CompTIA

Exam JK0-022

CompTIA Academic/E2C Security+ Certification Exam Voucher Only

Version: 10.0

[Total Questions: 1149]

Topic break down

Topic	No. of Questions
Topic 1: Network Security	180
Topic 2: Compliance and Operational Security	257
Topic 3: Threats and Vulnerabilities	200
Topic 4: Application, Data and Host Security	123
Topic 5: Access Control and Identity Management	117
Topic 6: Cryptography	116

Topic 1, Network Security

Question No : 1 - (Topic 1)

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

Explanation:

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key.

Question No : 2 - (Topic 1)

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

Explanation:

Remote Desktop Protocol (RDP) uses TCP port 3389.

Question No : 3 - (Topic 1)

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

Explanation:

The administrator is the person responsible for setting the security policy for an organization and is responsible for making decisions about the deployment and configuration of the IDS.

Question No : 4 - (Topic 1)

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 all 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

Explanation:

An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content inspection, or malware inspection.

Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic. If malware is detected, it can be blocked or logged and/or trigger an alert.

Question No : 5 - (Topic 1)

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. Firewall
C. NIPS
D. Spam filter

Answer: C

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

Question No : 6 - (Topic 1)

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. Firewall
B. Switch
C. URL content filter
D. Spam filter

Answer: C

Explanation:

URL filtering, also known as web filtering, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific path names, specific filenames, specific file extensions, or entire specific URLs. Many URL-filtering tools can obtain updated master URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list.

Question No : 7 - (Topic 1)

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

Explanation:

Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of files. Telnet uses TCP port 23. Because it's a clear text protocol and service, it should be avoided and replaced with SSH.

Question No : 8 - (Topic 1)

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

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. A virtual switch is a software application that allows communication between virtual machines. A combination of the two would best satisfy the question.

Question No : 9 - (Topic 1)

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

Explanation:

SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). SCP is commonly used on Linux and Unix platforms.

Question No : 10 - (Topic 1)

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

Explanation:

Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.

SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin.

Question No : 11 - (Topic 1)

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

Explanation:

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.

Question No : 12 - (Topic 1)

Which of the following is the MOST secure protocol to transfer files?

A. FTP
B. FTPS
C. SSH
D. TELNET

Answer: B

Explanation:

FTPS refers to FTP Secure, or FTP SSL. It is a secure variation of File Transfer Protocol (FTP).

Question No : 13 - (Topic 1)

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

Explanation:

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Question No : 14 - (Topic 1)

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

Explanation:

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

Question No : 15 - (Topic 1)

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

Explanation:

Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence.

Question No : 16 - (Topic 1)

Which of the following protocols is used by IPv6 for MAC address resolution?

A. NDP
B. ARP
C. DNS
D. NCP

Answer: A

Explanation:

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6).

Question No : 17 - (Topic 1)

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

Explanation:

ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping. ICMP offers no information If ICMP request queries go unanswered, or ICMP replies are lost or blocked.

Question No : 18 - (Topic 1)

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

Explanation:

The question asks how to prevent access to peer-to-peer file sharing websites. You access a website by browsing to a URL using a Web browser or peer-to-peer file sharing client software. A URL filter is used to block URLs (websites) to prevent users accessing the website.

Incorrect Answer:

A: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. Spam filters do not prevent users accessing peer-to-peer file sharing websites.

C: Content inspection is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content-control software determines what content will be available or perhaps more often what content will be blocked. Content inspection does not prevent users accessing peer-to-peer file sharing websites (although it could block the content of the sites as it is downloaded).

D: Malware inspection is the process of scanning a computer system for malware. Malware inspection does not prevent users accessing peer-to-peer file sharing websites.

References:

http://www.provision.ro/threat-management/web-application-security/url-filtering#pagei-

1|pagep-1|
Stewart, James Michael, *CompTIA Security+ Review Guide*, Sybex, Indianapolis, 2014, pp 18, 19.

Question No : 19 - (Topic 1)

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. Firewall
F. NIDS
G. URL filtering

Answer: D,E,G

Explanation:

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

Firewalls manage traffic using a rule or a set of rules.

A URL is a reference to a resource that specifies the location of the resource. A URL filter is used to block access to a site based on all or part of a URL.

Question No : 20 - (Topic 1)

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

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Question No : 21 - (Topic 1)

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

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

Question No : 22 - (Topic 1)

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

Explanation:

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

Question No : 23 - (Topic 1)

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

Explanation:

Ip tables are a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores.

Question No : 24 - (Topic 1)

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

Explanation:

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer. The PPTP GRE packet format is non-standard, including an additional acknowledgement field replacing the typical routing field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

Question No : 25 - (Topic 1)

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

Explanation:
DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers.

Question No : 26 - (Topic 1)

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

Explanation:
Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it’s a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn’t for public use.

Question No : 27 - (Topic 1)

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

Explanation: Cinderblock walls, metal cabinets, and other barriers can reduce signal strength significantly. Therefore, antenna placement is critical.

Question No : 28 - (Topic 1)

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

Explanation:

Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot.

Question No : 29 - (Topic 1)

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

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

Question No : 30 - (Topic 1)

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

Explanation:

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Question No : 31 - (Topic 1)

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

Explanation:

To test the wireless AP placement, a site survey should be performed.

Question No : 32 - (Topic 1)

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

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Question No : 33 - (Topic 1)

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

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Question No : 34 - (Topic 1)

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

Explanation:

NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.

Question No : 35 - (Topic 1)

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

Explanation:

With the given subnet mask, a maximum number of 30 hosts between IP addresses

10.4.4.161 and 10.4.4.190 are allowed. Therefore, option C and D would be hosts on the same subnet, and the other options would not.

References:
http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php

Question No : 36 - (Topic 1)

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

Explanation:
A secure remote administration solution and Remote Desktop protocol is required.
Secure Shell (SSH) is a secure remote administration solution and makes use of TCP port 22. Remote Desktop Protocol (RDP) uses TCP port 3389.

Question No : 37 - (Topic 1)

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

Explanation:

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

Question No : 38 - (Topic 1)

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

Explanation:

Remote Procedure Call (RPC) is a programming interface that allows a remote computer to run programs on a local machine.

Question No : 39 - (Topic 1)

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

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

Question No : 40 - (Topic 1)

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

Explanation:

Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Question No : 41 - (Topic 1)

Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Install a token on the authentication server
B. Install 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

Explanation:

When setting up a wireless network, you'll find two very different modes of Wi-Fi Protected Access (WPA) security, which apply to both the WPA and WPA2 versions.

The easiest to setup is the Personal mode, technically called the Pre-Shared Key (PSK) mode. It doesn't require anything beyond the wireless router or access points (APs) and uses a single passphrase or password for all users/devices.

The other is the Enterprise mode —which should be used by businesses and organizations—and is also known as the RADIUS, 802.1X, 802.11i, or EAP mode. It provides better security and key management, and supports other enterprise-type functionality, such as VLANs and NAP. However, it requires an external authentication server, called a Remote Authentication Dial In User Service (RADIUS) server to handle the 802.1X authentication of users.

To help you better understand the process of setting up WPA/WPA2-Enterprise and

802.1X, here’s the basic overall steps:
Choose, install, and configure a RADIUS server, or use a hosted service.
Create a certificate authority (CA), so you can issue and install a digital certificate onto the RADIUS server, which may be done as a part of the RADIUS server installation and configuration. Alternatively, you could purchase a digital certificate from a public CA, such as GoDaddy or Verisign, so you don’t have to install the server certificate on all the clients. If using EAP-TLS, you’d also create digital certificates for each end-user.
On the server, populate the RADIUS client database with the IP address and shared secret for each AP.
On the server, populate user data with usernames and passwords for each end-user.
On each AP, configure the security for WPA/WPA2-Enterprise and input the RADIUS server IP address and the shared secret you created for that particular AP.
On each Wi-Fi computer and device, configure the security for WPA/WPA2-Enterprise and set the 802.1X authentication settings.

Question No : 42 - (Topic 1)

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

Explanation:

Secure Shell (SSH) is a more secure replacement for Telnet, rlogon, rsh, and rcp. SSH can be called a remote access or remote terminal solution. SSH offers a means by which a command-line, text-only interface connection with a server, router, switch, or similar device can be established over any distance. SSH makes use of TCP port 22.

Question No : 43 - (Topic 1)

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

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Question No : 44 - (Topic 1)

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

Explanation:

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a signature-based system is that it can quickly and accurately detect any event from its database of signatures.

Question No : 45 - (Topic 1)

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

Explanation:

SCP copies files securely between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH. Unlike RCP, SCP will ask for passwords or passphrases if they are needed for authentication.
SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Question No : 46 - (Topic 1)

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

A. FTPS
B. SFTP
C. SSL
D. S/MIME

Answer: B

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Question No : 47 - (Topic 1)

Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP
B. Mac filtering
C. WPA2
D. WPA

Answer: A

Explanation:

TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it.

Question No : 48 - (Topic 1)

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

Explanation:

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer.

Question No : 49 - (Topic 1)

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

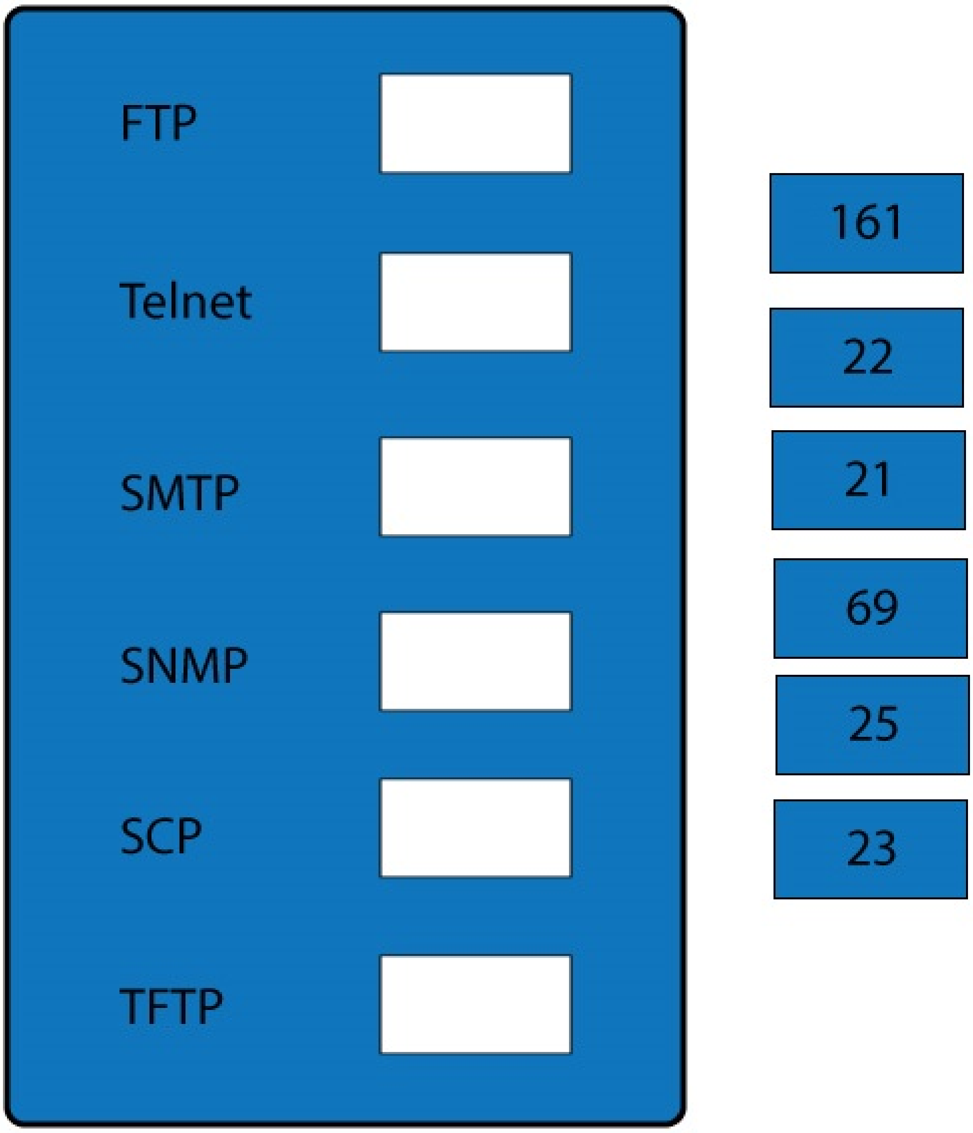
Answer: C

Explanation:

