

- 1 1. Account lockout is a mitigation strategy used by Jane, the administrator, to combat
which of the following attacks? (Choose two.)
- 2 A. Spoofing
- 3 B. Man-in-the-middle
- 4 C. Dictionary
- 5 D. Brute force
- 6 E. Privilege escalation
- 7
- 8 2. A recent audit has discovered that at the time of password expiration clients are
able to recycle the previous credentials for authentication. Which of the following
controls should be used together to prevent this from occurring? (Choose two.)
- 9 A. Password age
- 10 B. Password hashing
- 11 C. Password complexity
- 12 D. Password history
- 13 E. Password length
- 14
- 15 3. A password history value of three means which of the following?
- 16 A. Three different passwords are used before one can be reused.
- 17 B. A password cannot be reused once changed for three years.
- 18 C. After three hours a password must be re-entered to continue.
- 19 D. The server stores passwords in the database for three days.
- 20
- 21 4. An administrator discovers that many users have used their same passwords for years
even though the network requires that the passwords be changed every six weeks. Which
of the following, when used together, would BEST prevent users from reusing their
existing password? (Choose two.)
- 22 A. Length of password
- 23 B. Password history
- 24 C. Minimum password age
- 25 D. Password expiration
- 26 E. Password complexity
- 27 F. Non-dictionary words
- 28
- 29 5. A system administrator has noticed that users change their password many times to
cycle back to the original password when their passwords expire. Which of the following
would BEST prevent this behavior?
- 30 A. Assign users passwords based upon job role.
- 31 B. Enforce a minimum password age policy.
- 32 C. Prevent users from choosing their own passwords.
- 33 D. Increase the password expiration time frame.
- 34
- 35 6. Which of the following is an important implementation consideration when deploying a
wireless network that uses a shared password?
- 36 A. Authentication server
- 37 B. Server certificate
- 38 C. Key length
- 39 D. EAP method
- 40
- 41 7. A security administrator is reviewing the below output from a password auditing tool:
- 42 P@ss.
- 43 @pW1.
- 44 S3cU4
- 45
- 46 Which of the following additional policies should be implemented based on the tool's
output?
- 47 A. Password age
- 48 B. Password history
- 49 C. Password length
- 50 D. Password complexity
- 51
- 52 8. Several employee accounts appear to have been cracked by an attacker. Which of the
following should the security administrator implement to mitigate password cracking
attacks? (Choose two.)
- 53 A. Increase password complexity
- 54 B. Deploy an IDS to capture suspicious logins
- 55 C. Implement password history
- 56 D. Implement monitoring of logins
- 57 E. Implement password expiration

58 F. Increase password length
59
60 9. Human Resources suspects an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?
61 A. Shared accounts should be prohibited.
62 B. Account lockout should be enabled
63 C. Privileges should be assigned to groups rather than individuals
64 D. Time of day restrictions should be in use
65
66 10. A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?
67 A. Time of day restrictions
68 B. Group based privileges
69 C. User assigned privileges
70 D. Domain admin restrictions
71
72 11. A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?
73 A. Assign users manually and perform regular user access reviews
74 B. Allow read only access to all folders and require users to request permission
75 C. Assign data owners to each folder and allow them to add individual users to each folder
76 D. Create security groups for each folder and assign appropriate users to each group
77
78 12. A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?
79 A. Group based privileges
80 B. Generic account prohibition
81 C. User access review
82 D. Credential management
83
84 13. A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?
85 A. User assigned privileges
86 B. Password disablement
87 C. Multiple account creation
88 D. Group based privileges
89
90 14. Which of the following practices reduces the management burden of access management?
91 A. Password complexity policies
92 B. User account audit
93 C. Log analysis and review
94 D. Group based privileges
95
96 15. A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?
97 A. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
98 B. The supervisor should be removed from the human resources group and added to the accounting group.
99 C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
100 D. The supervisor should only maintain membership in the human resources group.
101
102 16. A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?
103 A. Leverage role-based access controls.
104 B. Perform user group clean-up.
105 C. Verify smart card access controls.
106 D. Verify SHA-256 for password hashes.

