

- 1 1. Which of the following types of malware is designed to provide access to a system
when normal authentication fails?
- 2 A. Rootkit
- 3 B. Botnet
- 4 ☒ C. Backdoor
- 5 D. Adware
- 6
- 7 2. Ann is concerned that the application her team is currently developing is vulnerable
to unexpected user input that could lead to issues within the memory is affected in a
detrimental manner leading to potential exploitation. Which of the following describes
this application threat?
- 8 A. Replay attack
- 9 B. Zero-day exploit
- 10 ☒ C. Distributed denial of service
- 11 ☒ D. Buffer overflow
- 12
- 13 3. Which of the following can be used for both encryption and digital signatures?
- 14 A. 3DES
- 15 ☒ B. AES
- 16 ☒ C. RSA
- 17 D. MD5
- 18
- 19 4. A user tries to visit a web site with a revoked certificate. In the background a
server from the certificate authority only sends the browser revocation information
about the domain the user is visiting. Which of the following is being used by the
certificate authority in this exchange?
- 20 A. CSR
- 21 B. Key escrow
- 22 ☒ C. OCSP
- 23 D. CRL
- 24
- 25 5. Joe wants to employ MD5 hashing on the company file server. Which of the following
is Joe trying to achieve?
- 26 A. Availability
- 27 B. Confidentiality
- 28 C. Non repudiation
- 29 ☒ D. Integrity
- 30
- 31 6. By hijacking unencrypted cookies an application allows an attacker to take over
existing web sessions that do not use SSL or end to end encryption. Which of the
following choices BEST mitigates the security risk of public web surfing? (Choose two.)
- 32 ☒ A. WPA2
- 33 ☒ B. WEP
- 34 C. Disabling SSID broadcasting
- 35 ☒ D. VPN
- 36 E. Proximity to WIFI access point
- 37
- 38 7. The security administration team at a company has been tasked with implementing a
data-at-rest solution for its company storage. Due to the large amount of storage the
Chief Information Officer (CISO) decides that a 128-bit cipher is needed but the CISO
also does not want to degrade system performance any more than necessary. Which of the
following encryptions needs BOTH of these needs?
- 39 A. SHA1
- 40 B. DSA
- 41 ☒ C. AES
- 42 D. 3DES
- 43
- 44 8. A company has a BYOD policy that includes tablets and smart phones. In the case of a
legal investigation, which of the following poses the greatest security issues?
- 45 ☒ A. Recovering sensitive documents from a device if the owner is unable or unwilling to
cooperate
- 46 B. Making a copy of all of the files on the device and hashing them after the owner has
provided the PIN
- 47 C. Using GPS services to locate the device owner suspected in the investigation
- 48 D. Wiping the device from a remote location should it be identified as a risk in the
investigation
- 49
- 50 9. After several thefts a Chief Executive Officer (CEO) wants to ensure unauthorized do
not have to corporate grounds or its employees. The CEO just approved new budget line

items for fences, lighting, locks and CCTVs. Which of the following is the primary focus?

- 51 ☒ A. Safety
- 52 B. Confidentiality
- 53 C. Availability
- 54 D. Integrity

56 10. Which of the following steps in incident response procedures entails of the incident and identification of knowledge gained that can be applied to future handling of incidents?

- 57 A. Recovery procedures
- 58 B. Escalation and notification
- 59 C. Reporting
- 60 ☒ D. Lessons learned

62 11. Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?

- 63 ☒ A. Fuzzing
- 64 B. Black box
- 65 C. Fault injection
- 66 D. SQL injection

68 12. A company's BYOD policy requires the installation of a company provide mobile agent on their on their personally owned devices which would allow auditing when an employee wants to connect a device to the corporate email system. Which of the following concerns will MOST affect the decision to use a personal device to receive company email?

- 69 ☒ A. Personal privacy
- 70 B. Email support
- 71 C. Data ownership
- 72 D. Service availability

74 13. A penetration tester is measuring a company's posture on social engineering. The penetration tester sends a phishing email claiming to be from IT asking employees to click a link to update their VPN software immediately. Which of the following reasons would explain why this attack could be successful?

