CompTIA SY0-401 Exam

Volume: 1149 Questions

Question No: 1
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

A. PAT

B. NAP

C. DNAT

D. NAC

Answer: A

Question No: 2
Which of the following devices is MOST likely being used when processing the following?

```
1 PERMIT IP ANY ANY EQ 80
2 DENY IP ANY ANY
```

A. Firewal

B. NIPS

C. Load balancer

D. URL filter

Answer: A

Question No: 3
The security administrator at ABC company received the following log information from an external party:

```
10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal
10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force
10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan
```

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

A. A NIDS was used in place of a NIPS.

B. The log is not in UTC.

C. The external party uses a firewall.

D. ABC company uses PAT.

Answer: D

Question No: 4
Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

A. Sniffer

B. Router

C. Firewall

D. Switch

Answer: C

Question No: 5
Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

A. Packet Filter Firewall

B. Stateful Firewall

C. Proxy Firewall

D. Application Firewal

Answer: B

Question No: 6
The Chief Information Security Officer (CISO) has mandated that al IT systems with credit card data be segregated from the main corporate network to prevent unauthorized access and that access to the IT

systems should be logged. Which of the following would BEST meet the CISO’s requirements?

A. Sniffers

B. NIDS

C. Firewalls

D. Web proxies

E. Layer 2 switches

Answer: C

Question No: 7
Which of the following network design elements allows for many internal devices to share one public IP address?

A. DNAT

B. PAT

C. DNS

D. DMZ

Answer: B

Question No: 8
Which of the following is a best practice when securing a switch from physical access?

A. Disable unnecessary accounts

B. Print baseline configuration

C. Enable access lists

D. Disable unused ports

Answer: D

Question No: 9
Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

A. Protocol analyzer

B. Load balancer

C. VPN concentrator

D. Web security gateway

Answer: B

Question No: 10
Pete, the system administrator, wishes to monitor and limit users' access to external websites.
Which of the following would BEST address this?

A. Block all traffic on port 80.

B. Implement NIDS.

C. Use server load balancers.

D. Install a proxy server.

Answer: D

Question No: 11
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS

B. Firewal

C. NIPS

D. Spam filter

Answer: C

Question No: 12
Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

A. HIPS on each virtual machine

B. NIPS on the network

C. NIDS on the network

D. HIDS on each virtual machine

Answer: A

Question No: 13
Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

A. NIPS

B. HIDS

C. HIPS

D. NIDS

Answer: A

Question No: 14
An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

A. NIDS

B. NIPS

C. HIPS

D. HIDS

Answer: B

Question No: 15
In intrusion detection system vernacular, which account is responsible for setting the security policy for an organization?

A. Supervisor

B. Administrator

C. Root

D. Director

Answer: B

Question No: 16
When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.
Which of the following is the type of vulnerability described?

A. Network based

B. IDS

C. Signature based

D. Host based

Answer: C

Question No: 17
The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

A. Signature Based IDS

B. Heuristic IDS

C. Behavior Based IDS

D. Anomaly Based IDS

Answer: A

Question No: 18

Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

A. Application Firewall

B. Anomaly Based IDS

C. Proxy Firewall

D. Signature IDS

Answer: B

Question No: 19

Matt, an administrator, notices a flood fragmented packet and retransmits from an email server.
After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

A. Spam filter

B. Protocol analyzer

C. Web application firewall

D. Load balancer

Answer: B

Question No: 20

Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH

B. ACK

C. SYN

D. URG

E. FIN

Answer: B,C

Question No: 21

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

A. Spam filter

B. URL filter

C. Content inspection

D. Malware inspection

Answer: B

Question No: 22

Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal?

A. Firewal

B. Switch

C. URL content filter

D. Spam filter

Answer: C

Question No: 23
The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

A. The access rules on the IDS

B. The pop up blocker in the employee's browser

C. The sensitivity level of the spam filter

D. The default block page on the URL filter

Answer: D

Question No: 24
Layer 7 devices used to prevent specific types of html tags are called:

A. Firewalls

B. Content filters

C. Routers

D. NIDS

Answer: B

Question No: 25
Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter

B. Firewal

C. Proxy server

D. Protocol analyzer

Answer: A

Question No: 26

A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan al web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

A. ACL

B. IDS

C. UTM

D. Firewall

Answer: C

Question No: 27

Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

A. WAF

B. NIDS

C. Routers

D. Switches

Answer: A

Question No: 28

Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

A. Spam filter

B. Load balancer

C. Antivirus

D. Proxies

E. Firewal

F. NIDS

G. URL filtering

Answer: D,E,G

Question No: 29
A security engineer is reviewing log data and sees the output below:
POST: /payload.php HTTP/1.1 HOST: localhost Accept: */* Referrer: http://localhost/ ******* HTTP/1.1 403 Forbidden Connection: close
Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

A. Host-based Intrusion Detection System

B. Web application firewall

C. Network-based Intrusion Detection System

D. Stateful Inspection Firewall

E. URL Content Filter

Answer: B

Question No: 30
An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start?

A. Review past security incidents and their resolution

B. Rewrite the existing security policy

C. Implement an intrusion prevention system

D. Install honey pot systems

Answer: C

Question No: 31

A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

A. Host-based firewall

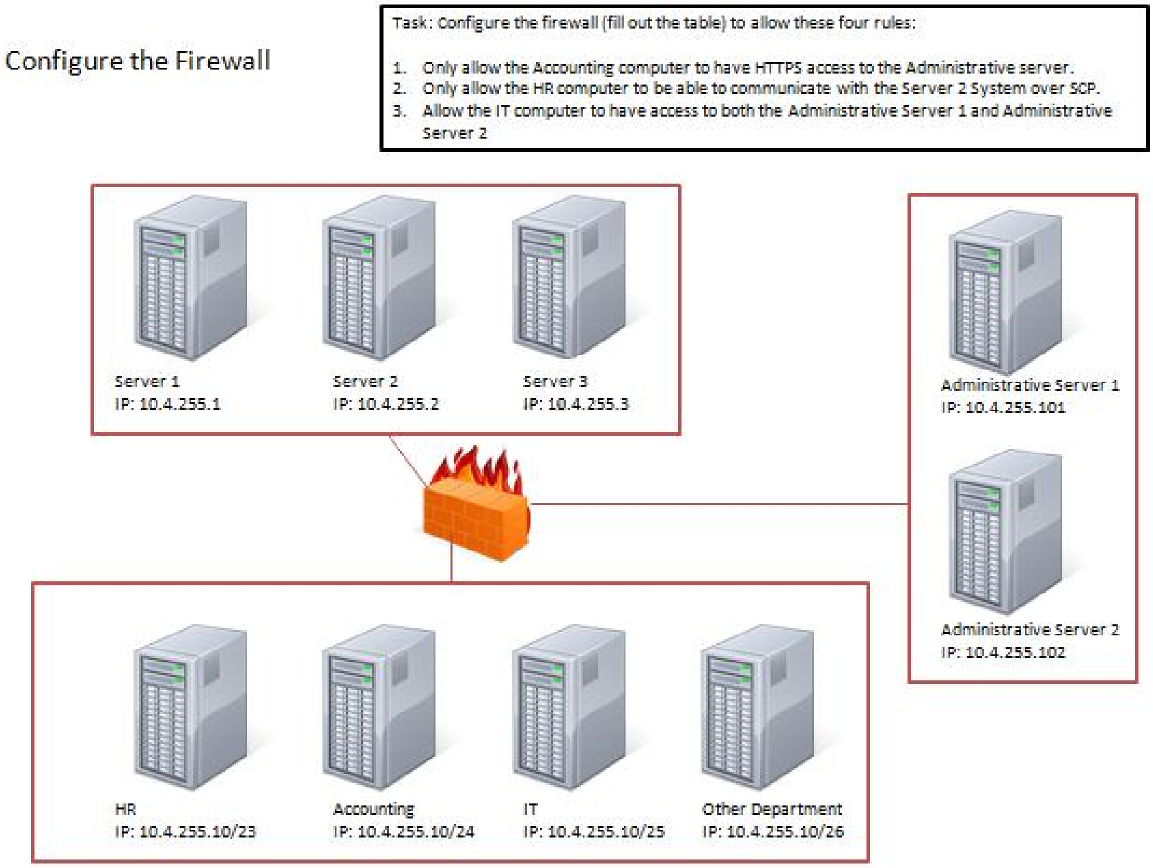
B. IDS

C. IPS

D. Honeypot

Answer: B

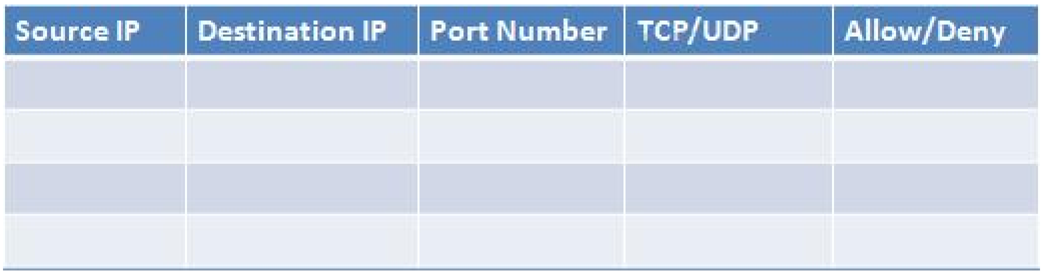
Question No: 32 CORRECT TEXT



Configure the Firewall

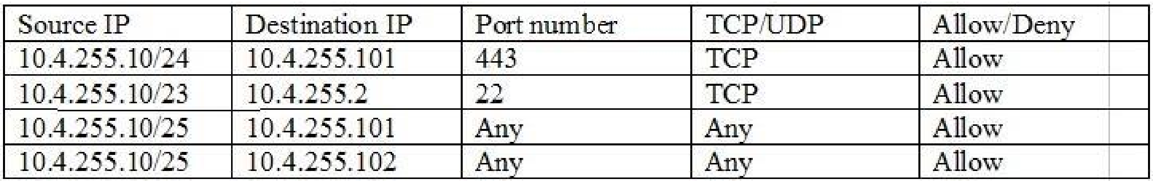
Task: Configure the firewall (fill out the table) to allow these four rules:

1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Answer:



Source IP	Destination IP	Port number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Question No: 33 HOTSPOT

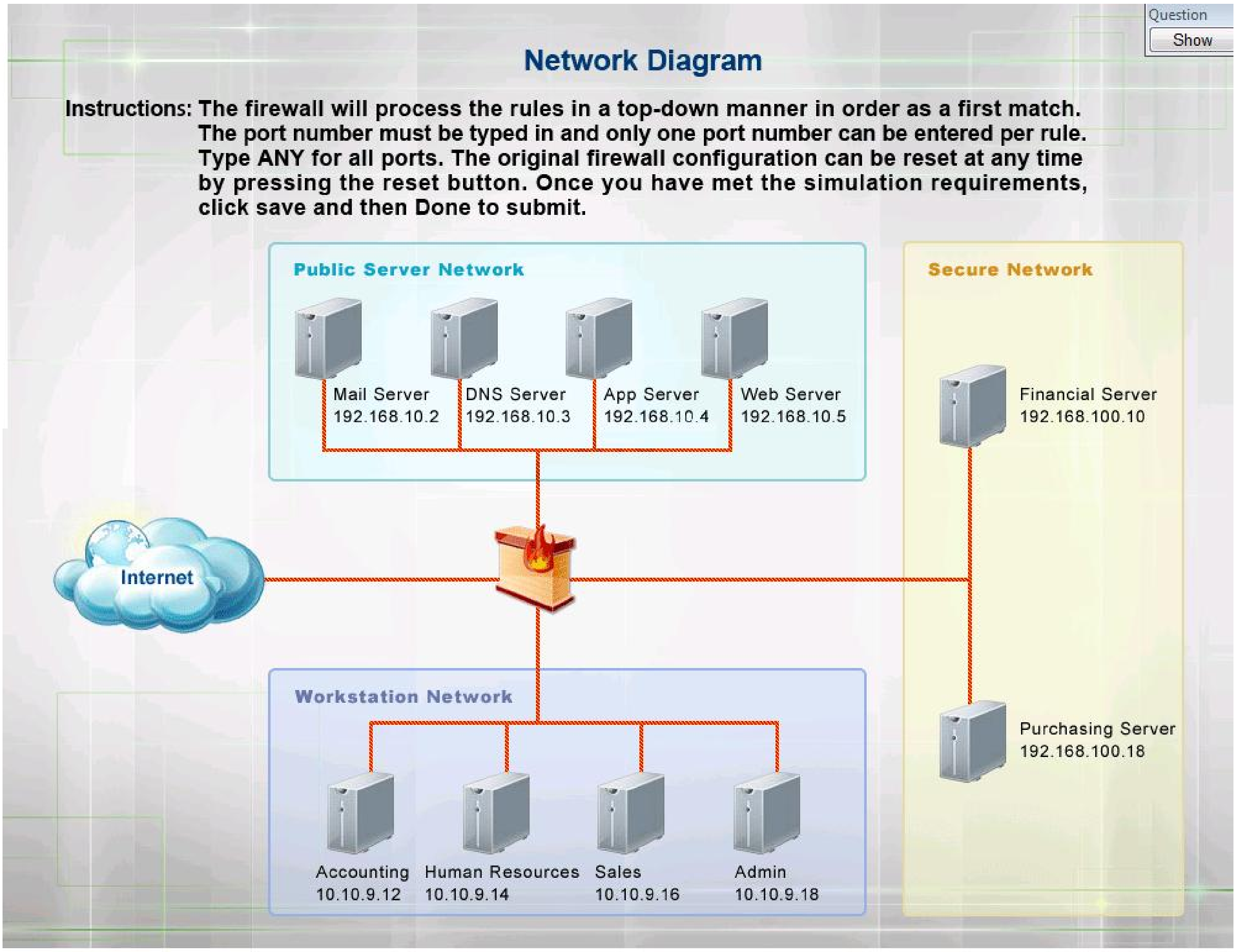
The security administrator has installed a new firewall which implements an implicit DENY policy by default. Click on the firewall and configure it to allow ONLY the following communication.

