<CHN>CHAPTER EIGHT

<CHT>WIRELESS NETWORK SECURITY

<COOT>Labs included in this chapter

* <COOH1>Lab 8.1 Research a SOHO Wireless Router/Access Point
* Lab 8.2 Installing and Configuring a Wireless Adapter
* Lab 8.3 Wireless Communication Policy and Standards
* Lab 8.4 Configuring Wireless Security
* Lab 8.5 Exploring Network Ports with Sparta

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 8.5

Techniques and Tools 8.1, 8.2, 8.3, 8.4, 8.5

Architecture and Design 8.1, 8.2, 8.3, 8.4

Identity and Access Management 8.3

Cryptography and PKI 8.1, 8.4

# <H1>Lab 8.1 Research a SOHO Wireless Router/Access Point

**<H2>Objectives**

<TX1>Wireless local area networks (WLANs) are so common today that, for less than $100, technically unsophisticated users can purchase a wireless router and share their Internet connections with other computers in their homes or offices. SOHO (small office/home office) networks are so common in residential neighborhoods and office buildings that it now takes some trial and error to find a radio frequency that does not suffer from interference from neighboring WLANs or microwave ovens and wireless telephones.

<TX2>The security of data transmitted over WLANs has not been addressed satisfactorily. The vulnerabilities in WEP (Wired Equivalent Privacy) are well documented. Although WEP can be cracked in fewer than 10 minutes, WEP WLANs—and completely unprotected WLANs—are still surprisingly common in locations where undetected proximity, a prerequisite for cracking, is easy to attain. Wi-Fi Protected Access (WPA) and its upgrade, WPA2, are much more secure than WEP; however, there are still ways to attack an improperly configured WPA2 WLAN.

<TX2>Most wireless devices connect to a wired network. Ad hoc mode wireless networks—direct connections between wireless stations, without the inclusion of wired systems—are occasionally used, but access to resources on the Internet and on business networks almost always requires that an infrastructure mode network be used. In infrastructure mode, wireless stations communicate through a system connected to the wired network called an access point. An access point, like wireless stations, has an antenna and a wireless transceiver; however, it also has a wired interface to the company network.

<TX2>In a SOHO network, the access point fulfills a number of other responsibilities and is usually not even called an access point. The most common term is wireless router. These devices typically act as an access point for wireless stations, a switch where wired computers can be connected, a gateway to another network (typically the Internet), a network address translation device (NAT) to allow internal clients to use nonpublic IP addresses, a router to direct traffic to and from the WLAN, a Dynamic Host Configuration Protocol (DHCP) server to assign internal clients IP addresses, a Domain Name System (DNS) server to resolve fully qualified domain names to IP addresses, and a firewall to filter traffic coming into and out of the internal network.

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

* <BL>Compare WEP, WPA, and WPA2 encryption
* Analyze the importance of a wireless access point
* Explain the main security features of a SOHO wireless router

**<H2>Materials Required**

This lab requires the following:

* <BL>Windows 10 computer with internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **25 minutes**

<TX1>In this lab, you research a Wireless-N Router, and examine some of its security features.

1. <NL\_FIRST>Open a web browser and navigate to <URL><http://www.amazon.com></URL>.
2. <NL\_MID>In the search bar, type **wireless N router** and press **Enter**.
3. Browse the top three choices. What brands are they? What are some of the features they offer?
4. Do they offer WPA, WPA2, or WEP encryption? Do they offer another type of encryption?
5. Do they support IPv6? Do the routers have EAP?
6. Fill in the following table with information about three different routers. Note three security features for each router. Try to find security features that are not common to all the routers.

|  |  |  |
| --- | --- | --- |
| <TBCH>Router name | Speed | Security features</TBCH> |
|  |  |  |
|  |  |  |
|  |  |  |

<TBN>Table 8-1 Router information

1. Search the Amazon site for **wireless access point**.
2. How do wireless access points differ from wireless routers?
3. Fill in the following table with information about three wireless access points.

|  |  |  |  |
| --- | --- | --- | --- |
|  | <TBCH>Wireless Access Point 1 | Wireless Access Point 2 | Wireless Access Point 3</TBCH> |
| <TBTX1>Name |  |  |  |
| Brand |  |  |  |
| SSID? |  |  |  |
| MAC filtering? |  |  |  |
| Signal strength range |  |  |  |
| Band selection/width |  |  |  |
| Antenna types and placements |  |  |  |
| Fat or thin? |  |  |  |
| Controller-based or standalone? |  |  |  |

<TBN>Table 8-2 Wireless Access Point information

1. Open a new tab in your web browser, navigate to <URL>[**www.howtogeek.com**](http://www.howtogeek.com)**</URL>**,and use the Search feature to find the article named **The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords**.
2. What are some of the characteristics of the three different encryption algorithms? Which one is preferred? Name some weaknesses of the encryption algorithms?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Install and configure network components, both hardware- and software-based, to support organizational security.
* 3.2 Given a scenario, implement secure network architecture concepts.
* 6.3 Given a scenario, install and configure wireless security settings.

