IT Essentials (ITE v6.0) Chapter 12 Exam Answers 100% 2016

1. **Which two security precautions will help protect a workplace against social engineering? (Choose two.)**

- performing daily data backups
- encrypting all sensitive data stored on the servers
- registering and escorting all visitors to the premises
- ensuring that all operating system and antivirus software is up to date
- ensuring that each use of an access card allows access to only one user at the time

2. **Which two characteristics describe a worm? (Choose two.)**

- executes when software is run on a computer
- is self-replicating
- hides in a dormant state until needed by an attacker
- infects computers by attaching to software code
- travels to new computers without any intervention or knowledge of the user

3. **Which type of security threat uses email that appears to be from a legitimate sender and asks the email recipient to visit a website to enter confidential information?**

- adware
- phishing
- stealth virus
- worm

4. **What is the primary goal of a DoS attack?**

- to facilitate access to external networks
- to prevent the target server from being able to handle additional requests
- to obtain all addresses in the address book within the server
- to scan the data on the target server

5. **Which type of attack involves the misdirection of a user from a legitimate web site to a fake web site?**

- SYN flooding
- DDoS
- DNS poisoning
- spoofing

6. **Which password is the strongest?**

- qwerty
- Abc123
- Im4ging!
- Gd^7123e!
- pAssword

7. **Which three questions should be addressed by organizations developing a security policy? (Choose three.)**

- What assets require protection?
- How should future expansion be done?
- What is to be done in the case of a security breach?
- When do the assets need protecting?
- What insurance coverage is required?
- What are the possible threats to the assets of the organization?

8. **The XYZ company has decided to upgrade some of its older PCs. What precaution should the company take before the disposal of the remaining older computers?**

- Perform a high-level format of the hard drive.
- Remove the RAM from the motherboard.
- Data wipe the hard drive.
- Destroy the monitor.
- Remove the CPU.

9. **Which two file-level permissions allow a user to delete a file? (Choose two.)**

- Read
- Modify
- Read and Execute
- Write
- Full Control
- List Contents

10. **What is the name given to the programming-code patterns of viruses?**

- grayware
- mirrors
- signatures
- virus definition tables

11. **What is the most effective way of securing wireless traffic?**

- WPA2
- SSID hiding
- WEP
- wireless MAC filtering

12. **Port triggering has been configured on a wireless router. Port 25 has been defined as the trigger port and port 113 as an open port. What effect does this have on network traffic?**

- Any traffic that comes into port 25 allows outgoing port 113 to be used.
- All traffic that is sent into port 25 to the internal network will also be allowed to use port 113.
- Any traffic that is using port 25 going out of the internal network will also be allowed to transmit out port 113.
- All traffic that is sent out port 25 will open port 113 to allow inbound traffic into the internal network through port 113.

13. **What are two physical security precautions that a business can take to protect its computers and systems? (Choose two.)**

- Perform daily data backups.
- Implement biometric authentication.
- Lock doors to telecommunications rooms.
- Replace software firewalls with hardware firewalls.
- Ensure that all operating system and antivirus software is up to date.

14. **What is the minimum level of Windows security required to allow a local user to restore backed up files?**

- Write
- Read
- Create
- Full

15. **What is the purpose of the user account idle timeout setting?**

- to log a user out of a computer after a specified amount of time
- to display a timeout message if a user has not typed a keystroke in a particular amount of time
- to turn the computer off if the user has not typed anything after a specified amount of time
- to create a log message of how long the computer was not used

16. **Which two security procedures are best practices for managing user accounts? (Choose two.)**

○ Disable authentication.
○ Limit the number of failed login attempts.
○ Restrict the time of day that users can log into a computer.
○ Enable AutoRun.
○ Enable port forwarding.

17. **Which Windows Firewall option allows the user to manually allow access to the ports required for an application to be allowed to run?**

○ Manage Security Settings
○ Automatically
○ Turn off Windows firewall
○ Turn on Windows firewall

18. **Which two Windows default groups are allowed to back up and restore all files, folders, and subfolders regardless of what permissions are assigned to those files and folders? (Choose two.)**

○ Administrators
○ Power Users
○ Backup Operators
○ Access Control Assistants
○ Cryptographic Operators

19. **A manager approaches a PC repair person with the issue that users are coming in to the company in the middle of the night to play games on their computers. What might the PC repair person do to help in this situation?**

○ Limit the login times.
○ Use Event View to document the times logged in and out of the computer.
○ Use Device Manager to limit access to the computer.
○ Enable power on passwords in the BIOS.

20. **Which question would be an example of an open-ended question that a technician might ask when troubleshooting a security issue?**

○ Is your security software up to date?
○ Have you scanned your computer recently for viruses?
○ Did you open any attachments from a suspicious email message?
○ What symptoms are you experiencing?

21. **Which action would help a technician to determine if a denial of service attack is being caused by malware on a host?**

- Disconnect the host from the network.
- Log on to the host as a different user.
- Disable ActiveX and Silverlight on the host.
- Install rogue antivirus software on the host.

22. **A technician is troubleshooting a computer security issue. The computer was compromised by an attacker as a result of the user having a weak password. Which action should the technician take as a preventive measure against this type of attack happening in the future?**

- Check the computer for the latest OS patches and updates.
- Verify the physical security of all offices.
- Ensure the security policy is being enforced.
- Scan the computer with protection software.

23. **It has been noted that the computers of employees who use removable flash drives are being infected with viruses and other malware. Which two actions can help prevent this problem in the future? (Choose two.)**

- Set virus protection software to scan removable media when data is accessed.
- Configure the Windows Firewall to block the ports that are used by viruses.
- Disable the autorun feature in the operating system.
- Repair, delete, or quarantine the infected files.
- Enable the TPM in the CMOS settings.

24. **A virus has infected several computers in a small office. It is determined that the virus was spread by a USB drive that was shared by users. What can be done to prevent this problem?**

- Destroy the USB drive.
- Activate Windows Firewall.
- Change the passwords on the computers.
- Set the antivirus software to scan removable media.

25. **A user is browsing the Internet when a rogue pop-up warning message appears indicating that malware has infected the machine. The warning message window is unfamiliar, and the user knows that the computer is already protected by antimalware software. What should the user do in this situation?**

- Allow the software to remove the threats.
- Click the warning window to close it.

- Update the current antimalware software.
- Close the browser tab or window.

26. **In what situation will a file on a computer using Windows 8.1 keep its original access permissions?**

- when it is copied to the same volume
- when it is moved to the same volume
- when it is copied to a different volume
- when it is moved to a different volume

27. **What security measure can be used to encrypt the entire volume of a removable drive?**

- EFS
- TPM
- BitLocker To Go
- NTFS permission

28. **A user calls the help desk reporting that a laptop is not performing as expected. Upon checking the laptop, a technician notices that some system files have been renamed and file permissions have changed. What could cause these problems?**

- The file system is corrupted.
- The laptop is infected by a virus.
- The display driver is corrupted.
- The file system has been encrypted.