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.

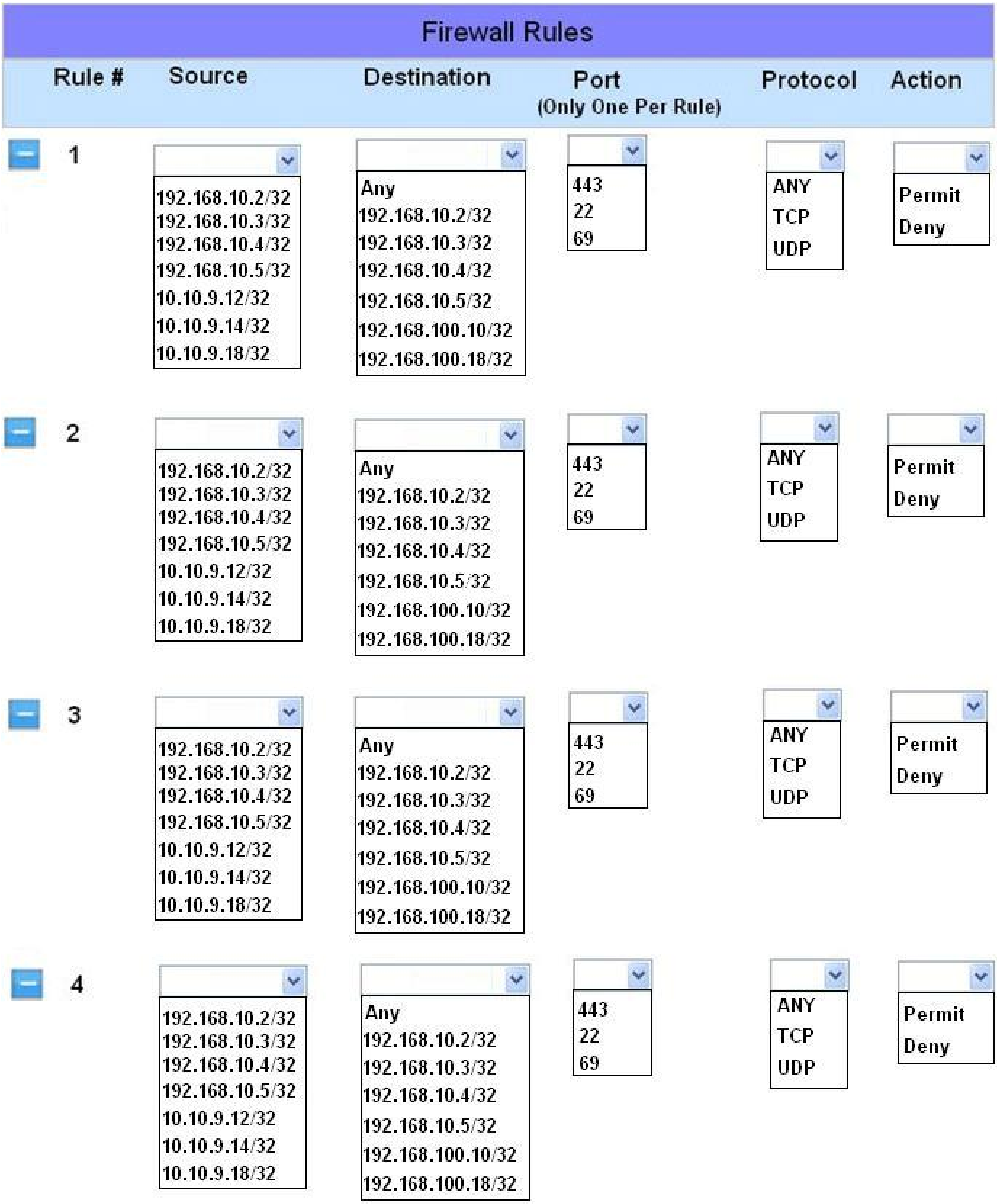


Question

Show

Network Diagram

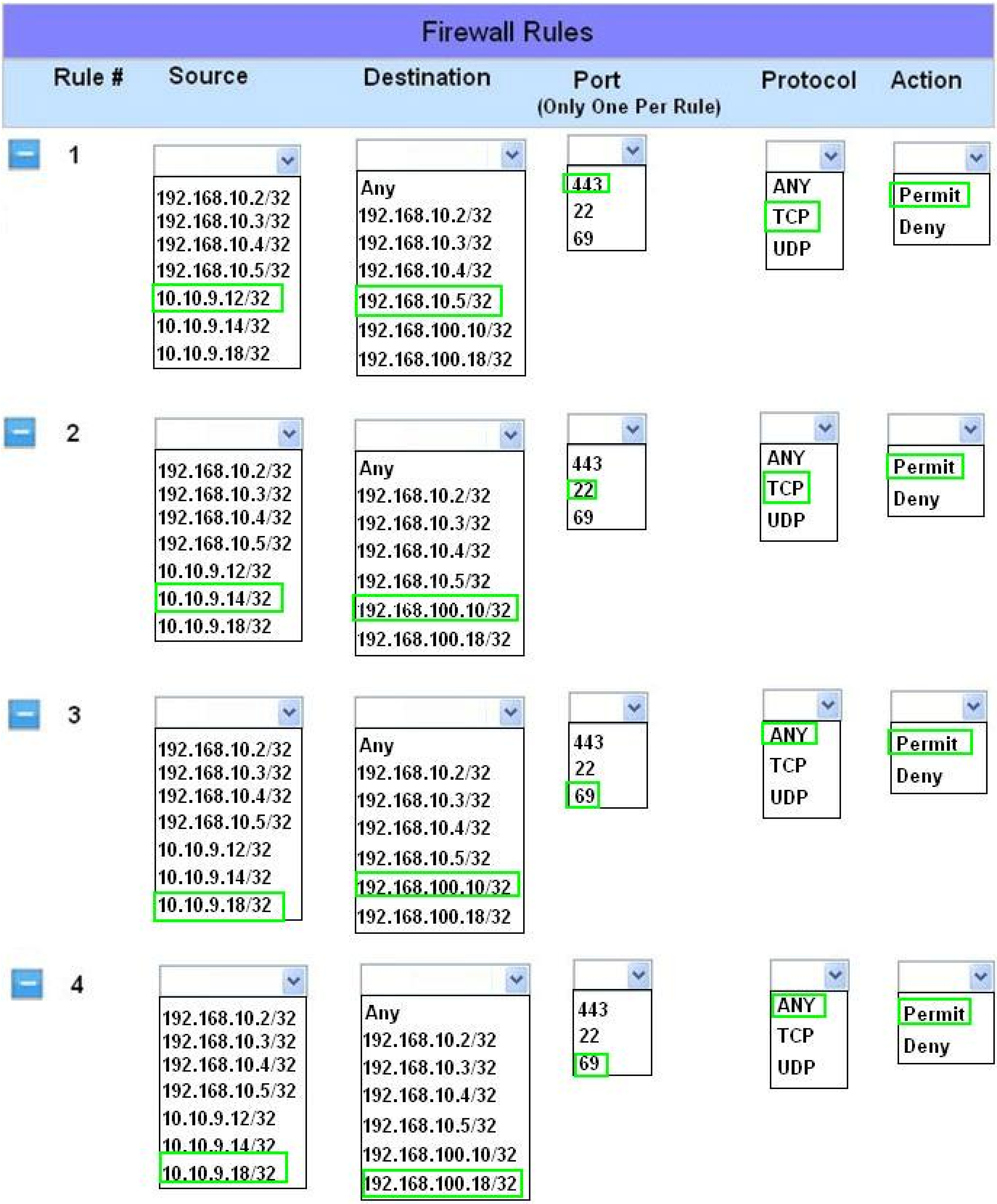
Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny

Answer:



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 10.10.9.12/32] 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 [✓ 192.168.10.5/32] 192.168.100.10/32 192.168.100.18/32	[✓ 443] 22 69	ANY [✓ TCP] UDP	[✓ Permit] Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 [✓ 10.10.9.14/32] 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 192.168.100.10/32] 192.168.100.18/32	443 [✓ 22] 69	ANY [✓ TCP] UDP	[✓ Permit] Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 [✓ 10.10.9.18/32]	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 192.168.100.10/32] 192.168.100.18/32	443 22 [✓ 69]	[✓ ANY] TCP UDP	[✓ Permit] Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 [✓ 10.10.9.18/32]	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 [✓ 192.168.100.18/32]	443 22 [✓ 69]	[✓ ANY] TCP UDP	[✓ Permit] Deny

Question No: 34

Which of the following firewall rules only denies DNS zone transfers?

A. deny udp any any port 53

B. deny ip any any

C. deny tcp any any port 53

D. deny all dns packets

Answer: C

Question No: 35
A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.
Which of the following would accomplish this task?

A. Deny TCP port 68

B. Deny TCP port 69

C. Deny UDP port 68

D. Deny UDP port 69

Answer: D

Question No: 36
Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor?

A. Allow incoming IPSec traffic into the vendor's IP address.

B. Set up a VPN account for the vendor, allowing access to the remote site.

C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.

D. Write a firewall rule to allow the vendor to have access to the remote site.

Answer: D

Question No: 37

A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

A. Implement a virtual firewall

B. Instal HIPS on each VM

C. Virtual switches with VLANs

D. Develop a patch management guide

Answer: C

Question No: 38

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks.
Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.

B. The switch has several VLANs configured on it.

C. The sub-interfaces are configured for VoIP traffic.

D. The sub-interfaces each implement quality of service.

Answer: B

Question No: 39

Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

A. Create a VLAN for the SCADA

B. Enable PKI for the MainFrame

C. Implement patch management

D. Implement stronger WPA2 Wireless

Answer: A

Question No: 40

The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented?

A. Implicit deny

B. VLAN management

C. Port security

D. Access control lists

Answer: D

Question No: 41

Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

A. Virtual switch

B. NAT

C. System partitioning

D. Access-list

E. Disable spanning tree

F. VLAN

Answer: A,F

Question No: 42

A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example?

A. Explicit deny

B. Port security

C. Access control lists

D. Implicit deny

Answer: C

Question No: 43
An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network?

A. Configure each port on the switches to use the same VLAN other than the default one

B. Enable VTP on both switches and set to the same domain

C. Configure only one of the routers to run DHCP services

D. Implement port security on the switches

Answer: D

Question No: 44
At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

A. Configure an access list.

B. Configure spanning tree protocol.

C. Configure port security.

D. Configure loop protection.

Answer: C

Question No: 45

On Monday, all company employees report being unable to connect to the corporate wireless network, which uses 802.1x with PEAP. A technician verifies that no configuration changes were made to the wireless network and its supporting infrastructure, and that there are no outages.

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

A. Too many incorrect authentication attempts have caused users to be temporarily disabled.

B. The DNS server is overwhelmed with connections and is unable to respond to queries.

C. The company IDS detected a wireless attack and disabled the wireless network.

D. The Remote Authentication Dial-In User Service server certificate has expired.

Answer: D

Question No: 46

A company determines a need for additional protection from rogue devices plugging into physical ports around the building.

Which of the following provides the highest degree of protection from unauthorized wired network access?

A. Intrusion Prevention Systems

B. MAC filtering

C. Flood guards

D. 802.1x

Answer: D

Question No: 47

While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources.

Which of the following should the administrator implement to ensure this happens?

A. Log Analysis

B. VLAN Management

C. Network separation

D. 802.1x

Answer: D

Question No: 48

A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interface.

PERMIT TCP ANY ANY 80
PERMIT TCP ANY ANY 443

Which of the following rules would accomplish this task? (Select TWO).

A. Change the firewall default settings so that it implements an implicit deny

B. Apply the current ACL to all interfaces of the firewall

C. Remove the current ACL

D. Add the following ACL at the top of the current ACL DENY TCP ANY ANY 53

E. Add the following ACL at the bottom of the current ACL DENY ICMP ANY ANY 53

F. Add the following ACL at the bottom of the current ACL DENY IP ANY ANY 53

Answer: A,F

Question No: 49

Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80
PERMIT TCP ANY HOST 192.168.0.10 EQ 443

A. It implements stateful packet filtering.

B. It implements bottom-up processing.

C. It failed closed.

D. It implements an implicit deny.

Answer: D

Question No: 50
The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates al subfolders and al subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

A. Remove the staff group from the payroll folder

B. Implicit deny on the payroll folder for the staff group

C. Implicit deny on the payroll folder for the managers group

D. Remove inheritance from the payroll folder

Answer: B

Question No: 51
A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

A. NAT and DMZ

B. VPN and IPSec

C. Switches and a firewall

D. 802.1x and VLANs

Answer: D

Question No: 52
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.