- 75 A. Principle of Scarcity
- 76 B. Principle of Intimidation
- 77 ☒ C. Principle of Urgency
- 78 D. Principle of liking

80 14. A new employee has joined the accounting department and is unable to access the accounting server. The employee can access other network resources and the Internet. Other accounting employees are able to access the accounting server without any issues. Which of the following is the MOST likely issue?

- 81 A. The server's IDS is blocking the new employee's connection
- 82 B. The workstation is unable to join the domain
- 83 C. The server's drive is not mapped on the new employee's workstation
- 84 ☒ D. The new account is not in the proper role-based profile

86 15. Joe a sales employee is connecting to a wireless network and has entered the network information correctly. His computer remains connected to the network but he cannot access any resources on the network. Which of the following is the MOST likely cause of this issue?

- 87 A. The encryption is too strong
- 88 B. The network SSID is disabled
- 89 C. MAC filtering is enabled
- 90 ☒ D. The wireless antenna power is set too low

92 16. Which of the following is used to inform users of the repercussions of releasing proprietary information?

- 93 A. OLA
- 94 B. SLA
- 95 ☒ C. NDA
- 96 D. MOU

98 17. A review of administrative access has discovered that too many accounts have been granted administrative rights. Which of the following will alert the security team when elevated access is applied?

- 99 A. Establishing user access reviews

- 100 B. Establishing user based privileges
101 ☒ C. Establishing monitoring on accounts
102 D. Establishing group based privileges
103
104 18. When an authorized application is installed on a server, the application triggers
an alert on the HIDS. This is known as a:
105 A. Vulnerability
106 B. False negative
107 ☒ C. False positive
108 D. Threat vector
109
110 19. In which of the following scenarios would it be preferable to implement file level
encryption instead of whole disk encryption?
111 A. A server environment where the primary security concern is integrity and not file
recovery
112 ☒ B. A cloud storage environment where multiple customers use the same hardware but
possess different encryption keys
113 C. A SQL environment where multiple customers access the same database
114 D. A large datacenter environment where each customer users dedicated hardware resources
115
116 20. For high availability which of the following would be MOST appropriate for fault
tolerance?
117 A. RAID 0
118 ☒ B. Clustering
119 C. JBOD
120 D. Load Balancing
121
122 21. When implementing a Public Key Infrastructure, which of the following should the
sender use to digitally sign a document?
123 A. A CSR
124 ☒ B. A private key
125 C. A certificate authority
126 ☒ D. A public key
127
128 22. A military base wants to incorporate biometrics into its new security measures, but
the head of security does not want them to be the sole method of authentication. For
unmanned entry points, which of the following solutions would work BEST?
129 A. Use voice print and a bollard
130 B. Use a retina scanner and a thumbprint
131 ☒ C. Use CCTV and a PIN
132 ☒ D. Use a retina scan and a PIN code
133
134 23. Ann, a security administrator, wants to limit access to the wireless network. Which
of the following can be used to do this without using certificates?
135 ☒ A. Employ EAP-TLS
136 B. Employ PEAP on all laptops
137 ☒ C. Enable MAC filtering
138 D. Disable SSID broadcasting
139
140 24. A user has an Android smartphone that supports full device encryption. However when
the user plugs into a computer all of the files are immediately accessible. Which of
the following should the user do to enforce full device confidentiality should the
phone be lost or stolen?
141 ☒ A. Establish a PIN passphrase
142 B. Agree to remote wipe terms
143 C. Generate new media encryption keys
144 D. Download the encryption control app from the store
145
146 25. The network manager has obtained a public IP address for use with a new system to
be available via the internet. This system will be placed in the DMZ and will
communicate with a database server on the LAN. Which of the following should be used to
allow fir proper communication between internet users and the internal systems?
147 A. VLAN
148 B. DNS
149 C. NAT
150 D. HTTP
151 ☒ E. SSL
152
153 26. After a new RADIUS server is added to the network, an employee is unable to connect

to the company's WPA2-Enterprise WIFI network, which is configured to prompt for the employee's network username and password. The employee reports receiving an error message after a brief connection attempt, but is never prompted for credentials. Which of the following issues could be causing the problem?

