Lab 4.1 Installing Certificate Services

Objectives

Asymmetric encryption is an elegant solution to a difficult problem: How do you safely exchange symmetric keys with people all over the world using a medium (the Internet) that is so unsecure you need to use encryption in the first place? The public/private key pair allows people to share their public keys freely and use their private keys to decrypt messages and create digital signatures. Once symmetric keys are exchanged, using asymmetric encryption, the rest of the transmission is encrypted with the much faster symmetric encryption. However, at some point, human trust is required for the Public Key Infrastructure (PKI)—the hierarchy of systems that request, issue, use, and revoke digital certificates—to provide a high level of information security. Asymmetric key pairs are mathematically related so that anything encrypted by one of the keys can only be decrypted by the other key. Digital certificates are used to send public keys. But how do you know that the digital certificate you receive came from the entity that claims to have sent it? If the certificate is digitally signed by a person or an organization you trust, such as a well-known commercial certificate authority, you can assume that the certificate is legitimate. The systems that issue certificates are called certificate authorities (CA), and in this lab, you will create one.

After completing this lab, you will be able to:

- Install a Windows Enterprise Certificate Authority
- Install a Windows 2016 Server

Materials Required

This lab requires the following:

- Windows 10 computer with VirtualBox installed
- Windows Server 2016 ISO

Activity

Estimated completion time: **80–90 minutes**

In this lab, you will install an Enterprise Certificate Authority.

1. Open your Windows 10 desktop.
2. Launch your browser and navigate to **https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016**.
3. Click the **Register to continue** button, add your contact information, and then click **Continue.**
4. Select **ISO** and click **Continue.**
5. If necessary, select the appropriate bit version (32 or 64) for your OS, and then select your language.

6. Click **Download.** Save the ISO to your hard drive.
7. Launch VirtualBox and create a new VM with the Windows Server 2016 ISO. Name the Virtual Machine **Windows Server,** select **Microsoft Windows** for the type, and select **Windows 2016** for the Version.
8. Start the Windows Server VM.
9. When prompted to select a start-up disk, navigate to the Windows Server 2016 ISO you downloaded. Click **Start.**
10. Click **Next.** If necessary select **Windows Server 2016 Standard Evaluation (Server with GUI)** and then click **Next.**
11. Click **Next** in the Language, Time, and Keyboard dialog box.
12. Click **Install now.**
13. Select **Windows Server 2016 Standard Evaluation (Desktop Experience)** and click **Next.**
14. Accept the license terms and click **Next.**
15. Select **Custom: Install Windows only (advanced)** and accept the default settings from this point on.
16. Set the default Administrator password as **Pa$$word** and click **Finish.**
17. Next, you need to make sure the server has Active Directory services installed. Logon as the administrator, open Server Manager, click **Manage,** then click **Add Roles and Features.** Click **Next** until you see the Server Roles window.
18. Select the **Active Directory Domain Services** check box and then, when prompted, click **Add Features.** Click **Next three times.** Click **Install.** This could take some time to finish.

Note

Active Directory domain services allow the server to manage centralized settings for user accounts. You can use Active Directory to set up certificates and policies on the domain server that regulate all user accounts that have a role on the server.

19. If necessary, wait for the server to restart, then click the notifications flag and select **Promote this server to a domain controller.**
20. Select **Add a new forest.** Enter **Test.local** for the Root domain name. Click **Next.**
21. Enter the password **Pa$$word,** confirm it and click **Next** twice.
22. Enter **TEST** for the NetBIOS domain name and click **Next** three times.
23. Allow the prerequisites check to run. Don't be concerned if you see warning messages, but if you receive errors, review your settings and make any necessary corrections. Once

you have successfully completed the prerequisites check, click **Install**. Restart the server if prompted to do so.

24. Open **Server Manager**, click **Manage**, and then click **Add Roles and Features**. Click **Next** until you reach the **Server Roles window**.
25. Select the **Active Directory Certificate Services** check box, and then, when prompted, click **Add Features**. Click **Next twice**.
26. Read the Active Directory Certificate Services (AD CS) page and click **Next**. In the Role Services window, and, if necessary, select the **Certification Authority and Certification Authority Web Enrollment** check box. If you are prompted to add features that are required for Certification Authority Web Enrollment, click **Add Features**. Click **Next three times**. In the Confirmation window, click **Install**.
27. Click **Close** after the installation has completed.
28. Click the **notifications** flag at the top of Server Manager, and then click **Configure Active Directory Certificate Services on the destination server**. Click **Next** in the Credentials window, and then select the **Certification Authority** and **Certificate Authority Web Enrollment** check box. Click **Next**.
29. On the Setup Type window, verify that Enterprise CA is selected and click **Next**. An enterprise CA uses Active Directory to authenticate users and help manage certificates. A stand-alone CA requires that an administrator approve every request for a certificate because Active Directory is not available to provide authentication. Stand-alone CAs are ideal for permitting secure network access to business partners, external consultants, or others who do not have Active Directory accounts. On the CA Type window, verify that Root CA is selected and click **Next** once.
30. On the Private Key window, verify that **Create a new private key** is selected and click **Next**. Read the default settings on the Cryptography window and click **Next**.
31. On the CA Name window, in the Common name for this CA box, note the default name and click **Next**.
32. On the Validity Period window, accept the default settings and click **Next**.
33. If necessary, click **Next** until you reach the Certificate Database window. Select **Choose and assign a certificate SSL later** and then click **Next**. (If you don't see this window, proceed to the next step.)
34. In the Confirmation window, click **Configure**, and then click **Close**.
35. Open a Microsoft Management Console by clicking **Search Windows** and typing **mmc**. Select the mmc if necessary. Click **File**, the click **Add/Remove Snap-ins**. Add Certificate Templates, Certification Authority (Local), Enterprise PKI, and Internet Information Services (IIS) Manager (not Internet Information Services 6.0) snap-ins, as shown in Figure 4-1. Save the console on your desktop as **PKI**.
36. Close all windows and log off.

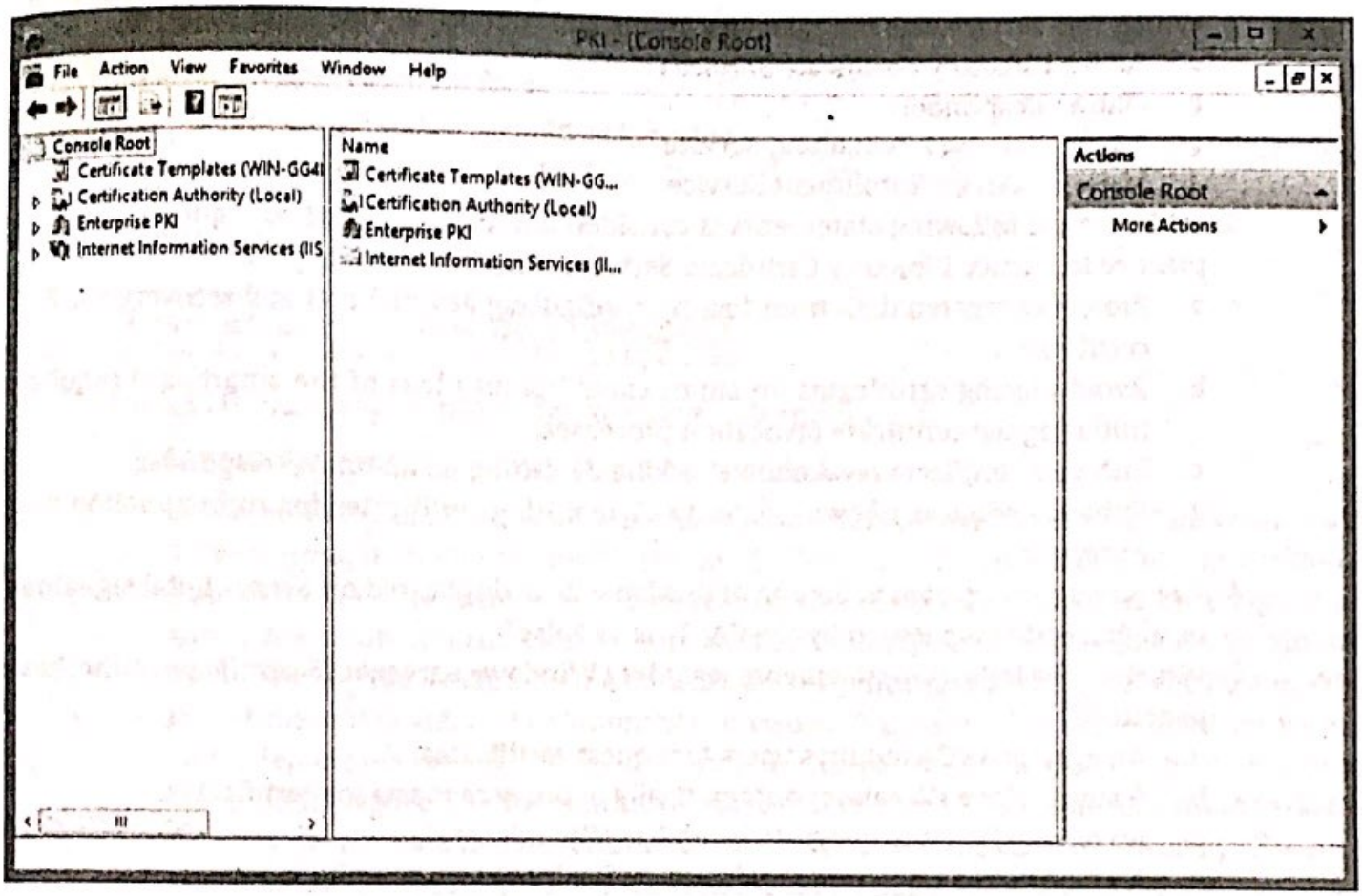

Figure 4-1 PKI console
Source: Microsoft LLC

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 4.3 Given a scenario, implement identity, and access management controls.
- 4.4 Given a scenario, differentiate common account management practices.
- 6.1 Compare and contrast basic concepts of cryptography.
- 6.4 Given a scenario, implement public key infrastructure.

Review Questions

1. Which of the following roles must be available on a network to implement an Enterprise CA that supports web enrollment? (Choose all that apply.)
   a. DNS server
   b. Active Directory Domain Services
   c. Certificate Services
   d. Web server

2. Which role service was not installed in this lab? (Choose all that apply.)
   a. Active Directory Certificate Services
   b. Online Responder
   c. World Wide Web Publishing Service
   d. Network Device Enrollment Service
3. Which of the following statements is considered a recommended configuration or best practice for Active Directory Certificate Services? (Choose all that apply.)
   a. Protect encrypted data from loss by configuring key archival and recovery for EFS certificates.
   b. Avoid placing certificates on smart cards because loss of the smart card requires initiating the certificate revocation processes.
   c. Enhance certificate revocation checking by setting up an online responder.
   d. Enhance wireless network security by requiring certificates for authentication and encryption.
4. The private key created in Step 32 of this lab will be duplicated on every digital signature or digital certificate issued by the CA. True or False?
5. Which of the following statements regarding Windows Server 2016 certificate authorities is correct?
   a. An enterprise CA requires users to request certificates.
   b. A stand-alone CA cannot automatically approve requests for certificates.
   c. An enterprise CA is integrated with the NWLink service.
   d. A stand-alone CA is integrated with Active Directory Domain Services.

Lab 4.2 Configuring Secure Sockets Layer

Objectives

Secure Sockets Layer, now incorporated into Transport Layer Security as SSL/TLS, has been the security standard for communications between web browsers and web servers for over 10 years. The client and the server exchange public keys, use asymmetric encryption to secure their negotiations, agree on a symmetric key, and then communicate using the symmetric key thereafter. The digital certificate presented to the client by the server has been signed by a commercial certificate authority trusted by the client. The root certificates placed in the client's certificate store by the operating system vendor determine which commercial CAs the client trusts. Of course, the client can install other certificates, but this is unusual in the e-commerce world. This is much more likely within intranets (private, corporate networks) where employees are using an in-house CA to provide certificates for encrypting email, installing on smart cards, digitally signing documents, and so forth. In this lab, you prepare the certificate authority to respond to clients' web requests for digital certificates.

After completing this lab, you will be able to:

- Configure a web server to support SSL connections
- Import a root certificate to a client system
- Explain how asymmetric and symmetric encryptions are used by SSL
- Configure Internet Explorer to trust a secure site

Materials Required

This lab requires the following:

- Windows 2010 with VirtualBox installed
- Successful completion of Lab 4.1

Activity

Estimated completion time: **30–40 minutes**

In this lab, you prepare the server to accept web enrollment.

1. Launch the Windows Server VM you created in Lab 4.1.
2. Open the **PKI** console on your desktop. Expand **Enterprise PKI** in the left pane and click **ServerName,** it should start with the word "Test." The Enterprise PKI utility tracks the state of the CA. Any items with red markers in the center pane have problems. Figure 4-2 shows the result of a successful setup, with no red markers. Double-click **CA Certificate** in the center pane. Notice, on the General tab, the purposes for using this certificate. Who issued the certificate, and to whom was it issued? This is the CA's self-signed certificate, and it represents the highest level of trust in this PKI implementation. In other words, since the CA signed its own certificate, users of any of the CA's certificates must trust the CA; they cannot look to other entities to assure them that the CA is trustworthy. Close the certificate and examine the other items in the center pane. What is a certificate revocation list? You should not see any warning icons on these items.