B. Remove the network from the routing table.

C. Create a virtual switch.

D. Commission a stand-alone switch.

Answer: C

Question No: 53
A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to stil be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement?

A. SaaS

B. MaaS

C. IaaS

D. PaaS

Answer: B

Question No: 54
Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

A. Failed authentication attempts

B. Network ping sweeps

C. Host port scans

D. Connections to port 22

Answer: D

Question No: 55
An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

A. Unified Threat Management

B. Virtual Private Network

C. Single sign on

D. Role-based management

Answer: A

Question No: 56
An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

A. Unified Threat Management

B. Virtual Private Network

C. Single sign on

D. Role-based management

Answer: A

Question No: 57
A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network?

A. VLAN

B. Subnet

C. VPN

D. DMZ

Answer: D

Question No: 58
Which of the following devices would MOST likely have a DMZ interface?

A. Firewal

B. Switch

C. Load balancer

D. Proxy

Answer: A

Question No: 59
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ

B. Cloud computing

C. VLAN

D. Virtualization

Answer: A

Question No: 60
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

A. VLAN

B. Subnetting

C. DMZ

D. NAT

Answer: C

Question No: 61

When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

A. DMZ

B. Cloud services

C. Virtualization

D. Sandboxing

Answer: A

Question No: 62

Which of the following BEST describes a demilitarized zone?

A. A buffer zone between protected and unprotected networks.

B. A network where all servers exist and are monitored.

C. A sterile, isolated network segment with access lists.

D. A private network that is protected by a firewall and a VLAN.

Answer: A

Question No: 63

Which of the following would allow the organization to divide a Class C IP address range into several ranges?

A. DMZ

B. Virtual LANs

C. NAT

D. Subnetting

Answer: D

Question No: 64
Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.125

B. 10.4.4.158

C. 10.4.4.165

D. 10.4.4.189

E. 10.4.4.199

Answer: C,D

Question No: 65
Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?
Server 1: 192.168.100.6
Server 2: 192.168.100.9
Server 3: 192.169.100.20

A. /24

B. /27

C. /28

D. /29

E. /30

Answer: D

Question No: 66
Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

A. NAT

B. Virtualization

C. NAC

D. Subnetting

Answer: D

Question No: 67
A small company can only afford to buy an al -in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the following should the company configure to protect the servers from the user devices? (Select TWO).

A. Deny incoming connections to the outside router interface.

B. Change the default HTTP port

C. Implement EAP-TLS to establish mutual authentication

D. Disable the physical switch ports

E. Create a server VLAN

F. Create an ACL to access the server

Answer: E,F

Question No: 68
A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.
Which of the following technologies should be employed to separate the administrative network from the network in which all of the employees' devices are connected?

A. VPN

B. VLAN

C. WPA2

D. MAC filtering

Answer: B

Question No: 69
Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

A. Connect the WAP to a different switch.

B. Create a voice VLAN.

C. Create a DMZ.

D. Set the switch ports to 802.1q mode.

Answer: B

Question No: 70
An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

A. Create three VLANs on the switch connected to a router

B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router

C. Install a firewall and connect it to the switch

D. Install a firewall and connect it to a dedicated switch for each device type

Answer: A

Question No: 71

An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

A. Routing

B. DMZ

C. VLAN

D. NAT

Answer: C

Question No: 72
Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

A. ACLs

B. VLANs

C. DMZs

D. NATS

Answer: B

Question No: 73
According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

A. NIDS

B. DMZ

C. NAT

D. VLAN

Answer: D

Question No: 74

Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]---------[10.2.2.10] LOGS

```
10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN
10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK
10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK
```

Given the above information, which of the following can be inferred about the above environment?

A. 192.168.1.30 is a web server.

B. The web server listens on a non-standard port.

C. The router filters port 80 traffic.

D. The router implements NAT.

Answer: D

Question No: 75

An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a:

A. stateful firewall

B. packet-filtering firewall

C. NIPS

D. NAT

Answer: D

Question No: 76

A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:
22, 25, 445, 1433, 3128, 3389, 6667
Which of the following protocols was used to access the server remotely?

A. LDAP

B. HTTP

C. RDP

D. HTTPS

Answer: C

Question No: 77
Which of the following is a programming interface that allows a remote computer to run programs on a local machine?

A. RPC

B. RSH

C. SSH

D. SSL

Answer: A

Question No: 78
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

A. Packet filtering firewall

B. VPN gateway

C. Switch

D. Router

Answer: B

Question No: 79
Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

A. Subnetting

B. NAT

C. Quality of service

D. NAC

Answer: C

Question No: 80
An auditor is given access to a conference room to conduct an analysis. When they connect their laptop's Ethernet cable into the wall jack, they are not able to get a connection to the Internet but have a link light. Which of the following is MOST likely causing this issue?

A. Ethernet cable is damaged

B. The host firewall is set to disallow outbound connections

C. Network Access Control

D. The switch port is administratively shutdown

Answer: C

Question No: 81
A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date.
Which of the following BEST describes this system type?

A. NAT

B. NIPS

C. NAC

D. DMZ

Answer: C

Question No: 82
Which of the following is required to allow multiple servers to exist on one physical server?

A. Software as a Service (SaaS)

B. Platform as a Service (PaaS)

C. Virtualization

D. Infrastructure as a Service (IaaS)

Answer: C

Question No: 83
A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

A. Virtualization

B. Subnetting

C. IaaS

D. SaaS

Answer: A

Question No: 84
The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

A. The administrator will need to deploy load balancing and clustering.

B. The administrator may spend more on licensing but less on hardware and equipment.

C. The administrator will not be able to add a test virtual environment in the data center.

D. Servers will encounter latency and lowered throughput issues.

Answer: B

Question No: 85

Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

A. Virtualization

B. Remote access

C. Network access control

D. Blade servers

Answer: A

Question No: 86

Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

A. The system is running 802.1x.

B. The system is using NAC.

C. The system is in active-standby mode.

D. The system is virtualized.

Answer: D

Question No: 87

Which of the following offers the LEAST amount of protection against data theft by USB drives?

A. DLP

B. Database encryption

C. TPM

D. Cloud computing

Answer: D

Question No: 88
A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model?

A. Software as a Service

B. DMZ

C. Remote access support

D. Infrastructure as a Service

Answer: A

Question No: 89
The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

A. Software as a Service

B. Infrastructure as a Service

C. Platform as a Service

D. Hosted virtualization service

Answer: A

Question No: 90
An IT director is looking to reduce the footprint of their company’s server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

A. Infrastructure as a Service

B. Storage as a Service

C. Platform as a Service

D. Software as a Service

Answer: A

Question No: 91
Which of the following offerings typically allows the customer to apply operating system patches?

A. Software as a service

B. Public Clouds

C. Cloud Based Storage

D. Infrastructure as a service

Answer: D

Question No: 92
Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention

B. Trusted platform module

C. Hard drive encryption

D. Cloud computing

Answer: D

Question No: 93
Multi-tenancy is a concept found in which of the following?

A. Ful disk encryption

B. Removable media

C. Cloud computing

D. Data loss prevention

Answer: C

Question No: 94
Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

A. Protocol filter

B. Load balancer

C. NIDS

D. Layer 7 firewall

Answer: D

Question No: 95
Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

A. Redundant systems.

B. Separation of duties.

C. Layered security.

D. Application control.

Answer: C

Question No: 96
A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

A. IPsec

B. SFTP

C. BGP

D. PPTP

Answer: A

Question No: 97
Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec

B. Ful disk encryption

C. 802.1x

D. PKI

Answer: A

Question No: 98
A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

A. IPv6

B. SFTP

C. IPSec

D. SSH

E. IPv4

Answer: A,C

Question No: 99
A network administrator needs to provide daily network usage reports on al layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

A. SNMP

B. SNMPv3

C. ICMP

D. SSH

Answer: B

Question No: 100
Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

A. SMTP

B. SNMPv3

C. IPSec

D. SNMP

Answer: B

Question No: 101
A recent vulnerability scan found that Telnet is enabled on all network devices. Which of the following protocols should be used instead of Telnet?

A. SCP

B. SSH

C. SFTP

D. SSL

Answer: B

Question No: 102
Which of the following is BEST used as a secure replacement for TELNET?

A. HTTPS

B. HMAC

C. GPG

D. SSH

Answer: D

Question No: 103
A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

A. SCP

B. SSH

C. SFTP

D. HTTPS

Answer: B

Question No: 104
A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).

A. RDP

B. SNMP

C. FTP

D. SCP

E. SSH

Answer: D,E

Question No: 105

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server

B. Apache server

C. Exchange server

D. RADIUS server

Answer: A

Question No: 106

When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

A. DNSSEC record

B. IPv4 DNS record

C. IPSEC DNS record

D. IPv6 DNS record

Answer: D

Question No: 107
Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on

B. IPv6

C. Secure zone transfers

D. VoIP

Answer: C

Question No: 108
A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

A. HTTPS

B. SSH

C. FTP

D. TLS

Answer: D

Question No: 109
Which of the following protocols is used to authenticate the client and server’s digital certificate?

A. PEAP

B. DNS

C. TLS

D. ICMP

Answer: C

Question No: 110
An administrator configures all wireless access points to make use of a new network certificate authority. Which of the following is being used?

A. WEP

B. LEAP

C. EAP-TLS

D. TKIP

Answer: C

Question No: 111
An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

A. TCP/IP

B. SSL

C. SCP

D. SSH

Answer: B

Question No: 112
Which of the following is the MOST secure protocol to transfer files?

A. FTP

B. FTPS

C. SSH

D. TELNET

Answer: B

Question No: 113
FTP/S uses which of the following TCP ports by default?

A. 20 and 21

B. 139 and 445

C. 443 and 22

D. 989 and 990

Answer: D

Question No: 114
Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP

B. SNMP

C. SFTP

D. SCP

E. TFTP

Answer: C,D

Question No: 115
After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely.
Which of the following is the MOST likely reason the PC technician is unable to ping those devices?

A. ICMP is being blocked

B. SSH is not enabled

C. DNS settings are wrong

D. SNMP is not configured properly

Answer: A

Question No: 116
A security administrator wishes to change their wireless network so that IPSec is built into the protocol and NAT is no longer required for address range extension. Which of the following protocols should be used in this scenario?

A. WPA2

B. WPA

C. IPv6

D. IPv4

Answer: C

Question No: 117
A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68. Which of the following replies has the administrator received?

A. The loopback address

B. The local MAC address

C. IPv4 address

D. IPv6 address

Answer: D

Question No: 118
Which of the following protocols is used by IPv6 for MAC address resolution?

A. NDP

B. ARP

C. DNS

D. NCP

Answer: A

Question No: 119
Which of the following protocols allows for the LARGEST address space?

A. IPX

B. IPv4

C. IPv6

D. Appletalk

Answer: C

Question No: 120
Pete, a network administrator, is implementing IPv6 in the DMZ. Which of the following protocols must he allow through the firewall to ensure the web servers can be reached via IPv6 from an IPv6 enabled Internet host?

A. TCP port 443 and IP protocol 46

B. TCP port 80 and TCP port 443

C. TCP port 80 and ICMP

D. TCP port 443 and SNMP

Answer: B

Question No: 121
Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP

B. 21/TCP

C. 22/UDP

D. 22/TCP

Answer: D

Question No: 122
A network administrator is asked to send a large file containing PII to a business associate.
Which of the following protocols is the BEST choice to use?

A. SSH

B. SFTP

C. SMTP

D. FTP

Answer: B

Question No: 123
Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.

B. TFTP is more secure than FTP.

C. TFTP utilizes TCP and FTP uses UDP.

D. TFTP utilizes UDP and FTP uses TCP.

Answer: D

Question No: 124
Which of the following is the default port for TFTP?

A. 20

B. 69

C. 21

D. 68

Answer: B

Question No: 125
A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site

B. Block port 23 on the network firewall

C. Block port 25 on the L2 switch at each remote site

D. Block port 25 on the network firewall

Answer: B

Question No: 126
A security analyst noticed a colleague typing the following command:
`Telnet some-host 443'
Which of the following was the colleague performing?

A. A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.

B. A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.

C. Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.