107
108 17. Privilege creep among long-term employees can be mitigated by which of the
following procedures?
109 A. User permission reviews
110 B. Mandatory vacations
111 C. Separation of duties
112 D. Job function rotation
113
114 18. A recent audit of a company's identity management system shows that 30% of active
accounts belong to people no longer with the firm. Which of the following should be
performed to help avoid this scenario? (Choose two.)
115 A. Automatically disable accounts that have not been utilized for at least 10 days.
116 B. Utilize automated provisioning and de-provisioning processes where possible.
117 C. Request that employees provide a list of systems that they have access to prior to
leaving the firm.
118 D. Perform regular user account review / revalidation process.
119 E. Implement a process where new account creations require management approval.
120
121 19. In order for network monitoring to work properly, you need a PC and a network card
running in what mode?
122 A. Launch
123 B. Exposed
124 C. Promiscuous
125 D. Sweep
126
127 20. Which of the following techniques enables a highly secured organization to assess
security weaknesses in real time?
128 A. Access control lists
129 B. Continuous monitoring
130 C. Video surveillance
131 D. Baseline reporting
132
133 21. A customer has provided an email address and password to a website as part of the
login process. Which of the following BEST describes the email address?
134 A. Identification
135 B. Authorization
136 C. Access control
137 D. Authentication
138
139 22. A company has 5 users. Users 1, 2 and 3 need access to payroll and users 3, 4 and 5
need access to sales. Which of the following should be implemented to give the
appropriate access while enforcing least privilege?
140 A. Assign individual permissions to users 1 and 2 for payroll. Assign individual
permissions to users 4 and 5 for sales. Make user 3 an administrator.
141 B. Make all users administrators and then restrict users 1 and 2 from sales. Then
restrict users 4 and 5 from payroll.
142 C. Create two additional generic accounts, one for payroll and one for sales that users
utilize.
143 D. Create a sales group with users 3, 4 and 5. Create a payroll group with users 1, 2
and 3.
144
145 23. An administrator implements SELinux on a production web server. After implementing
this, the web server no longer serves up files from users' home directories. To rectify
this, the administrator creates a new policy as the root user. This is an example of
which of the following? (Choose two.)
146 A. Enforcing SELinux in the OS kernel is role-based access control
147 B. Enforcing SELinux in the OS kernel is rule-based access control
148 C. The policy added by the root user is mandatory access control
149 D. Enforcing SELinux in the OS kernel is mandatory access control
150 E. The policy added by the root user is role-based access control
151 F. The policy added by the root user is rule-based access control
152
153 24. A security administrator has deployed all laptops with Self Encrypting Drives (SED)
and enforces key encryption. Which of the following represents the greatest threat to
maintaining data confidentiality with these devices?
154 A. Full data access can be obtained by connecting the drive to a SATA or USB adapter
bypassing the SED hardware.
155 B. A malicious employee can gain the SED encryption keys through software extraction
allowing access to other laptops.

156 C. If the laptop does not use a Secure Boot BIOS, the SED hardware is not enabled
allowing full data access.

157 D. Laptops that are placed in a sleep mode allow full data access when powered back on.

158

159 25. A recent review of accounts on various systems has found that after employees' passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Choose two.)

160 A. Reverse encryption

161 B. Minimum password age

162 C. Password complexity

163 D. Account lockouts

164 E. Password history

165 F. Password expiration

166

167 26. An organizations' security policy requires that users change passwords every 30 days. After a security audit, it was determined that users were recycling previously used passwords. Which of the following password enforcement policies would have mitigated this issue?

168 A. Password history

169 B. Password complexity

170 C. Password length

171 D. Password expiration

172

173 27. A security administrator must implement a system that will support and enforce the following file system access control model:

174 FILE NAME -- SECURITY LABEL

175 Employees.doc -- Confidential

176 Salary.xls -- Confidential

177 OfficePhones.xls -- Unclassified

178 PersonalPhones.xls -- Restricted

179

180 Which of the following should the security administrator implement?

181 A. White and black listing

182 B. SCADA system

183 C. Trusted OS

184 D. Version control

185

186 28. Which of the following is the BEST reason for placing a password lock on a mobile device?

187 A. Prevents an unauthorized user from accessing owner's data

188 B. Enables remote wipe capabilities

189 C. Stops an unauthorized user from using the device again

190 D. Prevents an unauthorized user from making phone calls

191

192 29. Ann is the data owner of financial records for a company. She has requested that she have the ability to assign read and write privileges to her folders. The network administrator is tasked with setting up the initial access control system and handing Ann's administrative capabilities. Which of the following systems should be deployed?

