

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.)

50 A. SHA for passwords
51 B. 3DES for passwords
52 C. RC4 for passwords
53 D. AES for credit cards
54 E. MD5 for credit cards
55 F. HMAC for credit cards
56

57 10. A company needs to provide a secure backup mechanism for key storage in a PKI.
Which of the following should the company implement?

58 A. Ephemeral keys
59 B. Steganography
60 C. Key escrow
61 D. Digital signatures
62

63 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.)

64 A. SHA
65 B. AES
66 C. RIPMED
67 D. NULL
68 E. DES
69 F. MD5
70 G. two FISH
71

72 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
several 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?

73 A. Risk Transference
74 B. Risk Acceptance
75 C. Risk Avoidance
76 D. Risk Deterrence
77

78 13. Which of the following cryptographic methods is most secure for a wireless access
point?

79 A. WPA with LEAP
80 B. TKIP
81 C. WEP with PSK
82 D. WPA2 with PSK
83

84 14. Which of the following is considered an environmental control?

85 A. Video surveillance
86 B. Proper lighting
87 C. EMI shielding
88 D. Fencing
89

90 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?

91 A. Bluejacking
92 B. WPS attack
93 C. Evil twin
94 D. War driving
95 E. Relay attack
96

97 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?

98 A. Perform a penetration test against the application
99 B. Conduct a source code review of the application
100 C. Perform a baseline review of the application
101 D. Scan the application with antivirus and anti-spyware products.
102

103 17. Which of the following is a black box testing methodology?

104 A. Code, function, and statement coverage review

105 B. Architecture and design review
106 C. Application hardening
107 D. Penetration testing
108
109 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?
110 A. Require clients to use 802.1x with EAPOL in order to restrict access
111 B. Implement a MAC filter on the desired access points
112 C. Upgrade the access points to WPA2 encryption
113 D. Use low range antennas on the access points that needed to be restricted
114
115 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?
116 A. Bluejacking
117 B. WPS attack
118 C. Evil twin
119 D. War driving
120 E. Replay attack
121
122 20. Which of the following may be used with a BNC connector?
123 A. 10GBaseT
124 B. 1000BaseSX
125 C. 100BaseFX
126 D. 10Base2
127
128 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?
129 A. Ping
130 B. Netstat
131 C. telnet
132 D. traceroute
133
134 22. A technician is configuring a switch to support VOIP 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?
135 A. PoE+
136 B. PBX
137 C. PSTN
138 D. POTS
139
140 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?
141 A. Rogue AP
142 B. Evil Twin
143 C. Man-in-the-middle
144 D. War driving
145
146 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?
147 A. Proxy server
148 B. Spam filter
149 C. Network firewall
150 D. Application firewall.
151
152 25. Which of the following should a company deploy to prevent the execution of some
types of malicious code?
153 A. Least privilege accounts
154 B. Host-based firewalls
155 C. Intrusion Detection systems
156 D. Application white listing
157
158 26. If an organization wants to implement a BYOD policy, which of the following

administrative control policy considerations MUST be addressed? (Choose two)

159 A. Data archiving
160 B. Data ownership
161 C. Geo-tagging
162 D. Acceptable use
163 E. Remote wipe
164

165 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?

166 A. Deny port 80 and 443 but allow proxies
167 B. Only allow port 80 and 443
168 C. Only allow ports above 1024
169 D. Deny ports 80 and allow port 443
170

171 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)

172 A. NAC
173 B. NAT
174 C. Subnetting
175 D. VLAN
176 E. DMZ
177 F. VPN
178

179 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)

180 A. Cipher locks
181 B. CCTV
182 C. Escape routes
183 D. K rated fencing
184 E. Fm200 fire suppression
185

186 30. Which of the following can take advantage of man-in-the-middle techniques to prevent data exfiltration?

187 A. DNS poisoning
188 B. URL hijacking
189 C. ARP spoofing
190 D. HTTPS inspection
191

192 31. An administrator must select an algorithm to encrypt data at rest. Which of the following could be used?

193 A. RIPEMD
194 B. Diffie-hellman
195 C. ECDSA
196 D. CHAP
197 E. Blowfish
198

199 32. RC4 is a strong encryption protocol that is general used with which of the following?