D. A mistaken port being entered because telnet servers typically do not listen on port 443.

Answer: B

Question No: 127

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP

B. BGP

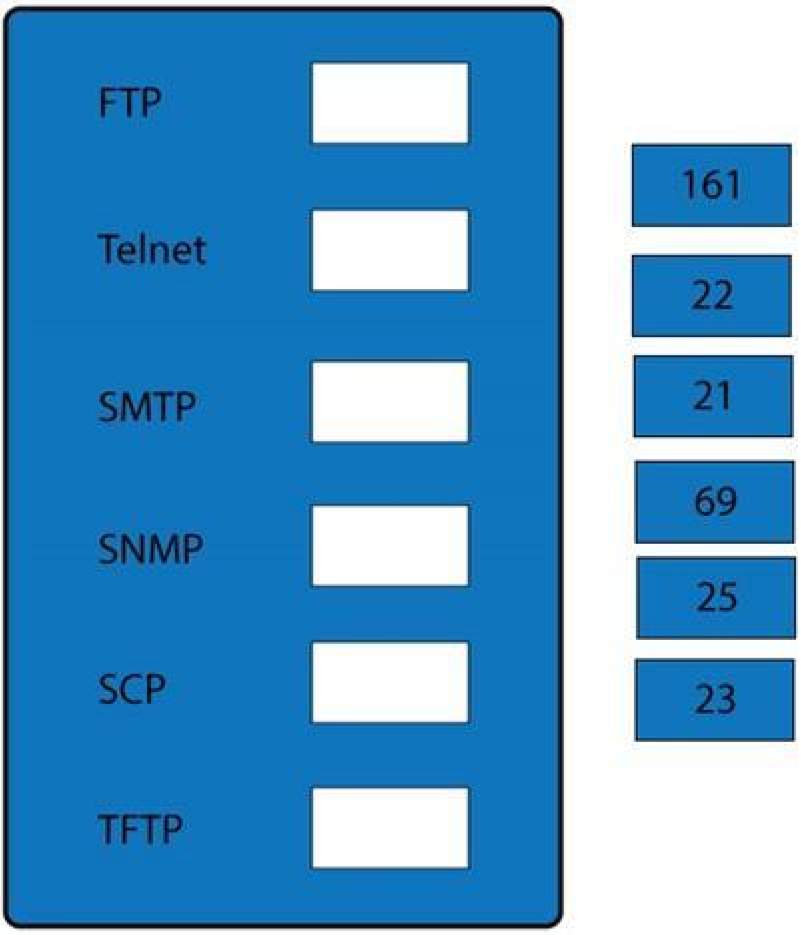
C. NetBIOS

D. DNS

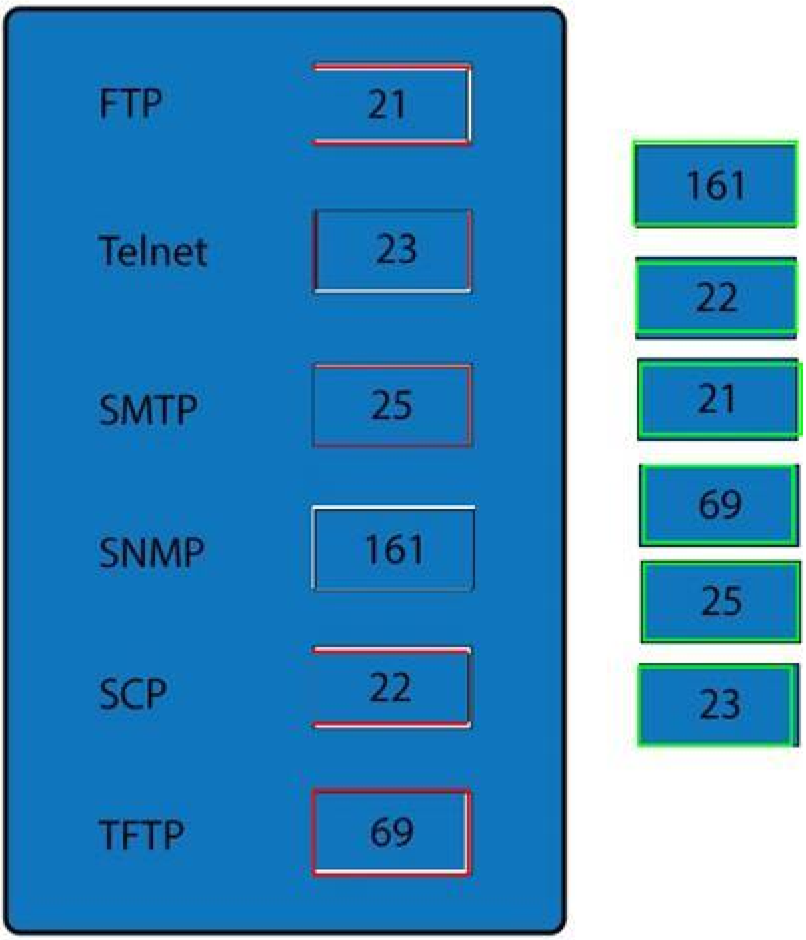
Answer: C

Question No: 128 DRAG DROP

Drag and drop the correct protocol to its default port.



Answer:



FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

161

22

21

69

25

23

Question No: 129

An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

A. RADIUS

B. Kerberos

C. TACACS+

D. LDAP

Answer: D

Question No: 130

A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP

B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS

C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS

D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Answer: B

Question No: 131

A company has implemented PPTP as a VPN solution. Which of the following ports would need to be opened on the firewall in order for this VPN to function properly? (Select TWO).

A. UDP 1723

B. TCP 500

C. TCP 1723

D. UDP 47

E. TCP 47

Answer: C,D

Question No: 132

After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25

B. 68

C. 80

D. 443

Answer: B

Question No: 133
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20

B. 21

C. 22

D. 23

Answer: B

Question No: 134
Which of the following ports is used for SSH, by default?

A. 23

B. 32

C. 12

D. 22

Answer: D

Question No: 135
By default, which of the following uses TCP port 22? (Select THREE).

A. FTPS

B. STELNET

C. TLS

D. SCP

E. SSL

F. HTTPS

G. SSH

H. SFTP

Answer: D,G,H

Question No: 136
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

A. TCP 23

B. UDP 69

C. TCP 22

D. TCP 21

Answer: C

Question No: 137
Which of the following uses port 22 by default? (Select THREE).

A. SSH

B. SSL

C. TLS

D. SFTP

E. SCP

F. FTPS

G. SMTP

H. SNMP

Answer: A,D,E

Question No: 138

Which of the following ports should be used by a system administrator to securely manage a remote server?

A. 22

B. 69

C. 137

D. 445

Answer: A

Question No: 139

Which of the following ports is used to securely transfer files between remote UNIX systems?

A. 21

B. 22

C. 69

D. 445

Answer: B

Question No: 140

Which of the following secure file transfer methods uses port 22 by default?

A. FTPS

B. SFTP

C. SSL

D. S/MIME

Answer: B

Question No: 141
During the analysis of a PCAP file, a security analyst noticed several communications with a remote server on port 53. Which of the following protocol types is observed in this traffic?

A. FTP

B. DNS

C. Email

D. NetBIOS

Answer: B

Question No: 142
A security technician needs to open ports on a firewall to allow for domain name resolution.
Which of the following ports should be opened? (Select TWO).

A. TCP 21

B. TCP 23

C. TCP 53

D. UDP 23

E. UDP 53

Answer: C,E

Question No: 143
A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

A. HTTP

B. DHCP

C. DNS

D. NetBIOS

Answer: C

Question No: 144
Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

A. 21

B. 25

C. 80

D. 3389

Answer: C

Question No: 145
A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22

B. 135

C. 137

D. 143

E. 443

F. 3389

Answer: A,F

Question No: 146
Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

A. 22

B. 139

C. 443

D. 3389

Answer: D

Question No: 147
Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP

B. IPSec

C. SCP

D. TCP

Answer: C

Question No: 148
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA

B. Disable SSID

C. Adjust antenna placement

D. Implement WEP

Answer: A

Question No: 149
A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

A. IV attack

B. WEP cracking

C. WPA cracking

D. Rogue AP

Answer: C

Question No: 150
Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Instal a token on the authentication server

B. Instal a DHCP server on the authentication server

C. Install an encryption key on the authentication server

D. Install a digital certificate on the authentication server

Answer: D

Question No: 151
A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their accounts. Additionally the system must support 3DS wireless encryption.
Which of the following should be implemented?

A. WPA2-CCMP with 802.1X

B. WPA2-PSK

C. WPA2-CCMP

D. WPA2-Enterprise

Answer: D

Question No: 152
Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

A. WPA2-Enterprise wireless network

B. DNS secondary zones

C. Digital certificates

D. Intrusion detection system

Answer: A

Question No: 153
A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.
Which of the following should the administrator implement?

A. WPA2 over EAP-TTLS

B. WPA-PSK

C. WPA2 with WPS

D. WEP over EAP-PEAP

Answer: D

Question No: 154
Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm.
Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.

B. The WEP key is stored in plain text and split in portions across 224 packets of random data.

Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.

C. The WEP key has a weak MD4 hashing algorithm used.
A simple rainbow table can be used to generate key possibilities due to MD4 collisions.

D. The WEP key is stored with a very small pool of random numbers to make the cipher text.
As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Answer: D

Question No: 155
Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5

B. WEP

C. PEAP-MSCHAPv2

D. EAP-TLS

Answer: C

Question No: 156
Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

A. EAP-TLS

B. EAP-FAST

C. PEAP-CHAP

D. PEAP-MSCHAPv2

Answer: D

Question No: 157
Which of the following means of wireless authentication is easily vulnerable to spoofing?

A. MAC Filtering

B. WPA - LEAP

C. WPA - PEAP

D. Enabled SSID

Answer: A

Question No: 158
Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect.
Which of the following is MOST likely the reason?

A. The company wireless is using a MAC filter.

B. The company wireless has SSID broadcast disabled.

C. The company wireless is using WEP.

D. The company wireless is using WPA2.

Answer: A

Question No: 159
After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:
PERMIT 0A: D1: FA. B1: 03: 37
DENY 01: 33: 7F: AB: 10: AB
Which of the following is preventing the device from connecting?

A. WPA2-PSK requires a supplicant on the mobile device.

B. Hardware address filtering is blocking the device.

C. TCP/IP Port filtering has been implemented on the SOHO router.

D. IP address filtering has disabled the device from connecting.

Answer: B

Question No: 160
A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up.
Which of the following BEST allows the analyst to restrict user access to approved devices?

A. Antenna placement

B. Power level adjustment

C. Disable SSID broadcasting

D. MAC filtering

Answer: D

Question No: 161
ON NO: 161
If you don’t know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it?

A. macconfig

B. ifconfig

C. ipconfig

D. config

Answer: B

Question No: 162
An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points?

A. SSID broadcast

B. MAC filter

C. WPA2

D. Antenna placement

Answer: A

Question No: 163
A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform al employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

A. Disabling SSID broadcasting

B. Implementing WPA2 - TKIP

C. Implementing WPA2 - CCMP

D. Filtering test workstations by MAC address

Answer: A

Question No: 164
While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

A. no longer used to authenticate to most wireless networks.

B. contained in certain wireless packets in plaintext.

C. contained in all wireless broadcast packets by default.

D. no longer supported in 802.11 protocols.

Answer: B

Question No: 165
A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

A. The SSID broadcast is disabled.

B. The company is using the wrong antenna type.

C. The MAC filtering is disabled on the access point.

D. The company is not using strong enough encryption.

Answer: A

Question No: 166
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering

B. UseWPA2-PSK

C. Disable SSID broadcast

D. Power down unused WAPs

Answer: C

Question No: 167
Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports

B. Use channels 1, 4 and 7 only

C. Enable MAC filtering

D. Disable SSID broadcast

E. Switch from 802.11a to 802.11b

Answer: C,D

Question No: 168
Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP

B. Mac filtering

C. WPA2

D. WPA

Answer: A

Question No: 169
A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

A. WPA2 CCMP

B. WPA

C. WPA with MAC filtering

D. WPA2 TKIP

Answer: A

Question No: 170
An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue?

A. WEP

B. CCMP

C. TKIP

D. RC4

Answer: B

Question No: 171
A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.

B. Set all nearby access points to operate on the same channel.

C. Configure the access point to use WEP instead of WPA2.

D. Enable al access points to broadcast their SSIDs.

Answer: A

Question No: 172
The security administrator has been tasked to update al the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

A. WEP

B. WPA2 CCMP

C. Disable SSID broadcast and increase power levels

D. MAC filtering

Answer: B

Question No: 173
A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

A. RC4

B. DES

C. 3DES

D. AES

Answer: D

Question No: 174
Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

A. Placement of antenna

B. Disabling the SSID

C. Implementing WPA2

D. Enabling the MAC filtering

Answer: A

Question No: 175
A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement

B. Interference

C. Use WEP

D. Single Sign on

E. Disable the SSID

F. Power levels

Answer: A,F

Question No: 176

Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

A. Implement TKIP encryption

B. Consider antenna placement

C. Disable the SSID broadcast

D. Disable WPA

Answer: B

Question No: 177
Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.
Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

A. Enable MAC filtering on the wireless access point.

B. Configure WPA2 encryption on the wireless access point.

C. Lower the antenna's broadcasting power.

D. Disable SSID broadcasting.

Answer: C

Question No: 178
After reviewing the firewall logs of her organization's wireless APs, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue?

A. Reduce the power level of the AP on the network segment

B. Implement MAC filtering on the AP of the affected segment

C. Perform a site survey to see what has changed on the segment

D. Change the WPA2 encryption key of the AP in the affected segment

Answer: A

Question No: 179

An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation?

