Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the** System Checker. The System Checker will confirm that your browser and network connection are ready to support virtual labs.

2. **Review the** Common Lab Tasks document. This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.

3. **When you've finished, use the Disconnect button to end your session and create a StateSave**. To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
   If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.

4. Technical Support **is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
   Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

Perhaps the most reiterated and fundamental concept in computer and network security is Defense in Depth (DID). The main principle of Defense in Depth is to build layers of redundant and complementary security tools, policies, controls, and practices around the organization's information and assets. The primary assumption of Defense in Depth is that no one single tool or practice will completely deter a resolved attacker.

Normally a great deal of thought and planning goes into securing the perimeter. Firewalls, Access Control Lists (on border routers), intrusion prevention systems, and network isolation all work hand in hand to "secure the border" and help keep out the unwanted. Internally Web application firewalls, security information and event management systems, access controls, network security monitoring, and change controls help to keep the "soft center" from becoming an easy target when the perimeter fails. However, no security program is complete without host-based security measures.

Some of the more important host-based security measures include anti-virus (and anti-malware), host-based firewall, system hardening (removing unwanted services), change control, and log management. While the aforementioned security protocols are commonly implemented on servers, administrators can find that the user's laptops and workstations are more politically charged. For example, users often complain that security measures make their systems "slow" and hard to use. Unless stringent security is mandated by policy, the security practitioner must always balance security with functionality and user adoption.

In this lab, you will use AVG, an anti-virus scanning program, to identify malware found on a compromised system. You will also examine the services available on the Windows LandingVM machine and disable an unnecessary service. In addition, you will configure the Windows Firewall, enable ICMP traffic, and create a new rule for the FileZilla Server application.

Learning Objectives

Upon completing this lab, you will be able to:

1. Identify the risks associated with viruses, malware, and malicious software on a Windows server
2. Apply security countermeasures to mitigate the risk caused by viruses, malware, and malicious software
3. Enable AVG as an anti-virus, malware, and malicious software security countermeasure on a Windows server
4. Disable unnecessary services in a Windows workstation

5. Configure a Windows workstation internal firewall to enable ports, applications, and services

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will run a virus scan and detect malware.

2. In the second part of the lab, you will document existing services and disable unwanted services.

3. In the third part of the lab, you will enable ports and applications within the Windows Firewall.

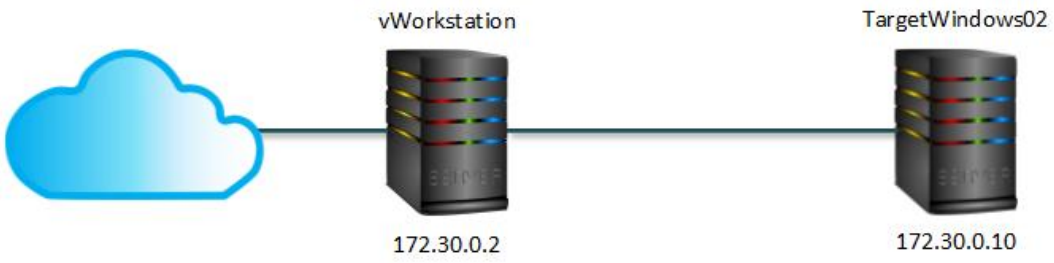
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will create an outbound rule and restrict the scope of the rule to a specific subnet.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindows02 (Windows Server 2016)



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- FileZilla
- Windows Firewall
- AVG Anti-Virus
- Windows Services

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- Virus details;
- Emptied Quarantine area (Virus Vault);
- Updated services list;
- Updated File and Printer Sharing rule in the firewall;
- Inbound FileZilla Server rule;

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- Scan Summary (Detection) page;
- Emptied Quarantine area (Virus Vault);
- Updated services list;
- Updated Email and accounts rules in the firewall;
- Outbound FileZilla Server rule;

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Part 1: Using AVG Business Edition to Perform a Virus Scan

Note: Malware consists of unwanted programs like Trojans and Viruses. Signs of malware include degraded system performance, unusual services and network traffic, altered or removed system logs, missing or inactive anti-virus, and any number of application anomalies. Trojans and viruses impact all three tenets of information systems security.

- **Confidentiality**: Malware can grant unauthorized access to the compromised machine and network.
- **Integrity**: Malware is able to steal and modify data.
- **Availability**: Viruses and malware tend to slow performance and availability to applications and data.

A Trojan will masquerade as a seemingly useful program while actually compromising system security and possibly acting as a “back door” allowing additional hack tools and access to the system. A standard “virus” is a program that will spread from one computer to another in any variety of means, taking advantage of application or OS vulnerabilities to propagate further and will generally try to stay undetected.

In the next steps, you will use AVG, an anti-virus program, to scan a folder on the TargetWindows02 machine to see how AVG and similar software programs identify malware. First, you will locate the malware file in the folder structure before running the scan.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.

2. In the Connections folder, **double-click** the **TargetWindows02 RDP shortcut** to open a remote connection to the TargetWindows02 machine.

   If prompted, **type** the following credentials and **click OK**.

   - Username: **`Administrator`**
   - Password: **`P@ssw0rd!`**

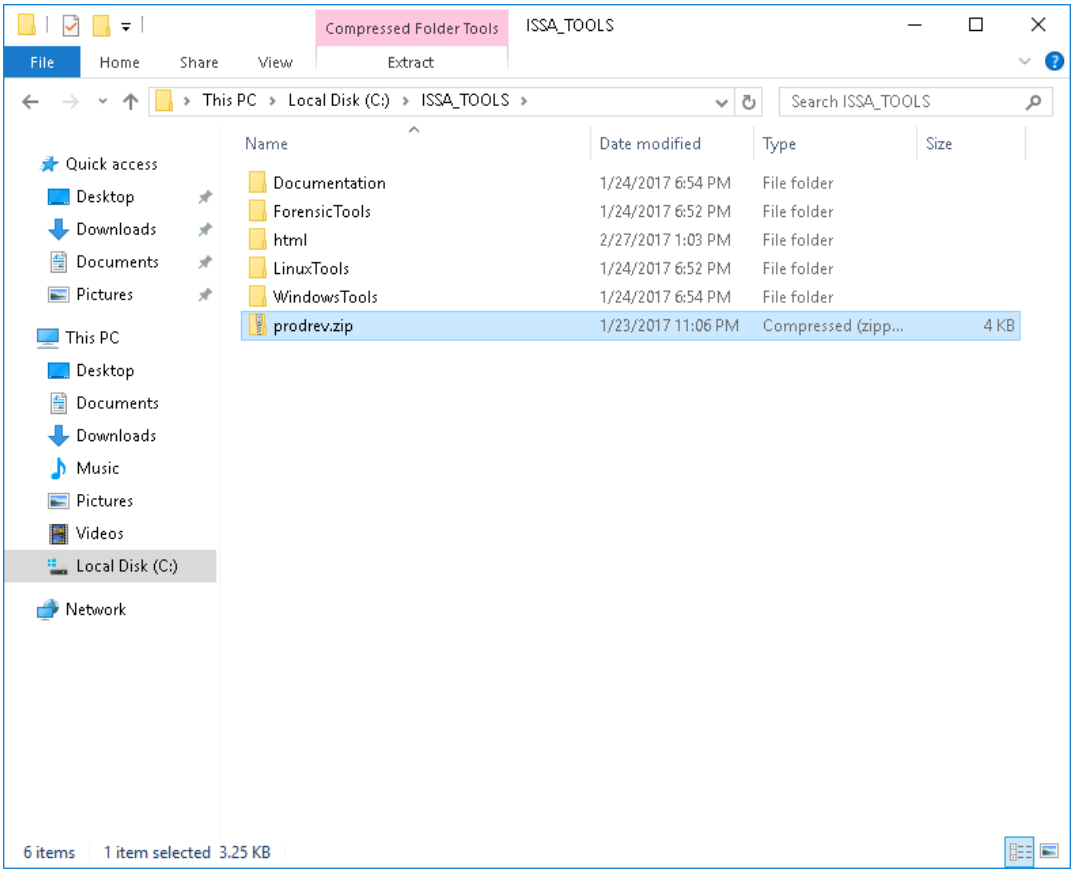
   The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

3. On the TargetWindows02 taskbar, **click** the **File Explorer icon** to open a new File Explorer

window.

4. In the File Explorer window, **navigate** to the ISSA_TOOLS folder (**Local Disk (C:) > ISSA_TOOLS**).

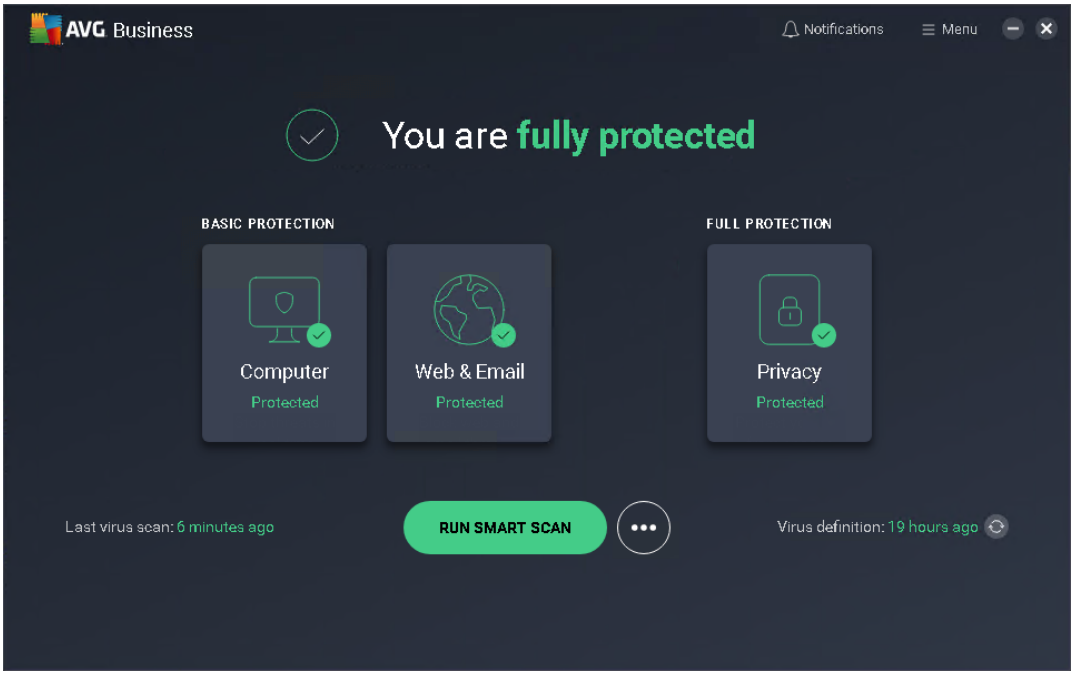
   The password-protected prodrev.zip archive file has been infected with malware. Continue the lab to discover how malware is identified.



Infected archive file

5. **Minimize** the **File Explorer window**.

6. On the TargetWindows02 desktop, **double-click** the **AVG Business Security icon** to launch the AVG antivirus application.



