BrainDumps Collection

CompTIA

SY0-401 Exam

CompTIA Security+ Exam

Thank you for Downloading SY0-401 exam PDF Demo

You can also try our SY0-401 practice exam software

Download Free Demo

https://www. braindumpscollection.com/SY0-401.html

DEMO VERSION (LIMITED CONTENT)

Questions & Answers

Version: 39.0

Question: 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.
Incorrect Answers:
B: NAP is a Microsoft technology for controlling network access of a computer host based on system health of the host.
C: Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet. DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding. DNAT does not allow for many internal devices to share one public IP address.
D: NAC is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.
References:
http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT
http://en.wikipedia.org/wiki/Network_Access_Protection
http://en.wikipedia.org/wiki/Network_address_translation#DNAT
http://en.wikipedia.org/wiki/Network_Access_Control

Question: 2

Which of the following devices is MOST likely being used when processing the following?
1 PERMIT IP ANY ANY EQ 80
2 DENY IP ANY ANY

A. 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.
Incorrect Answers:
B: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.
C: A load balancer is used to distribute network traffic load across several network links or network devices.
D: A URL filter is used to block URLs (websites) to prevent users accessing the website.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 10, 24
http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html
http://en.wikipedia.org/wiki/Intrusion_prevention_system
http://www.provision.ro/threat-management/web-application-security/url-filtering#pagei-1|pagep-1|

Question: 3

The security administrator at ABC company received the following log information from an external party:
10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal
10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force
10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan
The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

A. A NIDS was used in place of a NIPS.
B. The log is not in UTC.
C. The external party uses a firewall.
D. ABC company uses PAT.

Answer: D

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.
Incorrect Answers:
A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks. This will not have any bearing on the security administrator at ABC Company finding the root of the attack.
B: UTC is the abbreviation for Coordinated Universal Time, which is the primary time standard by which the world regulates clocks and time. The time in the log is not the issue in this case.
C: Whether the external party uses a firewall or not will not have any bearing on the security administrator at ABC Company finding the root of the attack.
References:
http://www.webopedia.com/TERM/P/PAT.html
http://en.wikipedia.org/wiki/Intrusion_prevention_system
http://en.wikipedia.org/wiki/Coordinated_Universal_Time

Question: 4

Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

A. Sniffer
B. Router
C. Firewall
D. Switch

Answer: C

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.
Incorrect Answers:
A: A sniffer is a tool used in the process of monitoring the data that is transmitted across a network.
B, D: A router is connected to two or more data lines from different networks, whereas a network switch is connected to data lines from one single network. These may include a firewall, but not by default.
References:
http://en.wikipedia.org/wiki/Iptables
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 342
http://en.wikipedia.org/wiki/Router_(computing)

Question: 5

Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

A. Packet Filter Firewall
B. Stateful Firewall
C. Proxy Firewall
D. Application Firewall

Answer: B

Explanation:
Stateful inspections occur at all levels of the network.
Incorrect Answers:
A: Packet-filtering firewalls operate at the Network layer (Layer 3) and the Transport layer (Layer 4) of the Open Systems Interconnect (OSI) model.
C: The proxy function can occur at either the application level or the circuit level.
D: Application Firewalls operates at the Application layer (Layer7) of the OSI model.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 98-100
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 6

Question: 6

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.
Incorrect Answers:
A: The terms protocol analyzer and packet sniffer are interchangeable. They refer to the tools used in the process of monitoring the data that is transmitted across a network.
B: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
D: Web proxies are used to forward HTTP requests.
E: Layer 2 switching uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Layer 2 switching is hardware based, which means switches use application-specific integrated circuit (ASICs) to build and maintain filter tables (also known as MAC address tables or CAM tables).
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex,

Indianapolis, 2014, p. 342
http://en.wikipedia.org/wiki/Intrusion_prevention_system
http://en.wikipedia.org/wiki/LAN_switching
http://en.wikipedia.org/wiki/Proxy_server#Web_proxy_servers

Question: 7

Which of the following network design elements allows for many internal devices to share one public IP address?

A. DNAT
B. PAT
C. DNS
D. DMZ

Answer: B

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.
Incorrect Answers:
A: Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet. DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding. DNAT does not allow for many internal devices to share one public IP address.
C: DNS (Domain Name System) is a service used to translate hostnames or URLs to IP addresses. DNS does not allow for many internal devices to share one public IP address.
D: A DMZ or demilitarized zone 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. A DMZ does not allow for many internal devices to share one public IP address.
References:
http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT
http://en.wikipedia.org/wiki/Network_address_translation#DNAT
http://en.wikipedia.org/wiki/Domain_Name_System

http://en.wikipedia.org/wiki/DMZ_(computing)

Question: 8

Which of the following is a best practice when securing a switch from physical access?