A. Dipole

B. Yagi

C. Sector

D. Omni

Answer: B

Question No: 180

A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

A. The old APs use 802.11a

B. Users did not enter the MAC of the new APs

C. The new APs use MIMO

D. A site survey was not conducted

Answer: D

Question No: 181

Three of the primary security control types that can be implemented are.

A. Supervisory, subordinate, and peer.

B. Personal, procedural, and legal.

C. Operational, technical, and management.

D. Mandatory, discretionary, and permanent.

Answer: C

Question No: 182
Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

A. Authentication

B. Blacklisting

C. Whitelisting

D. Acceptable use policy

Answer: C

Question No: 183
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management

B. Administrative

C. Technical

D. Operational

Answer: C

Question No: 184
Which of the following is a management control?

A. Logon banners

B. Written security policy

C. SYN attack prevention

D. Access Control List (ACL)

Answer: B

Question No: 185
Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation

B. Acceptable usage policies

C. False positives

D. Mandatory vacations

Answer: C

Question No: 186
A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system.
Which of the following describes this cause?

A. Application hardening

B. False positive

C. Baseline code review

D. False negative

Answer: B

Question No: 187
Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives

B. True positives

C. False positives

D. False negatives

Answer: C

Question No: 188
Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow.

B. Anti-virus identifies a benign application as malware.

C. Anti-virus protection interferes with the normal operation of an application.

D. A user account is locked out after the user mistypes the password too many times.

Answer: A

Question No: 189
A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

A. Command shell restrictions

B. Restricted interface

C. Warning banners

D. Session output pipe to /dev/null

Answer: C

Question No: 190
Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

A. Acceptable use policy

B. Risk acceptance policy

C. Privacy policy

D. Email policy

E. Security policy

Answer: A,C

Question No: 191
Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

A. Acceptable Use Policy

B. Privacy Policy

C. Security Policy

D. Human Resource Policy

Answer: A

Question No: 192
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.

B. Tel the application development manager to code the application to adhere to the company's password policy.

C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.

D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Answer: B

Question No: 193
A major security risk with co-mingling of hosts with different security requirements is:

A. Security policy violations.

B. Zombie attacks.

C. Password compromises.

D. Privilege creep.

Answer: A

Question No: 194
Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

A. To ensure that false positives are identified

B. To ensure that staff conform to the policy

C. To reduce the organizational risk

D. To require acceptable usage of IT systems

Answer: C

Question No: 195
Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

A. Privacy Policy

B. Least Privilege

C. Acceptable Use

D. Mandatory Vacations

Answer: D

Question No: 196

Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

A. Least privilege access

B. Separation of duties

C. Mandatory access control

D. Mandatory vacations

Answer: D

Question No: 197

Mandatory vacations are a security control which can be used to uncover which of the following?

A. Fraud committed by a system administrator

B. Poor password security among users

C. The need for additional security staff

D. Software vulnerabilities in vendor code

Answer: A

Question No: 198

While rarely enforced, mandatory vacation policies are effective at uncovering:

A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.

B. Collusion between two employees who perform the same business function.

C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.

D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

Answer: D

Question No: 199
A company that has a mandatory vacation policy has implemented which of the following controls?

A. Risk control

B. Privacy control

C. Technical control

D. Physical control

Answer: A

Question No: 200
Which of the following should Joe, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from his company?

A. Privacy Policy

B. Least Privilege

C. Acceptable Use

D. Mandatory Vacations

Answer: D

Question No: 201
A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

A. Implement privacy policies

B. Enforce mandatory vacations

C. Implement a security policy

D. Enforce time of day restrictions

Answer: B

Question No: 202
The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

A. Create a single, shared user account for every system that is audited and logged based upon time of use.

B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.

C. Enact a policy that employees must use their vacation time in a staggered schedule.

D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Answer: C

Question No: 203
A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.
Which of the following practices is being implemented?

A. Mandatory vacations

B. Job rotation

C. Least privilege

D. Separation of duties

Answer: B

Question No: 204
Which of the following types of risk reducing policies also has the added indirect benefit of cross training employees when implemented?

A. Least privilege

B. Job rotation

C. Mandatory vacations

D. Separation of duties

Answer: B

Question No: 205
In order to prevent and detect fraud, which of the following should be implemented?

A. Job rotation

B. Risk analysis

C. Incident management

D. Employee evaluations

Answer: A

Question No: 206
The Chief Technical Officer (CTO) has been informed of a potential fraud committed by a database administrator performing several other job functions within the company. Which of the following is the BEST method to prevent such activities in the future?

A. Job rotation

B. Separation of duties

C. Mandatory Vacations

D. Least Privilege

Answer: B

Question No: 207
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

A. More experienced employees from less experienced employees

B. Changes to program code and the ability to deploy to production

C. Upper level management users from standard development employees

D. The network access layer from the application access layer

Answer: B

Question No: 208
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

A. Account lockout policy

B. Account password enforcement

C. Password complexity enabled

D. Separation of duties

Answer: D

Question No: 209
Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

A. Separation of Duties

B. Mandatory Vacations

C. Discretionary Access Control

D. Job Rotation

Answer: A

Question No: 210
One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

A. Mandatory access

B. Rule-based access control

C. Least privilege

D. Job rotation

Answer: C

Question No: 211
A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

A. Mandatory vacations

B. Job rotation

C. Least privilege

D. Time of day restrictions

Answer: C

Question No: 212
Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

A. User rights reviews

B. Incident management

C. Risk based controls

D. Annual loss expectancy

Answer: A

Question No: 213

An IT security manager is asked to provide the total risk to the business. Which of the following calculations would he security manager choose to determine total risk?

A. (Threats X vulnerability X asset value) x controls gap

B. (Threats X vulnerability X profit) x asset value

C. Threats X vulnerability X control gap

D. Threats X vulnerability X asset value

Answer: D

Question No: 214

A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO).

A. Disk hashing procedures

B. Ful disk encryption

C. Data retention policies

D. Disk wiping procedures

E. Removable media encryption

Answer: B,D

Question No: 215

Identifying residual risk is MOST important to which of the following concepts?

A. Risk deterrence

B. Risk acceptance

C. Risk mitigation

D. Risk avoidance

Answer: B

Question No: 216
A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

A. Fault tolerance

B. Encryption

C. Availability

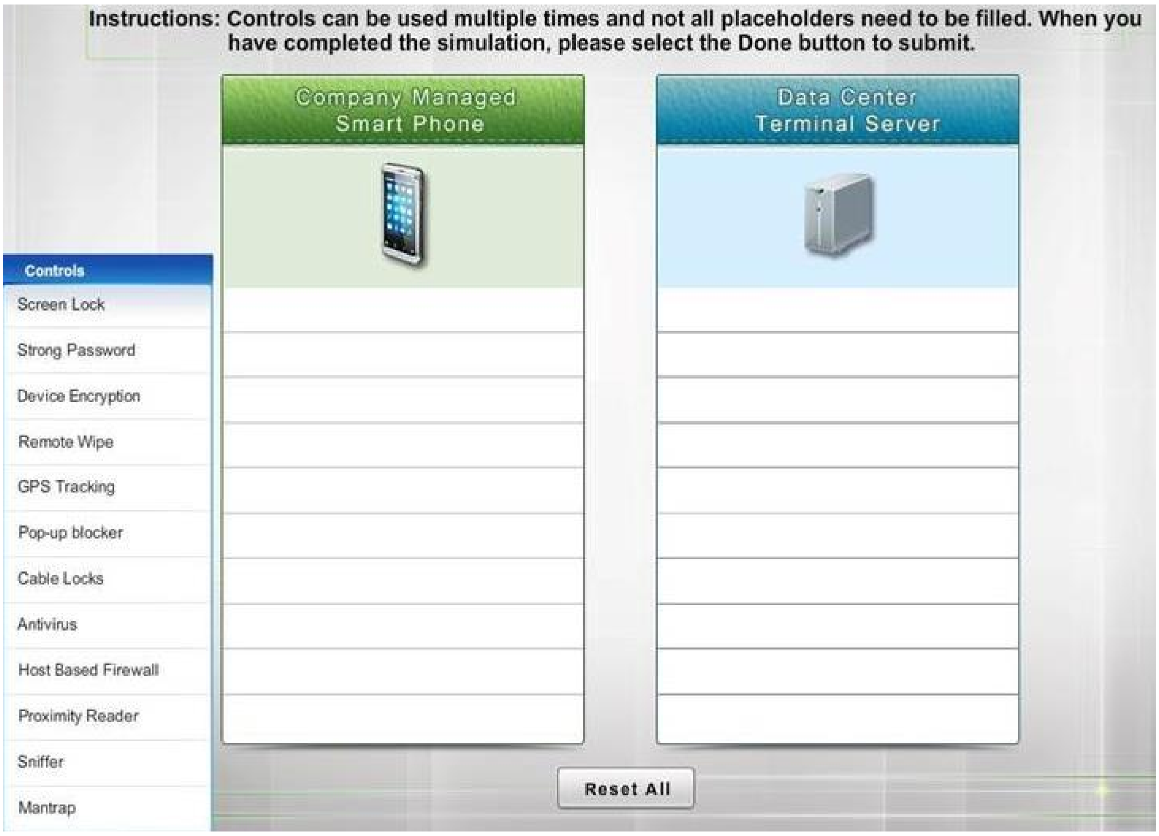
D. Integrity

E. Safety

F. Confidentiality

Answer: D,E

Question No: 217 DRAG DROP
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset type.
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.



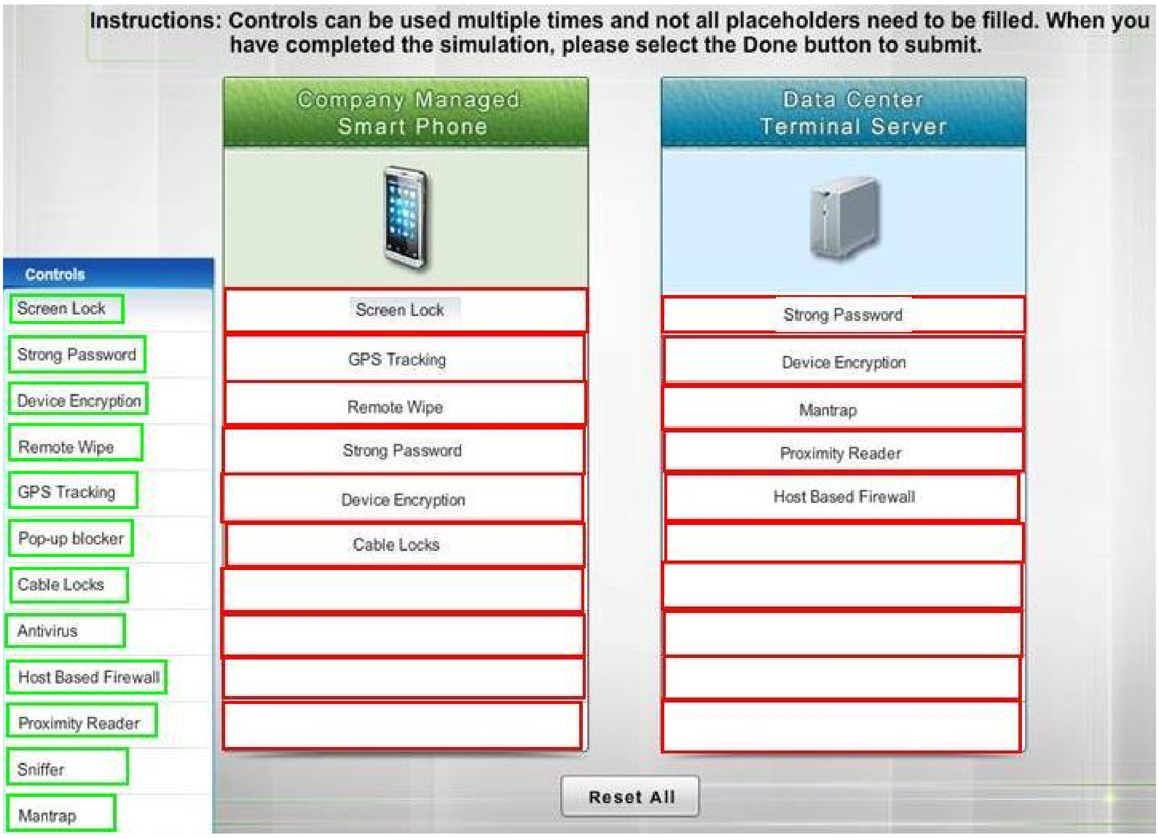
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Controls

- Screen Lock
- Strong Password
- Device Encryption
- Remote Wipe
- GPS Tracking
- Pop-up blocker
- Cable Locks
- Antivirus
- Host Based Firewall
- Proximity Reader
- Sniffer
- Mantrap

Company Managed Smart Phone	Data Center Terminal Server

Answer:



Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Controls

- Screen Lock
- Strong Password
- Device Encryption
- Remote Wipe
- GPS Tracking
- Pop-up blocker
- Cable Locks
- Antivirus
- Host Based Firewall
- Proximity Reader
- Sniffer
- Mantrap

Company Managed Smart Phone	Data Center Terminal Server
Screen Lock	Strong Password
GPS Tracking	Device Encryption
Remote Wipe	Mantrap
Strong Password	Proximity Reader
Device Encryption	Host Based Firewall
Cable Locks	

Question No: 218
Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR

B. MTBF

C. RPO

D. Warm site

Answer: C

Question No: 219
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years.
Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.
Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.