**<H2>Review Questions**

1. <MULT>Which of the following encryption protocols is most widely used?
   1. <MULTA>WEP
   2. **WPA**
   3. WPA2
   4. Wi-Fi
2. <MULT>Which encryption algorithm does WPA2 utilize?
   1. <MULTA>RSA 16
   2. RSA 32
   3. **AES**
   4. Two Factor authentication.
3. <MULT>TKIP stands for?
   1. **<MULTA>Temporal Key Integrity Protocol**
   2. Temporal Key Internet Protocol
   3. True Key Internet Protocol
   4. True Key Integrity Protocol
4. <FIB>WPA2 complies with the IEEE wireless standard \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>802.11b
   2. 802.11g
   3. 802.11i
   4. **802.11n**
5. <TF>Wireless access points contain their own encryption protocols? True or **False**?

# <H1>Lab 8.2 Installing and Configuring a Wireless Adapter

**<H2>Objectives**

<TX1>Although new portable devices generally have built-in wireless functionality, many desktop computers do not come with a wireless network adapter. In this lab, you install a USB wireless network adapter in Windows 10 VM and then use the wireless adapter to connect to the wireless router so that you can access the Windows Server on its wired network segment.

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

* <BL>Install the software and hardware elements of a USB wireless adapter
* Configure the D-Link wireless client software
* Connect to a wired network from a wireless station
* Configure SSID broadcasting and MAC filtering on a wireless router

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016 with Java-enabled web browser
* Linksys WRT400N Simultaneous Dual-Band Wireless-N Router
* Cat 5 straight-through cable
* Windows 10 VM
* D-Link DWA-160 Dual-Band N wireless USB adapter
* The successful completion of Lab 8.1

[BEGIN NOTE]

<B1TX1>An alternate wireless adapter may be used; however, the configuration directions in this lab may not then be applicable.

[END NOTE]

**<H2>Activity**

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

<TX1>In this lab, you install and configure a USB wireless adapter on Windows 10 VM, connect to Windows Server on its wired network segment, and configure increased security on the wireless router.

1. <NL\_FIRST>Log on to Windows 10 VM with an administrative account.
2. <NL\_MID>Right-click Start, click Device Manager, and click the expand arrow to the left of Network adapters. Disable any network adapters by right-clicking them and selecting Disable. Close the Computer Management window.
3. If your computer has a CD-ROM drive, insert the D-Link DWA-160 Dual-Band N wireless USB adapter software CD in the CD-ROM drive. The following steps presume you are using a CD-ROM. If your computer does not have a CD-ROM drive, then download and install the drivers from the Internet.
4. If the program does not start automatically or if you downloaded the drivers from the Internet, double-click the executable file either on the CD or from the download. Follow the default installation steps.
5. Plug the USB adapter into a USB port when instructed to do so, and then click Next. At the Get Connected! window, select Manually connect to a wireless network and click Next.
6. Type Windows Server in the Wireless Network Name (SSID) box and click Next. Verify that your wireless router has been recognized. Use your mouse to select your Windows Server network and click Next. On the Set Security! window, type Pa$$word in the WPA/WPA2-Personal Encryption Key box and press Next. In the Finished! window, click Next. In the Installation Complete window, click Finish.
7. In the D-Link window, deselect The D-Link Toolbar and then click Next. In the D-Link window, click Exit.
8. Notice that there is now a D-Link Wireless Connection Manager icon on your desktop. Double-click this icon to open the Wireless Connection Manager. Your results should be similar to Figure 8-1 (except you see the SSID Windows Server instead of the SSID Far).