193 A. Role-based

194 B. Mandatory

195 C. Discretionary

196 D. Rule-based

197

198 30. Ann was reviewing her company's event logs and observed several instances of GUEST accessing the company print server, file server, and archive database. As she continued to investigate, Ann noticed that it seemed to happen at random intervals throughout the day, but mostly after the weekly automated patching and often logging in at the same time. Which of the following would BEST mitigate this issue?

199 A. Enabling time of day restrictions

200 B. Disabling unnecessary services

201 C. Disabling unnecessary accounts

202 D. Rogue machine detection

203

204 31. Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:

205 Ann:read/write

206 Sales Group:read

207 IT Group:no access

208
209 If a discretionary access control list is in place for the files owned by Ann, which of
the following would be the BEST way to share the file with Joe?
210 A. Add Joe to the Sales group.
211 B. Have the system administrator give Joe full access to the file.
212 C. Give Joe the appropriate access to the file directly.
213 D. Remove Joe from the IT group and add him to the Sales group.
214
215 32. A network administrator, Joe, arrives at his new job to find that none of the users
have changed their network passwords since they were initially hired. Joe wants to have
everyone change their passwords immediately. Which of the following policies should be
enforced to initiate a password change?
216 A. Password expiration
217 B. Password reuse
218 C. Password recovery
219 D. Password disablement
220
221 33. 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?
222 A. Deploy a HIDS suite on the users' computers to prevent application installation.
223 B. Maintain the baseline posture at the highest OS patch level.
224 C. Enable the pop-up blockers on the users' browsers to prevent malware.
225 D. Create an approved application list and block anything not on it.
226
227 34. Which of the following should be used to authenticate and log connections from
wireless users connecting with EAP-TLS?
228 A. Kerberos
229 B. LDAP
230 C. SAML
231 D. RADIUS
232
233 35. Ann has recently transferred from the payroll department to engineering. While
browsing file shares, Ann notices she can access the payroll status and pay rates of
her new coworkers. Which of the following could prevent this scenario from occurring?
234 A. Credential management
235 B. Continuous monitoring
236 C. Separation of duties
237 D. User access reviews
238
239 36. An organization's security policy states that users must authenticate using
something you do. Which of the following would meet the objectives of the security
policy?
240 A. Fingerprint analysis
241 B. Signature analysis
242 C. Swipe a badge
243 D. Password
244
245 37. Which of the following protocols is MOST likely to be leveraged by users who need
additional information about another user?
246 A. LDAP
247 B. RADIUS
248 C. Kerberos
249 D. TACACS+
250
251 38. The security manager wants to unify the storage of credential, phone numbers,
office numbers, and address information into one system. Which of the following is a
system that will support the requirement on its own?
252 A. LDAP
253 B. SAML
254 C. TACACS
255 D. RADIUS
256
257 39. Joe, a network administrator, is able to manage the backup software console by
using his network login credentials. Which of the following authentication services is
the MOST likely using?
258 A. SAML
259 B. LDAP

260 C. iSCSI
261 D. Two-factor authentication
262
263 40. An organization is implementing a password management application which requires
that all local administrator passwords be stored and automatically managed. Auditors
will be responsible for monitoring activities in the application by reviewing the logs.
Which of the following security controls is the BEST option to prevent auditors from
accessing or modifying passwords in the application?
264 A. Time of day restrictions
265 B. Create user accounts for the auditors and assign read-only access
266 C. Mandatory access control
267 D. Role-based access with read-only
268
269 41. A security administrator is tackling issues related to authenticating users at a
remote site. There have been a large number of security incidents that resulted from
either tailgating or impersonation of authorized users with valid credentials. The
security administrator has been told to implement multifactor authentication in order
to control facility access. To secure access to the remote facility, which of the
following could be implemented without increasing the amount of space required at the
entrance?
270 A. MOTD challenge and PIN pad
271 B. Retina scanner and fingerprint reader
272 C. Voice recognition and one-time PIN token
273 D. One-time PIN token and proximity reader
274
275 42. The security administrator notices a user logging into a corporate Unix server
remotely as root. Which of the following actions should the administrator take?
276 A. Create a firewall rule to block SSH
277 B. Delete the root account
278 C. Disable remote root logins
279 D. Ensure the root account has a strong password
280
281 43. A company plans to expand by hiring new engineers who work in highly specialized
areas. Each engineer will have very different job requirements and use unique tools and
applications in their job. Which of the following is MOST appropriate to use?
282 A. Role-based privileges
283 B. Credential management
284 C. User assigned privileges
285 D. User access
286
287 44. A file on a Linux server has default permissions of rw-rw-r--. The system
administrator has verified that Ann, a user, is not a member of the group owner of the
file. Which of the following should be modified to assure that Ann has read access to
the file?
288 A. User ownership information for the file in question
289 B. Directory permissions on the parent directory of the file in question
290 C. Group memberships for the group owner of the file in question
291 D. The file system access control list (FACL) for the file in question
292
293 45. Which of the following protocols uses an asymmetric key to open a session and then
establishes a symmetric key for the remainder of the session?
294 A. SFTP
295 B. HTTPS
296 C. TFTP
297 D. TLS
298
299 46. A company uses PGP to ensure that sensitive email is protected. Which of the
following types of cryptography is being used here for the key exchange?
300 A. Symmetric
301 B. Session-based
302 C. Hashing
303 D. Asymmetric
304
305 47. Which of the following is true about asymmetric encryption?
306 A. A message encrypted with the private key can be decrypted by the same key
307 B. A message encrypted with the public key can be decrypted with a shared key.
308 C. A message encrypted with a shared key, can be decrypted by the same key.
309 D. A message encrypted with the public key can be decrypted with the private key.
310

