

3 juni 2013



"WE ARE ANONYMOUS, WE ARE LEGION, WE DO NOT FORGIVE, WE DO NOT FORGET. EXPECT US."

[KUNCI CHAPTER 10 IT ESSENTIALS: PC HARDWARE AND SOFTWARE]

Manfaatkan sebaik mungkin yeah kawan – kawan ku tercinta :) :D :*

1. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?
social engineering
2. Which two security precautions will help protect a workplace against social engineering?
ensuring that each use of an access card allows access to only one user at the time.
registering and escorting all visitors to the premises.
3. What are two typical physical security precautions that a business can take to protect its computers and systems?
Implement biometric authentication.
Disable the autorun feature in the operating system.
4. Which physical security technology can hold user authentication information, include software license protection, provide encryption, and provide hardware and software authentication that is specific to the host system?
Trusted Platform Module (TPM)
5. 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?
Set virus protection software to scan removable media when data is accessed.
Disable the autorun feature in the operating system.
6. In which situation would a computer technician use the **fixmbr** command at the command prompt of a Windows XP computer to resolve a security issue?
when a virus has damaged the master boot record of the system disk
7. All users working with a particular Windows 7 computer are able to install unauthorized software. In addition to educating the users about correct security behavior, which action should also be performed to solve this issue?
Enable UAC on the computer.
8. You want to dispose of a 2.5 terabyte hard drive that contains confidential financial information. What is the recommended procedure to achieve this?
Smash the platters with a hammer.
9. What is the most effective way of securing wireless traffic?
WPA2
10. Which two items are used in asymmetric encryption?
a private key
a public key
11. Which two characteristics describe a worm?
is self-replicating.
travels to new computers without any intervention or knowledge of the user.

12. 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?
phishing
13. Which three questions should be addressed by organizations developing a security policy?
What are the possible threats to the assets of the organization?
What is to be done in the case of a security breach?
What assets require protection?
14. What does a malware detection program look for when running a scan?
patterns in the programming code of the software on a computer
15. 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?
All traffic that is sent out port 25 will open port 113 to allow inbound traffic into the internal network through port 113.
16. Which two characteristics of network traffic are being monitored if a network technician configures the company firewall to operate as a packet filter?
protocols
ports
17. What is the primary goal of a DoS attack?
to prevent the target server from being able to handle additional requests
18. Which question would be an example of an open-ended question that a technician might ask when troubleshooting a security issue?
What symptoms are you experiencing?
19. 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.
20. 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?
Ensure the security policy is being enforced.
21. A user has reported that a computer web browser will not display the correct home page even if the default page is reset. What is the likely cause of this problem?
The computer has been infected with spyware.
22. What is the name given to the programming-code patterns of viruses?
signatures