the attacker while thinking the packets are going to the real destination. This can be the start of a man-in-the-middle attack, in which the attacker fools two hosts into thinking that they’re talking to each other directly when in fact the attacker is intercepting and then passing on the packets to their destinations. One limitation of this type of attack is that the attacker must have control of a host inside the network segment to interfere with the ARP broadcast process.

<TX2>After completing this lab, you will be able to:

* <BL>Discuss some of the capabilities of ettercap
* Use ettercap to perform ARP poisoning

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 With VirtualBox installed
* Windows Server 2016
* Completion of Lab 4.1
* Completion of Lab 5.1
* Completion of Lab 5.2

**<H2>Activity**

<FE1TX1>Estimated completion time: **40 minutes**

<TX1>In this lab, you monitor pings between two computers before and after the systems have been ARP poisoned.

1. <NL\_FIRST>Launch the Kali Linux VM and configure network connectivity as described in Lab 5.1. Click the Terminal button to open a terminal window. At the command prompt, type ifconfig and press Enter. Your results should be like what is shown in Figure 5-7. You will need this information to complete the table in Step 2.

**[Insert Figure 5-7 Here]**

1. <NL\_MID>Log on to *Windows Server* as the administrator. On both Server and *Windows 10 VM*, perform the following steps to complete and take note of the physical address and the IPV4 address. Click Start. In the Search box, type cmd and press Enter. At the command prompt, type ipconfig /all and press Enter.
2. On *Windows Server*, from a command prompt, type ping Windows10VMIPaddress (where *Win10*IPaddress is the Windows 10 IP address) and press Enter.
3. As a result of the ping command in Step 3, *Windows* Server and Windows 10 VM had to resolve each other’s IP address to a MAC address. This resolution can be found in each system’s ARP cache. On both *Windows* Server and Windows 10 VM, at the command prompt, type arp -a and press Enter. You are looking at the system’s ARP cache. Both have resolved the other’s IP address to a MAC address correctly.
4. Return to Kali Linux. If necessary, click the Terminal button, then type wireshark and press Enter. Configure Wireshark to start capturing traffic on your network interface, as you did in Lab 5.2.
5. On *Windows Server*, repeat the ping from Step 3 of this lab.
6. Return to Kali Linux and stop the Wireshark capture. You will not see evidence of the pings between Server and Windows 10 VM.
7. Click the Applications button, click Sniffing/Spoofing, then click ettercap-graphical. From the Sniff menu, click Unified sniffing and click OK on the ettercap Input window.
8. From the Hosts menu, click Scan for hosts. From the Hosts menu, click Hosts list. The addresses listed for *Windows Server* and *Windows 10 VM*’s should match the addresses you noted in Step 2.

[BEGIN NOTE]

<FE4TX1> This step may take a while to complete. If you do not have enough memory allocated to your VMware instance, your instance might freeze. Consider changing the setting to allocate as much memory as possible to the VMware instance before this step. </FE4TX1>

[END NOTE]

1. You will now begin ARP poisoning so that *Windows* Server and Windows 10 VM will be communicating with Kali Linux even though they think they are communicating with each other. Click the listing for *Windows Server* and click the Add to Target 1 button. Click the listing for Windows 10 VM and click the Add to Target 2 button. From the Start menu, select Start sniffing.
2. From the **Mitm** (man-in-the-middle) menu, click Arp poisoning. In the MITM Attack: ARP Poisoning window, select the **Sniff remote connections** checkbox and click OK. Notice the ARP poisoning victims listed in the lower frame of the ettercap window.
3. On *Windows Server*, perform another ping of Windows 10 VM. Check the ARP cache with the **arp** **-a** command on both *Windows Server* and Windows 10 VM. Notice that each lists the other’s MAC address as being the same as Kali Linux’s MAC address.
4. Repeat the ping, but this time, capture the result with Wireshark on Kali Linux. This time, there is evidence of the pings between *Windows Server* and Windows 10 VM.
5. Close the ettercap program. To repair the ARP cache on both *Windows Server* and Windows 10 VM, from a command prompt, type arp -d \* and press Enter. This clears the ARP cache; and now, since ettercap is no longer poisoning the ARP cache, when *Windows Server* and Windows 10 VM ping, they will broadcast ARP queries and obtain accurate resolutions.
6. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 1.3 Explain threat actor types and attributes.
* 1.4 Explain penetration testing concepts.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

**<H2>Review Questions**

1. <MULT>Which of the following attacks is available on ettercap? (Choose all that apply.)
   1. **<MULTA>ICMP redirection**
   2. Buffer overflow
   3. **Port stealing**
   4. **DHCP spoofing**
2. <ESQ>Why did you not see evidence of the pings between *Windows Server* and Windows 10 VM in Step 7 of this lab?

[Answer: Wireshark is capturing only traffic on Kali’s network interface. Directed frames between *Windows Server* and *Win* are not processed by Kali.]

1. <ESQ>Why did you see evidence of the pings between *Windows Server* and Windows 10 VM in Step 13 of this lab?

[Answer: Since *Windows Server* and *Windows 10 VM* think that Kali’s MAC address is the MAC address of the other Windows system, the ping responses are sent to Kali’s network interface.]