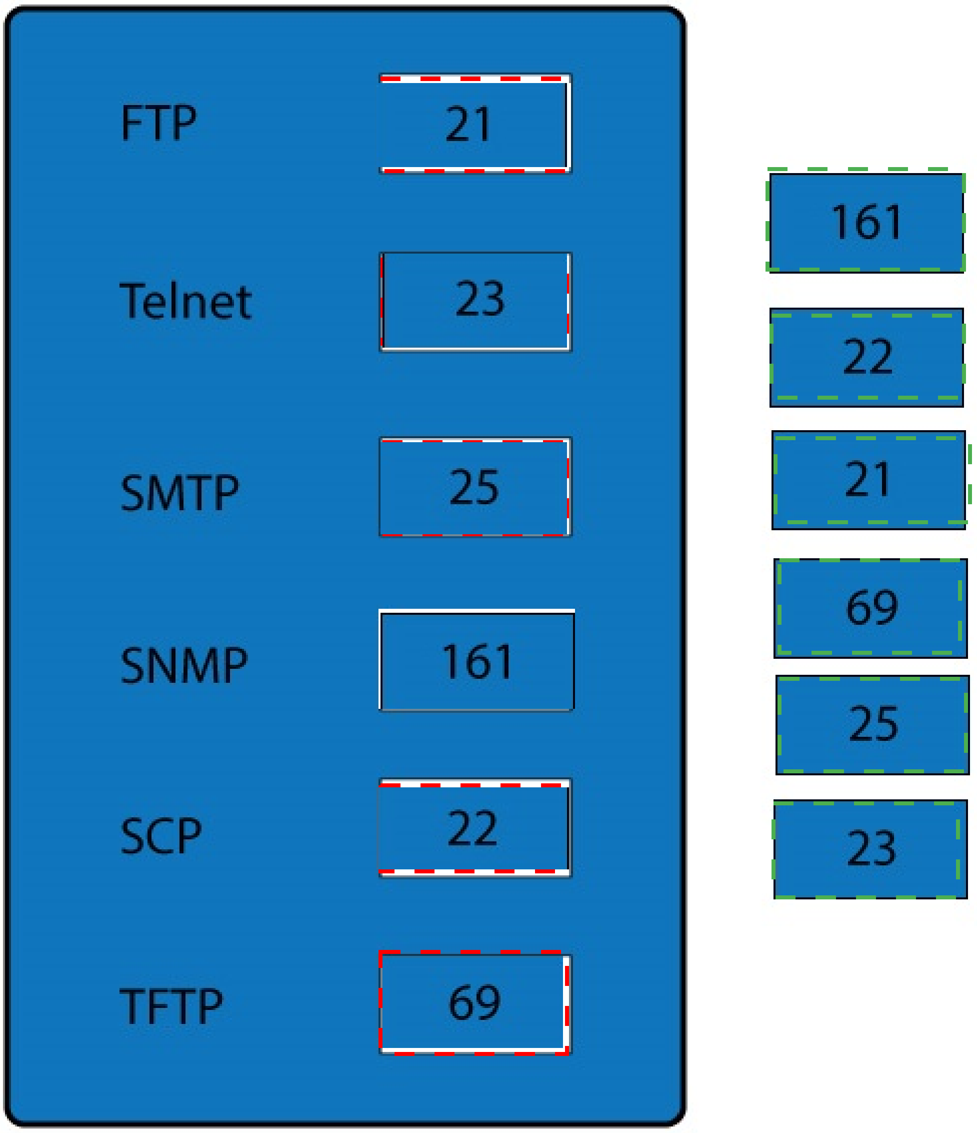
Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

Question No : 50 DRAG DROP - (Topic 1)

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

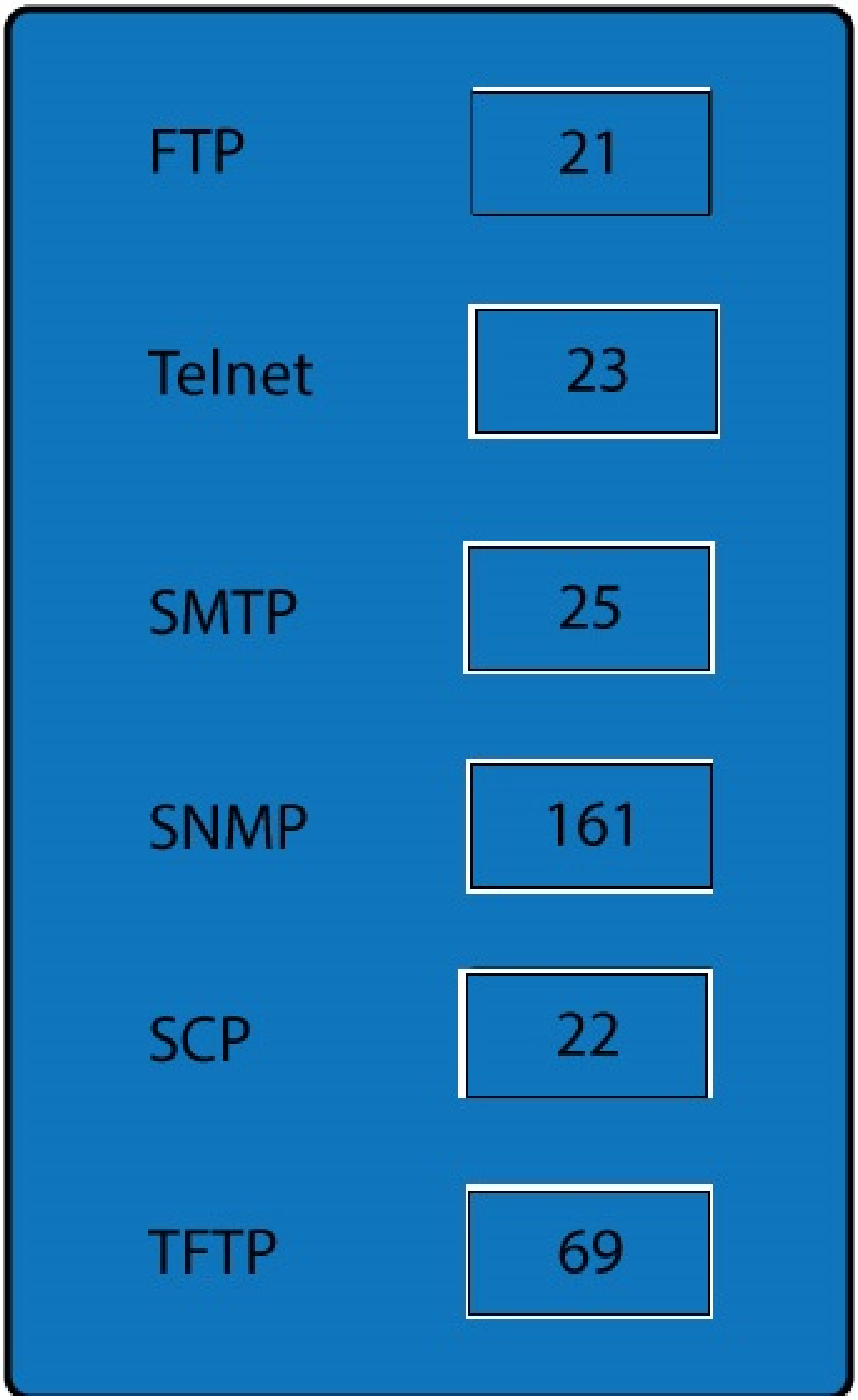
21

69

25

23

Explanation:



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

FTP uses TCP port 21.

Telnet uses port 23.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

SMTP uses TCP port 25.

Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162.

References:
Stewart, James Michael, *CompTIA Security+ Review Guide*, Sybex, Indianapolis, 2014, pp 42, 45, 51
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question No : 51 - (Topic 1)

ON 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 all subfolders and all 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

Explanation: Implicit deny is the default security stance that says if you aren’t specifically granted access or privileges for a resource, you’re denied access by default.

Question No : 52 - (Topic 1)

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

Explanation:

VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so.

Question No : 53 - (Topic 1)

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

Explanation:

HTTP and HTTPS, which uses TCP port 80 and TCP port 443 respectively, is necessary for Communicating with Web servers. It should therefore be allowed through the firewall.

Question No : 54 - (Topic 1)

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

Explanation: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

Question No : 55 - (Topic 1)

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

Explanation:

D: WPA-Enterprise is also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. RADIUS can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. Thus the RADIUS server can perform all authentications. This will require users to use their passwords on their user accounts.

Question No : 56 HOTSPOT - (Topic 1)

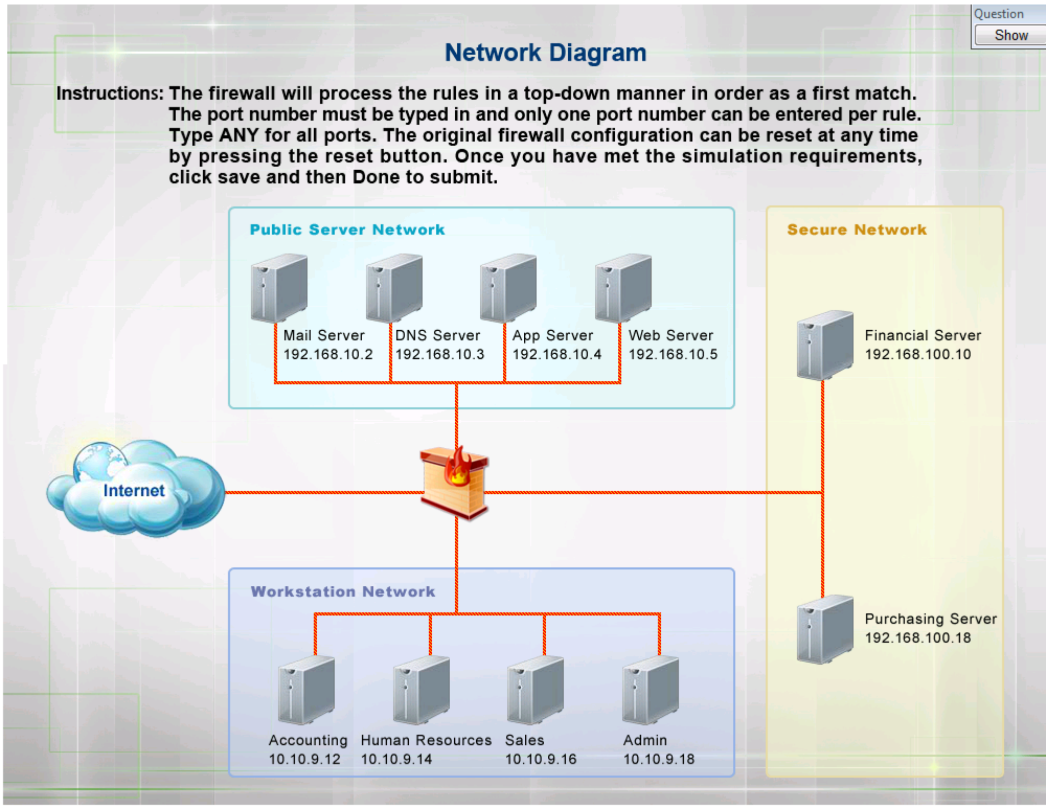
The security administrator has installed a new firewall which implements an implicit DENY policy by default. Click on the firewall and configure it to allow ONLY the following communication.

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

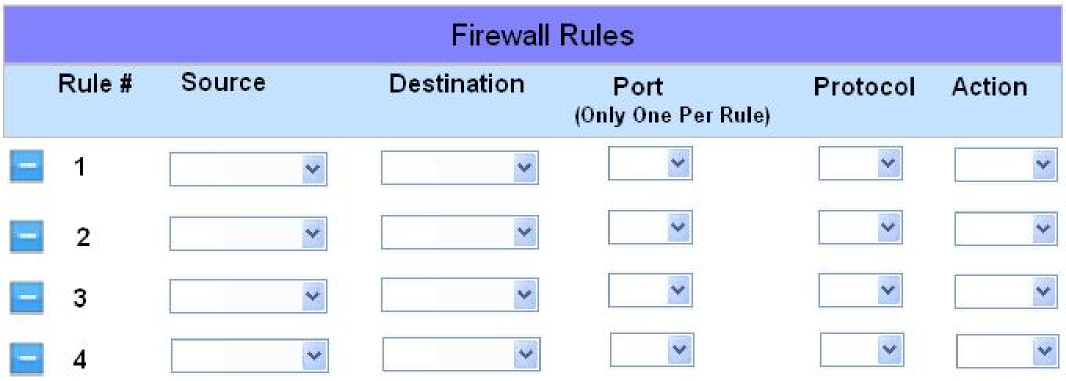
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

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.



