Lab 10 - Assessment Worksheet

Investigating and Responding to Security Incidents

Course Name and Number: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Lab Assessment Questions

1. List five types of system information that can be obtained from the Windows Task Manager. How can you use this information to confirm the presence of malware on a system? (*Hint: Look at the bandwidth and CPU utilization.*)

2. Windows Task Manager and Windows Computer Manager both provide information about system services. Compare and contrast the types of information (about system services) that can be obtained from these tools.

3. Explain how you could use one or more of the Windows log (Application, Security, Setup, System, and Forwarded Events logs) files to investigate a potential malware infection on a system. What types of information are available to you in your chosen log file?

4. Should you filter log files during an investigation into a security incident? Why or why not?

5. Should remote desktop services be enabled on employee workstations for use by IT Help Desk personnel? Why or why not?

6. How does Microsoft Baseline Security Analyzer (MBSA) differ from Windows Update? Why are Shares a source of system vulnerabilities?