1. What is a characteristic of the security onion analogy to visualizing defense-in-depth?

- The core or heart of the onion represents the firewall surround by protective layers.
- The outer skin of the onion represents hardened internet-facing systems.
- Each layer of the onion may reveal sensitive data that is not well secured.
- **All layers of the onion must be penetrated to gain access to vulnerable assets.**

Explanation: The analogy of an onion to represent the concept of defense-in-depth means that a threat actor would have to peel network defenses layer by layer in a manner similar to peeling an onion. Only after penetrating each layer would vulnerable assets be exposed. The outer layer of the onion is representative of the firewall as the first line of defense.

2. An administrator wishes to create a security policy document for end-users to protect against known unsafe websites and to warn the user about the dangers and handling of suspicious emails. What type of malware attack is being prevented?

- **phishing**
- DDoS
- trusted/untrusted sources verification
- adware protection

Explanation: Phishing is a type of malware attack where threat actors use unsafe websites and suspicious emails to entice users to give away personal information.

3. Which data type is protected through the use of an IPsec VPN?

- data in storage
- **data in transit**
- data in process
- data at rest

Explanation: When data is moving between devices it is considered data in transit. To protect data while it is in transit, IPsec and SSL VPNs can be implemented.

4. What technology can be used to protect the integrity of data in transit?

- IPsec tunnels
- **hashing**
- mutual authentication
- VPNs

Explanation: Data integrity refers to the accuracy and validity of the data. Hashing is used to ensure the integrity of data as it moves between devices.

5. The IT team of an organization is updating the policy and procedures regarding recovery controls. What are three examples of recovery controls? (Choose three.)

- firewall deployment
- **server clustering**
- **database shadowing**
- monitoring procedures
- **backup/restore operations**
- intrusion detection system

Explanation: Recovery security controls restore resources, functions, and capabilities back to a normal state after a violation of a security policy. Examples of recovery controls include backup/restore operations, fault tolerance drive systems, server clustering, and database shadowing.

6. A company has set a policy that employees will be required to report any observed or suspected security issues. Which control type has the company implemented?

- incident controls
- physical controls
- **administrative controls**
- technical controls

Explanation: Security controls are safeguards or countermeasures that an organization implements to avoid, detect, counteract, or minimize security risks to

organizational assets. The three control types are administrative controls, technical controls, and physical controls. Administrative controls consist of procedures and policies that an organization puts into place when dealing with sensitive information.

7. A company provides service to process transaction data for clients. The company deals with sensitive customer information of their clients. The improper release of the information poses a serious risk to the business of the company and their clients. The information security team in the company identifies threats coming from accidentally emailing the information to an unintended party. Which two action plans could the company implement to eliminate the risk? (Choose two.)

- Implement a firewall to filter all emails sent to customers.
- **Implement a technology to screen and block emails that contain sensitive information.**
- Move the business operation to a private cloud and require clients to use the private cloud as well.
- **Implement a policy prohibiting employees from including sensitive information in any emails to customers.**
- Require employees to use a VPN connection when emailing customers.

Explanation: To eliminate the risk of emailing sensitive information by accident, the company can implement a policy prohibiting employees from including sensitive information in emails. In addition, the company can implement a technology that can scan and block emails when necessary.

8. A cybersecurity consulting company is helping an organization to develop a cybersecurity policy to address a few operational issues and conditions that may require more detailed requirements and directions. Which type of cybersecurity policy are they developing?

- master cybersecurity policy
- **issue specific policy**
- system specific policy
- general cybersecurity management policy

Explanation: An issue specific policy is developed for certain operational issues, circumstances or conditions that may require more detailed requirements and directions.

9. The IT team in a company discovers that some employees are visiting newly established websites that are deemed inappropriate for conducting company business. What is the first action that the IT team should take in terms of the security policies?

- Update the Network Access Policy immediatley and get users to sign it.
- **Update the existing Acceptable Use Policy immediately and get all users to sign it.**
- Update the Remote Access Policy immediately and get users to sign it.
- Update the incident handling policy immediately and get the employees to sign it.

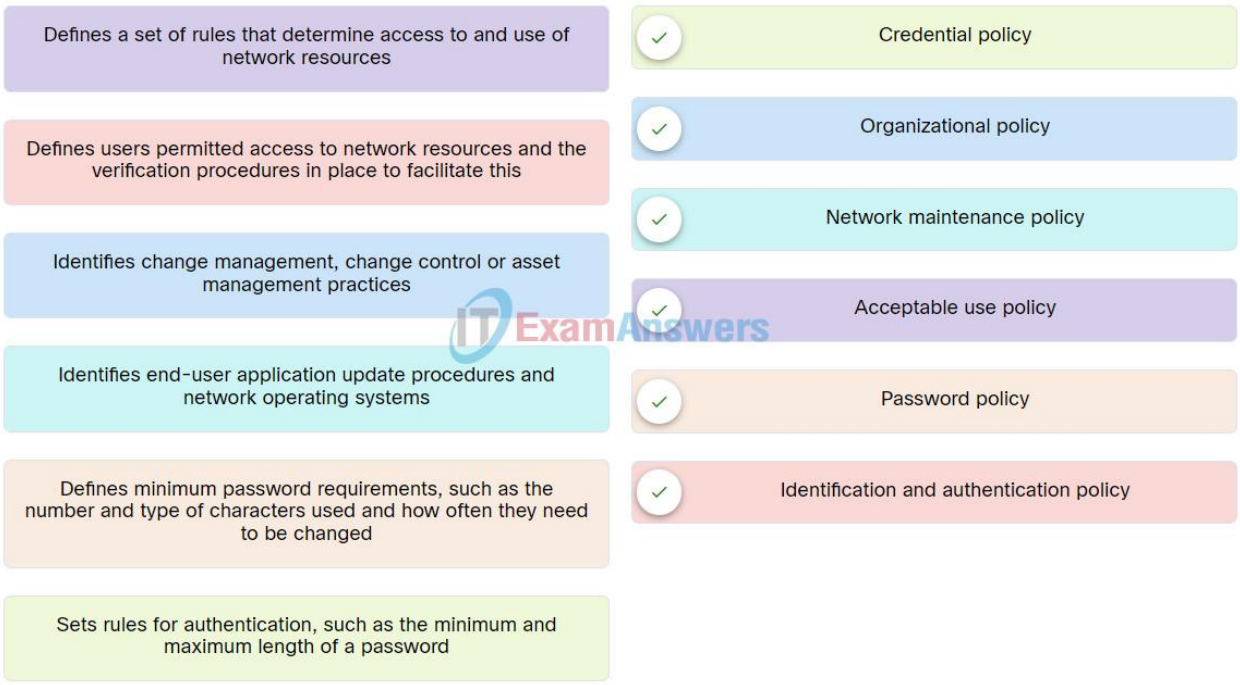
Explanation: The Acceptable use Policy (AUP) governs the users behaviour and should be addressed first.

10. An administrator has been granted top security clearance at a company. One day the administrator finds that certain confidential documents cannot be accessed. The administrator asks the IT team to verify the level of clearance and receives the confirmation that top security clearance is still valid. What could be the reason that the administrator cannot access the respective documents?

- The PKI certificate has been revoked.
- The firewall rules are in conflict with the access rights of the user.
- The PKI key of the user is invalid.
- **The principle of least privilege has been applied.**

Explanation: The principle of least privilege has been applied in the access control models. This would mean that, even though the employee has top security clearance to access the intelligence information, they would still not be given access to such information unless they needed it to be able to effectively perform their job duties.