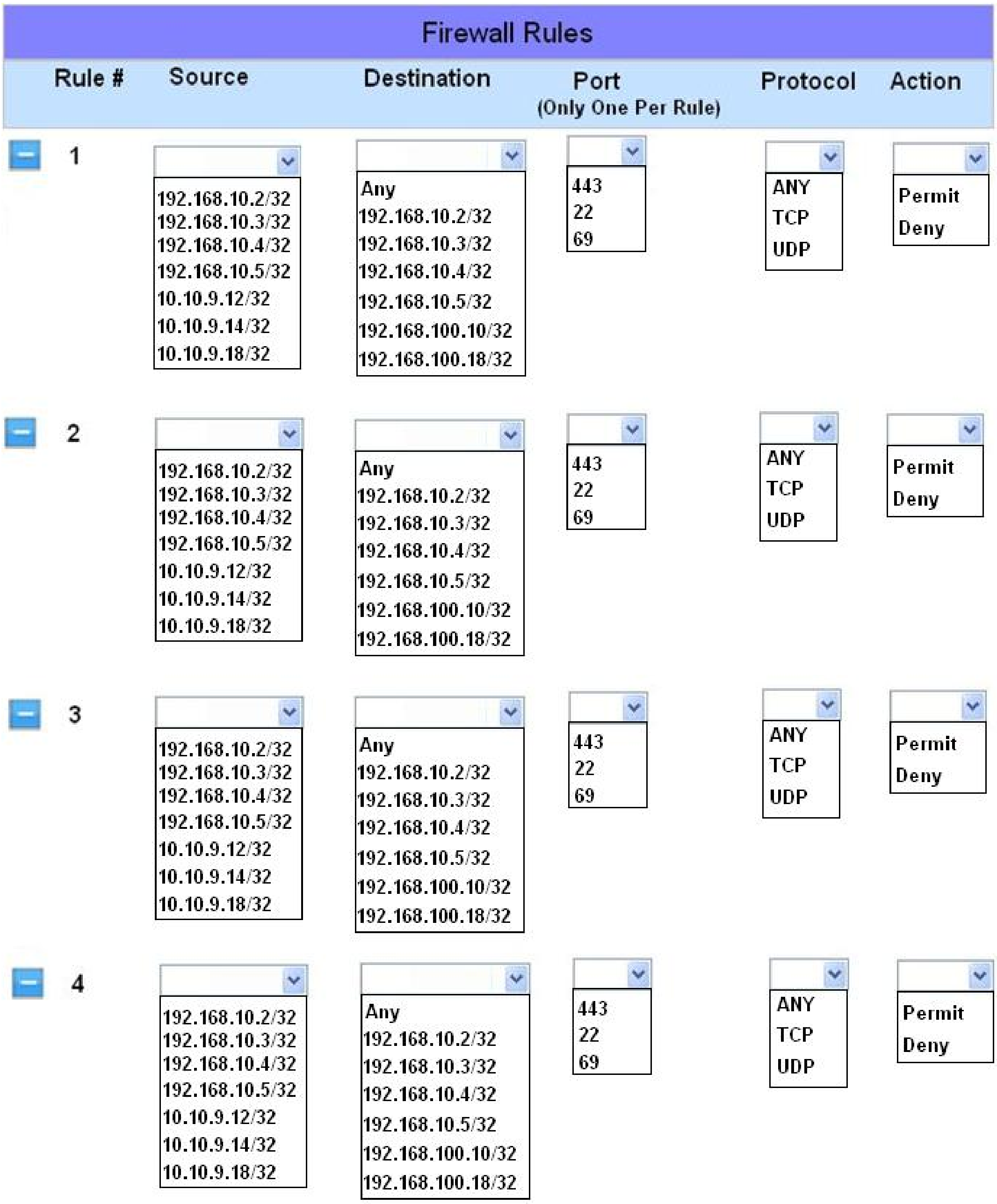
Network Diagram

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

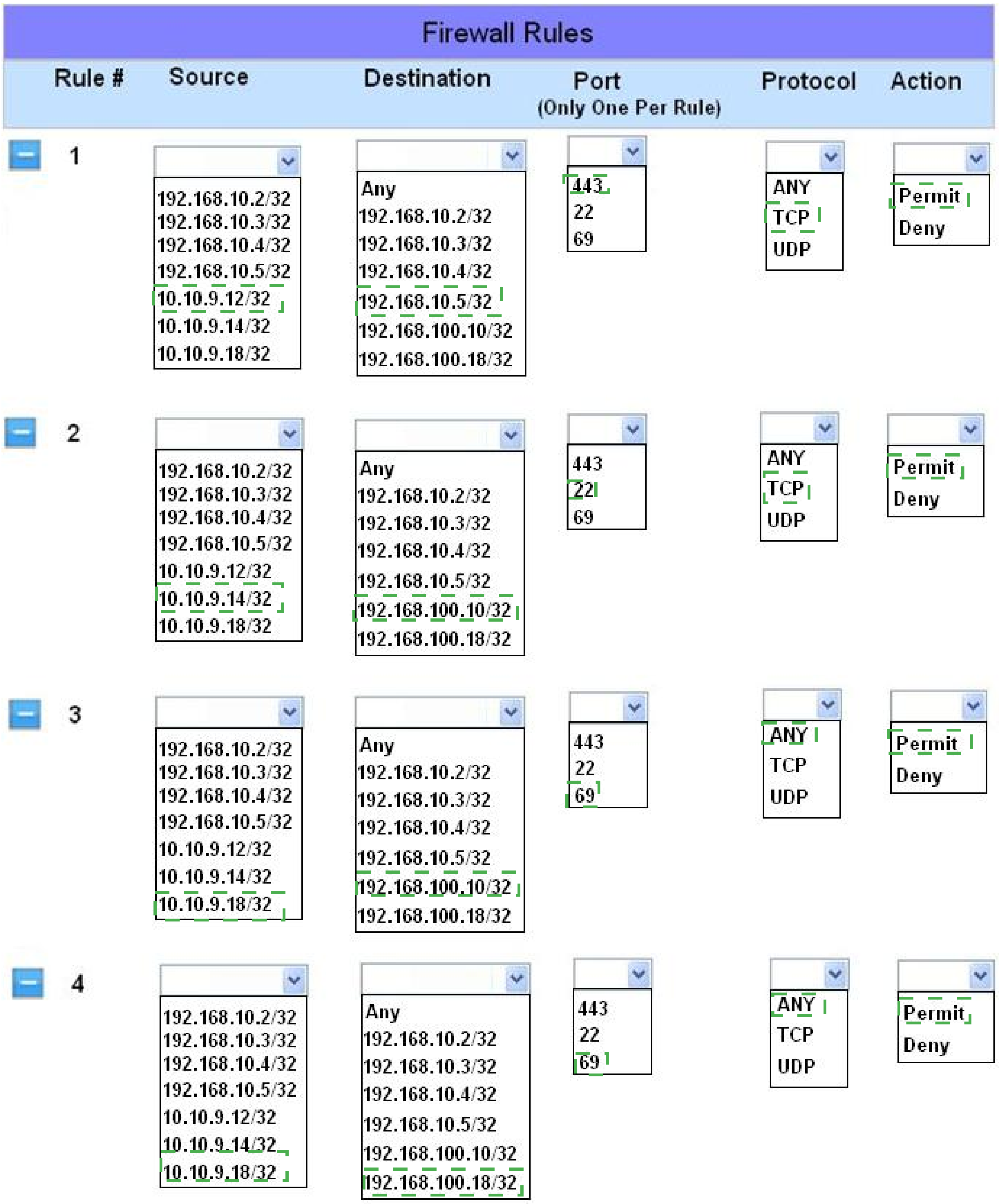
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1					
2					
3					
4					



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

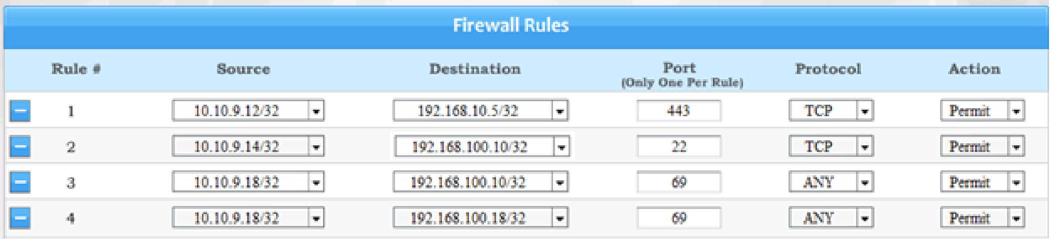
Answer:



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

Explanation:



Firewall Rules

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

Implicit deny is the default security stance that says if you aren’t specifically granted access or privileges for a resource, you’re denied access by default.

Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.

Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22
Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References:
Stewart, James Michael, *CompTIA Security+ Review Guide*, Sybex, Indianapolis, 2014, pp 26, 44.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question No : 57 - (Topic 1)

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

Explanation:
When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it.

Question No : 58 - (Topic 1)

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

Explanation:

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

Question No : 59 - (Topic 1)

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

Explanation:

To find MAC address of a Unix/Linux workstation, use *ifconfig* or *ip a*.

Question No : 60 - (Topic 1)

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

Explanation:

B: The Telnet program parameters are: telnet <hostname> <port>

<hostname> is the name or IP address of the remote server to connect to.

<port> is the port number of the service to use for the connection.

TCP port 443 provides the HTTPS (used for secure web connections) service; it is the default SSL port. By running the Telnet some-host 443 command, the security analyst is checking that routing is done properly and not blocked by a firewall.

Question No : 61 - (Topic 1)

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

Explanation:

Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.

Question No : 62 - (Topic 1)

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

Explanation:

Unified Threat Management (UTM) is, basically, the combination of a firewall with other abilities. These abilities include intrusion prevention, antivirus, content filtering, etc.
Advantages of combining everything into one:

You only have one product to learn.
You only have to deal with a single vendor.
IT provides reduced complexity.

Question No : 63 - (Topic 1)

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

Explanation:

Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn’t require authentication. It operates on UDP port 69.

Question No : 64 - (Topic 1)

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

Explanation:

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Question No : 65 - (Topic 1)

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

Explanation:

IPv6 addresses are 128-bits in length. An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). The hexadecimal digits are case-insensitive, but IETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

Question No : 66 - (Topic 1)

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

Explanation:

Implicit deny is the default security stance that says if you aren’t specifically granted access or privileges for a resource, you’re denied access by default. Implicit deny is the default response when an explicit allow or deny isn’t present.

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. These are zone file exchanges between DNS servers, special manual queries, or used when a response exceeds 512 bytes. UDP port 53 is used for most typical DNS queries.

Question No : 67 - (Topic 1)

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

Explanation:
BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon. This is the only option that directly involves DNS.

Question No : 68 - (Topic 1)

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

Explanation: Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it’s a discoverable value using a wireless packet sniffer.

Thus, the SSID should be disabled if the network isn’t for public use.

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Question No : 69 - (Topic 1)

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

Explanation:

The question states that traffic on port 21, 69, 80, and 137-139 is blocked, while ports 22 and 443 are allowed.

Port 21 is used for FTP by default.
Port 69 is used for TFTP.
Port 80 is used for HTTP.
Ports 137-139 are used for NetBIOS.
VMM uses SFTP over default port 22.
Port 22 is used for SSH by default.
SCP runs over TCP port 22 by default.
Port 443 is used for HTTPS.

Question No : 70 - (Topic 1)

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

Explanation:

CCMP is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard.

Question No : 71 - (Topic 1)

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

Explanation:

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

Question No : 72 - (Topic 1)

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

Explanation:

Network address translation (NAT) allows you to share a connection to the public Internet via a single interface with a single public IP address. NAT maps the private addresses to the public address. In a typical configuration, a local network uses one of the designated "private" IP address subnets. A router on that network has a private address (192.168.1.1) in that address space, and is also connected to the Internet with a "public" address (10.2.2.1) assigned by an Internet service provider.

Question No : 73 - (Topic 1)

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

Explanation:

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Question No : 74 - (Topic 1)

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

Explanation:

In the OSI model, IP addressing and IP routing are performed at layer 3 (the network layer). In this question we need to configure routing. When configuring routing, you specify which IP range (in this case, the IP subnet of the remote site) is allowed to route traffic through the router to the FTP server.

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

Question No : 75 - (Topic 1)

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

Explanation:

Telnet supports IPv6 connections.

IPv6 is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec is a compulsory component for IPv6.

IPsec operates at Layer 3 of the OSI model, whereas Telnet operates at Layer 7.

Question No : 76 - (Topic 1)

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

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Question No : 77 - (Topic 1)

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

Explanation:

D: Wired Equivalent Privacy (WEP) is designed to provide security equivalent to that of a wired network. WEP has vulnerabilities and isn’t considered highly secure. Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/ WPA2 standard are EAP-TLS, EAP-PSK, EAP-MD5, as well as LEAP and PEAP.

PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

Question No : 78 - (Topic 1)

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

Explanation:

WPA2-Enterprise is designed for enterprise networks and requires a RADIUS authentication server.

Question No : 79 - (Topic 1)

NO: 93

Multi-tenancy is a concept found in which of the following?

A. Full disk encryption
B. Removable media
C. Cloud computing
D. Data loss prevention

Answer: C

Explanation:

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This “multitenant” nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

Question No : 80 - (Topic 1)

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

Explanation:

There are three steps to penetrating a WPA-protected network.

Sniffing

Parsing

Attacking

Question No : 81 - (Topic 1)

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

Explanation:

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for distributing IP addresses for interfaces and services. DHCP makes use of port 68.

Question No : 82 - (Topic 1)

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

Explanation:

A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list.

Question No : 83 - (Topic 1)

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

Explanation:

IEEE 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to wireless devices connecting to a LAN or WLAN.

Question No : 84 - (Topic 1)

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

Explanation:

Firewall rules are used to define what traffic is able pass between the firewall and the internal network. Firewall rules block the connection, allow the connection, or allow the connection only if it is secured. Firewall rules can be applied to inbound traffic or outbound traffic and any type of network.

Question No : 85 - (Topic 1)

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

Explanation:

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Question No : 86 - (Topic 1)

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

Explanation:

Secure Shell (SSH) is a tunneling protocol originally used on Unix systems. It’s now available for both Unix and Windows environments. SSH is primarily intended for interactive terminal sessions.
SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

Question No : 87 - (Topic 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

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

Question No : 88 - (Topic 1)

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

Explanation:

RDP uses TCP port 3389.

Question No : 89 - (Topic 1)

Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec
B. Full disk encryption
C. 802.1x
D. PKI

Answer: A

Explanation:

IPSec can operate in tunnel mode or transport mode. It uses symmetric cryptography to provide encryption security. Furthermore, it makes use of Internet Security Association and Key Management Protocol (ISAKMP).

Question No : 90 - (Topic 1)

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

Explanation:

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Question No : 91 - (Topic 1)

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

Explanation:

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This “multitenant” nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

Question No : 92 - (Topic 1)

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

Explanation:

A proxy is a device that acts on behalf of other(s). In the interest of security, all internal user interaction with the Internet should be controlled through a proxy server. The proxy server should automatically block known malicious sites. The proxy server should cache often-accessed sites to improve performance.

