**<CHN>CHAPTER TWO**

<CHT>MALWARE AND SOCIAL ENGINEERING ATTACKS

<COOT>Labs included in this chapter

* <COOH1>Lab 2.1 Eicar Antivirus Test File
* Lab 2.2 Creating a Bootable Thumb Drive with Rufus
* Lab 2.3 Checking for Unsigned Programs
* Lab 2.4 Validating a Downloaded Program
* Lab 2.5 Acceptable Use Policy

<COOBT>CompTIA Security+ Exam Domains

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 2.1

Technologies and Tools 2.1, 2.3, 2.4

Architecture and Design 2.2

Risk Management 2.1, 2.5

<COOB\_LAST>Cryptography and PKI 2.4

<NOLB><NO>All labs in this book assume you are using Windows 10 as your operating system and the latest version of Microsoft Edge as your browser. If you use a different browser, you may have different outcomes. Throughout this book, the term “default account” refers to whatever name you have given your computer. The phrase “default user account settings” refers to the account on your computer that has administrator privileges.</NO>

# <H1>Lab 2.1 Eicar Antivirus Test File

**<H2>Objectives**

<TX1>Many anti-malware products are available on the Internet. Commercial products require payment for the software, then annual payments for updates to malware definitions, which are needed in order to keep up with the rapid proliferation of new malware threats. Several highly-respected free anti-malware also exist. Products differ in their abilities to detect and isolate malicious files, and it’s important to research and test the capabilities any product before implementing it in a production environment. In this lab, you will perform some simple experiments to determine the ability of two products to detect a test virus.

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

* <BL>Use Windows Defender to detect and remove malware
* Install and use Avast to detect and remove malware

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 with Internet access
* Eicar software
* AVG software
* Windows Firewall off
* Completion of Hands-On Project 1-3 in *Security+ Guide to Network Security Fundamentals* 6th edition.

**<H2>Activity**

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

<TX1>In this lab, you will test two antimalware products to determine their ability to detect a test virus file.

1. <NL\_FIRST>Launch the virtual machine created in Hands-On Project 1-3.
2. <NL\_MID>Open your web browser and enter http://www.eicar.org/86-0-Intended-use.html.

**<B1TX1>**It’s 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 “eicar.”

1. Read the **INTENDED USE** page.
2. Click **DOWNLOAD** in the menu to open the DOWNLOAD page
3. In the Download area, using the standard protocol http, click the eicar.com link, save the download to your desktop, and if necessary, click the Close button when the download is complete.
4. The anti-malware program that comes with Windows 10, called Windows Defender, should have detected the eicar file, identified it as potentially harmful, and displayed a balloon with a warning on the Taskbar, as shown in Figure 2-1. If a balloon does not appear, you may have to click the **white flag** in the tray on the status bar.

<FGN>2-1</FGN>

<FGLB>**Figure 2-1: Software detection warning**

1. Click the **balloon** warning to display the Windows Defender Alert window. Select the **History** tab. Select **Quarantined items**. Click View Details on the Windows Defender and read the contents shown in Figure 2-2.

<FGN>2-1</FGN>

<FGLB>**Figure 2-2: Windows Defender Alert**

1. Select the **checkbox** next to the eicar.com virus. Click **Remove** to remove the file.
2. Return to the eicar website and experiment to see how Windows Defender responds when you try to download eicar.com.txt, eicar\_com.zip, and eicarcom2.zip. Be sure to select the file and click Remove on the Windows Defender Alert window each time Windows Defender detects a threat. Close the alert window each time you remove the eicar file.
3. Use the Control Panel to turn off Windows Defender. Make sure you select all of the options for Windows Defender.
4. In Microsoft Edge, turn off the SmartScreen filter by clicking the More icon on the toolbar then click **Settings**. Then click **View** **Advanced Settings**. Then click the **SmartScreen** toggle button.
5. Return to the eicar website, click the eicar.com link again, save the file to your desktop, and click Close in the Download complete box.
6. To install a third-party antivirus program, open a new tab on your web browser and enter **www.avast.com/en-us/index**.

<B1TX1>It’s 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 “Avast.”