AVG Status

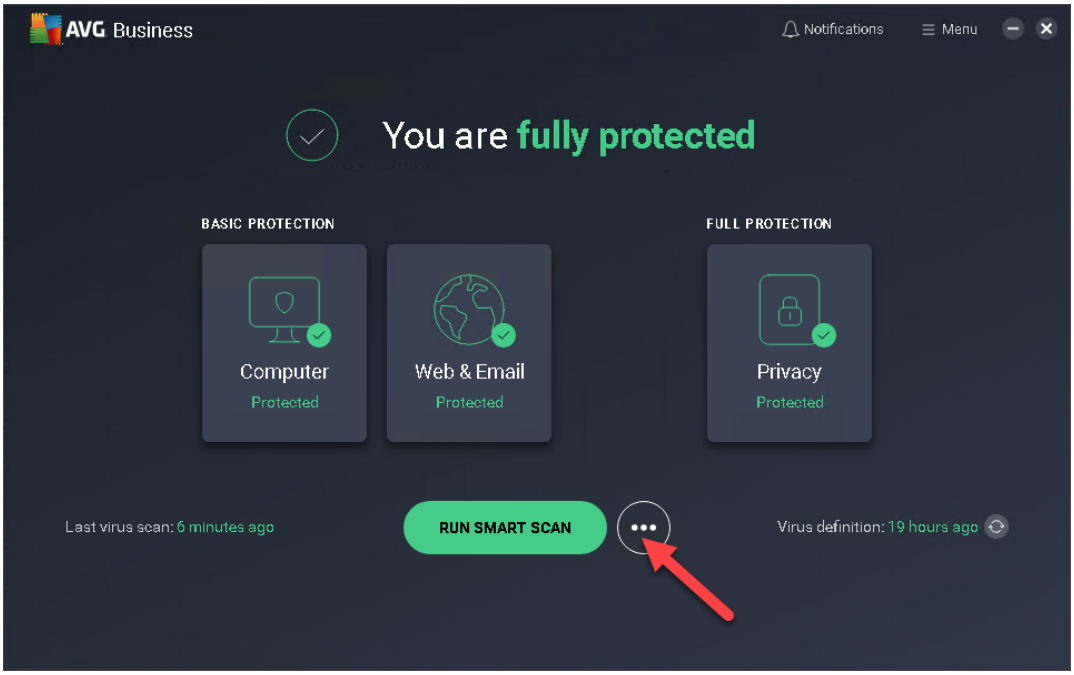
Note: Many new malware and viruses are detected every day. Usually, anti-virus vendors update their anti-virus signature files at least several times per week. To ensure you have coverage on the most recent malware and malicious software, it is recommended that you update your anti-virus signature files prior to performing a system scan.

7. In the lower-right corner of the AVG interface, **click** the **Update Virus Definitions button** (the circular arrows icon) to check for updates to the virus definitions.

   This will trigger the AVG Settings window to open with the Update tab (General > Update) selected and begin a check for virus definition updates. AVG will download and install any new virus definitions it has populated in its repository since the last update run on this instance.Once the update has completed, AVG should notify you that "Virus definitions are up to date."

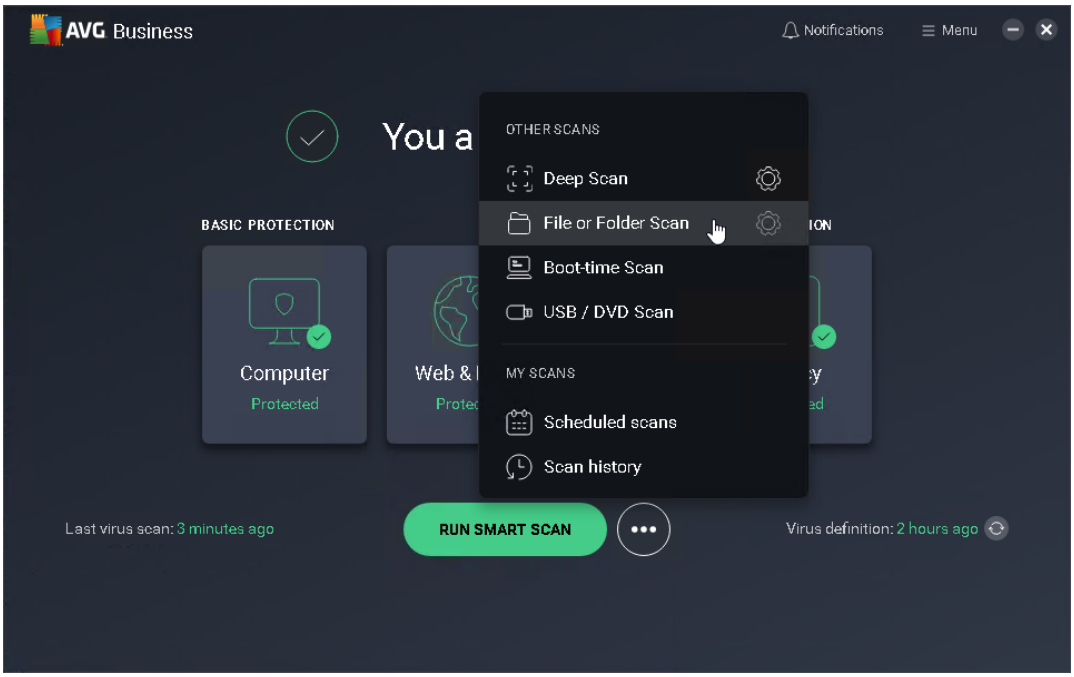
8. In the top-left corner of the AVG Settings window, **click** the **Close button** (the X icon) to return to the AVG Home page.

9. On the AVG Home page, **click** the **Other scans button** (the ellipsis to the right of the Run Smart Scan button) to open the Other Scans menu.



Other Scans button

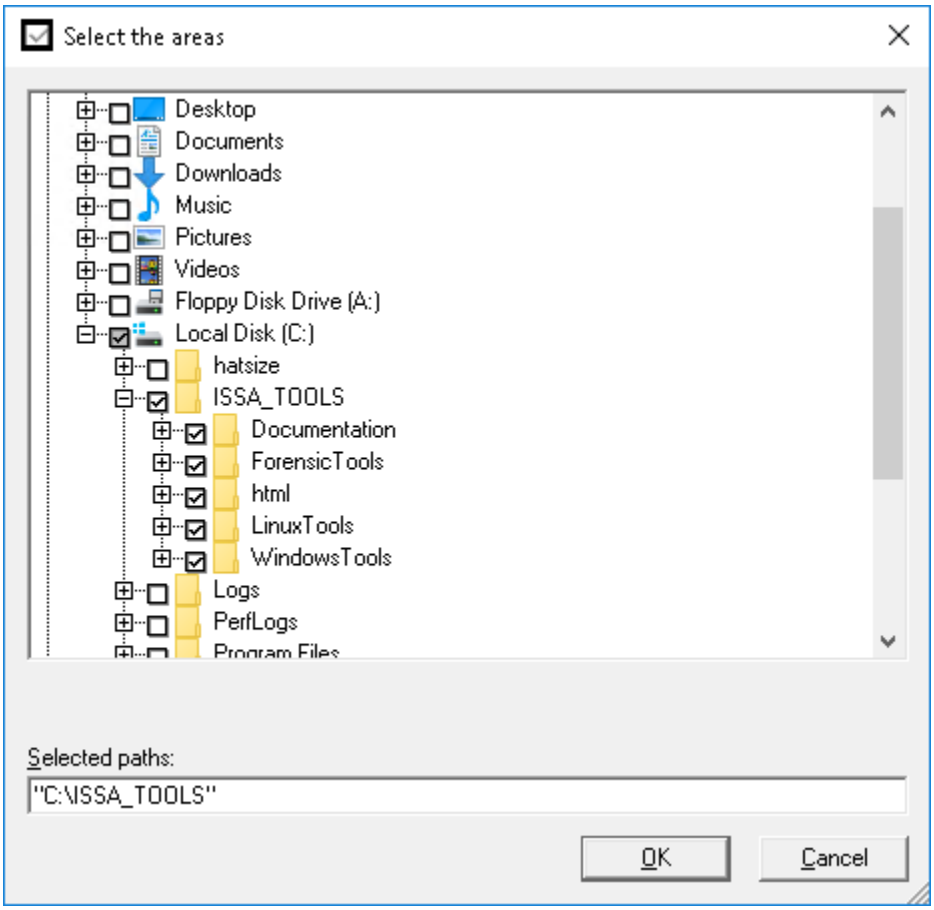
10. On the Other Scans page, **click** the **File or Folder Scan button** to open the Select the areas window and choose the files and/or folders to include in your AVG scan.



Other Scans page

11. In the Select the areas window, **navigate** to the ISSA_TOOLS folder **(C:\ISSA_TOOLS)** and **expand** the **folder**.

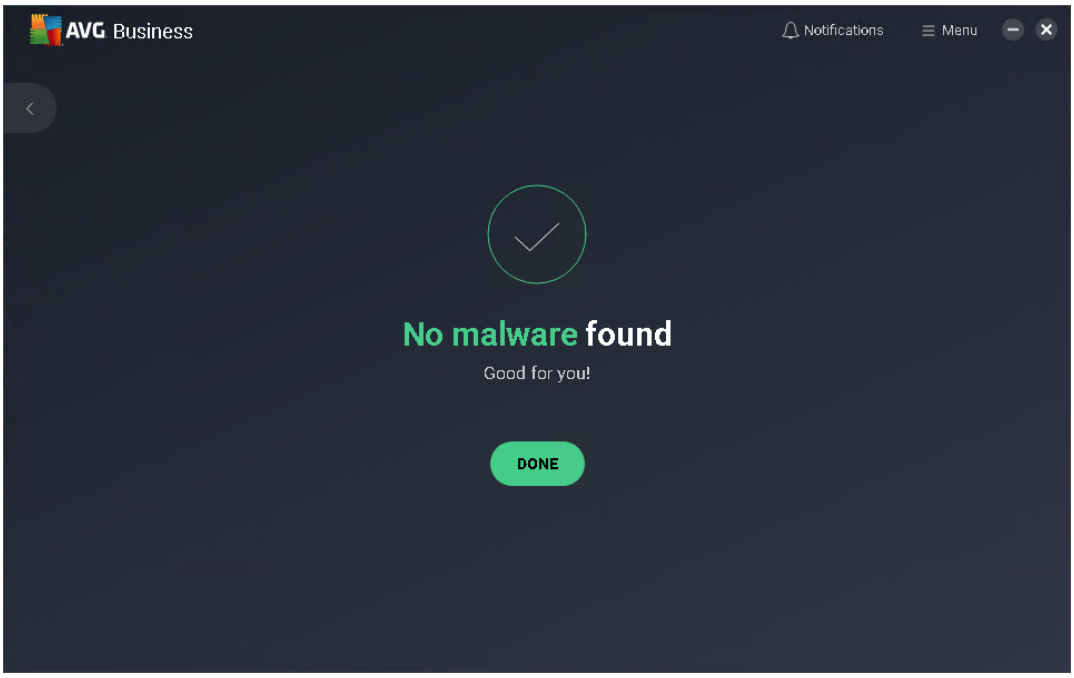
12. In the Select the areas window, **click** the **ISSA_TOOLS checkbox** to select that folder and all of its subfolders.



