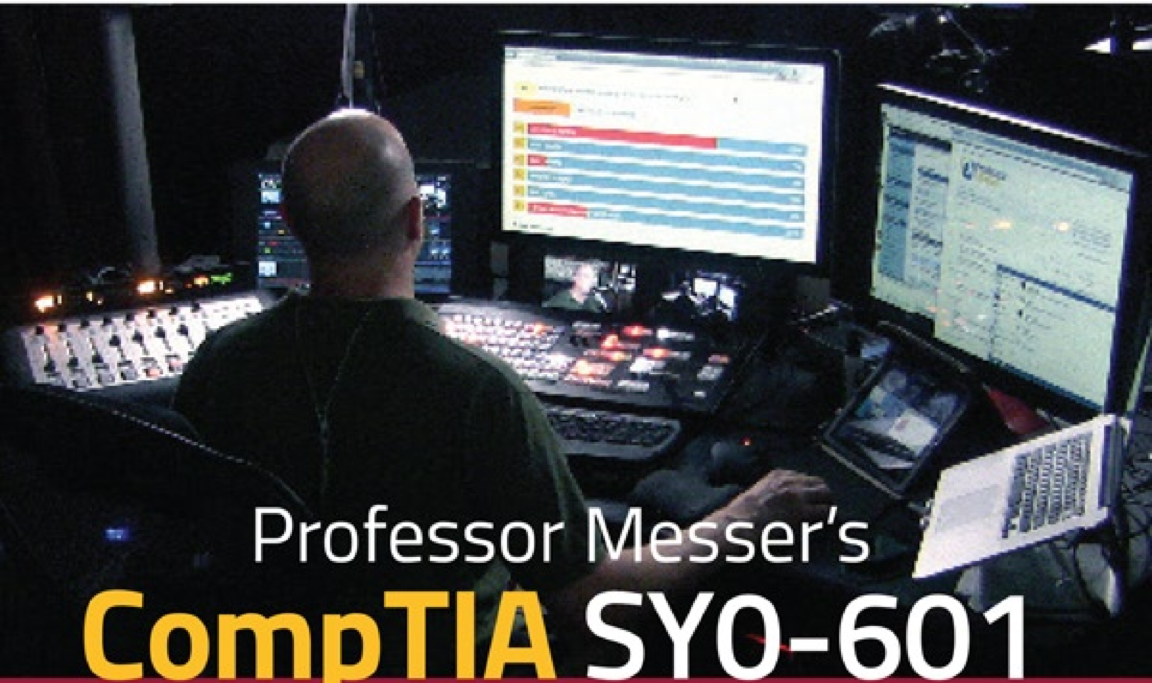
Professor Messer



Professor Messer's CompTIA SY0-601 Security+ Practice Exams

James "Professor" Messer

Professor Messer's CompTIA SY0-601 Security+ Practice Exams

by James "Professor" Messer

Professor Messer
http://www.ProfessorMesser.com

Professor Messer's CompTIA SY0-601 Security+ Practice Exams
Written by James "Professor" Messer

First Edition: June 2021
This is version 1.00

Trademark Acknowledgments

Warning and Disclaimer

This book is designed to provide information about the CompTIA SY0-601 Security+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

About the Author

James Messer is an information technology veteran whose career has included supercomputer operations, system administration, network management, and IT security.

James is also the founder and CEO of Messer Studios, a leading publisher of training materials for IT certification exams. With over 110 million videos viewed and over 500,000 subscribers, Professor Messer's training has helped thousands of students realize their goals of a profession in information technology.

Introduction

The process of answering a test question is our ultimate test of knowledge. After hours of video watching, book reading, and note taking, do you really know the material? If you're trying to prove yourself, nothing beats getting the right answer.

This book contains three sample exams containing performance-based and multiple-choice questions for the Security+ exam. I've personally curated every question to make sure this Q&A matches the expectations of the SY0-601 Security+ exam.

I hope this book will help you be the smartest one in the room. Best of luck with your studies!

- Professor Messer

The CompTIA SY0-601 Security+ Certification

CompTIA's Security+ certification is the entry point for IT security professionals. If you're planning on securing the data and networks on the world's largest networks, then you're in the right place.

Earning the Security+ certification requires the completion of one exam covering a broad range of security topics. After completing the certification, a CompTIA Security+ certified professional will have an understanding of attack types, network security technologies, secure network architecture concepts, cryptography, and much more.

Here's the breakdown of each domain and the percentage of each topic on the SY0-601 exam:

Domain 1.0 - Threats, Attacks, and Vulnerabilities - 24%
Domain 2.0 - Architecture and Design - 21%
Domain 3.0 - Implementation - 25%
Domain 4.0 - Operations and Incident Response - 16%
Domain 5.0 - Governance, Risk, and Compliance - 14%

How to Use This Book

This book contains three separate 90-question practice exams; Exam A, Exam B, and Exam C. The exams are designed to emulate the format and complexity of the actual Security+ exam.

- Take one exam at a time. The difficulty levels are similar between exam, so it doesn't matter which exam you take first.

- The actual Security+ exam is 90 minutes in length, so try setting a timer when you start your practice exam. Time management is an important part of the exam.

- The first section of each practice exam is the list of questions. There's a link after every question that will jump immediately to the quick answer page or the detailed answer page. If you're using the digital version, your PDF reader keys can quickly jump back to the question page. Adobe Reader in Windows uses **Alt-Left arrow** and macOS Preview uses **Command-[** to move back to the previous view. Be sure to check your PDF reader for specific navigation options.

- The quick answer page is a consolidated list of the answers without any detail or explanation. If you want to quickly check your answer sheet, this is the page for you.

- A detailed answer is available for each exam question. This section repeats the question, the possible answers, and shows the answer with a detailed explanation. This section is formatted to show only one answer per page to avoid giving away the answer to any other questions. Digital readers can use your PDF reader's back button to quickly jump back to the questions.

- As you go through the exam, write down the answers on a separate sheet of paper or separate text editor window. Some PDF readers also support on-screen annotation. You can check the answers after the 90 minutes have elapsed.

- You can grade your results against the quick answer page. For incorrect responses, be sure to check the detailed answer pages for information on why certain answers were considered correct or incorrect.

- After each detailed answer, a video link is available for more information on the topic. You can click the link in your PDF or use your camera to view the QR (Quick Response) code on the page. Your camera app will provide a notification message that will launch the video page in your browser. The URL is also provided for manual entry.

You have the option of using each practice test as a 90 minute timed exam, or as a casual Q&A. Try stepping through each question, picking an answer, and then jumping to the detailed explanation to learn more about each possible answer.

Here's a scoring chart:

> **Less than 63 questions correct / 70% and lower** - Use the exam objectives at the end of each detailed answer to determine where you might need some additional help.
>
> **63 to 72 questions correct / 70% to 80%** - You're so close! Keep working on the areas you're missing and fill in those gaps.
>
> **73 to 81 questions correct / 80% to 90%** - This is a strong showing, but some additional studying will help you earn points on the real exam.
>
> Although the actual Security+ exam does not calculate the final score as a percentage, getting an 85% on the practice exam can be considered a passing grade.
>
> **More than 81 questions correct / over 90%** - You're ready for the real thing! Book your exam and earn your Security+ certification!

The detailed answer pages break down every correct answer and every incorrect answer. Although it's useful to know when you got a question right, it's more important if you understand exactly why a question was marked wrong. If you understand all of the technologies on these sample exams, then you'll be ready for the real thing.

Practice Exam A

Performance-Based Questions

A1. Match the description with the most accurate attack type.
Not all attack types will be used.

Attack Types:

Hoax	**Social Engineering**
Spam	**Spoofing**
Vishing	**Supply Chain**
On-path	**DDoS**

Attacker obtains bank account number
and birth date by calling the victim

Select an Attack Type

Attacker modifies a legitimate DNS server to resolve
the IP address of a malicious site

Select an Attack Type

Attacker intercepts all communication between
a client and a web server

Select an Attack Type

Multiple attackers
overwhelm a web server

Select an Attack Type

A virus alert appears in your browser from Microsoft
with a phone number to call for support

Select an Attack Type

Answer Page: **35**

A2. The security team at a local public library system is creating a set of minimum security standards for the various computer systems.

Select the BEST security control for each available placeholder. **All of the available security controls will be used once.**

Security Controls:

- Biometric Reader
- Environmental Sensors
- Cable Lock
- Full-Disk Encryption
- Video Surveillance
- Locking Cabinets
- Smart Card

Location	Description		Security Controls
Library Web Server and Database Server	Computer Room High security		
Library Employee Laptops	Offsite use Contains PII		
Library Lending Systems	Manages the check-in and check-out process		
Digital Newspaper Reading Lab	Open Area No supervision Laptop computers		

Answer Page: **37**

A3. Fill in the blank with the BEST secure network protocol for the description:

__________ Accept customer purchases from your primary website

__________ Synchronize the time across all of your devices

__________ Access your switch using a CLI terminal screen

__________ Talk with customers on scheduled conference calls

__________ Gather metrics from routers at remote sites

Answer Page: **39**

A4. Match the appropriate authentication reference to each description. Each authentication factor or attribute will be used once.

Something you can do | Somewhere you are

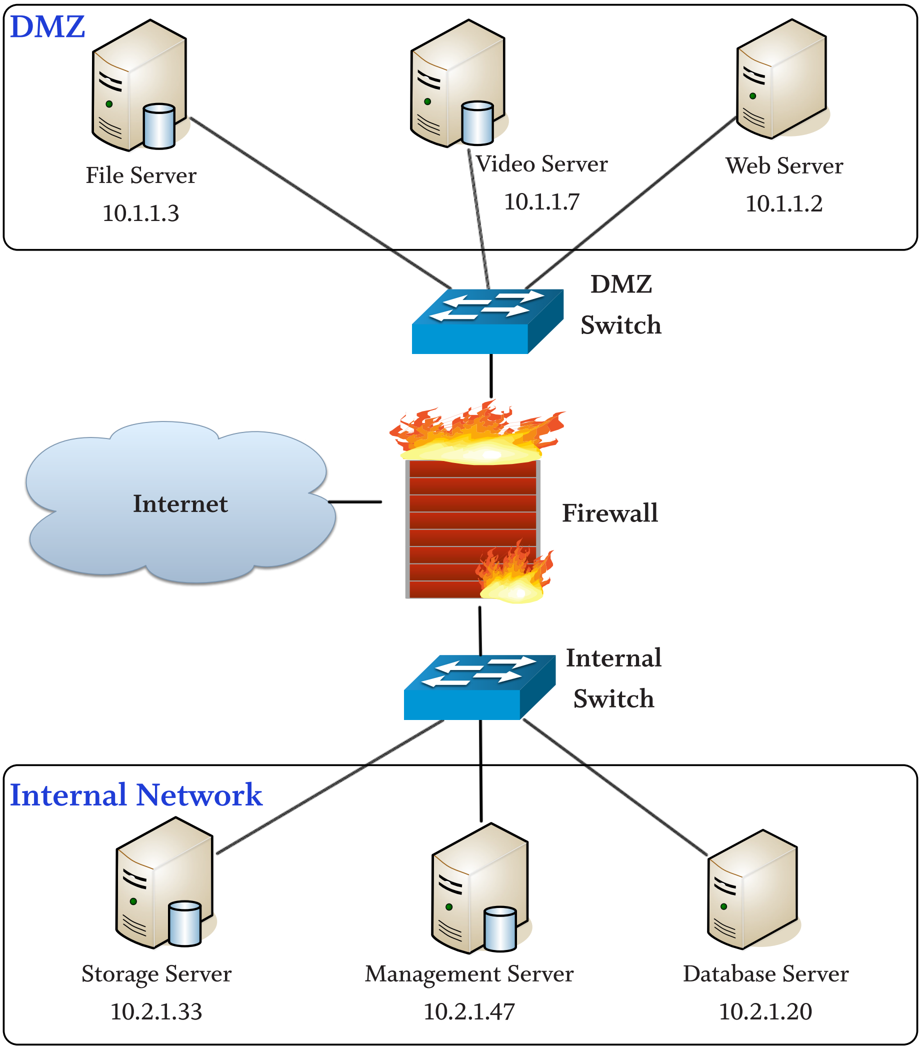
Something you have | Something you know | Something you are

Description	Authentication Factor
During the login process, your phone receives a text message with a one-time passcode	
You enter your PIN to make a deposit into an ATM	
You must sign a check-in sheet before entering a controlled area	
You can use your fingerprint to unlock the door to the data center	
Your login will not work unless you are connected to the VPN	

Answer Page: **40**

A5. Configure the following stateful firewall rules:

- Allow the Web Server to access the Database Server using LDAP
- Allow the Storage Server to transfer files to the Video Server over HTTPS
- Allow the Management Server to use a secure terminal on the File Server



Rule #	Source IP	Destination IP	Protocol (TCP/ UDP)	Port #	Allow/ Block
1					
2					
3					

Answer Page: **41**

Practice Exam A

Multiple Choice Questions

A6. You've hired a third-party to gather information about your company's servers and data. The third-party will not have direct access to your internal network but can gather information from any other source.
Which of the following would BEST describe this approach?

❍ **A.** Backdoor testing

❍ **B.** Passive footprinting

❍ **C.** OS fingerprinting

❍ **D.** Partially known environment

Quick Answer: **33**

The Details: **43**

A7. Which of these protocols use TLS to provide secure communication? (Select TWO)

❍ **A.** HTTPS

❍ **B.** SSH

❍ **C.** FTPS

❍ **D.** SNMPv2

❍ **E.** DNSSEC

❍ **F.** SRTP

Quick Answer: **33**

The Details: **44**

A8. Which of these threat actors would be MOST likely to attack systems for direct financial gain?

❍ **A.** Organized crime

❍ **B.** Hacktivist

❍ **C.** Nation state

❍ **D.** Competitor

Quick Answer: **33**

The Details: **45**

A9. A security incident has occurred on a file server. Which of the following data sources should be gathered to address file storage volatility? (Select TWO)

❍ **A.** Partition data

❍ **B.** Kernel statistics

❍ **C.** ROM data

❍ **D.** Temporary file systems

❍ **E.** Process table

Quick Answer: **33**

The Details: **46**

A10. An IPS at your company has found a sharp increase in traffic from all-in-one printers. After researching, your security team has found a vulnerability associated with these devices that allows the device to be remotely controlled by a third-party. Which category would BEST describe these devices?

❍ **A.** IoT

❍ **B.** RTOS

❍ **C.** MFD

❍ **D.** SoC

Quick Answer: **33**

The Details: **47**

A11. Which of the following standards provides information on privacy and managing PII?

❍ **A.** ISO 31000

❍ **B.** ISO 27002

❍ **C.** ISO 27701

❍ **D.** ISO 27001

Quick Answer: **33**

The Details: **48**

A12. Elizabeth, a security administrator, is concerned about the potential for data exfiltration using external storage drives. Which of the following would be the BEST way to prevent this method of data exfiltration?

❍ **A.** Create an operating system security policy to prevent the use of removable media

❍ **B.** Monitor removable media usage in host-based firewall logs

❍ **C.** Only allow applications that do not use removable media

❍ **D.** Define a removable media block rule in the UTM

Quick Answer: **33**

The Details: **49**

A13. A CISO (Chief Information Security Officer) would like to decrease the response time when addressing security incidents. Unfortunately, the company does not have the budget to hire additional security engineers. Which of the following would assist the CISO with this requirement?

❍ **A.** ISO 27701

❍ **B.** PKI

❍ **C.** IaaS

❍ **D.** SOAR

Quick Answer: **33**

The Details: **50**

A14. An insurance company has created a set of policies to handle data breaches. The security team has been given this set of requirements based on these policies:

- Access records from all devices must be saved and archived
- Any data access outside of normal working hours must be immediately reported
- Data access must only occur inside of the country
- Access logs and audit reports must be created from a single database

Which of the following should be implemented by the security team to meet these requirements? (Select THREE)

❍ **A.** Restrict login access by IP address and GPS location

❍ **B.** Require government-issued identification during the onboarding process

❍ **C.** Add additional password complexity for accounts that access data

❍ **D.** Conduct monthly permission auditing

❍ **E.** Consolidate all logs on a SIEM

❍ **F.** Archive the encryption keys of all disabled accounts

❍ **G.** Enable time-of-day restrictions on the authentication server

Quick Answer: **33**

The Details: **51**

A15. Rodney, a security engineer, is viewing this record from the firewall logs:

```
UTC 04/05/2018 03:09:15809   AV Gateway Alert
136.127.92.171  80 -> 10.16.10.14  60818
Gateway Anti-Virus Alert:
XPACK.A_7854 (Trojan) blocked.
```

Which of the following can be observed from this log information?

❍ **A.** The victim's IP address is 136.127.92.171

❍ **B.** A download was blocked from a web server

❍ **C.** A botnet DDoS attack was blocked

❍ **D.** The Trojan was blocked, but the file was not

Quick Answer: **33**

The Details: **53**

A16. A user connects to a third-party website and receives this message:

```
Your connection is not private.
NET::ERR_CERT_INVALID
```

Which of the following attacks would be the MOST likely reason
for this message?

❍ **A.** Brute force

❍ **B.** DoS

❍ **C.** On-path

❍ **D.** Disassociation

Quick Answer: **33**

The Details: **54**

A17. Which of the following would be the BEST way to provide a website login using existing credentials from a third-party site?

❍ **A.** Federation

❍ **B.** 802.1X

❍ **C.** PEAP

❍ **D.** EAP-FAST

Quick Answer: **33**

The Details: **55**

A18. A system administrator, Daniel, is working on a contract that will specify a minimum required uptime for a set of Internet-facing firewalls. Daniel needs to know how often the firewall hardware is expected to fail between repairs. Which of the following would BEST describe this information?

❍ **A.** MTBF

❍ **B.** RTO

❍ **C.** MTTR

❍ **D.** MTTF

Quick Answer: **33**

The Details: **56**

A19. An attacker calls into a company's help desk and pretends to be the director of the company's manufacturing department. The attacker states that they have forgotten their password and they need to have the password reset quickly for an important meeting. What kind of attack would BEST describe this phone call?

❍ **A.** Social engineering

❍ **B.** Tailgating

❍ **C.** Vishing

❍ **D.** On-path

Quick Answer: **33**

The Details: **57**

A20. A security administrator has been using EAP-FAST wireless authentication since the migration from WEP to WPA2. The company's network team now needs to support additional authentication protocols inside of an encrypted tunnel. Which of the following would meet the network team's requirements?

❍ **A.** EAP-TLS

❍ **B.** PEAP

❍ **C.** EAP-TTLS

❍ **D.** EAP-MSCHAPv2

Quick Answer: **33**

The Details: **58**

A21. Which of the following would be commonly provided by a CASB? (Select TWO)

❍ **A.** List of all internal Windows devices that have not installed the latest security patches

❍ **B.** List of applications in use

❍ **C.** Centralized log storage facility

❍ **D.** List of network outages for the previous month

❍ **E.** Verification of encrypted data transfers

❍ **F.** VPN connectivity for remote users

Quick Answer: **33**

The Details: **59**

A22. The embedded OS in a company's time clock appliance is configured to reset the file system and reboot when a file system error occurs. On one of the time clocks, this file system error occurs during the startup process and causes the system to constantly reboot. Which of the following BEST describes this issue?

❍ **A.** DLL injection

❍ **B.** Resource exhaustion

❍ **C.** Race condition

❍ **D.** Weak configuration

Quick Answer: **33**

The Details: **60**

A23. A recent audit has found that existing password policies do not include any restrictions on password attempts, and users are not required to periodically change their passwords. Which of the following would correct these policy issues? (Select TWO)

❍ **A.** Password complexity

❍ **B.** Password expiration

❍ **C.** Password history

❍ **D.** Password lockout

❍ **E.** Password recovery

Quick Answer: **33**

The Details: **61**

A24. What kind of security control is associated with a login banner?

❍ **A.** Preventive

❍ **B.** Deterrent

❍ **C.** Corrective

❍ **D.** Detective

❍ **E.** Compensating

❍ **F.** Physical

Quick Answer: **33**

The Details: **62**

A25. A security team has been provided with a non-credentialed vulnerability scan report created by a third-party. Which of the following would they expect to see on this report?

❍ **A.** A summary of all files with invalid group assignments

❍ **B.** A list of all unpatched operating system files

❍ **C.** The version of web server software in use

❍ **D.** A list of local user accounts

Quick Answer: **33**

The Details: **63**

A26. A business manager is documenting a set of steps for processing orders if the primary Internet connection fails. Which of these would BEST describe these steps?

❍ **A.** Communication plan

❍ **B.** Continuity of operations

❍ **C.** Stakeholder management

❍ **D.** Tabletop exercise

Quick Answer: **33**

The Details: **64**

A27. A security administrator is concerned about data exfiltration resulting from the use of malicious phone charging stations. Which of the following would be the BEST way to protect against this threat?

❍ **A.** USB data blocker

❍ **B.** Personal firewall

❍ **C.** MFA

❍ **D.** FDE

Quick Answer: **33**

The Details: **65**

A28. A company would like to protect the data stored on laptops used in the field. Which of the following would be the BEST choice for this requirement?

❍ **A.** MAC

❍ **B.** SED

❍ **C.** CASB

❍ **D.** SOAR

Quick Answer: **33**

The Details: **66**

A29. A file server has a full backup performed each Monday at 1 AM. Incremental backups are performed at 1 AM on Tuesday, Wednesday, Thursday, and Friday. The system administrator needs to perform a full recovery of the file server on Thursday afternoon. How many backup sets would be required to complete the recovery?

❍ **A.** 2

❍ **B.** 3

❍ **C.** 4

❍ **D.** 1

Quick Answer: **33**

The Details: **67**

A30. A company is creating a security policy that will protect all corporate mobile devices:

- All mobile devices must be automatically locked after a predefined time period.
- Some mobile devices will be used by the remote sales teams, so the location of each device needs to be traceable.
- All of the user's information should be completely separated from company data.

Which of the following would be the BEST way to establish these security policy rules?

❍ **A.** Containerization

❍ **B.** Biometrics

❍ **C.** COPE

❍ **D.** VDI

❍ **E.** Geofencing

❍ **F.** MDM

Quick Answer: **33**

The Details: **68**

A31. A security engineer runs a monthly vulnerability scan. The scan doesn't list any vulnerabilities for Windows servers, but a significant vulnerability was announced last week and none of the servers are patched yet. Which of the following best describes this result?

❍ **A.** Exploit

❍ **B.** Credentialed

❍ **C.** Zero-day attack

❍ **D.** False negative

Quick Answer: **33**

The Details: **70**

A32. A security administrator is adding additional authentication controls to the existing infrastructure. Which of the following should be added by the security administrator? (Select TWO)

❍ **A.** TOTP

❍ **B.** Least privilege

❍ **C.** Role-based awareness training

❍ **D.** Separation of duties

❍ **E.** Job rotation

❍ **F.** Smart Card

Quick Answer: **33**

The Details: **71**

A33. A network administrator would like each user to authenticate with their personal username and password when connecting to the company's wireless network. Which of the following should the network administrator configure on the wireless access points?

❍ **A.** WPA2-PSK

❍ **B.** 802.1X

❍ **C.** WPS

❍ **D.** WPA2-AES

Quick Answer: **33**

The Details: **72**

A34. A security administrator needs to identify all references to a Javascript file in the HTML of a web page. Which of the following tools should be used to view the source of the web page and search through the file for a specific filename? (Select TWO)

❍ **A.** tail

❍ **B.** openssl

❍ **C.** scanless

❍ **D.** grep

❍ **E.** Nmap

❍ **F.** curl

❍ **G.** head

Quick Answer: **33**

The Details: **73**

A35. A user has assigned individual rights and permissions to a file on their network drive. The user adds three additional individuals to have read-only access to the file. Which of the following would describe this access control model?

❍ **A.** DAC

❍ **B.** MAC

❍ **C.** ABAC

❍ **D.** RBAC

Quick Answer: **33**

The Details: **74**

A36. A remote user has received a text message requesting login details to the corporate VPN server. Which of the following would BEST describe this message?

❍ **A.** Brute force

❍ **B.** Prepending

❍ **C.** Typosquatting

❍ **D.** Smishing

Quick Answer: **33**

The Details: **75**

A37. A department store policy requires that a floor manager approves each transaction when a gift certificate is used for payment. The security team has found that some of these transactions have been processed without the approval of a manager. Which of the following would provide a separation of duties to enforce this store policy?

❍ **A.** Use a WAF to monitor all gift certificate transactions

❍ **B.** Disable all gift certificate transactions for cashiers

❍ **C.** Implement a discretionary access control policy

❍ **D.** Require an approval PIN for the cashier and a separate approval PIN for the manager

Quick Answer: **33**

The Details: **76**

A38. Which of the following is true of a rainbow table? (Select TWO)

❍ **A.** The rainbow table is built in real-time during the attack

❍ **B.** Rainbow tables are the most effective online attack type

❍ **C.** Rainbow tables require significant CPU cycles at attack time

❍ **D.** Different tables are required for different hashing methods

❍ **E.** A rainbow table won't be useful if the passwords are salted

Quick Answer: **33**

The Details: **77**

A39. A server administrator at a bank has noticed a decrease in the number of visitors to the bank's website. Additional research shows that users are being directed to a different IP address than the bank's web server. Which of the following would MOST likely describe this attack?

❍ **A.** Disassociation

❍ **B.** DDoS

❍ **C.** Buffer overflow

❍ **D.** DNS poisoning

Quick Answer: **33**

The Details: **78**

A40. Which of these cloud deployment models would share resources between a private virtualized data center and externally available cloud services?

❍ **A.** SaaS

❍ **B.** Community

❍ **C.** Hybrid

❍ **D.** Containerization

Quick Answer: **33**

The Details: **79**

A41. A company hires a large number of seasonal employees, and their system access should normally be disabled when the employee leaves the company. The security administrator would like to verify that their systems cannot be accessed by any of the former employees. Which of the following would be the BEST way to provide this verification?

❍ **A.** Confirm that no unauthorized accounts have administrator access

❍ **B.** Validate the account lockout policy

❍ **C.** Validate the processes and procedures for all outgoing employees

❍ **D.** Create a report that shows all authentications for a 24-hour period

Quick Answer: **33**

The Details: **80**

A42. A network administrator has installed a new access point, but only a portion of the wireless devices are able to connect to the network. Other devices can see the access point, but they are not able to connect even when using the correct wireless settings. Which of the following security features was MOST likely enabled?

❍ **A.** MAC filtering

❍ **B.** SSID broadcast suppression

❍ **C.** 802.1X authentication

❍ **D.** Anti-spoofing

Quick Answer: **33**

The Details: **81**

A43. A security administrator has gathered this information:

```
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6     416      0  2601:4c3:4080:82.63976 yv-in-x5e.1e100..https CLOSE_WAIT
tcp6       0      0  2601:4c3:4080:82.63908 atl14s80-in-x0a..https ESTABLISHED
tcp6       0      0  fe80::4de1:1d4:8.36253 fe80::38b0:a2b1:.1025  ESTABLISHED
tcp6       0      0  fe80::4de1:1d4:8.1024  fe80::38b0:a2b1:.1024  ESTABLISHED
```

Which of the following is being used to create this information?

❍ **A.** tracert

❍ **B.** netstat

❍ **C.** dig

❍ **D.** netcat

Quick Answer: **33**

The Details: **82**

A44. An attacker has discovered a way to disable a server by sending a specially crafted packet to the operating system. When the packet is received, the system crashes and must be rebooted to restore normal operations. Which of the following would BEST describe this situation?

❍ **A.** Privilege escalation

❍ **B.** Spoofing

❍ **C.** Replay attack

❍ **D.** DoS

Quick Answer: **33**

The Details: **83**

A45. A data breach has occurred in a large insurance company. A security administrator is building new servers and security systems to get all of the financial systems back online. Which part of the incident response process would BEST describe these actions?

❍ **A.** Lessons learned

❍ **B.** Isolation and containment

❍ **C.** Reconstitution

❍ **D.** Precursors

Quick Answer: **33**

The Details: **84**

A46. A manufacturing company has moved an inventory application from their internal systems to a PaaS service. Which of the following would be the BEST way to manage security policies on this new service?

❍ **A.** DLP

❍ **B.** SIEM

❍ **C.** IPS

❍ **D.** CASB

Quick Answer: **33**

The Details: **85**

A47. An organization has identified a significant vulnerability in a firewall used for Internet connectivity. The firewall company has stated there are no plans to create a patch for this vulnerability. Which of the following would BEST describe this issue?

❍ **A.** Lack of vendor support

❍ **B.** Improper input handling

❍ **C.** Improper key management

❍ **D.** End-of-life

Quick Answer: **33**

The Details: **86**

A48. A company has decided to perform a disaster recovery exercise during an annual meeting with the IT directors and senior directors. A simulated disaster will be presented, and the participants will discuss the logistics and processes required to resolve the disaster. Which of the following would BEST describe this exercise?

❍ **A.** After-action report

❍ **B.** Business impact analysis

❍ **C.** Alternate business practice

❍ **D.** Tabletop exercise

Quick Answer: **33**

The Details: **87**

A49. A security administrator needs to identify all computers on the company network infected with a specific malware variant. Which of the following would be the BEST way to identify these systems?

❍ **A.** Honeynet

❍ **B.** Data masking

❍ **C.** DNS sinkhole

❍ **D.** DLP

Quick Answer: **33**

The Details: **88**

A50. A system administrator has been called to a system that is suspected to have a malware infection. The administrator has removed the device from the network and has disconnected all USB flash drives. Which of these incident response steps is the administrator following?

❍ **A.** Lessons learned

❍ **B.** Containment

❍ **C.** Detection

❍ **D.** Reconstitution

Quick Answer: **33**

The Details: **89**

A51. How can a company ensure that all data on a mobile device is unrecoverable if the device is lost or stolen?

❍ **A.** Containerization

❍ **B.** Geofencing

❍ **C.** Screen locks

❍ **D.** Remote wipe

Quick Answer: **33**

The Details: **90**

A52. A security administrator is collecting information associated with a ransomware infection on the company's web servers. Which of the following log files would provide information regarding the memory contents of these servers?

❍ **A.** Web

❍ **B.** Packet

❍ **C.** Dump

❍ **D.** DNS

Quick Answer: **33**

The Details: **91**

A53. Which part of the PC startup process verifies the digital signature of the OS kernel?

❍ **A.** Measured Boot

❍ **B.** Trusted Boot

❍ **C.** Secure Boot

❍ **D.** POST

Quick Answer: **33**

The Details: **92**

A54. Which of these best describes two-factor authentication?

❍ **A.** A printer uses a password and a PIN

❍ **B.** The door to a building requires a fingerprint scan

❍ **C.** An application requires a TOTP code

❍ **D.** A Windows Domain requires a username, password, and smart card

Quick Answer: **33**

The Details: **93**

A55. A company is deploying a new mobile application to all of its employees in the field. Some of the problems associated with this rollout include:

- The company does not have a way to manage the mobile devices in the field
- Company data on mobile devices in the field introduces additional risk
- Team members have many different kinds of mobile devices

Which of the following deployment models would address these concerns?

❍ **A.** Corporate-owned

❍ **B.** COPE

❍ **C.** VDI

❍ **D.** BYOD

Quick Answer: **33**

The Details: **94**

A56. An organization is installing a UPS for their new data center. Which of the following would BEST describe this type of control?

❍ **A.** Compensating

❍ **B.** Preventive

❍ **C.** Administrative

❍ **D.** Detective

Quick Answer: **33**

The Details: **95**

A57. A manufacturing company would like to track the progress of parts as they are used on an assembly line. Which of the following technologies would be the BEST choice for this task?

❍ **A.** Quantum computing

❍ **B.** Blockchain

❍ **C.** Hashing

❍ **D.** Asymmetric encryption

Quick Answer: **33**

The Details: **96**

A58. A security administrator has been asked to respond to a potential security breach of the company's databases, and they need to gather the most volatile data before powering down the database servers. In which order should they collect this information?

❍ **A.** CPU registers, temporary files, memory, remote monitoring data

❍ **B.** Memory, CPU registers, remote monitoring data, temporary files

❍ **C.** Memory, CPU registers, temporary files, remote monitoring data

❍ **D.** CPU registers, memory, temporary files, remote monitoring data

Quick Answer: **33**

The Details: **97**

A59. A Linux administrator is downloading an updated version of her Linux distribution. The download site shows a link to the ISO and a SHA256 hash value. Which of these would describe the use of this hash value?

❍ **A.** Verifies that the file was not corrupted during the file transfer

❍ **B.** Provides a key for decrypting the ISO after download

❍ **C.** Authenticates the site as an official ISO distribution site

❍ **D.** Confirms that the file does not contain any malware

Quick Answer: **33**

The Details: **98**

A60. A company's security policy requires that login access should only be available if a person is physically within the same building as the server. Which of the following would be the BEST way to provide this requirement?

❍ **A.** TOTP

❍ **B.** Biometric scanner

❍ **C.** PIN

❍ **D.** SMS

Quick Answer: **33**

The Details: **99**

A61. Your development team has installed a new application and database to a cloud service. After running a vulnerability scanner on the application instance, you find that the database is available for anyone to query without providing any authentication. Which of these vulnerabilities is MOST associated with this issue?

❍ **A.** Improper error handling

❍ **B.** Open permissions

❍ **C.** Race condition

❍ **D.** Memory leak

Quick Answer: **33**

The Details: **100**

A62. Employees of an organization have received an email offering a cash bonus for completing an internal training course. The link in the email requires users to login with their Windows Domain credentials, but the link appears to be located on an external server. Which of the following would BEST describe this email?

❍ **A.** Whaling

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Phishing

Quick Answer: **33**

The Details: **101**

A63. Which of the following risk management strategies would include the purchase and installation of an NGFW?

❍ **A.** Transference

❍ **B.** Mitigation

❍ **C.** Acceptance

❍ **D.** Risk-avoidance

Quick Answer: **33**

The Details: **102**

A64. Which of the following would be the BEST way to confirm the secure baseline of a deployed application instance?

❍ **A.** Compare the production application to the sandbox

❍ **B.** Perform an integrity measurement

❍ **C.** Compare the production application to the previous version

❍ **D.** Perform QA testing on the application instance

Quick Answer: **33**

The Details: **103**

A65. A member of the accounting team was out of the office for two weeks, and an important financial transfer was delayed until they returned. Which of the following would have prevented this delay?

❍ **A.** Split knowledge

❍ **B.** Least privilege

❍ **C.** Job rotation

❍ **D.** Dual control

Quick Answer: **33**

The Details: **104**

A66. A security analyst has identified a number of sessions from a single IP address with a TTL equal to zero. One of the sessions has a destination of the Internet firewall, and a session immediately after has a destination of your DMZ server. Which of the following BEST describes this log information?

❍ **A.** Someone is performing a vulnerability scan against the firewall and DMZ server

❍ **B.** Users are performing DNS lookups

❍ **C.** A remote user is grabbing banners of the firewall and DMZ server

❍ **D.** Someone is performing a traceroute to the DMZ server

Quick Answer: **33**

The Details: **105**

A67. An attacker has sent more information than expected in a single API call, and this has allowed the execution of arbitrary code. Which of the following would BEST describe this attack?

❍ **A.** Buffer overflow

❍ **B.** Replay attack

❍ **C.** Session hijacking

❍ **D.** DDoS

Quick Answer: **33**

The Details: **106**

A68. A company encourages users to encrypt all of their confidential materials on a central server. The organization would like to enable key escrow as a backup. Which of these keys should the organization place into escrow?

❍ **A.** Private

❍ **B.** CA

❍ **C.** Session

❍ **D.** Public

Quick Answer: **33**

The Details: **107**

A69. A security administrator is designing an authentication process for a new remote site deployment. They would like the users to provide their credentials when they authenticate in the morning, and they do not want any additional authentication requests to appear during the rest of the day. Which of the following should be used to meet this requirement?

❍ **A.** TACACS+

❍ **B.** LDAPS

❍ **C.** Kerberos

❍ **D.** 802.1X

Quick Answer: **33**

The Details: **108**

A70. A manufacturing company would like to use an existing router to separate a corporate network and a manufacturing floor that use the same physical switch. The company does not want to install any additional hardware. Which of the following would be the BEST choice for this segmentation?

❍ **A.** Connect the corporate network and the manufacturing floor with a VPN

❍ **B.** Build an air gapped manufacturing floor network

❍ **C.** Use personal firewalls on each device

❍ **D.** Create separate VLANs for the corporate network and the manufacturing floor

Quick Answer: **33**

The Details: **109**

A71. When a home user connects to the corporate VPN, they are no longer able to print to their local network printer. Once the user disconnects from the VPN, the printer works normally. Which of the following would be the MOST likely reason for this issue?

❍ **A.** The VPN uses IPSec instead of SSL

❍ **B.** Printer traffic is filtered by the VPN client

❍ **C.** The VPN is stateful

❍ **D.** The VPN tunnel is configured for full tunnel

Quick Answer: **33**

The Details: **110**

A72. A data center manager has built a Faraday cage in the data center, and a set of application servers have been placed into racks inside the Faraday cage. Which of the following would be the MOST likely reason for the data center manager to install this configuration of equipment?

❍ **A.** Protect the servers against any unwanted electromagnetic fields

❍ **B.** Prevent physical access to the servers without the proper credentials

❍ **C.** Provide additional cooling to all devices in the cage

❍ **D.** Adds additional fire protection for the application servers

Quick Answer: **33**

The Details: **111**

A73. A recent report shows the return of a vulnerability that was previously patched four months ago. After researching this issue, the security team has found that a recent patch has reintroduced this vulnerability on the servers. Which of the following should the security administrator implement to prevent this issue from occurring in the future?

❍ **A.** Templates

❍ **B.** Elasticity

❍ **C.** Master image

❍ **D.** Continuous monitoring

Quick Answer: **33**

The Details: **112**

A74. A security manager would like to ensure that unique hashes are used with an application login process. Which of the following would be the BEST way to add random data when generating a set of stored password hashes?

❍ **A.** Salting

❍ **B.** Obfuscation

❍ **C.** Key stretching

❍ **D.** Digital signature

Quick Answer: **33**

The Details: **113**

A75. Which cryptographic method is used to add trust to a digital certificate?

❍ **A.** X.509

❍ **B.** Hash

❍ **C.** Symmetric encryption

❍ **D.** Digital signature

Quick Answer: **33**

The Details: **114**

A76. An MSP is designing a new server room for a large company. Which of the following should be included in the design to provide redundancy? (Select TWO)

❍ **A.** SIEM

❍ **B.** Temperature monitors

❍ **C.** RAID arrays

❍ **D.** Dual power supplies

❍ **E.** Hot and cold aisles

❍ **F.** Biometric locks

Quick Answer: **33**

The Details: **115**

A77. An organization maintains a large database of customer information for sales tracking and customer support. Which person in the organization would be responsible for managing the access rights to this data?

❍ **A.** Data processor

❍ **B.** Data owner

❍ **C.** Privacy officer

❍ **D.** Data custodian

Quick Answer: **33**

The Details: **116**

A78. An organization's content management system (CMS) currently labels files and documents as "Unclassified" and "Restricted." On a recent updated to the CMS, a new classification type of "PII" was added. Which of the following would be the MOST likely reason for this addition?

❍ **A.** Healthcare system integration

❍ **B.** Simplified categorization

❍ **C.** Expanded privacy compliance

❍ **D.** Decreased search time

Quick Answer: **33**

The Details: **117**

A79. A corporate security team would like to consolidate and protect the certificates across all of their web servers. Which of these would be the BEST way to securely store these certificates?

❍ **A.** Use an HSM

❍ **B.** Implement full disk encryption on the web servers

❍ **C.** Use a TPM

❍ **D.** Upgrade the web servers to use a UEFI BIOS

Quick Answer: **33**

The Details: **118**

A80. Jennifer is reviewing this security log from her IPS:

```
ALERT 2018-06-01 13:07:29 [163bcf65118-179b547b]
Cross-Site Scripting in JSON Data
222.43.112.74:3332 -> 64.235.145.35:80
URL/index.html - Method POST - Query String "-"
User Agent: curl/7.21.3 (i386-redhat-linux-gnu) libcurl/7.21.3
NSS/3.13.1.0 zlib/1.2.5 libidn/1.19 libssh2/1.2.7
Detail: token="<script>" key="key7" value="<script>alert(2)</script>"
```

Which of the following can be determined from this log information? (Select TWO)

❍ **A.** The alert was generated from a malformed User Agent header

❍ **B.** The alert was generated from an embedded script

❍ **C.** The attacker's IP address is 222.43.112.74

❍ **D.** The attacker's IP address is 64.235.145.35

❍ **E.** The alert was generated due to an invalid client port number

Quick Answer: **33**

The Details: **119**

A81. Which of the following describes a monetary loss if one event occurs?

❍ **A.** ALE

❍ **B.** SLE

❍ **C.** RTO

❍ **D.** ARO

Quick Answer: **33**

The Details: **120**

A82. A user with restricted access has typed this text in a search field of an internal web-based application:

```
USER77' OR '1'='1
```

After submitting this search request, all of the database records are displayed on the screen. Which of the following would BEST describe this search?

❍ **A.** CSRF

❍ **B.** Buffer overflow

❍ **C.** SQL injection

❍ **D.** SSL stripping

Quick Answer: **33**

The Details: **121**

A83. A user has opened a helpdesk ticket complaining of poor system performance, excessive pop up messages, and the cursor moving without anyone touching the mouse. This issue began after they opened a spreadsheet from a vendor containing part numbers and pricing information. Which of the following is MOST likely the cause of this user's issues?

❍ **A.** On-path

❍ **B.** Worm

❍ **C.** RAT

❍ **D.** Logic bomb

Quick Answer: **33**

The Details: **122**

A84. A web-based manufacturing company processes monthly charges to credit card information saved in the customer's profile. Which of the following standards would be required to maintain this payment information?

❍ **A.** GDPR

❍ **B.** ISO 27001

❍ **C.** PCI DSS

❍ **D.** CSA CCM

Quick Answer: **33**

The Details: **123**

A85. A security manager has created a report showing intermittent network communication from external IP addresses to certain workstations on the internal network. These traffic patterns occur at random times during the day. Which of the following would be the MOST likely reason for these traffic patterns?

❍ **A.** ARP poisoning

❍ **B.** Backdoor

❍ **C.** Polymorphic virus

❍ **D.** Trojan horse

Quick Answer: **33**

The Details: **124**

A86. The security policies in a manufacturing company prohibit the transmission of customer information. However, a security administrator has received an alert that credit card numbers were transmitted as an email attachment. Which of the following was the MOST likely source of this alert message?

❍ **A.** IPS

❍ **B.** DLP

❍ **C.** SMTP

❍ **D.** IPsec

Quick Answer: **33**

The Details: **125**

A87. A security administrator has configured a virtual machine in a screened subnet with a guest login account and no password. Which of the following would be the MOST likely reason for this configuration?

❍ **A.** The server is a honeypot for attracting potential attackers

❍ **B.** The server is a cloud storage service for remote users

❍ **C.** The server will be used as a VPN concentrator

❍ **D.** The server is a development sandbox for third-party programming projects

Quick Answer: **33**

The Details: **126**

A88. A company's outgoing email server currently uses SMTP with no encryption. The security administrator would like to implement encryption between email clients without changing the existing server-to-server communication. Which of the following would be the BEST way to implement this requirement?

❍ **A.** Implement Secure IMAP

❍ **B.** Require the use of S/MIME

❍ **C.** Install an SSL certificate on the email server

❍ **D.** Use a VPN tunnel between email clients

Quick Answer: **33**

The Details: **127**

A89. A company would like to securely deploy applications without the overhead of installing a virtual machine for each system. Which of the following would be the BEST way to deploy these applications?

❍ **A.** Containerization

❍ **B.** IaaS

❍ **C.** Proxies

❍ **D.** CASB

Quick Answer: **33**

The Details: **128**

A90. A company has just purchased a new application server, and the security director wants to determine if the system is secure. The system is currently installed in a test environment and will not be available to users until the rollout to production next week. Which of the following would be the BEST way to determine if any part of the system can be exploited?

❍ **A.** Tabletop exercise

❍ **B.** Vulnerability scanner

❍ **C.** Password cracker

❍ **D.** Penetration test

Quick Answer: **33**

The Details: **129**

Practice Exam A

Multiple Choice Quick Answers

A6. B
A7. A and C
A8. A
A9. A and D
A10. C
A11. C
A12. A
A13. D
A14. A, E, and G
A15. B
A16. C
A17. A
A18. A
A19. A
A20. C
A21. B and E
A22. C
A23. B and D
A24. B
A25. C
A26. B
A27. A
A28. B
A29. C
A30. F
A31. D
A32. A and F
A33. B
A34. D
A35. A
A36. D
A37. D
A38. D and E
A39. D
A40. C
A41. C
A42. A
A43. B
A44. D
A45. C
A46. D
A47. A
A48. D
A49. C
A50. B
A51. D
A52. C
A53. B
A54. D
A55. C
A56. A
A57. B
A58. D
A59. A
A60. B
A61. B
A62. D
A63. B
A64. B
A65. C
A66. D
A67. A
A68. A
A69. C
A70. D
A71. D
A72. A
A73. D
A74. A
A75. D
A76. C and D
A77. D
A78. C
A79. A
A80. B and C
A81. B
A82. C
A83. C
A84. C
A85. B
A86. B
A87. A
A88. B
A89. A
A90. D

Practice Exam A Detailed Answers

A1. Match the description with the most accurate attack type. Not all attack types will be used.

Attacker obtains bank account number and birth date by calling the victim

Vishing

Social engineering over the telephone continues to be an effective attack vector, and obtaining personal information such as a bank account or birth date would be considered phishing over voice, or vishing.

More information:
SY0-601, Objective 1.1 - Phishing
https://professormesser.link/601010101

Attacker modifies a legitimate DNS server to resolve the IP address of a malicious site

Spoofing

Spoofing happens any time a device pretends to be another device. If a DNS server has been modified to hand out the IP address of a different server, then it's spoofing the IP address of the attacker.

More information:
SY0-601, Objective 1.4 - DNS Attacks
https://professormesser.link/601010409

Attacker intercepts all communication between a client and a web server

On-path

On-path attacks are quite effective because the attacker can often sit invisibly between two devices and gather useful information or modify the data streams in real-time.

More information:
SY0-601, Objective 1.4 - On-path Attacks
https://professormesser.link/601010407

Multiple attackers
overwhelm a web server

DDoS

A DoS (Denial of Service) occurs when a service is unavailable due to the effects of a third-party. A DDoS (Distributed Denial of Service) occurs when multiple third-parties work together to create a service outage.

More information:
SY0-601, Objective 1.4 - Denial of Service
https://professormesser.link/601010410

A virus alert appears in your browser from Microsoft
with a phone number to call for support

Hoax

A threat that seems real but doesn't actually exist is a hoax. In this example, a fake web site message is trying to convince you that this fake threat is actually a real security issue.

More information:
SY0-601, Objective 1.1 - Hoaxes
https://professormesser.link/601010105

A2. The security team at a local public library system is creating a set of minimum security standards for the various computer systems used at the library. Select the BEST security control for each available placeholder. **All of the available security controls will be used once.**

Location	Description		Security Controls
Library Web Server and Database Server	Computer Room High security		Locking Cabinets Environmental Sensors Video Surveillance

The security in the computer room requires both physical security and ongoing surveillance. The locking cabinets will secure the physical equipment, and the video surveillance will provide a method to monitor the systems without being physically present. Including an environmental sensor will provide information about the temperature and humidity levels in the computer room.

Library Employee Laptops	Offsite use Contains PII		Full-Disk Encryption Biometric Reader

Since the laptops are used away from the main location, it's important to protect the data and provide additional authentication options. The storage drives on the laptop should be configured with FDE (full-disk encryption) and a biometric reader on the laptop can ensure that the proper users have access.

Library Lending Systems

Manages the check-in and check-out process

Smart Card

The lending library systems are only used inside of the library, and it would be common for employees to always have their identification cards available. When combined with a smart card, these identification cards can be used as a method of authentication for the lending systems.

Digital Newspaper Reading Lab

Open Area
No supervision
Laptop computers

Cable Lock

The reading lab computers are laptops that are used in a public area with no supervision. To prevent these portable systems from becoming too portable, they can be fitted with cable locks while in the reading lab.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

A3. Fill in the blank with the BEST secure network protocol for the description:

HTTPS Accept customer purchases from your primary website

NTPsec Synchronize the time across all of your devices

SSH Access your switch using a CLI terminal screen

SRTP Talk with customers on scheduled conference calls

SNMPv3 Gather metrics from routers at remote sites

On today's networks, it's important to maintain confidentiality of data across many different applications. The Security+ exam objectives include a list of secure protocols, and it's useful to know both the insecure and secure versions of each protocol type.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

A4. Match the appropriate authentication reference to each description. Each authentication factor or attribute will be used once.