1. Click DOWNLOAD FREE ANTIVIRUS. Save the file to your desktop. In the Download complete window, click Run, then click **Yes**, then click **INSTALL**
2. Click the **CONTINUE** button twice. Click **No, I don’t want to protect my Android phone**.
3. Close the Avast window.
4. Return to your desktop, right-click the **eicar** file, and select Scan eicar.com. The Scan results window of Avast appears.
5. Click the **Show Result**s button to see the file that was detected. The virus is quarantined and is set to be removed automatically.
6. Click **Apply** to remove the file, and then click **Close**.
7. Return to the eicar website and right-click the eicar.com.txt link in the Download area using the standard protocol http. Avast will stop the download as it detects the file as a virus. Temporarily disable Avast and download the file. Select Save Target As and save the file to your desktop.
8. On your desktop, right-click the eicar.com.txt file and select Scan eicar.com.txt. Avast’s Scan results window appears. Click the **Show Result**s button to see the file that was detected. The virus is quarantined and is set to be removed automatically, click **Apply** to remove the file. Then click **Close**.
9. Return to the eicar website and click the eicar.com link. This time, Avast responds differently and detects the threat, as shown in Figure 2-3.

<FGN>2-3</FGN>

<FGLB>**Figure 2-3: Avast Alert**

1. See how Avast responds when you try to download eicar\_com.zip and eicarcom2.zip.
2. See how Avast responds when you try to open one of the .zip files.
3. Close your web browser. Delete any eicar files and delete the Avast installation file. Leave the Avast shortcut on your desktop.
4. Enable Windows Defender.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
* 2.4 Given a scenario, analyze and interpret output from security technologies.
* 5.4 Given a scenario, follow incident response procedures.

**<H2>Review Questions**

1. <MULT>Which of the following categories of malware is recorded in Avast’s scan results? (Choose all that apply.)
   1. **<MULTA>Infections**
   2. **Worms**
   3. Spyware
   4. Rootkits
2. <MULT>Which of the following actions in response to malware is supported by Windows Defender? (Choose all that apply.)
   1. **<MULTA>Remove**
   2. **Quarantine**
   3. Disinfect
   4. Allow
3. <MULT>Which of the following statements is true about the responses of Windows Defender and Avast in Lab 2.1?
   1. <MULTA>Windows Defender updates itself automatically.
   2. **Avast is able to detect the eicar virus even when the eicar file is compressed.**
   3. **Windows Defender is able to detect the eicar virus even when the eicar file is compressed.**
   4. Avast Free Edition contains a software firewall.
4. <TF>Avast virus software will protect against all viruses on the Internet. True or <TFA>**False</TFA>**?
5. <MULT>Windows Defender is what type of software?
   1. <MULTA>Malware
   2. Firewall
   3. **Malware protection**
   4. Rootkit

# <H1>Lab 2.2 Creating a Bootable Thumb Drive with Rufus

**<H2>Objectives**

<TX1>Sometimes you might need to access/remove files from an infected computer. This can pose many issues. The files you access/remove from the old computer may be infected or they may be required by the previous filesystem for the computer to operate properly. A bootable thumb drive makes it possible to access the hard drive on a computer, bypassing normal operating systems secure controls.

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

* <BL>Create a bootable thumb drive
* Analyze a host computer from a virtualized environment

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>A USB thumb drive of at least 8 GB
* Windows 10 with Internet access
* Ubuntu ISO file
* Rufus software

**<H2>Activity**

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

<TX1>In this lab, you will create a bootable thumb drive that can be used to recover items from a disabled or infected PC.

1. <NL\_FIRST>Open your web browser and enter **https://www.ubuntu.com/download/desktop**

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 “Rufus.”

1. <NL\_MID>Click the **Download** button.
2. When you see a page asking for donations, click **Not now, take me to the download**
3. Download the desktop ISO of Ubuntu, save it to a folder on your computer.
4. Open your web browser and enter **http://rufus.akeo.ie/**

**<B1TX1>**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 “Rufus.”

1. **Find the latest version of Rufus and c**lick Download Rufus X.X.
2. Install the software and launch the application when done.
3. Insert a thumb drive into your computer.
4. Fill in the Rufus dialog, making sure to select the Ubuntu ISO file. See Figure 2-4.

<FGN>2-4</FGN>

<FGLB>**Figure 2-4: Rufus**

1. To the right of “Create a bootable disc using,” click the icon that looks like a disk drive**.** Navigate to the download of Ubuntu ISO file and select it.
2. Click the **Start** button on the Rufus dialog. If prompted to download files click the **Yes** button. See Figure 2-5.

<FGN>2-5</FGN>

<FGLB>**Figure 2-5: Rufus download required**

1. Click **Yes** in the ISOHybrid image detected dialog box. Click **OK** to overwrite all the files on the thumb drive. See Figure 2-6.

