P-4N

1. It is MOST difficult to harden against which of the following?
A. XSS
[✓ B.] Zero-day
C. Buffer overflow
D. DoS

2. A company has experienced problems with their ISP, which has failed to meet their informally agreed upon level of service. However the business has not negotiated any additional formal agreements beyond the standard customer terms. Which of the following is the BEST document that the company should prepare to negotiate with the ISP?
A. ISA
[✓ B.] SLA
C. MOU
D. PBA

3. A company would like to implement two-factor authentication for its vulnerability management database to require system administrators to use their token and random PIN codes. Which of the following authentication services accomplishes this objective?
A. SAML
B. TACACS+
C. Kerberos
[✓ D.] RADIUS

4. A company has a corporate infrastructure where end users manage their own certificate keys. Which of the following is considered the MOST secure way to handle master keys associated with these certificates?
[✓ A.] Key escrow with key recovery
B. Trusted first party
C. Personal Identity Verification
D. Trusted third party

5. A recent audit has revealed that several users have retained permissions to systems they should no longer have rights to after being promoted or changed job positions. Which of the following controls would BEST mitigate this issue?
A. Separation of duties
[✓ B.] User account reviews
C. Group based privileges
D. Acceptable use policies

6. Ann a new security specialist is attempting to access the internet using the company's open wireless network. The wireless network is not encrypted: however, once associated, ANN cannot access the internet or other company resources. In an attempt to troubleshoot, she scans the wireless network with NMAP, discovering the only other device on the wireless network is a firewall. Which of the following BEST describes the company's wireless network solution?
[✓ A.] The company uses VPN to authenticate and encrypt wireless connections and traffic
B. The company's wireless access point is being spoofed
C. The company's wireless network is unprotected and should be configured with WPA2
D. The company is only using wireless for internet traffic so it does not need additional encryption

7. Which of the following, if implemented, would improve security of remote users by reducing vulnerabilities associated with data-intransit?
A. Full-disk encryption
[✓ B.] A virtual private network
C. A thin-client approach
D. Remote wipe capability

8. A company wants to improve its overall security posture by deploying environmental controls in its datacenter. Which of the following is considered an environmental control that can be deployed to meet this goal?
A. Full-disk encryption
B. Proximity readers
C. Hardware locks
[✓ D.] Fire suppression

9. A programmer must write a piece of code to encrypt passwords and credit card information used by an online shopping cart. The passwords must be stored using one-way encryption, while credit card information must be stored using reversible encryption.

Which of the following should be used to accomplish this task? (Choose two.)
[✓ A. SHA for passwords]
B. 3DES for passwords
C. RC4 for passwords
[✓ D. AES for credit cards]
E. MD5 for credit cards
F. HMAC for credit cards

10. A company needs to provide a secure backup mechanism for key storage in a PKI. Which of the following should the company implement?
A. Ephemeral keys
B. Steganography
[✓ C. Key escrow]
D. Digital signatures

11. A security analyst must ensure that the company's web server will not negotiate weak ciphers with connecting web browsers. Which of the following supported list of ciphers MUST the security analyst disable? (Choose three.)
A. SHA
B. AES
C. RIPMED
[✓ D. NULL]
[✓ E. DES]
[✓ F. MD5]
G. two FISH

12. A company's application is hosted at a data center. The data center provides security controls for the infrastructure. The data center provides a report identifying serval vulnerabilities regarding out of date OS patches. The company recommends the data center assumes the risk associated with the OS vulnerabilities. Which of the following concepts is being implemented?
[✓ A. Risk Transference]
B. Risk Acceptance
C. Risk Avoidance
D. Risk Deterrence

13. Which of the following cryptographic methods is most secure for a wireless access point?
A. WPA with LEAP
B. TKIP
C. WEP with PSK
[✓ D. WPA2 with PSK]

14. Which of the following is considered an environmental control?
A. Video surveillance
B. Proper lighting
[✓ C. EMI shielding]
D. Fencing

15. An attacker Joe configures his service identifier to be the same as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following Best describes this type of attack?
A. Bluejacking
B. WPS attack
[✓ C. Evil twin]
D. War driving
E. Relay attack

16. A company used a partner company to develop critical components of an application. Several employees of the partner company have been arrested for cybercrime activities. Which of the following should be done to protect the interest of the company?
[✓ A. Perform a penetration test against the application]
B. Conduct a source code review of the application
C. Perform a baseline review of the application
D. Scan the application with antivirus and anti-spyware products.