11. Match the security policy to its description.



Explanation: Place the options in the following order:

Identifies change management,change control or asset management practices.	Organizational policy
Identifies end-user application update procedures and network operating systems.	Network maintenance policy
Sets rules for authentication,such as the minimum and maximum length of a password.	Credential policy

Defines minimum password requirements,such as the number and type of characters used and how often they need to be changed.	Password policy
Defines users permitted access to network resources and the verification procedures in place to facilitate this.	Identification and authentication policy
Defines a set of rules that determine access to and use of network resources.	Acceptable use policy

12. What is the most compressed representation of the IPv6 address 2001:0db8:0000:abcd:0000:0000:0000:0001?

- 2001:db8::abcd:0:1
- 2001:0db8:abcd::1
- 2001:0db8:0000:abcd::1
- **2001:db8:0:abcd::1**
- 2001:0db8:abcd::0001

Explanation: The IPv6 address 2001:0db8:0000:abcd:0000:0000:0000:0001 in its most compressed format would be 2001:db8:0:abcd::1. The one leading zero in the second hextet can be removed. The first hextet of zeros would be compressed to a single zero. The three consecutive hextets of zeros can be compressed to a double colon ::. The three leading zeros in the last hextet can be removed. The double colon :: can only be used once in an address.

13. A threat actor is using ping to discover hosts on a network. What type of attack is taking place?

- DoS
- address spoofing
- **ICMP**

- amplification

Explanation: In an ICMP attack, the threat actor uses ping to discover hosts and subnets on the network.

14. A cyber security analyst is reviewing security alerts in Sguil. What are three pieces of information included in an alert to identify the device generating the alert? (Choose three.)

- **IP protocol number**
- source and destination MAC address
- **source and destination Layer 4 port**
- **source and destination IP address**
- Layer 4 segment sequence number
- host domain name

Explanation: Sguil provides a console to view alerts generated by network security monitoring tools. The alerts will usually include five-tuples of information and time stamps. The five-tuples include the source and destination IP address, source and destination Layer 4 ports, and the IP protocol number.

15. Which tool is integrated into the Security Onion and displays full packet captures for analysis?

- Sguil
- Kibana
- Zeek
- **Wireshark**

Explanation: Security Onion uses several tools to integrate IDS logs into a single platform. Wireshark is a packet capture application that displays the full packet capture relevant to an analysis.

16. Refer to the exhibit. A router is configured with a zone-based policy firewall as shown. Which two statements describe how traffic between the LAN and external hosts will be processed? (Choose two.)

```
!
!<output omitted>
class-map type inspect match-any WEB-TRAFFIC
 match protocol http
 match protocol https
 match protocol dns
!
policy-map type inspect LAN-TO-EXT-POLICY
 class type inspect WEB-TRAFFIC
  inspect
 class type inspect class-default
  drop
!
!
!
zone security LAN
zone security EXTERNAL
zone-pair security LAN-EXT source LAN destination EXTERNAL
 service-policy type inspect LAN-TO-EXT-POLICY
!
```

Cybersecurity Pathway Exam Q16

- Any traffic originating from the EXTERNAL zone is inspected and permitted into the LAN zone.
- **Traffic originating from the LAN zone that matches the HTTP, HTTPS, or DNS protocols is inspected and permitted.**
- HTTP, HTTPS and DNS traffic destined for the router itself is not permitted by this policy.
- All HTTP, HTTPS, and DNS responses originating from the EXTERNAL zone destined for the LAN zone are dropped.
- **All traffic sourced from the LAN zone that does not match the HTTP, HTTPS, or DNS protocols is dropped.**

Explanation: HTTP, HTTPS, and DNS traffic sourced from the LAN zone and destined for the EXTERNAL zone will be inspected. Traffic sourced from the EXTERNAL zone and destined for the LAN zone will only be allowed if it is part of sessions originally initiated by LAN zone hosts. Also, notice thethat will drop all other traffic that is not a member of the WEB-TRAFFIC class. Traffic to and from the router is not affected unless the zone pairs are configured using the predefined self zone.

17. A technician enters the commands shown to configure a zone-pair between two security zones on a router.

```
Router(config)# zone-pair security PRIV-PUB source PRIVATE destination PUBLIC

Router(config-sec-zone-pair)#
```

What information must now be entered to specify which traffic can be sent across the zones and associate it with the zone-pair configuration?

- **a service policy-map that is to be applied to traffic between the zones**
- a list of other security zones that are included in this zone-pair
- a list of interfaces that are configured as members of the two zones
- access list statements that permit or deny specific traffic in and out of the zones

Explanation: After the firewall policy has been configured, it is applied to traffic between a pair of zones using the. To apply a policy, use the command to attach a policy-map and its associated action to the zone-pair. The zone pair needs to specify the source zone, the destination zone, and the policy for handling the traffic between the source and destination zones.

18. What type of attack disrupts services by overwhelming network devices with bogus traffic?

- **DDoS**
- Port scans
- Zero-day
- Brute force

Explanation: A Denial of Service attack or a Distributed Denial of Service attack sends an enormous amount of data to a network, host or application. This data overwhelms the destination devices and causes a major slowdown or a system crash.

19. Which of the following are commonly used port scanning applications? (Choose two.)

- Port number
- Sequence number
- **Nmap**
- **Zenmap**

Explanation: Two popular network discovery and port scanning applications are Network Mapper (Nmap) and Zenmap.

20. Which of the following protocols use the Advanced Encryption Standard (AES)? (Choose two.)

- **WPA2**
- EAP
- WEP
- TKIP
- **WPA**

Explanation: AES is the encryption method used by WPA2. It is currently the preferred method because it is a strong method of encryption. WPA can also use AES.

21. Which method of wireless authentication can take advantage of identity verification using a Radius server?

- WEP
- **WPA2-Enterprise**
- Open
- WPA-Personal

Explanation: Although more complicated to set up, WPA2-Enterprise provides additional security. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

22. Because of a pandemic, a company decides to let employees work from home. What security technology should be implemented to ensure that data communications between the employees and the company's network remain confidential?

- MD5
- SHA-1
- **AES**
- SHA-3

Explanation: MD5 and SHA are hash-generating algorithms that guarantee that no one intercepted the message and altered it thus ensuring the integrity of the

data. Advanced Encryption Standard (AES) is a symmetric encryption algorithm where each communicating party needs to know the pre-shared key thus ensuring that the data communication is confidential.

23. What is a difference between symmetric and asymmetric encryption algorithms?

- Symmetric encrption algorithms are slower then asymmetric encryption algorithms.
- Symmetric encryption algorithms are used to encrypt data and asymmetric encryption algorithms are used to decrypt data.
- Symmetric encryption algorithms have a maximum key length size of 512 bits but asymmetric encryption algorithms maximum key length size is 256 bits.
- **Symmetric encryption algorithms use pre-shared keys while asymmetric encryption algorithms use different keys to encrypt and decrypt data.**

Explanation: Asymmetric algorithms can use very long key lengths of up to 4096 bits for data encryption. The longer keys are commonly used for encrypting bulk data. This results in the use of significantly increased resources and time, compared to symmetric algorithms which only use 256 bits for data encryption.

