

- 1 1. The Chief Security Officer (CSO) for a datacenter in a hostile environment, is concerned about protecting the facility from car bomb attacks. Which of the following BEST would protect the building from this threat? (Choose two.)
- 2 A. Dogs
3 B. Fencing
4 C. CCTV
5 D. Guards
6 E. Bollards
7 F. Lighting
8
- 9 2. Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?
- 10 A. Malicious users can exploit local corporate credentials with their social media credentials
11 B. Changes to passwords on the social media site can be delayed from replicating to the company
12 C. Data loss from the corporate servers can create legal liabilities with the social media site
13 D. Password breaches to the social media affect the company application as well
14
- 15 3. A corporation has experienced several media leaks of proprietary data on various web forums. The posts were made during business hours and it is believed that the culprit is posting during work hours from a corporate machine. The Chief Information Officer (CIO) wants to scan internet traffic and keep records for later use in legal proceedings once the culprit is found. Which of the following provides the BEST solution?
- 16 A. Protocol analyzer
17 B. NIPS
18 C. Proxy server
19 D. HIDS
20
- 21 4. The security administrator runs an rpm verify command which records the MD5 sum, permissions, and timestamp of each file on the system. The administrator saves this information to a separate server. Which of the following describes the procedure the administrator has performed?
- 22 A. Host software base-lining
23 B. File snapshot collection
24 C. TPM
25 D. ROMDB verification
26
- 27 5. Users are trying to communicate with a network but are unable to do so. A network administrator sees connection attempts on port 20 from outside IP addresses that are being blocked. How can the administrator resolve this?
- 28 A. Enable stateful FTP on the firewall
29 B. Enable inbound SSH connections
30 C. Enable NETBIOS connections in the firewall
31 D. Enable HTTPS on port 20
32
- 33 6. In order to enter a high-security datacenter, users are required to speak the password into a voice recognition system. Ann a member of the sales department over hears the password and upon speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?
- 34 A. An authentication factor
35 B. Discretionary access
36 C. Time of day restrictions
37 D. Least privilege restrictions
38
- 39 7. Given the following list of corporate access points, which of the following attacks is MOST likely underway if the company wireless network uses the same wireless hardware throughout?
- 40 MAC SID
41 00:01:AB:FA:CD:34Corporate AP
42 00:01:AB:FA:CD:35Corporate AP
43 00:01:AB:FA:CD:36Corporate AP
44 00:01:AB:FA:CD:37Corporate AP
45 00:01:AB:FA:CD:34Corporate AP
46
- 47 A. Packet sniffing

- 48 B. Evil Twin
49 C. WPS attack
50 D. Rogue access point
51
- 52 8. A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?
53 A. SMTP
54 B. iSCSI
55 C. SNMP
56 D. IPSec
57
- 58 9. Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?
59 A. RAID
60 B. Tape Backup
61 C. Load Balancing
62 D. Clustering
63
- 64 10. Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?
65 A. OS hardening
66 B. Application control
67 C. Virtualization
68 D. Sandboxing
69
- 70 11. Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?
71 A. Preshared keys
72 B. Ticket exchange
73 C. Initialization vectors
74 D. Certificate exchange
75
- 76 12. A new security policy being implemented requires all email within the organization be digitally signed by the author using PGP. Which of the following would needs to be created for each user?
77 A. A certificate authority
78 B. A key escrow
79 C. A trusted key
80 D. A public and private key
81
- 82 13. Which of the following authentication provides users XML for authorization and authentication?
83 A. Kerberos
84 B. LDAP
85 C. RADIUS
86 D. SAML
87
- 88 14. A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?
89 A. MDM
90 B. IDS
91 C. DLP
92 D. HIPS
93
- 94 15. The pre-sales engineering team needs to quickly provide accurate and up-to-date information to potential clients. This information includes design specifications and engineering data that is developed and stored using numerous applications across the enterprise. Which of the following authentication technique is MOST appropriate?
95 A. Common access cards
96 B. TOTP
97 C. Single sign-on
98 D. HOTP
99
- 100 16. A network engineer is configuring a VPN tunnel connecting a company's network to a business partner. Which of the following protocols should be used for key exchange?

