**<CHN>CHAPTER TEN**

<CHT>MOBILE DEVICE SECURITY

<COOT>Labs included in this chapter

* <COOH1>Lab 10.1 File Transfer Using Bluetooth
* Lab 10.2 Getting Bluetooth Info with Bluesnarfer
* Lab 10.3 Kali Linux Mobile Device Security Tools
* Lab 10.4 Physical Security
* Lab 10.5 BYOD Policies

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 10.2, 10.3

Technologies and Tools 10.1, 10.2, 10.3, 10.4, 10.5

Architecture and Design 10.3, 10.4

Risk Management 10.4, 10.5

# <H1>Lab 10.1 File Transfer Using Bluetooth

<H2>Objectives

<TX1>Bluetooth technology was created in 1994 as an alternate to RS-232 cabling. The technology uses radio waves transmitted over a short distance. Bluetooth is designed to pair two devices and allow data to be transmitted between them. A Bluetooth-enabled device has two modes—discoverable and not discoverable. A device needs to be set to the discoverable option to be able to be paired with another device.

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

* <BL>Pair two computers using Bluetooth protocols
* Transfer a file between two mobile computers using Bluetooth

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Two laptop computers with Windows 10

<H2>Activity

<FE1TX1>Estimated completion time: **15 minutes**

<TX1>In this lab, you will configure the connection between two laptop computers via the Bluetooth protocol.

1. <NL\_FIRST>Start-up Laptop One and log into the default account.
2. <NL\_MID>Start-up Laptop Two and log into the default account.
3. On each computer, you will repeat the same steps:
4. Open Control Panel.
5. In the Search Control Panel box, type Bluetooth.
6. Click Add a Bluetooth device. Windows will look for any Bluetooth devices within range, as shown in Figure 10-1. After a short time, you should see the other computer’s name appear in the device window.

**[Insert Figure 10-1 Here]**

1. Select the computer to pair and click Next.
2. A dialog box appears that asks if the displayed pairing code number appears on the other computer (see Figure 10-2). Verify that the numbers match and click Next.

**[Insert Figure 10-2 Here]**

1. The computer then installs the drivers for the new device. Once the process is complete, you will see the Bluetooth Device Control window, as shown in Figure 10-3. A folder will also be created on the hard drive C:\\Users\accountname\My Documents\Bluetooth Exchange Folder, where accountname is your login account on the computer.

**[Insert Figure 10-3 Here]**

1. Open the Notepad application on Laptop One. Create a file that has a few simple lines of text in it.
2. Save the file in the Bluetooth Exchange Folder and then close the file.
3. On Laptop Two, refresh the Bluetooth Exchange Folder and confirm that the file now appears on the second laptop.
4. Open the file on the second laptop and add a few lines of text to the file.
5. Save and close the file in the Bluetooth Exchange Folder.
6. Open the file on Laptop One and identify that the file has changed and includes the new text.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.5 Given a scenario, deploy mobile devices securely.

**<H2>Review Questions**

1. <TF>Bluetooth file transfer protocol can work on both a PC and a Mac computer. **True** or False?
2. <TF>When pairing two computers, it is not essential that the pairing codes match for the pairing to be completed. True or **False**?
3. <TF>When the Bluetooth protocol completes its pairing, the Bluetooth Exchange Folder is not needed to transfer files between computers. True or **False**?
4. <TF>When pairing two Bluetooth devices, a third device can be paired at the same time. True or **False**?
5. <TF>Only computers can be paired using Bluetooth. True or **False**?

# <H1>Lab 10.2 Getting Bluetooth Info with Bluesnarfer

**<H2>Objectives**

<TX1>Bluetooth technology is a source of many security vulnerabilities. If the technology is not secured and handled properly, attackers can gain access to important information on an individual’s personal devices. Bluetooth technology is meant to pair two devices so that communication between the devices can be done seamlessly and without interruption. Using simple protocols like radio frequency communication (RFCOMM) and Bluetooth network encapsulation protocol (BNEP), devices can be paired and data can be communicated between the two devices.