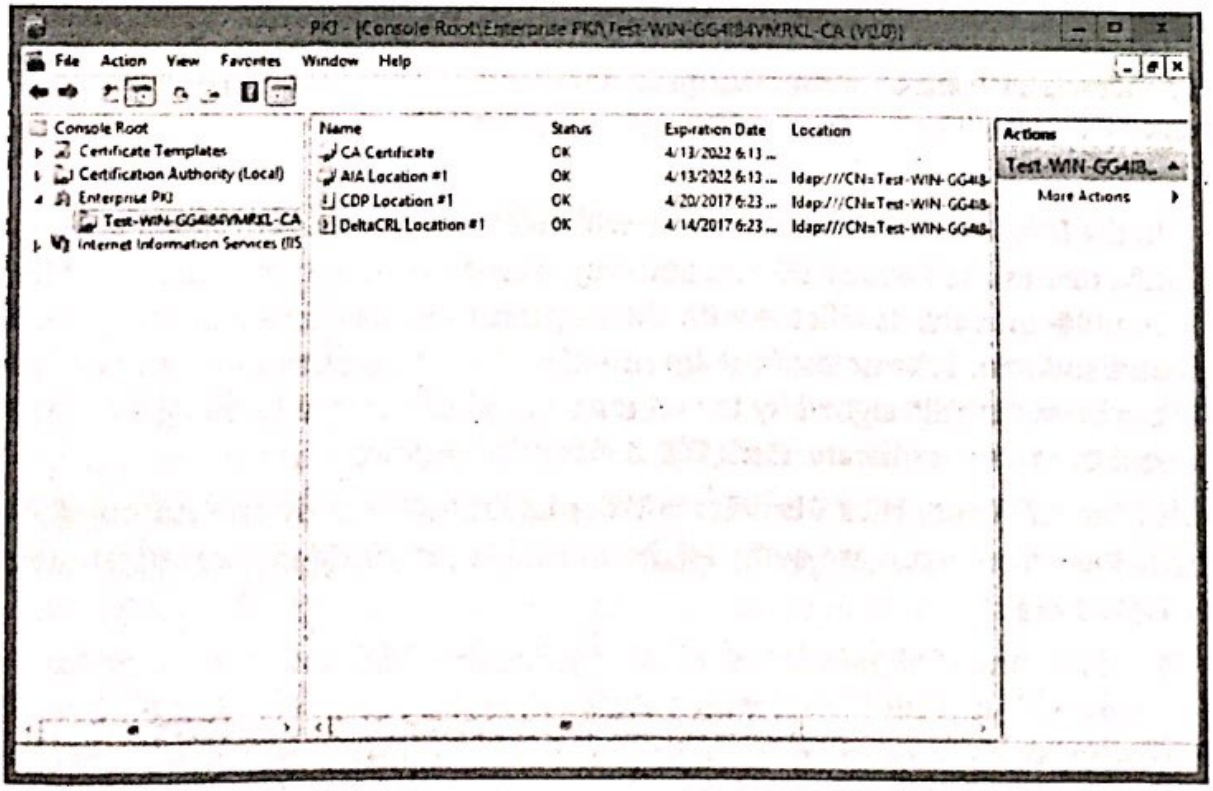

Figure 4-2 Enterprise PKI showing a healthy CA
Source: Microsoft LLC

3. Expand **Certification Authority (Local)** in the left pane; expand and then click your server's name. In the center pane are the certificate folders (see Figure 4-3). Explore the folders.

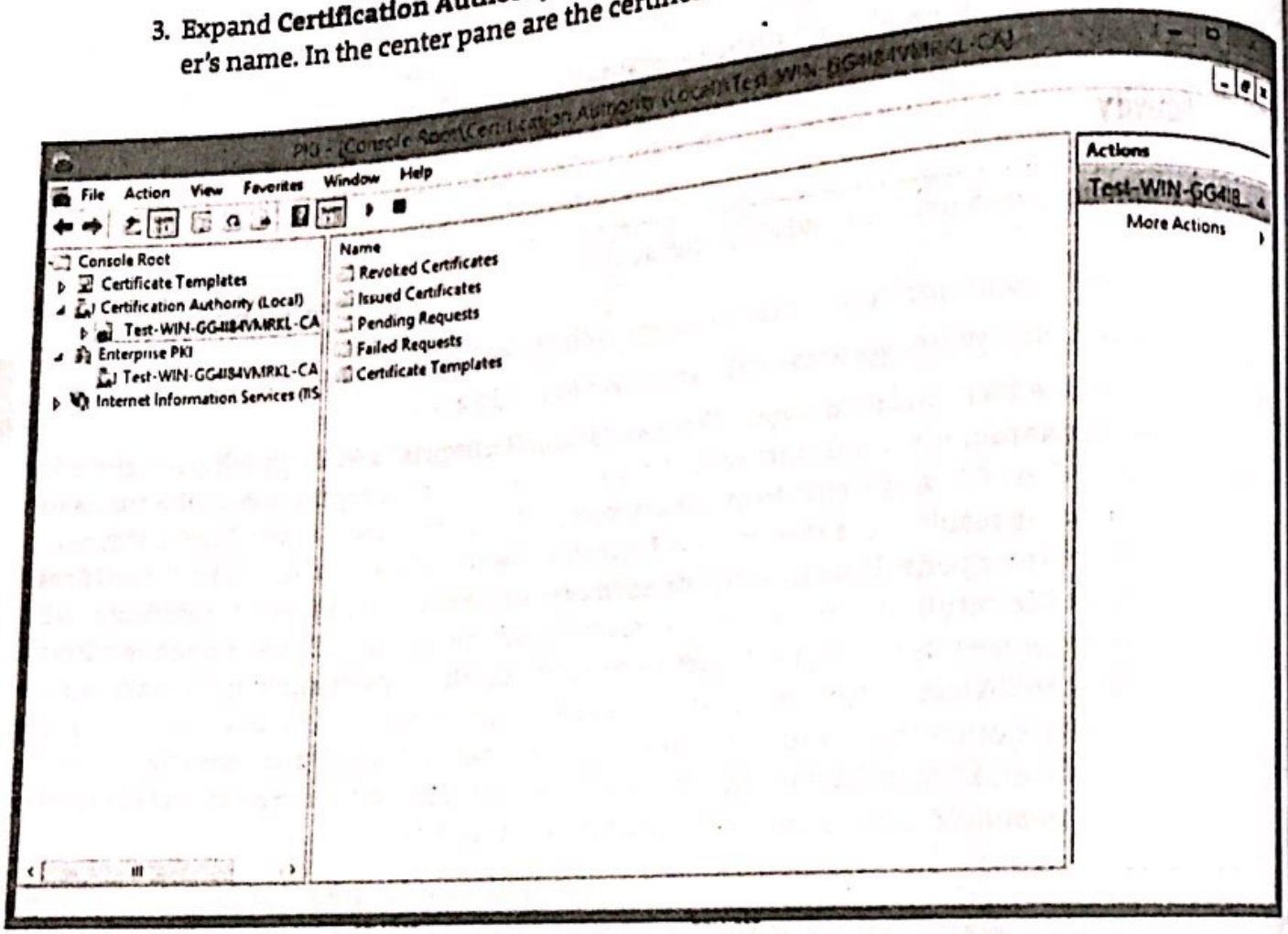

Figure 4-3 Certificate folders
Source: Microsoft LLC

In the Issued Certificates folder, you will find a certificate with a Request ID of 2. What certificate has the Request ID of 1, and why is it not shown in the Issued Certificates folder? Double-click the certificate with the Request ID of 2 and investigate its purpose, issuer, and so forth. Take note of the information on the Certification Path tab. This certificate has been digitally signed by the CA root. Any client or service that trusts the ServerName will trust this certificate. Click **OK** to close the certificate.

4. In the left pane, click **Certificate Templates** under Certificate Authority/ServerName. In the center pane are some of the available preconfigured certificate templates (see Figure 4-4).

These certificates permit a variety of functions. You should be familiar with the EFS Recovery Agent certificate, which allows recovery of an encrypted file if the user's key is corrupted or unavailable. Computer and User certificates are common, too. One template of note in this list is the Enrollment Agent certificate. This is required by the user who will generate certificates to be coded on smart cards. Close and save the PKI mmc.

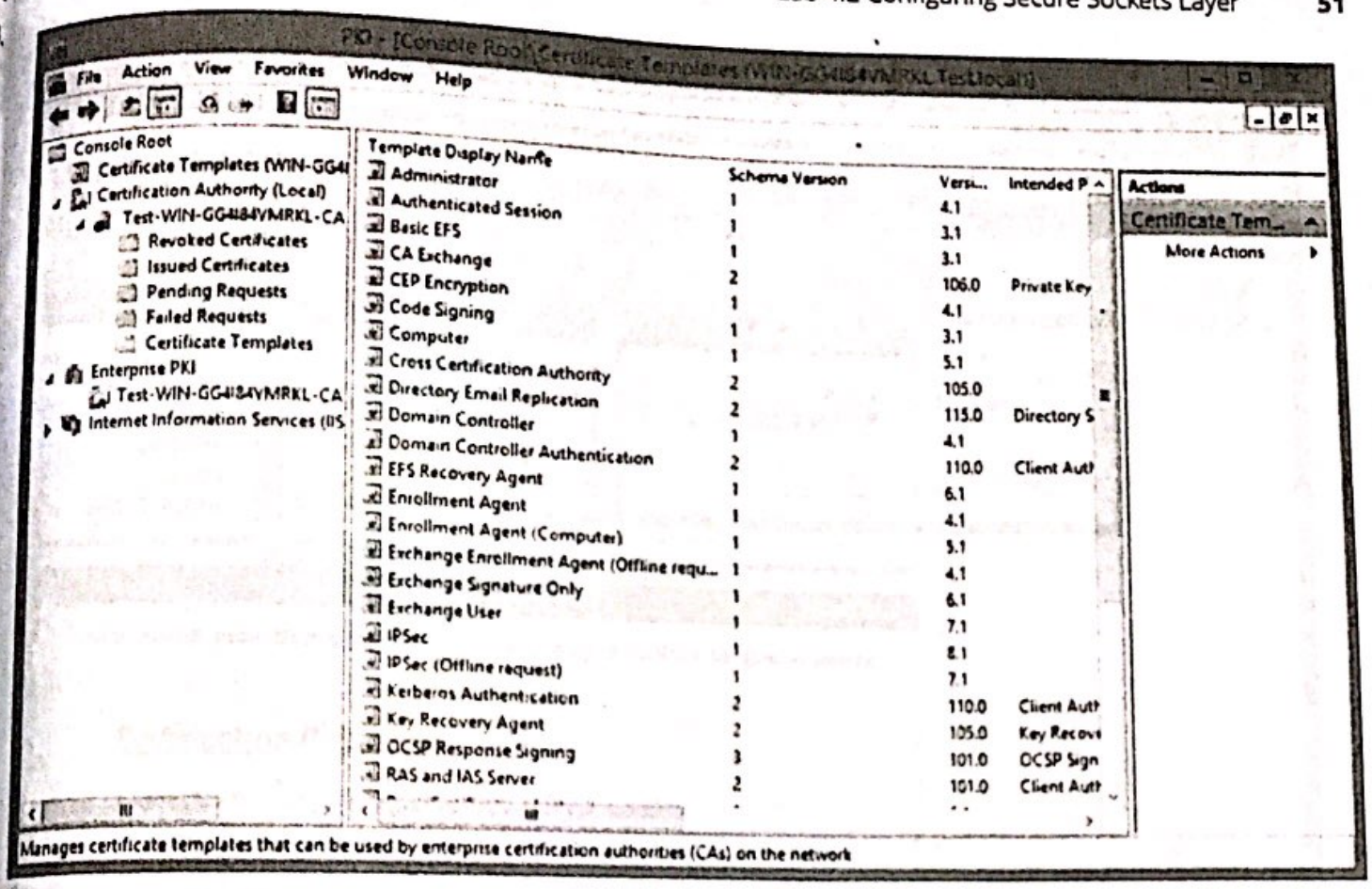

Figure 4-4 Certificate templates
Source: Microsoft LLC

5. Click **Start** on the server. Click **Windows Administrative Tools**, double-click the **Internet Information Services (IIS) Manager**. The IIS 10 Application Server Manager console appears (see Figure 4-5). In the Connections pane, expand your server's name. Click no if the Dialog pops-up. Expand the **Sites** folder and expand **Default Web Site**.
6. Verify that your server's name is selected in the left pane, and then double-click **Authentication**. Notice whether Anonymous Authentication is enabled. Normally, websites allow anonymous access to attract potential customers, but in a certificate service website, anonymous access would involve a serious security vulnerability. Click **Default Web Site** in the left panel and double-click **Authentication**. Here, notice the status of Anonymous Authentication. Click **Default Web Site** in the left pane. Scroll down and double-click **SSL Settings**.
7. Secure Sockets Layer provides authorization and encryption services for web-based communications. If the SSL boxes are dimmed, you need to bind HTTPS and a web server certificate to port 443, the standard HTTPS port. To set the binding, click *ServerName* in the left pane and, in the middle pane, scroll down and double-click **Server Certificates**. You should see two certificates in the middle pane. If only one certificate appears, reboot the server and then return to this console. Scroll horizontally to see more information about the certificates.
8. Double-click the top certificate and examine the three tabs, paying special attention to the purpose(s) of the certificate and the Certification Path. Click **OK** to close the Certificate

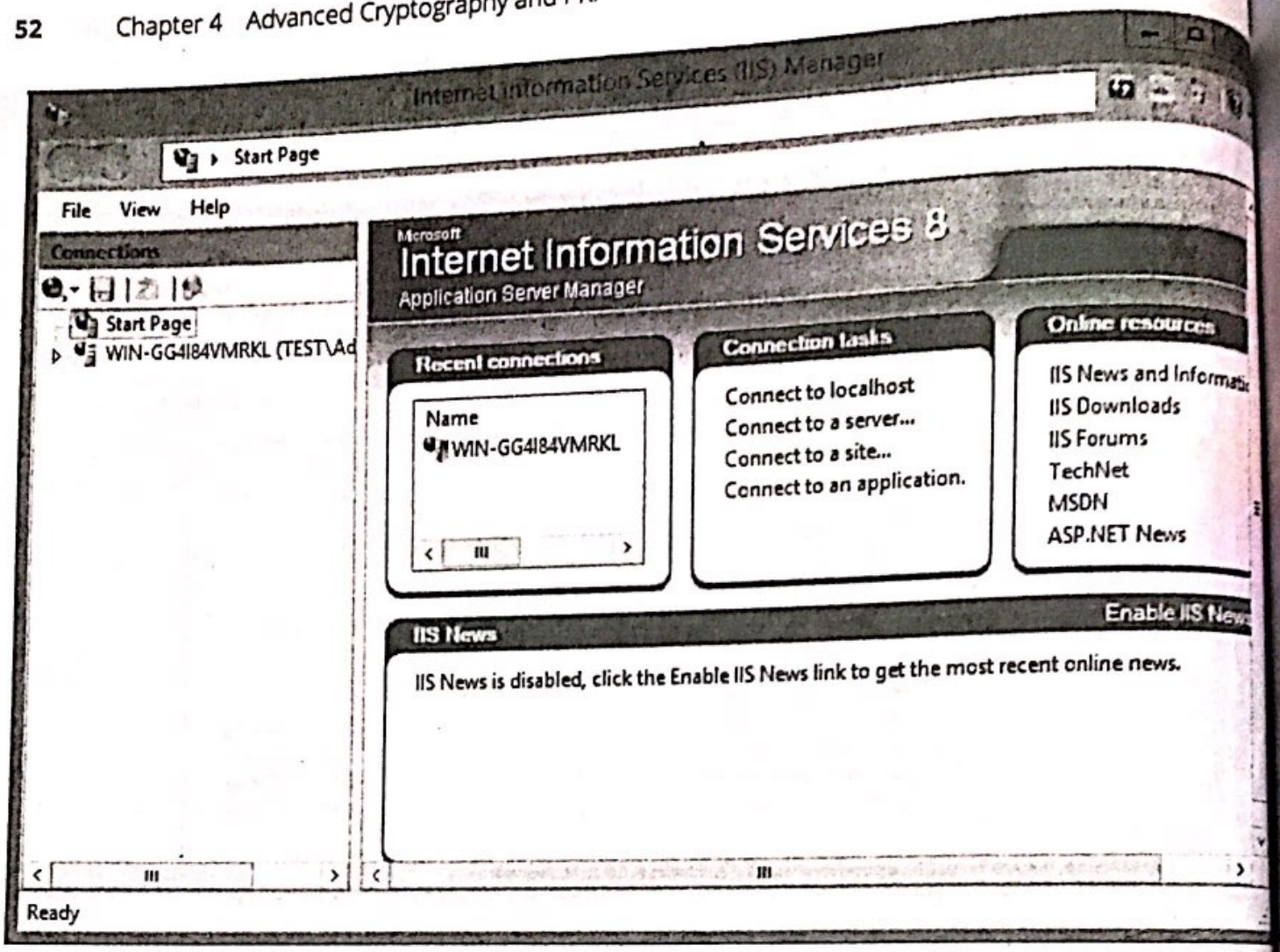

Figure 4-5 IIS Manager
Source: Microsoft LLC

window and double-click the other certificate. What are the purposes of the second certificate? Click **OK** to close the Certificate window.