- 101 A. SHA-1
102 B. RC4
103 C. Blowfish
104 D. Diffie-Hellman
105
- 106 17. Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?
107 A. Hybrid Cloud
108 B. Private cloud
109 C. Community cloud
110 D. Community cloud
111 E. Public cloud
112
- 113 18. The database server used by the payroll system crashed at 3 PM and payroll is due at 5 PM. Which of the following metrics is MOST important in this instance?
114 A. ARO
115 B. SLE
116 C. MTTR
117 D. MTBF
118
- 119 19. Which of the following is an attack designed to activate based on time?
120 A. Logic Bomb
121 B. Backdoor
122 C. Trojan
123 D. Rootkit
124
- 125 20. A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?
126 A. Disable unnecessary services on servers
127 B. Disable unused accounts on servers and network devices
128 C. Implement password requirements on servers and network devices
129 D. Enable auditing on event logs
130
- 131 21. Which of the following documents outlines the responsibility of both participants in an agreement between two organizations?
132 A. RFC
133 B. MOU
134 C. RFQ
135 D. SLA
136
- 137 22. Users in the HR department were recently informed that they need to implement a user training and awareness program which is tailored to their department. Which of the following types of training would be the MOST appropriate for this department?
138 A. Handing PII
139 B. Risk mitigation
140 C. Input validation
141 D. Hashing
142
- 143 23. Which of the following incident response plan steps would MOST likely engage business professionals with the security team to discuss changes to existing procedures?
144 A. Recovery
145 B. Incident identification
146 C. Isolation / quarantine
147 D. Lessons learned
148 E. Reporting
149
- 150 24. A company is starting to allow employees to use their own personal devices without centralized management. Employees must contact IT to have their devices configured to use corporate email; access is also available to the corporate cloud-based servers. Which of the following is the BEST policy to implement under these circumstances?
151 A. Acceptable use policy
152 B. Security policy
153 C. Group policy
154 D. Business Agreement policy
155
- 156 25. Which of the following BEST explains Platform as a Service?
157 A. An external entity that provides a physical or virtual instance of an installed

- operating system
158 B. A third party vendor supplying support services to maintain physical platforms and servers
159 C. An external group providing operating systems installed on virtual servers with web applications
160 D. An internal group providing physical server instances without installed operating systems or support
161
162 26. One of the senior managers at a company called the help desk to report to report a problem. The manager could no longer access data on a laptop equipped with FDE. The manager requested that the FDE be removed and the laptop restored from a backup. The help desk informed the manager that the recommended solution was to decrypt the hard drive prior to reinstallation and recovery. The senior manager did not have a copy of the private key associated with the FDE on the laptop. Which of the following tools or techniques did the help desk use to avoid losing the data on the laptop?
163 A. Public key
164 B. Recovery agent
165 C. Registration details
166 D. Trust Model
167
168 27. An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was not received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles BEST describes why this social engineering ploy was successful?
169 A. Scarcity
170 B. Familiarity
171 C. Social proof
172 D. Urgency
173
174 28. A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?
175 A. Create a separate printer network
176 B. Perform penetration testing to rule out false positives
177 C. Install patches on the print server
178 D. Run a full vulnerability scan of all the printers
179
180 29. A systems administrator has made several unauthorized changes to the server cluster that resulted in a major outage. This event has been brought to the attention of the Chief Information Office (CIO) and he has requested immediately implement a risk mitigation strategy to prevent this type of event from reoccurring. Which of the following would be the BEST risk mitigation strategy to implement in order to meet this request?
181 A. Asset Management
182 B. Change Management
183 C. Configuration Management
184 D. Incident Management
185
186 30. An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?
187 A. Password history
188 B. Password complexity
189 C. Account lockout
190 D. Account expiration
191
192 31. Joe needs to track employees who log into a confidential database and edit files. In the past, critical files have been edited, and no one admits to making the edits. Which of the following does Joe need to implement in order to enforce accountability?
193 A. Non-repudiation
194 B. Fault tolerance
195 C. Hashing
196 D. Redundancy
197