Something you can do | Somewhere you are

Something you have | Something you know | Something you are

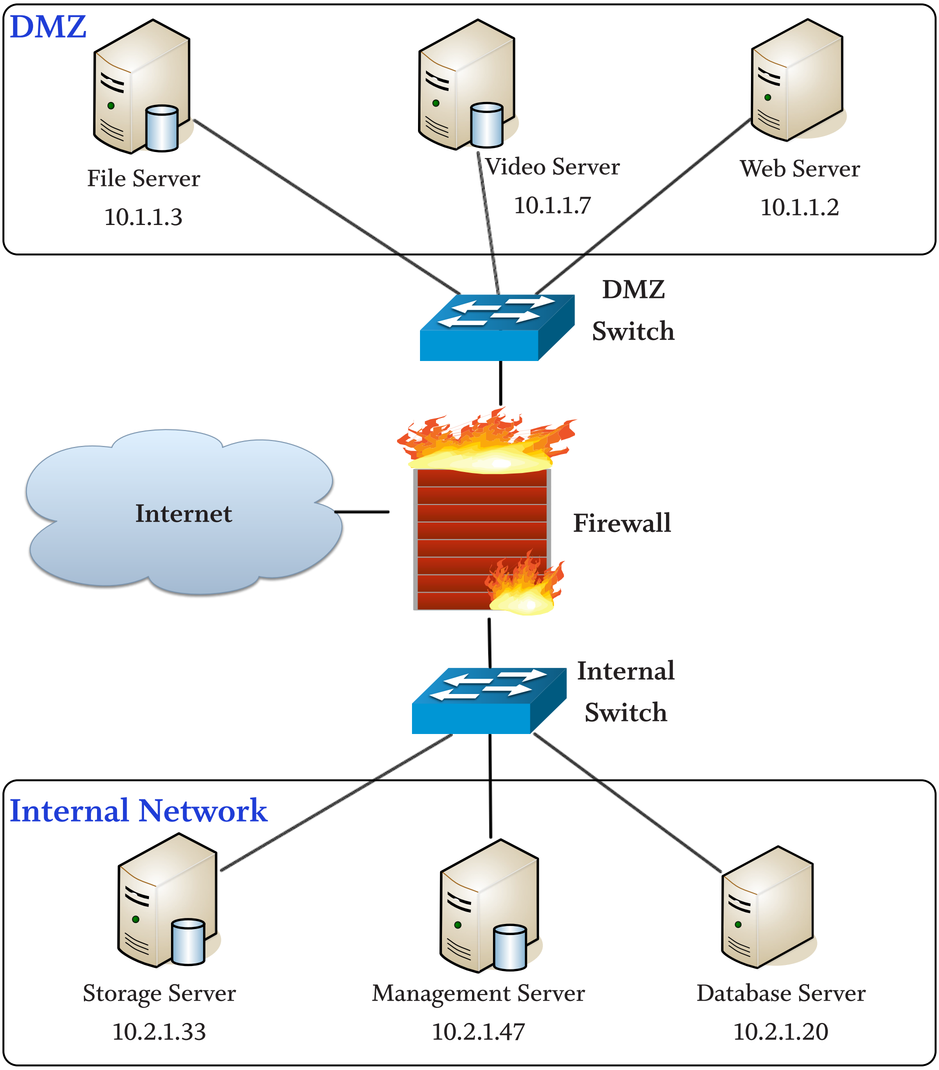
Description	Authentication Factor
During the login process, your phone receives a text message with a one-time passcode	Something you have
You enter your PIN to make a deposit into an ATM	Something you know
You must sign a check-in sheet before entering a controlled area	Something you can do
You can use your fingerprint to unlock the door to the data center	Something you are
Your login will not work unless you are connected to the VPN	Somewhere you are

Authentication factors are important to consider when developing applications or designing network infrastructures. It's useful to know each authentication factor and some examples of how that factor can be applied during the authentication process.

More information:
SY0-601, Objective 2.4 - Multi-factor Authentication
https://professormesser.link/601020403

A5. Configure the following stateful firewall rules:

- Allow the Web Server to access the Database Server using LDAP
- Allow the Storage Server to transfer files to the Video Server over HTTPS
- Allow the Management Server to use a secure terminal on the File Server



Rule #	Source IP	Destination IP	Protocol (TCP/ UDP)	Port #	Allow/ Block
1	10.1.1.2	10.2.1.20	TCP	389	Allow
2	10.2.1.33	10.1.1.7	TCP	443	Allow
3	10.2.1.47	10.1.1.3	TCP	22	Allow

Creating firewall policies is a foundational skill for any IT security professional. Fortunately, the process is relatively straightforward if each part of the firewall rule is broken down into individual pieces.

- Allow the Web Server to access the Database Server using LDAP

The first step is to determine the source and destination of the firewall rule. After referencing the diagram, we can see the source Web Server IP address is 10.1.1.2 and the destination Database Server is 10.2.1.20. This question requires a knowledge of TCP and UDP ports, and knowing the LDAP is TCP/389 provides the next two fields in the firewall rule. Finally, the rule is designed to permit traffic between these two devices, so the disposition is set to Allow.

Since this firewall is stateful, the firewall rule allows the first packet in the traffic flow and any return traffic in the flow will be automatically associated with this rule. A stateful firewall does not require a separate firewall rule for response traffic associated with the original traffic flow.

- Allow the Storage Server to transfer files to the Video Server over HTTPS

The Storage Server is 10.2.1.33, and the Video Server is 10.1.1.7. Notice that the traffic flow moves through the firewall in a different direction than the first rule, but these firewall rules are focused on the source and destination of the traffic flow. This rule specifies HTTPS traffic, so TCP/443 will be listed in the firewall rule. And finally, the firewall rule should allow these traffic flows.

- Allow the Management Server to use a secure terminal on the File Server

The management server IP address is 10.2.1.47, and the File Server is 10.1.1.3. A secure terminal would use the SSH protocol over TCP/22, and the firewall should be configured to allow this traffic.

More information:
SY0-601, Objective 3.3 - Firewalls
https://professormesser.link/601030306

A6. You've hired a third-party to gather information about your company's servers and data. The third-party will not have direct access to your internal network but can gather information from any other source. Which of the following would BEST describe this approach?

❍ **A.** Backdoor testing

❍ **B.** Passive footprinting

❍ **C.** OS fingerprinting

❍ **D.** Partially known environment

The Answer: B. Passive footprinting
Passive footprinting focuses on learning as much information from open sources such as social media, corporate websites, and business organizations.

The incorrect answers:
A. Backdoor testing
Some active reconnaissance tests will directly query systems to see if a backdoor has been installed.

C. OS fingerprinting
To fingerprint an operating system, you must actively query and receive responses across the network.

D. Partially known environment
A partially known environment penetration test is a focused approach that usually provides detailed information about specific systems or applications.

More information:
SY0-601, Objective 1.8 - Reconnaissance
https://professormesser.link/601010802

A7. Which of these protocols use TLS to provide secure communication? (Select TWO)

❍ **A.** HTTPS

❍ **B.** SSH

❍ **C.** FTPS

❍ **D.** SNMPv2

❍ **E.** DNSSEC

❍ **F.** SRTP

....

The Answer: A. HTTPS and **C.** FTPS
TLS (Transport Layer Security) is a cryptographic protocol used to encrypt network communication. HTTPS is the Hypertext Transfer Protocol over TLS, and FTPS is the File Transfer Protocol over TLS.

An earlier version of TLS is SSL (Secure Sockets Layer). Although we don't commonly see SSL in use any longer, you may see TLS communication referenced as SSL.

The incorrect answers:

B. SSH
SSH (Secure Shell) can use symmetric or asymmetric encryption, but those ciphers are not associated with TLS.

D. SNMPv2
SNMPv2 (Simple Network Management Protocol version 2) does not implement TLS, or any encryption, within the network communication.

E. DNSSEC
DNSSEC (DNS security extensions) do not provide any confidentiality of data.

F. SRTP
SRTP (Secure Real-time Transport Protocol) is a VoIP (Voice over IP) protocol used for encrypting conversations. SRTP protocol commonly uses AES (Advanced Encryption Standard) for confidentiality.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

A8. Which of these threat actors would be MOST likely to attack systems for direct financial gain?

❍ **A.** Organized crime

❍ **B.** Hacktivist

❍ **C.** Nation state

❍ **D.** Competitor

The Answer: A. Organized crime
An organized crime actor is motivated by money, and their hacking objectives are usually based around objectives that can be easily exchanged for financial capital.

The incorrect answers:
B. Hacktivist
A hacktivist is focused on a political agenda and not commonly on a financial gain.

C. Nation state
Nation states are already well funded, and their primary objective is not usually based on revenue or income.

D. Competitor
A competitor doesn't have any direct financial gain by disrupting a website or stealing customer lists, and often their objective is to disable a competitor's business or to harm their reputation. If there is a financial gain, it would often be an indirect result of an attack.

More information:
SY0-601, Objective 1.5 - Threat Actors
https://professormesser.link/601010501

A9. A security incident has occurred on a file server. Which of the following data sources should be gathered to address file storage volatility? (Select TWO)

○ **A.** Partition data

○ **B.** Kernel statistics

○ **C.** ROM data

○ **D.** Temporary file systems

○ **E.** Process table

The Answer: A. Partition data and **D.** Temporary file systems
Both temporary file system data and partition data are part of the file storage subsystem.

The incorrect answers:
B. Kernel statistics
Kernel statistics are stored in memory.

C. ROM data
ROM data is a type of memory storage.

E. Process table
The process table keeps track of system processes, and it stores this information in RAM.

More information:
SY0-601, Objective 4.5 - Forensics Data Acquisition
https://professormesser.link/601040502

A10. An IPS at your company has found a sharp increase in traffic from all-in-one printers. After researching, your security team has found a vulnerability associated with these devices that allows the device to be remotely controlled by a third-party. Which category would BEST describe these devices?

❍ **A.** IoT

❍ **B.** RTOS

❍ **C.** MFD

❍ **D.** SoC

The Answer: C. MFD
An all-in-one printer that can print, scan, and fax is often categorized as an MFD (Multifunction Device).

The incorrect answers:
A. IoT
Wearable technology and home automation devices are commonly called IoT (Internet of Things) devices.

B. RTOS
RTOS (Real-time Operating Systems) are commonly used in manufacturing and automobiles.

D. SoC
Multiple components that run on a single chip are categorized as an SoC (System on a Chip).

More information:
SY0-601, Objective 2.6 - Embedded Systems
https://professormesser.link/601020601

A11. Which of the following standards provides information on privacy and managing PII?

❍ **A.** ISO 31000

❍ **B.** ISO 27002

❍ **C.** ISO 27701

❍ **D.** ISO 27001

The Answer: C. ISO 27701
The ISO (International Organization for Standardization) 27701 standard extends the ISO 27001 and 27002 standards to include detailed management of PII (Personally Identifiable Information) and data privacy.

The incorrect answers:
A. ISO 31000
The ISO 31000 standard sets international standards for risk management practices.

B. ISO 27002
Information security controls are the focus of the ISO 27002 standard.

D. ISO 27001
The ISO 27001 standard is the foundational standard for Information Security Management Systems (ISMS).

More information:
SY0-601, Objective 5.2 - Security Frameworks
https://professormesser.link/601050202

A12. Elizabeth, a security administrator, is concerned about the potential for data exfiltration using external storage drives. Which of the following would be the BEST way to prevent this method of data exfiltration?

❍ **A.** Create an operating system security policy to prevent the use of removable media

❍ **B.** Monitor removable media usage in host-based firewall logs

❍ **C.** Only allow applications that do not use removable media

❍ **D.** Define a removable media block rule in the UTM

The Answer: A. Create an operating system security policy to prevent the use of removable media

Removable media uses hot-pluggable interfaces such as USB to connect storage drives. A security policy in the operating system can prevent any files from being written to a removable drive.

The incorrect answers:

B. Monitor removable media usage in host-based firewall logs
A host-based firewall monitors traffic flows and does not commonly log hardware or USB drive access.

C. Only allow applications that do not use removable media
File storage access options are not associated with applications, so it's not possible to allow based on external storage drive usage.

D. Define a removable media block rule in the UTM
A UTM (Unified Threat Manager) watches traffic flows across the network and does not commonly manage the storage options on individual computers.

More information:
SY0-601, Objective 1.5 - Attack Vectors
https://professormesser.link/601010502

A13. A CISO (Chief Information Security Officer) would like to decrease the response time when addressing security incidents. Unfortunately, the company does not have the budget to hire additional security engineers. Which of the following would assist the CISO with this requirement?

❍ **A.** ISO 27701

❍ **B.** PKI

❍ **C.** IaaS

❍ **D.** SOAR

The Answer: D. SOAR
SOAR (Security Orchestration, Automation, and Response) is designed to make security teams more effective by automating processes and integrating third-party security tools.

The incorrect answers:
A. ISO 27701
The ISO (International Organization for Standardization) 27701 standard focuses on privacy and securing PII.

B. PKI
A PKI (Public Key Infrastructure) describes the processes and procedures associated with maintaining digital certificates.

C. IaaS
IaaS (Infrastructure as a Service) describes a cloud service that provides the hardware required for deploying application instances and other cloud-based applications.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

A14. An insurance company has created a set of policies to handle data breaches. The security team has been given this set of requirements based on these policies:

- Access records from all devices must be saved and archived
- Any data access outside of normal working hours must be immediately reported
- Data access must only occur inside of the country
- Access logs and audit reports must be created from a single database

Which of the following should be implemented by the security team to meet these requirements? (Select THREE)

❍ **A.** Restrict login access by IP address and GPS location

❍ **B.** Require government-issued identification during the onboarding process

❍ **C.** Add additional password complexity for accounts that access data

❍ **D.** Conduct monthly permission auditing

❍ **E.** Consolidate all logs on a SIEM

❍ **F.** Archive the encryption keys of all disabled accounts

❍ **G.** Enable time-of-day restrictions on the authentication server

The Answer: **A.** Restrict login access by IP address and GPS location,
E. Consolidate all logs on a SIEM, and
G. Enable time-of-day restrictions on the authentication server

Adding location-based policies will prevent direct data access from outside of the country. Saving log information from all devices and creating audit reports from a single database can be implemented through the use of a SIEM (Security Information and Event Manager). Adding a check for the time-of-day will report any access that occurs during non-working hours.

The incorrect answers:
B. Require government-issued identification during the onboarding process

Requiring proper identification is always a good idea, but it's not one of the listed requirements.

C. Add additional password complexity for accounts that access data
Additional password complexity is another good best practice, but it's not part of the provided requirements.

D. Conduct monthly permission auditing
No requirements for ongoing auditing were included in the requirements, but ongoing auditing is always an important consideration.

F. Archive the encryption keys of all disabled accounts
If an account is disabled, there may still be encrypted data that needs to be recovered later. Archiving the encryption keys will allow access to that data after the account is no longer in use.

More information:
SY0-601, Objective 3.7 - Account Policies
https://professormesser.link/601030703

A15. Rodney, a security engineer, is viewing this record from the firewall logs:

```
UTC 04/05/2018 03:09:15809   AV Gateway Alert
136.127.92.171  80 -> 10.16.10.14  60818
Gateway Anti-Virus Alert:
XPACK.A_7854 (Trojan) blocked.
```

Which of the following can be observed from this log information?

❍ **A.** The victim's IP address is 136.127.92.171

❍ **B.** A download was blocked from a web server

❍ **C.** A botnet DDoS attack was blocked

❍ **D.** The Trojan was blocked, but the file was not

The Answer: B. A download was blocked from a web server
A traffic flow from a web server port number (80) to a device port (60818) indicates that this traffic flow originated on port 80 of the web server. A file download is one of the most common ways to deliver a Trojan, and this log entry shows that the file containing the XPACK.A_7854 Trojan was blocked.

The incorrect answers:
A. The victim's IP address is 136.127.92.171
The format for this log entry uses an arrow to differentiate between the attacker and the victim. The attacker IP address is 136.127.92.171, and the victim's IP address is 10.16.10.14.

C. A botnet DDoS attack was blocked
A botnet attack would not commonly include a Trojan horse as part of a distributed denial of service (DDoS) attack.

D. The Trojan was blocked, but the file was not
A Trojan horse attack involves malware that is disguised as legitimate software. The Trojan malware and the file are the same entity, so there isn't a way to decouple the malware from the file.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

A16. A user connects to a third-party website and receives this message:

```
Your connection is not private.
NET::ERR_CERT_INVALID
```

Which of the following attacks would be the MOST likely reason for this message?

❍ **A.** Brute force

❍ **B.** DoS

❍ **C.** On-path

❍ **D.** Disassociation

The Answer: C. On-path

An on-path attack is often associated with a third-party who is actively intercepting network traffic. This entity in the middle would not be able to provide a valid SSL certificate for a third-party website, and this error would appear in the browser as a warning.

The incorrect answers:

A. Brute force

A brute force attack is commonly associated with password hacks. Brute force attacks would not cause the certificate on a website to be invalid.

B. DoS

A DoS (Denial of Service) attack would prevent communication to a server and most likely provide a timeout error. This error is not related to a service availability issue.

D. Disassociation

Disassociation attacks are commonly associated with wireless networks, and they usually cause disconnects and lack of connectivity. The error message in this example does not appear to be associated with a network outage or disconnection.

More information:

SY0-601, Objective 1.4 - On-Path Attacks

https://professormesser.link/601010407

A17. Which of the following would be the BEST way to provide a website login using existing credentials from a third-party site?

❍ **A.** Federation

❍ **B.** 802.1X

❍ **C.** PEAP

❍ **D.** EAP-FAST

The Answer: A. Federation
Federation would allow members of one organization to authenticate using the credentials of another organization.

The incorrect answers:
B. 802.1X
802.1X is a useful authentication protocol, but it needs additional functionality to authenticate across multiple user databases.

C. PEAP
PEAP (Protected Extensible Authentication Protocol) provides a method of authentication over a protected TLS (Transport Layer Security) tunnel, but it doesn't provide the federation needed for these requirements.

D. EAP-FAST
EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) is an updated version of LEAP (Lightweight EAP) that was commonly used after WEP (Wired Equivalent Privacy) was replaced with WPA (Wi-Fi Protected Access).

More information:
SY0-601, Objective 2.4 - Authentication Methods
https://professormesser.link/601020401

A18. A system administrator, Daniel, is working on a contract that will specify a minimum required uptime for a set of Internet-facing firewalls. Daniel needs to know how often the firewall hardware is expected to fail between repairs. Which of the following would BEST describe this information?

❍ **A.** MTBF

❍ **B.** RTO

❍ **C.** MTTR

❍ **D.** MTTF

The Answer: A. MTBF
The MTBF (Mean Time Between Failures) is a prediction of how often a repairable system will fail.

The incorrect answers:
B. RTO
RTO (Recovery Time Objectives) define a set of objectives needed to restore a particular service level.

C. MTTR
MTTR (Mean Time to Restore) is the amount of time it takes to repair a component.

D. MTTF
MTTF (Mean Time to Failure) is the expected lifetime of a non-repairable product or system.

More information:
SY0-601, Objective 5.4 - Business Impact Analysis
https://professormesser.link/601050403

A19. An attacker calls into a company's help desk and pretends to be the director of the company's manufacturing department. The attacker states that they have forgotten their password and they need to have the password reset quickly for an important meeting. What kind of attack would BEST describe this phone call?

❍ **A.** Social engineering

❍ **B.** Tailgating

❍ **C.** Vishing

❍ **D.** On-path

The Answer: A. Social engineering
A social engineering attack takes advantage of authority and urgency principles in an effort to convince someone else to circumvent normal security controls.

The incorrect answers:
B. Tailgating
A tailgating attack follows someone else with proper credentials through a door. This allows the attack to gain access to an area that's normally locked.

C. Vishing
Vishing (voice phishing) attacks use the phone to obtain private information from others. In this example, the attacker was not asking for confidential information.

D. On-path
An on-path attack commonly occurs without any knowledge to the parties involved, and there's usually no additional notification that an attack is underway. In this question, the attacker contacted the help desk engineer directly.

More information:
SY0-601, Objective 1.1 - Principles of Social Engineering
https://professormesser.link/601010110

A20. A security administrator has been using EAP-FAST wireless authentication since the migration from WEP to WPA2. The company's network team now needs to support additional authentication protocols inside of an encrypted tunnel. Which of the following would meet the network team's requirements?

❍ **A.** EAP-TLS

❍ **B.** PEAP

❍ **C.** EAP-TTLS

❍ **D.** EAP-MSCHAPv2

The Answer: C. EAP-TTLS
EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) allows the use of multiple authentication protocols transported inside of an encrypted TLS (Transport Layer Security) tunnel. This allows the use of any authentication while maintaining confidentiality with TLS.

The incorrect answers:
A. EAP-TLS
EAP-TLS does not provide a mechanism for using multiple authentication types within a TLS tunnel.

B. PEAP
PEAP (Protected Extensible Authentication Protocol) encapsulates EAP within a TLS tunnel, but does not provide a method of encapsulating other authentication methods.

D. EAP-MSCHAPv2
EAP-MSCHAPv2 (EAP - Microsoft Challenge Handshake Authentication Protocol v2) is a common implementation of PEAP.

More information:
SY0-601, Objective 3.4 - Wireless Authentication Protocols
https://professormesser.link/601030403

A21. Which of the following would be commonly provided by a CASB? (Select TWO)

❍ **A.** List of all internal Windows devices that have not installed the latest security patches

❍ **B.** List of applications in use

❍ **C.** Centralized log storage facility

❍ **D.** List of network outages for the previous month

❍ **E.** Verification of encrypted data transfers

❍ **F.** VPN connectivity for remote users

The Answer: B. A list of applications in use
E. Verification of encrypted data transfers

A CASB (Cloud Access Security Broker) can be used to apply security policies to cloud-based implementations. Two common functions of a CASB are visibility into application use and data security policy use. Other common CASB functions are the verification of compliance with formal standards and the monitoring and identification of threats.

The incorrect answers:
A. List of all internal Windows devices that have not installed the latest security patches
A CASB focuses on policies associated with cloud-based services and not internal devices.

C. Centralized log storage facility
Using Syslog to centralize log storage is most commonly associated with a SIEM (Security Information and Event Manager).

D. List of network outages for the previous month
A network availability report would be outside the scope of a CASB.

F. VPN connectivity for remote users
VPN concentrators are commonly used to provide security connectivity for remote users.

More information:
SY0-601, Objective 3.6 - Cloud Security Solutions
https://professormesser.link/601030605

A22. The embedded OS in a company's time clock appliance is configured to reset the file system and reboot when a file system error occurs. On one of the time clocks, this file system error occurs during the startup process and causes the system to constantly reboot. Which of the following BEST describes this issue?

❍ **A.** DLL injection

❍ **B.** Resource exhaustion

❍ **C.** Race condition

❍ **D.** Weak configuration

The Answer: C. Race condition
A race condition occurs when two processes occur at similar times, usually with unexpected results. The file system problem is usually fixed before a reboot, but a reboot is occurring before the fix can be applied. This has created a race condition that results in constant reboots.

The incorrect answers:
A. DLL injection
One method of exploiting an application is to take advantage of the libraries reference by the application rather than the application itself. DLL (Dynamic Link Library) injection manipulates the library as the attack vector.

B. Resource exhaustion
If the time clock was running out of storage space or memory, it would most likely be unusable. In this example, the issue isn't based on a lack of resources.

D. Weak configuration
If the system is poorly configured, there may be unintended access to a service or data. This time clock issue wasn't related to any misconfiguration or weak configuration on the time clock appliance.

More information:
SY0-601, Objective 1.3 - Race Conditions
https://professormesser.link/601010309

A23. A recent audit has found that existing password policies do not include any restrictions on password attempts, and users are not required to periodically change their passwords. Which of the following would correct these policy issues? (Select TWO)

❍ **A.** Password complexity

❍ **B.** Password expiration

❍ **C.** Password history

❍ **D.** Password lockout

❍ **E.** Password recovery

The Answer: B. Password expiration and **D.** Password lockout
Password expiration would require a new password after the expiration date. Password lockout would disable an account after a predefined number of unsuccessful login attempts.

The incorrect answers:
A. Password complexity
A complex password would make it more difficult to brute force, but it would not solve the issues listed in this question.

C. Password history
Having a password history would prevent the reuse of any previous passwords.

E. Password recovery
The password recovery process provides a method for users to recover an account that has been locked out or has a forgotten password.

More information:
SY0-601, Objective 3.7 - Account Policies
https://professormesser.link/601030703

A24. What kind of security control is associated with a login banner?

❍ **A.** Preventive

❍ **B.** Deterrent

❍ **C.** Corrective

❍ **D.** Detective

❍ **E.** Compensating

❍ **F.** Physical

The Answer: B. Deterrent
A deterrent control does not directly stop an attack, but it may discourage an action.

The incorrect answers:
A. Preventive
A preventive control physically limits access to a device or area.

C. Corrective
A corrective control can actively work to mitigate any damage.

D. Detective
A detective control may not prevent access, but it can identify and record any intrusion attempts.

E. Compensating
A compensating security control doesn't prevent an attack, but it does restore from an attack using other means.

F. Physical
A physical control is real-world security, such as a fence or door lock.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

A25. A security team has been provided with a non-credentialed vulnerability scan report created by a third-party. Which of the following would they expect to see on this report?

❍ **A.** A summary of all files with invalid group assignments

❍ **B.** A list of all unpatched operating system files

❍ **C.** The version of web server software in use

❍ **D.** A list of local user accounts

The Answer: C. The version of web server software in use
A scanner like Nmap can query services and determine version numbers without any special rights or permissions, which makes it well suited for non-credentialed scans.

The incorrect answers:
A. A summary of all files with invalid group assignments
Viewing file permissions and rights requires authentication to the operating system, so you would not expect to see this information if the scan did not have credentials.

B. A list of all unpatched operating system files
Viewing detailed information about the operating system files requires authentication to the OS, and an uncredentialed scan does not have those permissions.

D. A list of local user accounts
Local user accounts are usually protected by the operating system, so you would need to have credentials to view this information.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

A26. A business manager is documenting a set of steps for processing orders if the primary Internet connection fails. Which of these would BEST describe these steps?

❍ **A.** Communication plan

❍ **B.** Continuity of operations

❍ **C.** Stakeholder management

❍ **D.** Tabletop exercise

The Answer: B. Continuity of operations
It's always useful to have an alternative set of processes to handle any type of outage or issue. Continuity of operations planning ensures that the business will continue to operate when these issues occur.

The incorrect answers:
A. Communication plan
A communication plan is a predefined list of contacts and processes used to inform key members of the organization.

C. Stakeholder management
Stakeholder management describes the ongoing relationship between the IT team and the business customer.

D. Tabletop exercise
A tabletop exercise usually consists of a meeting where members of a recovery team or disaster recovery talk through a disaster scenario.

More information:
SY0-601, Objective 4.2 - Incident Response Planning
https://professormesser.link/601040202

A27. A security administrator is concerned about data exfiltration resulting from the use of malicious phone charging stations. Which of the following would be the BEST way to protect against this threat?

❍ **A.** USB data blocker

❍ **B.** Personal firewall

❍ **C.** MFA

❍ **D.** FDE

The Answer: A. USB data blocker
USB data blockers are physical USB cables that allow power connections but prevent data connections. With a USB data blocker attached, any power source can be used without a security concern.

The incorrect answers:
B. Personal firewall
Personal firewall software is useful for blocking inbound network traffic, but it won't provide much security for physical USB connections.

C. MFA
MFA (Multi-Factor Authentication) is used during the authentication process. Incorporating multiple authentication factors won't prohibit the transfer of data over a USB connection.

D. FDE
FDE (Full Disk Encryption) is a security method for encrypting all data stored on a device. In this example, the encryption applied to the storage would not prevent the transfer of data through a malicious USB connection.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

A28. A company would like to protect the data stored on laptops used in the field. Which of the following would be the BEST choice for this requirement?

❍ **A.** MAC

❍ **B.** SED

❍ **C.** CASB

❍ **D.** SOAR

The Answer: B. SED
A SED (Self-Encrypting Drive) provides data protection of a storage device using full-disk encryption in the drive hardware.

The incorrect answers:
A. MAC
MAC (Mandatory Access Control) is an access control system that assigns labels to objects in an operating system. MAC would not prevent external access to data on a laptop's storage drive.

C. CASB
CASB (Cloud Access Security Broker) is a solution for administering and managing security policies in the cloud. CASB will not provide any security for data stored on laptops and other mobile devices.

D. SOAR
SOAR (Security Orchestration, Automation, and Response) describes a process for automating security activities. SOAR would not provide a mechanism for protecting data on a laptop's storage drive.

More information:
SY0-601, Objective 3.2 - Application Hardening
https://professormesser.link/601030205

A29. A file server has a full backup performed each Monday at 1 AM. Incremental backups are performed at 1 AM on Tuesday, Wednesday, Thursday, and Friday. The system administrator needs to perform a full recovery of the file server on Thursday afternoon. How many backup sets would be required to complete the recovery?

❍ **A.** 2

❍ **B.** 3

❍ **C.** 4

❍ **D.** 1

The Answer: C. 4
Each incremental backup will archive all of the files that have changed since the last full or incremental backup. To complete this full restore, the administrator will need the full backup from Monday and the incremental backups from Tuesday, Wednesday, and Thursday.

The incorrect answers:
A. 2
If the daily backup was differential, the administrator would only need the full backup and the differential backup from Thursday.

B. 3
Since the incremental backup only archives files that have changed, he will need all three daily incremental backups as well as Monday's full backup.

D. 1
To recover incremental backups, you'll need the full backup and all incremental backups since the full backup.

More information:
SY0-601, Objective 2.5 - Backup Types
https://professormesser.link/601020505

A30. A company is creating a security policy that will protect all corporate mobile devices:

- All mobile devices must be automatically locked after a predefined time period.
- Some mobile devices will be used by the remote sales teams, so the location of each device needs to be traceable.
- All of the user's information should be completely separated from company data.

Which of the following would be the BEST way to establish these security policy rules?

❍ **A.** Containerization

❍ **B.** Biometrics

❍ **C.** COPE

❍ **D.** VDI

❍ **E.** Geofencing

❍ **F.** MDM

The Answer: F. MDM
An MDM (Mobile Device Manager) provides a centralized management system for all mobile devices. From this central console, security administrators can set policies for many different types of mobile devices.

The incorrect answers:
A. Containerization
Mobile device containerization allows an organization to securely separate user data from company data on a mobile device. Implementing this strategy usually requires a mobile device manager (MDM), and containerization alone won't address all of the required security policies.

B. Biometrics
Biometrics can be used as another layer of device security, but you need more than biometrics to implement the required security policies in this question.

C. COPE
A device that is COPE (Corporately Owned and Personally Enabled) is commonly purchased by the corporation and allows the use of the mobile device for both business and personal use. The use of a COPE device does not address all of the required security policies.

D. VDI
A VDI (Virtual Desktop Infrastructure) separates the applications from the mobile device. This is useful for securing data, but it doesn't implement all of the requirements in this question.

E. Geofencing
Geofencing could be used to prevent mobile device use from other countries, but you would still need an MDM to implement the other requirements.

More information:
SY0-601, Objective 3.5 - Mobile Device Management
https://professormesser.link/601030502

A31. A security engineer runs a monthly vulnerability scan. The scan doesn't list any vulnerabilities for Windows servers, but a significant vulnerability was announced last week and none of the servers are patched yet. Which of the following best describes this result?

❍ **A.** Exploit

❍ **B.** Credentialed

❍ **C.** Zero-day attack

❍ **D.** False negative

The Answer: D. False negative
A false negative is a result that fails to detect an issue when one actually exists.

The incorrect answers:
A. Exploit
An exploit is an attack against a vulnerability. Vulnerability scans do not commonly attempt to exploit the vulnerabilities that they identify.

B. Credentialed
A credentialed scan would authenticate to the operating system and have access to files that would normally only be available to authorized users.

C. Zero-day attack
A zero-day attack focuses on previously unknown vulnerabilities. In this example, the vulnerability scan isn't an attack, and the vulnerabilities are already known and patches are available.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

A32. A security administrator is adding additional authentication controls to the existing infrastructure. Which of the following should be added by the security administrator? (Select TWO)

○ **A.** TOTP

○ **B.** Least privilege

○ **C.** Role-based awareness training

○ **D.** Separation of duties

○ **E.** Job rotation

○ **F.** Smart Card

The Answer: A. TOTP and **F.** Smart Card
TOTP (Time-based One-Time Passwords) and smart cards are useful authentication controls when used in conjunction with other authentication factors.

The incorrect answers:
B. Least privilege
Least privilege is a security principle that limits access to resources based on a person's job role. Least privilege is managed through security policy and is not an authentication control.

C. Role-based awareness training
Role-based awareness training is specialized training that is based on a person's control of data within an organization. This training is not part of the authentication process.

D. Separation of duties
A security policy that separates duties across different individuals is separation of duties. This separation is not part of the authentication process.

E. Job rotation
Job rotation is a security policy that moves individuals into different job roles on a regular basis. This rotation is not part of the authentication process.

More information:
SY0-601, Objective 2.4 - Authentication Methods
https://professormesser.link/601020401

A33. A network administrator would like each user to authenticate with their personal username and password when connecting to the company's wireless network. Which of the following should the network administrator configure on the wireless access points?

❍ **A.** WPA2-PSK

❍ **B.** 802.1X

❍ **C.** WPS

❍ **D.** WPA2-AES

The Answer: B. 802.1X
802.1X uses a centralized authentication server, and all users can use their normal credentials to authenticate to an 802.1X network.

The incorrect answers:
A. WPA2-PSK
The PSK (Pre-shared Key) is the shared password that this network administration would like to avoid using in the future.

C. WPS
WPS (Wi-Fi Protected Setup) connects users to a wireless network using a shared PIN (Personal Identification Number).

D. WPA2-AES
WPA2 (Wi-Fi Protected Access 2) encryption with AES (Advanced Encryption Standard) is a common encryption method for wireless networks, but it does not provide any centralized authentication functionality.

More information:
SY0-601, Objective 3.4 - Wireless Authentication Protocols
https://professormesser.link/601030403

A34. A security administrator needs to identify all references to a Javascript file in the HTML of a web page. Which of the following tools should be used to view the source of the web page and search through the file for a specific filename? (Select TWO)

❍ **A.** tail

❍ **B.** openssl

❍ **C.** scanless

❍ **D.** grep

❍ **E.** Nmap

❍ **F.** curl

❍ **G.** head

The Answer: D. grep and **F.** curl
The curl (Client URL) command will retrieve a web page and display it as HTML at the command line. The grep command can then be used to search through the file for a specific string of text.

The incorrect answers:
A. tail
The tail command will display the information at the end of a file.

B. openssl
OpenSSL is a cryptography library that is commonly used to support SSL/TLS encryption on web servers.

C. scanless
Scanless is a utility that can perform a port scan using a proxy service.

E. Nmap
The Nmap utility is a popular port scanning and reconnaissance utility.

G. head
The head command will display the information at the start of a file.

More information:
SY0-601, Objective 4.1 - Reconnaissance Tools Part 2
https://professormesser.link/601040102

A35. A user has assigned individual rights and permissions to a file on their network drive. The user adds three additional individuals to have read-only access to the file. Which of the following would describe this access control model?

❍ **A.** DAC

❍ **B.** MAC

❍ **C.** ABAC

❍ **D.** RBAC

The Answer: A. DAC
DAC (Discretionary Access Control) is used in many operating systems, and this model allows the owner of the resource to control who has access.

The incorrect answers:
B. MAC
MAC (Mandatory Access Control) allows access based on the security level assigned to an object. Only users with the object's assigned security level or higher may access the resource.

C. ABAC
ABAC (Attribute-based Access Control) combines many different parameters to determine if a user has access to a resource.

D. RBAC
RBAC (Role-based Access Control) assigns rights and permissions based on the role of a user. These roles are usually assigned by group.

More information:
SY0-601, Objective 3.8 - Access Control
https://professormesser.link/601030805

A36. A remote user has received a text message requesting login details to the corporate VPN server. Which of the following would BEST describe this message?

❍ **A.** Brute force

❍ **B.** Prepending

❍ **C.** Typosquatting

❍ **D.** Smishing

The Answer: D. Smishing

Smishing, or SMS phishing, is a social engineering attack that asks for personal information using SMS or text messages.

The incorrect answers:

A. Brute force

A brute force attack is an attack that tries multiple password combinations in an effort to identify the correct authentication details.

B. Prepending

Prepending adds information before a domain name in an attempt to fool the victim into visiting a website managed by the attacker.

C. Typosquatting

Typosquatting is a technique that uses a misspelling of a domain name to convince victims they are visiting a legitimate website.

More information:

SY0-601, Objective 1.1 - Phishing

https://professormesser.link/601010101

A37. A department store policy requires that a floor manager approves each transaction when a gift certificate is used for payment. The security team has found that some of these transactions have been processed without the approval of a manager. Which of the following would provide a separation of duties to enforce this store policy?

❍ **A.** Use a WAF to monitor all gift certificate transactions

❍ **B.** Disable all gift certificate transactions for cashiers

❍ **C.** Implement a discretionary access control policy

❍ **D.** Require an approval PIN for the cashier and a separate approval PIN for the manager

The Answer: D. Require an approval PIN for the cashier and a separate approval PIN for the manager

This separation of duties would be categorized as dual control, where two people must be present to perform the business function. In this example, the dual control is managed by using two separate PINs (Personal Identification Numbers) that would not be shared among individuals.

The incorrect answers:

A. Use a WAF to monitor all gift certificate transactions
A WAF (Web Application Firewall) is commonly used to monitor the input to web-based applications. WAFs do not commonly ensure separation of duties.

B. Disable all gift certificate transactions for cashiers
A separation of duties would give each person half of the information needed to complete the transaction, or it would require both persons to be present. Limiting the transaction to one person would not provide any separation between duties.

C. Implement a discretionary access control policy
A discretionary access control policy (DAC) is commonly used in operating system to allow the data owner to decide who has access to data. A DAC would not provide a way to manage separation of duties.

More information:
SY0-601, Objective 5.3 - Personnel Security
https://professormesser.link/601050301

A38. Which of the following is true of a rainbow table? (Select TWO)

❍ **A.** The rainbow table is built in real-time during the attack

❍ **B.** Rainbow tables are the most effective online attack type

❍ **C.** Rainbow tables require significant CPU cycles at attack time

❍ **D.** Different tables are required for different hashing methods

❍ **E.** A rainbow table won't be useful if the passwords are salted

The Answers: D. Different tables are required for different hashing methods, and **E.** A rainbow table won't be useful if the passwords are salted

A rainbow table is built prior to an attack to match a specific password hashing technique. If a different hashing technique is used, a completely different rainbow table must be built.

The use of a salt will modify the expected results of a hash. Since a salted hash will not be predictable, the rainbow table can't be built for these hashes.

The incorrect answers:
A. The rainbow table is built in real-time during the attack
One of the benefits of a rainbow table is that the table is built before an attack begins. This provides a significant speed increase at attack time.

B. Rainbow tables are the most effective online attack type
Rainbow tables are almost exclusively used as an offline attack type. The most common use of a rainbow table is for the attacker to obtain a list of password hashes from a system and then use the rainbow tables while offline.

C. Rainbow tables require significant CPU cycles at attack time
Rainbow tables are built prior to an attack, so most of the CPU (Central Processing Unit) calculations and time is spent building the tables before an attack begins.

More information:
SY0-601, Objective 1.2 - Password Attacks
https://professormesser.link/601010209

A39. A server administrator at a bank has noticed a decrease in the number of visitors to the bank's website. Additional research shows that users are being directed to a different IP address than the bank's web server. Which of the following would MOST likely describe this attack?

❍ **A.** Disassociation

❍ **B.** DDoS

❍ **C.** Buffer overflow

❍ **D.** DNS poisoning

The Answer: D. DNS poisoning
A DNS poisoning can modify a DNS server to modify the IP address provided during the name resolution process. If an attacker modifies the DNS information, they can direct client computers to any destination IP address.

The incorrect answers:
A. Disassociation
Disassociation attacks are commonly associated with wireless networks. The disassociation attack is used to remove devices from the wireless network, and it does not commonly redirect clients to a different website.

B. DDoS
A DDoS (Distributed Denial of Service) is used by attackers to cause services to be unavailable. In this example, the bank's website is operational but clients are not resolving the correct IP address.

C. Buffer overflow
Buffer overflows are associated with application attacks and can cause applications to crash or act in unexpected ways. A buffer overflow would not commonly redirect clients to a different website IP address.

More information:
SY0-601, Objective 1.4 - DNS Attacks
https://professormesser.link/601010409

A40. Which of these cloud deployment models would share resources between a private virtualized data center and externally available cloud services?

❍ **A.** SaaS

❍ **B.** Community

❍ **C.** Hybrid

❍ **D.** Containerization

The Answer: C. Hybrid
A hybrid cloud model combines both private and public cloud infrastructures.

The incorrect answers:
A. SaaS
Software as a Service (SaaS) is a cloud deployment model that provides on-demand software without any context about the software's location.

B. Community
A community cloud model allows multiple organizations to share the same cloud resources, regardless of the resource's location.

D. Containerization
Containerization can be used with mobile devices to partition user data and corporate data.

More information:
SY0-601, Objective 2.2 - Cloud Models
https://professormesser.link/601020201

A41. A company hires a large number of seasonal employees, and their system access should normally be disabled when the employee leaves the company. The security administrator would like to verify that their systems cannot be accessed by any of the former employees. Which of the following would be the BEST way to provide this verification?

❍ **A.** Confirm that no unauthorized accounts have administrator access

❍ **B.** Validate the account lockout policy

❍ **C.** Validate the processes and procedures for all outgoing employees

❍ **D.** Create a report that shows all authentications for a 24-hour period

The Answer: C. Validate the processes and procedures for all outgoing employees

The disabling of an employee account is commonly part of the offboarding process. One way to validate an offboarding policy is to perform an audit of all accounts and compare active accounts with active employees.

The incorrect answers:

A. Confirm that no unauthorized accounts have administrator access
It's always a good idea to periodically audit administrator accounts, but this audit won't provide any validation that all former employee accounts have been disabled.

B. Validate the account lockout policy
Account lockouts occur when a number of invalid authentication attempts have been made to a valid account. Disabled accounts would not be locked out because they are not currently valid accounts.

D. Create a report that shows all authentications for a 24-hour period
A list of all authentications would be quite large, and it would not be obvious to see which authentications were made with valid accounts and which authentications were made with former employee accounts.

More information:
SY0-601, Objective 5.3 - Personnel Security
https://professormesser.link/601050301

A42. A network administrator has installed a new access point, but only a portion of the wireless devices are able to connect to the network. Other devices can see the access point, but they are not able to connect even when using the correct wireless settings. Which of the following security features was MOST likely enabled?

❍ **A.** MAC filtering

❍ **B.** SSID broadcast suppression

❍ **C.** 802.1X authentication

❍ **D.** Anti-spoofing

The Answer: A. MAC filtering
Filtering addresses by MAC (Media Access Control) address will limit which devices can connect to the wireless network. If a device is filtered by MAC address, it will be able to see an access point but it will not be able to connect.

The incorrect answers:
B. SSID broadcast suppression
A suppressed SSID (Service Set Identifier) broadcast will hide the name from the list of available wireless networks. Properly configured client devices can still connect to the wireless network, even with the SSID suppression.

C. 802.1X authentication
With 802.1X authentication, users will be prompted for a username and password to gain access to the wireless network. Enabling 802.1X would not restrict properly configured devices.

D. Anti-spoofing
Anti-spoofing features are commonly used with routers to prevent communication from spoofed IP addresses. This issue in this question doesn't appear to involve any spoofed addresses.

More information:
SY0-601, Objective 3.3 - Port Security
https://professormesser.link/601030304

A43. A security administrator has gathered this information:

```
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6     416      0  2601:4c3:4080:82.63976 yv-in-x5e.1e100..https CLOSE_WAIT
tcp6       0      0  2601:4c3:4080:82.63908 atl14s80-in-x0a..https ESTABLISHED
tcp6       0      0  fe80::4de1:1d4:8.36253 fe80::38b0:a2b1:.1025  ESTABLISHED
tcp6       0      0  fe80::4de1:1d4:8.1024  fe80::38b0:a2b1:.1024  ESTABLISHED
```

Which of the following is being used to create this information?

○ **A.** tracert

○ **B.** netstat

○ **C.** dig

○ **D.** netcat

The Answer: B. netstat
The netstat command provides a list of network statistics, and the default view shows the traffic sessions between the local device and other devices on the network.

The incorrect answers:
A. tracert
Traceroute lists the route between devices and shows the IP address information of the routers at each hop.

C. dig
The dig (Domain Information Groper) command queries DNS servers for the fully-qualified domain name and IP address information of other devices.

D. netcat
The netcat command is used for reading or writing data to the network. The netcat command itself doesn't provide any statistical information about the network connection.

More information:
SY0-601, Objective 4.1 - Reconnaissance Tools Part 1
https://professormesser.link/601040101

A44. An attacker has discovered a way to disable a server by sending specially crafted packets from many remote devices to the operating system. When the packet is received, the system crashes and must be rebooted to restore normal operations. Which of the following would BEST describe this attack?

❍ **A.** Privilege escalation

❍ **B.** Spoofing

❍ **C.** Replay attack

❍ **D.** DDoS

The Answer: D. DDoS
A DDoS (Distributed Denial of Service) is an attack that overwhelms or disables a service to prevent the service from operating normally. Packets from multiple devices that disable a server would be an example of a DDoS attack.

The incorrect answers:
A. Privilege escalation
A privilege escalation attack allows a user to exceed their normal rights and permissions. In this example, user permission escalations were not required to perform this attack.

B. Spoofing
Spoofing is when a device pretends to be a different device or pretends to be something they aren't. This attack explanation did not appear to emulate or pretend to be a different user or address than the actual attacker.

C. Replay attack
A replay attack captures information and then replays that information as the method of attack. In this question, no mention was made of a prior data capture.

More information:
SY0-601, Objective 1.4 - Denial of Service
https://professormesser.link/601010410

A45. A data breach has occurred in a large insurance company. A security administrator is building new servers and security systems to get all of the financial systems back online. Which part of the incident response process would BEST describe these actions?

❍ **A.** Lessons learned

❍ **B.** Isolation and containment

❍ **C.** Reconstitution

❍ **D.** Precursors

The Answer: C. Reconstitution
The recovery after a breach can be a phased approach that may take months to complete.

The incorrect answers:
A. Lessons learned
Once the event is over, it's useful to revisit the process to learn and improve for next time.

B. Isolation and containment
During an incident, it's useful to separate infected systems from the rest of the network.

D. Precursors
Log files and alerts can often warn you of potential problems.

More information:
SY0-601, Objective 4.2 - Incident Response Process
https://professormesser.link/601040201

A46. A manufacturing company has moved an inventory application from their internal systems to a PaaS service. Which of the following would be the BEST way to manage security policies on this new service?

❍ **A.** DLP

❍ **B.** SIEM

❍ **C.** IPS

❍ **D.** CASB

The Answer: D. CASB
A CASB (Cloud Access Security Broker) is used to manage compliance with security policies when using cloud-based applications.

The incorrect answers:
A. DLP
DLP (Data Loss Prevention) can identify and block PII (Personally Identifiable Information) and other private details from being transferred across the network.

B. SIEM
A SIEM (Security Information and Event Manager) is a management system for log consolidation and reporting. A SIEM cannot managed cloud-based security policies.

C. IPS
An IPS (Intrusion Prevention System) can identify and block known vulnerabilities on the network, but it does not provide policy management for cloud-based systems.

More information:
SY0-601, Objective 3.6 - Cloud Security Solutions
https://professormesser.link/601030605

A47. An organization has identified a significant vulnerability in a firewall used for Internet connectivity. The firewall company has stated there are no plans to create a patch for this vulnerability. Which of the following would BEST describe this issue?

❍ **A.** Lack of vendor support

❍ **B.** Improper input handling

❍ **C.** Improper key management

❍ **D.** End-of-life

The Answer: A. Lack of vendor support
Security issues can be identified in a system or application at any time, so it's important to have a vendor that can support their software and correct issues as they are discovered. If a vendor won't provide security patches, then you may be susceptible to security vulnerabilities.

The incorrect answers:
B. Improper input handling
A best practice for application security is to provide the proper handling of invalid or unnecessary input. Adding a patch to firewall software for a vulnerability would probably not be related to input handling.

C. Improper key management
Cryptographic keys can be used for many security purposes, but managing those keys isn't part of the patching process from a vendor.

D. End-of-life
In this case, the firewall is a relatively new product. If the product was no longer officially sold or supported by the company, this would be an end-of-life issue.

More information:
SY0-601, Objective 1.6 - Third-party Risks
https://professormesser.link/601010602

A48. A company has decided to perform a disaster recovery exercise during an annual meeting with the IT directors and senior directors. A simulated disaster will be presented, and the participants will discuss the logistics and processes required to resolve the disaster. Which of the following would BEST describe this exercise?

❍ **A.** After-action report

❍ **B.** Business impact analysis

❍ **C.** Alternate business practice

❍ **D.** Tabletop exercise

The Answer: D. Tabletop exercise
A tabletop exercise allows a disaster recovery team to evaluate and plan disaster recovery processes without performing a full-scale drill.

The incorrect answers:
A. After-action report
An after-action report is commonly created after a disaster recovery drill to document which aspects of the plan worked or did not work.

B. Business impact analysis
A business impact analysis is usually created during the disaster recovery planning process. Once the disaster has occurred, it becomes much more difficult to complete an accurate impact analysis.

C. Alternate business practice
An alternate business practice may be one of the steps in completing a disaster recovery exercise, but it does not describe the exercise itself.

More information:
SY0-601, Objective 4.2 - Incident Response Planning
https://professormesser.link/601040202

A49. A security administrator needs to identify all computers on the company network infected with a specific malware variant. Which of the following would be the BEST way to identify these systems?

❍ **A.** Honeynet

❍ **B.** Data masking

❍ **C.** DNS sinkhole

❍ **D.** DLP

The Answer: C. DNS sinkhole
A DNS (Domain Name System) sinkhole can be used to redirect and identify devices that may attempt to communicate with an external command and control (C2) server. The DNS sinkhole will resolve an internal IP address and can report on all devices that attempt to access the malicious domain.

The incorrect answers:
A. Honeynet
A honeynet is a non-production network that has been specifically created to attract attackers. A honeynet is not commonly used to identify infected devices.

B. Data masking
Data masking provides a way to hide data by substitution, shuffling, encryption, and other methods. Data masking does not provide a method of identifying infected devices.

D. DLP
DLP (Data Loss Prevention) systems can identify and block private information from transferring between systems. DLP does not provide any direct method of identifying devices infected with malware.

More information:
SY0-601, Objective 2.1 - Honeypots and Deception
https://professormesser.link/601020106

A50. A system administrator has been called to a system that is suspected to have a malware infection. The administrator has removed the device from the network and has disconnected all USB flash drives. Which of these incident response steps is the administrator following?

❍ **A.** Lessons learned

❍ **B.** Containment

❍ **C.** Detection

❍ **D.** Reconstitution

The Answer: B. Containment

The containment phase isolates the system from any other devices to prevent the spread of any malicious software.

The incorrect answers:

A. Lessons learned

A post-incident meeting can help the incident response participants discuss the phases of the incident that went well and which processes can be improved for future events.

C. Detection

The detection phase occurred prior to the system administrator arriving and identified the potential infection.

D. Reconstitution

The reconstitution phase will recover the system and data back to the state prior to the malware infection.

More information:

SY0-601, Objective 4.2 - Incident Response Process

https://professormesser.link/601040201

A51. How can a company ensure that all data on a mobile device is unrecoverable if the device is lost or stolen?

○ **A.** Containerization

○ **B.** Geofencing

○ **C.** Screen locks

○ **D.** Remote wipe

The Answer: D. Remote wipe
Most organizations will use a mobile device manager (MDM) to manage mobile phones and tablets. Using the MDM, specific security policies can be created for each mobile device, including the ability to remotely send a remote wipe command that will erase all data on a mobile device.

