Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 9

Investigating and Responding to Security Incidents

**Section 1: Hands-On Demonstration**

Part 1: Prepare an Incident Response Report

From your local computer, download the Sample Security Incident Report from http://www.vlabsondemand.com/issa30/SecurityIncidentReport-Sample.pdf.

Review the Sample Security Incident Report

Use this sample as a guide to determine what actions and information you record throughout the lab. At the end of the lab, you will create your own incident response report.

Part 2: Use Antivirus Software to Scan the Infected System

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

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.

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

Note: It appears that the antivirus software was installed, but not fully configured. There is a high likelihood that the system is infected with some viruses. In the next steps, you will configure the antivirus software enough to scan the system.

On the AVG Home page, click the Fix Now button to enable the antivirus protection on all components.

Graphical user interface, application

Description automatically generated

For the purposes of this lab, you can disregard any notifications to update the virus definitions. In a real-world situation, you would want to ensure your virus definition files are updated on a regular basis, but they have been blocked in this lab to ensure no additional software updates are pushed out.

Note: Many new malware and viruses are detected every day, and anti-virus vendors usually update their anti-virus signature files several times per week. Updating the antivirus software with the latest virus definitions ensures the software has the latest information to identify and quarantine threats. AVG automatically updates the database on a regular basis, as long as the machine is able to reach the Internet or if there is an update server designated in the network. You can manually update the virus signatures on the workstation by clicking the Update Signatures button (the reverse arrow in the lower-right corner). For the purposes of this lab, this functionality has been deactivated.

In addition to updating the database, it is also important to apply any patches to the antivirus software itself. These patches often address vulnerabilities in the application as well. For the purposes of this lab, this functionality has also been deactivated.

On the AVG Home page, click the Scan Computer button to begin the scanning process and remove any identified threats.

A green logo with white text

Description automatically generated with medium confidence

By default, AVG will scan the whole computer. This process will take approximately 15-20 minutes to complete. Do not touch any keys until the scan is finished. When the scan has completed, AVG will display a Scan Summary showing the number of threats that have been identified and removed. The number of threats identified and removed is listed at the top of the Scan Summary.

When the scan is complete, review the Scan Summary.

Make a screen capture showing the Scan Summary (Detections) and paste it into your Lab Report file

A screenshot of a computer

Description automatically generated

Part 3: Investigate and Remove the Identified Threats

On the Scan Summary page, hover your cursor over one of the threats associated with the achtung.exe file to view additional details about this threat.

Each threat identified by AVG is given a threat severity rating of high, medium, and low. The page also indicates whether the threat was removed (green checkmark) or not removed (red exclamation mark) from your computer.

Note: Once you have the name and details for a virus, you can use that information to search the antivirus company’s web site or the Internet, in general, for more information about how the virus may have entered your network in the first place. You can take measures to protect yourself from a recurrence.

Make a screen capture showing the achtung.exe threat and paste it into your Lab Report file.

Graphical user interface, text, application

Description automatically generated

On your local computer, open a new Internet browser session.

Note: Because this lab contains live viruses, the virtual machines have been isolated from the Internet; you will need to conduct your research on your local machine.

From your favorite search engine, search for the achtung.exe threat identified by AVG.

Note: The Virus Encyclopedia, provided by the AVG Signal Blog, at https://www.avg.com/en/signal/what-is-a-computer-virus, is a useful resource for learning about viruses.

In your Lab Report file, document any information you discover about eradicating this threat.

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

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

Graphical user interface, text, application

Description automatically generated

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 quarantine area are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any suspicious file for a certain period of time, so that you can make sure you do not need the file anymore and manually delete it. If you find that AVG has quarantined a valid file (a false positive), it can be restored easily from this interface.

If you are assigned a lab assessment quiz, please note that one of the questions asks the name of the area where all removed files are stored until you take action on them. Virus Vault and Quarantine area are both provided as possible answers. This question has been removed from the latest version of the quiz, but if you encounter this question and your instructor has not manually edited the test bank, the correct answer will be Virus Vault. Avast changed the name of this feature in recent versions of AVG.

