



**Exam : SY0-601**

**Title : CompTIA Security+ Exam**

**Version : V15.02**

1.A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports.

Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module

B. A host-based firewall

C. A DLP solution

D. Full disk encryption

E. A VPN

F. Antivirus software

**Answer:** B,C

2.The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards.

Which of the following social-engineering techniques is the attacker using?

A. Phishing

B. Whaling

C. Tyro squatting

D. Pharming

**Answer:** B

3.A global pandemic is forcing a private organization to close some business units and reduce staffing at others.

Which of the following would be BEST to help the organization's executives determine the next course of action?

A. An incident response plan

B. A communications plan

C. A disaster recovery plan

D. A business continuity plan

**Answer:** D

**Explanation:**

Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident",<sup>[1]</sup> and business continuity planning <sup>[2][3]</sup> (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.<sup>[4]</sup> In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.<sup>[5]</sup> Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

4.When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider.

Which of the following risk management strategies is this an example of?

A. Acceptance

- B. Mitigation
- C. Avoidance
- D. Transference**

**Answer:** D

**Explanation:**

Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means. [https://www.bcmpedia.org/wiki/Risk\\_Transference](https://www.bcmpedia.org/wiki/Risk_Transference)

5.Which of the following types of controls is a turnstile?

- A. Physical**
- B. Detective
- C. Corrective
- D. Technical

**Answer:** A

6.A security auditor is reviewing vulnerability scan data provided by an internal security team.

Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs**
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

**Answer:** B

7.A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic.

Which of the following would be BEST to solve this issue?

- A. iPSec
- B. Always On
- C. Split tunneling**
- D. L2TP

**Answer:** C

8.A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server.

Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump**
- D. Syslog

**Answer:** C

**Explanation:**

Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated

by Windows or by the apps that crash, but you can also manually generate them  
<https://www.digitalcitizen.life/view-contents-dump-file/>

9.A startup company is using multiple SaaS and IaaS platform to stand up a corporate infrastructure and build out a customer-facing web application.

Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

**Answer:** C

10.Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS
- B. PaaS
- C. IaaS
- D. DaaS

**Answer:** C

11.A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices.

Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

**Answer:** A

**Explanation:**

<https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/>

12.An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab.

Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

- A. The theft of portable electronic devices
- B. Geotagging in the metadata of images
- C. Bluesnarfing of mobile devices
- D. Data exfiltration over a mobile hotspot

**Answer:** D

13.The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread

unhindered throughout the network and infect a large number of computers and servers.

Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.**
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

**Answer:** B

14. Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time.

Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

- A. COPE
- B. VDI**
- C. GPS
- D. TOTP
- E. RFID**
- F. BYOD

**Answer:** B,E

15. After entering a username and password, an administrator must gesture on a touch screen.

Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication**

**Answer:** D

16. Which of the following is a team of people dedicated to testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

- A. Red team**
- B. White team
- C. Blue team
- D. Purple team

**Answer:** A

**Explanation:**

Red team—performs the offensive role to try to infiltrate the target.

17. A public relations team will be taking a group of guests on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information**

- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

**Answer:** A

**Explanation:**

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

18.A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP**
- C. IMAP
- D. HIDS

**Answer:** B

**Explanation:**

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

19.A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned.

Which of the following attacks is MOST likely being detected?

- A. Pass-the-hash**
- B. Buffer overflow
- C. Cross-site scripting
- D. Session replay

**Answer:** A

**Explanation:**

<https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack>

20.An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft.

Which of the following would be the MOST acceptable?

- A. SED**
- B. HSM
- C. DLP
- D. TPM

**Answer:** A

21.A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet.

Which of the following would MOST likely allow the company to find the cause?

- A. Checksums
- B. Watermarks
- C. Order of volatility
- D. A log analysis
- E. A right-to-audit clause

**Answer:** D

**Explanation:**

<https://www.sumologic.com/glossary/log-analysis/>

22.In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

**Answer:** A

23.Phishing and spear-phishing attacks have been occurring more frequently against a company's staff.

Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

spf records in dns allow reverse lookup for discovery of ip addresses for a domain and then compared to the IP addresses in the email headers -

**Answer:** C

24.A security administrator suspects there may be unnecessary services running on a server.

Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

**Answer:** A

**Explanation:**

<https://nmap.org/book/man-version-detection.html>

NMAP scans running services and can tell you what services are running

25.A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process.

Which of the following methods would BEST accomplish this goal?

- A. Salting the magnetic strip information
- B. Encrypting the credit card information in transit.
- C. Hashing the credit card numbers upon entry.
- D. Tokenizing the credit cards in the database

**Answer:** D

26.A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP.

Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. Isolation

**Answer:** A

27.The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk.

Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer:** A,B

28.A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems.

Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

**Answer:** D

29.Which of the following is the purpose of a risk register?

- A. To define the level or risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

**Answer:** C

**Explanation:**

The Risk Register displays a list of all risks recorded and displays various risk details, including the residual risk level, risk source, risk owner, risk stage, and the treatment status of the risk.

<https://kb.wisc.edu/security/110450>

30. The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

**Answer:** D

31. Company engineers regularly participate in a public Internet forum with other engineers throughout the industry.

Which of the following tactics would an attacker MOST likely use in this scenario?

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

**Answer:** A

32. An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them.

Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

- A. Voice
- B. Gait
- C. Vein
- D. Facial
- E. Retina

#### F. Fingerprint

**Answer:** B,D

33.A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again.

Which of the following should the IT administrator do FIRST after recovery?

- A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
- B. Restrict administrative privileges and patch all systems and applications.
- C. Rebuild all workstations and install new antivirus software
- D. Implement application whitelisting and perform user application hardening

**Answer:** A

34.A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly.

Which of the following technologies should the IT manager use when implementing MFA?

- A. One-time passwords
- B. Email tokens
- C. Push notifications
- D. Hardware authentication

**Answer:** C

35.A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data.

Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@  
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @  
@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
The fingerprint for the RSA key sent by the remote host is  
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.  
Please contact your system administrator.  
RSA host key for 18.231.33.78 has changed and you have requested strict checking.  
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

**Answer:** C

#### Explanation:

the message is basically saying the known\_hosts that your client uses has a tuple that no longer matches this server, usually because the server is presenting a new key to the client, though it could be the same

key on a new ip also.

Which could be the result of a MITM attack. (key changed)

<https://serverfault.com/questions/193631/ssh-into-a-box-with-a-frequently-changed-ip> (ip changed)

<https://stackabuse.com/how-to-fix-warning-remote-host-identification-has-changed-on-mac-and-linux/>

36.Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption**
- E. SQL injection
- F. Server-side request forgery**

**Answer:** D,F

37.An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business.

The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

- A. Disallow new hires from using mobile devices for six months
- B. Select four devices for the sales department to use in a CYOD model
- C. Implement BYOD for the sales department while leveraging the MDM**
- D. Deploy mobile devices using the COPE methodology

**Answer:** C

38.A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom.

Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.**
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system updates automatically.

**Answer:** A

39.A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet.

Which of the following is the BEST solution to protect these designs?

- A. An air gap**
- B. A Faraday cage
- C. A shielded cable
- D. A demilitarized zone

**Answer: A**

40.A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying**
- D. Dictionary

**Answer: C**

**Explanation:**

Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

<https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=Password%20spraying%20is%20a%20type,rapid%20or%20frequent%20account%20lockouts.>

41.A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices.

Which of the following solutions would BEST support the policy?

- A. Mobile device management**
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

**Answer: A**

42.While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior.

Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.**
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fileless virus is spreading in the local network environment.

**Answer: A**

**Explanation:**

<https://www.howtogeek.com/362203/what-is-a-tar.gz-file-and-how-do-i-open-it/>

43.A small company that does not have security staff wants to improve its security posture.

Which of the following would BEST assist the company?

A. MSSP

**B. SOAR**

C. IaaS

D. PaaS

**Answer:** B

44.Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the real data?

A. Data encryption

**B. Data masking**

C. Data deduplication

D. Data minimization

**Answer:** B

**Explanation:**

<https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20based%20on%20the%20user%20permissions.>

The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles

[https://en.wikipedia.org/wiki/Data\\_masking](https://en.wikipedia.org/wiki/Data_masking)

45.A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks.

The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=/User[Username/text()='foo' or 7=7
or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.

**B. An injection attack is being conducted against a user authentication system.**

C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

**Answer:** B

46. A company wants to deploy PKI on its Internet-facing website.

The applications that are currently deployed are:

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

Which of the following certificate types would BEST meet the requirements?

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

**Answer:** B

47. Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continues to evade detection.

Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

**Answer:** C

**Explanation:**

Heuristic analysis is also one of the few methods capable of combating polymorphic viruses — the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature.

<https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

48. Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

**Answer:** B

**Explanation:**

Data Owner - the administrator/CEO/board/president of a company Data custodian - the ones taking care of the actual data - like IT staff (generally) or HR staff (for HR-related data)

<https://security.stackexchange.com/questions/218049/what-is-the-difference-between-data-owner-data-custodian-and-system-owner>

<https://www.nicolaaskham.com/blog/2019/4/12/whats-the-difference-between-data-owners-and-data-custodians>

49.A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers.

Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Basic awareness training

**Answer:** B

50.A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM.

The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

**Answer:** D

**Explanation:**

If a user tries to authenticate with a wrong password, the domain controller who handles the authentication request will increment an attribute called badPwdCount. As you can see in the image, the badpwdcount attribute for the user states that many passwords were used to try to log in without success. Password spraying is an attack that attempts to access a large number of accounts (usernames) with a few commonly used passwords.

<https://www.coalfire.com/the-coalfire-blog/march-2019/password-spraying-what-to-do-and-how-to-avoid-it>

<https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/>

51.A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications.

Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

**Answer:** C

**Explanation:**

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

52.A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute.

Which of the following intelligence sources should to security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

**Answer:** D

53.In which of the following situations would it be BEST to use a detective control type for mitigation?

- A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
- B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
- C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
- D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
- E. A company purchased liability insurance for flood protection on all capital assets.

**Answer:** D

54.An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information.

One of the posts says the following:

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  

```

forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

**Answer:** C

58.Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize.

Which of the following BEST describes this type of email?

- A. Spear phishing
- B. Whaling
- C. Phishing
- D. Vishing

**Answer:** C

**Explanation:**

<https://en.wikipedia.org/wiki/Phishing>

59.A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours.

Which of the following attacks was MOST likely used?

- A. Man-in- the middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poising

**Answer:** D

**Explanation:**

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer). [https://en.wikipedia.org/wiki/DNS\\_spoofing](https://en.wikipedia.org/wiki/DNS_spoofing)

60.The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls.

Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

**Answer:** B

**Explanation:**

Shadow IT solutions increase risks with organizational requirements for control, documentation, security,

reliability, etc - [https://en.wikipedia.org/wiki/Shadow\\_IT](https://en.wikipedia.org/wiki/Shadow_IT)

61.A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

**Answer:** D

62.A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred.

Which of the following is the analyst MOST likely seeing?

- A)  
`http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>`
  - B)  
`http://sample.url.com/someotherpageonsite/../../../../etc/shadow`
  - C)  
`http://sample.url.com/select-from-database-where-password-null`
  - D)  
`http://redirect.sample.url.sampleurl.com/malicious-dns-redirect`
- A. Option A
  - B. Option B
  - C. Option C
  - D. Option D

**Answer:** B

63.A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI.

Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

**Answer:** C

64.A network administrator has been alerted that web pages are experiencing long load times.

After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

**Answer:** D

65.A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

**Answer:** D

**Explanation:**

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat

[https://en.wikipedia.org/wiki/Common\\_Vulnerability\\_Scoring\\_System](https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System)

66.An organization needs to implement more stringent controls over administrator/root credentials and service accounts.

Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

**Answer:** D

67.A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment.

Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.

- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

**Answer:** B

68.A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions. Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

**Answer:** C

**Explanation:**

<https://www.hypr.com/encapsulating-security-payload-esp/> Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

69.A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet.

Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

**Answer:** D

70.An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments.

Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

**Answer:** C

71.A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner.

Which of the following access control schemes BEST fits the requirements?

- A. Role-based access control
- B. Discretionary access control
- C. Mandatory access control
- D. Attribute-based access control

**Answer: B**

72.A user enters a password to log in to a workstation and is then prompted to enter an authentication code.

Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

- A. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

**Answer: B,E**

73.A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release.

Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

**Answer: A**

74.A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk.

Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

**Answer: A**

75.After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical.

Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

**Answer: A**

76.Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

**Answer:** A

77.Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS.

Which of the following is MOST likely causing the malware alerts?

- A. A worm that has propagated itself across the intranet, which was initiated by presentation media
- B. A fileless virus that is contained on a vCard that is attempting to execute an attack
- C. A Trojan that has passed through and executed malicious code on the hosts
- D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

**Answer:** A

78.A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords.

Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

**Answer:** C

79.A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set.

Which of the following recommendations would BEST prevent this from reoccurring?

- A. Create a new acceptable use policy.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

**Answer:** C

80.Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment

D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

**Answer:** A

81.A user recent an SMS on a mobile phone that asked for bank delays.

Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

**Answer:** D

82.Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

- A. Integer overflow
- B. Zero-day
- C. End of life
- D. Race condition

**Answer:** B

83.A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing.

Which of the following should the CISO read and understand before writing the policies?

- A. PCI DSS
- B. GDPR
- C. NIST
- D. ISO 31000

**Answer:** B

**Explanation:**

GDPR is an international standard for data protection and privacy.

84.A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze.

The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin

- C. Bluejacking
- D. ARP poisoning

**Answer:** B

**Explanation:**

[https://en.wikipedia.org/wiki/Wi-Fi\\_deauthentication\\_attack](https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack)

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

85.Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

**Answer:** C

**Explanation:**

Separation of duties - is a means of establishing checks and balances against the possibility that critical system or procedures can be compromised by insider threats. Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers.

86.An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

**Answer:** C

87.Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

**Answer:** B

88.The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained.

Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones

- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

**Answer:** A

89.Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

**Answer:** C

90.DRAG DROP

A security engineer is setting up password less authentication for the first time.

### INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

The image shows a terminal window titled 'Commands' on the left and an 'SSH Client' window on the right. The 'Commands' window contains the following seven lines of text, each in a yellow box:

- chmod 644 ~/ssh/id\_rsa
- chmod 777 ~/ssh/authorized\_keys
- scp ~/ssh/id\_rsa user@server:ssh/authorized\_keys
- ssh root@server
- ssh-keygen -t rsa
- ssh-copy-id -i ~/ssh/id\_rsa.pub user@server
- ssh -i ~/ssh/id\_rsa user@server

The 'SSH Client' window has a grey header bar with the title 'SSH Client'. Below the header is a white area containing a yellow-bordered box with a question mark icon in the center.

**Answer:**

Commands	SSH Client
chmod 644 ~/ssh/id_rsa	
chmod 777 ~/ssh/authorized_keys	ssh root@server
scp ~/ssh/id_rsa user@server:ssh/authorized_keys	scp ~/ssh/id_rsa user@server:ssh/authorized_keys
ssh root@server	ssh -i ~/ssh/id_rsa user@server
ssh-keygen -t rsa	ssh-keygen -t rsa
ssh-copy-id -i ~/ssh/id_rsa.pub user@server	ssh-copy-id -i ~/ssh/id_rsa.pub user@server
ssh -i ~/ssh/id_rsa user@server	chmod 777 ~/ssh/authorized_keys
	chmod 644 ~/ssh/id_rsa

91.In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts.

In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradication
- D. Recovery
- E. Containment

**Answer:** E

92.A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels.

Which of the following access control schemes would be BEST for the company to implement?

- A. Discretionary
- B. Rule-based
- C. Role-based
- D. Mandatory

**Answer:** D

93.An organization is developing a plan in the event of a complete loss of critical systems and data.

Which of the following plans is the organization MOST likely developing?

- A. Incident response

- B. Communications
- C. Disaster recovery
- D. Data retention

**Answer:** C

94.A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text.

Which of the following would mitigate the damage done by this type of data exfiltration in the future?

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

**Answer:** A

95.A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil.

Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

**Answer:** D

96.Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

**Answer:** D,E

97.A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected. Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads.

Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping

- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

**Answer:** A,C

**Explanation:**

"According to its self-reported version, the Cisco IOS software running on the remote device is affected by a denial of service vulnerability in the Session Initiation Protocol (SIP) gateway implementation due to improper handling of malformed SIP messages. An unauthenticated, remote attacker can exploit this, via crafted SIP messages, to cause memory leakage, resulting in an eventual reload of the affected device."

98.An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away.

Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

**Answer:** B

99.A network administrator has been asked to install an IDS to improve the security posture of an organization.

Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

**Answer:** C

**Explanation:**

IDS = Intrusion Detection System. It is passive and only notifies instead of blocking anything.

100.An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button.

Which of the following would MOST likely contain that information?

- A. NGFW
- B. Pagefile**
- C. NetFlow
- D. RAM

**Answer:** B

101.The IT department's on-site developer has been with the team for many years. Each time an

application is released, the security team is able to identify multiple vulnerabilities.

Which of the following would BEST help the team ensure the application is ready to be released to production?

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.**

**Answer:** D

102.A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime.

Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply**
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming**
- E. Scheduled penetration testing
- F. Network-attached storage

**Answer:** A,D

**Explanation:**

<https://searchdatacenter.techtarget.com/definition/resiliency>

103.A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.**
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

**Answer:** C

~~104.A remote user recently took a two week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN.~~

~~Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?~~

- ~~A. Due to foreign travel, the user's laptop was isolated from the network.~~
- ~~B. The user's laptop was quarantined because it missed the latest patch update.~~
- ~~C. The VPN client was blacklisted.~~
- ~~D. The user's account was put on a legal hold.~~

**Answer:** A

105.Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape**
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

**Answer:** B

**Explanation:**

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor.

[https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs\)%20running%20on%20that%20host](https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs)%20running%20on%20that%20host).

106.After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker.

Which of the following will the company MOST likely review to trace this transaction?

- A. The public ledger**
- B. The NetFlow data
- C. A checksum
- D. The event log

**Answer:** A

107.A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff.

Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise**
- D. Running a simulation exercise

**Answer:** C

**Explanation:**

<https://www.redlegg.com/solutions/advisory-services/tabletop-exercise-pretty-much-everything-you-need-to-know>

108.A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory.

Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting**
- D. Credentialated vulnerability scanning

**Answer:** C

**Explanation:**

<https://www.comptia.org/blog/your-next-move-threat-hunter#:~:text=Threat%20hunters%20are%20IT%20professionals%20who%20proactively%20find,that%20might%20evoke%20the%20security%20operations%20center%20%28SOC%29>.

109.A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers.

Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.**
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

**Answer:** B

110.A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area.

Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker**
- D. Biometrics

**Answer:** C

111.A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

- A. Rogue access point
- B. Evil twin
- C. DNS poisoning
- D. ARP poisoning

**Answer:** B

~~112.A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber incident investigation.~~

~~An incident responder learns the following information:~~

- ~~□ The timeline of stolen card numbers corresponds closely with affected users making Internet based purchases from diverse websites via enterprise desktop PCs.~~

- All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
- Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

- A. HTTPS sessions are being downgraded to insecure cipher suites
- B. The SSL inspection proxy is feeding events to a compromised SIEM
- C. The payment providers are insecurely processing credit card charges
- D. The adversary has not yet established a presence on the guest WiFi network

**Answer:** C

113.A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string.

Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting**
- D. Hashing

**Answer:** C

114.Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR**
- D. NIPS

**Answer:** C

115.To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials.

Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit**
- D. A geofencing policy based on login history

**Answer:** C

116.Which of the following would MOST likely support the integrity of a voting machine?

- A. Asymmetric encryption
- B. Blockchain**
- C. Transport Layer Security
- D. Perfect forward secrecy

**Answer:** B

**Explanation:**

"Blockchain technology has a variety of potential applications. It can ensure the integrity and transparency of financial transactions, online voting systems, identity management systems, notarization, data storage, and more. "

117.Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

- A. MOU
- B. MTTR
- C. SLA
- D. NDA

**Answer:** C

**Explanation:**

Service level agreement (SLA). An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.

118.A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use.

Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

**Answer:** A,C

**Explanation:**

heat map and site survey will provide the wifi strength and identify the weakness areas..this will give the opportunity if we need to increase WiFi strength or give suggestion to the forklift drivers about the movement

119.Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

**Answer:** C

**Explanation:**

ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems. <https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701>

~~120.A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts.~~

~~Which of the following security practices would have addressed the issue?~~

- ~~A. A non-disclosure agreement~~
- ~~B. Least privilege~~
- ~~C. An acceptable use policy~~
- ~~D. Ofboarding~~

**Answer:** D

~~121.A company has drafted an insider-threat policy that prohibits the use of external storage devices.~~

~~Which of the following would BEST protect the company from data exfiltration via removable media?~~

- ~~A. Monitoring large data transfer transactions in the firewall logs~~
- ~~B. Developing mandatory training to educate employees about the removable media policy~~
- ~~C. Implementing a group policy to block user access to system files~~
- D. Blocking removable-media devices and write capabilities using a host-based security tool**

**Answer:** D

~~122.A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities.~~

~~Which of the following would BEST meet this need?~~

- ~~A. CVE~~
- ~~B. SIEM~~
- ~~C. SOAR~~
- D. CVSS**

**Answer:** D

**Explanation:**

The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

~~123.A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site.~~

~~Upon investigation, a security analyst identifies the following:~~

- ~~The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP~~
- ~~The forged website's IP address appears to be 10.2.12.99, based on NetFlow records~~
- ~~All three at the organization's DNS servers show the website correctly resolves to the legitimate IP~~
- ~~DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.~~

~~Which of the following MOST likely occurred?~~

- ~~A. A reverse proxy was used to redirect network traffic~~
- ~~B. An SSL strip MITM attack was performed~~
- ~~C. An attacker temporarily pawned a name server~~
- ~~D. An ARP poisoning attack was successfully executed~~

**Answer: B**

124.In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference

B. Avoidance

C. Acceptance

D. Mitigation

**Answer: A**

125.A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance.

Which of the following RAID levels should the administrator select?

A. 0

B. 1

C. 5

D. 6

**Answer: D**

126.A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network.

Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard

B. WPA-EAP

C. IP filtering

D. A WIDS

**Answer: B**

**Explanation:**

"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism."

[https://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010. Source:

<https://jaimelightfoot.com/blog/comptia-security-wireless-security/> “EAP has been expanded into multiple versions.”

- “The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3.”
- “The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3.”
- “The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3.”

Excerpt From: Wm. Arthur Conklin. “CompTIA Security+ All-in-One Exam Guide (Exam SY0-601)).”

127.A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO).

Which of the following would be BEST to allow a security analyst to gather information and confirm it is a

malicious document without executing any code it may contain?

- A. Open the document on an air-gapped network
- B. View the document's metadata for origin clues
- C. Search for matching file hashes on malware websites
- D. Detonate the document in an analysis sandbox

**Answer:** D

128.An organization suffered an outage and a critical system took 90 minutes to come back online.

Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes.

Which of the following is the 60-minute expectation an example of:

- A. MTBF
- B. RPO
- C. MTTR
- D. RTO

**Answer:** C

**Explanation:**

129.Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

**Answer:** A

~~130.During an incident response, a security analyst observes the following log entry on the web server.~~

~~Which of the following BEST describes the type of attack the analyst is experiencing?~~

- A. SQL injection
- B. Cross site scripting
- C. Pass the hash
- D. Directory traversal

~~**Answer:** D~~

131.A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control.

Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

**Answer:** B

132.A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard.

Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

**Answer:** A

~~133.A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end of life support and cannot be upgraded, so it is placed on a projected network segment.~~

~~Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?~~

- A. DNS sinkholing
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

~~**Answer:** D~~

134.HOTSPOT

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

### **INSTRUCTIONS**

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>

**Answer:**

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<ul style="list-style-type: none"> <li>Botnet</li> <li>RAT</li> <li>Logic Bomb</li> <li>Backdoor</li> <li>Virus</li> <li>Spyware</li> <li>Worm</li> <li>Adware</li> <li>Ransomware</li> <li>Keylogger</li> <li>Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Enable DDoS protection</li> <li>Patch vulnerable systems</li> <li>Disable vulnerable services</li> <li>Change the default system password</li> <li>Update the cryptographic algorithms</li> <li>Change the default application password</li> <li>Implement 2FA using push notification</li> <li>Conduct a code review</li> <li>Implement application fuzzing</li> <li>Implement a host-based IPS</li> <li>Disable remote access services</li> </ul>

135.A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application.

Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

**Answer:** C

**Explanation:**

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies

136.A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine.

Which of the following steps should also be taken to harden the smart switch?

- A. Set up an air gap for the switch.
- B. Change the default password for the switch.
- C. Place the switch In a Faraday cage.
- D. Install a cable lock on the switch

**Answer:** B

137.A company has limited storage available and online presence that cannot for more than four hours.

Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time.

In the event of a failure, which being mindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
- C. Implement nightly full backups every Sunday at 8:00 p.m
- D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

**Answer:** D

~~138.On which of the following is the live acquisition of data for forensic analysis MOST dependent?~~

~~(Choose two.)~~

- A. ~~Data accessibility~~
- B. ~~Legal hold~~
- C. ~~Cryptographic or hash algorithm~~
- D. ~~Data retention legislation~~
- E. ~~Value and volatility of data~~
- F. ~~Right to audit clauses~~

