Exam : CompTIA SY0-201

Title : CompTIA Security+(2008 Edition) Exam

Update : Jan-02-2009

1. All of the following provide confidentiality protection as part of the underlying protocol EXCEPT:
A.SSL.
B.SSH.
C.L2TP.
D.IPSec.WBerlin Sans FBArialZX
ANSWER: C

2. Which of the following allows an attacker to manipulate files by using the least significant bit(s) to secretly embed data?
A.Steganography
B.Worm
C.Trojan horse
D.VirusWBerlin Sans FBArialZX
ANSWER: A

3. Which of the following type of attacks would allow an attacker to capture HTTP requests and send back a spoofed page?
A.Teardrop
B.TCP/IP hijacking
C.Phishing
D.Replay WBerlin Sans FBArialZX
ANSWER: B

4. How should a company test the integrity of its backup data?
A.By conducting another backup
B.By using software to recover deleted files
C.By restoring part of the backup
D.By reviewing the written proceduresWBerlin Sans FBArialZX
ANSWER: C

5. Which of following can BEST be used to determine the topology of a network and discover unknown devices?
A.Vulnerability scanner
B.NIPS
C.Protocol analyzer
D.Network mapperWBerlin Sans FBArialZX
ANSWER: D

6. When should a technician perform penetration testing?
A.When the technician suspects that weak passwords exist on the network
B.When the technician is trying to guess passwords on a network
C.When the technician has permission from the owner of the network
D.When the technician is war driving and trying to gain accessWBerlin Sans FBArialZX

ANSWER: C

7. An administrator has implemented a new SMTP service on a server. A public IP address translates to the internal SMTP server. The administrator notices many sessions to the server, and gets notification that the servers public IP address is now reported in a spam real-time block list. Which of the following is wrong with the server?
A.SMTP open relaying is enabled.
B.It does not have a spam filter.
C.The amount of sessions needs to be limited.
D.The public IP address is incorrect.WBerlin Sans FBArialZX
ANSWER: A

8. Which of the following is MOST efficient for encrypting large amounts of data?
A.Hashing algorithms
B.Symmetric key algorithms
C.Asymmetric key algorithms
D.ECC algorithmsWBerlin Sans FBArialZX
ANSWER: B

9. Which of the following is a reason why a company should disable the SSID broadcast of the wireless access points?
A.Rogue access points
B.War driving
C.Weak encryption
D.Session hijackingWBerlin Sans FBArialZX
ANSWER: B

10. Which of the following BEST describes ARP?
A.Discovering the IP address of a device from the MAC address
B.Discovering the IP address of a device from the DNS name
C.Discovering the MAC address of a device from the IP address
D.Discovering the DNS name of a device from the IP addressWBerlin Sans FBArialZX
ANSWER: C

11. Which of the following would be BEST to use to apply corporate security settings to a device?
A.A security patch
B.A security hotfix
C.An OS service pack
D.A security templateWBerlin Sans FBArialZX
ANSWER: D

12. A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per

year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If the anti-malware software is purchased, which of the following is the expected net savings?

A.$900

B.$2,290

C.$2,700

D.$5,000b

ANSWER: B

13. Which of the following is the main objective of steganography?

A.Message digest

B.Encrypt information

C.Hide information

D.Data integrityWBerlin Sans FBArialZX

ANSWER: C

14. Which of the following would allow for secure key exchange over an unsecured network without a pre-shared key?

A.3DES

B.AES

C.DH-ECC

D.MD5WBerlin Sans FBArialZX

ANSWER: C

15. Which of the following improves security in a wireless system?

A.IP spoofing

B.MAC filtering

C.SSID spoofing

D.Closed networkWBerlin Sans FBArialZX

ANSWER: B

16. A user wants to implement secure LDAP on the network. Which of the following port numbers secure LDAP use by default?

A.53

B.389

C.443

D.636WBerlin Sans FBArialZX

ANSWER: D

17. On which of the following is a security technician MOST likely to find usernames?

A.DNS logs

B.Application logs

C.Firewall logs
D.DHCP logsWBerlin Sans FBArialZX
ANSWER: B

18. How many keys are utilized with asymmetric cryptography?
A.One
B.Two
C.Five
D.SevenWBerlin Sans FBArialZX
ANSWER: B

19. During a risk assessment it is discovered that only one system administrator is assigned several tasks critical to continuity of operations. It is recommended to cross train other system administrators to perform these tasks and mitigate which of the following risks?
A.DDoS
B.Privilege escalation
C.Disclosure of PII
D.Single point of failureWBerlin Sans FBArialZX
ANSWER: D

20. Which of the following network filtering devices will rely on signature updates to be effective?
A.Proxy server
B.Firewall
C.NIDS
D.HoneynetWBerlin Sans FBArialZX
ANSWER: C

21. Which of the following is a single server that is setup in the DMZ or outer perimeter in order to distract attackers?
A.Honeynet
B.DMZ
C.Honeypot
D.VLANWBerlin Sans FBArialZX
ANSWER: C

22. Which of the following encryption algorithms is decrypted in the LEAST amount of time?
A.RSA
B.AES
C.3DES
D.L2TPWBerlin Sans FBArialZX
ANSWER: B

23. An administrator is trying to secure a network from threats originating outside the network. Which of

the following
devices provides protection for the DMZ from attacks launched from the Internet?
A.Antivirus
B.Content filter
C.Firewall
D.Proxy serverWBerlin Sans FBArialZX
ANSWER: C

24. Which of the following is a way to manage operating system updates?
A.Service pack management
B.Patch application
C.Hotfix management
D.Change managementWBerlin Sans FBArialZX
ANSWER: D

25. Which of the following is a list of discrete entries that are known to be benign?
A.Whitelist
B.Signature
C.Blacklist
D.ACLWBerlin Sans FBArialZX
ANSWER: A

26. Which of the following increases the collision resistance of a hash?
A.Salt
B.Increase the input length
C.Rainbow Table
D.Larger key spaceWBerlin Sans FBArialZX
ANSWER: A

27. A programmer has decided to alter the server variable in the coding of an authentication function for a proprietary sales application. Before implementing the new routine on the production application server, which of the following processes should be followed?
A.Change management
B.Secure disposal
C.Password complexity
D.Chain of custodyWBerlin Sans FBArialZX
ANSWER: A

28. When deploying 50 new workstations on the network, which of following should be completed FIRST?
A.Install a word processor.
B.Run the latest spyware.
C.Apply the baseline configuration.
D.Run OS updates.WBerlin Sans FBArialZX

ANSWER: C

29. Which of the following should be implemented to have all workstations and servers isolated in their own broadcast domains?
A.VLANs
B.NAT
C.Access lists
D.IntranetWBerlin Sans FBArialZX
ANSWER: A

30. End users are complaining about receiving a lot of email from online vendors and pharmacies. Which of the following is this an example of?
A.Trojan
B.Spam
C.Phishing
D.DNS poisoningWBerlin Sans FBArialZX
ANSWER: B