On the Quarantine page, click the Select All Viruses checkbox to select all viruses in the Quarantine area.

Graphical user interface

Description automatically generated

On the Quarantine page, click the Delete button to delete all viruses, malware, and malicious software detected by the application.

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

Graphical user interface, application

Description automatically generated

On the Quarantine page, click the Close button to close the Quarantine area and return to the AVG Home page.

Close the AVG window.

Use the information you documented in your Lab Report file to complete the Security Incident Report.

You should use the sample report you downloaded earlier in the lab as a template.

Save the Security Incident Report as yourname\_S1\_SecurityIncidentReport, replacing yourname with your own name, and submit it with your lab deliverables.

**Section 2: Applied Learning**

Part 1: Prepare an Incident Response Report

On your local computer, download the Sample Security Incident Report from http://www.vlabsondemand.com/issa30/SecurityIncidentReport-Sample.pdf.

Review the Sample Security Incident Report.

Use this sample as a guide to determine what actions and information you record throughout the lab. At the end of the lab, you will create your own incident response report.

Part 2: Use Antivirus Software to Scan the Infected System

Open a remote connection to the TargetWindows02 machine.

Open the AVG antivirus application.

Note: It appears that the antivirus software was installed but not fully configured. There is a high likelihood that the system is infected with some viruses. In the next steps, you will configure the antivirus enough to scan the system.

From the AVG Home page, open the Menu, select Settings, and navigate to the Remote Admin page.

Graphical user interface, application

Description automatically generated

On the Remote Admin page, set the server to avg.securelabs.com, then apply the changes to return to the AVG Home page.

Graphical user interface, text, application

Description automatically generated

Click the Fix Now button to enable antivirus protection on all components.

**A picture containing graphical user interface

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

Do not update AVG itself or follow any prompts to Restart the Computer. While AVG can be updated to a newer version, newer versions of AVG may not work with the instructions in this lab guide.

Note: Since your company has a secure license and update server and you just completed configuring the AVG anti-virus application to communicate with the license server, you will notice that AVG is in all GREEN for being in full protection mode and ready to scan.

Run a Deep Scan on the entire TargetWindows02 machine.

By default, AVG will scan the whole computer. This process will take approximately 15-20 minutes to complete. Do not touch any keys until the scan is finished. When the scan has completed, AVG will display a Scan Summary showing the number of threats that have been identified and removed. The number of threats that have been identified and removed is listed at the top of the Scan Summary.

Review the Scan Summary.

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

Graphical user interface, text

Description automatically generated

Part 3: Investigate and Remove the Identified Threats

Review the threat details for one of the threats associated with the KEYCOPY.COM file.

Each threat identified by AVG is given a threat severity rating of high, medium, and low. The page also indicates whether the threat was removed (green checkmark) or not removed (red exclamation mark) from your computer.

Make a screen capture showing the KEYCOPY.COM threat details and paste it into your Lab Report file.

Graphical user interface, text, application

Description automatically generated

On your local computer, open a new Internet browser session.

Using your favorite search engine, search for the KEYCOPY.COM threat identified by AVG

Note: The Virus Encyclopedia, provided by the AVG Signal Blog, at https://www.avg.com/en/signal/what-is-a-computer-virus, is a useful resource for learning about different types of viruses.

In your Lab Report file, document any information you discover about eradicating this threat.

On TargetWindows02, close the AVG Scan Summary and return to the AVG Home page.

Open the Quarantine area.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

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 quarantine area are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any suspicious file for a certain period of time, so that you can make sure you do not need the file anymore and manually delete it. If you find that AVG has quarantined a valid file (a false positive), it can be restored easily from this interface.

Empty the Quarantine area to delete all viruses, malware, and malicious software detected by the application.

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, application

Description automatically generated

Close AVG, then use the information you documented in your Lab Report file to complete the Security Incident Report following the Sample template you downloaded at the beginning of the lab.

Save the Security Incident Report as yourname\_S2\_SecurityIncidentReport and submit it with your lab deliverables.