The incorrect answers:
A. Containerization
Containerization on a mobile device will separate the user's data from the company information. This allows the company to control their corporate data without modifying or accessing the end user's data.

B. Geofencing
Geofencing would allow the company to limit functionality or access based on the location of the mobile device. Geofencing does not securely wipe data from a device.

C. Screen locks
Screen locks are important, but won't help when you need to permanently remove data from a device.

More information:
SY0-601, Objective 3.5 - Mobile Device Management
https://professormesser.link/601030502

A52. A security administrator is collecting information associated with a ransomware infection on the company's web servers. Which of the following log files would provide information regarding the memory contents of these servers?

❍ **A.** Web

❍ **B.** Packet

❍ **C.** Dump

❍ **D.** DNS

The Answer: C. Dump
A dump file contains the contents of system memory. In Windows, this file can be created from the Task Manager.

The incorrect answers:
A. Web
Web server logs will document web pages that were accessed, but it doesn't show what information may be contained in the system RAM.

B. Packet
A packet trace would provide information regarding network communication, but it would not include any details regarding the contents of memory.

D. DNS
DNS (Domain Name System) server logs can show which domain names were accessed by internal systems, and this information can help identify systems that may be infected. However, the DNS log doesn't include any information about the memory contents of a server.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

A53. Which part of the PC startup process verifies the digital signature of the OS kernel?

❍ **A.** Measured Boot

❍ **B.** Trusted Boot

❍ **C.** Secure Boot

❍ **D.** POST

The Answer: B. Trusted Boot
The Trusted Boot portion of the startup process verifies the operating system kernel signature and starts the ELAM (Early Launch Anti-Malware) process.

The incorrect answers:
A. Measured Boot
Measured Boot occurs after the Trusted Boot process and verifies that nothing on the computer has been changed by malicious software or other processes.

C. Secure Boot
Secure Boot is a UEFI BIOS boot feature that checks the digital signature of the bootloader. The Trusted Boot process occurs after Secure Boot has completed.

D. POST
POST (Power-On Self-Test) is a hardware check performed prior to booting an operating system.

More information:
SY0-601, Objective 3.2 - Boot Integrity
https://professormesser.link/601030202

A54. Which of these best describes two-factor authentication?

❍ **A.** A printer uses a password and a PIN

❍ **B.** The door to a building requires a fingerprint scan

❍ **C.** An application requires a TOTP code

❍ **D.** A Windows Domain requires a username, password, and smart card

The Answer: D. A Windows Domain requires a username, password, and smart card

The multiple factors of authentication used to login to this Windows Domain are a password (something you know), and a smart card (something you have).

The incorrect answers:

A. A printer uses a password and a PIN
A password and a PIN (Personal Identification Number) are both something you know, so only one authentication factor is used.

B. The door to a building requires a fingerprint scan
A biometric scan (something you are) is a single factor of authentication.

C. An application requires a TOTP code
TOTP (Time-based One-Time Password) is usually provided using a hardware dongle or mobile app. This single factor of authentication is something you have.

More information:
SY0-601, Objective 2.4 - Multi-factor Authentication
https://professormesser.link/601020403

A55. A company is deploying a new mobile application to all of its employees in the field. Some of the problems associated with this rollout include:

- The company does not have a way to manage the mobile devices in the field
- Company data on mobile devices in the field introduces additional risk
- Team members have many different kinds of mobile devices

Which of the following deployment models would address these concerns?

❍ **A.** Corporate-owned

❍ **B.** COPE

❍ **C.** VDI

❍ **D.** BYOD

The Answer: C. VDI
A VDI (Virtual Desktop Infrastructure) would allow the field teams to access their applications from many different types of devices without the requirement of a mobile device management or concern about corporate data on the devices.

The incorrect answers:
A. Corporate-owned
A corporate-owned device would solve the issue of device standardization, but the corporate data would be stored on the mobile devices in the field.

B. COPE
COPE (Corporate Owned and Personally Enabled) devices are purchased by the company but are used as both a corporate device and a personal device. This would standardize the devices, but the corporate data would still be at-risk in the field.

D. BYOD
BYOD (Bring Your Own Device) means that the employee would choose the mobile platform. This would not address the issue of mobile device management, data security in the field, or standardization of mobile devices and apps.

More information:
SY0-601, Objective 3.5 - Mobile Deployment Models
https://professormesser.link/601030505

A56. An organization is installing a UPS for their new data center. Which of the following would BEST describe this type of control?

❍ **A.** Compensating

❍ **B.** Preventive

❍ **C.** Administrative

❍ **D.** Detective

The Answer: A. Compensating
A compensating security control doesn't prevent an attack, but it does restore from an attack using other means. In this example, the UPS does not stop a power outage, but it does provide alternative power if an outage occurs.

The incorrect answers:
B. Preventive
A preventive control physically limits access to a device or area.

C. Administrative
An administrative control sets a policy that is designed to control how people act.

D. Detective
A detective control may not prevent access, but it can identify and record any intrusion attempts.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

A57. A manufacturing company would like to track the progress of parts as they are used on an assembly line. Which of the following technologies would be the BEST choice for this task?

❍ **A.** Quantum computing

❍ **B.** Blockchain

❍ **C.** Hashing

❍ **D.** Asymmetric encryption

The Answer: B. Blockchain
The ledger functionality of a blockchain can be used to track or verify components, digital media, votes, and other physical or digital objects.

The incorrect answers:
A. Quantum computing
Quantum computing uses quantum theory to perform high-speed calculations. Quantum computing doesn't inherently provide any tracking mechanisms.

C. Hashing
Cryptographic hashes are commonly used to provide integrity verifications, but they don't necessarily include any method of tracking components on an assembly line.

D. Asymmetric encryption
Asymmetric encryption uses different keys for encryption and decryption. Asymmetric encryption does not provide any method for tracking objects on an assembly line.

More information:
SY0-601, Objective 2.8 - Blockchain Technology
https://professormesser.link/601020808

A58. A security administrator has been asked to respond to a potential security breach of the company's databases, and they need to gather the most volatile data before powering down the database servers. In which order should they collect this information?

❍ **A.** CPU registers, temporary files, memory, remote monitoring data

❍ **B.** Memory, CPU registers, remote monitoring data, temporary files

❍ **C.** Memory, CPU registers, temporary files, remote monitoring data

❍ **D.** CPU registers, memory, temporary files, remote monitoring data

The Answer: D. CPU registers, memory, temporary files, remote monitoring data

The most volatile data disappears quickly, so data such as the CPU registers and information in memory will be lost before temporary files and remote monitoring data are no longer available.

The incorrect answers:
A. CPU registers, temporary files, memory, remote monitoring data
Memory is more volatile than temporary files.

B. Memory, CPU registers, remote monitoring data, temporary files
CPU registers are more volatile than memory, and temporary files are more volatile than remote monitoring data.

C. Memory, CPU registers, temporary files, remote monitoring data
CPU registers are more volatile than information in memory.

More information:
SY0-601, Objective 4.5 - Forensics Data Acquisition
https://professormesser.link/601040502

A59. A Linux administrator is downloading an updated version of her Linux distribution. The download site shows a link to the ISO and a SHA256 hash value. Which of these would describe the use of this hash value?

❍ **A.** Verifies that the file was not corrupted during the file transfer

❍ **B.** Provides a key for decrypting the ISO after download

❍ **C.** Authenticates the site as an official ISO distribution site

❍ **D.** Confirms that the file does not contain any malware

The Answer: A. Verifies that the file was not corrupted during the file transfer

Once the file is downloaded, the administrator can calculate the file's SHA256 hash and confirm that it matches the value on the website.

The incorrect answers:
B. Provides a key for decrypting the ISO after download
ISO files containing public information are usually distributed without any encryption, and a hash value would not commonly be used as a decryption key.

C. Authenticates the site as an official ISO distribution site
Although it's important to download files from known good sites, providing a hash value on a site would not provide any information about the site's authentication.

D. Confirms that the file does not contain any malware
A hash value doesn't inherently provide any protection against malware.

More information:
SY0-601, Objective 2.8 - Hashing and Digital Signatures
https://professormesser.link/601020803

A60. A company's security policy requires that login access should only be available if a person is physically within the same building as the server. Which of the following would be the BEST way to provide this requirement?

❍ **A.** TOTP

❍ **B.** Biometric scanner

❍ **C.** PIN

❍ **D.** SMS

The Answer: B. Biometric scanner
A biometric scanner would require a person to be physically present to verify authentication.

The incorrect answers:

A. TOTP
A TOTP (Time-based One-Time Password) generator may be associated with a single person, but the TOTP code does not guarantee that a person is physically present.

C. PIN
Although a PIN (Personal Identification Number) can be used as an authentication factor, the use of the PIN does not guarantee that a person is physically present.

D. SMS
SMS messages are commonly used as authentication factors. However, the use of a mobile device to receive the SMS message does not guarantee that the owner of the mobile device is physically present.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

A61. Your development team has installed a new application and database to a cloud service. After running a vulnerability scanner on the application instance, you find that the database is available for anyone to query without providing any authentication. Which of these vulnerabilities is MOST associated with this issue?

❍ **A.** Improper error handling

❍ **B.** Open permissions

❍ **C.** Race condition

❍ **D.** Memory leak

The Answer: B. Open permissions
Just like your local systems, proper permissions and security controls are also required when information is added to a cloud-based system. If any of your systems leave an open door, your data may be accessible by anyone on the Internet.

The incorrect answers:
A. Improper error handling
This issue wasn't associated with any error messages, so this wouldn't be categorized as a problem with error handling.

C. Race condition
If two processes occur simultaneously without any prior consideration, bad things could happen. In this example, a single vulnerability scan has identified the issue and other processes do not appear to be involved.

D. Memory leak
An application with a memory leak will gradually use more and more memory until the system or application crashes. The issue in this question was related to permissions and not available resources.

More information:
SY0-601, Objective 1.6 - Vulnerability Types
https://professormesser.link/601010601

A62. Employees of an organization have received an email offering a cash bonus for completing an internal training course. The link in the email requires users to login with their Windows Domain credentials, but the link appears to be located on an external server. Which of the following would BEST describe this email?

○ **A.** Whaling

○ **B.** Vishing

○ **C.** Smishing

○ **D.** Phishing

The Answer: D. Phishing
Phishing is the process of manipulating a victim to disclose personal or private information. An email asking for login details from a server not under the control of the company would describe a phishing attempt.

The incorrect answers:
A. Whaling
Whaling is phishing targeted towards individuals at a higher level of an organization. These persons are usually in upper management or have access to the financial operations of the company.

B. Vishing
Vishing, or voice phishing, is using voice communication for the phishing process. This phishing attempt used an email message, so it would not be categorized as vishing.

C. Smishing
Smishing, or SMS phishing, is an attacker using SMS or text messaging when phishing. Smishing text messages often include a link to a server where personal information or login credentials may be requested by the attacker.

More information:
SY0-601, Objective 1.1 - Phishing
https://professormesser.link/601010101

A63. Which of the following risk management strategies would include the purchase and installation of an NGFW?

❍ **A.** Transference

❍ **B.** Mitigation

❍ **C.** Acceptance

❍ **D.** Risk-avoidance

The Answer: B. Mitigation
Mitigation is a strategy that decreases the threat level. This is commonly done through the use of additional security systems and monitoring, such as an NGFW (Next-Generation Firewall).

The incorrect answers:
A. Transference
Transference would move the risk from one entity to another. Adding an NGFW would not transfer any risk to another party.

C. Acceptance
The acceptance of risk is a position where the owner understands the risk and has decided to accept the potential results.

D. Risk-avoidance
With risk-avoidance, the owner of the risk decides to stop participating in a high-risk activity. This effectively avoids the risky activity and prevents any future issues.

More information:
SY0-601, Objective 5.6 - Risk Management Types
https://professormesser.link/601050401

A64. Which of the following would be the BEST way to confirm the secure baseline of a deployed application instance?

❍ **A.** Compare the production application to the sandbox

❍ **B.** Perform an integrity measurement

❍ **C.** Compare the production application to the previous version

❍ **D.** Perform QA testing on the application instance

The Answer: B. Perform an integrity measurement
An integrity measurement is designed to check for the secure baseline of firewall settings, patch levels, operating system versions, and any other security components associated with the application. These secure baselines may vary between different application versions.

The incorrect answers:
A. Compare the production application to the sandbox
A sandbox is commonly used as a development environment. Security baselines in a production environment can be quite different when compared to the code in a sandbox.

C. Compare the production application to the previous version
The newer version of an application may have very different security requirements than previous versions.

D. Perform QA testing on the application instance
QA (Quality Assurance) testing is commonly used for finding bugs and verifying application functionality. The primary task of QA is not generally associated with verifying security baselines.

More information:
SY0-601, Objective 2.3 - Secure Deployments
https://professormesser.link/601020301

A65. A member of the accounting team was out of the office for two weeks, and an important financial transfer was delayed until they returned. Which of the following would have prevented this delay?

❍ **A.** Split knowledge

❍ **B.** Least privilege

❍ **C.** Job rotation

❍ **D.** Dual control

The Answer: C. Job rotation

Job rotation moves employees through different job roles as part of their normal work environment. This policy limits the potential for fraud and allows others to cover responsibilities if someone is out of the office.

The incorrect answers:

A. Split knowledge

The use of split knowledge limits the information that any one person would know. In this example, having knowledge of part of the process would not have helped with processing the financial transfer.

B. Least privilege

Least privilege is a security policy that limits the rights and permissions of a user to only those tasks required for their job role. In this example, having properly configured privileges would not have provided any contingency for this delayed transaction.

D. Dual control

With dual control, two persons must be present to perform a business function. In this example, one of the employees is out of the office and dual control would not be possible.

More information:

SY0-601, Objective 5.3 - Personnel Security

https://professormesser.link/601050301

A66. A security analyst has identified a number of sessions from a single IP address with a TTL equal to zero. One of the sessions has a destination of the Internet firewall, and a session immediately after has a destination of your DMZ server. Which of the following BEST describes this log information?

❍ **A.** Someone is performing a vulnerability scan against the firewall and DMZ server

❍ **B.** Users are performing DNS lookups

❍ **C.** A remote user is grabbing banners of the firewall and DMZ server

❍ **D.** Someone is performing a traceroute to the DMZ server

The Answer: D. Someone is performing a traceroute to the DMZ server
A traceroute maps each hop by slowly incrementing the TTL (Time to Live) value during each request. When the TTL reaches zero, the receiving router drops the packet and sends an ICMP (Internet Control Message Protocol) TTL Exceeded message back to the original station.

The incorrect answers:
A. Someone is performing a vulnerability scan against the firewall and DMZ server
Vulnerability scans are usually very specific requests, and they won't get to their destination if the TTL is zero. The question did not provide any information that would indicate an active vulnerability scan.

B. Users are performing DNS lookups
Properly working DNS (Domain Name System) responses would not have a TTL of zero, and nothing in the question indicated information that would commonly be included in a DNS query.

C. A remote user is grabbing banners of the firewall and DMZ server
Banners can provide useful reconnaissance information about a service, but the TTL of zero and the lack of connection to a specific service would not indicate a banner grabbing session.

More information:
SY0-601, Objective 4.1 - Reconnaissance Tools Part 1
https://professormesser.link/601040101

A67. An attacker has sent more information than expected in a single API call, and this has allowed the execution of arbitrary code. Which of the following would BEST describe this attack?

❍ **A.** Buffer overflow

❍ **B.** Replay attack

❍ **C.** Session hijacking

❍ **D.** DDoS

The Answer: A. Buffer overflow
The results of a buffer overflow can cause random results, but sometimes the actions can be repeatable and controlled. In the best possible case for the hacker, a buffer overflow can be manipulated to execute code on the remote device.

The incorrect answers:
B. Replay attack
A replay attack does not require the sending of more information than expected, and often a replay attack consists of normal traffic and expected application input.

C. Session hijacking
Session hijacking doesn't require any data overflows, and commonly the hijack occurs without any unusual input.

D. DDoS
A DDoS (Distributed Denial of Service) renders a service unavailable, and it involves the input of many devices to operate. A DDoS would not require sending more information than expected, and it rarely results in the execution of arbitrary code.

More information:
SY0-601, Objective 1.3 - Buffer Overflows
https://professormesser.link/601010304

A68. A company encourages users to encrypt all of their confidential materials on a central server. The organization would like to enable key escrow as a backup. Which of these keys should the organization place into escrow?

❍ **A.** Private

❍ **B.** CA

❍ **C.** Session

❍ **D.** Public

The Answer: A. Private
With asymmetric encryption, the private key is used to decrypt information that has been encrypted with the public key. To ensure continued access to the encrypted data, the company must have a copy of each private key.

The incorrect answers:
B. CA
A CA (Certificate Authority) key is commonly used to validate the digital signature from a trusted CA. This is not commonly used for user data encryption.

C. Session
Session keys are commonly used temporarily to provide confidentiality during a single session. Once the session is complete, the keys are discarded. Session keys are not used to provide long-term data encryption.

D. Public
In asymmetric encryption, a public key is already available to everyone. It would not be necessary to escrow a public key.

More information:
SY0-601, Objective 3.9 - Certificate Concepts
https://professormesser.link/601030904

A69. A security administrator is designing an authentication process for a new remote site deployment. They would like the users to provide their credentials when they authenticate in the morning, and they do not want any additional authentication requests to appear during the rest of the day. Which of the following should be used to meet this requirement?

❍ **A.** TACACS+

❍ **B.** LDAPS

❍ **C.** Kerberos

❍ **D.** 802.1X

The Answer: C. Kerberos
Kerberos uses a ticket-based system to provide SSO (Single Sign-On) functionality. You only need to authenticate once with Kerberos to gain access to multiple resources.

The incorrect answers:
A. TACACS+
TACACS+ (Terminal Access Controller Access-Control System) is a common authentication method, but it does not provide any single sign-on functionality.

B. LDAPS
LDAPS (Lightweight Directory Access Protocol Secure) is a standard for accessing a network directory. This can provide an authentication method, but it does not provide any single sign-on functionality.

D. 802.1X
802.1X is a standard for port-based network access control (PNAC), but it does not inherently provide any single sign-on functionality.

More information:
SY0-601, Objective 3.8 - Identity and Access Services
https://professormesser.link/601030803

A70. A manufacturing company would like to use an existing router to separate a corporate network and a manufacturing floor that use the same physical switch. The company does not want to install any additional hardware. Which of the following would be the BEST choice for this segmentation?

❍ **A.** Connect the corporate network and the manufacturing floor with a VPN

❍ **B.** Build an air gapped manufacturing floor network

❍ **C.** Use personal firewalls on each device

❍ **D.** Create separate VLANs for the corporate network and the manufacturing floor

The Answer: D. Create separate VLANs for the corporate network and the manufacturing floor

Creating VLANs (Virtual Local Area Networks) will segment a network without requiring additional switches.

The incorrect answers:

A. Connect the corporate network and the manufacturing floor with a VPN

A VPN (Virtual Private Network) would encrypt all information between the two networks, but it would not provide any segmentation. This process would also commonly require additional hardware to provide VPN connectivity.

B. Build an air gapped manufacturing floor network

An air gapped network would require separate physical switches on each side of the gap, and this would require the purchase of an additional switch.

C. Use personal firewalls on each device

While personal firewalls provide protection for individual devices, they do not segment networks. It's also uncommon for personal firewalls to be installed on manufacturing equipment.

More information:

SY0-601, Objective 3.3 - Network Segmentation

https://professormesser.link/601030302

A71. When a home user connects to the corporate VPN, they are no longer able to print to their local network printer. Once the user disconnects from the VPN, the printer works normally. Which of the following would be the MOST likely reason for this issue?

❍ **A.** The VPN uses IPSec instead of SSL

❍ **B.** Printer traffic is filtered by the VPN client

❍ **C.** The VPN is stateful

❍ **D.** The VPN tunnel is configured for full tunnel

The Answer: D. The VPN tunnel is configured for full tunnel
A split tunnel is a VPN (Virtual Private Network) configuration that only sends a portion of the traffic through the encrypted tunnel. A split tunnel would allow work-related traffic to securely traverse the VPN, and all other traffic would use the non-tunneled option. In this example, the printer traffic is being redirected through the VPN instead of the local home network because of the non-split/full tunnel.

The incorrect answers:
A. The VPN uses IPSec instead of SSL
There are many protocols that can be used to send traffic through an encrypted tunnel. IPsec is commonly used for site-to-site VPN connections, and SSL (Secure Sockets Layer) is commonly used for end-user VPN connections. However, either protocol can technically be used for any VPN tunnel, and the choice of protocol would have no difference on the operation of the local printer.

B. Printer traffic is filtered by the VPN client
VPN clients are usually tasked with sending traffic unfiltered through the encrypted tunnel. Although data could be filtered at some point along the communication path, it's not commonly filtered by the VPN client.

C. The VPN is stateful
A stateful communication is commonly associated with firewalls, and it refers to the firewall's ability to track traffic flows. Stateful communication would not be a technology commonly associated with a VPN, and it would not be part of the user's printing issue.

More information:
SY0-601, Objective 3.3 - Virtual Private Networks
https://professormesser.link/601030303

A72. A data center manager has built a Faraday cage in the data center, and a set of application servers have been placed into racks inside the Faraday cage. Which of the following would be the MOST likely reason for the data center manager to install this configuration of equipment?

❍ **A.** Protect the servers against any unwanted electromagnetic fields

❍ **B.** Prevent physical access to the servers without the proper credentials

❍ **C.** Provide additional cooling to all devices in the cage

❍ **D.** Adds additional fire protection for the application servers

The Answer: A. Protect the servers against any unwanted electromagnetic fields

A Faraday cage is a mesh of conductive material that will cancel electromagnetic fields.

The incorrect answers:

B. Prevent physical access to the servers without the proper credentials
A Faraday cage does not provide any protection against system logins.

C. Provide additional cooling to all devices in the cage
A Faraday cage does not provide any additional cooling features.

D. Adds additional fire protection for the application servers
A Faraday cage does not provide any additional fire protection features.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

A73. A recent report shows the return of a vulnerability that was previously patched four months ago. After researching this issue, the security team has found that a recent patch has reintroduced this vulnerability on the servers. Which of the following should the security administrator implement to prevent this issue from occurring in the future?

❍ **A.** Templates

❍ **B.** Elasticity

❍ **C.** Master image

❍ **D.** Continuous monitoring

The Answer: D. Continuous monitoring
It's common for organizations to continually monitor services for any changes or issues. A nightly vulnerability scan across important servers would identify issues like this one.

The incorrect answers:
A. Templates
Templates can be used to easily build the basic structure of an application instance. These templates are not used to identify or prevent the introduction of vulnerabilities.

B. Elasticity
Elasticity is important when scaling resources as the demand increases or decreases. Unfortunately, elasticity will not help with the identification of vulnerabilities.

C. Master image
A master image is used to quickly copy a server for easy deployment. This image will need to be updated and maintained to prevent the issues associated with unexpected vulnerabilities.

More information:
SY0-601, Objective 2.3 - Automation and Scripting
https://professormesser.link/601020305

A74. A security manager would like to ensure that unique hashes are used with an application login process. Which of the following would be the BEST way to add random data when generating a set of stored password hashes?

❍ **A.** Salting

❍ **B.** Obfuscation

❍ **C.** Key stretching

❍ **D.** Digital signature

The Answer: A. Salting
Adding random data, or salt, to a password when performing the hashing process will create a unique hash, even if other users have chosen the same password.

The incorrect answers:
B. Obfuscation
Obfuscation is the process of making something difficult for humans to read or understand. The obfuscation process isn't commonly associated with adding random information to hashes.

C. Key stretching
Key stretching is a process that uses a key multiple times for additional protection against brute force attacks. Key stretching by itself does not commonly add random data to the hashing process.

D. Digital signature
Digital signatures use a hash and asymmetric encryption to provide integrity of data. Digital signatures aren't commonly used for storing passwords.

More information:
SY0-601, Objective 2.8 - Hashing and Digital Signatures
https://professormesser.link/601020803

A75. Which cryptographic method is used to add trust to a digital certificate?

❍ **A.** X.509

❍ **B.** Hash

❍ **C.** Symmetric encryption

❍ **D.** Digital signature

The Answer: D. Digital signature
A certificate authority will digitally sign a certificate to add trust. If you trust the certificate authority, you can then trust the certificate.

The incorrect answers:
A. X.509
The X.509 standard defines the structure of a certificate. This standard format makes it easy for everyone to view the contents of a certificate, but it doesn't provide any additional trust.

B. Hash
A hash can help verify that the certificate has not been altered, but it does not provide additional third-party trust.

C. Symmetric encryption
Symmetric encryption has the same issue as asymmetric encryption. The information in a certificate commonly needs to be viewable by others.

More information:
SY0-601, Objective 3.9 - Public Key Infrastructure
https://professormesser.link/601030901

A76. An MSP is designing a new server room for a large company. Which of the following should be included in the design to provide redundancy? (Select TWO)

❍ **A.** SIEM

❍ **B.** Temperature monitors

❍ **C.** RAID arrays

❍ **D.** Dual power supplies

❍ **E.** Hot and cold aisles

❍ **F.** Biometric locks

The Answer: C. RAID arrays and **D.** Dual power supplies
RAID (Redundant Array of Independent Disks) and dual power supplies can both provide uptime and availability if a drive or component fails. Many RAID configurations can continue to operate if a drive fails, and a system with two power supplies can continue to operate if one of those was to fail.

The incorrect answers:
A. SIEM
A SIEM (Security Information and Event Manager) is a useful part of any network configuration, but it does not provide for uptime and availability during a failure.

B. Temperature monitors
Temperature monitors can provide an early-warning notification of an HVAC (Heating, Ventilation, and Air Conditioning) issue, but they don't provide any redundancy if the cooling system fails.

E. Hot and cold aisles
Hot and cold aisles will provide the most efficient cooling, but they don't provide any redundant features.

F. Biometric locks
Biometric locks are commonly found on server room and data center entrances, but they don't provide any redundancy for the systems inside.

More information:
SY0-601, Objective 2.5 - Disk Redundancy
https://professormesser.link/601020501

A77. An organization maintains a large database of customer information for sales tracking and customer support. Which person in the organization would be responsible for managing the access rights to this data?

❍ **A.** Data processor

❍ **B.** Data owner

❍ **C.** Privacy officer

❍ **D.** Data custodian

The Answer: D. Data custodian
The data custodian manages access rights and sets security controls to the data.

The incorrect answers:
A. Data processor
The data processor manages the operational use of the data, but not the rights and permissions to the information.

B. Data owner
The data owner is usually a higher-level executive who makes business decisions regarding the data.

C. Privacy officer
A privacy officer sets privacy policies and implements privacy processes and procedures.

More information:
SY0-601, Objective 5.5 - Data Roles and Responsibilities
https://professormesser.link/601050504

A78. An organization’s content management system (CMS) currently labels files and documents as “Unclassified” and “Restricted.” On a recent updated to the CMS, a new classification type of “PII” was added. Which of the following would be the MOST likely reason for this addition?

❍ **A.** Healthcare system integration

❍ **B.** Simplified categorization

❍ **C.** Expanded privacy compliance

❍ **D.** Decreased search time

The Answer: C. Expanded privacy compliance
The labeling of PII (Personally Identifiable Information) is often associated with privacy and compliance concerns.

The incorrect answers:
A. Healthcare system integration
Healthcare data would most likely be labeled as PHI (Protected Health Information). Personal information isn’t necessarily health-related.

B. Simplified categorization
Adding additional categories would not commonly be considered a simplification.

D. Decreased search time
Adding additional classifications would not necessarily provide any decreased search times.

More information:
SY0-601, Objective 5.5 - Data Classifications
https://professormesser.link/601050502

A79. A corporate security team would like to consolidate and protect the certificates across all of their web servers. Which of these would be the BEST way to securely store these certificates?

❍ **A.** Use an HSM

❍ **B.** Implement full disk encryption on the web servers

❍ **C.** Use a TPM

❍ **D.** Upgrade the web servers to use a UEFI BIOS

The Answer: A. Use an HSM
An HSM (Hardware Security Module) is a high-end cryptographic hardware appliance that can securely store keys and certificates for all devices.

The incorrect answers:
B. Implement full disk encryption on the web servers
Full-disk encryption would only protect the certificates if someone does not have the proper credentials, and it won't help consolidate all of the web server keys to a central point.

C. Use a TPM
A TPM (Trusted Platform Module) is used on individual devices to provide cryptographic functions and securely store encryption keys. Individual TPMs would not provide any consolidation of web server certificates.

D. Upgrade the web servers to use a UEFI BIOS
A UEFI (Unified Extensible Firmware Interface) BIOS (Basic Input/Output System) does not provide any additional security or consolidation features for web server certificates.

More information:
SY0-601, Objective 3.3 - Other Network Appliances
https://professormesser.link/601030310

A80. Jennifer is reviewing this security log from her IPS:

```
ALERT 2018-06-01 13:07:29 [163bcf65118-179b547b]
Cross-Site Scripting in JSON Data
222.43.112.74:3332 -> 64.235.145.35:80
URL/index.html - Method POST - Query String "-"
User Agent: curl/7.21.3 (i386-redhat-linux-gnu) libcurl/7.21.3
NSS/3.13.1.0 zlib/1.2.5 libidn/1.19 libssh2/1.2.7
Detail: token="<script>" key="key7" value="<script>alert(2)</script>"
```

Which of the following can be determined from this log information? (Select TWO)

❍ **A.** The alert was generated from a malformed User Agent header

❍ **B.** The alert was generated from an embedded script

❍ **C.** The attacker's IP address is 222.43.112.74

❍ **D.** The attacker's IP address is 64.235.145.35

❍ **E.** The alert was generated due to an invalid client port number

The Answer: B. The alert was generated from an embedded script and
C. The attacker's IP address is 222.43.112.74

The details of the IPS (Intrusion Prevention System) alert show a script value embedded into JSON (JavaScript Object Notation) data. The IPS log also shows the flow of the attack with an arrow in the middle. The attacker was IP address 222.43.112.74 with port 3332, and the victim was 64.235.145.35 over port 80.

The incorrect answers:

A. The alert was generated from a malformed User Agent header
The user agent information is provided as additional supporting data associated with the alert. The agent itself is not the cause of this alert.

D. The attacker's IP address is 64.235.145.35
The attacker's IP address is listed first, so the victim's IP address is 64.235.145.35.

E. The alert was generated due to an invalid client port number
The port number associated with the client, 3332, is a valid port number and not associated with the cause of the alert.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

A81. Which of the following describes a monetary loss if one event occurs?

❍ **A.** ALE

❍ **B.** SLE

❍ **C.** RTO

❍ **D.** ARO

The Answer: B. SLE
SLE (Single Loss Expectancy) describes the financial impact of a single event.

The incorrect answers:
A. ALE
ALE (Annual Loss Expectancy) is the financial loss over an entire 12-month period.

C. RTO
RTO (Recovery Time Objectives) define a set of objectives needed to restore a particular service level.

D. ARO
The ARO (Annualized Rate of Occurrence) is the number of times an event will occur in a 12-month period.

More information:
SY0-601, Objective 5.4 - Risk Analysis
https://professormesser.link/601050402

A82. A user with restricted access has typed this text in a search field of an internal web-based application:

```
USER77' OR '1'='1
```

After submitting this search request, all of the database records are displayed on the screen. Which of the following would BEST describe this search?

❍ **A.** CSRF

❍ **B.** Buffer overflow

❍ **C.** SQL injection

❍ **D.** SSL stripping

The Answer: C. SQL injection
SQL (Structured Query Language) injection takes advantage of poor input validation to circumvent the application and perform queries directly to the database.

The incorrect answers:
A. CSRF
CSRF (Cross-Site Request Forgery) takes advantage of a third-party trust to a web application. The attack demonstrated in this question does not use another user's credentials or access rights to obtain information.

B. Buffer overflow
A buffer overflow uses an application vulnerability to submit more information than an application can properly manage. The attack syntax in this question is specific to SQL injections, and it does not appear to be manipulating a buffer overflow vulnerability.

D. SSL stripping
SSL stripping allows an on-path attack to rewrite web site addresses to gain access to encrypted information. The attack in this question does not include a third-party or on-path entity.

More information:
SY0-601, Objective 1.3 - Injection Attacks
https://professormesser.link/601010303

A83. A user has opened a helpdesk ticket complaining of poor system performance, excessive pop up messages, and the cursor moving without anyone touching the mouse. This issue began after they opened a spreadsheet from a vendor containing part numbers and pricing information. Which of the following is MOST likely the cause of this user's issues?

❍ **A.** On-path

❍ **B.** Worm

❍ **C.** RAT

❍ **D.** Logic bomb

The Answer: C. RAT
A RAT (Remote Access Trojan) is malware that can control a computer using desktop sharing and other administrative functions. Because the installation program is often disguised as something else, the victim often doesn't realize they're installing malware. Once the RAT is installed, the attacker can control the desktop, capture screenshots, reboot the computer, and many other administrative functions.

The incorrect answers:
A. Man-in-the-middle
A man-in-the-middle attack commonly occurs without any knowledge to the parties involved, and there's usually no additional notification that an attack is underway.

B. Worm
A worm is malware that can replicate itself between systems without any user intervention, so a spreadsheet that requires additional a user to click warning messages would not be categorized as a worm.

D. Logic bomb
A logic bomb is malware that installs and operates silently until a certain event occurs. Once the logic bomb has been triggered, the results usually involve loss of data or a disabled operating system.

More information:
SY0-601, Objective 1.2 - Trojans and RATs
https://professormesser.link/601010204

A84. A web-based manufacturing company processes monthly charges to credit card information saved in the customer's profile. Which of the following standards would be required to maintain this payment information?

❍ **A.** GDPR

❍ **B.** ISO 27001

❍ **C.** PCI DSS

❍ **D.** CSA CCM

The Answer: C. PCI DSS
The PCI DSS (Payment Card Industry Data Security Standard) specifies the minimum security requirements for storing and protecting credit card information.

The incorrect answers:
A. GDPR
GDPR (General Data Protection Regulation) is a European Union regulation that governs data protection and privacy for individuals in the EU.

B. ISO 27001
The ISO (International Organization for Standardization) 27001 standard focuses on the requirements for an Information Security Management System (ISMS).

D. CSA CCM
The CSA CCM (Cloud Security Alliance Cloud Controls Matrix) provides documents for implementing and managing cloud-specific security controls.

More information:
SY0-601, Objective 5.2 - Security Regulations and Standards
https://professormesser.link/601050201

A85. A security manager has created a report showing intermittent network communication from external IP addresses to certain workstations on the internal network. These traffic patterns occur at random times during the day. Which of the following would be the MOST likely reason for these traffic patterns?

○ **A.** ARP poisoning

○ **B.** Backdoor

○ **C.** Polymorphic virus

○ **D.** Trojan horse

The Answer: B. Backdoor
A backdoor would allow an attacker to access a system at any time without any user intervention. If there are inbound traffic flows that cannot be identified, it may be necessary to isolate that computer and examine it for signs of a compromised system.

The incorrect answers:
A. ARP poisoning
ARP (Address Resolution Protocol) poisoning is a local exploit that is often associated with a man-in-the-middle attack. The attacker must be on the same local IP subnet as the victim, so this is not often associated with an external attack.

C. Polymorphic virus
Polymorphic viruses will modify themselves each time they are downloaded. Although a virus could potentially install a backdoor, a polymorphic virus would not be able to install itself without user intervention.

D. Trojan horse
A Trojan horse is malware that is hidden inside of a seemingly harmless application. Once the Trojan horse is executed, the malware will be installed onto the victim's computer. Trojan horse malware could possibly install backdoor malware, but the Trojan horse itself would not be the reason for these traffic patterns.

More information:
SY0-601, Objective 1.2 - Trojans and RATs
https://professormesser.link/601010204

A86. The security policies in a manufacturing company prohibit the transmission of customer information. However, a security administrator has received an alert that credit card numbers were transmitted as an email attachment. Which of the following was the MOST likely source of this alert message?

❍ **A.** IPS

❍ **B.** DLP

❍ **C.** SMTP

❍ **D.** IPsec

The Answer: B. DLP
DLP (Data Loss Prevention) technologies can identify and block the transmission of sensitive data across the network.

The incorrect answers:
A. IPS
IPS (Intrusion Prevention System) signatures are useful for identifying known vulnerabilities, but they don't commonly provide a way to identify and block PII (Personally Identifiable Information) or sensitive data.

C. SMTP
SMTP (Simple Mail Transfer Protocol) is a protocol used to transfer email messages between servers. SMTP does not identify the transmission of sensitive data.

D. IPsec
IPsec (Internet Protocol Security) is a protocol suite for authenticating and encrypting network communication. IPsec does not include any features for identifying and alerting on sensitive information.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

A87. A security administrator has configured a virtual machine in a screened subnet with a guest login account and no password. Which of the following would be the MOST likely reason for this configuration?

❍ **A.** The server is a honeypot for attracting potential attackers

❍ **B**. The server is a cloud storage service for remote users

❍ **C.** The server will be used as a VPN concentrator

❍ **D.** The server is a development sandbox for third-party programming projects

The Answer: A. The server is a honeypot for attracting potential attackers
A screened subnet is a good location to configure services that can be accessed from the Internet, and building a system that can be easily compromised is a common tactic for honeypot systems.

The incorrect answers:
B. The server is a cloud storage service for remote users
Although cloud storage is a useful service, configuring storage on a server with an open guest account is not a best practice.

C. The server will be used as a VPN concentrator
VPN (Virtual Private Networking) concentrators should be installed on secure devices, and configuring an open guest account would not be considered a secure configuration.

D. The server is a development sandbox for third-party programming projects
It would not be secure to configure a development sandbox on a system with an open guest account.

More information:
SY0-601, Objective 2.1 - Honeypots and Deception
https://professormesser.link/601020106

A88. A company's outgoing email server currently uses SMTP with no encryption. The security administrator would like to implement encryption between email clients without changing the existing server-to-server communication. Which of the following would be the BEST way to implement this requirement?

❍ **A.** Implement Secure IMAP

❍ **B.** Require the use of S/MIME

❍ **C.** Install an SSL certificate on the email server

❍ **D.** Use a VPN tunnel between email clients

The Answer: B. Require the use of S/MIME
S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a way to integrate public key encryption and digital signatures into most modern email clients. This would encrypt all email information from client to client, regardless of the communication used between email servers.

The incorrect answers:
A. Implement Secure IMAP
Secure IMAP (Internet Message Access Protocol) would encrypt communication downloaded from an email server, but it would not provide any security for outgoing email messages.

C. Install an SSL certificate on the email server
An SSL certificate on an email server could potentially be used to encrypt server-to-server communication, but the security administrator is looking for an encryption method between email clients.

D. Use a VPN tunnel between email clients
Email communication does not occur directly between email clients, so configuring a VPN between all possible email recipients would not be a valid implementation.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

A89. A company would like to securely deploy applications without the overhead of installing a virtual machine for each system. Which of the following would be the BEST way to deploy these applications?

○ **A.** Containerization

○ **B.** IaaS

○ **C.** Proxies

○ **D.** CASB

The Answer: A. Containerization
Application containerization uses a single virtual machine to use as a foundation for separate application "containers." These containers are implemented as isolated instances, and an application in one container is not inherently accessible from other containers on the system.

The incorrect answers:
B. IaaS
IaaS (Infrastructure as a Service) is a cloud-based service that provides the basic infrastructure for installing operating systems and applications. By itself, IaaS does not provide any method of application deployments or virtual machines.

C. Proxies
Proxies can be used as security devices, but they aren't used for deploying application instances without virtual machines.

D. CASB
A CASB (Cloud Access Security Broker) is a cloud security solution to manage visibility, compliance, threat prevention, and other security features for cloud-based applications.

More information:
SY0-601, Objective 2.2 - Designing the Cloud
https://professormesser.link/601020203

A90. A company has just purchased a new application server, and the security director wants to determine if the system is secure. The system is currently installed in a test environment and will not be available to users until the rollout to production next week. Which of the following would be the BEST way to determine if any part of the system can be exploited?

❍ **A.** Tabletop exercise

❍ **B.** Vulnerability scanner

❍ **C.** Password cracker

❍ **D.** Penetration test

The Answer: D. Penetration test
A penetration test can be used to actively exploit potential vulnerabilities in a system or application. This could cause a denial of service or loss of data, so the best practice is to perform the penetration test during non-production hours or in a test environment.

The incorrect answers:
A. Tabletop exercise
A tabletop exercise is used to talk through a security event with an incident response team around a conference room table. This is commonly performed as a training device instead of performing a full-scale disaster drill.

B. Vulnerability scanner
Vulnerability scanners may identify a vulnerability, but they do not actively attempt to exploit the vulnerability.

C. Password cracker
A password cracker is usually an offline brute force tool used against a list of password hashes. A password cracker may be able to identify weak passwords, but it would not identify any other types of vulnerabilities.

More information:
SY0-601, Objective 1.8 - Penetration Testing
https://professormesser.link/601010801

Practice Exam B

Performance-Based Questions

B1. Select the values associated with the following RAID specifications:

	RAID 0	RAID 1	RAID 5
Minimum Number of Drives	1 2 3 4	1 2 3 4	1 2 3 4
Striping	Yes No	Yes No	Yes No
Mirroring	Yes No	Yes No	Yes No
Parity Data	Yes No	Yes No	Yes No

Answer Page: **165**

B2. An organization is deploying a mobile app to its sales force in the field. The application will be accessed from tablets for all remote sales team members and a browser-based front-end on desktops for corporate office users. The company would like to enable security features for both platforms.

The application contains sensitive customer information, and two forms of authentication are required to launch the application.

Select three security features that would apply to each platform. A security feature will only be used once. Not all security features will be used.

Security Features

- Host-based Firewall
- Remote Wipe
- Environmental Sensors
- Anti-Malware
- Locking Cabinets
- Smart Card
- Full Device Encryption
- Face recognition

Tablet for Field Sales

Desktop with Browser-based Front-end

Answer Page: **166**

B3. Sam, a security administrator, is responsible for gathering evidence from a server that was part of a security breach. Which items should Sam prioritize for forensic evidence gathering? Order the following from highest priority to least priority.

Temporary files | CPU registers | Backup tapes

Routing table | Event logs

Answer Page: **167**

B4. Match the security technology to the implementation:

Digital signature | Perfect Forward Secrecy | Key escrow

Certificate Authority | Hashing | Encryption

	Store a password on an authentication server
	Verify a sender's identity
	Protect private information sent over an insecure channel
	Use a secondary decryption key
	Trust a website without prior contact with the site owner
	Use a different encryption key for each session

Answer Page: **168**

B5. Select the data state that best fits the description. Each data state will be used more than once.

Data in-transit   Data at-rest   Data in-use

	All switches in a data center are connected with an 802.1Q trunk
	Sales information is uploaded daily from a remote site using a satellite network
	A company stores customer purchase information in a MySQL database
	An application decrypts credit card numbers and expiration dates to validate for approval
	An authentication program performs a hash of all passwords
	An IPS identifies a SQL injection attack and removes the attack frames from the network
	An automatic teller machine validates a user's PIN before allowing a deposit
	Each time a spreadsheet is updated, all of the cells containing formulas are automatically updated
	All weekly backup tapes are transported to an offsite storage facility
	All user spreadsheets are stored on a cloud-based file sharing service

Answer Page: **169**

Practice Exam B
Multiple Choice Questions

B6. A security administrator has performed an audit of the organization's production web servers, and the results have identified banner information leakage, web services running from a privileged account, and inconsistencies with SSL certificates. Which of the following would be the BEST way to resolve these issues?

❍ **A.** Server hardening

❍ **B.** Multi-factor authentication

❍ **C.** Enable HTTPS

❍ **D.** Run operating system updates

Quick Answer: **163**

The Details: **170**

B7. A shipping company stores information in small regional warehouses around the country. The company keeps an IPS online at each warehouse to watch for suspicious traffic patterns. Which of the following would BEST describe the security control used at the warehouse?

❍ **A.** Administrative

❍ **B.** Compensating

❍ **C.** Physical

❍ **D.** Detective

Quick Answer: **163**

The Details: **171**

B8. The Vice President of Sales has asked the IT team to create daily backups of the sales data. The Vice President is an example of a:

❍ **A.** Data owner

❍ **B.** Data protection officer

❍ **C.** Data steward

❍ **D.** Data processor

Quick Answer: **163**

The Details: **172**

B9. A security engineer is preparing to conduct a penetration test. Part of the preparation involves reading through social media posts for information about a third-party website. Which of the following describes this practice?

❍ **A.** Partially known environment

❍ **B.** OSINT

❍ **C.** Exfiltration

❍ **D.** Active footprinting

Quick Answer: **163**

The Details: **173**

B10. A company would like to automate their response when a virus is detected on company devices. Which of the following would be the BEST way to implement this function?

❍ **A.** Active footprinting

❍ **B.** IaaS

❍ **C.** Vulnerability scan

❍ **D.** SOAR

Quick Answer: **163**

The Details: **174**

B11. A user in the accounting department has received an email from the CEO requesting payment for a recently purchased tablet. However, there doesn't appear to be a purchase order associated with this request. Which of the following would be the MOST likely attack associated with this email?

❍ **A.** Spear phishing

❍ **B.** Watering hole attack

❍ **C.** Invoice scam

❍ **D.** Credential harvesting

Quick Answer: **163**

The Details: **175**

B12. A company has been informed of a hypervisor vulnerability that could allow users on one virtual machine to access resources on another virtual machine. Which of the following would BEST describe this vulnerability?

❍ **A.** Containerization

❍ **B.** Service integration

❍ **C.** SDN

❍ **D.** VM escape

Quick Answer: **163**

The Details: **176**

B13. While working from home, users are attending a project meeting over a web conference. When typing in the meeting link, the browser is unexpectedly directed to a different website than the web conference. Users in the office do not have any issues accessing the conference site. Which of the following would be the MOST likely reason for this issue?

❍ **A.** Bluejacking

❍ **B.** Wireless disassociation

❍ **C.** DDoS

❍ **D.** DNS poisoning

Quick Answer: **163**

The Details: **177**

B14. A company is launching a new internal application that will not start until a username and password is entered and a smart card is plugged into the computer. Which of the following BEST describes this process?

❍ **A.** Federation

❍ **B.** Accounting

❍ **C.** Authentication

❍ **D.** Authorization

Quick Answer: **163**

The Details: **178**

B15. An online retailer is planning a penetration test as part of their PCI DSS validation. A third-party organization will be performing the test, and the online retailer has provided the Internet-facing IP addresses for their public web servers but no other details. What penetration testing methodology is the online retailer using?

❍ **A.** Known environment

❍ **B.** Passive footprinting

❍ **C.** Partially known environment

❍ **D.** Ping scan

Quick Answer: **163**

The Details: **179**

B16. A manufacturing company makes radar used by commercial and military organizations. A recently proposed policy change would allow the use of mobile devices inside the facility. Which of the following would be the MOST significant security issue associated with this change in policy?

❍ **A.** Unauthorized software on rooted devices

❍ **B.** Remote access clients on the mobile devices

❍ **C.** Out of date mobile operating systems

❍ **D.** Photo and video use

Quick Answer: **163**

The Details: **180**

B17. A company is designing an application that will have a high demand and will require significant computing resources during the summer. During the winter, there will be little to no application use and resource use should be minimal. Which of these characteristics BEST describe this application requirement?

❍ **A.** Availability

❍ **B.** Orchestration

❍ **C.** Imaging

❍ **D.** Elasticity

Quick Answer: **163**

The Details: **181**

B18. Vala, a security analyst, has received an alert from her IPS regarding active exploit attempts from the Internet. Which of the following would provide detailed information about these exploit attempts?

❍ **A.** Netstat

❍ **B.** Nmap

❍ **C.** Nessus

❍ **D.** Wireshark

Quick Answer: **163**

The Details: **182**

B19. A user in the accounting department would like to send a spreadsheet with sensitive information to a list of third-party vendors. Which of the following could be used to transfer this spreadsheet to the vendors?

❍ **A.** SNMPv3

❍ **B.** SRTP

❍ **C.** DNSSEC

❍ **D.** FTPS

Quick Answer: **163**

The Details: **183**

B20. A system administrator would like to segment the network to give the marketing, accounting, and manufacturing departments their own private network. The network communication between departments would be restricted for additional security. Which of the following should be configured on this network?

❍ **A.** VPN

❍ **B.** RBAC

❍ **C.** VLAN

❍ **D.** NAT

Quick Answer: **163**

The Details: **184**

B21. A technician at an MSP has been asked to manage devices on third-party private network. The technician needs command line access to internal routers, switches, and firewalls. Which of the following would provide the necessary access?

❍ **A.** HSM

❍ **B.** Jump server

❍ **C.** NAC

❍ **D.** Air gap

Quick Answer: **163**

The Details: **185**

B22. A transportation company is installing new wireless access points in their corporate offices. The manufacturer estimates that the access points will operate an average of 100,000 hours before a hardware-related outage. Which of the following describes this estimate?

❍ **A.** MTTR

❍ **B.** RPO

❍ **C.** RTO

❍ **D.** MTBF

Quick Answer: **163**

The Details: **186**

B23. A security administrator has been asked to create a policy that would prevent access to a secure area of the network. All users who are not physically located in the corporate headquarters building would be prevented from accessing this area. Which of these should the administrator use?

❍ **A.** WAF

❍ **B.** VPN

❍ **C.** Geofencing

❍ **D.** Proxy

Quick Answer: **163**

The Details: **187**

B24. Which of the following would be considered multi-factor authentication?

❍ **A.** PIN and fingerprint

❍ **B.** USB token and smart card

❍ **C.** Username, password, and email address

❍ **D.** Face scan and voiceprint

Quick Answer: **163**

The Details: **188**

B25. Sam, a security administrator, is configuring the authentication process used by technicians when logging into a router. Instead of using accounts that are local to the router, Sam would like to pass all login requests to a centralized database. Which of the following would be the BEST way to implement this requirement?

❍ **A.** PAP

❍ **B.** RADIUS

❍ **C.** IPsec

❍ **D.** MS-CHAP

Quick Answer: **163**

The Details: **189**

B26. A recent audit has determined that many IT department accounts have been granted Administrator access. The audit recommends replacing these permissions with limited access rights. Which of the following would BEST describe this policy?

❍ **A.** Separation of duties

❍ **B.** Offboarding

❍ **C.** Least privilege

❍ **D.** Discretionary Access Control

Quick Answer: **163**

The Details: **190**

B27. A recent security audit has discovered email addresses and passwords located in a packet capture. Which of the following did the audit identify?

