Exam : **JK0-015**

Title : CompTIA E2C Security+ (2008 Edition) Exam

Version : Demo

1.Which of the following logical access control methods would a security administrator need to modify in order to control network traffic passing through a router to a different network?
A. Configuring VLAN 1
B. ACL
C. Logical tokens
D. Role-based access control changes
Answer: B

2.Which of the following tools limits external access to the network.?
A. IDS
B. VLAN
C. Firewall
D. DMZ
Answer: C

3.Which of the following tools was created for the primary purpose of reporting the services that are open for connection on a networked workstation?
A. Protocol analyzer
B. Port scanner
C. Password crackers
D. Vulnerability scanner
Answer: B

4.Which of the following is MOST likely to be an issue when turning on all auditing functions within a system?
A. Flooding the network with all of the log information
B. Lack of support for standardized log review tools
C. Too much information to review
D. Too many available log aggregation tools
Answer: C

5.Upon opening the browser, a guest user is redirected to the company portal and asked to agree to the acceptable use policy. Which of the following is MOST likely causing this to appear?
A. NAT
B. NAC
C. VLAN
D. DMZ
Answer: B

6.USB devices with a virus delivery mechanism are an example of which of the following security threats?
A. Adware
B. Trojan
C. Botnets
D. Logic bombs

Answer: B

7.Cell phones with network access and the ability to store data files are susceptible to which of the following risks?
A. Input validation errors
B. SMTP open relays
C. Viruses
D. Logic bombs
Answer: C

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 algorithms provides better protection against brute force attacks by using a 160-bit message digest?
A. MD5
B. SHA-1
C. LANMAN
D. NTLM
Answer: B

10.Which of the following access control technologies provides a rolling password for one-time use?
A. RSA tokens
B. ACL
C. Multifactor authentication
D. PIV card
Answer: A

11.Which of the following technologies is used to verify that a file was not altered?
A. RC5
B. AES
C. DES
D. MD5
Answer: D

12.Which of the following uses an RC4 key that can be discovered by eavesdropping on plain text initialization vectors?
A. WEP
B. TKIP

C. SSH
D. WPA
Answer: A

13.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

14.A user reports that each time they attempt to go to a legitimate website, they are sent to an inappropriate website. The security administrator suspects the user may have malware on the computer, which manipulated some of the user's files. Which of the following files on the user's system would need to be checked for unauthorized changes?
A. SAM
B. LMhosts
C. Services
D. Hosts
Answer: D

15.An administrator needs to limit and monitor the access users have to the Internet and protect the internal network. Which of the following would MOST likely be implemented?
A. A heuristic firewall
B. DNS caching on the client machines
C. A pushed update modifying users' local host file
D. A content-filtering proxy server
Answer: D

16.Which of the following is a malicious program used to capture information from an infected computer?
A. Trojan
B. Botnet
C. Worm
D. Virus
Answer: A

17.The security administrator needs to make a change in the network to accommodate a new remote location. The new location will be connected by a serial interface, off the main router, through a commercial circuit. This remote site will also have traffic completely separated from all other traffic. Which of the following design elements will need to be implemented to accommodate the new location?
A. VLANs need to be added on the switch but not the router.
B. The NAT needs to be re-configured to allow the remote location.
C. The current IP scheme needs to be subnetted.

D. The switch needs to be virtualized and a new DMZ needs to be created
Answer: C

18.Which of the following is the MOST secure authentication method?
A. Smartcard
B. Iris
C. Password
D. Fingerprints
Answer: B

19.Mitigating security risks by updating and applying hot fixes is part of:
A. patch management.
B. vulnerability scanning.
C. baseline reporting.
D. penetration testing.
Answer: A

20.When reviewing IDS logs, the security administrator notices many events pertaining to a "NOOP sled". Which of the following attacks is occurring?
A. Man-in-the-middle
B. SQL injection
C. Buffer overflow
D. Session hijacking
Answer: C