17. Which of the following is a black box testing methodology?
A. Code, function, and statement coverage review

B. Architecture and design review
C. Application hardening
[✓ D.] Penetration testing

18. A security administrator wishes to prevent certain company devices from using specific access points, while still allowing them on others. All of the access points use the same SSID and wireless password. Which of the following would be MOST appropriate in this scenario?
A. Require clients to use 802.1x with EAPOL in order to restrict access
[✓ B.] Implement a MAC filter on the desired access points
C. Upgrade the access points to WPA2 encryption
D. Use low range antennas on the access points that ne4ed to be restricted

19. An attacker Joe configures his service identifier to be as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following BEST describes this of attack?
A. Bluejacking
B. WPS attack
[✓ C.] Evil twin
D. War driving
E. Replay attack

20. Which of the following may be used with a BNC connector?
A. 10GBaseT
B. 1000BaseSX
[✓ C.] 100BaseFX
[✓ D.] 10Base2

21. A network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST information about the path taken across the network to this website?
A. Ping
B. Netstat
C. telnet
[✓ D.] tracert

22. A technician is configuring a switch to support VOPIP phones. The technician wants to ensure the phones do not require external power packs. Which of the following would allow the phones to be powered using the network connection?
[✓ A.] PoE+
B. PBX
C. PSTN
D. POTS

23. A technician reports a suspicious individual is seen walking around the corporate campus. The individual is holding a smartphone and pointing a small antenna, in order to collect SSIDs. Which of the following attacks is occurring?
A. Rogue AP
B. Evil Twin
C. Man-in-the-middle
[✓ D.] War driving

24. Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?
A. Proxy server
[✓ B.] Spam filter
C. Network firewall
D. Application firewall.

25. Which of the following should a company deploy to prevent the execution of some types of malicious code?
A. Least privilege accounts
B. Host-based firewalls
C. Intrusion Detection systems
[✓ D.] Application white listing

26. If an organization wants to implement a BYOD policy, which of the following

administrative control policy considerations MUST be addressed? (Choose two)
A. Data archiving
[✓ B.] Data ownership
C. Geo-tagging
[✓ D] Acceptable use
E. Remote wipe

27. A security technician wants to implement stringent security controls over web traffic by restricting the client source TCP ports allowed through the corporate firewall. Which of the following should the technician implement?
[✓ A.] Deny port 80 and 443 but allow proxies
B. Only allow port 80 and 443
C. Only allow ports above 1024
D. Deny ports 80 and allow port 443

28. An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups? (Choose two)
A. NAC
B. NAT
[✓ C.] Subnetting
[✓ D.] VLAN
E. DMZ
F. VPN

29. A datacenter has suffered repeated burglaries which led to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps were installed to prevent tailgating, the thieves crashed through the wall of datacenter with a vehicle after normal business hours. Which of the following options could improve the safety and security of the datacenter further? (Choose two)
A. Cipher locks
[✓ B.] CCTV
C. Escape routes
[✓ D.] K rated fencing
E. Fm200 fire suppression

30. Which of the following can take advantage of man-in-the-middle techniques to prevent data exfiltration?
[✓ A.] DNS poisoning
B. URL hijacking
C. ARP spoofing
D. HTTPS inspection

31. An administrator must select an algorithm to encrypt data at rest. Which of the following could be used?
A. RIPEMD
B. Diffie-hellman
C. ECDSA
[✓ D.] CHAP
E. Blowfish

32. RC4 is a strong encryption protocol that is general used with which of the following?
A. WPA2 CCMP
[✓ B.] PEAP
C. WEP
D. EAP-TLS

33. An outside security consultant produces a report of several vulnerabilities for a particular server. Upon further investigation, it is determine that the vulnerability reported does not apply to the platform the server is running on. Which of the following should the consultant do in order to produce more accurate results?
A. A black box test should be used to increase the validity of the scan
[✓ B.] Perform a penetration test in addition to a vulnerability scan
C. Use banner grabbing to identify the target platform
D. Use baseline reporting to determine the actual configuration