❍ **A.** Weak encryption

❍ **B.** Improper patch management

❍ **C.** Insecure protocols

❍ **D.** Open ports

Quick Answer: **163**

The Details: **191**

B28. A company has connected their wireless access points and have enabled WPS. Which of the following security issues would be associated with this configuration?

❍ **A.** Brute force

❍ **B.** Client hijacking

❍ **C.** Cryptographic vulnerability

❍ **D.** Spoofing

Quick Answer: **163**

The Details: **192**

B29. An organization has traditionally purchased insurance to cover a ransomware attack, but the costs of maintaining the policy have increased above the acceptable budget. The company has now decided to cancel the insurance policies and deal with ransomware issues internally. Which of the following would best describe this action?

❍ **A.** Mitigation

❍ **B.** Acceptance

❍ **C.** Transference

❍ **D.** Risk-avoidance

Quick Answer: **163**

The Details: **193**

B30. Which of these threat actors would be the MOST likely to deface a website to promote a political agenda?

❍ **A.** Organized crime

❍ **B.** Nation state

❍ **C.** Hacktivist

❍ **D.** Competitor

Quick Answer: **163**

The Details: **194**

B31. An IPS report shows a series of exploit attempts were made against externally facing web servers. The system administrator of the web servers has identified a number of unusual log entries on each system. Which of the following would be the NEXT step in the incident response process?

❍ **A.** Check the IPS logs for any other potential attacks

❍ **B.** Create a plan for removing malware from the web servers

❍ **C.** Disable any breached user accounts

❍ **D.** Disconnect the web servers from the network

Quick Answer: **163**

The Details: **195**

B32. A security administrator is viewing the logs on a laptop in the shipping and receiving department and identifies these events:

```
8:55:30 AM | D:\Downloads\ChangeLog-5.0.4.scr | Quarantine Success
9:22:54 AM | C:\Program Files\Photo Viewer\ViewerBase.dll | Quarantine Failure
9:44:05 AM | C:\Sales\Sample32.dat | Quarantine Success
```

Which of the following would BEST describe the circumstances surrounding these events?

❍ **A.** The antivirus application identified three viruses and quarantined two viruses

❍ **B.** The host-based firewall blocked two traffic flows

❍ **C.** A host-based whitelist has blocked two applications from executing

❍ **D.** A network-based IPS has identified two known vulnerabilities

Quick Answer: **163**

The Details: **196**

B33. In the past, an organization has relied on the curated Apple App Store to avoid the issues associated with malware and insecure applications. However, the IT department has discovered an iPhone in the shipping department that includes applications that are not available on the Apple App Store. How did the shipping department user install these apps on their mobile device?

○ **A.** Sideloading

○ **B.** MMS install

○ **C.** OTA updates

○ **D.** Tethering

Quick Answer: **163**

The Details: **198**

B34. A security administrator is designing a storage array that would maintain an exact replica of all data without striping. The array needs to operate normally if a single drive was to fail. Which of the following would be the BEST choice for this storage system?

○ **A.** RAID 1

○ **B.** RAID 5

○ **C.** RAID 0

○ **D.** RAID 10

Quick Answer: **163**

The Details: **199**

B35. A transportation company has moved their reservation system to a cloud-based infrastructure. The security manager would like to monitor data transfers, identify potential threats, and ensure that all data transfers are encrypted. Which of the following would be the BEST choice for these requirements?

○ **A.** VPN

○ **B.** CASB

○ **C.** NGFW

○ **D.** DLP

Quick Answer: **163**

The Details: **200**

B36. Which of the following control types is associated with a bollard?

❍ **A.** Physical

❍ **B.** Corrective

❍ **C.** Detective

❍ **D.** Compensating

Quick Answer: **163**

The Details: **201**

B37. Jack, a hacker, has identified a number of devices on a corporate network that use the username of "admin" and the password of "admin." Which vulnerability describes this situation?

❍ **A.** Improper error handling

❍ **B.** Default configuration

❍ **C.** Weak cipher suite

❍ **D.** NULL pointer dereference

Quick Answer: **163**

The Details: **202**

B38. A security administrator attends an annual industry convention with other security professionals from around the world. Which of the following attacks would be MOST likely in this situation?

❍ **A.** Smishing

❍ **B.** Supply chain

❍ **C.** Impersonation

❍ **D.** Watering hole

Quick Answer: **163**

The Details: **203**

B39. A transportation company headquarters is located in an area with frequent power surges and outages. The security administrator is concerned about the potential for downtime and hardware failures. Which of the following would provide the most protection against these issues? Select TWO.

❍ **A.** UPS

❍ **B.** NIC teaming

❍ **C.** Incremental backups

❍ **D.** Port aggregation

❍ **E.** Load balancing

❍ **F.** Dual power supplies

Quick Answer: **163**

The Details: **204**

B40. An organization has developed an in-house mobile device app for order processing. The developers would like the app to identify revoked server certificates without sending any traffic over the corporate Internet connection. Which of the following MUST be configured to allow this functionality?

❍ **A.** CSR

❍ **B.** OCSP stapling

❍ **C.** Key escrow

❍ **D.** Hierarchical CA

Quick Answer: **163**

The Details: **205**

B41. Sam, a security administrator, is configuring an IPsec tunnel to a remote site. Which protocol should she enable to protect all of the data traversing the VPN tunnel?

❍ **A.** AH

❍ **B.** Diffie-Hellman

❍ **C.** ESP

❍ **D.** SHA-2

Quick Answer: **163**

The Details: **206**

B42. A Linux administrator has received a ticket complaining of response issues with a database server. After connecting to the server, the administrator views this information:

```
Filesystem  Size  Used Avail Use% Mounted on
/dev/xvda1  158G  158G     0 100% /
```

Which of the following would BEST describe this information?

❍ **A.** Buffer overflow

❍ **B.** Resource exhaustion

❍ **C.** SQL injection

❍ **D.** Race condition

Quick Answer: **163**

The Details: **207**

B43. Which of the following would limit the type of information a company can collect from their customers?

❍ **A.** Minimization

❍ **B.** Tokenization

❍ **C.** Anonymization

❍ **D.** Masking

Quick Answer: **163**

The Details: **208**

B44. A security administrator has identified a DoS attack against the company's web server from an IPv4 address on the Internet. Which of the following security tools would provide additional details about the attacker's location? (Select TWO)

❍ **A.** tracert

❍ **B.** arp

❍ **C.** ping

❍ **D.** ipconfig

❍ **E.** dig

❍ **F.** netcat

Quick Answer: **163**

The Details: **209**

B45. A hacker is planning an attack on a large corporation. Which of the following would provide the attacker with details about the company's domain names and IP addresses?

❍ **A.** Information sharing center

❍ **B.** Vulnerability databases

❍ **C.** Automated indicator sharing

❍ **D.** Open-source intelligence

Quick Answer: **163**

The Details: **210**

B46. A security administrator is designing a network to be PCI DSS compliant. Which of the following would be the BEST choice to provide this compliance?

❍ **A.** Implement RAID for all storage systems

❍ **B.** Connect a UPS to all servers

❍ **C.** DNS should be available on redundant servers

❍ **D.** Perform regular audits and vulnerability scans

Quick Answer: **163**

The Details: **211**

B47. A security administrator would like to test a server to see if a specific vulnerability exists. Which of the following would be the BEST choice for this task?

❍ **A.** FTK Imager

❍ **B.** Autopsy

❍ **C.** Metasploit

❍ **D.** Netcat

Quick Answer: **163**

The Details: **212**

B48. A company has rolled out a new application that requires the use of a hardware-based token generator. Which of the following would be the BEST description of this access feature?

❍ **A.** Something you know

❍ **B.** Something you do

❍ **C.** Something you are

❍ **D.** Something you have

Quick Answer: **163**

The Details: **213**

B49. A company has signed an SLA with an Internet service provider. Which of the following would BEST describe the content of this SLA?

❍ **A.** The customer will connect to partner locations over an IPsec tunnel

❍ **B.** The service provider will provide 99.999% uptime

❍ **C.** The customer applications use HTTPS over tcp/443

❍ **D.** Customer application use will be busiest on the 15th of each month

Quick Answer: **163**

The Details: **214**

B50. An attacker has created many social media accounts and is posting information in an attempt to get the attention of the media. Which of the following would BEST describe this attack?

❍ **A.** On-path

❍ **B.** Watering hole

❍ **C.** Influence campaign

❍ **D.** Phishing

Quick Answer: **163**

The Details: **215**

B51. Which of the following would be the BEST way to protect credit card account information when performing real-time purchase authorizations?

❍ **A.** Masking

❍ **B.** DLP

❍ **C.** Tokenization

❍ **D.** NGFW

Quick Answer: **163**

The Details: **216**

B52. The network design of an online women's apparel company includes a primary data center in the United States and secondary data centers in London and Tokyo. Customers place orders online via HTTPS to servers at the closest data center, and these orders and customer profiles are then centrally stored in the United States data center. The connections between all data centers use Internet links with IPsec tunnels. Fulfillment requests are sent from the United States data center to shipping locations in the customer's country. Which of the following should be the CIO's MOST significant security concern with this existing network design?

❍ **A.** IPsec connects data centers over public Internet links

❍ **B.** Fulfillment requests are shipped within the customer's country

❍ **C.** Customer information is transferred between countries

❍ **D.** The data centers are located geographically distant from each other

Quick Answer: **163**

The Details: **217**

B53. A government transport service has installed access points that support WPA3. Which of the following technologies would provide enhanced security for PSK while using WPA3?

❍ **A.** 802.1X

❍ **B.** SAE

❍ **C.** WEP

❍ **D.** WPS

Quick Answer: **163**

The Details: **218**

B54. A security administrator has found a keylogger installed alongside an update of accounting software. Which of the following would prevent the transmission of the collected logs?

❍ **A.** Prevent the installation of all software

❍ **B.** Block all unknown outbound network traffic at the Internet firewall

❍ **C.** Install host-based anti-virus software

❍ **D.** Scan all incoming email attachments at the email gateway

Quick Answer: **163**

The Details: **219**

B55. A user in the marketing department is unable to connect to the wireless network. After authenticating with a username and password, the user receives this message: The AP is configured with WPA3 encryption and 802.1X authentication.

```
-- -- --
The connection attempt could not be completed.
The Credentials provided by the server could not be validated.
Radius Server: radius.example.com
Root CA: Example.com Internal CA Root Certificate
-- -- --
```

Which of the following is the MOST likely reason for this login issue?

❍ **A.** The user's computer is in the incorrect VLAN

❍ **B.** The RADIUS server is not responding

❍ **C.** The user's computer does not support WPA3 encryption

❍ **D.** The user is in a location with an insufficient wireless signal

❍ **E.** The client computer does not have the proper certificate installed

Quick Answer: **163**

The Details: **220**

B56. A security administrator has created a new policy that prohibits the use of MD5 hashes due to collision problems. Which of the following describes the reason for this new policy?

❍ **A.** Two different messages have different hashes

❍ **B.** The original message can be derived from the hash

❍ **C.** Two identical messages have the same hash

❍ **D.** Two different messages share the same hash

Quick Answer: **163**

The Details: **222**

B57. Jack, a security administrator, has been tasked with hardening all of the internal web servers to prevent on-path attacks and to protect the application traffic from protocol analysis. These requirements should be implemented without changing the configuration on the client systems. Which of the following should Jack include in his project plan?
(Select TWO)

❍ **A.** Add DNSSEC records on the internal DNS servers

❍ **B.** Use HTTPS over port 443 for all server communication

❍ **C.** Use IPsec for client connections

❍ **D.** Create a web server certificate and sign it with the internal CA

❍ **E.** Require FTPS for all file transfers

Quick Answer: **163**

The Details: **223**

B58. A security administrator has identified the installation of a RAT on a database server and has quarantined the system. Which of the following should be followed to ensure that the integrity of the evidence is maintained?

❍ **A.** Perfect forward secrecy

❍ **B.** Non-repudiation

❍ **C.** Chain of custody

❍ **D.** Legal hold

Quick Answer: **163**

The Details: **224**

B59. Which of the following would be the BEST option for application testing in an environment that is completely separated from the production network?

❍ **A.** Virtualization

❍ **B.** VLANs

❍ **C.** Cloud computing

❍ **D.** Air gap

Quick Answer: **163**

The Details: **225**

B60. To process the company payroll, a manager logs into a third-party browser-based application and enters the hours worked for each employee. The financial transfers and physical check mailings are all provided by the third-party company. The manager does not maintain any servers or virtual machines within his company. Which of the following would BEST describe this application model?

❍ **A.** PaaS

❍ **B.** Private

❍ **C.** SaaS

❍ **D.** IaaS

Quick Answer: **163**

The Details: **226**

B61. Which of the following BEST describes the modification of application source code that removes white space, shortens variable names, and rearranges the text into a compact format?

❍ **A.** Confusion

❍ **B.** Obfuscation

❍ **C.** Encryption

❍ **D.** Diffusion

Quick Answer: **163**

The Details: **227**

B62. Which of the following vulnerabilities would be the MOST significant security concern when protecting against a competitor?

❍ **A.** Data center access with only one authentication method

❍ **B.** Spoofing of internal IP addresses when accessing an intranet server

❍ **C.** Employee VPN access uses a weak encryption cipher

❍ **D.** Lack of patch updates on an Internet-facing database server

Quick Answer: **163**

The Details: **228**

B63. A third-party vulnerability scan reports that a company's web server software version is susceptible to a memory leak vulnerability. Which of the following would be the expected result if this vulnerability was exploited?

❍ **A.** DDoS

❍ **B.** Data theft

❍ **C.** Unauthorized system access

❍ **D.** Rootkit installation

Quick Answer: **163**

The Details: **229**

B64. Which of the following would be the BEST way to determine if files have been modified after the forensics data acquisition process has occurred?

❍ **A.** Use a tamper seal on all storage devices

❍ **B.** Create a hash of the data

❍ **C.** Create an image of each storage device for future comparison

❍ **D.** Take screenshots of file directories with file sizes

Quick Answer: **163**

The Details: **230**

B65. A system administrator is implementing a password policy that would require letters, numbers, and special characters to be included in every password. Which of the following controls MUST be in place to enforce this password policy?

❍ **A.** Length

❍ **B.** Lockout

❍ **C.** Reuse

❍ **D.** Complexity

Quick Answer: **163**

The Details: **231**

B66. Which of the following applies scientific principles to provide a post-event analysis of an intrusion?

❍ **A.** MITRE ATT&CK framework

❍ **B.** ISO 27701

❍ **C.** Diamond model

❍ **D.** NIST RMF

Quick Answer: **163**

The Details: **232**

B67. Which of the following would be the MOST likely result of plaintext application communication?

❍ **A.** Buffer overflow

❍ **B.** Replay attack

❍ **C.** Resource exhaustion

❍ **D.** Directory traversal

Quick Answer: **163**

The Details: **233**

B68. Daniel, a system administrator, believes that certain configuration files on a Linux server have been modified from their original state. Daniel has reverted the configurations to their original state, but he would like to be notified if they are changed again. Which of the following would be the BEST way to provide this functionality?

❍ **A.** HIPS

❍ **B.** File integrity check

❍ **C.** Application allow list

❍ **D.** WAF

Quick Answer: **163**

The Details: **234**

B69. A security administrator is updating the network infrastructure to support 802.1X authentication. Which of the following would be the BEST choice for this configuration?

❍ **A.** LDAP

❍ **B.** HTTPS

❍ **C.** SNMPv3

❍ **D.** MS-CHAP

Quick Answer: **163**

The Details: **235**

B70. Your company owns a purpose-built appliance that doesn’t provide any access to the operating system and doesn't provide a method to upgrade the firmware. Which of the following describes this appliance?

❍ **A.** End-of-life

❍ **B.** Weak configuration

❍ **C.** Improper input handling

❍ **D.** Embedded system

Quick Answer: **163**

The Details: **236**

B71. Last month, a finance company disposed of seven-year-old printed customer account summaries that were no longer required for auditing purposes. A recent online search has now found that images of these documents are available as downloadable torrents. Which of the following would MOST likely have prevented this information breach?

❍ **A.** Pulping

❍ **B.** Degaussing

❍ **C.** NDA

❍ **D.** Fenced garbage disposal areas

Quick Answer: **163**

The Details: **237**

B72. A security manager believes that an employee is using their laptop to circumvent the corporate Internet security controls through the use of a cellular hotspot. Which of the following could be used to validate this belief? (Select TWO)

❍ **A.** HIPS

❍ **B.** UTM appliance logs

❍ **C.** Web application firewall events

❍ **D.** Host-based firewall logs

❍ **E.** Next-generation firewall logs

Quick Answer: **163**

The Details: **238**

B73. An application developer is creating a mobile device app that will include extensive encryption and decryption. Which of the following technologies would be the BEST choice for this app?

❍ **A.** AES

❍ **B.** Elliptic curve

❍ **C.** Diffie-Hellman

❍ **D.** PGP

Quick Answer: **163**

The Details: **239**

B74. Which of the following would be a common result of a successful vulnerability scan?

❍ **A.** A list of usernames and password hashes from a server

❍ **B.** A list of Microsoft patches that have not been applied to a server

❍ **C.** A copy of image files from a private file share

❍ **D.** The BIOS configuration of a server

Quick Answer: **163**

The Details: **240**

B75. A security administrator is researching an issue with conference room users at a remote site. When connected to the wireless network, users receive an IP address that is not part of the corporate addressing scheme. Communication over this network also appears to have slower performance than the wireless connections elsewhere in the building. Which of the following would be the MOST likely reason for these issues?

❍ **A.** Rogue access point

❍ **B.** Domain hijack

❍ **C.** DDoS

❍ **D.** MAC flooding

Quick Answer: **163**

The Details: **241**

B76. A company has identified a compromised server, and the security team would like to know if an attacker has used this device to move between systems. Which of the following would be the BEST way to provide this information?

❍ **A.** DNS server logs

❍ **B.** Penetration test

❍ **C.** NetFlow logs

❍ **D.** Email header

Quick Answer: **163**

The Details: **242**

B77. A system administrator has protected a set of system backups with an encryption key. The system administrator used the same key when restoring files from this backup. Which of the following would BEST describe this encryption type?

❍ **A.** Asymmetric

❍ **B.** Key escrow

❍ **C.** Symmetric

❍ **D.** Out-of-band key exchange

Quick Answer: **163**

The Details: **243**

B78. A new malware variant takes advantage of a vulnerability in a popular email client. Once installed, the malware forwards all email attachments containing credit card information to an external email address. Which of the following would limit the scope of this attack?

❍ **A.** Enable MFA on the email client

❍ **B.** Scan outgoing traffic with DLP

❍ **C.** Require users to enable the VPN when using email

❍ **D.** Update the list of malicious URLs in the firewall

Quick Answer: **163**

The Details: **244**

B79. An organization has identified a security breach and has removed the affected servers from the network. Which of the following is the NEXT step in the IR process?

❍ **A.** Eradication

❍ **B.** Preparation

❍ **C.** Recovery

❍ **D.** Identification

❍ **E.** Containment

Quick Answer: **163**

The Details: **245**

B80. A manager of the accounting department would like to minimize the opportunity for embezzlement and fraud from any of the current accounting team employees. Which of these policies should the manager use to avoid these issues?

❍ **A.** Background checks

❍ **B.** Clean desk policy

❍ **C.** Mandatory vacations

❍ **D.** Acceptable use policy

Quick Answer: **163**

The Details: **246**

B81. Which of the following would be the MAIN reasons why a system administrator would use a TPM when configuring full disk encryption? (Select TWO)

❍ **A.** Allows the encryption of multiple volumes

❍ **B.** Uses burned-in cryptographic keys

❍ **C.** Stores certificates in a hardware security module

❍ **D.** Protects against EMI leakage

❍ **E.** Includes built-in protections against brute-force attacks

Quick Answer: **163**

The Details: **247**

B82. A security administrator would like to create an access control where each file or folder is assigned a security clearance level, such as "confidential" or "secret." The security administrator would then assign a maximum security level to each user. What type of access control would be used in this network?

❍ **A.** Mandatory

❍ **B.** Rule-based

❍ **C.** Discretionary

❍ **D.** Role-based

Quick Answer: **163**

The Details: **248**

B83. Cameron, a security administrator, is reviewing a report that shows a number of devices on internal networks attempting to connect with servers in the data center network. Which of the following security controls should Cameron add to prevent internal systems from accessing data center devices?

❍ **A.** VPN
❍ **B.** IPS
❍ **C.** NAT
❍ **D.** ACL

Quick Answer: **163**

The Details: **249**

B84. A financial services company is headquartered in an area with a high occurrence of tropical storms and hurricanes. Which of the following would be MOST important when restoring services disabled by a storm?

❍ **A.** Disaster recovery plan
❍ **B.** Stakeholder management
❍ **C.** Communication plan
❍ **D.** Retention policies

Quick Answer: **163**

The Details: **250**

B85. A user in the mail room has reported an overall slowdown of his shipping management software. An anti-virus scan did not identify any issues, but a more thorough malware scan identified a kernel driver that was not part of the original operating system installation. Which of the following malware was installed on this system?

❍ **A.** Rootkit
❍ **B.** RAT
❍ **C.** Bot
❍ **D.** Ransomware
❍ **E.** Keylogger

Quick Answer: **163**

The Details: **251**

B86. A virus scanner has identified a macro virus in a word processing file attached to an email. Which of the following information could be obtained from the metadata of this file?

❍ **A.** IPS signature name and number

❍ **B.** Operating system version

❍ **C.** Date and time when the file was created

❍ **D.** Alert disposition

Quick Answer: **163**

The Details: **252**

B87. If a person is entering a data center facility, they must check-in before they are allowed to move further into the building. People who are leaving must be formally checked-out before they are able to exit the building. Which of the following would BEST facilitate this process?

❍ **A.** Access control vestibule

❍ **B.** Air gap

❍ **C.** Faraday cage

❍ **D.** Protected distribution

Quick Answer: **163**

The Details: **253**

B88. A security administrator has discovered that an employee has been exfiltrating confidential company information by embedding the data within image files and emailing the images to a third-party. Which of the following would best describe this activity?

❍ **A.** Digital signatures

❍ **B.** Steganography

❍ **C.** Block cipher

❍ **D.** Perfect forward secrecy

Quick Answer: **163**

The Details: **254**

B89. A security engineer is running a vulnerability scan on their own workstation. The scanning software is using the engineers account access to perform all scans. What type of scan is running?

❍ **A.** Unknown environment

❍ **B.** Passive

❍ **C.** Credentialed

❍ **D.** Agile

Quick Answer: **163**

The Details: **255**

B90. Which of the following would be the best way to describe the estimated number of laptops that might be stolen in a fiscal year?

❍ **A.** ALE

❍ **B.** SLE

❍ **C.** ARO

❍ **D.** MTTR

Quick Answer: **163**

The Details: **256**

Practice Exam B

Multiple Choice Quick Answers

B6. A
B7. D
B8. A
B9. B
B10. D
B11. C
B12. D
B13. D
B14. C
B15. C
B16. D
B17. D
B18. D
B19. D
B20. C
B21. B
B22. D
B23. C
B24. A
B25. B
B26. C
B27. C
B28. A
B29. B
B30. C
B31. D
B32. A
B33. A
B34. A
B35. B
B36. A
B37. B
B38. D
B39. A and F
B40. B
B41. C
B42. B
B43. A
B44. A and E
B45. D
B46. D
B47. C
B48. D
B49. B
B50. C
B51. C
B52. C
B53. B
B54. B
B55. E
B56. D
B57. B and D
B58. C
B59. D
B60. C
B61. B
B62. D
B63. A
B64. B
B65. D
B66. C
B67. B
B68. B
B69. A
B70. D
B71. A
B72. A and D
B73. B
B74. B
B75. A
B76. C
B77. C
B78. B
B79. A
B80. C
B81. B and E
B82. A
B83. D
B84. A
B85. A
B86. C
B87. A
B88. B
B89. C
B90. C

Practice Exam B Detailed Answers

B1. Select the values associated with the following RAID specifications:

	RAID 0	**RAID 1**	**RAID 5**
Minimum Number of Drives	2	2	3
Striping	Yes	No	Yes
Mirroring	No	Yes	No
Parity Data	No	No	Yes

Understanding the configurations of different RAID (Redundant Array of Inexpensive Disks) arrays is useful when designing and building storage systems.

RAID 0 is also known as striping, and requires a minimum of two drives. Data is alternatively copied to multiple drives, or striped. Since the data is not mirrored and parity data is not available, a single drive failure will result in loss of data. We often refer to RAID 0 as having 0 redundancy.

RAID 1 is a mirrored configuration where data is duplicated across multiple drives, and at least two drives are required to provide a duplicate copy. Since an exact replica of data resides on another drive, parity data is not required. If a single drive fails, data on the RAID 1 array will continue to be available on the replica drive.

RAID 5 is a combination of striping and parity. Information is striped between at least three physical drives, and additional parity information is stored on one of the drives. If a single drive fails, the missing data will be recalculated from the parity information.

More information:
SY0-601, Objective 2.5 - Disk Redundancy
https://professormesser.link/601020501

B2. An organization is deploying a mobile app to its sales force in the field. The application will be accessed from tablets for all remote sales team members and a browser-based front-end on desktops for corporate office users. The company would like to enable security features for both platforms.

The application contains sensitive customer information, and two forms of authentication are required to launch the application.

Select three security features that would apply to each platform. A security feature will only be used once. Not all security features will be used.

Security Features

Environmental Sensors

Locking Cabinets

Tablet for Field Sales

Desktop with Browser-based Front-end

Tablet for Field Sales	Desktop with Browser-based Front-end
Remote Wipe	Host-based Firewall
Full Device Encryption	Anti-Malware
Face recognition	Smart Card

This question focuses on security features for end-user computing devices.

As a mobile device, a tablet will need additional security for remote wiping of data and encryption of all data on the device. As an additional security feature, face recognition can provide additional authentication options using the built-in camera on the tablet.

Since a desktop does not often move, the security requirements are different than a mobile device. A host-based firewall and anti-virus software is common on a desktop computer, and a smart card can provide an additional authentication factor.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

More information:
SY0-601, Objective 3.5 - Mobile Device Management
https://professormesser.link/601030502

B3. Sam, a security administrator, is responsible for gathering evidence from a server that was part of a security breach. Which items should Sam prioritize for forensic evidence gathering? Order the following from highest priority to least priority.

CPU registers

Routing table

Temporary files

Event logs

Backup tapes

When gathering information for evidence, the volatility of the data becomes important. The proper order for collecting this information would be to gather the most volatile data first, followed by the next least-volatile, and so on.

CPU registers can change millions of times a second, making them a very volatile data source.

Routing tables can update themselves dynamically, and it's common to see updates occur every thirty seconds or less.

Temporary files are usually stored while an application is in use, so they may be available to collect for a few minutes or a few hours.

Event logs tend to be stored for longer periods, but some logs may be deleted every few hours or at the end of the day.

Backup tapes are the least-volatile in this list, and it's not uncommon to see backup data archived for years at a time.

More information:
SY0-601, Objective 4.5 - Forensics Data Acquisition
https://professormesser.link/601040502

B4. Match the security technology to the implementation:

Hashing	Store a password on an authentication server
Digital signature	Verify a sender's identity
Encryption	Protect private information sent over an insecure channel
Key escrow	Use a secondary decryption key
Certificate Authority	Trust a website without prior contact with the site owner
Perfect Forward Secrecy	Use a different encryption key for each session

Hashing provides a one-way cryptographic algorithm that allows for the secure storage of passwords.

Digital signatures use hashing and asymmetric encryption to ensure integrity and non-repudiation of data.

Data encryption ensures that information can be securely transmitted from a source to a destination.

Key escrow is commonly used as a method of storing decryption keys with a trusted third-party.

Certificate authorities are used as a method of trusting a certificate. If a certificate has been signed by a trusted CA, then the certificate owner can also be trusted.

Perfect forward secrecy uses temporary encryption keys that change between sessions. This constant switching of keys makes it more difficult for a third-party to decrypt the data later.

More information:
SY0-601, Assorted topics in Objective 2.8 - Cryptography
https://professormesser.link/601020801

B5. Select the data state that best fits the description. Each data state will be used more than once.

Data in-transit	All switches in a data center are connected with an 802.1Q trunk
Data in-transit	Sales information is uploaded daily from a remote site using a satellite network
Data at-rest	A company stores customer purchase information in a MySQL database
Data in-use	An application decrypts credit card numbers and expiration dates to validate for approval
Data in-use	An authentication program performs a hash of all passwords
Data in-transit	An IPS identifies a SQL injection attack and removes the attack frames from the network
Data in-use	An automatic teller machine validates a user's PIN before allowing a deposit
Data in-use	Each time a spreadsheet is updated, all of the cells containing formulas are automatically updated
Data at-rest	All weekly backup tapes are transported to an offsite storage facility
Data at-rest	All user spreadsheets are stored on a cloud-based file sharing service

Data in-transit is moving across the network.

Data at-rest is located on a storage device.

Data in-use is in the memory of a device.

More information:
SY0-601, Objective 2.1 - Protecting Data
https://professormesser.link/601020102

B6. A security administrator has performed an audit of the organization's production web servers, and the results have identified banner information leakage, web services running from a privileged account, and inconsistencies with SSL certificates. Which of the following would be the BEST way to resolve these issues?

❍ **A.** Server hardening

❍ **B.** Multi-factor authentication

❍ **C.** Enable HTTPS

❍ **D.** Run operating system updates

The Answer: A. Server hardening
Many applications and services include secure configuration guides that can assist in hardening the system. These hardening steps will make the system as secure as possible while simultaneously allowing the application to run efficiently.

The incorrect answers:
B. Multi-factor authentication
Although multi-factor authentication is always a good best practice, simply enabling multiple authentication methods would not resolve the issues identified during the audit.

C. Enable HTTPS
Most web servers will use HTTPS to ensure that network communication is encryption. However, the encrypted network traffic would not correct the issues identified during the audit.

D. Run operating system updates
Keeping the system up to date is another good best practice, but the issues identified during the audit were not bugs related to the operating systems. All of the issues identified in the audit appear to be related to the configuration of the web server, so any resolution will focus on correcting these configuration issues.

More information:
SY0-601, Objective 5.2 - Secure Configurations
https://professormesser.link/601050203

B7. A shipping company stores information in small regional warehouses around the country. The company keeps an IPS online at each warehouse to watch for suspicious traffic patterns. Which of the following would BEST describe the security control used at the warehouse?

❍ **A.** Administrative

❍ **B.** Compensating

❍ **C.** Physical

❍ **D.** Detective

The Answer: D. Detective
An IPS can detect and record any intrusion attempt.

The incorrect answers:
A. Administrative
Administrative controls would control how people act, such as security policies and standard operating procedures.

B. Compensating
A compensating control can't prevent an attack, but it can compensate when an attack occurs. For example, a compensating control would be the re-imaging process or a server restored from backup if an attack had been identified.

C. Physical
A physical control would block access. For example, a door lock or security guard would be a physical control.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

B8. The Vice President of Sales has asked the IT team to create daily backups of the sales data. The Vice President is an example of a:

❍ **A.** Data owner

❍ **B.** Data protection officer

❍ **C.** Data steward

❍ **D.** Data processor

The Answer: A. Data owner
The data owner is accountable for specific data, and is often a senior officer of the organization.

The incorrect answers:
B. Data protection officer
The data protection officer (DPO) is responsible for the organization's data privacy. The DPO commonly sets processes and procedures for maintaining the privacy of data.

C. Data steward
The data steward manages access rights to the data. In this example, the IT team would be the data steward.

D. Data processor
The data processor is often a third-party that processes data on behalf of the data controller.

More information:
SY0-601, Objective 5.5 - Data Roles and Responsibilities
https://professormesser.link/601050504

B9. A security engineer is preparing to conduct a penetration test. Part of the preparation involves reading through social media posts for information about a third-party website. Which of the following describes this practice?

○ **A.** Partially known environment

○ **B.** OSINT

○ **C.** Exfiltration

○ **D.** Active footprinting

The Answer: B. OSINT
OSINT (Open Source Intelligence) describes the process of obtaining information from open sources, such as social media sites, corporate websites, online forums, and other publicly available locations.

The incorrect answers:
A. Partially known environment
A partially known environment test describes how much information the attacker knows about the test. The attacker may have access to some information about the test, but not all information is disclosed.

C. Exfiltration
Exfiltration describes the theft of data by an attacker.

D. Active footprinting
Active footprinting would show some evidence of data gathering. For example, performing a ping scan or DNS query wouldn't exploit a vulnerability, but it would show that someone was gathering information.

More information:
SY0-601, Objective 1.8 - Reconnaissance
https://professormesser.link/601010802

B10. A company would like to automate their response when a virus is detected on company devices. Which of the following would be the BEST way to implement this function?

❍ **A.** Active footprinting

❍ **B.** IaaS

❍ **C.** Vulnerability scan

❍ **D.** SOAR

The Answer: D. SOAR
SOAR (Security Orchestration, Automation, and Response) provides security teams with integration and automation of processes and procedures.

The incorrect answers:
A. Active footprinting
Active footprinting will gather information about a system, but it does not provide any ongoing monitoring or response features.

B. IaaS
IaaS (Infrastructure as a Service) is a type of cloud service that provides the basic hardware required to install an OS and application. IaaS does not provide ongoing monitoring for security events or automation features.

C. Vulnerability scan
A vulnerability scan will identify any known vulnerabilities that may be associated with a system. However, a vulnerability scan will not identify real-time infections or automate the response.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

B11. A user in the accounting department has received an email from the CEO requesting payment for a recently purchased tablet. However, there doesn't appear to be a purchase order associated with this request. Which of the following would be the MOST likely attack associated with this email?

❍ **A.** Spear phishing

❍ **B.** Watering hole attack

❍ **C.** Invoice scam

❍ **D.** Credential harvesting

The Answer: C. Invoice scam
Invoice scams attempt to take advantage of the miscommunication between different parts of the organization. Fake invoices are submitted by the attacker, and these invoices can sometimes be incorrectly paid without going through the expected verification process.

The incorrect answers:
A. Spear phishing
Spear phishing is a directed attack that attempts to obtain private or personal information. In this example, the result was to obtain payment and not to gather private information.

B. Watering hole attack
A watering hole attack requires users to visit a central website or location. This example did not require the user to visit any third-party websites.

D. Credential harvesting
Credential harvesting attempts to transfer password files and authentication information from other computers.

More information:
SY0-601, Objective 1.1 - Other Social Engineering Attacks
https://professormesser.link/601010109

B12. A company has been informed of a hypervisor vulnerability that could allow users on one virtual machine to access resources on another virtual machine. Which of the following would BEST describe this vulnerability?

❍ **A.** Containerization

❍ **B.** Service integration

❍ **C.** SDN

❍ **D.** VM escape

The Answer: D. VM escape
A VM (Virtual Machine) escape is a vulnerability that allows communication between separate VMs.

The incorrect answers:
A. Containerization
Containerization is an application deployment architecture that uses a self-contained group of application code and dependencies. Many separate containers can run on a single system

B. Service integration
Service Integration and Management (SIAM) allows the integration of many different service providers into a single management system. This simplifies the application management and deployment process when using separate cloud providers.

C. SDN
SDN (Software-Defined Networking) separates the control plane of networking devices from the data plane. This allows for more automation and dynamic changes to the infrastructure.

More information:
SY0-601, Objective 2.2 - Virtualization Security
https://professormesser.link/601020205

B13. While working from home, users are attending a project meeting over a web conference. When typing in the meeting link, the browser is unexpectedly directed to a different website than the web conference. Users in the office do not have any issues accessing the conference site. Which of the following would be the MOST likely reason for this issue?

❍ **A.** Bluejacking

❍ **B.** Wireless disassociation

❍ **C.** DDoS

❍ **D.** DNS poisoning

The Answer: D. DNS poisoning
An attacker that gains access to a DNS (Domain Name System) server can modify the configuration files and redirect users to a different website. Anyone using a different DNS server may not see any problems with connectivity to the original site.

The incorrect answers:
A. Bluejacking
Bluejacking allows a third-party to send unsolicited messages to another device using Bluetooth. The attack in this example did not use Bluetooth as an attack vector.

B. Wireless disassociation
Wireless disassociation would cause users on a wireless network to constantly disconnect. Wireless disassociation would not cause a redirection of a website URL (Uniform Resource Locator).

C. DDoS
DDOS (Distributed Denial of Service) would attack a service from many different devices and cause the service to be unavailable. In this example, the service did not have any availability problems to valid users.

More information:
SY0-601, Objective 1.4 - DNS Attacks
https://professormesser.link/601010409

B14. A company is launching a new internal application that will not start until a username and password is entered and a smart card is plugged into the computer. Which of the following BEST describes this process?

❍ **A.** Federation

❍ **B.** Accounting

❍ **C.** Authentication

❍ **D.** Authorization

The Answer: C. Authentication
The process of proving who you say you are is authentication. In this example, the password and smart card are two factors of authentication, and both reasonably prove that the person logging in is authentic.

The incorrect answers:
A. Federation
Federation provides a way to authenticate and authorize between two different organizations. In this example, the authentication process uses internal information without any type of connection or trust to a third-party.

B. Accounting
Accounting will document information regarding a user's session, such as login time, data sent and received, files transferred, and logout time.

D. Authorization
The authorization process assigns users to resources. This process commonly occurs after the authentication process is complete.

More information:
SY0-601, Objective 2.4 - Authentication Methods
https://professormesser.link/601020401

B15. An online retailer is planning a penetration test as part of their PCI DSS validation. A third-party organization will be performing the test, and the online retailer has provided the Internet-facing IP addresses for their public web servers but no other details. What penetration testing methodology is the online retailer using?

❍ **A.** Known environment

❍ **B.** Passive footprinting

❍ **C.** Partially known environment

❍ **D.** Ping scan

The Answer: C. Partially known environment
A partially known environment test is performed when the attacker knows some information about the victim, but not all information is available.

The incorrect answers:
A. Known environment
A known environment test is performed when the attacker has complete details about the victim's systems and infrastructure.

B. Passive footprinting
Passive footprinting is the process of gathering information from publicly available sites, such as social media or corporate websites.

D. Ping scan
A ping scan is a type of network scan that can identify devices connected to the network. A ping scan is not a type of penetration test.

More information:
SY0-601, Objective 1.8 - Penetration Testing
https://professormesser.link/601010801

B16. A manufacturing company makes radar used by commercial and military organizations. A recently proposed policy change would allow the use of mobile devices inside the facility. Which of the following would be the MOST significant security issue associated with this change in policy?

❍ **A.** Unauthorized software on rooted devices

❍ **B.** Remote access clients on the mobile devices

❍ **C.** Out of date mobile operating systems

❍ **D.** Photo and video use

The Answer: D. Photo and video use
The exfiltration of company confidential information is relatively simple with an easily transportable camera or video recorder. Organizations associated with sensitive products or services must always be aware of the potential for information leaks using photos or video.

The incorrect answers:
A. Unauthorized software on rooted devices
Although unauthorized software use can be a security issue, it isn't as significant as the exfiltration of company confidential information.

B. Remote access clients on the mobile devices
It's sometimes convenient to have a remote access client available, and this type of access can certainly be a concern if the proper security is not in place. However, the much more significant security issue in this list would be associated with the ease of photos and videography when working with confidential information.

C. Out of date mobile operating systems
Having an outdated operating system can potentially include security vulnerabilities, but these vulnerabilities do not have the significance of an active data exfiltration method.

More information:
SY0-601, Objective 3.5 - Mobile Device Enforcement
https://professormesser.link/601030504

B17. A company is designing an application that will have a high demand and will require significant computing resources during the summer. During the winter, there will be little to no application use and resource use should be minimal. Which of these characteristics BEST describe this application requirement?

○ **A.** Availability

○ **B.** Orchestration

○ **C.** Imaging

○ **D.** Elasticity

The Answer: D. Elasticity
Elasticity is the process of providing resources when demand increases and scaling down when the demand is low.

The incorrect answers:
A. Availability
Availability describes the ability to use a service, but it doesn't directly describe the ability of the service resources to grow or shrink based on demand.

B. Orchestration
The process of automating the configuration, maintenance, and operation of an application instance is called orchestration. The description of the application requirement didn't mention the use of automation when scaling resources.

C. Imaging
Imaging is a technique that allows a system administrator to build a specific operating system and application configuration. This configuration can then be saved as an "image" and easily deployed to other systems.

More information:
SY0-601, Objective 2.3 - Provisioning and Deprovisioning
https://professormesser.link/601020302

B18. Vala, a security analyst, has received an alert from her IPS regarding active exploit attempts from the Internet. Which of the following would provide detailed information about these exploit attempts?

○ **A.** Netstat

○ **B.** Nmap

○ **C.** Nessus

○ **D.** Wireshark

The Answer: D. Wireshark
Wireshark is a protocol analyzer, and it can provide information about every frame that traverses the network. From a security perspective, the protocol decode can show the exploitation process and details about the payloads used during the attempt.

The incorrect answers:
A. Netstat
The netstat command can display connectivity information about a device, but it won't provide any additional details about an exploit attempt.

B. Nmap
An Nmap scan is a useful tool for understanding the potential exploit vectors of a device, but it won't show information about an active exploitation attempt.

C. Nessus
Nessus is a vulnerability scanner that can help identify potential exploit vectors, but it's not useful for showing active exploitation attempts by a third-party.

More information:
SY0-601, Objective 4.1 - Packet Tools
https://professormesser.link/601040105

B19. A user in the accounting department would like to send a spreadsheet with sensitive information to a list of third-party vendors. Which of the following could be used to transfer this spreadsheet to the vendors?

❍ **A.** SNMPv3

❍ **B.** SRTP

❍ **C.** DNSSEC

❍ **D.** FTPS

The Answer: D. FTPS
FTPS (File Transfer Protocol Secure) provides mechanisms for transferring files using encrypted communication.

The incorrect answers:
A. SNMPv3
SNMPv3 (Simple Network Management Protocol version 3) uses encrypted communication to manage devices, but it is not used for secure file transfers between devices.

B. SRTP
SRTP (Secure Real-Time Transport Protocol) is used for secure voice over IP and media communication across the network.

C. DNSSEC
DNSSEC (Domain Name System Secure Extensions) are used on DNS servers to validate DNS responses using public key cryptography.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

B20. A system administrator would like to segment the network to give the marketing, accounting, and manufacturing departments their own private network. The network communication between departments would be restricted for additional security. Which of the following should be configured on this network?

❍ **A.** VPN

❍ **B.** RBAC

❍ **C.** VLAN

❍ **D.** NAT

The Answer: C. VLAN
A VLAN (Virtual Local Area Network) is a common method of logically segmenting a network. The devices in each segmented VLAN can only communicate with other devices in the same VLAN. A router is used to connect VLANs, and this router can often be used to control traffic flows between VLANs.

The incorrect answers:
A. VPN
A VPN (Virtual Private Network) is an encryption technology that can be used to secure network connections between sites or remote end-user communication. VPNs are not commonly used to segment internal network communication.

B. RBAC
RBAC (Role-Based Access Control) describes a control mechanism for managing rights and permissions in an operating system. RBAC is not used for network segmentation.

D. NAT
NAT (Network Address Translation) is used to modify the source or destination IP address or port number of a network traffic flow. NAT would not be used when segmenting internal networks.

More information:
SY0-601, Objective 3.3 - Network Segmentation
https://professormesser.link/601030302

B21. A technician at an MSP has been asked to manage devices on third-party private network. The technician needs command line access to internal routers, switches, and firewalls. Which of the following would provide the necessary access?

❍ **A.** HSM

❍ **B.** Jump server

❍ **C.** NAC

❍ **D.** Air gap

The Answer: B. Jump server
A jump server is a highly secured device commonly used to access secure areas of another network. The technician would first connect to the jump server using SSH or a VPN tunnel, and then "jump" from the jump server to other devices on the inside of the protected network. This would allow technicians at an MSP (Managed Service Provider) to securely access devices on their customer's network.

The incorrect answers:
A. HSM
An HSM (Hardware Security Module) is a secure method of cryptographic key backup and hardware-based cryptographic offloading.

C. NAC
NAC (Network Access Control) is a broad term describing access control based on a health check or posture assessment. NAC will deny access to devices that don't meet the minimum security requirements.

D. Air gap
An air gap is a segmentation strategy that separates devices or networks by physically disconnecting them from each other.

More information:
SY0-601, Objective 3.3 - Other Network Appliances
https://professormesser.link/601030310

B22. A transportation company is installing new wireless access points in their corporate offices. The manufacturer estimates that the access points will operate an average of 100,000 hours before a hardware-related outage. Which of the following describes this estimate?

○ **A.** MTTR

○ **B.** RPO

○ **C.** RTO

○ **D.** MTBF

The Answer: D. MTBF

The MTBF (Mean Time Between Failures) is the average time expected between outages. This is usually an estimation based on the internal device components and their expected operational lifetime.

The incorrect answers:

A. MTTR

MTTR (Mean Time to Repair) is the time required to repair a product or system after a failure.

B. RPO

RPO (Recovery Point Objectives) define how much data loss would be acceptable during a recovery.

C. RTO

RTO (Recovery Time Objectives) define the minimum objectives required to get up and running to a particular service level.

More information:

SY0-601, Objective 5.4 - Business Impact Analysis

https://professormesser.link/601050403

B23. A security administrator has been asked to create a policy that would prevent access to a secure area of the network. All users who are not physically located in the corporate headquarters building would be prevented from accessing this area. Which of these should the administrator use?

❍ **A.** WAF

❍ **B.** VPN

❍ **C.** Geofencing

❍ **D.** Proxy

The Answer: C. Geofencing
Geofencing uses location information from GPS (Global Positioning System), 802.11 wireless, and other methods to use as an access control method.

The incorrect answers:
A. WAF
A WAF (Web Application Firewall) is used to protect exploits against web-based applications.

B. VPN
A VPN (Virtual Private Network) is commonly used to provide access to local resources from outside the local network. A VPN-connected user would not be physically located in the corporate office.

D. Proxy
A proxy is used to make network or application requests on behalf of another person or device. A proxy does not ensure that someone would be physically located in the headquarters building.

More information:
SY0-601, Objective 3.7 - Account Policies
https://professormesser.link/601030703

B24. Which of the following would be considered multi-factor authentication?

❍ **A.** PIN and fingerprint

❍ **B.** USB token and smart card

❍ **C.** Username, password, and email address

❍ **D.** Face scan and voiceprint

The Answer: A. PIN and fingerprint
A PIN (Personal Identification Number) is something you know, and a fingerprint is something you are.

The incorrect answers:
B. USB token and smart card
A USB token and a smart card are both something you have. Both of these describe a single factor of authentication.

C. Username, password, and email address
A password is something you know, but a username and email address claim an identity but do not authenticate or prove the identity.

D. Face scan and voiceprint
Both a face scan and a voiceprint are biometric factors, or something you are. Both of these describe a single factor of authentication.

More information:
SY0-601, Objective 2.4 - Multi-factor Authentication
https://professormesser.link/601020403

B25. Sam, a security administrator, is configuring the authentication process used by technicians when logging into a router. Instead of using accounts that are local to the router, Sam would like to pass all login requests to a centralized database. Which of the following would be the BEST way to implement this requirement?

○ **A.** PAP

○ **B.** RADIUS

○ **C.** IPsec

○ **D.** MS-CHAP

The Answer: B. RADIUS
The RADIUS (Remote Authentication Dial-In User Service) protocol is a common method of centralizing authentication for users. Instead of having separate local accounts on different devices, users can authenticate with account information that is maintained in a centralized database.

The incorrect answers:
A. PAP
PAP (Password Authentication Protocol) is an authentication method that can validate a username and password, but PAP does not provide any mechanism for a centralized authentication database.

C. IPsec
IPsec is commonly used as an encrypted tunnel between sites or endpoints. It’s useful for protecting data sent over the network, but IPsec isn’t used to centralize the authentication process.

D. MS-CHAP
MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) was commonly used in Microsoft’ PPTP (Point-to-Point Tunneling Protocol), but vulnerabilities related to the use of DES (Data Encryption Standard) encryption make it relatively easy to brute force the NTLM hash used in MS-CHAP.

More information:
SY0-601, Objective 3.8 - Identity and Access Services
https://professormesser.link/601030803

B26. A recent audit has determined that many IT department accounts have been granted Administrator access. The audit recommends replacing these permissions with limited access rights. Which of the following would BEST describe this policy?

❍ **A.** Separation of duties

❍ **B.** Offboarding

❍ **C.** Least privilege

❍ **D.** Discretionary Access Control

The Answer: C. Least privilege
The policy of least privilege limits the rights and permissions of a user account to only the access required to accomplish their objectives. This policy would limit the scope of an attack originating from a user in the IT department.

The incorrect answers:
A. Separation of duties
A separation of duties policy ensures that multiple users are required to complete a single business process. Limiting the access of a user account to match their normal job requirements would not be a separation of duties.

B. Offboarding
The offboarding process describes the policies and procedures associated with someone leaving the organization or someone who is no longer an employee of the company.

D. Discretionary Access Control
With discretionary access control (DAC), access and permissions are determined by the owner or originator of the files or resources.

More information:
SY0-601, Objective 5.3 - Personnel Security
https://professormesser.link/601050301

B27. A recent security audit has discovered email addresses and passwords located in a packet capture. Which of the following did the audit identify?

❍ **A.** Weak encryption

❍ **B.** Improper patch management

❍ **C.** Insecure protocols

❍ **D.** Open ports

The Answer: C. Insecure protocols
An insecure protocol will transmit information "in the clear," or without any type of encryption or protection.

The incorrect answers:
A. Weak encryption
A weak encryption cipher will appear to protect data, but instead can be commonly circumvented to reveal the plaintext. In this example, the email addresses and passwords were not encrypted and could be viewed in a packet capture.

B. Improper patch management
Maintaining systems to the latest patch version will protect against vulnerabilities and security issues. Sending information in the clear over the network is not commonly associated with an unpatched system.

D. Open ports
Open ports are usually associated with a service or application on a device. An open port is not commonly associated with any encryption or protected network communication.

More information:
SY0-601, Objective 1.6 - Vulnerability Types
https://professormesser.link/601010601

B28. A company has connected their wireless access points and have enabled WPS. Which of the following security issues would be associated with this configuration?

❍ **A.** Brute force

❍ **B.** Client hijacking

❍ **C.** Cryptographic vulnerability

❍ **D.** Spoofing

The Answer: A. Brute force
A WPS personal identification number (PIN) was designed to have only 11,000 possible iterations, making a brute force attack possible if the access point doesn't provide any protection against multiple guesses.

