Exam : **SY0-201**

Title : CompTIA Security+(2008 Edition) Exam

Version : Demo

1.An administrator is explaining the conditions under which penetration testing is preferred over vulnerability testing. Which of the following statements correctly describes these advantages?
A. Identifies surface vulnerabilities and can be run on a regular basis
B. Proves that the system can be compromised
C. Safe for even inexperienced testers to conduct
D. Can be fairly fast depending on number of hosts
Answer: B

2.Which of the following is a public key cryptosystem?
A. RSA
B. SHA-1
C. 3DES
D. MD5
Answer: A

3.A technician visits a customer site which prohibits portable data storage devices. Which of the following items would be prohibited? (Select TWO).
A. USB Memory key
B. Bluetooth-enabled cellular phones
C. Wireless network detectors
D. Key card
E. Items containing RFID chips
Answer: AB

4.A user wants to edit a file that they currently have read-only rights to; however, they are unable to provide a business justification, so the request is denied. This is the principle of:
A. separation of duties.
B. job-based access control.
C. least privilege.
D. remote access policy.
Answer: C

5.Conducting periodic user rights audits can help an administrator identify:
A. new user accounts that have been created.
B. users who are concurrently logged in under different accounts.
C. unauthorized network services.
D. users who can view confidential information.
Answer: D

6.Which of the following malicious programs compromises system security by exploiting system access through a virtual backdoor?
A. Virus
B. Trojan
C. Spam

D. Adware
Answer: B

7.Which of the following is a malicious program that infects a host computer and has the ability to replicate itself?
A. Spyware
B. Virus
C. Rootkit
D. Spam
Answer: B

8.When establishing a connection between two IP based routers, which of the following protocols is the MOST secure?
A. TFTP
B. HTTPS
C. FTP
D. SSH
Answer: D

9.Which of the following security precautions needs to be implemented when securing a wireless network? (Select THREE).
A. Enable data encryption on all wireless transmissions using WPA2.
B. Enable the lowest power setting necessary to broadcast to the targeted range.
C. Enable the highest power setting possible to make sure the broadcast reaches the targeted range.
D. Enable data encryption on all wireless transmissions using WEP.
E. Authentication should take place using a pre-shared key (PSK) of no more than six characters.
F. Enable the ability to verify credentials on an authentication server.
Answer: ABF

10.Which of the following BEST describes where L2TP is used?
A. VPN encryption
B. Authenticate users using CHAP
C. Default gateway encryption
D. Border gateway protocol encryption
Answer: A

11.Which of the following BEST describes how the mandatory access control (MAC) method works?
A. It is an access policy based on a set of rules.
B. It is an access policy based on the role that the user has in an organization.
C. It is an access policy based on biometric technologies.
D. It is an access policy that restricts access to objects based on security clearance.
Answer: D

12.Which of the following defines the role of a root certificate authority (CA) in PKI?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.
Answer: C

13.A port scan of a network identified port 25 open on an internal system. Which of the following types of traffic is this typically associated with?
A. Web traffic
B. File sharing traffic
C. Mail traffic
D. Network management traffic
Answer: C

14.The BEST location for a spam filter is:
A. on the local LAN.
B. on a proxy server.
C. behind the firewall.
D. in front of the mail relay server.
Answer: D

15.Biometrics is an example of which of the following type of user authentication?
A. Something the user is
B. Something the user has
C. Something the user does
D. Something the user knows
Answer: A

16.A recent security audit shows an organization has been infiltrated with a former administrator's credentials. Which of the following would be the BEST way to mitigate the risk of this vulnerability?
A. Conduct periodic audits of disaster recovery policies.
B. Conduct periodic audits of password policies.
C. Conduct periodic audits of user access and rights.
D. Conduct periodic audits of storage and retention policies.
Answer: C

17.A technician needs to ensure that all major software revisions have been installed on a critical network machine. Which of the following must they install to complete this task?
A. HIDS
B. Hotfixes
C. Patches
D. Service packs
Answer: D

18.Every company workstation contains the same software prior to being assigned to workers. Which of the following software options would give remote users the needed protection from outside attackers when they are outside of the company's internal network
A. HIDS
B. Vulnerability scanner
C. Personal firewall
D. NIPS
Answer: C

19.A company has just recovered from a major disaster. Which of the following should signify the completion of a disaster recovery?
A. Verify all servers are back online and working properly.
B. Update the disaster recovery plan based on lessons learned.
C. Conduct post disaster recovery testing.
D. Verify all network nodes are back online and working properly.
Answer: B

20.In order to prevent data loss in case of a disk error which of the following options would an administrator MOST likely deploy?
A. Redundant connections
B. RAID
C. Disk striping
D. Redundant power supplies
Answer: B

21.Which of the following tools can execute a ping sweep?
A. Protocol analyzer
B. Anti-virus scanner
C. Network mapper
D. Password cracker
Answer: C

22.Purchasing insurance on critical equipment is an example of which of the following types of risk mitigation techniques?
A. Risk avoidance
B. Risk transfer
C. Risk retention
D. Risk reduction
Answer: B

23.Which of the following describes a port that is left open in order to facilitate access at a later date?
A. Honeypot
B. Proxy server
C. Open relay

D. Back door
Answer: D

24.A technician has installed security software; shortly thereafter the response time slows considerably. Which of the following can be used to determine the effect of the new software?
A. Event logs
B. System monitor
C. Performance monitor
D. Protocol analyzer
Answer: C

25.Which of the following can increase risk? (Select TWO).
A. Vulnerability
B. Mantrap
C. Configuration baselines
D. Threat source
E. Mandatory vacations
Answer: AD

26.A technician reviews the system log entries for an internal DNS server. Which of the following entries MOST warrants further investigation?
A. DNS query from a source outside the organization
B. DNS query from a source inside the organization
C. Zone transfer to a source inside the organization
D. Zone transfer to a source outside the organization
Answer: D

27.An administrator wants to crack passwords on a server with an account lockout policy. Which of the following would allow this without locking accounts?
A. Try guessing passwords slow enough to reset the bad count interval.
B. Try guessing passwords with brute force.
C. Copy the password file offline and perform the attack on it.
D. Try only real dictionary words.
Answer: C

28.Which of the following devices hooks into a LAN and captures traffic?
A. Protocol analyzer
B. Protocol filter
C. Penetration testing tool
D. Vulnerability assessment tool
Answer: A

29.Which of the following elements has the ability to hide a node's internal address from the public

network?
A. NAT
B. NAC
C. NIDS
D. VLAN
Answer: A

30.An administrator would like to update a network machine with a number of vendor fixes concurrently. Which of the following would accomplish this with the LEAST amount of effort?
A. Install a service pack.
B. Install a patch.
C. Install a hotfix.
D. Install a new version of the program.
Answer: A