1. <TF>The ettercap log analyzer can handle only uncompressed logfiles. True or **False**?
2. <FIB>The configuration file for ettercap is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>/bin/cfg/etter.c
   2. **/etc/ettercap/etter.conf**
   3. /local/bin/help/ettercap.txt
   4. /etc/ettercap/conf

# <H1>Lab 5.4 Man-in-the-Middle Attack

**<H2>Objectives**

<TX1>A man-in-the-middle attack occurs when an attacker interposes himself between two victims. The attacker can simply capture the transmissions between the victims, or he can modify the communications. In either case, the victims are unaware that they are not directly communicating with their intended targets. Some man-in-the-middle techniques pose problems for the attacker. For example, in one approach, the attacker tries to anticipate the TCP sequence number that the potential victim is expecting from the system with which it is communicating. Because packets travel so quickly, this approach is not easy.

<TX2>ARP poisoning is a much easier way to get a victim to communicate with an attacker unknowingly, but it has the disadvantage of requiring local network access. On a typical Windows operating system, dynamic IP to MAC address resolutions are stored temporarily in the local ARP cache for two minutes unless the resolution is used a second time, in which case the resolution remains in the ARP cache for 10 minutes. ARP resolutions can be statically created, and these will remain active until the system is rebooted. Some administrators of small networks create login scripts that populate the ARP cache with static entries of local network ARP resolutions. This not only helps control the information collected in the ARP cache but also cuts down on network broadcasts.

<TX2>After completing this lab, you will be able to:

* <BL>Explain how a man-in-the-middle attack can be performed using ARP poisoning
* Use ettercap to perform a man-in-the-middle attack

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Completion of Lab 4.1
* Windows 10 with VirtualBox installed
* Kali Linux VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **10 minutes**

<TX1>In this lab, you use ettercap to perform a man-in-the-middle attack. Then, you intercept and transmit a victim’s attempts to access webpages.

1. <NL\_FIRST>Log on to *Windows Server* as administrator. Open your web browser, access any website to verify that you have Internet connectivity, and then close your web browser.
2. <NL\_MID>Launch the VMware instance of Kali Linux, open a terminal window, and ping *Windows Server* to verify connectivity. If the ping is not successful, then troubleshoot the connectivity.

[BEGIN NOTE]

<FE4TX1> Making both VMs on a NAT network resolves this issue most of the time. </FE4TX1>

[END NOTE]

1. Click the Applications button, click Kali Linux, click Sniffing/Spoofing, click Network Sniffers, and then click ettercap-graphical. From the **Sniff** menu, click Unified sniffing and click OK on the ettercap Input window.
2. From the **Hosts** menu, click Scan for hosts. From the **Host**s menu, click Hosts list.
3. Select the Hosts list entry that represents the router (default gateway) as identified by your instructor. Click Add to Target 1. Select the entry that represents *Windows Server* and click Add to Target 2.
4. From the **Start** menu, click Start sniffing.
5. From the **Mitm** menu, click Arp poisoning. In the MITM Attack: ARP Poisoning window, select the Sniff remote connections checkbox and click OK.
6. From the **Plugins** menu, click Manage the plugins. Scroll down and double-click the plugin named remote\_browser.
7. On *Windows Server*, open your web browser. In the address window, type <URL>www.google.com</URL> and press Enter. The website appears. Notice what happens in the lower frame of the ettercap window.
8. Close ettercap.
9. On *Windows Server*, enter <URL>www.yahoo.com</URL> in your browser’s address window and press Enter. Notice that the website does not appear.
10. Open a command prompt, type arp -d \* and then press Enter.
11. Return to your web browser and enter <URL>www.yahoo.com</URL> in your browser’s address window, and then press Enter. Notice that the website now appears.
12. You may want to leave your systems running and use the *arp* command and Wireshark as you answer the Review Questions.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 1.5 Explain Vulnerability scanning concepts.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

**<H2>Review Questions**

1. <ESQ>Why did the website not appear in Step 11 of this lab? Please be specific.

[Answer: The ARP poisoning performed in Steps 3–8 altered *Windows Server*’s ARP cache so that Kali’s MAC address was listed as belonging to the router. Even after the attack was terminated, the false MAC resolution remains in the victim’s ARP cache for at least two minutes. When *Windows Server* tried to access the Web, it sent the request to Kali instead of to the router, but because Kali was no longer performing the man-in-the-middle attack and does not function as a router, the request could not leave the local network to reach the Internet.]

1. <ESQ>Why did the website appear in Step 13 of this lab? Please be specific.

[Answer: The arp –d \* command cleared *Windows Server*’sARP cache. Then, when *Windows Server* attempted to access the Internet, it had to send an ARP broadcast in order to resolve the default gateway’s IP address to MAC address because there was no listing for the default gateway in its ARP cache. Without interference from Kali, *Windows Server* was able to resolve the default gateway’s address accurately, and the default gateway provided access to the Internet.]

1. <FIB>During the man-in-the-middle attack in this lab, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. **<FIBA>an analysis of the network layer headers would indicate that Server was communicating directly with the Internet**
   2. **an analysis of the data-link layer headers would indicate that Server was communicating directly with Kali Linux**
   3. an analysis of the network layer headers would indicate that Server was communicating directly with Kali Linux
   4. an analysis of the data-link layer headers would indicate that Server was communicating directly with the Internet
2. <MULT>Which of the following attacks is supported by ettercap? (Choose all that apply.)
   1. <MULTA>SQL injection
   2. **DNS spoofing**
   3. **DOS attack**
   4. Zero-day attack
3. <MULT>Which of the following actions could limit ARP poisoning as performed in this lab?
   1. <MULTA>Static IP addressing
   2. Dynamic IP addressing
   3. **Static ARP tables**
   4. Dynamic ARP tables