24. What is a drawback of using a single-root PKI topology?

- It allows for the creation of unsecure hierarchical and cross-certification topologies.
- It can issue insecure certificates to end users and to a subordinate CA.
- It requires de-centralized administration that can lead to multiple points of failure.
- **It is difficult to scale to a large environment.**

Explanation: The drawback of using a single-root PKI topology is that it is difficult to scale to a large environment. A single-root PKI topology requires a strictly centralized administration, which creates a single point of failure.

25. What is used by PKI entities to verify the validity of a digital certificate?

- SSL
- **CRL**
- X.509

- S/MIME

Explanation: The Certificate Revocation List (CRL) contains a list of revoked certificate serial numbers that have been invalidated because they have expired. The CRL can be polled by PKI entities to determine the validity of the digital certificate in question.

26. A cyberanalyst is looking for an open source malware analysis tool that can run locally on the network. Which tool would meet the needs of the cyberanalyst?

- AMP
- ANY.RUN
- Threat Grid Globebox
- **Cuckoo Sandbox**

Explanation: Cuckoo Sandbox is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis. A number of other online public sandboxes exist.

27. What is a feature of the ANY.RUN malware sandbox?

- It runs on the local network and can analyze multiple malware samples.
- It is a Cisco tool that can track the trajectory of malware that has entered the network and can roll back network events to obtain a copy of the downloaded malware file.
- **It is an online sandbox tool and can capture screenshots of interactive elements of the malware.**
- It is an open source tool that can be used to create signatures to prevent the malware file from entering the network again.

Explanation: ANY.RUN is an online sandbox tool with interactive reporting functions. Multiple malware samples can be uploaded to ANY.RUN for analysis. It also has the ability to capture screenshots of interactive elements of the malware.

28. An organization needs a solution that will generate alerts on malware that has made it through the network perimeter and infected internal

systems. What technology would be an appropriate solution for the organization?

- zone-based policy firewall
- sandbox
- **host intrusion detection system**
- honeypot

Explanation: Malware can make it past network perimeter security devices such as firewalls and infect systems on the network. To protect against malware that has made it though the network perimeter, host based intrusion detection systems can be installed on network host systems to create alerts for suspected malware.

29. What are the most effective ways to defend against malware? (Choose two.)

- **Update the operating system and other application software**
- **Install and update antivirus software**
- Implement network firewalls
- Implement RAID
- Implement strong passwords
- Implement a VPN

Explanation: Two of the best methods to protect an organization from malware are to install and update antivirus software and to keep the OS and all applications up to date.

30. A software company uses a public cloud service for hosting software development and deployment services. The company is concerned that software code in development might leak to competitors and result in the loss of intellectual property. Which two security coding techniques can the company implement to address the concern? (Choose two.)

- stored procedure
- **obfuscation**
- input validation
- normalization
- **camouflage**

Explanation: The software company can use obfuscation and camouflage to prevent software from being reverse engineered. Obfuscation hides original data with random characters or data. Camouflage replaces sensitive data with realistic fictional data.

31. A software company uses a public cloud service for hosting development and deployment services. The company is evaluating options to protect against data breaches and compromised login credentials. What two countermeasures should be implemented? (Choose two.)

- Perform a daily backup of data.
- **Use an advanced encryption algorithm.**
- Develop and implement compliance policies.
- Install host-based intrusion detection software on VMs in the cloud.
- **Implement a multi-factor authentication process.**
- Deploy development and deployment services across multiple zones.

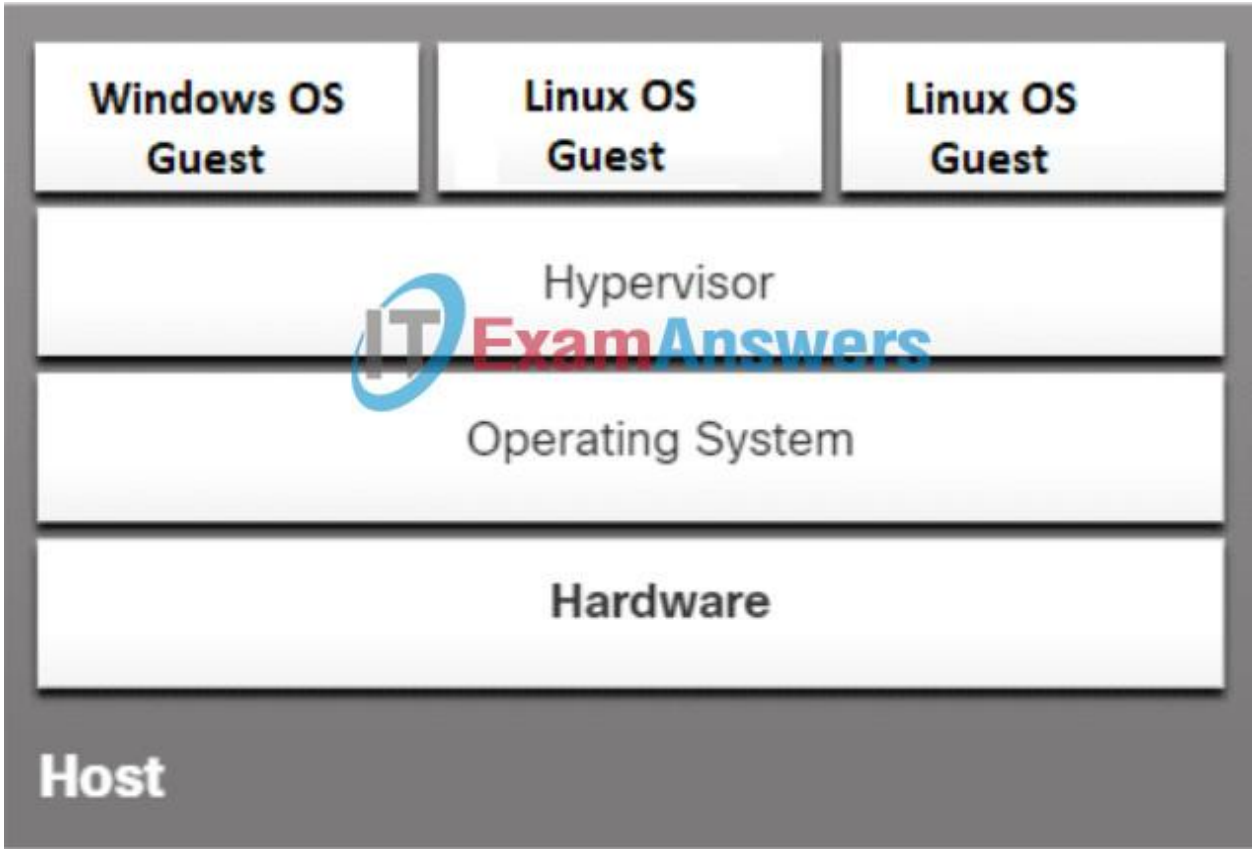
Explanation: Using an advanced encryption algorithm to encrypt data in transition and in storage and implementing multi-factor authentication can protect against data breaches and compromised login credentials.

32. What is a benefit of a Type 1 hypervisor implementation over a Type 2 hypervisor environment?

- Console software on the Type 1 hypervisor host system prevents or limits VM sprawl.
- Machines running Type 1 hypervisors can also run other host-based applications simultaneously.
- Type 1 hypervisor systems are immune to hacker attacks and VM escape exploits.
- **Type 1 hypervisors do not require a separate operating system be loaded on the host machine.**

Explanation: A Type 1 hypervisor system interfaces directly with the host hardware and does not require that a separate server operating system, such as Windows or Linux, be loaded on the host system. Type 2 hypervisors are software systems that run on the host operating system.