The incorrect answers:
B. Client hijacking
The processes of adding a device through WPS occurs well before any app or client is used.

C. Cryptographic vulnerability
The vulnerability in WPS is based on a limited number of PIN options and not a cryptographic shortcoming.

D. Spoofing
Spoofing an existing device would not provide access to a WPS-enabled network.

More information:
SY0-601, Objective 3.4 - Wireless Authentication Methods
https://professormesser.link/601030402

B29. An organization has traditionally purchased insurance to cover a ransomware attack, but the costs of maintaining the policy have increased above the acceptable budget. The company has now decided to cancel the insurance policies and deal with ransomware issues internally. Which of the following would best describe this action?

❍ **A.** Mitigation

❍ **B.** Acceptance

❍ **C.** Transference

❍ **D.** Risk-avoidance

The Answer: B. Acceptance
Risk acceptance is a business decision that places the responsibility of the risky activity on the organization itself.

The incorrect answers:
A. Mitigation
If the organization was to purchase additional backup facilities and update their backup processes to include offline backup storage, they would be mitigating the risk of a ransomware infection.

C. Transference
Purchasing insurance to cover a risky activity is a common method of transferring risk from the organization to the insurance company.

D. Risk-avoidance
To avoid the risk of ransomware, the organization would need to completely disconnect from the Internet and disable all methods that ransomware might use to infect a system. This risk response technique would most likely not apply to ransomware.

More information:
SY0-601, Objective 5.4 - Risk Management Types
https://professormesser.link/601050401

B30. Which of these threat actors would be the MOST likely to deface a website to promote a political agenda?

❍ **A.** Organized crime

❍ **B.** Nation state

❍ **C.** Hacktivist

❍ **D.** Competitor

The Answer: C. Hacktivist
A hacktivist often has a political statement to make, and their hacking efforts would commonly result in a public display of that information.

The incorrect answers:
A. Organized crime
Organized crime is usually motivated by money. An organized crime group is more interested in stealing information than defacing sites.

B. Nation state
Nation states are highly sophisticated hackers, and their efforts are usually focused on obtaining confidential government information or disrupting governmental operations.

D. Competitor
A competitor may be interested in making another company look bad, but the reason for the denial of services is not commonly based on a political agenda.

More information:
SY0-601, Objective 1.5- Threat Actors
https://professormesser.link/601010501

B31. An IPS report shows a series of exploit attempts were made against externally facing web servers. The system administrator of the web servers has identified a number of unusual log entries on each system. Which of the following would be the NEXT step in the incident response process?

❍ **A.** Check the IPS logs for any other potential attacks

❍ **B.** Create a plan for removing malware from the web servers

❍ **C.** Disable any breached user accounts

❍ **D.** Disconnect the web servers from the network

The Answer: D. Disconnect the web servers from the network
The unusual log entries on the web server indicate that the system may have been exploited. In that situation, the servers should be isolated to prevent access to or from those systems.

The incorrect answers:
A. Check the IPS logs for any other potential attacks
Before looking for additional exploits, the devices showing a potential exploit should be isolated and contained.

B. Create a plan for removing malware from the web servers
The recovery process should occur after the systems have been isolated and contained.

C. Disable any breached user accounts
This is part of the recovery process, and it should occur after isolation and containment of the exploited servers.

More information:
SY0-601, Objective 4.2 - Incident Response Process
https://professormesser.link/601040201

B32. A security administrator is viewing the logs on a laptop in the shipping and receiving department and identifies these events:

```
8:55:30 AM | D:\Downloads\ChangeLog-5.0.4.scr | Quarantine Success
9:22:54 AM | C:\Program Files\Photo Viewer\ViewerBase.dll | Quarantine Failure
9:44:05 AM | C:\Sales\Sample32.dat | Quarantine Success
```

Which of the following would BEST describe the circumstances surrounding these events?

❍ **A.** The antivirus application identified three viruses and quarantined two viruses

❍ **B.** The host-based firewall blocked two traffic flows

❍ **C.** A host-based whitelist has blocked two applications from executing

❍ **D.** A network-based IPS has identified two known vulnerabilities

The Answer: A. The antivirus application identified three viruses and quarantined two viruses

The logs are showing the name of files on the local device and a quarantine disposition, which indicates that two of the files were moved (quarantined) to a designated area of the drive. This will prevent the malicious files from executing and will safely store the files for any future investigation. The second file in the list failed the quarantine process, and was most likely because the library was already in use by the operating system and could not be moved.

The incorrect answers:

B. The host-based firewall blocked two traffic flows

A host-based firewall will allow or deny traffic flows based on IP address, port number, application, or other criteria. A host-based firewall does not block traffic flows based on the name of an existing file, and the firewall process would not quarantine or move files to other folders.

C. A host-based whitelist has blocked two applications from executing
The "quarantine" disposition refers to a file that has been moved from one location to another. A whitelist function would simply stop the application from executing without changing the location of an application file.

D. A network-based IPS has identified two known vulnerabilities
The logs from a network-based IPS (Intrusion Prevention System) would not commonly be located on a user's laptop, and those logs would display allow or deny dispositions based on the name of a known vulnerability. A network-based IPS would also not commonly move (quarantine) files on an end-user's computer.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

B33. In the past, an organization has relied on the curated Apple App Store to avoid issues associated with malware and insecure applications. However, the IT department has discovered an iPhone in the shipping department that includes applications that are not available on the Apple App Store. How did the shipping department user install these apps on their mobile device?

❍ **A.** Sideloading

❍ **B.** MMS install

❍ **C.** OTA updates

❍ **D.** Tethering

The Answer: A. Sideloading
If Apple's iOS has been circumvented using jailbreaking, then apps can be installed without using the Apple App Store. This installation process that circumvents the App Store is called sideloading.

The incorrect answers:
B. MMS install
Text messages that prompt to install an application will link to the App Store version of the application.

C. OTA updates
OTA (Over the Air) updates are commonly provided from the carrier and are not part of mobile app installations.

D. Tethering
Tethering uses a mobile phone as a communications medium to the Internet, and it does not have any relationship to the apps that are installed on the mobile device.

More information:
SY0-601, Objective 3.5 - Mobile Device Enforcement
https://professormesser.link/601030504

B34. A security administrator is designing a storage array that would maintain an exact replica of all data without striping. The array needs to operate normally if a single drive was to fail. Which of the following would be the BEST choice for this storage system?

❍ **A.** RAID 1

❍ **B.** RAID 5

❍ **C.** RAID 0

❍ **D.** RAID 10

The Answer: A. RAID 1
RAID (Redundant Array of Independent Disks) type 1 maintains a mirror (or exact duplicate) of data across multiple drives. If a single drive was to fail, the mirror would continue to operate with the redundant data.

The incorrect answers:
B. RAID 5
RAID 5 provides redundancy through striping with parity. Although RAID 5 arrays would continue to operate through a single drive failure, the data is not replicated across drives.

C. RAID 0
RAID 0 is a striped storage system with no parity, and a single drive failure does not maintain uptime or any redundancy of data.

D. RAID 10
RAID 10 or RAID 1+0 maintains mirrored drives that contain striped data.

More information:
SY0-601, Objective 2.5 - Disk Redundancy
https://professormesser.link/601020501

B35. A transportation company has moved their reservation system to a cloud-based infrastructure. The security manager would like to monitor data transfers, identify potential threats, and ensure that all data transfers are encrypted. Which of the following would be the BEST choice for these requirements?

❍ **A.** VPN

❍ **B.** CASB

❍ **C.** NGFW

❍ **D.** DLP

The Answer: B. CASB
A CASB (Cloud Access Security Broker) is used to implement and manage security policies when working in a cloud-based environment.

The incorrect answers:
A. VPN
A VPN (Virtual Private Network) can provide an encrypted tunnel for data transfers, but it doesn't provide any monitoring or threat identification.

C. NGFW
An NGFW (Next-Generation Firewall) is a useful security tool, but it doesn't provide any cloud-based security policy monitoring.

D. DLP
DLP (Data Loss Prevention) can monitor data to prevent the transfer of sensitive information, but it doesn't identify threats or force the transfer of encrypted data.

More information:
SY0-601, Objective 3.6 - Cloud Security Solutions
https://professormesser.link/601030605

B36. Which of the following control types is associated with a bollard?

❍ **A.** Physical

❍ **B.** Corrective

❍ **C.** Detective

❍ **D.** Compensating

The Answer: A. Physical
A physical control includes real-world security features such as fences, locks, or bollards.

The incorrect answers:
B. Corrective
A corrective control is designed to mitigate any potential damage. A bollard does not provide any mitigation functions.

C. Detective
A detective security control may not prevent access, but it can identify and record a security event. A bollard does not identify or record security events.

D. Compensating
A compensating attack doesn't provide any prevention, but it can restore access through other means. A bollard does not have any method of compensating for a potential attack.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

B37. Jack, a hacker, has identified a number of devices on a corporate network that use the username of "admin" and the password of "admin." Which vulnerability describes this situation?

○ **A.** Improper error handling

○ **B.** Default configuration

○ **C.** Weak cipher suite

○ **D.** NULL pointer dereference

The Answer: B. Default configuration
When a device is first installed, it will often have a default set of credentials, such as admin/password or admin/admin. Many times, these default credentials are never changed and can allow access by anyone who knows the default configuration.

The incorrect answers:
A. Improper error handling
Error messages can sometimes provide additional information about a system. In this case, there were no error messages to provide additional reconnaissance.

C. Weak cipher suite
A weak cipher suite implies that the cryptography used in a system may be circumvented or decrypted. In this question, there wasn't any cryptography to consider as a weakness.

D. NULL pointer dereference
A NULL pointer dereference is a programming issue that causes application crashes and a potential denial of service. In this question, the issue wasn't relating to crashes or DoS issues.

More information:
SY0-601, Objective 1.6 - Vulnerability Types
https://professormesser.link/601010601

B38. A security administrator attends an annual industry convention with other security professionals from around the world. Which of the following attacks would be MOST likely in this situation?

❍ **A.** Smishing

❍ **B.** Supply chain

❍ **C.** Impersonation

❍ **D.** Watering hole

The Answer: D. Watering hole
A watering hole attack infects a third-party visited by the intended victims. An industry convention would be a perfect location to attack security professionals.

The incorrect answers:

A. Smishing
Smishing, or SMS phishing, is a phishing attack over text messaging. A security administrator attending an industry event would not be the best possible scenario for smishing.

B. Supply chain
A supply chain attack infects part of the product manufacturing process in an attempt to also infect everything further down the chain. An industry trade event would not be a common vector for a supply chain attack.

C. Impersonation
Impersonation attacks use misdirection and pretext to allow an attacker to pretend they are someone else. An industry trade show is not a common environment for an impersonation attack.

More information:
SY0-601, Objective 1.1 - Watering Hole Attacks
https://professormesser.link/601010106

B39. A transportation company headquarters is located in an area with frequent power surges and outages. The security administrator is concerned about the potential for downtime and hardware failures. Which of the following would provide the most protection against these issues? Select TWO.

❍ **A.** UPS

❍ **B.** NIC teaming

❍ **C.** Incremental backups

❍ **D.** Port aggregation

❍ **E.** Load balancing

❍ **F.** Dual power supplies

The Answers: A. UPS and **F.** Dual power supplies
A UPS (Uninterruptible Power Supply) can provide backup power when the main power source is unavailable, and dual power supplies can maintain uptime when power surges cause physical damage to one of the power supplies in a system.

The incorrect answers:
B. NIC teaming
NIC (Network Interface Card) teaming can be used for redundant network paths from a server, but it won't help with power-related issues.

C. Incremental backups
Backups are an important part of any recovery plans, but they won't avoid any power issues.

D. Port aggregation
Port aggregation is used to increase network bandwidth between switches or devices. Port aggregation won't provide any protection for power surges or power outages.

E. Load balancing
Load balancers provide a way to manage busy services by increasing the number of available servers and balancing the load between them. A load balancer won't provide any help with power issues, however.

More information:
SY0-601, Objective 2.5 - Power Redundancy
https://professormesser.link/601020503

B40. An organization has developed an in-house mobile device app for order processing. The developers would like the app to identify revoked server certificates without sending any traffic over the corporate Internet connection. Which of the following MUST be configured to allow this functionality?

❍ **A.** CSR

❍ **B.** OCSP stapling

❍ **C.** Key escrow

❍ **D.** Hierarchical CA

The Answer: B. OCSP stapling
The use of OCSP (Online Certificate Status Protocol) requires communication between the client and the CA that issued a certificate. If the CA is an external organization, then validation checks will communicate across the Internet. The certificate holder can verify their own status and avoid client Internet traffic by storing the status information on an internal server and "stapling" the OCSP status into the SSL/TLS handshake.

The incorrect answers:
A. CSR
A CSR (Certificate Signing Request) is used during the key creation process. The public key is sent to the CA to be signed as part of the CSR.

C. Key escrow
Key escrow will provide a third-party with access to decryption keys. The escrow process is not involved in real-time server revocation updates.

D. Hierarchical CA
A hierarchical CA design will create intermediate CAs to distributed the certificate management load and minimize the impact if a CA certificate needs to be revoked. The hierarchical design is not involved in the certification revocation check process.

More information:
SY0-601, Objective 3.9 - Certificate Concepts
https://professormesser.link/601030904

B41. Sam, a security administrator, is configuring an IPsec tunnel to a remote site. Which protocol should she enable to protect all of the data traversing the VPN tunnel?

- ❍ **A.** AH
- ❍ **B.** Diffie-Hellman
- ❍ **C.** ESP
- ❍ **D.** SHA-2

The Answer: C. ESP
The ESP (Encapsulation Security Payload) protocol encrypts the data that traverses the VPN.

The incorrect answers:
A. AH
The AH (Authentication Header) is used to hash the packet data for additional data integrity.

B. Diffie-Hellman
Diffie-Hellman is an algorithm used for two devices to create identical shared keys without transferring those keys across the network.

D. SHA-2
SHA-2 (Secure Hash Algorithm) is a hashing algorithm, and does not provide any data encryption.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

B42. A Linux administrator has received a ticket complaining of response issues with a database server. After connecting to the server, the administrator views this information:

```
Filesystem  Size  Used Avail Use% Mounted on
/dev/xvda1  158G  158G     0 100% /
```

Which of the following would BEST describe this information?

❍ **A.** Buffer overflow

❍ **B.** Resource exhaustion

❍ **C.** SQL injection

❍ **D.** Race condition

The Answer: B. Resource exhaustion
The available storage on the local filesystem has been depleted, and the information shows 0 bytes available. More drive space would need to be available for the server to return to normal response times.

The incorrect answers:
A. Buffer overflow
A buffer overflow allows an attacker to manipulate the contents of memory. A filesystem at 100% utilization does not describe the contents in memory.

C. SQL injection
A SQL injection is a network attack type used to access database information directly. A SQL injection would not cause significant storage drive utilization.

D. Race condition
A race condition is a programming issue where a portion of the application is making changes that are not seen by other parts of the application. A race condition does not commonly use all available storage space on the device.

More information:
SY0-601, Objective 1.3 - Other Application Attacks
https://professormesser.link/601010310

B43. Which of the following would limit the type of information a company can collect from their customers?

❍ **A.** Minimization

❍ **B.** Tokenization

❍ **C.** Anonymization

❍ **D.** Masking

The Answer: A. Minimization
Data minimization is a guideline that limits the amount of collected information to necessary data. This guideline is part of many data privacy regulations, including HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation).

The incorrect answers:
B. Tokenization
Tokenization replaces sensitive data with a non-sensitive placeholder. Tokenization is commonly used for NFC (Near-Field Communication) payment systems.

C. Anonymization
Anonymization changes data to remove or replace identifiable information. For example, an anonymized purchase history database might change the first and last names to random values but keep the purchase information intact.

D. Masking
Data masking hides some of the original data to protect sensitive information.

More information:
SY0-601, Objective 5.5 - Enhancing Privacy
https://professormesser.link/601050503

B44. A security administrator has identified a DoS attack against the company's web server from an IPv4 address on the Internet. Which of the following security tools would provide additional details about the attacker's location? (Select TWO)

❍ **A.** tracert

❍ **B.** arp

❍ **C.** ping

❍ **D.** ipconfig

❍ **E.** dig

❍ **F.** netcat

The Answer: A. tracert and **E.** dig

Tracert (traceroute) provides a summary of hops between two devices. In this example, tracert can be used to determine the local ISP's IP addresses and more information about the physical location of the attacker. The dig (Domain Information Groper) command can be used to perform a reverse-lookup of the IPv4 address and determine the IP address block owner that may be responsible for this traffic.

The incorrect answers:

B. arp

The arp (Address Resolution Protocol) command shows a mapping of IP addresses to local MAC addresses. This information doesn't provide any detailed location information outside of the local IP subnet.

C. ping

The ping command can be used to determine if a device may be connected to the network, but it doesn't help identify any geographical details.

D. ipconfig

The ipconfig command shows the IP address configuration of a local device, but it doesn't provide any information about a remote computer.

F. netcat

Netcat reads or writes information to the network. Netcat is often used as a reconnaissance tool, but it has limited abilities to provide any location information of a device.

More information:

SY0-601, Objective 4.1 - Reconnaissance Tools Part 1

https://professormesser.link/601040101

B45. A hacker is planning an attack on a large corporation. Which of the following would provide the attacker with details about the company's domain names and IP addresses?

❍ **A.** Information sharing center

❍ **B.** Vulnerability databases

❍ **C.** Automated indicator sharing

❍ **D.** Open-source intelligence

The Answer: D. Open-source intelligence
Open-source intelligence, or OSINT, describes reconnaissance gathering from publicly available sources. In this example, information about domain names and IP address would be easily retrieved from a query to a public DNS (Domain Name System) server.

The incorrect answers:
A. Information sharing center
The IT security community has a number of sharing centers for threat intelligence. These sharing centers focus on security threats and don't generally provide information about specific company domain names or IP addresses.

B. Vulnerability databases
Vulnerability databases usually contain information about vulnerable operating systems and applications. IP address and domain name details aren't commonly associated with vulnerability databases.

C. Automated indicator sharing
Automated indicator sharing (AIS) is a standard format and transfer mechanism for distributing security intelligence between different organizations.

More information:
SY0-601, Objective 1.5 - Threat Intelligence
https://professormesser.link/601010503

B46. A security administrator is designing a network to be PCI DSS compliant. Which of the following would be the BEST choice to provide this compliance?

❍ **A.** Implement RAID for all storage systems

❍ **B.** Connect a UPS to all servers

❍ **C.** DNS should be available on redundant servers

❍ **D.** Perform regular audits and vulnerability scans

The Answer: D. Perform regular audits and vulnerability scans
A focus of PCI DSS (Payment Card Industry Data Security Standard) is to keep credit card information private. The only option in this list that matches this requirement is scheduled and ongoing audits.

The incorrect answers:
A. Implement RAID for all storage systems
RAID (Redundant Array of Independent Disks) is an important consideration for any project that stores data, but using a RAID array is not part of PCI DSS compliance. Although PCI DSS compliance does require backups, RAID is not a backup technology.

B. Connect a UPS to all servers
Integrating a UPS (Uninterruptible Power Supply) is an important way to maintain power during an outage, but it's not required for PCI DSS compliance.

C. DNS should be available on redundant servers
Name resolution can be an important service on the network, but maintaining redundant DNS servers isn't required for PCI DSS compliance.

More information:
SY0-601, Objective 5.2 - Security Regulations and Standards
https://professormesser.link/601050201

B47. A security administrator would like to test a server to see if a specific vulnerability exists. Which of the following would be the BEST choice for this task?

❍ **A.** FTK Imager

❍ **B.** Autopsy

❍ **C.** Metasploit

❍ **D.** Netcat

The Answer: C. Metasploit
Metasploit is an exploitation framework that can use known vulnerabilities to gain access to remote systems. Metasploit performs penetration tests and can verify the existence of a vulnerability.

The incorrect answers:
A. FTK Imager
FTK Imager is a third-party storage drive imaging tool and it can support many different drive types and encryption methods. FTK Imager will not identify software vulnerabilities.

B. Autopsy
Autopsy is a forensics tool that can view and recover data from storage devices. Autopsy does not identify operating system or application vulnerabilities.

D. Netcat
Netcat is a utility that can read and write data to the network. Netcat would not be the best choice for identifying system vulnerabilities.

More information:
SY0-601, Objective 4.1 - Forensics Tools
https://professormesser.link/601040106

B48. A company has rolled out a new application that requires the use of a hardware-based token generator. Which of the following would be the BEST description of this access feature?

❍ **A.** Something you know

❍ **B.** Something you do

❍ **C.** Something you are

❍ **D.** Something you have

The Answer: D. Something you have
The use of the hardware token generator requires that the user be in possession of the device during the login process.

The incorrect answers:
A. Something you know
The number, or token, created by the token generator isn't previously known by the user, and there's no requirement to remember the tokens once the authentication process is complete.

B. Something you do
The process of pressing the button on the token generator isn't something that would be unique to an individual user.

C. Something you are
The token generator works without any type of biometric scan or voiceprint.

More information:
SY0-601, Objective 2.4 - Multi-factor Authentication
https://professormesser.link/601020403

B49. A company has signed an SLA with an Internet service provider. Which of the following would BEST describe the content of this SLA?

❍ **A.** The customer will connect to partner locations over an IPsec tunnel

❍ **B.** The service provider will provide 99.999% uptime

❍ **C.** The customer applications use HTTPS over tcp/443

❍ **D.** Customer application use will be busiest on the 15th of each month

The Answer: B. The service provider will provide 99.999% uptime
An SLA (Service Level Agreement) is a contract that specifies the minimum terms for provided services. It's common to include uptime, response times, and other service metrics in an SLA.

The incorrect answers:
A. The customer will connect to partner locations over an IPsec tunnel
A service level agreement describes the minimum service levels provided to the customer. You would not commonly see descriptions of how the service will be used in the SLA contract.

C. The customer applications use HTTPS over tcp/443
The protocols used by the customer's applications aren't part of the service requirements from the ISP.

D. Customer application use will be busiest on the 15th of each month
The customer's application usage isn't part of the service requirements from the ISP.

More information:
SY0-601, Objective 5.3 - Third-party Risk Management
https://professormesser.link/601050302

B50. An attacker has created many social media accounts and is posting information in an attempt to get the attention of the media. Which of the following would BEST describe this attack?

❍ **A.** On-path

❍ **B.** Watering hole

❍ **C.** Influence campaign

❍ **D.** Phishing

The Answer: C. Influence campaign
Influence campaigns are carefully crafted attacks that exploit social media and traditional media.

The incorrect answers:
A. On-path
An on-path attack uses an attacker in the middle of a conversation to capture or modify information as it traverses the network.

B. Watering hole
A watering hole attack uses a carefully selected attack location to infect visitors to a specific website.

D. Phishing
A phishing attack traditionally uses email in an effort to convince the victim to disclose private or sensitive information.

More information:
SY0-601, Objective 1.1 - Influence Campaigns
https://professormesser.link/601010108

B51. Which of the following would be the BEST way to protect credit card account information when performing real-time purchase authorizations?

❍ **A.** Masking

❍ **B.** DLP

❍ **C.** Tokenization

❍ **D.** NGFW

The Answer: C. Tokenization

Tokenization is a technique that replaces user data with a non-sensitive placeholder, or token. Tokenization is commonly used on mobile devices to purchase using a credit card without transmitting the credit card number.

The incorrect answers:

A. Masking

Data masking hides sensitive data by hiding the information or replacing it with a non-sensitive alternative. An example of masking would be replacing an account number on a receipt with hash marks.

B. DLP

DLP (Data Loss Prevention) solutions can identify and block sensitive data from being sent over the network. DLP does not provide any additional security or protection for real-time financial transactions.

D. NGFW

An NGFW (Next-Generation Firewall) is an application-aware security technology. NGFW solutions can provide additional controls for specific applications, but they won't provide any additional account protections when sending financial details.

More information:

SY0-601, Objective 2.1 - Protecting Data

https://professormesser.link/601020102

B52. The network design of an online women's apparel company includes a primary data center in the United States and secondary data centers in London and Tokyo. Customers place orders online via HTTPS to servers at the closest data center, and these orders and customer profiles are then centrally stored in the United States data center. The connections between all data centers use Internet links with IPsec tunnels. Fulfillment requests are sent from the United States data center to shipping locations in the customer's country. Which of the following should be the CIO's MOST significant security concern with this existing network design?

❍ **A.** IPsec connects data centers over public Internet links

❍ **B.** Fulfillment requests are shipped within the customer's country

❍ **C.** Customer information is transferred between countries

❍ **D.** The data centers are located geographically distant from each other

The Answer: C. Customer information is transferred between countries
Data sovereignty laws can mandate how data is handled. Data that resides in a country is usually subject to the laws of that country, and compliance regulations may not allow the data to be moved outside of the country.

The incorrect answers:
A. IPsec connects data centers over public Internet links
Connecting remote locations using IPsec tunnels over public Internet connections is a common method of securely linking sites together. If someone was to capture the data traversing these links, they would find that all of the data was encrypted.

B. Fulfillment requests are shipped within the customer's country
There are no significant security issues associated with shipments within the same country.

D. The data centers are located geographically distant from each other
A best practice for many international organizations is to have data centers in geographically diverse locations to minimize the impact of any single data center outage.

More information:
SY0-601, Objective 2.1 - Protecting Data
https://professormesser.link/601020102

B53. A government transport service has installed access points that support WPA3. Which of the following technologies would provide enhanced security for PSK while using WPA3?

❍ **A.** 802.1X

❍ **B.** SAE

❍ **C.** WEP

❍ **D.** WPS

The Answer: B. SAE
WPA3 (Wi-Fi Protected Access 3) enhances the PSK (Pre-Shared Key) authentication process by privately deriving session keys instead of sending the key hashes across the network.

The incorrect answers:
A. 802.1X
802.1X is a standard for authentication using AAA (Authentication, Authorization and Accounting) services. 802.1X is commonly used in conjunction with LDAP, RADIUS, or a similar authentication service.

C. WEP
WEP (Wired Equivalent Privacy) is an older wireless encryption algorithm that was ultimately found to have cryptographic vulnerabilities.

D. WPS
WPS (Wi-Fi Protected Setup) is a standard method of connecting devices to a wireless network without requiring a PSK or passphrase.

More information:
SY0-601, Objective 3.4 - Wireless Cryptography
https://professormesser.link/601030401

B54. A security administrator has found a keylogger installed alongside an update of accounting software. Which of the following would prevent the transmission of the collected logs?

❍ **A.** Prevent the installation of all software

❍ **B.** Block all unknown outbound network traffic at the Internet firewall

❍ **C.** Install host-based anti-virus software

❍ **D.** Scan all incoming email attachments at the email gateway

The Answer: B. Block all unknown outbound network traffic at the Internet firewall

Keylogging software has two major functions; record keystrokes, and transmit those keystrokes to a remote location. Local file scanning and software best-practices can help prevent the initial installation, and controlling outbound network traffic can block unauthorized file transfers.

The incorrect answers:

A. Prevent the installation of all software
Blocking software installations may prevent the initial malware infection, but it won't provide any control of outbound keylogged data.

C. Install host-based anti-virus software
A good anti-virus application can identify malware before the installation occurs, but anti-virus does not commonly provide any control of network communication.

D. Scan all incoming email attachments at the email gateway
Malware can be installed from many sources, and sometimes the source is unexpected. Scanning or blocking executables at the email gateway can help prevent infection but it won't provide any control of outbound file transfers.

More information:
SY0-601, Objective 1.2 - An Overview of Malware
https://professormesser.link/601010201

B55. A user in the marketing department is unable to connect to the wireless network. After authenticating with a username and password, the user receives this message:

```
-- -- --
The connection attempt could not be completed.
The Credentials provided by the server could not be validated.
Radius Server: radius.example.com
Root CA: Example.com Internal CA Root Certificate
-- -- --
```

The AP is configured with WPA3 encryption and 802.1X authentication.

Which of the following is the MOST likely reason for this login issue?

❍ **A.** The user's computer is in the incorrect VLAN

❍ **B.** The RADIUS server is not responding

❍ **C.** The user's computer does not support WPA3 encryption

❍ **D.** The user is in a location with an insufficient wireless signal

❍ **E.** The client computer does not have the proper certificate installed

The Answer: E. The client computer does not have the proper certificate installed

The error message states that the server credentials could not be validated. This indicates that the certificate authority that signed the server's certificate is either different than the CA certificate installed on the client's workstation, or the client workstation does not have an installed copy of the CA's certificate. This validation process ensures that the client is communicating to a trusted server and there are no man-in-the-middle attacks occurring.

The incorrect answers:

A. The user's computer is in the incorrect VLAN

The RADIUS server certificate validation process should work properly from all VLANs. The error indicates that the communication process is working properly, so an incorrect VLAN would not be the cause of this issue.

B. The RADIUS server is not responding
If the RADIUS server had no response to the user, then the process would simply timeout. In this example, the error message indicates that the communication process is working between the RADIUS server and the client's computer.

C. The user's computer does not support WPA3 encryption
The first step when connecting to a wireless network is to associate with the 802.11 access point. If WPA3 encryption was not supported, the authentication process would not have occurred and the user's workstation would not have seen the server credentials.

D. The user is in a location with an insufficient wireless signal
The error message regarding server validation indicates that the wireless signal is strong enough to send and receive data on the wireless network.

More information:
SY0-601, Objective 3.9 - Public Key Infrastructure
https://professormesser.link/601030901

B56. A security administrator has created a new policy that prohibits the use of MD5 hashes due to collision problems. Which of the following describes the reason for this new policy?

❍ **A.** Two different messages have different hashes

❍ **B.** The original message can be derived from the hash

❍ **C.** Two identical messages have the same hash

❍ **D.** Two different messages share the same hash

The Answer: D. Two different messages share the same hash
A well-designed hashing algorithm will create a unique hash value for every possible input. If two different inputs create the same hash, the hash algorithm has created a collision.

The incorrect answers:
A. Two different messages have different hashes
In normal operation, two different inputs will create two different hash outputs.

B. The original message can be derived from the hash
Hashing is a one-way cipher, and you cannot derive the original message from a hash value.

C. Two identical messages have the same hash
Two identical messages should always create exactly the same hash output.

More information:
SY0-601, Objective 1.2 - Cryptographic Attacks
https://professormesser.link/601010214

B57. Jack, a security administrator, has been tasked with hardening all of the internal web servers to prevent on-path attacks and to protect the application traffic from protocol analysis. These requirements should be implemented without changing the configuration on the client systems. Which of the following should Jack include in his project plan? (Select TWO)

❍ **A.** Add DNSSEC records on the internal DNS servers

❍ **B.** Use HTTPS over port 443 for all server communication

❍ **C.** Use IPsec for client connections

❍ **D.** Create a web server certificate and sign it with the internal CA

❍ **E.** Require FTPS for all file transfers

The Answer: B. Use HTTPS over port 443 for all server communication, and **D.** Create a web server certificate and sign it with the internal CA

Using the secure HTTPS (Hypertext Transfer Protocol Secure) protocol will ensure that all network communication is protected between the web server and the client devices. If someone manages to capture the network traffic, they would be viewing encrypted data. A signed certificate from a trusted internal CA (Certificate Authority) allows web browsers to trust that the web server is the legitimate server endpoint. If someone attempts an on-path attack, the certificate presented will not validate and a warning message will appear in the browser.

The incorrect answers:

A. Add DNSSEC records on the internal DNS servers
DNSSEC (Domain Name System Security Extensions) records are useful to validate the IP address of a device, but they would not prevent an on-path attack. DNSSEC also doesn't provide any security of the network communication itself.

C. Use IPsec for client connections
IPsec (IP Security) would provide encrypted communication, but it is not commonly used between a web client and web server. It would also require additional configuration changes on the client devices.

E. Require FTPS for all file transfers
Web server communication occurs with HTTP or the encrypted HTTPS protocols. The FTPS (File Transfer Protocol Secure) protocol is not commonly used between web clients and servers.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

B58. A security administrator has identified the installation of a RAT on a database server and has quarantined the system. Which of the following should be followed to ensure that the integrity of the evidence is maintained?

❍ **A.** Perfect forward secrecy

❍ **B.** Non-repudiation

❍ **C.** Chain of custody

❍ **D.** Legal hold

The Answer: C. Chain of custody
A chain of custody is a documented record of the evidence. The chain of custody also documents the interactions of every person who comes into contact with the evidence.

The incorrect answers:
A. Perfect forward secrecy
Perfect forward secrecy (PFS) is an encryption technique that limits the use of session keys. PFS is not used to insure the integrity of evidence.

B. Non-repudiation
Non-repudiation ensures that the author of a document cannot be disputed. Non-repudiation does not provide any method of tracking and managing digital evidence.

D. Legal hold
A legal hold is a technique for preserving important evidence, but it doesn't provide any mechanism for the ongoing integrity of that evidence.

More information:
SY0-601, Objective 4.5 - Digital Forensics
https://professormesser.link/601040501

B59. Which of the following would be the BEST option for application testing in an environment that is completely separated from the production network?

❍ **A.** Virtualization

❍ **B.** VLANs

❍ **C.** Cloud computing

❍ **D.** Air gap

The Answer: D. Air gap
An air gapped network removes all connectivity between components and ensures that there would be no possible communication path between the test network and the production network.

The incorrect answers:
A. Virtualization
Although virtualization provides the option to connect devices in a private network, there's still the potential for a misconfigured network configuration or an application to communicate externally.

B. VLANs
VLANs (Virtual Local Area Networks) are a common segmentation technology, but a router could easily connect the VLANs to the production network.

C. Cloud computing
Cloud-based technologies provide for many network options, and it's common to maintain a connection between the cloud and the rest of the network.

More information:
SY0-601, Objective 2.7 - Secure Areas
https://professormesser.link/601020702

B60. To process the company payroll, a manager logs into a third-party browser-based application and enters the hours worked for each employee. The financial transfers and physical check mailings are all provided by the third-party company. The manager does not maintain any servers or virtual machines within his company. Which of the following would BEST describe this application model?

○ **A.** PaaS

○ **B.** Private

○ **C.** SaaS

○ **D.** IaaS

The Answer: C. SaaS

The SaaS (Software as a Service) model generally has no local application installation, no ongoing maintenance tasks, and no local infrastructure requirements. A third-party provides the application and the support, and the user simply logs in, uses the service, and logs out.

The incorrect answers:

A. PaaS

PaaS (Platform as a Service) is a model that provides a building block of features, and requires the end user to customize their own application from the available modules. There can be a significant development effort to build an application with a PaaS model.

B. Private

A private model requires that the end user purchase, install, and maintain their own application hardware and software. The SaaS model doesn't require any initial hardware or software capital purchase.

D. IaaS

IaaS (Infrastructure as a Service) is a model that provides the user with the hardware needed to get up and running, and the end user is responsible for the operating system, the application, and any ongoing maintenance tasks.

More information:

SY0-601, Objective 2.2 - Cloud Models

https://professormesser.link/601020201

B61. Which of the following BEST describes the modification of application source code that removes white space, shortens variable names, and rearranges the text into a compact format?

❍ **A.** Confusion

❍ **B.** Obfuscation

❍ **C.** Encryption

❍ **D.** Diffusion

The Answer: B. Obfuscation
Obfuscation is the process of taking something that is normally understandable and making it very difficult to understand. Many developers will obfuscate their source code to prevent others from following the logic used in the application.

The incorrect answers:
A. Confusion
Confusion is a concept associated with data encryption where the encrypted data is drastically different than the plaintext.

C. Encryption
Encrypting source code will effectively make it impossible to use unless you have the decryption key. In this example, the source code remained usable, but the readability of the source code was dramatically affected by the changes.

D. Diffusion
Diffusion is an encryption concept where changing one character of the input will cause many characters to change in the output.

More information:
SY0-601, Objective 2.3 - Secure Coding Techniques
https://professormesser.link/601020303

B62. Which of the following vulnerabilities would be the MOST significant security concern when protecting against a competitor?

○ **A.** Data center access with only one authentication method

○ **B.** Spoofing of internal IP addresses when accessing an intranet server

○ **C.** Employee VPN access uses a weak encryption cipher

○ **D.** Lack of patch updates on an Internet-facing database server

The Answer: D. Lack of patch updates on an Internet-facing database server

One of the easiest ways for a competitor to obtain information is through an existing Internet connection. An unpatched server could be exploited to obtain customer data that would not normally be available otherwise.

The incorrect answers:

A. Data center access with only one authentication method
Most competitors don't have access to walk around inside of your building, and they certainly wouldn't have access to secure areas. A single authentication method would commonly prevent unauthorized access to a data center for both employees and non-employees, although more authentication factors would provide some additional security.

B. Spoofing of internal IP addresses when accessing an intranet server
Intranet servers are not accessible from the outside. This makes them an unlikely target for competitors and other non-employees.

C. Employee VPN access uses a weak encryption cipher
A weak encryption cipher can be a security issue, but a potential exploitation would need the raw network traffic to begin any decryption attempts. Although this scenario would technically be possible if someone was to catch an employee on a public wireless network, it's not the most significant security issue in the available list.

More information:
SY0-601, Objective 1.5 - Threat Actors
https://professormesser.link/601010501

B63. A third-party vulnerability scan reports that a company's web server software version is susceptible to a memory leak vulnerability. Which of the following would be the expected result if this vulnerability was exploited?

❍ **A.** DDoS

❍ **B.** Data theft

❍ **C.** Unauthorized system access

❍ **D.** Rootkit installation

The Answer: A. DDoS
A DDoS (Distributed Denial of Service) can easily exploit a memory leak. Unused memory is not properly released, and eventually the leak uses all available memory. The system eventually crashes due to lack of resources.

The incorrect answers:
B. Data theft
A memory leak doesn't provide any additional access to data, so the theft of private information would not be an expected result.

C. Unauthorized system access
A memory leak can prevent all access to the system, but it doesn't allow any unauthorized access to the system.

D. Rootkit installation
A rootkit installation would need to be executed on the operating system, and a memory leak doesn't provide any opportunity for this installation to run.

More information:
SY0-601, Objective 1.4 - Denial of Service
http://professormesser.link/601010410

B64. Which of the following would be the BEST way to determine if files have been modified after the forensics data acquisition process has occurred?

❍ **A.** Use a tamper seal on all storage devices

❍ **B.** Create a hash of the data

❍ **C.** Create an image of each storage device for future comparison

❍ **D.** Take screenshots of file directories with file sizes

The Answer: B. Create a hash of the data
A hash will create a unique value that can be quickly validated at any time in the future. If the hash value changes, then the data must have also changed.

The incorrect answers:
A. Use a tamper seal on all storage devices
A physical tamper seal will identify if a device has been opened, but it cannot identify any changes to the data on the storage device.

C. Create an image of each storage device for future comparison
A copy of the data would allow for comparisons later, but the process of doing the comparison would take much more time than validating a hash value. It's also possible that someone could tamper with both the original data and the copy of the data.

D. Take screenshots of file directories with file sizes
It's very easy to change the contents of a file without changing the size of the file.

More information:
SY0-601, Objective 4.5 - Digital Forensics
https://professormesser.link/601040501

B65. A system administrator is implementing a password policy that would require letters, numbers, and special characters to be included in every password. Which of the following controls MUST be in place to enforce this password policy?

❍ **A.** Length

❍ **B.** Lockout

❍ **C.** Reuse

❍ **D.** Complexity

The Answer: D. Complexity
Adding different types of characters to a password requires technical controls that increase password complexity.

The incorrect answers:
A. Length
Adding all of these character types to a password do not necessarily change the length of the password.

B. Lockout
A good best-practice is to automatically lock an account with multiple invalid authentication attempts. However, a lockout policy does not enforce any password requirements.

C. Reuse
The controls that prohibit the reuse of passwords do not control the characters used in the password.

More information:
SY0-601, Objective 3.7 - Account Policies
https://professormesser.link/601030703

B66. Which of the following applies scientific principles to provide a post-event analysis of an intrusion?

❍ **A.** MITRE ATT&CK framework

❍ **B.** ISO 27701

❍ **C.** Diamond model

❍ **D.** NIST RMF

The Answer: C. Diamond model
The diamond model was created by the United State intelligence community as a way to standardize the attack reporting and the analysis of the intrusions.

The incorrect answers:
A. MITRE ATT&CK framework
MITRE provides the ATT&CK framework as a knowledgebase of attack types, techniques, and mitigation options.

B. ISO 27701
The ISO 27701 standard focuses on the implementation and maintenance of a privacy information management system (PIMS).

D. NIST RMF
The NIST (National Institute of Standards and Technology) RMF (Risk Management Framework) is a guide to help understand, manage, and rate the risks found in an organization.

More information:
SY0-601, Objective 4.2 - Attack Frameworks
https://professormesser.link/601040203

B67. Which of the following would be the MOST likely result of plaintext application communication?

❍ **A.** Buffer overflow

❍ **B.** Replay attack

❍ **C.** Resource exhaustion

❍ **D.** Directory traversal

The Answer: B. Replay attack
To perform a replay attack, the attacker needs to capture the original non-encrypted content. If an application is not using encrypted communication, the data capture process is a simple process for the attacker.

The incorrect answers:
A. Buffer overflow
A buffer overflow takes advantage of an application vulnerability and can perform this overflow over both an encrypted or non-encrypted channel.

C. Resource exhaustion
Resource exhaustion can take many different forms, but those resource issues don't necessarily require the network communication to be send in the clear.

D. Directory traversal
Directory traversal is commonly associated with moving around the file system of a server. Non-encrypted communication is not a prerequisite in a directory traversal attack.

More information:
SY0-601, Objective 1.3 - Replay Attacks
https://professormesser.link/601010305

B68. Daniel, a system administrator, believes that certain configuration files on a Linux server have been modified from their original state. Daniel has reverted the configurations to their original state, but he would like to be notified if they are changed again. Which of the following would be the BEST way to provide this functionality?

❍ **A.** HIPS

❍ **B.** File integrity check

❍ **C.** Application allow list

❍ **D.** WAF

The Answer: B. File integrity check
A file integrity check (i.e., Tripwire, System File Checker, etc.) can be used to monitor and alert if there are any changes to a file.

The incorrect answers:
A. HIPS
HIPS (Host-based Intrusion Prevention System) would help identify any security vulnerabilities, but there's nothing relating to this issue that would indicate that this issue was caused by an operating system or application vulnerability. A HIPS would not commonly alert on the modification of a specific file.

C. Application allow list
In this example, we're not sure how the file was changed or if a separate application or editor was even used. If the change was made with a valid application, an allow list would not provide any feedback or alerts.

D. WAF
A WAF (Web Application Firewall) is used to protect web-based applications from malicious attack. The example in this question was not related to a web-based application.

More information:
SY0-601, Objective 3.3 - Secure Networking
https://professormesser.link/601030305

B69. A security administrator is updating the network infrastructure to support 802.1X authentication. Which of the following would be the BEST choice for this configuration?

❍ **A.** LDAP

❍ **B.** HTTPS

❍ **C.** SNMPv3

❍ **D.** MS-CHAP

The Answer: A. LDAP

LDAP (Lightweight Directory Access Protocol) is a common protocol to use for centralized authentication. Other protocols such as RADIUS, TACACS+, or Kerberos would also be valid options for 802.1X authentication.

The incorrect answers:

B. HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is commonly used to encrypt web server communication. HTTPS is not an authentication protocol.

C. SNMPv3

SNMPv3 (Simple Network Management Protocol version 3) is used to manage servers and infrastructure devices. SNMP is not an authentication protocol.

D. MS-CHAP

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) was commonly used to authenticate devices using Microsoft's Point-to-Point Tunneling Protocol (PPTP). Security issues related to the use of DES (Data Encryption Standard) encryption in MS-CHAP eliminate it from consideration for modern authentication.

More information:

SY0-601, Objective 3.4 - Wireless Authentication Protocols

https://professormesser.link/601030403

B70. Your company owns a purpose-built appliance that doesn't provide any access to the operating system and doesn't provide a method to upgrade the firmware. Which of the following describes this appliance?

❍ **A.** End-of-life

❍ **B.** Weak configuration

❍ **C.** Improper input handling

❍ **D.** Embedded system

The Answer: D. Embedded system
An embedded system usually does not provide access to the OS and may not even provide a method of upgrading the system firmware.

The incorrect answers:
A. End-of-life
A device at its end-of-life is no longer supported by the vendor. In this example, the vendor support status isn't mentioned.

B. Weak configuration
A weak configuration would leave the system easily accessible by an attacker. In this example, the described scenario doesn't describe any weak configurations.

C. Improper input handling
Improper handling of user input can sometimes result in an exploit. In this example, no specific user input issues were described.

More information:
SY0-601, Objective 2.6 - Embedded Systems Constraints
https://professormesser.link/601020603

B71. Last month, a finance company disposed of seven-year-old printed customer account summaries that were no longer required for auditing purposes. A recent online search has now found that images of these documents are available as downloadable torrents. Which of the following would MOST likely have prevented this information breach?

❍ **A.** Pulping

❍ **B.** Degaussing

❍ **C.** NDA

❍ **D.** Fenced garbage disposal areas

The Answer: A. Pulping
Pulping places the papers into a large washing tank to remove the ink, and the paper is broken down into pulp and recycled. The information on the paper is not recoverable after pulping.

The incorrect answers:
B. Degaussing
Degaussing removes the electromagnetic field of storage media and electronics. Degaussing will not have any effect on paper items.

C. NDA
A non-disclosure agreement is only valid to the people who have signed the agreement. In this case, it can be assumed that the papers were obtained by a third-party after being placed in the trash.

D. Fenced garbage disposal areas
Although a fenced disposal area would have protected this information while it was on-site, the papers could have been obtained once they left the facility. The best choice for this question would be the option that would render the information on the pages unreadable.

More information:
SY0-601, Objective 2.7 - Secure Data Destruction
https://professormesser.link/601020703

B72. A security manager believes that an employee is using their laptop to circumvent the corporate Internet security controls through the use of a cellular hotspot. Which of the following could be used to validate this belief? (Select TWO)

❍ **A.** HIPS

❍ **B.** UTM appliance logs

❍ **C.** Web application firewall events

❍ **D.** Host-based firewall logs

❍ **E.** Next-generation firewall logs

The Answer: A. HIPS and **D.** Host-based firewall logs
If the laptop is not communicating across the corporate network, then the only evidence of the traffic would be contained on the laptop itself. A HIPS (Host-based Intrusion Prevention System) and host-based firewall logs may contain information about recent traffic flows to systems outside of the corporate network.

The incorrect answers:
B. UTM appliance logs
A unified threat management appliance is commonly located in the core of the network. The use of a cellular hotspot would circumvent the UTM and would not be logged.

C. Web application firewall events
Web application firewalls are commonly used to protect internal web servers. Outbound Internet communication would not be logged, and anyone circumventing the existing security controls would also not be logged.

E. Next-generation firewall logs
Although a next-generation firewall keeps detailed logs, any systems communicating outside of the normal corporate Internet connection would not appear in those logs.

More information:
SY0-601, Objective 3.2 - Endpoint Protection
https://professormesser.link/601030201

B73. An application developer is creating a mobile device app that will include extensive encryption and decryption. Which of the following technologies would be the BEST choice for this app?

❍ **A.** AES

❍ **B.** Elliptic curve

❍ **C.** Diffie-Hellman

❍ **D.** PGP

The Answer: B. Elliptic curve
ECC (Elliptic Curve Cryptography) uses smaller keys than non-ECC encryption and has smaller storage and transmission requirements. These characteristics make it an efficient option for mobile devices.

The incorrect answers:
A. AES
AES (Advanced Encryption Standard) is a useful encryption cipher, but the reduced overhead of elliptic curve cryptography is a better option for this scenario.

C. Diffie-Hellman
Diffie-Hellman is a key-agreement protocol, and Diffie-Hellman does not provide for any encryption or authentication.

D. PGP
PGP's public-key cryptography requires much more overhead than the elliptic curve cryptography option.

More information:
SY0-601, Objective 2.8
Symmetric and Asymmetric Cryptography
https://professormesser.link/601020802

B74. Which of the following would be a common result of a successful vulnerability scan?

○ **A.** A list of usernames and password hashes from a server

○ **B.** A list of Microsoft patches that have not been applied to a server

○ **C.** A copy of image files from a private file share

○ **D.** The BIOS configuration of a server

The Answer: B. A list of Microsoft patches that have not been applied to a server

A vulnerability scan will identify known vulnerabilities, but it will stop short of exploiting these vulnerabilities.

The incorrect answers:

A. A list of usernames and password hashes from a server
This type of secure information cannot be obtained through a vulnerability scan.

C. A copy of image files from a private file share
A private file share would prevent any access by unauthorized users, including vulnerability scans.

D. The BIOS configuration of a server
Private information, such as a device's BIOS configuration, is not available from a vulnerability scan.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

B75. A security administrator is researching an issue with conference room users at a remote site. When connected to the wireless network, users receive an IP address that is not part of the corporate addressing scheme. Communication over this network also appears to have slower performance than the wireless connections elsewhere in the building. Which of the following would be the MOST likely reason for these issues?

❍ **A.** Rogue access point

❍ **B.** Domain hijack

❍ **C.** DDoS

❍ **D.** MAC flooding

The Answer: A. Rogue access point
A rogue access point is an unauthorized access point added by a user or attacker. This access point may not necessarily be malicious, but it does create significant security concerns and unauthorized access to the corporate network.

The incorrect answers:

B. Domain hijack
A domain hijacking would be associated with unauthorized access to a domain name. In this example, the wireless IP addressing and performance issues do not appear to be related to a domain hijack.

C. DDoS
A DDOS (Distributed Denial of Service) would cause outages or slow performance to a service. A DDoS would not commonly modify or update any local IP addresses.

D. MAC flooding
MAC (Media Access Control) flooding can certainly create performance issues, but the unmatching IP address scheme on the wireless network does not appear to be related to a MAC flood.

More information:
SY0-601, Objective 1.4 - Rogue Access Points and Evil Twins
https://professormesser.link/601010401

B76. A company has identified a compromised server, and the security team would like to know if an attacker has used this device to move between systems. Which of the following would be the BEST way to provide this information?

❍ **A.** DNS server logs

❍ **B.** Penetration test

❍ **C.** NetFlow logs

❍ **D.** Email header

The Answer: C. NetFlow logs
NetFlow information can provide a summary of network traffic, application usage, and details of network conversations. The NetFlow logs will show all conversations from this device to any others in the network.

The incorrect answers:
A. DNS server logs
DNS server logs will document all name resolutions, but an attacker may not use a DNS server and may prefer accessing devices by IP address.