Question No : 93 - (Topic 1)

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

Explanation:

Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. SFTP is a secured alternative to standard FTP.

Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Question No : 94 - (Topic 1)

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. Firewall
B. NIPS
C. Load balancer
D. URL filter

Answer: A

Explanation:

Firewalls, routers, and even switches can use ACLs as a method of security management. An access control list has a *deny ip any any* implicitly at the end of any access control list. ACLs deny by default and allow by exception.

Question No : 95 - (Topic 1)

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

Explanation:

FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69.

Question No : 96 - (Topic 1)

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

Explanation:

CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA. CCMP provides the following security services:

Data confidentiality; ensures only authorized parties can access the information

Authentication; provides proof of genuineness of the user

Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation.

Question No : 97 - (Topic 1)

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

Explanation: The AAAA Address record links a FQDN to an IPv6 address.

Question No : 98 - (Topic 1)

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

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

Question No : 99 - (Topic 1)

The security administrator has been tasked to update all 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

Explanation:

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Question No : 100 - (Topic 1)

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

Explanation:

SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server.

Question No : 101 - (Topic 1)

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

Explanation:

Port security in IT can mean several things:

The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port.

The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (of TCP or UDP) are closed if a service isn’t actively using them.

Port knocking is a security system in which all ports on a system appear closed. However, if the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service.

Question No : 102 - (Topic 1)

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

Explanation:

Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can easily change, or “spoof,” MAC addresses in software.

Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. This isn’t a great security tool because people can spoof their MAC addresses.

Question No : 103 - (Topic 1)

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

Explanation:

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Question No : 104 - (Topic 1)

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

Explanation:

DNS links IP addresses and human-friendly fully qualified domain names (FQDNs), which are made up of the Top-level domain (TLD), the registered domain name, and the Subdomain or hostname.

Therefore, if the DNS ports are blocked websites will not be reachable.

Question No : 105 - (Topic 1)

Which of the following is the default port for TFTP?

A. 20
B. 69
C. 21
D. 68

Answer: B

Explanation:

TFTP makes use of UDP port 69.

Question No : 106 - (Topic 1)

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

Explanation:

A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.

Question No : 107 - (Topic 1)

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

Explanation: FTPS uses ports 989 and 990.

Question No : 108 - (Topic 1)

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

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

Question No : 109 - (Topic 1)

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

Explanation:

A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels.

Question No : 110 - (Topic 1)

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

Explanation:

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards. Only servers running Network Policy Server

(NPS) or PEAP-MS-CHAP v2 are required to have a certificate.

Question No : 111 - (Topic 1)

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

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Question No : 112 - (Topic 1)

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

Explanation:

A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network.

Question No : 113 - (Topic 1)

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

Explanation:

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

Question No : 114 - (Topic 1)

A network administrator needs to provide daily network usage reports on all 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

Explanation:

Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

Question No : 115 - (Topic 1)

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

Explanation:

C: A primary DNS server has the "master copy" of a zone, and secondary DNS servers keep copies of the zone for redundancy. When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone. This is done through zone transfers. If you allow zone transfers to any server, all the resource records in the zone are viewable by any host that can contact your DNS server. Thus you will need to secure the zone transfers to stop an attacker from mapping out your addresses and devices on your network.

Question No : 116 - (Topic 1)

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

Explanation:

To establish a TCP connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.
ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to

one more than the received sequence number i.e. B+1.

Question No : 117 - (Topic 1)

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

Explanation:

Because Virtualization allows a single set of hardware to host multiple virtual machines, it requires less hardware to maintain the current scenario.

Question No : 118 - (Topic 1)

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

Explanation:

An application-level gateway firewall filters traffic based on user access, group membership, the application or service used, or even the type of resources being transmitted. This type of firewall operates at the Application layer (Layer 7) of the OSI model.

Question No : 119 - (Topic 1)

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

Explanation:

Migrating to a virtual server environment reduces cost by eliminating the need to purchase, manage, maintain and power physical machines. The fewer physical machines you have, the less money it costs.

Question No : 120 - (Topic 1)

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

Explanation:

When you combine a firewall with other abilities (intrusion prevention, antivirus, content filtering, etc.), what used to be called an all-in-one appliance is now known as a unified threat management (UTM) system. The advantages of combining everything into one include a reduced learning curve (you only have one product to learn), a single vendor to deal with, and—typically—reduced complexity.

Question No : 121 - (Topic 1)

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

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Question No : 122 - (Topic 1)

Which of the following protocols allows for the LARGEST address space?

A. IPX
B. IPv4
C. IPv6
D. Appletalk

Answer: C

Explanation:

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4.

Question No : 123 - (Topic 1)

A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still 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

Explanation:

Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services and applications within the cloud.

Question No : 124 - (Topic 1)

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

Explanation:

G: Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

D: SCP stands for Secure Copy. SCP is used to securely copy files over a network. SCP uses SSH to secure the connection and therefore uses port 22.

H: SFTP stands for stands for Secure File Transfer Protocol and is used for transferring files using FTP over a secure network connection. SFTP uses SSH to secure the connection and therefore uses port 22.

Question No : 125 - (Topic 1)

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 all access points to broadcast their SSIDs.

Answer: A

Explanation:

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Question No : 126 - (Topic 1)

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

Explanation:

Cloud computing refers to performing data processing and storage elsewhere, over a network connection, rather than locally. Because users have access to the data, it can easily be copied to a USB device.

Question No : 127 - (Topic 1)

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

Explanation:

The question states that the network uses 802.1x with PEAP. The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS). A RADIUS server will be configured with a digital certificate. When a digital certificate is created, an expiration period is configured by the Certificate Authority (CA). The expiration period is commonly one or two years.

The question states that no configuration changes have been made so it’s likely that the certificate has expired.

Question No : 128 - (Topic 1)

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

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Question No : 129 - (Topic 1)

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

Explanation:

The majority of the EAP-TLS implementations require client-side X.509 certificates without giving the option to disable the requirement.

Question No : 130 - (Topic 1)

Which of the following is BEST used as a secure replacement for TELNET?

A. HTTPS
B. HMAC
C. GPG
D. SSH

Answer: D

Explanation:

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

Question No : 131 - (Topic 1)

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

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Question No : 132 - (Topic 1)

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

Explanation:

VPNs are usually employed to allow remote access users to connect to and access the network, and offer connectivity between two or more private networks or LANs. A VPN gateway (VPN router) is a connection point that connects two LANs via a nonsecure network such as the Internet.

Question No : 133 - (Topic 1)

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

Explanation: Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

Question No : 134 - (Topic 1)

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

Explanation:

A protocol analyzer is a tool used to examine the contents of network traffic. Commonly known as a sniffer, a protocol analyzer can be a dedicated hardware device or software installed onto a typical host system. In either case, a protocol analyzer is first a packet capturing tool that can collect network traffic and store it in memory or onto a storage device. Once a packet is captured, it can be analyzed either with complex automated tools and scripts or manually.

Question No : 135 - (Topic 1)

A security architect wishes to implement a wireless network with connectivity to the company’s internal network. Before they inform all 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

Explanation:

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

Question No : 136 - (Topic 1)

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

Explanation:

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present.

Question No : 137 - (Topic 1)

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

Explanation:

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Question No : 138 - (Topic 1)

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

Explanation:

Load balancing refers to shifting a load from one device to another. A load balancer can be implemented as a software or hardware solution, and it is usually associated with a device—a router, a firewall, NAT appliance, and so on. In its most common implementation, a load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available.

Question No : 139 - (Topic 1)

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

Explanation:

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

Question No : 140 - (Topic 1)

Which of the following devices would MOST likely have a DMZ interface?

A. Firewall
B. Switch
C. Load balancer
D. Proxy

Answer: A

Explanation: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Question No : 141 - (Topic 1)

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. Install HIPS on each VM
C. Virtual switches with VLANs
D. Develop a patch management guide

Answer: C

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

Question No : 142 - (Topic 1)

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

Explanation:

A Yagi-Uda antenna, commonly known simply as a Yagi antenna, is a directional antenna consisting of multiple parallel dipole elements in a line, usually made of metal rods. It consists of a single driven element connected to the transmitter or receiver with a transmission line, and additional parasitic elements: a so-called reflector and one or more directors. The reflector element is slightly longer than the driven dipole, whereas the directors are a little shorter. This design achieves a very substantial increase in the antenna's directionality and gain compared to a simple dipole.

Question No : 143 - (Topic 1)

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

Explanation:

WEP is based on RC4, but due to errors in design and implementation, WEP is weak in a number of areas, two of which are the use of a static common key and poor implementation of initiation vectors (IVs). When the WEP key is discovered, the attacker can join the network and then listen in on all other wireless client communications.

Question No : 144 - (Topic 1)

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

Explanation:

SSL (Secure Sockets Layer) is used for establishing an encrypted link between two computers, typically a web server and a browser. SSL is used to enable sensitive information such as login credentials and credit card numbers to be transmitted securely.

Question No : 145 - (Topic 1)

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

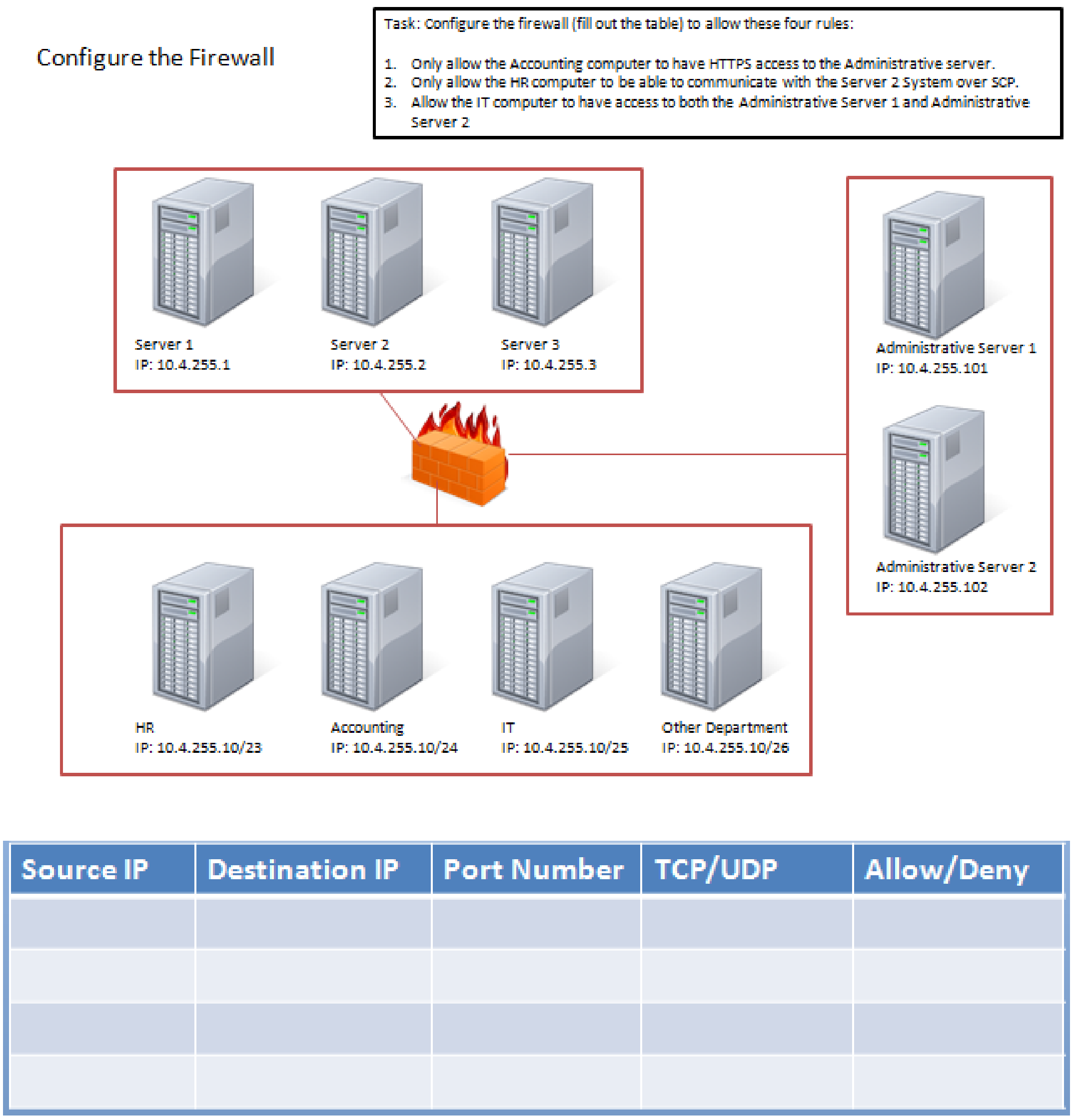
B. Anomaly Based IDS
C. Proxy Firewall
D. Signature IDS

Answer: B

Explanation:

Anomaly-based detection watches the ongoing activity in the environment and looks for abnormal occurrences. An anomaly-based monitoring or detection method relies on definitions of all valid forms of activity. This database of known valid activity allows the tool to detect any and all anomalies. Anomaly-based detection is commonly used for protocols. Because all the valid and legal forms of a protocol are known and can be defined, any variations from those known valid constructions are seen as anomalies.

