**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** *Technologies and Tools*

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | John is looking for a new firewall for a small company. He is concerned about DoS attacks, particularly the SYN flood. Which type of firewall would give the best protection against the SYN flood?  **A.** Packet filter **B.** Application gateway **C.** Bastion **D.** SPI |
|  | 2. | You are responsible for network security at an insurance company. A lot of employees bring their own devices. You have security concerns about this. You have decided to implement a process whereby when users connect to your network, their devices are scanned. If a device does not meet your minimum security requirements, it is not allowed to connect. What best describes this?  **A.** NAC **B.** SPI **C.** IDS **D.** BYOD |
|  | 3. | Ahmed is responsible for VPN connections at his company. His company uses IPSec exclusively. He has decided to implement IPSec in a mode that encrypts the data of only the packet, not the headers. What is this called? **A.** Tunneling **B.** IKE **C.** ESP **D.** Transport |
|  | 4. | Maria is responsible for monitoring IDS activity on her company’s network. Twice in the past month there has been activity reported on the IDS that investigation has shown was legitimate traffic. What best describes this?  **A.** False negative **B.** Passive **C.** Active **D.** False positive |
|  | 5. | Juanita is a network administrator for a large university. The university has numerous systems, each with logs she must monitor and analyze. What would be the best approach for her to view and analyze logs from a central server?  **A.** NAC **B.** Port forwarding **C.** IDS **D.** SIEM |
|  | 6. | Enrique is responsible for web application security at his company. He is concerned about attacks such as SQL injection. Which of the following devices would provide the best protection for web attacks on his web application server? **A.** ACL **B.** SPI **C.** WAF **D.** IDS |
|  | 7. | ACME Company has several remote offices. The CIO wants to set up permanent secure connections between the remote offices and the central office. What would be the best solution for this?  **A.** L2TP VPN **B.** IPSEC VPN  **C.** Site-to-site VPN **D.** Remote-access VPN |
|  | 8. | Mary is responsible for network security at a medium-sized insurance company. She is concerned that the offices are too open to public traffic and someone could simply connect a laptop to an open RJ45 jack and access the network. Which of the following would best address this concern?  **A.** ACL 　**B.** IDS　 **C.** VLAN 　**D.** Port security |
|  | 9. | You are the network administrator for an e-commerce company. You are responsible for the web server cluster. You are concerned about not only failover, but also load-balancing and using all the servers in your cluster to accomplish load-balancing. What should you implement?  **A.** Active-active 　**B.** Active-passive　 **C.** Affinity 　**D.** Round-robin |
|  | 10. | Donald is working as a network administrator. He is responsible for the database cluster. Connections are load-balanced in the cluster by each new connection being simply sent to the next server in the cluster. What type of load-balancing is this?  **A.** Round-robin 　**B.** Affinity 　**C.** Weighted　 **D.** Rotating |
|  | 11. | Gerald is setting up new wireless access points throughout his company’s building. The wireless access points have just the radio transceiver, with no additional functionality. What best describes these wireless access points?  **A.** Fat 　**B.** Repeater 　**C.** Thick 　**D.** Thin |
|  | 12. | Mohaned is an IT manager for a hotel. His hotel wants to put wireless access points on each floor. The specifications state that the wireless access points should have minimal functionality, with all the configuration, authentication, and other functionality centrally controlled. What type of wireless access points should Mohaned consider purchasing?  **A.** Fat 　**B.** Controller-based 　**C.** Stand-alone 　**D.** 801.11i |
|  | 13. | What IPSec protocol provides authentication and encryption?  **A.** AH 　**B.** ESP　 **C.** IKE 　**D.** ISAKMP |
|  | 14. | Terrance is implementing IPSec. He wants to ensure that the packets are encrypted, and that the packet and all headers are authenticated. What should he implement?  **A.** AH 　**B.** ESP 　**C.** AH and ESP 　**D.** IKE |
|  | 15. | You are responsible for security at your company. One of management’s biggest concerns is that employees might exfiltrate sensitive data. Which of the following would you implement first?  **A.** IPS 　　　　　**B.** Routine audits of user machines  **C.** VLAN 　　　　**D.** USB blocking |
|  | 16. | You are responsible for email server security in your company. You want to implement encryption of all emails, using third-party authenticated certificates. What protocol should you implement?  **A.** IMAP 　**B.** S/MIME　 **C.** PGP　 **D.** SMTP-S |
|  | 17. | Joanne is responsible for all remote connectivity to her company’s network. She knows that administrators frequently log in to servers remotely to execute command-line commands and Linux shell commands. She wants to make sure this can only be done if the transmission is encrypted. What protocol should she use?  **A.** HTTPS **B.** RDP **C.** Telnet **D.** SSH |
|  | 18. | You are responsible for network management at your company. You have been using SNMP for many years. You are currently using SNMP v2. A colleague has recently suggested you upgrade to SNMP v3. What is the primary benefit of SNMP v3?  **A.** It is much faster. **B.** It integrates with SIEM.  **C.** It uses CHAP authentication. **D.** It is encrypted. |
|  | 19. | Employees in your company are allowed to use tablets. They can select a tablet from four different models approved by the company but purchased by the employee. What best describes this?  **A.** BYOD **B.** CYOD **C.** COPE **D.** BYOE |
|  | 20. | Mahmoud is considering moving all company desktops to a VDI deployment. Which of the following would be a security advantage of VDI?  **A.** Employees can work from any computer in the company.  **B.** VDI is more resistant to malware.  **C.** Patch management is centrally controlled.  **D.** It eliminates man-in-the-middle attacks |
|  | 21. | You have been assigned to select a backup communication method for your company to use in case of significant disasters that disrupt normal communication. Which option would provide the most reliability?  **A.** Cellular 　**B.** WiFi 　**C.** SATCOM 　**D.** VoIP |