B. Penetration test
A penetration test may identify any vulnerabilities that exist on the server, but it won't provide any information about traffic flows or connections initiated by an attacker.

D. Email header
An email header usually contains information of email servers used to transfer the message and security signatures to verify the sender. An email header would not contain information on traffic flows associated with this attacker.

More information:
SY0-601, Objective 4.3 - Log Management
https://professormesser.link/601040304

B77. A system administrator has protected a set of system backups with an encryption key. The system administrator used the same key when restoring files from this backup. Which of the following would BEST describe this encryption type?

❍ **A.** Asymmetric

❍ **B.** Key escrow

❍ **C.** Symmetric

❍ **D.** Out-of-band key exchange

The Answer: C. Symmetric
Symmetric encryption uses the same key for both encryption and decryption.

The incorrect answers:
A. Asymmetric
Asymmetric encryption uses different keys for encryption and decryption.

B. Key escrow
Key escrow is when a third-party holds the decryption keys for your data.

D. Out-of-band key exchange
Keys can be transferred between people or systems over the network (in-band) or outside the normal network communication (out-of-band). In this example, the key wasn't exchanged between people or systems, since the system administrator is the same person who encrypted and decrypted.

More information:
SY0-601, Objective 2.8 -
Symmetric and Asymmetric Cryptography
https://professormesser.link/601020802

B78. A new malware variant takes advantage of a vulnerability in a popular email client. Once installed, the malware forwards all email attachments containing credit card information to an external email address. Which of the following would limit the scope of this attack?

❍ **A.** Enable MFA on the email client

❍ **B.** Scan outgoing traffic with DLP

❍ **C.** Require users to enable the VPN when using email

❍ **D.** Update the list of malicious URLs in the firewall

The Answer: B. Scan outgoing traffic with DLP
DLP (Data Loss Prevention) systems are designed to identify sensitive data transfers. If the DLP finds a data transfer with financial details, personal information, or other private information, the DLP can block the data transfer.

The incorrect answers:
A. Enable MFA on the email client
MFA (Multi-Factor Authentication) can provide more security during the authentication process, but the description of the malware did not associate the exploit with the login process. The malware will most likely wait for the user to login before exfiltrating the data.

C. Require users to enable the VPN when using email
A VPN (Virtual Private Network) can protect data between systems, but it won't prevent malware from sending data once it connects to the email system.

D. Update the list of malicious URLs in the firewall
Blocking known URLs (Uniform Resource Locators) in a firewall is a useful way to prevent access to known malicious sites, but it won't prevent malware from sending email messages.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

B79. An organization has identified a security breach and has removed the affected servers from the network. Which of the following is the NEXT step in the IR process?

❍ **A.** Eradication

❍ **B.** Preparation

❍ **C.** Recovery

❍ **D.** Identification

❍ **E.** Containment

The Answer: A. Eradication
The IR (Incident Response) process is preparation, identification, containment, eradication, recovery, and lessons learned. Once a system has been contained, any malware or breached user accounts should be removed from the system.

The incorrect answers:
B. Preparation
Before an incident occurs, you should compile contact information, incident handling hardware and software, analysis resources, and other important tools and policies.

C. Recovery
The focus of the recovery process is to get all of the systems back to normal. This phase removes malware, deletes breached user accounts, and fixes any vulnerabilities.

D. Identification
Identification of an event can be challenging, but it usually consists of IPS reports, anti-virus alerts, configuration change notifications, and other indicators.

E. Containment
In this example, the containment and isolation occurred when the affected servers were removed from the network.

More information:
SY0-601, Objective 4.2 - Incident Response Process
https://professormesser.link/601040201

B80. A manager of the accounting department would like to minimize the opportunity for embezzlement and fraud from any of the current accounting team employees. Which of these policies should the manager use to avoid these issues?

❍ **A.** Background checks

❍ **B.** Clean desk policy

❍ **C.** Mandatory vacations

❍ **D.** Acceptable use policy

The Answer: C. Mandatory vacations
It's difficult to maintain fraudulent activities if the person executing the fraud is out of the office. In financial environments, it's not uncommon to require at least a week of consecutive vacation time at some point during the year.

The incorrect answers:
A. Background checks
Background checks are useful to discover information prior to hiring someone, but these checks are not commonly performed after someone is an employee.

B. Clean desk policy
If confidential information was left available on someone's desk, then it would be appropriate to institute a clean desk policy. In this example, the fraudulent activity did not include any mention of confidential information on a desk.

D. Acceptable use policy
The acceptable use policy (AUP) of an organization describes how company assets are to be used, especially computers, Internet connections, and mobile devices.

More information:
SY0-601, Objective 5.3 - Personnel Security
https://professormesser.link/601050301

B81. Which of the following would be the MAIN reasons why a system administrator would use a TPM when configuring full disk encryption? (Select TWO)

❍ **A.** Allows the encryption of multiple volumes

❍ **B.** Uses burned-in cryptographic keys

❍ **C.** Stores certificates in a hardware security module

❍ **D.** Protects against EMI leakage

❍ **E.** Includes built-in protections against brute-force attacks

The Answer: B. Uses burned-in cryptographic keys and
E. Includes built-in protections against brute-force attacks

A TPM (Trusted Platform Module) is hardware that is part of a computer's motherboard, and it's specifically designed to assist and protect with cryptographic functions. Full disk encryption (FDE) can use the burned-in TPM keys to verify that the local device hasn't changed, and there are security features in the TPM that will prevent brute-force or dictionary attacks against the full disk encryption login credentials.

The incorrect answers:

A. Allows the encryption of multiple volumes
The use of a TPM is not associated with the number of volumes that may be encrypted with FDE.

C. Stores certificates in a hardware security module
A hardware security module (HSM) is high-end cryptographic hardware specifically designed for large-scale secured storage on the network. An HSM server is a separate device that is not associated with an individual device's TPM.

D. Protects against EMI leakage
The leakage of EMI (Electromagnetic Interference) from keyboards, storage drives, or network connections can be a security concern, but it is not related to the use of a trusted platform module.

More information:
SY0-601, Objective 3.2 - Boot Integrity
https://professormesser.link/601030202

B82. A security administrator would like to create an access control where each file or folder is assigned a security clearance level, such as "confidential" or "secret." The security administrator would then assign a maximum security level to each user. What type of access control would be used in this network?

❍ **A.** Mandatory

❍ **B.** Rule-based

❍ **C.** Discretionary

❍ **D.** Role-based

The Answer: A. Mandatory
Mandatory access control uses a series of security levels (i.e., public, private, secret) and assigns those levels to each object in the operating system. Users are assigned a security level, and they would only have access to objects that meet or are below that assigned security level.

The incorrect answers:
B. Rule-based
Rule-based access control determines access based on a series of system-enforced rules. An access rule might require that a particular browser be used to complete a web page form, or that access to a file or system is only allowed during certain times of the day.

C. Discretionary
Discretionary access control allows the owner of an object to assign access. If a user creates a spreadsheet, the user can then assign users and groups to have a particular level of access to that spreadsheet.

D. Role-based
Role-based access control assigns a user's permissions based on their role in the organization. For example, a manager would have a different set of rights and permissions than a team lead.

More information:
SY0-601, Objective 3.8 - Access Control
https://professormesser.link/601030805

B83. Cameron, a security administrator, is reviewing a report that shows a number of devices on internal networks attempting to connect with servers in the data center network. Which of the following security controls should Cameron add to prevent internal systems from accessing data center devices?

❍ **A.** VPN

❍ **B.** IPS

❍ **C.** NAT

❍ **D.** ACL

The Answer: D. ACL
An ACL (Access Control List) is a security control commonly implemented on routers to allow or restrict traffic flows through the network.

The incorrect answers:
A. VPN
A VPN (Virtual Private Network) can be used to secure data traversing the network, but it's not commonly used to control traffic flows on an internal network.

B. IPS
An IPS (Intrusion Prevention System) is designed to identify and block known vulnerabilities traversing the network. An IPS is not used to control other traffic flows.

C. NAT
NAT (Network Address Translation) is a method of modifying the source and/or destination IP addresses of network traffic. NAT is not a security control.

More information:
SY0-601, Objective 3.3 - Firewalls
https://professormesser.link/601030306

B84. A financial services company is headquartered in an area with a high occurrence of tropical storms and hurricanes. Which of the following would be MOST important when restoring services disabled by a storm?

❍ **A.** Disaster recovery plan

❍ **B.** Stakeholder management

❍ **C.** Communication plan

❍ **D.** Retention policies

The Answer: A. Disaster recovery plan

A disaster recovery plan is a comprehensive set of processes to follow for large-scale outages that affect the organization. Natural disasters, technology failures, and human-created disasters would be reasons to implement a disaster recovery plan.

The incorrect answers:

B. Stakeholder management

Stakeholder management describes the relationship that IT has with the their customers. Although stakeholder management is an important ongoing process, the priority after a major event is to start the disaster recovery process.

C. Communication plan

A communication plan is a list of everyone who needs to be contacted during an incident. The communication plan will be important documentation after a disaster recovery process has started.

D. Retention policies

Retention policies are specify the type and amount of data that must be backed up and stored. These policies are often self-imposed or part of a larger set of rules and regulations.

More information:

SY0-601, Objective 4.2 - Incident Response Planning

https://professormesser.link/601040202

B85. A user in the mail room has reported an overall slowdown of his shipping management software. An anti-virus scan did not identify any issues, but a more thorough malware scan identified a kernel driver that was not part of the original operating system installation. Which of the following malware was installed on this system?

❍ **A.** Rootkit

❍ **B.** RAT

❍ **C.** Bot

❍ **D.** Ransomware

❍ **E.** Keylogger

The Answer: A. Rootkit
A rootkit traditionally modifies core system files and becomes effectively invisible to the rest of the operating system. The modification of system files and specialized kernel-level drivers are common rootkit techniques.

The incorrect answers:

B. RAT
A RAT (Remote Administration Tool) is often installed as a Trojan horse and used for malicious purposes. Although these utilities are sometimes installed subversively, they can still be identified through normal malware scans and host-based firewall software.

C. Bot
A bot is relatively active malware that can usually be seen in a process list and by examining network communication. Botnet participants can often be identified using traditional anti-malware software.

D. Ransomware
Ransomware makes itself quite visible on your system, and it usually presents warning messages and information on how to remove the ransomware from the system.

E. Keylogger
A keylogger is a utility that captures keyboard and mouse input and sends that information to another device. This usually means that the keylogger has a visible component in the list of processes and traffic that can be seen on the network.

More information:
SY0-601, Objective 1.2 - Rootkits
https://professormesser.link/601010205

B86. A virus scanner has identified a macro virus in a word processing file attached to an email. Which of the following information could be obtained from the metadata of this file?

❍ **A.** IPS signature name and number

❍ **B.** Operating system version

❍ **C.** Date and time when the file was created

❍ **D.** Alert disposition

The Answer: C. Date and time when the file was created
The data and time the file was created is commonly found in the metadata of a file.

The incorrect answers:
A. IPS signature name and number
The metadata is stored in the word processing file, and the IPS will not change the information stored in the file.

B. Operating system version
Word processing files are not specific to an operating system, so it would not be common to find OS information stored in the metadata of a word processing file.

D. Alert disposition
The alert information created when the macro virus was discovered would not be included as part of the word processing file metadata.

More information:
SY0-601, Objective 4.3 - Log Management
https://professormesser.link/601040304

B87. If a person is entering a data center facility, they must check-in before they are allowed to move further into the building. People who are leaving must be formally checked-out before they are able to exit the building. Which of the following would BEST facilitate this process?

❍ **A.** Access control vestibule

❍ **B.** Air gap

❍ **C.** Faraday cage

❍ **D.** Protected distribution

The Answer: A. Access control vestibule
An access control vestibule is commonly used to control the flow of people through a particular area. Unlocking the one door of the vestibule commonly restricts the other door from opening, thereby preventing someone from walking through without stopping. It's common in large data centers to have a single room as the access control vestibule where users are checked in and out of the facility.

The incorrect answers:

B. Air gap
An air gap is a technical control that creates a physical separation between devices or networks. An air gap is not used to manage the flow of people.

C. Faraday cage
A Faraday cage is used to block electromagnetic fields, and it is useful in environments where electromagnetic and radio signals can be an issue.

D. Protected distribution
A protected distribution system (PDS) is a physically secure cabled network. Cable and fiber in a protected distribution are protected from taps, cuts, or similar security breaches.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

B88. A security administrator has discovered that an employee has been exfiltrating confidential company information by embedding the data within image files and emailing the images to a third-party. Which of the following would best describe this activity?

❍ **A.** Digital signatures

❍ **B.** Steganography

❍ **C.** Block cipher

❍ **D.** Perfect forward secrecy

The Answer: B. Steganography
Steganography is the process of hiding information within another document. For example, one common method of steganography will embed data or documents within image files.

The incorrect answers:
A. Digital signatures
A digital signature is a cryptographic method to check the integrity, authentication, and non-repudiation of a message. Digital signatures are not used to hide information within image files.

C. Block cipher
A block cipher is used to encrypt fixed-length groups of data. Block ciphers do not hide data within another object.

D. Perfect forward secrecy
Perfect forward secrecy is a key exchange method that creates a new and unique set of session keys for each session.

More information:
SY0-601, Objective 2.8 - Steganography
https://professormesser.link/601020805

B89. A security engineer is running a vulnerability scan on their own workstation. The scanning software is using the engineers account access to perform all scans. What type of scan is running?

❍ **A.** Unknown environment

❍ **B.** Passive

❍ **C.** Credentialed

❍ **D.** Agile

The Answer: C. Credentialed
A credentialed scan uses valid access rights to perform the scanning functions. This type of scan is designed to show what someone on the inside with these rights would be able to exploit.

The incorrect answers:
A. Black box
Black box information is generally associated with penetration testing. Someone performing a black box penetration test will not have any prior knowledge of the systems under attack.

B. Passive
Passive information gathering is usually associated with penetration testing. Passive reconnaissance is the process of gathering information from outside sources, such as social media sites and online forums.

D. Agile
An agile environment is often associated with a development life-cycle model that focuses on rapid development and constant collaboration.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

B90. Which of the following would be the best way to describe the estimated number of laptops that might be stolen in a fiscal year?

❍ **A.** ALE

❍ **B.** SLE

❍ **C.** ARO

❍ **D.** MTTR

The Answer: C. ARO
The ARO (Annualized Rate of Occurrence) describes the number of instances that an event would occur in a year. For example, if the organization expect to lose seven laptops to theft in a year, the ARO for laptop theft is seven.

The incorrect answers:
A. ALE
The ALE (Annual Loss Expectancy) is the expected cost for all events in a single year. If it costs $1,000 to replace a single laptop (the SLE) and you expect to lose seven laptops in a year (the ARO), the ALE for laptop theft is $7,000.

B. SLE
SLE (Single Loss Expectancy) is the monetary loss if a single event occurs. If one laptop is stolen, the cost to replace that single laptop is the SLE,
or $1,000.

D. MTTR
MTTR (Mean Time to Repair) is the time required to repair a product or system after a failure.

More information:
SY0-601, Objective 5.4 - Risk Analysis
https://professormesser.link/601050402

Practice Exam C

Performance-Based Questions

C1. Refer to the following firewall ruleset:

Rule #	Source IP	Destination IP	Protocol (TCP/ UDP)	Port #	Allow/ Block
1	Any	10.1.10.88	TCP	22	Allow
2	Any	10.1.10.120	TCP	80	Allow
3	Any	10.1.10.120	TCP	443	Allow
4	Any	10.1.10.61	TCP	3389	Allow
5	Any	Any	UDP	53	Allow
6	Any	Any	UDP	123	Allow
7	Any	Any	ICMP		Block

Categorize the following traffic flows as ALLOWED or BLOCKED through the firewall:

__________ Use a secure terminal to connect to 10.1.10.88

__________ Share the desktop on server 10.1.10.120

__________ Perform a DNS query from 10.1.10.88 to 9.9.9.9

__________ View web pages on 10.1.10.120

__________ Authenticate to an LDAP server at 10.1.10.61

__________ Synchronize the clock on a server at 10.1.10.17

Answer Page: **293**

C2. Match the device to the description. Some device types will not be used.

WAF	Proxy	Load balancer	Access point
MDM	Router	VPN concentrator	IPS

	Block SQL injection over an Internet connection
	Intercept all browser requests and cache the results
	Forward packets between separate VLANs
	Configure a group of redundant web servers
	Evaluate the input to a browser-based application

Answer Page: **295**

C3. Match the characteristic to the attack type:

Phishing	Dictionary	Spoofing
Rootkit	Tailgating	DoS

	A website stops responding to normal requests
	IP addresses are cloned to gain access without authenticating
	The malware is designed to remain hidden on a computer system
	A list of common passwords are attempted with a known username
	An email link redirects a user to a site that requests login credentials
	A person gains unauthorized access to a secure storage room

Answer Page: **296**

C4. Match the technology to the description:

PFS　Collision　Obfuscation

Asymmetric　Confusion　Diffusion

	One character changes, and the resulting hash is very different
	The encrypted data is drastically different than the plaintext
	Different inputs create the same hash
	The process of making something unclear
	A different key is used for decryption than encryption
	Use a different encryption key for every session

Answer Page: **297**

C5. Match the PKI component to the description:

CRL　CA

OCSP　RA　CSR

	Verifies the entity requesting the certificate
	A list of invalidated certificates
	Send the public key to the CA to be signed
	Deploy and manage certificates
	The browser checks for certificate revocation

Answer Page: **298**

Practice Exam C
Multiple Choice Questions

C6. A finance company is legally required to maintain seven years of tax records for all of their customers. Which of the following would be the BEST way to implement this requirement?

❍ **A.** Create an automated script to remove all tax information more than seven years old

❍ **B.** Print and store all tax records in a seven-year cycle

❍ **C.** Allow users to download tax records from their account login

❍ **D.** Create a separate daily backup archive for all applicable tax records

Quick Answer: **291**

The Details: **299**

C7. A system administrator is designing a data center for an insurance company's new public cloud and would like to restrict user access to sensitive data. Which of the following would provide ongoing visibility, data security, and control of cloud-based applications?

❍ **A.** HSM

❍ **B.** CASB

❍ **C.** 802.1X

❍ **D.** EDR

Quick Answer: **291**

The Details: **300**

C8. A device is exhibiting intermittent connectivity when viewing remote web sites. A security administrator views the local device ARP table:

```
Internet Address      Physical Address
192.168.1.1           60:3d:26:69:71:fc
192.168.1.101         e2:c3:53:79:4c:51
192.168.1.102         7a:3b:8f:21:86:57
192.168.1.103         60:3d:26:69:71:fc
192.168.1.104         00:80:92:c7:c8:49
192.168.1.105         d0:81:7a:d3:f0:d5
```

Which of the following would be the MOST likely explanation of this connectivity issue?

❍ **A.** DDoS

❍ **B.** Wireless disassociation

❍ **C.** Rogue access point

❍ **D.** ARP poisoning

Quick Answer: **291**

The Details: **301**

C9. A security administrator has identified an internally developed application that allows users to modify SQL queries through a web-based front-end. To prevent this modification, the administrator has recommended that all queries be completely removed from the application front-end and placed onto the back-end of the application server. Which of the following would describe this implementation?

❍ **A.** Input validation

❍ **B.** Code signing

❍ **C.** Stored procedures

❍ **D.** Obfuscation

Quick Answer: **291**

The Details: **302**

C10. A system administrator is implementing a fingerprint scanner to provide access to the data center. Which of these metrics should be kept at a minimum in order to prevent unauthorized persons from accessing the data center?

❍ **A.** TOTP

❍ **B.** FRR

❍ **C.** HOTP

❍ **D.** FAR

Quick Answer: **291**

The Details: **303**

C11. The IT department of a transportation company maintains an on-site inventory of chassis-based network switch interface cards. If a failure occurs, the on-site technician can replace the interface card and have the system running again in sixty minutes. Which of the following BEST describes this recovery metric?

❍ **A.** MTBF

❍ **B.** MTTR

❍ **C.** RPO

❍ **D.** RTO

Quick Answer: **291**

The Details: **304**

C12. A company maintains a server farm in a large data center. These servers are for internal use only and are not accessible externally. The security team has discovered that a group of servers was breached before the latest updates were applied. Breach attempts were not logged on any other servers. Which of these threat actors would be MOST likely involved in this breach?

❍ **A.** Competitor

❍ **B.** Insider

❍ **C.** Nation state

❍ **D.** Script kiddie

Quick Answer: **291**

The Details: **305**

C13. An organization has contracted with a third-party to perform a vulnerability scan of their Internet-facing web servers. The report shows that the web servers have multiple Sun Java Runtime Environment (JRE) vulnerabilities, but the server administrator has verified that JRE is not installed. Which of the following would be the BEST way to handle this report?

❍ **A.** Install the latest version of JRE on the server

❍ **B.** Quarantine the server and scan for malware

❍ **C.** Harden the operating system of the web server

❍ **D.** Ignore the JRE vulnerability alert

Quick Answer: **291**

The Details: **306**

C14. A user downloaded and installed a utility for compressing and decompressing files. Immediately after installing the utility, the user's overall workstation performance degraded, and it now takes twice as much time to perform any tasks on the computer. Which of the following is the BEST description of this malware infection?

❍ **A.** Ransomware

❍ **B.** Adware

❍ **C.** Logic bomb

❍ **D.** Trojan

Quick Answer: **291**

The Details: **307**

C15. Which of the following is the process for replacing sensitive data with a non-sensitive and functional placeholder?

❍ **A.** Minimization

❍ **B.** Tokenization

❍ **C.** Retention

❍ **D.** Masking

Quick Answer: **291**

The Details: **308**

C16. A security administrator has installed a new firewall to protect a web server VLAN. The application owner requires that all web server sessions communicate over an encrypted channel. Which of these rules should the security administrator include in the firewall rulebase? (Select TWO)

❍ **A.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 23, Deny`

❍ **B.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Deny`

❍ **C.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Deny`

❍ **D.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Allow`

❍ **E.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Allow`

Quick Answer: **291**

The Details: **309**

C17. Which of these would be used to provide multi-factor authentication?

❍ **A.** USB-connected storage drive with FDE

❍ **B.** Employee policy manual

❍ **C.** Null-modem serial cable

❍ **D.** Smart card with picture ID

Quick Answer: **291**

The Details: **310**

C18. An IT manager is leading a project to implement a global standard for a privacy information management system. Which of these standards would BEST apply to this project?

❍ **A.** ISO 27701

❍ **B.** PCI DSS

❍ **C.** SSAE SOC 2

❍ **D.** CSA CCM

Quick Answer: **291**

The Details: **311**

C19. A company's security cameras have identified an unknown person walking into a fenced disposal area in the back of the building and then leaving with a box containing printed documents. Which of the following attacks is this person attempting?

❍ **A.** Dumpster diving

❍ **B.** Shoulder surfing

❍ **C.** Tailgating

❍ **D.** Phishing

Quick Answer: **291**

The Details: **312**

C20. A technology company is manufacturing a military-grade radar tracking system that can instantly identify any nearby unmanned aerial vehicles (UAVs). The UAV detector must be able to instantly identify and react to a vehicle without delay. Which of the following would BEST describe this tracking system?

❍ **A.** RTOS

❍ **B.** IoT

❍ **C.** ICS

❍ **D.** MFD

Quick Answer: **291**

The Details: **313**

C21. A private company uses an SSL proxy to examine the contents of an encrypted application during transmission. How could the application developers prevent the use of this proxy examination in the future?

❍ **A.** OCSP stapling

❍ **B.** Offline CAs

❍ **C.** Certificate chaining

❍ **D.** Certificate pinning

Quick Answer: **291**

The Details: **314**

C22. A security administrator is concerned that a user may have installed a rogue access point on the corporate network. Which of the following could be used to confirm this suspicion?

❍ **A.** UTM log

❍ **B.** WAF log

❍ **C.** Switch log

❍ **D.** DLP log

Quick Answer: **291**

The Details: **315**

C23. During a ransomware outbreak, an organization was forced to rebuild database servers from known good backup systems. In which of the following incident response phases were these database servers brought back online?

❍ **A.** Recovery

❍ **B.** Lessons learned

❍ **C.** Containment

❍ **D.** Identification

Quick Answer: **291**

The Details: **316**

C24. Which of the following cloud deployments would include CPU, storage, and networking, but not include any operating system or application?

❍ **A.** SaaS

❍ **B.** DaaS

❍ **C.** IaaS

❍ **D.** PaaS

Quick Answer: **291**

The Details: **317**

C25. A network IPS has created this log entry:

```
Frame 4: 937 bytes on wire (7496 bits),
    937 bytes captured

Ethernet II, Src: HewlettP_82:d8:31,
     Dst: Cisco_a1:b0:d1

Internet Protocol Version 4, Src: 172.16.22.7,
     Dst: 10.8.122.244

Transmission Control Protocol, Src Port: 3863,
     Dst Port: 1433

Application Data: SELECT * FROM users WHERE
     username='x' or 'x'='x' AND
     password='x' or 'x'='x'
```

Which of the following would describe this log entry?

○ **A.** Phishing

○ **B.** Brute force

○ **C.** SQL injection

○ **D.** Cross-site scripting

Quick Answer: **291**

The Details: **318**

C26. An incident response team would like to validate their disaster recovery plans without making any changes to the infrastructure. Which of the following would be the best course of action?

○ **A.** Tabletop exercise

○ **B.** Hot site fail-over

○ **C.** Simulation

○ **D.** Penetration test

Quick Answer: **291**

The Details: **319**

C27. A system administrator has installed a new firewall between the corporate user network and the data center network. When the firewall is turned on with the default settings, users complain that the application in the data center is no longer working. Which of the following would be the BEST way to correct this application issue?

○ **A.** Create a single firewall rule with an explicit deny

○ **B.** Build a separate VLAN for the application

○ **C.** Create firewall rules that match the application traffic flow

○ **D.** Disable spanning tree protocol

Quick Answer: **291**

The Details: **320**

C28. Which of these would be used to provide HA for a web-based database application?

❍ **A.** SIEM

❍ **B.** UPS

❍ **C.** DLP

❍ **D.** VPN concentrator

Quick Answer: **291**

The Details: **321**

C29. Each year, a certain number of laptops are lost or stolen and must be replaced by the company. Which of the following would describe the total cost the company spends each year on laptop replacements?

❍ **A.** SLE

❍ **B.** SLA

❍ **C.** ALE

❍ **D.** ARO

Quick Answer: **291**

The Details: **322**

C30. A network administrator is viewing a log file from a web server:

```
https://www.example.com/?s=/Index/think/
app/invokefunction&function=call_user_
func_array&vars[0]=md5&vars[1][0]=
__HelloThinkPHP
```

Which of the following would be the BEST way to prevent this attack?

❍ **A.** Static code analyzer

❍ **B.** Input validation

❍ **C.** Allow list

❍ **D.** Secure cookies

Quick Answer: **291**

The Details: **323**

C31. Sam, a user in the purchasing department, would like to send an email to Jack. Which of these would allow Jack to verify the sender of the email?

❍ **A.** Digitally sign it with Sam's private key

❍ **B.** Digitally sign it with Sam's public key

❍ **C.** Digitally sign it with Jack's private key

❍ **D.** Digitally sign it with Jack's public key

Quick Answer: **291**

The Details: **324**

C32. The contract of a long-term temporary employee is ending. Which of these would be the MOST important part of the off-boarding process?

❍ **A.** Perform an on-demand audit of the user's privileges

❍ **B.** Archive the decryption keys associated with the user account

❍ **C.** Document the user's outstanding tasks

❍ **D.** Obtain a signed copy of the Acceptable Use Policies

Quick Answer: **291**

The Details: **325**

C33. Daniel, a cybersecurity analyst, has been asked to respond to a denial of service attack against a web server. Daniel first collects information in the ARP cache, then a copy of the server's temporary file system, and finally system logs from the web server. What part of the forensics gathering process did Daniel follow?

❍ **A.** Chain of custody

❍ **B.** Data hashing

❍ **C.** Legal hold

❍ **D.** Order of volatility

Quick Answer: **291**

The Details: **326**

C34. An attacker was able to download ten thousand company employee login credentials containing usernames and hashed passwords. Less than an hour later, a list containing all ten thousand usernames and passwords in plain text were posted to an online file storage repository. Which of the following would BEST describe how this attacker was able to post this information?

❍ **A.** Improper certificate management

❍ **B.** Phishing

❍ **C.** Untrained users

❍ **D.** Weak cipher suite

Quick Answer: **291**

The Details: **327**

C35. A security administrator is researching the methods used by attackers to gain access to web servers. Which of the following would provide additional information about these techniques?

❍ **A.** IPS

❍ **B.** Hashing

❍ **C.** Obfuscation

❍ **D.** Honeypot

Quick Answer: **291**

The Details: **328**

C36. A server administrator is building a new web server and needs to provide operating system access to the web server executable. Which of the following account types should be configured?

❍ **A.** User

❍ **B.** Privileged

❍ **C.** Service

❍ **D.** Guest

Quick Answer: **291**

The Details: **329**

C37. A company is implementing a series of automated processes when responding to a security event. Which of the following would provide a linear checklist of steps to perform?

❍ **A.** MDM

❍ **B.** DLP

❍ **C.** Runbook

❍ **D.** Zero trust

Quick Answer: **291**

The Details: **330**

C38. A transportation company maintains a scheduling application and a database in a virtualized cloud-based environment. Which of the following would be the BEST way to backup these services?

❍ **A.** Full

❍ **B.** Snapshot

❍ **C.** Differential

❍ **D.** Incremental

Quick Answer: **291**

The Details: **331**

C39. In an environment using discretionary access controls, which of these would control the rights and permissions associated with a file or directory?

❍ **A.** Administrator

❍ **B.** Owner

❍ **C.** Group

❍ **D.** System

Quick Answer: **291**

The Details: **332**

C40. A security administrator has installed a network-based DLP solution to determine if file transfers contain PII. Which of the following describes the data during the file transfer?

❍ **A.** In-use

❍ **B.** In-transit

❍ **C.** At-rest

❍ **D.** Highly available

Quick Answer: **291**

The Details: **333**

C41. A medical imaging company would like to connect all remote locations together with high speed network links. The network connections must maintain high throughput rates and must always be available during working hours. In which of the following should these requirements be enforced with the network provider?

❍ **A.** Service level agreement

❍ **B.** Memorandum of understanding

❍ **C.** Non-disclosure agreement

❍ **D.** Acceptable use policy

Quick Answer: **291**

The Details: **334**

C42. A security administrator would like to encrypt all telephone communication on the corporate network. Which of the following protocols would provide this functionality?

❍ **A.** TLS

❍ **B.** SRTP

❍ **C.** SSH

❍ **D.** S/MIME

Quick Answer: **291**

The Details: **335**

C43. A security administrator is preparing a phishing email that will be sent to employees as part of a periodic security test. The email is spoofed to appear as an unknown third-party and asks employees to immediately click a link or their state licensing will be revoked. Which of these social engineering principles are used by this email?

❍ **A.** Familiarity

❍ **B.** Social Proof

❍ **C.** Authority

❍ **D.** Urgency

Quick Answer: **291**

The Details: **336**

C44. A security administrator would like to minimize the number of certificate status checks made by web site clients to the certificate authority. Which of the following would be the BEST option for this requirement?

❍ **A.** OCSP stapling

❍ **B.** Certificate chaining

❍ **C.** CRL

❍ **D.** Certificate pinning

Quick Answer: **291**

The Details: **337**

C45. A company is concerned their EDR solution will not be able to stop more advanced ransomware variants. Technicians have created a backup and restore utility that will get most systems up and running less than an hour after an attack. What type of security control is associated with this restore process?

❍ **A.** Managerial

❍ **B.** Compensating

❍ **C.** Preventive

❍ **D.** Detective

Quick Answer: **291**

The Details: **338**

C46. To upgrade an internal application, the development team provides the operations team with a patch and instructions for backing up, patching, and reverting the patch if needed. The operations team schedules a date for the upgrade, informs the business divisions, and tests the upgrade process after completion. Which of the following describes this process?

❍ **A.** Agile

❍ **B.** Continuity planning

❍ **C.** Usage auditing

❍ **D.** Change management

Quick Answer: **291**

The Details: **339**

C47. A company is implementing a public file-storage and cloud-based sharing service, but does not want to build a separate authentication front-end. Instead, the company would like users to authenticate with an existing account on a trusted third-party web site. Which of the following should the company implement?

❍ **A.** SSO

❍ **B.** Federation

❍ **C.** Transitive trust

❍ **D.** X.509 certificates signed by a trusted CA

Quick Answer: **291**

The Details: **340**

C48. A system administrator is viewing this output from Microsoft's System File Checker:

```
15:43:01 - Repairing corrupted file C:\Windows\System32\kernel32.dll
15:43:03 - Repairing corrupted file C:\Windows\System32\netapi32.dll
15:43:07 - Repairing corrupted file C:\Windows\System32\user32.dll
15:43:43 - Repair complete
```

Which of the following malware types is the MOST likely cause of this output?

❍ **A.** RAT

❍ **B.** Logic bomb

❍ **C.** Rootkit

❍ **D.** Bot

Quick Answer: **291**

The Details: **341**

C49. What type of vulnerability would be associated with this log information?

```
GET http://example.com/show.asp?view=../../Windows/
     system.ini HTTP/1.1
```

❍ **A.** Buffer overflow

❍ **B.** Directory traversal

❍ **C.** DoS

❍ **D.** Cross-site scripting

Quick Answer: **291**

The Details: **342**

C50. A developer has created an application that will store password information in a database. Which of the following BEST describes a way of protecting these credentials by adding random data to the password?

❍ **A.** Hashing

❍ **B.** PFS

❍ **C.** Salting

❍ **D.** Asymmetric encryption

Quick Answer: **291**

The Details: **343**

C51. Which of the following processes merges developed code, tests for issues, and automatically moves the newly developed application to production without any human intervention?

❍ **A.** Continuous deployment

❍ **B.** Continuity of operations

❍ **C.** Continuous delivery

❍ **D.** Continuous integration

Quick Answer: **291**

The Details: **344**

C52. Which of the following BEST describes a risk matrix?

❍ **A.** A visual summary of a risk assessment

❍ **B.** Identification of risk at each step of a project plan

❍ **C.** A list of cybersecurity requirements based on the identified risks

❍ **D.** Ongoing group discussions regarding cybersecurity

Quick Answer: **291**

The Details: **345**

C53. A security administrator would like to implement an authentication system that uses cryptographic tickets to validate users. Which of the following would provide this functionality?

❍ **A.** RADIUS

❍ **B.** LDAP

❍ **C.** Kerberos

❍ **D.** TACACS

Quick Answer: **291**

The Details: **346**

C54. Richard is reviewing this information from an IPS log:

```
MAIN_IPS: 22June2019 09:02:50 reject 10.1.111.7
Alert: HTTP Suspicious Webdav OPTIONS Method Request; Host: Server
Severity: medium; Performance Impact:3;
Category: info-leak; Packet capture; disable
Proto:tcp; dst:192.168.11.1; src:10.1.111.7
```

Which of the following can be associated with this log information? (Select TWO)

❍ **A.** The attacker sent a non-authenticated BGP packet to trigger the IPS

❍ **B.** The source of the attack is 192.168.11.1

❍ **C.** The event was logged but no packets were dropped

❍ **D.** The source of the attack is 10.1.111.7

❍ **E.** The attacker sent an unusual HTTP packet to trigger the IPS

Quick Answer: **291**

The Details: **347**

C55. A company has contracted with a third-party to provide penetration testing services. The service includes a port scan of each externally-facing device. This is an example of:

❍ **A.** Initial exploitation

❍ **B.** Escalation of privilege

❍ **C.** Pivot

❍ **D.** Active reconnaissance

Quick Answer: **291**

The Details: **348**

C56. An access point in a corporate headquarters office has the following configuration:

```
IP address: 10.1.10.1
Subnet mask: 255.255.255.0
DHCPv4 Server: Enabled
SSID: Wireless
Wireless Mode: 802.11g
Security Mode: WEP-PSK
Frequency band: 2.4 GHz
Software revision: 2.1
MAC Address: 60:3D:26:71:FF:AA
IPv4 Firewall: Enabled
```

Which of the following would apply to this configuration?

❍ **A.** Invalid frequency band

❍ **B.** Weak encryption

❍ **C.** Incorrect IP address and subnet mask

❍ **D.** Invalid software version

Quick Answer: **291**

The Details: **349**

C57. An application does not properly release unused memory, and eventually it grows so large that it uses all available memory. Which of the following would describe this issue?

❍ **A.** Integer overflow

❍ **B.** NULL pointer dereference

❍ **C.** Memory leak

❍ **D.** Data injection

Quick Answer: **291**

The Details: **350**

C58. A company is receiving complaints of slowness and disconnections to their Internet-facing web server. A network administrator monitors the Internet link and finds excessive bandwidth utilization from thousands of different IP addresses. Which of the following would be the MOST likely reason for these performance issues?

❍ **A.** DDoS

❍ **B.** Wireless jamming

❍ **C.** MAC cloning

❍ **D.** Rogue access point

Quick Answer: **291**

The Details: **351**

C59. A penetration tester is researching a company using information gathered from user profiles and posts on a social media site. Which of the following would describe this activity?

❍ **A.** Pivot

❍ **B.** Passive footprinting

❍ **C.** White box testing

❍ **D.** Persistence

Quick Answer: **291**

The Details: **352**

C60. A system administrator is configuring an IPsec VPN to a remote location and would like to ensure that the VPN provides confidentiality for both the original IP header and the data. Which of the following should be configured on the VPN?

❍ **A.** ECB

❍ **B.** AH

❍ **C.** PEAP

❍ **D.** HMAC

❍ **E.** ESP

Quick Answer: **291**

The Details: **353**

C61. Which of these cloud deployment models would BEST describe a company that would build a cloud for their own use and use systems and storage platforms in their data center?

❍ **A.** Private

❍ **B.** Community

❍ **C.** Hybrid

❍ **D.** Public

Quick Answer: **291**

The Details: **354**

C62. Which of the following malware types would cause a workstation to participate in a DDoS?

❍ **A.** Bot

❍ **B.** Logic bomb

❍ **C.** Ransomware

❍ **D.** Keylogger

Quick Answer: **291**

The Details: **355**

C63. Which of these are used to force the preservation of data for later use in court?

❍ **A.** Chain of custody

❍ **B.** Data loss prevention

❍ **C.** Legal hold

❍ **D.** Order of volatility

Quick Answer: **291**

The Details: **356**

C64. A network administrator is installing a series of access points in a public library. Which of the following would be the BEST way to prevent theft of his laptop while performing this work?

❍ **A.** Biometrics

❍ **B.** Cable lock

❍ **C.** Protected distribution

❍ **D.** Faraday cage

Quick Answer: **291**

The Details: **357**

C65. A company would like to install an IPS to observe normal network activity and block any traffic that deviates from this baseline. Which of these IPS types would be the BEST fit for this requirement?

❍ **A.** Heuristic

❍ **B.** Anomaly-based

❍ **C.** Behavior-based

❍ **D.** Signature-based

Quick Answer: **291**

The Details: **358**

C66. A security engineer is capturing packets on an internal company network and is documenting the IP addresses and MAC addresses associated with the local network devices. Which of these commands would provide the MAC address of the default gateway at 10.11.1.1?

❍ **A.**
```
ping 10.11.1.1
arp -a
```

❍ **B.** `tracert 10.11.1.1`

❍ **C.** `dig 10.11.1.1`

❍ **D.** `ipconfig /all`

Quick Answer: **291**

The Details: **359**

C67. A network administrator needs to identify all inbound connections to a Linux web server. Which of the following utilities would be the BEST choice for this task?

❍ **A.** netcat

❍ **B.** nmap

❍ **C.** net view

❍ **D.** netstat

Quick Answer: **291**

The Details: **360**

C68. A company has identified a web server data breach that resulted in the theft of financial records from 150 million customers. A security update to the company's web server software was available for two months prior to the breach. Which of the following would have prevented this breach from occurring?

❍ **A.** Patch management

❍ **B.** Full disk encryption

❍ **C.** Disable unnecessary services

❍ **D.** Application allow lists

Quick Answer: **291**

The Details: **361**

C69. A security administrator is deploying a web server and needs to understand the methods an attacker could use to gain access to the system. Which of the following would be the BEST source of this information?

❍ **A.** MITRE ATT&CK

❍ **B.** Diamond model

❍ **C.** Tabletop exercise

❍ **D.** ISO 27701

Quick Answer: **291**

The Details: **362**

C70. A system administrator has identified an unexpected username on a database server, and the user has been transferring database files to an external server over the company's Internet connection. The administrator then performed these tasks:

- Physically disconnected the Ethernet cable on the database server
- Disabled the unknown account
- Configured a firewall rule to prevent file transfers from the server

Which of the following would BEST describe this part of the incident response process?

❍ **A.** Eradication
❍ **B.** Containment
❍ **C.** Lessons learned
❍ **D.** Preparation

Quick Answer: **291**

The Details: **363**

C71. Which of the following would be the MOST effective use of asymmetric encryption?

❍ **A.** Real-time video encryption
❍ **B.** Store passwords
❍ **C.** Protect data on mobile devices
❍ **D.** Securely derive a session key

Quick Answer: **291**

The Details: **364**

C72. Each salesperson in a company will receive a laptop with applications and data to support their sales efforts. The IT manager would like to prevent third-parties from gaining access to this information if the laptop is stolen. Which of the following would be the BEST way to protect this data?

❍ **A.** Remote wipe
❍ **B.** Full disk encryption
❍ **C.** Biometrics
❍ **D.** BIOS user password

Quick Answer: **291**

The Details: **365**

C73. During sales meetings, visitors often require an Internet connection for demonstrations. Which of the following should the company implement to maintain the security of the internal network resources?

❍ **A.** NAT

❍ **B.** Ad hoc wireless workstations

❍ **C.** Intranet

❍ **D.** Guest network with captive portal

Quick Answer: **291**

The Details: **366**

C74. A company's web server has been infected with malware, and the security administrator has contained the system and would like to create a bit-by-bit image of the server storage drive. Which of the following would be the BEST choice for this task?

❍ **A.** Memdump

❍ **B.** chmod

❍ **C.** dd

❍ **D.** tcpdump

Quick Answer: **291**

The Details: **367**

C75. A set of corporate security policies is what kind of security control?

❍ **A.** Compensating

❍ **B.** Detective

❍ **C.** Administrative

❍ **D.** Physical

Quick Answer: **291**

The Details: **368**

C76. Which of the following would be the MOST significant security concern when protecting against criminal syndicates?

❍ **A.** Prevent users from posting passwords near their workstations

❍ **B.** Require identification cards for all employees and guests

❍ **C.** Maintain reliable backup data

❍ **D.** Use access control vestibules at all data center locations

Quick Answer: **291**

The Details: **369**

C77. An application team has been provided with a hardened version of Linux to use with a new application rollout, and they are installing a web service and the application code on the server. Which of the following would BEST protect the application from attacks?

❍ **A.** Build a backup server for the application

❍ **B.** Run the application in a cloud-based environment

❍ **C.** Implement a secure configuration of the web service

❍ **D.** Send application logs to the SIEM via syslog

Quick Answer: **291**

The Details: **370**

C78. A system administrator has configured MAC filtering on the corporate access point, but access logs show that unauthorized users are accessing the network. The administrator has confirmed that the address filter includes only authorized MAC addresses. Which of the following should the administrator configure to prevent this authorized use?

❍ **A.** Enable WPA3 encryption

❍ **B.** Remove unauthorized MAC addresses from the filter

❍ **C.** Modify the SSID name

❍ **D.** Modify the channel

Quick Answer: **291**

The Details: **371**

C79. A company is building a broad set of conditional steps to follow when investigating a data breach. Which of the following would BEST describe these steps?

❍ **A.** Managerial controls

❍ **B.** DAC

❍ **C.** Playbook

❍ **D.** Order of volatility

Quick Answer: **291**

The Details: **372**

C80. During an initial network connection, a supplicant communicates to an authenticator, which then sends an authentication request to an Active Directory database. Which of the following would BEST describe this authentication technology?

❍ **A.** Federation

❍ **B.** AES

❍ **C.** 802.1X

❍ **D.** PKI

Quick Answer: **291**

The Details: **373**

C81. A security administrator would like use employee-owned mobile phones to unlock the door of the data center using a sensor on the wall. The users would authenticate on their phones with a fingerprint before the door would unlock. Which of the following features should the administrator use? (Select TWO)

❍ **A.** NFC

❍ **B.** Remote wipe

❍ **C.** Containerization

❍ **D.** Biometrics

❍ **E.** Push notification

Quick Answer: **291**

The Details: **374**

C82. Visitors to a corporate data center must enter through the main doors of the building. Which of the following security controls would be the BEST choice to successfully guide people to the front door? (Select TWO)

❍ **A.** Cable locks

❍ **B.** Bollards

❍ **C.** Biometrics

❍ **D.** Fencing

❍ **E.** Industrial camouflage

❍ **F.** Video surveillance

Quick Answer: **291**

The Details: **375**

C83. A company is contracting with a third-party to find vulnerabilities that employees could possibly exploit on the company's internal networks. Which of the following would be the BEST way for the third-party to meet this requirement?

❍ **A.** Run a credentialed vulnerability scan

❍ **B.** Capture packets of the application traffic flows from the internal network

❍ **C.** Identify an exploit and perform a privilege escalation

❍ **D.** Scan the network during normal working hours

Quick Answer: **291**

The Details: **376**

C84. A company has recently moved from one accounting system to another, and the new system includes integration with many other divisions of the organization. Which of the following would ensure that the correct access has been provided to the proper employees in each division?

❍ **A.** Location-based policies

❍ **B.** On-boarding process

❍ **C.** Account deprovisioning

❍ **D.** Permission and usage audit

Quick Answer: **291**

The Details: **377**

C85. An attacker has circumvented a web-based application to send commands directly to a database. Which of the following would describe this attack type?

❍ **A.** Session hijack

❍ **B.** SQL injection

❍ **C.** Cross-site scripting

❍ **D.** On-path

Quick Answer: **291**

The Details: **378**

C86. A group of business partners is using blockchain technology to monitor and track raw materials and parts as they are transferred between companies. Where would a partner find these tracking details?

❍ **A.** Ledger
❍ **B.** HSM
❍ **C.** SIEM
❍ **D.** SED

Quick Answer: **291**

The Details: **379**

C87. A network technician at a bank has noticed a significant decrease in traffic to the bank's public website. After additional investigation, the technician finds that users are being directed to a web site that looks similar to the bank's site but is not under the bank's control. Flushing the local DNS cache and changing the DNS entry does not have any effect. Which of the following has most likely occurred?

❍ **A.** DDoS
❍ **B.** Disassociation attack
❍ **C.** Evil twin
❍ **D.** Domain hijacking

Quick Answer: **291**

The Details: **380**

C88. A company runs two separate applications in their data center. The security administrator has been tasked with preventing all communication between these applications. Which of the following would be the BEST way to implement this security requirement?

❍ **A.** Firewall
❍ **B.** Protected distribution
❍ **C.** Air gap
❍ **D.** VLANs

Quick Answer: **291**

The Details: **381**

C89. A receptionist at a manufacturing company recently received an email from the CEO asking for a copy of the internal corporate employee directory. The receptionist replied to the email and attached a copy of the directory. It was later determined that the email address was not sent from the CEO and the domain associated with the email address was not a corporate domain name. What type of training could help prevent this type of situation in the future?

❍ **A.** Recognizing social engineering

❍ **B.** Using emails for personal use

❍ **C.** Proper use of social media

❍ **D.** Understanding insider threats

Quick Answer: **291**

The Details: **382**

C90. A company's security engineer is working on a project to simplify the employee onboarding and offboarding process. One of the project goals is to allow individuals to use their personal phones for work purposes. If the user leaves the company, the company data will be removed but the user's data would remain intact. Which of these technologies would meet this requirement?

❍ **A.** Policy management

❍ **B.** Geofencing

❍ **C.** Containerization

❍ **D.** Storage encryption

Quick Answer: **291**

The Details: **383**

Practice Exam C

Multiple Choice Quick Answers

C6. D
C7. B
C8. D
C9. C
C10. D
C11. B
C12. B
C13. D
C14. D
C15. B
C16. C and D
C17. D
C18. A
C19. A
C20. A
C21. D
C22. C
C23. A
C24. C
C25. C
C26. A
C27. C
C28. B
C29. C
C30. B
C31. A
C32. B
C33. D
C34. D
C35. D
C36. C
C37. C
C38. B
C39. B
C40. B
C41. A
C42. B
C43. D
C44. A
C45. B
C46. D
C47. B
C48. C
C49. B
C50. C
C51. A
C52. A
C53. C
C54. D and E
C55. D
C56. B
C57. C
C58. A
C59. B
C60. E
C61. A
C62. A
C63. C
C64. B
C65. B
C66. A
C67. D
C68. A
C69. A
C70. B
C71. D
C72. B
C73. D
C74. C
C75. C
C76. C
C77. C
C78. A
C79. C
C80. C
C81. A and D
C82. B and D
C83. A
C84. D
C85. B
C86. A
C87. D
C88. C
C89. A
C90. C

Practice Exam C Detailed Answers

C1. Refer to the following firewall ruleset:

Rule #	Source IP	Destination IP	Protocol (TCP/ UDP)	Port #	Allow/ Block
1	Any	10.1.10.88	TCP	22	Allow
2	Any	10.1.10.120	TCP	80	Allow
3	Any	10.1.10.120	TCP	443	Allow
4	Any	10.1.10.61	TCP	3389	Allow
5	Any	Any	UDP	53	Allow
6	Any	Any	UDP	123	Allow
7	Any	Any	ICMP		Block

Categorize the following traffic flows as ALLOWED or BLOCKED through the firewall:

ALLOWED Use a secure terminal to connect to 10.1.10.88

The use a secure terminal requires SSH (Secure Shell) over TCP port 22. Rule 1 allows any IP address to connect to 10.1.10.88 over TCP/22.

BLOCKED Share the desktop on server 10.1.10.120

Sharing a desktop using RDP (Remote Desktop Protocol) requires the use of TCP/3389. Although a rule 4 allows TCP/3389 to communicate to 10.1.10.61, the firewall rules for destination 10.1.10.120 only include TCP/80 and TCP/443.

ALLOWED Perform a DNS query from 10.1.10.88 to 9.9.9.9

Rule 5 allows DNS queries to run over UDP/53 from any IP address to any IP address.