33. Refer to the exhibit. What type of software is installed on the host system to support the three virtual machines?

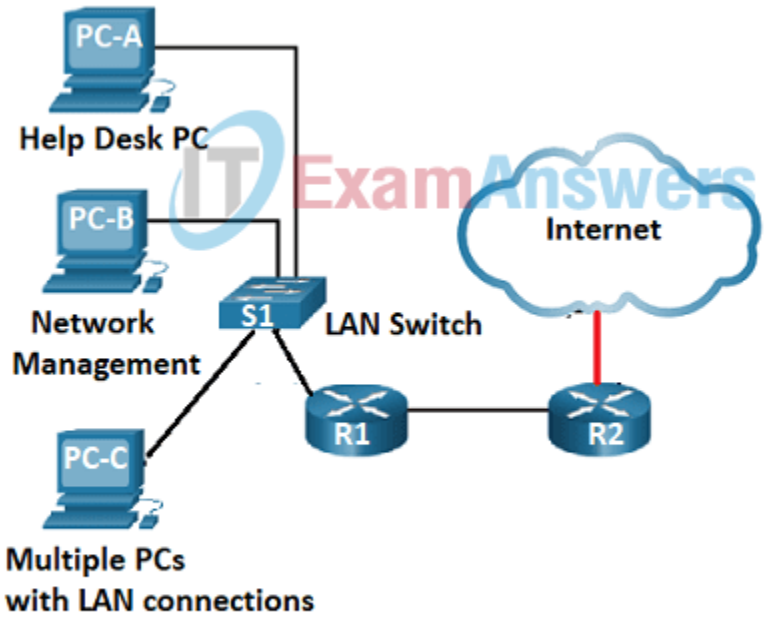


- Type 1 hypervisor software
- edge computing software
- virtual container platform
- **Type 2 hypervisor software**

Explanation: Type 2 hypervisor software runs on top of a host machine's operating system. A type 1 hypervisor does not require the host system to have an additional operating system in place to manage the hardware and system processes.

34. Refer to the exhibit. The help desk receives a work order describing an issue with a management application running on PC-B. The work order states that the network management application cannot receive syslog messages from the LAN switch after upgrading PC-B to the latest version of Windows 10. A ping request from PC-A to PC-B fails, but both PCs are able to successfully ping the connected switch VLAN1 IP address. The technician temporarily disables the Windows Defender Firewall on PC-B for

both the private and public networks. The ping request from PC-A to PC-B succeeds and the application on PC-B can receive the syslog messages from the switch. Which action should the technician perform to correct the reported issue without compromising the security of the LAN?



- Create a rule using IPtables to permit syslog and ICMP traffic sourced from private addresses to enter PC-B.
- Leave the Windows Defender Firewall on PC-B disabled for the private network and re-enable it for the public network only.
- Disable the Windows Defender Firewall and install a third-party host-based intrusion detection system.
- **Re-enable the firewall for both networks and create a custom inbound rule on PC-B to permit the desired protocols.**

Explanation: To solve the issue without further compromising LAN security, a custom rule can be created in Windows Defender Firewall to permit the necessary protocols from the switch IP address. IPtables is a Linux firewall utility that is not available on Windows 10.

35. What Windows utility should be used to configure password rules and account lockout policies on a system that is not part of a domain?

- Active Directory Security tool

- Event Viewer security log
- **Local Security Policy tool**
- Computer Management

Explanation: A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities. Local Security Policy, Event Viewer, and Computer Management are Windows utilities that are all used in the security equation.

36. An e-commerce website encourages users to authenticate using their individual social media account credentials. What type of a security solution enables users to use the same credentials to login to multiple networks belonging to different enterprises?

- Radius authorization
- public key infrastructure
- **federated identity management**
- two-factor authentication

Explanation: Federated identity management links the electronic identity of a subject across separate identity management systems, such as being able to access several websites using the same social login credentials. From a user perspective, federated identity management can provide a single sign-on for the web.

37. A Linux administrator creates new user accounts using the useradd command. Which two files on the system contain the new user account information? (Choose two.)

- **/etc/shadow**
- **/etc/passwd**
- /users/account
- /etc/users
- /etc/users/groups

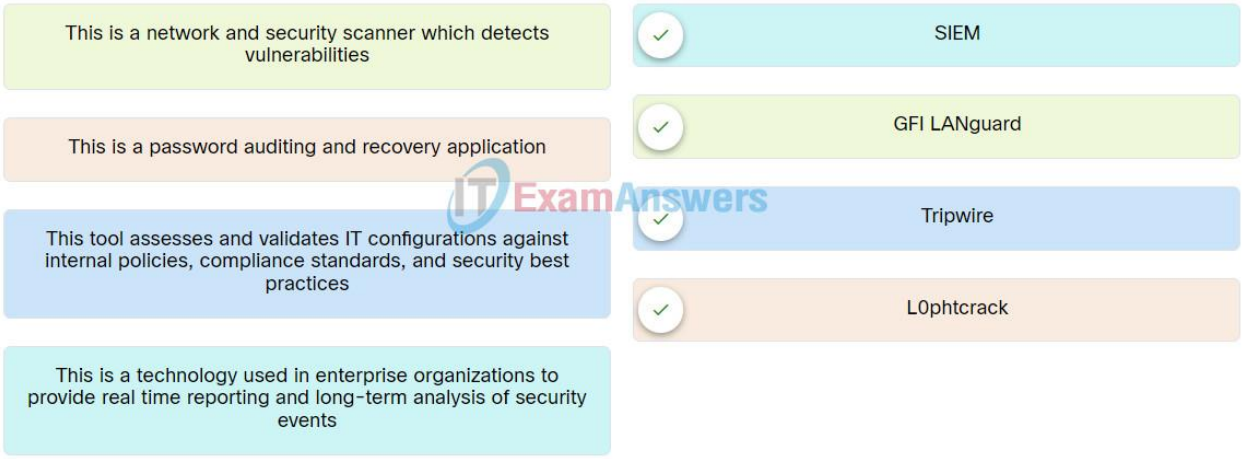
Explanation: The /etc/passwd file contains a line for each user on the system. Information in the file contains the username and unique ID, as well as additional information such as user home directory and default group membership. The file contains the username and the encrypted user password.

38. A cloud service company forms a security team to handle risks of disruption of cloud services caused by cyber-attacks. What should the team do first in the risk management process?

- **Frame the risk.**
- Monitor the risk.
- Assess the risk.
- Respond to the risk.

Explanation: Risk management is a formal process that measures the impact of a threat and the cost to implement controls or countermeasures to mitigate that threat. The first step in the risk management process is framing the risk by identifying the threats throughout the organization that increase risk.

39. Match the network testing tool with its description.



40. A penetration tester wants to collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets. What is this process called?