34. A programmer has allocated a 32 bit variable to store the results of an operation between two user supplied 4 byte operands. To which of the following types of attack is

this application susceptible?
A. XML injection
B. Command injection
[✓ C. Integer overflow]
D. Header manipulation

35. A security administrator is reviewing logs and notices multiple attempts to access the HVAC controls by a workstation with an IP address from the open wireless network. Which of the following would be the best way to prevent this type of attack from occurring again?
[✓ A. Implement VLANs to separate the HVAC]
B. Enable WPA2 security for the wireless network
C. Install a HIDS to protect the HVAC system
D. Enable Mac filtering for the wireless network

36. An application developer needs to allow employees to use their network credentials to access a new application being developed. Which of the following should be configured in the new application to enable this functionality?
[✓ A. LDAP]
B. ACLs
C. SNMP
D. IPSec

37. During a routine audit it is discovered that someone has been using a state administrator account to log into a seldom used server. The person used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could BEST prevent this from occurring again?
A. Credential management
[✓ B. Group policy management]
C. Acceptable use policies
D. Account expiration policies

38. A security engineer would like to analyze the effect of deploying a system without patching it to discover potential vulnerabilities. Which of the following practices would best allow for this testing while keeping the corporate network safe?
A. Perform grey box testing of the system to verify the vulnerabilities on the system
B. Utilize virtual machine snapshots to restore from compromises
[✓ C. Deploy the system in a sandbox environment on the virtual machine]
D. Create network ACLs that restrict all incoming connections to the system

39. The internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?
[✓ A. Periodic access review]
B. Group based privileges
C. Least privilege
D. Account lockout

40. In order to gain an understanding of the latest attack tools being used in the wild, an administrator puts a Unix server on the network with the root users password to set root. Which of the following best describes this technique?
A. Pharming
[✓ B. Honeypot]
C. Gray box testing
D. phishing

41. An administrator, Ann, wants to ensure that only authorized devices are connected to a switch. She decides to control access based on MAC addresses. Which of the following should be configured?
[✓ A. Implicit deny]
B. Private VLANS
C. Flood guard
D. Switch port security

42. A one time security audit revealed that employees do not have the appropriate access to system resources. The auditor is concerned with the fact that most of the accounts audited have unneeded elevated permission to sensitive resources. Which of the

following was implemented to detect this issue?
A. Continuous monitoring
[✓ B.] Account review
C. Group based privileges
D. Credential management

43. A security analyst has a sample of malicious software and needs to know what the sample in a carefully controlled and monitored virtual machine to observe the software's behavior. After the software has run, the analyst returns the virtual machines OS to a predefined know good state using what feature of virtualization?
A. Host elasticity
B. Antivirus
C. sandbox
[✓ D.] snapshots

44. Joe, the chief technical officer (CTO) is concerned that the servers and network devices may not be able to handle the growing needs of the company. He has asked his network engineer to being monitoring the performance of these devices and present statistics to management for capacity planning. Which of the following protocols should be used to this?
[✓ A.] SNMP
B. SSH
C. TLS
D. ICMP

45. A security administrator is responsible for ensuring that there are no unauthorized devices utilizing the corporate network. During a routine scan, the security administrator discovers an unauthorized device belonging to a user in the marketing department. The user is using an android phone in order to browse websites. Which of the following device attributes was used to determine that the device was unauthorized?
A. An IMEI address
B. A phone number
[✓ C.] A MAC address
D. An asset ID

46. A website is breached, exposing the usernames and MD5 password hashes of its entire user base. Many of these passwords are later cracked using rainbow tables. Which of the following actions could have helped prevent the use of rainbow tables on the password hashes?
[✓ A.] use salting when computing MD5 hashes of the user passwords
B. Use SHA as a hashing algorithm instead of MD%
C. Require SSL for all user logins to secure the password hashes in transit
D. Prevent users from using a dictionary word in their password

47. Joe a network administrator is setting up a virtualization host that has additional storage requirements. Which of the following protocols should be used to connect the device to the company SAN? (Choose Two)
[✓ A.] Fibre channel
B. SCP
[✓ C.] iSCSI
D. FDDI
E. SSL

