|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. TCP/IP uses its own four-layer architecture that includes the Network Interface, Internet, Transport, and Application layers.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. The most popular implementation of DNS is the Unix Internet Name Domain.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Trivial File Transfer Protocol (TFTP) uses a more memory when compared to FTP.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. SNMP-managed devices must have an agent or a service that listens for commands and then executes them.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. S/MIME can be used when mail is accessed through a web browser.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. A DDoS mitigator is a software device that identifies and blocks real-time distributed denial of service (DDoS) attacks.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. A correlation engine aggregates and correlates content from different sources to uncover an attack.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Type I hypervisors run on the host operating system.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. A private cloud is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. File integrity check (FIC) is a service that can monitor any changes made to computer files, such as operating system files.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What protocol suite below is the most commonly used protocol for local area network (LAN) communication?   |  |  |  | | --- | --- | --- | |  | a. | UDP | |  | b. | IPX/SPX | |  | c. | TCP/IP | |  | d. | Appletalk |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. At what level of the OSI model does the IP protocol function?   |  |  |  | | --- | --- | --- | |  | a. | Transport Layer | |  | b. | Network Layer | |  | c. | Data link Layer | |  | d. | Presentation Layer |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. Which layer of the OSI model contains the TCP protocol, which is used for establishing connections and reliable data transport between devices?   |  |  |  | | --- | --- | --- | |  | a. | Application Layer | |  | b. | Presentation Layer | |  | c. | Network Layer | |  | d. | Transport Layer |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. When using SNMPv1 or SNMPv2, what piece of information is needed to view information from an agent?   |  |  |  | | --- | --- | --- | |  | a. | entity | |  | b. | community string | |  | c. | MIB | |  | d. | OID |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Select the TCP/IP protocol that resolves a symbolic name to its corresponding IP address using a database consisting of an organized hierarchy tree.   |  |  |  | | --- | --- | --- | |  | a. | WINS | |  | b. | NIS | |  | c. | TACACS+ | |  | d. | DNS |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. DNS poisoning can be prevented using the latest edition of what software below?   |  |  |  | | --- | --- | --- | |  | a. | BIND | |  | b. | DHCP | |  | c. | WINS | |  | d. | finger |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. An administrator needs to examine FTP commands that are being passed to a server. What port should the administrator be monitoring?   |  |  |  | | --- | --- | --- | |  | a. | 19 | |  | b. | 20 | |  | c. | 21 | |  | d. | 22 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. What device operates at the Network Layer (layer 3) of the OSI model and forwards packets across computer networks?   |  |  |  | | --- | --- | --- | |  | a. | bridge | |  | b. | router | |  | c. | switch | |  | d. | hub |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. How can a network of physical devices be grouped into logical units, regardless of what network switches they may be connected to?   |  |  |  | | --- | --- | --- | |  | a. | VLAN | |  | b. | subnets | |  | c. | IP address | |  | d. | MAC address |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. When setting up a server virtualization environment, what component below manages the virtual machine operating systems and supports one or more guest systems?   |  |  |  | | --- | --- | --- | |  | a. | kernel | |  | b. | supervisor | |  | c. | hypercard | |  | d. | hypervisor |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Which Cloud computing service model uses the cloud computing vendor to provide access to the vendor's software applications running on a cloud infrastructure?   |  |  |  | | --- | --- | --- | |  | a. | Application as a Service | |  | b. | Infrastructure as a Service | |  | c. | Software as a Service | |  | d. | System as a Service |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. In what type of cloud computing does the customer have some control over the operating systems, storage, and their installed applications?   |  |  |  | | --- | --- | --- | |  | a. | Application as a Service | |  | b. | Infrastructure as a Service | |  | c. | Software as a Service | |  | d. | System as a Service |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Which of the following protocols is used to manage network equipment and is supported by most network equipment manufacturers?   |  |  |  | | --- | --- | --- | |  | a. | TCP/IP | |  | b. | FTP | |  | c. | SNMP | |  | d. | SRTP |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. Which of the following protocols is unsecured?   |  |  |  | | --- | --- | --- | |  | a. | HTTPS | |  | b. | TLS | |  | c. | SSL | |  | d. | FTP |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Select the email protocols that are not secure? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | TLS | |  | b. | S/MIME | |  | c. | POP | |  | d. | IMAP |  |  |  | | --- | --- | | *ANSWER:* | c, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What secure protocol is recommended for time synchronization?   |  |  |  | | --- | --- | --- | |  | a. | SRTP | |  | b. | S/MIME | |  | c. | NTP | |  | d. | POP |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. What secure protocol is recommended for voice and video?   |  |  |  | | --- | --- | --- | |  | a. | SRTP | |  | b. | S/MIME | |  | c. | IMAP | |  | d. | IPsec |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What hardware component can be inserted into a web server that contains one or more co-processors to handle SSL/TLS processing?   |  |  |  | | --- | --- | --- | |  | a. | SSL/TLS tap | |  | b. | SSL/TLS accelerator | |  | c. | SSL/TLS access point | |  | d. | SSL/TLS mirror |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. If a network administrator needs to configure a switch to copy traffic that occurs on some or all ports to a designated monitoring port on the switch, what switch technology will need to be supported?   |  |  |  | | --- | --- | --- | |  | a. | interface capture | |  | b. | port identity | |  | c. | port snooping | |  | d. | port mirroring |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What hardware device can be inserted into a network to allow an administrator to monitor traffic?   |  |  |  | | --- | --- | --- | |  | a. | network tap | |  | b. | network mirror | |  | c. | shark box | |  | d. | shark tap |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What type of switch is used to combine multiple network connections into a single link?   |  |  |  | | --- | --- | --- | |  | a. | core switch | |  | b. | gateway switch | |  | c. | aggregation switch | |  | d. | access switch |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Select the security tool that is an inventory of applications and associated components that have been pre-approved and authorized to be active and present on the device?   |  |  |  | | --- | --- | --- | |  | a. | malware management | |  | b. | inventory permissions | |  | c. | application whitelist | |  | d. | application control |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What secure protocol is recommended for Network address translation?   |  |  |  | | --- | --- | --- | |  | a. | SRTP | |  | b. | S/MIME | |  | c. | IMAP | |  | d. | IPsec |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What specific issues are associated with log management? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | The multiple devices generating logs. | |  | b. | The different log formats. | |  | c. | The fast network transfer speeds. | |  | d. | The large volume of data that needs to be logged |  |  |  | | --- | --- | | *ANSWER:* | a, b, c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of system is designed to collect and consolidate logs from multiple sources for easy analysis?   |  |  |  | | --- | --- | --- | |  | a. | centralized device log analyzer | |  | b. | core device log analyzer | |  | c. | network log device | |  | d. | system log manager |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which technology is a means of managing and presenting computer resources by function without regard to their physical layout or location?   |  |  |  | | --- | --- | --- | |  | a. | IaaS | |  | b. | cloud computing | |  | c. | virtualization | |  | d. | PaaS |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. What type of computing environment allows servers, storage, and the supporting networking infrastructure to be shared by multiple enterprises over a remote network connection that had been contracted for a specific period?   |  |  |  | | --- | --- | --- | |  | a. | virtual services | |  | b. | hosted services | |  | c. | cloud services | |  | d. | volume computing |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following is the process of running a user desktop inside a virtual machine that resides on a server?   |  |  |  | | --- | --- | --- | |  | a. | PaaS | |  | b. | SDN | |  | c. | VDI | |  | d. | SaaS |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. What are the planes used to allow SDN to virtualize parts of the physical network so that it can be more quickly and easily reconfigured? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | data plane | |  | b. | management plane | |  | c. | control plane | |  | d. | data plane |  |  |  | | --- | --- | | *ANSWER:* | a, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. On and SDN network, what specific unit gives traffic the permission to flow through the network?   |  |  |  | | --- | --- | --- | |  | a. | SDN router | |  | b. | SDN firewall | |  | c. | SDN gateway | |  | d. | SDN controller |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |
| --- | --- | --- |
| 41. What are the two types of community strings?   |  |  | | --- | --- | | *ANSWER:* | There are two types of community strings: a read-only string will allow information from the agent to be viewed, and a read-write string allows settings on the device to be changed. | |