**[Insert Figure 8-1 Here]**

1. Notice that MAC addresses are listed as well as signal intensity and channel. Right-click the SSID column header and notice that you can add the frequency and mode columns by selecting them.
2. Click MY WIRELESS NETWORKS and then click **Windows Server**. Notice the Profile Details section at the bottom of the window. On this screen, you can add profiles for other wireless networks to which you connect.
3. Close the Wireless Connection Manager window.
4. Although the WPA2-PSK security is very strong, you can also increase security marginally by disabling SSID broadcasting. As long as the stations have wireless profiles configured with the details of the connection (SSID, passphrase, security type), they will be able to connect to the network without receiving broadcasts of the SSID from the router. Log on to Windows Server, open Internet Explorer, and go to <URL>http://192.188.1.1</URL>. This is the default IP address for the router’s web management interface. Authenticate to the router with the username Admin and the password Pa$$word. Click the Wireless tab. In both the 5GHz and 2.4GHz Wireless Settings sections, at the SSID Broadcast item, click the radio button to the left of Disabled. Scroll to the bottom of the window, click Save Settings, and when the Settings are successful screen appears, click Continue.
5. Click the Wireless MAC Filter subtab. Click the radio button to the left of Enabled. In the Access restriction section, click the radio button to the left of Permit. On both Windows 10 VM and Windows Server, open a command prompt, type ipconfig/all, and press Enter. The physical address is the MAC address. Enter both these numbers as MAC 01 and MAC 02 in the MAC Address Filter List on the router’s web interface. Scroll to the bottom of the window, click Save Settings, and when the Settings are successful screen appears, click continue. You have now disabled SSID broadcasts and enabled MAC address filtering that will allow no computers other than Windows 10 VM and Windows Server to connect to your wireless router. Naturally, in a larger network, you would need to add all the systems in the network to the MAC Address Filter List—an administrative nightmare. Close your web browser.
6. If possible, have another student on a machine other than your Windows Server or Windows 10 VM try to connect to your network. Even though they may know your SSID and password as a result of reading this lab, they won’t be able to connect.
7. You may want to keep the systems open while you answer the Review Questions.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Install and configure network components, both hardware- and software-based, to support organizational security
* 2.3 Given a scenario, troubleshoot common security issues
* 2.6 Given a scenario, implement secure protocols
* 3.2 Given a scenario, implement secure network architecture concepts

**<H2>Review Questions**

1. <FIB>The Linksys Address Filter List restricts associations with the router based on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>Internet Protocol addresses
   2. **Media Access Control addresses**
   3. Network Basic Input/Output System names
   4. fully qualified domain names
2. <MULT>Which of the following statements regarding a wireless USB adapter is incorrect? (Choose all that apply.)
   1. **<MULTA>Because a wireless USB adapter is not integrated with the motherboard, it must have a static IP address.**
   2. **A wireless USB adapter must have its MAC address registered with an access point if it is used on a wireless station that has previously associated with the access point using an embedded wireless adapter.**
   3. **Wireless USB adapters are a security risk because if they are lost, the finder will have open access to the last encrypted WLAN with which the adapter associated.**
   4. **All wireless USB adapters should be scanned for viruses before each use.**
3. <MULT>Which of the following might create radio-frequency interference and disrupt transmissions for a station using an 802.11n adapter? (Choose all that apply.)
   1. <MULTA>A television with a cable connection
   2. **A station using an 802.11a adapter**
   3. **A station using an 802.11b adapter**
   4. **A microwave oven**
4. <MULT>You have just installed a new 802.11n wireless router in your home office. You have connected your cable modem to the router’s Internet port and connected two desktop computers to the router’s LAN ports. You accessed the router’s web-based utility through one of the desktop systems, verified that you have Internet access, and configured strong encryption. You disabled SSID broadcasting, enabled MAC filtering, and allowed your two laptop computers to access the router by entering their MAC address in the “allowed” list. When you try to access your router from either laptop, you are unsuccessful. From your laptops, you can “see” the WLANs of two of your neighbors, but you cannot “see” your own. One of your neighbors has not enabled security on his WLAN, and you are able to associate with his wireless router and access the Internet through your neighbor’s WLAN from either of your wireless laptops. What is the most likely reason that you are unable to connect to your own WLAN?
   1. **<MULTA>SSID broadcasting is disabled**.
   2. MAC filtering is enabled.
   3. WPA2-PSK (AES) does not support nonenterprise networks.
   4. Your router’s reception port has not been configured.
5. <MULT>After solving the problem with your WLAN that was described in question 4, you were able to access your own router and, through it, the Internet on both your laptops. After a week of your SOHO WLAN working perfectly, you are starting to have problems: your notebooks have started being “dropped” from the network. You can reconnect using the wireless client software, but it is only a matter of minutes before you are dropped again. Your workstations have not had the same problem and continue to work well. What action is most likely to solve your connectivity problems?
   1. <MULTA>Change the SSID.
   2. Change the router’s MAC address.
   3. Change the type of encryption used.
   4. **Change the wireless channel.**

# <H1>Lab 8.3 Wireless Communication Policy and Standards

**<H2>Objectives**

<TX1>An important part of network security is making sure you have implemented the proper security and maintenance policies. Knowing when the routers and switches should be maintained or replaced is essential to ensuring the network stays safe. Creating proper policies that allow for the maintenance of networks is also important. The network configuration and design should be well thought-out and reflect the policy guidelines.