**Answer:** E,F

139.A security assessment determines DES and 3DES are still being used on recently deployed production servers.

Which of the following did the assessment identify?

- A. Unsecme protocols
- B. Default settings
- C. Open permissions
- D. Weak encryption**

**Answer:** D

140.A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day.

Which of the following would MOST likely show where the malware originated?

- A. The DNS logs**
- B. The web server logs
- C. The SIP traffic logs
- D. The SNMP logs

**Answer:** A

141.A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider.

Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP**
- E. Microservices

**Answer:** D

~~142.A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously.~~

~~Which of the following RAID configurations should the administration use?~~

- ~~A. RA1D 0~~
- ~~B. RAID1~~
- ~~C. RAID 5~~
- ~~D. RAID-10~~

**Answer:** C

**Explanation:**

<https://techgenix.com/raid-10-vs-raid-5/>

143.A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL: <http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us>

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

<http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us>

Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

**Answer:** D

~~144.An organization is concerned that its hosted web servers are not running the most updated version of the software.~~

~~Which of the following would work BEST to help identify potential vulnerabilities?~~

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup port=80 comptia.org

**Answer:** C

**Explanation:**

~~Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.~~

145.An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled.

Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

**Answer:** D

**Explanation:**

<https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>

[https://csrc.nist.gov/glossary/term/advanced\\_persistent\\_threat](https://csrc.nist.gov/glossary/term/advanced_persistent_threat)

146.CORRECT TEXT

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

## INSTRUCTIONS

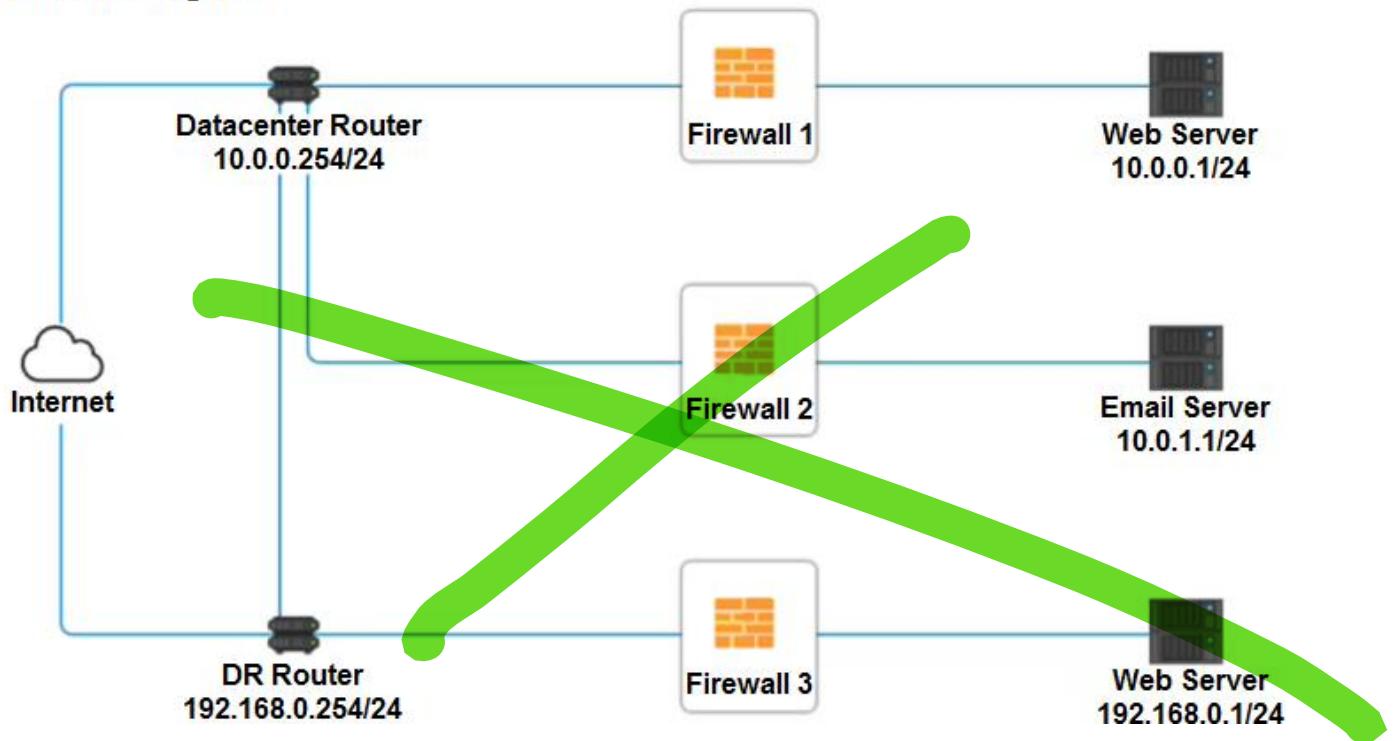
Click on each firewall to do the following:

- Deny cleartext web traffic.
- Ensure secure management protocols are used. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

## Network Diagram



**Firewall 1**

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

**Firewall 2**

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

**Firewall 3**

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

**Reset Answer** **Save** **Close**

**Answer:**

Firewall 1:

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer      Save      Close

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer      Save      Close

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT

Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

**Incorrect Answer:** Firewall 2 has a rule that permits management traffic from the internet to the firewall itself. This is a security risk and should be removed.

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

No changes should be made to this firewall

Firewall 3:

**Incorrect Answer:** Firewall 3 has a rule that permits management traffic from the internet to the firewall itself. This is a security risk and should be removed.

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

~~DNS Rule ANY > ANY > DNS > PERMIT~~

~~HTTPS Outbound 192.168.0.1/24 > ANY > HTTPS > PERMIT~~

~~Management ANY > ANY > SSH > PERMIT~~

~~HTTPS Inbound ANY > ANY > HTTPS > PERMIT~~

~~HTTP Inbound ANY > ANY > HTTP > DENY~~

147.Which of the following will provide the BEST physical security countermeasures to stop intruders?  
(Select TWO.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Mantraps**
- E. Fencing**
- F. Sensors

**Answer:** D,E

148.An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password.

Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints**
- C. PIN
- D. TPM

**Answer:** B

~~149.A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members.~~

~~Which of the following should the administrator implement?~~

- ~~A. DAG~~

- B. ABAC
- C. SCAP
- D. SOAR

**Answer:** D

~~150. An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DIP appliance, the VPN server and the datacenter itself.~~

~~Which of the following is the WEAKEST design element?~~

- A. The DLP appliance should be integrated into a NGFW.
- B. Split tunnel connections can negatively impact the DLP appliance's performance
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network
- D. Adding two hops in the VPN tunnel may slow down remote connections

**Answer:** C

~~151. A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures.~~

~~Which of the following RAID levels meets this requirements?~~

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

**Answer:** D

152. Which of the following algorithms has the SMALLEST key size?

- A. DES
- B. Twofish
- C. RSA
- D. AES

**Answer:** A

~~153. A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy.~~

~~The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:~~

- ~~• Mobile device OSs must be patched up to the latest release~~
- ~~• A screen lock must be enabled (passcode or biometric)~~
- ~~• Corporate data must be removed if the device is reported lost or stolen~~

~~Which of the following controls should the security engineer configure? (Select TWO)~~

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe
- E. Full device encryption

F. Geofencing

**Answer:** D,E

~~154.A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use.~~

~~Which of the following would add another factor of authentication?~~

- ~~A. Hard token~~
- ~~B. Retina scan~~
- ~~C. SMS text~~
- ~~D. Keypad PIN~~

**Answer:** B

155.An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness.

Which of the following will the CSO MOST likely use?

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise**
- D. A red-team engagement

**Answer:** C

~~156.Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution.~~

~~The security team has received the following requirements:~~

- ~~• There must be visibility into how teams are using cloud-based services.~~
- ~~• The company must be able to identify when data related to payment cards is being sent to the cloud.~~
- ~~• Data must be available regardless of the end user's geographic location.~~
- ~~• Administrators need a single pane of glass view into traffic and trends.~~

~~Which of the following should the security analyst recommend?~~

- ~~A. Create firewall rules to restrict traffic to other cloud service providers.~~
- ~~B. Install a DLP solution to monitor data in transit.~~
- C. Implement a CASB solution.**
- ~~D. Configure a web-based content filter.~~

**Answer:** B

157.A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports.

Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat**
- C. Nmap
- D. Nessus

**Answer:** B

158.A company was recently breached Part of the company's new cybersecurity strategy is to centralize the logs from all security devices.

Which of the following components forwards the logs to a central source?

- A. Log enrichment
- B. Log aggregation
- C. Log parser
- D. Log collector**

**Answer:** D

159.A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided.

During which of the following stages of the response process will this activity take place?

- A. Recovery
- B. Identification
- C. Lessons learned**
- D. Preparation

**Answer:** C

~~160.Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?~~

- ~~A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.~~
- ~~B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.~~
- ~~C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox~~
- ~~D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites~~

**Answer:** D

~~161.An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139.~~

~~Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?~~

- ~~A. The vulnerability scan output~~
- ~~B. The security logs~~
- ~~C. The baseline report~~
- ~~D. The correlation of events~~

**Answer:** A

162.A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks.

Which of the following methods would BEST prevent data? (Select TWO)

- A. VPN
- B. Drive encryption**
- C. Network firewall

D. File-level encryption

**E. USB blocker**

F. MFA

**Answer:** B,E

163.Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot access the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic.

Which of the following attacks is MOST likely occurring?

A. DDoS

B. Man-in-the-middle

C. MAC flooding

D. Domain hijacking

**Answer:** A

164.A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication if Active Directory is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS.

**B. Configure AAA on the switch with local login as secondary.**

C. Configure port security on the switch with the secondary login method.

D. Implement TACACS+

E. Enable the local firewall on the Active Directory server.

F. Implement a DHCP server.

**Answer:** A,B

165.A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company.

Which of the following solutions will BEST meet these requirements?

A. An NGFW

**B. A CASB**

C. Application whitelisting

D. An NG-SWG

**Answer:** B

**Explanation:**

The Official CompTIA Security+ Student Guide (Exam SY0-601) | 426-427

CASBs provide you with visibility into how clients and other network nodes are using cloud services.

Some of the functions of a CASB are:

- Enable single sign-on authentication and enforce access controls and authorizations from the enterprise network to the cloud provider.

- Scan for malware and rogue or non-compliant device access.
- Monitor and audit user and resource activity.
- Mitigate data exfiltration by preventing access to unauthorized cloud services from managed devices

166.Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

**Answer:** C

167.A security analyst needs to perform periodic vulnerability scans on production systems.

Which of the following scan Types would produce the BEST vulnerability scan report?

- A. Port
- B. Intrusive
- C. Host discovery
- D. Credentialated

**Answer:** D

168.An attacker is attempting to exploit users by creating a fake website with the URL users.

Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typosquatting
- C. Impersonation
- D. Watering-hole attack

**Answer:** A

169.A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall.

Which of the following would be the BEST option to remove the rules?

- A. # iptables -t mangle -X
- B. # iptables -F
- C. # iptables -Z
- D. # iptables -P INPUT -j DROP

**Answer:** B

170.A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs.

Which of the following should the university use to BEST protect these assets deployed in the facility?

- A. Visitor logs
- B. Cable locks
- C. Guards

- D. Disk encryption
- E. Motion detection

**Answer:** B

171.Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB
- C. UTM
- D. DLP**

**Answer:** D

172.Which of the following would be BEST to establish between organizations that have agreed to cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. An NDA
- C. A BPA
- D. An MOU**

**Answer:** D

173.A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack**
- D. A keylogger attack

**Answer:** C

174.Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP**
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Answer:** A

175.A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks.

Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

**Answer:** B,E

176. Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident.

Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer:** A

177. Which of the following will MOST likely cause machine learning and AI-enabled systems to operate with unintended consequences?

- A. Stored procedures
- B. Buffer overflows
- C. Data bias
- D. Code reuse

**Answer:** C

**Explanation:**

<https://lionbridge.ai/articles/7-types-of-data-bias-in-machine-learning/>

<https://bernardmarr.com/default.asp?contentID=1827>

178. An attacker is exploiting a vulnerability that does not have a patch available.

Which of the following is the attacker exploiting?

- A. Zero-day
- B. Default permissions
- C. Weak encryption
- D. Unsecure root accounts

**Answer:** A

179. Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU

C. An SLA

D. A BPA

**Answer:** C

**Explanation:**

Most SLA include a monetary penalty if the vendor is unable to meet the agreed-upon expectations

180.A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks.

Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists

B. White-hat hackers

C. Script kiddies

D. Insider threats

**Answer:** A

**Explanation:**

Hacktivists - "a person who gains unauthorized access to computer files or networks in order to further social or political ends."

181.To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving.

Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

**Answer:** C

182.A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security.

Which of the following controls will the analyst MOST likely recommend?

A. MAC

B. ACL

C. BPDU

D. ARP

**Answer:** A

**Explanation:**

MAC operates at layer 2 which is the data link layer.

183.A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open.

Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware

- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

**Answer:** D

184.An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device.

Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

**Answer:** D

~~185.A systems analyst is responsible for generating a new digital forensics chain of custody form.~~

~~Which of the following should the analyst include in this documentation? (Select TWO).~~

- A. The order of volatility
- B. A checksum
- C. The location of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

**Answer:** A,E

186.An organization has decided to host its web application and database in the cloud.

Which of the following BEST describes the security concerns for this decision?

- A. Access to the organization's servers could be exposed to other cloud-provider clients
- B. The cloud vendor is a new attack vector within the supply chain
- C. Outsourcing the code development adds risk to the cloud provider
- D. Vendor support will cease when the hosting platforms reach EOL.

**Answer:** B

**Explanation:**

Supply chain attacks piggyback legitimate processes to gain uninhibited access into a business's ecosystem. This attack begins with infiltrating a vendor's security defences. This process is usually much simpler than attacking a victim directly due to the unfortunate myopic cybersecurity practices of many vendors.<sup>26 May 2021</sup>

<https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/#:~:text=That%20insidious%20and%20increasingly%20common,piece%20of%20software%20or%20hardware.>

<https://resources.infosecinstitute.com/topic/cloud-computing-attacks-vectors-and-counter-measures/>

187.The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating
- B. reconnaissance
- C. pharming

D. prepending

**Answer:** B

188.When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization

B. Data masking

**C. Normalization**

D. Obfuscation

**Answer:** C

189.An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload.

Which of the following services would BEST meet the criteria?

A. TLS

B. PFS

**C. ESP**

D. AH

**Answer:** C

190.A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata.

Which of the following would be part of the images if all the metadata is still intact?

**A. The GPS location**

B. When the file was deleted

C. The total number of print jobs

D. The number of copies made

**Answer:** A

191.A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident During which of the following phases of the response process is this activity MOST likely occurring?

A. Containment

**B. Identification**

C. Recovery

D. Preparation

**Answer:** B

~~192.A security engineer has enabled two-factor authentication on all workstations.~~

~~Which of the following approaches are the MOST secure? (Select TWO).~~

~~A. Password and security question~~

~~B. Password and CAPTCHA~~

~~C. Password and smart card~~

~~D. Password and fingerprint~~

E. Password and one-time token

F. Password and voice

**Answer:** C,D

193.A user is concerned that a web application will not be able to handle unexpected or random input without crashing.

Which of the following BEST describes the type of testing the user should perform?

A. Code signing

**B. Fuzzing**

C. Manual code review

D. Dynamic code analysis

**Answer:** B

194.Which of the following relates to applications and systems that are used within an organization without consent or approval?

**A. Shadow IT**

B. OSINT

C. Dark web

D. Insider threats

**Answer:** A

195.An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis.

Which of the following tools should the analyst use to further review the pcap?

A. Nmap

B. cURL

C. Netcat

**D. Wireshark**

**Answer:** D

**Explanation:**

[https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20\(also,packet%20data%20from%20 a%20network.](https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,packet%20data%20from%20 a%20network.)

196.A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment.

Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF

B. RPO

**C. RTO**

D. MTTR

**Answer:** C

197.A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue.

Which of the following BEST explains what happened?

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.
- D. The HVAC was connected to the maintenance vendor.

**Answer:** A

198.A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80 200 200
[02/Feb/2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=../../../../etc/passwd HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

- A. Secure cookies
- B. Input validation**
- C. Code signing
- D. Stored procedures

**Answer:** B

199.A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop.

The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

- A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
- B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file**
- C. An attacker was able to install malware to the C:\asdf234 folder and use it to gain administrator rights and launch Outlook

D. An attacker was able to phish user credentials successfully from an Outlook user profile

**Answer:** B

200.Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.

**B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.**

C. A security control objective cannot be met through a technical change, so the company changes its method of operation

D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

**Answer:** B

201.The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached.

Which of the following would BEST address this security concern?

A. install a smart meter on the staff WiFi.

B. Place the environmental systems in the same DHCP scope as the staff WiFi.

C. Implement Zigbee on the staff WiFi access points.

**D. Segment the staff WiFi network from the environmental systems network.**

**Answer:** D

202.Local guidelines require that all information systems meet a minimum-security baseline to be compliant.

Which of the following can security administrators use to assess their system configurations against the baseline?

A. SOAR playbook

B. Security control matrix

C. Risk management framework

**D. Benchmarks**

**Answer:** D

203.A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet.

Which of the following should the analyst implement to authenticate the entire packet?

**A. AH**

B. ESP

C. SRTP

D. LDAP

**Answer:** A

204.A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager learned the reports were previously sent via email but then quickly

generated and backdated the reports before submitting them via a new email message.

Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody
- B. Inspect the file metadata
- C. Reference the data retention policy
- D. Review the email event logs**

**Answer:** D

205.An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

- A. Reputation damage**
- B. Identity theft
- C. Anonymlization
- D. Interrupted supply chain

**Answer:** A

206.A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility.

Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection**
- B. Cross-over error rate
- C. Efficacy rale
- D. Attestation

**Answer:** A

207.Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

- A. Staging**
- B. Test
- C. Production
- D. Development

**Answer:** A

208.A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed.

Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy**

- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
- D. Refrain from completing a forensic analysis of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

**Answer:** B

**Explanation:**

"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker."

For purposes of knowing, <https://security.opentext.com/tableau/hardware/details/t8u> write blockers like this are the most popular hardware blockers

209.A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network.

Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTR ATT\$CK**
- D. OWASP

**Answer:** C

210.A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.

Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption**
- B. Network usage rules
- C. Geofencing
- D. Containerization**
- E. Application whitelisting
- F. Remote control

**Answer:** A,D

211.A company needs to centralize its logs to create a baseline and have visibility on its security events.

Which of the following technologies will accomplish this objective?

- A. Security information and event management**
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

**Answer:** A

212.Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

- A. An RTO report
- B. A risk register**
- C. A business impact analysis
- D. An asset value register
- E. A disaster recovery plan

**Answer:** B

213.Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly.

Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting**
- C. Data loss prevention
- D. Web application firewalls

**Answer:** B

**Explanation:**

Application whitelisting is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications. In general, a whitelist is an index of approved entities. In information security (infosec), whitelisting works best in centrally managed environments, where systems are subject to a consistent workload.

<https://searchsecurity.techtarget.com/definition/application-whitelisting>

214.A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots.

Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.**
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

**Answer:** C

215.An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day.

The only recent log entry regarding the user's computer is the following:

```

Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80

```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server.

**Answer:** A

216.A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

**Answer:** A

217.An attacker has successfully exfiltrated several non-salted password hashes from an online system.

Given the logs below:

```

Session          : hashcat
Status          : cracked
Hash.Type       : MD5
Hash.Target     : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started    : Fri Mar 10 10:18:45 2020
Recovered       : 1/1 (100%) Digests
Progress        : 28756845 / 450365879 (6.38%) hashes
Time.Stopped    : Fri Mar 10 10:20:12 2020
Password found  : Th3B3stp@55w0rd!

```

Which of the following BEST describes the type of password attack the attacker is performing?

- A. Dictionary
- B. Pass-the-hash
- C. Brute-force
- D. Password spraying

**Answer:** C

218.A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers.

Which of the following tools should the analyst use?

- A. netstat
- B. net share
- C. netcat
- D. nbtstat
- E. net session

**Answer:** A

219.An incident response technician collected a mobile device during an investigation.

Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

**Answer:** A

220.After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company.

Which of the following risk management strategies is the manager adopting?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

**Answer:** C

221.A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing.

The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment.

Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability
- D Replace the business's wired network with a wireless network.

**Answer:** C

222.A network administrator has been asked to design a solution to improve a company's security posture.

The administrator is given the following, requirements?

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

- A. HIDS
- B. NIDS
- C. HIPS
- D. NIPS

**Answer:** D

223.A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack.

Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- A. Open-source intelligence
- B. The dark web
- C. Vulnerability databases

**Answer:** C

224.A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has Just informed investigators that other log files are available for review.

Which of the following did the administrator MOST likely configure that will assist the investigators?

- A. Memory dumps
- B. The syslog server
- C. The application logs
- D. The log retention policy

**Answer:** B

225.A symmetric encryption algorithm Is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Answer:** B

226.Which of the following types of controls is a CCTV camera that is not being monitored?

- A. Detective
- B. Deterrent
- C. Physical
- D. Preventive

**Answer:** A

227.A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes

database resources.

Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location**
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer:** B

**Explanation:**

creating a whole new hot site just because of DDoS seems extremely expensive. Instead, deploying a countermeasure like challenge response would mitigate the DDoS.

<https://www.radware.com/security/ddos-knowledge-center/ddospedia/http-challenge>

[https://www.nexusguard.com/hubfs/Nexusguard\\_Whitepaper\\_DDoS\\_Mitigation\\_EN\\_A4.pdf?t=1487581897757](https://www.nexusguard.com/hubfs/Nexusguard_Whitepaper_DDoS_Mitigation_EN_A4.pdf?t=1487581897757)

228.A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe.

One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:  
Which of the following will the forensics investigator MOST likely determine has occurred?

- A. SQL injection
- A. CSRF**
- B. XSS
- C. XSRF

**Answer:** B

229.A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message.

Which of the following BEST describes the cause of the error?

- A. The examiner does not have administrative privileges to the system**
- B. The system must be taken offline before a snapshot can be created
- C. Checksum mismatches are invalidating the disk image
- D. The swap file needs to be unlocked before it can be accessed

**Answer:** A

230.A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective.

Which of the following would BEST detect the presence of a rootkit in the future?

- C. FDE
- A. NIDS
- B. EDR**
- C. DLP

**Answer:** C

231.A company is designing the layout of a new datacenter so it will have an optimal environmental

temperature.

Which of the following must be included? (Select TWO)

- A. An air gap
- B. A cold aisle**
- C. Removable doors
- D. A hot aisle**
- E. An IoT thermostat
- F. A humidity monitor

**Answer:** B,D

**Explanation:**

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/secure-areas/>

232.A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts.

While reviewing the log files, the analyst discovers the following:

```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.  
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.  
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.  
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.  
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.  
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.  
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.  
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.  
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.  
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.  
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.  
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.  
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.  
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force**

**Answer:** D

**Explanation:**

"Brute force attack in which stolen user account names and passwords are tested against multiple websites." CompTIA SY0-601 Official Study Guide Page 690 This is a poorly worded question and while credential stuffing is a type of brute force attack, the information given does not indicate multiple websites. At best, this looks like a password spraying attack, but it is more likely a brute-force attack. Also note the output reads "unsername" and not "username" - perhaps irrelevant but the little things can and do matter

233.Which of the following control sets should a well-written BCP include? (Select THREE)

- A. Preventive**
- B. Detective
- C. Deterrent

- D. Corrective
- E. Compensating
- F. Physical
- G. Recovery

**Answer:** A,D,G

234.A security analyst is configuring a large number of new company-issued laptops.

The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-technology-overview>

235.A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague.

Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OCSP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

**Answer:** B

236.A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them.

Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.

D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

**Answer:** A

237.The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

**Answer:** A

238.During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset inventory. WiFi access is protected with 256-bit encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode.

Which of the following should the administrator implement to find and remediate the issue? (Select TWO).

- A. Check the SIEM for failed logins to the LDAP directory.
- B. Enable MAC filtering on the switches that support the wireless network.
- C. Run a vulnerability scan on all the devices in the wireless network
- D. Deploy multifactor authentication for access to the wireless network
- E. Scan the wireless network for rogue access points.
- F. Deploy a honeypot on the network

**Answer:** B,E

**Explanation:**

security is pretty good already up to a point, clearly Rogue AP bypass is in the picture MAC filtering on the switch the AP's hang from will ensure the only AP's allowed to touch the core network are approved known AP's and ze "bad guys" will find themselves trapped on an AP island with nowhere to go!

239.An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load.

Which of the following are the BEST options to accomplish this objective'? (Select TWO)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual Power Supply
- F. NIC teaming

Answer: A,D

240.A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the internet.

While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- A. Pass-the-hash
- B. MAC flooding
- D. Directory traversal
- E. ARP poisoning

**Answer:** E

**Explanation:**

<https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning>

241.An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers.

Which of the following is the consultant MOST likely to recommend to prepare for eradication?

- A. Quarantining the compromised accounts and computers, only providing them with network access
- B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
- C. Isolating the compromised accounts and computers, cutting off all network and internet access.
- D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

**Answer:** C

242.A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in.

Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

**Answer:** C

243.An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete.

Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

**Answer: D**

244.A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive data.

Which of the following should a security engineer do to prevent such an attack in the future?

- A. Use password hashing.
- B. Enforce password complexity.
- C. Implement password salting.**
- D. Disable password reuse.

**Answer: C**

245.A large enterprise has moved all it's data to the cloud behind strong authentication and encryption A sales director recently had a laptop stolen and later, enterprise data was found to have been compromised database.

Which of the following was the MOST likely cause?

- A. Shadow IT**
- B. Credential stuffing
- C. SQL injection
- D. Man-in-the-browser
- E. Bluejacking

**Answer: A**

246.Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward**
- D. The data privacy officer.

**Answer: C**

247.A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter.

Which of the following should the security manager implement to achieve the objective?

- A. Segmentation**
- B. Containment
- C. Geofencing
- D. Isolation

**Answer: A**

248.A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office Priority must be given to areas that are currently experiencing latency and connection issues.

Which of the following would be the BEST resource for determining the order of priority?

- A. Nmap

- B. Heat maps
- C. Network diagrams
- D. Wireshark

**Answer:** B

**Explanation:**

engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently.

Site surveys and heat maps provide the following benefits: Identify trouble areas to help eliminate slows speeds and poor performance

249.An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications.