Select the areas

13. In the Select the areas window, **click OK** to begin the scanning process and remove any identified threats.

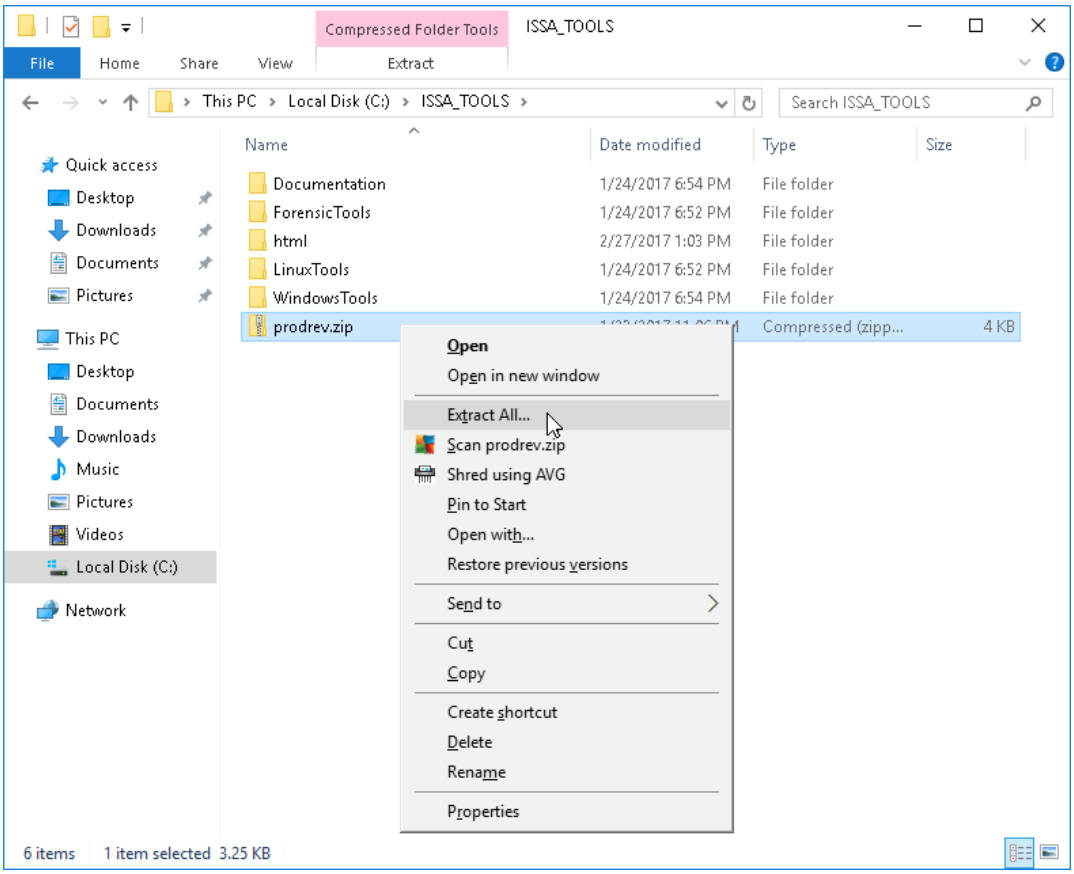
    When the scan is completed, AVG will display a screen indicating any threats that it identified. Notice that the tool did not identify the prodrev.zip file because anti-virus software cannot open encrypted files for scanning. Hackers will often send zipped and encrypted files and attachments, as they will often reach the recipient unless there is a mail rule blocking encrypted and/or zipped files.



Scan results

14. On the TargetWindows02 taskbar, **click** the **File Explorer icon** to restore the ISSA_TOOLS folder.

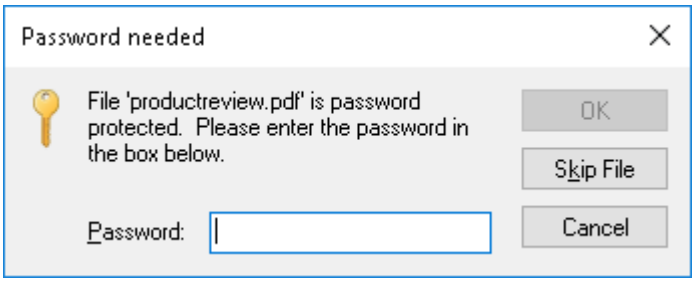
15. In the ISSA_TOOLS folder, **right-click** the **prodrev.zip file** and **select Extract All** from the context menu.



Extract the archive file

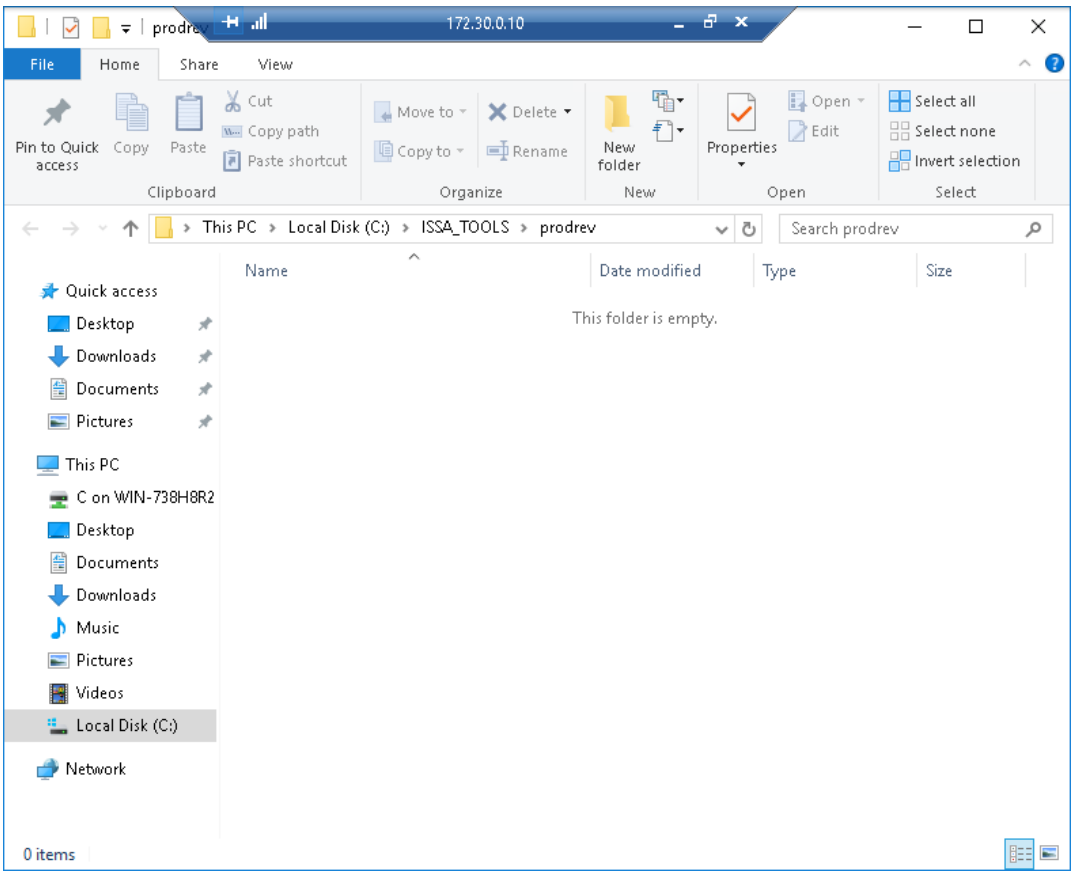
16. In the resulting window, **click** the **Extract button** to unpack the zip file in the same folder.

17. When prompted for the file's password, **type** **`password123`** and **click OK** to decrypt the zipped file and begin the unpacking process.



Password prompt

Notice the extraction resulted in an empty folder. This is because AVG (File Shield), running in the background, detected and immediately quarantined the threat.



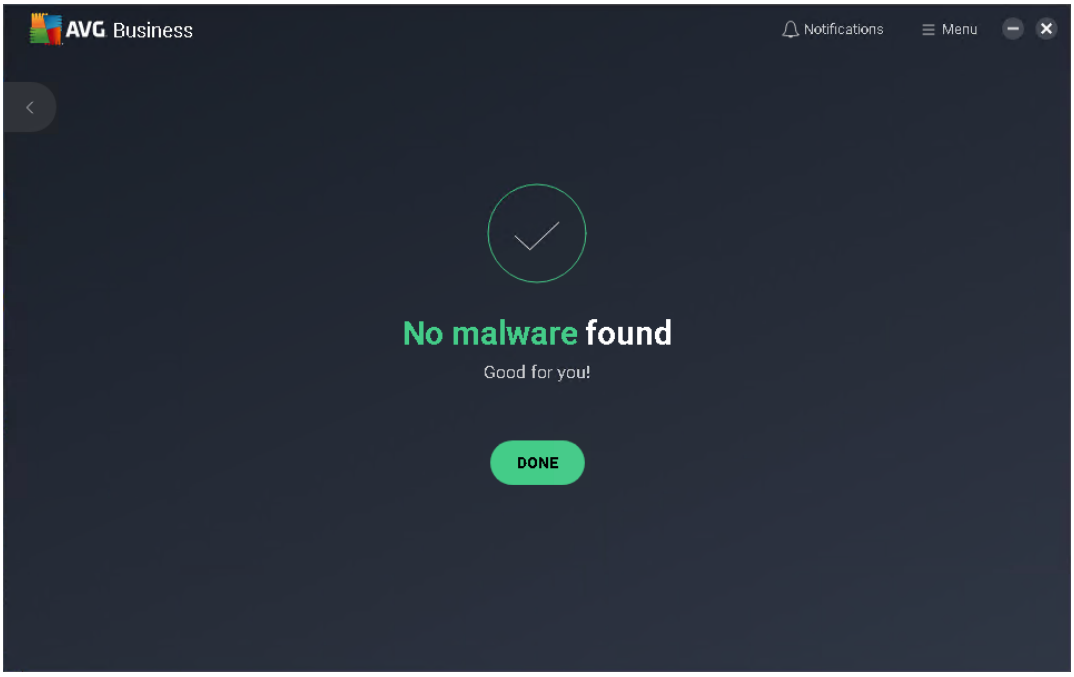
Empty prodrev folder

18. **Close** the **prodrev File Explorer window**.

19. **Close** the **ISSA_TOOLS File Explorer window**.

