**Telecommunication and Network Security**

1. Which of the following media is MOST resistant to EMI interference?
   1. microwave
   2. fiber optic
   3. twisted pair
   4. coaxial cable
2. The basic function of a Failure Resistant Disk System (FRDS) is which of the following?
   1. protect file servers from data loss and a loss of availability due to disk failure.
   2. persistent file servers from data gain and a gain of availability due to disk failure.
   3. prudent file servers from data loss and a loss of acceptability due to disk failure.
   4. packet file servers from data loss and a loss of accountability due to disk failure.
3. A packet containing a long string of NOP's followed by a command is usually indicative of what?
   1. A syn scan
   2. A half-port scan
   3. A buffer overflow
   4. A packet destined for the network's broadcast address.
4. Which of the following LAN devices typically examines the entire packet?
   1. Routers
   2. Brouters
   3. Switches
   4. Gateways
5. The general philosophy for DMZ's is that:
   1. any system on the DMZ can be compromised because it's accessible from the Internet.
   2. any system on the DMZ cannot be compromized because it's not accessible from the Internet.
   3. some systems on the DMZ can be compromized because they are accessible from the Internet.
   4. any system on the DMZ cannot be compromized because it's by definition 100 percent safe and not accessible from the Internet.
6. In SSL/TLS protocol, what kind of authentication is supported?
   1. Peer-to-peer authentication
   2. Only server authentication (optional)
   3. Server authentication (mandatory) and client authentication (optional)
   4. Role based authentication scheme
7. Which one of the following is not a primary component or aspect of firewall systems?
   1. protocol filtering
   2. packet switching
   3. rule enforcement engine
   4. extended logging capability
8. Which of the following is used to find the Ethernet address that matches an Internet Protocol (IP) address?
   1. Address Resolution Protocol (ARP).
   2. Reverse Address Resolution Protocol (RARP).
   3. Internet Control Message protocol (ICMP).
   4. User Datagram Protocol (UDP).
9. Which of the following is an advantage of proxies?
   1. Proxies provide a single point of access, control, and logging.
   2. Proxies must exist for each service.
   3. Proxies create a single point of failure.
   4. Proxies do not protect the base operating system.
10. Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?
    1. TCP sequence number attack
    2. IP spoofing attack
    3. Piggybacking attack
    4. Teardrop attack
11. Application Level Firewalls can control which services are used by a workstation (FTP and so on), and it also aids in protecting the network from outsiders who may be trying to get information about the:
    1. network's design.
    2. user base.
    3. operating system design.
    4. net BIOS' design.
12. If an organization were to deploy only one Intrusion Detection System (IDS) sensor to protect its information system from the Internet:
    1. It should be host-based and installed on the most critical system in the DMZ, between the external router and the firewall.
    2. It should be network-based and installed in the DMZ, between the external router and the firewall.
    3. It should be network-based and installed between the firewall to the DMZ and the intranet.
    4. It should be host-based and installed between the external router and the Internet.
13. What are suitable protocols for securing e-mail?
    1. PGP and S/MIME
    2. IPsec and IKE
    3. TLS and SSL
    4. SSH

1. The two current conceptual approaches to Intrusion Detection methodology are knowledge-based ID systems and behavior-based ID systems, sometimes referred to as:
   1. signature-based ID and statistical anomaly-based ID, respectively.
   2. signature-based ID and dynamical anomaly-based ID, respectively.
   3. anomaly-based ID and statistical-based ID, respectively.
   4. signature-based ID and motion anomaly-based ID, respectively.
2. Which IPSec operational mode encrypts the entire data packet into an IPSec packet?
   1. Authentication mode
   2. Tunnel mode
   3. Transport mode
   4. Safe mode
3. Which of the following should never be allowed through a firewall?
   1. HTTP
   2. DNS
   3. IMAP
   4. NetBIOS
4. What is a packet sniffer?
   1. It tracks network connections to off-site locations.
   2. It monitors network traffic for illegal packets.
   3. It scans network segments for cabling faults.
   4. It captures network traffic for later analysis.
5. Several methods provide telecommunications continuity. Which of the following is a method of routing traffic through split cable or duplicate cable facilities?