Which of the following BEST represents the type of testing that will occur?

- A. Bug bounty
- B. Black-box
- C. Gray-box
- D. White-box

**Answer:** C

**Explanation:**

250.An attacked is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users.

Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typo squatting
- C. Impersonation
- D. Watering-hole attack

**Answer:** A

251.A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

- A. SQLi
- B. CSRF
- C. Session replay
- D. API

**Answer:** C

252.A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS.  
Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

- A. DNSSEC
- B. Reverse proxy
- C. VPN concentrator
- D. PKI
- E. Active Directory
- F. RADIUS

**Answer:** D,F

253.An organization is concerned that its hosted web servers are not running the most updated version of the software.

Which of the following would work BEST to help identify potential vulnerabilities?

- A. hping3 -S corsptia.org -p 80
- B. nc —1 —v comptia.org -p 80
- C. nmap comptia.org -p 80 —sV
- D. nslookup -port=80 comptia.org

**Answer:** C

254.A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string.  
Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssi
- G. dd

**Answer:** A,C

**Explanation:**

- A - "analyst needs to review the first transactions quickly"
- C - "search the entire series of requests for a particular string"

255.Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

- A. Testing security systems and processes regularly

- B. Installing and maintaining a web proxy to protect cardholder data
- C. Assigning a unique ID to each person with computer access
- D. Encrypting transmission of cardholder data across networks
- E. Benchmarking security awareness training for contractors
- F. Using vendor-supplied default passwords for system passwords

**Answer:** C,D

**Explanation:**

256.A security analyst is hardening a Linux workstation and must ensure it has public keys forwarded to remote systems for secure login.

Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

- A. Forward the keys using ssh-copy-id.
- B. Forward the keys using scp.
- C. Forward the keys using ash -i.
- D. Forward the keys using openssl -s.
- E. Forward the keys using ssh-keygen.

**Answer:** A,B

257.An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims.

Which of the following is the attacker MOST likely attempting?

- A. A spear-phishing attack
- B. A watering-hole attack
- C. Typosquatting
- D. A phishing attack

**Answer:** B

258.A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked.

Which of the following would BEST these requirement?

- A. RA
- B. OCSP
- C. CRL
- D. CSR

**Answer:** B

**Explanation:**

259.Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21] [ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- A. Rainbow table
- B. Dictionary**
- C. Password spraying
- D. Pass-the-hash

**Answer:** B

260.The website <http://companywebsite.com> requires users to provide personal Information, Including security question responses, for registration.

Which of the following would MOST likely cause a data breach?

- A. Lack of input validation
- B. Open permissions
- C. Unsecure protocol**
- D. Missing patches

**Answer:** C

261.Which of the following disaster recovery tests is.

The LEAST time consuming for the disaster recovery team?

- A. Tabletop**
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer:** A

262.An organization blocks user access to command-line interpreters but hackers still managed to invoke the interpreters using native administrative tools.

Which of the following should the security team do to prevent this from Happening in the future?

- A. Implement HIPS to block Inbound and outbound SMB ports 139 and 445.
- B. Trigger a SIEM alert whenever the native OS tools are executed by the user
- C. Disable the built-in OS utilities as long as they are not needed for functionality.**
- D. Configure the AV to quarantine the native OS tools whenever they are executed

**Answer:** C

263.The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

- A. data controller.
- B. data owner
- C. data custodian.**

D. data processor

**Answer:** C

264.A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform.

Which of the following is the BEST approach to implement the desired solution?

- A. OAuth
- B. TACACS+
- C. SAML
- D. RADIUS

**Answer:** A

265.Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

- A. Data encryption
- B. Data masking
- C. Anonymization
- D. Tokenization

**Answer:** A

266.A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard.

Which of the following types of controls should be used to reduce the risk created by this scenario?

- A. B. Physical
- B. Detective
- C. Preventive
- D. Compensating

**Answer:** D

267.A security analyst is reviewing information regarding recent vulnerabilities.

Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS
- D. CVE

**Answer:** D

**Explanation:**

CVE entries are brief. They don't include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations.

Across these different systems, CVE IDs give users a reliable way to tell one unique security flaw from another.

268.Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding
- B. Mandatory vacation**
- C. Job rotation**
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Answer:** B,C

269.A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message.

Which of the following is the MOST likely cause of the issue?

- A. The S/MIME plug-in is not enabled.
- B. The SSL certificate has expired.**
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

**Answer:** B

270.A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the Windows server first.

Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords**
- D. Remove all user accounts.

**Answer:** C

271.Which of the following is an example of risk avoidance?

- A. Installing security updates directly in production to expedite vulnerability fixes
- B. Buying insurance to prepare for financial loss associated with exploits
- C. Not installing new software to prevent compatibility errors**
- D. Not taking preventive measures to stop the theft of equipment

**Answer:** C

272.A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China.

Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers.

Which of the following frameworks should the management team follow?

- A. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

**Answer:** D

273.A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned that servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

**Answer:** BF

274.A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure.

Which of the following technologies will the coffee shop MOST likely use in place of PSK?

- A. WEP
- B. MSCHAP
- C. WPS
- D. SAE

**Answer:** D

**Explanation:**

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.[3][4]. The new standard uses 128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise)[5] and forward secrecy.[6]. The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode

[https://en.wikipedia.org/wiki/Simultaneous\\_Authentication\\_of\\_Equals#:~:text=In%20cryptography%2C%20Simultaneous%20Authentication%20of,password%2Dauthenticated%20key%20agreement%20method](https://en.wikipedia.org/wiki/Simultaneous_Authentication_of_Equals#:~:text=In%20cryptography%2C%20Simultaneous%20Authentication%20of,password%2Dauthenticated%20key%20agreement%20method).

275.The website <http://companywebsite.com> requires users to provide personal information including security responses, for registration. which of the following would MOST likely cause a date breach?

- A. LACK OF INPUT VALIDATION
- B. OPEN PERMISSIONS
- C. UNSCURE PROTOCOL

#### D. MISSING PATCHES

**Answer:** C

276.While investigating a data leakage incident, a security analyst reviews access control to cloud-hosted data.

The following information was presented in a security posture report.

~~Policy to control external application integration: admin authorized only  
- 47 active integration to third-party applications  
- 2 applications authorized by admin  
- 45 applications authorized by users  
- 32 OAuth apps authorize to access data~~

Based on the report, which of the following was the MOST likely attack vector used against the company?

- A. Spyware
- B. Logic bomb
- C. Potentially unwanted programs
- D. Supply chain

**Answer:** D

277.A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data.

The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize  
-AssignDriveLetter C| Format-Volume -DriveLetter C -  
FileSystemLabel "New"-FileSystem NTFS - Full -Force  
-Confirm:$false |
```

Which of the following is the malware using to execute the attack?

- A. PowerShell
- B. Python
- C. Bash
- D. Macros

**Answer:** A

278.A new plug-and-play storage device was installed on a PC in the corporate environment.

Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

- A. Change the default settings on the PC.
- B. Define the PC firewall rules to limit access.
- C. Encrypt the disk on the storage device.
- D. Plug the storage device in to the UPS

**Answer:** C

279.A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly

concerned about an unauthorized party who is intercepting information that is in transit between the two organizations.

Which of the following would address the CSO's concerns?

- A. B. SPF
- B. DMARC
- C. SSL
- D. DKIM
- E. TLS**

**Answer:** E

Reference:

280.A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer.

Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS**
- C. A generator
- D. B. APDU

**Answer:** B

281.During an investigation, a security manager receives notification from local authorities that company proprietary data was found on a former employees home computer. The former employee's corporate workstation has since been repurposed, and the data on the hard drive has been overwritten.

Which of the following would BEST provide the security manager with enough details to determine when the data was removed from the company network?

- A. Properly configured hosts with security logging
- B. Properly configured endpoint security tool with dunting
- C. Properly configured SIEM with retention policies**
- D. Properly configured USB blocker with encryption

**Answer:** C

282.A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business.

Which of the following constraints BEST describes the reason the findings cannot be remediated?

- A. inability to authenticate
- B. Implied trust
- C. Lack of computing power
- D. Unavailable patch**

**Answer:** D

283.An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in

Europe.

To which of the following frameworks should the security officer map the existing controls? (Select TWO).

- A. ISO
- B. PCI DSS**
- C. SOC
- D. GDPR**
- E. CSA
- F. NIST

**Answer:** B,D

284.A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details.

An investigation into the matter reveals the following

- \* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
- \* One of the websites the manager used recently experienced a data breach.
- \* The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

- A. Remote access Trojan
- C. Brute-force
- D. Dictionary
- E. Credential stuffing**
- F. Password spraying

**Answer:** E

285.A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user information between nodes.

Which of the following roles should the developer configure to meet these requirements? (Select TWO).

- A. Identity processor
- B. Service requestor
- C. Identity provider**
- D. Service provider**
- E. Tokenized resource
- F. Notarized referral

**Answer:** C,D

286.A desktop support technician recently installed a new document-scanning software program on a computer However, when the end user tried to launch the program, it did not respond.

Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.

- B. The system was quarantined for missing software updates
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software.

**Answer:** C

287.A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe.

One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

`<a href="https://www.company.com/payto.do?routing=00001111&acct=22223334&amount=250">Click here to unsubscribe</a>`

Which of the following will the forensics investigator MOST likely determine has occurred?

- A. SQL injection
- B. Broken authentication
- C. XSS
- B. XSRF**

**Answer:** D

288.After segmenting the network, the network manager wants to control the traffic between the segments.

Which of the following should the manager use to control the network traffic?

- A. A DMZ
- B. A VPN
- C. A VLAN
- D. An ACL**

**Answer:** D

289.Security analyst must enforce policies to harden an MOM infrastructure.

The requirements are as follows

- Ensure mobile devices can be tracked and wiped.
- Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

- A. Geofencing
- B. Biometric authentication
- C. Geolocation**
- D. Geotagging

**Answer:** C

290.An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model.

Which of the following BEST describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols

C. Default settings

D. Open permissions

**Answer:** C

291.A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices.

Which of the following is a cost-effective approach to address these concerns?

- A. Enhance resiliency by adding a hardware RAID.
- B. Move data to a tape library and store the tapes off site
- C. Install a local network-attached storage.
- D. Migrate to a cloud backup solution**

**Answer:** D

292.Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Hashing**
- B. Private key**
- C. Perfect forward secrecy
- D. Salting
- E. Symmetric keys

**Answer:** A,B

293.During a security assessment, a security finds a file with overly permissive permissions.

Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. 1s
- B. chflags
- C. chmod**
- D. lsof
- E. setuid

sarath@localhost ~]\$ chmod 4755 /path/to/file/or/executable

**Answer:** C

**Explanation:**

Reference:

<https://www.computerhope.com/jargon/s/setuid.htm#:~:text=Setuid%2C%20which%20stands%20for%20set,certain%20programs%20with%20escalated%20privileges>

294.Which of the following is the correct order of volatility from MOST to LEAST volatile?

- A. Memory, temporary filesystems, routing tables, disk, network storage
- B. Cache, memory, temporary filesystems, disk, archival media**
- C. Memory, disk, temporary filesystems, cache, archival media
- D. Cache, disk, temporary filesystems, network storage, archival media

**Answer:** B

295.A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols.

A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

- A. Allow DNS access from the internet.
- B. Block SMTP access from the Internet
- C. Block HTTPS access from the Internet
- D. Block SSH access from the Internet.**

**Answer:** D

296.A security operations analyst is using the company's SIEM solution to correlate alerts.

Which of the following stages of the incident response process is this an example of?

- A. C. Eradication
- B. Recovery
- C. Identification**
- D. Preparation

**Answer:** C

297.Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

- A. A right-to-audit clause allowing for annual security audits**
- B. Requirements for event logs to be kept for a minimum of 30 days
- C. Integration of threat intelligence in the company's AV
- D. A data-breach clause requiring disclosure of significant data loss

**Answer:** A

298.Which of the following is a reason why an organization would define an AUP?

- A. To define the lowest level of privileges needed for access and use of the organization's resources
- B. To define the set of rules and behaviors for users of the organization's IT systems**
- C. To define the intended partnership between two organizations
- D. To define the availability and reliability characteristics between an IT provider and consumer

**Answer:** B

299.Which of the following would satisfy three-factor authentication?

- A. Password, retina scanner, and NFC card**
- B. Password, fingerprint scanner, and retina scanner
- C. Password, hard token, and NFC card

D. Fingerprint scanner, hard token, and retina scanner

**Answer:** A

300.A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2fetc2fpasswd  
GET index.php?page=..2f..2f..2f..2f..2f..2f..2fetc2fpasswd  
GET index.php?page=..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal

B. SQL injection

C. API

D. Request forgery

**Answer:** A

301.A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel.

Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

**Answer:** A

302.An organization's finance department is implementing a policy to protect against collusion.

Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

A. Corrective

B. Deterrent

C. Preventive

D. Mandatory vacations

E. Job rotation

F. Separation of duties

**Answer:** E,F

303.Which of the following controls would BEST identify and report malicious insider activities?

A. An intrusion detection system

B. A proxy

C. Audit trails

D. Strong authentication

**Answer:** A

**Explanation:**

An intrusion detection system (IDS; also intrusion protection system or IPS) is a device or software application that monitors a network or systems for malicious activity or policy violations.[1] Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

304.A cyberthreat intelligence analyst is gathering data about a specific adversary using OSINT techniques.

Which of the following should the analyst use?

- A. Internal log files
- B. Government press releases
- C. Confidential reports
- D. Proprietary databases

**Answer:** A

**Explanation:**

<https://www.eccouncil.org/cyber-threat-intelligence/>

305.The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted file. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again.

Which of the following is MOST capable of accomplishing both tasks?

- A. HIDS
  - B. Allow list
  - C. TPM
  - D. NGFW
- Answer:** D
- Network based question  
A next generation firewall (NGFW) is, as Gartner defines it, a “deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.”

306.A company recently experienced an attack during which its main website was directed to the attacker’s web server, allowing the attacker to harvest credentials from unsuspecting customers.

Which of the following should the company implement to prevent this type of attack occurring in the future?

- A. IPSec
- B. SSL/TLS
- C. DNSSEC
- D. S/MIME

**Answer:** C

307.A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters.

Which of the following is the primary use case for this scenario?

- A. Implementation of preventive controls

- B. Implementation of detective controls
- C. Implementation of deterrent controls
- D. Implementation of corrective controls

**Answer:** B

308.Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

- A. RTO
- B. MTBF
- C. MTTR
- D. RPO

**Answer:** C

**Explanation:**

Mean time to repair (MTTR) is a measure of the maintainability of a repairable item, which tells the average time required to repair a specific item or component and return it to working status. It is a basic measure of the maintainability of equipment and parts. This includes the notification time, diagnosis and the time spent on actual repair as well as other activities required before the equipment can be used again. Mean time to repair is also known as mean repair time.

<https://www.techopedia.com/definition/2719/mean-time-to-repair-mttr>

309.Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

- A. Development
- B. Staging
- C. Production
- D. Test

**Answer:** A

310.Which of the following corporate policies is used to help prevent employee fraud and to detect system log modifications or other malicious activity based on tenure?

- A. Background checks
- B. Mandatory vacation
- C. Social media analysis
- D. Separation of duties

**Answer:** B

### 311.HOTSPOT

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

### INSTRUCTIONS

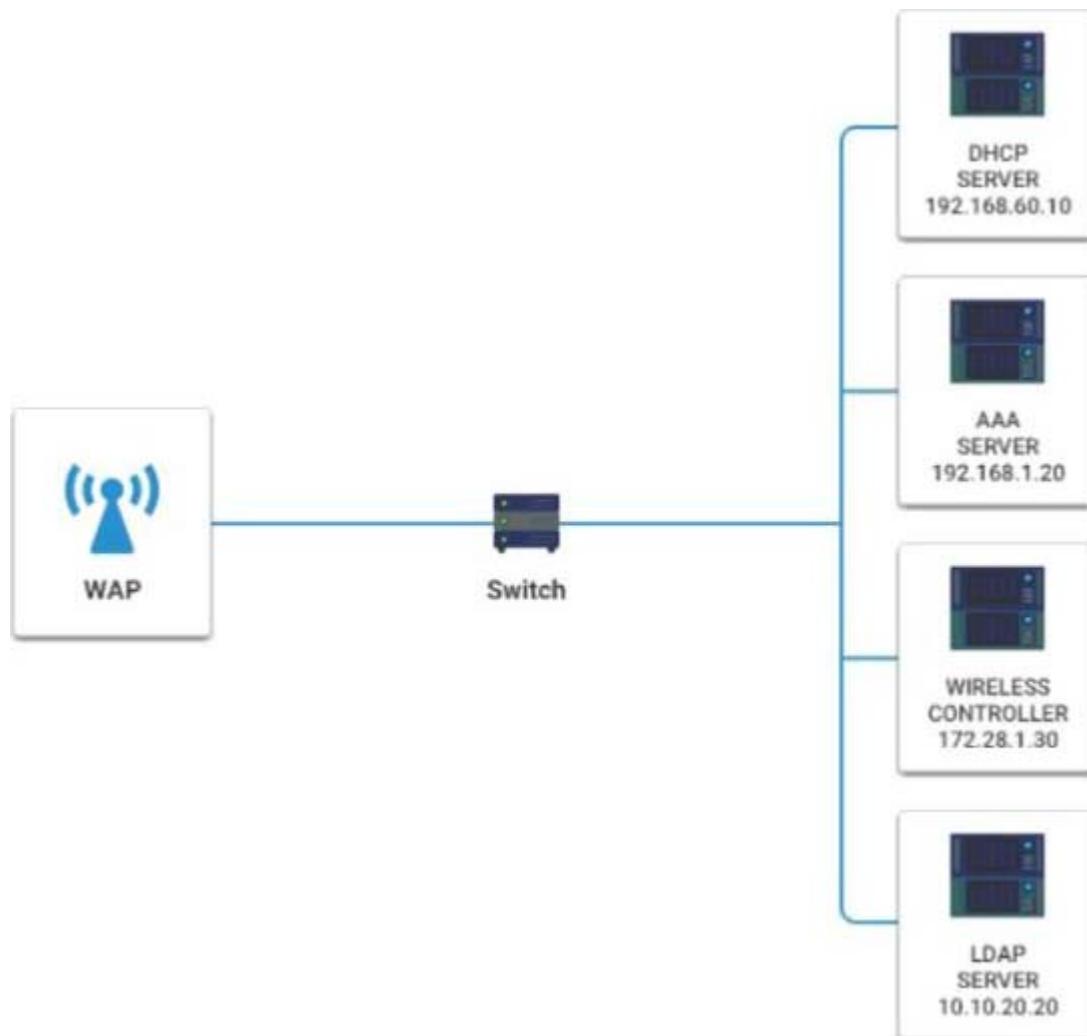
Please click on the below items on the network diagram and configure them accordingly:

- WAP
- DHCP Server
- AAA Server

⟳ Wireless Controller

⟳ LDAP Server

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



**Wireless Access Point**

Basic Wireless Settings		Wireless Security
Wireless Network Mode:	<input type="button" value="MIXED"/> <input type="button" value="B ONLY"/> <input type="button" value="G ONLY"/>	
Wireless Network Name(SSID):	DEFAULT	
Wireless Channel:	<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> <input type="button" value="6"/> <input type="button" value="7"/> <input type="button" value="8"/> <input type="button" value="9"/> <input type="button" value="10"/> <input type="button" value="11"/>	
Wireless SSID Broadcast:	<input checked="" type="radio"/> enable <input type="radio"/> disable	
<input type="button" value="Cancel Changes"/> <input type="button" value="Save Settings"/>		

**Wireless Access Point**

Basic Wireless Settings		Wireless Security
Security Mode:	<input type="button" value="Disabled"/> <input type="button" value="WEP"/> <input type="button" value="WPA Enterprise"/> <input type="button" value="WPA Personal"/> <input type="button" value="WPA2 Enterprise"/> <input type="button" value="WPA2 Personal"/> <input type="button" value="RADIUS"/>	
<input type="button" value="Cancel Changes"/> <input type="button" value="Save Settings"/>		

**Answer:**

**Wireless Access Point**

Basic Wireless Settings		Wireless Security
Wireless Network Mode:	<input type="button" value="MIXED"/> <input type="button" value="B ONLY"/> <input type="button" value="G ONLY"/>	
Wireless Network Name(SSID):	DEFAULT	
Wireless Channel:	<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> <input type="button" value="6"/> <input type="button" value="7"/> <input type="button" value="8"/> <input type="button" value="9"/> <input type="button" value="10"/> <input type="button" value="11"/>	
Wireless SSID Broadcast:	<input checked="" type="radio"/> enable <input type="radio"/> disable	
<input type="button" value="Cancel Changes"/> <input type="button" value="Save Settings"/>		

**Wireless Access Point**

Basic Wireless Settings		Wireless Security
Security Mode:	<input type="button" value="Disabled"/> <input type="button" value="WEP"/> <input type="button" value="WPA Enterprise"/> <input type="button" value="WPA Personal"/> <input type="button" value="WPA2 Enterprise"/> <input type="button" value="WPA2 Personal"/> <input type="button" value="RADIUS"/>	
<input type="button" value="Cancel Changes"/> <input type="button" value="Save Settings"/>		

**Explanation:**

Wireless Access Point

Network Mode – G only

Wireless Channel – 11

Wireless SSID Broadcast – disable

Security settings – WPA2 Professional

312.A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support.

Which of the following should the administrator employ to meet these criteria?

- A. Implement NAC.
- B. Implement an SWG.
- C. Implement a URL filter.
- D. Implement an MDM.

A secure web gateway (SWG) protects users from web-based threats in addition to applying and enforcing corporate acceptable use policies

**Answer:** B

313.A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN.

Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

**Answer:** B,F

314.A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds.

Which of the following types of attacks does this scenario describe?

- B. (A)Vishing
- C. Phishing
- D. Spear phishing
- E. Whaling

**Answer:** A

**Explanation:**

Reference: [https://en.wikipedia.org/wiki/Voice\\_phishing](https://en.wikipedia.org/wiki/Voice_phishing)

Voice\_phishing

315.A user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides.

Which of the following authentication concepts are in use?

- A. Something you know, something you have, and somewhere you are
- B. Something you know, something you can do, and somewhere you are
- C. Something you are, something you know, and something you can exhibit
- D. Something you have, somewhere you are, and someone you know

**Answer:** A

316.A security analyst is reviewing the following output from a system:

```
TCP 192.168.10.10:80 192.168.1.2:60101 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60102 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60103 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60104 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60105 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60106 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60107 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60108 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60109 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60110 TIME_WAIT
```

Which of the following is MOST likely being observed?

- A. ARP poisoning
- B. Man in the middle
- C. Denial of service
- D. DNS poisoning

**Answer:** C

317.

After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time.

Which of the following BEST explains what happened?

- A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
- B. Multiple alerts were generated due to an attack occurring at the same time.
- C. An error in the correlation rules triggered multiple alerts.
- D. The SIEM was unable to correlate the rules, triggering the alerts.

**Answer:** A

318.After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session.

Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

**Answer:** B

**Explanation:**

In session attack the hacker take over the session of a user by hacking its session id

319.Which of the following types of attacks is specific to the individual it targets?

- A. Whaling
- B. Pharming
- C. Smishing
- D. Credential harvesting

**Answer:** A

320.A network administrator at a large organization Is reviewing methods to improve the security of the wired LAN Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only.

Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. SSO to authenticate corporate users
- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

**Answer:** C

321.A security an analyst needs to implement security features across smartphones, laptops, and tablets.

Which of the following would be the MOST effective across heterogeneous platforms?

- A. Enforcing encryption
- B. Deploying GPOs
- C. Removing administrative permissions
- D. Applying MDM software

**Answer:** D

322.Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

- A. An inability to monitor 100%, of every facility could expose the company to unnecessary risk.
- B. The cameras could be compromised if not patched in a timely manner.
- C. Physical security at the facility may not protect the cameras from theft.
- D. Exported videos may take up excessive space on the file servers.

**Answer:** B

323.A security analyst b concerned about traffic initiated to the dark web from the corporate LAN.

Which of the following networks should he analyst monitor?

- D. A:: SFTP
- E. B:: AS
- F. C:: TOR
- G. D: IoC
- H. **Answer:** C

324.A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- [www.companysite.com](http://www.companysite.com)
- [shop.companysite.com](http://shop.companysite.com)
- [about-us.companysite.com](http://about-us.companysite.com)
- [contact-us.companysite.com](http://contact-us.companysite.com)
- [secure-logon.companysite.com](http://secure-logon.companysite.com)

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate
- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate**
- E. An extended validation certificate

**Answer:** D

325.A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced.

Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack**
- D. A logic bomb
- E. Misconfigured BIOS

**Answer:** C

326.Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB**
- C. UTM
- D. EDR

**Answer:** B

327.Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

- A. Unsecured root accounts
- B. Zero day
- C. Shared tenancy**
- D. Insider threat

**Answer:** C

328.A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security strategy for mitigating risks within the perimeter.

Which of the following solutions would BEST support the organization's strategy?

- A FIM
- B
- C EDR
- D UTM

329.An organization recently acquired an ISO 27001 certification.

Which of the following would MOST likely be considered a benefit of this certification?

- A. It allows for the sharing of digital forensics data across organizations
- B. It provides insurance in case of a data breach
- C. It provides complimentary training and certification resources to IT security staff.
- D. It certifies the organization can work with foreign entities that require a security clearance
- E. It assures customers that the organization meets security standards

**Answer:** E

**Explanation:**

According to the ISO <https://www.iso.org/standard/54534.html>

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

330.A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks.

Which of the following would be the BEST control for the company to require from prospective vendors'?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

**Answer:** B

331.Which of the following represents a biometric FRR?

- A. Authorized users being denied access
- B. Users failing to enter the correct PIN
- C. The denied and authorized numbers being equal
- D. The number of unauthorized users being granted access

**Answer:** A

Reference: <https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience>

332.A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security.

Which of the following configuration should an analyst enable to improve security? (Select Two)

- A. RADIUS
- B. PEAP
- C. WPS
- D. WEP-TKIP
- E. SSL
- F. WPA2-PSK

**Answer:** A,F

333.A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating.

The incident, the analyst identified the following Input in the username field:

`admin' or 1=1--`

Which of the following BEST explains this type of attack?

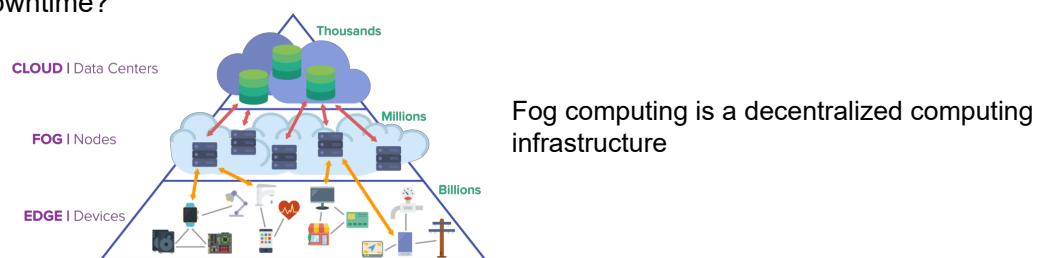
- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication
- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

**Answer:** B

334.Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

- A. MSSP
- B. Public cloud
- C. Hybrid cloud
- D. Fog computing

**Answer:** D

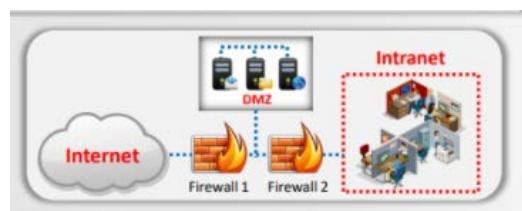


335.A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks.

When of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. VLAN
- D. A screened subnet

**Answer:** D



336.DRAG DROP

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

- Hostname: ws01

- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left hand column and values belong in the right hand column.

Server		Certificate Signing Request	
Hostname:	ws01	Extension	Value
Domain:	comptia.org		
IPv4:	10.1.9.50		
IPv4:	10.2.10.50		
Root:	home.aspx		
DNS CNAME:	homesite		
Extensions			
subjectAltName	commonname		
subjectAltName	intermediateKeyUsage		
Values			
serverAuth			
OCSP URI: http://ocsp.pki.comptia.org			
URL=http://homesite.comptia.org/home.aspx			
ws01.comptia.org			
DNS Name=*.comptia.org			
identAuth			
DNS Name=homesite.comptia.org			

**Answer:**

**Server**

Hostname:	ws01
Domain:	comptia.org
IPv4:	10.1.9.50
IPv4:	10.2.10.50
Root:	home.aspx
DNS CHANNE:	homewebsite

**Extensions**

policyIdentifier	commonName
subjectAltName	extendedKeyUsage

**Values**

serverAuth
OCSP:URI:http://ocsp.pki.comptia.org
URL=http://homewebsite.comptia.org/home.aspx
ws01.comptia.org
DNS Name=*.comptia.org
clientAuth
DNS Name=homewebsite.comptia.org

**Certificate Signing Request**

Extension	Value
commonName	ws01.comptia.org
extendedKeyUsage	OCSP:URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homewebsite.comptia.org/home.aspx
subjectAltName	DNS Name=*.comptia.org


**Explanation:**

Graphical user interface, application

Description automatically generated

337.A security analyst has been reading about a newly discovered cyber attack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

- A. Security research publications
- B. The MITRE ATT&CK framework**
- C. The Diamond Model of Intrusion Analysis
- D. The Cyber Kill Chain

**Answer:** B

338.Which of the following often operates in a client-server architecture to act as a service repository. providing enterprise consumers access to structured threat intelligence data?

- C. STIX
- D. CIRT
- E. OSINT
- F. TAXII**

**Answer:** F

339.Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP**

- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Answer:** A

340.Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

- A. Hashing
- B. Salting
- C. Integrity
- D. Digital signature

**Answer:** A

341.A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage.

Which of the following BEST describes these threat actors?

- A. Semi-authorized hackers
- B. State actors
- C. Script kiddies
- D. Advanced persistent threats

**Answer:** B

342.A systems analyst is responsible for generating a new digital forensics chain-of-custody form.

Which of the following should the analyst include in this documentation? (Choose two.)

- A. The order of volatility
- B. A CRC32 checksum
- C. The provenance of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

**Answer:** B,E

343.Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody.

Which of the following should Ann use?

- A. Chain of custody
- B. Checksums
- C. Non-repudiation
- D. Legal hold

**Answer:** B

344.A systems administrator needs to install the same X.509 certificate on multiple servers.

Which of the following should the administrator use?

- A. Key escrow
- B. A self-signed certificate**
- C. Certificate chaining
- D. An extended validation certificate

**Answer:** B

345.Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

- A. Production
- B. Test**
- C. Staging
- D. Development

**Answer:** B

346.A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account.

Which of the following types of service providers is being used?

- A. Telecommunications service provider
- B. Cloud service provider**
- C. Master managed service provider
- D. Managed security service provider

**Answer:** B

347.A cloud administrator is configuring five compute instances under the same subnet in a VPC Three instances are required to communicate with one another, and the other two must he logically isolated from all other instances in the VPC.

Which of the following must the administrator configure to meet this requirement?

- A. One security group
- B. Two security groups
- C. Three security groups**
- D. Five security groups

**Answer:** C

348.A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

- A. Preventive
- B. Compensating
- C. Corrective
- D. Detective**

**Answer:** D

349.A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network.

Which of the following would BEST support the office's business needs? (Select TWO)

- A. Installing WAPs with strategic placement
- B. Configuring access using WPA3
- C. Installing a WIDS
- D. Enabling MAC filtering
- E. Changing the WiFi password every 30 days
- F. Reducing WiFi transmit power throughout the office

**Answer:** B,D

350.A security analyst is investigating a malware incident at a company. The malware is accessing a command-and-control website at www.comptia.com. All outbound Internet traffic is logged to a syslog server and stored in /logfiles/messages.

Which of the following commands would be BEST for the analyst to use on the syslog server to search for recent traffic to the command-and-control website?

- A. head -500 www.comptia.com | grep /logfiles/messages
- B. cat /logfiles/messages | tail -500 www.comptia.com
- C. tail -500 /logfiles/messages | grep www.comptia.com
- D. grep -500 /logfiles/messages | cat www.comptia.com

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** C

351.A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery.

Which of the following resiliency techniques will provide these capabilities?

- A. Redundancy
- B. RAID 1+5
- C. Virtual machines
- D. Full backups

**Answer:** D

352.A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage.

Which of the following is MOST likely the cause?

- A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.

- B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
- C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
- D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

**Answer:** D

353.Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

- A. Production
- B. Test
- C. Research and development
- D. PoC
- E. UAT
- F. SDLC

User acceptance testing (UAT) is the safeguard against such unfinished, ineffective or faulty software products reaching rollout.

**Answer:** B,E

354.Which of the following holds staff accountable while escorting unauthorized personnel?

- A. B. Locks
- B. Badges
- C. Cameras
- D. Visitor logs

**Answer:** B

355.An attacker was easily able to log in to a company's security camera by performing a baste online search for a setup guide for that particular camera brand and model.

Which of the following BEST describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols
- C. Default settings
- D. Open permissions

**Answer:** C

356.A security analyst is hardening a network infrastructure.

The analyst is given the following requirements;

- Preserve the use of public IP addresses assigned to equipment on the core router.
- Enable "in transport 'encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Select TWO).

- A. Configure VLANs on the core router
- B. Configure NAT on the core router
- C. Configure BGP on the core router
- D. Configure AES encryption on the web server

- E. Enable 3DES encryption on the web server
- F. Enable TLSv2 encryption on the web server

**Answer:** B,F

357.A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports.

Which of the following attacks is happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- A. Jamming
- B. Rogue access point
- C. Disassociation

**Answer:** B

358.An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services.

Given this output from Nmap:

PORT	STATE
21/tcp	filtered
22/tcp	open
23/tcp	open
443/tcp	open

Which of the following should the analyst recommend to disable?

- A. 21/tcp
- B. 22/tcp
- C. 23/tcp
- D. 443/tcp

**Answer:** C

359.

A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files, and can work in conjunction with proxies or UTM.

Which of the following would BEST meet the CSO's requirements?

- A. Fuzzing
- B. Sandboxing
- C. Static code analysis
- D. Code review

**Answer:** B

360.A security researcher is attempting to gather data on the widespread use of a Zero-day exploit.

Which of the following will the researcher MOST likely use to capture this data?

- A. A DNS sinkhole
- B. A honeypot**
- C. A vulnerability scan
- D. cvss

**Answer:** B

361.An organization is building backup server room in geographically diverse locations. The Chief information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing sewer room.

Which of the following should the systems engineer consider?

- A. Purchasing hardware from different vendors**
- B. Migrating workloads to public cloud infrastructure
- C. Implementing a robust patch management solution
- D. Designing new detective security controls

**Answer:** A      Since it is an INHOUSE build -- Vendor Diversity - nothing about outsourcing to cloud

362.A company is implementing an insider threat detection program,. The primary concern is that users may be accessing confidential data without authorization.

Which of the fallowing should be deployed to detect a potential insider threat?

- A. A honeyfile**
- B. A DMZ
- C. ULF
- B. File integrity monitoring

**Answer:** A

363.A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location.

Which of the following would BEST meet the architect's objectives?

- A. Trusted Platform Module
- B. IaaS
- C. HSMaaS**
- D. PaaS
- E. Key Management Service

**Answer:** C

364.Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.

Which of the following documents did Ann receive?

- A. An annual privacy notice**
- B. A non-disclosure agreement
- C. A privileged-user agreement

D. A memorandum of understanding

**Answer:** A

365.An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

A. MDM

B. MAM

C. VDI

D. DLP

**Answer:** A

366.If a current private key is compromised, which of the following would ensure it cannot be used to decrypt all historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

**Answer:** A

367.An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account.

Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.

B. Perform only non-intrusive scans of workstations.

C. Use non-credentialed scans against high-risk servers.

D. Log and alert on unusual scanner account logon times.

**Answer:** D

368.A user's account is constantly being locked out.

Upon further review, a security analyst found the following in the SIEM

Time		Log Message
9:00:00 AM	login: user	password: aBG23TMV
9:00:01 AM	login: user	password: aBG33TMV
9:00:02 AM	login: user	password: aBG43TMV
9:00:03 AM	login: user	password: aBG53TMV

Which of the following describes what is occurring?

A. An attacker is utilizing a password-spraying attack against the account.

B. An attacker is utilizing a dictionary attack against the account.

C. An attacker is utilizing a brute-force attack against the account.

D. An attacker is utilizing a rainbow table attack against the account.

**Answer:** C

369.Remote workers in an organization use company-provided laptops with locally installed applications

and locally stored data. Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public.

Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE

B. TPM

C. HIDS

D. VPN

**Answer:** A

370. The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3$"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history

B. Account expiration

C. Password complexity

D. Account lockout

**Answer:** D

371. A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications. After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes.

Which of the following would BEST meet the CSO's objectives?

A. DLP

B. SWG

C. CASB

D. Virtual network segmentation

E. Container security

**Answer:** A

372. An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box.

Which of the following should be the first lines of defense against such an attack? (Select TWO).

A. MAC filtering

B. Zero Trust segmentation

C. Network access control

D. Access control vestibules

C. Guards [F]

D. Bollards [G]

**Answer:** D,F

373.A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords.

Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering

C. 802.1X

D. Captive portal

E. WPS

**Answer:** E

374.A security analyst has received several reports of an issue on an internal web application. Users stale they are having to provide their credential twice lo log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several loos the analyst decades to run some commands on the gateway and obtains the following output

Internet address

Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0c-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding

B. URL redirection

C. ARP poisoning

D. DNS hijacking

**Answer:** C

375.An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly.

Which of the following should the engineer select to meet these requirements?

A. Laptops

B. Containers

C. Thin clients

D. Workstations

**Answer:** C

376.Which of the following should a technician consider when selecting an encryption method for data

that needs to remain confidential for a specific length of time?

- A. The key length of the encryption algorithm
- B. The encryption algorithm's longevity**
- C. A method of introducing entropy into key calculations
- D. The computational overhead of calculating the encryption key

**Answer:** B

The estimated time period during which data protected by a specific cryptographic algorithm remains secure, given that the key has not been compromised. The estimated time period during which data protected by a specific cryptographic algorithm remains secure

377. When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

- A. Z-Wave compatibility
- B. Network range
- C. Zigbee configuration
- D. Communication protocols**

**Answer:** D

378. After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices.

Which of the following will achieve the administrator's goal? (Select TWO).

- A. Disabling guest accounts**
- B. Disabling service accounts
- C. Enabling network sharing
- D. Disabling NetBIOS over TCP/IP**
- E. Storing LAN manager hash values
- F. Enabling NTLM

**Answer:** A,D

379. A security researcher is tracking an adversary by noting its attack and techniques based on its capabilities, infrastructure, and victims.

Which of the following is the researcher MOST likely using?

- A. The Diamond Model of intrusion Analysis**
- B. The Cyber Kill Chain\
- C. The MITRE CVE database
- D. The incident response process

**Answer:** A

**Explanation:**

Reference:

<https://cyware.com/educational-guides/incident-response/what-is-the-diamond-model-of-intrusion-analysis-5f02>

380. Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

- A. ISO 27701
- B. The Center for Internet Security

C. SSAE SOC 2

D. NIST Risk Management Framework

**Answer:** D

381.A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down.

Which of the following should the administrator implement to avoid disruption?

A. NIC teaming

B. High availability

resiliency in data centers is dual hardware - NIC/Dual Power

C. Dual power supply

a note for other like questions

B. IaaS

**Answer:** B

382.Several employees have noticed other bystanders can clearly observe a terminal where passcodes are being entered.

Which of the following can be eliminated with the use of a privacy screen?

A. Shoulder surfing

B. Spear phishing

C. Impersonation attack

D. Card cloning

**Answer:** A

383.Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

A. An NDA

B. An AUP

C. An ISA

D. An MOU

**Answer:** A

384.DRAG DROP

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

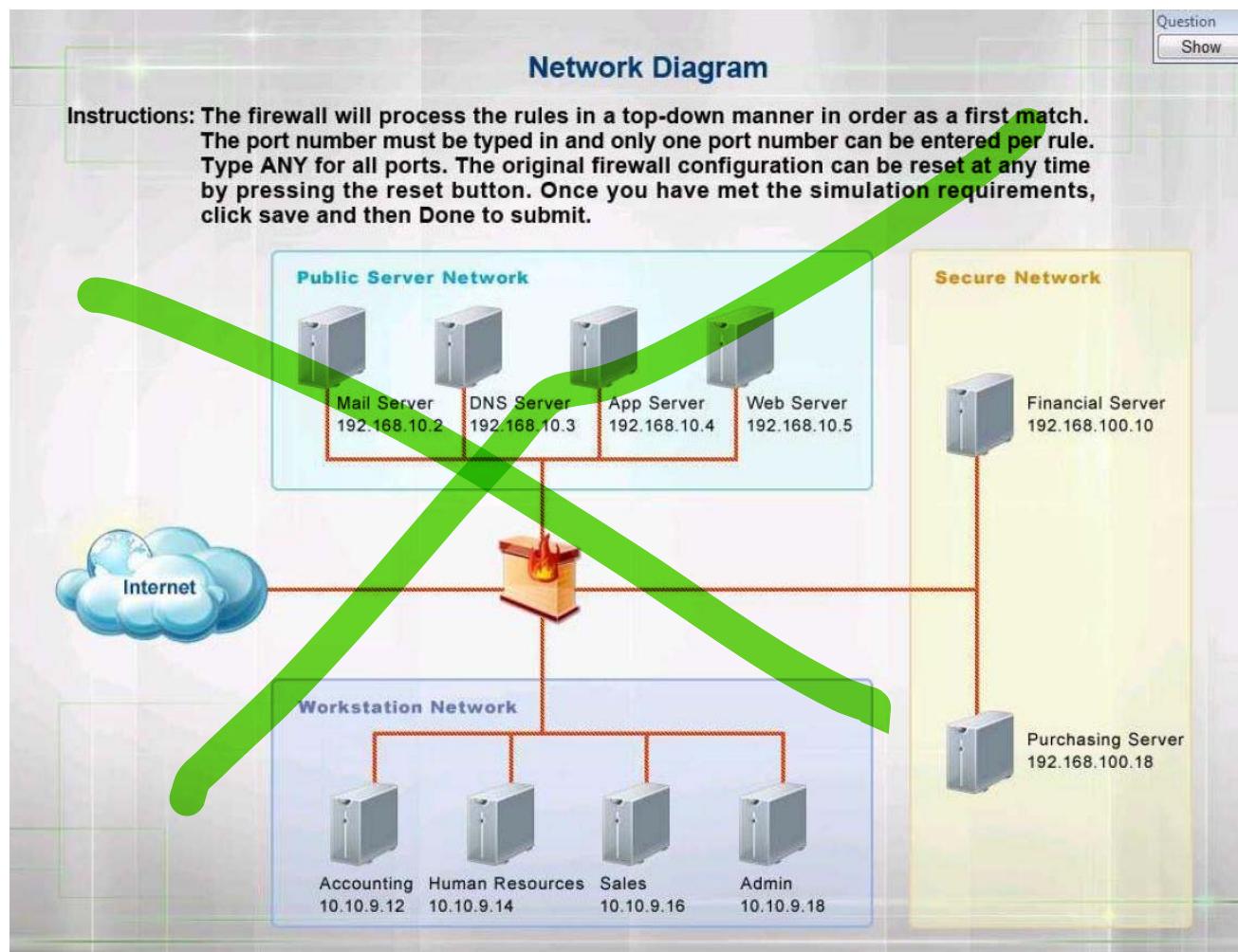
#### **INSTRUCTIONS:**

Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The

original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Hot Area:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 10.10.9.12/32 <input type="checkbox"/> 10.10.9.14/32 <input type="checkbox"/> 10.10.9.18/32	<input type="checkbox"/> Any <input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 192.168.100.10/32 <input type="checkbox"/> 192.168.100.18/32	<input type="checkbox"/> 443 <input type="checkbox"/> 22 <input type="checkbox"/> 69	<input type="checkbox"/> ANY <input type="checkbox"/> TCP <input type="checkbox"/> UDP	<input type="checkbox"/> Permit <input type="checkbox"/> Deny
2	<input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 10.10.9.12/32 <input type="checkbox"/> 10.10.9.14/32 <input type="checkbox"/> 10.10.9.18/32	<input type="checkbox"/> Any <input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 192.168.100.10/32 <input type="checkbox"/> 192.168.100.18/32	<input type="checkbox"/> 443 <input type="checkbox"/> 22 <input type="checkbox"/> 69	<input type="checkbox"/> ANY <input type="checkbox"/> TCP <input type="checkbox"/> UDP	<input type="checkbox"/> Permit <input type="checkbox"/> Deny
3	<input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 10.10.9.12/32 <input type="checkbox"/> 10.10.9.14/32 <input type="checkbox"/> 10.10.9.18/32	<input type="checkbox"/> Any <input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 192.168.100.10/32 <input type="checkbox"/> 192.168.100.18/32	<input type="checkbox"/> 443 <input type="checkbox"/> 22 <input type="checkbox"/> 69	<input type="checkbox"/> ANY <input type="checkbox"/> TCP <input type="checkbox"/> UDP	<input type="checkbox"/> Permit <input type="checkbox"/> Deny
4	<input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 10.10.9.12/32 <input type="checkbox"/> 10.10.9.14/32 <input type="checkbox"/> 10.10.9.18/32	<input type="checkbox"/> Any <input type="checkbox"/> 192.168.10.2/32 <input type="checkbox"/> 192.168.10.3/32 <input type="checkbox"/> 192.168.10.4/32 <input type="checkbox"/> 192.168.10.5/32 <input type="checkbox"/> 192.168.100.10/32 <input type="checkbox"/> 192.168.100.18/32	<input type="checkbox"/> 443 <input type="checkbox"/> 22 <input type="checkbox"/> 69	<input type="checkbox"/> ANY <input type="checkbox"/> TCP <input type="checkbox"/> UDP	<input type="checkbox"/> Permit <input type="checkbox"/> Deny

**Answer:**

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<input type="button" value="Remove"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>10.10.9.12/32</b> <b>10.10.9.14/32</b> <b>10.10.9.18/32</b>	<input type="button" value="Remove"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>192.168.100.10/32</b> 192.168.100.18/32	<input type="button" value="Remove"/> 443 22 69	ANY TCP UDP	<input type="button" value="Permit"/> <input type="button" value="Deny"/>
2	<input type="button" value="Remove"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>10.10.9.12/32</b> <b>10.10.9.14/32</b> <b>10.10.9.18/32</b>	<input type="button" value="Remove"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>192.168.100.10/32</b> 192.168.100.18/32	<input type="button" value="Remove"/> 443 22 69	ANY TCP UDP	<input type="button" value="Permit"/> <input type="button" value="Deny"/>
3	<input type="button" value="Remove"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>10.10.9.12/32</b> <b>10.10.9.14/32</b> <b>10.10.9.18/32</b>	<input type="button" value="Remove"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>192.168.100.10/32</b> 192.168.100.18/32	<input type="button" value="Remove"/> 443 22 <b>69</b>	ANY TCP UDP	<input type="button" value="Permit"/> <input type="button" value="Deny"/>
4	<input type="button" value="Remove"/> 192.168.10.2/32 192.168.10.3/32 <b>192.168.10.4/32</b> 192.168.10.5/32 <b>10.10.9.12/32</b> <b>10.10.9.14/32</b> <b>10.10.9.18/32</b>	<input type="button" value="Remove"/> Any 192.168.10.2/32 192.168.10.3/32 <b>192.168.10.4/32</b> 192.168.10.5/32 <b>192.168.100.10/32</b> 192.168.100.18/32	<input type="button" value="Remove"/> 443 22 <b>69</b>	ANY TCP UDP	<input type="button" value="Permit"/> <input type="button" value="Deny"/>

**Explanation:**

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

Graphical user interface

Description automatically generated with medium confidence

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.14/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

Graphical user interface

Description automatically generated

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443. Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22. Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References: Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

385.Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling

- B. Spam
- C. Invoice scam
- D. Pharming

**Answer:** D

386.An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics.

Which of the following should the organization consult for the exact requirements for the cloud provider?

- A. SLA
- B. BPA
- C. NDA
- D. MOU

**Answer:** A

387.A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread.

Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody.
- B. Inspect the file metadata.
- C. Reference the data retention policy.
- D. Review the email event logs

**Answer:** B

388.Customers reported their antivirus software flagged one of the company's primary software products as suspicious. The company's Chief Information Security Officer has tasked the developer with determining a method to create a trust model between the software and the customer's antivirus software.

Which of the following would be the BEST solution?

- A. Code signing
- B. Domain validation
- C. Extended validation
- A. Self-signing

**Answer:** A      PKI is a TRUST MODEL -- code signing provides Authentication and non-rep

389Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access.

Which of the following types of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

**Answer:** C

390.While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device.

Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

- A. Conduct a ping sweep.
- B. Physically check each system,
- C. Deny Internet access to the "UNKNOWN" hostname.
- D. Apply MAC filtering,

**Answer:** D

391.An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day.

Which of the following VPN solutions would BEST support the new office?

- A. Always On
- B. Remote access
- C. Site-to-site
- D. Full tunnel

**Answer:** C

392.A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees.

Which of the following controls. should the company consider using as part of its IAM strategy? (Select TWO).

- A. A complex password policy
- B. Geolocation
- C. An impossible travel policy
- D. Self-service password reset
- E. Geofencing
- F. Time-based logins

**Answer:** B,F

393.A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS.

Which of the following is the MOST likely attack type?

- A. Request forgery
  - B. Session replay
  - C. DLL injection
  - D. Shimming**
- Answer:** D

64 bit API can communicate with 32 bit API  
in the 90's called THUNKING LOL

394.Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

- A. Something you exhibit
- B. Something you can do
- C. Someone you know
- D. Somewhere you are**

**Answer:** D

395.A security analyst is investigating a vulnerability in which a default file permission was set incorrectly.  
The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

- A. ssh
- B. chmod**
- C. 1s
- D. setuid
- E. nessus
- F. nc

**Answer:** B

Reference:

<https://www.freecodecamp.org/news/the-linux-ls-command-how-to-list-files-in-a-directory-with-options/>

396.An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services.

Given this output from Nmap.

PORT	STATE
21/tcp	filtered
22/tcp	open
23/tcp	open
443/tcp	open

Which of the following should the analyst recommend to disable?

- A. 21/tcp
- B. 22/tcp
- C. 23/tcp**
- D. 443/tcp

**Answer:** C

397.Users reported several suspicious activities within the last two weeks that resulted in several unauthorized transactions.

Upon investigation, the security analyst found the following:

- Multiple reports of breached credentials within that time period
- Traffic being redirected in certain parts of the network
- Fraudulent emails being sent by various internal users without their consent.

Which of the following types of attacks was MOST likely used?

- A. Replay attack
- B. Race condition
- C. Cross site scripting
- D. Request forgeries

**Answer:** C

398.A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware.

Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

- A. BYOD
- B. VDI
- C. COPE
- D. CYOD

**Answer:** D

399.Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

- A. Test
- B. Staging
- C. Development
- D. Production

**Answer:** A

400.An external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network.

Which of the following will BEST assist with this investigation?

- A. Perform a vulnerability scan to identify the weak spots.
- B. Use a packet analyzer to Investigate the NetFlow traffic.
- C. Check the SIEM to review the correlated logs.
- D. Require access to the routers to view current sessions.

**Answer:** C

401.A developer is concerned about people downloading fake malware-infected replicas of a popular game.

Which of the following should the developer do to help verify legitimate versions of the game for users?

- A. Digitally sign the relevant game files.

- B. Embed a watermark using steganography.
- C. Implement TLS on the license activation server.
- D. Fuzz the application for unknown vulnerabilities.

**Answer:** A

**Explanation:**

<https://us-cert.cisa.gov/ncas/tips/ST04-018#:~:text=A%20digital%20signature%E2%80%94a%20type,%2C%20or%20a%20digital%20document>.

<https://www.techtarget.com/searchsecurity/definition/digital-signature>

402.A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks.

Which of the following will this practice reduce?

- A. Dumpster diving
- B. Shoulder surfing
- C. Information elicitation
- D. Credential harvesting

**Answer:** A

403.A security administrator is trying to determine whether a server is vulnerable to a range of attacks.

After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache
```

```
root:s9fyf983#:0:1:System Operator:/::bin/bash
daemon:*:1:1:::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

- A. Memory leak
- B. Race conditions
- C. SQL injection
- D. Directory traversal

**Answer:** D