<FGN>2-6</FGN>

<FGLB>**Figure 2-6: Rufus ISOHybrid image detected**

1. Click Close when the Rufus software finishes.
2. Determine how to start your computer from a thumb drive. This may involve changing your boot order in your BIOS. To do so, enter your BIOS and go to Advanced Settings. Find the Boot order and make the USB rom drive the first option of the boot order. (WARNING: Do not change settings in your BIOS casually. If you are uncomfortable doing this please ask your instructor for help.)
3. Restart the computer and boot from the Thumb drive. When the machine restarts select **Run without installing Ubuntu**.
4. When the computer starts from the USB thumb drive, the Ubuntu image will mount the hard drive. This is very useful if the computer is infected and you need to retrieve personal files from a Windows machine. You can also use the thumb drive to access a secondary storage device or a mounted device via the Ubuntu OS, and copy the files from the hard drive to the secondary storage. In addition, the thumb drive allows you to run virus cleaning software on the Windows hard drive and remove malicious software without Windows security measures getting in the way.
5. When you are finished exploring Ubuntu, shut the computer down and remove the thumb drive. Restart your machine and enter the BIOS. Return the boot order to its original state. Save and exit your BIOS, and your machine should boot to the Windows desktop.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.2 Given a scenario, implement secure network architecture concepts.
* 3.3 Given a scenario, implement secure systems design.
* 3.7 Summarize cloud and virtualization concepts

**<H2>Review Questions**

1. <MULT>Ubuntu is based on what operating system?
   1. **<MULTA>Linux**
   2. Windows
   3. Mac
   4. Debian
2. <MULT>Rufus software allows you to create what easily?
   1. <MULTA>A bootable hard drive
   2. A bootable CD-ROM
   3. **A bootable thumb drive**
   4. A bootable Cloud drive
3. <MULT>Which of the following is not a benefit of creating a bootable thumb drive?
   1. **<MULTA>It is expensive**
   2. It is inexpensive
   3. It can be used to run software on the host computer
   4. It mounts the hard drive of the computer it is run on
4. <MULT>The default file system the Rufus need to use is?
   1. <MULTA>NTFS
   2. FAT16
   3. **FAT32**
   4. FAT
5. <TF>When downloading ISO files from the Internet, I should disable my virus software to help the download happen faster. True or <TFA>**False**</TFA>?

# <H1>Lab 2.3 Checking for Unsigned Programs

**<H2>Objectives**

<TX1>Attackers sometimes succeed in installing malicious code on a target by tricking the victims into installing the programs themselves. Users frequently download programs from the Internet. Most of the time this isn’t a problem, particularly if a reputable website is hosting the program. However, if an attacker succeeds in using a man-in-the-middle attack, the attacker can intercept the packets sent from the host website and send malware to the user.

<TX2>To protect against the possibility of downloading malicious software, you should verify the authenticity of downloaded software by validating the program developer’s digital signature. A digital signature is a cryptographic form of authentication. In this lab, you download and install a program that allows you to check which of your programs are unsigned.

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

* <BL>Download and install a command-line security utility
* Use Sigcheck to examine files for digital signatures

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 computer
* Sigcheck

**<H2>Activity**

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

<TX1>In this lab, you download a file validation tool called Sigcheck.

1. <NL\_FIRST>Open your web browser and enter technet.microsoft.com/en-us/sysinternals/bb897441.aspx.

<B1TX1>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 “Sigcheck.”

1. <NL\_MID>Click Download Sigcheck.
2. Direct the download to your desktop and click the Close button when the download is complete.
3. Double-click the Sigcheck.zip archive.
4. Click Extract all files.
5. Verify that the archive will extract to your desktop and click Extract.
6. From the extracted Sigcheck folder, move sigcheckXX.exe to the C:\Windows directory. Where the XX is either nothing or 64 based on your operating system. Sigcheck is a command-line utility, so it is necessary to place the program file in a directory that is listed in the path (the list of directories in which the operating system looks for executable files).
7. In the Ask Me Anything window, type CMD. Right-click Command Prompt, then click Run as administrator.
8. If the command prompt starts you at C:\Windows\System32, navigate to the C: drive by typing **cd ..\..\**
9. At the C:\Windows command prompt, type sigcheckXX.exe /? and press Enter. The SigCheck License Agreement may appear. If it does, click Agree. Review the syntax and options available.
10. Type sigcheckXX.exe –a –h C:\Windows > C:\SCtest.txt and press Enter. This command runs a check on the programs in the C:\Windows directory and redirects the output of the command from the console to a file called SCtest.txt.
11. If it did not appear earlier, the SigCheck License Agreement may appear now. If so, click Agree on the SigCheck License Agreement.
12. Wait until your command prompt reappears, and then, from your C drive open and examine the file SCtest.txt.
13. Notice that some of the programs are digitally signed (check the verified line) whereas others are not.
14. Run the SigcheckXX.exe on the C:\ drive and check to see if the Sigcheck program itself is digitally signed?
15. Close all windows and log off.

