**NAME:**

**Lab #1 (Required): Identifying and Removing Malware on a Windows System**[[1]](#footnote-1)\*

**Introduction to Information Security (IST323)**

**School of Information Studies**

**Syracuse University**

**Disclaimer:** The contents of this document are solely for educational purpose. Misused knowledge of this lab may result in damage of data, security breach, privacy violation, or other undesirable situations. Therefore, using knowledge of this lab other than for the original purpose is prohibited.

**Learning Objectives**

In this lab, you will use a scanner to identify the viruses, worms, Trojans, malware, or other malicious software found on a compromised Windows machine. You will complete a scan of the entire computer, learn how to exclude folders to avoid false positives, and understand the importance of maintaining the signatures database. You will discover the difference between a full computer scan and a Resident Shield scan. Finally, you will also permanently remove the malware identified by the antivirus software and schedule the scan to run automatically.

Upon completing this lab, you will be able to:

* Identify malware and other malicious software on a Windows desktop using antivirus software.
* Exclude specific drives or folders from an antivirus scan to prevent false positives.
* Detect a hidden virus embedded in a PDF document.
* Quarantine malware and other malicious software for further investigation and removal.
* Recommend remediation steps for mitigating malware found by an antivirus scan.

**Lab Structure**

This lab has the following parts, which should be completed in the order specified.

1. In the first part of this lab, you will use AVG (Anti-Virus Guard) to scan the vWorkstation and download a copy of the scan results.
2. In the second part of this lab, you will use AVG's Resident Shield feature to identify a threat in an encrypted archive file.
3. In the third part of this lab, you will permanently remove malware quarantined by AVG and schedule the scan to run automatically.

**Tools and Software**

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

* AVG (Anti-Virus Guard) AntiVirus Business Edition

**Lab Submission**

* Convert this file to pdf and submit your deliverables through Blackboard/Assignment Submission.
* The screenshots should be readable.
* Make sure you include all the items required in your report.

**Student Deliverables**

**SECTION 1**

***Part 1: Use Antivirus Software to Scan the Infected System***

Document the threat details for the first high severity threat reported by AVG

Contents of the *yourname*\_S1\_AVGscan file

[PASTE SCREENSHOT HERE]

***Part 2: Identify Threats in Encrypted Archive Files***

Pdfka-FC threat detection in the FileSystemShield file

[PASTE SCREENSHOT HERE]

***Part 3: Manage AVG Scans and the Quarantine area***

empty Quarantine area (Virus Vault)

[PASTE SCREENSHOT HERE]

Scheduled scan

[PASTE SCREENSHOT HERE]

**SECTION 2**

***Part 1: Use Antivirus Software to Scan the Infected System***

Document threat details

[PASTE SCREENSHOT HERE]

Summary information at the top of the *yourname*\_S2\_AVGscan file

[PASTE SCREENSHOT HERE]

***Part 2: Identify Threats in Encrypted Archive Files***

Threat details

[PASTE SCREENSHOT HERE]

Contents of the FileSystemShield file

[PASTE SCREENSHOT HERE]

***Part 3: Manage AVG Scans and the Virus Vault***

Empty Quarantine area (Virus Vault)

[PASTE SCREENSHOT HERE]

Scheduled scan

[PASTE SCREENSHOT HERE]

**Challenge Question Answers (Optional):**

1. Using Google, research WinNuke and why it is considered dangerous at its time of release, then write a paragraph on your opinion of why this is still dangerous or why it is not dangerous.
2. Use the Internet to identify three commercially available antivirus software distributions for home users. Compare the features of each and describe which one you would choose for your own purposes, and why.
3. In the File Explorer, navigate to the C:\viral\_DONOTTOUCH folder and extract the archive files contained in the subfolders of that directory. Do not extract the files into the C:\viral\_DONOTTOUCH folder. What is the result? Explain.

**Lessons Learned:**

*Provide 2 paragraphs on what you feel is important about the lab. And share 3 bullet points of your main takeaways.*

1. \* Customized lab manual by Dr. Joon S. Park at the School of Information Studies for the virtual online labs provided by Jones & Bartlett Learning. [↑](#footnote-ref-1)