kasneb

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK SECURITY

TUESDAY: 2 December 2025. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. Which one of the following basic transformations is carried out by the substitution technique in cryptography?
   A. Breaking up data blocks into smaller packets for quicker transmission
   B. Before encryption, compressing the original file
   C. Changing every character or symbol in the plaintext
   D. Concealing messages in pictures or videos (2 marks)

2. A university wants to protect its internal network from unauthorised access and data theft while allowing students to use public Wi-Fi. Which one of the following types of network security focuses on controlling who can access network resources?
   A. Physical security
   B. Access control
   C. Antivirus protection
   D. Data encryption (2 marks)

3. Which of the following types of attacks are prevented by the combination of people, policies, technology and procedures that make up network security?
   A. Insider manipulation and social engineering
   B. Device malfunction and hardware deterioration
   C. Power variations and environmental risks
   D. Cyberattacks, illegal access and data loss (2 marks)

4. A Network Administrator discovers that it is possible to abuse a business server's many outdated services remotely. This is referred to as ________________.
   A. configurational vulnerability
   B. hardware vulnerability
   C. vulnerability in social engineering
   D. phishing susceptibility (2 marks)

5. Which one of the following security features of information systems is the **MAIN** target of a passive attack?
   A. Integrity
   B. Availability
   C. Authenticity
   D. Confidentiality (2 marks)

6. A bank is assessing the likelihood and impact of potential cyberattacks on its online banking platform. Which one of the following steps in risk management involves quantifying potential threats and their consequences?
   A. Patch management
   B. Disaster recovery
   C. Risk assessment
   D. Incident response (2 marks)

7. A corporate IT team is designing a network layout to separate internal resources from public-facing servers. Which one of the following network structure concepts involves creating different segments with specific security policies?
A. Demilitarised zone
B. Firewall bypass
C. VLAN hopping
D. Open network (2 marks)

8. Network security operates in which layers of the OSI stack?
A. Layers 1 and 2, the physical and data link layers of the OSI stack
B. Layers 5 and 6, the session and presentation layers of the OSI stack
C. Layers 7 and 8, the application and user layers of the OSI stack
D. Layers 3 and 4, the network and transport layers of the OSI stack (2 marks)

9. A company is implementing guidelines to ensure systematic protection of its network, including policies, processes and tools. The overarching structure that defines network security management practices is known as ________________.
A. intrusion detection system
B. security framework
C. antivirus suite
D. disaster recovery plan (2 marks)

10. An organisation wants to formalise rules regarding acceptable use of its IT systems and consequences for violations. Which one of the following documents outlines proper behaviour and security requirements for network users?
A. Patch management schedule
B. Firewall rule set
C. Network diagram
D. Security policy (2 marks)

11. Which one of the following particular unethical actions is prevented by a non-repudiation service for both the sender and the recipient after a message is transmitted?
A. Deleting encrypted files from storage
B. Altering the communication hardware setup
C. Denying participation in message transmission
D. Modifying authentication credentials (2 marks)

12. The IT department wants to prevent unauthorised personnel from accessing server rooms. Which one of the following measures **BEST** enforces physical security?
A. Biometric access controls
B. Encryption of data in transit
C. Network firewall rules
D. Password complexity requirements (2 marks)

13. A company wants to prevent employees from accessing confidential files without proper clearance. Which one of the following is a logical security control suitable for achieving the company's objective?
A. Surveillance cameras
B. Role-based access control
C. Security guards
D. Locked doors (2 marks)

14. Before rolling out a new firewall configuration, the IT team sets up a simulation environment to test its impact on business operations. Which one of the following steps of the network testing plan ensures that production services are not disrupted during evaluation?
A. Running tests without documenting outcomes
B. Disabling all monitoring tools during the test
C. Conducting tests in a controlled lab environment
D. Applying updates directly to production servers (2 marks)

15. A financial institution hires security experts to mimic cybercriminals and identify exploitable weaknesses. Which one of the following types of penetration testing assumes no prior knowledge of the network?
A. Black-box testing
B. Grey-box testing
C. Targeted testing
D. White-box testing (2 marks)

16. An online retail company secures all transactions by ensuring that payment information cannot be read by unauthorised users. Which one of the following protects information during transmission?
A. Intrusion prevention
B. Encryption
C. Intrusion detection
D. Hashing (2 marks)

17. A network outage occurs when the data center's air conditioning system fails, leading to server overheating. This vulnerability is **BEST** classified as ________________.
A. configuration vulnerability
B. human-related vulnerability
C. software vulnerability
D. environmental vulnerability (2 marks)

18. A System Administrator identifies that a critical update has not been applied to the company's email servers. Which one of the following statements **BEST** illustrates the risk of leaving email servers without critical updates?
A. Routine maintenance tasks could increase due to outdated software versions
B. Cooling efficiency might be reduced, leading to gradual performance decline
C. Attackers could exploit known flaws to gain unauthorised access to email data
D. The servers could draw slightly higher power during normal daily operations (2 marks)

19. An airline company evaluates whether to upgrade its intrusion detection system by weighing cost against the potential financial losses of a breach. Which one of the following types of risk analysis involves assigning monetary values to threats?
A. Quantitative risk analysis
B. Qualitative risk analysis
C. Comparative risk analysis
D. Operational risk analysis (2 marks)

20. An organisation isolates its production database from the internet-facing web servers using layered defenses. The network design principle applied here is ________________.
A. layered security
B. defense in depth
C. zero trust
D. least privilege bypass (2 marks)

21. A multinational organisation aligns its network security measures with internationally recognised standards to ensure compliance and consistency. Which one of the following frameworks is widely adopted to provide guidelines for managing cybersecurity risks?
A. COBIT Governance Framework
B. PRINCE2 Project Management Framework
C. ITIL Service Management Framework
D. NIST Cybersecurity Framework (2 marks)

22. A company requires employees to change their passwords regularly and prohibits reusing old ones. Which one of the following aspects of a security policy does this enforce?
A. Password policy
B. Access control policy
C. Acceptable use policy
D. Incident response policy (2 marks)

23. Security administrators use automated scanning software to identify vulnerabilities in corporate servers before attackers exploit them. A suitable tool to use in this scenario is ______________________.

A. Wireshark
B. Nessus
C. Nmap
D. Suricata (2 marks)

24. To prevent unauthorised access, a company enforces login requirements using both a password and a mobile verification code. Which one of the following actions is a logical control measure the company has deployed?

A. Single sign-on authentication
B. Network firewall configuration
C. Biometric identity scanning
D. Multi-factor authentication (2 marks)

25. A network audit involves stress testing systems to determine how they perform under heavy traffic loads. Which one of the following types of testing focuses on measuring system performance under peak usage?

A. Load testing
B. Penetration testing
C. Vulnerability testing
D. Bug bounty (2 marks)

26. Before conducting a penetration test, security professionals collect publicly available details such as domain names, IP addresses and employee information about the target organisation. Which one of the following activities does this process describe?

A. Enumeration
B. Footprinting
C. Reconnaissance
D. Scanning (2 marks)

27. To secure data in transit, the term "key range and key size" primarily determines which one of the following aspects of cryptographic strength?

A. The level of difficulty in breaking the encryption algorithm
B. The transmission speed of encrypted messages
C. The physical location of stored cryptographic keys
D. The length of plain text segments before encryption (2 marks)

28. A security team deploys honeypots and closely monitors network logs to detect and mislead attackers who are attempting to gather information about the organisation. Which one of the following is a defensive technique illustrated by this?

A. Active reconnaissance
B. Passive reconnaissance
C. Open Source Intelligence (OSINT)
D. Counter-reconnaissance (2 marks)

29. An attacker exploits an outdated encryption algorithm used by a wireless access point. This scenario is an example of which one of the following types of network weaknesses?

A. Improper network device setup
B. Insecure hardware configuration
C. Weak cryptographic protocol
D. Poor user security practices (2 marks)

30. A hospital evaluates potential network security threats and ranks them as "high," "medium" or "low" based on their severity and impact. Which one of the following types of network risk analysis is being applied in this case?

A. Quantitative risk analysis
B. Qualitative risk analysis
C. Predictive risk analysis
D. Automated risk analysis (2 marks)

31. To strengthen its defenses, a government agency trains staff to analyse cyber threats at different layers, such as the application, transport, internet and network access layers. Which one of the following reference models is being applied in this network security approach?
A. TCP/IP Model
B. SMTP Protocol
C. NIST Framework
D. OSI Model (2 marks)

32. Employees are instructed not to install unauthorised applications on company laptops. Which one of the following types of security control is illustrated in this scenario?
A. Reckless operation
B. Physical control
C. Technical control
D. Administrative control (2 marks)

33. A cybersecurity team deploys a system that analyses traffic on the network as well as activities on individual hosts to detect suspicious behaviour. Which one of the following types of intrusion detection systems (IDS) is **BEST** suited for this task?
A. Host-based IDS
B. Network-based IDS
C. Hybrid-based IDS
D. Application-based IDS (2 marks)

34. A company uses digital certificates to confirm the authenticity of a user before granting network access. Which one of the following controls is implemented in this case?
A. Surveillance monitoring control
B. Identity and access management control
C. Physical security guards control
D. Electronic motion detectors control (2 marks)

35. A new patch is deployed in a test environment to check compatibility with existing software before a company-wide rollout. Which one of the following types of tests is being performed?
A. Exploit testing
B. Packet sniffing
C. Port scanning
D. Regression testing (2 marks)

36. Security analysts observed suspicious incoming traffic that attempted to exploit a vulnerable web application by injecting malicious code. The security tool that can be used to prevent this type of attack is referred to as _____________.
A. network intrusion detection system
B. web application firewall
C. data loss prevention
D. next-generation firewall (2 marks)

37. A financial institution noticed that employees frequently fell victim to phishing campaigns despite repeated notifications. Management decided to address this recurring problem through preventive measures. Which one of the following statements **BEST** illustrates the way to curb the problem?
A. Increase the number of security notifications sent to employees about phishing attacks
B. Conduct regular phishing awareness training sessions and simulated phishing exercises for employees
C. Deploy a stricter firewall configuration to block all suspicious traffic
D. Enforce a policy requiring employees to immediately report all suspicious emails without training (2 marks)

38. A government agency uses separate Data Loss Prevention (DLP) tools for its email servers, cloud storage and endpoint devices. Which one of the following strategies can be used to enforce a uniform security policy across all platforms?
A. Centralised management console
B. Endpoint DLP agent isolation
C. Network-based DLP appliances
D. Cloud Access Security Broker (CASB) integration (2 marks)

39. A user unknowingly installed a program disguised as legitimate software. Once executed, the malicious application created a backdoor that allowed unauthorised remote access to the system. Which one of the following types of malware **BEST** describes this scenario?

