Lab #9 - Assessment Worksheet

Investigating and Responding to Security Incidents

Course Name and Number: ITNET 280 - Ethical Hacking

Student Name: Connor Morrissy

Instructor Name: Darnell Payne

Lab Due Date: -

Lab Assessment Questions & Answers

1. When you are notified that a user's workstation or system is acting strangely and log files indicate system compromise, what is the first thing you should do to the workstation or system and why?

   Disconnect it from the network so nothing can spread to other devices.

2. When an antivirus program identifies a virus and quarantines this file, has the malware been eradicated?

   No.

3. What is the SANS Institute's six-step incident handling process?

   Preparation, Identification, Containment, Eradication, Recovery, and Lessons learned.

4. What is the risk of starting to contain an incident prior to completing the identification process?

   There can be hidden files and objects that are open that need to be found and fixed and you probably don't have all the information about the risk.

5. Why is it a good idea to have a security policy that defines the incident response process in your organization?

   This way everyone in the company knows or has reference to how to handle an incident.

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?

   Because this way, you and coworkers will learn from it and know how to prevent or handle a similar situation in the future.