   1. diverse routing
   2. alternative routing
   3. last mile circuit protection
   4. long haul network diversity
6. Encapsulating Security Payload (ESP) authentication capabilities are limited due to:
   1. Non-inclusion of IP header information in authentication process
   2. Because it is designed only for confidentiality
   3. Because ESP provide payload padding and this change authentication parameters
   4. Rule-based Access control
7. Which of the following media is MOST resistant to tapping?
   1. microwave
   2. twisted pair
   3. coaxial cable
   4. fiber optic
8. Hierarchical Storage Management (HSM) is commonly employed in:
   1. very large data retrieval systems.
   2. very small data retrieval systems.
   3. shorter data retrieval systems.
   4. most data retrieval systems.
9. RAID Level 15 is created by combining which of the following?
   1. level 1 (mirroring) with level 5 (interleave).
   2. level 0 (striping) with level 5 (interleave).
   3. level 2 (hamming) with level 5 (interleave).
   4. level 10 (striping and mirroring) with level 5 (interleave).
10. Which of the following layers does IPSec operate at?
    1. Session
    2. Transport
    3. Network
    4. Data Link
11. Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?
    1. User datagram protocol (UDP)
    2. Internet protocol (IP)
    3. Internetwork Packet Exchange (IPX)
    4. Internet control message protocol (ICMP)
12. Which of the following ISO/OSI layers does network address translation operate at?
    1. Transport layer
    2. Session layer
    3. Data link layer
    4. Network layer
13. Which of the following transmission media would NOT be affected by cross talk or interference?
    1. Coaxial cables
    2. Shielded twisted pairs (STP)
    3. Satellite radiolink systems
    4. Fiber optic cables
14. All following observations about IPSec are correct except:
    1. Default Hashing protocols are HMAC-MD5 or HMAC-SHA-1
    2. Default Encryption protocol is Cipher Block Chaining mode DES, but other algorithms like ECC (Elliptic curve cryptosystem) can be used
    3. Support two communication modes - Tunnel mode and Transport mode
    4. Works only with Secret Key Cryptography
15. What is the main difference between a Smurf and a Fraggle attack?
    1. A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.
    2. A Smurf attack is UDP-based and a Fraggle attack is TCP-based.
    3. Smurf attack packets cannot be spoofed.
    4. A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.
16. Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?
    1. File services.
    2. Mail services.
    3. Print services.
    4. Client/Server services.
17. Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?
    1. S-Telnet
    2. SSL
    3. Rlogin
    4. SSH
18. Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?
    1. Digital Video Tape (DVT).
    2. Digital Analog Tape (DAT).
    3. Digital Voice Tape (DVT).
    4. Digital Audio Tape (DAT).
19. CAT3 is an older specification with a:
    1. longer effective distance.
    2. shorter effective distance.
    3. longer effective strength.
    4. higher EMI protection.
20. Which of the following statements pertaining to RAID technologies is incorrect?
    1. RAID-5 has a higher performance in read/write speeds than the other levels.
    2. RAID-3 uses byte-level striping with dedicated parity .
    3. RAID-0 relies solely on striping.
    4. RAID-4 uses dedicated parity.
21. What is the greatest danger from DHCP?
    1. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
    2. Having multiple clients on the same LAN having the same IP address.
    3. Having the wrong router used as the default gateway.
    4. Having the organization's mail server unreachable.
22. Which of the following is not a basic security service defined by the OSI?
    1. Routing control
    2. Authentication
    3. Data confidentiality
    4. Logging and monitoring
23. Which of the following functions does RAID Level 0 perform?
    1. It creates one large disk by using several disks.
    2. It creates several smaller disks from one large disk.
    3. It recovers one large disk by using several smaller disks.
    4. It removes one large disk as it creates several smaller disks.
24. Which of the following is NOT an essential component of a VPN?
    1. VPN Server
    2. NAT Server
    3. authentication
    4. encryption
25. Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?