- ☒ A. The employee's account is locked out in the directory service
- B. The new RADIUS server is overloading the wireless access point
- C. The new RADIUS server's certificate is not trusted by the employee's PC
- D. The employee's account is disabled in the RADIUS server's local database

27. Ann the security administrator has been reviewing logs and has found several overnight sales personnel are accessing the finance department's network shares. Which of the following security controls should be implemented to BEST remediate this?

- A. Mandatory access
- B. Separation of duties
- C. Time of day restrictions
- ☒ D. Role based access

28. A fiber company has acquired permission to bury a fiber cable through a farmer's land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

- A. No farm animals will graze near the burial site of the cable
- ☒ B. No digging will occur near the burial site of the cable
- C. No buildings or structures will be placed on top of the cable
- D. No crops will be planted on top of the cable

29. The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

- A. Threat
- B. Risk
- C. Attack
- ☒ D. Vulnerability

30. A security technician would like to use ciphers that generate ephemeral keys for secure communication. Which of the following algorithms support ephemeral modes? (Choose two.)

- ☒ A. Diffie-Hellman
- B. RC4
- C. RIPEMD
- D. NTLMv2
- E. PAP
- ☒ F. RSA

31. A security technician would like an application to use random salts to generate short lived encryption keys during the secure communication handshake process to increase communication security. Which of the following concepts would BEST meet this goal?

- A. Ephemeral keys
- ☒ B. Symmetric Encryption Keys
- C. AES Encryption Keys
- D. Key Escrow

32. A security administrator wishes to implement a method of generating encryption keys from user passwords to enhance account security. Which of the following would accomplish this task?

- A. NTLMv2
- B. Blowfish
- ☒ C. Diffie-Hellman
- D. PBKDF2

33. A security technician wants to improve the strength of a weak key by making it more secure against brute force attacks. Which of the following would achieve this?

- A. Blowfish
- ☒ B. Key stretching
- C. Key escrow
- D. Recovery agent

34. A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the

- security posture during deployment? (Choose two.)
- 204 A. Deploy a honeypot
 - 205 ☒ B. Disable unnecessary services
 - 206 ☒ C. Change default passwords
 - 207 D. Implement an application firewall
 - 208 E. Penetration testing
 - 209
35. A local hospital with a large four-acre campus wants to implement a wireless network so that doctors can use tablets to access patients' medical data. The hospital also wants to provide guest access to the internet for hospital patients and visitors in select areas. Which of the following areas should be addressed FIRST?
- 211 A. MAC filters
 - 212 ☒ B. Site Survey
 - 213 C. Power level controls
 - 214 D. Antenna types
 - 215
36. After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he did not accidentally make a change during his investigation. Which of the following should he perform?
- 217 ☒ A. Take a hash of the image and compare it to the one being investigated
 - 218 B. Compare file sizes of all files prior to and after investigation
 - 219 C. Make a third image and compare it to the second image being investigated
 - 220 D. Compare the logs of the copy to the actual server
 - 221
37. Which of the following attacks is generally initiated from a botnet?
- 222 A. Cross site scripting attack
 - 223 B. HTTP header injection
 - 224 ☒ C. Distributed denial of service
 - 225 D. A war driving attack
 - 226
 - 227
38. A network security analyst has confirmed that the public facing web server has been compromised. Which of the following stages if the Incident Handling Response does this describe?
- 229 A. Analyzing
 - 230 ☒ B. Recovering
 - 231 ☒ C. Identification
 - 232 D. Mitigation
 - 233
39. Deploying compensating security controls is an example of:
- 234 A. Risk avoidance
 - 235 ☒ B. Risk mitigation
 - 236 C. Risk transference
 - 237 D. Risk acceptance
 - 238
 - 239
40. A web startup wants to implement single sign-on where its customers can log on to the site by using their personal and existing corporate email credentials regardless of which company they work for. Is this directly supported by SAML?
- 240 ☒ A. No not without extensive partnering and API integration with all required email providers
 - 241 B. Yes SAML is a web based single sign-on implementation exactly fir this purpose
 - 242 C. No a better approach would be to use required email providers LDAP or RADIUS repositories
 - 243 D. Yes SAML can use oauth2 to provide this functionality out of the box
 - 244
 - 245
41. A security administrator is installing a single camera outside in order to detect unauthorized vehicles in the parking lot. Which of the following is the MOST important consideration when deploying a CCTV camera to meet the requirement?
- 246 A. Training
 - 247 B. Expense
 - 248 C. Resolution
 - 249 ☒ D. Field of view
 - 250
 - 251
42. A system administrator wants to configure a setting that will make offline password cracking more challenging. Currently the password policy allows upper and lower case characters a minimum length of 5 and a lockout after 10 invalid attempts. Which of the following has the GREATEST impact on the time it takes to crack the passwords?
- 252 ☒ A. Increase the minimum password length to 8 while keeping the same character set
 - 253 B. Implement an additional password history and reuse policy
 - 254 C. Allow numbers and special characters in the password while keeping the minimum
 - 255