<TX2>Bluetooth protocol is typically separated into two stacks: the controller stack and the host stack. The controller stack is typically implemented in a device that contains the Bluetooth radio and the microprocessor. The host stack is typically part of the operating system. For integrated Bluetooth devices, the two stacks are typically run on the same microprocessor to save costs of producing the devices.

<TX2>It is important for device security to keep the Bluetooth discovery setting off until it is needed. If you leave your device discoverable, anyone within range can attempt to access the contents of your device at any time. For this reason, iPhone devices have removed file-sharing capabilities between Host and Controller stacks. To perform this action on an iPhone, you would need to install a Bluetooth file sharing application from the App store.

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

* <BL>Gather information from a device through the Bluetooth protocol
* Configure the hciconfig tool to access Bluetooth devices
* Configure and run the Bluesnarfing tool through Kali Linux

**<H2>Materials Required**

<H1>This lab requires the following:

* <BL>Completion of Lab 5.1
* A Windows 10 computer
* Kali Linux VM
* Android mobile phone with Bluetooth capability

**<H2>Activity**

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

<TX1>In this lab, you configure and run the Bluesnarfer application to access a remote device (a mobile phone) to retrieve the device’s user name.

1. <NL\_FIRST>Launch the VMware instance of Kali Linux.
2. <NL\_MID>Launch the Terminal command prompt.
3. Create a directory using the command: mkdir -p /dev/bluetooth/rfcomm
4. Make a node within the rfcomm protocol folder as follows: mknod -m 666 /dev /bluetooth/rfcomm0 c 216 0
5. Configure the Bluetooth connected devices: hciconfig hci0 up
6. Identify what devices are connected to the computer: hciconfig hci0
7. View the available commands for the hciconfig command: hciconfig –h
8. Turn the Android phone on, and set its Bluetooth feature to On.
9. Scan the devices for potential vulnerabilities: hcitool scan hci0
10. Look for the MAC address of the Android phone that is near the computer.
11. Using the MAC address of the device, you can determine if the device is active: l2ping <mac addr of Android device>
12. Determine what channels the device has open: sdptool browse --tree --l2cap <mac addr of Android phone>
13. View the commands used for Bluesnarfer: bluesnarfer –h
14. Set up Bluesnarfer to take control of the mobile phone: bluesnarfer -r 1-100 -C 7 -b <mac addr of Android device>

**<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.
* 2.5 Given a scenario, deploy mobile devices securely.

**<H2>Review Questions**

1. <FIB>When using the Bluesnarfer utility, you give it the numbers 1–100 after the –r command to signify \_\_\_\_\_\_\_\_\_\_\_\_\_.
2. **<FIBA>the range of ports to scan**
3. the IP address of the device
4. the priority in which the command will be executed
5. the version of Bluesnarfer to use
6. <MULT>The l2ping command returns data back to the host computer in the frequency of
7. <MULTA>Seconds
8. **Milliseconds**
9. Microseconds
10. Nanoseconds
11. <TF>The MAC address of the devices is unique. **True** or False?
12. <TF>The Bluesnarfer tool is a form of ethical hacking. True or **False**?
13. <TF>If you disable the Bluetooth capability on your device, you stop the Bluesnarfer tool from attacking your device. **True** or False?

# <H1>Lab 10.3 Kali Linux Mobile Device Security Tools

**<H2>Objectives**

<TX1>As seen in Chapter 5, Kali Linux is a very powerful tool to assist with intrusion detection and general hacking tools. Kali Linux has its roots in Knoppix Linux, which was a precursor to BackTrack Linux. The company Offensive Security (<URL>www.offensive-security.com</URL>) was the creator of Knoppix, BackTrack Linux, and now Kali Linux. The tools incorporated into the standard build are meant to assist individuals or companies with many different security needs.