9. Click **Default Web Site** in the left pane. In the Actions section of the right pane, click **Bindings**. Note that HTTP is already bound to port 80. If HTTPS is not bound, then Click **Add**, set Type to **https** (note that port is set to 443), and in the SSL certificate box, use the drop-down menu to select the certificate that is named with the fully qualified domain name of *ServerName* (see Figure 4-6). Click **OK** and click **Close**.
10. Click **Default Web Site** in the left panel and then scroll down and double-click **SSL Settings**. Now, SSL is available. Select the **Require SSL** check box. Click **Apply** in the Actions pane.
11. Create a domain user account for **Anthony Newman**, with the username **anewman** and the password **Pa$$word**. Double-click Anthony Newman's account and, on the General tab, in the E-mail box, type **anewman@teamx.net** and click **OK**. Note: you may need this account for testing purposes.
12. Close all windows and shut down the VM.

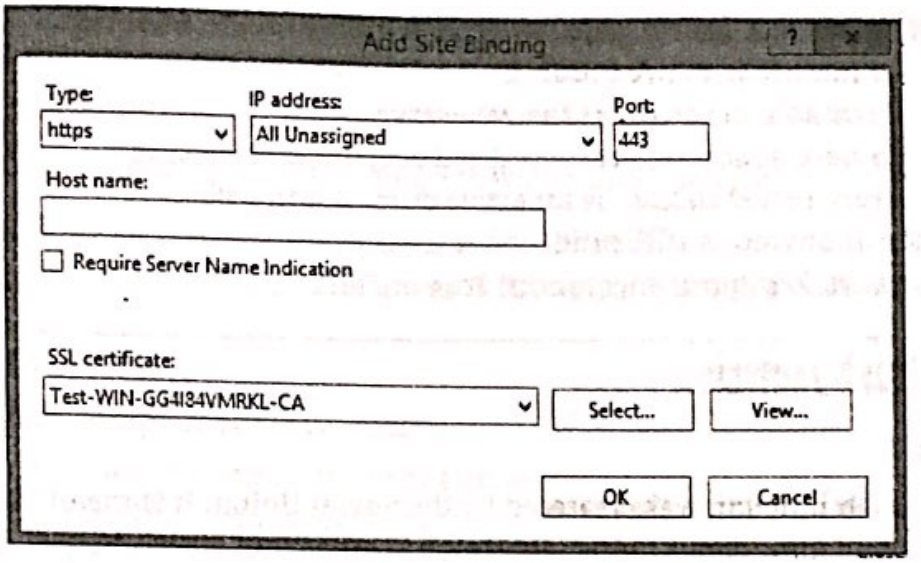

Figure 4-6 HTTPS binding configured
Source: Microsoft LLC

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 1.2 Given a scenario, implement secure protocols.
- 2.3 Given a scenario, troubleshoot common security issues.
- 4.3 Given a scenario, implement identity and access management controls.
- 6.4 Given a scenario, implement public key infrastructure.

Review Questions

1. The most common method of securing e-commerce transmissions is dependent on _____.
   a. the client trusting the entity that digitally signed the web server's certificate
   b. the web server installing its root certificate in the client's certificate store
   c. the web server installing its public key on the client using a cookie
   d. the client and web server exchanging root certificates
2. The default port for HTTPS is _____.
   a. 25
   b. 80
   c. 110
   d. 443
3. In this lab, if SSL was initially not selectable; you could not configure SSL because _____.
   a. the CA had not yet issued an SSL certificate
   b. SSL requires greater than 128-bit encryption
   c. anonymous authentication was permitted
   d. no port had been configured to "listen" for https requests

4. The purpose of enabling Active Domain Services on the server is?
   a. To minimize network traffic
   b. To be able to configure the web server
   c. To have a location for centralized account maintenance
   d. Every server should be an active domain controller.
5. When anonymous authentication is used with IIS, the username and password travers the network without encryption. True or False?

Lab 4.3 GOST Hash Function

Objectives

The GOST hash function was created by the Soviet Union. It is meant to be the standard fo hash functions throughout the Soviet Union. The overall structure of GOST is very closely related to the US DES standard. GOST is an iterative function that produces a 256-bit hash value. The benefit of the iterative process is that it generates a checksum over the entire input message. The GOST function is also often referred to as a block cipher because the iterative process is done in blocks of input streams.

After completing this lab, you will be able to:

- Analyze a hash function
- Evaluate hash functions for their strengths and weaknesses

Materials Required

This lab requires the following:

- Windows 10
- Access to the Internet

Activity

Estimated completion time: **20–30 minutes**

In this lab, you compare and contrast different hashing algorithms.

1. Open Windows 10 and launch your browser.
2. Navigate to **https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf**.
3. Read the article and take notes on the characteristics of the function and how it works. Don't be concerned if you can't understand the entire algorithm; focus on the process, especially inputs and outputs.
4. Per the article, what is a collision attack?
5. Per the article, how does GOST handle collision attacks?
6. Describe the birthday paradox referred to in the article.
7. How can the birthday paradox be used to limit the number of possibilities offered by the hash function?

8. Open another tab in your browser and navigate to **https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf**.
9. Click **Download PDF** in the right panel. Read the article.
10. What similarities can you determine between GOST and DES?
11. Describe any advantages of using one over the other.
12. Why was DES created and where was it first used? Is it still in use today?

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 1.2 Compare and contrast types of attacks.
- 6.1 Compare and contrast basic concepts of cryptography.
- 6.2 Explain cryptography algorithms and their basic characteristics.

Review Questions

1. What is the highest complexity of evaluations that can be handled by the GOST algorithm?
   a. 2^{256}
   b. 2^{128}
   c. 2^{32}
   d. 2^{96}
2. The GOST algorithm produces a _____ bit hash value.
   a. 32
   b. 64
   c. 128
   d. 256
3. GOST is an iterated hash function. True or False?
4. DES is meant to be used on what type of cipher?
   a. Block
   b. Streaming
   c. Segmented
   d. Changing
5. It is possible that a one-way hash function maps pairs of values to the same output. True of False?

Lab 4.4 Configuring Certificate Auto-Enrollment

Objectives

Most users do not care about digital certificates. They use them for encrypting and decrypting files and emails and digitally signing documents only when corporate security policy requires them to do so. For most users, the less they know about security details, the better; they would find the process of manually requesting certificates on a webpage an odious task. Ideally, security measures would be completely transparent to the average user. We are not there yet, but with group policies, users and their computers can be issued certificates,

have them installed, and receive renewed versions when they expire without ever being aware of the process.

In Windows Server 2016, a CA administrator implements certificate auto-enrollment as follows:

a. An auto-enrollment group policy is enabled for users, computers, or both.
b. Either a custom certificate is created or a certificate template is duplicated.
c. Permissions are set on the new template to allow Read, Enroll, and Autoenroll permissions for the Active Directory security group of users or computers that require the certificate.

After completing this lab, you will be able to:

- Configure and implement group policies for auto-enrollment of certificates
- Configure and implement certificates from certificate templates
- Explain how group policies can make the implementation of certificates transparent to users

Materials Required

This lab requires the following:

- Windows 10 with VirtualBox installed
- Windows Server 2016 ISO
- Completion of Lab 4-2

Activity

Estimated completion time: **20–30 minutes**

In this lab, you implement certificate auto-enrollment through group policy, create a digital certificate from a certificate template, issue and install the template on a client, and verify the success of the procedure.

1. Launch the Windows server VM that was created in Lab 4-2.
2. Open the **PKI** console on your desktop. Add the **Group Policy Management** snap-in. The Add or Remove Snap-ins window should now be like Figure 4-7.
3. Create a group policy for auto-enrollment as follows: From the PKI console, expand **Group Policy Management**, expand **Forest: Test.local**, expand **Domains**, expand **Test.local**, right-click **Default Domain Policy**, and click **Edit**. Expand **User Configuration** if necessary, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and click **Public Key Policies**; in the right pane, right-click **Certificate Services Client – Auto-Enrollment** and click **Properties**. On the Enrollment Policy Configuration tab, set the Configuration Model to **Enabled** and place check marks in the boxes to the left of **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**. Your configuration should look like Figure 4-8.
4. Click **OK**. Close the **Group Policy Management Editor**.