- **non-intrusive scan**
- intrusive scan
- brute force attack
- credentialed scan

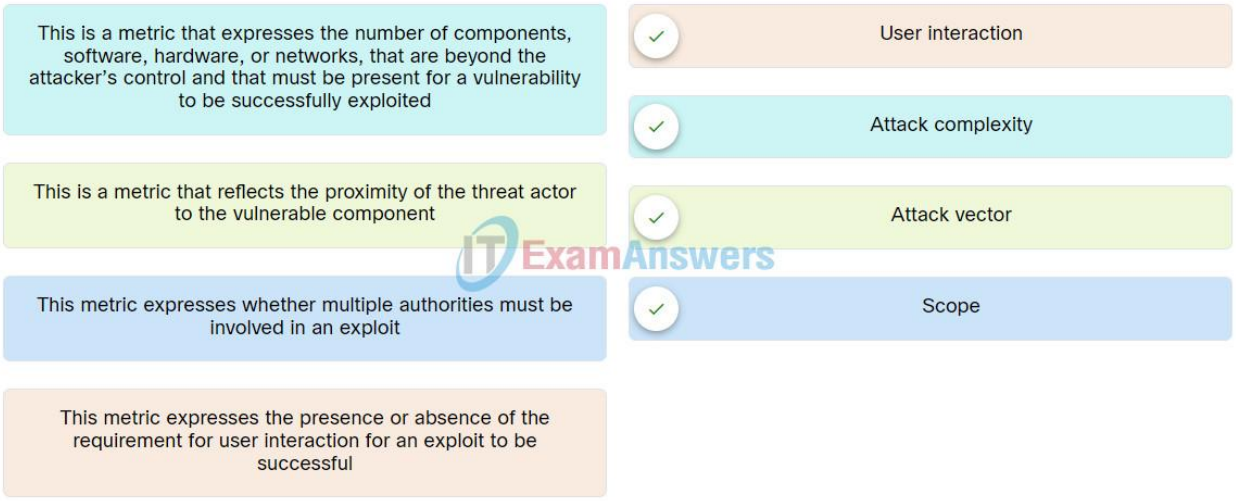
Explanation: A non-intrusive scan allows a penetration tester to assess a target and collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets.

41. When using a CVSS risk assessment tool, what must be completed first in order for a score to be calculated for the Temporal Metric Group?

- **Base Metric Group**
- Redemption level
- CVSS calculator
- Enviromental Metric Group

Explanation: The CVSS Base Metrics Group is designed as a way to assess security vulnerabilities that are found in software and hardware systems. It describes the severity of a vulnerability based on the characteristics of a successful exploit of the vulnerability. The Base Metric Group should be created first in order to create the Temporal Metric Group.

42. Match the criteria for the Base Metric Group Exploitability metrics with its description.



Explanation: Place the options in the following order:

This metric expresses whether multiple authorities must be involved in an exploit.	Scope

This is a metric that expresses the number of components,software,hardware,or networks,that are beyond the attacker's control and that must be present for a vulnerability to be successfully exploited.	Attack complexity
This is a metric that reflects the proximity of the threat actor to the vulnerable component.	Attack vector
This metric expresses the presence or absence of the requirement for user interaction for an exploit to be successful.	User interaction

43. The IT security team of an organization is charged with cybersecurity threat assessment and risk management. Which Cisco service would assist the task by providing information about security incident detection rule sets for the Snort.org, ClamAV, and SpamCop network security tools?

- MITRE
- FireEye
- **Talos**
- AIS

Explanation: Cisco Talos maintains the security incident detection rule sets for the Snort.org, ClamAV, and SpamCop network security tools. Talos helps protect enterprise users, data, and infrastructure from active adversaries. The Talos team collects information about active, existing, and emerging threats. Talos then provides comprehensive protection against these attacks and malware to its subscribers.

44. A cybersecurity technician sets up a honeypot within a separate DMZ of the enterprise network. What is the purpose of doing this?

- **to attract threat actors in order to gather attack-related information that can then be shared with threat intelligence platform subscribers**
- to gather virus signatures so that antivirus signature database can be updated
- to set up an audit trail of threat actors who access the platform
- to gather malware signatures so that they can patch the attack surface

Explanation: Honeypots are simulated networks or servers that are designed to attract threat actors in order to gather attack-related information that can then be shared with threat intelligence platform subscribers.

45. Forensic procedures must be followed exactly to ensure the integrity of data obtained in an investigation. When making copies of data from a machine that is being examined, which of the following should be done to ensure it is an exact duplicate?

- **Perform a cyclic redundancy check using a checksum or hashing algorithm**
- Change the attributes of data to make it read-only
- Do nothing — imaging software always makes an accurate image
- Open files on the original media and compare them to the copied data

Explanation: To verify that a copy of data is an exact match, it is necessary to perform a cyclic redundancy check using a checksum or hashing algorithm.

46. What procedure should be avoided in a digital forensics investigation?

- Secure physical access to the computer under investigation.
- **Reboot the affected system upon arrival.**
- Make a copy of the hard drive.
- Recover deleted files.

Explanation: Digital forensic investigation is the science of collecting and examining electronic evidence that can evaluate damage to a computer as a result of an electronic attack or that can recover lost information from a system in order to prosecute a criminal. To prevent tampering and alteration of the suspect data, a data forensic analysis should be conducted on a copy of the suspect computer. Furthermore, restarting a computer may change or overwrite files and inadvertently destroy evidence.

47. A cybersecurity team needs to investigate several incidents. In which step of the NIST incident response life cycle are the tools and assets, required to do this investigation, acquired and deployed?

- detection and analysis
- post-incident activities
- **preparation**
- containment, eradication, and recovery,

Explanation: Preparation is the first phase of the incident response life cycle. In this phase the Computer Security Incident Response Team CSIRT is created and deployed. Also in this phase the tools and assets needed by the team to investigate incidents are acquired and deployed.

48. In which phase of the NIST Incident Response Life Cycle are the vulnerabilities that have been exploited by the attacker corrected and patched?

- Post-Incident Activities
- Detection and Analysis
- Preparation
- **Containment, Eradication, and Recovery**

Explanation: In the Containment, Eradication, and Recovery phase all of the hosts that need remediation are identified and all of the effects of the security incident are eliminated. In addition, all of the vulnerabilities that were exploited by the attacker must also be corrected or patched so that the incident does not occur again.

49. Which of the following is the simplest exercise to use for training employees and testing an organization's disaster recovery plan?

- **Tabletop exercise**
- A full operational exercise
- A simulation
- Functional test

Explanation: The simplest is a tabletop exercise in which participants sit around a table with a facilitator who supplies information related to a scenario incident and processes that are being examined. No actual processes or procedures are invoked; they are just discussed.

50. What is an example of a business continuity plan?

- Ensuring critical systems are online during a disaster
- Identifying and analyzing potential events that may negatively impact an organization's assets
- Identifying critical business processes, resources and relationships between systems by focusing on the consequences of an interruption to critical business functions
- **Getting critical systems to another location while the repair of the original facility is underway**

Explanation: A business continuity plan (BCP) is a broader plan than a disaster recovery plan (DRP) because it can include getting critical systems to another location while the repair of the original facility is underway. In such a scenario, personnel continues to perform all business processes in an alternate manner until normal operations resume.

51. What is a function of a protocol analyzer?

- monitor network systems for malicious activity or policy violations
- provide real time reporting and long-term analysis of security events
- **analyze the value and contents of the protocol fields of captured packets**
- permit or deny traffic based on Layer 3 and Layer 4 protocol information

Explanation: Protocol analyzers capture packets on the network and can look into the various fields of the packets to detect network problems.

52. A user wants to store data where it is accessible from any computer with internet access. What storage technology meets the needs of the user?