```
[root@localhost:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

[www.x.com/../../../../etc/passwd](http://www.x.com/../../../../etc/passwd)

404.A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed.

Which of the following is required to assess the vulnerabilities resident in the application?

- A. Repository transaction logs
- B. Common Vulnerabilities and Exposures
- C. Static code analysis
- D. Non-credentialed scans

**Answer:** C

**Explanation:**

Static Code Analysis commonly refers to the running of Static Code Analysis tools that attempt to highlight possible vulnerabilities within 'static' (non-running) source code by using techniques such as Taint

### Analysis and Data Flow Analysis.

405.To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic.

Which of the following solutions would BEST accomplish this objective?

- A. Install a hypervisor firewall to filter east-west traffic.
- B. Add more VLANs to the hypervisor network switches.
- C. Move exposed or vulnerable VMs to the DMZ.
- D. Implement a zero-trust policy and physically segregate the hypervisor servers.

**Answer:** B

**Explanation:** Hypervisor-mode virtual firewalls require a modification to the physical host hypervisor kernel in order to install process hooks or modules allowing the virtual firewall system access to VM information and direct access to the virtual network switches and virtualized network interfaces moving packet traffic between

406.An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources.

Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

**Answer:** D

The QoS for VPN feature allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

407.An organization that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 3mi (4.8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices.

Which of the following controls should the organization implement?

- A. Geofencing
- B. Lockout
- C. Near-field communication
- D. GPS tagging

**Answer:** A

### 408.CORRECT TEXT

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

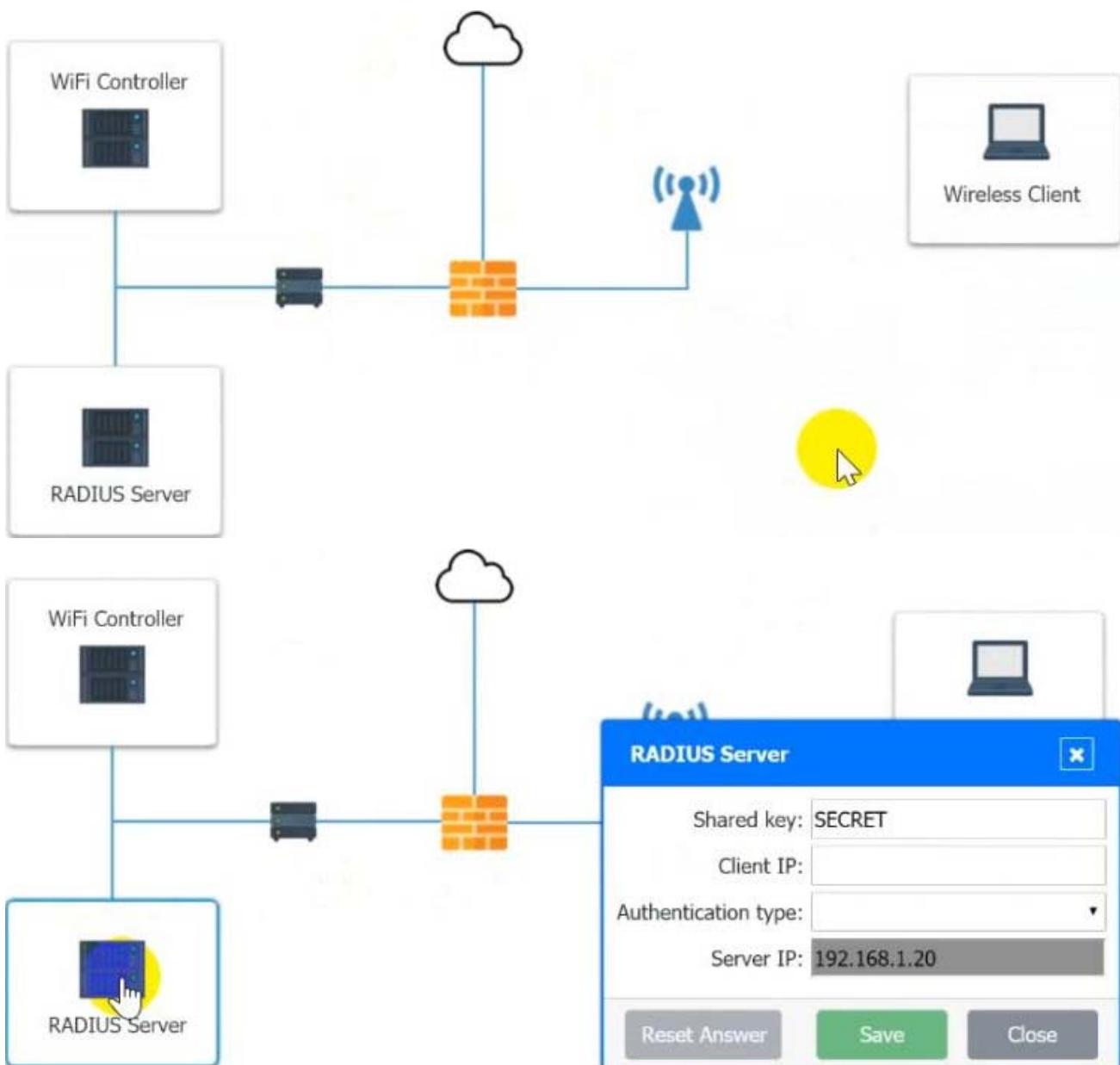
Perform the following steps:

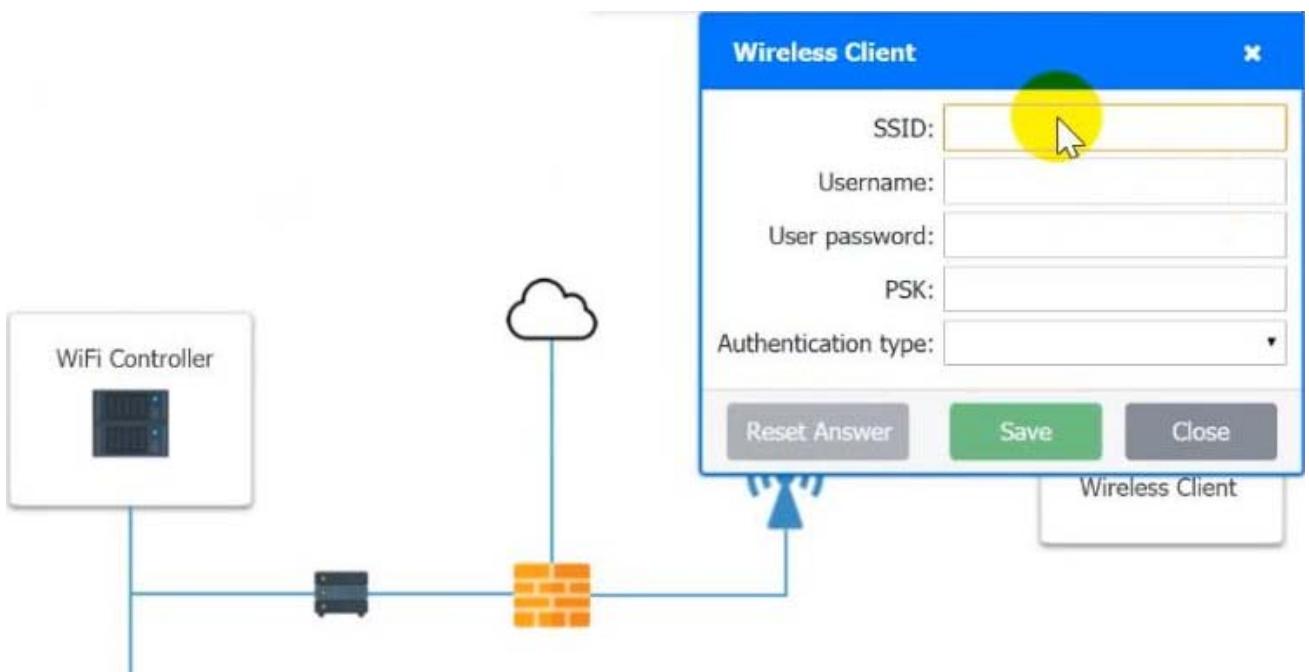
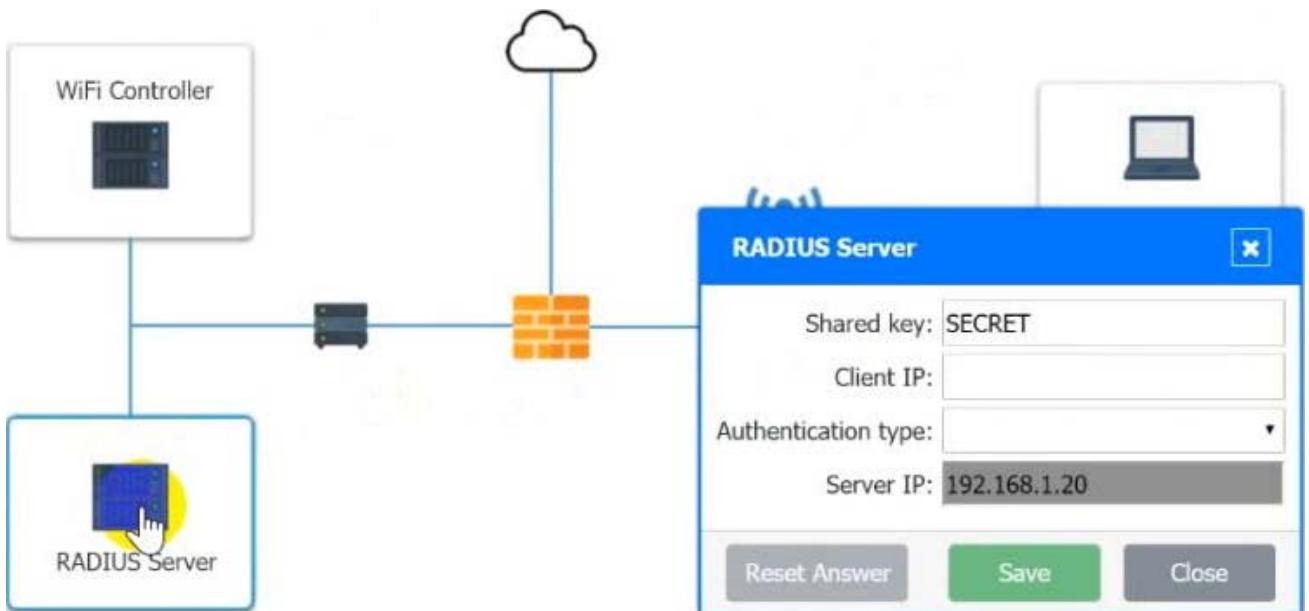
1. Configure the RADIUS server.
2. Configure the WiFi controller.
3. Preconfigure the client for an incoming guest.

The guest AD credentials are:

User: guest01

Password: guestpass





**Answer:**

Use the same settings as described in below images.



Graphical user interface, application  
Description automatically generated



Graphical user interface, text, application, chat or text message  
Description automatically generated

409.An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system.

Which of the following does the organization need to determine for this to be successful?

- A. The baseline
- B. The endpoint configurations
- C. The adversary behavior profiles
- D. The IPS signatures

**Answer:** A

410.A security researcher has alerted an organization that its sensitive user data was found for sale on a website.

Which of the following should the organization use to inform the affected parties?

- A. An incident response plan
- B. A communications plan

- C. A business continuity plan
- D. A disaster recovery plan

**Answer:** A

411.A company's cybersecurity department is looking for a new solution to maintain high availability.

Which of the following can be utilized to build a solution? (Select Two)

- A. A stateful inspection
- B. IP hashes
- C. A round robin
- D. A VLAN**
- E. A DMZ**

**Answer:** D,E

412.A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet.

The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 10.0.0.1
```

Internet Address	Physical Address
10.10.255.255	ff-ff-ff-ff-ff-ff
10.0.0.1	aa-aa-aa-aa-aa-aa
10.0.0.254	aa-aa-aa-aa-aa-aa
224.0.0.2	01-00-5e-00-00-02

Based on the loCS, which of the following was the MOST likely attack used to compromise the network communication?

- A. Denial of service
- B. ARP poisoning**
- C. Command injection
- D. MAC flooding

**Answer:** B

413.A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data.

Which of the following should the company do to help to accomplish this goal?

- A. Classify the data**
- D. Mask the data
- E. Assign the application owner
- F. Perform a risk analysis

**Answer:** A

414.An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise.

Which of the following will accomplish this goal?

- A. Antivirus

- B. IPS
- C. FTP
- D. FIM

**Answer:** D

**Explanation:**

Data tampering prevention can include simple security measures such as the encryption of data, and can include lengths such as using file integrity monitoring (FIM) systems for better security.

<https://www.cypressdatadefense.com/blog/data-tampering-prevention/>

Reference: <https://www.cypressdatadefense.com/blog/data-tampering-prevention/>

415.A company is considering transitioning to the cloud. The company employs individuals from various locations around the world. The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required.

Which of the following solutions would BEST meet the needs of the company?

- A. Private cloud
- B. Hybrid environment
- C. Managed security service provider
- D. Hot backup site

**Answer:** B

416.When planning to build a virtual environment, an administrator need to achieve the following,

- Establish policies in Limit who can create new VMs
- Allocate resources according to actual utilization‘
- Require justification for requests outside of the standard requirements.
- Create standardized categories based on size and resource requirements

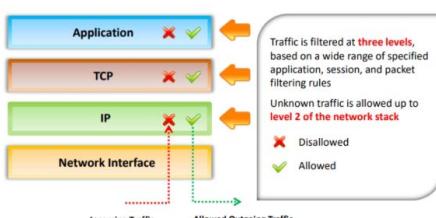
Which of the following is the administrator MOST likely trying to do?

- A. Implement IaaS replication
- B. Protect against VM escape
- C. Deploy a PaaS
- D. Avoid VM sprawl

**Answer:** D

417.Which two features are available only in next-generation firewalls? (Choose two )

- A. deep packet inspection
- B. packet filtering
- C. application awareness
- D. stateful inspection
- E. virtual private network



418.Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers' accounts.

Which of the following should be implemented to prevent similar situations in the future?

- A. Ensure input validation is in place to prevent the use of invalid characters and values.
- B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.
- C. Configure the web application firewall to look for and block session replay attacks.
- D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

**Answer:** A

419.A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users PCs.

Which of the following is the MOST likely cause of this issue?

- A. TFTP was disabled on the local hosts
- B. SSH was turned off instead of modifying the configuration file
- C. Remote login was disabled in the networkd.config instead of using the sshd.conf
- D. Network services are no longer running on the NAS

**Answer:** C

420.The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity.

Which of the following Is the BEST solution for the pilot?

- A. Geofencing
- B. Self-sovereign identification
- C. PKI certificates
- D. SSO

**Answer:** A

421.A security analyst needs to find real-time data on the latest malware and locs.

Which of the following best describe the solution the analyst should pursue?

- A. Advisories and Bulletins
- B. Threat Feeds
- C. Security News Articles
- D. Peer-Reviewed Content

**Answer:** B

422.A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of \$20,000 is credited to the account mentioned In the email.

This BEST describes a scenario related to:

- A. whaling.
- B. smishing.
- C. spear phishing
- D. vishing

**Answer:** A

423.An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF.

MOM, HIPS, and CASB systems.

Which of the following is the BEST way to improve the situation?

- A. Remove expensive systems that generate few alerts.
- B. Modify the systems to alert only on critical issues.
- C. Utilize a SIEM to centralize logs and dashboards.**
- D. Implement a new syslog/NetFlow appliance.

**Answer:** C

424. The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago.

Which of the following BEST describes the method being used to exploit the system?

- A. Baseline modification
- B. A fileless virus
- C. Tainted training data**
- D. Cryptographic manipulation

**Answer:** C

425. An organization has implemented a two-step verification process to protect user access to data that's stored in the cloud. Each employee now uses an email address and mobile number to receive a code to allow access to the data.

Which of the following authentication methods did the organization implement?

- A. Token key
- B. Static code
- C. Push notification**
- A. HOTP

**Answer:** C

426. A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO).

Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

- A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities
- B. Install a sandbox to run the malicious payload in a safe environment**
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

**Answer:** B

427. An organization has various applications that contain sensitive data hosted in the cloud. The company's leaders are concerned about lateral movement across applications of different trust levels.

Which of the following solutions should the organization implement to address the concern?

- A. ISFW
- B. UTM
- C. SWG

#### D. CASB

**Answer:** D

#### **Explanation:**

Once the full extent of cloud usage is revealed, the CASB then determines the risk level associated with each by determining what the application is, what sort of data is within the app, and how it is being shared.  
<https://www.mcafee.com/enterprise/en-au/security-awareness/cloud/what-is-a-casb.html>

A cloud access security broker (CASB) (sometimes pronounced cas-bee) is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies.[1] A CASB can offer a variety of services such as monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware. [https://en.wikipedia.org/wiki/Cloud\\_access\\_security\\_broker](https://en.wikipedia.org/wiki/Cloud_access_security_broker)

428.An end user reports a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-digit number ta an IP address once a day.

The only resent log entry regarding the user's computer is the following:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\harddiskvolume1\Users\jdoe\AppData\Local\Microsoft\Windows\Notifications\18pdftodocx.msi
Connection Details: 19.242.219.224:80
```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed 2 PUP from a web browser.
- B. 4 bot on the computer is rule forcing passwords against a website.
- C. A hacker Is attempting to exfiltrated sensitive data.
- D. Ransomwere is communicating with a command-and-control server.