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

* <BL>Identify the different categories of tools that Kali Linux offers

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10
* Successful completion of Lab 5-1
* Kali Linux VM

**<H2>Activity**

<FE1TX1>Estimated completion time: 15–20 minutes

<TX1>In this lab, you will familiarize yourself with Kali Linux and the tools it has to offer.

* 1. <NL\_FIRST>Launch the VMware instance of Kali Linux.
  2. <NL\_MID>Click Applications. Explore the Kali Linux menu option.
  3. One of the most powerful hacking tools is the Fern Wi-Fi cracker, which can be found at \Applications\Wireless Attacks\802.11 Wireless Attacks\fern wifi-cracker. This tool offers a GUI interface for hacking Wi-Fi networks. Given the correct access point and a little bit of time, the tool will decrypt messages and passwords on the wireless network.
  4. Kali Linux also includes tools that do brute force password cracking, such as HydraGTK, which cannot be found in the menu. To access these tools, click **show applications** on the left menu and search for **Hydra**. The Hydra tool allows you to attack a single user or multiple users at the same time. You provide the list of users and the password dictionary you would like to use, and the tool does the rest.
  5. Open the Kali Linux menu and find a tool that can be used for Cisco attacks. These tools communicate with Cisco equipment and understand the architecture of the equipment.
  6. Find the nmap tool at \Applications\Information Gathering\Network & Port Scanners\nmap. After launching the tool, you will see a description page. Toward the bottom of that page, notice the option to scan all networks using the IPv6 protocols. This tool allows you to scan the complete network and identify if there are any security risks at any of the open IP addresses.
  7. Explore some of the many other tools in Kali Linux. Do some experimentation with the tools.
  8. One final Kali Linux tool to explore is Maltegoce. This tool allows you to do network analysis and determine which machines are connected to which other machines and what protocols are being used for the communications. The tool can be found at \Applications\Information Gathering\OSINT Analysis\maltegoce.

**<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.
* 2.6 Given a scenario, implement secure protocols.
* 3.2 Given a scenario, implement secure network architecture concepts.

**<H2>Review Questions**

* 1. <MULT>A brute force password attack is typically done by:

1. <MULTA>Generating random passwords and trying them as the credentials to log in
2. **Using a preset set of words, typically in some file, and trying each of the words as credentials to log in**
3. Scanning the person’s personal information to see if the password can be guessed
4. None of the above
   1. <TF>You have to pay money for each tool you use in Kali Linux. True or **False**?
   2. <FIB>The Wireshark application found in Kali Linux analyzes \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
5. <FIBA>HTTP protocols only
6. **all network traffic**
7. only wireless network traffic
8. only accounts for which you have the username and password
   1. <TF>Running Kali Linux in a VMware instance decreases the abilities of the host operating system. True or **False**?
   2. <MULT>Which of the following is not an option on the Kali Linux Applications menu?
9. <MULTA>Sniffing & Spoofing
10. Wireless Attacks
11. **Hardware Hacking**
12. Password Hacking

# <H1>Lab 10.4 Physical Security

**<H2>Objectives**

<TX1>Physical security is generally overlooked for mobile devices. Physical security can be as simple as cables that attach a laptop to a desk, or password-locking screens. Physical security comes in many forms. It could involve armed security guards at doorways or it could be software installed on the devices.