- **cloud**
- NAS
- RAID
- DAS

Explanation: Cloud storage is a remote storage option that stores data in the data center of a cloud storage provider. The data is then available over the internet to users with the appropriate credentials.

53. An organization is implementing security requirements for teleworkers to access the corporate network. What are two examples of technical control for the implementation? (Choose two.)

- **Install and configure a VPN appliance.**
- Implement smart card usage.
- Move the data center to cloud.
- **Enable multi-factor authentication.**
- Ask teleworkers to review and sign off on an access control policy.

Explanation: Security controls are safeguards or countermeasures that an organization implements to avoid, detect, counteract, or minimize security risks to organizational assets. The three control types are administrative controls, technical controls, and physical controls. Technical controls involve hardware and/or software implemented to manage risk and provide protection.

54. An online store has set a control objective to maintain the highest level of website availability. Which two possible control mechanisms should the online store implement? (Choose two.)

- Configure the web server with the latest CPU product.
- Require the highest internet connection bandwidth from the ISP.
- Ensure that the web server contains the maximum local storage space.
- **Implement a server cluster for web services.**
- **Deploy web services on multiple cloud service providers.**

Explanation: High website availability requires control to manage the failure of the web server. The key mechanism to control and manage web server failure is to implement fault tolerance. Implementing a server cluster provides web server fault tolerance and deploying web services on multiple sites provides hosting site fault tolerance. Using the latest CPU and the highest internet connection bandwidth provides better web server performance and response time, but does not directly contribute to high availability.

55. Refer to the exhibit. A specialist in the information security team is reviewing the Webroot threat report 2020. Based on the findings in the report, what is a technique used by ransomware attackers that results in making it more difficult for legal teams to track their activities?

Ransomware didn't show up in force until 2015. Before that, we saw a fair amount of fake antivirus software in which a popup alarmingly informed the user that their system had been compromised, and they needed to click a link to "clean" their system. This action typically incurred some sort of cost and further compromised the system. By the mid-2010s, hackers began using cryptocurrency to make it more difficult for legal authorities to track their activities. This advantage coupled with the high value of the currency made it a booming business. With the evolution of ransomware came offers for free single-file decryption, multi-language support and customer service—all from the bad actors who had perpetrated the attack in the first place.

Junior Cybersecurity Analyst Career Path Exam Q55

- using an advanced encryption algorithm
- **employing cryptocurrency**
- using fake antivirus software
- requiring the victim to click a link to clear their system

Explanation: According to the Webroot threat 2020 report, by the mid-2010s, ransomware attackers began using cryptocurrency to make it more difficult for legal authorities to track their activities.

56. Why does an organization need to conform to a standard data governance framework?

- to provide guidelines on how to select a service provider for cloud data storage
- **to ensure that an organization can manage data in a consistent manner and ensure that data is trustworthy**
- to define security controls to protect data owned by the organization
- to define the data model for the online applications used by the organization

Explanation: Data governance determines who is authorized to make decisions about data within an organization. With an effective data governance, an organization can manage data in a consistent manner and ensure that data is trustworthy.

57. Which two business and technical challenges does implementing virtualization within a data center help businesses to overcome? (Choose two.)

- virus and spyware attacks
- operating system license requirements
- server hardware needs
- **power and air conditioning**
- **physical footprint**

Explanation: Traditionally, one server was built within one machine with one operating system. This server required power, a cool environment, and a method of backup. Virtualized servers require more robust hardware than a standard machine because a computer or server that is in a virtual machine commonly shares hardware with one or more servers and operating systems. By placing multiple servers within the same physical case, space is saved. Virtualized systems still need the proper licenses for operating systems or applications or both and still need the proper security applications and settings applied.

58. Match the alert classification to the description.

Explanation: Place the options in the following order:

an alert which does not indicate an actual security incident	false positive

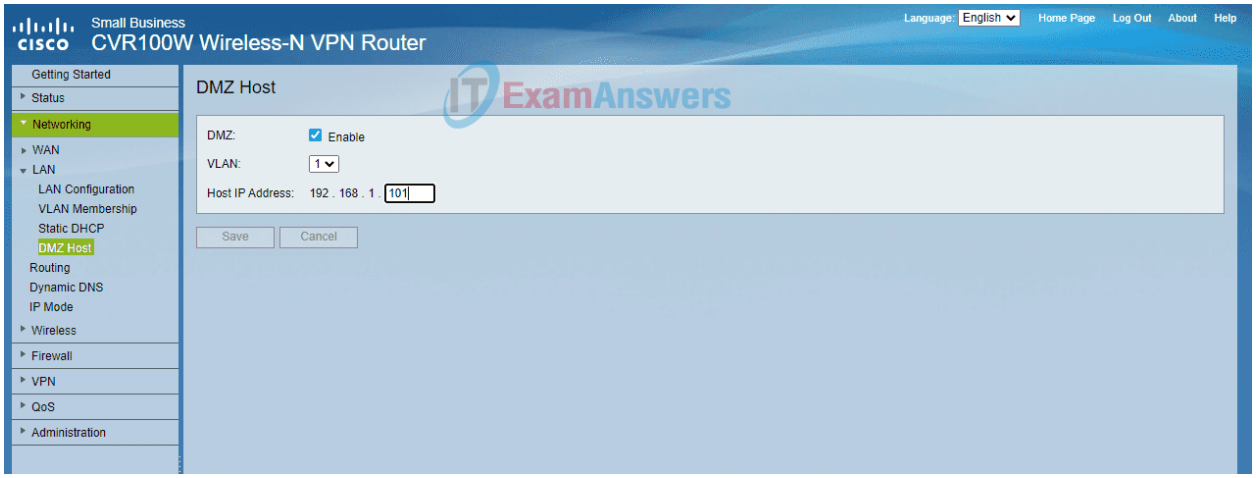
there is no alert issued and benign normal traffic is correctly ignored	true negative
there is no alert issued,however exploits are occurring undetected	false negative
a verified alert indicating an actual security incident	true positive

59. What type of activity occurs during the deployment phase of the asset lifecycle?

- Modifications and maintenance are performed on an asset.
- An asset is added to the inventory of the organization.
- **An asset is moved from inventory to in-use.**
- Upgrades, patches, and new licenses are applied to an asset.

Explanation: The deployment phase of the asset life cycle involves moving an asset from inventory to use.

60. Refer to the exhibit. The wireless router firewall is configured as shown. What action will be taken when packets that originate from the internet and have a destination IP address of 192.168.1.101 are received by the firewall?



- Only inbound traffic that is addressed to HTTP ports is forwarded to the server.
- **The detected inbound traffic is forwarded to the switch port where the server is connected.**
- All devices on the network receive the traffic, but only the server is permitted to respond.
- Any traffic that is not in response to requests originating from the server is dropped.

Explanation: With a wireless router, a simple DMZ can be set up that allows an internal server to be accessible by outside hosts. To accomplish this, the server requires a static IP address that must be specified in the DMZ configuration. The wireless router isolates traffic destined to the IP address specified. This traffic is then forwarded only to the switch port where the server is connected.

61. What names are given to a database where all cryptocurrency transactions are recorded? (Choose two.)

- Table
- **Blockchain**
- Spreadsheet
- **Ledger**

Explanation: Cryptocurrency owners keep their money in encrypted, virtual 'wallets.' When a transaction takes place between the owners of two digital wallets, the details are recorded in a decentralized, electronic ledger or blockchain system. This means it is carried out with a degree of anonymity and is

self-managed, with no interference from third parties such as central banks or government entities.