<TX1>Other policies, such as wireless communication policies and wireless communication standards are also essential if your organization has a Wi-Fi network or if you plan to allow individuals to BYOD.

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

* <BL>Create a proper policy for wireless, routers, and switches
* Analyze a BYOD policy to determine its strengths and weaknesses
* Identify key components of a new security policy

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 computer with internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **40–50 minutes**

<TX1>In this activity, you will research three policies from the SANS website. You will analyze these templates and create a policy that could be implemented in any business. You will also read and analyze a published paper by SANS detailing their issues with BYOD policies.

[BEGIN NOTE]

<B1TX1>This lab does not include a separate set of Review Questions, because the questions are included in the following numbered steps.

[END NOTE]

1. <NL\_FIRST>Open a web browser, navigate to <URL>[**www.sans.org**](http://www.sans.org)**</URL>**, click **Resources**, and then click **Security Policy Project**. Click **Network Security**, and then download the following templates: Router and Switch Security Policy, Wireless Communication Policy, and Wireless Communication Standard.
2. <NL\_MID>Open and read the Router and Switch Security Policy template. Modify the information in the template to depict a company that matches the description provided by your instructor. Pay special attention to item 5 and how it will be implemented.
3. What is the purpose of the access control list referred to in the policy? Where should this list be kept?
4. Open and read the Wireless Communication Policy template. Modify the information in the template to depict a company that matches the description provided by your instructor. Pay special attention to the Lab Security Policy referred to in the policy. You also may want to download that template and read it.
5. What are the challenges of creating a wireless communications policy?
6. Open and read the Wireless Communication Standard template. Modify the information in the template to depict a company that matches the description provided by your instructor.
7. What is the difference between the Wireless Communication Policy and the Wireless Communication Standard? Which one would have a stronger influence on a company?
8. What are the similarities between the policy and the standard?
9. Return to your web browser, navigate to <URL>**www.sans.org</URL>**  and then use the Search feature to search for **Managing the Implementation of a BYOD Policy**.
10. Read the document. Do a brief Strength, Weakness, Opportunity, and Threat (SWOT) analysis of the paper and the policy. Make sure you discuss the issues with enforcing and maintenance of the BYOD policy.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues
* 2.5 Given a scenario, deploy mobile devices securely
* 3.2 Given a scenario, implement secure network architecture concepts
* 4.3 Given a scenario, implement identity and access management controls

# <H1>Lab 8.4 Configuring Wireless Security

**<H2>Objectives**

The history of the development of wireless security techniques is similar to the history of the development of digital systems in general: uncontrolled chaos becomes controlled chaos as a result of industry standardization. Eventually, a temporary period of stability arrives. However, as soon as the development of new technologies makes the relatively stable functionality of a system outdated, another cycle of innovation, implementation, and chaos ensues.

<TX2>Because digital technology is now a lucrative and competitive industry, hardware and software vendors often rush their products and technologies to market without careful testing and validation. Consumer-targeted wireless technologies were pushed to market before effective security systems were in place. WEP (Wired Equivalent Privacy), the first encryption and authentication scheme included in the 802.11 standard, was never intended to be uncrackable, but it turned out that WEP was much easier to crack than anticipated by its developers.

<TX2>TKIP (Temporal Key Integrity Protocol) was created to shore up WEP while the IEEE 802.11i committee could come up with a stronger security mechanism. The wait was too long for wireless vendors, however, and the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) and began marketing products advertised as being compliant with the expected 802.11i standards. Eventually, the 802.11i standard was ratified and the Wi-Fi Alliance released WPA2, which fully complies with the completed 802.11i.

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

* <BL>Configure security settings on an enterprise-class access point
* Configure security settings on a wireless station

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM
* Cisco Aironet 1200 access point
* Cat 5 straight-through cable
* D-Link DWA-160 Dual-Band N wireless USB adapter

[BEGIN NOTE]

<B1TX1>An alternate wireless adapter may be used; however, the configuration directions in this lab may not then be applicable.