A. Spyware

B. Rootkit

C. Ransomware

D. Trojan (2 marks)

40. A global e-commerce company encrypts customer data during online transactions so attackers cannot read it if intercepted. Which network security property is ensured?

A. Mitigation

B. Confidentiality

C. Risk reduction

D. Integrity (2 marks)

41. During a penetration test, an analyst gained admin privileges by exploiting a vulnerability from a low-privileged account but had not yet established persistence. This phase can be categorised as _______________.

A. reconnaissance

B. exploitation

C. privilege escalation

D. post-exploitation (2 marks)

42. During a penetration test, an analyst delivered malicious code to a workstation to exploit a vulnerability, but network segmentation prevented the code from reaching the restricted database server. Which one of the following components of the attack is being demonstrated?

A. Payload

B. Attack vectors

C. Threat landscape

D. Attack surface (2 marks)

43. In a networked environment, administrators configure servers and network devices to prevent unauthorised access attempts, stopping malware from reaching sensitive systems even if it evades antivirus detection. Which one of the following **BEST** illustrates this security mechanism?

A. Regular patching of operating systems

B. Antivirus software scanning files on endpoints

C. Encryption of sensitive data at rest

D. Firewall filtering traffic between networks (2 marks)

44. A network administrator initiates a scan of the company's servers using default credentials without administrator rights. The results only provide limited details about vulnerabilities. Which one of the following scanning methods is being conducted in this situation?

A. Authenticated scan

B. Unauthenticated scan

C. Network scan

D. Port scan (2 marks)

45. A financial services firm wants to ensure that sensitive financial reports can only be read by authorised users. Each report is individually encrypted so that only recipients with the correct decryption key can access its contents. Which one of the following security mechanisms **BEST** illustrates this scenario?

A. Keystore

B. Keytool

C. OpenPGP

D. OpenSSL (2 marks)

46. A corporation notices an attacker intercepting traffic between two systems on the same local network and manipulating communications without users noticing. Which one of the following types of attack intercepts traffic between two systems?

A. Man-in-the-Middle (MitM) attack

B. Denial of Service (DoS) attack

C. Phishing attack

D. SQL Injection (2 marks)

47. An attacker deceived an employee by posing as the company's help desk and convinced them to disclose a one-time passcode for system access. This type of social engineering attack can be classified as ________________.

A. baiting
B. spear phishing
C. tailgating
D. pretexting (2 marks)

48. Which one of the following particular facets of information system protection is the primary focus of network security?

A. Data stored locally
B. System hardware maintenance
C. Data during transmission
D. Software licensing management (2 marks)

49. A company wants to connect its branch office to its headquarters securely over the internet. The solution must encrypt all IP traffic at the network layer to ensure confidentiality and integrity. Which one of the following types of Virtual Private Network (VPN) is being used?

A. Remote Access VPN
B. IPsec VPN
C. SSL/TLS VPN
D. MPLS VPN (2 marks)

50. Which one of the following crucial connections between encryption and decryption is used by asymmetric cryptography?

A. Two distinct keys with mathematical connections
B. One common password key
C. The same keys are kept on several servers
D. Characters chosen at random from the plaintext (2 marks)

……………………………………………………………………………………

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK SECURITY

TUESDAY: 19 August 2025. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. The assurance that the communication is authentic and true to its source is known as _________________.
   A. mitigation procedure
   B. origin authentication
   C. exploit vulnerability
   D. risk prevention (2 marks)

2. Which one of the following social engineering techniques involves an attacker closely following an authorised individual to gain unauthorised access to a secure area?
   A. Phishing
   B. Baiting
   C. Tailgating
   D. Pretexting (2 marks)

3. A company allows employees to access internal apps over Wi-Fi. Guests on the same network gain visibility into internal devices. This could be caused by _______________________.
   A. lack of WPA3 encryption
   B. poor firewall firmware
   C. overuse of port security
   D. missing network isolation (2 marks)

4. An intern discovers after completing a security scan that a hidden program on her computer is secretly sending her data to an unknown destination. Which type of malware is responsible for secretly giving hackers access to a user's personal information?
   A. Worm
   B. Spyware
   C. Trojan horse
   D. Rootkit (2 marks)

5. Keyloggers often use stealth techniques to evade detection by traditional antivirus software. Which essential feature do end-point security tools use to detect such hidden threats?
   A. Basic signature-based detection
   B. Real-time file backup
   C. Manual virus definition updates
   D. Behaviour-based analysis (2 marks)

6. An organisation quickly restores operations after a network attack that caused a system failure by using a previously generated image of its server. What is the name of the technique for restoring an entire system that restores configurations and data?

A. System Patching
B. Disk Cloning
C. Image-Based Backup
D. Incremental Backup (2 marks)

7. Spear phishing threat actors frequently use social media sites for reconnaissance. Which privacy settings should people check and modify to reduce their vulnerability to these kinds of reconnaissance attempts?

A. Location sharing and post visibility
B. Screen resolution and font size
C. Background image and color theme
D. Notification sounds and vibration settings (2 marks)

8. A mid-sized company has experienced a surge in malware infections due to unpatched systems across its network. After implementing an automated patch management system, which one of the following outcomes would **BEST** demonstrate its effectiveness in reducing malware risk?

A. Employee surveys show improved satisfaction with software performance
B. The IT team reports patch deployment time reduced from an average of 120 days to 30 days
C. The network perimeter firewall logs increase in blocked external connection attempts
D. Laptop battery power consumption reduction following the installation of the latest operating system updates (2 marks)

9. Which one of the following **BEST** describes how SHA hash algorithms are applied in networked systems to verify software update integrity and detect unauthorised modifications?

A. They encrypt software updates to ensure confidentiality during transmission
B. They compress update files to reduce bandwidth consumption
C. They generate a unique hash value that is compared before and after transmission
D. They assign digital certificates to software packages to validate the identity of the sender (2 marks)

10. Which physical security control uses video monitoring to detect and deter suspicious activity or unauthorised access in areas such as server rooms and data centers?

A. Surveillance cameras
B. Motion alarm devices
C. Biometric scanners
D. Access badge systems (2 marks)

11. After looking through firewall logs, a system administrator discovered a series of SYN packets sent to many ports on several hosts without finishing the TCP handshake. Which reconnaissance activity does this **BEST** represent?

A. Packet sniffing
B. Banner grabbing
C. Ping sweep
D. TCP SYN scan (2 marks)

12. An employee received an email from an unknown sender requesting them to review an attached invoice. The attachment contained malicious code. What type of attack does this **BEST** illustrate?

A. Spoofing
B. Email Malware
C. Phishing
D. Spear Phishing (2 marks)

13. Port scanning helps both security professionals and attackers determine the services running on a system. Which one of the following **BEST** explains why accurately interpreting port scan results is essential for identifying potential system vulnerabilities?

A. It reveals if antivirus software is outdated and needs updating
B. It shows open ports with services that may be misconfigured
C. It ensures that systems are safe from all zero-day threats
D. It performs automatic patching of any detected weaknesses (2 marks)

14. Which one of the following types of malware has the potential to encrypt important documents and system files that could halt services and productivity in a local area network?

A. Spyware
B. Threatware
C. Adware
D. Ransomware (2 marks)

15. During an investigation, it was discovered that one employee was selling old business hard drives online without deleting the data. Which component of the media disposal policy was **MOST** likely ignored?

A. Physical destruction of media
B. Inventory management
C. Acceptable use policy
D. Backup retention schedule (2 marks)

16. To protect its network infrastructure from internal and external threats, an organisation implements a comprehensive strategy involving rules, processes and controls. This strategy is best described as ____________.

A. penetration testing
B. firewall configuration
C. security policy
D. network monitoring (2 marks)

17. In a Man-in-the-Middle (MITM) attack, a threat actor intercepts and potentially alters communication between two parties who believe they are communicating directly. Which one of the following tools is commonly used by attackers to intercept and manipulate network traffic?

A. Ettercap
B. Nessus
C. Wireshark in passive mode
D. Burp Suite in passive scan (2 marks)

18. Address spoofing is the process of modifying packet headers to impersonate another device on the network. Which one of the following scenarios could result from effective address spoofing?

A. Increased wireless signal strength
B. Encrypted communication by default
C. Improved routing efficiency
D. Unauthorised access to network resources (2 marks)

19. Which one of the following is the **BEST** practice to protect against an insider attack?

A. Protect non-critical assets
B. Enforce policies
C. Increase volatility
D. Promote non-culture changes (2 marks)

20. Access Control Lists (ACLs) regulates packets allowed or prohibited on a network, making them an essential security tool. What is the most critical factor to consider to ensure effective packet filtering?
A. The number of ACL entries
B. The placement of the ACL in the network
C. The length of the ACL rules
D. The version of the operating system running on the router (2 marks)

21. A healthcare institution recently moved its patient data management system to a cloud-based platform. Which one of the following methods is the **MOST** appropriate method to identify exploitable weaknesses before an actual breach occurs?
A. Security Information and Event Management (SIEM) monitoring
B. Vulnerability Assessment
C. Business Impact Analysis (BIA)
D. Post-incident forensic analysis (2 marks)

22. A telecom company assesses the possibility and consequences of cyberattacks on customer data stored in the cloud as part of its continuous risk analysis. This step is best described as ________________.
A. data classification
B. incident response
C. risk avoidance
D. risk assessment (2 marks)

23. An endpoint connects to the network and immediately floods it with ARP requests. Antivirus shows no alerts. What is likely going on?
A. Signature mismatch
B. VLAN trunking is broken
C. Antivirus is not network-aware
D. Transport Layer Security (TLS) inspection is misconfigured (2 marks)

24. A Security Operations Centre (SOC) Analyst uses Wireshark to capture and analyse network packets after detecting unusual traffic. This network security tool is mainly used for __________________.
A. packet sniffing and protocol analysis
B. blocking unauthorised access to the network
C. encrypting network communication
D. scanning for open ports on a system (2 marks)

25. The IT department of a university wants to ensure that only authorised individuals can remotely access its internal academic resources. Which one of the following methods would **BEST** help achieve this goal?
A. Use antivirus software on all university devices
B. Require VPN access with multi-factor authentication
C. Limit access to specific working hours only
D. Block all incoming traffic using firewall rules (2 marks)

26. A pharmaceutical company is revising its password policy to protect patient data in its internal health records system, aiming to reduce unauthorised access and improve overall account security. Which one of the following password policy implementations would **BEST** support this goal?
A. Use default passwords and change them after 30 days use
B. Allow the last 3 passwords and set expiration at 60 days total
C. Set a 15-day expiration with a 6-character minimum password length (2 marks)
D. Enforce 14-character minimum with complexity and history checks

27. A user from the HR department accesses finance resources without a valid business case. What firewall feature could enforce boundaries?