**Answer:** A

429.A systems administrator is looking for a solution that will help prevent OAuth applications from being leveraged by hackers to trick users into authorizing the use of their corporate credentials.

Which of the following BEST describes this solution?

#### D. CASB

- E. UEM
- F. WAF
- G. VPC

**Answer:** D

430.Acompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS.

Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

**Answer: D**

431.A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at <https://www.company.com>.

A security analyst then examines the user's Internet usage logs and observes the following output:  
date; username; url; destinationport; responsecode

2020-03-01; userann; http://www.company.org/;80;302

2020-03-01; userann; http://www.company.org/secure\_login/;80;200

2020-03-01; userann; http://www.company.org/dashboard/;80;200

Which of the following has MOST likely occurred?

- A. Replay attack
- B. SQL injection
- C. SSL stripping
- D. Race conditions

**Answer: C**

432.A SOC is currently being outsourced.

Which of the following is being used?

- A. Microservices
- B. SaaS
- C. MSSP
- D. PaaS

**Answer: C**

**Explanation:**

<https://www.datashieldprotect.com/blog/pros-and-cons-of-an-outsourced-soc>

433.A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN.

Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?  
(Select TWO).

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest patch update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.
- E. The laptop is still configured to connect to an international mobile network operator.
- F. The user is unable to authenticate because they are outside of the organization's mobile geofencing configuration.

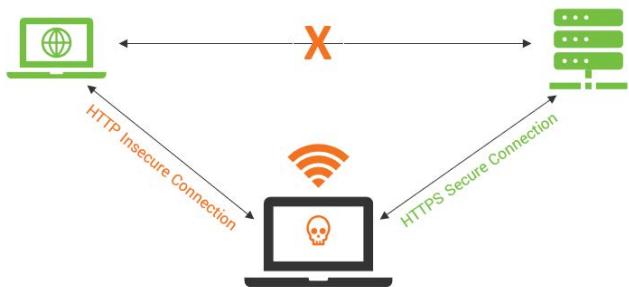
**Answer: A,B**

434.A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic.

Which of the following log sources would be BEST to show the source of the unusual traffic?

- A. HIDS
- B. UEBA

### How an SSL Stripping Attack Works



C. CASB

D. VPC

**Answer:** C

435.A user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is MOST likely cause of the infection?

A. The driver has malware installed and was refactored upon download to avoid detection.

B. The user's computer has a rootkit installed that has avoided detection until the new driver overwrote key files.

C. The user's antivirus software definition were out of date and were damaged by the installation of the driver

D. The user's computer has been infected with a logic bomb set to run when new driver was installed.

**Answer:** B

436.Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective.

Joe ran a set of commands and received the following output:

```
Domain Name: COMPTIA.ORG
Registry Domain ID: 1234554321
Registrar Server: whois.networksolutions.com
Updated Date: 2018-12-01T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC
Registrar IANA ID: 2
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: YourBusiness Corporation
Registrant Organization: YourBusiness Corporation
Registrant Street: 500 Pennsylvania Ave
Registrant City: Downers Grove
Registrant State: IL
Registrant Postal Code: 11105
Registrant Country: US
Registrant Phone: 1 800 555 5555
Registrant Fax: 1 800 555 5556
Registrant Email: info@comptia.org
Admin: Jason Doe
Admin Organization: ComptIA
```

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

A. Joe used Who is to produce this output.

B. Joe used cURL to produce this output.

C. Joe used Wireshark to produce this output

D. The organization has adequate information available in public registration.

E. The organization has too much information available in public registration.

F. The organization has too little information available in public registration

**Answer:** A,D

437.Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

- A. Pulverizing
- B. Shredding**
- C. Incinerating
- D. Degaussing

**Answer:** B

**Explanation:**

Another form of physical destruction, shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid state drives and have reached their end-of-life. It's also very effective for optical drives, smartphones, tablets, motherboards, thumb drives and credit card swipe devices, to name a few.

Shredding is a great way to destroy data if you have a large data enterprise center or a large stockpile of old hard drives and media that you want to destroy. It's very secure, fast and efficient. Shredding reduces electronic devices to pieces no larger than 2 millimeters. If you work in a high-security environment with high-security data, shredding should be your number one choice as it guarantees that all data is obliterated.

<https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/>

438.Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

- A. GOPR
- B. CIS controls
- C. ISO 27001**
- D. ISO 37000

**Answer:** C

439.A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL.

Which of the following is needed to meet the objective?

- A. A reverse proxy**
- B. A decryption certificate
- C. A split-tunnel VPN
- D. Load-balanced servers

**Answer:** A

440.The cost of movable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure. The Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established.

Which of the following security features should the network administrator implement to prevent unwanted data exposure to users in partner laboratories?

- A. VLAN zoning with a file-transfer server in an external-facing zone
- B. DLP running on hosts to prevent file transfers between networks**
- C. NAC that permits only data-transfer agents to move data between networks
- D. VPN with full tunneling and NAS authenticating through the Active Directory

**Answer:** B

441.A security analyst must determine if either SSH or Telnet is being used to log in to servers.

Which of the following should the analyst use?

- A. logger
- B. Metasploit
- C. tcpdump
- D. netstat**

**Answer:** D

442.A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information.

Which of the following methods did the attacker MOST likely use to gain access?

- A. A bot
- B. A fileless virus
- C. A logic bomb
- D. A RAT**

**Answer:** D

**Explanation:**

A remote access Trojan (RAT) is a type of malware that allows attackers to take control of systems from remote locations. It is often delivered via drive-by downloads.

... Some RATs automatically collect and log keystrokes, usernames and passwords, incoming and outgoing email, chat sessions, and browser history as well as take screenshots. The RAT can then automatically send the data to the attackers at predetermined times. ... It's common for attackers to exploit this one infected system and quickly infect the entire network with additional malware, including installing RATs on other systems. (Darril Gibson's Get Certified Get Ahead p. 442)

443.A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.

Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure DLP solutions**
- B. Disable peer-to-peer sharing.
- C. Enable role-based access controls
- D. Mandate job rotation.
- E. Implement content filters

**Answer:** A

444.A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMV1,. Which of the following BEST explains the findings?

- A. Default settings on the servers
- B. Unsecured administrator accounts
- C. Open ports and services**
- D. Weak Data encryption

**Answer:** C

445.An attacker is attempting, to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password. the logon screen displays the following message:

Which of the following should the analyst recommend be enabled?

446.A security analyst is reviewing the following command-line output:

Internet address	Physical address	Type
192.168.1.1	aa-bb-cc-00-11-22	dynamic
192.168.1.2	aa-bb-cc-00-11-22	dynamic
192.168.1.3	aa-bb-cc-00-11-22	dynamic
192.168.1.4	aa-bb-cc-00-11-22	dynamic
192.168.1.5	aa-bb-cc-00-11-22	dynamic
---output omitted---		
---		
192.168.1.251	aa-bb-cc-00-11-22	dynamic
192.168.1.252	aa-bb-cc-00-11-22	dynamic
192.168.1.253	aa-bb-cc-00-11-22	dynamic
192.168.1.254	aa-bb-cc-00-11-22	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static

Which of the following is the analyst observing?

- A. IGMP spoofing
- B. URL redirection
- C. MAC address cloning**
- D. DNS poisoning

**Answer:** C

447.A financial institution would like to store its customer data securely but still allow the data to be

accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds.

Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homeomorphic
- D. Ephemeral

**Answer:** C

**Explanation:**

"In a nutshell, homomorphic encryption is a method of encryption that allows any data to remain encrypted while it's being processed and manipulated. It enables you or a third party (such as a cloud provider) to apply functions on encrypted data without needing to reveal the values of the data."

<https://www.thesslstore.com/blog/what-is-homomorphic-encryption/>

Reference: [https://en.wikipedia.org/wiki/Homomorphic\\_encryption](https://en.wikipedia.org/wiki/Homomorphic_encryption)

448. While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches.

Which of the following is the security analyst MOST likely observing?

- A. SNMP traps
- B. A Telnet session
- C. An SSH connection
- D. SFTP traffic

**Answer:** B

**Explanation:**

Reference: <https://en.wikipedia.org/wiki/Telnet>

449. Joe, an employee, is transferring departments and is providing copies of his files to a network share folder for his previous team to access. Joe is granting read-write-execute permissions to his manager but giving read-only access to the rest of the team.

Which of the following access controls is Joe using?

- A. FACL
- B. DAC
- C. ABAC
- D. MAC

**Answer:** B

450. Which of the following is a difference between a DRP and a BCP?

- A. A BCP keeps operations running during a disaster while a DRP does not.
- B. A BCP prepares for any operational interruption while a DRP prepares for natural disasters
- C. A BCP is a technical response to disasters while a DRP is operational.
- D. A BCP is formally written and approved while a DRP is not.

**Answer:** A

The differences are that a disaster recovery plan is referring to restoring data and accessing backups while a business continuity plan refers to getting systems back online and the business operations and areas associated with running the business.

451.The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

- A. federation.
- B. a remote access policy. SAML tends to be specific to a user, while OAuth tends to be specific to an application.
- C. multifactor authentication.
- D. single sign-on.

**Answer:** A

452.An attack relies on an end user visiting a website the end user would typically visit, however, the site is compromised and uses vulnerabilities in the end users browser to deploy malicious software.

Which of the blowing types of attack does this describe?

- A. Smishing
- B. Whaling
- C. Watering hole
- D. Phishing

**Answer:** C

453.An enterprise needs to keep cryptographic keys in a safe manner.

Which of the following network appliances can achieve this goal?

- A. HSM
- B. CASB
- C. TPM
- D. DLP

**Answer:** A

**Explanation:**

A hardware security module (HSM) is a security device you can add to a system to manage, generate, and securely store cryptographic keys.

High performance HSMs are external devices connected to a network using TCP/IP. Smaller HSMs come as expansion cards you install within a server, or as devices you plug into computer ports.

454.A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic.

Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

**Answer:** D

455.A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted.

Which of the following resiliency techniques was applied to the network to prevent this attack?

- A. NIC Teaming
- B. Port mirroring

C. Defense in depth

D. High availability

E. Geographic dispersal

**Answer:** C

456.Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems.

**B. To keep all software and hardware fully patched for known vulnerabilities**

C. To only allow approved, organization-owned devices onto the business network

D. To standardize by selecting one laptop model for all users in the organization

**Answer:** B

**Explanation:**

Without effective asset management, an organization's cybersecurity plan is missing a crucial component.

The reasons why should be clear when you stop and think about it.

How can you keep your IT resources secure if you don't know precisely what those systems contain?

Outdated hardware and software quickly become vulnerable to attacks. Asset tracking enables an organization to keep these updated on a regular schedule to ensure nothing falls through the cracks.

457.A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words.

Which of the following would be the BEST to use?

A. IDS solution

B. EDR solution

C. HIPS software solution

**D. Network DLP solution**

**Answer:** D

458.The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls.

This is an example of:

A. prepping.

**B. an influence campaign**

C. a watering-hole attack

D. intimidation

E. information elicitation

**Answer:** B

**Explanation:**

Reference: <https://www.darpa.mil/program/influence-campaign-awareness-and-sensemaking>

459.To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain.

Which of the following is being used?

A. PFS

- B. SPF
- C. DMARC
- D. DNSSEC**

**Answer:** D

460.An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space.

Which of the following will the organization MOST likely consult?

- A. The business continuity plan**
- B. The disaster recovery plan
- C. The communications plan
- D. The incident response plan

**Answer:** A

461.A SOC is implementing an insider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization.

Which of the following should be deployed to detect a potential insider threat?

- A. A honeyfile**
- B. ADMZ
- C. DLP
- D. File integrity monitoring

**Answer:** A

462.A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation.

Which of the following would dispute the analyst's claim of innocence?

- A. Legal hold
- B. Order of volatility
- C. Non-repudiation**
- D. Chain of custody

**Answer:** C

**Explanation:**

Reference: <https://en.wikipedia.org/wiki/Non-repudiation>

463.A company wants to deploy systems alongside production systems in order to entice threat actors and to learn more about attackers.

Which of the following BEST describe these systems?

- A. DNS sinkholes
- B. Honeypots**
- C. Virtual machines
- D. Neural network

**Answer:** B

464.A security analyst is investigating multiple hosts that are communicating to external IP addresses

during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software.

Which of the following types of malware is MOST likely infecting the hosts?

- A. A RAT
- B. Ransomware
- C. Polymorphic
- D. A worm

**Answer:** C

465.Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically.

Which of the following concepts does this BEST represent?

- A. Functional testing
- B. Stored procedures
- C. Elasticity
- D. Continuous integration

**Answer:** D

**Explanation:**

466.The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC monitors the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator.

To which of the following groups should the analyst report this real-world event?

- A. The NOC team
- B. The vulnerability management team
- C. The CIRT
- D. The red team

**Answer:** C

467.An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports.

Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

- A. SFTP FTPS
- B. SNMPv2 SNMPv3
- C. HTTP, HTTPS
- D. TFTP FTP

E. SNMPv1, SNMPv2

F. Telnet SSH

G. TLS, SSL

H. POP, IMAP

I. Login, rlogin

**Answer:** B,C,F

468.A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss.

Which of the following would be the BEST backup strategy to implement?

A. Incremental backups followed by differential

backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backups followed by differential backups

**Answer:** E

469.A hospital's administration is concerned about a potential loss of patient data that is stored on tablets.

A security administrator needs to implement controls to alert the SOC any time the devices are near exits.

Which of the following would BEST achieve this objective?

A. Geotargeting

B. Geolocation

C. Geotagging

D. Geofencing

**Answer:** D

470.During an asset inventory, several assets, supplies, and miscellaneous items were noted as missing.

The security manager has been asked to find an automated solution to detect any future theft of equipment.

Which of the following would be BEST to implement?

A. Badges

B. Fencing

C. Access control vestibule

D. Lighting

E. Cameras

**Answer:** E

471.A security analyst needs to perform periodic vulnerability scans on production systems.

Which of the following scan types would produce the BEST vulnerability scan report?

A. Port

B. Intrusive

C. Host discovery

D. Credentialated

**Answer:** D

472.An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved.

Which of the following attacks MOST likely explains the behavior?

- A. Birthday
- B. Rainbow table
- C. Impersonation
- D. Whaling

**Answer:** A

473.A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home.

Some of the requirements are:

- \* Employees must provide an alternate work location (i.e., a home address)
- \* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

**Answer:** D

474.The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications t make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT administrators are concerned about network traffic and load if all users simultaneously download the application.

Which of the following would work BEST to allow each geographic region to download the software without negatively impacting the corporate network?

- A. Update the host IDS rules.
- B. Enable application whitelisting.
- C. Modify the corporate firewall rules.
- D. Deploy all applications simultaneously.

**Answer:** C

475.The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the worker's PC.

Which of the following would be BEST to help prevent this type of attack in the future?

- A. Data loss prevention

- B. Segmentation
- C. Application whitelisting
- D. Quarantine

**Answer:** C

476.Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

- A. Mantraps
- B. Security guards
- C. Video surveillance
- D. Fences
- E. Bollards
- F. Antivirus

**Answer:** A,B

477.A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline.

The manager would like to Implement a high availability pair to:

- A. decrease the mean time between failures
- B. remove the single point of failure
- C. cut down the mean time to repair
- D. reduce the recovery time objective

**Answer:** B

478.A company is required to continue using legacy software to support a critical service.

Which of the following BEST explains a risk of this practice?

- A. Default system configuration
- B. Unsecure protocols
- C. Lack of vendor support
- D. Weak encryption

**Answer:** C

479.Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

risk tolerance is the level of risk that an organization can accept per individual risk, whereas risk appetite is the total risk that the organization can bear in a given risk profile,

**Answer:** D

480.A company was compromised, and a security analyst discovered the attacker was able to get access to a service account.

The following logs were discovered during the investigation:

User account 'JHDoe' does not exist...  
User account 'VMAadmin' does not exist..  
User account 'tomcat' wrong password...  
User account 'Admin' does not exist...

Which of the following MOST likely would have prevented the attacker from learning the service account name?

- A. Race condition testing
- B. Proper error handling**
- C. Forward web server logs to a SIEM
- D. Input sanitization

**Answer:** B

481.An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions.

Which of the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs**
- D. Antivirus

**Answer:** C