Domain 4 Questions

1. Routers chat among themselves in order to learn about networks not directly connected to them. This information is stored in routing tables and is used by the _____.

- [ ] a. Data Link Layer
- [ ] b. Network Layer
- [ ] c. Transport Layer
- [ ] d. Session Layer

2. Which of these is NOT a feature of MPLS (Multi Protocol Label Switching)?

- [ ] a. Traffic engineering
- [ ] b. Better route performance
- [ ] c. Built-in encryption
- [ ] d. Built-in tunneling

3. Which of the following wireless solutions is BEST used for small group networking?

- [ ] a. WiMax
- [ ] b. Bluetooth
- [ ] c. Cellular
- [ ] d. Wireless LAN

4. What is the difference between an amplifier and a repeater?

- [ ] a. None, they are one and the same
- [ ] b. An amplifier boosts noise and signal, a repeater just boosts signal
- [ ] c. An amplifier boosts noise and signal, a repeater makes a new original signal
- [ ] d. An amplifier allows for longer cable runs without the need for a repeater

5. Which of these is NOT part of the RFC 1918 private address pool?

- [ ] a. 10.0.0.0 to 10.255.255.255
- [ ] b. 169.254.0.0 to 169.254.255.255
- [ ] c. 172.16.0.0 to 172.31.255.255
- [ ] d. 192.168.0.0 to 192.168.255.255

6. A branch office and its headquarters both use addresses from the RFC 1918 pools. In order to set up an IPSec link between them, they would need to use _____.

- [ ] a. Tunnel mode IPSec
- [ ] b. IPSec with NAT
- [ ] c. Transport mode IPSec
- [ ] d. Natural mode IPSec

7. Wireless 802.11 LANs primarily use _____.

- [ ] a. Polling
- [ ] b. CSMA/CD
- [ ] c. CSMA/CA
- [ ] d. Deterministic Token Passing Rings

8. When comparing cable modems to DSL service for the home user, which of the following is the GREATEST benefit of cable modems?

- [ ] a. Higher data rates than DSL
- [ ] b. "Always on" encryption
- [ ] c. Greater availability than DSL
- [ ] d. Lower cost than DSL

9. SDN (Software Defined Networking) has three layers. Which of these is NOT one of them?

- [ ] a. Application
- [ ] b. Control
- [ ] c. Communications
- [ ] d. Infrastructure

10. A PVLAN is a Private VLAN. There are three types of nodes in PVLANs. Which of these is NOT one of them?

- [ ] a. Promiscuous: can talk to any node in the VLAN
- [ ] b. Isolated: can only talk to a promiscuous node
- [ ] c. Community: can talk to others in the community and any promiscuous node
- [ ] d. Controlled: can talk to others on an approved list and any promiscuous node

11. Enumeration is also known as _____

- [ ] a. exploiting known weaknesses in an organization's system
- [ ] b. finding all of an organization's systems that are up and running
- [ ] c. determining the open ports on systems that are up and running
- [ ] d. running vulnerability scans on specific ports on organizational systems

12. Which of these attacks is LEAST likely to be effective on modern network devices?

- [ ] a. SYN flood
- [ ] b. IP address spoofing
- [ ] c. Ping of Death
- [ ] d. Smurf attack

13. What is the difference between an incident and an event?

- ☐ a. No difference, they are the same.
- ☐ b. An event is something that can be measured, an incident is an event that can cause harm.
- ☐ c. An incident is something that can be measured, and event is an incident that can cause harm.
- ☐ d. An event will trigger an investigation, an incident will trigger litigation.

14. Which of the following are the correct names for the Open Systems Interconnection (OSI) model layers 1, 6, 7, and 3?

- ☐ a. Physical, application, presentation, and network
- ☐ b. Data link, network, application, and session
- ☐ c. Physical, data link, network, and application
- ☐ d. Physical, presentation, application, and network

15. Which of the following provides the best and most scalable access control for a corporate wireless network?

- ☐ a. A Stateful firewall that also does Network Address Translation (NAT).
- ☐ b. WPA2 Enterprise with IEEE 802.1x.
- ☐ c. WPA2 Personal with long pre-shared keys
- ☐ d. A carefully monitored MAC filtering plan.