311 48. Encryption used by RADIUS is BEST described as:
312 A. Quantum
313 B. Elliptical curve
314 C. Asymmetric
315 D. Symmetric
316
317 49. Symmetric encryption utilizes _____, while asymmetric encryption utilizes
318 _____.
319 A. Public keys, one time
320 B. Shared keys, private keys
321 C. Private keys, session keys
322 D. Private keys, public keys
323
324 50. Users need to exchange a shared secret to begin communicating securely. Which of
325 the following is another name for this symmetric key?
326 A. Session Key
327 B. Public Key
328 C. Private Key
329 D. Digital Signature
330
331 51. In order to securely communicate using PGP, the sender of an email must do which of
332 the following when sending an email to a recipient for the first time?
333 A. Import the recipient's public key
334 B. Import the recipient's private key
335 C. Export the sender's private key
336 D. Export the sender's public key
337
338 52. A network stream needs to be encrypted. Sara, the network administrator, has
339 selected a cipher which will encrypt 8 bits at a time before sending the data across
340 the network. Which of the following has Sara selected?
341 A. Block cipher
342 B. Stream cipher
343 C. CRC
344 D. Hashing algorithm
345
346 53. The concept of rendering data passing between two points over an IP based network
347 impervious to all but the most sophisticated advanced persistent threats is BEST
348 categorized as which of the following?
349 A. Stream ciphers
350 B. Transport encryption
351 C. Key escrow
352 D. Block ciphers
353
354 54. Which of the following transportation encryption protocols should be used to ensure
355 maximum security between a web browser and a web server?
356 A. SSLv2
357 B. SSHv1
358 C. RSA
359 D. TLS
360
361 55. When employing PKI to send signed and encrypted data the individual sending the
362 data must have: (Choose two.)
363 A. The receiver's private key
364 B. The root certificate
365 C. The sender's private key
366 D. The sender's public key
367 E. The receiver's public key
368
369 56. Which of the following concepts is enforced by certifying that email communications
370 have been sent by who the message says it has been sent by?
371 A. Key escrow
372 B. Non-repudiation
373 C. Multifactor authentication
374 D. Hashing
375
376 57. All of the following are valid cryptographic hash functions EXCEPT:
377 A. RIPEMD.
378 B. RC4.
379 C. SHA-512.

370 D. MD4.

371

372 58. Which of the following concepts is used by digital signatures to ensure integrity
of the data?

373 A. Non-repudiation

374 B. Hashing

375 C. Transport encryption

376 D. Key escrow

377

378 59. A security administrator discovers an image file that has several plain text
documents hidden in the file. Which of the following security goals is met by
camouflaging data inside of other files?

379 A. Integrity

380 B. Confidentiality

381 C. Steganography

382 D. Availability

383

384 60. A security analyst discovered data such as images and word documents hidden within
different types of files. Which of the following cryptographic concepts describes what
was discovered?

385 A. Symmetric encryption

386 B. Non-repudiation

387 C. Steganography

388 D. Hashing

389

390 61. Which of the following can hide confidential or malicious data in the whitespace of
other files (e.g. JPEGs)?