- 198 - 32. A new mobile banking application is being developed and uses SSL / TLS certificates but penetration tests show that it is still vulnerable to man-in-the-middle attacks, such as DNS hijacking. Which of the following would mitigate this attack?
- 199 A. Certificate revocation
200 B. Key escrow
201 C. Public key infrastructure
202 D. Certificate pinning
- 203
- 204 33. One month after a software developer was terminated, the helpdesk started receiving calls that several employees' computers were being infected with malware. Upon further research, it was determined that these employees had downloaded a shopping toolbar. It was this toolbar that downloaded and installed the errant code. Which of the following attacks has taken place?
- 205 A. Logic bomb
206 B. Cross-site scripting
207 C. SQL injection
208 D. Malicious add-on
- 209
- 210 - 34. Which of the following would an attacker use to generate and capture additional traffic prior to performing an IV attack?
- 211 A. DNS poisoning
212 B. DDoS
213 C. Replay attack
214 D. Dictionary attack
- 215
- 216 35. An administrator has concerns regarding the company's server rooms Proximity badge readers were installed, but it is discovered this is not preventing unapproved personnel from tailgating into these area. Which of the following would BEST address this concern?
- 217 A. Replace proximity readers with turn0based key locks
218 B. Install man-traps at each restricted area entrance
219 C. Configure alarms to alert security when the areas are accessed
220 D. Install monitoring cameras at each entrance
- 221
- 222 36. Which of the following would be a reason for developers to utilize an AES cipher in CCM mode (Counter with Chain Block Message Authentication Code)?
- 223 A. It enables the ability to reverse the encryption with a separate key
224 B. It allows for one time pad inclusions with the passphrase
225 C. Counter mode alternates between synchronous and asynchronous encryption
226 D. It allows a block cipher to function as a steam cipher
- 227
- 228 - 37. One of the findings of risk assessment is that many of the servers on the data center subnet contain data that is in scope for PCI compliance, Everyone in the company has access to these servers, regardless of their job function. Which of the following should the administrator do?
- 229 A. Segment the network
230 B. Use 802.1X
231 C. Deploy a proxy sever
232 D. Configure ACLs
233 E. Write an acceptable use policy
- 234
- 235 - 38. Various employees have lost valuable customer data due to hard drives failing in company provided laptops. It has been discovered that the hard drives used in one model of laptops provided by the company has been recalled by the manufactory. The help desk is only able to replace the hard drives after they fail because there is no centralized record of the model of laptop given to each specific user. Which of the following could have prevented this situation from occurring?
- 236 A. Data backups
237 B. Asset tracking
238 C. Support ownership
239 D. BYOD policies
- 240
- 241 39. Attempting to inject 50 alphanumeric key strokes including spaces into an application input field that only expects four alpha characters in considered which of the following attacks?
- 242 A. XML injection
243 B. Buffer overflow
244 C. LDAP Injection
245 D. SQL injection

