|  |
| --- |
| **True / False** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. The OSI model breaks networking steps down into a series of six layers.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. Behavior-based monitoring attempts to overcome the limitations of both anomaly-based monitoring and signature-based monitoring by being more adaptive and proactive instead of reactive.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. All modern operating systems include a hardware firewall, usually called a host-based firewall.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4. Workgroup switches must work faster than core switches.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5. An intranet is a separate open network that anyone can access without prior authorization.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6. NAT is not a specific device, technology, or protocol. It is a technique for substituting IP addresses.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7. A security advantage of VLANs is that they can be used to prevent direct communication between servers.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8. An agent may be a permanent NAC agent and reside on end devices until uninstalled, but it cannot be a dissolvable NAC agent.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9. One use of data loss prevention (DLP) is blocking the copying of files to a USB flash drive.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10. Anomaly monitoring is designed for detecting statistical anomalies.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |
| --- |
| **Multiple Choice** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. An early networking device that functioned at layer 1 of the OSI model and added devices to a single segment is known as which of the following choices?   |  |  |  | | --- | --- | --- | |  | a. | switch | |  | b. | router | |  | c. | firewall | |  | d. | hub | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What data unit is associated with the Open Systems Interconnection layer four?   |  |  |  | | --- | --- | --- | |  | a. | segment | |  | b. | packet | |  | c. | frame | |  | d. | bit | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What data unit is associated with the Open Systems Interconnection layer two?   |  |  |  | | --- | --- | --- | |  | a. | segment | |  | b. | packet | |  | c. | frame | |  | d. | bit | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What kind of networking device forwards packets across different computer networks by reading destination addresses?   |  |  |  | | --- | --- | --- | |  | a. | switch | |  | b. | router | |  | c. | bridge | |  | d. | firewall | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. An administrator has two servers that host the same web content, but only one server is utilized at a given time. What can be configured that can help to evenly distribute work across the network, and make use of both servers in a manner that is transparent to the end users?   |  |  |  | | --- | --- | --- | |  | a. | stateful packet filtering | |  | b. | Load balancing | |  | c. | failover servers | |  | d. | proxy servers | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. A firewall that keeps a record of the state of a connection between an internal computer and an external device is using what technology below?   |  |  |  | | --- | --- | --- | |  | a. | Stateful frame filtering | |  | b. | Stateless frame filtering | |  | c. | Stateful packet filtering | |  | d. | Stateless packet filtering | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. What is the name of a computer or application program that intercepts user requests from the internal secure network and then processes that request on behalf of the user?   |  |  |  | | --- | --- | --- | |  | a. | forward proxy server | |  | b. | DNS server | |  | c. | VPN server | |  | d. | telnet server | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Which of the following is a server that routes incoming requests coming from an external network to the correct internal server?   |  |  |  | | --- | --- | --- | |  | a. | forward proxy | |  | b. | application proxy | |  | c. | system proxy | |  | d. | reverse proxy | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. What technology enables authorized users to use an unsecured public network, such as the Internet as if it were a secure private network?   |  |  |  | | --- | --- | --- | |  | a. | IKE tunnel | |  | b. | VPN | |  | c. | endpoint | |  | d. | router | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. Select the technology that can be used to examine content through application-level filtering.   |  |  |  | | --- | --- | --- | |  | a. | Application gateway | |  | b. | Security proxy | |  | c. | Web security gateway | |  | d. | Firewall | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What type of monitoring compares network traffic, activities, transactions, or behavior against a database of known attack patterns?   |  |  |  | | --- | --- | --- | |  | a. | application-based | |  | b. | protocol-based | |  | c. | behavioral-based | |  | d. | signature-based | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What is the name of an instruction that interrupts a program being executed and requests a service from the operating system?   |  |  |  | | --- | --- | --- | |  | a. | system call | |  | b. | unit call | |  | c. | hardware instruction | |  | d. | system exception | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. When a private network uses a single public IP address, and each outgoing TCP packet uses a different port to allow for proper translation, what networking technology is in use?   |  |  |  | | --- | --- | --- | |  | a. | PAT | |  | b. | PNAT | |  | c. | NAPT | |  | d. | NAT | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. Which network address below is not a private IP address network?   |  |  |  | | --- | --- | --- | |  | a. | 10.4.5.0 | |  | b. | 172.63.255.0 | |  | c. | 192.168.255.0 | |  | d. | 172.17.16.0 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. A web server must be accessible to untrusted outside users. What can be done to isolate this host and any additional hosts with similar requirements from more secured hosts on a network?   |  |  |  | | --- | --- | --- | |  | a. | Install a VPN, configure host | |  | b. | Set up a proxy in front of the web server | |  | c. | Create a DMZ, add necessary hosts. | |  | d. | Configure a reduction point on a firewall | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What vendor neutral protocol implements support for VLAN tagging?   |  |  |  | | --- | --- | --- | |  | a. | ISL | |  | b. | VTP | |  | c. | 802.1Q | |  | d. | VSTP | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. The management in your corporate office needs to group users on the network together logically even though they are attached to separate network switches. How can this be done?   |  |  |  | | --- | --- | --- | |  | a. | Create a subnet for each network switch in use | |  | b. | Create additional subnets for the separate groups | |  | c. | Add all users to a single network segment | |  | d. | Create a VLAN and add the users' computers / ports to the correct VLAN | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What technology will examine the current state of a network device before allowing it can to connect to the network and force any device that does not meet a specified set of criteria to connect only to a quarantine network?   |  |  |  | | --- | --- | --- | |  | a. | network access control | |  | b. | virtual LANs | |  | c. | network address translation | |  | d. | host health checks | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What type of dedicated cryptographic processor that provides protection for cryptographic keys?   |  |  |  | | --- | --- | --- | |  | a. | SSL/TLS accelerator | |  | b. | media gateway | |  | c. | SSL decryptor | |  | d. | hardware security module | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. Which of the following is a software-based application that runs on a local host computer that can detect an attack as it occurs?   |  |  |  | | --- | --- | --- | |  | a. | local-based intrusion detection system | |  | b. | host-based intrusion detection system | |  | c. | host-based application protection | |  | d. | local-based application protection | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. When VPN network traffic is routing only some traffic over the secure VPN while other traffic directly accesses the Internet, what technology is being used?   |  |  |  | | --- | --- | --- | |  | a. | priority tunnel | |  | b. | split tunneling | |  | c. | full tunnel | |  | d. | shared tunneling | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. What dedicated hardware device aggregates hundreds or thousands of VPN connections?   |  |  |  | | --- | --- | --- | |  | a. | VPN server | |  | b. | VPN gateway | |  | c. | VPN switch | |  | d. | VPN concentrator | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What specific type of hardware card inserts into a web server that contains one or more co-processors to handle SSL/TLS processing?   |  |  |  | | --- | --- | --- | |  | a. | SSL/TLS accelerator | |  | b. | media gateway | |  | c. | SSL decryptor | |  | d. | security module | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What type of network is a private network that belongs to an organization that can only be accessed by approved internal users?   |  |  |  | | --- | --- | --- | |  | a. | extranet | |  | b. | intranet | |  | c. | enterprise network | |  | d. | guest network | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of network is a private network that can also be accessed by authorized external customers, vendors, and partners?   |  |  |  | | --- | --- | --- | |  | a. | extranet | |  | b. | intranet | |  | c. | enterprise network | |  | d. | guest network | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. If a network is completely isolated by an air gap from all other outside networks it is using what type of configuration?   |  |  |  | | --- | --- | --- | |  | a. | physical network segregation | |  | b. | complete network segregation | |  | c. | network isolation | |  | d. | logical network segregation | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. What term is used to describe the software agents that are used by NAC and installed on devices to gather information?   |  |  |  | | --- | --- | --- | |  | a. | NAC check agents | |  | b. | server health agents | |  | c. | host agent health checks | |  | d. | network health agents | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. What type of network access control uses Active Directory to scan a device to verify that it is in compliance?   |  |  |  | | --- | --- | --- | |  | a. | agentless NAC | |  | b. | dissolvable NAC | |  | c. | dependent NAC | |  | d. | permanent NAC | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is defined as a security analysis of the transaction within its approved context?   |  |  |  | | --- | --- | --- | |  | a. | USB blocking | |  | b. | content inspection | |  | c. | storage sensors | |  | d. | data loss prevention | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following is a system of security tools that are used to recognize and identify data that is critical to the organization and ensure that it is protected?   |  |  |  | | --- | --- | --- | |  | a. | USB blocking | |  | b. | content inspection | |  | c. | storage sensors | |  | d. | data loss prevention | |

|  |
| --- |
| **Subjective Short Answer** |

|  |
| --- |
| 41. List and describe two advantages of a proxy server. |

|  |
| --- |
| 42. What are the two TCP/IP protocols that are used by mail servers for clients accessing incoming mail? |

|  |
| --- |
| 43. Describe how Internet content filters are used. |

|  |
| --- |
| 44. Discuss the two advantages that NAT provides. |

|  |
| --- |
| 45. Describe how Network Access Control (NAC) works. |

|  |
| --- |
| 46. Describe the difference between subnetting and VLANs. |

|  |
| --- |
| 47. Describe how VLAN communication takes place. |

|  |
| --- |
| 48. How does a Unified Threat Management (UTM) security product help reduce administrative overhead? |

|  |
| --- |
| 49. What is the difference between anomaly based monitoring and signature based monitoring? |

|  |
| --- |
| 50. Describe how a mail gateway operates? |