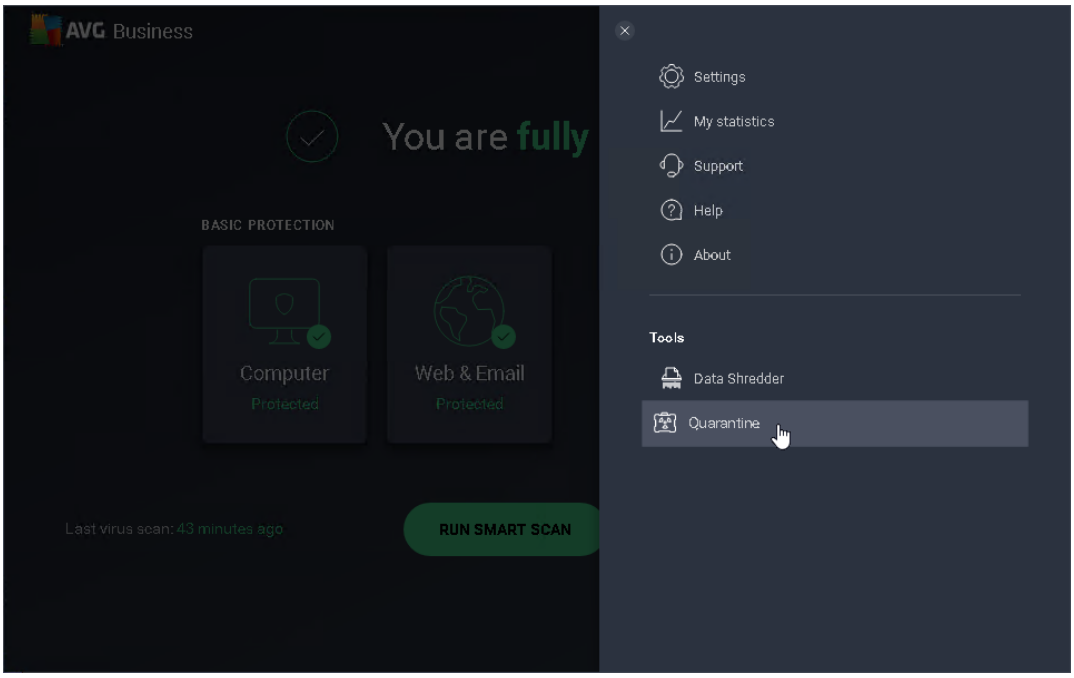
Note: In the next steps, you will view the details of the discovered threat in AVG's Quarantine. The Quarantine area (previously referred to as the Virus Vault) is where all removed files, virus infected or suspicious, are stored until you take action on them. All of the files in the vault are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any deleted file for a certain period of time, so that you can make sure you do not need the file any more. If you find out that the missing file is causing problems, you can send it for analysis, try to heal it, or restore it to the original location.

20. On the Scan Summary page, **click** the **Done button** to return the AVG Home page.



AVG Done button

21. On the AVG Home page, **click** the **Menu icon**, then **select Quarantine** from the available options to open the Quarantine area.

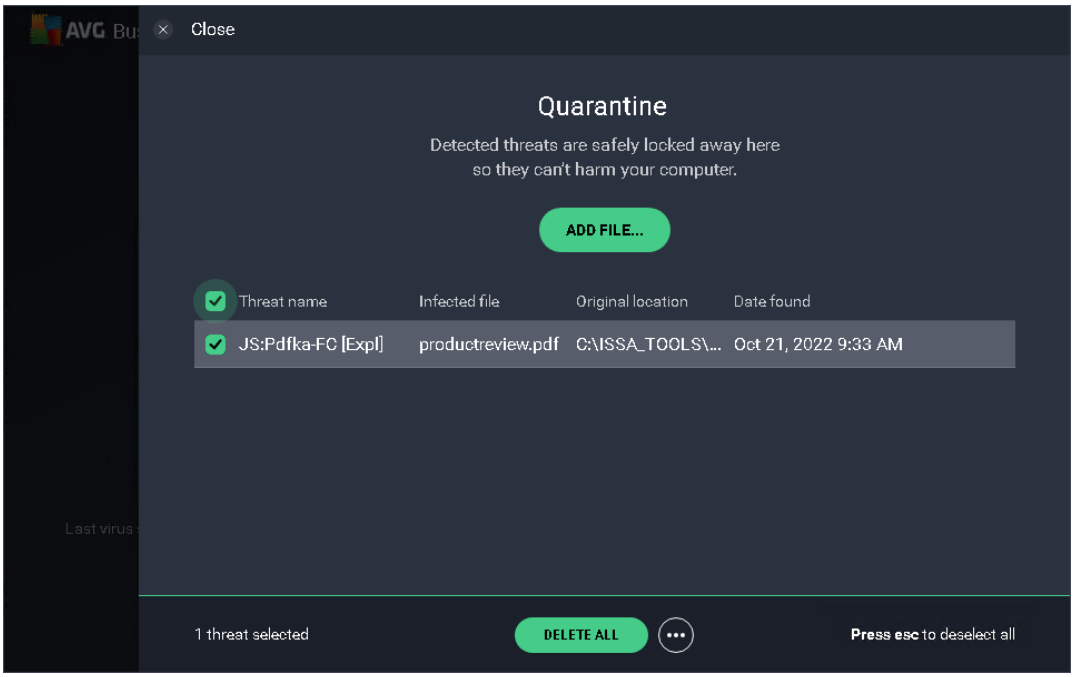


Options menu

Note: You should have one item in the quarantine, corresponding to the threat detected in the prodrev.zip file during your extraction. AVG provides information about the actual name of the virus (JS:Pdfka-fc) and reports that the infected file (productreview.pdf, part of the prodrev.zip file) has been deleted and the virus has been moved to the Quarantine area (Virus Vault).

22. **Make a screen capture** showing the **virus details** in the AVG quarantine and **paste** it into your Lab Report file.

23. On the AVG Quarantine page, **click** the **top checkbox** (beside the Threat name column) to select all viruses in the Quarantine area



Quarantine area

24. On the AVG Quarantine page, **click** the **Delete All button** to remove all selected viruses.

25. **Make a screen capture** showing the **empty Quarantine area (Virus Vault)** and **paste** it into your Lab Report file.

26. **Click** the **Close button** to close the AVG Quarantine page.

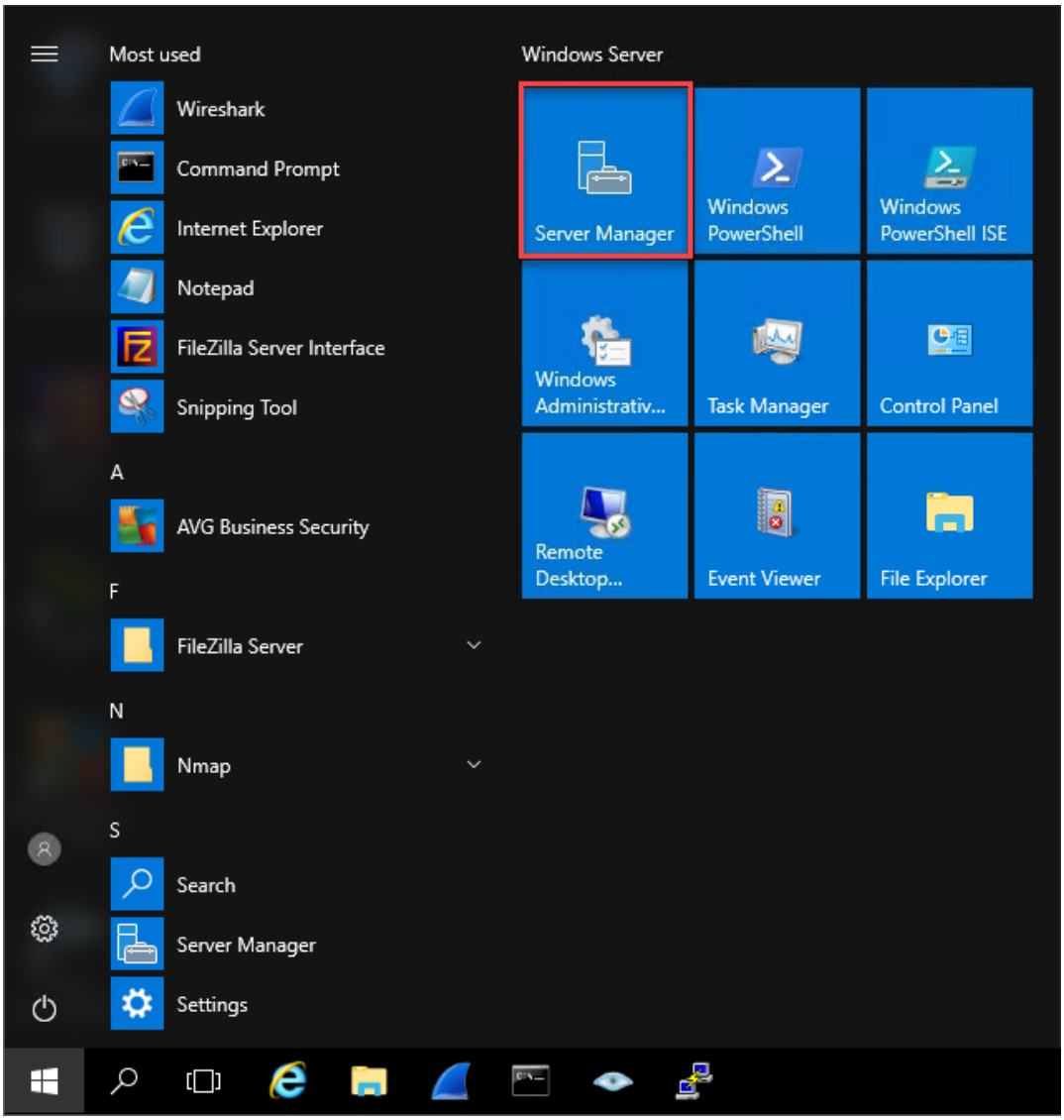
27. **Close** the **AVG window**.

Part 2: Disabling Unwanted Services

Note: In the next steps, you will document and disable an unwanted service running on the TargetWindows02 virtual machine. Like an up-to-date anti-virus, managing system services is an important element in a given organization's security program. Other elements include (but are not limited to) standardized configurations and settings based on organization-wide security policy definition, a layered security strategy to mitigate the threat from entering the IT infrastructure, email filtering/quarantining, frequency of anti-virus and malicious software prevention tool updates, as well

as operating system and application updates to close known vulnerabilities.

1. On the TargetWindows02 taskbar, **click** the **Windows Start button** and **select Server Manager** from the Start menu.

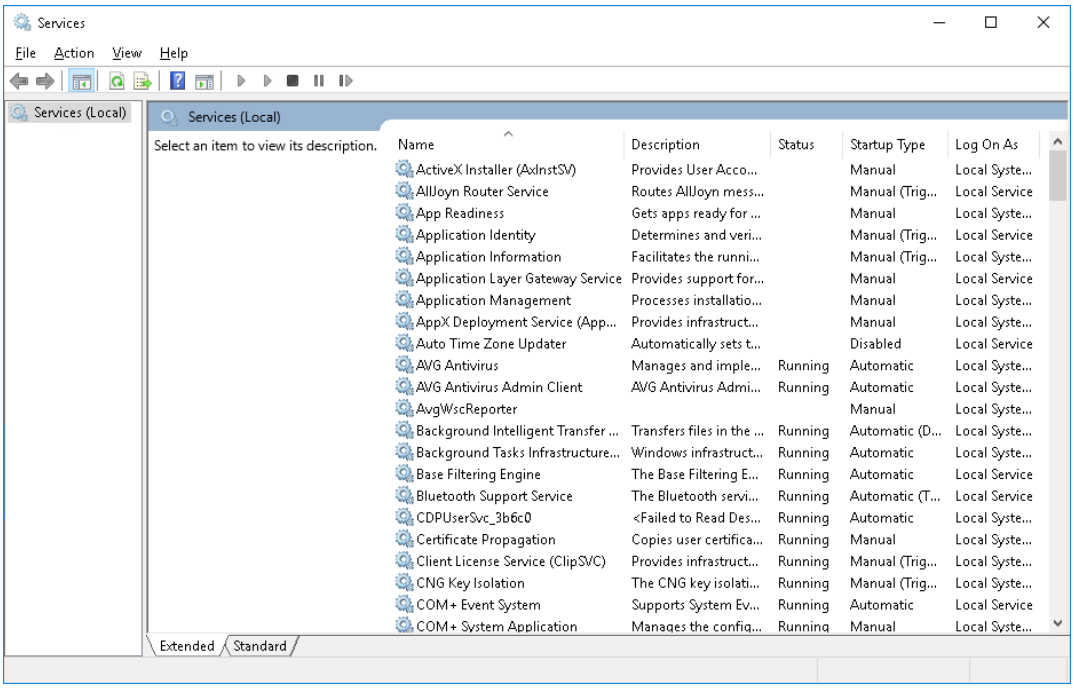


Start menu

2. From the Server Manager toolbar, **click Tools** and **select Services** to view a list of the services running on this virtual machine.

