

Lab #9 – Assessment Worksheet

Eliminating Threats with a Layered Security Approach

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you used AVG, an antivirus scanning program, to identify malware found on a compromised system. You also examined the services available on the Windows vWorkstation machine and disabled an unnecessary service. In addition, you configured the Windows Firewall, enabled ICMP traffic, and created a new rule for the FileZilla Server application.

Lab Assessment Questions & Answers

1. What is the main difference between a virus and a Trojan?
2. A virus or malware can impact which of the three tenets of information systems security (confidentiality, integrity, or availability)? In what way?
3. Why is it recommended to do an antivirus signature file update before performing an antivirus scan on your computer?
4. Why might your coworker suggest encrypting an archive file before e-mailing it?
5. What kind of network traffic can you filter with the Windows Firewall with Advanced Security?
6. What are typical indicators that your computer system is compromised?
7. What elements are needed in a workstation domain policy regarding use of antivirus and malicious

2 | Lab #9: Eliminating Threats with a Layered Security Approach

software prevention tools?