**<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
* 2.4 Given a scenario, analyze and interpret output from security technologies.

<H2>**Review Questions**

1. <MULT>Which of the following statements regarding Sigcheck is correct? (Choose all that apply.)
   1. <MULTA>Sigcheck examines hidden files.
   2. **Sigcheck examines only executable files.**
   3. **Sigcheck can be used to verify that a digital signature is authentic.**
   4. Sigcheck can check for certificate revocation.
2. <MULT>Which option would you use with Sigcheck to do a recursive subdirectory scan?
   1. <MULTA>-d
   2. -sub
   3. **-s**
   4. -ls
3. <MULT>On the Sigcheck help page, in the Usage section, the syntax for command usage is presented. In interpreting the syntax of a command, anything in square brackets ([ ]) indicates that the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. **<MULTA>option is not required**
   2. option will be explained below
   3. option can be entered either in uppercase or lowercase
   4. options have to be used in alphabetical order
4. <TF>The potential security issues addressed by Sigcheck apply to programs installed locally (from a CD or DVD) as well as programs downloaded over the Internet. <TFA>**True</TFA>** or False?
5. <MULT>Sigcheck needs to run as an administrator because?
   1. **<MULTA>It is a command line application and needs access to executable files**
   2. It needs complete control of the operating system
   3. It needs to bypass security controls
   4. It needs access to more memory to run

# <H1>Lab 2.4 Validating a Downloaded Program

**<H2>Objectives**

<TX1>When attackers successfully interpose themselves between websites hosting software for download and the users downloading the software, the attackers can deceive the user into installing a malicious program. This is bad for users and for organizations that host downloadable programs. To combat this threat, many developers allow users to check an encrypted, unique “signature” (or hash) to verify that they have downloaded the file they thought they were downloading. Even the slightest change to a program file causes the program’s hash to change dramatically, indicating that the program may not be legitimate. Developers publish hashes, usually on their website, to make them easy for users to access.

<TX2>The downside of this strategy is that it relies on the users, once they’ve downloaded the file, to determine if the hash of the downloaded file is the same as the one published by the developer. The average user is not technically sophisticated enough to perform this security check. In addition, even those who are able to check hashes of the programs they download do not always do so. Technical security controls can go a long way toward securing information systems, but when users are unable or unwilling to use security controls properly, they, not technology, become the weakest link in the security chain.

<TX1>After completing this lab, you will be able to:

* <BL>Examine the digital hash of a program provided by the developer
* Download a program file and validate its integrity using Sigcheck

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 computer with Internet access
* WinSCP
* Completion of Lab 2-3 Checking for Unsigned Programs

**<H2>Activity**

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

<TX1>In this lab, you download a program from the Internet and determine if the hash published by the developer is the same as the hash of the downloaded program.

1. <NL\_FIRST>Open your web browser and enter winscp.net/eng/download.php#download2.

<B1TX1>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 “WinSCP.”

1. **<NL\_MID>**Click the link Release Notes, Checksums.
2. Examine the release notes for the first winscp listing (it has an .exe extension), as shown in Figure 2-7.

<FGN>2-7</FGN>

1. <FGLB>**Figure 2-7: Release notes of WinSCP** Write down the MD5 hash of the program. The developers of the program WinSCP want you to be able to compare their hash with the one you derive from the file once you have downloaded it.
2. Click the Back button on your web browser, then click the Installation package link. If the file download is blocked by the web browser, you will see a bar on top of the WinSCP window. Click that bar and select Download File, if necessary.
3. Direct the download to the root of the C:\ drive and click the Close button when the download is complete.
4. In order to maximize system security, you should derive the hash of the downloaded program and compare it to the publisher’s hash before installing the program.
5. Open a command prompt.
6. Navigate to the root of the C:\ drive by typing cd / and pressing Enter.
7. Enter the **dir** command to see the files in the C:\ drive. Make note of the exact name of the WinSCP exe file.
8. Enter the following command: **sigcheckXX.exe –a –h** ***the full name of the WinSCP .exe file***.
9. Examine the result. It should be similar to what is shown in Figure 2-8. Does your MD5 hash match the one posted on the developer’s website?