length at 5

256 D. Implement an account lockout policy after three unsuccessful logon attempts

257

258 43. Establishing a method to erase or clear memory is an example of securing which of the following?

259 A. Data in transit

260 ☒ B. Data at rest

261 C. Data in use

262 D. Data in motion

263

264 44. Joe processes several requisitions during the day and during the night shift they are approved by Ann. This is an example of which of the following?

265 ☒ A. Separation of duties

266 B. Discretionary access

267 C. Mandatory access

268 D. Time of day restrictions

269

270 45. A security administrator would like to write an access rule to block the three IP addresses given below. Which of the following combinations should be used to include all of the given IP addresses?

271 192.168.12.255

272 192.168.12.227

273 192.168.12.229

274 A. 192.168.12.0/25

275 B. 192.168.12.128.28

276 C. 192.168.12.224/29

277 D. 192.168.12.225/30

278

279 46. After installing a new Linux system, the administrator runs a command that records the size, permissions, and MD5 sum of all the files on the system. Which of the following describes what the administrator is doing?

280 A. Identifying vulnerabilities

281 B. Design review

282 ☒ C. Host software baselining

283 D. Operating system hardening

284

285 47. An intrusion has occurred in an internet facing system. The security administrator would like to gather forensic evidence while the system is still in operation. Which of the following procedures should the administrator perform FIRST on the system?

286 A. Make a drive image

287 B. Take hashes of system data

288 C. Collect information in RAM

289 ☒ D. Capture network traffic

290

291 48. Which of the following wireless standards is backwards compatible with 802.11g?

292 A. 802.11a

293 ☒ B. 802.11b

294 C. 802.11n

295 D. 802.11q

296

297 49. Joe uses his badge to enter the server room, Ann follows Joe entering without using her badge. It is later discovered that Ann used a USB drive to remove confidential data from a server. Which of the following principles is potentially being violated? (Choose two.)

298 A. Clean desk policy

299 B. Least privilege

300 ☒ C. Tailgating

301 D. Zero-day exploits

302 E. Data handling

303

304 50. The below report indicates that the system is MOST likely infected by which of the following?