    1. Using a TACACS+ server.
    2. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
    3. Setting modem ring count to at least 5.
    4. Only attaching modems to non-networked hosts.
26. Which of the following statements pertaining to incident response is correct?
    1. As Computer Emergency Response Team (CERT) is copyrighted, Computer Incident Response Team (CIRT) is more often used.
    2. As Computer Incident Response Team (CIRT) is copyrighted, Computer Emergency Response Team (CERT) is more often used.
    3. Computer Incident Response Team (CIRT) and Computer Emergency Response Team (CERT) are used interchangeably.
    4. Computer Incident Management Team (CIMT) is sometimes used, but Computer Emergency Response Team (CERT) should be preferred.
27. What refers to legitimate users accessing networked services that would normally be restricted to them?
    1. Spoofing
    2. Piggybacking
    3. Eavesdropping
    4. Logon abuse
28. Both TCP and UDP use port numbers of what length?
    1. 32 bits
    2. 16 bits
    3. 8 bits
    4. 4 bits
29. A demilitarized zone is:
    1. an area in front of your firewall, accessible from the Internet
    2. an area behind your firewall, not accessible from the Internet
    3. a firewall
    4. an area behind your firewall, accessible from the Internet
30. Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provide following service except:
    1. Authentication
    2. Integrity
    3. Replay resistance and non-repudiations
    4. Confidentiality
31. Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps)?
    1. Category 5 UTP
    2. Category 2 UTP
    3. Category 3 UTP
    4. Category 8 UTP
32. ARP and RARP map between which of the following?
    1. DNS addresses and IP addresses
    2. 32-bit hardware addresses and 48-bit IPv6 addresses
    3. 32-bit hardware addresses and 48-bit IPv4 addresses
    4. 32-bit addresses in IPv4 and 48-bit hardware addresses
33. Which of the following networking devices allows the interconnection of two or more homogeneous LANs in a simple way?
    1. Gateways
    2. Routers
    3. Bridges
    4. Firewalls
34. Which of the following is true of Network-based ID systems?
    1. They commonly reside on a discrete network segment and monitor the traffic on that network segment.
    2. They commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
    3. They commonly reside on a discrete network segment but do not monitor the traffic on that network segment.
    4. They commonly do not reside on a discrete network segment and monitor the traffic on that network segment.
35. Which of the following methods of multiplexing data allocates bandwidth dynamically to channels having information to transmit?
    1. Time-division multiplexing
    2. Asynchronous time-division multiplexing
    3. Statistical multiplexing
    4. Frequency division multiplexing
36. Which of the following NAT firewall translation modes is required to make internal hosts available for connection from external hosts?
    1. Dynamic translation
    2. Load balancing translation
    3. Static translation
    4. Network redundancy translation
37. All except which of the follow are not used to ensure integrity?
    1. firewall services
    2. communications security management
    3. intrusion detection services
    4. compliance monitoring services
38. A server farm is an example of which of the following?
    1. Server clustering
    2. Redundant servers
    3. Multiple servers
    4. Server fault tolerance
39. Network security is a(n):
    1. Product
    2. protocols
    3. ever evolving process
    4. quick-fix solution
40. Which of the following protocols operates at the session layer (layer 5)?
    1. RPC
    2. IGMP
    3. LPD
    4. SPX
41. Which of the following is the most secure firewall implementation?
    1. Dual-homed host firewalls
    2. Screened-subnet firewalls
    3. Screened-host firewalls
    4. Packet-filtering firewalls
42. Which layer of the TCP/IP protocol model controls the communication flow between hosts?
    1. Internet layer
    2. Host-to-host transport layer
    3. Application layer
    4. Network access layer

1. Which of the following is a disadvantage of a behavior-based ID system?
   1. The activity and behavior of the users while in the networked system may not be static enough to effectively implement a behavior-based ID system.
   2. The activity and behavior of the users while in the networked system may be dynamic enough to effectively implement a behavior-based ID system.
   3. The activity and behavior of the users while in the networked system may not be dynamic enough to effectively implement a behavior-based ID system.