A. User-aware policies
B. Default deny rule
C. Stateful inspection
D. Packet capture logging (2 marks)

28. A local bank is implementing network access controls to prevent employees from accessing non-business-related websites during work hours. Which one of the following technologies would **BEST** assist the organisation in monitoring and filtering outbound web traffic?

A. DNS Server
B. Proxy Server
C. Load Balancer
D. DHCP Server (2 marks)

29. An organisation discovered that several dismissed employees retained access to critical systems weeks after their termination. Which administrative security measure would be most effective in preventing this issue?

A. Conducting regular security awareness training
B. Implementing a formal offboarding process
C. Installing endpoint detection and response (EDR) tools
D. Enforcing multi-factor authentication (MFA) (2 marks)

30. An attacker uses stolen employee credentials to access the internal CRM over the VPN. What would **BEST** reduce the impact of this breach?

A. Role-based network policies
B. Encrypted USB storage
C. VLAN mirroring for logging
D. Protocol whitelisting (2 marks)

31. Malicious software is intended to interfere with, harm, or obtain unauthorised access to computer systems. Which one of the following types of malware is used to extort payment from victims to restore access to their data?

A. Trojan
B. Spyware
C. Rootkit
D. Ransomware (2 marks)

32. A backdoor is installed by a penetration tester to keep continuous access to the system after they have successfully exploited a vulnerability. Which one of the following **BEST** describes this phase of penetration testing?

A. Cracking
B. Exploitation
C. Post-exploitation
D. Reporting (2 marks)

33. Threat actors usually exploit lateral movement to access sensitive systems once inside a network. How does network segmentation help in limiting an attacker's lateral movement after a successful breach?

A. It isolates systems using defined security boundaries
B. It distributes user credentials across multiple domains
C. It hides internal IP addresses using address translation
D. It monitors user activity through behavior analytics (2 marks)

34. Antivirus software now includes heuristic analysis in addition to signature-based detection to combat digital threats. How does heuristic analysis help antivirus software detect previously unknown malware?

A. It blocks network traffic using preset access rules
B. It updates virus definitions from online servers
C. It deletes known files listed in virus databases
D. It scans for code patterns that seem suspicious (2 marks)

35. ABC Ltd. wants to conduct a vulnerability scan that yields more complete and accurate results by logging into systems using approved credentials. Which one of the following scanning methods should be used?

A. Non-intrusive scan
B. Credentialed scan
C. Non-credentialed scan
D. Blind scan (2 marks)

36. Which one of the following statements **BEST** describes how information is secured to prevent unauthorised access while being transmitted?

A. Strong password requirements for user accounts
B. Firewalls to block unwanted inbound connections
C. Encryption techniques to protect data in transit
D. Access control policies for limiting user privileges (2 marks)

37. XYZ Tours and Travel Agency wants to restrict access to its internal network but finds that unauthorised IP addresses can still communicate with internal systems. Which one of the following is the **MOST** likely cause?

A. Misconfigured firewall access control list
B. Host-based intrusion prevention system
C. Improper disk encryption
D. Incorrect DNS resolution (2 marks)

38. A pretexting attack entails an attacker creating a fabricated scenario to manipulate a victim into revealing sensitive information. Which one of the following methods is **NOT** used to curb pretexting?

A. Implementing regular employee awareness training
B. Verifying identities before disclosing any sensitive information
C. Establishing a strong password policy
D. Encouraging employees to trust all internal communications (2 marks)

39. After implementing VLANs to separate network traffic, the organisation's security team begins investigating potential vulnerabilities. They discover that, despite the absence of proper routing, packets are still being transferred between VLANs. This activity suggests what type of attack?

A. DHCP starvation
B. ARP poisoning
C. VLAN hopping
D. MAC flooding (2 marks)

40. What procedure should be included in a network testing plan to ensure that all network changes are safely tested in a controlled environment, reducing the risk of unexpected outages in the production network?

A. Perform unscheduled updates during live hours
B. Conduct a simulated test lab before deployment
C. Apply updates directly to production systems
D. Bypass backup systems during network changes (2 marks)

41. Which one of the following statements **BEST** explains the importance of conducting regular cybersecurity awareness training in maintaining organisational network security?

A. It helps to eliminate all human errors from daily operations
B. It limits the responsibility of IT teams in securing the network
C. It ensures that staff are informed about evolving cyber threats
D. It reduces the need for expensive cybersecurity tools and solutions (2 marks)

42. Employees frequently have access to confidential data. What measures can organisations put in place to regulate user privileges and monitor internal operations in order to avoid unauthorised access or deliberate data leaks?
A. Disable system updates for users
B. Increase internet browsing speed
C. Use firewalls and website filters only
D. Implement role-based access control (2 marks)

43. As remote work becomes more common, employees often access corporate resources from various locations. Cryptography can help protect remote access and guarantee that sensitive data can only be decrypted by authorised users by _______________.
A. encrypting traffic and using digital certificates to verify remote users
B. compressing data and restricting access based on IP addresses only
C. assigning unique usernames and enforcing password complexity rules
D. installing antivirus tools and updating the remote workstation regularly (2 marks)

44. A penetration tester simulates an attack on an organisation's internal network by passively gathering data from publicly available sources like company websites, social media and WHOIS records. Which type of penetration testing is being conducted in this scenario?
A. White-box testing
B. Black-box testing
C. Grey-box testing
D. Open-box testing (2 marks)

45. Recently, your organisation implemented a Bring Your Own Device (BYOD) policy. Your supervisor has tasked you with ensuring that personal devices connecting to the corporate network comply with the organisation's security standards. Which one of the following policies would **BEST** support this directive?
A. Remote Access Policy
B. Data Classification Policy
C. Acceptable Use Policy
D. Network Access Control Policy (2 marks)

46. A forensic analysis revealed that malicious software had connected with a command-and-control server after infiltrating the network via a phishing email. Which one of the following network security tool would be **MOST** effective in blocking this communication?
A. Network Intrusion Detection System (NIDS)
B. Web Application Firewall (WAF)
C. Data Loss Prevention (DLP) System
D. Next-Generation Firewall (NGFW) (2 marks)

47. How can network segmentation and strong authentication mechanisms help reduce the risk of large-scale security breaches in networks with integrated IoT devices?
A. They limit access to internal systems and prevent lateral movement of threats
B. They make the devices invisible to end-users and shut down unused ports
C. They allow automatic updates and enable high-speed data transfers only
D. They remove the need for firewalls and prevent software installation errors (2 marks)

48. A law firm is creating a security policy to specify how its IT systems should be used. To stop illegal use, which one of the following should be included?

A. Steps to disable all antivirus software
B. A list of games allowed on lab computers
C. Instructions for installing personal software on servers
D. Guidelines for using strong and unique passwords (2 marks)

49. Malicious actors now have more options to take advantage of human psychology because of digital communication and online platforms. Which social engineering technique usually entails sending fake emails that seem legitimate?

A. Shoulder surfing
B. Pretexting acts
C. Phishing scams
D. Baiting attacks (2 marks)

50. The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses within a local network. Which one of the following statements **BEST** describes the goal of ARP spoofing in a compromised network?

A. Preventing network devices from resolving IP addresses
B. Associating the attacker's MAC address with a legitimate IP address
C. Encrypting ARP replies for secure communication
D. Enhancing ARP table accuracy (2 marks)

……………………………..………………………………………….

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK SECURITY

TUESDAY: 3 December 2024. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. A technician is tasked with preventing unauthorised access to a corporate Wi-Fi network. Which of the following security protocol should be implemented to achieve the highest level of security?
A. WEP
B. WPA
C. WPA2
D. Open network (2 marks)

2. Which one of the following security activity is **NOT** crucial for gaining a foundational understanding of the network infrastructure and detecting potential vulnerabilities?
A. Conducting a vulnerability scan on the network
B. Performing a thorough inventory of all network devices
C. Reviewing historical data on network performance
D. Implementing an intrusion detection system (2 marks)

3. During a security assessment, a technician discovers that several employees are using weak passwords. What is the **BEST** action the technician should recommend to enhance password security?
A. Increase the password length and complexity requirements
B. Implement a mandatory password change every week
C. Educate employees on password sharing
D. Disable all accounts with weak passwords immediately (2 marks)

4. When evaluating network performance, which metric is **MOST** critical for determining the speed at which data is transmitted?
A. Latency
B. Packet loss rate
C. Jitter
D. Throughput (2 marks)

5. The subset(s) of packet filtering that allows a firewall to react to an emergent event and update or create rules to deal with the event is known as ____________________.
A. dynamic
B. static
C. stateful
D. protocol (2 marks)

6. Which one of the following actions is **LEAST** likely to mitigate the risk of internal threats to an organisation's network security posture?
   A. Implementing strict access controls and regular audits of user permissions
   B. Educating employees about security best practices and potential threats
   C. Restricting network access to only essential services and applications
   D. Allowing unrestricted access to all network resources for improved employee efficiency (2 marks)

7. Wendy is facing frequent pop-up ads, a slow computer and unexpected redirects, leading her to suspect malware. What type of malware is responsible for displaying unwanted ads?
   A. Cryptojacking
   B. Spyware
   C. Adware
   D. Rootkit (2 marks)

8. Which one of the following authentication processes is based on something that the user is?
   A. Password
   B. Retina scan
   C. Key
   D. Smart card (2 marks)

9. Which of the following statements describes a potential negative consequence that could arise from performing an aggressive network scan?
   A. Detecting vulnerabilities
   B. Enhancing network security
   C. Identifying firewall misconfigurations
   D. Slowing down network traffic (2 marks)