305 Protocol -- LOCAL IP -- FOREIGN IP -- STATE

306 TCP -- 0.0.0.0:445 -- 0.0.0.0:0 -- Listening

307 TCP -- 0.0.0.0:3390 -- 0.0.0.0:0 -- Listening

308 ☒ A. Trojan

309 B. Worm

310 C. Logic bomb

311 D. Spyware

312
313 51. A security administrator is required to submit a detailed implementation plan and
back out plan to get approval prior to updating the firewall and other security
314 devices. Which of the following types of risk mitigation strategies is being followed?
315 A. Change management
316 B. Routine audit
317 C. Rights and permissions review
318 ☒ D. Configuration management
319
320 52. Which of the following authentication services uses a default TCP of 389?
321 A. SAML
322 B. TACACS+
323 C. Kerberos
324 ☒ D. LDAP
325
326 53. A software company sends their offsite backup tapes to a third party storage
facility. TO meet confidentiality the tapes should be:
327 ☒ A. Labeled
328 B. Hashed
329 C. Encrypted
330 D. Duplicated
331
332 54. Ann, a technician, wants to implement a single protocol on a remote server which
will enable her to encrypt and proxy all of her traffic though the remote server via
SOCKS5. Which of the following should Ann enable to support both encryption and proxy
333 services?
334 ☒ A. SSH
335 B. IPSEC
336 C. TLS
337 D. HTTPS
338
339 55. Ann, a system analyst, discovered the following log. Which of the following or
techniques does this indicate?
340 {bpl@localmachine}\$ ls-al
341 Total 12
342 Drwxrwxr-x
343 ☒ A. Protocol analyzer
344 B. Port scanner
345 C. Vulnerability
346 D. Banner grabbing
347
348 56. A company discovers an unauthorized device accessing network resources through one
of many network drops in a common area used by visitors. The company decides that is
wants to quickly prevent unauthorized devices from accessing the network but policy
prevents the company from making changes on every connecting client. Which of the
349 following should the company implement?
350 ☒ A. Port security
351 B. WPA2
352 C. Mandatory Access Control
353 D. Network Intrusion Prevention
354
355 57. The helpdesk is receiving numerous reports that a newly installed biometric reader
at the entrance of the data center has a high of false negatives. Which of the
356 following is the consequence of this reported problem?
357 ☒ A. Unauthorized employees have access to sensitive systems
358 B. All employees will have access to sensitive systems
359 C. No employees will be able to access the datacenter
360 D. Authorized employees cannot access sensitive systems
361
362 58. A software developer places a copy of the source code for a sensitive internal
application on a company laptop to work remotely. Which of the following policies is
MOST likely being violated?
363 ☒ A. Clean desk
364 B. Data handling
365 C. Chain of custody
366 D. Social media
367
368 59. While testing a new host based firewall configuration a security administrator
inadvertently blocks access to localhost which causes problems with applications

running on the host. Which of the following addresses refer to localhost?

365 A. ::0
366 B. 127.0.0.0
367 ☒ C. 127.0.0.1
368 D. 127.0.0/8
369 E. 127::0.1
370

371 60. A user has reported inadvertently sending an encrypted email containing PII to an incorrect distribution group. Which of the following potential incident types is this?

372 A. Data sharing
373 ☒ B. Unauthorized viewing
374 C. Data breach
375 D. Unauthorized access
376

377 61. A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?

378 A. Credential management
379 B. Support ownership
380 C. Device access control
381 ☒ D. Antivirus management
382

383 62. A security engineer discovers that during certain times of day, the corporate wireless network is dropping enough packets to significantly degrade service. Which of the following should be the engineer's FIRST step in troubleshooting the issues?

384 A. Configure stronger encryption
385 ☒ B. Increase the power level
386 C. Change to a higher gain antenna
387 D. Perform a site survey
388

389 63. A security administrator is reviewing the web logs and notices multiple attempts by users to access:
390 <http://www.comptia.org/idapsearch?user->
391

392 Having identified the attack, which of the following will prevent this type of attack on the web server?

393 ☒ A. Input validation on the web server
394 B. Block port 389 on the firewall
395 C. Segregate the web server by a VLAN
396 D. Block port 3389 on the firewall
397

398 64. A breach at a credit card company resulted in customers credit card information being exposed . The company has conducted a full forensic investigation and identified the source of the breach. Which of the following should the company do NEXT?

399 A. Move to the incident identification phase
400 B. Implement the risk assessment plan
401 ☒ C. Implement damage and loss control procedures
402 D. Implement first responder processes
403

404 65. Joe a user upon arriving to work on Monday morning noticed several files were deleted from the system. There were no records of any scheduled network outages or upgrades to the system. Joe notifies the security department of the anomaly found and removes the system from the network. Which of the following is the NEXT action that Joe should perform?

405 ☒ A. Screenshots of systems
406 B. Call the local police
407 C. Perform a backup
408 D. Capture system image
409

410 66. The user of a news service accidentally accesses another user's browsing history. From this the user can tell what competitors are reading, querying, and researching. The news service has failed to properly implement which of the following?