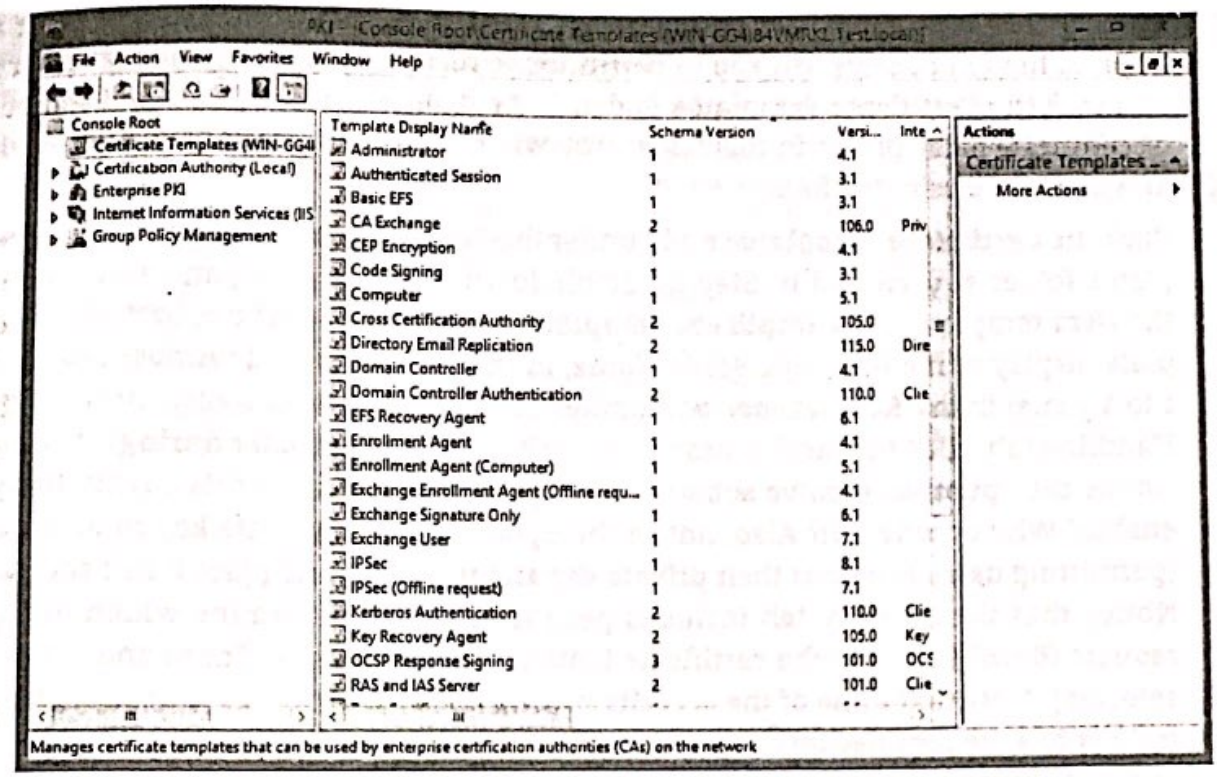

Figure 4-7 Revised PKI Console
Source: Microsoft LLC

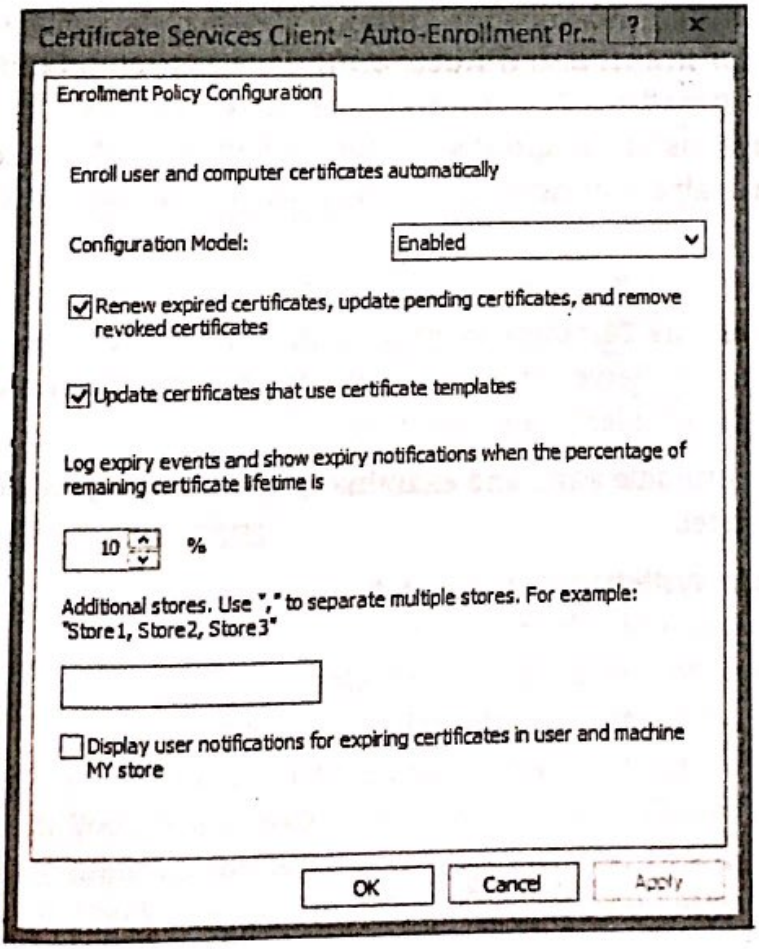

Figure 4-8 Auto-enrollment group policy
Source: Microsoft LLC

5. Make a certificate template available for distribution through auto-enrollment as follows: In the PKI console, expand **Certification Authority (Local)**, expand **ServerName**, and click the **Certificate Templates** folder. To be distributed to users and computers, a certificate must be placed in this folder. You will modify an existing certificate template and then place it in this folder.
6. Click the **Certificate Templates** node under the Console Root (not the Certificate Templates folder you viewed in Step 4). Scroll down in the middle pane and right-click the **User** template. Click **Duplicate Template**. Click the **General** tab, then in the Template display name box, type ServerName; in the Validity period number box, change 1 to **2** years; in the Renewal period number box, change 6 to **12** weeks. In the Request Handling tab, click the radio button to the left of **Prompt the user during enrollment**. Notice the option to Archive subject's encryption private key. Is this a risky setting to enable? Why or why not? Also, notice the option to Allow private key to be exported (permitting users to export their private key and remove it and place it in a safe place). Notice that the Security tab includes permissions that determine which users can request (Enroll) or have the certificate installed automatically (Enroll and Autoenroll selected). Note that none of the security principles listed in the template's access control list has the permissions necessary to enable auto-enrollment: Allow Read, Enroll, and Autoenroll.
7. On the **Security** tab, click the **Add** button; in the Enter the object names to select box, type **Anthony Newman** and click **OK**. In the Group or user names box, select **Anthony Newman**, and in the Permissions for Anthony Newman box, place check marks in the **Allow** column for **Enroll** and **Autoenroll** (leaving the default Allow Read permission enabled). Normally, it is poor administrative practice to assign permissions to individual users instead of groups, but just to demonstrate the auto-enrollment policy function in a lab environment, this user assignment is acceptable. Click **OK**.
8. Return to Certification Authority (Local)/ServerName-CA and right-click **Certificate Templates**. Click **New** and click **Certificate Template to Issue**. In the Enable Certificate Templates window, scroll down and select ServerName and click **OK**. The new certificate now appears in the Certificate Templates folder (see Figure 4-9).
9. Double-click **ServerName** in the middle pane and examine the purposes for which the certificate can be used. Click **Cancel**.
10. Close all windows and log off the systems.

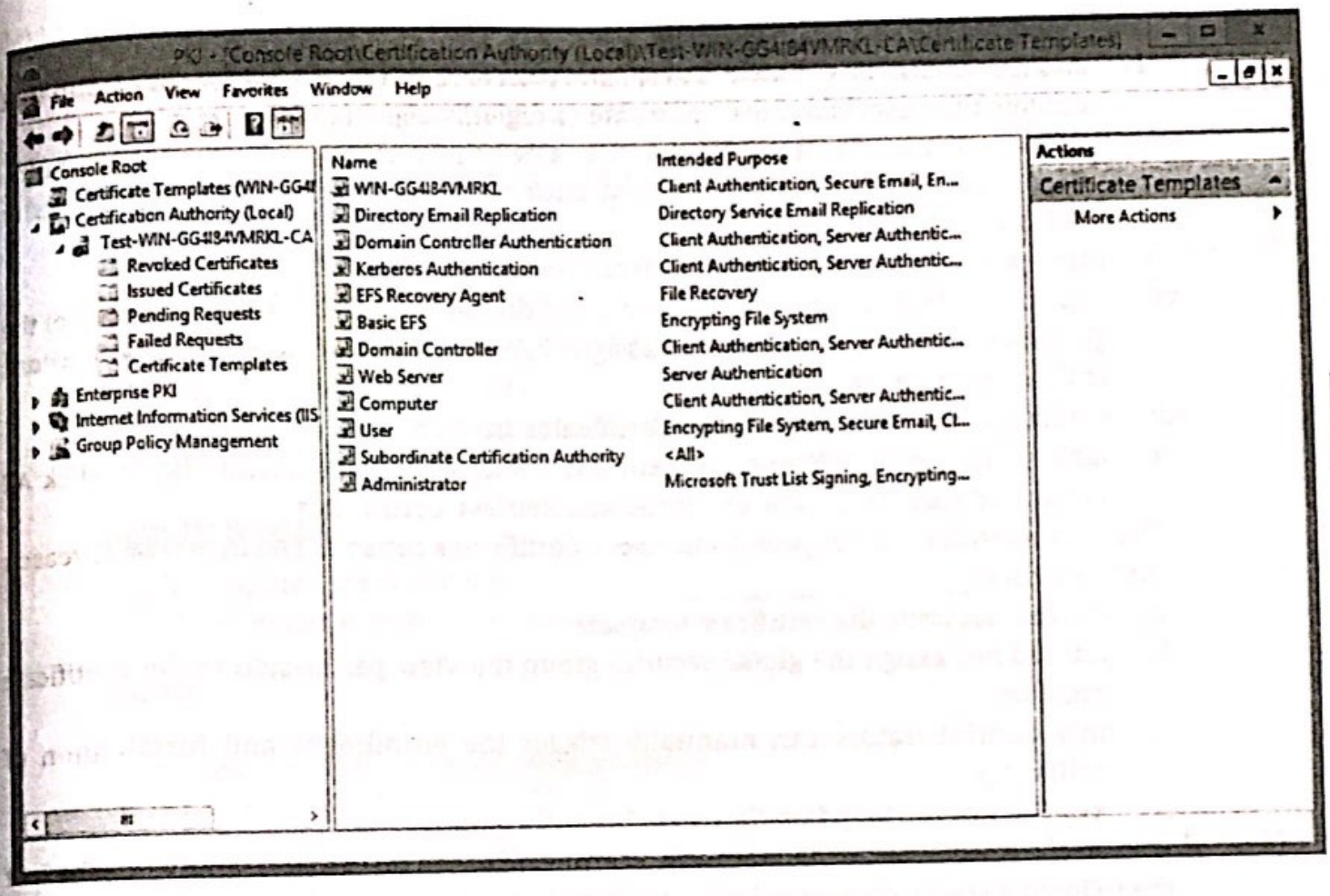

Figure 4-9 New Certificate Template
Source: Microsoft LLC

4

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 1.2 Given a scenario, implement secure protocols.
- 2.3 Given a scenario, troubleshoot common security issues.
- 4.3 Given a scenario, implement identity and access management controls.
- 6.4 Given a scenario, implement public key infrastructure.

Review Questions

1. Which of the following is considered a best practice in the handling of EFS certificates?
   a. Users should export their public keys and store them in a safe place.
   b. Recovery agents should export their private keys and store them in a safe place.
   c. Users should export their symmetric keys and store them in a safe place.
   d. EFS key pairs should always be encrypted.
2. You are a network administrator of a Windows Server 2016 domain tasked with implementing the auto-enrollment of user certificates, which will be used to digitally sign emails. You perform the following procedures:
   i. Install an enterprise root CA.
   ii. Choose a certificate template that allows users to digitally sign emails.

iii. Duplicate the certificate template.
iv. Assign permissions of Read, Enroll, and Autoenroll to the global security group that contains the users who need to be able to digitally sign emails.
v. Edit the Default Domain Policy and enable the Certificate Services Client Auto-Enrollment policy in User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies.
vi. Run gpupdate /force on the domain controller.
vii. Log on to a domain workstation with a test domain account that is a member of the global security group to which you assigned Read, Enroll, and Autoenroll permissions to the certificate template.
viii. Create an mmc that contains the Certificates snap-in.
ix. Right-click the Certificates—Current User node under the Console Root, click All Tasks, and click Automatically Enroll and Retrieve Certificates.

The certificate does not appear in the user's Certificates console. The most likely reason for this is that _____.

a. you did not issue the certificate template
b. you did not assign the global security group the View permission to the certificate template
c. only administrators can manually trigger the enrollment and installation of certificates
d. you did not run gpupdate /force on the workstation

3. In Lab 4.4, Anthony Newman received a certificate based on the User template. Which of the following statements regarding these certificates is correct? (Choose all that apply.)
   a. Both certificates allow Anthony Newman to use the Encrypting File System.
   b. Once a User certificate is issued to a user, the best practice is to revoke the user's EFS certificate.
   c. The User certificate contains three different private keys, one for each of the three purposes of the certificate.
   d. Both certificates were issued by *ServerName*.
4. In this lab, the auto-enrollment policy was configured so that all domain users could receive the certificate based on the User certificate template. True or False?
5. Anthony used the certificate he received in Lab 4.4 to place his digital signature on an email to a customer named Helene Grimaud. For Helene to be sure that the email came from Anthony, she must _____.
   a. trust ServerName
   b. install Anthony's certificate
   c. compare the thumbprint on Anthony's certificate with the result of her own hashing of his certificate
   d. send Anthony her certificate

Lab 5.1 Getting Started with Kali Linux

Objectives

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.

After completing this lab, you will be able to:

- Load and configure Kali Linux in a VMware share
- Configure network connectivity on Kali Linux

Materials Required

This lab requires the following:

- Kali Linux ISO
- Windows 10 with VirtualBox installed

Activity

Estimated completion time: **20–30 minutes**

Note

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

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

1. If you do not yet have a Kali Linux ISO, open your web browser, enter **www.kali.orgdownloads/**, and click the **Kali Linux 64 bit ISO** button.

Note

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

2. 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.

Note

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

3. Launch Oracle VM VirtualBox software and click **New.**
4. In the Name textbox use the name **Kali Linux.**
5. Type **Linux.**
6. Version is **Linux 2.6/3.x/4.x (xx-bit).**
7. Click **Next.**
8. Leave the Memory as the default amount and click **Next.**
9. Choose **Create a virtual hard disk now** and click **Create.**
10. Select **VDI (VirtualBox Disk Image)** and click **Next.**
11. Select **Dynamically allocated** and click **Next.**
12. Set the **File location as size** to at least 25GB and click **Create.**
13. Select the **Kali Linux** and click **Start.**
14. 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.**

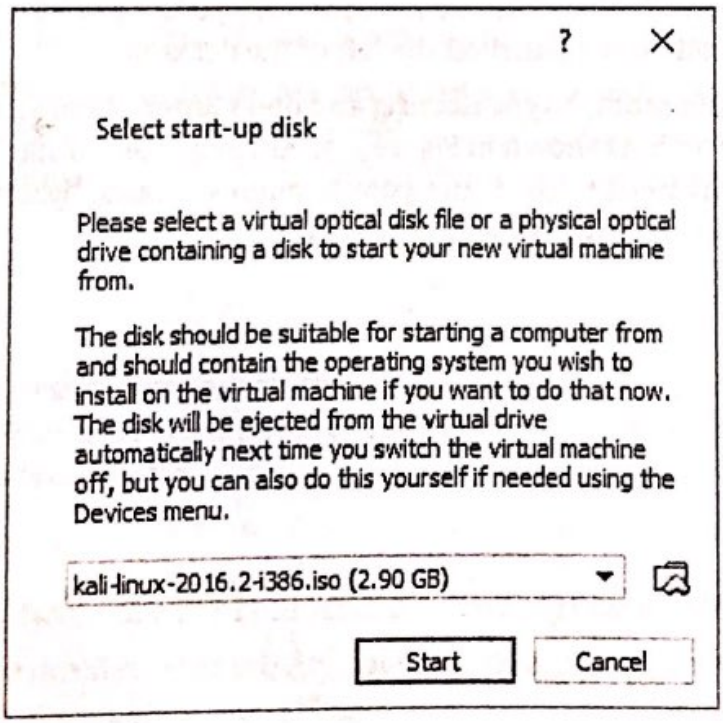

Figure 5-1 Virtual Machine start-up disk
Source: Oracle VirtualBox

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

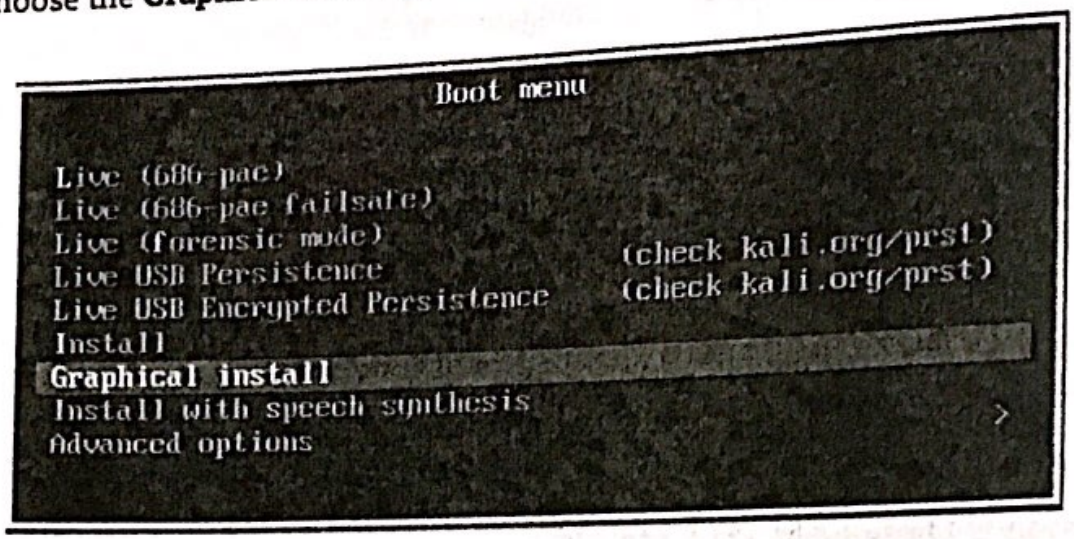

Figure 5-2 Selecting graphical Install
Source: Oracle VirtualBox

16. 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**.
17. When asked to partition disks, select **Yes** and click **Continue**.
18. When asked to configure the package manager, select **No** and click **Continue**.
19. 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.
20. Enter **root** for the user name and **admin** for the password.
21. 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.
22. 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.