10. You receive an urgent email from a senior executive requesting payment for a critical project, but it's a whaling attack designed to trick you into transferring company funds. What action should you take?
   A. Delete the email immediately without taking any action, as it may be a phishing attempt
   B. Reply to the email requesting more information about the payment and vendor before taking any action
   C. Forward the email to your IT department or security team for verification and follow their instructions
   D. Click the link in the email to authorise the payment, as it seems to be from a trusted executive (2 marks)

11. When establishing a Zone-Based Firewall for an enterprise, which of the following approaches is the **MOST** effective in guaranteeing comprehensive network protection?
   A. Configuring firewall rules based on individual IP addresses
   B. Creating specific allow rules based on necessary services and applications
   C. Using a single set of rules for all zones without distinguishing between internal and external traffic
   D. Allowing all traffic and only blocking known threats (2 marks)

12. Which one of the following network testing methods is used to measure the throughput and performance of a network?
   A. Load testing
   B. Packet sniffing
   C. Port scanning
   D. DNS resolution testing (2 marks)

13. Which of the following mechanisms is **BEST** for securely connecting remote users to an enterprise network with encrypted data transmission?
A. Virtual Private Network (VPN)
B. Intrusion Detection System (IDS)
C. Intrusion Prevention System(IPS)
D. Access Control List (ACL) (2 marks)

14. Which of the following statements represents a crucial factor to consider for ensuring effective protection of sensitive data?
A. Assigning static IP addresses to all devices
B. Using a single subnet for all devices
C. Implementing a firewall between subnets
D. Disabling DHCP on all routers (2 marks)

15. What practice is crucial for regularly updating and applying software fixes to prevent attackers from exploiting vulnerabilities?
A. Access control list
B. Patch management
C. Backup and recovery
D. Disaster recovery (2 marks)

16. The process of recording information about an employee's action when interacting with data and systems as well as information about the operations of your networking devices is referred to as ___________________.
A. accountability
B. authenticity
C. availability
D. non-repudiation (2 marks)

17. Which one of the following is primarily intended to safeguard devices from malware and viruses that may compromise data carried across a network?
A. Generic routing encapsulation
B. IP security
C. Firewall
D. Anti-virus software (2 marks)

18. How does disaster recovery planning help reduce downtime and prevent data loss in a network during a major IT incident?
A. By outlining specific procedures for restoring network services
B. By increasing the number of network administrators to handle all IT-related issues
C. By providing a set of guidelines for employees on how to handle day-to-day operations
D. Securing network infrastructure against attacks (2 marks)

19. What practice is essential for maintaining data integrity when multiple users are simultaneously accessing and editing a shared database in a new customer relationship management (CRM) system?
A. Regular data backups
B. Access controls
C. Data redundancy
D. Data archiving (2 marks)

20. Which one of the following steps **BEST** improves the security of a wireless network?
A. Changing the default SSID and network name regularly
B. Disabling guest access on the wireless router
C. Setting up a separate network for IoT devices
D. Using WPA3 encryption for wireless communication (2 marks)

21. Network setup involves connecting multiple devices to share resources and communicate with each other. What is a key benefit of implementing advanced encryption protocols for sensitive data?
A. Increased network speed
B. Enhanced data privacy
C. Improved device compatibility
D. Reduced hardware costs (2 marks)

22. Which one of the following is a potential benefit of adding network security measures to improve overall system efficiency?
A. Increased bandwidth usage
B. Hardware malfunction
C. Improved system performance
D. Exploitation of known vulnerabilities by attackers (2 marks)

23. What potential issues might arise when network devices are not properly configured?
A. Enhanced data encryption
B. Streamlined network traffic
C. Unauthorised access to sensitive data
D. Improved network speed (2 marks)

24. Which of the following represents an impact of password-cracking techniques on the security of user accounts and data?
A. They increase network performance by optimising user access
B. They help in identifying and fixing network vulnerabilities
C. They enhance the security of user accounts through better encryption methods
D. They may lead to unauthorised access and data theft (2 marks)

25. Which of the following statements describes potential risks that can occur for failing to implement effective login and monitoring practices to maintain system integrity and compliance?
A. Increased vulnerability to undetected breaches
B. Enhanced performance and reduced system latency
C. Improved data accuracy and quicker system recovery
D. Lowered costs and simplified system management (2 marks)

26. Which one of the following threats is **MOST** likely to be identified and addressed using automated network security tools and monitoring systems?
A. Social engineering attacks
B. Distributed denial-of-service attacks
C. Insider threats
D. Zero-day exploits (2 marks)

27. Which of the following is the **BEST** technique that network administrators could use to ensure intermediary devices are properly configured and maintained to prevent security breaches and improve network performance?
A. Avoid conducting routine performance and security assessments to minimise disruptions
B. Use outdated protocols to maintain compatibility with legacy systems, even if they are less secure
C. Disable login on devices to reduce the amount of stored data and avoid potential security risks
D. Regularly update device firmware to fix vulnerabilities and improve functionality (2 marks)

28. An object, person or other entity that represents a constant danger to information systems digital asset is known as a ____________________.
A. vulnerability
B. attack
C. threat
D. social engineering (2 marks)

29. What process involves gathering information about a target system or network to identify vulnerabilities before launching an attack?
A. Crypto mining
B. Reconnaissance
C. Brute force
D. Stalking (2 marks)

30. Which one of the following statements describes an attack where malicious code is inserted into a website to exploit vulnerabilities and potentially compromise user data?
A. Cross-Site Scripting (XSS)
B. Phishing Attack
C. Denial of Service (DoS)
D. SQL Injection (2 marks)

31. Which one of the following statements defines an impact of common issues related to software conflicts within a network?
A. Faster data transfer rates
B. Enhanced network security
C. Increased network bandwidth
D. Unresponsive network devices (2 marks)

32. Which one of the following tools optimises network resource performance in real-time?
A. Network Monitoring System (NMS)
B. Network Access Control (NAC)
C. Intrusion Detection System (IDS)
D. Proxy server (2 marks)

33. Which protocol is commonly used to securely manage and allocate network resources in Internet Protocol networks and the backbone of modern communication?
A. File Transfer Protocol (FTP)
B. Hypertext Transfer Protocol Secure (HTTPS)
C. Dynamic Host Configuration Protocol (DHCP)
D. Simple Mail Transfer Protocol (SMTP) (2 marks)

34. What security solution could be **MOST** effective in restricting unauthorised applications from accessing network resources while allowing granular control over functions within authorised applications?

A. Network Access Gateway
B. Network Application Control
C. Network Administration Console
D. Network Automation Control (2 marks)

35. Which strategy is used to optimise network resource usage by prioritising traffic based on its type?

A. Network Address Translation (NAT)
B. Network Time Protocol (NTP)
C. Simple Network Management Protocol (SNMP)
D. Quality of Service (QoS) (2 marks)

36. ___________________ occurs when unauthorised parties infiltrate computer systems, networks or databases to gain access to confidential information.

A. Phishing
B. Data breach
C. Exfiltration
D. Malware (2 marks)

37. Which one of the following statements **BEST** describes how Security Information and Event Management (SIEM) solutions assist organisations in identifying threats?

A. SIEM solutions analyse and correlate data to detect suspicious activities
B. SIEM solutions integrate with firewalls to block unauthorised access attempts
C. SIEM solutions collect and store sensitive business data to prevent breaches
D. SIEM solutions encrypt all network traffic to enhance security (2 marks)

38. Which one of the following security measures requires users to provide two forms of identification before being granted access to a system or account?

A. Biometric authentication
B. Two-factor authentication
C. Password-based authentication
D. Multi-factor authentication (2 marks)

39. Which one of the following statements **BEST** describes the importance of regularly reviewing and updating a network security policy?

A. It improves the performance of the network and speeds up data transmission
B. It reduces the need for user authentication across the organisation
C. It increases employee productivity by reducing security protocols
D. It ensures compliance with evolving legal and regulatory requirements (2 marks)

40. In the context of risk analysis, which method is most frequently employed to evaluate vulnerabilities within a network?

A. Penetration testing
B. Network monitoring
C. Data encryption
D. Firewalls (2 marks)

41. Which practice is **NOT** part of the implementation phase of a network security framework for a small tech startup company that has conducted a risk assessment and developed security protocols?

A. Conducting a vulnerability assessment
B. Deploying firewalls and intrusion detection systems
C. Developing security awareness training materials
D. Reviewing and updating security policies (2 marks)

42. Which one of the following is **MOST** likely to be recognised as a critical asset during network assessment?

A. Standard employee records
B. Routine email communications
C. Sensitive financial data
D. Publicly available company brochures (2 marks)

43. Which one of the following methods is used to manage user permissions and access to systems and data within the framework of logical security controls?

A. Data encryption
B. Network segmentation
C. Physical access control
D. Role-based access control (2 marks)

44. Which one of the following techniques is **MOST** effective for detecting and analysing anomalies in network traffic protocols?

A. Stress testing
B. Network monitoring
C. Protocol analysis
D. Packet capture (2 marks)

45. What is the primary objective of a ransomware attack on a company's IT infrastructure, considering that ransomware has become increasingly sophisticated and poses a serious threat to individuals and organisations worldwide?

A. To demand payment for decrypting files
B. To improve system performance
C. To steal financial data
D. To enhance network security (2 marks)

46. Which one of the following is a potential drawback of implementing a robust network security system?

A. Increased risk of unauthorised access
B. Higher operational costs
C. Simplified management and monitoring
D. Increased network performance (2 marks)

47. Which type of fraudulent activity targeting a network involves using fake support requests to obtain sensitive data from employees?

A. Shoulder surfing
B. Pretexting
C. Vishing
D. Scareware (2 marks)

48. Which one of the following attack methods exploits weaknesses in a trusted third-party vendor to get access to a target organisation’s systems?

A. Watering hole attack
B. Dumpster diving
C. Supply chain attack
D. Fileless malware (2 marks)

49. Which one of the following is a likely impact of Malware attack?

A. Disruption of essential services and potential endangerment of public safety
B. Enhanced collaboration between governmental and private sectors for cybersecurity
C. Increased public awareness and education about cybersecurity
D. Improved security measures and resilience in public safety systems (2 marks)

50. The following practices are part of a network security implementation, **EXCEPT** ________________.

A. Risk assessment
B. Asset management
C. Incident response
D. Data protection (2 marks)

……………………………..…………………………………………….