62. What are the two important components of a public key infrastructure (PKI) used in network security? (Choose two.)

- pre-shared key generation
- **digital certificates**
- intrusion prevention system
- symmetric encryption algorithms
- **certificate authority**

Explanation: A public key infrastructure uses digital certificates and certificate authorities to manage asymmetric key distribution. PKI certificates are public information. The PKI certificate authority (CA) is a trusted third-party that issues the certificate. The CA has its own certificate (self-signed certificate) that contains the public key of the CA.

63. You are asked for advice on how to best prevent unauthorized hosts from accessing the home network of employees. Which of the following security measures do you think would be most effective?

- Implementing a VLAN
- **Implementing a firewall**
- Implementing a RAID
- Implementing instruction detection systems

Explanation: Implementing a firewall will control remote access to the home network. Operating systems include a firewall, or a user can purchase or download software from a third party.

64. A SOHO company is planning to use public cloud computing for hosting an online ordering application. The company is evaluating options to prevent sensitive data loss from cloud storage. What two countermeasures could be implemented to address the issue? (Choose two.)

- **Deploy the application and data across multiple zones.**
- Implement multi-factor authentication processes.
- Install antivirus and host-based intrusion detection software on VMs in the cloud.

- Develop and implement compliance policies.
- **Perform a daily backup of data.**

Explanation: Data backup procedures and deploying the application and data across multiple zones can protect against loss of data.

65. Which type of DNS attack involves a threat actor creating multiple bogus sub-domains under a legitimate parent domain?

- DNS Tunneling attacks
- DNS Stealth attacks
- **DNS Domain Shadowing attacks**
- DNS Open Resolver attacks

Explanation: A DNS domain shadowing attack occurs when the credentials for a domain have been compromised and the malicious user has access to the customer DNS domain account. The attacker will then begin to set up new sub domains off of the root domain that point to malicious servers.

66. A network technician is assigned the task of hardening a Cisco switch before placing it into the LAN. The technician configures and encrypts the user and privilege mode passwords, creates a new management VLAN, and verifies that the IOS is up-to-date. What action should the technician take to ensure that remote access to the system is secure during transmission?

- **Restrict VTY ports to only accept SSH connections.**
- Configure local users and encrypt their passwords.
- Shutdown all unused Ethernet ports on the switch.
- Configure port security on all Ethernet ports.

Explanation: SSH provides security for remote connections by providing strong encryption when a device authenticates (username and password) and when transmitting data between the communicating devices. Using the command on the VTY lines restricts the device to only accept SSH connections.

67. A network security technician is configuring account settings on Windows laptops that will be used by employees from their homes. Which Local Security Policy setting can prevent or discourage brute-force password attacks?

- User Rights Assignment

- **Account Lockout Policy**
- Software Restriction Policies
- Password Policy

Explanation: An account lockout policy locks an account for a set duration when too many incorrect login attempts occur. Setting a lockout threshold, lockout duration, and a time limit before resetting the invalid login counters can prevent or discourage brute-force password attacks.

68. A cloud service company provides web service to clients. The company is assessing the risk of service disruption due to hardware failure. The company decides to add another data center in a different building. Which risk management action level is the company implementing?

- **mitigation**
- transfer
- avoidance
- accept

Explanation: Risk management is the identification, evaluation, and prioritization of risks. Organizations manage risk in one of four ways: avoidance (elimination), mitigation (reduction), transfer, and accept. Risk mitigation involves implementing controls that allow the organization to continue to perform an activity while using mechanisms to reduce the risk from a particular threat.

69. What is the purpose of penetration testing?

- **It involves hacking a website, network or server with the permission of the respective organization.**
- It fixes issues found by a vulnerability scanner.
- It is used to audit enterprise patch management.
- It is used to passively scan OS attack platforms.

Explanation: Penetration testing involves hacking a website, network or server with the permission of an organization. Ethical hackers try to gain access to resources using various methods that real-life black hat hackers would use.

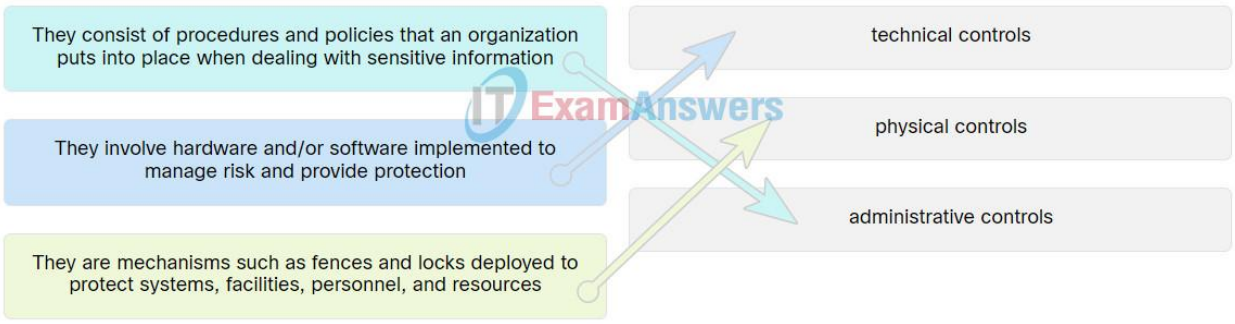
70. What tool is used to lure an attacker so that an administrator can capture, log and analyze the behavior of the attack?

- IDS

- **Honeypot**
- NetFlow
- Nmap

Explanation: Administrators can use a tool called a honeypot to lure an attacker so that their behavior can be analyzed.

71. Match the security control type to the appropriate description.



72. The results of an audit on cybersecurity practices revealed that several company servers were not updated with the latest patches. The audit also revealed that several user accounts had escalated privileges and were allowed unauthorized network resource access. Which two security policies should be enforced to address these issues? (Choose two.)

- data policy
- organizational policy
- **network maintainance policy**
- credential policy
- **identification and authentication policy**

Explanation: Identification and authentication policy defines users network access and verification methods used, while the network maintainanace policy defines procedures for updating network operating systems.

73. What type of cipher encrypts plaintext one byte or one bit at a time?

- block
- enigma
- elliptical
- **stream**
- hash

Explanation: Stream ciphers encrypt plaintext one byte or one bit at a time, and can be much faster than block ciphers.

74. A network technician is preparing a number of laptops to be loaned to employees while they are traveling. These employees will not be logging into the corporate directory server when they are away from the office. Which type of software should be configured on the laptops in order to filter incoming and outgoing network connections?

- **host-based firewall**
- virus and malware scanner
- host intrusion detection system
- IOS stateful firewall

Explanation: A host-based firewall runs on a device to restrict incoming and outgoing network activity for that device. It can allow or deny traffic between the device and the network.

75. The administrator of a Linux server uses the chmod 777 /usr/phones.txt command to assign permissions to a file that contains the company phone directory. What permissions are assigned with this command?

- **All users have read, write and execute permissions to the file.**
- Only members of the administrators group can read, write, and execute the file.
- No users have write permission to the file, other than root.
- All users have read permission to the file, but not write or execute.

Explanation: There are two methods to set permissions on a file or directory using the command in Linux. The first is symbolic notation, which use the lettersto symbolize the read, write and execute permissions. The second method is to use absolute or octal permission settings. In absolute permission assignments, the 7 represents all three permissions: read, write and execute. The assignment 777 assigns full permissions to the owner, group, and other users.