B. Ignore the risk saving $5,000.

C. Mitigate the risk saving $10,000.

D. Transfer the risk saving $5,000.

Answer: D

Question No: 220
Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

A. Confidentiality

B. Availability

C. Integrity

D. Authorization

E. Authentication

F. Continuity

Answer: A,B,C

Question No: 221
Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity

B. Data confidentiality

C. Availability of servers

D. Integrity of data

Answer: B

Question No: 222
The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

A. Cloud computing

B. Ful disk encryption

C. Data Loss Prevention

D. HSM

Answer: A

Question No: 223
Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

A. Malicious users can exploit local corporate credentials with their social media credentials

B. Changes to passwords on the social media site can be delayed from replicating to the company

C. Data loss from the corporate servers can create legal liabilities with the social media site

D. Password breaches to the social media site affect the company application as well

Answer: D

Question No: 224
Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

A. Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.

B. MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.

C. MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.

D. MOUs between two companies working together cannot be held to the same legal standards as SLAs.

Answer: C

Question No: 225
Which of the following describes the purpose of an MOU?

A. Define interoperability requirements

B. Define data backup process

C. Define onboard/offboard procedure

D. Define responsibilities of each party

Answer: D

Question No: 226

A company has decided to move large data sets to a cloud provider in order to limit the costs of new infrastructure. Some of the data is sensitive and the Chief Information Officer wants to make sure both parties have a clear understanding of the controls needed to protect the data.

Which of the following types of interoperability agreement is this?

A. ISA

B. MOU

C. SLA

D. BPA

Answer: A

Question No: 227

Which of the following is the primary security concern when deploying a mobile device on a network?

A. Strong authentication

B. Interoperability

C. Data security

D. Cloud storage technique

Answer: C

Question No: 228

A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of $2,000. Patching the application today would cost $140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

A. Avoid the risk to the user base allowing them to re-enable their own accounts

B. Mitigate the risk by patching the application to increase security and saving money

C. Transfer the risk replacing the application now instead of in five years

D. Accept the risk and continue to enable the accounts each month saving money

Answer: D

Question No: 229

Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party?

A. The data should be encrypted prior to transport

B. This would not constitute unauthorized data sharing

C. This may violate data ownership and non-disclosure agreements

D. Acme Corp should send the data to ABC Services' vendor instead

Answer: C

Question No: 230

An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.
Which of the following strategies would the administrator MOST likely implement?

A. Ful backups on the weekend and incremental during the week

B. Ful backups on the weekend and ful backups every day

C. Incremental backups on the weekend and differential backups every day

D. Differential backups on the weekend and full backups every day

Answer: A

Question No: 231

A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

A. The request needs to be sent to the incident management team.

B. The request needs to be approved through the incident management process.

C. The request needs to be approved through the change management process.

D. The request needs to be sent to the change management team.

Answer: C

Question No: 232
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

A. Incident management

B. Clean desk policy

C. Routine audits

D. Change management

Answer: D

Question No: 233
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management

B. Server clustering

C. Change management

D. Forensic analysis

Answer: C

Question No: 234
The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

A. Application hardening

B. Application firewall review

C. Application change management

D. Application patch management

Answer: C

Question No: 235

Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

A. Risk transference

B. Change management

C. Configuration management

D. Access control revalidation

Answer: B

Question No: 236

A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

A. Patch Audit Policy

B. Change Control Policy

C. Incident Management Policy

D. Regression Testing Policy

E. Escalation Policy

F. Application Audit Policy

Answer: B,D

Question No: 237
A user has received an email from an external source which asks for details on the company’s new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

A. Contact their manager and request guidance on how to best move forward

B. Contact the help desk and/or incident response team to determine next steps

C. Provide the requestor with the email information since it will be released soon anyway

D. Reply back to the requestor to gain their contact information and call them

Answer: B

Question No: 238
Which of the following is BEST carried out immediately after a security breach is discovered?

A. Risk transference

B. Access control revalidation

C. Change management

D. Incident management

Answer: D

Question No: 239
A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

A. Procedure and policy management

B. Chain of custody management

C. Change management

D. Incident management

Answer: D

Question No: 240
Requiring technicians to report spyware infections is a step in which of the following?

A. Routine audits

B. Change management

C. Incident management

D. Clean desk policy

Answer: C

Question No: 241
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.

B. Perform routine user permission reviews.

C. Implement periodic vulnerability scanning.

D. Disable user accounts that have not been used within the last two weeks.

Answer: B

Question No: 242
An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

A. User rights reviews

B. Least privilege and job rotation

C. Change management

D. Change Control

Answer: A

Question No: 243
A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.

B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.

C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.

D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Answer: A

Question No: 244
Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

A. User rights and permissions review

B. Configuration management

C. Incident management

D. Implement security controls on Layer 3 devices

Answer: A

Question No: 245
After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

A. Mandatory access control enforcement.

B. User rights and permission reviews.

C. Technical controls over account management.

D. Account termination procedures.

E. Management controls over account management.

F. Incident management and response plan.

Answer: B,E

Question No: 246
The security administrator is currently unaware of an incident that occurred a week ago. Which of the following will ensure the administrator is notified in a timely manner in the future?

A. User permissions reviews

B. Incident response team

C. Change management

D. Routine auditing

Answer: D

Question No: 247
The system administrator has deployed updated security controls for the network to limit risk of attack.
The security manager is concerned that controls continue to function as intended to maintain appropriate security posture.
Which of the following risk mitigation strategies is MOST important to the security manager?

A. User permissions

B. Policy enforcement

C. Routine audits

D. Change management

Answer: C

Question No: 248
Which of the following security account management techniques should a security analyst implement to prevent staff, who has switched company roles, from exceeding privileges?

A. Internal account audits

B. Account disablement

C. Time of day restriction

D. Password complexity

Answer: A

Question No: 249
Encryption of data at rest is important for sensitive information because of which of the following?

A. Facilitates tier 2 support, by preventing users from changing the OS

B. Renders the recovery of data harder in the event of user password loss

C. Allows the remote removal of data following eDiscovery requests

D. Prevents data from being accessed following theft of physical equipment

Answer: D

Question No: 250
A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

A. Content filtering

B. IDS

C. Audit logs

D. DLP

Answer: D

Question No: 251
Several employees have been printing files that include personally identifiable information of customers. Auditors have raised concerns about the destruction of these hard copies after they are created, and management has decided the best way to address this concern is by preventing these files from being printed.
Which of the following would be the BEST control to implement?

A. File encryption

B. Printer hardening

C. Clean desk policies

D. Data loss prevention

Answer: D

Question No: 252
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies

B. Deterrent strategies

C. Containment strategies

D. Detection strategies

Answer: C

Question No: 253

Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

A. Matt should implement access control lists and turn on EFS.

B. Matt should implement DLP and encrypt the company database.

C. Matt should install Truecrypt and encrypt the company server.

D. Matt should install TPMs and encrypt the company database.

Answer: B

Question No: 254
An employee recently lost a USB drive containing confidential customer data. Which of the following controls could be utilized to minimize the risk involved with the use of USB drives?

A. DLP

B. Asset tracking

C. HSM

D. Access control

Answer: A

Question No: 255
Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

A. DLP

B. CRL

C. TPM

D. HSM

Answer: A

Question No: 256
Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.

B. Scanning of outbound IM (Instance Messaging).

C. Scanning copying of documents to USB.

D. Scanning of SharePoint document library.

E. Scanning of shared drives.

F. Scanning of HTTP user traffic.

Answer: B,F

Question No: 257
Which of the following assets is MOST likely considered for DLP?

A. Application server content

B. USB mass storage devices

C. Reverse proxy

D. Print server

Answer: B

Question No: 258
The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A. HPM technology

B. Ful disk encryption

C. DLP policy

D. TPM technology

Answer: C

Question No: 259
Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

A. Email scanning

B. Content discovery

C. Database fingerprinting

D. Endpoint protection

Answer: D

Question No: 260
A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

A. Automatically encrypt impacted outgoing emails

B. Automatically encrypt impacted incoming emails

C. Monitor impacted outgoing emails

D. Prevent impacted outgoing emails

Answer: A

Question No: 261
Which of the following is a best practice when a mistake is made during a forensics examination?

A. The examiner should verify the tools before, during, and after an examination.

B. The examiner should attempt to hide the mistake during cross-examination.

C. The examiner should document the mistake and workaround the problem.

D. The examiner should disclose the mistake and assess another area of the disc.

Answer: C

Question No: 262

An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

A. Using a software file recovery disc

B. Mounting the drive in read-only mode

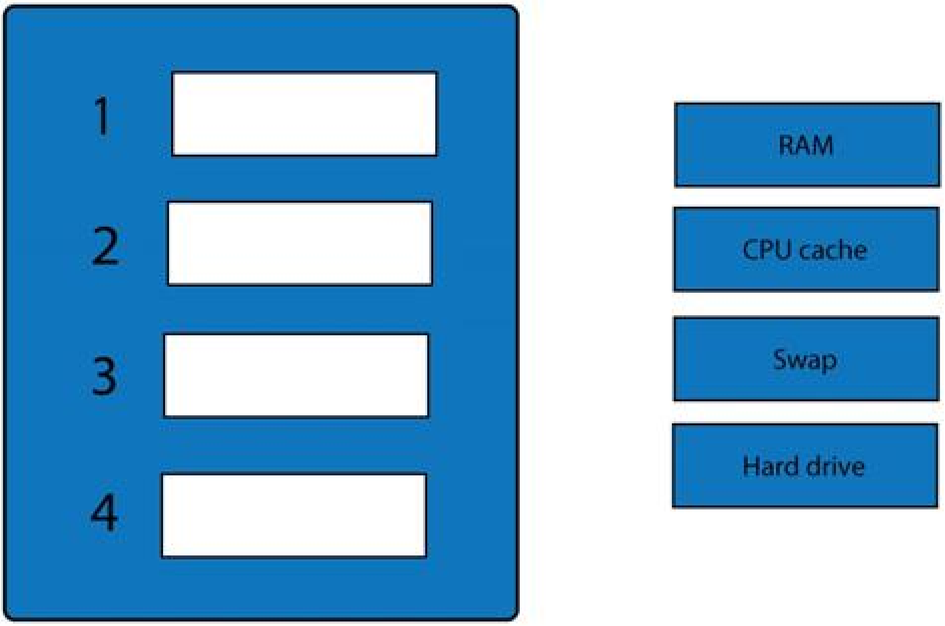
C. Imaging based on order of volatility

D. Hashing the image after capture

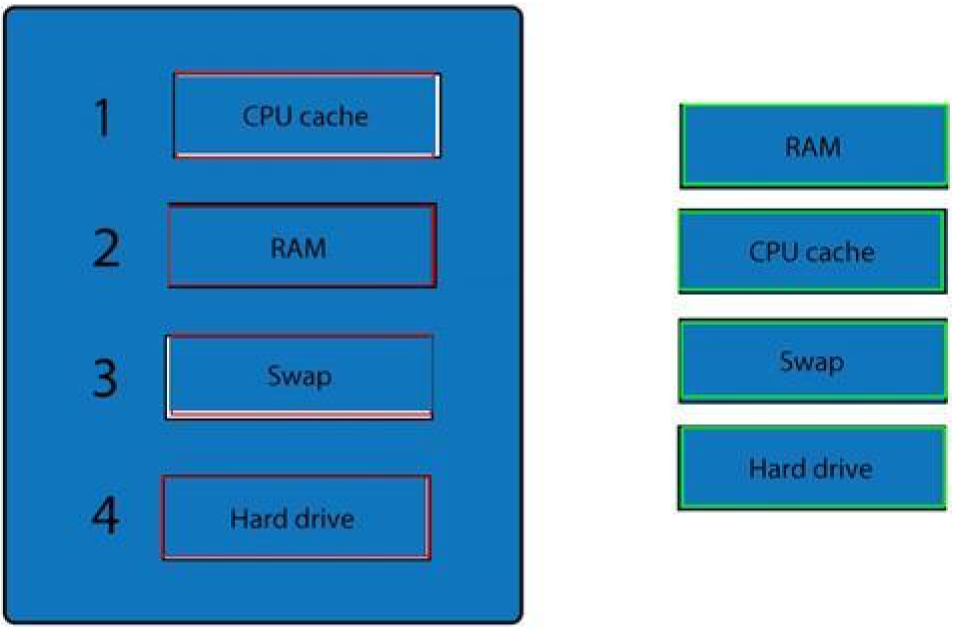
Answer: B

Question No: 263 DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.



Answer:



Question No: 264
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits

B. Disconnect system from network

C. Capture system image

D. Interview witnesses

Answer: C

Question No: 265
Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate?

A. Taking screenshots

B. System image capture

C. Chain of custody

D. Order of volatility

Answer: B

Question No: 266
To ensure proper evidence collection, which of the following steps should be performed FIRST?

