CYBS 7357 Lab 10 Quiz

\* Answers are highlighted in yellow

1. Which of the following statements is true regarding security incidents?

a. Security incidents cannot occur when security measures such as firewalls, properly configured VPNs, and secure network procedures are in place.

b. Security incidents can arise from a number of sources, including human error or mistakes.

c. Deliberate actions that cause loss or harm to the organization are not considered security incidents.

d. Organizations must simply learn to live with the impact and associated costs of security incidents.

2. The five-step formula that serves as the basis for incident response processes and procedures includes:

a. accept, adjust, adapt, acclimate, and relate to security incidents.

b. refute, deter, discourage, defend, and correct security incidents.

c. identify, research, reject, process, and detail security incidents.

d. prevent, detect, respond, control, and document security incidents.

3. What types of automated tools provide information about the current operating state of a computer system?

a. System configuration tools

b. System information tools

c. System administration tools

d. System analysis tools

4. What types of automated tools are used to scan an operating system and key software applications for security issues?

a. System configuration tools

b. System information tools

c. System administration tools

d. System analysis tools

5. Windows Computer Management and Windows Task Manager are what type of tools?

a. System configuration tools

b. System information tools

c. System administration tools

d. System analysis tools

6. Microsoft Baseline Security Analyzer (MBSA) is a:

a. system configuration tool.

b. system information tool.

c. system administration tool.

d. system analysis tool.

7. Which tool provides information about currently running tasks, use of system resources, and system performance?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Windows Computer Management

c. Windows 2012

d. Windows Task Manager

8. Which tool provides detailed information about the system, including lists of services and their current state, computer hardware configuration, security and system events, and scheduled tasks?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Windows Computer Management

c. Windows 2012

d. Windows Task Manager

9. Which tool checks for system administration and misconfiguration problems, application software issues including missing patches and updates, and missing or partially installed system security updates?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Windows Computer Management

c. Windows 2012

d. Windows Task Manager

10. Microsoft Baseline Security Analyzer (MBSA) is a system scanning tool that scans workstations and servers running:

a. any operating system.

b. Linux.

c. Windows.

d. Linux, Apple OS X, or Windows.

11. Which of the following statements is true regarding gathering system performance information?

a. System performance information supplements information gathered by automated tools.

b. It is poor practice for an IT Help Desk to ask an end user to perform any information gathering tasks.

c. A support technician should not provide instruction to a user on how to enable remote desktop services.

d. A support technician should not use a remote log in to gather information and run tests on a user’s workstation.

12. Which of the following statements is true regarding remote desktop services?

a. Remote desktop services should not be used to gather system performance information.

b. Remote desktop services typically cost an organization a significant amount of time and money.

c. Remote desktop services typically require several desk-side support visits by IT Help Desk technicians.

d. Remote login services can become a vulnerability that is exploited both internally and externally.

13. Processes, Performance, Users, Details, and Services are the five types of system information that can be obtained from the:

a. Windows Task Manager.

b. Windows Desktop.

c. Windows Event Viewer.

d. Microsoft Baseline Security Analyzer (MBSA).

14. Which Windows log records information about events, including successful operations, system warnings, error messages about failed operations, and information about both successful and unsuccessful logon attempts?

a. The Setup Log

b. The Security Log

c. The Application Log

d. The System Log

15. Which of the following statements is true regarding filtering log files?

a. Filters should not be used on log files during an investigation into a security incident.

b. Most log files are easily scanned by eye when looking for evidence.

c. Using a filter can help an analyst to quickly find events of interest.

d. The drawback to using filtering is that it increases the number of entries.

16. Which Windows log contains information about system security status?

a. The Setup Log

b. The Security Log

c. The Application Log

d. The System Log

17. Which Windows log contains information about system startup, shutdown, and status changes for key system processes?

a. The Setup Log

b. The Security Log

c. The Application Log

d. The System Log

18. Which of the following provides brief descriptions of services and their statuses and also provides the name and process ID (PID) for each service that is running?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Windows Application Manager

c. Windows Computer Management

d. Windows Task Manager

19. Which of the following provides detailed information about each service and also provides the startup type (automatic, automatic/delayed start, disabled, manual) and logon information (logon as local service, local system, and network service)?

a. Microsoft Baseline Security Analyzer (MBSA)

b. Windows Application Manager

c. Windows Computer Management

d. Windows Task Manager

20. Which of the following statements is true regarding Microsoft Baseline Security Analyzer (MBSA)?

a. In the lab, you used MBSA to scan Internet Explorer and Microsoft Office for vulnerabilities.

b. MBSA can be configured to check for missing updates and recommended security settings on Linux servers.

c. Windows Update is more powerful than MBSA because it checks system and software settings in the registry in addition to checking for required software updates.

d. MBSA generates a report that identifies security issues and provides recommendations for system configuration changes.

NAME:

Natnael kebede