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK SECURITY

TUESDAY: 20 August 2024. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. What is the principal objective of instituting Network Access Control (NAC) within an organisation?
   A. To enhance the overall performance and efficiency of the network infrastructure
   B. To continuously monitor and analyse network traffic for security and optimisation
   C. To enforce and manage policies governing access to network resources
   D. To secure data by encrypting it during transmission across the network (2 marks)

2. What is the **MAIN** difference between penetration testing and vulnerability assessment as used in network security?
   A. Penetration testing aims to exploit vulnerabilities, while vulnerability assessment identifies and quantifies them
   B. Vulnerability assessment focuses on network performance, while penetration testing tests software functionality
   C. Penetration testing scans for malware, while vulnerability assessment tests network encryption
   D. Vulnerability assessment evaluates network speed, while penetration testing assesses firewall effectiveness (2 marks)

3. Which one among the following is a potential risk associated with performing a network scan?
   A. Improved network performance
   B. Accidental disclosure of sensitive information
   C. Unintended escalation of network security vulnerabilities
   D. Enhanced user productivity (2 marks)

4. Which one of the following actions should be taken after receiving an email containing phishing content?
   A. Click on the provided link to confirm your identity
   B. Ignore the email and delete it immediately
   C. Forward the email to your friends and family to warn them about the phishing attempt
   D. Reply to the email with your account details to verify your identity and secure your account (2 marks)

5. In the context of Network security, which one of the following statements **BEST** depicts the purpose of Firewall?
   A. Encrypting network traffic
   B. Authenticating users
   C. Detecting and removing malware
   D. Monitoring and controlling network traffic (2 marks)

6. Which one of the following is a common indicator of a Distributed Denial of Service (DDoS) attack?
   A. Unusually high network traffic volume
   B. Unexpected software fixes and updates
   C. Increased system uptime
   D. Decreased CPU usage (2 marks)

7. In terms of network security, what is the purpose of network segmentation?
A. Encrypting network traffic
B. Monitoring network activity
C. Dividing the network into smaller, isolated segments
D. Identifying and removing malware infections (2 marks)

8. Which security measure determines who has access to network resources and what actions should be taken?
A. Patch Management
B. Access Control
C. Intrusion Detection
D. Disaster Recovery (2 marks)

9. Which testing method involves having full knowledge of the network and systems being tested?
A. Black-box testing
B. White-box testing
C. Gray-box testing
D. Blue-box testing (2 marks)

10. How do network technicians utilise logging and monitoring in network security operations?
A. Encrypting network traffic
B. Establishing secure connections
C. Providing authentication
D. Identifying security incidents (2 marks)

11. Which one of the following describes a proactive security approach in which security experts actively look for indications of malicious activity or advanced threats within the network environment of an organisation?
A. Threat Modelling
B. Threat Intelligence
C. Threat hunting
D. Threat landscape (2 marks)

12. What is the primary objective of network security's incident response and disaster recovery procedures?
A. Minimising the impact of security breaches
B. Preventing unauthorised access
C. Monitoring network activity
D. Securing network infrastructure against attacks (2 marks)

13. Which network security concept involves ensuring that users have access only to the resources they are authorised to use?
A. Strong Password Policy
B. Network Hardening
C. Least Privilege
D. Data Encryption (2 marks)

14. Which one of the following statements **BEST** depicts the essence of network security for business operations?
A. It ensures uninterrupted business operations
B. It reduces the cost of hardware
C. It simplifies software development
D. It lowers employee training costs (2 marks)

15. Which feature of network security promotes confidence among customers and partners?
A. Reducing the cost of IT services
B. Enhancing data protection
C. Simplifying network management
D. Increasing network traffic (2 marks)

16. Which one of the following techniques involves concealing the true destination of data by modifying its headers?
A. Network Address Translation (NAT)
B. Data masking
C. Firewall configuration
D. Digital encryption (2 marks)

17. Which one of the following actions is as a result of misconfigured network devices?
A. Enhanced network performance
B. Open unintended access points
C. Reduced power consumption
D. Automatic software updates (2 marks)

18. Which is the **MAIN** threat posed by Man-in-the-Middle (MitM) attacks?
A. Decreasing network bandwidth
B. Enhancing encryption methods
C. Disabling network hardware
D. Altering data between two parties (2 marks)

19. Which component of network security structure involves defining roles, responsibilities and procedures to ensure network protection?
A. Security policy management
B. Network intrusion management
C. Security operations
D. Identity and access management (2 marks)

20. Which one of the following statements **BEST** describess a potential insider threat?
A. External hackers trying to penetrate the network
B. Contractors using their network access maliciously
C. Automated malware infections
D. Natural disasters affecting network infrastructure (2 marks)

21. What technology is commonly used to achieve non-repudiation in network communications?
A. Firewalls
B. Anti-Malware
C. Digital signatures
D. Intrusion Detection Systems (IDS) (2 marks)

22. In the context of encryption algorithms, which one of the following is considered a symmetric key encryption method?
A. RSA
B. Diffie-Hellman
C. ECC
D. AES (2 marks)

23. Which term defines the persuasion of persons into disclosing secret information or taking activities that jeopardise security?
A. Credential Stuffing
B. Cryptojacking
C. Social Engineering
D. Advanced Persistent Threat (APT) (2 marks)

24. The primary purpose of implementing Network Segmentation in a large enterprise network is to _____________.
A. simplify network management tasks
B. isolate and contain security breaches
C. increase network latency
D. reduce the need for encryption (2 marks)

25. In the context of encryption algorithms, which one of the following is a public-key cryptography algorithm which uses prime factorisation as the trapdoor one-way function.?

A. RSA
B. Diffie-Hellman
C. ECC
D. AES (2 marks)

26. Which type of network security device tracks the state of active connections and makes decisions based on the context of the traffic?

A. Packet-filtering Firewall
B. Proxy Firewall
C. Next-Generation Firewall
D. Stateful Inspection Firewall (2 marks)

27. Which one of the following is **NOT** a security solution that helps organisations manage and secure access network resources?

A. Intrusion Detection System (IDS)
B. Network Access Control (NAC)
C. Virtual Private Network (VPN)
D. Firewall (2 marks)

28. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols designed to provide secure communication over a network. Which of the following aspects of the two cryptographic protocols ensures that data transmitted over a network is only readable by the intended recipient?

A. Authentication
B. Encryption
C. Data Integrity
D. Handshake Process (2 marks)

29. A centralised interface that allows network administrators to manage, monitor and maintain a network's infrastructure to ensure the security and performance of network components is known as __________________.

A. Network Access Gateway
B. Network Application Control
C. Network Administration Console
D. Network Automation Control (2 marks)

30. Which endpoint security component is intended to detect and respond to threats on specific devices?

A. Intrusion Detection System (IDS)
B. Endpoint Detection and Response (EDR)
C. Firewall
D. Proxy Server (2 marks)

31. Which security measure helps protect web applications from common vulnerabilities?

A. Intrusion Prevention System (IPS)
B. Network Address Translation (NAT)
C. Web Application Firewall (WAF)
D. Content Delivery Network (CDN) (2 marks)

32. Which one of the following is the main function of Security Information and Event Management (SIEM) systems?

A. Provide real-time analysis of security alerts
B. Encrypt data transmissions
C. Filter network traffic
D. Establish secure connections over the internet (2 marks)

33. The physical security measure that is typically emphasised from a security perspective is ___________________.

A. two-factor authentication
B. encryption protocols
C. security cameras
D. anti-virus software (2 marks)

34. Why is it essential for a security policy to align closely with an organisation's specific requirements?
A. It increases the likelihood of security incidents
B. It ensures compliance with industry standards
C. It improves employee morale
D. It mitigates risks effectively (2 marks)

35. Which security principle emphasises the importance of regularly updating software and systems to protect against vulnerabilities?
A. Least privilege
B. Patch management
C. Defense-in-depth
D. Network segmentation (2 marks)

36. Which one of the following is an example of a network vulnerability?
A. Regular software updates
B. Strong encryption protocols
C. Weak password policies
D. Employee training programs (2 marks)

37. Which one of the following is **NOT** a logical security control measure?
A. Firewalls
B. Encryption
C. Intrusion Detection Systems (IDS)
D. Physical access controls (2 marks)

38. Which security measure entails checking systems for flaws and deploying updates quickly?
A. User education and awareness
B. Vulnerability management
C. Application security
D. Incident response planning (2 marks)

39. A set of rules or patterns that security systems use to identify and classify malicious activity is referred to as ________________.
A. attack pattern
B. attack path
C. attack surface
D. attack signature (2 marks)

40. Which one of the following statements **BEST** describes the main purpose of a network testing plan?
A. To design the network topology
B. To ensure the reliability, security and performance of the network
C. To install network hardware
D. To monitor network traffic (2 marks)

41. Which one of the following is an example of a testing method used in a network testing plan?
A. Conducting vulnerability assessments
B. Installing antivirus software
C. Monitoring network traffic
D. Configuring firewalls (2 marks)

42. Which one of the following **BEST** describes an internal threat to an organisation's Network security posture?
A. Malware attacks from external hackers
B. Unauthorised access by a former employee
C. Distributed denial-of-service (DDoS) attacks
D. Natural disasters causing infrastructure damage (2 marks)

43. Hackers attempting to infiltrate an organisation's network from outside can be categorised as ________________.
A. internal threat
B. physical threat
C. cyber threat
D. environmental threat (2 marks)

44. Which one of the following consequences is posed by a ransomware attack?
A. Employee misconduct
B. Physical damage to company property
C. Destruction of hardware components
D. Disruption of business operations (2 marks)

45. Which one of the following statements distinguishes pretexting from phishing?
A. It primarily uses emails to deceive targets
B. It relies on exploiting software vulnerabilities
C. It uses technical tools to intercept data
D. It involves creating a fabricated identity (2 marks)

46. Which strategy of reverse social engineering entails conducting penetration testing to identify vulnerabilities within an organisation?
A. Awareness Training
B. Counterintelligence
C. Behavioral Analysis
D. Mock Attacks (2 marks)

47. Which is the common method used to prevent unauthorised access to a wireless network?
A. Implementing IP routing
B. Using MAC address filtering
C. Using HTTP Secure (HTTPS)
D. Performing data backups (2 marks)

48. Which type of malware is designed to spread from one infected machine to another?
A. Trojan Horse
B. Spyware
C. Worm
D. Ransomware (2 marks)

49. Which one of the following is **NOT** usually included in a network security framework?
A. Security Policies and Procedures
B. Network Monitoring Software
C. Encryption
D. Social Media Platforms (2 marks)

50. In the context of network setup, what is the primary objective of security audits and assessments?
A. To provide remote access to the network
B. To enforce security policies and procedures
C. To identify and address security vulnerabilities
D. To increase network performance (2 marks)

…………………………..……………………………………………….