411 A. Application white listing
412 B. In-transit protection
413 ☒ C. Access controls
414 D. Full disk encryption
415

416 67. A system requires administrators to be logged in as the "root" in order to make administrator changes. Which of the following controls BEST mitigates the risk

- associated with this scenario?
- 417 A. Require that all administrators keep a log book of times and justification for
accessing root
- 418 B. Encrypt all users home directories using file-level encryption
- 419 C. Implement a more restrictive password rotation policy for the shared root account
- 420 ☒ D. Force administrator to log in with individual accounts and switch to root
- 421 E. Add the administrator to the local group
- 422
- 423 68. A defense contractor wants to use one of its classified systems to support programs
from multiple intelligence agencies. Which of the following MUST be in place between
the intelligence agencies to allow this?
- 424 A. A DRP
- 425 B. An SLA
- 426 ☒ C. A MOU
- 427 D. A BCP
- 428
- 429 69. A penetration tester was able to obtain elevated privileges on a client workstation
and multiple servers using the credentials of an employee. Which of the following
controls would mitigate these issues? (Choose two.)
- 430 A. Separation of duties
- 431 ☒ B. Least privilege
- 432 C. Time of day restrictions
- 433 ☒ D. Account expiration
- 434 E. Discretionary access control
- 435 F. Password history
- 436
- 437 70. Which of the following is considered the MOST effective practice when securing
printers or scanners in an enterprise environment?
- 438 ☒ A. Routine vulnerability scanning of peripherals
- 439 B. Install in a hardened network segment
- 440 C. Turn off the power to the peripherals at night
- 441 D. Enable print sharing only from workstations
- 442
- 443 71. After a few users report problems with the wireless network, a system administrator
notifies that a new wireless access point has been powered up in the cafeteria. The
access point has the same SSID as the corporate network and is set to the same channel
as nearby access points. However, the AP has not been connected to the Ethernet
network. Which of the following is the MOST likely cause of the user's wireless problems?
- 444 A. AP channel bonding
- 445 ☒ B. An evil twin attack
- 446 C. Wireless interference
- 447 D. A rogue access point
- 448
- 449 72. A network technician at a company, Joe is working on a network device. He creates a
rule to prevent users from connecting to a toy website during the holiday shopping
season. This website is blacklisted and is known to have SQL injections and malware.
Which of the following has been implemented?
- 450 A. Mandatory access
- 451 B. Network separation
- 452 ☒ C. Firewall rules
- 453 D. Implicit Deny
- 454
- 455 73. Company XYZ has suffered leaks of internally distributed confidential documents.
Ann the network security analyst has been tasked to track down the culprit. She has
decided to embed a four letter string of characters in documents containing proprietary
information. Which of the following initial steps should Ann implement before sending
documents?
- 456 A. Store one of the documents in a honey pot
- 457 B. Start antivirus scan on all the suspected computers
- 458 ☒ C. Add a signature to the NIDS containing the four letter string
- 459 D. Ask employees to report suspicious behaviors
- 460
- 461 74. Which of the following should a company deploy to prevent the execution of some
types of malicious code?
- 462 A. Least privilege accounts
- 463 B. Host-based firewalls
- 464 C. Intrusion Detection systems
- 465 ☒ D. Application white listing
- 466

467 75. An administrator is investigating a system that may potentially be compromised and
sees the following log entries on the router.
468 Jul 15 14:47:29.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet
0/3) - > 10.10.1.5 (6667), 3 packets.
469 Jul 15 14:47:38.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet
0/3) - > 10.10.1.5 (6667), 6 packets.
470 Jul 15 14:47:45.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet
0/3) - > 10.10.1.5 (6667), 8 packets.
471
472 Which of the following BEST describes the compromised system?
473 A. It is running a rogue web server
474 B. It is being used in a man-in-the-middle attack
475 ☒ C. It is participating in a botnet
476 D. It is an ARP poisoning attack
477
478 76. Ann the IT director wants to ensure that as hoc changes are not making their way to
the production applications. Which of the following risk mitigation strategies should
she implement in her department?
479 ☒ A. Change management
480 B. Permission reviews
481 C. Incident management
482 D. Perform routine audits
483
484 77. Which of the following would allow users from outside of an organization to have
access to internal resources?
485 A. NAC
486 B. VLANs
487 ☒ C. VPN
488 D. NAT
489
490 78. Which of the following is BEST described by a scenario where management chooses not
to implement a security control for a given risk?
491 A. Mitigation
492 B. Avoidance
493 ☒ C. Acceptance
494 D. Transference
495
496 79. When confidentiality is the primary concern which of the following types of
encryption should be chosen?
497 A. Digital Signature
498 B. Symmetric
499 ☒ C. Asymmetric
500 D. Hashing
501
502 80. A Windows- based computer is infected with malware and is running too slowly to
boot and run a malware scanner. Which of the following is the BEST way to run the
malware scanner?
503 A. Kill all system processes
504 B. Enable the firewall
505 ☒ C. Boot from CD/USB
506 D. Disable the network connection
507
508 81. Ann a member of the Sales Department has been issued a company-owned laptop for use
when traveling to remote sites. Which of the following would be MOST appropriate when
configuring security on her laptop?
509 A. Configure the laptop with a BIOS password
510 B. Configure a host-based firewall on the laptop
511 C. Configure the laptop as a virtual server
512 ☒ D. Configure a host-based IDS on the laptop
513
514 82. A security technician has removed the sample configuration files from a database
server. Which of the following application security controls has the technician
attempted?
515 ☒ A. Application hardening
516 B. Application baselines
517 C. Application patch management
518 D. Application input validation
519
520 83. Data confidentiality must be enforced on a secure database. Which of the following