391 A. Hashing

392 B. Transport encryption

393 C. Digital signatures

394 D. Steganography

395

396 62. Which of the following must a user implement if they want to send a secret message
to a coworker by embedding it within an image?

397 A. Transport encryption

398 B. Steganography

399 C. Hashing

400 D. Digital signature

401

402 63. Digital Signatures provide which of the following?

403 A. Confidentiality

404 B. Authorization

405 C. Integrity

406 D. Authentication

407 E. Availability

408

409 64. Matt, a security analyst, needs to select an asymmetric encryption method that
allows for the same level of encryption strength with a lower key length than is
typically necessary. Which of the following encryption methods offers this capability?

410 A. Twofish

411 B. Diffie-Hellman

412 C. ECC

413 D. RSA

414

415 65. Which of the following types of cryptography should be used when minimal overhead
is necessary for a mobile device?

416 A. Block cipher

417 B. Elliptical curve cryptography

418 C. Diffie-Hellman algorithm

419 D. Stream cipher

420

421 66. A security technician is attempting to access a wireless network protected with
WEP. The technician does not know any information about the network. Which of the
following should the technician do to gather information about the configuration of the
wireless network?

422 A. Spoof the MAC address of an observed wireless network client

423 B. Ping the access point to discover the SSID of the network

424 C. Perform a dictionary attack on the access point to enumerate the WEP key

425 D. Capture client to access point disassociation packets to replay on the local PC's

loopback

- 426
427 67. The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to this?
- 428 A. Disable the SSID broadcasting
429 B. Configure the access points so that MAC filtering is not used
430 C. Implement WEP encryption on the access points
431 D. Lower the power for office coverage only
432
- 433 68. Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?
- 434 A. Disable default SSID broadcasting.
435 B. Use WPA instead of WEP encryption.
436 C. Lower the access point's power settings.
437 D. Implement MAC filtering on the access point.
438
- 439 69. Which of the following provides the strongest authentication security on a wireless network?
- 440 A. MAC filter
441 B. WPA2
442 C. WEP
443 D. Disable SSID broadcast
444
- 445 70. Which of the following is a concern when encrypting wireless data with WEP?
- 446 A. WEP displays the plain text entire key when wireless packet captures are reassembled
447 B. WEP implements weak initialization vectors for key transmission
448 C. WEP uses a very weak encryption algorithm
449 D. WEP allows for only four pre-shared keys to be configured
450
- 451 71. Which of the following provides the HIGHEST level of confidentiality on a wireless network?
- 452 A. Disabling SSID broadcast
453 B. MAC filtering
454 C. WPA2
455 D. Packet switching
456
- 457 72. While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?
- 458 A. EAP-TLS
459 B. PEAP
460 C. WEP
461 D. WPA
462
- 463 73. Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises. A security technician was asked to prepare a report of files that had changed since last night's integrity scan. Which of the following could the technician use to prepare the report? (Choose two.)
- 464 A. PGP
465 B. MD5
466 C. ECC
467 D. AES
468 E. Blowfish
469 F. HMAC
470
- 471 74. Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?
- 472 A. Whole disk encryption
473 B. SSH
474 C. Telnet
475 D. MD5
476
- 477 75. Which of the following is used to verify data integrity?
- 478 A. SHA
479 B. 3DES
480 C. AES

481 D. RSA
482
483 76. Which of the following can be implemented with multiple bit strength?
484 A. AES
485 B. DES
486 C. SHA-1
487 D. MD5
488 E. MD4
489
490 77. To ensure compatibility with their flagship product, the security engineer is
tasked to recommend an encryption cipher that will be compatible with the majority of
third party software and hardware vendors. Which of the following should be recommended?
491 A. SHA
492 B. MD5
493 C. Blowfish
494 D. AES
495
496 78. Which of the following provides additional encryption strength by repeating the
encryption process with additional keys?
497 A. AES
498 B. 3DES
499 C. TwoFish
500 D. Blowfish
501
502 79. Which of the following are restricted to 64-bit block sizes? (Choose two.)
503 A. PGP
504 B. DES
505 C. AES256
506 D. RSA
507 E. 3DES
508 F. AES
509
510 80. A bank has a fleet of aging payment terminals used by merchants for transactional
processing. The terminals currently support single DES but require an upgrade in order
to be compliant with security standards. Which of the following is likely to be the
simplest upgrade to the aging terminals which will improve in-transit protection of
transactional data?
511 A. AES
512 B. 3DES
513 C. RC4
514 D. WPA2
515
516 81. Which of the following would Matt, a security administrator, use to encrypt
transmissions from an internal database to an internal server, keeping in mind that the
encryption process must add as little latency to the process as possible?
517 A. ECC
518 B. RSA
519 C. SHA
520 D. 3DES
521
522 82. Which of the following MUST Matt, a security administrator, implement to verify
both the integrity and authenticity of a message while requiring a shared secret?
523 A. RIPEMD
524 B. MD5
525 C. SHA
526 D. HMAC
527
528 83. Which of the following cryptographic algorithms is MOST often used with IPSec?
529 A. Blowfish
530 B. Twofish
531 C. RC4
532 D. HMAC
533
534 84. When creating a public / private key pair, for which of the following ciphers would
a user need to specify the key strength?
535 A. SHA
536 B. AES
537 C. DES
538 D. RSA