A. Take hashes from the live system

B. Review logs

C. Capture the system image

D. Copy all compromised files

Answer: C

Question No: 267
A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

A. cp /dev/sda /dev/sdb bs=8k

B. tail -f /dev/sda > /dev/sdb bs=8k

C. dd in=/dev/sda out=/dev/sdb bs=4k

D. locate /dev/sda /dev/sdb bs=4k

Answer: C

Question No: 268
A security technician wishes to gather and analyze all Web traffic during a particular time period.
Which of the following represents the BEST approach to gathering the required data?

A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.

B. Configure a proxy server to log all traffic destined for ports 80 and 443.

C. Configure a switch to log all traffic destined for ports 80 and 443.

D. Configure a NIDS to log al traffic destined for ports 80 and 443.

Answer: B

Question No: 269
A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

A. Detective

B. Deterrent

C. Corrective

D. Preventive

Answer: C

Question No: 270
Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

A. Place a full-time guard at the entrance to confirm user identity.

B. Instal a camera and DVR at the entrance to monitor access.

C. Revoke al proximity badge access to make users justify access.

D. Install a motion detector near the entrance.

Answer: B

Question No: 271
The incident response team has received the following email message.
From: monitor@ext-company.com To: security@company.com Subject: Copyright infringement
A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT.
After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident.
09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john

```
09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne
10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov
11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok
```

Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident?

A. The logs are corrupt and no longer forensically sound.

B. Traffic logs for the incident are unavailable.

C. Chain of custody was not properly maintained.

D. Incident time offsets were not accounted for.

Answer: D

Question No: 272
A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of al servers to ensure that:

A. HDD hashes are accurate.

B. the NTP server works properly.

C. chain of custody is preserved.

D. time offset can be calculated.

Answer: D

Question No: 273
A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

A. Chain of custody

B. Tracking man hours

C. Record time offset

D. Capture video traffic

Answer: C

Question No: 274
Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.
Which of the following does this illustrate?

A. System image capture

B. Record time offset

C. Order of volatility

D. Chain of custody

Answer: D

Question No: 275
A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident?

A. Eye Witness

B. Data Analysis of the hard drive

C. Chain of custody

D. Expert Witness

Answer: C

Question No: 276
The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division

confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

A. Chain of custody

B. System image

C. Take hashes

D. Order of volatility

Answer: A

Question No: 277
Which of the following is the MOST important step for preserving evidence during forensic procedures?

A. Involve law enforcement

B. Chain of custody

C. Record the time of the incident

D. Report within one hour of discovery

Answer: B

Question No: 278
During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

A. Lessons Learned

B. Preparation

C. Eradication

D. Identification

Answer: B

Question No: 279

The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

A. Lessons Learned

B. Eradication

C. Recovery

D. Preparation

Answer: D

Question No: 280
The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

A. Recovery

B. Follow-up

C. Validation

D. Identification

E. Eradication

F. Containment

Answer: D

Question No: 281
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team

B. Internal auditors

C. Incident response team

D. Software vendors

Answer: C

Question No: 282
In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

A. Mitigation

B. Identification

C. Preparation

D. Lessons learned

Answer: D

Question No: 283
After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies?

A. Change management

B. Implementing policies to prevent data loss

C. User rights and permissions review

D. Lessons learned

Answer: D

Question No: 284
A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was extracted. Which of the following incident response procedures is best suited to restore the server?

A. Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup.

B. Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan.

C. Format the storage and reinstall both the OS and the data from the most current backup.

D. Erase the storage, reinstal the OS from most current backup and only restore the data that was not compromised.

Answer: A

Question No: 285
In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

A. Take hashes

B. Begin the chain of custody paperwork

C. Take screen shots

D. Capture the system image

E. Decompile suspicious files

Answer: A,D

Question No: 286
Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers

B. RAID cache

C. RAM

D. Hard drive

Answer: D

Question No: 287
The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

A. Business Impact Analysis

B. First Responder

C. Damage and Loss Control

D. Contingency Planning

Answer: B

Question No: 288
After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

A. Information Security Awareness

B. Social Media and BYOD

C. Data Handling and Disposal

D. Acceptable Use of IT Systems

Answer: A

Question No: 289
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

A. Acceptable Use Policy

B. Physical security controls

C. Technical controls

D. Security awareness training

Answer: D

Question No: 290

Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

A. Acceptable use of social media

B. Data handling and disposal

C. Zero day exploits and viruses

D. Phishing threats and attacks

E. Clean desk and BYOD

F. Information security awareness

Answer: D,F

Question No: 291

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

A. Security awareness training.

B. BYOD security training.

C. Role-based security training.

D. Legal compliance training.

Answer: A

Question No: 292

Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

A. Disable the wireless access and implement strict router ACLs.

B. Reduce restrictions on the corporate web security gateway.

C. Security policy and threat awareness training.

D. Perform user rights and permissions reviews.

Answer: C

Question No: 293
Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

A. To ensure proper use of social media

B. To reduce organizational IT risk

C. To detail business impact analyses

D. To train staff on zero-days

Answer: B

Question No: 294
Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

A. Digital Signatures

B. Hashing

C. Secret Key

D. Encryption

Answer: D

Question No: 295
Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks?

A. User Awareness

B. Acceptable Use Policy

C. Personal Identifiable Information

D. Information Sharing

Answer: C

Question No: 296
End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

A. Date of birth.

B. First and last name.

C. Phone number.

D. Employer name.

Answer: A

Question No: 297
Which of the following concepts is a term that directly relates to customer privacy considerations?

A. Data handling policies

B. Personally identifiable information

C. Information classification

D. Clean desk policies

Answer: B

Question No: 298
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling

B. Password policy

C. Chain of custody

D. Zero day exploits

Answer: A

Question No: 299
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status

B. Favorite movie

C. Pet's name

D. Birthday

E. Ful name

Answer: D,E

Question No: 300
Which of the following helps to apply the proper security controls to information?

A. Data classification

B. Deduplication

C. Clean desk policy

D. Encryption

Answer: A

Question No: 301
Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training

B. Personally owned device policy training

C. Tailgating awareness policy training

D. Information classification training

Answer: D

Question No: 302
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning

B. Quantitative assessment

C. Data classification

D. Qualitative assessment

Answer: C

Question No: 303
What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)?

A. Enticement

B. Entrapment

C. Deceit

D. Sting

Answer: A

Question No: 304
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks

B. Best practice

C. Access control methodologies

D. Compliance activity

Answer: B

Question No: 305
Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?

A. Enticement

B. Entrapment

C. Deceit

D. Sting

Answer: B

Question No: 306
Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password

B. line console 0 password password line vty 0 4 password P@s5W0Rd

C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd

D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd

Answer: C

Question No: 307
Why would a technician use a password cracker?

A. To look for weak passwords on the network

B. To change a user's passwords when they leave the company

C. To enforce password complexity requirements

D. To change users passwords if they have forgotten them

Answer: A

Question No: 308
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset

B. Clean desk policy

C. Cloud computing

D. Routine log review

Answer: B

Question No: 309
The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

A. Fire- or water-proof safe.

B. Department door locks.

C. Proximity card.

D. 24-hour security guard.

E. Locking cabinets and drawers.

Answer: A,E

Question No: 310

XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night.
The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

A. Social media policy

B. Data retention policy

C. CCTV policy

D. Clean desk policy

Answer: D

Question No: 311

Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.

B. Only allow employees to enter or leave through one door at specified times of the day.

C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.

D. Train employees on risks associated with social engineering attacks and enforce policies.

Answer: D

Question No: 312

Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network?

A. Cross-platform compatibility issues between personal devices and server-based applications

B. Lack of controls in place to ensure that the devices have the latest system patches and signature files

C. Non-corporate devices are more difficult to locate when a user is terminated

D. Non-purchased or leased equipment may cause failure during the audits of company-owned assets

Answer: B

Question No: 313
Several employees submit the same phishing email to the administrator. The administrator finds that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received?

A. Configure an ACL

B. Implement a URL filter

C. Add the domain to a block list

D. Enable TLS on the mail server

Answer: C

Question No: 314
A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature?

A. TCP/IP socket design review

B. Executable code review

C. OS Baseline comparison

D. Software architecture review

Answer: C

Question No: 315
A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

A. Peer to Peer

B. Mobile devices

C. Social networking

D. Personally owned devices

Answer: C

Question No: 316
The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

A. Rainbow tables attacks

B. Brute force attacks

C. Birthday attacks

D. Cognitive passwords attacks

Answer: D

Question No: 317
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

A. No competition with the company's official social presence

B. Protection against malware introduced by banner ads

C. Increased user productivity based upon fewer distractions

D. Elimination of risks caused by unauthorized P2P file sharing

Answer: B

Question No: 318
Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

A. Data integrity is susceptible to being compromised.

B. Monitoring data changes induces a higher cost.

C. Users are not responsible for data usage tracking.

D. Limiting the amount of necessary space for data storage.

Answer: A

Question No: 319
Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

A. Subnetting

B. NAT

C. Jabber

D. DMZ

Answer: C

Question No: 320
The use of social networking sites introduces the risk of:

A. Disclosure of proprietary information

B. Data classification issues

C. Data availability issues

D. Broken chain of custody

Answer: A

Question No: 321
Which of the following statements is MOST likely to be included in the security awareness training about P2P?

A. P2P is always used to download copyrighted material.

B. P2P can be used to improve computer system response.

C. P2P may prevent viruses from entering the network.

D. P2P may cause excessive network bandwidth.

Answer: D

Question No: 322
A security team has established a security awareness program. Which of the following would BEST prove the success of the program?

A. Policies

B. Procedures

C. Metrics

D. Standards

Answer: C

Question No: 323
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access

B. Dial-up access

C. Changing environmental controls

D. Ping of death

Answer: C

Question No: 324

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability

B. Integrity

C. Confidentiality

D. Fire suppression

Answer: A

Question No: 325

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system

B. Electrical

C. HVAC

D. Video surveillance

Answer: C

Question No: 326

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

A. Increased availability of network services due to higher throughput

B. Longer MTBF of hardware due to lower operating temperatures

C. Higher data integrity due to more efficient SSD cooling

D. Longer UPS run time due to increased airflow

Answer: B

Question No: 327
Which of the following fire suppression systems is MOST likely used in a datacenter?

A. FM-200

B. Dry-pipe

C. Wet-pipe

D. Vacuum

Answer: A

Question No: 328
When implementing fire suppression controls in a datacenter it is important to:

A. Select a fire suppression system which protects equipment but may harm technicians.

B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.

C. Integrate maintenance procedures to include regularly discharging the system.

D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

Answer: B

Question No: 329
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

A. CCTV

B. Environmental monitoring

C. Multimode fiber

D. EMI shielding

Answer: D

Question No: 330
Environmental control measures include which of the following?

A. Access list

B. Lighting

C. Motion detection

D. EMI shielding

Answer: D

Question No: 331
When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

A. Humidity sensors

B. EMI shielding

C. Channel interference

D. Cable kinking

Answer: B

Question No: 332
The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed?

A. Hot and cold aisles

B. Humidity control

C. HVAC system

D. EMI shielding

Answer: A

Question No: 333
Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

A. Fire suppression

B. Raised floor implementation

C. EMI shielding

D. Hot or cool aisle containment

Answer: D

Question No: 334
Which of the following results in datacenters with failed humidity controls? (Select TWO).

A. Excessive EMI

B. Electrostatic charge

C. Improper ventilation

D. Condensation

E. Irregular temperature

Answer: B,D

Question No: 335
The datacenter manager is reviewing a problem with a humidity factor that is too low. Which of the following environmental problems may occur?

A. EMI emanations

B. Static electricity

C. Condensation

D. Dry-pipe fire suppression

Answer: B

Question No: 336
A technician is investigating intermittent switch degradation. The issue only seems to occur when the building's roof air conditioning system runs. Which of the following would reduce the connectivity issues?