|  | 22. | John is concerned about the security of data on smartphones and tablets that his company issues to employees. Which of the following would be most effective in preventing data loss, should a device be stolen?  **A.** Remote wipe 　　**B.** Geolocation  **C.** Strong PIN 　　　**D.** Limited data storage |
|  | 23. | What does geofencing accomplish?  **A.** Provides the location for a mobile device.  **B.** Limits the range a mobile device can be used in.  **C.** Determines WiFi coverage areas. 　　　**D.** Segments the WiFi. |
|  | 24. | What best describes mobile device content management?  **A.** Limiting how much content can be stored.  **B.** Limiting the type of content that can be stored.  **C.** Blocking certain websites. 　**D.** Digitally signing authorized content. |
|  | 25. | Frank believes there could be a problem accessing the DHCP server from a specific client. He wants to check by getting a new dynamic IP. What command will do this?  **A.** ipconfig /request 　　 **B.** NETSTAT -renew  **C.** ipconfig /renew 　　　**D.** NETSTAT /request |
|  | 26. | Teresa is responsible for network administration at a health club chain. She is trying for find a communication technology that uses low power and can spend long periods in low-power sleep modes. Which of the following technologies would be the best fit?  **A.** WiFi 　**B.** Cellular 　**C.** Bluetooth 　**D.** ANT |
|  | 27. | What technology was first introduced in Windows Vista and still exists in Windows that helps prevent malware by requiring user authorization to run executables?  **A.** DEP 　**B.** DLP 　**C.** UTM　 **D.** ANT |
|  | 28. | John is responsible for security of his company’s new e-commerce server. He wants to ensure that online transactions are secure. What technology should he use?  **A.** L2TP 　**B.** IPSec 　**C.** SSL 　**D.** TLS |
|  | 29. | Frank is a network administrator for a small college. The college has implemented a simple NIDS. However, the NIDS seems to only catch well-known attacks. What technology is this NIDS likely missing?  **A.** Heuristic scanning 　　　**B.** Signature scanning  **C.** Passive scanning 　　　　**D.** Active scanning |
|  | 30. | You are concerned about an attacker enumerating all of your network. What protocol might help at least mitigate this issue?  **A.** HTTPS　**B.** TLS 　**C.** IPSec　 **D.** LDAPS |
|  | 31. | You have been asked to implement a secure protocol for transferring files that uses digital certificates. Which protocol would be the best choice?　　 **A.** FTP 　　**B.** SFTP 　　**C.** FTPS　　 **D.** SCP |
|  | 32. | Ahmed is responsible for VoIP at his company. He has been directed to ensure that all VoIP calls have the option to be encrypted. What protocol is best suited for security VoIP calls?  **A.** SIP 　　**B.** TLS 　　**C.** SRTP　　 **D.** SSH |
|  | 33. | What is the purpose of screen locks on mobile devices?  **A.** To encrypt the device 　　　　**B.** To limit access to the device  **C.** To load a specific user’s apps 　**D.** To connect to WiFi |
|  | 34. | Maria is a security engineer with a large bank. Her CIO has asked her to investigate the use of context-aware authentication for online banking. Which of the following best describes context-aware authentication?  **A.** In addition to username and password, authentication is based on the entire context (location, time of day, action being attempted, etc.).  **B.** Without a username or password, authentication is based on the entire context (location, time of day, action being attempted, etc.).  **C.** Authentication that requires a username and password, but in the context of a token or digital certificate  **D.** Authentication that requires a username and password, but not in the context of a token or digital certificate |
|  | 35. | What does application management accomplish for mobile devices?  **A.** Only allows applications from the iTunes store to be installed  **B.** Ensures the company has a list of all applications on the devices  **C.** Ensures only approved applications are installed on the devices  **D.** Updates patches on all applications on mobile devices |
|  | 36. | Dominick is responsible for security at a medium-sized insurance company. He is very concerned about detecting intrusions. The IDS he has purchased states that he must have an IDS on each network segment. What type of IDS is this?  **A.** Active 　**B.** IPS 　**C.** Passive　 **D.** Inline |
|  | 37. | Remote employees at your company frequently need to connect to both the secure company network via VPN and open public websites, simultaneously. What technology would best support this?  **A.** Split tunnel 　**B.** IPSec 　**C.** Full tunnel　 **D.** TLS |
|  | 38. | Denish is looking for a solution that will allow his network to retrieve information from a wide range of web resources, while all traffic passes through a proxy. What would be the best solution?  **A.** Forward proxy 　**B.** Reverse proxy  **C.** SPI 　　　　　**D.** Open proxy |
|  | 39. | Someone has been rummaging through your company’s trash bins seeking to find documents, diagrams, or other sensitive information that has been thrown out. What is this called?  **A.** Dumpster diving 　　　 **B.** Trash diving  **C.** Social engineering 　　　**D.** Trash engineering |
|  | 40. | Derrick is responsible for a web server cluster at his company. The cluster uses various load-balancing protocols. Derrick wants to ensure that clients connecting from Europe are directed to a specific server in the cluster. What would be the best solution to his problem?  **A.** Affinity 　**B.** Binding 　**C.** Load balancing　 **D.** Round-robin |
|  | 41. | Teresa is responsible for WiFi security in her company. Her main concern is that there are many other offices in the building her company occupies and that someone could easily attempt to breach their WiFi from one of these locations. What technique would be best in alleviating her concern?  **A.** Using thin WAPs 　　　　　　**B.** Geofencing  **C.** Securing the Admin screen 　　**D.** WAP placement |
|  | 42. | Juan is responsible for the SIEM in his company. The SIEM aggregates logs from 12 servers. In the event that a breach is discovered, which of the following would be Juan’s most important concern?  **A.** Event duplication 　　 **B.** Time synchronization  **C.** Impact assessment 　　**D.** Correlation |
|  | 43. | . When you are considering an NIDS or NIPS, what are your two most important concerns?  **A.** Cost and false positives 　　**B.** False positives and false negatives  **C.** Power consumption and cost 　**D.** Management interface and cost |