   The Startup Type column indicates whether those services start automatically, manually, or have been disabled.

3. In the Services window, **drag** the **column borders** to view the data in all columns, as shown in the following figure.



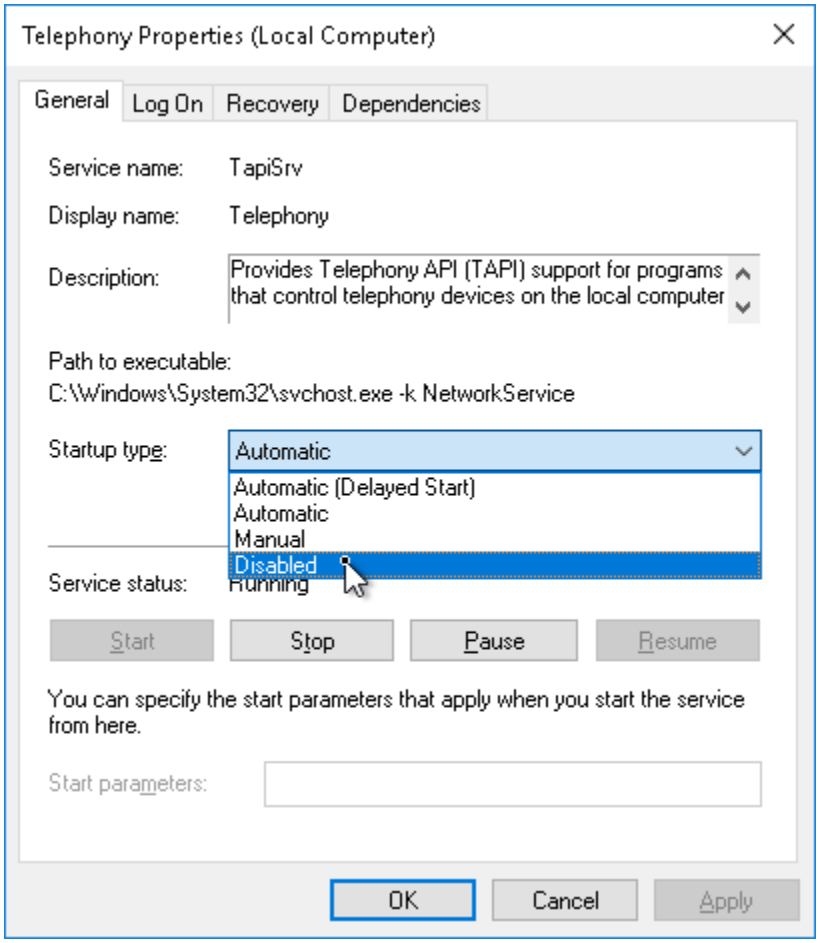
Local services

4. At the bottom of the Services window, **click** the **Standard tab** to display only the standard services.

5. At the bottom of the Services window, **click** the **Extended tab** to return to the original view.

6. In the Services list, **double-click** the **Telephony** service to open the Properties dialog box for this service.

7. In the Telephony Properties dialog box, **select Disabled** from the Startup type drop-down menu in the center of the screen.



Properties dialog box

8. **Click OK** to change the Startup type.

9. **Make a screen capture** showing the **changed startup type in the list of services** and **paste** it into the Lab Report file.

10. **Close** the **Services window**.

11. **Close** the **Server Manager window**.

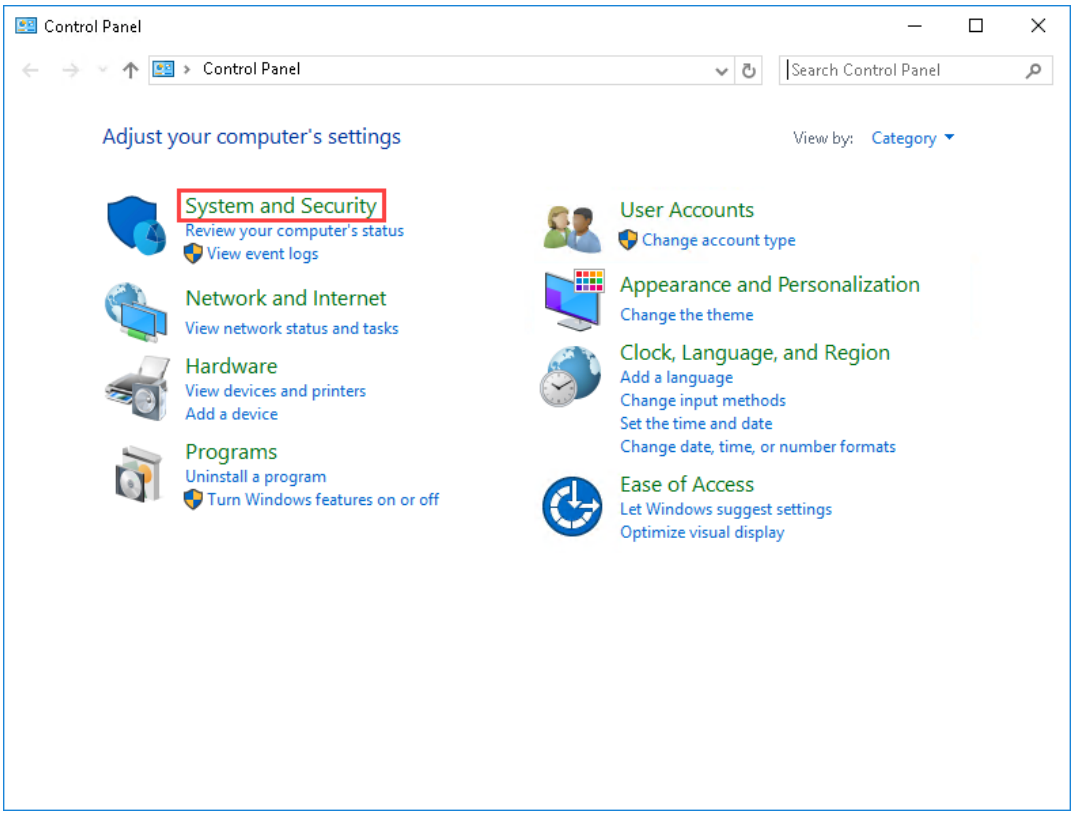
Part 3: Configuring the Windows Firewall

Note: The Windows Firewall with Advanced Security is a personal firewall that filters incoming and outgoing traffic by blocking unauthorized traffic to the local computer. It can be configured to support separate profiles based on whether the computer is connected to a network at the office, or connected at home, or at a public location, such as the local coffee shop. Using the Advanced Security profiles, network traffic can be filtered based on Active Directory users and groups, both source and destination IP addresses, port number, specific programs and services.

Enabled on the network and properly configured, a firewall can block outside sources from being able to insert malware and viruses. By default, the Windows Firewall disables several important services like File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP), which includes the Ping command. In the next steps, you will manually configure the Windows Internal Firewall to enable the ICMP service on the TargetWindows02 machine.

1. On the TargetWindows02 taskbar, **right-click** the **Windows Start button** and **select Control Panel** from the context menu.

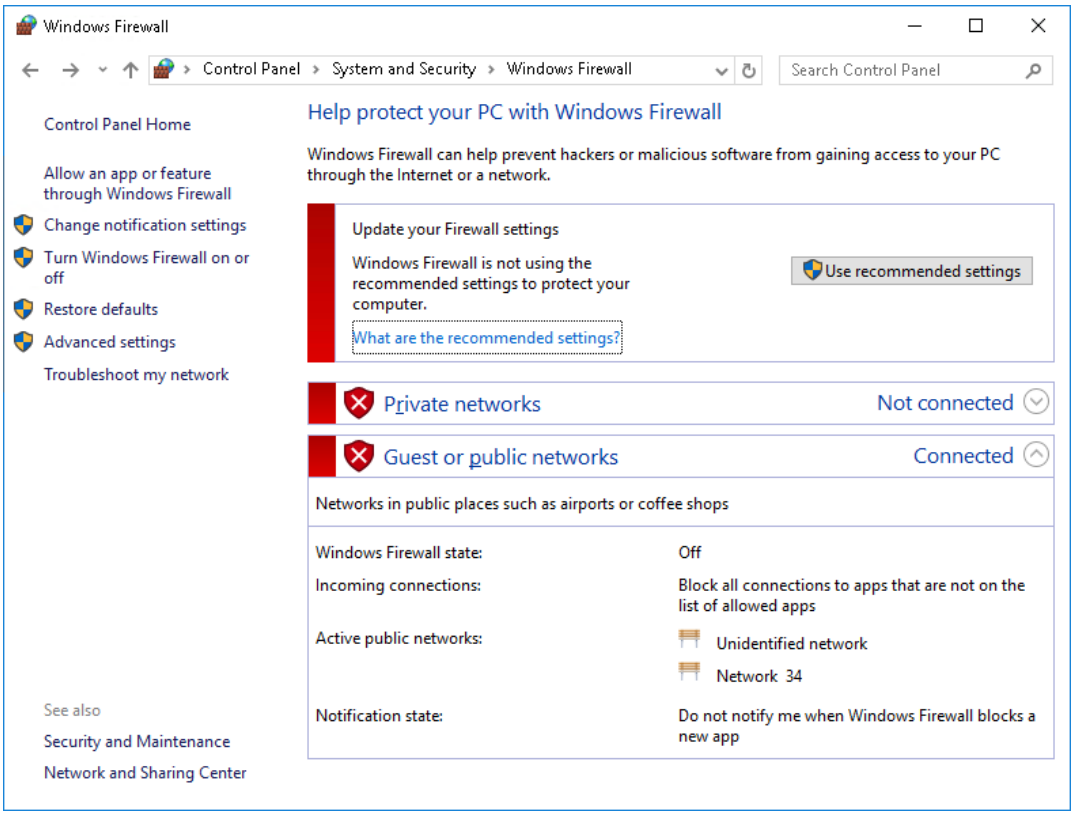
2. In the Control Panel window, **click** the **System and Security link**, then **click** the **Windows Firewall link** on the resulting page**.**