- 246
247 40. An organization is required to log all user internet activity. Which of the following would accomplish this requirement?
248 A. Configure an access list on the default gateway router. Configure the default gateway router to log all web traffic to a syslog server
249 B. Configure a firewall on the internal network. On the client IP address configuration, use the IP address of the firewall as the default gateway, configure the firewall to log all traffic to a syslog server
250 C. Configure a proxy server on the internal network and configure the proxy server to log all web traffic to a syslog server
251 D. Configure an access list on the core switch, configure the core switch to log all web traffic to a syslog server
- 252
253 41. An agent wants to create fast and efficient cryptographic keys to use with Diffie-Hellman without using prime numbers to generate the keys. Which of the following should be used?
254 A. Elliptic curve cryptography
255 B. Quantum cryptography
256 C. Public key cryptography
257 D. Symmetric cryptography
- 258
259 42. Joe an application developer is building an external facing marketing site. There is an area on the page where clients may submit their feedback to articles that are posted. Joe filters client-side JAVA input. Which of the following is Joe attempting to prevent?
260 A. SQL injections
261 B. Watering holes
262 C. Cross site scripting
263 D. Pharming
- 264
265 43. A video surveillance audit recently uncovered that an employee plugged in a personal laptop and used the corporate network to browse inappropriate and potentially malicious websites after office hours. Which of the following could BEST prevent a situation like this from occurring again?
266 A. Intrusion detection
267 B. Content filtering
268 C. Port security
269 D. Vulnerability scanning
- 270
271 44. A server administrator notes that a fully patched application often stops running due to a memory error. When reviewing the debugging logs they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describes?
272 A. Malicious add-on
273 B. SQL injection
274 C. Cross site scripting
275 D. Zero-day
- 276
277 45. A resent OS patch caused an extended outage. It took the IT department several hours to uncover the cause of the issue due to the system owner who installed the patch being out of the office. Which of the following could help reduce the likelihood of this situation occurring in the future?
278 A. Separation of duties
279 B. Change management procedures
280 C. Incident management procedures
281 D. User rights audits and reviews
- 282
283 46. The Chief Information Security Officer (CISO) is concerned that users could bring their personal laptops to work and plug them directly into the network port under their desk. Which of the following should be configured on the network switch to prevent this from happening?
284 A. Access control lists
285 B. Loop protection
286 C. Firewall rule
287 D. Port security
- 288
289 47. Ann a network administrator has been tasked with strengthening the authentication of users logging into systems in area containing sensitive information. Users log in with usernames and passwords, following by a retinal scan. Which of the following could

- she implement to add an additional factor of authorization?
- A. Requiring PII usage
B. Fingerprint scanner
C. Magnetic swipe cards
D. Complex passphrases
48. In an environment where availability is critical such as Industrial control and SCADA networks, which of the following technologies in the MOST critical layer of defense for such systems?
- A. Log consolidation
B. Intrusion Prevention system
C. Automated patch deployment
D. Antivirus software
49. A security manager installed a standalone fingerprint reader at the data center. All employees that need to access the data center have been enrolled to the reader and local reader database is always kept updated. When an employee who has been enrolled uses the fingerprint reader the door to the data center opens. Which of the following does this demonstrate? (Choose three.)
- A. Two-factor authentication
B. Single sign-on
C. Something you have
D. Identification
E. Authentication
F. Authorization
50. A network technician is configuring clients for VLAN access. The network address for the sales department is 192.168.0.64 with a broadcast address of 192.168.0.71. Which of the following IP address/subnet mask combinations could be used to correctly configure a client machine in the sales department?
- A. 192.168.0.64/29
B. 192.168.0.66/27
C. 192.168.0.67/29
D. 192.168.0.70/28
51. The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due, in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?
- A. Load balancer**
B. Spam filter
C. VPN Concentrator
D. NIDS
52. Two organizations want to share sensitive data with one another from their IT systems to support a mutual customer base. Both organizations currently have secure network and security policies and procedures. Which of the following should be the PRIMARY security considerations by the security managers at each organization prior to sharing information? (Choose three.)
- A. Physical security controls** B6F
B. Device encryption
C. Outboarding/Offboarding
D. Use of digital signatures
E. SLA/ISA
F. Data ownership
G. Use of smartcards or common access cards
H. Patch management
53. A company's password and authentication policies prohibit the use of shared passwords and transitive trust. Which of the following if implemented would violate company policy? (Choose two.)
- A. Discretionary access control**
B. Federation
C. Single sign-on
D. TOTP
E. Two-factor authentication

338 54. Which of the following types of attacks is based on coordinating small slices of a task across multiple systems?