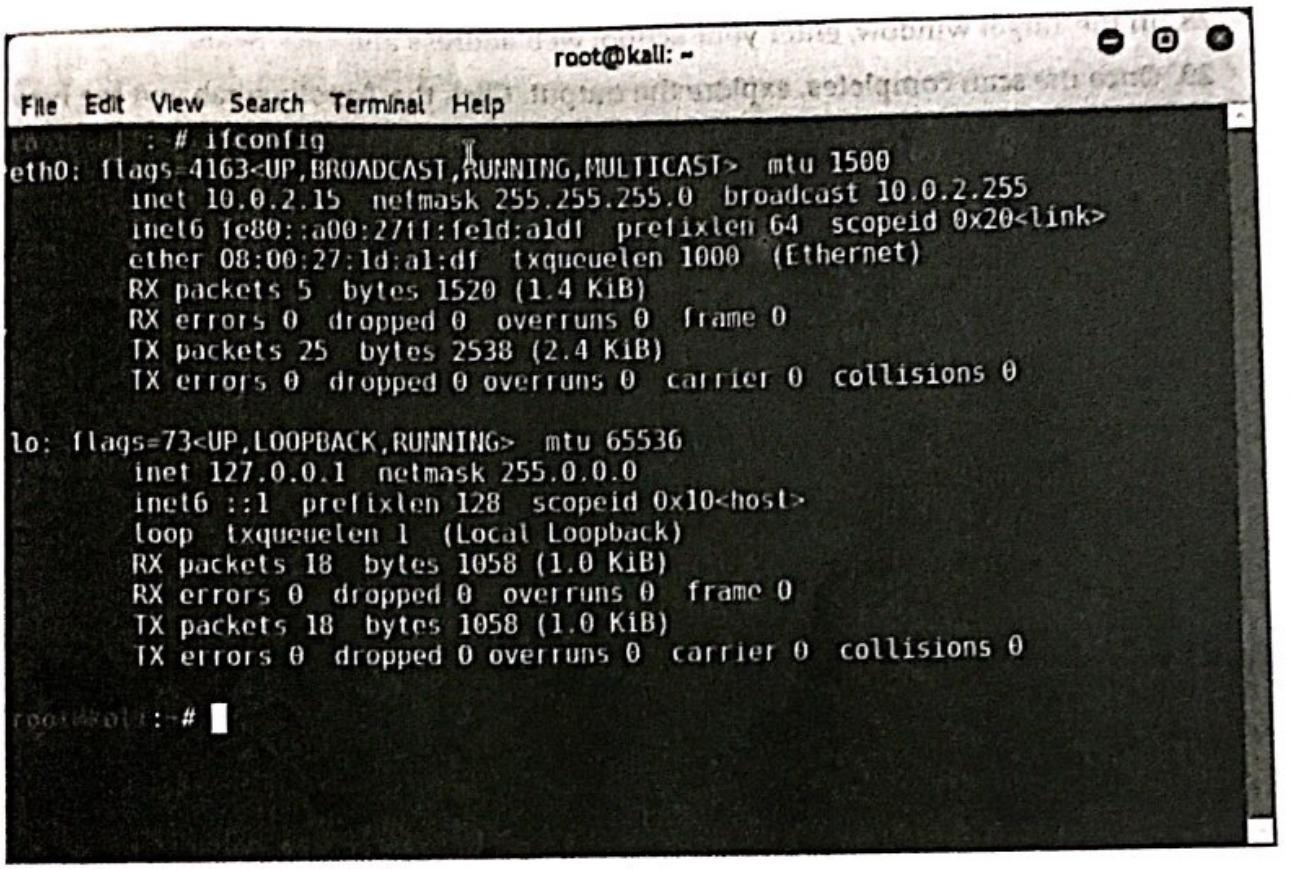

Figure 5-3 Network Configuration — Ifconfig
Source: Kali Linux

23. 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.
24. 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.

Note

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.

25. On Kali Linux, from the command prompt, type **ping www.yahoo.com** and press **Enter.**
26. Once you have verified connectivity between Kali Linux and the Internet, spend some time exploring the Kali Linux interface.
27. Launch the ZenMap application from the Applications/Information Gathering menu.

28. In the Target window, enter your school web address and click **Scan.**
29. 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.
30. On the Nmap Output tab check for any vulnerabilities.
31. Log off all systems.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 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.

Review Questions

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

Lab 5.2 IP Spoofing with Hping3

Objectives

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. After completing this lab, you will be able to:

- Explain some of the packet crafting options in hping3
- Use hping3 to probe a remote system
- Use hping3 to spoof an IP address

Materials Required

This lab requires the following:

- Kali Linux ISO
- Windows 10 with VirtualBox installed
- Windows 10 ISO
- Completion of Lab 4.1

Activity

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*.

Note

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.

1. 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**.

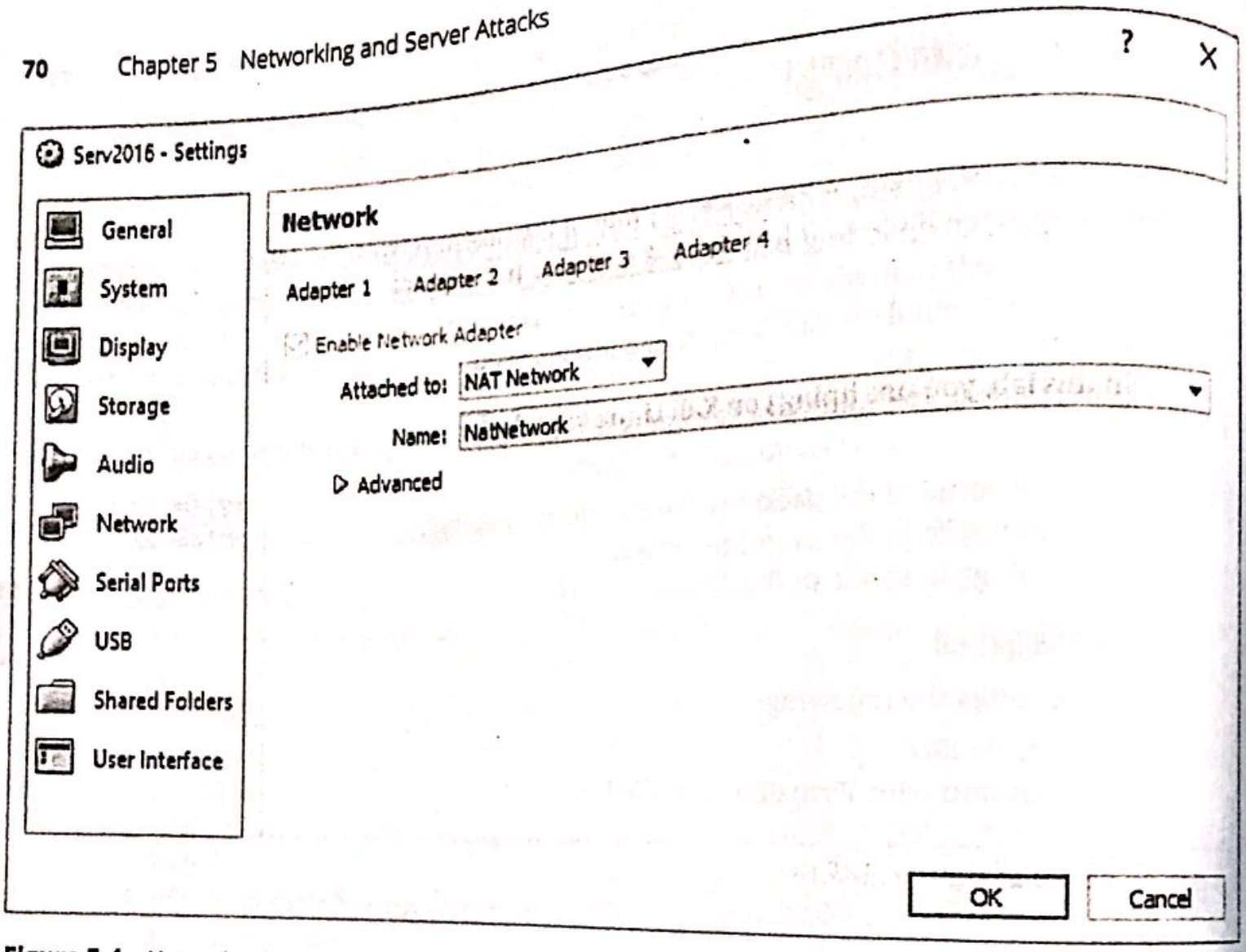

Figure 5-4 Network Selection
Source: Oracle VirtualBox

2. Repeat the steps for the Kali Linux VM you created in Lab 5.1.
3. 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**.
4. 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.

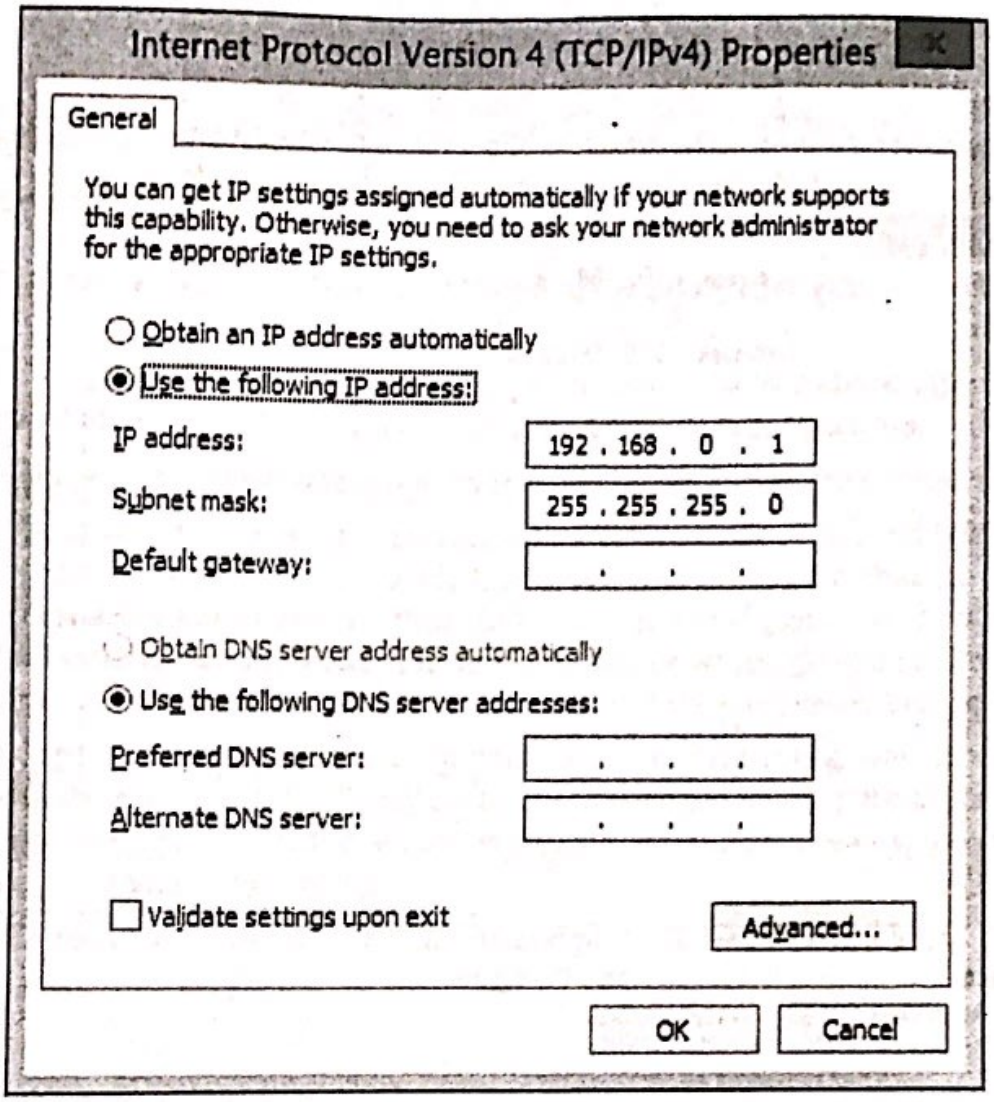

Figure 5-5 Internet Protocol Version 4 Dialog box
Source: Microsoft LLC

5. Create a new Windows 10 VM with the ISO. Accept all the defaults.
6. 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**.
7. Click **Change adapters settings**.
8. Right-click **Ethernet** and select **Properties**.
9. 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.
10. 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**.
11. 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.
12. Click **Apply**. Close all windows until you are at the desktop.

