Exam Code: SY0-201

Exam Name: CompTIA Security+ (2008 Edition) Exam

Vendor: CompTIA

Version: DEMO

Part: A

1: All of the following are part of the disaster recovery plan EXCEPT:

A.obtaining management buy-in.

B.identifying all assets.

C.system backups.

D.patch management software.

Correct Answers: D

2: Which of the following describes a host-based system that provides access control?

A.Personal software firewalls

B.Antivirus software

C.HIDS

D.Pop-up blockers

Correct Answers: A

3: Which of the following is a way to gather reconnaissance information from a printer resource?

A.HTTP

B.SMTP

C.RADIUS

D.SNMP

Correct Answers: D

4: An administrator wants to setup their network with only one public IP address. Which of the following would allow for this?

A.DMZ

B.VLAN

C.NIDS

D.NAT

Correct Answers: D

5: To prevent the use of stolen PKI certificates on web servers, which of the following should an administrator ensure is available to their web servers?

A.Registration

B.CA

C.CRL

D.Key escrow

Correct Answers: C

6: Which of the following explains the difference between a public key and a private key?

A.The public key is only used by the client while the private key is available to all. Both keys are mathematically related.

B.The private key only decrypts the data while the public key only encrypts the data. Both keys are mathematically related.

C.The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.

D.The private key is only used by the client and kept secret while the public key is available to all.

Correct Answers: D

7: A user was trying to update an open file but when they tried to access the file they were denied. Which of the following would explain why the user could not access the file?

A.Audit only access

B.Execute only access

C.Rights are not set correctly

D.Write only access

Correct Answers: C

8: User A is a member of the payroll security group. Each member of the group should have read/write permissions to a share. User A was trying to update a file but when the user tried to access the file the user was denied. Which of the following would explain why User A could not access the file?

A.Privilege escalation

B.Rights are not set correctly

C.Least privilege

D.Read only access

Correct Answers: B

9: All of the following show up in a security log EXCEPT:

A.true positive.

B.false negative.

C.known anomalies.

D.false positive.

Correct Answers: B

10: Which of the following is a system that will automate the deployment of updates to workstations and servers?

A.Service pack

B.Remote access

C.Patch management

D.Installer package

Correct Answers: C

11: Which of the following authentication models uses a KDC?

A.CHAP

B.PKI

C.PGP

D.Kerberos

Correct Answers: D

12: Which of the following attacks commonly result in a buffer overflow?
A.ARP Poisoning
B.DNS Poisoning
C.Replay
D.DoS
Correct Answers: D

13: A corporation has a contractual obligation to provide a certain amount of system uptime to a client. Which of the following is this contract an example of?
A.PII
B.SLA
C.Due diligence
D.Redundancy
Correct Answers: B

14: A technician is implementing a new wireless network for an organization. The technician should be concerned with all of the following wireless vulnerabilities EXCEPT:
A.rogue access points.
B.802.11 mode.
C.weak encryption.
D.SSID broadcasts.
Correct Answers: B

15: An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns. Which of the following is an example of this threat?
A.An attacker using the phone remotely for spoofing other phone numbers
B.Unauthorized intrusions into the phone to access data
C.The Bluetooth enabled phone causing signal interference with the network
D.An attacker using exploits that allow the phone to be disabled
Correct Answers: B