<FGN>2-8</FGN>

1. **<FGLB>Figure 2-8: Sigcheck of WinSCP** Close all windows and log off.

**<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.
* 2.4 Given a scenario, analyze and interpret output from security technologies.
* 6.2 Explain cryptography algorithms and their basic characteristics.

**<H2>Review Questions**

1. <MULT>Which of the following statements regarding validation of downloaded programs is correct? (Choose all that apply.)
   1. **<MULTA>When the hashes of two files are the same, you can be assured that the two files are the same.**
   2. When the hash of a program on the Internet is the same as the hash of the file you downloaded, you can be sure that the program does not contain malware.
   3. **If you suspect that the website offering downloads of programs is not legitimate, it makes sense to email or telephone the developer of the program and double-check the hash.**
   4. When the hash of a program on the Internet is different from the hash of the file you downloaded, you can be sure that the program contains malware.
2. <MULT>Which of the following is a useful way to decrease the chance of inadvertently installing malware? (Choose all that apply.)
   1. **<MULTA>Scan the program file with antivirus software.**
   2. Shut down and reboot the system after the program is first installed.
   3. **Check for reports of security problems with the program on technical newsgroups, email lists, and websites that track program threats and vulnerabilities.**
   4. **Download programs only from reputable sites.**
3. <TF>You can determine the hash of a program in Windows 10 by right-clicking the program file, selecting Properties, and accessing the Details tab. True or <TFA>**False</TFA>**?
4. <MULT>Which of the following is a reasonable way to increase system security? (Choose all that apply.)
   1. **<MULTA>Use a program that automatically hashes your original operating system files periodically to determine if an attacker has modified a system file.**
   2. Boot the system from different boot files (i.e., a rescue CD-ROM or a dedicated USB flash drive), then scan the system with a rootkit detector.
   3. Use an automatic hashing program to screen emails and instant messages.
   4. **Back up your system regularly**.
5. <TF>One weakness with comparing hashes to verify program integrity is the frequency of false positive results when, even though the two programs are the same, the filename has been modified. This will cause the hashes not to match. True or <TFA>**False**</TFA>?

# <H1>Lab 2.5 Acceptable Use Policy

**<H2>Objectives**

<TX1>In an effort to stop malware and social engineering attacks, a computer security specialist should have a strong understanding of an Acceptable Use Policy. An Acceptable Use Policy is a tool for an organization that can be used to educate and create an awareness of what and/or how the information within the system will be used. The policy details how equipment should be maintained and how information is to be maintained internally within a company. The policy outlines both acceptable and unacceptable use of computer equipment.

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

* <BL>Create an Acceptable Use Policy
* Identify the components of an Acceptable Use Policy and how it should be integrated into a company

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 with Internet connection
* A word processor that can modify a DOC file

**<H2>Activity**

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

1. <NL\_FIRST>Open a web browser and navigate to www.sans.org/security-resources/policies/general#acceptable-use-policy.
2. <NL\_MID>Download the DOC template for an Acceptable Use Policy.
3. Open the template after downloading it to your computer.
4. Read the entire document and replace all instances of <Company Name> with *Your\_Last\_Name* Securities. (For example if your last name is Smith, then the company name should be Smith Securities.)
5. Identify to whom this policy pertains.
6. Specify to whom this policy should be disseminated.
7. Identify section 4.3 Unacceptable Use and identify when exceptions can be given to not follow this section of the policy.
8. If desired, save the file with a naming convention provided to you by your instructor.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>4.4 Given a scenario, differentiate common account management practices
* 5.1 Explain the importance of policies, plans and procedures related to organizational security.
* 5.3 Explain risk management processes and concepts.

**<H2>Review Questions**

1. <MULT>How many other types of policies are referenced in this policy?
   1. <MULTA>2
   2. 3
   3. 4
   4. **5**
2. <TF>The Acceptable Use Policy should not be disseminated to all employees of a company. True or <TFA>**False**</TFA>?
3. <TF>According to the policy it is OK to share account information with your coworkers when working on a project together. True or <TFA>**False</TFA>**?
4. <MULT>All mobile devices that connect to the internal network must comply with what policy?
   1. <MULTA>Password Policy
   2. Email Policy
   3. **Minimum Access Policy**
   4. Data Protection Standard Policy
5. <TFA>Port scanning is allowed in an Acceptable use policy. True or <TFA>**False**</TFA>?