339 A. DDos

340 B. Spam

341 C. Spoofing

342 D. Dos

343

344 55. A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?

345 A. Taking screenshots

346 B. Analyzing Big Data metadata

347 C. Analyzing network traffic and logs

348 D. Capturing system image

349

350 56. The security manager reports that the process of revoking certificates authority is too slow and should be automated. Which of the following should be used to automate this process?

351 A. CRL (old ver of OCSP)

352 B. GPG

353 C. OCSP

Online Certificate Status Protocol

354 D. Key escrow

355

356 57. A user attempts to install a new and relatively unknown software program recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

357 A. Application black listing

358 B. Network Intrusion Prevention System

359 C. Group Policy

360 D. Application White Listing

361

362 58. A company needs to provide web-based access to shared data sets to mobile users, while maintaining a standardized set of security controls. Which of the following technologies is the MOST appropriate storage?

363 A. Encrypted external hard drives

364 B. Cloud storage

365 C. Encrypted mobile devices

366 D. Storage Area Network

367

368 59. An employee's mobile device associates with the company's guest WiFi SSID, but then is unable to retrieve email. The email settings appear to be correct. Which of the following is the MOST likely cause?

369 A. The employee has set the network type to WPA instead of WPA2

370 B. The network uses a captive portal and requires a web authentication

371 C. The administrator has blocked the use of the personal hot spot feature

372 D. The mobile device has been placed in airplane mode

373

374 60. A malicious individual used an unattended customer service kiosk in a busy store to change the prices of several products. The alteration was not noticed until several days later and resulted in the loss of several thousand dollars for the store. Which of the following would BEST prevent this from occurring again?

375 A. Password expiration

376 B. Screen locks

377 C. Inventory control

378 D. Asset tracking

379

380 61. In order to enter a high-security data center, users are required to speak the password into a voice recognition system. Ann, a member of the sales department, overhears the password and later speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

381 A. An authentication factor

382 B. Discretionary Access

383 C. Time of Day Restrictions

384 D. Least Privilege Restrictions

385

386 62. A company requires that all users enroll in the corporate PKI structure and digitally sign all emails. Which of the following are primary reasons to sign emails with digital certificates? (Choose two.)

- 387 A. To establish non-repudiation
388 B. To ensure integrity
389 C. To prevent SPAM
390 D. To establish data loss prevention
391 E. To protect confidentiality
392 F. To establish transport encryption
393
- 394 63. The Chief Information Officer (CIO) has asked a security analyst to determine the estimated costs associated with each potential breach of their database that contains customer information. Which of the following is the risk calculation that the CIO is asking for?
395 A. Impact
396 B. SLE *Single-loss expectancy*
397 C. ARO
398 D. ALE
399
- 400 64. A security assurance officer is preparing a plan to measure the technical state of a customer's enterprise. The testers employed to perform the audit will be given access to the customer facility and network. The testers will not be given access to the details of custom developed software used by the customer. However the testers will have access to the source code for several open source applications and pieces of networking equipment used at the facility, but these items will not be within the scope of the audit. Which of the following BEST describes the appropriate method of testing or technique to use in this scenario? (Choose two.)
401 A. Social engineering
402 B. All source
403 C. Black box
404 D. Memory dumping
405 E. Penetration
406
- 407 65. Which of the following authentication services combines authentication and authorization in a user profile and uses UDP?
408 A. LDAP
409 B. Kerberos
410 C. TACACS+
411 D. RADIUS
412
- 413 66. A security administrator is designing an access control system, with an unlimited budget, to allow authenticated users access to network resources. Given that a multifactor authentication solution is more secure, which of the following is the BEST combination of factors?
414 A. Retina scanner, thumbprint scanner, and password
415 B. Username and password combo, voice recognition scanner, and retina scanner
416 C. Password, retina scanner, and proximity reader
417 D. One-time password pad, palm-print scanner, and proximity photo badges
418
- 419 67. The access control list (ACL) for a file on a server is as follows:
420 User: rwx
421 User: Ann: r- -
422 User: Joe: r- -
423
424 Group: rwx
425 Group: sales: r-x
426
427 Other: r-x
428
- 429 Joe and Ann are members of the Human Resources group. Will Ann and Joe be able to run the file?
430 A. No since Ann and Joe are members of the Sales group owner of the file
431 B. Yes since the regular permissions override the ACL for the file
432 C. No since the ACL overrides the regular permissions for the file
433 D. Yes since the regular permissions and the ACL combine to create the effective permissions on the file
434
- 435 68. Using a protocol analyzer, a security consultant was able to capture employee's credentials. Which of the following should the consultant recommend to the company, in order to mitigate the risk of employees' credentials being captured in the same manner in the future?
436 A. Wiping of remnant data