48. A security administrator finds that an intermediate CA within the company was recently breached. The certificates held on this system were lost during the attack, and it is suspected that the attackers had full access to the system. Which of the following is the NEXT action to take in this scenario?
A. Use a recovery agent to restore the certificates used by the intermediate CA
[✓ B.] Revoke the certificate for the intermediate CA
C. Recover the lost keys from the intermediate CA key escrow
D. Issue a new certificate for the root CA

49. A recent online password audit has identified that stale accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?
A. Password length
[✓ B.] Account disablement
C. Account lockouts
D. Password complexity

50. The security administrator generates a key pair and sends one key inside a request file to a third party. The third party sends back a signed file. In this scenario, the file sent by the administrator is a:
A. CA
B. CRL
C. KEK
D. PKI
[✓ E.] CSR

51. Joe, a security technician, is configuring two new firewalls through the web on each. Each time Joe connects, there is a warning message in the browser window about the certificate being untrusted. Which of the following will allow Joe to configure a certificate for the firewall so that firewall administrators are able to connect both firewalls without experiencing the warning message?
A. Apply a permanent override to the certificate warning in the browser
B. Apply a wildcard certificate obtained from the company's certificate authority
[✓ C.] Apply a self-signed certificate generated by each of the firewalls
D. Apply a single certificate obtained from a public certificate authority

52. A company has had their web application become unavailable several times in the past few months due to increased demand. Which of the following should the company perform to increase availability?
A. Implement a web application firewall to prevent DDoS attacks'
B. Configure the firewall to work with the IPS to rate limit customer requests
[✓ C.] Implement a load balancer to distribute traffic based on back end server utilization
D. Configure the web server to detect race conditions and automatically restart the web services

53. A system administrator wants to prevent password compromises from offline password attacks. Which of the following controls should be configured to BEST accomplish this task? (Choose two.)
A. Password reuse
[✓ B.] Password length
[✓ C.] Password complexity
~~D.~~ Password history
~~E.~~ Account lockouts

54. A company recently experienced several security breaches that resulted in confidential data being infiltrated form the network. The forensic investigation revealed that the data breaches were caused by an insider accessing files that resided in shared folders who then encrypted the data and sent it to contacts via third party email. Management is concerned that other employees may also be sending confidential files outside of the company to the same organization. Management has requested that the IT department implement a solution that will allow them to:

Track access and sue of files marked confidential;
Provide documentation that can be sued for investigations;
Prevent employees from sending confidential data via secure third party email; and
Identify other employees that may be involved in these activities.

Which of the following would be the best choice to implement to meet the above requirements?
A. Web content filtering capable of inspe4cting and logging SSL traffic used by third party webmail providers
B. Full disk encryption on all computers with centralized event logging and monitoring enabled
C. Host based firewalls with real time monitoring and logging enabled
[✓ D.] Agent-based DLP software with correlations and logging enabled

data loss prevention

55. Which of the following BEST describes malware that tracks a user's web browsing habits and injects the attacker's advertisements into unrelated web pages? (Choose two.)
A. Logic bomb
B. Backdoor
C. Ransomware
[✓ D.] Adware
E. Botnet
[✓ F.] Spyware

56. The chief security officer (CSO) has issued a new policy to restrict generic or shared accounts on company systems. Which of the following sections of the policy

requirements will have the most impact on generic and shared accounts?
A. Account lockout
B. Password length
[✓ C. Concurrent logins]
D. Password expiration

57. Joe an end user has received a virus detection warning. Which of the following is the first course of action that should be taken?
A. Recovery
[✓ B. Reporting]
C. Remediation
D. Identification

58. A company has several public conference room areas with exposed network outlets. In the past, unauthorized visitors and vendors have used the outlets for internet access. The help desk manager does not want the outlets to be disabled due to the number of training sessions in the conference room and the amount of time it takes to get the ports either patched in or enabled. Which of the following is the best option for meeting this goal?
A. Flood guards
B. Port security
[✓ C. 802.1x]
D. Loop protection
E. IPSec

59. An attacker unplugs the access point at a coffee shop. The attacker then runs software to make a laptop look like an access point and advertises the same network as the coffee shop normally does. Which of the following describes this type of attack?
A. IV
B. Xmas
C. Packet sniffing
[✓ D. Evil twin]
E. Rouge AP