Question No : 146 CORRECT TEXT - (Topic 1)



Configure the Firewall

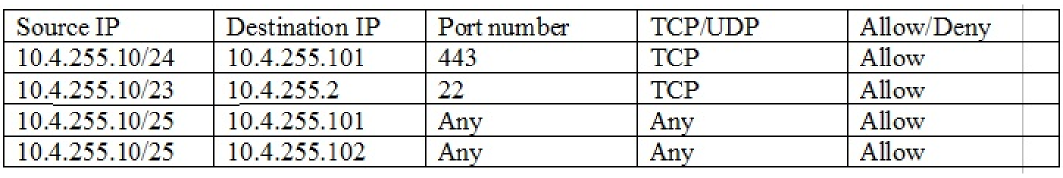
Task: Configure the firewall (fill out the table) to allow these four rules:

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: Use the following answer for this simulation task.

Explanation:



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

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections – HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1)

Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

References:

Dulaney, Emmett and Chuck Eastton, *CompTIA Security+ Study Guide*, Sixth Edition, Sybex, Indianapolis, 2014, pp 77, 83, 96, 157.

Question No : 147 - (Topic 1)

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

Explanation:

A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It’s intended to be an application-specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks.

Question No : 148 - (Topic 1)

TION NO: 134

Which of the following ports is used for SSH, by default?

A. 23
B. 32
C. 12
D. 22

Answer: D

Explanation:

Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

Question No : 149 - (Topic 1)

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

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

Question No : 150 - (Topic 1)

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

Explanation:

802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and be distinct from other VLAN port designations. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Question No : 151 - (Topic 1)

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

Explanation:

Layer 2 Tunneling Protocol (L2TP) came about through a partnership between Cisco and Microsoft with the intention of providing a more secure VPN protocol. L2TP is considered to be a more secure option than PPTP, as the IPSec protocol which holds more secure encryption algorithms, is utilized in conjunction with it. It also requires a pre-shared certificate or key. L2TP's strongest level of encryption makes use of 168 bit keys, 3 DES encryption algorithm and requires two levels of authentication.

L2TP has a number of advantages in comparison to PPTP in terms of providing data integrity and authentication of origin verification designed to keep hackers from compromising the system. However, the increased overhead required to manage this elevated security means that it performs at a slower pace than PPTP.

Question No : 152 - (Topic 1)

The Chief Information Security Officer (CISO) has mandated that all 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

Explanation:

The basic purpose of a firewall is to isolate one network from another.

Question No : 153 - (Topic 1)

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

Explanation:

Port 80 is used by HTTP, which is the foundation of data communication for the World Wide Web.

Question No : 154 - (Topic 1)

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

Explanation:

The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

Question No : 155 - (Topic 1)

TION 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

Explanation:

You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

Question No : 156 - (Topic 1)

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

Explanation:

Cipher Block Chaining Message Authentication Code Protocol (CCMP) makes use of 128-bit AES encryption with a 48-bit initialization vector.

Question No : 157 - (Topic 1)

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

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Question No : 158 - (Topic 1)

Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP
B. IPSec
C. SCP
D. TCP

Answer: C

Explanation:

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.

Question No : 159 - (Topic 1)

Layer 7 devices used to prevent specific types of html tags are called:

A. Firewalls
B. Content filters
C. Routers
D. NIDS

Answer: B

Explanation:

A content filter is a is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model.

Question No : 160 - (Topic 1)

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

Explanation:

LDAP makes use of port 389.

Question No : 161 - (Topic 1)

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

Explanation:

Disabling unused switch ports a simple method many network administrators use to help secure their network from unauthorized access.

All ports not in use should be disabled. Otherwise, they present an open door for an attacker to enter.

Question No : 162 - (Topic 1)

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

Explanation:

It is a common and recommended practice to separate voice and data traffic by using VLANs. Separating voice and data traffic using VLANs provides a solid security boundary, preventing data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data.

Question No : 163 - (Topic 1)

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

Explanation:

DNS (Domain Name System) uses port 53.

Question No : 164 - (Topic 1)

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

Explanation:

The SSID is still required for directing packets to and from the base station, so it can be discovered using a wireless packet sniffer.

Question No : 165 - (Topic 1)

A small company can only afford to buy an all-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

Explanation:

We can protect the servers from the user devices by separating them into separate VLANs (virtual local area networks).

The network device in the question is a router/switch. We can use the router to allow access from devices in one VLAN to the servers in the other VLAN. We can configure an ACL (Access Control List) on the router to determine who is able to access the server.

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN.

This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN.

Question No : 166 - (Topic 1)

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

Explanation:

802.1x is a port-based authentication mechanism. It’s based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it’s often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System’s Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

Question No : 167 - (Topic 1)

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

Explanation: Of the options supplied, WiFi Protected Access (WPA) is the most secure and is the replacement for WEP.

Question No : 168 - (Topic 1)

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

Explanation:

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

Question No : 169 - (Topic 1)

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

Explanation:

The LMHOSTS file provides a NetBIOS name resolution method that can be used for small networks that do not use a WINS server. NetBIOS has been adapted to run on top of TCP/IP, and is still extensively used for name resolution and registration in Windows-based environments.

Question No : 170 - (Topic 1)

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 Firewall

Answer: B

Explanation:

Stateful inspections occur at all levels of the network.

Question No : 171 - (Topic 1)

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

Explanation:

Software as a Service (SaaS) allows for on-demand online access to specific software applications or suites without having to install it locally. This will allow the data center to continue providing network and security services.

Question No : 172 - (Topic 1)

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

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

Question No : 173 - (Topic 1)

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

Explanation: Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

Question No : 174 - (Topic 1)

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

Explanation:

Quality of Service (QoS) facilitates the deployment of media-rich applications, such as video conferencing and Internet Protocol (IP) telephony, without adversely affecting network throughput.

Question No : 175 - (Topic 1)

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. Firewall
C. Proxy server
D. Protocol analyzer

Answer: A

Explanation:

Web filtering software is designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means.

Question No : 176 - (Topic 1)

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

Explanation:

IPSec security is built into IPv6.

Question No : 177 - (Topic 1)

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

Explanation:

DNS uses TCP and UDP port 53. TCP port 53 is used for zone transfers, whereas UDP port 53 is used for queries.

Question No : 178 - (Topic 1)

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

Explanation:

Using this option will result in all three servers using host addresses on different broadcast domains.

Question No : 179 - (Topic 1)

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

Explanation:

PAT would ensure that computers on ABC's LAN translate to the same IP address, but with a different port number assignment. The log information shows the IP address, not the port number, making it impossible to pin point the exact source.

Question No : 180 - (Topic 1)

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

Explanation:

Layered security is the practice of combining multiple mitigating security controls to protect resources and data.

Topic 2, Compliance and Operational Security

Question No : 181 - (Topic 2)

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

A. Installing anti-malware
B. Implementing an IDS
C. Taking a baseline configuration
D. Disabling unnecessary services

Answer: D

Explanation:

Preventive controls are to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred. By disabling all unnecessary services you would be reducing the attack surface because then there is less opportunity for risk incidents to happen. There are many risks with having many services enabled since a service can provide an attack vector that someone could exploit against your system. It is thus best practice to enable only those services that are absolutely required.

Question No : 182 - (Topic 2)

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

Explanation:

Internal account auditing will allow you to switch the appropriate users to the proper accounts required after the switching of roles occurred and thus check that the principle of least privilege is followed.

Question No : 183 - (Topic 2)

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

Explanation:

Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

Question No : 184 - (Topic 2)

Digital certificates can be used to ensure which of the following? (Select TWO).

A. Availability
B. Confidentiality
C. Verification
D. Authorization
E. Non-repudiation

Answer: B,E

Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. Digital certificates refer to cryptography which is mainly concerned with Confidentiality, Integrity, Authentication, Nonrepudiation and Access Control. Nonrepudiation prevents one party from denying actions they carried out.

Question No : 185 - (Topic 2)

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. Full disk encryption
C. Data retention policies
D. Disk wiping procedures
E. Removable media encryption

Answer: B,D

Explanation:

B: Full disk encryption is when the entire volume is encrypted; the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption.

D: Disk wiping is the process of overwriting data on the repeatedly, or using a magnet to alter the magnetic structure of the disks. This renders the data unreadable.

Question No : 186 - (Topic 2)

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

Explanation:

Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage.

Question No : 187 - (Topic 2)

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

Explanation:

There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation. This is a more effective way of controlling temperature to safeguard your equipment in a data center.

Question No : 188 - (Topic 2)

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

Explanation:

Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it. Residual risk is always present and will remain a risk thus it should be accepted (risk acceptance)

Question No : 189 - (Topic 2)

A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company $4,000 with downtime costing $3,000. Which of the following is the ALE for the company?

A. $7,000
B. $10,000
C. $17,500

D. $35,000

Answer: C

Explanation:

SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

SLE =($4000 + $3000) x 5 = $35000

ARO = 2 years Thus per year it would be 50% = 0,5

The ALE is thus $35000 x 0.5 = $17500

Question No : 190 - (Topic 2)

Which of the following provides the BEST application availability and is easily expanded as demand grows?

A. Server virtualization
B. Load balancing
C. Active-Passive Cluster
D. RAID 6

Answer: B

Explanation:

Load balancing is a way of providing high availability by splitting the workload across multiple computers.

Question No : 191 - (Topic 2)

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

Explanation:

With sending your data to a third party is already a risk since the third party may have a different policy than yours. Data ownership and non-disclosure is already a risk that you will have to accept since the data will be sent for debugging /troubleshooting purposes which will result in definite disclosure of the data.

Question No : 192 - (Topic 2)

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

Explanation:

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you’re open to dispute about possible evidence tampering.

Question No : 193 - (Topic 2)

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

Explanation:

A policy that states employees should use their vacation time in a staggered schedule is a way of employing mandatory vacations. A mandatory vacation policy requires all users to take time away from work while others step in and do the work of that employee on vacation. This will afford the CSO the opportunity to see who is using the company assets responsibly and who is abusing it.

Question No : 194 - (Topic 2)

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

Explanation:

Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up banners) that appear before the login telling similar information—authorized access only, violators will be prosecuted, and so forth. Such banners convey warnings or regulatory information to the user that they must “accept” in order to use the machine or network. You need to make staff aware that they may legally be prosecuted and a message is best given via a banner so that all staff using workstation will get notification.

Question No : 195 - (Topic 2)

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

A. Warm site
B. Load balancing
C. Clustering
D. RAID

Answer: C

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy.

Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

Question No : 196 - (Topic 2)

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

Explanation:

Change management is the structured approach that is followed to secure a company's assets. Promoting code to application on a SMZ web server would be change management.

Question No : 197 - (Topic 2)

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

Explanation:

A system image would be a snapshot of what exists at the moment. Thus capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

Question No : 198 - (Topic 2)

A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

A. High availability
B. Load balancing
C. Backout contingency plan
D. Clustering

Answer: A

Explanation:

High availability (HA) refers to the measures used to keep services and systems operational during an outage. In short, the goal is to provide all services to all users, where they need them and when they need them. With high availability, the goal is to have key services available 99.999 percent of the time (also known as five nines availability).

Question No : 199 - (Topic 2)

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

Explanation:

Containment strategies is used to limit damages, contain a loss so that it may be controlled, much like quarantine, and loss incident isolation.

Question No : 200 - (Topic 2)

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

Explanation:

EMI can cause circuit overload, spikes, or even electrical component failure. In the question it is mentioned that switch degradation occurs when the building’s roof air-conditioning system is also running. All electromechanical systems emanate EMI. Thus you could alleviate the problem using EMI shielding.

Question No : 201 - (Topic 2)

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

Explanation:

Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means. Furthermore best practices are applied to all aspects in the work environment.

Question No : 202 - (Topic 2)

Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

A. Clustering
B. RAID
C. Load balancing
D. Virtualization

Answer: A

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

Question No : 203 - (Topic 2)

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

Explanation:

Jabber is a new unified communications application and could possible expose you to attackers that want to capture conversations because Jabber provides a single interface across presence, instant messaging, voice, video messaging, desktop sharing and conferencing.

Question No : 204 - (Topic 2)

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

Explanation:

dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. dd can duplicate data across files, devices, partitions and volumes

On Unix, device drivers for hardware (such as hard disks) and special device files (such as /dev/zero and /dev/random) appear in the file system just like normal files; dd can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The dd program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from the ASCII and EBCDIC text encodings.

An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size.

Question No : 205 - (Topic 2)

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

Explanation:

A: Take Hashes. NIST (the National Institute of Standards and Technology) maintains a National Software Reference Library (NSRL). One of the purposes of the NSRL is to collect "known, traceable software applications" through their hash values and store them in a Reference Data Set (RDS). The RDS can then be used by law enforcement, government agencies, and businesses to determine which files are important as evidence in criminal investigations.

D: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

Question No : 206 - (Topic 2)

Which of the following is the BEST concept to maintain required but non-critical server availability?

A. SaaS site
B. Cold site
C. Hot site
D. Warm site

Answer: D

Explanation:

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. Another term for a warm site/reciprocal site is active/active model.

Question No : 207 - (Topic 2)

Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a $5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server?

A. $500
B. $5,000
C. $25,000
D. $50,000

Answer: B

Explanation:

SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

(5000 x 10) x 0.1 = 5000

Question No : 208 - (Topic 2)

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

Explanation:

The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical.

Question No : 209 - (Topic 2)

Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device’s removable media in the event that the device is lost or stolen?