   4. The system is characterized by high false negative rates where intrusions are missed.
2. Which protocol matches an Internet Protocol (IP) address to a known Ethernet address?
   1. Address Resolution Protocol (ARP).
   2. Reverse Address Resolution Protocol (RARP).
   3. Internet Control Message protocol (ICMP).
   4. User Datagram Protocol (UDP).
3. Which of the following services relies on UDP?
   1. FTP
   2. Telnet
   3. DNS
   4. SMTP
4. These techniques to prevent, detect, and correct errors so that integrity, availability, and the confidentiality of transactions over networks may be maintained by:
   1. Information security
   2. Networks security
   3. Client security
   4. Communications security
5. Which of the following protects Kerberos against replay attacks?
   1. Tokens
   2. Passwords
   3. Cryptography
   4. Time stamps
6. Intrusion detection has which of the following sets of characteristics?
   1. It is adaptive rather than preventative.
   2. It is administrative rather than preventative.
   3. It is disruptive rather than preventative.
   4. It is detective rather than preventative.
7. Which of the following is based on the learned patterns with an alarm is triggered when an activity is considered intrusive?
   1. behavior-based ID systems
   2. network-based ID systems.
   3. host-based ID systems.
   4. knowledge-based ID systems.
8. Which of the following Common Data Network Services is used to share data files and subdirectories on file servers?
   1. File services.
   2. Mail services.
   3. Print services.
   4. Client/Server services.
9. Which of the following protocols does not operate at the data link layer (layer 2)?
   1. PPP
   2. RARP
   3. L2F
   4. ICMP
10. Which of the following offers confidentiality to an e-mail message?
    1. The sender encrypting it with its private key.
    2. The sender encrypting it with its public key.
    3. The sender encrypting it with the receiver's public key.
    4. The sender encrypting it with the receiver's private key.
11. Which of the following layers provides end-to-end service?
    1. Network Layer
    2. Link Layer
    3. Transport Layer
    4. Presentation Layer
12. Which of the following is not addressed by backups?
    1. Availability
    2. Recovery
    3. Integrity
    4. Confidentiality
13. Which of the following statements pertaining to packet filtering is incorrect?
    1. It is based on ACLs.
    2. It is not application dependant.
    3. It operates at the network layer.
    4. It keeps track of the state of a connection.
14. Which layer of the TCP/IP protocol model ensures error-free delivery and packet sequencing?
    1. Internet layer
    2. Network access layer
    3. Host-to-host transport layer
    4. Application layer
15. Secure Sockets Layer (SSL) provides security services at which layer of the OSI model?
    1. Network Layer
    2. Transport Layer
    3. Session Layer
    4. Application Layer
16. Which OSI/ISO layer establishes a logical connection between the sending host and destination host on a network?
    1. Session layer
    2. Transport layer
    3. Network layer
    4. Data link layer
17. Which of the following is a common LAN media access method?
    1. CSMA/CD
    2. Ethernet
    3. Mesh
    4. UTP
18. Which backup method only copies files that have been recently added or changed?
    1. Full backup method
    2. Incremental backup method
    3. Fast backup method
    4. Differential backup method
19. Which OSI/ISO layer best handles congestion control?
    1. Physical layer
    2. Data link layer
    3. Transport layer
    4. Network layer
20. Which of the following is a LAN transmission protocol?
    1. Ethernet
    2. Ring topology
    3. Unicast
    4. Polling
21. Which of the following statements pertaining to firewalls is incorrect?
    1. Firewalls create bottlenecks between the internal and external network.
    2. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
    3. Strong firewalls can protect a network at all layers of the OSI models.
    4. Firewalls are used to create security checkpoints at the boundaries of private networks.
22. Which of the following are not Remote User Management issues?
    1. Justification for and the validation of the use of remote computing systems
    2. Hardware and software distribution
    3. User support and remote assistance issues
    4. Access badges
23. All hosts on an IP network have a logical ID called a(n):
    1. IP address.
    2. MAC address.
    3. TCP address.
    4. Datagram address.
24. A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:
    1. server cluster.
    2. client cluster.