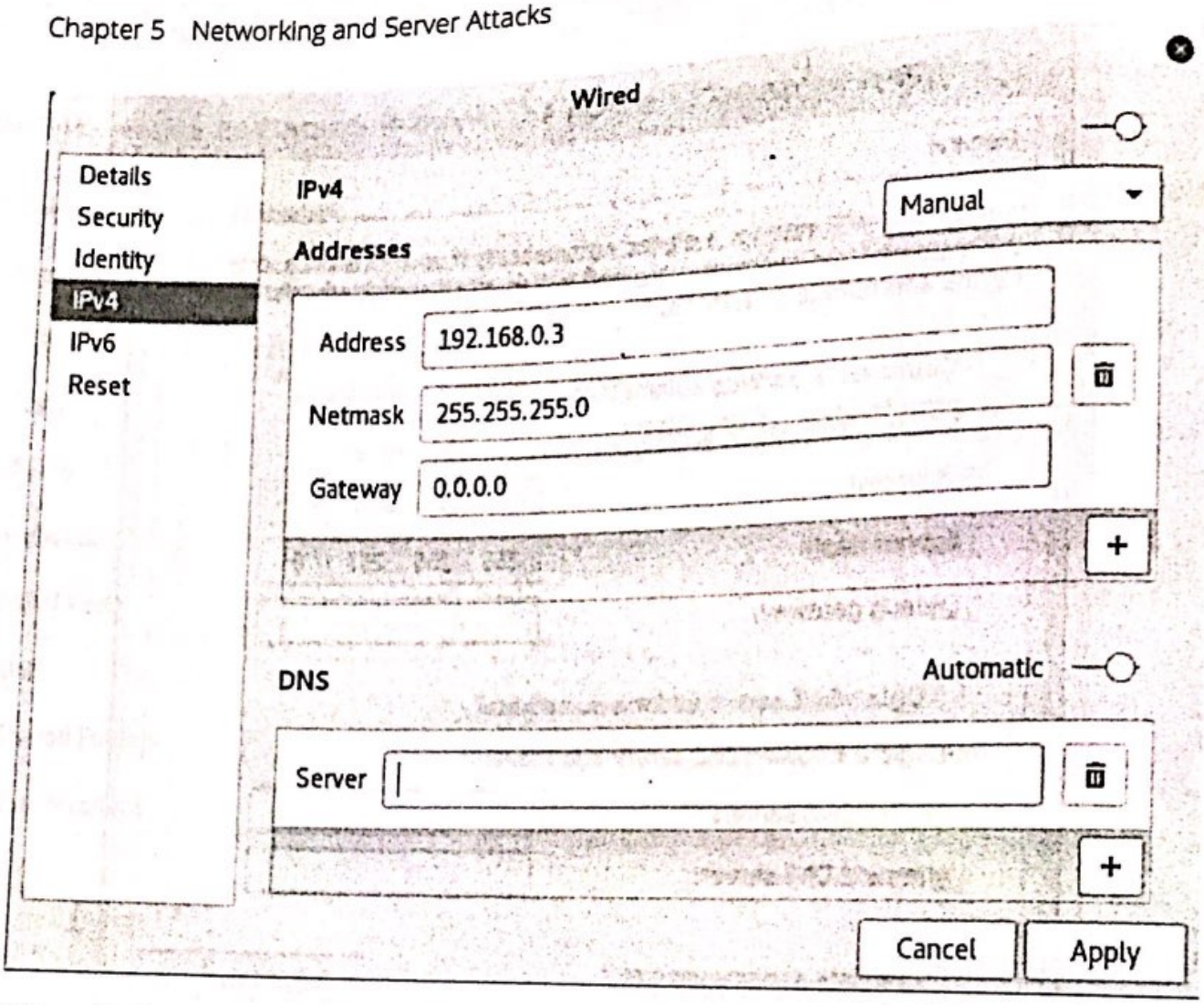

Figure 5-6 Internet Protocol Version 4 Dialog box
Source: Kali Linux

13. 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.
14. In the Kali Linux VM, click the **Terminal button**. At the command prompt, type **wireshark** and press **Enter**.
15. Wireshark displays a warning about running the program as the root user (Linux administrator). Click **OK**.
16. 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*.
17. Open a terminal window. At the command prompt, type **hping3 –s *ipAddress*** and press **Enter**, replacing *ipAddress* with the IP address of *Windows Server*.

Note

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

18. In the Capture area of the Welcome to Wireshark window, click **etho,** then click **Capture/ Start.**
19. 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.**
20. On the terminal window, where hping3 is still running, press **Ctrl+c** to stop hping3.
21. 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.
22. 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).
23. Go to the command prompt in Kali Linux and press **Ctrl+c** to stop hping3.

Note

You may want to keep Kali Linux running while you answer the Review Questions.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 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.

Review Questions

1. 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?
2. 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?

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

Lab 5.3 ARP Poisoning

Objectives

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.

After completing this lab, you will be able to:

- Discuss some of the capabilities of ettercap
- Use ettercap to perform ARP poisoning

Materials Required

This lab requires the following:

- Windows 10 With VirtualBox installed
- Windows Server 2016
- Completion of Lab 4.1
- Completion of Lab 5.1
- Completion of Lab 5.2

Activity

Estimated completion time: **40 minutes**

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

1. Launch the Kali Linux VM and configure network connectivity as described in Lab 5.1. Click the **Terminal button** icon 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.

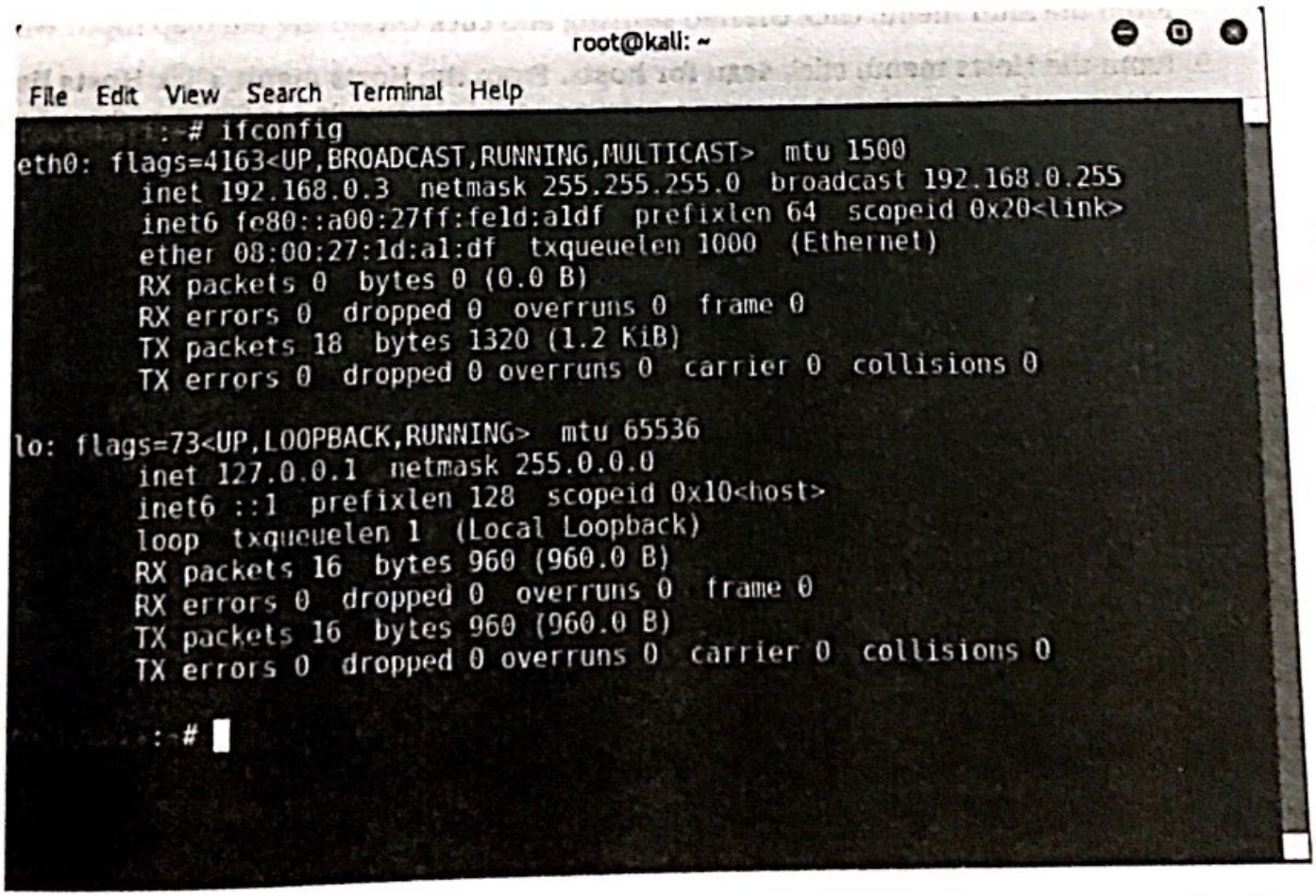

Figure 5-7 Network Configuration — Ifconfig

Source: Kali Linux

2. 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**.
3. On *Windows Server*, from a command prompt, type **ping *Windows10VMIPaddress*** (where *Win10IPaddress* is the Windows 10 IP address) and press **Enter**.
4. 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.
5. 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.
6. On *Windows Server*, repeat the ping from Step 3 of this lab.
7. Return to Kali Linux and stop the Wireshark capture. You will not see evidence of the pings between *Server* and *Windows 10 VM*.
8. 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.
9. 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.

Note

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.

10. 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**.
11. 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.
12. 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.

13. 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*.
14. 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.
15. Close all windows and log off.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 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.

Review Questions

1. Which of the following attacks is available on ettercap? (Choose all that apply.)
   a. ICMP redirection
   b. Buffer overflow
   c. Port stealing
   d. DHCP spoofing
2. Why did you not see evidence of the pings between *Windows Server* and *Windows 10 VM* in Step 7 of this lab?
3. Why did you see evidence of the pings between *Windows Server* and *Windows 10 VM* in Step 13 of this lab?
4. The ettercap log analyzer can handle only uncompressed logfiles. True or False?
5. The configuration file for ettercap is _____.
   a. /bin/cfg/etter.c
   b. /etc/ettercap/etter.conf
   c. /local/bin/help/ettercap.txt
   d. /etc/ettercap/conf

Lab 5.4 Man-in-the-Middle Attack

Objectives

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.

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.

After completing this lab, you will be able to:

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

Materials Required

This lab requires the following:

- Completion of Lab 4.1
- Windows 10 with VirtualBox installed
- Kali Linux VM

Activity

Estimated completion time: **10 minutes**

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. 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. 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.

Note

Making both VMs on a NAT network resolves this issue most of the time.

3. 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.
4. From the **Hosts** menu, click **Scan for hosts**. From the **Hosts** menu, click **Hosts list**.

5. 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**.
6. From the **Start** menu, click **Start sniffing**.
7. From the **Mitm** menu, click **Arp poisoning**. In the MITM Attack: ARP Poisoning window, select the **Sniff remote connections** checkbox and click **OK**.
8. From the **Plugins** menu, click **Manage the plugins**. Scroll down and double-click the plugin named **remote_browser**.
9. On *Windows Server*, open your web browser. In the address window, type **www.google.com** and press **Enter**. The website appears. Notice what happens in the lower frame of the ettercap window.
10. Close ettercap.
11. On *Windows Server*, enter **www.yahoo.com** in your browser's address window and press **Enter**. Notice that the website does not appear.
12. Open a command prompt, type **arp -d *** and then press **Enter**.
13. Return to your web browser and enter **www.yahoo.com** in your browser's address window, and then press **Enter**. Notice that the website now appears.
14. You may want to leave your systems running and use the *arp* command and Wireshark as you answer the Review Questions.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 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.

Review Questions

1. Why did the website not appear in Step 11 of this lab? Please be specific.
2. Why did the website appear in Step 13 of this lab? Please be specific.
3. During the man-in-the-middle attack in this lab, _____. (Choose all that apply.)
   a. an analysis of the network layer headers would indicate that *Server* was communicating directly with the Internet
   b. an analysis of the data-link layer headers would indicate that *Server* was communicating directly with Kali Linux
   c. an analysis of the network layer headers would indicate that *Server* was communicating directly with Kali Linux
   d. an analysis of the data-link layer headers would indicate that *Server* was communicating directly with the Internet

4. Which of the following attacks is supported by ettercap? (Choose all that apply.)
   a. SQL injection
   b. DNS spoofing
   c. DOS attack
   d. Zero-day attack
5. Which of the following actions could limit ARP poisoning as performed in this lab?
   a. Static IP addressing
   b. Dynamic IP addressing
   c. Static ARP tables
   d. Dynamic ARP tables

Lab 9.1 Verifying the Integrity of the Hosts File

Objectives

When computers were first connected by transmission media, there were very few computers to connect. Networking protocol stacks, such as TCP/IP, were just being developed, and only a few computers, mostly at universities, were connected. There was no need for the Domain Name System (DNS), which is the massive, distributed, worldwide database of computer addresses that we use now. Early networked computers did need the ability to find each other, and some sort of address directory was needed. The TCP/IP solution was to create a text file that contained the name and address of each computer on the network. This file, called hosts, was copied to all the networked computers. If a new computer was added (which was not a common event), a letter was sent or a phone call was made, letting the computer scientists know the changes they should make to the hosts file.

The hosts file is still used today. The file can contain the IP addresses of computers as well as their fully qualified domain names (for example, 172.31.157.33 server01.compcol.net). In fact, most systems have nothing more than the local loopback address listed in the hosts file. We have the DNS system of distributed databases, and the millions of computers on the Internet query these DNS servers to find out a system's IP address. Note, however, that these DNS queries can take up a lot of network bandwidth. This is why some administrators still use the hosts file. When a client tries to resolve a fully qualified domain name (FQDN), such as server01.compcol.net, to its IP address, such as 172.31.157.33, the first thing the client does is determine if its own FQDN is server01.compcol.net. When this query comes back negative, instead of querying its DNS server right away, the client checks its own hosts file. If server01.compcol.net is a system that an organization's users access frequently, the network administrator might have entered server01's resolution information in the hosts files of all workstations in the company so that the network bandwidth isn't used unnecessarily in querying the DNS server.

However, the hosts file is a vulnerability. If an attacker modified a client's hosts file so that the attacker's server address was listed instead of the real IP address, the client would be redirected to the fake server. Obviously, this would be a serious security breach. Thus, it is important for network security personnel to know when the hosts file, or any other important system file, changes without authorization. Intrusion detection techniques usually monitor this kind of activity, and in this lab, you learn the technique used by some IDS systems—a cryptographic technique called hashing—to monitor the validity and integrity of system files.

After completing this lab, you will be able to:

- Detect changes to a system file using hashing
- Explain the mechanism used by intrusion detection systems to monitor unauthorized changes to system files

Materials Required

This lab requires the following:

- Windows Server 2016 or Windows 10 VM

Activity

Estimated completion time: **15–20 minutes**

In this lab, you download a cryptographic hashing tool and test the integrity of your hosts file before and after its modification.

1. Log on to either Windows 10 VM or Windows Server with an administrative account, open your web browser, and go to **https://github.com/jessek/hashdeep/releases/tag/release-4.4.**

   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 "md5deep."

2. Scroll down and click the **md5deep-4.4.zip** link.
3. Internet Explorer may block the file download and display a message bar on top of the webpage. If so, click this bar and click **Download File**. On the File Download window, click **Save**, and in the Save As window, save the file to your desktop.
4. Close the Download complete window and close your web browser.
5. Double-click the **md5deep-4.4** archive file on your desktop. In the md5deep window, click **Extract.** Then click **Extract all files**, and in the Extract Compressed (Zipped) Folders window, click the **Browse** button and navigate to **Local Disk (C:)**. Click **OK** in the Select a destination window, and click **Extract.**
6. For ease in navigation from the command prompt, rename the md5deep-4.4 folder to **md5.**
7. Open **Notepad**. From the File menu, click **Open** and navigate to **C:\Windows\System32\drivers\etc.** In the drop-down box that says Text Documents (*.txt), change the setting to **All Files.** Open the **hosts** file. (See Figure 9-1.)