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 22 April 2024. Afternoon Paper. **Time Allowed: 3 hours.**

Answer ALL questions. This paper has two sections. SECTION I has twenty (20) short response questions. Each question is allocated two (2) marks. SECTION II has three (3) practical questions of sixty (60) marks. Marks allocated to each question are shown at the end of the question.

Required Resources:

- **Windows Server 2016/2019/2022 image**
- **Oracle Virtual box**
- **Linux/Windows computer**

SECTION I (40 MARKS)

1. The role responsible for centralising the management of identity and access in Windows Server is known as: (2 marks)

2. What is the term used to describe the middle tier of a three-tier client-server architecture? (2 marks)

3. What is the name of a network operating system that maintains a centralised database of user accounts, group memberships and networked devices, making administration and resource access easier? (2 marks)

4. A type of Network Operating System (NOS) where in the network is controlled centrally is referred to as: (2 marks)

5. Write down the Windows server role which is responsible for providing certificate services including digital certificate creation and maintenance. (2 marks)

6. State the hierarchical directory structure that allows logical and structured approach to store and retrieve information with the root directory and subdirectories branching out from it. (2 marks)

7. State the name of the command used to prepare a file system for usage on a Windows operating system-based storage medium, such as a USB drive, hard disk or other storage device. (2 marks)

8. During booting, the primary partition containing the operating system and marked as active is referred to as: (2 marks)

9. In the context of Network Operating system, how many primary partitions exists in a conventional Master Boot Record (MBR)? (2 marks)

10. During installation, the component that controls how the underlying hardware and the way Network Operating system communicates is referred to as: (2 marks)

11. What is the name given to installation technique that enables the Network operating system to be installed simultaneously on several computers by the administrator from a single location? (2 marks)

12. A feature in network operating system that allows administrators to define and manage system settings for users and computers within an Active Directory environment is known as: (2 marks)

13. Which configuration setting present in many operating systems governs how the graphical user interface (GUI) looks and functions? (2 marks)

14. Which feature of Active Directory Certificate Services (ADCS) allows non-Windows devices like routers, switches and network appliances to get digital certificates for secure network communication? (2 marks)

15. What should be considered while selecting a network operating system in terms of compatibility? (2 marks)

16. What is the term used to describe a network's ability to prioritise particular types of traffic, ensuring that key applications receive the resources they require while being unaffected by non-essential traffic? (2 marks)

17. A security component in a network operating system environment designed to protect a network by monitoring and controlling incoming and outgoing traffic is known as: (2 marks)

18. The process of dividing a disk into sectors that the disk controller can read and write, before a disk can store data is known as: (2 marks)

19. What is the term used to describe a logical grouping of network objects like people, computers and devices that share a common directory database? (2 marks)

20. Which type of networking technology allows sites from two networking operating systems to connect securely and encrypted through the internet? (2 marks)

SECTION II (60 MARKS)

Create a word processing document named "Question 21" and use it to save your answers to questions (a) to (f) below.

21. In a network context, a file server is a type of server role that is in charge of organising, controlling and granting access to files and folders.

(a) Configure file services as a server role. (4 marks)

(b) Enable group policy management feature. (2 marks)

(c) Display the disk, volume and storage pool. (2 marks)

(d) Display Windows Update Services (WSUS) Content Properties. (2 marks)

(e) Using WSUS display the performance alert threshold for CPU usage and memory. (6 marks)

(f) Using system configuration tool, enable Microsoft iSCSI target server service. (4 marks)

Save "Question 21" document and upload. **(Total: 20 marks)**

22. Create a word processing document named “Question 22” and use it to save your answers to questions (a) to (e) below.

Using local security policy settings of your server manager enable the following:

(a) Limit with default settings of local account use of blank passwords to console logon only. (3 marks)

(b) Enable Require domain controller authentication to unlock workstation. (3 marks)

(c) Enable temporary state of networks that are in the process of being identified to private. (4 marks)

(d) State the number logon attempts that causes a user account to be locked out to be 3. (4 marks)

(e) Configure the firewall to be in a position to block inbound connection and allow outbound connections. (6 marks)

Save “Question 22” document and upload. **(Total: 20 marks)**

23. Create a word processing document named “Question 23” and use it to save your answers to questions (a) to (e) below.

PowerShell is a cross-platform task automation system consisting of a command-line shell, a scripting language and a configuration management framework. Use PowerShell to perform the following:

(a) Use appropriate command utility to display network connection profiles on the system. (4 marks)

(b) Use appropriate command utility to retrieve information about IP addresses assigned to network Interfaces. (4 marks)

(c) Use appropriate command utility to display retrieves DNS server addresses configured on the system. (4 marks)

(d) Use appropriate command utility to retrieve information about the firewall profiles on the system. (4 marks)

(e) Use appropriate command utility to retrieve information about active TCP connections on the system. (4 marks)

Save “Question 23” document and upload. **(Total: 20 marks)**

……….…………………………………………………………………………

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 4 December 2023. Afternoon Paper. **Time Allowed: 3 hours.**

Answer ALL questions. This paper has two sections. SECTION I has twenty (20) short response questions. Each question is allocated two (2) marks. SECTION II has three (3) practical questions of sixty (60) marks. Marks allocated to each question are shown at the end of the question.

Required Resources:

- **Windows Server 2016/2019/2022 image**
- **Oracle Virtual box**
- **Linux/Windows computer**

SECTION I (40 MARKS)

1. State the types of drives appropriate in a network operating system environment because of their speed, dependability, durability and energy efficiency for applications demanding high-speed access, decreased latency and enhanced reliability: (2 marks)

2. State the peer-to-peer (P2P) network feature which ensures that users manage their own resources, determine which resources to share and regulates who gets access to their resources. (2 marks)

3. The network operating system utility primarily used to check the integrity of a storage device's file system is known as: (2 marks)

4. The type of network operating system that lets users share network resources saved in a common, accessible location and where all devices are treated equally in terms of functionality is known as: (2 marks)

5. What is the name of the feature that improves the security of system limiting application software to standard user privileges until an administrator authorises an increase or elevation. (2 marks)

6. The process of installing and configuring software on a computer or device without the assistance of a graphical user interface (GUI), physical monitor, keyboard and mouse is known as: (2 marks)

7. State the type feature of network operating system that allows users to collaborate and work together more efficiently and also helps to reduce cost by allowing multiple users to share expensive resources. (2 marks)

8. State the policy type that allows Active Directory to guard against brute force attacks by blocking an account after a certain number of failed login attempts? (2 marks)

9. What are the lightweight commands that perform specific actions or operations within the PowerShell environment? (2 marks)

10. When using Active Directory, state the containers that are used to represent an organisation's hierarchical structure, such as departments, teams or geographical locations. (2 marks)

11. A distributed data repository with a subset of properties for all objects in the forest is referred to as: (2 marks)

12. Which computer configuration allows you to install and operate numerous operating systems on a single computer or device and is beneficial for a variety of tasks such as testing alternative operating systems, running older software or separating work and personal environments? (2 marks)

13. A directory that contains the files required to install an operating system on a computer over the network is known as: (2 marks)

14. In the event that something goes wrong during the installation or upgrade process, which method of a software installation is utilised to provide an organised and documented plan for reverting to the prior state or version of a system? (2 marks)

15. In network operating systems and settings such as Active Directory, which security model is utilised to implement strict access control restrictions based on security labels and clearances? (2 marks)

16. To enable certain network tasks and user authentication, what is the name of the network operating system that normally provides such features like web servers, email servers and Active Directory? (2 marks)

17. Which software applications and utilities are used to assist network administrators and IT professionals in ensuring that networks run smoothly, provide a positive user experience and quickly discover and resolve issues? (2 marks)

18. Which users in a network operating system often refer to individuals or accounts having greater control and access to various resources, configurations and settings than normal or standard users? (2 marks)

19. State the command utility which is used to join a machine to a domain and is specifically built for administering Active Directory domains and trusts. (2 marks)

20. The process of enhancing a server's performance, capacity and capabilities in a computer network or data center is referred to as: (2 marks)

SECTION II (60 MARKS)

Required Resources:

- **Windows server 2016/2019/2022 Image**
- **Oracle Virtual box**
- **Linux/Windows computer**

21. Create a word processing document named "Firewall" and use it to save your answers to questions (a) to (e) below:

Proper configuration of firewall is crucial for securing network operating system and controlling traffic based on an organisation's needs and security policies.

(a) Open windows defender firewall with advanced security settings and display the following active Firewall Rules. (2 marks)

(b) Customise the outbound rule for email and account properties on local area network and remote access only. (4 marks)

(c) Allow edge traversal for windows remote management (HTTP-In) properties. (4 marks)

(d) Create a connection Rule named LAN - Authentication to Authenticate your computer to the gateway with appropriate Certificate Authority? (6 marks)

(e) Customise the logging settings for domain profile to allow dropped packets and successful connections. (4 marks)

Save "Firewall" document and upload. **(Total: 20 marks)**

22. Create a word processing document named “Group policy” and use it to save your answers to questions (a) to (d) below:

Group Policy allows a system administrator to centrally manage and apply various settings and preferences to user and computer objects in Active Directory domain.

(a) Configure the network operating system to automatically connect to suggested open hotspot, network shared by contacts and to hotspot offering paid services. (4 marks)

(b) Configure the network operating system to let applications access cellular data. (4 marks)

(c) Open policy-based quality of service and enable Inbound TCP throughput to maximum. (6 marks)

(d) Configure user permissions to allow users to change the network name, location and icon on a connected network. (6 marks)

Save “Group policy” document and upload. **(Total: 20 marks)**

23. Create a word processing-document named “NPAS” and use it to save your answers to questions (a) to (e) below.

Network policy and access services (NPAS) plays a crucial role in managing network access and enforcing network policies within your organisation's infrastructure.