200 A. WPA2 CCMP
201 B. PEAP
202 C. WEP
203 D. EAP-TLS
204

205 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?

206 A. A black box test should be used to increase the validity of the scan
207 B. Perform a penetration test in addition to a vulnerability scan
208 C. Use banner grabbing to identify the target platform
209 D. Use baseline reporting to determine the actual configuration
210

211 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?

212 A. XML injection
213 B. Command injection
214 C. Integer overflow
215 D. Header manipulation
216

217 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?

218 A. Implement VLANs to separate the HVAC
219 B. Enable WPA2 security for the wireless network
220 C. Install a HIDS to protect the HVAC system
221 D. Enable Mac filtering for the wireless network
222

223 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?

224 A. LDAP
225 B. ACLs
226 C. SNMP
227 D. IPSec
228

229 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?

230 A. Credential management
231 B. Group policy management
232 C. Acceptable use policies
233 D. Account expiration policies
234

235 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?

236 A. Perform grey box testing of the system to verify the vulnerabilities on the system
237 B. Utilize virtual machine snapshots to restore from compromises
238 C. Deploy the system in a sandbox environment on the virtual machine
239 D. Create network ACLs that restrict all incoming connections to the system
240

241 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?

242 A. Periodic access review
243 B. Group based privileges
244 C. Least privilege
245 D. Account lockout
246

247 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?

248 A. Pharming
249 B. Honeytrap
250 C. Gray box testing
251 D. phishing
252

253 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?

254 A. Implicit deny
255 B. Private VLANs
256 C. Flood guard
257 D. Switch port security
258

259 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?

260 A. Continuous monitoring
261 B. Account review
262 C. Group based privileges
263 D. Credential management
264

265 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?

266 A. Host elasticity
267 B. Antivirus
268 C. sandbox
269 D. snapshots
270

271 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?

272 A. SNMP
273 B. SSH
274 C. TLS
275 D. ICMP
276

277 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?

278 A. An IMEI address
279 B. A phone number
280 C. A MAC address
281 D. An asset ID
282

283 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?

284 A. use salting when computing MD5 hashes of the user passwords
285 B. Use SHA as a hashing algorithm instead of MD5
286 C. Require SSL for all user logins to secure the password hashes in transit
287 D. Prevent users from using a dictionary word in their password
288

289 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)

290 A. Fibre channel
291 B. SCP
292 C. iSCSI
293 D. FDDI
294 E. SSL
295

296 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?

297 A. Use a recovery agent to restore the certificates used by the intermediate CA
298 B. Revoke the certificate for the intermediate CA
299 C. Recover the lost keys from the intermediate CA key escrow
300 D. Issue a new certificate for the root CA
301

302 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?

303 A. Password length
304 B. Account disablement
305 C. Account lockouts
306 D. Password complexity
307

308 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:

309 A. CA
310 B. CRL
311 C. KEK
312 D. PKI
313 E. CSR
314

315 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?

316 A. Apply a permanent override to the certificate warning in the browser
317 B. Apply a wildcard certificate obtained from the company's certificate authority
318 C. Apply a self-signed certificate generated by each of the firewalls
319 D. Apply a single certificate obtained from a public certificate authority
320

321 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?

322 A. Implement a web application firewall to prevent DDoS attacks'
323 B. Configure the firewall to work with the IPS to rate limit customer requests
324 C. Implement a load balancer to distribute traffic based on back end server utilization
325 D. Configure the web server to detect race conditions and automatically restart the web
services
326

327 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.)

328 A. Password reuse
329 B. Password length
330 C. Password complexity
331 D. Password history
332 E. Account lockouts
333

334 54. A company recently experienced several security breaches that resulted in
confidential data being infiltrated from 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:

335 Track access and sue of files marked confidential;
336 Provide documentation that can be sued for investigations;
337 Prevent employees from sending confidential data via secure third party email; and
338 Identify other employees that may be involved in these activities.
339

340 Which of the following would be the best choice to implement to meet the above
requirements?

341 A. Web content filtering capable of inspe4cting and logging SSL traffic used by third
party webmail providers
342 B. Full disk encryption on all computers with centralized event logging and monitoring
enabled
343 C. Host based firewalls with real time monitoring and logging enabled
344 D. Agent-based DLP software with correlations and logging enabled
345

346 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.)