controls meets this goal? (Choose two.)

- 521 ☒ A. MAC
- 522 ☐ B. Lock and key
- 523 ☒ C. Encryption
- 524 ☐ D. Non-repudiation
- 525 ☐ E. Hashing

526

527 84. A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site do not record any footage. Which of the following types of controls was being used?

- 528 ☐ A. Detective
- 529 ☐ B. Corrective
- 530 ☒ C. Deterrent
- 531 ☐ D. Preventive

532

533 85. A network security administrator is trying to determine how an attacker gained access to the corporate wireless network. The network is configured with SSID broadcast disabled. The senior network administrator explains that this configuration setting would only have deterred an unsophisticated attacker because of which of the following?

- 534 ☒ A. The SSID can be obtained with a wireless packet analyzer.
- 535 ☐ B. The required information can be brute forced over time.
- 536 ☐ C. Disabling the SSID only hides the network from other WAPs.
- 537 ☐ D. The network name could be obtained through a social engineering campaign.

538

539 86. Joe a system administrator receives reports that users attempting to reach the corporate website are arriving at an unfamiliar website instead. An investigation by a forensic analyst found that the name server log has several corporate IP addresses that were changed using Joe's credentials. Which of the following is this attack called?

- 540 ☐ A. Xmas attack
- 541 ☒ B. DNS poisoning
- 542 ☐ C. Web server attack
- 543 ☐ D. Spoofing attack

544

545 87. Joe a technician initiated scans if the company's 10 routers and discovered that half if the routers were not changed from their default configuration prior installed on the network. Which of the following would address this?

- 546 ☒ A. Secure router configuration
- 547 ☐ B. Implementing 802.1x
- 548 ☐ C. Enabling loop protection
- 549 ☐ D. Configuring port security

550

551 88. An employee attempts to go to a well-known bank site using the company-standard web browser by correctly typing in the address of the site into the web browser. The employee is directed to a website that looks like the bank's site but is not the actual bank site. The employee's user name and password are subsequently stolen. This is an example of which of the following?

- 552 ☐ A. Watering hole attack
- 553 ☐ B. Cross-site scripting
- 554 ☒ C. DNS poisoning
- 555 ☐ D. Man-in-the-middle attack

556

557 89. A user authenticates to a local directory server. The user then opens a virtualization client to connect to a virtual server. Instead of supplying a username/password combination, the user simply checks a "use directory credentials" checkbox to authenticate to the virtual server. Which of the following authentication types has been utilized?

- 558 ☐ A. Transitive trust
- 559 ☐ B. Common access card
- 560 ☐ C. Multifactor authentication
- 561 ☒ D. Single sign-on

562

563 90. The new Chief Information Officer (CIO) of company ABC, Joe has noticed that company XWY is always one step ahead with similar products. He tasked his Chief Security Officer to implement new security controls to ensure confidentiality of company ABC's proprietary data and complete accountability for all data transfers. Which of the following security controls did the Chief Security Officer implement to BEST meet these requirements? (Choose Two)

- 564 ☐ A. Redundancy
- 565 ☒ B. Hashing

566 C. DRP
567 D. Digital Signatures
568 ☒ E. Encryptions
569
570 91. A worker dressed in a fire suppression company's uniform asks to be let into the server room to perform the annual check in the fire extinguishers. The system administrator allows the worker into the room, only to discover hours later that the worker was actually a penetration tester. Which of the following reasons allowed the penetration tester to access the server room?