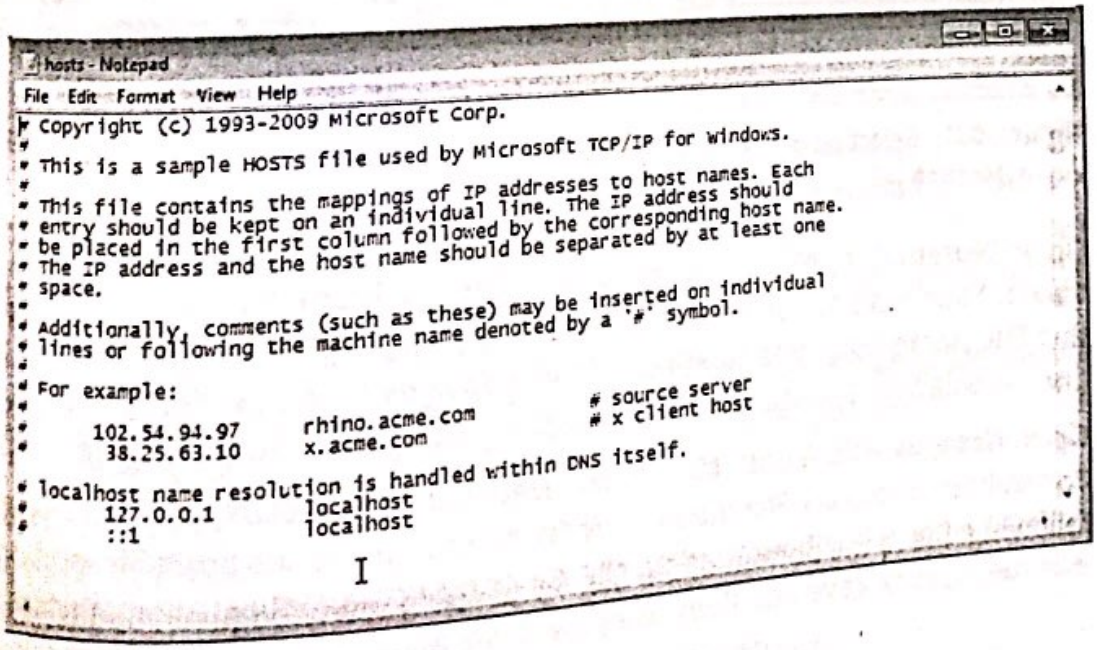

Figure 9-1 The hosts file

Source: Microsoft LLC

8. Note that the first lines are preceded by the # sign. This symbol tells the operating system to disregard the lines. These lines are remarks for the user to read and are said to have been "rem'ed out" (remarked out). Your hosts should be similar to those shown in Figure 9-1. The last two lines provide the system's IPv4 and IPv6 loopback addresses, which tell the system how to refer to itself. Note that on Windows 10 VM and Windows Server these last two lines are rem'ed out.
9. Close the hosts file. Click **Start**, type **cmd**, and press **Enter.**
10. At the command prompt, type **cd C:\md5** to navigate to the md5 directory and then type **dir** and press **Enter.**
11. Notice that several files have an .exe extension. These allow you to hash files using different hashing algorithms.
12. At the command prompt, type **sha256deep C:\Windows\System32\Drivers\etc\hosts** and press **Enter.**
13. Highlight and copy the hash to the clipboard (see Figure 9-2).

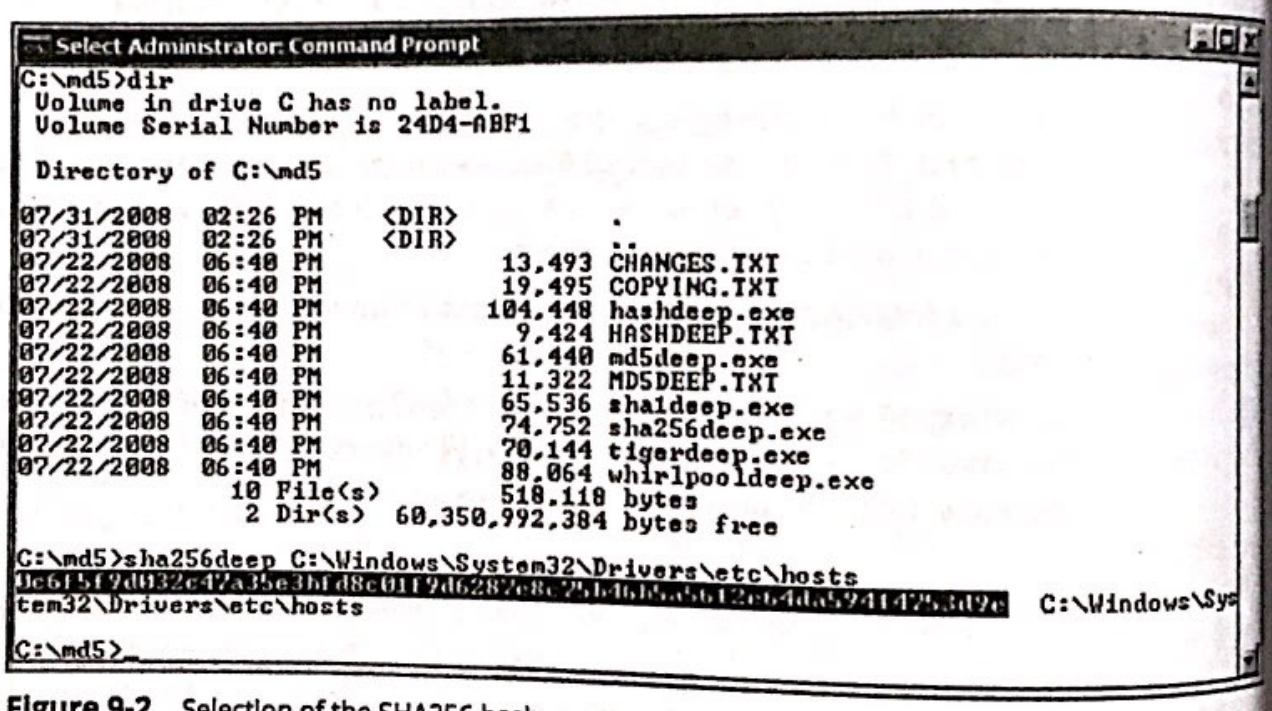

Figure 9-2 Selection of the SHA256 hash
Source: Microsoft LLC

14. Open **Notepad**, right-click anywhere inside the blank Notepad document, and select **Paste**. Your hash of the hosts file should appear. From the File menu, click **Save As**. In the File name box, type **hosthash**. In the *Save as type* box, verify that Text Documents (.txt) is selected. Navigate to your desktop, click **Save**, and then close the file.
15. Open **Notepad** with Administrative privileges and, if necessary, click **Yes** in the User Account Control box. From the File menu, click **Open**, navigate to the hosts file, and open it. Add the following line to the bottom of the file: **69.32.133.79 www.boguswebaddress.net**. From the File menu, click **Save** and then close the hosts file.

16. Repeat Steps 13 and 14, and then open **hosthash.txt** and paste the second hash in the file. Compare the two hashes. Do the two hashes look similar? If this process were automated for all system files, it would be easy to tell when a file has been altered.
17. Open your web browser and go to **www.boguswebaddress.net**. Explain the results.
18. Close all windows and log off.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 2.6 Given a scenario, implement secure protocols.
- 6.0 Compare and contrast basic concepts of cryptography.
- 6.2 Explain cryptography algorithms and their basic characteristics.

Review Questions

1. What is the DNS record type for an IPv6 address?
   a. A
   b. AA
   c. AAAA
   d. AV6
2. What is the IPv6 loopback address?
   a. 0.0.0.0
   b. 127.0.0.1
   c. 255.255.255.255
   d. ::1
3. How many hexadecimal characters are needed to express 256 bits?
   a. 16
   b. 32
   c. 64
   d. 128
4. Which of the following statements regarding hashes is true?
   a. When a 200 MB file that has been previously hashed has one byte changed, a second hash of the file will be nearly similar to the first hash.
   b. When a 200 MB file that has been previously hashed has one byte changed, a second hash will be more similar to the first if SHA1 were used than if SHA256 were used.
   c. When a 200 MB file that has been previously hashed has one byte changed, a second hash of the file will be much less similar to the first hash than would be the case if the file had only been 200 KB in size.
   d. When a file of any size is modified, there is no relationship between the pre- and post-modification hashes and the number of bytes modified.
5. Hashing is a useful tool in _____.
   a. intrusion detection
   b. maintaining data availability
   c. prevention of unauthorized file modification
   d. the development of secure cryptographic algorithms

Lab 9.2 Installing the FTP Server Service and Wireshark

Objectives

The most common way to maintain the confidentiality of data in transit is to use encryption. The assumption is that even if an attacker were to capture (sniff) the traffic, the expense and time required to decrypt the data without the decryption key would be prohibitive. On the other hand, traffic that is not encrypted is readily available to anyone with access to the network medium and a protocol analyzer. With the growing number of wireless networks, it is very easy to get access to the network medium; it is in the air. At a café with wireless Internet access or in the parking lot outside an office building, wireless transmissions may be captured and analyzed by relatively unsophisticated attackers. Many people transmit their logon credentials "in the clear"—that is, unencrypted (usually called plaintext)—without being aware of it. Generally speaking, when you open your email client to check your email, your username and password for your mail server account are transmitted unencrypted. This is true of many DSL connections, too.

One of the most notable networking protocols that does not encrypt data in transit is FTP (File Transfer Protocol). FTP is commonly used on the Internet to transfer files. You have probably used it many times when you have downloaded software. In this lab, you install an FTP server and a protocol analyzer.

After completing this lab, you will be able to:

- Install and configure the FTP service on Windows Server 2016
- Install and configure the protocol analyzer Wireshark

Materials Required

This lab requires the following:

- Completion of Lab 4.1
- Windows 10 VM

Activity

Estimated completion time: **20–30 minutes**

In this lab, you install and configure an FTP server on Windows Server 2016 and download and install the protocol analyzer Wireshark.

1. Log on to Windows Server as **Administrator**.
2. If necessary, click the **Server Manager** icon on the task bar.
3. Click **Manage**, then click **Add Roles and Features**, and click **Next** at the Before You Begin window. In the Installation Type window, click **Next**. In the Server Selection window, click **Next**.
4. In the Server Roles window, place a check mark in the box to the left of **Web Server (IIS)**, and in the Add Roles and Features wizard, click **Add Features**.

5. Click **Next** three times, and in the Role Services window, scroll down and expand the **FTP Server**, and place a check mark in the **FTP Service** check box.
6. Click **Next.**
7. Click **Install.**
8. When the installation has completed, click **Close** in the Roles and Features Wizard dialog box.
9. In Server Manager, click **Tools**, then click **Internet Information Services (IIS) Manager.** If necessary, click **No** in the Internet Information Services (IIS) Manager dialog box.
10. You must configure your IIS server to handle FTP protocols. In the Server Manager Dashboard, click **Add roles and features.**
11. If the Before you begin page of Add Roles and Features Wizard is displayed, click **Next.**
12. On the Select installation type page, select **Role-based or feature-based installation,** and click **Next.**
13. On the Select destination server page, click **Select a server from the server pool,** select your server from the Server Pool list, and then click **Next.**
14. On the Select server roles page, expand the **Web Server (IIS)** node, and then expand the **FTP Server** node.
15. If necessary, select the **FTP Server check box** and the **FTP Service check box,** and then click **Next.**
16. If necessary, on the Select features page, click **Next.**
17. If necessary, on the Confirm installation selections page, click **Install.**
18. On the Windows server, create a folder named **FTP Data** on the C: drive. Within that folder, create a file called **Credentials.txt** that contains your name and the current date.
19. Open the IIS Manager dialog box and expand the **Windows Server** node. Right click the **Sites** node and select **Add FTP site.**
20. n the FTP site name text box, enter **FTP Data**. In the Physical Path, navigate to the FTP Data folder you created in step 19. Click **Next.**
21. Notice in the Bindings and SSL Settings window that the FTP server will be listening for requests for FTP service at TCP port 21, the standard FTP control port. In the IP Address drop down, select the server's IP address. Select the **No SSL** option and click **Next.**
22. Select **Basic** and **Anonymous** in the Authentication area.
23. In the Authorization area, select **All users** from the dropdown and verify that Permissions are set to both Read and Write. Click **Finish.**
24. In the search box type **wf.msc** to open Windows Firewall. Turn off the firewall for Domain, Private, and Public. Click **Apply** and then **OK.**

Note

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 "Wireshark."

25. Log on to Windows 10 VM with an administrative account.
26. Open your web browser and go to **www.wireshark.org**.
27. Click the **Download—Get Started Now** button. On the Download Wireshark page, click **Windows Installer (*XX*-bit)** where *XX* is the numbers of bits for your version of the OS. In the File Download window, click **Save** and save the file to your desktop.
28. In the Download complete window, click **Run**, and if you receive a warning stating that the publisher could not be verified, click **Run** again. If necessary, click **Yes** on the User Account Control Dialog.
29. Click **Next** on the Welcome to the Wireshark Setup Wizard page, click **I Agree** at the License Agreement page, accept the default components on the Choose Components page, and click **Next**. Accept the default settings on the Select Additional Tasks page and click **Next**, accept the default Destination Folder and click **Next**, and then accept the default settings on the Install WinPcap page and click **Install**.
30. Click **Next** at the Welcome to the WinPcap Setup Wizard page, click **Next** again, and then click **I Agree** at the License Agreement page.
31. Click **Install**, click **Finish** at the Completing the WinPCap Setup Wizard, click **Next**, and then click **Finish** on the final page.
32. Close all windows and log off.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 2.6 Given a scenario, implement secure protocols.
- 3.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guide.

Review Questions

1. Your Windows Server 2106 is named servero2.acme.com. It is running the FTP server service. While reviewing the FTP logs, you notice entries indicating that a user named IUSR_SERVERo2 has been logging on and accessing the FTP directory. What is the significance of these log entries?
   a. Anonymous access is permitted by your FTP server.
   b. Users from the Internet have accessed your FTP server.
   c. Log maintenance has been performed by the IUSR service.
   d. It is likely that your system has been attacked.