347 A. Logic bomb
348 B. Backdoor
349 C. Ransomware
350 D. Adware
351 E. Botnet
352 F. Spyware
353

354 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?

355 A. Account lockout
356 B. Password length
357 C. Concurrent logins
358 D. Password expiration
359

360 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?

361 A. Recovery
362 B. Reporting
363 C. Remediation
364 D. Identification
365

366 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?

367 A. Flood guards
368 B. Port security
369 C. 802.1x
370 D. Loop protection
371 E. IPSec
372

373 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?

374 A. IV
375 B. Xmas
376 C. Packet sniffing
377 D. Evil twin
378 E. Rouge AP
379

380 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?

381 A. Deploy an evil twin with mac filtering
382 B. Flood access point with random mac addresses
383 C. Sniff and clone a mac address
384 D. DNS poison the access point
385

386 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:

387 A. Gray box testing
388 B. Active control testing
389 C. White box testing
390 D. Black box testing
391

392 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?

393 A. Least privilege
394 B. Separation of duties
395 C. Time-based access control
396 D. Dual control
397

398 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?

399 A. DLP
400 B. HIDS
401 C. Firewall

402 D. Web content filtering
403
404 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?
405 A. CRL
406 B. OCSP
407 C. TPM
408 D. HSM
409
410 65. Which of the following are unique to white box testing methodologies? (Choose two)
411 A. Application program interface API testing
412 B. Bluesnarfing
413 C. External network penetration testing
414 D. Function, statement and code coverage
415 E. Input fuzzing
416
417 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?
418 A. Substitute wireless bridges for wireless access points
419 B. Replace the 802.11n bridges with 802.11ac bridges
420 C. Configure both bridges to use 5GHz instead of 2.4GHz
421 D. Replace the current antennae with Yagi antennae
422
423 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?
424 A. Peer code review
425 B. Application whitelisting
426 C. Patch management
427 D. Host-based firewall
428
429 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)
430 A. IP ACLs should have been enabled on the console port on the router
431 B. Console access to the router should have been disabled
432 C. Passwords should have been enabled on the virtual terminal interfaces on the router
433 D. Virtual terminal access to the router should have been disabled
434 E. Physical access to the router should have been restricted
435
436 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?
437 A. Duty separation
438 B. Mandatory
439 C. Least privilege
440 D. Role-based
441
442 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.)
443 A. Digital signatures
444 B. Hashing
445 C. Asymmetric encryption
446 D. OpenID
447 E. Key escrow
448
449 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?
450 A. Lsof
451 B. Tcpdump
452 C. Top
453 D. Ifconfig

454
455 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?
456 A. Mobile device management
457 B. Jailbreak detection
458 C. Network segmentation
459 D. Application firewalls
460
461 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:
462 A. Vulnerability assessment
463 B. White box test
464 C. Penetration test
465 D. Peer review
466
467 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?
468 A. Black hat testing
469 B. Vulnerability scanning
470 C. Black box testing
471 D. Penetration testing
472
473 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?
474 A. The maximum-mac settings of the ports should be set to zero
475 B. The maximum-mac settings of the ports should be set to one
476 C. The maximum-mac settings of the ports should be set to two
477 D. The maximum mac settings of the ports should be set to three
478
479 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?
480 A. SHA
481 B. MD5
482 C. RIPEMD
483 D. HMAC
484
485 77. Which of the following is the FIRST step in a forensics investigation when a breach
of a client's workstation has been confirmed?
486 A. Transport the workstation to a secure facility
487 B. Analyze the contents of the hard drive
488 C. Restore any deleted files and / or folders
489 D. Make a bit-for-bit copy of the system
490
491 78. Company XYZ's laptops was recently stolen from a user which led to the exposure of
confidential information. Which of the following should the security team implement on
laptops to prevent future compromise?
492 A. Cipher locks
493 B. Strong passwords
494 C. Biometrics
495 D. Full Disk Encryption
496
497 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?
498 A. Excessive wireless access coverage
499 B. Interference with nearby access points
500 C. Exhaustion of DHCP address pool
501 D. Unauthorized wireless access
502
503 80. Which of the following is a software vulnerability that can be avoided by using

input validation?

504 A. Buffer overflow
505 B. Application fuzzing
506 C. Ininput
507 D. Error handling
508

509 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?