|  |  |  |
| --- | --- | --- |
| 42. Why is the Physical Layer omitted in the TCP/IP model?   |  |  | | --- | --- | | *ANSWER:* | The Physical Layer is omitted in the TCP/IP model because TCP/IP views the Network Interface Layer as the point where the connection between the TCP/IP protocol and the networking hardware occurs. | |

|  |  |  |
| --- | --- | --- |
| 43. Discuss the problems associated with storing the entire database of names and IP addresses in one location.   |  |  | | --- | --- | | *ANSWER:* | First, it would cause a bottleneck and slow down the Internet for all users trying to access one copy of the database. Second, if something happened to this one database, then the entire Internet would be affected. Instead of being on only one server, the DNS database is divided and distributed to many different servers on the Internet, each of which is responsible for different areas of the Internet. | |

|  |  |  |
| --- | --- | --- |
| 44. List the steps of a DNS lookup.   |  |  | | --- | --- | | *ANSWER:* | Step 1. The request for the IP address of the site www.nashville.com goes from the user's computer to the local DNS server that is part of the LAN to which it is connected. Step 2. The local DNS server does not know the IP address of www.nashville.com yet it does know the IP address of a DNS server that contains the top-level domains and their IP numbers. A request is sent to this top-level domain DNS server. Step 3. This top-level DNS server sends back the IP address of the DNS server that contains information about addresses that end in .COM. The local DNS server then sends a request to this second DNS server, which contains the IP address of the DNS server that contains the information about nashville.com. Step 4. After receiving back that information, the local DNS server contacts the third DNS server responsible for nashville.com, which looks up the IP address of www.nashville.com. Step 5. This information is finally returned to the local DNS server, which sends it back to the user's computer. | |

|  |  |  |
| --- | --- | --- |
| 45. Describe the ways you can use FTP on a local host computer.   |  |  | | --- | --- | | *ANSWER:* | From a command prompt. Commands can be typed at an operating system prompt, such as ls (list files), get (retrieve a file from the server), and put (transfer a file to the server). Using a Web browser. Instead of prefacing a URL with the protocol http://, the FTP protocol is entered with a preface of ftp://. Using an FTP client. A separate FTP client application can be installed that displays files on the local host as well as the remote server. | |

|  |  |  |
| --- | --- | --- |
| 46. Discuss at least two security advantages of a host running virtualization.   |  |  | | --- | --- | | *ANSWER:* | The latest security updates can be downloaded and run in a virtual machine to determine compatibility. A snapshot of a state of a virtual machine can be saved for later use. Testing the existing security configuration, known as security control testing, can be performed using a simulated network environment on a computer using multiple virtual machines. Virtual machines can promote security segregation and isolation. A virtual machine can be used to test for potential malware. | |

|  |  |  |
| --- | --- | --- |
| 47. Discuss the Software as a Service (SaaS) model used in cloud computing.   |  |  | | --- | --- | | *ANSWER:* | In the Software as a Service (SaaS) model the cloud computing vendor provides access to the vendor's software applications running on a cloud infrastructure. These applications, which can be accessed through a web browser, do not require any installation, configuration, upgrading, or management from the user. | |

|  |  |  |
| --- | --- | --- |
| 48. Discuss the Infrastructure as a Service (IaaS) model used in cloud computing.   |  |  | | --- | --- | | *ANSWER:* | In the Infrastructure as a Service (IaaS) model, the customer has the highest level of control. The cloud computing vendor allows customers to deploy and run their own software, including operating systems and applications. Consumers have some control over the operating systems, storage, and their installed applications, but do not manage or control the underlying cloud infrastructure. | |

|  |  |  |
| --- | --- | --- |
| 49. Explain the basic operating principals used in software defined networking.   |  |  | | --- | --- | | *ANSWER:* | An SDN virtualizes parts of the physical network so that it can be more quickly and easily reconfigured. This is accomplished by separating the control plane from the data plane. The control plane consists of one or more SDN servers and performs the complex functions such as routing and security checks. It also defines the data flows through the data plane. | |

|  |  |  |
| --- | --- | --- |
| 50. What Microsoft Windows feature prevents attackers from using buffer overflows to execute malware?   |  |  | | --- | --- | | *ANSWER:* | Data Execution Prevention (DEP) | |