60. A network administrator argues that WPA2 encryption is not needed, as MAC filtering is enabled on the access point. Which of the following would show the administrator that wpa2 is also needed?
A. Deploy an evil twin with mac filtering
B. Flood access point with random mac addresses
[✓ C. Sniff and clone a mac address]
D. DNS poison the access point

61. A security director has contracted an outside testing company to evaluate the security of a newly developed application. None of the parameters or internal workings of the application have been provided to the testing company prior to the start of testing. The testing company will be using:
A. Gray box testing
B. Active control testing
C. White box testing
[✓ D. Black box testing]

62. While preparing for an audit a security analyst is reviewing the various controls in place to secure the operation of financial processes within the organization. Based on the pre assessment report, the department does not effectively maintain a strong financial transaction control environment due to conflicting responsibilities held by key personnel. If implemented, which of the following security concepts will most effectively address the finding?
A. Least privilege
[✓ B. Separation of duties]
C. Time-based access control
D. Dual control

63. A Chief Privacy Officer, Joe, is concerned that employees are sending emails to addresses outside of the company that contain PII. He asks that the security technician to implement technology that will mitigate this risk. Which of the following would be the best option?
[✓ A. DLP]
B. HIDS
C. Firewall

D. Web content filtering

64. The key management organization has implemented a key escrowing function. Which of the following technologies can provide protection for the PKI's escrowed keys?
~~A.~~ CRL
B. OCSP
C. TPM
[✓ D.] HSM Hard ware Security module

65. Which of the following are unique to white box testing methodologies? (Choose two)
[✓ A.] Application program interface API testing
B. Bluesnarfing
C. External network penetration testing
[✓ D.] Function, statement and code coverage
E. Input fuzzing

66. A technician installed two ground plane antennae on 802.11n bridges connecting two buildings 500 feet apart. After configuring both radios to work at 2.4ghz and implementing the correct configuration, connectivity tests between the two buildings are unsuccessful. Which of the following should the technician do to resolve the connectivity problem?
A. Substitute wireless bridges for wireless access points
B. Replace the 802.11n bridges with 802.11ac bridges
C. Configure both bridges to use 5GHz instead of 2.4GHz
[✓ D.] Replace the current antennae with Yagi antennae

67. A company has had several security incidents in the past six months. It appears that the majority of the incidents occurred on systems with older software on development workstations. Which of the following should be implemented to help prevent similar incidents in the future?
A. Peer code review
B. Application whitelisting
[✓ C.] Patch management
D. Host-based firewall

68. A router was shut down as a result of a DoS attack. Upon review of the router logs, it was determined that the attacker was able to connect to the router using a console cable to complete the attack. Which of the following should have been implemented on the router to prevent this attack? (Choose two)
A. IP ACLs should have been enabled on the console port on the router
[✓ B.] Console access to the router should have been disabled
C. Passwords should have been enabled on the virtual terminal interfaces on the router
D. Virtual terminal access to the router should have been disabled
[✓ E.] Physical access to the router should have been restricted

69. A systems administrator is configuring a new file server and has been instructed to configure writeable to by the department manager, and read only for the individual employee. Which of the following is the name for the access control methodology used?
A. Duty separation
B. Mandatory
C. Least privilege
[✓ D.] Role-based

70. An administrator is implementing a security control that only permits the execution of allowed programs. Which of the following are cryptography concepts that should be used to identify the allowed programs? (Choose two.)
[✓ A.] Digital signatures
[✓ B.] Hashing
C. Asymmetric encryption
D. OpenID
~~E.~~ Key escrow

71. While responding to an incident on a Linux server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?
[✓ A.] Lsof
B. Tcpdump
C. Top
D. Ifconfig

72. A bank Chief Information Security Officer (CISO) is responsible for a mobile banking platform that operates natively on iOS and Android. Which of the following security controls helps protect the associated publicly accessible API endpoints?
A. Mobile device management
B. Jailbreak detection
C. Network segmentation
[✓ D. Application firewalls]

73. A company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a:
[✓ A. Vulnerability assessment]
B. White box test
C. Penetration test
D. Peer review

74. Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is Joe attempting to complete?
A. Black hat testing
[✓ B. Vulnerability scanning]
C. Black box testing
D. Penetration testing

75. A classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?
~~A.~~ The maximum-mac settings of the ports should be set to zero
[✓ B. The maximum-mac settings of the ports should be set to one]
C. The maximum-mac settings of the ports should be set to two
D. The maximum mac settings of the ports should be set to three

76. A security administrator implements a web server that utilizes an algorithm that requires other hashing standards to provide data integrity. Which of the following algorithms would meet the requirement?
A. SHA
B. MD5
C. RIPEMD
[✓ D. HMAC]

77. Which of the following is the FIRST step in a forensics investigation when a breach of a client's workstation has been confirmed?
A. Transport the workstation to a secure facility
B. Analyze the contents of the hard drive
C. Restore any deleted files and / or folders
[✓ D. Make a bit-for-bit copy of the system]

78. Company XYZ's laptops was recently stolen from a user which led to the exposure if confidential information. Which of the following should the security team implement on laptops to prevent future compromise?
A. Cipher locks
B. Strong passwords
C. Biometrics
[✓ D. Full Disk Encryption]

79. A wireless site survey has been performed at a company. One of the results of the report is that the wireless signal extends too far outside the building. Which of the following security issues could occur as a result of this finding?
A. Excessive wireless access coverage
B. Interference with nearby access points
C. Exhaustion of DHCP address pool
[✓ D. Unauthorized wireless access]

80. Which of the following is a software vulnerability that can be avoided by using

input validation?
[✓ A.] Buffer overflow
B. Application fuzzing
[✓ C.] Ininput
D. Error handling

81. A university has a building that holds the power generators for the entire campus. A risk assessment was completed for the university and the generator building was labeled as a high risk. Fencing and lighting was installed to reduce risk. Which of the following security goals would this meet?
A. Load balancing
B. Non-repudiation
C. Disaster recovery
[✓ D.] Physical security

82. Log file analysis on a router reveals several unsuccessful telnet attempts to the virtual terminal (VTY) lines. Which of the following represents the BEST configuration used in order to prevent unauthorized remote access while maintaining secure availability for legitimate users?
[✓ A.] Disable telnet access to the VTY lines, enable SHH access to the VTY lines with RSA encryption
B. Disable both telnet and SSH access to the VTY lines, requiring users to log in using HTTP
C. Disable telnet access to the VTY lines, enable SHH access to the VTY lines with PSK encryption
D. Disable telnet access to the VTY lines, enable SSL access to the VTY lines with RSA encryption

83. Four weeks ago a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff begins to spread, the IDS alerted the network administrator that access to sensitive client files had risen for above normal. Which of the following kind of IDS is in use?
A. Protocol based
B. Heuristic based
C. Signature based
[✓ D.] Anomaly based

84. A BYOD policy in which employees are able to access the wireless guest network is in effect in an organization. Some users however are using the Ethernet port in personal laptops to the wired network. Which of the following could an administrator use to ensure that unauthorized devices are not allowed to access the wired network?
A. VLAN access rules configured to reject packets originating from unauthorized devices
B. Router access lists configured to block the IP addresses of unauthorized devices
C. Firewall rules configured to block the MAC addresses of unauthorized devices
[✓ D.] Port security configured shut down the port when unauthorized devices connect

85. During an office move a sever containing the employee information database will be shut down and transported to a new location. Which of the following would BEST ensure the availability of the employee database should happen to the server during the move?
A. The contents of the database should be encrypted; the encryption key should be stored off-site
B. A hash of the database should be taken and stored on an external drive prior to the move
C. The database should be placed on a drive that consists of a RAID array prior to the move
[✓ D.] A backup of the database should be stored on an external hard drive prior to the move

86. Which of the following is primarily used to provide fault tolerance at the application level? (Choose two.)
A. Load balancing
[✓ B.] RAID array
C. RAID 6
[✓ D.] Server clustering
E. JBOD array

87. A security administrator would like the corporate webserver to select perfect forward secrecy ciphers first. Which of the following cipher suites should the administrator select to accomplish this goal?
A. DH-DSS-CAMELLA256-SHA

