Lab #10 – Assessment Worksheet

Investigating and Responding to Security Incidents

Course Name and Number: ITN263

Student Name: Afeefah Manzoor

Instructure Name:

Lab Due Date: 9/11/20

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.)

Performance,

processes,

networking,

users,

services,

1. 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.

Computer management shows the users all the software and hardware that is operational while task manager shows what programs are currently running and any backgrounds apps/software that are running.

1. 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?

the user can use log files to identify malware from the incident logs that were made, which should tell the user when something was downloaded/uploaded.

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

If the admin knows what they are looking for then they should use the filter but if they do not know then they should not use the filter.

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

The remote desktop services be used with limitations and she be logged in the event something were to happen to the systems.

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

Windows updates only download and install patches. MBSA scans and ID’s vulnerabilities and report it to whoever conducts the scans and shares what can become a weak spot.