|  | 44. | Shelly is very concerned about unauthorized users connecting to the company routers. She would like to prevent spoofing. What is the most essential antispoofing technique for routers?  **A.** ACL　 **B.** Logon　 **C.** NIPS 　**D.** NIDS |
|  | 45. | Farès has implemented a flood guard. What type of attack is this most likely to defend against?  **A.** SYN attack 　　　**B.** DNS poisoning  **C.** MAC spoofing 　　**D.** ARP spoofing |
|  | 46. | Terrance is trying to get all of his users to connect to a certificate server on his network. However, some of the users are using machines that are incompatible with the certificate server, and changing those machines is not an option. Which of the following would be the best solution for Terrance?  **A.** Use an application proxy for the certificate server.  **B.** Use NAT with the certificate server.  **C.** Change the server. 　　　　**D.** Implement a protocol analyzer. |
|  | 47. | John is implementing virtual IP load-balancing. He thinks this might alleviate network slowdowns, and perhaps even mitigate some of the impact of a denial-of-service attack. What is the drawback of virtual IP load-balancing?  **A.** It is resource-intensive. 　　**B.** Most servers don’t support it.  **C.** It is connection-based, not load-based.  **D.** It works only on Unix/Linux servers. |
|  | 48. | There has been a breach of the ACME network. John manages the SIEM at ACME. Part of the attack disrupted NTP; what SIEM issue would this most likely impact?  **A.** Time synchronization 　　　　 **B.** Correlation  **C.** Event duplication 　　　　　　**D.** Events not being logged |
|  | 49. | What command would produce the image shown here?    **A.** ping -n 6 -l 100 192.168.1.1 　**B.** ping 192.168.1.1 -n 6 -s 100  **C.** ping #6 s 100 192.168.1.1 　　**D.** ping -s 6 -w 100 192.168.1.1 |
|  | 50. | You are a security officer for a large law firm. You are concerned about data loss prevention. You have limited the use of USBs and other portable media, you use an IDS to look for large volumes of outbound data, and a guard searches all personnel and bags before they leave the building. What is a key step in DLP that you have missed?  **A.** Portable drives　 **B.** Email 　**C.** Bluetooth 　**D.** Optical media |
|  | 51. | Which of the following email security measures would have the most impact on phishing emails?  **A.** Email encryption 　　　　**B.** Hardening the email server  **C.** Digitally signing email 　　**D.** Spam filter |
|  | 52. | Joanne has implemented TLS for communication with many of her networks servers. She wants to ensure that the traffic cannot be sniffed. However, users now complain that this is slowing down connectivity. Which of the following is the best solution?  **A.** Increase RAM on servers.  **B.** Change routers to give more bandwidth to traffic to these servers.  **C.** Implement TLS accelerators.  **D.** Place all servers in clusters with extensive load-balancing. |
|  | 53. | Olivia has discovered steganography tools on an employee’s computer. What is the greatest concern regarding employees having steganography tools?  **A.** Password cracking　　　 **B.** Data exfiltration  **C.** Hiding network traffic 　　**D.** Malware |
|  | 54. | What command would generate the output shown here?    **A.** netstat -a 　**B.** netstat –o　 **C.** arp -a 　**D.** arp -g |
|  | 55. | John has discovered that an attacker is trying to get network passwords by using software that attempts a number of passwords from a list of common passwords. What type of attack is this?  **A.** Dictionary 　　**B.** Rainbow table  **C.** Brute force 　　**D.** Session hijacking |
|  | 56. | Isabella has found netcat installed on an employee’s computer. That employee is not authorized to have netcat. What security concern might this utility present?  **A.** It is a password cracker. 　　　　　　**B.** It is a packet sniffer.  **C.** It is a network communication utility. 　**D.** It is a DoS tool |
|  | 57. | Omar is a network administrator for ACME Company. He is responsible for the certificate authorities within the corporate network. The CAs publish their CRLs once per week. What, if any, security issue might this present?  **A.** Revoked certificates still being used  **B.** Invalid certificates being issued  **C.** No security issue  **D.** Certificates with weak keys |
|  | 58. | Hans is a network administrator for a large bank. He is concerned about employees violating software licenses. What would be the first step in addressing this issue?  **A.** Performing software audits  **B.** Scanning the network for installed applications  **C.** Establishing clear policies  **D.** Blocking the ability of users to install software |
|  | 59. | You are responsible for authentication methods at your company. You have implemented fingerprint scanners to enter server rooms. Frequently people are being denied access to the server room, even though they are authorized. What problem is this?  **A.** FAR 　**B.** FRR 　**C.** CER 　**D.** EER |
|  | 60. | John is responsible for network security at a very small company. Due to both budget constraints and space constraints, John can select only one security device. What should he select?  **A.** Firewall 　**B.** Antivirus 　**C.** IDS　 **D.** UTM |
|  | 61. | You are responsible for security at Acme Company. Recently, 20 new employee network accounts were created, with the default privileges for the network. You have discovered that eight of these have privileges that are not needed for their job tasks. Which security principle best describes how to avoid this problem in the future?  **A.** Least privileges　　 **B.** Separation of duties  **C.** Implicit deny 　　　**D.** Weakest link |
|  | 62. | Mary is concerned that SIEM logs at her company are not being stored long enough, or securely enough. She is aware that it is possible a breach might not be discovered until long after it occurs. This would require the company to analyze older logs. It is important that Mary find an SIEM log backup solution that can a) handle all the aggregate logs of the SIEM, b) be maintained for a long period of time, and c) be secure. What solution would be best for her?  **A.** Back up to large-capacity external drives.  **B.** Back up to large-capacity backup tapes.  **C.** Back up to WORM storage.  **D.** Back up to tapes that will be stored off-site |