ALLOWED View web pages on 10.1.10.120

Rule 2 allows TCP/80 traffic flows to 10.1.10.120, and rule 3 allows TCP/443 traffic to 10.1.10.120. Both of these rules would allow HTTP and HTTPS traffic to communicate to the web server at 10.1.10.120.

BLOCKED Authenticate to an LDAP server at 10.1.10.61

LDAP commonly uses TCP/389 for traffic flows, and none of the firewall rules specify this protocol. A firewall's implicit deny will block all traffic that does not match a specific rule.

ALLOWED Synchronize the clock on a server at 10.1.10.17

NTP (Network Time Protocol) uses UDP/123 for time syncronization, and firewall rule 6 allows NTP traffic from any IP address to any IP address.

More information:
SY0-601, Objective 3.3 - Firewalls
https://professormesser.link/601030306

C2. Match the device to the description. Some device types will not be used.

IPS

Block SQL injection over an Internet connection

An IPS (Intrusion Prevention System) monitors network traffic for exploit attempts such as buffer overflows, cross-site scripting, SQL injections, or other known exploits. If an exploit attempt is identified in the traffic flow, the IPS will block the traffic and prevent the attack.

Proxy

Intercept all browser requests and cache the results

Proxies are commonly installed between the users and the external network. The proxy will intercept the user requests and make the requests on their behalf. The proxy will provide access control, content scanning, and caching of web site traffic.

Router

Forward packets between separate VLANs

Routers forward traffic between separate IP subnets or VLANs, and use the destination IP address to determine which interface on the router will be used as the next hop to the end destination.

Load balancer

Configure a group of redundant web servers

Load balancers distribute traffic loads between servers. This allows an organization to build large-scale implementations of server farms to provide scalability and fault tolerance. If one of the servers on a load balancer were to fail, the other servers will balance the additional load to prevent any downtime.

WAF

Evaluate the input to a browser-based application

A WAF (Web Application Firewall) examines user input to a browser-based application and allows or denies traffic based on the expected input. This is commonly used to prevent SQL injections, cross-site scripting, or similar input-related security concerns.

More information:
SY0-601, Section 3.3 videos - Intrusion Prevention
https://professormesser.link/601030309

C3. Match the characteristic to the attack type:

DoS	A website stops responding to normal requests

A DoS (Denial of Service) forces a service to fail, and it usually succeeds by taking advantage of a design failure or vulnerability.

Spoofing	IP addresses are cloned to gain access without authenticating

One common method of attacking a network is for the attacker to make their system appear to be a trusted system. An attacker will spoof email addresses, IP addresses, caller ID numbers, and other identifiers to attempt to gain access to systems or information.

Rootkit	The malware is designed to remain hidden on a computer system

Malware installed as rootkit often modifies core system files to help remain invisible on the infected system.

Dictionary	A list of common passwords are attempted with a known username

Attackers will use a list of common passwords when reverse engineering authentication credentials. These passwords are stored in a list called a "dictionary."

Phishing	An email link redirects a user to a site that requests login credentials

Phishing uses copycat websites and a bit of social engineering to convince victims to give up authentication credentials or personal information.

Tailgating	A person gains unauthorized access to a secure storage room

An easy way to gain access to a secure area is to simply walk behind someone who has already gained access to that area.

More information:
SY0-601, Section 1.2 videos - Attack Types
https://professormesser.link/sy0601

C4. What secure protocols should be used to provide these application flows?

Diffusion	One character changes, and the resulting hash is very different

Encryption should be a very random process. If you modify a single character in the plaintext, the encrypted data or hash should change dramatically. This change in the output is called diffusion.

Confusion	The encrypted data is drastically different than the plaintext

The randomization of the encryption process should provide a very different result than the original plaintext. Confusion describes the drastic differences between the plaintext and the encrypted data.

Collision	Different inputs create the same hash

The resulting hash of some information should be a unique value. If two different pieces of information are providing the same hash, then a collision has occurred.

Obfuscation	The process of making something unclear

Hiding information can be useful, and the process of making something difficult to understand is obfuscation.

Asymmetric	A different key is used for decryption than encryption

Unlike symmetric encryption that uses the same key for both encryption and decryption, asymmetric encryption uses one key for the encryption process and a completely different key for the decryption process.

PFS	Use a different encryption key for every session

PFS (Perfect Forward Secrecy) is an encryption method that creates asymmetric encryption key pairs dynamically, uses them for the duration of the session, and then discards them.

More information:
SY0-601, Section 2.8 videos - Cryptography Concepts
https://professormesser.link/sy0601

C5. Match the PKI component to the description:

RA

Registration Authority -
Verifies the entity requesting the certificate

The registration authority works with the certificate authority to identify and authenticate the certificate requester.

CRL

Certificate Revocation List -
A list of invalidated certificates

The certificate revocation list is a file containing a list of the revoked certificates. This list is maintained by the associated certificate authority.

CSR

Certificate Signing Request -
Send the public key to the CA to be signed

The certificate signing request is sent with the public key to the certificate authority. Once the certificate information has been verified, the CA will digitally sign the public key certificate.

CA

Certificate Authority -
Deploy and manage certificates

The certificate authority, or CA, is the administrative control for any public key infrastructure deployment.

OCSP

Online Certificate Status Protocol -
The browser checks for certificate revocation

OCSP is a protocol used by the browser to check the revocation status of a certificate.

More information:
SY0-601, Section 3.9 - Public Key Infrastructure
https://professormesser.link/601030901

C6. A finance company is legally required to maintain seven years of tax records for all of their customers. Which of the following would be the BEST way to implement this requirement?

❍ **A.** Create an automated script to remove all tax information more than seven years old

❍ **B.** Print and store all tax records in a seven-year cycle

❍ **C.** Allow users to download tax records from their account login

❍ **D.** Create a separate daily backup archive for all applicable tax records

The Answer: D. Create a separate daily backup archive for all applicable tax records

The important consideration for a data retention mandate is to always have access to the information over the proposed time frame. In this example, a daily backup would ensure that tax information is constantly archived over a seven year period and could always be retrieved if needed. If data was inadvertently deleted from the primary storage, the backup would still maintain a copy.

The incorrect answers:

A. Create an automated script to remove all tax information more than seven years old

The requirement is to maintain data for at least seven years, but there's no requirement to remove that data once it's more than seven years old. For example, some financial information may need to be retained well beyond the seven year mandate.

B. Print and store all tax records in a seven-year cycle

Paper has its place, but creating physical output of tax records and storing them for seven years would include a significant cost in time, materials, and inventory space. The requirement to store data for seven years doesn't require the information to be stored in a physical form.

C. Allow users to download tax records from their account login

Including a feature to allow users access to their records is useful for the user community, but it doesn't provide any data protection for the seven year retention period.

More information:

SY0-601, Objective 5.3 - Managing Data

https://professormesser.link/601050303

C7. A system administrator is designing a data center for an insurance company's new public cloud and would like to restrict user access to sensitive data. Which of the following would provide ongoing visibility, data security, and control of cloud-based applications?

❍ **A.** HSM

❍ **B.** CASB

❍ **C.** 802.1X

❍ **D.** EDR

The Answer: B. CASB
A CASB (Cloud Access Security Broker) allows the security administrator to manage security policies for cloud-based applications.

The incorrect answers:
A. HSM
An HSM (Hardware Security Module) manages certificates, digital keys, and can often offload cryptographic functions. An HSM is not used for visibility and control of cloud-based applications.

C. 802.1X
802.1X is an authentication standard for port-based network access control, or NAC. 802.1X does not provide visibility or control of cloud-based applications.

D. EDR
EDR (Endpoint Detection and Response) is a security solution for end-user devices to protect against malicious software and threats.

More information:
SY0-601, Objective 3.6 - Cloud Security Solutions
https://professormesser.link/601030605

C8. A device is exhibiting intermittent connectivity when viewing remote web sites. A security administrator views the local device ARP table:

```
Internet Address     Physical Address
192.168.1.1          60:3d:26:69:71:fc
192.168.1.101        e2:c3:53:79:4c:51
192.168.1.102        7a:3b:8f:21:86:57
192.168.1.103        60:3d:26:69:71:fc
192.168.1.104        00:80:92:c7:c8:49
192.168.1.105        d0:81:7a:d3:f0:d5
```

Which of the following would be the MOST likely explanation of this connectivity issue?

❍ **A.** DDoS

❍ **B.** Wireless disassociation

❍ **C.** Rogue access point

❍ **D.** ARP poisoning

The Answer: D. ARP poisoning
The duplicate MAC (Media Access Control) address from 192.168.1.1 and 192.168.1.103 indicates MAC spoofing or ARP (Address Resolution Protocol) poisoning. There should not be duplicate MAC addresses associated with two IP addresses on the same subnet.

The incorrect answers:
A. DDoS
A DDoS (Distributed Denial of Service) attack would not duplicate a MAC address on an IP subnet.

B. Wireless disassociation
Wireless disassociation uses specially crafted wireless management frames to disconnect wireless devices from a network. A duplicate MAC address does not indicate a wireless disassociation attack.

C. Rogue access point
A rogue access point would have its own MAC address and it would not be duplicated on the local IP subnet.

More information:
SY0-601, Objective 1.4 - On-Path Attacks
https://professormesser.link/601010407

C9. A security administrator has identified an internally developed application that allows users to modify SQL queries through a web-based front-end. To prevent this modification, the administrator has recommended that all queries be completely removed from the application front-end and placed onto the back-end of the application server. Which of the following would describe this implementation?

❍ **A.** Input validation

❍ **B.** Code signing

❍ **C.** Stored procedures

❍ **D.** Obfuscation

The Answer: C. Stored procedures
Stored procedures are SQL queries that execute on the server side instead of the client application. The client application calls the stored procedure on the server, and this prevents the client from making any changes to the actual SQL queries.

The incorrect answers:
A. Input validation
Input validation would examine the input from the client and make sure that it is expected. In this example, moving the SQL queries to the back-end server process would not require any validation of the SQL queries. As a best practice, any additional input from the client would still need validation.

B. Code signing
Code that has been digitally signed by the application developer can be evaluated to ensure that nothing has changed with the application code since it was published.

D. Obfuscation
Obfuscation makes something that is normally understandable very difficult to understand. The move of SQL queries to the server changes the processing of the application itself, but it isn't a method of obfuscation.

More information:
SY0-601, Objective 2.3 - Secure Coding Techniques
https://professormesser.link/601020303

C10. A system administrator is implementing a fingerprint scanner to provide access to the data center. Which of these metrics should be kept at a minimum in order to prevent unauthorized persons from accessing the data center?

❍ **A.** TOTP

❍ **B.** FRR

❍ **C.** HOTP

❍ **D.** FAR

The Answer: D. FAR
FAR (False Acceptance Rate) is the likelihood that an unauthorized user will be accepted. The FAR should be kept as close to zero as possible.

The incorrect answers:

A. TOTP
A TOTP (Time-based One-Time Password) is an algorithm that provides a pseudo-random number as an authentication factor. A TOTP does not describe the accuracy of a biometric system.

B. FRR
FRR (False Rejection Rate) is the likelihood that an authorized user will be rejected. If the FRR is incrementing, then authorized users will not gain access to the data center. This value is not associated with unauthorized access.

C. HOTP
HOTP (HMAC-based One-Time Password) is an algorithm that provides an authentication factor based on a one-time password. An HOTP does not describe the accuracy of a biometric system.

More information:
SY0-601, Objective 2.4 - Biometrics
https://professormesser.link/601020402

C11. The IT department of a transportation company maintains an on-site inventory of chassis-based network switch interface cards. If a failure occurs, the on-site technician can replace the interface card and have the system running again in sixty minutes. Which of the following BEST describes this recovery metric?

❍ **A.** MTBF

❍ **B.** MTTR

❍ **C.** RPO

❍ **D.** RTO

The Answer: B. MTTR
MTTR (Mean Time To Restore) is the amount of time required to get back up and running. This is sometimes called Mean Time To Repair.

The incorrect answers:

A. MTBF
MTBF (Mean Time Between Failures) is a prediction of how long the system will be operational before a failure occurs.

C. RPO
An RPO (Recovery Point Objective) is a qualifier that determines when the system is recovered. A recovered system may not be completely repaired, but it will be running well enough to maintain a certain level of operation.

D. RTO
An RTO (Recovery Time Objective) is the service level goal to work towards when recovering a system and getting back up and running.

More information:
SY0-601, Objective 5.4 - Business Impact Analysis
https://professormesser.link/601050403

C12. A company maintains a server farm in a large data center. These servers are for internal use only and are not accessible externally. The security team has discovered that a group of servers was breached before the latest updates were applied. Breach attempts were not logged on any other servers. Which of these threat actors would be MOST likely involved in this breach?

○ **A.** Competitor

○ **B.** Insider

○ **C.** Nation state

○ **D.** Script kiddie

The Answer: B. Insider
None of these servers were accessible from the outside, and the only servers with any logged connections were those that also were susceptible to the latest vulnerabilities. To complete this attack, you would need a very specific knowledge of the exact systems that were vulnerable and a way to communicate with those servers. For either of those reasons, the Insider threat as would be the most likely from the available list.

The incorrect answers:
A. Competitor
Although an unethical competitor could be interested in disabling certain systems, the specificity of this attack and the lack of accessibility to the systems would seem to dismiss a competitor.

C. Nation state
A nation state would have the resources needed to attack a network, gain access to the internal systems, and then somehow monitor the update processes for each server. However, the scope and breadth of such an attack would be complex, and this would make the nation state a very speculative option and not the most likely option from the available list.

D. Script kiddie
Script kiddies don't generally have access to an internal network, and they aren't discerning enough to track the status of which systems may have been recently updated.

More information:
SY0-601, Objective 1.5 - Threat Actors
https://professormesser.link/601010501

C13. An organization has contracted with a third-party to perform a vulnerability scan of their Internet-facing web servers. The report shows that the web servers have multiple Sun Java Runtime Environment (JRE) vulnerabilities, but the server administrator has verified that JRE is not installed. Which of the following would be the BEST way to handle this report?

❍ **A.** Install the latest version of JRE on the server

❍ **B.** Quarantine the server and scan for malware

❍ **C.** Harden the operating system of the web server

❍ **D.** Ignore the JRE vulnerability alert

The Answer: D. Ignore the JRE vulnerability alert
It's relatively common for vulnerability scans to show vulnerabilities that don't actually exist, especially if the scans are not credentialed. An issue that is identified but does not actually exist is a false positive, and it can be dismissed once the alert has been properly researched.

The incorrect answers:
A. Install the latest version of JRE on the server
The system administrator verified that JRE was not currently installed on the server, so it would not be possible for that vulnerability to actually exist. Installing an unneeded version of JRE on the server could potentially open the server to actual vulnerabilities.

B. Quarantine the server and scan for malware
The JRE false positive isn't an indication of malware, and no mention is made of the report including any additional vulnerabilities or reports of malware.

C. Harden the operating system of the web server
Although it's always a good best practice to harden the operating system of an externally-facing server, this vulnerability scan report doesn't indicate any particular vulnerability with the operating system itself. If the scan identified specific OS vulnerabilities, then additional hardening may be required.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

C14. A user downloaded and installed a utility for compressing and decompressing files. Immediately after installing the utility, the user's overall workstation performance degraded, and it now takes twice as much time to perform any tasks on the computer. Which of the following is the BEST description of this malware infection?

❍ **A.** Ransomware

❍ **B.** Adware

❍ **C.** Logic bomb

❍ **D.** Trojan

The Answer: D. Trojan
A Trojan horse is malicious software that pretends to be something benign. The user will install the software with the expectation that it will perform a particular function, but in reality it is installing malware on the computer.

The incorrect answers:
A. Ransomware
Ransomware will lock a system and present a message to the user with instructions on how to unlock the system. This usually involves sending the attacker money in exchange for the unlock key.

B. Adware
Adware is obvious due to the increased number of advertisements that will be displayed after the infection.

C. Logic bomb
A logic bomb will execute when a certain event occurs, such as a specific date and time.

More information:
SY0-601, Objective 1.2 - Trojans and RATs
https://professormesser.link/601010204

C15. Which of the following is the process for replacing sensitive data with a non-sensitive and functional placeholder?

❍ **A.** Minimization

❍ **B.** Tokenization

❍ **C.** Retention

❍ **D.** Masking

The Answer: B. Tokenization
Tokenization replaces sensitive data with a token, and this token can be used as a functional placeholder for the original data. Tokenization is commonly used with credit card processing and mobile devices.

The incorrect answers:
A. Minimization
Minimization is a data collection policy that limits the amount of personal or private information that can be gathered. With minimization, information outside of the required scope would not be collected.

C. Retention
Data retention specifies the amount of time that data should be stored or saved. Retention policies do not commonly replace sensitive data.

D. Masking
Data masking hides some of the original data to protect it from view. While hidden, this data cannot be used for any functional purpose.

More information:
SY0-601, Objective 5.5 - Enhancing Privacy
https://professormesser.link/601050503

C16. A security administrator has installed a new firewall to protect a web server VLAN. The application owner requires that all web server sessions communicate over an encrypted channel. Which of these rules should the security administrator include in the firewall rulebase? (Select TWO)

❍ **A.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 23, Deny`

❍ **B.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Deny`

❍ **C.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Deny`

❍ **D.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Allow`

❍ **E.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Allow`

The Answers:

C. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Deny`

D. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Allow`

Most web servers use tcp/80 for HTTP (Hypertext Transfer Protocol) communication and tcp/443 for HTTPS (Hypertext Transfer Protocol Secure). HTTP traffic sends traffic in the clear, so the first firewall rule would block any tcp/80 traffic before it hits the web server. The second rule allows HTTPS encrypted traffic to continue to the web server over tcp/443.

The incorrect answers:

A. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 23, Deny`
The insecure Telnet protocol commonly uses tcp/23, but most web servers would not be listening on tcp/23. An explicit tcp/23 deny rule would not provide any additional web server security.

B. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Deny`
The encrypted HTTPS protocol uses tcp/443, so the security administrator would not want to deny that traffic through the firewall.

E. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Allow`
Since the application owner requires encrypted communication, allowing HTTP over tcp/80 should not be allowed through the firewall.

More information:
SY0-601, Objective 3.3 - Firewalls
https://professormesser.link/601030306

C17. Which of these would be used to provide multi-factor authentication?

❍ **A.** USB-connected storage drive with FDE

❍ **B.** Employee policy manual

❍ **C.** Null-modem serial cable

❍ **D.** Smart card with picture ID

The Answer: D. Smart card with picture ID
A smart card commonly includes a certificate that can be used as a multifactor authentication of something you have. These smart cards are commonly combined with an employee identification card, and often require a separate PIN (Personal Identification Number) as an additional authentication factor.

The incorrect answers:
A. USB-connected storage drive with FDE
FDE (Full Disk Encryption) will protect the data on a drive, but it doesn't provide a factor of authentication.

B. Employee policy manual
Employee policy manuals aren't commonly associated with a specific individual, so they are not a good factor of authentication.

C. Null-modem serial cable
A null-modem serial cable is an important accessory for any field technician, but it doesn't provide any authentication factors.

More information:
SY0-601, Objective 2.4 - Multi-Factor Authentication
https://professormesser.link/601020403

C18. An IT manager is leading a project to implement a global standard for a privacy information management system. Which of these standards would BEST apply to this project?

❍ **A.** ISO 27701

❍ **B.** PCI DSS

❍ **C.** SSAE SOC 2

❍ **D.** CSA CCM

The Answer: A. ISO 27701
The ISO (International Organization for Standardization) 27701 framework is designed to enhance privacy controls towards adding or improving a Privacy Information Management System (PIMS).

The incorrect answers:
B. PCI DSS
The PCI DSS (Payment Card Industry Data Security Standard) is a set of security rules and guidelines for storing credit card information.

C. SSAE SOC 2
The SSAE SOC 2 (Statement on Standards for Attestation Engagements, System and Organization Controls 2) is an auditing standard for IT systems.

D. CSA CCM
The CSA CCM (Cloud Security Alliance Cloud Controls Matrix) provides security information and guidelines for cloud-based applications.

More information:
SY0-601, Objective 5.2 - Security Frameworks
https://professormesser.link/601050202

C19. A company's security cameras have identified an unknown person walking into a fenced disposal area in the back of the building and then leaving with a box containing printed documents. Which of the following attacks is this person attempting?

❍ **A.** Dumpster diving

❍ **B.** Shoulder surfing

❍ **C.** Tailgating

❍ **D.** Phishing

The Answer: A. Dumpster diving
A company can often throw out useful information, and attackers will literally climb through the trash bin to obtain this information.

The incorrect answers:
B. Shoulder surfing
Shoulder surfing is viewing someone else's screen, which is effectively over their shoulder.

C. Tailgating
If you follow someone through a locked door without providing any credentials or using an access card, you would be tailgating.

D. Phishing
Phishing is the process of tricking someone into providing their personal information.

More information:
SY0-601, Objective 1.1 - Dumpster Diving
https://professormesser.link/601010103

C20. A technology company is manufacturing a military-grade radar tracking system that can instantly identify any nearby unmanned aerial vehicles (UAVs). The UAV detector must be able to instantly identify and react to a vehicle without delay. Which of the following would BEST describe this tracking system?

❍ **A.** RTOS

❍ **B.** IoT

❍ **C.** ICS

❍ **D.** MFD

The Answer: A. RTOS

This tracking system requires an RTOS (Real-Time Operating System) that can instantly react to input without any significant delays or queuing in the operating system. Operating systems used by the military, automobile manufacturers, and industrial equipment developers often use RTOS to ensure that certain transactions can be processed without any significant delays.

The incorrect answers:

B. IoT

IoT (Internet of Things) devices are generally associated with home automation and do not have a requirement for real-time operation.

C. ICS

An ICS (Industrial Control System) is often a dedicated network used exclusively to manage and control manufacturing equipment, power generation equipment, water management systems, and other industrial machines. Although some industrial control systems may use an RTOS, using a real-time operating system is not a requirement of an ICS.

D. MFD

A multifunction device (MFD) is commonly associated with a device that can print, scan, and fax. There are no real-time OS requirements in a typical MFD.

More information:

SY0-601, Objective 2.6 - Embedded Systems

https://professormesser.link/601020601

C21. A private company uses an SSL proxy to examine the contents of an encrypted application during transmission. How could the application developers prevent the use of this proxy examination in the future?

❍ **A.** OCSP stapling

❍ **B.** Offline CAs

❍ **C.** Certificate chaining

❍ **D.** Certificate pinning

The Answer: D. Certificate pinning

Certificate pinning embeds or "pins" a certificate inside of an application. When the application contacts a service, the service certificate will be compared to the pinned certificate. If the certificates match, the application knows that it can trust the service. If the certificates don't match, then the application can choose to shut down, show an error message, or make the user aware of the discrepancy. An SSL proxy will use a different certificate than the service certificate, so an application using certificate pinning can identify and react to this situation.

The incorrect answers:

A. OCSP stapling

OCSP (Online Certificate Status Protocol) stapling is a method that has the certificate holder verify their own certificate status. The OCSP status is commonly "stapled" into the SSL handshake process.

B. Offline CAs

An offline CA (Certificate Authority) is a common way to prevent the exploitation of a root authority. If the CA is offline, then you can't hack it. However, an online or offline CA won't prevent the use of an SSL proxy.

C. Certificate chaining

Intermediate certificates are often listed between a web server's SSL certificate and the root certificate. This list of intermediate certificates is called a "chain." It's important to configure web servers with the proper chain, or the end user may receive an error in their browser that the server can't be trusted.

More information:

SY0-601, Objective 3.9 - Certificate Concepts

http://professormesser.link/601030904

C22. A security administrator is concerned that a user may have installed a rogue access point on the corporate network. Which of the following could be used to confirm this suspicion?

❍ **A.** UTM log

❍ **B.** WAF log

❍ **C.** Switch log

❍ **D.** DLP log

The Answer: C. Switch log
A rogue access point would be difficult to identify once it's on the network, but at some point the access point would need to physically connect to the corporate network. An analysis of switch interface activity would be able to identify any new devices and their MAC addresses.

The incorrect answers:
A. UTM log
A UTM (Unified Threat Management) gateway is an all-in-one device that provides firewall services, URL filtering, spam filtering, and more. From the UTM's perspective, the traffic from a rogue access point would look similar to all other traffic on the network.

B. WAF log
A WAF (Web Application Firewall) would not be able to determine if web server traffic was from a rogue access point or a legitimate wired device.

D. DLP log
DLP (Data Loss Prevention) is important for stopping the transfer of confidential data, but it would not be able to identify traffic from a rogue access point.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

C23. During a ransomware outbreak, an organization was forced to rebuild database servers from known good backup systems. In which of the following incident response phases were these database servers brought back online?

❍ **A.** Recovery

❍ **B.** Lessons learned

❍ **C.** Containment

❍ **D.** Identification

The Answer: A. Recovery
The recovery phase focuses on getting things back to normal after an attack. This is the phase that removes malware, fixes vulnerabilities, and recovers the damaged systems.

The incorrect answers:
B. Lessons learned
Once an event is over, it's useful to have a post-incident meeting to discuss the things that worked and things that didn't.

C. Containment
When an event occurs, it's important to minimize the impact. Isolation and containment can help to limit the spread and effect of an event.

D. Identification
Identifying the event is an important step that initiates the rest of the incident response processes.

More information:
SY0-601, Objective 4.2 - Incident Response
https://professormesser.link/601040201

C24. Which of the following cloud deployments would include CPU, storage, and networking, but not include any operating system or application?

❍ **A.** SaaS

❍ **B.** DaaS

❍ **C.** IaaS

❍ **D.** PaaS

The Answer: C. IaaS
IaaS (Infrastructure as a Service) describes a cloud model that provides the base hardware of a system. The administrator of the system would still need to install an OS and applications on the IaaS system.

The incorrect answers:

A. SaaS
SaaS (Software as a Service) is a cloud model that provides everything for the end user. End users on a SaaS model would not usually have access to the operating system or the application code.

B. DaaS
DaaS (Desktop as a Service) describes a virtual computing environment with managed desktops in the cloud.

D. PaaS
PaaS (Platform as a Service) provides the foundational building blocks for application development and requires the users to build their own applications on the cloud platform.

More information:
SY0-601, Objective 2.2 - Cloud Models
https://professormesser.link/601020201

C25. A network IPS has created this log entry:

```
Frame 4: 937 bytes on wire (7496 bits), 937 bytes captured
Ethernet II, Src: HewlettP_82:d8:31, Dst: Cisco_a1:b0:d1
Internet Protocol Version 4, Src: 172.16.22.7, Dst: 10.8.122.244
Transmission Control Protocol, Src Port: 3863, Dst Port: 1433
Application Data: SELECT * FROM users WHERE username='x'
     or 'x'='x' AND password='x' or 'x'='x'
```

Which of the following would describe this log entry?

❍ **A.** Phishing

❍ **B.** Brute force

❍ **C.** SQL injection

❍ **D.** Cross-site scripting

The Answer: C. SQL injection
The SQL injection is contained in the application data. The attacker was attempting to circumvent the authentication through the use of equivalent SQL statements ('x'='x').

The incorrect answers:
A. Phishing
Phishing attempts are a social engineering method of gaining access to private or sensitive information. This example does not appear to contain any private information.

B. Brute force
A brute force attempt would include many failed attempts at a password. This log does not appear to have any repeated password attempts.

D. Cross-site scripting
Cross-site scripting takes advantage of the trust a user has for a site. This example does not appear to take advantage of any previous authentication or trust.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

C26. An incident response team would like to validate their disaster recovery plans without making any changes to the infrastructure. Which of the following would be the best course of action?

❍ **A.** Tabletop exercise

❍ **B.** Hot site fail-over

❍ **C.** Simulation

❍ **D.** Penetration test

The Answer: A. Tabletop exercise
A tabletop exercise is a walk-through exercise where the disaster recovery process can be discussed in a conference room without making any changes to the existing systems.

The incorrect answers:
B. Hot site fail-over
A fail-over to a hot site would involve significant changes to the infrastructure, services, and operations teams.

C. Simulation
A simulation is a useful test of disaster recovery processes, but it often requires a change to the existing systems to properly test the simulated disaster.

D. Penetration test
A penetration test will identify vulnerabilities, but it will not provide any evaluation of the disaster recovery process or policies.

More information:
SY0-601, Objective 4.2 - Incident Response Planning
https://professormesser.link/601040202

C27. A system administrator has installed a new firewall between the corporate user network and the data center network. When the firewall is turned on with the default settings, users complain that the application in the data center is no longer working. Which of the following would be the BEST way to correct this application issue?

❍ **A.** Create a single firewall rule with an explicit deny

❍ **B.** Build a separate VLAN for the application

❍ **C.** Create firewall rules that match the application traffic flow

❍ **D.** Disable spanning tree protocol

The Answer: C. Create firewall rules that match the application traffic flow

By default, firewalls implicitly deny all traffic. Firewall rules must be built that match the traffic flows, and only then will traffic pass through the firewall.

The incorrect answers:

A. Create a single firewall rule with an explicit deny
By default, the firewall has an implicit deny as the last policy in the firewall rulebase. If traffic does not match any other firewall rule, then the implicit deny drops that traffic. Manually configuring an explicit deny doesn't provide any additional traffic control because of the already-existing implicit deny, and it doesn't allow any traffic to pass through the firewall because it's a rule that denies all traffic.

B. Build a separate VLAN for the application
VLAN (Virtual Local Area Network) separation can be used to manage traffic flows or provide additional security options, but a VLAN alone won't bypass an existing firewall deny rule.

D. Disable spanning tree protocol
Spanning tree protocol (STP) is configured on most switches to prevent any layer 2 switching loops. Disabling spanning tree won't bypass any firewall security controls, and it would put the network at risk if a misconfiguration creates a switching loop. A good best practice is to always use STP on a switched network.

More information:
SY0-601, Objective 3.3 - Firewalls
https://professormesser.link/601030306

C28. Which of these would be used to provide HA for a web-based database application?

❍ **A.** SIEM

❍ **B.** UPS

❍ **C.** DLP

❍ **D.** VPN concentrator

The Answer: B. UPS
HA (High Availability) means that the service should always be on and available. The only device on this list that would provide HA is the UPS (Uninterruptible Power Supply). If power is lost, the UPS will provide electricity using battery power or a gas-powered generator.

The incorrect answers:
A. SIEM
A SIEM (Security Information and Event Management) system consolidates data from devices on the network and provides log searching and reporting features. A SIEM does not provide any HA functionality.

C. DLP
DLP (Data Loss Prevention) is a method of identifying and preventing the transfer of personal or confidential information through the network. DLP does not provide any HA functionality.

D. VPN concentrator
A VPN (Virtual Private Network) concentrator is used as an endpoint to an endpoint VPN solution. VPN concentrators do not provide any HA functionality.

More information:
SY0-601, Objective 2.5 - Power Redundancy
https://professormesser.link/601020503

C29. Each year, a certain number of laptops are lost or stolen and must be replaced by the company. Which of the following would describe the total cost the company spends each year on laptop replacements?

❍ **A.** SLE

❍ **B.** SLA

❍ **C.** ALE

❍ **D.** ARO

The Answer: C. ALE

The ALE (Annual Loss Expectancy) is the total amount of the loss over an entire year.

The incorrect answers:

A. SLE

SLE (Single Loss Expectancy) describes the loss for a single incident.

B. SLA

SLA (Service Level Agreement) is a contractual agreement that specifies a minimum service level.

D. ARO

An ARO (Annualized Rate of Occurrence) is the number of times an event is expected to occur in a year.

More information:

SY0-601, Objective 5.4 - Risk Analysis

https://professormesser.link/601050402

C30. A network administrator is viewing a log file from a web server:

```
https://www.example.com/?s=/Index/think/
app/invokefunction&function=call_user_func_
array&vars[0]=md5&vars[1][0]=__HelloThinkPHP
```

Which of the following would be the BEST way to prevent this attack?

❍ **A.** Static code analyzer

❍ **B.** Input validation

❍ **C.** Allow list

❍ **D.** Secure cookies

The Answer: B. Input validation
In this example, the attacker is attempting to use a remote code execution vulnerability. Input validation can be used to create a very specific filter of allowed input, and a strict validation process would have prevented the web server from processing this attack information.

The incorrect answers:
A. Static code analyzer
A static code analyzer is useful when evaluating the security of existing source code. In this example, the input is dynamic and is initiated by the attacker.

C. Allow list
An allow list would limit user access to an application, but it would not limit the type of input from the users.

D. Secure cookies
Secure cookies ensure that the information contained in the browser cookie is encrypted and only viewable by the end user. Secure cookies would not prevent a remote code execution attack.

More information:
SY0-601, Objective 3.2 - Application Security
https://professormesser.link/601030204

C31. Sam, a user in the purchasing department, would like to send an email to Jack. Which of these would allow Jack to verify the sender of the email?

- ❍ **A.** Digitally sign it with Sam's private key
- ❍ **B.** Digitally sign it with Sam's public key
- ❍ **C.** Digitally sign it with Jack's private key
- ❍ **D.** Digitally sign it with Jack's public key

The Answer: A. Digitally sign it with Sam's private key
The sender of a message digitally signs with their own private key to ensure integrity, authentication, and non-repudiation of the signed contents. The digital signature is validated with the sender's public key.

The incorrect answers:
B. Digitally sign it with Sam's public key
Since everyone effectively has access to public keys, adding a digital signature with a publicly available key doesn't provide any security features.

C. Digitally sign it with Jack's private key
Jack's private key would only be available to Jack, so Sam could not possibly use Jack's private key when performing any cryptographic functions.

D. Digitally sign it with Jack's public key
As with Sam's public key that would be available to anyone, using Jack's public key would not provide any security features.

More information:
SY0-601, Objective 2.8 - Hashing and Digital Signatures
https://professormesser.link/601020803

C32. The contract of a long-term temporary employee is ending. Which of these would be the MOST important part of the off-boarding process?

❍ **A.** Perform an on-demand audit of the user's privileges

❍ **B.** Archive the decryption keys associated with the user account

❍ **C.** Document the user's outstanding tasks

❍ **D.** Obtain a signed copy of the Acceptable Use Policies

The Answer: B. Archive the decryption keys associated with the user account

Without the decryption keys, it will be impossible to access any of the user's protected files once they leave the company. Given the other possible answers, this one is the only one that would result in unrecoverable data loss if not properly followed.

The incorrect answers:

A. Perform an on-demand audit of the user's privileges
The user's account will be disabled once they leave the organization, so an audit of their privileges would not be very useful.

C. Document the user's outstanding tasks
Creating documentation is important, but it's not as important as retaining the user's data with the decryption keys.

D. Obtain a signed copy of the Acceptable Use Policies
Acceptable Use Policies (AUPs) are usually signed during the on-boarding process. You won't need an AUP if the user is no longer accessing the network.

More information:
SY0-601, Objective 5.3 - Personnel Security
https://professormesser.link/601050301

C33. Daniel, a cybersecurity analyst, has been asked to respond to a denial of service attack against a web server. Daniel first collects information in the ARP cache, then a copy of the server's temporary file system, and finally system logs from the web server. What part of the forensics gathering process did Daniel follow?

❍ **A.** Chain of custody

❍ **B.** Data hashing

❍ **C.** Legal hold

❍ **D.** Order of volatility

The Answer: D. Order of volatility
Order of volatility ensures that data will be collected before it becomes unrecoverable. For example, information stored in a router table is more volatile than data stored on a backup tape, so the router table data will be collected first and the backup tape data will be collected second.

The incorrect answers:
A. Chain of custody
Chain of custody ensures that the integrity of evidence is maintained. The contents of the evidence are documented, and each person who contacts the evidence is required to document their activity.

B. Data hashing
Data hashing creates a unique message digest based on stored data. If the data is tampered with, a hash taken after the change will differ from the original value. This allows the forensic engineer to identify that information has been changed.

C. Legal hold
A legal hold is a legal technique to preserve relevant information. This will ensure the data remains accessible for any legal preparation that needs to occur prior to litigation.

More information:
SY0-601, Objective 4.5 - Forensics Data Acquisition
https://professormesser.link/601040502

C34. An attacker was able to download ten thousand company employee login credentials containing usernames and hashed passwords. Less than an hour later, a list containing all ten thousand usernames and passwords in plain text were posted to an online file storage repository. Which of the following would BEST describe how this attacker was able to post this information?

❍ **A.** Improper certificate management

❍ **B.** Phishing

❍ **C.** Untrained users

❍ **D.** Weak cipher suite

The Answer: D. Weak cipher suite

Creating a password hash is a one-way process that can't be reversed. If the hash has not been salted, then a rainbow table lookup would be an easy way to find the plaintext passwords. Since none of the answers in this question included rainbow tables as an option, the most reasonable of the remaining choices would be a weak cipher suite that allowed for a very fast brute force attack of the password hashes.

The incorrect answers:

A. Improper certificate management

As a best practice, passwords are never stored or transmitted as plain text or in a form that could be recovered to plain text. If a certificate was mis-managed, the attacker might be able to decode network traffic or perform on-path attacks. However, they would not be able to view a user's password, since those passwords are already hashed. Since all ten thousand accounts were downloaded, it's unlikely the attacker collected them one user at a time over the network.

B. Phishing

Phishing is a useful attack for gathering information from one user at a time, but it doesn't scale when you need to collect data from ten thousand accounts.

C. Untrained users

Individual users might accidentally disclose their password information, but you would not expect ten thousand users to perform the same security breach simultaneously.

More information:

SY0-601, Objective 1.6 - Vulnerability Types

https://professormesser.link/601010601

C35. A security administrator is researching the methods used by attackers to gain access to web servers. Which of the following would provide additional information about these techniques?

❍ **A.** IPS

❍ **B.** Hashing

❍ **C.** Obfuscation

❍ **D.** Honeypot

The Answer: D. Honeypot
A honeypot simulates a production environment without putting any of the production data at risk. As attackers attempt to exploit the honeypot, their techniques and methods are logged. With these logs, administrators can gain additional insights into the attacks and processes used by the attackers.

The incorrect answers:
A. IPS
An IPS would identify known attacks against an application or device, but it would not provide any proactive identification or detailed security information.

B. Hashing
Hashing can be used as an integrity check, but it's not used to obtain information about an attack.

C. Obfuscation
Obfuscation is the process of making something difficult for humans to read or understand. Obfuscation does not provide any additional information about attack methods or techniques.

More information:
SY0-601, Objective 2.1 - Honeypots and Deception
https://professormesser.link/601020106

C36. A server administrator is building a new web server and needs to provide operating system access to the web server executable. Which of the following account types should be configured?

❍ **A.** User

❍ **B.** Privileged

❍ **C.** Service

❍ **D.** Guest

The Answer: C. Service
A service account is commonly used by local services on a system, but service accounts are not generally enabled for interactive logins. Web servers, database servers, and other local servers use service accounts.

The incorrect answers:
A. User
A user account is associated with an interactive user or person. Because user accounts have additional functionality over service accounts, the best practice is to avoid assigning user account access to a service.

B. Privileged
A privileged account is an Administrator or root account, and it generally has complete access to the operating system. This should be your most protected account type, and you would not associate a privileged account to a service.

D. Guest
A guest account often has very limited operating system access, so it would not be a useful account type to use for a service.

More information:
SY0-601, Objective 3.7 - Account Types
https://professormesser.link/601030702

C37. A company is implementing a series of automated processes when responding to a security event. Which of the following would provide a linear checklist of steps to perform?

❍ **A.** MDM

❍ **B.** DLP

❍ **C.** Runbook

❍ **D.** Zero trust

The Answer: C. Runbook
A runbook is a set of steps required to complete a task. An example of a runbook would be the process of resetting a password, creating a website certificate, or backing up application data.

The incorrect answers:

A. MDM
An MDM (Mobile Device Manager) provides management and configuration of remote devices. An MDM does not provide a list of processes.

B. DLP
DLP (Data Loss Prevention) is a security solution for identifying and blocking the transfer of sensitive information across the network. A DLP would not provide a checklist of security tasks.

D. Zero trust
Zero trust is a security philosophy that considers all devices to be untrusted. Inherent trust and trusted connections between devices are not part of a zero trust model. Zero trust does not provide linear checklists for security tasks.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

C38. A transportation company maintains a scheduling application and a database in a virtualized cloud-based environment. Which of the following would be the BEST way to backup these services?

❍ **A.** Full

❍ **B.** Snapshot

❍ **C.** Differential

❍ **D.** Incremental

The Answer: B. Snapshot
Virtual machines (VMs) have a snapshot backup feature that can capture both a full backup of the virtual system and incremental changes that occur over time. It's common to take a snapshot of a VM for backup purposes and before making any significant changes to the VM. If the changes need to be rolled back, a previous snapshot can be selected and instantly applied to the VM.

The incorrect answers:
A. Full
A full backup is used to copy every file system object to the backup media. To restore the operating system, the entire full backup session would be restored to the file system. In a virtual environment, a partition of a virtual machine is stored as a single file, so it's much easier to back up that single file as a snapshot than backing up the individual files that are stored inside of that virtual partition.

C. Differential
A differential backup will copy all files that have been changed since the last full backup. As mentioned above, using the snapshot feature of a VM is much more efficient than copying individual files in the file system.

D. Incremental
An incremental backup will copy all files that have been changed since the last incremental backup. The VM's snapshot feature is much more efficient way to backup and restore incremental changes to a virtual machine.

More information:
SY0-601, Objective 2.5 - Resiliency
https://professormesser.link/601020506

C39. In an environment using discretionary access controls, which of these would control the rights and permissions associated with a file or directory?

❍ **A.** Administrator

❍ **B.** Owner

❍ **C.** Group

❍ **D.** System

The Answer: B. Owner
The owner of an object is the one who controls access in a discretionary access control model. The object and type of access is at the discretion of the owner, and they can determine who can access the file and the type of access they would have.

The incorrect answers:
A. Administrator
Administrators generally label objects when using mandatory access control, but they are not involved with discretionary access control.

C. Group
Assigning rights and permissions to a group and then assigning users to the group are common when using role-based access control.

D. System
The system does not determine individual user rights and permissions when using discretionary access control.

More information:
SY0-601, Objective 3.8 - Access Control
https://professormesser.link/601030805

C40. A security administrator has installed a network-based DLP solution to determine if file transfers contain PII. Which of the following describes the data during the file transfer?

❍ **A.** In-use

❍ **B.** In-transit

❍ **C.** At-rest

❍ **D.** Highly available

The Answer: B. In-transit
Data in-transit is data that is in the process of moving across the network. As the information passes through switches and routers, it is considered to be in-transit.

The incorrect answers:

A. In-use
Data in-use is in the memory of a system and is accessible to an application.

C. At-rest
Data at-rest resides on a storage device.

D. Highly available
High availability (HA) is usually associated with redundancy or fault-tolerance. Data moving through the network would not be considered highly available.

More information:
SY0-601, Objective 2.1 - Protecting Data
https://professormesser.link/601020102

C41. A medical imaging company would like to connect all remote locations together with high speed network links. The network connections must maintain high throughput rates and must always be available during working hours. In which of the following should these requirements be enforced with the network provider?

❍ **A.** Service level agreement

❍ **B.** Memorandum of understanding

❍ **C.** Non-disclosure agreement

❍ **D.** Acceptable use policy

The Answer: A. Service level agreement
A service level agreement (SLA) is used to contractually define the minimum terms for services. In this example, the medical imaging company would require an SLA from the network provider for the necessary throughput and uptime metrics.

The incorrect answers:
B. Memorandum of understanding
A memorandum of understanding (MOU) is an informal letter of intent. The MOU is not a signed contract, and there are no contractual obligations associated with the content of an MOU.

C. Non-disclosure agreement
A non-disclosure agreement (NDA) is used between entities to prevent the use and dissemination of confidential information.

D. Acceptable use policy
An acceptable use policy (AUP) commonly details the rules of behavior for employees using an organization's network and computing resources.

More information:
SY0-601, Objective 5.3 - Third-Party Risk Management
https://professormesser.link/601050302

C42. A security administrator would like to encrypt all telephone communication on the corporate network. Which of the following protocols would provide this functionality?

❍ **A.** TLS

❍ **B.** SRTP

❍ **C.** SSH

❍ **D.** S/MIME

The Answer: B. SRTP
SRTP (Secure Real-Time Transport Protocol) is an encrypted version of the RTP (Real-Time Transport Protocol) VoIP (Voice over IP) protocol. SRTP uses AES (Advanced Encryption Standard) to encrypt the voice and video over a VoIP connection.

The incorrect answers:
A. TLS
TLS (Transport Layer Security) is the modern version of SSL (Secure Sockets Layer), and it's commonly used for encrypting communication to a web server.

C. SSH
SSH (Secure Shell) is used to encrypt terminal communication. The best practice is to use SSH instead of the insecure Telnet protocol.

D. S/MIME
S/MIME (Secure/Multipurpose Internet Mail Extensions) provides security for the content of an email message.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

C43. A security administrator is preparing a phishing email that will be sent to employees as part of a periodic security test. The email is spoofed to appear as an unknown third-party and asks employees to immediately click a link or their state licensing will be revoked. Which of these social engineering principles are used by this email?

❍ **A.** Familiarity

❍ **B.** Social Proof

❍ **C.** Authority

❍ **D.** Urgency

The Answer: D. Urgency
The need to complete this task as quickly as possible (immediately) is the primary social engineering principle in this description. Any task that encourages a person to act quickly (instead of thinking about it) is associated with urgency.

The incorrect answers:
A. Familiarity
If the email making this request was from someone we knew, then the social engineering principle of familiarity would be included. In this example, the email was from an unknown third-party.

B. Social Proof
Social proof encourages action by convincing the user that this is normally expected. If the email stated that others have completed this task in the past, social proof would imply that it's perfectly acceptable for you to complete this task as well.

C. Authority
In this example, the request was made by an unknown third-party. If the request was from someone at a higher level in the company, then the social engineering principle of authority would be used.

More information:
SY0-601, Objective 1.1 - Principles of Social Engineering
https://professormesser.link/601010110

C44. A security administrator would like to minimize the number of certificate status checks made by web site clients to the certificate authority. Which of the following would be the BEST option for this requirement?

❍ **A.** OCSP stapling

❍ **B.** Certificate chaining

❍ **C.** CRL

❍ **D.** Certificate pinning

The Answer: A. OCSP stapling

OCSP (Online Certificate Status Protocol) stapling allows the certificate holder verify their own certificate status. The OCSP status is commonly "stapled" into the SSL handshake process. Instead of contacting the certificate authority to verify the certificate, the verification is included with the initial network connection to the server.

The incorrect answers:

B. Certificate chaining

Intermediate certificates are often listed in a "chain" between a web server's SSL certificate and the root certificate. It's important to configure web servers with the proper chain, or the end user may receive an error in their browser that the server can't be trusted. A certificate chain does not provide the end station with any revocation information.

C. CRL

A CRL (Certificate Revocation List) is a list of revoked certificates that is maintained by the certificate authority. To view the CRL, an end-user client would directly access the CA.

D. Certificate pinning

Certificate pinning embeds or "pins" a certificate inside of an application. When the application contacts a service, the service certificate will be compared to the pinned certificate. If the certificates match, the application knows that it can trust the service. If the certificates don't match, then the application can choose to shut down, show an error message, or make the user aware of the discrepancy. Certificate pinning does not necessarily provide any revocation checks.

More information:

SY0-601, Objective 3.9 - Certificate Concepts

https://professormesser.link/601030904

C45. A company is concerned their EDR solution will not be able to stop more advanced ransomware variants. Technicians have created a backup and restore utility that will get most systems up and running less than an hour after an attack. What type of security control is associated with this restore process?

○ **A.** Managerial

○ **B.** Compensating

○ **C.** Preventive

○ **D.** Detective

The Answer: B. Compensating
Instead of preventing an attack, a compensating control is used to restore systems using other means. A streamlined backup and restore process compensates for the limited security features of the EDR (Endpoint Detection and Response) software.

The incorrect answers:
A. Managerial
Managerial controls are policies that determine how processes should be followed, but they won't provide a method for recovering from a ransomware infection.

C. Preventive
A preventive control will block access. The EDR software on a workstation is an example of a preventive control.

D. Detective
A detective control may not be able to block an attack, but it can identify and alert if an attack is underway.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

C46. To upgrade an internal application, the development team provides the operations team with a patch and instructions for backing up, patching, and reverting the patch if needed. The operations team schedules a date for the upgrade, informs the business divisions, and tests the upgrade process after completion. Which of the following describes this process?

❍ **A.** Agile

❍ **B.** Continuity planning

❍ **C.** Usage auditing

❍ **D.** Change management

The Answer: D. Change management

Change management is the process for making any type of change. This could be a software upgrade, a hardware replacement, or any other type of modification to the existing environment. Having a formal change management process minimizes the risk of a change and makes everyone aware of the changes as they occur.

The incorrect answers:

A. Agile

Agile is a systems development life cycle model that focuses on creating content as quickly as possible and refining the content until the final product is complete.

B. Continuity planning

Continuity planning focuses on keeping the business running when a disruption occurs. Disaster recovery planning is a type of continuity plan.

C. Usage auditing

Usage auditing is used to determine how resources are used. For example, a system administrator may perform a usage audit to determine which resources are used with a particular application or service.

More information:

SY0-601, Objective 5.3 - Organizational Policies

https://professormesser.link/601050305

C47. A company is implementing a public file-storage and cloud-based sharing service, but does not want to build a separate authentication front-end. Instead, the company would like users to authenticate with an existing account on a trusted third-party web site. Which of the following should the company implement?

○ **A.** SSO

○ **B.** Federation

○ **C.** Transitive trust

○ **D.** X.509 certificates signed by a trusted CA

The Answer: B. Federation
Federation provides a way to authenticate and authorize between two entities using a separate trusted authentication platform. For example, a web site could allow authentication using an existing account on a third-party social media site.

The incorrect answers:
A. SSO
SSO (Single Sign-On) does not inherently require authentication to be processed by a third-party. SSO allows a user to authenticate one time and gain access to all assigned resources. No additional authentication is required after the initial SSO login process is complete.

C. Transitive trust
A transitive trust states that if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A trusts Domain C. This trust relationship is not associated with the authentication process that occurs in any of these domains.

D. X.509 certificates signed by a trusted CA
Assigning a certificate to each user or device is commonly used as an authentication factor, and this would require the company to implement some type of authentication process to create and assign certificates.

