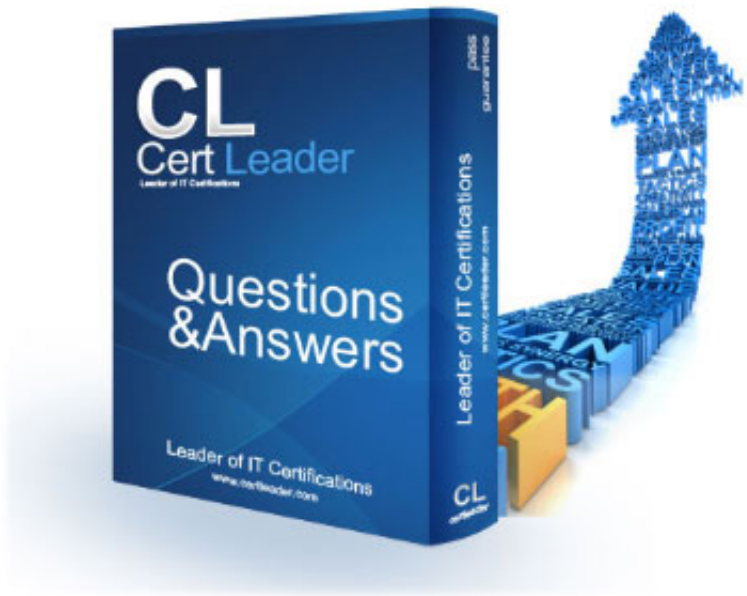
JK0-022 - CompTIA Academic/E2C Security+ Certification Exam Voucher Only

http://www.certleader.com/JK0-022-dumps.html



1.An attacker used an undocumented and unknown application exploit to gain access to a file server. Which of the following BEST describes this type of attack?

A. Integer overflow

B. Cross-site scripting

C. Zero-day

D. Session hijacking

E. XML injection

Answer: C

2. A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.

B. Set all nearby access points to operate on the same channel.

C. Configure the access point to use WEP instead of WPA2.

D. Enable all access points to broadcast their SSIDs.

Answer: A

3. A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interfacE.

PERMIT TCP ANY ANY 80

PERMIT TCP ANY ANY 443

Which of the following rules would accomplish this task? (Select TWO).

A. Change the firewall default settings so that it implements an implicit deny

B. Apply the current ACL to all interfaces of the firewall

C. Remove the current ACL

D. Add the following ACL at the top of the current ACL DENY TCP ANY ANY 53

E. Add the following ACL at the bottom of the current ACL DENY ICMP ANY ANY 53

F. Add the following ACL at the bottom of the current ACL DENY IP ANY ANY 53

Answer: A,F

4. A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.

Which of the following is the BEST approach for implementation of the new application on the virtual server?

A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.

B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.

C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.

D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

Answer: C

5. An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO).

A. Password Complexity

B. Password Expiration

C. Password Age

D. Password Length

E. Password History

Answer: A,D

6. A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server

B. Apache server

C. Exchange server

D. RADIUS server

Answer: A

7. Which of the following is the primary security concern when deploying a mobile device on a network?

A. Strong authentication

B. Interoperability

C. Data security

D. Cloud storage technique

Answer: C

8. Which of the following would allow the organization to divide a Class C IP address range into several ranges?

A. DMZ

B. Virtual LANs

C. NAT

D. Subnetting

Answer: D

9. Ann has read and write access to an employee database, while Joe has only read access.

Ann is leaving for a conference. Which of the following types of authorization could be utilized to trigger write access for Joe when Ann is absent?

A. Mandatory access control

B. Role-based access control

C. Discretionary access control

D. Rule-based access control

Answer: D

10. A company determines a need for additional protection from rogue devices plugging into physical ports around the building. Which of the following provides the highest degree of protection from unauthorized wired network access?

A. Intrusion Prevention Systems

B. MAC filtering

C. Flood guards

D. 802.1x

Answer: D

11. Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw.

Which of the following attacks has MOST likely occurred?

A. Cookie stealing

B. Zero-day

C. Directory traversal

D. XML injection

Answer: B

12. A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented?

A. RC4

B. AES

C. MD5

D. TKIP

Answer: A

13. While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?

A. Log Analysis

B. VLAN Management

C. Network separation

D. 802.1x

Answer: D

14. A recently installed application update caused a vital application to crash during the middle of the workday. The application remained down until a previous version could be reinstalled on the server, and this resulted in a significant loss of data and revenue.

Which of the following could BEST prevent this issue from occurring again?

A. Application configuration baselines

B. Application hardening

C. Application access controls

D. Application patch management

Answer: D

15. A company needs to receive data that contains personally identifiable information. The company requires both the transmission and data at rest to be encrypted. Which of the following achieves this goal? (Select TWO).

A. SSH

B. TFTP

C. NTLM

D. TKIP

E. SMTP

F. PGP/GPG

Answer: A,F

16. Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwisE.

A. user accounts may be inadvertently locked out.

B. data on the USB drive could be corrupted.

C. data on the hard drive will be vulnerable to log analysis.

D. the security controls on the USB drive can be bypassed.

Answer: D

17. Which of the following network design elements allows for many internal devices to share one public IP address?

A. DNAT

B. PAT

C. DNS

D. DMZ

Answer: B

18. Which of the following is used to verify data integrity?

A. SHA

B. 3DES

C. AES

D. RSA

Answer: A

19. Which of the following types of authentication packages user credentials in a ticket?

A. Kerberos

B. LDAP

C. TACACS+

D. RADIUS

Answer: A

20. A security technician is attempting to improve the overall security posture of an internal mail server.

Which of the following actions would BEST accomplish this goal?

A. Monitoring event logs daily

B. Disabling unnecessary services

C. Deploying a content filter on the network

D. Deploy an IDS on the network

Answer: B

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your JK0-022 Exam with Our Prep Materials Via below:

http://www.certleader.com/JK0-022-dumps.html