|  | 63. | Elizabeth is responsible for SIEM systems in her company. She monitors the company’s SIEM screens every day, checking every hour. What, if any, would be a better approach for her to keep up with issues that appear in the logs?  **A.** Automatic alerts  **B.** Having logs forwarded to her email  **C.** Nothing, this is fine.  **D.** Review SIEM logs primarily when an incident occurs. |
|  | 64. | You are responsible for network security at a university. Faculty members are issued laptops. However, many of the faculty members leave the laptops in their offices most of the time (sometimes even for weeks). You are concerned about theft of laptops. In this scenario, what would be the most cost-effective method of securing the laptops?  **A.** FDE 　**B.** GPS tagging 　**C.** Geofencing 　**D.** Tethering |
|  | 65. | You work at a defense contracting company. You are responsible for mobile device security. Some researchers in your company use company-issued tablets for work. These tablets may contain sensitive, even classified data. What is the most important security measure for you to implement?  **A.** FDE 　**B.** GPS tagging　 **C.** Geofencing 　**D.** Content management |
|  | 66. | When using any HIDS/HIPS or NIDS/NIPS, the output is specific to the vendor. However, what is the basic set of information that virtually all HIDSs/HIPSs or NIDSs/NIPSs provide?  **A.** IP addresses (sender and receiver), ports (sender and receiver), and protocol  **B.** IP addresses (sender and receiver), ports (sender and receiver), and attack type  **C.** IP addresses (sender and receiver), ports (sender and receiver), usernames, and machine names  **D.** Usernames, machine names, and attack type |
|  | 67. | You are responsible for firewalls in your company. You are reviewing the output of the gateway firewall. What basic information would any firewall have in its logs?  **A.** For all traffic: the source and destination IP and port, protocol, and whether it was allowed or denied  **B.** For only blocked traffic: the source and destination IP and port as well as the reason for the traffic being denied/blocked  **C.** For all traffic: the source and destination IP and port, whether it was allowed or denied, and the reason it was denied/blocked  **D.** For only blocked traffic: the source and destination IP, protocol, and the reason it was denied/blocked |
|  | 68. | Teresa is responsible for incident response at ACME Company. There was a recent breach of the network. The breach was widespread and affected many computers. As part of the incident response process, Teresa will collect the logs from the SIEM, which aggregates logs from 20 servers. Which of the following should she do first?  **A.**de-duplication  **B.** Log forwarding  **C.** Identify the nature of the attack  **D.** Identify the source IP of the attack |
|  | 69. | Hector is responsible for NIDS/NIPS in his company. He is configuring a new NIPS solution. What part of the NIPS collects data?  **A.** Sensor 　**B.** Data source 　**C.** Manager　 **D.** Analyzer |
|  | 70. | Gerald is a network administrator for a small financial services company. He is responsible for controlling access to resources on his network. What mechanism is responsible for blocking access to a resource based on the requesting IP address?  **A.** ACL 　**B.** NIPS 　**C.** HIPS 　**D.** Port blocking |
|  | 71. | Elizabeth is responsible for secure communications at her company. She wants to give administrators the option to log in remotely and to execute command-line functions, but she wants this to only be possible via a secure, encrypted connection. What action should she take on the firewall?  **A.** Block port 23 and allow ports 20 and 21.  **B.** Block port 22 and allow ports 20 and 21.  **C.** Block port 22 and allow port 23.  **D.** Block port 23 and allow port 22. |
|  | 72. | Mark is looking for a proxy server for his network. The purpose of the proxy server is to ensure that the web servers are hidden from outside clients. All of the different web servers should appear to the outside world as if they were the proxy server. What type of proxy server would be best for Mark to consider?  **A.** Forward 　**B.** Reverse 　**C.** Transparent　 **D.** Firewall |
|  | 73. | Your company has hired an outside security firm to perform various tests of your network. During the vulnerability scan you will provide that company with logins for various systems (i.e., database server, application server, web server, etc.) to aid in their scan. What best describes this?  **A.** A white-box test 　　　**B.** A gray-box test  **C.** A credentialed scan　　 **D.** A logged-in scan |
|  | 74. | . Lars is responsible for incident response at ACME Company. He is particularly concerned about the network segment that hosts the corporate web servers. He wants a solution that will detect potential attacks and notify the administrator so the administrator can take whatever action he or she deems appropriate. Which of the following would be the best solution for Lars?  **A.** HIDS 　　**B.** HIPS 　　**C.** NIDS 　　**D.** NIPS |
|  | 75. | Mia is responsible for security devices at her company. She is concerned about detecting intrusions. She wants a solution that would work across entire network segments. However, she wants to ensure that false positives do not interrupt work flow. What would be the best solution for Mia to consider?  **A.** HIDS 　　**B.** HIPS　　 **C.** NIDS　　 **D.** NIPS |
|  | 76. | Abigail is a security manager for a small company. Many employees want to use handheld devices, such as smartphones and tablets. The employees want to use these devices both for work and outside of work. Abigail is concerned about security issues. Which of the following would be the most secure solution?  **A.** COPE 　　**B.** CYOD 　　**C.** Geotagging　　 **D.** BYOD |
|  | 77. | You are responsible for always-on VPN connectivity for your company. You have been told that you must use the most secure mode for IPSec that you can. Which of the following would be the best for you to select?  **A.** Tunneling 　　**B.** AH 　　**C.** IKE　　 **D.** Transport |
|  | 78. | Debra is the network administrator for her company. Her company’s web servers are all in a cluster. Her concern is this: if one of the servers in the cluster fails, will the backup server be capable of running for a significant amount of time? She wants to make sure that the backup won’t soon fail. What would be her best choice in clustering?  **A.** Active-active 　　　**B.** Round-robin  **C.** Affinity 　　　　　 **D.** Active-passive |
|  | 79. | Omar is responsible for wireless security in his company. He wants completely different WiFi access (i.e., a different SSID, different security levels, and different authentication methods) in different parts of the company. What would be the best choice for Omar to select in WAPs?  **A.** Fat 　**B.** Thin　 **C.** Repeater 　**D.** Full |