(a) Open server manager in your network operating system and install Network policy and Access Services. (6 marks)

(b) Configure NPAS to log accounting data to a local text file on a local computer. (4 marks)

(c) Within NPAS, display Network Interface Card teaming for the server. (4 marks)

(d) Display Network operating system server logs in relation to Network policy and access services. (4 marks)

(e) Display the way a user can shutdown a server from NPAS. (2 marks)

Save “Network policy” document and upload. **(Total: 20 marks)**

……….………………………………………………………………………

kasneb

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINISTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 21 August 2023. Afternoon Paper. **Time Allowed: 3 hours.**

Answer ALL questions. This paper has two sections. SECTION I has twenty (20) short response questions. Each question is allocated two (2) marks. SECTION II has three (3) practical questions of sixty (60) marks. Marks allocated to each question are shown at the end of the question.

Required Resources:

- Windows Server 2016/2019/2022 image
- Oracle Virtual box
- Linux/Windows computer

SECTION I (40 MARKS)

1. The network operating system feature that allows the network administrator to configure the server to assign IP addresses to clients on the network is called ______________________. (2 marks)

2. What is the name of a small program responsible for locating and loading the network operating system? (2 marks)

3. The type of network operating system that provides users with access to resources through a server is called ____________________. (2 marks)

4. What is the name of a network operating system feature that improves the security of system limiting application software to standard user privileges until an administrator authorises an increase or elevation? (2 marks)

5. Active Directory (AD) groups simplify the administration of user accounts or computers in different AD domains by collating them and assigning ubiquitous access rights. How many types of groups are available in Active Directory? (2 marks)

6. The active directory service that keeps track of domain members, verifies their credentials and establishes their access privileges is called? (2 marks)

7. What is the name of an image of the system configuration and settings that helps in restoring the system to an earlier date when the system was running perfectly? (2 marks)

8. Rana, a newly hired intern at an IT consulting company logs into Active Directory on a workstation and then discovers user home directory does not redirect to a network share on a file server. State the command which could be used to verify the group policy settings? (2 marks)

9. A network technician was preparing to install a Network Operating System (NOS) in a workstation. The process that prepares a file system in a partition for files to be stored is known as __________________. (2 marks)

10. The activity that determines the hardware that servers require is referred to as ___________________. (2 marks)

11. State the term that describes the type of installation used to install a network operating system on a brand new server. (2 marks)

12. The process of dividing a disk into one or more regions to ensure better data organisation is called __________________. (2 marks)

13. A network security device that monitors, filters incoming, and outgoing network traffic based on an organisation's previously established security policies is called _____________________. (2 marks)

14. The network operating that distributes traffic across several servers by using the TCP/IP networking protocol is referred to as ____________________. (2 marks)

15. The term that best describes the hardware and software that enables network connectivity and communication between users, devices and applications is called ____________________. (2 marks)

16. An object-oriented automation engine and scripting language with an interactive command-line shell that was developed to help IT professionals configure systems and automate network administrative tasks is known as _____________________. (2 marks)

17. Name the term that describes the digital ecosystem that allows devices and users to communicate and share data in a network. (2 marks)

18. What is the name given to separate form of volume management that allows volumes to have noncontiguous extents on one or more physical disks? (2 marks)

19. The use of unique biological features for digital authentication and access control is known as ____________________. (2 marks)

20. The universal tool used to reboot or repair a system or boot a live system from a USB is referred to as ___________________. (2 marks)

SECTION II (60 MARKS)

INSTRUCTIONS

Required Resources:

- Windows server 2016/2019/2022 Image
- Oracle Virtual box
- Linux/Windows computer

21. Create a word processing document named "Task manager" and use it to save your answers to questions (a) to (d) below:

Task Manager provides information about computer performance and running software such as processes, CPU and GPU load, commit charge, I/O details, logged-in users, and Windows services.

Using task manager of the network operating system perform the following:

(a) Open performance tab and display the following:
   (i) CPU Utilisation of the server
   (ii) Memory Usage
   (iii) Ethernet Throughput

(b) Open Resource monitor and display the current TCP connections with listening ports. (6 marks)

(c) Display the user of the system with the running process. (4 marks)

(d) Display process ID with the status. (4 marks)

Save "Task manager" document and upload.

(Total: 20 marks)

22. Create a word processing document named “Environment variable” and use it to save your answers to questions (a) to (d) below.

Use the network operating system to display the following:

(a) The environment variables for your Network operating system. (6 marks)

(b) The window for adjusting the settings for processor scheduling to allocate resources to programs. (6 marks)

(c) Active directory site and services console. (4 marks)

(d) Active directory users and computers console document. (4 marks)

Save “Environment variable” and upload.

(Total: 20 marks)

23. Create a word processing document known as “Quota Management” and use it to save your answers to questions (a) to (e) below.

Using the network operating system perform the following:

(a) Display procedure for compressing drive to save disk space of your Network operating system. (4 marks)

(b) Display tools for error checking and Optimizing/Defragmenting the drive. (4 marks)

(c) Enable Quota Management for the disk. (4 marks)

(d) Display Windows Management Instrumentation control properties for security. (4 marks)

(e) Display the window for turning on Active Directory Lightweight Directory Services. (4 marks)

Save “Quota Management” document and upload.

(Total: 20 marks)

……………………………………………………………………………

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINSTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 24 April 2023. Afternoon Paper. **Time Allowed: 3 hours.**

Answer ALL questions. This paper has two sections. SECTION I has twenty (20) short response questions. Each question is allocated two (2) marks. SECTION II has three (3) practical questions of sixty (60) marks. Marks allocated to each question are shown at the end of the question.

Required Resources:

- Windows Server 2016/2019/2022 image
- Oracle Virtual box
- Linux/Windows computer

SECTION I (40 MARKS)

1. What is the name of the default terminal server application in Windows Server? (2 marks)

2. The task performed by the Central Processing Unit that decides the way and order in which processes should be executed is known as: (2 marks)

3. The name of the group that provides users with access to network resources and to assign permissions to control access to these resources is known as: (2 marks)

4. Raid ensures data is copied onto multiple drives for faster throughput, error correction, fault tolerance and improved mean time between failures. Which type of RAID can be used to configure two drives for maximum performance? (2 marks)

5. Multitasking operating system (OS) can work on more than one task at a time by switching between the tasks very rapidly. Which part of an operating system is the active program running but not visible to the user? (2 marks)

6. A cross-platform command-line shell designed for system administration such as automation and configuration is known as: (2 marks)

7. A level of security where only digitally signed programs from trusted publishers are allowed to run, and all user-installed programs are blocked is known as: (2 marks)

8. Which is the service that is used to transfer files between computers on a network? (2 marks)

9. What is the name given to a client-server interface that allows computers in a network to be booted from the server on the network before deploying the obtained PC image in local and remote offices? (2 marks)

10. Kennedy wishes to install an operating system into his computer and maintain his files. Which type of operating system installation preserves system settings, personal files, and applications from an older operating system version? (2 marks)

11. What is the name of the logical drive that is created to create more than one physical part of the same size? (2 marks)

12. Which component of a network operating system uses both hardware and software to enable a computer to compensate for physical memory shortages, temporarily transferring data from random access memory (RAM) to disk storage? (2 marks)

13. Which specification of a software program is used by operating system to communicate and provide a lightweight BIOS alternative that uses only the information needed to launch the OS boot process? (2 marks)

14. Which is the unique identifiers assigned to each user or group in Windows Server that controls access to resources on the network? (2 marks)

15. A tool used by administrators in a network operating system to examine the way programs running on their computers affect performance in real time is known as: (2 marks)

16. What is the name given to a logical construct used by Active Directory Domain Services (ADDS) to group one or more domains? (2 marks)

17. The process of creating multiple virtual instances of an operating system on a single physical server is called: (2 marks)

18. What is the name given to the process of removing a user sensitive data a set of data in an active directory by randomising data using various data shuffling and manipulation techniques? (2 marks)

19. Boot Configuration Data (BCD) files provide a store that is used to describe boot applications and boot application settings. Which command line tool is used to display and modify the boot configuration datastore? (2 marks)

20. Which storage mechanism is used to retrieve processes from the secondary storage into the main memory? (2 marks)

SECTION II (60 MARKS)

INSTRUCTIONS

Install Oracle virtual box and Window server image to your computer and answer the following questions:

Required Resources:

- Windows server 2016/2019/2022 Image
- Oracle Virtual box
- Linux/Windows computer

21. Create a word processing document named “Question 21” and use it to save your answers to questions (a) to (e).

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web.

(a) Add appropriate web server. Capture a screen shot. (6 marks)

(b) Open a web browser and type 127.0.0.1 at the address bar. Capture the image. (2 marks)

(c) Locate the wwwroot file and capture the screen shot of its contents: (2 marks)

(d) In the folder wwwroot, create a file index.html and key in the following text. Capture an appropriate screen shot: (5 marks)

(e) Reopen a web browser and type 127.0.0.1 at the address bar. Capture the screen shot: (5 marks)

Upload “Question 21” document.

(Total: 20 marks)

22. Create a word document named "Question 22" and use it to save your answers to questions (a) to (c):

(a) Display the number of processor and maximum memory used by your Network Operating System. Capture the screen shot. (4 marks)

(b) Using appropriate tool activate the following services.

(i) Network connectivity assistant. Capture the screen shot. (3 marks)

(ii) Network connections. Capture a suitable screen shot. (3 marks)

(iii) Network list service. Capture a suitable screen shot. (3 marks)

(iv) Network setup. Capture a suitable screen shot. (3 marks)

(c) Display in-depth record of events related to the system of your Network operating system. Capture the screen shot' . (4 marks)

Upload "Question 22" document.

(Total: 20 marks)

23. Create a word document known as "Question 23" and use it to save your answers to questions (a) to (e).

Kerberos is the default authentication policy used by Network Operating system to authenticate computers and users on a network.

(a) Enable enforcement of user logon restrictions. Capture a screen shot. (4 marks)

(b) Set maximum lifetime for service ticket to 10hrs. Capture a screen shot. (4 marks)

(c) Set maximum lifetime for user ticket to 10hrs. Capture a screen shot. (4 marks)

(d) Set maximum lifetime for user renewal to 7 days. Capture a screen shot. (4 marks)

(e) Set maximum tolerance for computer clock synchronization 5 minutes. Capture a screen shot. (4 marks)

Upload "Question 23" document.

(Total: 20 marks)

....

DIPLOMA IN COMPUTER NETWORKS AND SYSTEMS ADMINSTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 5 December 2022. Afternoon Paper. **Time Allowed: 3 hours.**

Answer ALL questions. This paper has two sections. SECTION I has twenty (20) short response questions. Each question is allocated two (2) marks. SECTION II has three (3) practical questions of sixty (60) marks. Marks allocated to each question are shown at the end of the question.