System and Security

3. On the Windows Firewall page, **review** the **state** of the Windows Firewall.

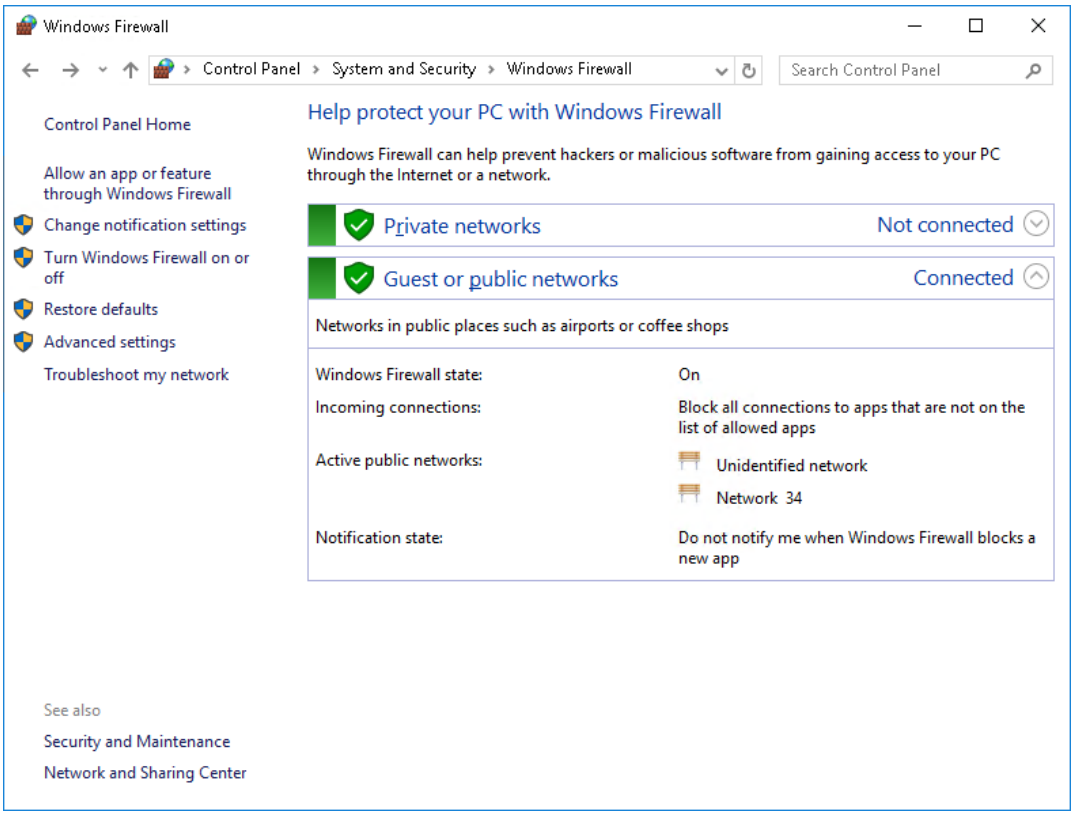
   The Windows Firewall is currently not enabled.



Windows Firewall

4. On the Windows Firewall page, **click** the **Use recommended settings button** to enable the Windows Firewall.

   Notice that the recommended settings block all incoming connections to apps that don't appear on a list of allowed apps.



Windows Firewall settings

5. In the navigation pane on the left, **click** the **Advanced settings link** to open the Windows Firewall with Advanced Security window.

6. In the left pane of the Windows Firewall with Advanced Security window, **click Inbound Rules** to open the inbound rules list.

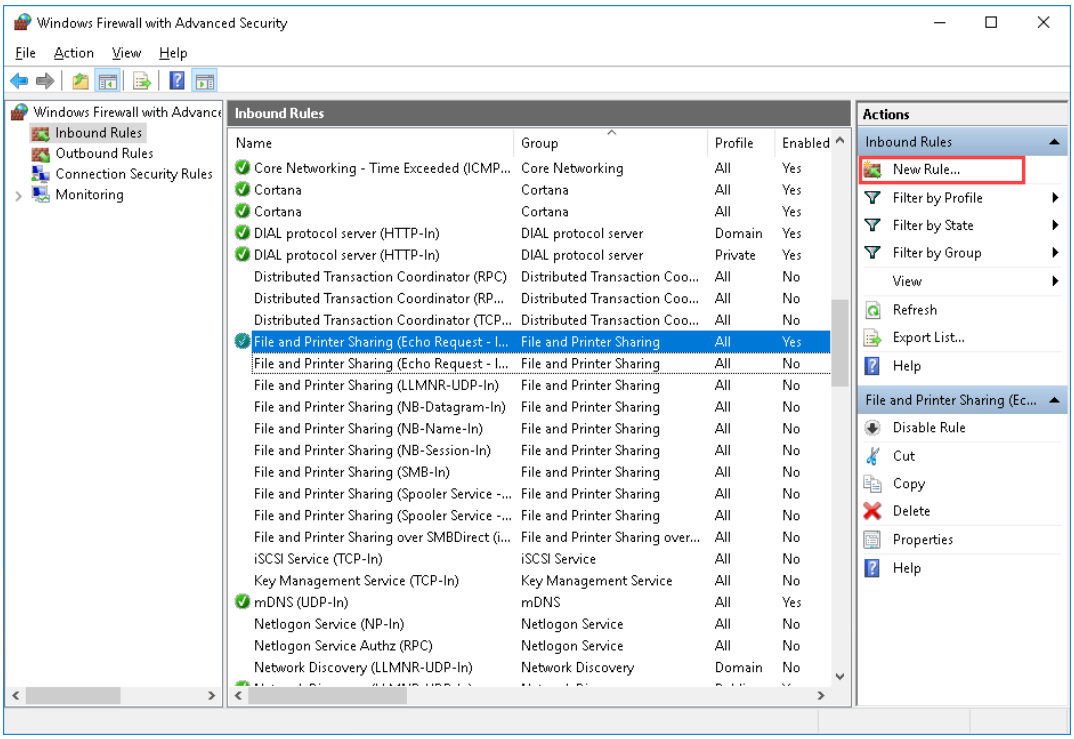
   This option enables you to set rules for all incoming traffic.

7. From the inbound rules list, **right-click File and Printer Sharing (Echo Request – ICMPv4-In)** and **select Enable Rule** from the context menu.

   Use the scrollbar to locate the rule in the list.

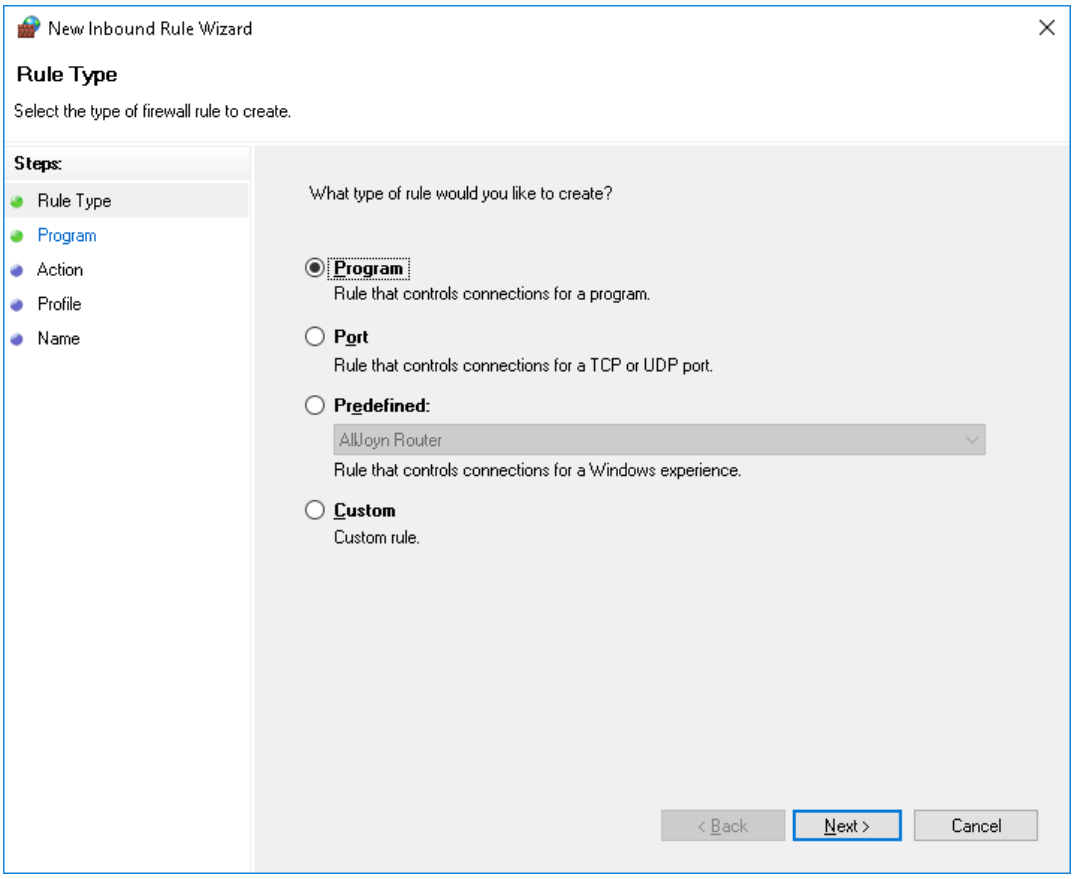
8. **Make a screen capture** showing **the updated File and Printer Sharing (Echo Request – ICMPv4-In) rule** and **paste** it into the Lab Report file.

9. In the Actions pane on the right, **click** the **New Rule link** to create a new inbound rule.



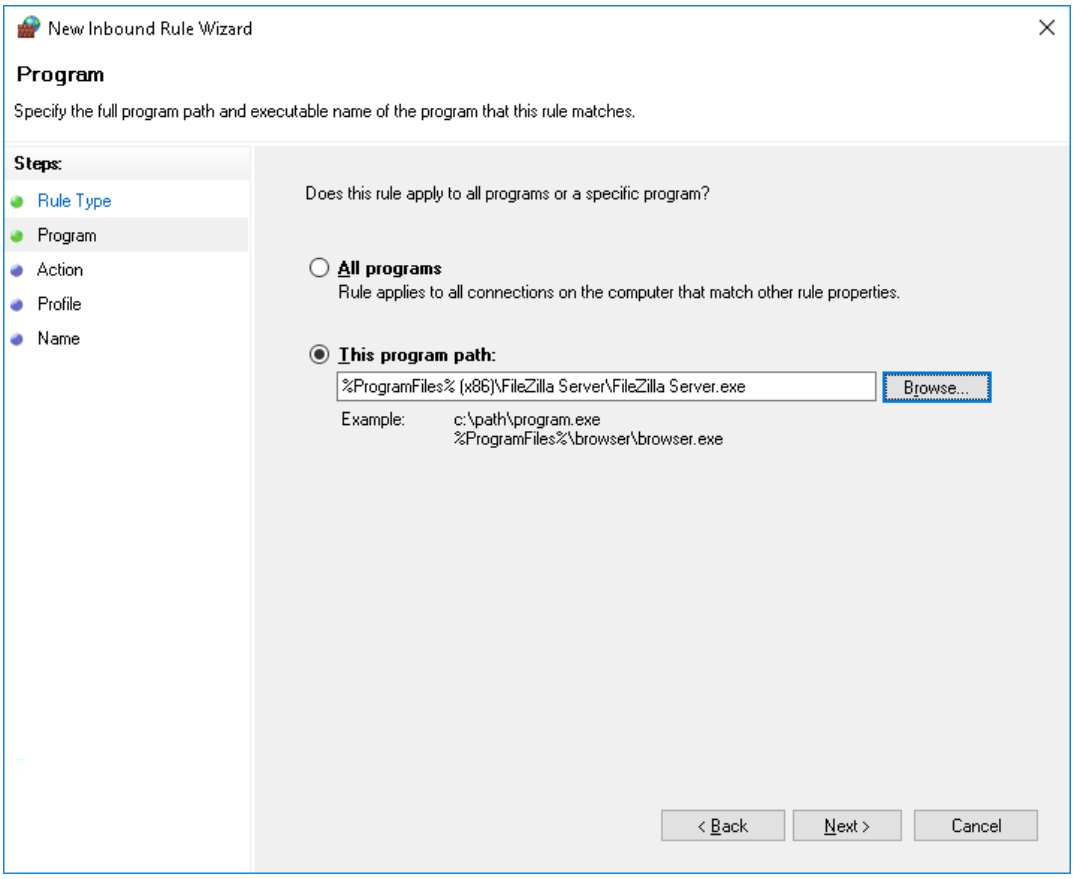
Create a new firewall rule

10. In the New Inbound Rule Wizard, **click Next** to accept the default option to create a rule that applies to a specific program.



