

## 30 sample CompTIA questions

### For 2008 Sy0-201

Correct answer are highlighted.

---

1. Kernel-level rootkits are designed to do what on a computer? (Choose two.)



- To extract confidential information from a computer
  - To hide evidence of an attacker's presence
  - To make a computer more susceptible to pop-up advertisements
  - To hide a back door into the system
  - To intercept a user's password
- 

2. What is a potential risk associated with WEP when it is used to secure a WLAN?



- Required SSID broadcast
- Vulnerability to rogue access points
- Weak encryption
- Data emanation
- No protection against war driving

3. You are designing network access control so that remote users are limited to accessing the network during normal business hours only. Policies regarding user access apply to all users.

This is an example of what type of access control?



- MAC
- Role-based access control
- DAC

Rule-based access control

4. You have been tasked to perform a risk assessment for an organization.

What should you do first?

||

- Identify vulnerabilities.
- Identify organizational assets.
- Identify potential monetary impact.
- Identify threats and threat likelihood.

5. You discover that company confidential information is being encoded into graphics files and sent to a destination outside of the company.

This is an example of what kind of cryptography?

||

- Confidentiality
- Non-repudiation
- Digital signature
- Steganography

6. Which type of social engineering attack on a business typically relies on impersonation to gain personal information?

||

- Hoaxes
- Phishing
- Dumpster diving
- Shoulder surfing

7. Which of the following can be used to launch a coordinated DDoS attack?



Worm



Rootkit



Botnet



Adware

8. What can you prevent when you deploy wireless devices inside a TEMPEST-certified building?



War driving



Weak encryption



Bluesnarfing



Blue jacking

9. You are designing a secure application environment. You need to ensure that data is kept as secure as possible. You need to select the strictest access control model.

What access control model should you use?



DAC



MAC



Role-based access control



Rule-based access control

10. You are performing risk assessment for an organization. What should you do during impact assessment?



Determine how likely it is that a threat might actually occur.

- Determine how well the organization is prepared to manage the threat.
- Determine the potential monetary costs related to a threat.
- Determine actions that can be taken to mitigate a potential threat.

11. For which of the following is centralized key management most complicated?



- Symmetric key
- Whole disk encryption
- Asymmetric key
- TPM

12. You are determining environmental control requirements for a data center that will contain several computers?

What is the role of an HVAC system in this environment? (Choose two.)



- Maintain appropriate humidity levels
- Shield equipment from EMI
- Provide an appropriate ambient temperature
- Provide isolation in case of a fire
- Vent fumes from the data center

13. A virus is designed to format a computer's hard disk based on a specific calendar date.

What kind of threat is this?



- Logic bomb
- Spyware

- Bot
- Adware

14. You suspect that someone is trying to gather information about your network. Your network is isolated from the Internet by a perimeter network.

You need to gather as much information about the attacker as possible. You want to prevent the attacker from knowing that the attempt has been detected.

What should you do?



- Deploy a honeypot in the perimeter network.
- Deploy a proxy server in the perimeter network.
- Deploy a NIPS outside the perimeter network.
- Deploy a protocol analyzer in the internal network.

15. You are designing a Web-based application. You design the application so that it runs under a security context that allows only those privileges required for the application to run to minimize risk in the event of an attack.

This is an example of which of the following?



- Implicit deny
- Separation of duties
- Principle of least privilege
- MAC

16. You are preparing to perform vulnerability analysis on a network. Which tools require a computer with a network adapter that can be placed in promiscuous mode? (Choose two.)



- Vulnerability scanner

- Password cracker
- Port scanner
- Protocol analyzer
- Network mapper

17. The 802.11i standard specifies support for which encryption algorithms? (Choose two.)

- ECC
- AES
- RSA
- DES
- TKIP

18. Which environmental control is part of TEMPEST compliance?

- Fire suppression
- Biometric scans
- Shielding
- HVAC

19. An attacker forces a Windows service that uses the Local System account as its service account to crash. The attacker is able to access administrator-level resources as a result.

What kind of attack is this?