539
540 85. Which of the following uses both a public and private key?
541 A. RSA
542 B. AES
543 C. MD5
544 D. SHA
545
546 86. Which of the following ciphers would be BEST used to encrypt streaming video?
547 A. RSA
548 B. RC
549 C. SHA1
550 D. 3DES
551
552 87. Due to hardware limitation, a technician must implement a wireless encryption
algorithm that uses the RC4 protocol. Which of the following is a wireless encryption
solution that the technician should implement while ensuring the STRONGEST level of
security?
553 A. WPA2-AES
554 B. 802.11ac
555 C. WPA-TKIP
556 D. WEP
557
558 88. A security administrator must implement a wireless encryption system to secure
mobile devices' communication. Some users have mobile devices which only support 56-bit
encryption. Which of the following wireless encryption methods should be implemented?
559 A. RC4
560 B. AES
561 C. MD5
562 D. TKIP
563
564 89. Which of the following can use RC4 for encryption? (Choose two.)
565 A. CHAP
566 B. SSL
567 C. WEP
568 D. AES
569 E. 3DES
570
571 90. Which of the following would provide the STRONGEST encryption?
572 A. Random one-time pad
573 B. DES with a 56-bit key
574 C. AES with a 256-bit key
575 D. RSA with a 1024-bit key
576
577 91. Which of the following symmetric key algorithms are examples of block ciphers?
(Choose three.)
578 A. RC4
579 B. 3DES
580 C. AES
581 D. MD5
582 E. PGP
583 F. Blowfish
584
585 92. Which of the following should be used when a business needs a block cipher with
minimal key size for internal encryption?
586 A. AES
587 B. Blowfish
588 C. RC5
589 D. 3DES
590
591 93. Sara, a security engineer, is testing encryption ciphers for performance. Which of
the following ciphers offers strong encryption with the FASTEST speed?
592 A. 3DES
593 B. Blowfish
594 C. Serpent
595 D. AES256
596
597 94. Jane, a VPN administrator, was asked to implement an encryption cipher with a
MINIMUM effective security of 128-bits. Which of the following should Jane select for
the tunnel encryption?

598 A. Blowfish
599 B. DES
600 C. SHA256
601 D. HMAC
602
603 95. When using PGP, which of the following should the end user protect from compromise?
(Choose two.)
604 A. Private key
605 B. CRL details
606 C. Public key
607 D. Key password
608 E. Key escrow
609 F. Recovery agent
610
611 96. A security administrator must implement a system to allow clients to securely
negotiate encryption keys with the company's server over a public unencrypted
communication channel. Which of the following implements the required secure key
negotiation? (Choose two.)
612 A. PBKDF2
613 B. Symmetric encryption
614 C. Steganography
615 D. ECDHE
616 E. Diffie-Hellman
617
618 97. An administrator has two servers and wants them to communicate with each other
using a secure algorithm. Which of the following choose to provide both CRC integrity
checks and RCA encryption?
619 A. NTLM
620 B. RSA
621 C. CHAP
622 D. ECDHE
623
624 98. Connections using point-to-point protocol authenticate using which of the
following? (Choose two.)
625 A. RIPEMD
626 B. PAP
627 C. CHAP
628 D. RC4
629 E. Kerberos
630
631 99. Which of the following offers the LEAST secure encryption capabilities?
632 A. TwoFish
633 B. PAP
634 C. NTLM
635 D. CHAP
636
637 100. Which of the following algorithms has well documented collisions? (Choose two.)
638 A. AES
639 B. MD5
640 C. SHA
641 D. SHA-256
642 E. RSA