2. Which of the following is a capture file format that can be read by Wireshark? (Choose all that apply.)
   a. Microsoft Network Monitor captures
   b. Cisco Secure Ingress Log output
   c. Novell LANalyzer captures
   d. tcpdump
3. Which of the following statements best describes the function of WinPcap?
   a. WinPcap provides the logging functions for Wireshark.
   b. WinPcap allows applications to capture and transmit network packets bypassing the protocol stack.
   c. WinPcap is a device driver that allows applications to communicate with the Windows operating system.
   d. WinPcap adds functionality to Wireshark, including skins, fonts, extended color depth, and advanced rendering.
4. In a Windows Server 2106 FTP server, configuration options in the FTP site's Properties/Directory Security permit administrators to block specific computers from connecting with the FTP server based on the client's IP address or NetBIOS name. True or False?
5. You have decided to track user activity on your Windows Server 2106 FTP server by storing your FTP log file information on a Microsoft Access database. What would be the most sensible choice of formats in which to save your FTP log files?
   a. W3C Extended Log File Format
   b. ODBC logging
   c. Microsoft IIS Log File Format
   d. Comma Separated Value Format

Lab 9.3 Capturing and Analyzing FTP Traffic

Objectives

FTP is a commonly used protocol. On some websites from which software can be downloaded, users are given the option of using HTTP or FTP as the download protocol. On others, the user is automatically switched to FTP to receive the download. Most web browsers allow the use of HTTP or FTP in the address bar. For example, if you wanted to connect to an FTP server called ftp.acme.com, you could type the following in the web browser address bar: ftp://ftp.acme.com. Note that it is the service identification (http:// or ftp://) that determines the protocol used and service accessed, not the "www" or the "ftp" that are found in many fully qualified domain names. If an FTP server were named files.acme.com, it could be accessed in a web browser by entering ftp://files.acme.com.

FTP software is frequently used by webpage administers to upload webpages and files. Note that in all these applications of FTP, the data are traversing the Internet in the clear. Because confidential information is not sent, there is no real security risk in downloading software using FTP (unless, of course, the software is malicious). However, web administrators who send their authentication credentials during their webpage uploads should not be surprised if their website is targeted for defacement or worse. In this lab, you capture and analyze FTP traffic.

After completing this lab, you will be able to:

- Capture network traffic with Wireshark
- Analyze captured FTP traffic

Materials Required

This lab requires the following:

- The successful completion of Lab 9.2

Activity

Estimated completion time: **30–60 minutes**

In this lab, you use a protocol analyzer to capture FTP traffic and analyze the results.

1. Log on to Windows 10 VM as the administrator.
2. Click **Start**, type **WireShark**, and then click the **Wireshark** program.
3. Select the Ethernet controller you wish to capture packets from.
4. Click the **Start** button. Unless there is no network traffic, you will see frames, appearing as rows, added to your screen. If you are on a switched network, you will not see all the traffic on the network. Focus on the communication between Windows 10 VM and Windows Server. On the **Capture** menu, click **Stop** so you can set up your connection to the FTP server.
5. Start the Wireshark capture.
6. Open a command prompt, type **cd **, and press **Enter**.
7. Type **ftp** ***IP address of Windows Server*** and press **Enter**.
8. Log into the FTP server (See Figure 9-3) using the administrator account credentials.

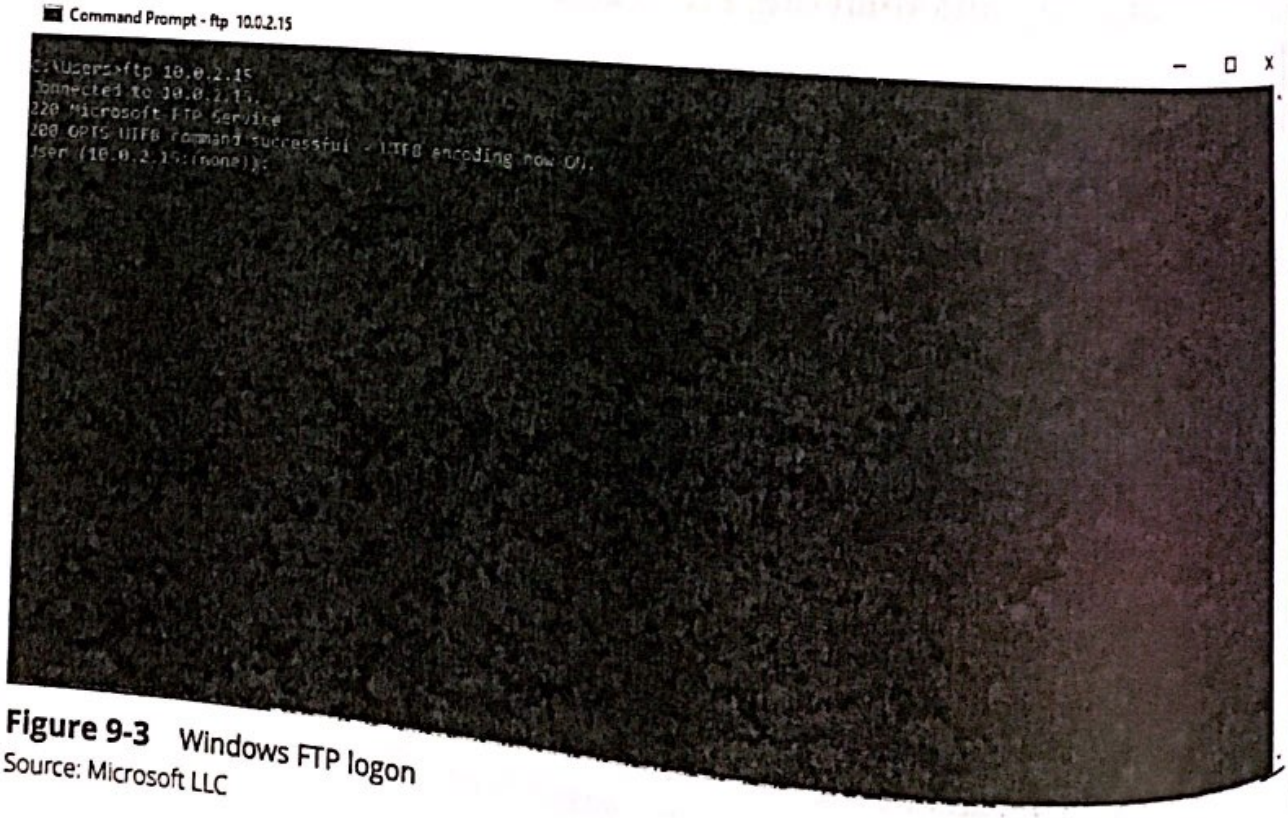

Figure 9-3 Windows FTP logon
Source: Microsoft LLC

9. Log on to the FTP server as **mbloom**. (If you have not previously created this user, In Server Manager, click **Tools**, then click **Active Directory Users and Computers**, expand your domain, right-click the **Users** container, click **New**, and click **User**. Create a user with the full name **Molly C Bloom**, the User login name **mbloom**, and the password **Pa$$word.**) Press **Enter.**
10. Type Molly Bloom's password as **Pa$$word** and press **Enter.**

Note

If too much time elapses between entering the username and entering the password, the system rejects the access attempt. If this happens, type **bye**, press **Enter**, and try the ftp *IP Address* command again.

11. At the ftp> prompt, type **dir** and press **Enter** to see what files are in the FTP server's home directory. If you get a Windows Firewall error, click **Unblock** and click **Continue** at the User Account Control window. You should now see the file Confidential.txt listed.
12. Download Confidential.txt to your C: drive as follows: Type **get Confidential.txt** and press **Enter.**
13. Type **bye** and press **Enter** to disconnect from the FTP server; return to Wireshark and, from the Capture menu, click **Stop.**
14. Click the Windows **Start** button, click **Computer**, navigate to **C:\Users\Administrator.Team1\Confidential.txt** and open it to verify that you downloaded it successfully.
15. Return to Wireshark and examine the captured packets.
16. If, in the Source and Destination columns, you see a lot of IP addresses or MAC addresses that don't belong to your Windows 10 VM or your FTP server, click **Capture** and then select **Capture Filters.** This opens the dialog box shown in Figure 9-4, where you can filter the addresses Wireshark is listening for.

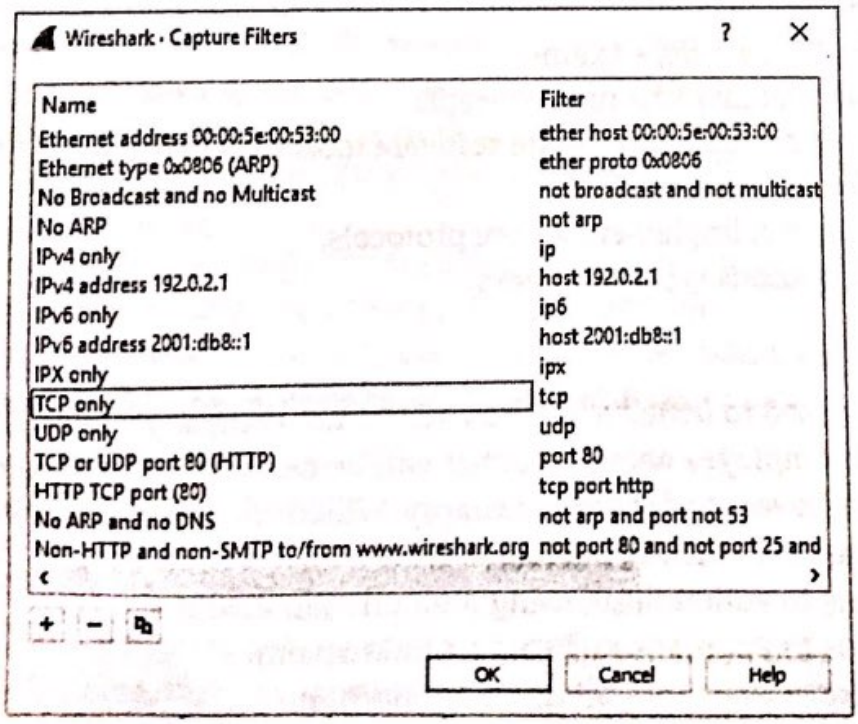

Figure 9-4 Wireshark Capture Filters
Source: The Wireshark Foundation

17. Examine the frames and look at the Info column for clues to the purpose or content of the frame; keep an eye on the ASCII representation of the data portion of the frame in the lower window (see Figure 9-5). What parts of the FTP session would be readable to an attacker sniffing the network with a protocol analyzer like Wireshark?

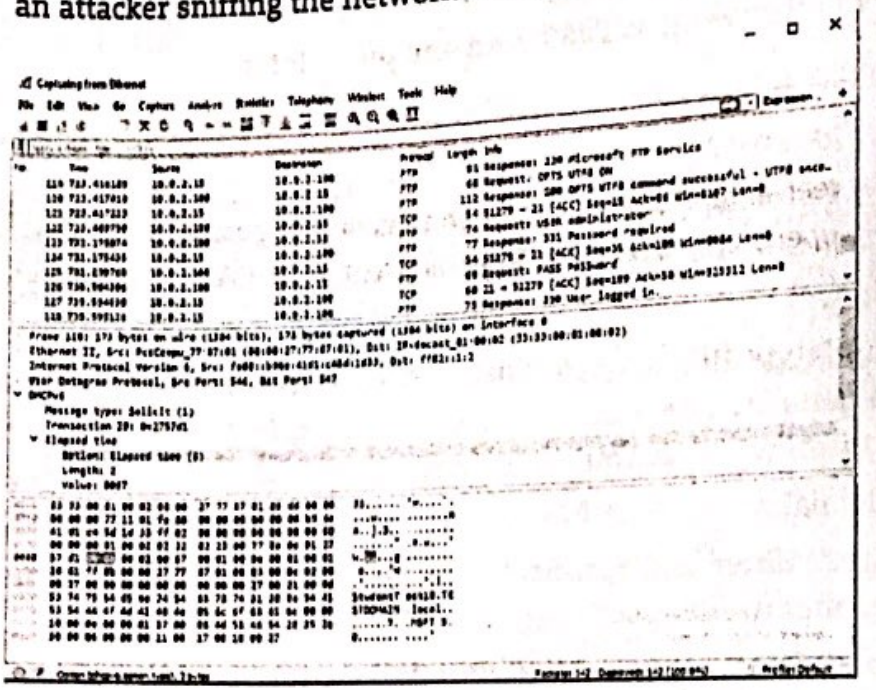

Figure 9-5 Wireshark Capture
Source: The Wireshark Foundation

18. Return to the Windows Server and restore Windows Firewall to its original settings.
19. Close Wireshark without saving the capture. Close all open windows and log off.

Certification Objectives

Objectives for CompTIA Security+ Exam:

- 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 Summarize various types of attacks.

Review Questions

1. You have been asked to install an FTP server on the company's internal network, to be used only by an employee committee that will be working on an advertising campaign to encourage employees to donate to a charity. Which of the following would be the most secure configuration of the FTP server?
   a. Require users to authenticate using their domain account.
   b. Require users to authenticate using a local account.
   c. Require users to use anonymous authentication.
   d. Allow users to share a single username and password.

2. In this lab, what is listed in the Info column of the frame in which the content of the file Confidential.txt is visible?
   a. FTP Data
   b. Response
   c. Request
   d. get-request
3. Which of the following statements is the most accurate description of the communication between Windows 10 VM and the FTP server in this lab?
   a. Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flags SYN and ACK set.
   b. Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flag ACK set.
   c. Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flag SYN set.
   d. The FTP server initiated the connection by sending a packet to Windows 10 VM with TCP flag SYN set.
4. Which of the following statements is the most accurate description of the communication between the Windows 10 VM system and the FTP server in this lab?
   a. Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flags SYN and ACK set.
   b. Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flag ACK set.
   c. Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flag SYN set.
   d. The FTP server was not first contacted by Windows 10 VM; it advertised its FTP service, and Windows 10 VM responded.
5. Which of the following statements is the most accurate description of the communication between the Windows 10 VM system and the FTP server in this lab?
   a. The teardown of the TCP session began when the FTP server sent a packet to Windows 10 VM with the TCP flag FIN set.
   b. The teardown of the TCP session began when Windows 10 VM sent a FIN packet to the FTP server.
   c. The teardown of the TCP session began when the FTP server sent a packet to Windows 10 VM with the TCP flags FIN and ACK set.
   d. The teardown of the TCP session began when Windows 10 VM sent a packet to the FTP server with the TCP flags FIN and ACK set.

9.4 Physical Security Planning

Objectives

You have been brought in as a consultant to a software engineering company that is planning its new office building. They are extremely concerned with the layout of the office and ask for advice on making it more physically secure. The floor plan for the building is shown in Figure 9-6.