- Spyware
- SPIM

- Spam
- Trojan
- Privilege escalation

20. What kinds of attacks involve intercepting and modifying network packets? (Choose two.)

- DNS poisoning
- Spoofing
- Man-in-the-middle
- TCP/IP hijacking
- DoS
- Null session

21. You are designing security for a financial application. You need to ensure that all tasks relating to the transfer of money require actions by more than one user through a series of checks and balances. All activity must be audited and logged.

On what access control method should you design your security model?

- Implicit deny
- Job rotation
- Principle of least privilege
- Separation of duties

22.

---

You need to determine if intermittent spikes in network activity are related to an attempt to breach the network. You need to identify exactly when the activity is occurring and what type of traffic is causing the activity.

What should you do?



- Use Windows Performance Monitor.
  - Use a network mapper.
  - Use a systems monitor.
  - Use a protocol analyzer.
- 

23. You are trying to determine the most appropriate encryption algorithm to use for an application. You need to compare features of symmetric and asymmetric algorithms. Which of the following are symmetric and which are asymmetric algorithms?

In the list on the right, select the appropriate algorithms. Place your selections in the list on the left under the appropriate node by clicking the node, clicking the item in the list on the right, and then clicking the arrow. You may use items from the list on the right more than once, and you do not have to use each item from the list.

Asymmetric:

- RSA
- ECC

Symmetric:

- 3DES
- AES
- DES
- AES256

24. You need to ensure that an organization can be back up and running as quickly as possible in case of fire, flood, or other natural disaster.

What should you do?



- Provide a location for offsite backup storage.
- Set up a hot backup site.

- Set up a cold backup site.
- Deploy redundant servers in the office.

25. You are looking for ways to protect data on a network. Your solution should:

- \* Provide for easy backup of all user data.
- \* Minimize risk of physical data theft.
- \* Minimize the impact of the failure of any one file server.

Which solution should you use?



- Use internal hard disks installed in file servers. Lock the file servers in a secure area.
- Back up user files to USB hard disks attached to user systems. Store the USB hard disks in a secure area after hours.
- Use file servers with removable hard disks. Secure the hard disks in a separate area after hours.
- Use file servers attached to an NAS system. Lock the file servers and NAS in a secure area.

26. You are designing a solution to protect your network from Internet-based attacks. You need to provide:

- \* Pre-admission security checks
- \* Automated remediation

The solution should integrate existing network infrastructure devices.

What should you do?



- Implement subnetting.
- Implement a VLAN.
- Implement NAT.
- Implement NAC.

27. Your network is configured as a Windows Server 2003 Active Directory domain. The Finance group has read permission to the Reports and History shared folders as well as

other shared folders. The Accounting group has read and write permissions to the Reports, AccountRecs, and Statements shared folders. Several users are members of both the Finance and Accounting groups.

All of the folders are located on a file server named FS0. The Everyone group is granted the Full Control NTFS permission for each folder through inheritance, but non-administrative users do not have the right to log on locally at the server. Access to the shared folders is managed through share permissions.

It is determined that the Finance group should no longer have read access to the Reports folder. This change should not affect access permissions granted through membership in other groups.

What should you do?



- Remove the read permission from the Finance group for the Reports folder.
- Deny the read permission individually for each member of the Finance group for the Reports folder.
- Delete the Finance group.
- Deny the read permission to the Finance group for the Reports folder.

28. You are configuring security for a network that is isolated from the Internet by a perimeter network. Three Web servers and an NIDS are deployed in the perimeter network.

You need to test the network's ability to detect and respond to a DoS attack against the applications running on the Web servers.

What should you do?



- Use vulnerability scanning.
- Use penetration testing.
- Use port scanning.
- Use network analysis.

29. You have several computers that use the NTLM authentication protocol for client authentication. Network policy requires user passwords with at least 16 characters.

What hash algorithm is used for password authentication?



- SHA
- AES
- LM hash
- MD5

30. You need to ensure that a critical server has minimal down time. You need to ensure data fault tolerance for the server.

What should you do?



- Configure a redundant server.
- Deploy a UPS.
- Provide spare parts.
- Use RAID.