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

* <BL>Identify basic physical protections available to users of mobile devices
* Identify that employee training should be a part of physical security

**<H2>Materials Required**

<TX!>This lab requires the following:

* <BL>Windows 10

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

* 1. <NL\_FIRST>Open a web browser and navigate to <URL>**https://www.sans.edu/cyber-research/security-laboratory/article/281</URL>**.
  2. <NL\_MID>Read the article and find the part of the article that is titled Laptop/Desktop Protection.
  3. Read the section on User Awareness (making individuals aware of their role in the act of security).
  4. Read the second item, Laptop Locks, which details that security cables should be physically connected to the laptop and then attached to the desk. This might not stop a determined attacker from cutting the cable and taking the device, but it might deter an attacker by making access more difficult.
  5. Read the next section of the document, Rings Approach to Physical Security Defense in Depth. Based on that section, draw a diagram or create a report that details the four levels or rings of physical security for a scenario provided by your instructor.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 3.2 Given a scenario, implement secure network architecture concepts.
* 3.9 Explain the importance of physical security controls.
* 5.1 Explain the importance of policies, plans, and procedures related to organizational security.

**<H2>Review Questions**

* 1. <TF>Physical security is concerned only about the loss of physical devices. True or **False**?
  2. <MULT>The Rings Approach to Physical Security Defense includes: (Choose all that apply.)

1. **<MULTA>Human factors**
2. **Internal location of the business building**
3. **Immediate area around the business building/environment**
4. **Areas on the perimeter of the business building**
   1. <MULT>According to the article, which is the most important aspect of security?
5. **<MULTA>Physical cables**
6. Security guards
7. User awareness
8. Policies
   1. <MULT>According to the article, which type of protection has not been widely implemented because of its high cost?
9. **<MULTA>Biometrics**
10. User awareness
11. Laptop locks
12. OS hardening
    1. <TF>Proper user awareness training eliminates the need for virus protection. True or **False**?

# <H1>Lab 10.5 BYOD Policies

**<H2>Objectives**

<TX1>Many organizations are implementing bring your own device (BYOD) practices. This allows professionals to work on devices they are comfortable with, but it also puts a strain on the IT department of a company. The company’s IT professionals in this situation must often work with unfamiliar hardware and allow it to connect to the company network. This puts the network and computer systems at risk.

<TX2>Most IT departments have policy documents detailing how devices must be maintained before they can connect to the computer network. It is typical that the IT department demands that the device, as well as any software that exists on the device, has all the latest updates provided by the manufacturer. This creates a large overhead for the IT professionals because they have to constantly monitor devices to assure that BYOD policies are being followed.

<TX2>Therefore, it is helpful for the IT department to have a consistent process for creating and deploying BYOD policies, and to educate employees on the directions within the policy.

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

* <BL>Create a BYOD policy
* Evaluate different BYOD policy templates and compare and contrast the benefits of each

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10
* Microsoft Word or a comparable word processor

**<H2>Activity**

<FE1TX1>Estimated completion time: **25–35 minutes**

<TX1>In this lab, you create a BYOD policy from a template. Your instructor should provide you with a scenario for which you are going to create a BYOD policy.

1. <NL\_FIRST>Open your web browser and navigate to the following websites:
   1. **<URL>http://www.code3pse.com/public/media/22845.pdf</URL>**
   2. **<URL>http://www.itmanagerdaily.com/byod-policy-template/</URL>**
2. <NL\_MID>Download each of the templates to a location on your computer.
3. Open each template and read through each document.
4. Compare and contrast what each document has to offer and what document best suits the needs of your scenario. If there are components of more than one policy that you would like to use, you can incorporate those sections into one document.
5. Create your policy and share it with your instructor or your classmates to identify if any of the wording needs to be adapted for your scenario.

**<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.
* 5.2 Summarize business impact analysis concepts.

**<H2>Review Questions**

* 1. <TF>Password policies should not be referenced in a BYOD policy. True or **False**?
  2. <TF>The templates recommend that personal information should be kept separate from work information. True or **False**?
  3. <FIB>When the BYOD policy refers to limiting access based on users’ roles, this refers to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ models.

1. **<FIBA>access control**
2. network monitoring
3. administrative control
4. none of the above
   1. <TF>A BYOD policy should detail the consequences for not following the policy. **True** or False?
   2. <TF>The BYOD policy should incorporate an acknowledgement sheet that the employee is asked to sign. **True** or False?