[✓ B. ECDHE-RSA-AES1280SHA]
C. DH-RSA-AES128-SHA256
D. ADH-AES256-SHA

88. An administrator is having difficulty configuring WPA2 Enterprise using EAP-PEAP-MSCHAPv2. The administrator has configured the wireless access points properly, and has configured policies on the RADIUS server and configured settings on the client computers. Which of the following is missing?
[✓ A. Client certificates are needed]
B. A third party LEAP client must be installed
C. A RADIUS server certificate is needed
D. The use of CCMP rather than TKIP

89. A business has recently adopted a policy allowing employees to use personal cell phones and tablets to access company email accounts while out of the office. Joe, an employee, was using a personal cell phone for email access and was recently terminated. It is suspected that Joe saved confidential client emails on his personal cell phone. Joe claims that the data on the phone is completely personal and refuse to allow the company access to inspect the cell phone. Which of the following is the MOST likely cause of this dispute?
A. Onboarding procedures
B. Fair use policy
[✓ C. Device ownership]
D. User acceptance

90. Mobile tablets are used by employees on the sales floor to access customer data. Ann a customer recently reported that another customer was able to access her personal information on the tablet after the employee left the area. Which of the following would BEST prevent these issues from reoccurring?
[✓ A. Screen Locks]
B. Full-device encryption
C. Application control
D. Asset tracking

91. Which of the following metrics is important for measuring the extent of data required during backup and recovery?
A. MOU
B. ARO
C. ALE
[✓ D. RPO] Recovery Pt Object

92. Which of the following can be used to ensure that sensitive records stored on a backend server can only be accessed by a front end server with the appropriate record key?
A. File encryption
B. Storage encryption
[✓ C. Database encryption]
D. Full disk encryption

93. Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?
A. Access control list
[✓ B. 802.1X]
C. Port security
D. Load balancers

94. A company has identified a watering hole attack. Which of the following Best describes this type of attack?
A. Emails are being spoofed to look like they are internal emails
B. A cloud storage site is attempting to harvest user IDS and passwords
C. An online news site is hosting ads in iframes from another site
[✓ D. A local restaurant chains online menu is hosting malicious code]

95. A security manager is discussing change in the security posture of the network, if a proposed application is approved for deployment. Which of the following is the MOST important the security manager must rely upon to help make this determination?
A. Ports used by new application
[✓ B. Protocols/services used by new application]
C. Approved configuration items

D. Current baseline configuration

96. Joe the system administrator has noticed an increase in network activity from outside sources. He wishes to direct traffic to avoid possible penetration while heavily monitoring the traffic with little to no impact on the current server load. Which of the following would be BEST course of action?
A. Apply an additional firewall ruleset on the user PCs.
[✓ B.] Configure several servers into a honeynet
C. Implement an IDS to protect against intrusion
D. Enable DNS logging to capture abnormal traffic

97. An assessment too reports that the company's web server may be susceptible to remote buffer overflow. The web server administrator insists that the finding is a false positive. Which of the following should the administrator do to verify if this is indeed a false positive?
A. Use a banner grabbing tool or B
B. Run a vulnerability scan
C. Enforce company policies
[✓ D.] Perform a penetration test

98. The sales force in an organization frequently travel to remote sites and requires secure access to an internal server with an IP address of 192.168.0.220. Assuming services are using default ports, which of the following firewall rules would accomplish this objective? (Choose Two)
A. Permit TCP 20 any 192.168.0.200
B. Permit TCP 21 any 192.168.0.200
[✓ C.] Permit TCP 22 any 192.168.0.200
D. Permit TCP 110 any 192.168.0.200
E. Permit TCP 139 any 192.168.0.200
[✓ F.] Permit TCP 3389 any 192.168.0.200

99. Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?
A. Deploy a HIDS suite on the users' computer to prevent application installation
B. Maintain the baseline posture at the highest OS patch level
C. Enable the pop-up blockers on the user's browsers to prevent malware
[✓ D.] Create an approved application list and block anything not on it

100. Which of the following will provide data encryption, key management and secure application launching?
A. TKIP
[✓ B.] HSM
C. EFS
D. DLP

MDA

olive Hatches

- JIRA

- Testing As Users Space

? - Govt owned SDK

TS: Jacob

Dane

David

Nerve / DSIL