

Lab #9 – Assessment Worksheet

Investigating and Responding to Security Incidents

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you acted as a member of the incident response team who had been assigned an incident response in the form of a help desk trouble ticket. You followed the phases of a security incident response to investigate the event, contain the malware, eradicate the suspicious files, re-test the system in readiness for returning it to service, and complete a detailed security incident response report in the provided template. You used AVG AntiVirus Business Edition to scan the infected workstation and documented your findings as you proceeded.

Lab Assessment Questions & Answers

1. When you are notified that a user's workstation or system is acting strange and log files indicate system compromise, what is the first thing you should do to the workstation or system and why?
2. When an antivirus program identifies a virus and quarantines this file, has the malware been eradicated?
3. What is the SANS Institute's six-step incident handling process?
4. What is the risk of starting to contain an incident prior to completing the identification process?
5. Why is it a good idea to have a security policy that defines the incident response process in your organization?
6. The post-mortem "lessons learned" step is the last in the incident response process. Why is this the most important step in the process?

2 | Lab #9: Investigating and Responding to Security Incidents