|  | 80. | . Lilly is a network administrator for a medium-sized financial services company. She wants to implement company-wide encryption and digital signing of emails. But she is concerned about cost, since there is a very limited budget for this. What would be her best choice?  **A.** SMTPS 　　**B.** S/MIME　　 **C.** IMAPS 　　**D.** PGP |
|  | 81. | Edward is a security manager for a bank. He has recently been reading a great deal about malware that accesses system memory. He wants to find a solution that would stop programs from utilizing system memory. Which of the following would be the best solution?  **A.** DEP　　 **B.** FDE 　　**C.** UTM 　　**D.** IDS |
|  | 82. | Sarah is the CIO for a small company. She recently had the entire company’s voice calls moved to VoIP. Her new VoIP system is using SIP with RTP. What might be the concern with this?  **A.** SIP is not secure. 　　　**B.** RTP is not secure.  **C.** RTP is too slow. 　　　**D.** SIP is too slow. |
|  | 83. | What command would generate the output shown here?    **A.** nslookup 　**B.** ipconfig 　**C.** netstat -a 　**D.** dig |
|  | 84. | Emiliano is a network administrator for a large web-hosting company. His company also issues digital certificates to web-hosting clients. He wants to ensure that a digital certificate will not be used once it has been revoked. He also wants to ensure that there will be no delay between when the certificate is revoked and when browsers are made aware that it is revoked. What solution would be best for this?  **A.** OCSP 　**B.** X.509　 **C.** CRL 　**D.** PKI |
|  | 85. | Elizabeth is responsible for security at a defense contracting company. She is concerned about users within her network exfiltrating data by attaching sensitive documents to emails. What solution would best address this concern?  **A.** Email encryption 　**B.** USB blocking  **C.** NIPS 　　　　　　**D.** Content filtering |
|  | 86. | Victor is concerned about data security on BYOD and COPE. He is concerned specifically about data exposure should the device become lost or stolen. Which of the following would be most effective in countering this concern?  **A.** Geofencing 　　　**B.** Screen lock  **C.** GPS tagging　　 　**D.** Device encryption |
|  | 87. | Gabriel is using nmap to scan one of his servers whose IP address is 192.168.1.1. He wants to perform a ping scan, but the network blocks ICMP, so he will try a TCP ping scan and do so very slowly. Which of the following would accomplish that?  **A.** nmap -O -PT -T1 192.168.1.1 　**B.** nmap -O – T3 192.168.1.1  **C.** nmap -T -T1 192.168.1.1 　　**D.** nmap -PT -T5 192.168.1.1 |
|  | 88. | Mary is a network administrator for ACME Company. She sometimes needs to run a packet sniffer so that she can view the network traffic. She wants to find a well-known packet sniffer that works on Linux. Which of the following would be her best choice?  **A.** Ophcrack 　　**B.** Nmap 　　**C.** Wireshark　　 **D.** Tcpdump |
|  | 89. | What command produced the output shown here?  **A.** tracert -h 10 [www.chuckeasttom.com](http://www.chuckeasttom.com)  **B.** tracert [www.chuckeasttom.com](http://www.chuckeasttom.com)  **C.** netstat [www.chuckeasttom.com](http://www.chuckeasttom.com)  **D.** nmap www.chuckeasttom.com |
|  | 90. | Daryll has been using a packet sniffer to observe traffic on his company’s network. He has noticed that traffic between the web server and the database server is sent in clear text. He wants a solution that will not only encrypt that traffic, but also leverage the existing digital certificate infrastructure his company has. Which of the following would be the best solution for Daryll?  **A.** TLS 　　**B.** SSL 　　**C.** IPSec 　　**D.** WPA2 |
|  | 91 | Jarod is concerned about DLP in his organization. Employees all have cloud-based solutions for data storage. What DLP-related security hazard, if any, might this create?  **A.** No security hazard  **B.** Malware from the cloud  **C.** Data exfiltration through the cloud  **D.** Security policies don’t apply to the cloud |
|  | 92 | Derrick is a network administrator for a large company. The company network is segmented into zones of high security, medium security, low security, and the DMZ. He is concerned about external intruders and wishes to install a honeypot. Which is the most important zone to put the honeypot in?  **A.** High security 　**B.** Medium security 　**C.** Low security 　**D.** DMZ |
|  | 93 | Sheila is responsible for data backups for all the company servers. She is concerned about frequency of backup and about security of the backup data. Which feature, found in some backup utility software, would be most important to her?  **A.** Using data encryption 　　　　　　 **B.** Digitally signing the data  **C.** Using automated backup scheduling **D.** Hashing the backup data |
|  | 94 | . Frank is a web server administrator for a large e-commerce company. He is concerned about someone using netcat to connect to the company web server and retrieving detailed information about the server. What best describes his concern?  **A.** Passive reconnaissance **B.** Active reconnaissance  **C.** Banner grabbing **D.** Vulnerability scanning |
|  | 95 | Mike is responsible for testing security at his company. He is using a tool that identifies vulnerabilities and provides mechanisms to test them by attempting to exploit them. What best describes this type of tool?  **A.** Vulnerability scanner **B.** Exploit framework  **C.** Metasploit **D.** Nessus |
|  | 96 | William is a security officer for a large bank. When executives’ laptops are decommissioned, he wants to ensure that the data on those laptops is completely wiped so that it cannot be recovered, even using forensic tools. How many times should William wipe a hard drive?  **A.** 1 **B.** 3 **C.** 5 **D.** 7 |
|  | 97 | You are responsible for firewalls in your organization. You are concerned about ensuring that all firewalls are properly configured. The gateway firewall is configured as follows: to only allow inbound traffic on a very few specific, required ports; all traffic (allowed or blocked) is logged and logs forwarded to the SIEM. What, if anything, is missing from this configuration?  **A.** Nothing, it is a good configuration.  **B.** Encrypting all traffic  **C.** Outbound connection rules  **D.** Digital certificate authentication for inbound traffic |