16. Which statement BEST describes the functions of the data link layer (DLL) and the presentation layer (PL)?

- ☐ a. The DLL provides media access control and transmits signals as frames, the PL handles formatting.
- ☐ b. The DLL converts port numbers into signals, the PL handles data formatting.
- ☐ c. The DLL provides framing, the PL converts bits into signals.
- ☐ d. The DLL converts a network packet into signals, the PL converts an application packet into a datagram.

17. Which PKI component publishes the Certificate Revocation List (CRL)?

- ☐ a. The Central Directory (CD)
- ☐ b. The Registration Authority (RA)
- ☐ c. The Certificate Authority (CA)
- ☐ d. The Certificate Manager (CM)

18. Wired Equivalent Privacy's (WEP's) successor that did not require change in hardware was called _____, and used what technology?

- ☐ a. Wi-Fi Protected Access II (WPA2), and it used the Advanced Encryption Standard (AES).
- ☐ b. Wi-Fi Protected Access II (WPA2), and it used the Temporal Key Integrity Protocol (TKIP).
- ☐ c. Wi-Fi Protected Access (WPA), and it used the Temporal Key Integrity Protocol (TKIP).
- ☐ d. Wi-Fi Protected Access (WPA), and it used the Advanced Encryption Standard (AES).

19. If you used a system that included Network Intrusion Detection (NIDS), Host Intrusion Detection (HIDS), and Host Intrusion Preventions (HIPS) capabilities, which of the following would be the MOST difficult to successfully monitor?

- ☐ a. Web server traffic using the HIDS on the Web Server.
- ☐ b. Database server traffic using the HIPS on the database server.
- ☐ c. Incoming e-commerce traffic using the NIDS on the corporate DMZ.
- ☐ d. Outgoing Telnet and FTP traffic using the NIDS within the DMZ.

20. What is the MAIN security advantage of installing website control filters to block sites such as Facebook, or fantasy sports sites?

- ☐ a. Making your employees more productive since they are not wasting time on the blocked social networking sites.
- ☐ b. Deterring employees from betting on sports events.
- ☐ c. Stopping leakage of personal information.
- ☐ d. Avoiding malware.

21. Your company has a border router/firewall to connect its network to the Internet. It also has a 64-port switch to connect all your internal users and printers. To isolate your general users from seeing the normal, but sensitive, traffic among the Human Resources (HR) employees, you placed the HR employees into a separate VLAN. What risks remain with the use of the VLAN?

- ☐ a. None, the data is encrypted.
- ☐ b. None, the data being communicated is air gapped.
- ☐ c. The HR data might be exposed through VLAN leaking.
- ☐ d. The HR data might be exposed through a denial of service

22. To contain an ongoing incident where your E-mail server is being attacked, which answer is BEST?

- ☐ a. Disconnect the E-mail server from the network.
- ☐ b. Use network segmentation to isolate the E-mail server.
- ☐ c. Put new and tighter E-mail filtering rules into your firewall.
- ☐ d. Put more specific E-mail rules into your border router.

23. A hacker sniffs network traffic and then uses an IP address and TCP header information to insert packets into the network. This type of attack is usually called

- ☐ a. IP Spoofing
- ☐ b. Session hijacking
- ☐ c. Fraggle
- ☐ d. Smurf

24. If you found a rogue Certificate Authority (CA) among the list of CAs in your Public Key Infrastructure (PKI) cache, your browser would:

- ☐ a. Not trust any of the certificates the rogue CA has signed.
- ☐ b. Always prompt you to reject it, as the rogue CA's certificate is in your browser's cache.
- ☐ c. Always trust any certificate the rogue CA had previously signed.
- ☐ d. Not cause any harm, as rogue CAs aren't as effective.

25. A malicious software attack that frequently requires human action to introduce and attaches itself to another program to facilitate replication and distribution is called a _____.