- 437 B. Hashing and encryption of data in-use
438 C. Encryption of data in-transit
439 D. Hashing of data at-rest
440
- 441 69. A Company has recently identified critical systems that support business operations. Which of the following will once defined, be the requirement for restoration of these systems within a certain period of time?
442 A. Mean Time Between Failure
443 B. Mean Time to Restore
444 C. Recovery Point Objective
445 D. Recovery Time Objective
446
- 447 70. The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the application servers. Which of the following practices are they following to ensure application integrity?
448 A. Job rotation
449 B. Implicit deny
450 C. Least privilege
451 D. Separation of duties
452
- 453 71. Ann is traveling for business and is attempting to use the hotel's wireless network to check for new messages. She selects the hotel's wireless SSID from a list of networks and successfully connects. After opening her email client and waiting a few minutes, the connection times out. Which of the following should Ann do to retrieve her email messages?
454 A. Change the authentication method for her laptop's wireless card from WEP to WPA2.
455 B. Open a web browser and authenticate using the captive portal for the hotel's wireless network.
456 C. Contact the front desk and have the MAC address of her laptop added to the MAC filter on the hotel's wireless network.
457 D. Change the incoming email protocol from IMAP to POP3.
458
- 459 72. Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?
460 A. Dictionary
461 B. Hybrid
462 C. Watering hole
463 D. Brute Force
464
- 465 73. Ann, a security administrator, is strengthening the security controls of the company's campus. Her goal is to prevent people from accessing open locations that are not supervised, such as around the receiving dock. She is also concerned that employees are using these entry points as a way of bypassing the security guard at the main entrance. Which of the following should Ann recommend that would BEST address her concerns?
466 A. Increase the lighting surrounding every building on campus
467 B. Build fences around campus with gates at entrances
468 C. Install cameras to monitor the unsupervised areas
469 D. Construct bollards to prevent vehicle entry in non-supervised areas
470
- 471 74. While an Internet café a malicious user is causing all surrounding wireless connected devices to have intermittent and unstable connections to the access point. Which of the following is MOST likely being used?
472 A. Evil Twin
473 B. Interference
474 C. Packet sniffer
475 D. Rogue AP
476
- 477 75. A password audit has revealed that a significant percentage if end-users have passwords that are easily cracked. Which of the following is the BEST technical control that could be implemented to reduce the amount of easily "crackable" passwords in use?
478 A. Credential management
479 B. Password history
480 C. Password complexity
481 D. Security awareness training
482
- 483 76. While working on a new project a security administrator wants to verify the integrity of the data in the organizations archive library. Which of the following is