|  | 98 | Charles is responsible for security for web servers in his company. Some web servers are used for an internal intranet, and some for external websites. He has chosen to encrypt all web traffic, and he is using self-signed X.509 certificates. What, if anything, is wrong with this approach?  **A.** He cannot encrypt all HTTP traffic.  **B.** He should use PGP certificates.  **C.** He should not use self-signed certificates.  **D.** Nothing; this is an appropriate configuration. |
|  | 99 | You are responsible for the security of web servers at your company. You are configuring the WAF and want to allow only encrypted traffic to and from the web server, including traffic from administrators using a command-line interface. What should you do?  **A.** Open port 80 and 23, and block port 443.  **B.** Open port 443 and 23, and block port 80.  **C.** Open port 443 and 22, and block port 80 and 23.  **D.** Open port 443, and block all other ports. |
|  | 100 | Francis is a security administrator at a large law firm. She is concerned that confidential documents, with proprietary information, might be leaked. The leaks could be intentional or accidental. She is looking for a solution that would embed some identifying information into documents in such a way that it would not be seen by the reader but could be extracted with the right software. What technology would best meet Francis’s needs?  **A.** Symmetric encryption **B.** Steganography  **C.** Hashing **D.** Asymmetric encryption |
|  | 101 | You are responsible for the gateway firewall for your company. You need to configure a firewall to allow only email that is encrypted to be sent or received. What action should you take?  **A.** Allow ports 25, 110, and 143. Block ports 465, 993, and 995.  **B.** Block ports 25, 110, and 143. Allow ports 465, 993, and 995.  **C.** Allow ports 25, 110, and 443. Block ports 465, 993, and 143.  **D.** Block ports 465, 994, and 464. Allow ports 25, 110, and 80. |
|  | 102 | Mark is responsible for security for a small bank. He has a firewall at the gateway as well as one at each network segment. Each firewall logs all accepted and rejected traffic. Mark checks each of these logs regularly. What is the first step Mark should take to improve his firewall configuration?  **A.** Integrate with SIEM. **B.** Add a honeypot.  **C.** Integrate with AD. **D.** Add a honeynet. |
|  | 103 | You are setting up VPNs in your company. You are concerned that anyone running a packet sniffer could obtain metadata about the traffic. You have chosen IPSec. What mode should you use to accomplish your goals of preventing metadata being seen?  **A.** AH **B.** ESP **C.** Tunneling **D.** Transport |
|  | 104 | John is responsible for configuring security devices in his network. He has implemented a robust NIDS in his network. However, on two occasions the NIDS has missed a breach. What configuration issue should John address?  **A.** False negative **B.** Port blocking  **C.** SPI **D.** False positive |
|  | 105 | You are responsible for communications security at your company. Your company has a large number of remote workers, including traveling salespeople. You wish to make sure that when they connect to the network, it is in a secure manner. What should you implement?  **A.** L2TP VPN 　　　　　　　　　　　　　 **B.** IPSec VPN  **C.** Site-to-site VPN 　　　　　　　　　　　**D.** Remote-access VPN |
|  | 106 | Your company is issuing portable devices to employees for them to use for both work and personal use. This is done so the company can control the security of the devices. What, if anything, is an issue this process will cause?  **A.** Personal information being exposed  **B.** Company data being exfiltrated  **C.** Devices being insecurely configured  **D.** No issues |
|  | 107 | Marsha is responsible for mobile device security. Her company uses COPE for mobile devices. All phones and tablets have a screen lock and GPS tagging. What is the next, most important step for Marsha to take to secure the phones?  **A.** Implement geofencing.　 **B.** Implement application management.  **C.** Implement geolocation. 　**D.** Implement remote wipe |
|  | 108 | Valerie is responsible for mobile device security at her company. The company is using BYO**D.** She is concerned about employees’ personal device usage compromising company data on the phones. What technology would best address this concern?  **A.** Containerization 　　 　　　**B.** Screen lock  **C.** Full disk encryption 　　　　　　　　　　　　　**D.** Biometrics |
|  | 109 | Jack is a chief information security officer (CISO) for a small marketing company. The company’s sales staff travel extensively and all use mobile devices. He has recently become concerned about sideloading. Which of the following best describes sideloading?  **A.** Installing applications to Android devices via USB  **B.** Loading software on any device via WiFi  **C.** Bypassing the screen lock  **D.** Loading malware on a device without the user being aware |
|  | 110 | You are responsible for DLP at a large company. Some employees have COPE and others BYO**D.** What DLP issue might these devices present?  **A.** COPE can be USB OTG.  **B.** BYOD can be USB OTG.  **C.** COPE and BYOD can be USB OTG.  **D.** Only jailbroken COPE or BYOD can be USB OTG |
|  | 111 | John is responsible for network security at a large company. He is concerned about a variety of attacks but DNS poisoning in particular. Which of the following protocols would provide the most help in mitigating this issue?  **A.** IPSec 　　　**B.** DNSSEC 　　　**C.** L2TP　　　 **D.** TLS |
|  | 112 | You are responsible for network security at your company. You have discovered that NTP is not functioning properly. What security protocol will most likely be affected by this?  **A.** Radius　　　 **B.** DNSSEC　　 　**C.** IPSec　　　 **D.** Kerberos |
|  | 113 | Frank is concerned about DHCP starvation attacks. He is even more worried since he learned that anyone can download software called a “gobbler” and execute a DHCP starvation attack. What technology would most help him mitigate this risk?  **A.** Encrypt all DHCP communication with TLS.  **B.** FDE on the DHCP server  **C.** Network Address Allocation  **D.** IPSec for all DHCP communications |
|  | 114 | You are trying to allocate appropriate numbers of IP addresses for various subnets in your network. What would be the proper CIDR notation for an IP v4 subnet with 59 nodes?  **A.** /27 　　**B.** /29　　 **C.** /24　　 **D.** /26 |
