Assessment Worksheet

Eliminating Threats with a Layered Security Approach

Course and Section: CIS481-20

Student Name: James Ryg

Lab Due Date: 6/19/2016

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

- What is the main difference between a virus and a Trojan?

A virus is a generic term, describing malware as a catch-all term, but more specifically is any malicious software that has the capability of spreading, and also has the ability to manipulate normal systems operation. In comparison, a trojan horse appears as useful software, but when executed, also executes its malicious code, but do not tend to self propogate.

- A virus or malware can impact which of the three tenets of information systems security (confidentiality, integrity, or availability)? In what way?

Malware can all easily negatively impact availability by reducing the stability of the system, or bringing it down in its entirety. In addition, it threatens the integrity of the data by having the capability to edit files, or even damage the hardware storage medium. Finally, confidentiality can be breached by malware opening the system up to external attack, or allowing someone who already succeeded to access files on a system.

- Why is it recommended to do an antivirus signature file update before performing an antivirus scan on your computer?

Most antivirus suites use signatures left by malware to detect, and enable quarantining of the affected files. Without a current signature file, which is updated multiple times a week, antivirus software would be unable to respond to new threats.

- Why might your coworker suggest encrypting an archive file before e-mailing it?

Encrypting a file would allow sharing an archive between two users, and can reduce the risk of threatened confidentiality during transit. In addition, once that is complete, a secondary exchange including the key must occur, making it have the same security benefit as a symmetric encryption configuration.

- What kind of network traffic can you filter with the Windows Firewall with Advanced Security?

Using windows firewall, you can filter application traffic, including system services. In addition, you can differentiate between certain general behaviors specific to the application as well.

- What are typical indicators that your computer system is compromised?

Generally, signs such as abnormal system behavior, modification of user preferences, as well as an impact on performance are good signs of a compromised system. The book also notes that on a security administration approach, modified logs, as well as evidence of reconnaisance are clear indicators.

- What elements are needed in a workstation domain policy regarding use of antivirus and malicious software prevention tools?

A workstation domain policy should encompass procedures that ensure that the requisite tools are installed. For instance, requiring proper configuration and operation before being able to access any resources that require authorization is a good first step. In addition, the policy should enforce a requirement for up-to-date versions as well.