- the MOST secure combination to implement to meet this goal? (Choose two.)
- 484 A. Hash with SHA
485 B. Encrypt with Diffie-Hellman
486 C. Hash with MD5
487 D. Hash with RIPEMD
488 E. Encrypt with AES
489
- 490 77. A company has been attacked and their website has been altered to display false information. The security administrator disables the web server service before restoring the website from backup. An audit was performed on the server and no other data was altered. Which of the following should be performed after the server has been restored?
- 491 A. Monitor all logs for the attacker's IP
492 B. Block port 443 on the web server
493 C. Install and configure SSL to be used on the web server
494 D. Configure the web server to be in VLAN 0 across the network
495
- 496 78. A security administrator suspects that an employee in the IT department is utilizing a reverse proxy to bypass the company's content filter and browse unapproved and non-work related sites while at work. Which of the following tools could BEST be used to determine how the employee is connecting to the reverse proxy?
- 497 A. Port scanner
498 B. Vulnerability scanner
499 C. Honeypot
500 D. Protocol analyzer
501
- 502 79. Joe, a company's network engineer, is concerned that protocols operating at the application layer of the OSI model are vulnerable to exploitation on the network. Which of the following protocols should he secure?
- 503 A. SNMP
504 B. SSL
505 C. ICMP
506 D. NetBIOS
507
- 508 80. Ann a security technician receives a report from a user that is unable to access an offsite SSH server. Ann checks the firewall and sees the following rules:
- 509 Allow TCP 80
510 Allow TCP 443
511 Deny TCP 23
512 Deny TCP 20
513 Deny TCP 21
514
- 515 Which of the following is preventing the users from accessing the SSH server?
- 516 A. Deny TCP 20
517 B. Deny TCP 21
518 C. Deny TCP 23
519 D. Implicit deny
520
- 521 81. An administrator uses a server with a trusted OS and is configuring an application to go into production tomorrow. In order to make a new application work properly, the administrator creates a new policy that labels the application and assigns it a security context within the trusted OS. Which of the following control methods is the administrator using by configuring this policy?
- 522 A. Time based access control
523 B. Mandatory access control
524 C. Role based access control
525 D. Rule based access control
526
- 527 82. A security administrator has been tasked with assisting in the forensic investigation of an incident relating to employee misconduct. The employee's supervisor believes evidence of this misconduct can be found on the employee's assigned workstation. Which of the following choices BEST describes what should be done? (Choose two.)
- 528 A. Record time as offset as required and conduct a timeline analysis
529 B. Update antivirus definitions and conduct a full scan for infected files
530 C. Analyze network traffic, system, and file logs
531 D. Create an additional local admin account on that workstation to conduct work from
532 E. Delete other user profiles on the system to help narrow down the search space
533 F. Patch the system before reconnecting it to the network

- 534
535 83. Joe a web developer wants to make sure his application is not susceptible to cross-site request forgery attacks. Which of the following is one way to prevent this type of attack?
536 A. The application should always check the HTTP referrer header
537 B. The application should always check the HTTP Request header
538 C. The application should always check the HTTP Host header
539 D. The application should always use SSL encryption
- 540
541 84. A custom PKI application downloads a certificate revocation list (CRL) once per day. Management requests the list be checked more frequently. Which of the following is the BEST solution?
542 A. Refresh the CA public key each time a user logs in
543 B. Download the CRL every 60 seconds
544 C. Implement the OCSP protocol *(Online Certificate Status Protocol)*
545 D. Prompt the user to trust a certificate each time it is used
- 546
547 85. A rogue programmer included a piece of code in an application to cause the program to halt at 2:00 PM on Monday afternoon when the application is most utilized. This is Which of the following types of malware?
548 A. Trojan
549 B. Virus
550 C. Logic Bomb
551 D. Botnets
- 552
553 86. After connecting to the corporate network a user types the URL of a popular social media website in the browser but reports being redirected to a login page with the corporate logo. Which of the following is this an example of?
554 A. LEAP
555 B. MAC filtering
556 C. WPA2-Enterprise
557 D. Captive portal
- 558
559 87. The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?
560 A. Grey box testing
561 B. White box testing
562 C. Penetration testing
563 D. Black box testing
- 564
565 88. A user Ann has her assigned token but she forgotten her password. Which of the following appropriately categorizes the authentication factor that will fail in this scenario?
566 A. Something you do
567 B. Something you know
568 C. Something you are
569 D. Something you have
- 570
571 89. An employee from the fire Marshall's office arrives to inspect the data center. The operator allows him to bypass the multi-factor authentication to enter the data center. Which of the following types of attacks may be underway?
572 A. Impersonation
573 B. Hoax
574 C. Tailgating
575 D. Spoofing
- 576
577 90. A company recently received accreditation for a secure network, In the accreditation letter, the auditor specifies that the company must keep its security plan current with changes in the network and evolve the systems to adapt to new threats. Which of the following security controls will BEST achieve this goal?
578 A. Change management
579 B. Group Policy
580 C. Continuous monitoring
581 D. Credential management
- 582
583 91. A cyber security administrator receives a list of IPs that have been reported as attempting to access the network. To identify any possible successful attempts across the enterprise, which of the following should be implemented?