571 A. Testing the fire suppression system represented a critical urgency
572 ☒ B. The pen tester assumed the authority of a reputable company
573 C. The pen tester used an intimidation technique on the administrator
574 D. The administrator trusted that the server room would remain safe
575

576 92. A company uses port security based on an approved MAC list to secure its wired network and WPA2 to secure its wireless network. Which of the following prevents an attacker from learning authorized MAC addresses?

577 ☒ A. Port security prevents access to any traffic that might provide an attacker with authorized MAC addresses
578 B. Port security uses certificates to authenticate devices and is not part of a wireless protocol
579 C. Port security relies in a MAC address length that is too short to be cryptographically secure over wireless networks
580 D. Port security encrypts data on the network preventing an attacker from reading authorized MAC addresses
581

582 93. A security technician is implementing PKI on a Network. The technician wishes to reduce the amount of bandwidth used when verifying the validity of a certificate. Which of the following should the technician implement?

583 A. CSR
584 B. Key escrow
585 ☒ C. OSCR
586 ☒ D. CRL
587

588 94. The network security manager has been notified by customer service that employees have been sending unencrypted confidential information via email. Which of the following should the manager select to BEST detect and provide notification of these occurrences?

589 ☒ A. DLP
590 B. SSL
591 C. DEP
592 D. UTM
593

594 95. While troubleshooting a new wireless 802.11 ac network an administrator discovers that several of the older systems cannot connect. Upon investigation the administrator discovers that the older devices only support 802.11 and RC4. The administrator does not want to affect the performance of the newer 802.11 ac devices on the network. Which of the following should the administrator do to accommodate all devices and provide the MOST security?

595 A. Disable channel bonding to allow the legacy devices and configure WEP fallback
596 B. Configure the AP in protected mode to utilize WPA2 with CCMP
597 ☒ C. Create a second SSID on the AP which utilizes WPA and TKIP
598 D. Configure the AP to utilize the 5Gh band only and enable WEP
599

600 96. A security administrator is troubleshooting an authentication issues using a network sniffer. The security administrator reviews a packet capture of the authentication process and notices that authentication is performed using extensible markup over SOAP. Which of the following authentication services is the security administrator troubleshooting?

601 ☒ A. SAML
602 B. XTACACS
603 ☒ C. Secure LDAP
604 D. RADIUS
605

606 97. Given a class C network a technician has been tasked with creating a separate subnet for each of the eight departments in the company. Which of the following network masks would allow for each department to have a unique network space and what is the maximum number of hosts each department could have?

607 A. Network 255.255.255.192, 62 hosts

- 608 ☒ B. Network 255.255.255.224, 30 hosts
609 C. Network 255.255.255.240, 16 hosts
610 D. Network 255.255.255.248, 32 hosts
611
612 98. A software security concern when dealing with hardware and devices that have embedded software or operating systems is:
613 ☒ A. Patching may not always be possible
614 B. Configuration support may not be available
615 C. There is no way to verify if a patch is authorized or not
616 D. The vendor may not have a method for installation of patches
617
618 99. A major medical corporation is investigating deploying a web based portal for patients to access their medical records. The medical corporation has a long history of maintaining IT security but is considering having a third party vendor create the web portal. Which of the following areas is MOST important for the Chief Information Security Officer to focus on when reviewing proposal from vendors interested in creating the web portal?
619 A. Contractor background check
620 ☒ B. Confidentiality and availability
621 C. Redundancy and privacy
622 D. Integrity and confidentiality
623
624 100. Which of the following authentication methods requires the user, service provider and an identity provider to take part in the authentication process?
625 A. RADIUS
626 ☒ B. SAML
627 C. Secure LDAP
628 D. Kerberos
629