Required Resources:

- Windows Server 2016/2019/2022 image
- Oracle Virtual box
- Linux/Windows computer

SECTION I (40 MARKS)

1. An institution has a policy in place to undertake a full backup every Sunday. Every other day of the week, staff members are required to back up only the changes since the last full backup. State the name of the backup type to be used for Thursday. (2 marks)

2. The installation feature in network operating system that provides a minimal environment for running specific server roles such as reduction of the maintenance and management requirements is known as: (2 marks)

3. What is name given to the network operating system tool intended to duplicate, test and deliver new installation based on an established installation? (2 marks)

4. A consortium that has been operational for a good number of years have requested you to setup 10 servers and 20 workstations. Windows deployment services are used whenever a new workstation is setup. Advise on the tool to be used to automate installation with little human interaction. (2 marks)

5. Group policy has been used to manage users and computers in Active Directory Domain Services (AD DS) running on network operating system. State what you would use to view the effect of applied group policy on individual computer. (2 marks)

6. A user account is an identity created for a person in a computer or computing system. You are required to grant a set of users permissions to a specific folder. State the group in which the user accounts should be placed. (2 marks)

7. A computer network for a Law firm contains Active Directory domain named lawfirm.com. The Active Directory Recycle bin is enabled for lawfirm.com. A support technician accidentally deletes a user account named learnedfriend1. You need to restore the learnedfriend1 account. Write down the appropriate tool that should be used. (2 marks)

8. State the command utility that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). (2 marks)

9. State the name given to a security feature in Network operating system to prevent unauthorised changes to the operating system. (2 marks)

10. Write down the protocol that uses an arbitrary authentication method, such as certificates, smart cards, or credentials on network operating system. (2 marks)

11. Which settings of a Network operating system (NOS) can be configured on a log file server for data collected to ensure the contents are automatically deleted when the file reaches 100MB in size? (2 marks)

12. An in-depth analysis on a network showed it contained a Hyper-V host named Server1 that hosts 20 virtual machines. You need to view the amount of memory resources and processor resources each virtual machine uses currently. Which tool can be used on the server to view the amount of memory and processor resources used by each of the virtual machine? (2 marks)

13. Which feature that is used to control the types of files users can save and generate notifications when users attempt to save unauthorised files in a network operating system? (2 marks)

14. State the tool that could be used to track all connections to shared resources on a Network operating system? (2 marks)

15. The policy setting which when enabled ensures file access, modification and deletion can be tracked in the event log is referred to as? (2 marks)

16. Indicate the tool in network operating system that can be used by administrators to examine the way system programs are running and their effect on performance. (2 marks)

17. The administrative tool which provides a view of all organisational units, domains and sites across an enterprise is called____________________. (2 marks)

18. Which command utility can be used to create Network Access Protection event to trace log files in client computer? (2 marks)

19. What is the name given to the tool used to mount a Network operating system image from Virtual Hard Disk (VHD) file? (2 marks)

20. State the name of the graphical user interface (GUI) tool with scope pane on left used to navigate Active Directory namespace. (2 marks)

SECTION II (60 MARKS)

INSTRUCTIONS

Install Oracle virtual box and Window server image to your computer and answer the following questions:

Required Resources:

- Windows server 2016/2019/2022 Image
- Oracle Virtual box
- Linux/Windows computer

Create a word processing document named “Task Manager” and use it to save your answers to questions (a) to (e).

21. Task manager, which is regarded as a system monitor is very common with the Network operating system. It assists in giving information about computer performance and running software.

Required:

Using task manager of your Network operating system:

(a) Capture a screenshot of statuses that are running and stopped**.** (**4 marks)

(b) Display the current CPU utilisation. (3 marks)

(c) Display the streams of instructions currently running. (3 marks)

(d) Click on the memory chart and display the following:

(i) Total physical memory (MB). (2 marks)

(ii) Total available memory. (2 marks)

(e) Click on the Ethernet chart and display the following:

(i) Link speed. (2 marks)

(ii) Network Connection. (2 marks)

(iii) IPv4 address in use. (2 marks)

Capture and save screenshots to show how you have performed the above task.

Upload "Task Manager" document.

(Total: 20 marks)

22. Create a word processing document named "Memory Usage" and use it to save your answers to questions (a) to (e) below:

With the help of task manager, perform the following:

(a) Click on Memory heading and state the effect exhibited on the columns. (4 marks)

(b) Display the memory usage to be in percentage values. (4 marks)

(c) State the way memory usage in Percent values could be useful to a system administrator (2 marks)

(d) Display list of the usernames which are logged into the system. (4 marks)

(e) Display the tabs that perform the following:

(i) List the processes that are started automatically. (2 marks)

(ii) Lists the historical resources usage (2 marks)

(iii) Displays process information such as process ID (PID), status, and memory utilisation. (2 marks)

Upload "Memory usage" document.

(Total: 20 marks)

23. Create a word processing document named "Virtual memory" and use it to save answers to questions (a) to (d) below:

Virtual memory is a common technique used in Network operating systems. It is used on both hardware and software to enable a computer compensate for physical memory shortages, temporarily transferring data from random access memory (RAM) to disk storage.

Required:

(a) List current size of the virtual memory (paging file) used by your network operating system. (4 marks)

(b) Display the Drive [Volume Label] that contains the paging file. (6 marks)

(c) Capture a screenshot to illustrate the way you can use Disk Management to create a second partition with at least 2GB. (6 marks)

(d) Capture a screenshot showing configuration of the virtual memory using the recommended file size in the Initial size (MB) field and file size in the Maximum size (MB) field. (4 marks)

Upload "Virtual memory" document.

(Total: 20 marks)

....

kasneb

DIPLOMA IN COMPUTER NETWORKS AND SYSTEM ADMINSTRATION (DCNSA)

LEVEL II

NETWORK OPERATING SYSTEMS

MONDAY: 1 August 2022. Afternoon paper. **Time Allowed: 3 hours.**

This paper has two sections. SECTION I has twenty (20) short response questions. SECTION II has three practical questions of sixty (60) marks. All questions are compulsory. Marks allocated to each question are shown at the end of the question.

SECTION I

1. A _______________ is a computer program or device that provides a service to another computer program and its user, also known as the client. (2 marks)

2. __________Manages the Virtual Machines and provides access to host computer resources . (2 marks)

3. What is the mode of operation where two or more processors in an operating system simultaneously process two or more different portions of the same program? (2 marks)

4. A collection of active directory objects such as users and computers are called a _____________? (2 marks)

5. __________comprises hardware and software, systems and devices, and it enables computing and communication between users, services, applications and processes. (2 marks)

6. A System Administrator was planning to deploy a Nano Server to function as a Hyper-V server for Finance network. Which parameter would you advise to include on the nano server image command line? (2 marks)

7. Virtualisation has become an important tool in network administration. Which advantage of Virtualisation is attributed to deployment of new virtual servers that can be accomplished in hours, rather than the days needed to approve, obtain, and install hardware for a new physical server? (2 marks)

8. ______________________enables administrators to manage permissions and access to network resources and stores data as objects. (2 marks)

9. _____________________is a collection of policy settings available to define the configuration or behavior of users or Computers**.** (2 marks)

10. Which of the role provided by a windows server is seen as an inhibiting use of IPV6 in networks? (2 marks)

11. Which command utility in command line interface (CLI) can be used to view computers IP address? (2 marks)

12. ____________________is a server computer that responds to security authentication requests such as logging within a Windows domain. (2 marks)

13. A server role is a set of software programs that, when they are installed and properly configured, lets a computer perform a specific function for multiple users or other computers within a network. What server role must be installed on a server in order for it to be considered a domain controller? (2 marks)

14. Windows____________ is setting the appearance of the desktop and apps make it look better and reflect your personal likes. (2 marks

15. Assuming you have been tasked by your immediate supervisor to create a new user account on Network operating system using the command prompt. Which command would you use? (2 marks)

16. You have recently been hired as administrator for a small pharmaceutical company with four servers. You have one file server named X that runs Windows Server 2016. You have a junior administrator who needs to do backups on this server. You need to ensure that the junior admin can use Windows Server Backup to create a complete backup of X. What should you configure to allow the junior admin to do the backups? (2 marks)

17. ____________is an Active Directory object that represents a replication connection from a source domain controller to a destination domain controller. (2 marks)

18. Which active directory service is responsible for establishing the replication topology and ensuring that all domain controllers are kept up-to-date? (2 marks)

19. ________________is a communication protocol that Microsoft created for providing shared access to files and printers across nodes on a network. (2 marks)

20. Which DOS command would you use to immediately restart a server whose graphical user interface has failed?

SECTION II

21. Windows Server is a group of operating systems that supports enterprise-level management, data storage, applications and communications.

Install oracle virtual box and Window server image to your Linux or windows computer and answer the following questions:

Required Resources

- Windows server 2016/2019/2022 Image
- Oracle Virtual box
- Linux/Windows computer

Create a word processing document named Question 21 and use it to save answers to questions (i) to (v).

(i) Capture a screenshot displaying server based operating system Dashboard (4 marks)

(ii) Capture a screenshot displaying local server properties (4 marks)

(iii) Display Routed Protocol configuration details (4 marks)

(iv) Capture a screenshot displaying add roles and features wizard (4 marks)

(v) Configure Role based installation (4 marks)

Upload Question 21.

(Total: 20 marks)

22. Create a word processor document named Question 22 and use it to save answers to questions (i) to (iv) below.

(i) Capture a screenshot displaying the active directory domain services window configuration. (6 marks)

(ii) Create user account objects of Active Directory Users using the correct snap-in console (4 marks)

(iii) Configure server domain name to be "togetherasone" (6 marks)

(iv) Capture a screenshot restricting logon of users at specific times and days. (4 marks)

Upload Question 22 document.

(Total: 20 marks)

23. Create a word processor document named Question 23 and use it to save answers to questions (i) to (iv) below. Set the following settings on windows server:

(i) Enforce password history to 5 times

(ii) Maximum password age 30 days

(iii) Minimum password length 5 characters

(iv) Password complexity requirements:

Disable the following settings:
- Contain at least one character, either uppercase (A a Z), lowercase (a - z)
- a numeric digit (0 to 9)
- non-alphabetic characters such as $% #).

Upload Question 23.

(Total: 20 marks)

…………………………………………………………………………