- 584 A. Monitor authentication logs
585 B. Disable unnecessary accounts
586 C. Time of day restrictions
587 D. Separation of duties
588
- 589 92. Which of the following exploits either a host file on a target machine or vulnerabilities on a DNS server in order to carry out URL redirection?
590 A. Pharming
591 B. Spoofing
592 C. Vishing
593 D. Phishing
594
- 595 93. Ann a new small business owner decides to implement WiFi access for her customers. There are several other businesses nearby who also have WiFi hot spots. Ann is concerned about security of the wireless network and wants to ensure that only her customers have access. Which of the following choices BEST meets her intent of security and access?
596 A. Enable port security
597 B. Enable WPA
598 C. Disable SSID broadcasting
599 D. Enable WEP
600
- 601 94. A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Choose two.)
602 A. PGP/GPG
603 B. S/MIME
604 C. IPSEC
605 D. Secure POP3
606 E. IMAP
607 F. HMAC
608
- 609 95. Which of the following is the GREATEST security concern of allowing employees to bring in their personally owned tablets and connecting to the corporate network?
610 A. Tablet network connections are stored and accessible from the corporate network
611 B. The company's attack surface increases with the non-corporate devices
612 C. Personally purchased media may be available on the network for others to stream
613 D. Encrypted tablets are harder to access to determine if they are infected
614
- 615 96. Searching for systems infected with malware is considered to be which of the following phases of incident response?
616 A. Containment
617 B. Preparation
618 C. Mitigation
619 D. Identification
620
- 621 97. A technician has deployed a new VPN concentrator. The device needs to authenticate users based on a backend directory service. Which of the following services could be run on the VPN concentrator to perform this authentication?
622 A. Kerberos
623 B. RADIUS
624 C. GRE
625 D. IPsec
626
- 627 98. A webpage displays a potentially offensive advertisement on a computer. A customer walking by notices the displayed advertisement and files complaint. Which of the following can BEST reduce the likelihood of this incident occurring again?
628 A. Clean-desk policies
629 B. Screen-locks
630 C. Pop-up blocker
631 D. Antispyware software
632
- 633 99. Which of the following is an attack designed to activate based on date?
634 A. Logic bomb
635 B. Backdoor
636 C. Trojan
637 D. Rootkit
638
- 639 100. A malicious user has collected the following list of information:
640 -- 192.168.1.5 OpenSSH-Server_5.8

641 -- 192.168.1.7 OpenSSH-Server_5.7
642 -- 192.168.1.9 OpenSSH-Server_5.7
643
644 Which of the following techniques is MOST likely to gather this type of data?
645 A. Banner grabbing
646 B. Port scan
647 C. Host scan
648 D. Ping scan
649