|  | 115 | Lydia is trying to reduce costs at her company and at the same time centralize network administration and maintain direct control of the network. Which of the following solutions would provide the most network administration centralization and control while reducing costs?  **A.** Outsourcing network administration 　　　　　　　　　**B.** IaaS  **C.** PaaS 　　　　　　　　　　　　**D.** Moving all OSs to open source |
|  | 116 | You are investigating a remote access protocol for your company to use. The protocol needs to fully encrypt the message, use reliable transport protocols, and support a range of network protocols. Which of the following would be the best choice?  **A.** RADIUS　　　 **B.** Diameter 　　　**C.** TACACS +　　　 **D.** IPSec |
|  | 117 | Carrol is responsible for network connectivity in her company. The sales department is transitioning to VoIP. What are two protocols she must allow through the firewall?  **A.** RADIUS and SNMP 　　　　　　　　　**B.** TCP and UDP  **C.** SIP and RTP 　　　　　　　　　　　　**D.** RADIUS and SIP |
|  | 118 | John is setting up all the database servers on their own subnet. He has placed them on 10.10.3.3/29. How many nodes can be allocated in this subnet?  **A.** 32 　　　**B.** 16 　　　**C.** 8 　　　**D.** 6 |
|  | 119 | Carlos is a security manager for a small company that does medical billing and records management. He is using application blacklisting to prevent malicious applications from being installed. What, if anything, is the weakness with this approach?  **A.** None, this is the right approach.  **B.** It might block legitimate applications.  **C.** It might fail to block malicious applications.  **D.** It will limit productivity. |
|  | 120 | Joanne is a security administrator for a large company. She discovered that approximately 100 machines on her network were recently attacked by a major virus. She is concerned because there was a patch available that would have stopped the virus from having any impact. What is the best solution for her to implement on her network?  **A.** Installing patch management software  **B.** Using automatic updates  **C.** Putting unpatched machines on a Bridge  **D.** Scanning all machines for patches every day |
|  | 121 | A review of your company’s network traffic shows that most of the malware infections are caused by users visiting illicit websites. You want to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following technologies would be the best solution?  **A.** IDS 　　　　　**B.** Firewall 　　　　　**C.** UTM 　　　　**D.** SIEM |
|  | 122 | You work for a large bank. The bank is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the best solution to this problem?  **A.** IDS 　　　　**B.** DLP　　　 **C.** Content filtering 　　　　**D.** NIPS |
|  | 123 | Match the letter of the functionality with the device in the following table.  **A.** Detect intrusions on a single machine 　　　**B.** Use aggregate logs  **C.** Filter network packets based on a set of rules **D.** Detect intrusions on a network segment |
|  | 124 | Francine is concerned about employees in her company jailbreaking their COPE devices. What would be the most critical security concern for jailbroken devices?  **A.** They would no longer get security patches.  **B.** It would disable FDE.  **C.** Unauthorized applications could be installed.  **D.** Data could be exfiltrated on these devices. |
|  | 125 | You are responsible for mobile device security in your company. Employees have COPE devices. Many employees only enter the office infrequently, and you are concerned that their devices are not receiving firmware updates on time. What is the best solution for this problem?  **A.** Scheduled office visits for updates  **B.** OTA updates  **C.** Moving from COPE to BYOD  **D.** A policy that requires users to update their firmware regularly |
|  | 126 | Frank is looking for a remote authentication and access protocol. It must be one that uses UDP due to firewall rules. Which of the following would be the best choice?  **A.** RADIUS 　　　**B.** Diameter　　　 **C.** TACACS + 　　**D.** IPSec |
|  | 127 | You have discovered that one of the employees at your company tethers her smartphone to her work PC to bypass the corporate web security and access prohibited websites while connected to the LAN. What would be the best way to prevent this?  **A.** Disable wireless access. 　　　　　　　　**B.** Implement a WAF.  **C.** Implement a policy against tethering. 　　**D.** Implement an HIPS. |
|  | 128 | You work for a large bank. One of your responsibilities is to ensure that web banking logins are as secure as possible. You are concerned that a customer’s account login could be compromised and someone else would use that login to access the customer’s account. What is the best way to mitigate this threat?  **A.** Use SMS authentication for any logins from an unknown location or computer.  **B.** Encrypt all traffic via TLS.  **C.** Require strong passwords.  **D.** Do not allow customers to log on from any place other than their home computer. |
|  | 129 | You have discovered that some employees in your company have installed custom firmware on their portable devices. What security flaw would this most likely lead to?  **A.** Unauthorized software can run on the device.  **B.** The device may not connect to the network.  **C.** The device will overheat.  **D.** This is not really a security issue. |
|  | 130 | You are configuring BYOD access for your company. You want the absolute most robust security for the BYOD on your network. What would be the best solution?  **A.** Agentless NAC 　　　　　　　　　**B.** Agent NAC  **C.** Digital certificate authentication　　 **D.** Two-factor authentication |
|  | 131 | You work for a large law firm and are responsible for network security. It is common for guests to come to the law firm (clients, expert witnesses, etc.) who need to connect to the firm’s WiFi. You wish to ensure that you provide the maximum security when these guests connect with their own devices, but you also wish to provide assurance to the guest that you will have minimal impact on their device. What is the best solution?  **A.** Permanent NAC agent　　　　　 **B.** Agentless NAC  **C.** Dissolvable NAC agent 　　　　　**D.** Implement COPE |
|  | 132 | Tom is concerned about how his company can best respond to breaches. He is interested in finding a way to identify files that have been changed during the breach. What would be the best solution for him to implement?  **A.** NAC 　　　　　　　　　　　　**B.** NIDS  **C.** File integrity checker 　　　　　**D.** Vulnerability scanner |