510 A. Load balancing
511 B. Non-repudiation
512 C. Disaster recovery
513 D. Physical security
514

515 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?

516 A. Disable telnet access to the VTY lines, enable SSH access to the VTY lines with RSA encryption
517 B. Disable both telnet and SSH access to the VTY lines, requiring users to log in using HTTP
518 C. Disable telnet access to the VTY lines, enable SSH access to the VTY lines with PSK encryption
519 D. Disable telnet access to the VTY lines, enable SSL access to the VTY lines with RSA encryption
520

521 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?

522 A. Protocol based
523 B. Heuristic based
524 C. Signature based
525 D. Anomaly based
526

527 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?

528 A. VLAN access rules configured to reject packets originating from unauthorized devices
529 B. Router access lists configured to block the IP addresses of unauthorized devices
530 C. Firewall rules configured to block the MAC addresses of unauthorized devices
531 D. Port security configured shut down the port when unauthorized devices connect
532

533 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?

534 A. The contents of the database should be encrypted; the encryption key should be stored off-site
535 B. A hash of the database should be taken and stored on an external drive prior to the move
536 C. The database should be placed on a drive that consists of a RAID array prior to the move
537 D. A backup of the database should be stored on an external hard drive prior to the move
538

539 86. Which of the following is primarily used to provide fault tolerance at the application level? (Choose two.)

540 A. Load balancing
541 B. RAID array
542 C. RAID 6
543 D. Server clustering
544 E. JBOD array
545

546 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?

547 A. DH-DSS-CAMELLA256-SHA

548 B. ECDHE-RSA-AES1280SHA
549 C. DH-RSA-AES128-SHA256
550 D. ADH-AES256-SHA
551
552 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?
553 A. Client certificates are needed
554 B. A third party LEAP client must be installed
555 C. A RADIUS server certificate is needed
556 D. The use of CCMP rather than TKIP
557
558 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?
559 A. Onboarding procedures
560 B. Fair use policy
561 C. Device ownership
562 D. User acceptance
563
564 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?
565 A. Screen Locks
566 B. Full-device encryption
567 C. Application control
568 D. Asset tracking
569
570 91. Which of the following metrics is important for measuring the extent of data
required during backup and recovery?
571 A. MOU
572 B. ARO
573 C. ALE
574 D. RPO
575
576 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?
577 A. File encryption
578 B. Storage encryption
579 C. Database encryption
580 D. Full disk encryption
581
582 93. Which of the following would be used to allow a subset of traffic from a wireless
network to an internal network?
583 A. Access control list
584 B. 802.1X
585 C. Port security
586 D. Load balancers
587
588 94. A company has identified a watering hole attack. Which of the following Best
describes this type of attack?
589 A. Emails are being spoofed to look like they are internal emails
590 B. A cloud storage site is attempting to harvest user IDS and passwords
591 C. An online news site is hosting ads in iframes from another site
592 D. A local restaurant chains online menu is hosting malicious code
593
594 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?
595 A. Ports used by new application
596 B. Protocols/services used by new application
597 C. Approved configuration items

598 D. Current baseline configuration
599
600 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?
601 A. Apply an additional firewall ruleset on the user PCs.
602 B. Configure several servers into a honeynet
603 C. Implement an IDS to protect against intrusion
604 D. Enable DNS logging to capture abnormal traffic
605
606 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?
607 A. Use a banner grabbing tool
608 B. Run a vulnerability scan
609 C. Enforce company policies
610 D. Perform a penetration test
611
612 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)
613 A. Permit TCP 20 any 192.168.0.200
614 B. Permit TCP 21 any 192.168.0.200
615 C. Permit TCP 22 any 192.168.0.200
616 D. Permit TCP 110 any 192.168.0.200
617 E. Permit TCP 139 any 192.168.0.200
618 F. Permit TCP 3389 any 192.168.0.200
619
620 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?
621 A. Deploy a HIDS suite on the users' computer to prevent application installation
622 B. Maintain the baseline posture at the highest OS patch level
623 C. Enable the pop-up blockers on the user's browsers to prevent malware
624 D. Create an approved application list and block anything not on it
625
626 100. Which of the following will provide data encryption, key management and secure
application launching?
627 A. TKIP
628 B. HSM
629 C. EFS
630 D. DLP
631