A. Hashing
B. Screen locks
C. Device password
D. Encryption

Answer: D

Explanation:

Encryption is used to ensure the confidentiality of information.

Question No : 210 - (Topic 2)

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

Explanation:

Encryption is done to protect confidentiality and integrity of data. It also provides authentication, nonrepudiation and access control to the data. Since all emails go through a DLP scanner and it is outgoing main that requires protection then the best option is to put a system in place that will encrypt the outgoing emails automatically.

Question No : 211 - (Topic 2)

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

Explanation:

Threats X vulnerability X asset value is equal to asset value (AV) times exposure factor (EF). This is used to calculate a risk.

Question No : 212 - (Topic 2)

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 all traffic destined for ports 80 and 443.

Answer: B

Explanation:

A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data.

Question No : 213 - (Topic 2)

When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.
B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
C. Developed recovery strategies, test plans, post-test evaluation and update processes.
D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.
E. Methods to review and report on system logs, incident response, and incident handling.

Answer: A,B

Explanation:

A: External emergency communications that should fit into your business continuity plan include notifying family members of an injury or death, discussing the disaster with the media, and providing status information to key clients and stakeholders. Each message needs to be prepared with the audience (e.g., employees, media, families, government regulators) in mind; broad general announcements may be acceptable in the initial aftermath of an incident, but these will need to be tailored to the audiences in subsequent releases.

B: A typical emergency communications plan should be extensive in detail and properly planned by a business continuity planner. Internal alerts are sent using either email, overhead building paging systems, voice messages or text messages to cell/smartphones with instructions to evacuate the building and relocate at assembly points, updates on the status of the situation, and notification of when it's safe to return to work.

Question No : 214 - (Topic 2)

Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.

B. The website is using a wildcard certificate issued for the company's domain.

C. HTTPS://127.0.01 was used instead of HTTPS://localhost.

D. The website is using an expired self signed certificate.

Answer: C

Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. In typical public key infrastructure (PKI) arrangements, a digital signature from a certificate authority (CA) attests that a particular public key certificate is valid (i.e., contains correct information). Users, or their software on their behalf, check that the private key used to sign some certificate matches the public key in the CA's certificate. Since CA certificates are often signed by other, "higher-ranking," CAs, there must necessarily be a highest CA, which provides the ultimate in attestation authority in that particular PKI scheme.

Localhost is a hostname that means this computer and may be used to access the computer's own network services via its loopback network interface. Using the loopback interface bypasses local network interface hardware. In this case the HTTPS://127.0.01 was used and not HTTPS//localhost

Question No : 215 - (Topic 2)

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing
B. RAID
C. A cold site
D. A host standby

Answer: B

Explanation:

Fault tolerance is the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves overengineering systems by adding redundant components and subsystems. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

Question No : 216 - (Topic 2)

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

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Described in the question is a situation where a security breach had occurred and its response which shows that lessons have been learned and used to put in place measures that will prevent any future security breaches of the same kind.

Question No : 217 - (Topic 2)

Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

A. Structured walkthrough
B. Full Interruption test
C. Checklist test
D. Tabletop exercise

Answer: A

Explanation:

A structured walkthrough test of a recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required.

Question No : 218 - (Topic 2)

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 all 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

Explanation:

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

Question No : 219 - (Topic 2)

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

Explanation:

incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). The events that could occur include security breaches.

Question No : 220 - (Topic 2)

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive’s laptop they notice several pictures of the employee’s pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

A. Social engineering
B. Steganography
C. Hashing
D. Digital signatures

Answer: B

Explanation:

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Question No : 221 - (Topic 2)

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

Explanation:

MOU or Memorandum of Understanding is a document outlining which party is responsible for what portion of the work.

Question No : 222 - (Topic 2)

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

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that there is differentiation between users, employees and duties per se which form part of best practices.

Question No : 223 - (Topic 2)

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

Explanation:

Every step in an incident response should be documented, including every action taken by end users and the incident-response team.

Question No : 224 - (Topic 2)

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

A. Hashing
B. Stream ciphers
C. Steganography
D. Block ciphers

Answer: A

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way – it is not reversible.

Question No : 225 - (Topic 2)

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

Explanation:
Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

Question No : 226 - (Topic 2)

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

Explanation:
Video surveillance is making use of a camera, or CCTV that is able to record everything it sees and is always running. This way you will be able to check exactly who enters secure

areas.

Question No : 227 - (Topic 2)

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

Explanation:

A backout (regression testing) is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout.
A change control policy refers to the structured approach that is followed to secure a company's assets in the event of changes occurring.

Question No : 228 - (Topic 2)

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

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case 'scheduled system patching'.

Question No : 229 - (Topic 2)

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

A. Availability
B. Integrity
C. Accounting
D. Confidentiality

Answer: B

Explanation:

Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring nonrepudiation via digital signatures supports integrity.

Question No : 230 - (Topic 2)

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

Explanation:

Zero-Day Exploits begin exploiting holes in any software the very day it is discovered. It is very difficult to respond to a zero-day exploit. Often, the only thing that you as a security administrator can do is to turn off the service. Although this can be a costly undertaking in terms of productivity, it is the only way to keep the network safe. In this case you want to check if the executable file is malicious. Since a baseline represents a secure state is would be possible to check the nature of the executable file in an isolated environment against the OS baseline.

Question No : 231 - (Topic 2)

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

Explanation:

Aspects such as fencing, proper lighting, locks, CCTV, Escape plans Drills, escape routes and testing controls form part of safety controls.
Integrity refers to aspects such as hashing, digital signatures, certificates and non-repudiation – all of which has to do with data integrity.

Question No : 232 - (Topic 2)

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

A. Recipient’s private key
B. Sender’s public key
C. Recipient’s public key
D. Sender’s private key

Answer: B

Explanation:

When the sender wants to send a message to the receiver. It’s important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender’s public key to verify the sender’s identity.

Question No : 233 - (Topic 2)

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

Explanation:

The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

Two numbers follow the keyword VTY because there is more than one VTY line for router access. The default number of lines is five on many Cisco routers. Here, I’m configuring one password for all terminal (VTY) lines. I can specify the actual terminal or VTY line numbers as a range. The syntax that you’ll see most often, vty 0 4, covers all five terminal access lines.

Question No : 234 - (Topic 2)

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

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data.

Question No : 235 - (Topic 2)

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

Explanation:

FM200 is a gas and the principle of a gas system is that it displaces the oxygen in the room, thereby removing this essential component of a fi re. in a data center is is the preferred choice of fire suppressant.

Question No : 236 - (Topic 2)

Environmental control measures include which of the following?

A. Access list
B. Lighting
C. Motion detection
D. EMI shielding

Answer: D

Explanation:

Environmental controls include HVAC, Fire Suppression, EMI Shielding, Hot and Cold Aisles, Environmental monitoring as well as Temperature and Humidity controls.

Question No : 237 - (Topic 2)

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

A. Integrity of downloaded software.
B. Availability of the FTP site.
C. Confidentiality of downloaded software.
D. Integrity of the server logs.

Answer: A

Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

Question No : 238 - (Topic 2)

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. Tell 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

Explanation:

Since the application is violating the security policy it should be coded differently to comply with the password policy.

Question No : 239 - (Topic 2)

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

A. To allow load balancing for cloud support
B. To allow for business continuity if one provider goes out of business
C. To eliminate a single point of failure
D. To allow for a hot site in case of disaster
E. To improve intranet communication speeds

Answer: B,C

Explanation:

A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.

Note: Recovery Time Objective

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during BIA creation.

Question No : 240 - (Topic 2)

A company recently experienced data loss when a server crashed due to a midday power outage.

Which of the following should be used to prevent this from occurring again?

A. Recovery procedures
B. EMI shielding
C. Environmental monitoring
D. Redundancy

Answer: D

Explanation:

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction (in this case a power outage). Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored.

Question No : 241 - (Topic 2)

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

Explanation:

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

Question No : 242 - (Topic 2)

Which of the following would a security administrator use to verify the integrity of a file?

A. Time stamp
B. MAC times
C. File descriptor
D. Hash

Answer: D

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and it is a one-way transformation in order to validate the integrity of data.

Question No : 243 - (Topic 2)

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

Explanation:

Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category.

Question No : 244 - (Topic 2)

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

Explanation:

With a false negative, you are not alerted to a situation when you should be alerted.

Question No : 245 - (Topic 2)

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

Explanation:

With employees who want to bring their own devices you will have to make them understand why they cannot. You do not want them plugging in a flash drive, let alone a camera, smartphone, tablet computer, or other device, on which company files could get intermingled with personal files. Allowing this to happen can create situations where data can leave the building that shouldn't as well as introduce malware to the system.
Employees should not sync unauthorized smartphones to their work systems. Some smartphones use multiple wireless spectrums and unwittingly open up the possibility for an attacker in the parking lot to gain access through the phone to the internal network. Thus if you do not have controls in place then your network is definitely at risk.

Question No : 246 - (Topic 2)

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

Explanation:

A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can prevent the two members from colluding to steal the information that they have access to.

Question No : 247 - (Topic 2)

Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

A. Use hardware already at an offsite location and configure it to be quickly utilized.
B. Move the servers and data to another part of the company's main campus from the server room.
C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Answer: A

Explanation:

A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement.
Warm sites may be for your exclusive use, but they don't have to be. A warm site requires more advanced planning, testing, and access to media for system recovery. Warm sites represent a compromise between a hot site, which is very expensive, and a cold site, which

isn’t preconfigured.

Question No : 248 - (Topic 2)

Customers’ credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

A. Application firewalls
B. Manual updates
C. Firmware version control
D. Encrypted TCP wrappers

Answer: D

Explanation:

Wrapping sensitive systems with a specific control is required when protecting data in transit. TCP wrappers are also security controls. TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or inetd query replies, to be used as tokens on which to filter for access control purposes.

TCP Wrapper should not be considered a replacement for a properly configured firewall. Instead, TCP Wrapper should be used in conjunction with a firewall and other security enhancements in order to provide another layer of protection in the implementation of a security policy.

Question No : 249 - (Topic 2)

Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO).

A. DAC
B. ALE
C. SLE
D. ARO

E. ROI

Answer: B,C

Explanation:

ALE (Annual Loss Expectancy) is equal to the SLE (Single Loss Expectancy) times the annualized rate of occurrence. SLE (Single Loss Expectancy) is equal to asset value (AV) times exposure factor (EF).

Question No : 250 - (Topic 2)

Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

A. A disk-based image of every computer as they are being replaced.
B. A plan that skips every other replaced computer to limit the area of affected users.
C. An offsite contingency server farm that can act as a warm site should any issues appear.
D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

Answer: D

Explanation:

A backout is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied.

Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout.

Question No : 251 - (Topic 2)

The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter
B. Geographically disparate site redundant datacenter
C. Localized clustering of the datacenter
D. Cold site implementation for the datacenter

Answer: B

Explanation:

Data backups, redundant systems, and disaster recovery plans all support availability. AN in this case a geographically disparate site redundant datacenter represents 100% availability regardless of whether a disaster event occurs.

Question No : 252 - (Topic 2)

Which of the following may significantly reduce data loss if multiple drives fail at the same time?

A. Virtualization
B. RAID
C. Load balancing
D. Server clustering

Answer: B

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

Question No : 253 - (Topic 2)

A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peak shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department with the BEST solution?

A. Attach cable locks to each laptop
B. Require each customer to sign an AUP

C. Install a GPS tracking device onto each laptop
D. Install security cameras within the perimeter of the café

Answer: A

Explanation:

All laptop cases include a built-in security slot in which a cable lock can be inserted to prevent it from easily being removed from the premises.

Question No : 254 - (Topic 2)

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

Explanation:

Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security and web browser security, leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts.

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person’s name to a fingerprint (think biometrics), credit card number, or patient record.

Thus a PII handling policy can be used to protect data.

Question No : 255 - (Topic 2)

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

A. Succession planning
B. Disaster recovery plan

C. Information security plan
D. Business impact analysis

Answer: B

Explanation:

A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

Question No : 256 - (Topic 2)

The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

A. TwoFish
B. SHA-512
C. Fuzzy hashes
D. HMAC

Answer: C

Explanation:

Hashing is used to ensure that a message has not been altered. It can be useful for positively identifying malware when a suspected file has the same hash value as a known piece of malware. However, modifying a single bit of a malicious file will alter its hash value. To counter this, a continuous stream of hash values is generated for rolling block of code. This can be used to determine the similarity between a suspected file and known pieces of malware.

Question No : 257 - (Topic 2)

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

Explanation:

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

Question No : 258 - (Topic 2)

A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company $1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating?

A. Succession plan
B. Continuity of operation plan
C. Disaster recovery plan
D. Business impact analysis

Answer: D

Explanation:

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

Question No : 259 - (Topic 2)

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

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person’s name to a fingerprint (think biometrics), credit card number, or patient record. This has a direct relation to customer privacy considerations.

Question No : 260 - (Topic 2)

Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

A. Email Encryption
B. Steganography
C. Non Repudiation
D. Access Control

Answer: C

Explanation:

Nonrepudiation prevents one party from denying actions they carried out.

Question No : 261 - (Topic 2)

Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE).

A. Authentication
B. Data leakage
C. Compliance
D. Malware
E. Non-repudiation

F. Network loading

Answer: B,C,D

Explanation:

In a joint enterprise, data may be combined from both organizations. It must be determined, in advance, who is responsible for that data and how the data backups will be managed. Data leakage, compliance and Malware issues are all issues concerning data ownership and backup which are both impacted on by corporate IM.