    3. guest cluster.
    4. host cluster.
25. Which of the following statements pertaining to disk mirroring is incorrect?
    1. Mirroring offers better performance in read operations but writing hinders system performance.
    2. Mirroring is a hardware-based solution.
    3. Mirroring offers a higher fault tolerance than parity.
    4. Mirroring is not usually a cost-effective solution.
26. Which common backup method is the fastest on a daily basis?
    1. Full backup method
    2. Incremental backup method
    3. Fast backup method
    4. Differential backup method
27. Which of the following is an advantage that UDP has over TCP?
    1. UDP is connection-oriented whereas TCP is not.
    2. UDP is more reliable than TCP.
    3. UDP is faster than TCP.
    4. UDP makes a better effort to deliver packets.
28. Which of the following OSI layers provides non-repudiation services?
    1. presentation
    2. application
    3. transport
    4. data link
29. Which of the following is unlike the other three?
    1. El Gamal
    2. Teardrop
    3. Buffer Overflow
    4. Smurf
30. Which of the following takes the concept of RAID 1 (mirroring) and applies it to a pair of servers?
    1. A redundant server implementation
    2. A redundant client implementation
    3. A redundant guest implementation
    4. A redundant host implementation
31. Which of the following elements of telecommunications are not used to ensure confidentiality?
    1. Network security protocols
    2. Network authentication services
    3. Data encryption services
    4. Passwords
32. In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
    1. Both client and server
    2. The client's browser
    3. The web server
    4. The merchant's Certificate Server
33. Secure Sockets Layer (SSL) is a socket layer security protocol and is a two-layered protocol that contains the SSL Record Protocol and the:
    1. Secure Sockets Layer (SSL) Internet Protocol.
    2. Secure Sockets Layer (SSL) Data Protocol.
    3. Secure Sockets Layer (SSL) Link Protocol.
    4. Secure Sockets Layer (SSL) Handshake Protocol.
34. The DMZ does not normally contain:
    1. encryption server
    2. web server
    3. external DNS server
    4. mail relay
35. Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for private connections and asymmetric or public key cryptography for:
    1. peer authentication.
    2. peer identification.
    3. server authentication.
    4. name resolution.
36. How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?
    1. 6 bits
    2. 12 bits
    3. 16 bits
    4. 24 bits
37. A demilitarized zone is:
    1. a part of a network perfectly safe from hackers
    2. a militarized network segment
    3. a firewall
    4. a network segment off the firewall for systems that require different levels of access than other network components
38. What type of attack involves IP spoofing, ICMP ECHO and a bounce site?
    1. IP spoofing attack
    2. Teardrop attack
    3. SYN attack
    4. Smurf attack
39. What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?
    1. SYN Flood attack
    2. Smurf attack
    3. Ping of Death attack
    4. Denial of Service (DOS) attack
40. Network-based ID systems:
    1. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
    2. Commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
    3. Commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
    4. Commonly does not reside on a discrete network segment and monitor the traffic on that network segment.
41. Which of the following is most affected by denial-of-service (DOS) attacks?
    1. Confidentiality
    2. Integrity
    3. Accountability
    4. Availability
42. In stateful inspection firewalls, packets are queued and then:
    1. accessed at only one Open Systems Interconnect (OSI) layer.
    2. analyzed at all Open Systems Interconnect (OSI) layers.
    3. decapsulated at all Open Systems Interconnect (OSI) layers.
    4. encapsulated at all Open Systems Interconnect (OSI) layers.
43. Address Resolution Protocol (ARP) interrogates the network by sending out a?
    1. broadcast.
    2. multicast.
    3. unicast.
    4. semicast.
44. Which of the following statements pertaining to IPSec is incorrect?
    1. A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
    2. Integrity and authentication for IP datagrams are provided by AH.
    3. ESP provides for integrity, authentication and encryption to IP datagrams.
    4. In transport mode, ESP only encrypts the data payload of each packet.
45. Which of the following is the biggest concern with wireless technologies?
    1. Availability
    2. Confidentiality
    3. Reliability
    4. Integrity