- ☐ a. Vishing attack
- ☐ b. Worm attack
- ☐ c. A logic bomb attack
- ☐ d. A virus attack

26. Which attack uses options in the "ping" command to create a denial-of-service attack?

- ☐ a. An overlapping fragment attack
- ☐ b. The Fraggle attack
- ☐ c. The Smurf attack
- ☐ d. The Double Teardrop attack

27. The process that enables two Root Certificate Authorities (CAs) to allow users within the PKI to use trust certificates generated by the other CA is called

- ☐ a. Subordinate CA to Subordinate CA Trust
- ☐ b. Cross-certification
- ☐ c. RA to RA Cooperation
- ☐ d. Certificate Authority Reciprocity

28. Which list contains one IP Networking port number in the “Well known” range, one in the “Registered” range, and one in the “Dynamic” range?

- ☐ a. 69 1007 and 50001
- ☐ b. 1443 8080 and 49152
- ☐ c. 23 80 and 1443
- ☐ d. 809 1812 and 53652

29. What application layer device provides translation services for different environments?

- ☐ a. A Voice over IP (VoIP) to Plain Old Telephone Service (POTS) gateway
- ☐ b. An Ethernet to Token Ring bridge
- ☐ c. An ASCII to EBCDIC gateway
- ☐ d. A Router connecting two different LAN segments

30. Which statement below BEST describes the purpose of a Software Defined Network?

- ☐ a. It is used to separate traditional network traffic into three components: raw data, the way in which the data are sent, and the purpose the data server.
- ☐ b. It is used to provide redundancy in cloud environments.
- ☐ c. It abstracts network traffic into three layers which are called Application, Communications, and Interface
- ☐ d. It creatively uses TCP/IP networking standards to move data over different paths.

31. Which statement BEST describes the differences among different network cabling media?

- ☐ a. Coaxial cable has more environmental protection that Shielded Twisted Pair (STP), but is harder to install.
- ☐ b. Twisted pair copper cabling comes in two modes, Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).
- ☐ c. Fiber Optic cabling comes in two modes, single mode and multi-mode.
- ☐ d. Shielded Twisted Pair (STP) is more expensive than coaxial cable, but it is easier to install than Fiber Optic.

32. Which of the following uses the User Datagram Protocol (UDP) to create a denial-of-service attack?

- ☐ a. A session hijacking attack
- ☐ b. The Double Teardrop attack
- ☐ c. The Fraggle attack
- ☐ d. The Smurf attack

33. The IPSEC protocol can be used as a _____.

- ☐ a. A protocol used by virtual private networks (VPNs) that can both tunnel and encrypt.
- ☐ b. A protocol used by Local Area Networks (LANs) that can both tunnel and encrypt.
- ☐ c. A local area network (LAN) protocol that can encrypt but not tunnel.
- ☐ d. A virtual private network (VPN) protocol that can only tunnel.

34. What would be the BEST tool to deal with a distributed port scan?

- ☐ a. Penetration test
- ☐ b. Event log
- ☐ c. Network Intrusion Detection System (NIDS)
- ☐ d. Host Intrusion Detection System (HIDS)

35. An attacker is sending ICMP echo_request messages into the network. The destination address is directed broadcast and the source is actually the address of the victim. What type of attack is the hacker doing?

- ☐ a. Fraggle
- ☐ b. Smurf
- ☐ c. Teardrop
- ☐ d. Land

36. In a very large organization where the user population is dynamic and static passwords are undesirable, which method of authentication would be desirable?

- ☐ a. Challenge Handshake Authentication Protocol (CHAP)
- ☐ b. Password Authentication Protocol (PAP)
- ☐ c. Lightweight directory access protocol (Ldap)
- ☐ d. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

37. All of the following activities are examples of active attacks EXCEPT which one?

- ☐ a. Sending a packet into the network with a spoofed source address
- ☐ b. Using a network analyzer to intercept and read FTP data
- ☐ c. ARP cache poisoning
- ☐ d. RIP route poisoning

38. Max and Lola need to communicate confidentially and are the only two trusted entities on the network. Which layer is LEAST suitable when end to end communication is needed?

- ☐ a. Data Link
- ☐ b. Network
- ☐ c. Transport
- ☐ d. Application

39. Which one of the following network technologies would be best suited to operate in an error-prone environment?

- ☐ a. Frame Relay
- ☐ b. Asynchronous Transfer Mode
- ☐ c. X.25
- ☐ d. Ethernet

40. Spoofing can be defined as:

- ☐ a. Listening to a conversation between people or systems to obtain information.
- ☐ b. A person or a process pretending to be a person or a process in order to obtain access to the system.
- ☐ c. A hostile or unexpected entity concealed within another entity.
- ☐ d. The testing of all possibilities to obtain information.

