9628-05 Level 4 Diploma in Network Security (for the Level 4 Network Engineer Apprenticeship)
9628-405 Network Security

Sample question paper

Duration: 45 minutes

Candidate's name:

Candidate's enrolment number:

Centre name:

Centre number:

Date:

1 Which one of the following concepts ensures that **only** authorised users can access data?

a. Integrity.
b. Recovery.
c. Availability.
d. Confidentiality.

2 Which one of the following statements **best** describes a vulnerability?

a. An incident which causes damage to systems.
b. A weakness that can be exploited during an incident.
c. Damage to the reputation of an organisation following an incident.
d. The potential for the loss or corruption of data resulting from an incident.

3 What technology inspects data and blocks or manipulates the flow if it determines that the data is malicious?

a. IPS
b. NAT
c. IDS
d. NTP

4 What document contains details of the probability and impact of a vulnerability?

a. Fault log.
b. Risk register.
c. System log.
d. Issues register.

5 What type of attack occurs when a hacker takes control of an IEEE 802.15 compatible device?

a. Bluejacking.
b. Keylogging.
c. Smurfing.
d. Phishing.

6 What type of attack could be used to defeat a weak password using a trial and error method?

a. DOS.
b. Hoax.
c. Dictionary.
d. Spoofing.

7 Which one of the following threats poses as a legitimate programme in order to encourage users to run it?

a. Botnet.
b. Cookie.
c. Virus.
d. Trojan.

8 What type of malware replicates itself across a network without user or system interaction?

a. Virus.
b. Spam.
c. Trojan.
d. Worm.

9 What type of threat uses targeted emails that appear to be from a trusted source to gain access to sensitive information?

a. Botnet.
b. Cookie.
c. Phishing.
d. Ransomware.

10 What type of attack uses multiple systems in different physical locations to disrupt the services provided by an organisation?

a. DoS.
b. DDoS.
c. DNS hijacking.
d. DHCP flooding.

11 For which one of the following reasons would an organisation choose to adopt an acceptance policy?

a. To ensure regulatory body acceptance.
b. When the cost outweighs the benefit of accepting the risk.
c. To ensure the acceptance of QoS standards.
d. When the benefit outweighs the cost of accepting the risk.

12 Which one of the following metrics is used to calculate the duration of an incident from the point of malfunction until the service is fully restored and functioning as expected?

a. Mean time to recover.
b. Mean time between failures.
c. System policy compliance.
d. Recovery point objective.

13 Which one of the following countermeasures can be used to establish a physical barrier around a building?

a. Doors.
b. Cameras.
c. Fences.
d. Alarms.

14 Which countermeasure is used to monitor **both** OSs and application files that are executable for changes that may indicate an attack?

a. Host based packet sniffer.
b. Network based packet sniffer.
c. Host based intrusion detection system.
d. Network based intrusion detection system.

15 Which one of the following is the **most** suitable way of ensuring that all end users are aware of the potential dangers associated with opening email attachments?

a. Email individual end users.
b. Update anti-virus definitions.
c. Initiate the incident response process.
d. Provide threat awareness training for staff.

16 What Windows-based security control uses a Resultant Set of Policies that apply to a specific computer or user?

a. MAC
b. GPO
c. DAC
d. IPSec

17 Which one of the following ensures that the security features of an OS remain up to date?

a. Restore point.
b. System backups.
c. Disk defragmentation.
d. Automatic system patching.

18 Which one of the following technologies is used to establish secure communications for remote workers via the internet?

a. VPN
b. SSH
c. NAT
d. PAT

19 Which one of the following technologies is used to ensure that all data contained on portable storage devices remains confidential?

a. Hashing.
b. IPSec.
c. Certification services.
d. Whole disk encryption.

20 When working with a Microsoft Windows OS, which file and folder permission allows a user to delete a file?

a. Write.
b. Modify.
c. Read & write.
d. Read & execute.

21 What protocol provides authentication as part of the process of transferring data across networks?

a. SSH
b. SSID
c. IPSec
d. Hashing

22 Which one of the following firewall configurations is **most** likely to result in a remote device being unable to interact with a server?

a. Implicit port redirection.
b. Implicit denial of access.
c. Stateful packet inspection.
d. Stateless packet inspection.

23 What Microsoft Windows-based encryption feature is used to secure a single file that contains sensitive information?

a. 3DES.
b. EFS.
c. Twofish.
d. Bitlocker.

24 Why is hashing used as part of the data transfer process?

a. To ensure integrity of data.
b. To enable secure tunnelling.
c. To enforce non-repudiation.
d. To disguise the origins of the data.

25 Which one of the following countermeasures is suitable for identifying potential threats to data that is closely monitored and isolated from the main network?

a. Firewall.
b. Honeypot.
c. Port filtering.
d. Runtime protection.

26 Which one of the following methods is **most** suitable for use by security organisations to communicate information regarding emerging threats to a wide audience?

a. Technical updates.
b. Virus definition updates.
c. Online threat lists.
d. Emailing IT technicians.

27 Which one of the following mitigation methods is an appropriate response to the introduction of a virus on to a system via a portable storage device?

a. Enable TCP ports.
b. Disable USB ports.
c. Enable port scanning.
d. Disable port forwarding.

28 Which one of the following stages of incident response follows the containment of the attack?

a. Analysis.
b. Restoration of data.
c. Eradication.
d. Summarise the impact.

29 When anti-virus software identifies a file with a suspicious signature that matches a known threat, which one of the following actions does the software take?

a. Segments the file.
b. Morphs the file.
c. Quarantines the file.
d. Conceals the file.

30 An organisation's backup strategy consists of a full backup on Sunday followed by differential backups. Which one of the following media combinations would be required to restore data if the system crashed on Wednesday?

a. Monday and Tuesday.
b. Full backup and Monday.
c. Full backup and Tuesday.
d. Full backup, Monday and Tuesday.

NOW GO BACK AND CHECK YOUR WORK

- IMPORTANT -
  Are the details at the top of the answer sheet correct?