A. Adding a heat deflector

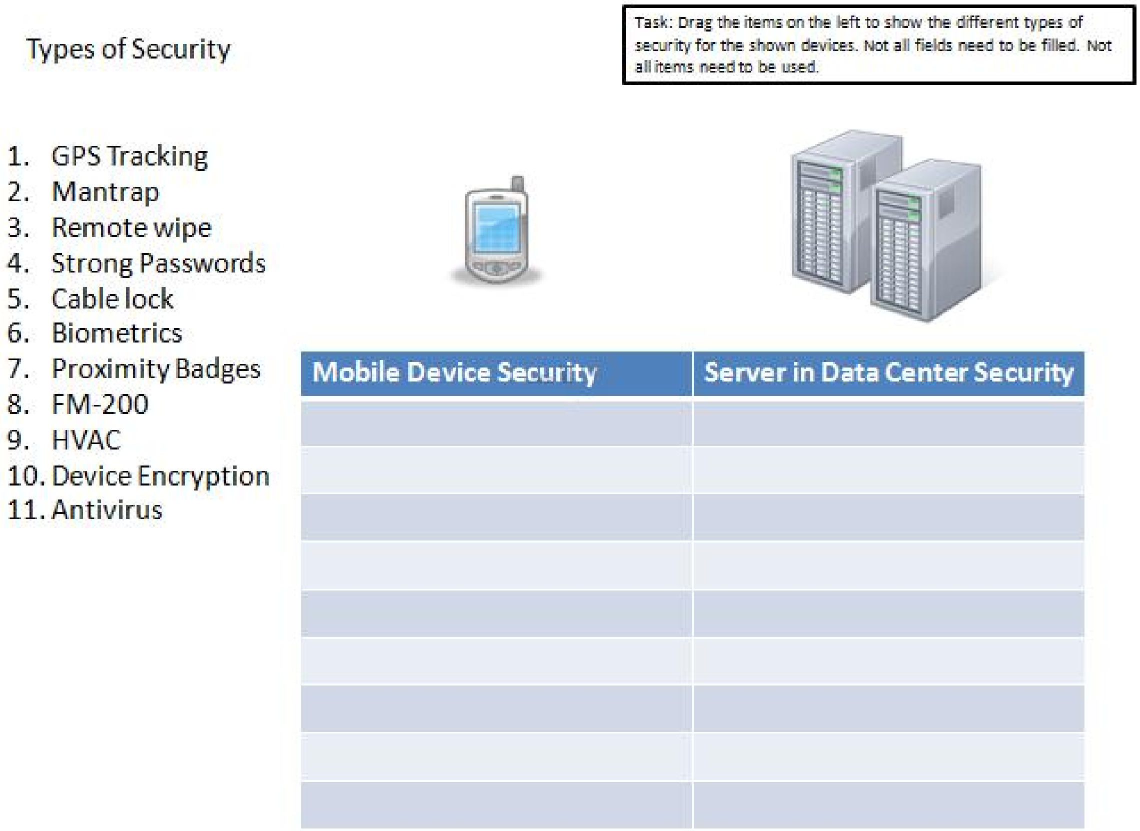
B. Redundant HVAC systems

C. Shielding

D. Add a wireless network

Answer: C

Question No: 337 DRAG DROP
Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.



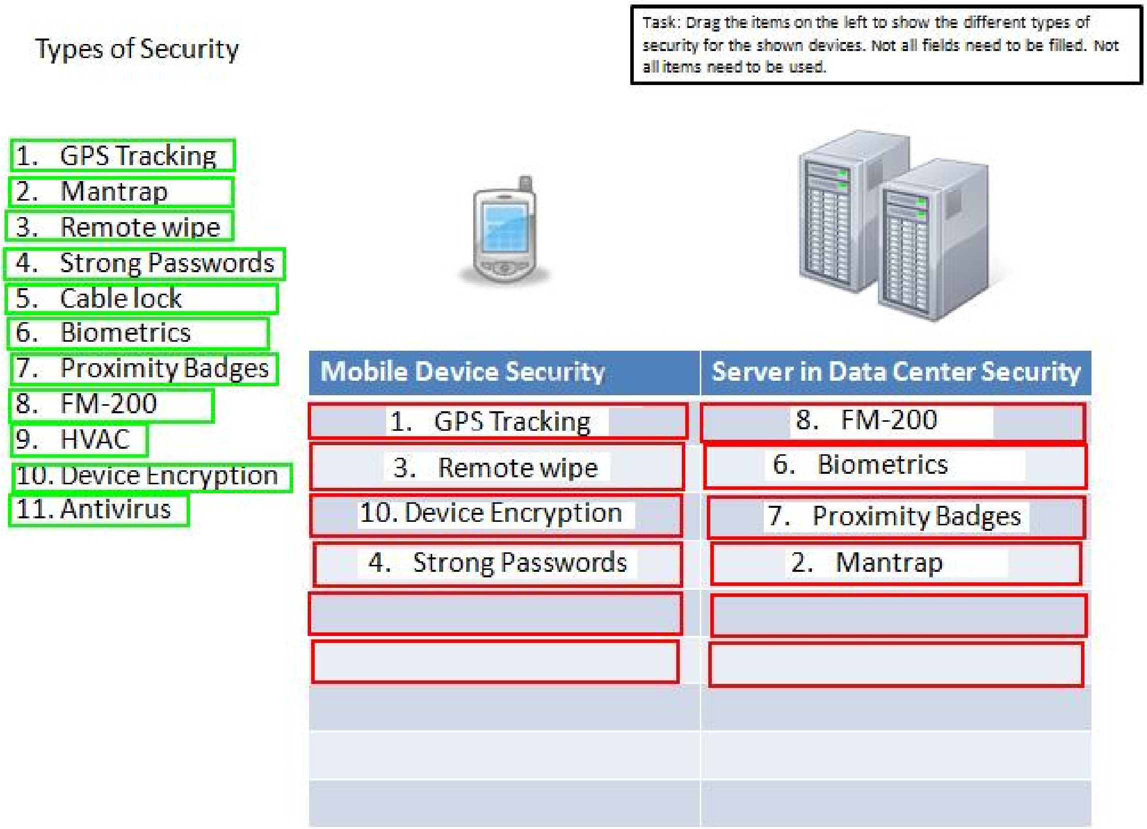
Types of Security

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Mobile Device Security	Server in Data Center Security

Answer:



Types of Security

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

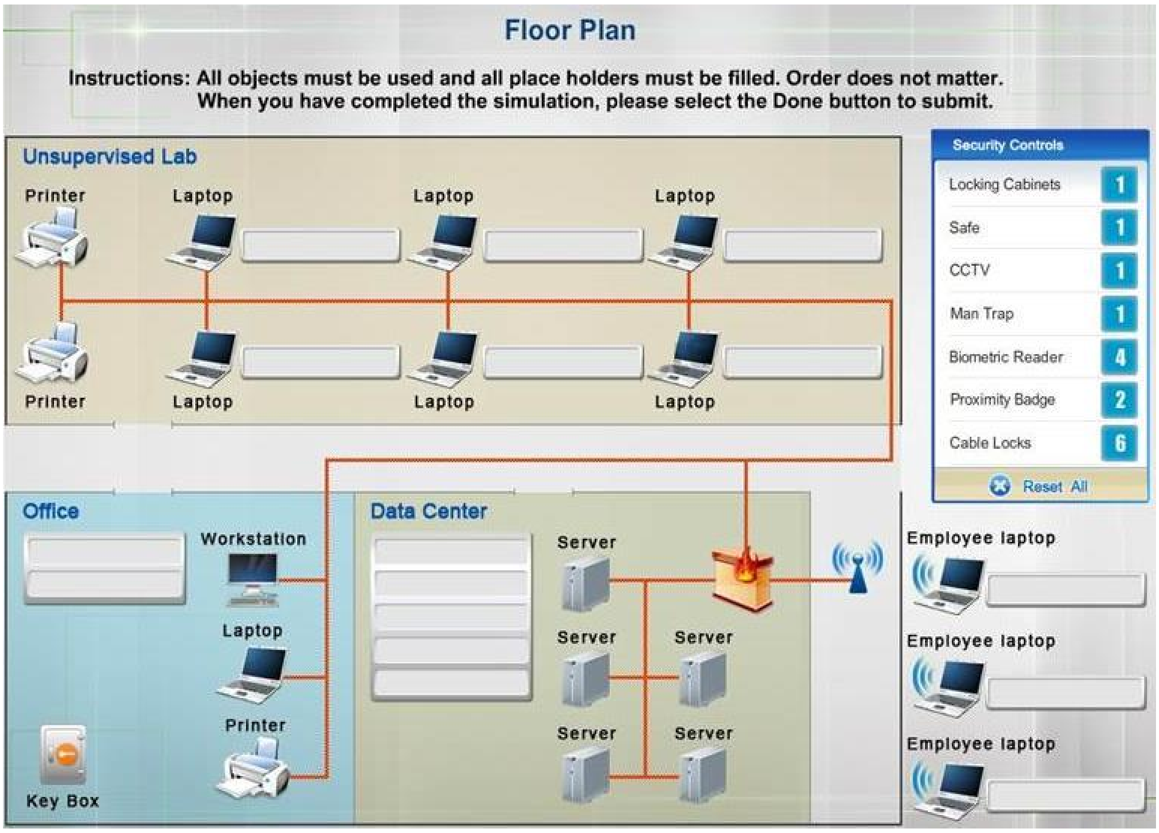
1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Mobile Device Security	Server in Data Center Security
1. GPS Tracking	8. FM-200
3. Remote wipe	6. Biometrics
10. Device Encryption	7. Proximity Badges
4. Strong Passwords	2. Mantrap

Question No: 338 DRAG DROP

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

Instructions: All objects must be used and al place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

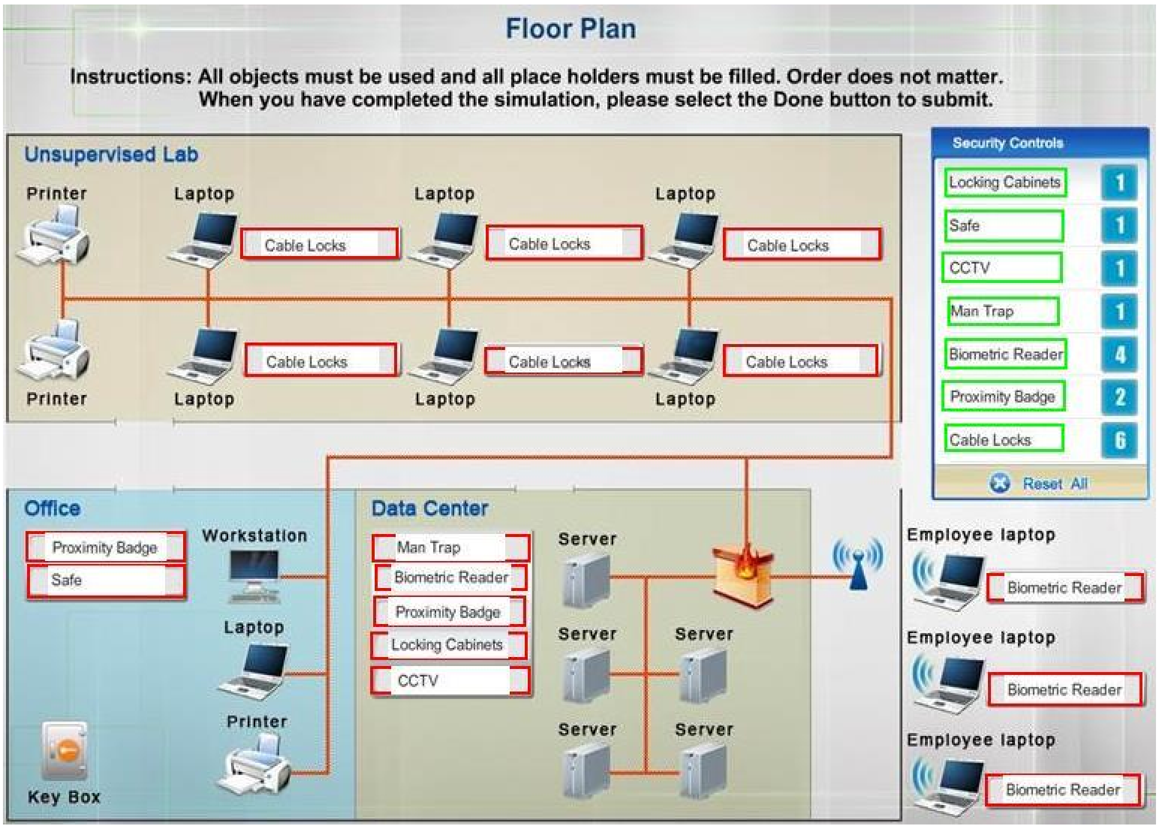


Floor Plan

Instructions: All objects must be used and all place holders must be filled. Order does not matter.
When you have completed the simulation, please select the Done button to submit.

Security Controls	
Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Answer:



Floor Plan

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Question No: 339

A malicious person gained access to a datacenter by ripping the proximity badge reader off the wall near the datacenter entrance. This caused the electronic locks on the datacenter door to release because the:

A. badge reader was improperly installed.

B. system was designed to fail open for life-safety.

C. system was installed in a fail closed configuration.

D. system used magnetic locks and the locks became demagnetized.

Answer: B

Question No: 340

A company is trying to implement physical deterrent controls to improve the overall security posture of their data center. Which of the following BEST meets their goal?

A. Visitor logs

B. Firewal

C. Hardware locks

D. Environmental monitoring

Answer: C

Question No: 341

Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs

B. Mantrap

C. Video surveillance

D. HVAC

Answer: B

Question No: 342

Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

A. Tailgating

B. Fencing

C. Screening

D. Mantrap

Answer: D

Question No: 343

A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing

B. Mantrap

C. A guard

D. Video surveillance

Answer: B

Question No: 344
Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

A. Bollards

B. Video surveillance

C. Proximity readers

D. Fencing

Answer: B

Question No: 345
A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal?

A. CCTV

B. Environmental monitoring

C. RFID

D. EMI shielding

Answer: C

Question No: 346
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective?

A. Password reuse

B. Phishing

C. Social engineering

D. Tailgating

Answer: D

Question No: 347
Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement?

A. Set up mantraps to avoid tailgating of approved users.

B. Place a guard at the entrance to approve access.

C. Install a fingerprint scanner at the entrance.

D. Implement proximity readers to scan users' badges.

Answer: B

Question No: 348
A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

A. Guards

B. CCTV

C. Bollards

D. Spike strip