New Rule Type window

11. On the Program page, **click** the **Browse button** and **navigate** to the executable file for the FileZilla Server application (**C:\Program Files(x86)\FileZilla Server\FileZilla Server.exe**), then **click Open** to specify the program.



Path to the FileZilla executable

12. **Click Next** to continue.

13. On the Action page, **click Next** to accept the default option to allow the connection.

14. On the Profile page, **click Next** to accept the default settings to apply this rule for every profile.

15. On the Name page, **type** `FileZilla Server` in the Name field, then **click Finish**.

    If necessary, **restore** the **Windows Firewall with Advanced Security window**.

16. In the Inbound Rules pane, **locate** the **new FileZilla Server rule**.

If you do not see the new rule, **click** the **Refresh link** in the Actions pane.

17. **Make a screen capture** showing the **new FileZilla Server rule** and **paste** it into the text document.

18. **Close** the **Windows Firewall with Advanced Security window**.

19. **Close** the **Windows Firewall window**.

20. **Close** the **remote TargetWindows02 connection** to return to the vWorkstation.

Note: This completes Section 1 of this lab. There are no deliverable files for this section.

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will create an outbound rule and restrict the scope of the rule to a specific subnet.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
   a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.

   b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.

3. **Proceed** with **Part 1**.

Part 1: Using AVG Business Edition to Perform a Virus Scan

Note: Malware consists of unwanted programs like Trojans and Viruses. Signs of malware include degraded system performance, unusual services and network traffic, altered or removed system logs, missing or inactive anti-virus, and any number of application anomalies. Trojans and viruses impact all three tenets of information systems security.

- **Confidentiality**: Malware can grant unauthorized access to the compromised machine and network.
- **Integrity**: Malware is able to steal and modify data.
- **Availability**: Viruses and malware tend to slow performance and availability to applications and data.

A Trojan will masquerade as a seemingly useful program while actually compromising system security and possibly acting as a “back door” allowing additional hack tools and access to the system. A standard “virus” is a program that will spread from one computer to another in any variety of means, taking advantage of application or OS vulnerabilities to propagate further and will generally try to stay undetected.

In the next steps, you will use AVG, an anti-virus program, to scan a folder on the TargetWindows02 machine to see how AVG and similar software programs identify malware.

1. **Open a remote connection** to the **TargetWindows02** machine.

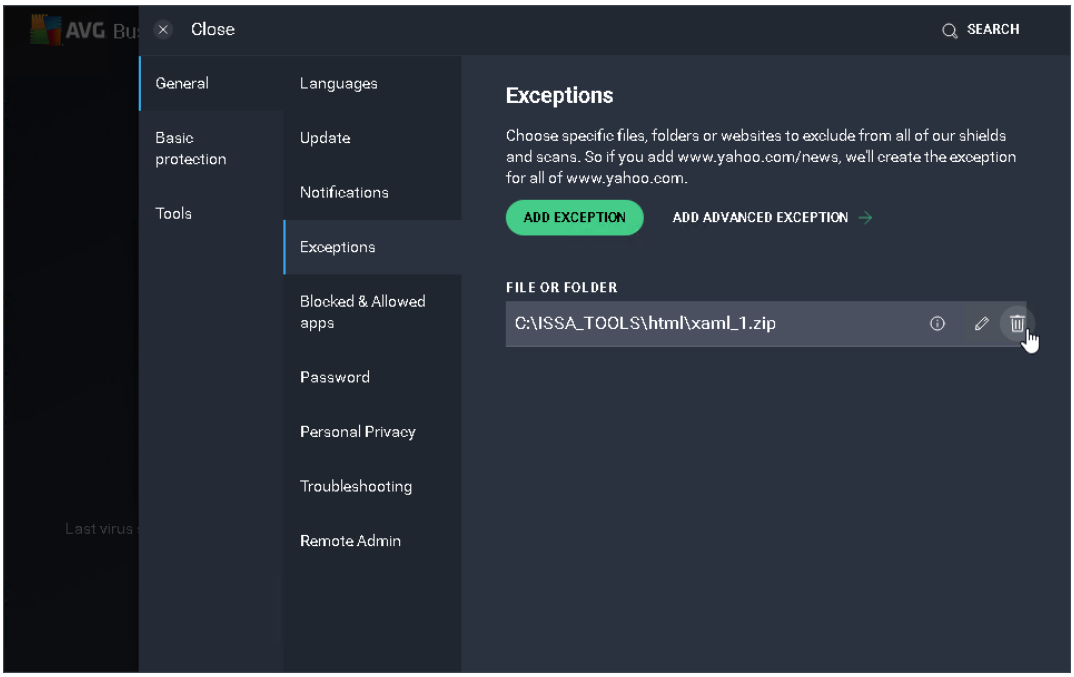
2. **Launch AVG.**

3. **Update** the **AVG Virus Definitions**(the circular arrows icon).

   This will trigger the AVG Settings window to open with the Update tab (General > Update) selected and begin a check for virus definition updates. AVG will download and install any new virus definitions it has populated in its repository since the last update run on this instance.Once the update has completed, AVG should notify you that "Virus definitions are up to date."

4. On the AVG Home page, **click** the **Menu icon** and **select Settings** from the available options.

5. From the General Settings page, **remove** the **exception** for the **xaml_1.zip file.**



Exceptions

6. **Run a File or Folder Scan** on the ISSA_TOOLS folder (**This PC > Local Disk (C:) > ISSA_TOOLS**).

7. When the scan is complete, **review** the **Scan Summary**.

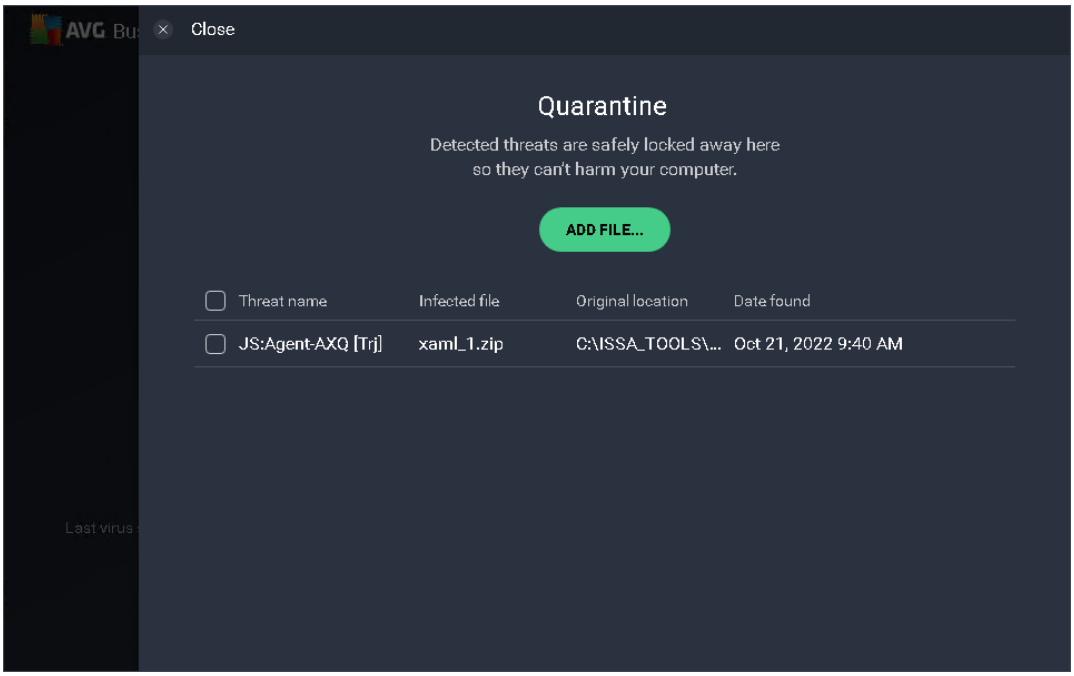
   The Scan Summary displays all threats that the scan identified. Notice that AVG flagged the xaml_1.zip file in the html folder. While a zipped and encrypted file may evade AVG's detection - like prodrev.zip did in Section 1 - a zipped file without encryption can still be detected by a targeted scan.

   AVG identified the virus name and reported that both the infected file (xaml_1.htm, part of the xaml_1.zip file) and the zip file containing the infected file were deleted, and the virus is being held in the AVG Quarantine area.

8. **Make a screen capture** showing the **Scan Summary (Detections) page** and **paste** it into the Lab Report file.

9. **Click** the **Done button** to return the AVG main screen.

10. **Open** the **Quarantine area**.



Quarantine (Virus vault)

Note: The Quarantine area (previously referred to as the Virus Vault) is where all removed files, virus infected or suspicious, are stored until you take action on them. All of the files in the vault are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any deleted file for a certain period of time, so that you can make sure you do not need the file any more. If you find out that the missing file is causing problems, you can send it for analysis, try to heal it, or restore it to the original location.

11. **Empty** the **Quarantine area**.

12. **Make a screen capture** showing the **empty Quarantine area (Virus Vault)** and **paste** it into your Lab Report file.

13. **Close** the **Quarantine Area**.

14. **Close** the **AVG window**.

Part 2: Disabling Unwanted Services

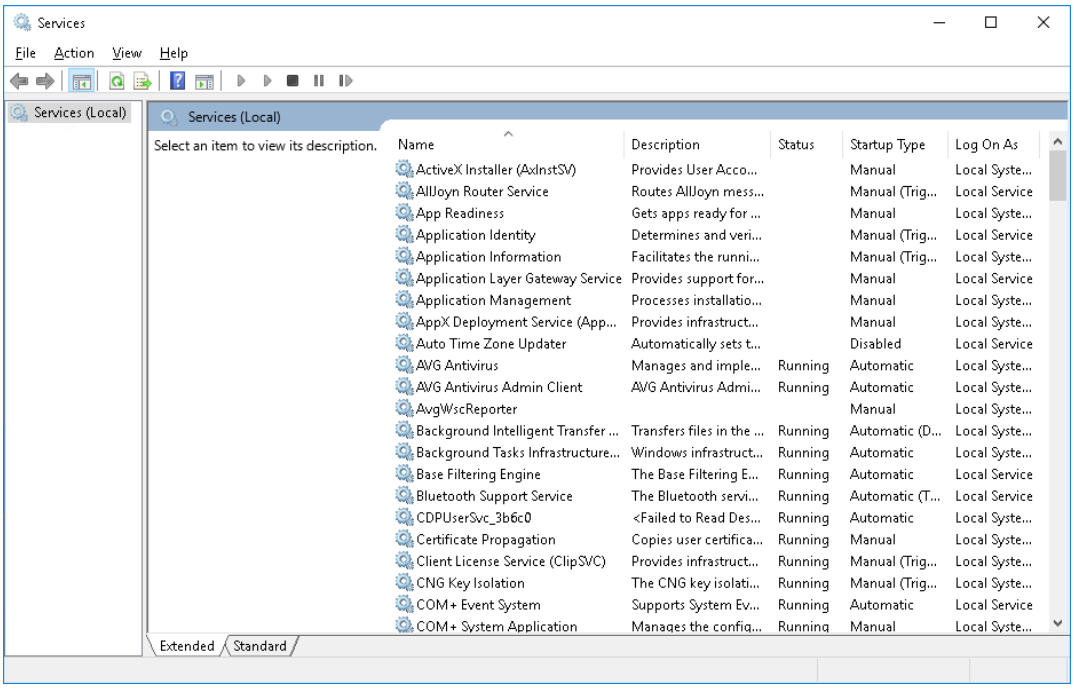
Note: In the next steps, you will document and disable an unwanted service running on the TargetWindows02 virtual machine. Like an up-to-date anti-virus, managing system services is an important element in a given organization's security program. Other elements include (but are not limited to) standardized configurations and settings based on organization-wide security policy definition, a layered security strategy to mitigate the threat from entering the IT infrastructure, email filtering/quarantining, frequency of anti-virus and malicious software prevention tool updates, as well as operating system and application updates to close known vulnerabilities.

