Vendor: CompTIA

Exam Code: JK0-018

Exam Name: CompTIA Security+ Certification Exam

Version: DEMO
QUESTION NO: 1
Which of the following elements of PKI are found in a browser’s trusted root CA?
A. Private key
B. Symmetric key
C. Recovery key
D. Public key
Answer: D

QUESTION NO: 2
Which of the following protocols only encrypts password packets from client to server?
A. XTACACS
B. TACACS
C. RADIUS
D. TACACS+
Answer: C

QUESTION NO: 3
Where are revoked certificates stored?
A. Recovery agent
B. Registration
C. Key escrow
D. CRL
Answer: D

QUESTION NO: 4
DRPs should contain which of the following?
A. Hierarchical list of non-critical personnel
B. Hierarchical list of critical systems
C. Hierarchical access control lists
D. Identification of single points of failure
Answer: B

QUESTION NO: 5
A system administrator could have a user level account and an administrator account to prevent:
A. password sharing.
B. escalation of privileges.
C. implicit deny.
D. administrative account lockout.
Answer: B
QUESTION NO: 6
Which of the following is the BEST way to mitigate data loss if a portable device is compromised?
A. Full disk encryption
B. Common access card
C. Strong password complexity
D. Biometric authentication
Answer: A

QUESTION NO: 7
Which of the following protocols should be blocked at the network perimeter to prevent host enumeration by sweep devices?
A. HTTPS
B. SSH
C. IPv4
D. ICMP
Answer: D

QUESTION NO: 8
Which of the following is specific to a buffer overflow attack?
A. Memory addressing
B. Directory traversal
C. Initial vector
D. Session cookies
Answer: C

QUESTION NO: 9
Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the ciphertext?
A. Private
B. Escrow
C. Public
D. Preshared
Answer: C

QUESTION NO: 10
Which of the following should a security administrator implement to prevent users from disrupting
network connectivity, if a user connects both ends of a network cable to different switch ports?
A. VLAN separation
B. Access control
C. Loop protection
D. DMZ
Answer: C

QUESTION NO: 11
A new enterprise solution is currently being evaluated due to its potential to increase the company's profit margins. The security administrator has been asked to review its security implications. While evaluating the product, various vulnerability scans were performed. It was determined that the product is not a threat but has the potential to introduce additional vulnerabilities. Which of the following assessment types should the security administrator also take into consideration while evaluating this product?
A. Threat assessment
B. Vulnerability assessment
C. Code assessment
D. Risk assessment
Answer: D

QUESTION NO: 12
Which of the following requires special handling and explicit policies for data retention and data distribution?
A. Personally identifiable information
B. Phishing attacks
C. Zero day exploits
D. Personal electronic devices
Answer: A

QUESTION NO: 13
Centrally authenticating multiple systems and applications against a federated user database is an example of:
A. smart card.
B. common access card.
C. single sign-on.
D. access control list.
Answer: C
QUESTION NO: 14
WEP is seen as an unsecure protocol based on its improper use of which of the following?
A. RC6
B. RC4
C. 3DES
D. AES
Answer: B

QUESTION NO: 15
Which of the following should be performed if a smartphone is lost to ensure no data can be retrieved from it?
A. Device encryption
B. Remote wipe
C. Screen lock
D. GPS tracking
Answer: B

QUESTION NO: 16
In an 802.11n network, which of the following provides the MOST secure method of both encryption and authorization?
A. WEP with 802.1x
B. WPA Enterprise
C. WPA2-PSK
D. WPA with TKIP
Answer: B

QUESTION NO: 17
Which of the following methods of access, authentication, and authorization is the MOST secure by default?
A. Kerberos
B. TACACS
C. RADIUS
D. LDAP
Answer: A

QUESTION NO: 18
Which of the following facilitates computing for heavily utilized systems and networks?
A. Remote access
B. Provider cloud
C. VPN concentrator
QUESTION NO: 19
With which of the following is RAID MOST concerned?
A. Integrity
B. Confidentiality
C. Availability
D. Baseline
Answer: C

QUESTION NO: 20
Which of the following reduces the likelihood of a single point of failure when a server fails?
A. Clustering
B. Virtualization
C. RAID
D. Cold site
Answer: A

QUESTION NO: 21
A user downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?
A. Logic bomb
B. Worm
C. Trojan
D. Adware
Answer: C

QUESTION NO: 22
Which of the following is used in conjunction with PEAP to provide mutual authentication between peers?
A. LEAP
B. MSCHAPv2
C. PPP
D. MSCHAPv1
Answer: B

QUESTION NO: 23
A targeted email attack sent to the company's Chief Executive Officer (CEO) is known as which of the following?

A. Whaling
B. Bluesnarfing
C. Vishing
D. Dumpster diving

Answer: A

QUESTION NO: 24
Which of the following uses TCP port 22 by default?

A. SSL, SCP, and TFTP
B. SSH, SCP, and SFTP
C. HTTPS, SFTP, and TFTP
D. TLS, TELNET, and SCP

Answer: B

QUESTION NO: 25
Actively monitoring data streams in search of malicious code or behavior is an example of:

A. load balancing.
B. an Internet proxy.
C. URL filtering.
D. content inspection.

Answer: D

QUESTION NO: 26
A user is no longer able to transfer files to the FTP server. The security administrator has verified the ports are open on the network firewall. Which of the following should the security administrator check?

A. Anti-virus software
B. ACLs
C. Anti-spam software
D. NIDS

Answer: B

QUESTION NO: 27
A Human Resource manager is assigning access to users in their specific department performing the same job function. This is an example of:

A. role-based access control.
B. rule-based access control.
C. centralized access control.

D. mandatory access control.

Answer: A

QUESTION NO: 28
Which of the following BEST describes the process of key escrow?
A. Maintains a copy of a user's public key for the sole purpose of recovering messages if it is lost
B. Maintains a secured copy of a user's private key to recover the certificate revocation list
C. Maintains a secured copy of a user's private key for the sole purpose of recovering the key if it is lost
D. Maintains a secured copy of a user's public key in order to improve network performance

Answer: C

QUESTION NO: 29
Which of the following network devices would MOST likely be used to detect but not react to suspicious behavior on the network?
A. Firewall
B. NIDS
C. NIPS
D. HIDS

Answer: B

QUESTION NO: 30
Which of the following is an example of allowing a user to perform a self-service password reset?
A. Password length
B. Password recovery
C. Password complexity
D. Password expiration

Answer: B