76. Which control should an organization use to restore a system back to its normal state?

- Compensative
- **Corrective**

- Preventive
- Detective

Explanation: Corrective controls restore the system after a disaster or an event. Detective controls discover unwanted events and new potential threats. Preventive controls prevent a disaster from occurring.

77. A network administrator notices that several company wireless access points are using WEP for encryption and authentication. The administrator needs to update the encryption and authentication configurations. Which security policy would address the process of updating AP configurations?

- credential policy
- network maintenance policy
- identification and authentication policy
- **organizational policy**

Explanation: Since the hotspots are part of the company's assets, the organizational policy would address any change control or asset management practices.

78. An organization needs to implement a solution that would enable them to determine the order of security events occurring on the network. What technology should be implemented?

- NAT
- DHCP
- SNMP
- **NTP**

Explanation: To accurately timestamp events on a network, time must be synchronized between devices. Network Time Protocol (NTP), allows devices on the network to synchronize their time with an NTP server or master clock.

79. What statement describes a function that the Diffie-Hellman algorithm provides to IPsec VPNs?

- It is used to identify the source of data that is sent through the VPN.
- It is an encryption algorithm that is used to ensure that data cannot be intercepted.

- It ensures that data has not been changed between the sender and receiver.
- **It allows two parties to establish a shared secret key over an unsecured channel.**

Explanation: The Diffie-Hellman algorithm allows two end devices to create a shared secret key that can be used for encryption. This key can be generated over an insecure channel while ensuring that no other device can get the key.

80. A small company uses a public cloud service provider to host an online store. The online store uses a web application as the front end and a database as the backend. When a customer places an order in the web form, the request is then sent to the database to check the inventory, current price, and customer information thereby completing the order. The IT manager is learning that threat attackers may launch attacks by injecting malformed data into the web application. What is a security coding technique that the company can use to minimize such attacks?

- multi-factor authentication
- obfuscation
- **input validation**
- encryption

Explanation: User input validation rules can help ensure the security of applications and databases by checking to see if data meets certain rules when entered into a feld in a web form. A validation rule checks that data falls within the parameters defned by the database designer. This helps to ensure the completeness, accuracy, and consistency of data.

81. What security tool allows an organization to collect data about security threats from various sources, and respond to low-level events without human intervention?

- **SOAR**
- Nessus
- GFI LanGaurd
- SIEM

Explanation: Security Orchestration Automation and Response (SOAR) tools allow an organization to collect data about security threats from various sources, and respond to low-level events without human intervention.

82. Which parameter is used to identify applications when a user sends a service request to a remote server?

- **destination port number**
- TCP sequence number
- server IP address
- source port number

Explanation: In TCP/IP transmissions, the protocols at the transport layer of both the OSI and TCP/IP model use port addressing to enable multiple conversations to be tracked and connected with the correct applications. The destination port number in the packets sent by the source device identifies the requested application.

83. A network technician is charged with researching and collecting information regarding recent cybersecurity incidents. The technician decides to start with web sites that are opensource intelligence (OSINT). Which two statements describes OSINT types of web sites? (Choose two.)

- Their operations are in compliance with government regulations and policies.
- **Most of them provide free access to their database.**
- They are all run by government agencies.
- **They collect information that is available to the general public.**
- They usually require user registration and a small monthly fee.

Explanation: Open-source intelligence (OSINT) is derived from data and information that is available to the general public. Some companies and government agencies offer near real-time, high-quality cyber threat information through their web sites, which is mostly free to visitors.

84. What are three actions taken in the Detection & Analysis phase of the NIST Incident Response Life Cycle? (Choose three.)

- The CSIRT is created and trained.

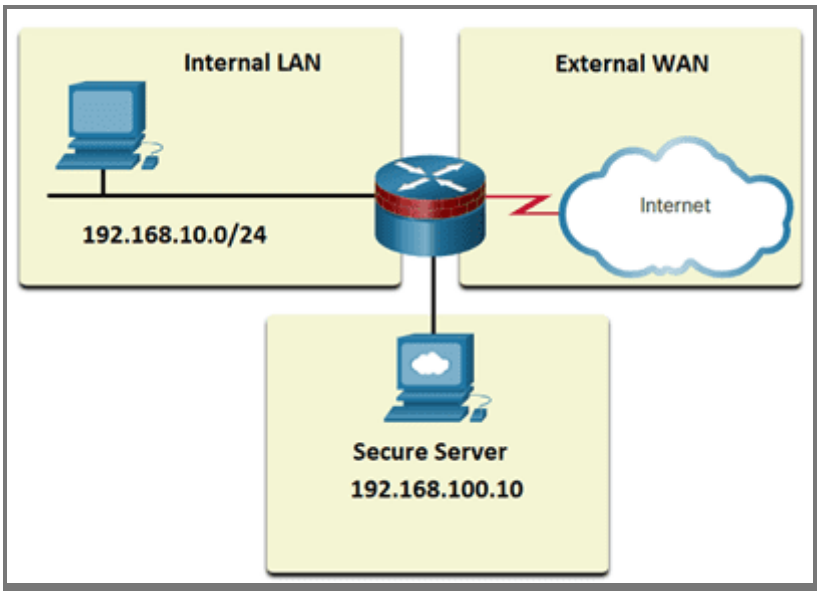
- The effectiveness of the incident handling process is reviewed and any necessary hardening for existing security controls and practices is identified.
- **The type of incident and the extent of the effects are determined.**
- **The appropriate stakeholders and outside parties are notified so that all who need to be involved can play their role.**
- The incident is contained and subsequent actions are determined.
- **The CSIRT performs an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected, who or what originated the incident, and how the incident is occurring.**

Explanation: The Detection & Analysis phase of the Incident Response Life Cycle includes actions such as determining which networks, systems, or applications are affected, who or what originated the incident, and how the incident is occurring. It also includes notifying the appropriate stakeholders and outside parties so that all who need to be involved can play their role, determining the type of incident, and measuring the characteristics of expected activity in networking devices and systems so that changes to it can be more easily identified.

85. Refer to the exhibit. What type of traffic will the policy be applied to when the router is configured with the class-map and policy-map shown?

```
class-map type inspect match-all INTERNAL-WEB
 match protocol https
 match access-group 101
!
policy-map type inspect SEC-INT-WEB
 class type inspect INTERNAL-WEB
 inspect
!

access-list 101 permit tcp 192.168.10.0 0.0.0.255 host 192.168.100.10
```



- only HTTPS traffic sourced from any internal or external source address destined for the secure server
- **only HTTPS traffic sourced from the internal LAN IP address range destined for the secure server**
- all traffic that is using either the HTTP protocol or is sourced from the internal LAN IP address range
- all traffic from the internal LAN IP address range to the secure server using any TCP protocol

Explanation: When the class-map is configured with the match-all criteria, all packets must meet all of the criteria to be considered to be a member of the class. In this example, there are two criteria that must be matched: the HTTPS protocol and the permitted traffic defined by the access list 101. Only packets meeting both conditions will be inspected and passed.

86. What key considerations does a business impact analysis (BIA) examine? Choose four correct answers

- **Recovery time objectives (RTOs)**
- **Recovery point objectives (RPOs)**
- Recovery point times (RPTs)
- Mean time between objectives (RBOs)
- **Mean time between failures (MTBF)**
- **Mean time to repair (MTTR)**