1. **Launch** the **Server Manager**.

2. From the Server Manager toolbar, **select Tools > Services** to display a list of the services running on this virtual machine.

   The Startup Type column indicates whether those services start automatically, manually, or have been disabled.

3. **Drag** the **column borders** to view the data in all columns as shown in the following figure.



Local services

4. **Stop** the following services and **set their startup type** to **disabled**:

    - **Bluetooth Support Service**
    - **Print Spooler**
    - **SNMP Trap**

5. **Make a screen capture** showing the **updated list of services** and **paste** it into the Lab Report file.

    You may need multiple screen captures to record the complete list of services.

6. **Close** the **Services window**.

7. **Close** the **Server Manager window**.

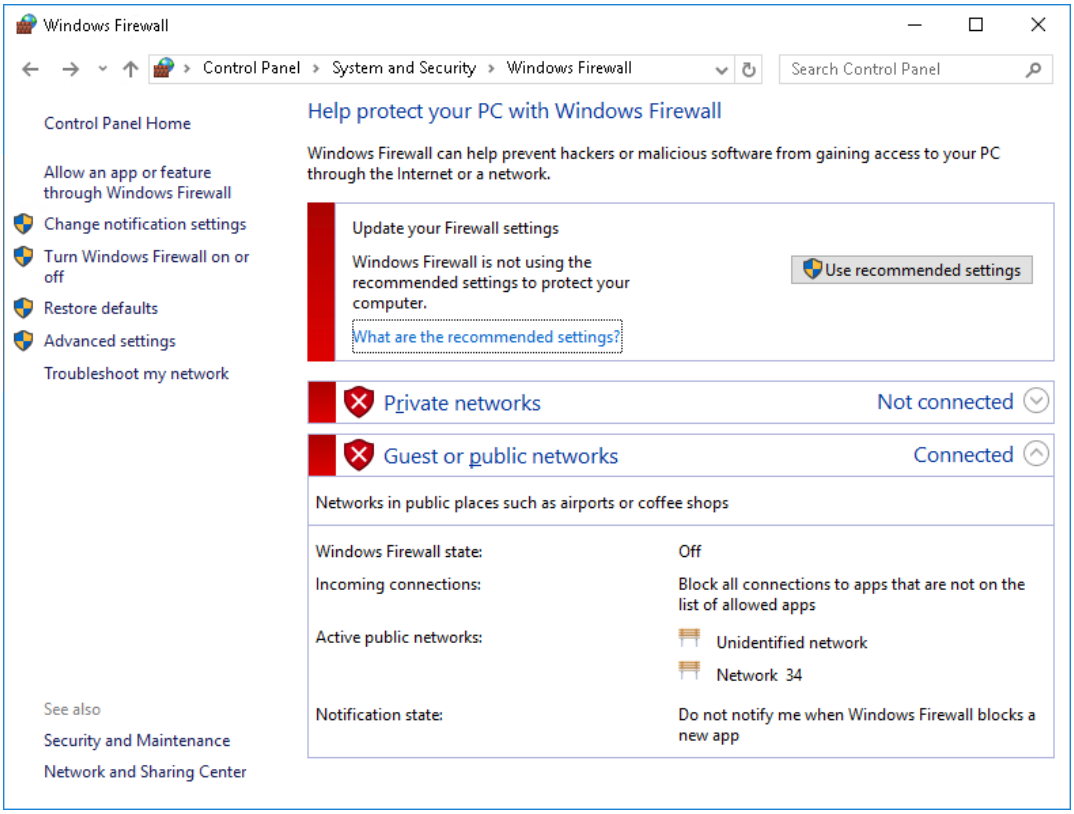
Part 3: Configuring the Windows Firewall

Note: The Windows Firewall with Advanced Security is a personal firewall that filters incoming and outgoing traffic by blocking unauthorized traffic to the local computer. It can be configured to support separate profiles based on whether the computer is connected to a network at the office, or connected at home, or at a public location, such as the local coffee shop. Using the Advanced Security profiles, network traffic can be filtered based on Active Directory users and groups, both source and destination IP addresses, port number, specific programs and services.

Enabled on the network and properly configured, a firewall can block outside sources from being able to insert malware and viruses. By default, the Windows Firewall disables several important services like File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP), which includes the Ping command. In the next steps, you will manually configure the Windows Internal Firewall to enable the ICMP service on the TargetWindows02 machine.

1. **Open** the **Control Panel**.

2. In the Control Panel, **navigate** to **System and Security** > **Windows Firewall**.



Windows Firewall

3. **Activate** the **Windows Firewall**.

4. **Open** the **Advanced Settings console**.

5. **Open** the **Outbound Rules list**.

   This option enables you to set rules for all outbound traffic.

6. **Disable** both **Email and accounts rules**.

7. **Make a screen capture** showing **the updated Email and accounts rules** and **paste** it into the Lab Report file.

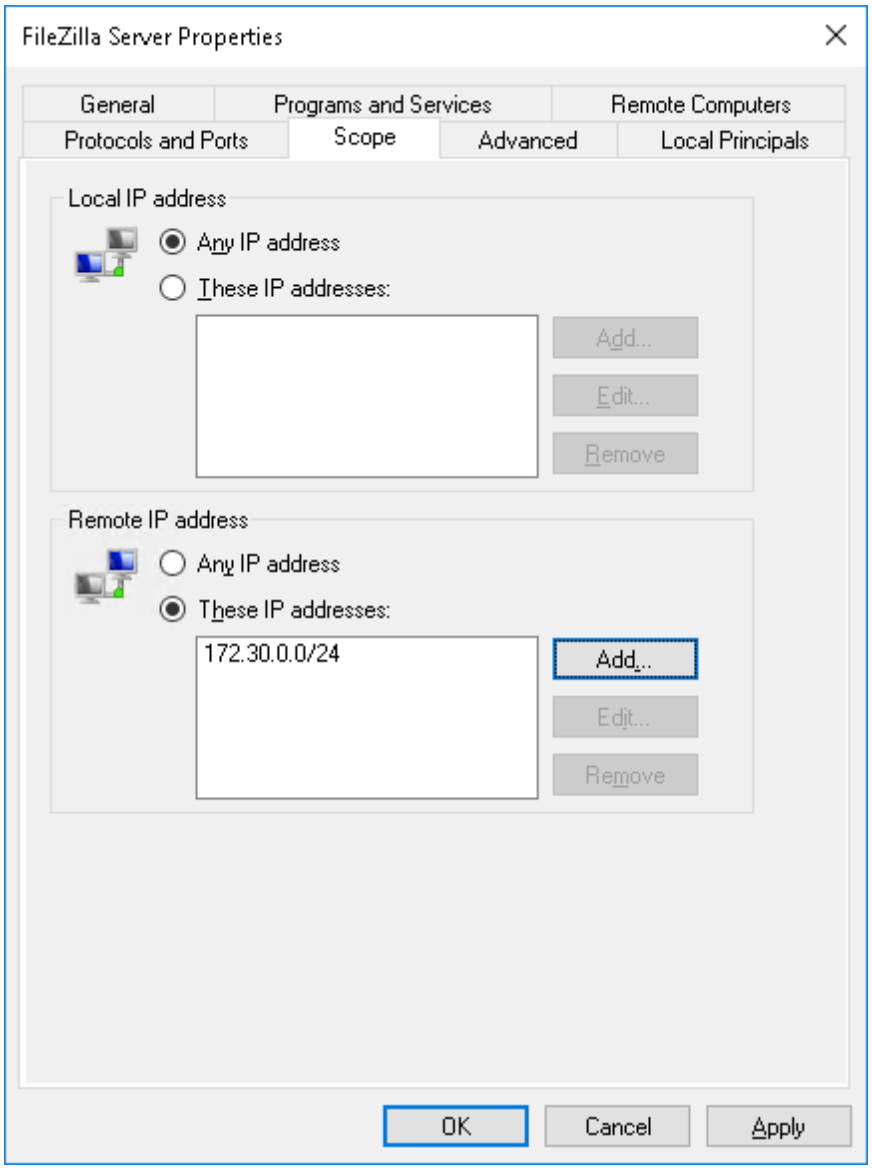
8. **Create** a new **Outbound Rule** that matches the following conditions:

   - Rule Type: **Program**
   - Program path: **C:\Program Files(x86)\FileZilla Server\FileZilla Server.exe**
   - Action: **Allow the connection**
   - Profile: **Domain, Private, and Public**
   - Name: **FileZilla Server**

9. **Make a screen capture** showing the **new FileZilla Server outbound rule** and **paste** it into the Lab Report file.

10. **Open** the **Properties window** for the FileZilla Server Outbound Rule.

11. **Restrict the scope** of the rule to the following remote subnet address: **172.30.0.0/24**



Restrict the scope of a rule

Note: When implementing firewall rules, it is best practice never to issue a wide-open rule (blanket rule) for services such as FTP. Instead, you can create a firewall pinhole with a specific open port, or allow only specific IP addresses to access the services.

12. **Close** the **Windows Firewall with Advanced Security window**.

13. **Close** the **Windows Firewall window**.

14. **Close** the **remote TargetWindows02 connection**.

Note: This completes Section 2 of this lab. There are no deliverable files for this section.

Section 3: Lab Challenge and Analysis

Note: The following questions are provided to allow you the opportunity for independent, unguided research, similar to what you will encounter in a real situation. Some questions will challenge you to find command line syntax for tasks you performed in the lab, others may ask you to extend your learning from the lab. Use screen captures where possible to illustrate your answers.

Part 1: Analysis and Discussion

This lab contained two viruses—one in Section 1 and another in Section 2. Research a virus you encountered in this lab to find a summary of the virus and how it affects the victim's machine.

Part 2: Tools and Commands

Research Windows services. Using the screen captures you made in Part 2 of the lab, identify at least three additional services that could be disabled safely. Explain your choices.

Part 3: Challenge Exercise

Run a virus scan on your own computer using your existing antivirus program. Provide a summary of the findings and the actions you will take to address them; include screenshots as desired. If you do not currently have an antivirus program, research three programs available and compare their features.