More information:
SY0-601, Objective 2.4 - Authentication Methods
https://professormesser.link/601020401

C48. A system administrator is viewing this output from Microsoft's System File Checker:

```
15:43:01 - Repairing corrupted file C:\Windows\System32\kernel32.dll
15:43:03 - Repairing corrupted file C:\Windows\System32\netapi32.dll
15:43:07 - Repairing corrupted file C:\Windows\System32\user32.dll
15:43:43 - Repair complete
```

Which of the following malware types is the MOST likely cause of this output?

❍ **A.** RAT

❍ **B.** Logic bomb

❍ **C.** Rootkit

❍ **D.** Bot

The Answer: C. Rootkit
A rootkit modifies operating system files to become part of the core OS. The kernel, user, and networking libraries in Windows are core operating system files.

The incorrect answers:
A. RAT
A RAT (Remote Access Trojan) is a remote administration tool that installs itself as a service or application on the host computer. RATs do not commonly modify core operating system files.

B. Logic bomb
A logic bomb waits for a predefined event to begin operation. Logic bombs do not commonly modify core operating system files.

D. Bot
Bot (robot) malware infects devices to make them part of a larger network of bots. These infections do not commonly modify core operating system files.

More information:
SY0-601, Objective 1.2 - Rootkits
https://professormesser.link/601010205

C49. What type of vulnerability would be associated with this log information?

```
GET http://example.com/show.asp?view=../../Windows/
     system.ini HTTP/1.1
```

❍ **A.** Buffer overflow

❍ **B.** Directory traversal

❍ **C.** DoS

❍ **D.** Cross-site scripting

The Answer: B. Directory traversal
Directory traversal attempts to read or access files that are outside the scope of the web server's file directory. The pair of dots in a file path (..) refers to the parent directory, so this example is attempt to move back two parent directories before proceeding into the /Windows directory. In a properly configured web server, this traversal should not be possible.

The incorrect answers:
A. Buffer overflow
A buffer overflow would attempt to store information into an area of memory that overflows the boundary of the buffer. The information in the log does not show any overflow attempt.

C. DoS
A DoS (Denial of Service) is designed to make a system or service unavailable. Although running any unknown command can be unpredictable, it would be unusual for a these commands to cause any downtime.

D. Cross-site scripting
A cross-site scripting attack would normally include a script that would reference another site that was trusted by the browser. In this example, the commands appear to be related to the existing URL and not a third-party site.

More information:
SY0-601, Objective 1.3 - Other Application Attacks
https://professormesser.link/601010310

C50. A developer has created an application that will store password information in a database. Which of the following BEST describes a way of protecting these credentials by adding random data to the password?

❍ **A.** Hashing

❍ **B.** PFS

❍ **C.** Salting

❍ **D.** Asymmetric encryption

The Answer: C. Salting
Passwords are often stored as hashes, but the hashes themselves are often subject to brute force or rainbow table attacks. It's common to add some additional random data (a salt) to a password before the hashing process. This ensures that each password is truly random when stored, and it makes it more difficult for an attacker to discover all of the stored passwords.

The incorrect answers:
A. Hashing
Hashing is a one-way cryptographic function that takes an input, such as a password, and creates a fixed size string of random information. The process of adding additional information to the original data before the hashing process is called salting.

B. PFS
PFS (Perfect Forward Secrecy) is a method of encryption that uses temporary session keys for the encryption and decryption process. Once the encrypted communication is complete, the session keys are discarded. PFS is not used to add additional random information to a password hashing process.

D. Asymmetric encryption
Asymmetric encryption is an encryption method that uses one key for encryption and a different key for decryption. Asymmetric encryption does not add additional random information to a hash.

More information:
SY0-601, Objective 3.2 - Database Security
https://professormesser.link/601030203

C51. Which of the following processes merges developed code, tests for issues, and automatically moves the newly developed application to production without any human intervention?

❍ **A.** Continuous deployment

❍ **B.** Continuity of operations

❍ **C.** Continuous delivery

❍ **D.** Continuous integration

The Answer: A. Continuous deployment
Continuous deployment automates every aspect of deploying software. After the developer creates the code, the testing and deployment process is completely hands-off and does not need any human intervention.

The incorrect answers:
B. Continuity of operations
Continuity of operations is used during disaster recovery or incident recovery. This process provides options for keeping the business processes available during or after the incident.

C. Continuous delivery
Continuous delivery automates the testing process, but it requires human intervention for the final deployment to production.

D. Continuous integration
With continuous integration, code is constantly written and merged into the central repository many times each day.

More information:
SY0-601, Objective 2.3 - Automation and Scripting
https://professormesser.link/601020305

C52. Which of the following BEST describes a risk matrix?

❍ **A.** A visual summary of a risk assessment

❍ **B.** Identification of risk at each step of a project plan

❍ **C.** A list of cybersecurity requirements based on the identified risks

❍ **D.** Ongoing group discussions regarding cybersecurity

The Answer: A. A visual summary of a risk assessment
A risk matrix, or risk heat map, is often presented as a graphical chart comparing the likelihood of risk with the consequence.

The incorrect answers:
B. Identification of risk at each step of a project plan
A risk register is a detailed identification and documentation of risk, the application of possible solutions, and ongoing monitoring of the risk at each step of a project.

C. A list of cybersecurity requirements based on the identified risks
Risk control assessment provides a security administrator with the information needed to build proper security controls for the documented risk.

D. Ongoing group discussions regarding cybersecurity
Risk awareness involves constant monitoring and analysis of current trends, risks, and response options. This information can be gathered from group discussions, expert presentations, and security conferences and programs.

More information:
SY0-601, Objective 5.4 - Risk Analysis
https://professormesser.link/601050402

C53. A security administrator would like to implement an authentication system that uses cryptographic tickets to validate users. Which of the following would provide this functionality?

❍ **A.** RADIUS

❍ **B.** LDAP

❍ **C.** Kerberos

❍ **D.** TACACS

The Answer: C. Kerberos

Kerberos is a network authentication protocol that provides single sign-on and mutual authentication using cryptographic "tickets" for the behind-the-scenes authentication process.

The incorrect answers:

A. RADIUS

The RADIUS (Remote Authentication Dial-in User Service) authentication protocol is commonly used across many different devices and operating systems, but it does not use cryptographic tickets.

B. LDAP

LDAP (Lightweight Directory Access Protocol) is another common standard that is often used for authentication, but LDAP does not use cryptographic tickets.

D. TACACS

TACACS (Terminal Access Controller Access-Control System) is a flexible remote authentication protocol, but it does not use cryptographic tickets during the authentication process.

More information:

SY0-601, Objective 3.8 - Identity and Access Services

https://professormesser.link/601030803

C54. Richard is reviewing this information from an IPS log:

```
MAIN_IPS: 22June2019 09:02:50 reject 10.1.111.7
Alert: HTTP Suspicious Webdav OPTIONS Method Request; Host: Server
Severity: medium; Performance Impact:3;
Category: info-leak; Packet capture; disable
Proto:tcp; dst:192.168.11.1; src:10.1.111.7
```

Which of the following can be associated with this log information? (Select TWO)

❍ **A.** The attacker sent a non-authenticated BGP packet to trigger the IPS

❍ **B.** The source of the attack is 192.168.11.1

❍ **C.** The event was logged but no packets were dropped

❍ **D.** The source of the attack is 10.1.111.7

❍ **E.** The attacker sent an unusual HTTP packet to trigger the IPS

The Answer: D. The source of the attack is 10.1.111.7 and
E. The attacker sent an unusual HTTP packet to trigger the IPS

The second line of the IPS log shows the type of alert, and this record indicates that a suspicious HTTP packet was sent. The last line of the IPS log shows the protocol, destination, and source IP address information. The source IP address is 10.1.111.7.

The incorrect answers:

A. The attacker sent a non-authenticated BGP packet to trigger the IPS
The alert for this IPS log does not indicate any non-authenticated packets or BGP packets.

B. The source of the attack is 192.168.11.1
The last line of the log identifies the protocol and IP addresses. The "src" address is the source of the packet and is identified as 10.1.111.7.

C. The event was logged but no packets were dropped
The first line of the log shows the name of the IPS that identified the issue, the date and time, and disposition. In this log entry, the packet was rejected from IP address 10.1.111.7.

More information:
SY0-601, Objective 4.3 - Log Files
https://professormesser.link/601040303

C55. A company has contracted with a third-party to provide penetration testing services. The service includes a port scan of each externally-facing device. This is an example of:

❍ **A.** Initial exploitation

❍ **B.** Escalation of privilege

❍ **C.** Pivot

❍ **D.** Active footprinting

The Answer: D. Active footprinting
Active footprinting sends traffic across the network that can be viewed and/or logged. Performing a port scan will send network traffic to a server, and most port scan attempts can be identified and logged by an IPS.

The incorrect answers:
A. Initial exploitation
An exploit attempt is common when performing a penetration test, but a port scan is not exploiting any vulnerabilities.

B. Escalation of privilege
If a penetration test is able to exploit a system and obtain a higher level of rights and permissions, then the test is successful at escalating the access privileges. A port scan does not gain access to a system, and it will not provide any privilege escalation.

C. Pivot
Once a penetration test has exploited a vulnerability and gained access to a system, the tester will use this foothold as a pivot point to access to other devices. Since the inside of the network is usually less secure than the perimeter, this pivot can often provide many more opportunities than the initial exploitation.

More information:
SY0-601, Objective 1.8 - Reconnaissance
https://professormesser.link/601010802

C56. An access point in a corporate headquarters office has the following configuration:

```
IP address: 10.1.10.1
Subnet mask: 255.255.255.0
DHCPv4 Server: Enabled
SSID: Wireless
Wireless Mode: 802.11g
Security Mode: WEP-PSK
Frequency band: 2.4 GHz
Software revision: 2.1
MAC Address: 60:3D:26:71:FF:AA
IPv4 Firewall: Enabled
```

Which of the following would apply to this configuration?

❍ **A.** Invalid frequency band

❍ **B.** Weak encryption

❍ **C.** Incorrect IP address and subnet mask

❍ **D.** Invalid software version

The Answer: B. Weak encryption
A common issue is weak or outdated security configurations. Older encryptions such as DES and WEP should be updated to use newer and stronger encryption technologies.

The incorrect answers:
A. Invalid frequency band
The 2.4 GHz frequency band is a valid frequency range for 802.11g networks.

C. Incorrect IP address and subnet mask
None of the listed configuration settings show any issues with the IP address or subnet mask.

D. Invalid software version
The software version of the access point does not have any configuration options and would not be considered invalid.

More information:
SY0-601, Objective 1.6 - Vulnerability Types
https://professormesser.link/601010601

C57. An application does not properly release unused memory, and eventually it grows so large that it uses all available memory. Which of the following would describe this issue?

❍ **A.** Integer overflow

❍ **B.** NULL pointer dereference

❍ **C.** Memory leak

❍ **D.** Data injection

The Answer: C. Memory leak
A memory leak is when a poorly written application allocates memory for use by the application, but then does not release that memory after it is no longer needed. If the application runs on a system for an extended period of time, this memory leak can grow so large that it eventually uses all available memory and crashes the operating system.

The incorrect answers:

A. Integer overflow
An integer overflow attempts to store a large number into a smaller sized memory space. This can sometimes improperly change the value of memory areas that are outside of the smaller space.

B. NULL pointer dereference
If an application is written to reference a portion of memory, but nothing is currently allocated to that area of memory, a NULL pointer dereference will occur. This can cause the application to crash, display debug information, or create a denial of service (DoS).

D. Data injection
The unwanted injection of data into a database, library, or any other data flow is an injection attack. An application that does not properly release sections of memory is a badly written application and would not be related to a data injection attack.

More information:
SY0-601, Objective 1.3 - Other Application Attacks
https://professormesser.link/601010310

C58. A company is receiving complaints of slowness and disconnections to their Internet-facing web server. A network administrator monitors the Internet link and finds excessive bandwidth utilization from thousands of different IP addresses. Which of the following would be the MOST likely reason for these performance issues?

❍ **A.** DDoS

❍ **B.** Wireless jamming

❍ **C.** MAC cloning

❍ **D.** Rogue access point

The Answer: A. DDoS
A DDoS (Distributed Denial of Service) is the failure of a service caused by many different remote devices. In this example, the DDoS is related to a bandwidth utilization exhaustion caused by excessive server requests.

The incorrect answers:
B. Wireless jamming
Wireless jamming is caused by interference of the wireless spectrum. In this example, a wireless network was not part of the web server or any issues associated with the server.

C. MAC cloning
MAC (Media Access Control) address cloning is when a third-party device changes their MAC address to be the same as another station. In this example, the issue is related to a large number of inbound IP addresses.

D. Rogue access point
A rogue access point is an unauthorized wireless access point. This issue does not appear to be related to a wireless network.

More information:
SY0-601, Objective 1.4 - Denial of Service
https://professormesser.link/601010410

C59. A penetration tester is researching a company using information gathered from user profiles and posts on a social media site. Which of the following would describe this activity?

❍ **A.** Pivot

❍ **B.** Passive footprinting

❍ **C.** White box testing

❍ **D.** Persistence

The Answer: B. Passive footprinting

Passive footprinting gathers information from as many open sources as possible without performing any vulnerability checks or scans. Passive footprinting would include gathering information from social media, online forums, or social engineering.

The incorrect answers:

A. Pivot

Once an exploit is successful, the attacker will use an exploited system as a foothold point and pivot to other parts of the network from this point.

C. White box testing

Prior to performing a penetration test, an attacker may already have information about the target network. If information on all of the devices in the scope of the penetration test are made available to the attacker, the test is considered to be a white box penetration test.

D. Persistence

If a system has been exploited, it's common for the attacker to create a normal user account or backdoor to maintain access if the vulnerability becomes patched.

More information:

SY0-601, Objective 1.8 - Reconnaissance

https://professormesser.link/601010802

C60. A system administrator is configuring an IPsec VPN to a remote location and would like to ensure that the VPN provides confidentiality for both the original IP header and the data. Which of the following should be configured on the VPN?

❍ **A.** ECB

❍ **B.** AH

❍ **C.** PEAP

❍ **D.** HMAC

❍ **E.** ESP

The Answer: E. ESP
ESP (Encapsulation Security Payload) encrypts the data in the IP packet. In IPsec (Internet Protocol Security) transport mode, the IP header is not encrypted and is used for routing. In tunnel mode, both the original IP header and data are encrypted and encapsulated within a separate IP header.

The incorrect answers:

A. ECB
ECB (Electronic Codebook) is a block cipher mode where each block is encrypted with the same key. For IPsec (and most use cases), ECB is too simple to ensure data confidentiality.

B. AH
The AH (Authentication Header) contains a hash of the IPsec packet to provide integrity protection of the data. The AH does not encrypt data.

C. PEAP
PEAP (Protected Extensible Authentication Protocol) is an authentication protocol that encapsulates EAP in a TLS (Transport Layer Security) tunnel to ensure a protected authentication process. PEAP is not used to protect IPsec data.

D. HMAC
HMAC (Hash-based Message Authentication Code) is a hashing algorithm commonly used with the AH field of IPsec. HMAC does not provide any data confidentiality.

More information:
SY0-601, Objective 3.1 - Secure Protocols
https://professormesser.link/601030101

C61. Which of these cloud deployment models would BEST describe a company that would build a cloud for their own use and use systems and storage platforms in their data center?

❍ **A.** Private

❍ **B.** Community

❍ **C.** Hybrid

❍ **D.** Public

The Answer: A. Private
A private model requires that the end user purchase, install, and maintain their own application hardware and software. This model also provides a high level of security.

The incorrect answers:
B. Community
A community cloud model allows multiple organizations to share the same cloud resources. A cloud built in a company data center for personal use would not provide any community cloud features.

C. Hybrid
A hybrid cloud model combines both private and public cloud infrastructures. The description provided in the question does not include any public resources.

D. Public
A public cloud is built on an infrastructure that would be open to all users on the Internet.

More information:
SY0-601, Objective 2.2 - Cloud Models
https://professormesser.link/601020201

C62. Which of the following malware types would cause a workstation to participate in a DDoS?

❍ **A.** Bot

❍ **B.** Logic bomb

❍ **C.** Ransomware

❍ **D.** Keylogger

The Answer: A. Bot
A bot (robot) is malware that installs itself on a system and then waits for instructions. It's common for botnets to use thousands of bots to perform DDoS (Distributed Denial of Service) attacks.

The incorrect answers:
B. Logic bomb
A logic bomb waits for a predefined event to occur. The scope of devices infected with a logic bomb are relatively small and localized as compared to a botnet.

C. Ransomware
Ransomware locks a system and prevents it from operating. The locked device does not commonly participate in a DDoS.

D. Keylogger
A keylogger will silently capture keystrokes and transmit an archive of those keystrokes to a third-party. A keylogger does not commonly participate in a DDoS.

More information:
SY0-601, Objective 1.2 - Bots and Botnets
https://professormesser.link/601010207

C63. Which of these are used to force the preservation of data for later use in court?

❍ **A.** Chain of custody

❍ **B.** Data loss prevention

❍ **C.** Legal hold

❍ **D.** Order of volatility

The Answer: C. Legal hold
A legal hold is a legal technique to preserve relevant information. This process will ensure the data remains accessible for any legal preparation that occurs prior to litigation.

The incorrect answers:
A. Chain of custody
Chain of custody ensures that the integrity of evidence is maintained. The contents of the evidence are documented, and each person who contacts the evidence is required to document their activity.

B. Data loss prevention
Data loss prevention (DLP) is a technique for identifying sensitive information transmitted across the network, such as Social Security numbers, credit card numbers, and other PII (Personally Identifiable Information). DLP is not a legal technique.

D. Order of volatility
The order of volatility is a list of how long data will remain available before it is unrecoverable. For example, information stored in a router table is more volatile than data stored on a backup tape.

More information:
SY0-601, Objective 4.5 - Digital Forensics
https://professormesser.link/601040501

C64. A network administrator is installing a series of access points in a public library. Which of the following would be the BEST way to prevent theft of his laptop while performing this work?

❍ **A.** Biometrics

❍ **B.** Cable lock

❍ **C.** Protected distribution

❍ **D.** Faraday cage

The Answer: B. Cable lock
A cable lock would attach the laptop to a solid object and prevent it from being moved or taken.

The incorrect answers:
A. Biometrics
Biometrics can provide a useful authentication factor, but they won't stop a laptop from moving.

C. Protected distribution
A protected distribution describes a hardened series of conduits for network cable and fiber. A protected distribution would not prevent a laptop from being stolen.

D. Faraday cage
A Faraday cage prevents the transmission of electromagnetic signals. Using a Faraday cage around a laptop would not prevent laptop theft.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

C65. A company would like to install an IPS to observe normal network activity and block any traffic that deviates from this baseline. Which of these IPS types would be the BEST fit for this requirement?

❍ **A.** Heuristic

❍ **B.** Anomaly-based

❍ **C.** Behavior-based

❍ **D.** Signature-based

The Answer: B. Anomaly-based
Anomaly-based detection will build a baseline of what it considers to be normal. Once the baseline is established, the IPS (Intrusion Prevention System) will then block any traffic that deviates from the baseline.

The incorrect answers:
A. Heuristic
Heuristic IPS technology uses artificial intelligence to identify attacks that have no prior signature.

C. Behavior-based
Behavior-based IPS technology will alert if a particular type of bad behavior occurs. For example, a URL with an apostrophe and SQL command would indicate a SQL injection, and someone trying to view /etc/shadow would indicate an attempt to gain access to a protected part of the file system. This is universally considered to be bad behavior, and it would be flagged by a behavior-based IPS.

D. Signature-based
A signature-based IPS is looking for a specific traffic flow pattern, and once that traffic matches the signature the traffic can be blocked.

More information:
SY0-601, Objective 3.3 - Intrusion Prevention
https://professormesser.link/601030309

C66. A security engineer is capturing packets on an internal company network and is documenting the IP addresses and MAC addresses associated with the local network devices. Which of these commands would provide the MAC address of the default gateway at 10.11.1.1?

❍ **A.** `ping 10.11.1.1`
`arp -a`

❍ **B.** `tracert 10.11.1.1`

❍ **C.** `dig 10.11.1.1`

❍ **D.** `ipconfig /all`

The Answer: A. `ping 10.11.1.1`
`arp -a`

The arp (Address Resolution Protocol) command can be used to view the local ARP cache. The cache contains a lookup table containing IP addresses and their associated MAC (Media Access Control) address. If an engineer pings a device on the local network and then views the ARP cache, they will see the MAC address that was resolved during the ARP process.

The incorrect answers:

B. `tracert 10.11.1.1`

The tracert (traceroute) command will display the IP addresses of routers between two devices. MAC addresses are not displayed in the traceroute output.

C. `dig 10.11.1.1`

The dig (Domain Information Groper) command is used to gather information from DNS (Domain Name System) servers. MAC address information is not viewable with the dig command.

D. `ipconfig /all`

The ipconfig command will display IP address and MAC address information for the local Windows computer, but it does not show the MAC address information of the default gateway.

More information:

SY0-601, Objective 4.1 - Reconnaissance Tools Part 1

https://professormesser.link/601040101

C67. A network administrator needs to identify all inbound connections to a Linux web server. Which of the following utilities would be the BEST choice for this task?

❍ **A.** netcat

❍ **B.** nmap

❍ **C.** net view

❍ **D.** netstat

The Answer: D. netstat
The netstat command can view inbound and outbound statistics for all connections to a device.

The incorrect answers:
A. netcat
The netcat command can read or write information to the network. Netcat can be used to create an open connection on a device or to access a connection on a remote machine.

B. nmap
The Nmap utility is commonly used to locate open ports and identify services running on a remote device.

C. net view
The Windows net view command is used to list the available file shares on a Windows computer.

More information:
SY0-601, Objective 4.1 - Reconnaissance Tools Part 1
https://professormesser.link/601040101

C68. A company has identified a web server data breach that resulted in the theft of financial records from 150 million customers. A security update to the company's web server software was available for two months prior to the breach. Which of the following would have prevented this breach from occurring?

❍ **A.** Patch management

❍ **B.** Full disk encryption

❍ **C.** Disable unnecessary services

❍ **D.** Application allow lists

The Answer: A. Patch management
This question describes an actual breach that occurred in 2017 to web servers at a large credit bureau. This breach resulted in the release of almost 150 million customer names, Social Security numbers, addresses, and birth dates. A web server vulnerability announced in March of 2017 was left unpatched, and attackers exploited the vulnerability two months later in May. The attackers were in the credit bureau network for 76 days before they were discovered. A formal patch management process would have clearly identified this vulnerability and would have given the credit bureau the opportunity to mitigate or patch the vulnerability well before it would have been exploited.

The incorrect answers:
B. Full disk encryption
Full disk encryption (FDE) would prevent unauthenticated access to the data, but the web server would be an authorized user and would have normal access to the areas of the operating system that are necessary for normal operation. Enabling FDE would not provide any additional security against a data breach.

C. Disable unnecessary services
It's always a good best practice to disable unnecessary services, but this breach attacked a very necessary web service.

D. Application allow lists
Application allow lists would prevent unauthorized applications from running, but it would not prevent an attack to the web service application.

More information:
SY0-601, Objective 3.2 - Application Hardening
https://professormesser.link/601030205

C69. A security administrator is deploying a web server and needs to understand the methods an attacker could use to gain access to the system. Which of the following would be the BEST source of this information?

❍ **A.** MITRE ATT&CK

❍ **B.** Diamond model

❍ **C.** Tabletop exercise

❍ **D.** ISO 27701

The Answer: A. MITRE ATT&CK
The MITRE ATT&CK framework is a knowledgebase that contains points of intrusion, methods used for attackers to move around, and a list of security techniques to prevent future attacks.

The incorrect answers:
B. Diamond model
The diamond model is a way to summarize the aftermath of an intrusion. Documentation for this model includes information about the adversary, capability, infrastructure, and the victim.

C. Tabletop exercise
A tabletop exercise is used to step through a disaster recovery scenario in a conference room without going through the time-consuming steps of an actual simulation. Problems with processes and procedures can often be resolved during the tabletop exercise.

D. ISO 27701
The ISO (International Organization for Standardization) 27701 standard focuses on the processes associated with a privacy information management system (PIMS).

More information:
SY0-601, Objective 4.2 - Attack Frameworks
https://professormesser.link/601040203

C70. A system administrator has identified an unexpected username on a database server, and the user has been transferring database files to an external server over the company's Internet connection. The administrator then performed these tasks:

- Physically disconnected the Ethernet cable on the database server
- Disabled the unknown account
- Configured a firewall rule to prevent file transfers from the server

Which of the following would BEST describe this part of the incident response process?

❍ **A.** Eradication

❍ **B.** Containment

❍ **C.** Lessons learned

❍ **D.** Preparation

The Answer: B. Containment
The containment phase isolates events that can quickly spread and get out of hand. A file transfer from a database server can quickly be contained by disabling any ability to continue the file transfer.

The incorrect answers:
A. Eradication
Eradication focuses on removing the cause of the event and restoring the systems back to their non-compromised state.

C. Lessons learned
After the event is over, the lessons learned phase helps everyone learn and improve the process for the next event.

D. Preparation
Before an event occurs, it's important to have the contact numbers, tools, and processes ready to go.

More information:
SY0-601, Objective 4.2 - Incident Response Process
https://professormesser.link/601040201

C71. Which of the following would be the MOST effective use of asymmetric encryption?

❍ **A.** Real-time video encryption

❍ **B.** Store passwords

❍ **C.** Protect data on mobile devices

❍ **D.** Securely derive a session key

The Answer: D. Securely derive a session key
The Diffie-Hellman process can combine public and private keys to derive the same session key on both sides of a conversation without sending that session key across the network.

The incorrect answers:
A. Real-time video encryption
The high speeds require for real-time video encryption and decryption would not be an efficient use for asymmetric encryption. Most high-speed or large-scale encryption uses symmetric encryption.

B. Store passwords
The best practice for password storage is to use hashes instead of encryption. Hashes ensure that a stored password can't be reverse engineered to produce the original password.

C. Protect data on mobile devices
The limited CPU and power available on a mobile device requires a more efficient form of confidentiality than asymmetric encryption. It's common for mobile devices to use elliptic curve cryptography (ECC), for example.

More information:
SY0-601, Objective 2.8 -
Symmetric and Asymmetric Cryptography
https://professormesser.link/601020802

C72. Each salesperson in a company will receive a laptop with applications and data to support their sales efforts. The IT manager would like to prevent third-parties from gaining access to this information if the laptop is stolen. Which of the following would be the BEST way to protect this data?

○ **A.** Remote wipe

○ **B.** Full disk encryption

○ **C.** Biometrics

○ **D.** BIOS user password

The Answer: B. Full disk encryption
With full disk encryption, everything written to the laptop's local drive is stored as encrypted data. If the laptop was stolen, the thief would not have the credentials to decrypt the drive data.

The incorrect answers:
A. Remote wipe
Although a remote wipe function is useful, it's a reactive response that does not provide any data protection prior to the wipe.

C. Biometrics
Biometric authentication can limit access to the operating system, but the laptop's storage drive can still be removed and read from another computer.

D. BIOS user password
Adding a power-on BIOS password would help prevent any unauthorized access to the operating system, but the password doesn't provide any protection for the data on the laptop's storage drive.

More information:
SY0-601, Objective 3.2 - Application Hardening
https://professormesser.link/601030205

C73. During sales meetings, visitors often require an Internet connection for demonstrations. Which of the following should the company implement to maintain the security of the internal network resources?

❍ **A.** NAT

❍ **B.** Ad hoc wireless workstations

❍ **C.** Intranet

❍ **D.** Guest network with captive portal

The Answer: D. Guest network with captive portal
A guest network would allow access to the Internet but prevent any access to the internal network. The captive portal would prompt each guest for authentication or to agree to terms of use before granting access to the network.

The incorrect answers:
A. NAT
NAT (Network Address Translation) is a method of modifying IP addresses when traversing the network, but NAT itself does not provide any additional security mechanisms.

B. Ad hoc wireless workstations
Ad hoc wireless devices are able to communicate with each other without the use of an access point. There are no additional security features included with an ad hoc connection.

C. Intranet
The intranet is a private internal network used by company employees. It's common to provide the highest protection to the intranet resources, so a company would not commonly connect the intranet to a public conference room.

More information:
SY0-601, Objective 3.4 - Wireless Authentication Methods
https://professormesser.link/601030402

C74. A company's web server has been infected with malware, and the security administrator has contained the system and would like to create a bit-by-bit image of the server storage drive. Which of the following would be the BEST choice for this task?

❍ **A.** Memdump

❍ **B.** chmod

❍ **C.** dd

❍ **D.** tcpdump

The Answer: C. dd
The Linux dd command is commonly used to create an image of a partition or disk.

The incorrect answers:
A. Memdump
The memdump command is used to make a copy of everything stored in local system memory. This dump of memory does not contain any local storage drive files.

B. chmod
The Linux chmod (change mode) command is used to modify the access rights and permissions of files stored on the system. The chmod command is not used to create system images.

D. tcpdump
The tcpdump utility is used to capture and store network packets. The tcpdump utility does not create images from stored data.

More information:
SY0-601, Objective 4.1 - Forensic Tools
https://professormesser.link/601040106

C75. A set of corporate security policies is what kind of security control?

❍ **A.** Compensating

❍ **B.** Detective

❍ **C.** Managerial

❍ **D.** Physical

The Answer: C. Managerial
A managerial control is a guideline that would control how people act, such as security policies and standard operating procedures.

The incorrect answers:

A. Compensating
A compensating security control doesn't prevent an attack, but it does restore from an attack using other means. A security policy does not provide a way to restore from an attack.

B. Detective
A detective control may not prevent access, but it can identify and record any intrusion attempts. Security policies do not provide any identification or recording of intrusions.

D. Physical
A physical control would block access. For example, a door lock or security guard would be a physical control.

More information:
SY0-601, Objective 5.1 - Security Controls
https://professormesser.link/601050101

C76. Which of the following would be the MOST significant security concern when protecting against criminal syndicates?

○ **A.** Prevent users from posting passwords near their workstations

○ **B.** Require identification cards for all employees and guests

○ **C.** Maintain reliable backup data

○ **D.** Use access control vestibules at all data center locations

The Answer: C. Maintain reliable backup data
Organized crime is often after data, and can sometimes encrypt or delete data on a service. A good set of backups can often resolve these issues quickly and without any ransomware payments to an organized crime entity.

The incorrect answers:
A. Prevent users from posting passwords near their workstations
Criminal syndicate members usually access systems remotely. Although it's important that users don't write down their passwords, the organized crime members aren't generally in a position to see them.

B. Require identification cards for all employees and guests
Since the criminal syndicate members rarely visit a site, having identification for employees and visitors isn't the largest concern associated with this threat actor.

D. Use access control vestibules at all data center locations
Access control vestibules control the flow of people through an area, and organized crime members aren't usually visiting a data center.

More information:
SY0-601, Objective 1.5 - Threat Actors
https://professormesser.link/601010501

C77. An application team has been provided with a hardened version of Linux to use with a new application rollout, and they are installing a web service and the application code on the server. Which of the following would BEST protect the application from attacks?

❍ **A.** Build a backup server for the application

❍ **B.** Run the application in a cloud-based environment

❍ **C.** Implement a secure configuration of the web service

❍ **D.** Send application logs to the SIEM via syslog

The Answer: C. Implement a secure configuration of the web service
The tech support resources for many services will include a list of hardening recommendations. This hardening may include account restrictions, file permission settings, internal service configuration options, and other settings to ensure that the service is as secure as possible.

The incorrect answers:
A. Build a backup server for the application
Of course, you should always have a backup. Although the backup may help recover quickly from an attack, the backup itself won't protect the application from attacks.

B. Run the application in a cloud-based environment
The location of the application service won't provide any significant protection against attacks. Some cloud-based services may include some additional security features, but many do not. Given the options available, running the application in the cloud would not be the best option available.

D. Send application logs to the SIEM via syslog
It's always useful to have a consolidated set of logs, but the logs on the SIEM (Security Information and Event Management) server won't protect the application from attacks.

More information:
SY0-601, Objective 5.2 - Secure Configurations
https://professormesser.link/601050203

C78. A system administrator has configured MAC filtering on the corporate access point, but access logs show that unauthorized users are accessing the network. The administrator has confirmed that the address filter includes only authorized MAC addresses. Which of the following should the administrator configure to prevent this authorized use?

❍ **A.** Enable WPA3 encryption

❍ **B.** Remove unauthorized MAC addresses from the filter

❍ **C.** Modify the SSID name

❍ **D.** Modify the channel

The Answer: A. Enable WPA3 encryption
A MAC (Media Access Control) address can be spoofed on a remote device, which means anyone within the vicinity of the access point can view legitimate MAC addresses and spoof them to avoid the MAC filter. To ensure proper authentication, the system administrator can enable WPA3 (Wi-Fi Protected Access version 3) with a shared key, or configure 802.1X to integrate with an existing authentication database.

The incorrect answers:
B. Remove unauthorized MAC addresses from the filter
Since MAC addresses are visible when capturing packets, any unauthorized users affected by the removal of a MAC address would simply obtain the remaining MAC addresses in use and spoof those addresses to gain access.

C. Modify the SSID name
The SSID (Service Set Identifier) is the name associated with the wireless network. The name of the access point is not a security feature, so changing the name would not provide any additional access control.

D. Modify the channel
The frequencies used by the access point are chosen to minimize interference with nearby wireless devices. These wireless channels are not security features and changing the frequency would not limit unauthorized access.

More information:
SY0-601, Objective 3.4 - Wireless Cryptography
https://professormesser.link/601030401

C79. A company is building a broad set of conditional steps to follow when investigating a data breach. Which of the following would BEST describe these steps?

❍ **A.** Managerial controls

❍ **B.** DAC

❍ **C.** Playbook

❍ **D.** Order of volatility

The Answer: C. Playbook
A playbook describes a broad set of steps to follow to manage a security event. For example, a playbook might describe the processes to follow when investigating a data breach or when recovering from a ransomware attack.

The incorrect answers:
A. Managerial controls
Managerial security controls describe administrative security methods, such as security policies and rules.

B. DAC
DAC (Discretionary Access Control) describes an access control method where the user decides which users can access their data and the permissions associated with that access.

D. Order of volatility
The order of volatility describes the lifetime associated with digital data. These volatility rates are important when determining which forensic data should be gathered first.

More information:
SY0-601, Objective 4.4 - Security Configurations
https://professormesser.link/601040402

C80. During an initial network connection, a supplicant communicates to an authenticator, which then sends an authentication request to an Active Directory database. Which of the following would BEST describe this authentication technology?

❍ **A.** Federation

❍ **B.** AES

❍ **C.** 802.1X

❍ **D.** PKI

The Answer: C. 802.1X
IEEE 802.1X is a standard for port-based network access control (NAC). When 802.1X is enabled, devices connecting to the network do not gain access until they provide the correct authentication credentials. This 802.1X standard refers to the client as the supplicant, the switch is commonly configured as the authenticator, and the back-end authentication server is a centralized user database such as Active Directory.

The incorrect answers:
A. Federation
Federation would allow members of one organization to authenticate to the network of another organization using their normal credentials.

B. AES
AES (Advanced Encryption Standard) is a common encryption protocol, and it does not describe a supplicant, authenticator, or authentication server.

D. PKI
PKI (Public Key Infrastructure) is a method of describing the public-key encryption technologies and its supporting policies and procedures. PKI does not require the use of supplicants, authenticators, or authentication servers.

More information:
SY0-601, Objective 3.4 - Wireless Authentication Protocols
https://professormesser.link/601030403

C81. A security administrator would like use employee-owned mobile phones to unlock the door of the data center using a sensor on the wall. The users would authenticate on their phones with a fingerprint before the door would unlock. Which of the following features should the administrator use? (Select TWO)

❍ **A.** NFC

❍ **B.** Remote wipe

❍ **C.** Containerization

❍ **D.** Biometrics

❍ **E.** Push notification

The Answer: A. NFC and **D.** Biometrics
The wall sensor will be activated with the phone's NFC (Near-field Communication) electronics and would authenticate using the biometric fingerprint reader on the phone.

The incorrect answers:
B. Remote wipe
Although remote wipe can be a useful management tool for a mobile device, there's no need to include remote wipe capabilities with this particular application. The door unlocking process would still require authentication using the user's fingerprint if the phone was lost or stolen.

C. Containerization
This application doesn't appear to store any confidential local data, so keeping the enterprise data separate from the personal data isn't a significant concern.

E. Push notification
A push notification will cause alerts to appear on the phone without any user intervention. In this app, all of the actions are initiated by the user.

More information:
SY0-601, Objective 3.5 - Mobile Networks
https://professormesser.link/601030501

C82. Visitors to a corporate data center must enter through the main doors of the building. Which of the following security controls would be the BEST choice to successfully guide people to the front door? (Select TWO)

❍ **A.** Cable locks

❍ **B.** Bollards

❍ **C.** Biometrics

❍ **D.** Fencing

❍ **E.** Industrial camouflage

❍ **F.** Video surveillance

The Answers: B. Bollards and **D.** Fencing
Both bollards and fencing provide physical security controls that can direct people through an area by limiting their access to other areas.

The incorrect answers:
A. Cable locks
A cable lock would help keep a computer or laptop securely fastened to a table or desk, but it wouldn't help direct people to a particular entrance.

C. Biometrics
Biometrics provide a unique authentication factor, but they aren't commonly used to direct people to a particular building entrance.

E. Industrial camouflage
Industrial camouflage would not draw any attention to the entrance, and would ultimately make the entrance more difficult to find.

F. Video surveillance
Video surveillance would make it easy to monitor and view visitors approaching the building, but it would not provide any directions to the front doors.

More information:
SY0-601, Objective 2.7 - Physical Security Controls
https://professormesser.link/601020701

C83. A company is contracting with a third-party to find vulnerabilities that employees could possibly exploit on the company's internal networks. Which of the following would be the BEST way for the third-party to meet this requirement?

❍ **A.** Run a credentialed vulnerability scan

❍ **B.** Capture packets of the application traffic flows from the internal network

❍ **C.** Identify an exploit and perform a privilege escalation

❍ **D.** Scan the network during normal working hours

The Answer: A. Run a credentialed vulnerability scan
A credentialed scan would provide login access and allow the scan to run as a standard user on the network.

The incorrect answers:
B. Capture packets of the application traffic flows from the internal network
A non-intrusive packet capture would not provide any significant vulnerability information, and it would not be possible to test for additional vulnerabilities with just the packets.

C. Identify an exploit and perform a privilege escalation
There's no guarantee that any of the systems will be vulnerable to an exploit, and there's also no guarantee that such an exploit would provide any user access.

D. Scan the network during normal working hours
Scanning a network from the outside or without credentials would not provide a list of vulnerabilities from the user's perspective, regardless of the time of day.

More information:
SY0-601, Objective 1.7 - Vulnerability Scans
https://professormesser.link/601010702

C84. A company has recently moved from one accounting system to another, and the new system includes integration with many other divisions of the organization. Which of the following would ensure that the correct access has been provided to the proper employees in each division?

❍ **A.** Location-based policies

❍ **B.** On-boarding process

❍ **C.** Account deprovisioning

❍ **D.** Permission and usage audit

The Answer: D. Permission and usage audit
A permission and usage audit will verify that all users have the correct permissions and that all users meet the practice of least privilege.

The incorrect answers:
A. Location-based policies
Location-based policies would assign rights and permissions based on physical location. For example, a location-based policy might allow users to login from local IP address ranges but not from locations outside of the corporate offices.

B. On-boarding process
The on-boarding process is used when a new person is hired or transferred into the organization. In this example, none of the users were identified as new employees.

C. Account deprovisioning
Account deprovisioning is the disabling of an account and archiving of user information. This process usually occurs when an employee has left the organization.

More information:
SY0-601, Objective 3.7 - Account Policies
https://professormesser.link/601030703

C85. An attacker has circumvented a web-based application to send commands directly to a database. Which of the following would describe this attack type?

❍ **A.** Session hijack

❍ **B.** SQL injection

❍ **C.** Cross-site scripting

❍ **D.** On-path

The Answer: B. SQL injection

A SQL (Structured Query Language) injection takes advantage of poorly written web applications. These web applications do not properly restrict the user input, and the resulting attack bypasses the application and "injects" SQL commands directly into the database itself.

The incorrect answers:

A. Session hijack

If a third-party obtained the session ID of an already-authenticated user, they could effectively communicate directly to the application without a username and password. A session hijack by itself would not allow for direct database communication.

C. Cross-site scripting

A cross-site scripting attack commonly uses scripts at one web site to execute commands on other sites. These types of attacks take advantage of the trust of a local browser, but they don't commonly have direct access to a database.

D. On-path

An on-path attack is often used to capture, monitor, or inject information into an existing data flow. An on-path attack is not commonly used for SQL injection attacks.

More information:

SY0-601, Objective 1.3 - Injection Attacks

https://professormesser.link/601010303

C86. A group of business partners is using blockchain technology to monitor and track raw materials and parts as they are transferred between companies. Where would a partner find these tracking details?

❍ **A.** Ledger

❍ **B.** HSM

❍ **C.** SIEM

❍ **D.** SED

The Answer: A. Ledger
The ledger is a shared document with a list of all blockchain transactions. The ledger is shared among everyone in the blockchain, and all transactions are available to view on this central ledger.

The incorrect answers:
B. HSM
An HSM (Hardware Security Module) provides secure key storage and cryptographic functions for servers and applications. An HSM does not provide tracking services.

C. SIEM
A SIEM (Security Information and Event Manager) is commonly used to consolidate log files and create reports. A SIEM is not used to monitor blockchain transactions.

D. SED
A SED (Self-Encrypting Drive) ensures confidentiality by automatically encrypting everything saved to the drive. A SED does not provide any tracking functionality.

More information:
SY0-601, Objective 2.8 - Blockchain Technology
https://professormesser.link/601020808

C87. A network technician at a bank has noticed a significant decrease in traffic to the bank's public website. After additional investigation, the technician finds that users are being directed to a web site that looks similar to the bank's site but is not under the bank's control. Flushing the local DNS cache and changing the DNS entry does not have any effect. Which of the following has most likely occurred?

❍ **A.** DDoS

❍ **B.** Disassociation attack

❍ **C.** Evil twin

❍ **D.** Domain hijacking

The Answer: D. Domain hijacking
A domain hijacking will modify the primary DNS (Domain Name System) settings for a domain and will allow an attacker to direct users to any IP address.

The incorrect answers:
A. DDoS
A DDoS (Distributed Denial of Service) would prevent users from accessing a service. In this example, users were accessing an unauthorized service.

B. Disassociation attack
A disassociation attack is a wireless attack that operates by removing devices from a wireless network.

C. Evil twin
An evil twin is a wireless access point that looks similar to the authentic AP. In this example, the issue is not related to a single wireless network and is occurring on many different devices.

More information:
SY0-601, Objective 1.4 - DNS Attacks
https://professormesser.link/601010409

C88. A company runs two separate applications in their data center. The security administrator has been tasked with preventing all communication between these applications. Which of the following would be the BEST way to implement this security requirement?

❍ **A.** Firewall

❍ **B.** Protected distribution

❍ **C.** Air gap

❍ **D.** VLANs

The Answer: C. Air gap
An air gap is a physical separation between networks. Air gapped networks are commonly used to separate networks that must never communicate to each other.

The incorrect answers:

A. Firewall
A firewall would provide a method of filtering traffic between networks, but firewalls can often be misconfigured and inadvertently allow some traffic to pass. Although this is one option, it's not the best option given the alternative of an air gap.

B. Protected distribution
A protected distribution is a physically secure cabled network. This usually consists of a sealed metal conduit to protect from taps and cable cuts. A protected distribution does not restrict traffic between networks.

D. VLANs
A VLAN (Virtual Local Area Network) is a logical method of segmenting traffic within network switches. Although this segmentation is effective, it's not as secure as an air gap.

More information:
SY0-601, Objective 2.7 - Secure Areas
https://professormesser.link/601020702

C89. A receptionist at a manufacturing company recently received an email from the CEO asking for a copy of the internal corporate employee directory. The receptionist replied to the email and attached a copy of the directory. It was later determined that the email address was not sent from the CEO and the domain associated with the email address was not a corporate domain name. What type of training could help prevent this type of situation in the future?

❍ **A.** Recognizing social engineering

❍ **B.** Using emails for personal use

❍ **C.** Proper use of social media

❍ **D.** Understanding insider threats

The Answer: A. Recognizing social engineering
Impersonating the CEO is a common social engineering technique. There are many ways to recognize a social engineering attack, and it's important to train everyone to spot these situations when they are occurring.

The incorrect answers:
B. Using emails for personal use
It's important that everyone understands the proper use of email and avoid personal use of the corporate email service. In this instance, however, the receptionist was not using email for personal use.

C. Proper use of social media
The attack vector used in this situation was email. Social media sites were not used in this particular example.

D. Understanding insider threats
Although the attacker wasn't identified, we could assume that an employee would already have access to the internal corporate employee directory.

More information:
SY0-601, Objective 1.1 - Impersonation
https://professormesser.link/601010102

C90. A company's security engineer is working on a project to simplify the employee onboarding and offboarding process. One of the project goals is to allow individuals to use their personal phones for work purposes. If the user leaves the company, the company data will be removed but the user's data would remain intact. Which of these technologies would meet this requirement?

○ **A.** Policy management

○ **B.** Geofencing

○ **C.** Containerization

○ **D.** Storage encryption

The Answer: C. Containerization
The storage segmentation of containerization keeps the enterprise apps and data separated from the user's apps and data. During the offboarding process, only the company information is deleted and the user's personal data is retained.

The incorrect answers:

A. Policy management
Policies can often be managed through a mobile device manager, allowing the security administrator to limit the use of certain apps, camera functions, or data storage. These management functions are important, but they don't necessarily affect the separation of storage or removal of data inside of the mobile device.

B. Geofencing
Geofencing restricts or allows features when a mobile device is in a particular location. Geofencing will not have any effect on the separation of data inside of a mobile device.

D. Storage encryption
If a mobile device is lost or stolen, storage encryption ensures that the data will remain confidential. The encryption process itself does not provide any separation between enterprise data and user data.

More information:
SY0-601, Objective 3.5 - Mobile Device Management
https://professormesser.link/601030502

Continue your journey on **ProfessorMesser.com:**

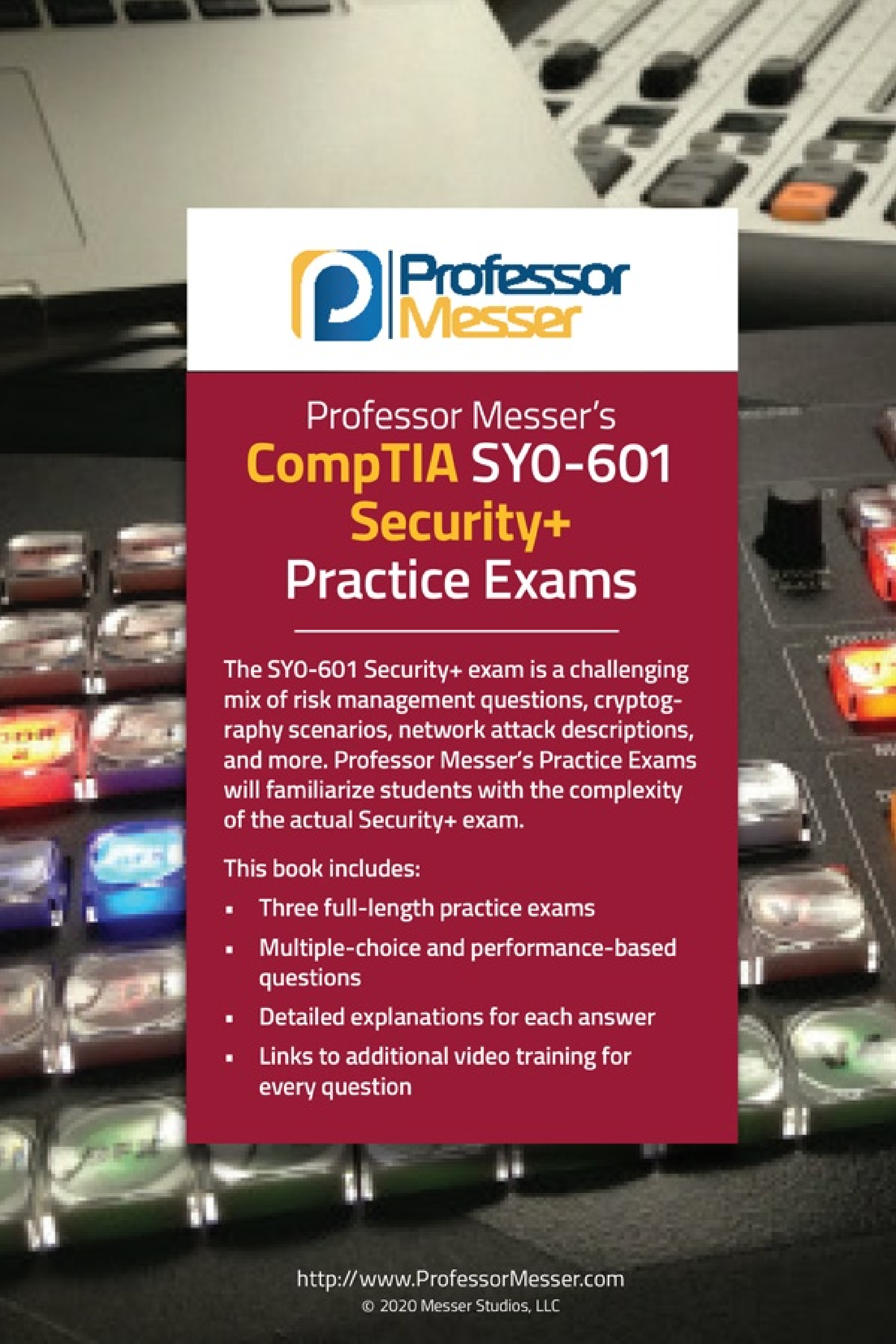
**Professor Messer's
Security+ Training Course**

Monthly Security+ Study Group Live Streams

24 x 7 Live Chat

**Professor Messer's
Security+ Course Notes**

Discount Exam Vouchers



Professor Messer

Professor Messer's CompTIA SY0-601 Security+ Practice Exams

The SY0-601 Security+ exam is a challenging mix of risk management questions, cryptography scenarios, network attack descriptions, and more. Professor Messer's Practice Exams will familiarize students with the complexity of the actual Security+ exam.

This book includes:

- Three full-length practice exams
- Multiple-choice and performance-based questions
- Detailed explanations for each answer
- Links to additional video training for every question

http:// www.ProfessorMesser.com