41. When deploying a network in an environment that is heavily populated with Radio Frequency (RF) energy, which transmission media would offer the highest level of protection?

- ☐ a. Unshielded Twisted Pair (UTP)
- ☐ b. Shielded Twisted Pair (STP)
- ☐ c. Microwave
- ☐ d. Single mode fiber optics

42. Which of the following is a list of active attacks against Wireless Local Area Networks (WLANs)?

- ☐ a. Authentication, Authorization, and Availability
- ☐ b. Authentication, Availability, and Access Control
- ☐ c. Authentication, Authorization, and Accountability
- ☐ d. Authentication, Authorization, and Access Control

44. Monitoring and capturing wireless signals may provide a hacker with what significant advantage?

- ☐ a. Defeat the TEMPEST safeguards
- ☐ b. Bypass the security built into applications
- ☐ c. Gather system information or data without physically trespassing
- ☐ d. Undetectable active monitoring of the network traffic

45. Why are local area networks more vulnerable to data compromise than mainframe computers?

- ☐ a. Transmission capacity
- ☐ b. Storage capacity
- ☐ c. Multiple points of access
- ☐ d. Removable media

46. What would you find in an ARP cache?

- ☐ a. History of sites visited by a user
- ☐ b. Configuration tables for a firewall
- ☐ c. Domain registry information
- ☐ d. Cross-reference of IP and MAC addresses

47. Poisoning the Domain Name Server (DNS) may result in:

- ☐ a. A user’s IP address being deleted
- ☐ b. A user unable to reach an organization via its IP address
- ☐ c. A user being routed to the wrong organization’s server
- ☐ d. A user being denied access to a remote server

48. Which VPN is LEAST suitable for an employee remote connection from a customer site to the company?

- ☐ a. IP Security (IPSec)
- ☐ b. Layer Two Transport Protocol (L2TP)
- ☐ c. Transport Layer Security (TLS)
- ☐ d. Secure Socket Layer (SSL)

49. In which of the following situations is the principal security risk of broadband Internet access proliferation for home users?

- ☐ a. Users using peer-to-peer file sharing networks for breaches of intellectual property.
- ☐ b. PCs connected permanently to the Internet are prone to receive more spam mails, thereby increasing the risk for the user to become infected with viruses and Trojans
- ☐ c. PCs will become infected with dialers on DSL lines (run over telephone lines), thereby exposing the user to almost limitless financial risk.
- ☐ d. Home computers that are not securely configured or maintained and are permanently connected to the Internet become easy prey for attackers.

50. Why is traffic across a packet switched network (e.g. frame relay, X.25) difficult to monitor?

- ☐ a. Packets are link encrypted to the carrier
- ☐ b. Government regulations forbid monitoring
- ☐ c. Packets are transmitted on multiple paths
- ☐ d. The network factor is too high

51. Which of the following is a reasonable response from a network-based intrusion detection system when it detects Internet Protocol (IP) packets where the IP source is the same as the IP destination address?

- ☐ a. The Intrusion Detection System (IDS) will record the event.
- ☐ b. The IDS will reset the TCP connection.
- ☐ c. The IDS will correct the destination address and process the packet.
- ☐ d. The IDS will work with the NAT device to translate the source address and forward the packet.

52. Attenuation is described as:

- ☐ a. Line noise that is superimposed on the supply circuit can cause a fluctuation of power.
- ☐ b. Disruptions on a line cause by things like fluorescent lighting.
- ☐ c. Electromagnetic interference caused by motors, lightning, etc.
- ☐ d. The loss of signal strength as it travels.

53. What purpose does Encapsulating Security Payload (ESP) serve in the IPSec Architecture for Internet Protocol layer?

- ☐ a. To provide non-repudiation and confidentiality of transmissions.
- ☐ b. To provide integrity and confidentiality for IP transmissions.
- ☐ c. To provide integrity and authentication for IP transmissions.
- ☐ d. To provide integrity and authentication for IP transmissions.