[END NOTE]

**<H2>Activity**

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

<TX1>In this lab, you configure encryption and MAC filtering on an access point and then configure a wireless station to access the secured network.

1. <NL\_FIRST>Log on to the Windows Server as Administrator. Disable the firewall.
2. <NL\_MID>Open the **Network and Sharing Center**, click Change adapter settings, right-click Ethernet, click Properties, double-click Internet Protocol Version 4 (TCP/IPv4), and remove all current configurations. Set the IP address to 10.0.0.2 and the subnet mask to 255.0.0.0. Click OK twice, and then close the Network Connections and Network and Sharing Center windows.
3. Connect a Cat 5 straight-through cable to the Windows Server’s NIC and to the Ethernet port on the access point. Verify connectivity by typing from a command prompt the following: ping 10.0.0.1. Press Enter. This ping attempt should succeed. Normally, the Ethernet port of the access point would be connected to a switch to which computers, or other switches, would connect, making up the wired network. In this lab, the server represents the wired network.
4. Open Internet Explorer and go to <URL>http://10.0.0.1</URL>. You will encounter a log on screen. Type Cisco as the User name, type Cisco as the password, and click OK. If prompted, add the site to your Trusted Sites.
5. The access point’s web-based administration utility opens. Click Express Set-up in the left frame. Notice the available configurations in this frame. Click Express Security in the left frame. In the SSID box, type ServerAP and place a check mark in the box to the left of Broadcast SSID in Beacon (see Figure 8-2). Notice that no security is configured. Scroll down and click Apply.

**[Insert Figure 8-2 Here]**

1. Click Security in the left frame and then click Encryption Manager.
2. In the Encryption Modes section, select Cipher. In the Cipher drop-down box, select AES CCMP + TKIP + WEP 128 bit. (This stands for “Advanced Encryption Standard, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol + Temporal Key Integrity Protocol + Wired Equivalent Privacy.”)
3. Scroll down to the Global Properties section and, in the Broadcast Key Rotation Interval, select Enable Rotation with Interval and enter 10 in the box. In the WPA Group Key Update section, select Enable Group Key Update On Membership Termination. Click Apply, and in the Warning box, click OK.
4. In the left frame, click SSID Manager, and in the Current SSID List, click WindowsServerAP. Scroll down the Client Authenticated Key Management section, set Key Management to Optional, and select WPA. In the WPA Pre-shared Key box, enter Pa$$word. Scroll to the bottom of the page and click Apply.
5. Determine the MAC address of Windows 10 VM by accessing a command prompt on Windows 10 VM, typing ipconfig/all, and pressing Enter. The MAC address is the value labeled *Physical Address*. On Windows Server, in the left frame, click Advanced Security and verify that the Mac Address Authentication tab is selected. Scroll down to the Local MAC Address List and, in the New MAC Address box, enter the MAC address of Windows 10 VM.

Use the following format when entering the MAC address: HHHH.HHHH.HHHH (including the periods). Click Apply and click OK on the Warning box.

1. Log on to Windows 10 VM with an administrative account. Launch the D-Link Wireless Connection Manager.
2. Because security has been enabled on the access point, you will not be able to connect to the Windows Server network with the existing profile. Click My Wireless Networks. Click New. In the Profile Settings window, type WindowsServerAP in both the Profile Name and SSID boxes. Verify that Network Type is set to Infrastructure. In the Set Security Option section, click the radio button to the left of WPA/WPA2-Personal. In the Passphrase Settings, verify that the radio button to the left of Auto is selected and type Pa$$word in the Key box. Click OK. The connection should be successful. Verify connectivity by pinging Windows Server at 10.0.0.2.
3. On Windows Server, create a folder called C:\Wireless. Right-click the folder and click Share. Click the Share button. Add a file to the folder.
4. On Windows 10 VM, from a command prompt, type net use \*\\Windows Server \Wireless /user:administrator. If prompted, enter the password Pa$$word. Once the drive has been mapped, click Start, click Computer, open the network drive mapped to the Wireless shared folder, and copy the file inside it to your desktop.
5. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Install and configure network components, both hardware- and software-based, to support organizational security
* 2.3 Given a scenario, troubleshoot common security issues
* 2.6 Given a scenario, implement secure protocols
* 3.2 Given a scenario, implement secure network architecture concepts
* 6.2 Explain cryptography algorithms and their basic characteristics