Question No : 262 - (Topic 2)

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

Explanation:

Social networking and having you company's application authentication 'linked' to users' credential that they use on social media sites exposes your company's application exponentially more than is necessary. You should strive to practice risk avoidance.

Question No : 263 - (Topic 2)

Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

A. Confidentiality
B. Compliance
C. Integrity
D. Availability

Answer: C

Explanation:

Integrity means the message can’t be altered without detection.

Question No : 264 - (Topic 2)

A network administrator has recently updated their network devices to ensure redundancy is in place so that:

A. switches can redistribute routes across the network.
B. environmental monitoring can be performed.
C. single points of failure are removed.
D. hot and cold aisles are functioning.

Answer: C

Explanation:

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction. The best way to remove an SPOF from your environment is to add redundancy.

Question No : 265 - (Topic 2)

A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

A. Integrity
B. Availability
C. Confidentiality
D. Safety

Answer: D

Explanation:

Fencing is used to increase physical security and safety. Locks are used to keep those who are unauthorized out.

Question No : 266 - (Topic 2)

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

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person’s name to a fingerprint (think biometrics), credit card number, or patient record. Employees should be made aware of this type of attack by means of training.

Question No : 267 - (Topic 2)

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

Explanation:

Social Networking Dangers are ‘amplified’ in that social media networks are designed to mass distribute personal messages. If an employee reveals too much personal information it would be easy for miscreants to use the messages containing the personal information to work out possible passwords.

Question No : 268 - (Topic 2)

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

Explanation:

The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations.

Question No : 269 - (Topic 2)

A company replaces a number of devices with a mobile appliance, combining several functions.

Which of the following descriptions fits this new implementation? (Select TWO).

A. Cloud computing
B. Virtualization
C. All-in-one device
D. Load balancing
E. Single point of failure

Answer: C,E

Explanation:

The disadvantages of combining everything into one include a potential single point of failure, and the dependence on the one vendor. The all –in-one device represents a single point of failure risk being taken on.

Question No : 270 - (Topic 2)

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

Explanation:

Clean Desk Policy Information on a desk—in terms of printouts, pads of note paper, sticky notes, and the like—can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This will mitigate the risk of data loss when applied.

Question No : 271 - (Topic 2)

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

Explanation:

When one person fills in for another, such as for mandatory vacations, it provides an opportunity to see what the person is doing and potentially uncover any fraud.

Question No : 272 - (Topic 2)

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, reinstall the OS from most current backup and only restore the data that was not compromised.

Answer: A

Explanation:

Rootkits are software programs that have the ability to hide certain things from the operating system. With a rootkit, there may be a number of processes running on a system that do not show up in Task Manager or connections established or available that do not appear in a netstat display—the rootkit masks the presence of these items. The rootkit is able to do this by manipulating function calls to the operating system and filtering out information that would normally appear. Theoretically, rootkits could hide anywhere that there is enough memory to reside: video cards, PCI cards, and the like. The best way to handle this situation is to wipe the server and reinstall the operating system with the original installation disks and then restore the extracted data from your last known good backup. This way you can eradicate the rootkit and restore the data.

Question No : 273 - (Topic 2)

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

Explanation:

Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

Question No : 274 - (Topic 2)

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Select TWO).

A. The CA's public key
B. Joe's private key
C. Ann's public key
D. The CA's private key
E. Joe's public key
F. Ann's private key

Answer: A,E

Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. This process provides message integrity, nonrepudiation, and authentication.

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual.

If Joe wants to send Ann an encrypted e-mail, there should be a mechanism to verify to Ann that the message received from Mike is really from Joe. If a third party (the CA) vouches for Joe and Ann trusts that third party, Ann can assume that the message is authentic because the third party says so.

Question No : 275 - (Topic 2)

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

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Developing and updating all internal operating and standard operating procedures documentation to handle future incidents is preparation.

Question No : 276 - (Topic 2)

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

Explanation:

Confidentiality, integrity, and availability are the three most important concepts in security. Thus they form the security triangle.

Question No : 277 - (Topic 2)

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

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Date of birth is personally identifiable information.

Question No : 278 - (Topic 2)

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

Explanation:

Mandatory vacations also provide an opportunity to discover fraud apart from the obvious benefits of giving employees a chance to refresh and making sure that others in the company can fill those positions and make the company less dependent on those persons; a sort pf replication and duplication at all levels.

Question No : 279 - (Topic 2)

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. Firewall
C. Hardware locks
D. Environmental monitoring

Answer: C

Explanation:

Hardware security involves applying physical security modifications to secure the system(s) and preventing them from leaving the facility. Don’t spend all of your time worrying about intruders coming through the network wire while overlooking the obvious need for physical security. Hardware security involves the use of locks to prevent someone from picking up and carrying out your equipment.

Question No : 280 - (Topic 2)

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

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company’s assets. Thus the actual switch configuration should first be subject to the change management approval.

Question No : 281 - (Topic 2)

Which of the following provides the LEAST availability?

A. RAID 0
B. RAID 1
C. RAID 3
D. RAID 5

Answer: A

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID 0 is disk striping. It uses multiple drives and maps them together as a single physical drive. This is done primarily for performance, not for fault tolerance. If any drive in a RAID 0 array fails, the entire logical drive becomes unusable.

Question No : 282 - (Topic 2)

Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

A. Hot site
B. Warm site
C. Cold site
D. Mobile site

Answer: D

Explanation:

Not having a dedicated site means that the mobile site can fill the role of either being a hot, warm or cold site as a disaster recovery measure.

Question No : 283 - (Topic 2)

A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

A. Authentication
B. Integrity
C. Confidentiality
D. Availability

Answer: D

Explanation:

Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability.

Question No : 284 - (Topic 2)

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

Explanation:

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

Question No : 285 - (Topic 2)

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

Explanation:

Mounting the drive in read-only mode will prevent any executable commands from being executed. This is turn will have the least impact on potential evidence using the drive in question.

Question No : 286 - (Topic 2)

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

Explanation:

Blocking e-mail is the same as preventing the receipt of those e-mails and this is done by applying a filter. But the filter must be configured to block it. Thus you should add that specific domain from where the e-mails are being sent to the list of addresses that is to be blocked.

Question No : 287 - (Topic 2)

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

Explanation:

Data that is not kept separate or segregated will impact on that data’s confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root-level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database. Data segregation is crucial; keep your data on secure servers.

Question No : 288 - (Topic 2)

In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

A. Business Impact Analysis
B. IT Contingency Plan
C. Disaster Recovery Plan
D. Continuity of Operations

Answer: A

Explanation:

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn’t concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

Question No : 289 - (Topic 2)

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

A. Steganography
B. Hashing

C. Encryption
D. Digital Signatures

Answer: D

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Question No : 290 - (Topic 2)

An advantage of virtualizing servers, databases, and office applications is:

A. Centralized management.
B. Providing greater resources to users.
C. Stronger access control.
D. Decentralized management.

Answer: A

Explanation:

Virtualization consists of allowing one set of hardware to host multiple virtual Machines and in the case of software and applications; one host is all that is required. This makes centralized management a better prospect.

Question No : 291 - (Topic 2)

Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

A. Warm site
B. Hot site
C. Cold site
D. Co-location site

Answer: B

Explanation:

A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. Databases can be kept up-to-date using network connections. These types of facilities are expensive, and they're primarily suitable for short-term situations.

Question No : 292 - (Topic 2)

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

Explanation:

Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability; as does environmental support by means of HVAC.

Question No : 293 - (Topic 2)

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

Explanation:

A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

Question No : 294 - (Topic 2)

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

Explanation:

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job and in this way the company can potentially uncover any fraud perhaps committed by the incumbent.

Question No : 295 - (Topic 2)

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

Explanation:

This is an incident that has to be responded to by the person who discovered it- in this case the user. An incident is any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. It’s important that an incident response policy establish at least the following items:
Outside agencies that should be contacted or notified in case of an incident
Resources used to deal with an incident
Procedures to gather and secure evidence
List of information that should be collected about an incident
Outside experts who can be used to address issues if needed
Policies and guidelines regarding how to handle an incident

Since the spec sheet has been marked Internal Proprietary Information the user should refer the incident to the incident response team.

Question No : 296 - (Topic 2)

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

Explanation:

The Memorandum of Understanding This document is used in many settings in the information industry. It is a brief summary of which party is responsible for what portion of the work. For example, Company A may be responsible for maintaining the database server and Company B may be responsible for telecommunications. MOUs are not legally binding but they carry a degree of seriousness and mutual respect, stronger than a gentlemen’s agreement. Often, MOUs are the first steps towards a legal contract.

Question No : 297 - (Topic 2)

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

Explanation:

A least privilege policy is to give users only the permissions that they need to do their work and no more. That is only allowing security administrators to be able to make changes to the firewall by practicing the least privilege principle.

Question No : 298 - (Topic 2)

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

Explanation:

EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. Thus all wiring should be shielded to mitigate data theft.

Question No : 299 - (Topic 2)

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

Explanation:

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock.

Question No : 300 - (Topic 2)

After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

A. Fencing
B. Proximity readers
C. Video surveillance
D. Bollards

Answer: D

Explanation:

To stop someone from entering a facility, barricades or gauntlets can be used. These are often used in conjunction with guards, fencing, and other physical security measures. Bollards are physical barriers that are strong enough to withstand impact with a vehicle.

Question No : 301 - (Topic 2)

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

Explanation:

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what results in the false positives.

Question No : 302 - (Topic 2)

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

Explanation:

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

Question No : 303 - (Topic 2)

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

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. In this scenario the security officer is carrying out an incident response measure that will address and be of benefit to those in the vanguard, i.e. the employees and they are the first responders.

Question No : 304 - (Topic 2)

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

Explanation:

An example of OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Of the options stated in the question the hard drive would be the least volatile.

Question No : 305 - (Topic 2)

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

Explanation:

Banner, or header information messages sent with data to find out about the system(s) does happen. Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it.

Question No : 306 - (Topic 2)

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

Explanation:

Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to $30,000 and it is better to save $5,000.

Question No : 307 - (Topic 2)

Which of the following provides data the best fault tolerance at the LOWEST cost?

A. Load balancing
B. Clustering
C. Server virtualization
D. RAID 6

Answer: D

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software thus representing the lowest cost option.

Question No : 308 - (Topic 2)

Certificates are used for: (Select TWO).

A. Client authentication.
B. WEP encryption.
C. Access control lists.
D. Code signing.
E. Password hashing.

Answer: A,D

Explanation:

Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication.

Question No : 309 - (Topic 2)

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

Explanation:

Education and training with regard to Information Security Awareness will reduce the risk of data leaks and as such forms an integral part of Security Awareness. By employing social engineering data can be leaked by employees and only when company users are made aware of the methods of social engineering via Information Security Awareness Training, you can reduce the risk of data leaks.

Question No : 310 - (Topic 2)

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

Explanation:

Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).

Question No : 311 - (Topic 2)

A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.

Which of the following is occurring?

A. The user is encrypting the data in the outgoing messages.
B. The user is using steganography.
C. The user is spamming to obfuscate the activity.
D. The user is using hashing to embed data in the emails.

Answer: B

Explanation:

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Question No : 312 - (Topic 2)

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

A. Confidentiality
B. Availability
C. Succession planning
D. Integrity

Answer: B

Explanation:

Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability.

Question No : 313 - (Topic 2)

Digital signatures are used for ensuring which of the following items? (Select TWO).

A. Confidentiality
B. Integrity
C. Non-Repudiation

D. Availability
E. Algorithm strength

Answer: B,C

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party ‘vouches’ for the individuals in the two-key system. Thus non-repudiation also impacts on integrity.

Question No : 314 - (Topic 2)

Key elements of a business impact analysis should include which of the following tasks?

A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

Answer: D

Explanation:

The key components of a Business impact analysis (BIA) include:

Identifying Critical Functions

Prioritizing Critical Business Functions

Calculating a Timeframe for Critical Systems Loss

Estimating the Tangible and Intangible Impact on the Organization

Question No : 315 - (Topic 2)

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

Explanation:

Mobile devices, such as laptops, tablet computers, and smartphones, provide security challenges above those of desktop workstations, servers, and such in that they leave the office and this increases the odds of their theft which makes data security a real concern. At a bare minimum, the following security measures should be in place on mobile devices: Screen lock, Strong password, Device encryption, Remote Wipe or Sanitation, voice encryption, GPS tracking, Application control, storage segmentation, asses tracking and device access control.

Question No : 316 - (Topic 2)

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

Answer: A

Explanation:

A guard can be intimidating and respond to a situation and in a case where you want to limit an individual’s access to a sensitive area a guard would be the most effective.

Question No : 317 - (Topic 2)

A security administrator is reviewing the company’s continuity plan. The plan specifies an

RTO of six hours and RPO of two days. Which of the following is the plan describing?

A. Systems should be restored within six hours and no later than two days after the incident.
B. Systems should be restored within two days and should remain operational for at least six hours.
C. Systems should be restored within six hours with a minimum of two days worth of data.
D. Systems should be restored within two days with a minimum of six hours worth of data.

Answer: C

Explanation:

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still to be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during the business impact analysis (BIA) creation. The recovery point objective (RPO) is similar to RTO, but it defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). As a general rule, the closer the RPO matches the item of the crash, the more expensive it is to obtain.