|  | 133 | Mary works for a large insurance company and is responsible for cybersecurity. She is concerned about insiders and wants to detect malicious activity on the part of insiders. But she wants her detection process to be invisible to the attacker. What technology best fits these needs?  **A.** Hybrid NIDS　　 **B.** Out-of-band NIDS　　 **C.** NIPS 　　**D.** NNIDS |
|  | 134 | Denish is responsible for security at a large financial services company. The company frequently uses SSL/TLS for connecting to external resources. He has concerns that an insider might exfiltrate data using an SSL/TLS tunnel. What would be the best solution to this issue?  **A.** NIPS 　　**B.** SSL decryptor 　　**C.** NIDS 　　**D.** SSL accelerator |
|  | 135 | You want to allow a media gateway to be accessible through your firewall. What ports should you open? (Choose two.)  **A.** 2427　　 **B.** 1707 　　**C.** 2227 　　**D.** 1727 |
|  | 136 | Match the letter with the protocol in the following table.   1. Wireless security 　**B.** Voice over IP 2. **C.** VPN 　　　　　**D.** Secure command-line interface |
|  | 137 | Dennis is implementing wireless security throughout his network. He is using WPA2. However, there are some older machines that cannot connect to WPA2—they only support WEP. At least for now, he must keep these machines. What is the best solution for this problem?  **A.** Put those machines on a different VLAN.  **B.** Deny wireless capability for those machines.  **C.** Put those machines on a separate wireless network with separate WAP.  **D.** Encrypt their traffic with TLS. |
|  | 138 | You are a security administrator for Acme Company. Employees in your company routinely upload and download files. You are looking for a method that allows users to remotely upload or download files in a secure manner. The solution must also support more advanced file operations such as creating directories, deleting files, and so forth. What is the best solution for this?  **A.** SFTP　　 **B.** SSH　　 **C.** SCP　　 **D.** IPSec |
|  | 139 | Your company allows BYOD on the network. You are concerned about the risk of malicious apps being introduced to your network. Which of the following policies would be most helpful in mitigating that risk?  **A.** Prohibiting apps from third-party stores **B.** Application blacklisting  **C.** Antimalware scanning 　　　　　　　**D.** Requiring FDE on BYOD |
|  | 140 | John is the CISO for a small company. The company has password policies, but John is not sure the policies are adequate. He is concerned that someone might be able to “crack” company passwords. What is the best way for John to determine whether his passwords are vulnerable?  **A.** Run a good vulnerability scan.  **B.** Perform a password policy audit.  **C.** Use one or more password crackers himself.  **D.** Ensure that passwords are stored as a hash. |
|  | 141 | You are scanning your network using a packet sniffer. You are seeing traffic on ports 25 and 110. What security flaw would you most likely notice on these ports?  **A.** Website vulnerabilities　 **B.** Unencrypted credentials  **C.** Misconfigured FTP　　　 **D.** Digital certificate errors |
|  | 142 | Abigail is a network administrator with ACME Company. She believes that a network breach has occurred in the data center as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should she search for in the logs to confirm if such a breach occurred?  **A.** Traffic on port 23 　　　　　**B.** Traffic on port 22  **C.** Unencrypted credentials 　　**D.** Malformed network packets |
|  | 143 | Gianna is evaluating the security of her company. The company has a number of mobile apps that were developed in house for use on COPE devices. She wants to ensure that these apps are updated as soon as an update is available. What should she ensure is being used?  **A.** Firmware OTA 　　　**B.** Push notifications  **C.** Scheduled updates 　**D.** A policy against custom firmware |
|  | 144 | Liam is concerned about the security of both COPE and BYOD devices. His company uses a lot of Android-based devices, and he is concerned about users getting administrative access and altering security features. What should he prohibit in his company?  **A.** Third-party app stores 　　**B.** Jailbreaking  **C.** Custom firmware 　　　　**D.** Rooting |
|  | 145 | Heidi works for a large company that issues various mobile devices (tablets and phones) to employees. She is concerned about unauthorized access to mobile devices. Which of the following would be the best way to mitigate that concern?  **A.** Biometrics 　　　　　　　**B.** Screen lock  **C.** Context-aware authentication **D.** Storage segmentation |
|  | 146 | You are looking for a point-to-point connection method that would allow two devices to synchronize data. The solution you pick should not be affected by EMI (electromagnetic interference) and should be usable over distances exceeding 10 meters, provided there is a line-of-sight connection. What would be the best solution?  **A.** Bluetooth 　　**B.** WiFi 　　**C.** Infrared 　　**D.** RF |
|  | 147 | You wish to use nmap to scan one of your servers, whose IP address is 192.168.1.16. The target is one of your own Windows servers. You want a scan that is the most thorough, and you are not concerned about it being detected. Which of the following would best accomplish that?  **A.** nmap -sW -sL -T1 192.168.1.16/24  **B.** nmap -sW -sT -T1 192.168.1.16  **C.** nmap -sW -sT -T5 192.168.1.16/24  **D.** nmap -sW -sT -sO -T5 192.168.1.16 |
|  | 148 | What command would produce the output shown here?    **A.** nestat –a　　 **B.** arp -a 　　**C.** arp -s 　　**D.** netstat -s |
|  | 149 | Ethan has noticed some users on his network accessing inappropriate videos. His network uses a proxy server that has content filtering with blacklisting. What is the most likely cause of this issue?  **A.** Sites not on the blacklist  **B.** Misconfigured content filtering  **C.** Misconfigured proxy server  **D.** Someone circumventing the proxy server |
|  | 150 | You are looking for tools to assist in penetration testing your network. Which of the following best describes Metasploit?  **A.** Hacking tool 　　　　　 **B.** Vulnerability scanner  **C.** Exploit framework 　　　**D.** Network scanner |
|  | 151 | Logan is responsible for enforcing security policies in his company. There are a number of policies regarding the proper configuration of public-facing servers. Which of the following would be the best way for Logan to check to see if such policies are being enforced?  **A.** Periodically audit selected servers.  **B.** Implement a configuration compliance scanning solution.  **C.** Conduct routine penetration tests of those servers.  **D.** Implement a vulnerability scanning solution. |