**<H2>Review Questions**

1. <MULT>In Step 9 of this lab, you selected Enable Group Key Update On Membership Termination. How does this setting provide security?
   1. **<MULTA>The access point generates and distributes a new group key when any authenticated station disassociates from the access point.**
   2. The access point generates and distributes a new group key when the access point disassociates from another access point.
   3. The access point generates and distributes a new initialization vector key when a new station authenticates.
   4. The access point generates and distributes a new Message Integrity Check sequence to validate group keys when any authenticated station dissociates from the access point.
2. <MULT>Which of the following statements regarding access points is not correct?
   1. <MULTA>MAC filtering attempts to limit access to the WLAN based on physical addresses.
   2. An access point configured with WEP and TKIP has weaker security than an access point configured with WPA.
   3. **A wireless station configured with a WEP key that is identical to the access point’s WPA2 key will be able to authenticate to the access point.**
   4. As a wireless station moves farther away from an access point, transmission bandwidth decreases.
3. <MULT>Which of the following statements about MAC addresses is correct? (Choose all that apply.)
   1. <MULTA>A MAC address contains between 32 and 48 bits.
   2. The longer the MAC address, the more difficult it is to spoof.
   3. **A MAC address can be spoofed easily.**
   4. **MAC addresses are sent unencrypted during the process of association between a wireless station and an access point.**
4. <MULT>What information is available on a Windows 10 VM system when using the command *ipconfig /all*? (Choose all that apply.)
   1. **<MULTA>The host’s computer name**
   2. The SSID of any WLAN with which the host is associated
   3. **The host’s MAC address**
   4. **A description of the host’s wireless adapter**
5. <TF>The net use command is generally considered a secure command because the /user:username option supports encryption. True or **False**?

# <H1>Lab 8.5 Exploring Network Ports with Sparta

**<H2>Objectives**

<TX1>Kali Linux provides a stable environment for hacking and penetration testing. The tools included with Kali Linux range from password-cracking tools to networking mapping software. The Sparta software included with Kali offers the ability to do a robust port scan that can divulge important information about a network. Sparta works in conjunction with Hydra networking mapping software.

<TX1>If SPARTA scans a server with a faulty configuration, it may alert you to many vulnerabilities, which of course you should not attempt to take advantage of. Remember, the ability to use software like SPARTA comes with great responsibility. You should not try to access any server or information that you do not normally have permission to access.

<TX2>In this lab, you use Sparta to identify open ports.

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

* <BL>Configure Sparta for penetration testing
* Analyze the need for port hardening.

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 Machine with VirtualBox installed.
* Completion of Lab 5.1.

**<H2>Activity**

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

<TX1>In this lab, you configure the Sparta penetration testing software to do port scans.

1. <NL\_FIRST>Determine the IP address of your local college. Launch the command window and use the *ping* command to ping your college’s web address. Note your school’s IP address.
2. <NL\_MID>Launch the Kali Linux VM that you created in Lab 5.1.
3. Click **Applications**, click **Vulnerability Analysis**, and then select **Sparta**.
4. In the Hosts window, click the **IP Range** box, and type the IP address of your school with a range after it. (See Figure 8-3). Click **Add to scope**.

**[Insert Figure 8-3 Here]**

1. Wait for the scan to complete. This could take as long as 20 minutes. Take note of the ports and items detected by the scan. Figure 8-4 shows sample scan results. Yours will differ.

**[Insert Figure 8-4 Here]**

1. Click the nikto tabs near the top of the SPARTA window. Were any open ports or passwords found? If you find either or both you should report them to the network administrator for the IP address you are searching.
2. Explore the other tabs in the SPARTA window to learn more about SPARTA’s powerful features. Note that you can use the Brute tab to begin a brute force penetration attack against a specific IP address.
3. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.5 Explain vulnerability scanning concepts
* 1.6 Explain the impact associated with types of vulnerabilities
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

**<H2>Review Questions**

1. <MULT>The main IP address used for the Sparta software identifies which port first?
   1. <MULTA>SSH
   2. FTP
   3. HTTPS
   4. **TCP**
2. <MULT>Penetration testing is used for?
   1. **<MULTA>Device hardening**
   2. Port replication
   3. Port Blocking
   4. Web server setup
3. <MULT>Which port is basic HTTP access done through?
   1. <MULTA>223
   2. 128
   3. **80**
   4. 256
4. <TF>Using the Sparta software cannot find all open ports in the computer. **True** or False?
5. <TF>When using the Sparta software, you can only use the password or dictionary list that the software supplies when trying to crack passwords. True or **False**?