Question No : 318 - (Topic 2)

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

Explanation:

This is a risk acceptance measure that has to be implemented since the cost of patching would be too high compared to the cost to keep the system going as is. Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices (i.e. risk deterrence, mitigation, transference or avoidance) exceeds the value of the harm that would occur if the risk came to fruition.

Question No : 319 - (Topic 2)

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

Explanation:

Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. User permissions may be the most basic aspect of security and is best coupled with a principle of least privilege. And related to permissions is the concept of the access control list (ACL). An ACL is literally a list of who can access what resource and at what level. Thus the best risk mitigation steps insofar as access control rights are concerned, is the regular/routine review of user permissions.

Question No : 320 - (Topic 2)

A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

A. Clustering
B. Mirrored server
C. RAID
D. Tape backup

Answer: C

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

Question No : 321 - (Topic 2)

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

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

Question No : 322 - (Topic 2)

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

Explanation:

Separation of duties means that there is differentiation between users, employees and duties per se which form part of best practices.

Question No : 323 - (Topic 2)

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

Explanation:

After you have implemented security controls based on risk, you must perform routine audits. These audits should include reviews of user rights and permissions as well as specific events. You should pay particular attention to false positives and negatives.

Question No : 324 - (Topic 2)

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

Explanation:

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. This should be prevented in this case.

Question No : 325 - (Topic 2)

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

Explanation:
A job rotation policy defines intervals at which employees must rotate through positions.

Question No : 326 - (Topic 2)

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

Explanation:
Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock. Most environmental systems also regulate humidity; however, a malfunctioning system can cause the humidity to be almost entirely extracted from a room. Make sure that environmental systems are regularly serviced. Electrostatic damage can

occur when humidity levels get too low. Condensation is a direct result from failed humidity levels.

Question No : 327 - (Topic 2)

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

Explanation:

Mantraps are designed to contain an unauthorized, potentially hostile person/individual physically until authorities arrive. Mantraps are typically manufactured with bulletproof glass, high-strength doors, and locks and to allow the minimal amount of individuals depending on its size. Some mantraps even include scales that will weigh the person. The doors are designed in such a way as to open only when the mantrap is occupied or empty and not in-between. This means that the backdoor must first close before the front door will open. Mantraps are in most cases also combined with guards. This is the most physical protection any one measure will provide.

Question No : 328 - (Topic 2)

An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

A. CRL
B. Non-repudiation
C. Trust models
D. Recovery agents

Answer: B

Explanation:

Nonrepudiation prevents one party from denying actions they carried out. This means that the identity of the email sender will not be repudiated.

Question No : 329 - (Topic 2)

Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment
B. Business impact analysis
C. Risk management framework
D. Quantitative risk assessment

Answer: D

Explanation:

Quantitative analysis / assessment is used to the show the logic and cost savings in replacing a server for example before it fails rather than after the failure. Quantitative assessments assign a dollar amount.

Question No : 330 - (Topic 2)

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

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more.

Question No : 331 - (Topic 2)

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

Explanation:

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you’re open to dispute about possible evidence tampering. Thus to preserve evidence during a forensic procedure the chain of custody is of utmost importance.

Question No : 332 - (Topic 2)

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

Explanation:

ISA/ Interconnection Security Agreement is an agreement between two organizations that have connected systems. The agreement documents the technical requirements of the connected systems.

Question No : 333 - (Topic 2)

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

Explanation:

Clean Desk Policy Information on a desk—in terms of printouts, pads of note paper, sticky notes, and the like—can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

Question No : 334 - (Topic 2)

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

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. DLP systems share commonality with network intrusion prevention systems. Endpoint protection provides security and management over both physical and virtual environments.

Question No : 335 - (Topic 2)

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

Explanation:

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

Question No : 336 - (Topic 2)

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

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Encryption is used to protect data.

Question No : 337 - (Topic 2)

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

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. These categories make applying the appropriate policies and security controls practical.

Question No : 338 - (Topic 2)

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. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full 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

Explanation:

A full backup is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it's performed. Once a full backup is made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some files may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system.

An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small.

Question No : 339 - (Topic 2)

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

Explanation:

Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions. Also reviewing user rights and permissions will afford the security analyst the opportunity to put the principle of least privilege in practice as well as update the security policy

Question No : 340 - (Topic 2)

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

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. A USB presents the most likely device to be used to steal data because of its physical size.

Question No : 341 - (Topic 2)

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

Explanation:

Using a safe and locking cabinets to protect backup media, documentation, and any other physical artifacts that could do harm if they fell into the wrong hands would form part of keeping employees desks clean as in a clean desk policy.

Question No : 342 - (Topic 2)

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

Explanation:

Mantraps make use of electronic locks and are designed to allow you to limit the amount of individual allowed access to an area at any one time.

Question No : 343 - (Topic 2)

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

Explanation:

A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more.

Question No : 344 - (Topic 2)

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

Explanation:

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. Many social engineering intruders needing physical access to a site will use this method of gaining entry. Educate users to beware of this and other social engineering ploys and prevent them from happening.

Question No : 345 - (Topic 2)

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

Explanation:

A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed – as in this case the cameras were already there, it just had to be adjusted to perform its function as intended.

Question No : 346 - (Topic 2)

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

Explanation:

Ideally, a security awareness training program for the entire organization should cover the following areas:

Importance of security

Responsibilities of people in the organization

Policies and procedures

Usage policies

Account and password-selection criteria

Social engineering prevention

You can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk.

Question No : 347 - (Topic 2)

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

Explanation:

The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned.

Question No : 348 - (Topic 2)

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

A. The CA's public key
B. Ann's public key
C. Joe's private key
D. Ann's private key
E. The CA's private key
F. Joe's public key

Answer: D,F

Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn’t been tampered with and the originator is verified as the person they claim to be.

Question No : 349 - (Topic 2)

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

Explanation:

Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. In this case you are experiencing intermittent connectivity since Electro Magnetic Interference (EMI) was not taken into account when running the cables over fluorescent lighting.

Question No : 350 - (Topic 2)

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

A. Clustering
B. RAID
C. Backup Redundancy
D. Cold site

Answer: A

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.

Question No : 351 - (Topic 2)

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

Explanation:

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

Question No : 352 - (Topic 2)

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

Explanation:

Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state.

Question No : 353 - (Topic 2)

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

Explanation:

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job.

Question No : 354 - (Topic 2)

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

Explanation:

A guard can be instructed to deny access until authentication has occurred will address the situation adequately.

Question No : 355 - (Topic 2)

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

Explanation:

RFID is radio frequency identification that works with readers that work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read. Fitting out the equipment with RFID will allow you to provide automated notification of item removal in the event of any of the equipped items is taken off the premises.

Question No : 356 - (Topic 2)

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

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data ‘unknown sensitivity’

Question No : 357 - (Topic 2)

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

Explanation:

Encryption is used to prevent unauthorized users from accessing data. Data encryption will support the confidentiality of the email.

Question No : 358 - (Topic 2)

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

Explanation:

Incident management is the steps followed when security incident occurs.

Question No : 359 - (Topic 2)

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

Explanation:

DLP systems monitor the contents of systems (workstations, servers, networks) to make sure key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Outbound IM and HTTP user traffic refers to data over a network which falls within the DLP strategy.

Question No : 360 - (Topic 2)

The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

A. Cold site
B. Load balancing
C. Warm site
D. Hot site

Answer: C

Explanation:

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement.

Question No : 361 - (Topic 2)

Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

A. Employ encryption on all outbound emails containing confidential information.
B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
C. Employ hashing on all outbound emails containing confidential information.
D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

Answer: A

Explanation:

Encryption is used to ensure the confidentiality of information and in this case the outbound email that contains the confidential information should be encrypted.

Question No : 362 - (Topic 2)

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

Explanation:

Risk mitigation is done anytime you take steps to reduce risks. Thus mandatory vacation implementation is done as a risk control measure because it is a step that is taken as risk mitigation.

Question No : 363 - (Topic 2)

An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

A. certificate, private key, and intermediate certificate chain
B. certificate, intermediate certificate chain, and root certificate
C. certificate, root certificate, and certificate signing request
D. certificate, public key, and certificate signing request

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE
100-105 Dump PDF VCE
200-001 Dump PDF VCE
200-105 Dump PDF VCE
200-120 Dump PDF VCE
200-125 Dump PDF VCE
200-150 Dump PDF VCE
200-155 Dump PDF VCE
200-310 Dump PDF VCE
200-355 Dump PDF VCE
200-401 Dump PDF VCE
200-601 Dump PDF VCE
210-060 Dump PDF VCE
210-065 Dump PDF VCE
210-250 Dump PDF VCE
210-255 Dump PDF VCE
210-260 Dump PDF VCE
210-451 Dump PDF VCE
210-455 Dump PDF VCE
300-070 Dump PDF VCE
300-075 Dump PDF VCE
300-080 Dump PDF VCE
300-085 Dump PDF VCE
300-101 Dump PDF VCE
300-115 Dump PDF VCE
300-135 Dump PDF VCE
300-160 Dump PDF VCE
300-165 Dump PDF VCE
300-180 Dump PDF VCE
300-206 Dump PDF VCE
300-207 Dump PDF VCE
300-208 Dump PDF VCE
300-209 Dump PDF VCE
300-210 Dump PDF VCE
300-320 Dump PDF VCE
300-360 Dump PDF VCE
300-365 Dump PDF VCE
300-370 Dump PDF VCE
300-375 Dump PDF VCE
300-465 Dump PDF VCE
300-470 Dump PDF VCE
300-475 Dump PDF VCE
350-018 Dump PDF VCE
352-001 Dump PDF VCE
400-051 Dump PDF VCE
400-101 Dump PDF VCE
400-151 Dump PDF VCE
400-201 Dump PDF VCE
400-251 Dump PDF VCE
400-351 Dump PDF VCE
500-006 Dump PDF VCE
500-007 Dump PDF VCE
500-051 Dump PDF VCE
500-052 Dump PDF VCE
500-170 Dump PDF VCE
500-201 Dump PDF VCE
500-202 Dump PDF VCE
500-254 Dump PDF VCE
500-258 Dump PDF VCE
500-260 Dump PDF VCE
500-265 Dump PDF VCE
500-275 Dump PDF VCE
500-280 Dump PDF VCE
500-285 Dump PDF VCE
500-290 Dump PDF VCE
500-801 Dump PDF VCE
600-199 Dump PDF VCE
600-210 Dump PDF VCE
600-211 Dump PDF VCE
600-212 Dump PDF VCE
600-455 Dump PDF VCE
600-460 Dump PDF VCE
600-501 Dump PDF VCE
600-502 Dump PDF VCE
600-503 Dump PDF VCE
600-504 Dump PDF VCE
640-692 Dump PDF VCE
640-875 Dump PDF VCE
640-878 Dump PDF VCE
640-911 Dump PDF VCE
640-916 Dump PDF VCE
642-035 Dump PDF VCE
642-732 Dump PDF VCE
642-747 Dump PDF VCE
642-737 Dump PDF VCE
642-742 Dump PDF VCE
642-883 Dump PDF VCE
642-885 Dump PDF VCE
642-887 Dump PDF VCE
642-889 Dump PDF VCE
642-980 Dump PDF VCE
642-996 Dump PDF VCE
642-997 Dump PDF VCE
642-998 Dump PDF VCE
642-999 Dump PDF VCE
644-066 Dump PDF VCE
644-068 Dump PDF VCE
644-906 Dump PDF VCE
646-048 Dump PDF VCE
646-365 Dump PDF VCE
646-580 Dump PDF VCE
646-671 Dump PDF VCE
646-985 Dump PDF VCE
648-232 Dump PDF VCE
648-238 Dump PDF VCE
648-244 Dump PDF VCE
648-247 Dump PDF VCE
648-375 Dump PDF VCE
648-385 Dump PDF VCE
650-032 Dump PDF VCE
650-042 Dump PDF VCE
650-059 Dump PDF VCE
650-082 Dump PDF VCE
650-127 Dump PDF VCE
650-128 Dump PDF VCE
650-148 Dump PDF VCE
650-159 Dump PDF VCE
650-281 Dump PDF VCE
650-393 Dump PDF VCE
650-472 Dump PDF VCE
650-474 Dump PDF VCE
650-575 Dump PDF VCE
650-621 Dump PDF VCE
650-663 Dump PDF VCE
650-665 Dump PDF VCE
650-754 Dump PDF VCE
650-667 Dump PDF VCE
650-669 Dump PDF VCE
650-752 Dump PDF VCE
650-756 Dump PDF VCE
650-968 Dump PDF VCE
700-001 Dump PDF VCE
700-037 Dump PDF VCE
700-038 Dump PDF VCE
700-039 Dump PDF VCE
700-101 Dump PDF VCE
700-104 Dump PDF VCE
700-201 Dump PDF VCE
700-205 Dump PDF VCE
700-260 Dump PDF VCE
700-270 Dump PDF VCE
700-280 Dump PDF VCE
700-281 Dump PDF VCE
700-295 Dump PDF VCE
700-501 Dump PDF VCE
700-505 Dump PDF VCE
700-601 Dump PDF VCE
700-602 Dump PDF VCE
700-603 Dump PDF VCE
700-701 Dump PDF VCE
700-702 Dump PDF VCE
700-703 Dump PDF VCE
700-801 Dump PDF VCE
700-802 Dump PDF VCE
700-803 Dump PDF VCE
810-403 Dump PDF VCE
820-424 Dump PDF VCE
840-425 Dump PDF VCE