A. Disable unnecessary accounts
B. Print baseline configuration
C. Enable access lists
D. Disable unused ports

Answer: D

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.
Incorrect Answers:
A: Disabling unnecessary accounts would only block those specific accounts.
B: A security baseline is a standardized minimal level of security that all systems in an organization must comply with. Printing it would not secure the switch from physical access.
C: The purpose of an access list is to identify specifically who can enter a facility.
References:
http://orbit-computer-solutions.com/How-To-Configure-Switch-Security.php
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 60
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 207

Question: 9

Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

A. Protocol analyzer
B. Load balancer
C. VPN concentrator
D. Web security gateway

Answer: B

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.

Incorrect Answers:
A: The terms protocol analyzing and packet sniffing are interchangeable. They refer to the process of monitoring the data that is transmitted across a network.
C: A VPN concentrator is a hardware device used to create remote access VPNs. The concentrator creates encrypted tunnel sessions between hosts, and many use two-factor authentication for additional security.
D: One of the newest buzzwords is web security gateway, which can be thought of as a proxy server (performing proxy and caching functions) with web protection software built in. Depending on the vendor, the "web protection" can range from a standard virus scanner on incoming packets to monitoring outgoing user traffic for red flags as well.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 103, 104, 118

Question: 10

Pete, the system administrator, wishes to monitor and limit users' access to external websites.
Which of the following would BEST address this?

A. Block all traffic on port 80.
B. Implement NIDS.
C. Use server load balancers.
D. Install a proxy server.

Answer: D

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.
Incorrect Answers:
A: A network-based IDS (NIDS) approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic.
B: This would block all web traffic, as port 80 is used for World Wide Web.
C: 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.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 98, 103, 111

Question: 11

Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS

B. 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.
Incorrect Answers:
A: A host-based IDS (HIDS) watches the audit trails and log fi les of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
B: Firewalls provide protection by controlling traffic entering and leaving a network.
D: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam). Spam is most commonly associated with email, but spam also exists in instant messaging (IM), short message service (SMS), Usenet, and web discussions/forums/comments/blogs.
References:
http://en.wikipedia.org/wiki/Intrusion_prevention_system
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 42, 47

Question: 12

Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

A. HIPS on each virtual machine
B. NIPS on the network
C. NIDS on the network
D. HIDS on each virtual machine

Answer: A

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.
Incorrect Answers:
B: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.
C: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
D: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
References:
http://en.wikipedia.org/wiki/Intrusion_prevention_system

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 21

Question: 13

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

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

Answer: A

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
Incorrect Answers:
B: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
C: 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.
D: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
References:
http://en.wikipedia.org/wiki/Intrusion_prevention_system
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 21

Question: 14

An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

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

Answer: B

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

Incorrect Answers:
A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
C: 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.
D: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
References:
http://en.wikipedia.org/wiki/Intrusion_prevention_system
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 21

Question: 15

In intrusion detection system vernacular, which account is responsible for setting the security policy for an organization?

A. Supervisor
B. Administrator
C. Root
D. Director

Answer: B

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.
Incorrect Answers:
A, C: Almost every operating system in use today employs the concept of differentiation between users and groups at varying levels. As an example, there is always a system administrator (SA) account that has godlike control over everything: root in Unix/Linux, admin (or a deviation of it) in Windows, administrator in Apple OS X, supervisor in Novell NetWare, and so on.
D: A director is a person from a group of managers who leads or supervises a particular area of a company, program, or project.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 107, 153
http://en.wikipedia.org/wiki/Director_(business)

Question: 16

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.
Which of the following is the type of vulnerability described?

A. Network based
B. IDS
C. Signature based
D. Host based

Answer: C

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.
Incorrect Answers:
A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
B: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.
C: A host-based IDS (HIDS) watches the audit trails and log fi les of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 21

Question: 17

The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

A. Signature Based IDS
B. Heuristic IDS
C. Behavior Based IDS
D. Anomaly Based IDS

Answer: A

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.
Incorrect Answers:
B, C: The technique used by anomaly-based IDS/IPS systems is also referred as network behavior analysis or heuristics analysis.
D: An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.
References:

https://technet.microsoft.com/en-us/library/dd277353.aspx
http://en.wikipedia.org/wiki/Intrusion_detection_system#Signature-based_IDS
http://en.wikipedia.org/wiki/Intrusion_detection_system#Statistical_anomaly-based_IDS

Question: 18

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

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

Answer: B

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.
Incorrect Answers:
A: An application aware firewall provides filtering services for specific applications.
C: Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rule-based decisions about whether the request should be forwarded or refused. The proxy intercepts all of the packets and reprocesses them for use internally.
D: A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 16, 20
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 98

Question: 19

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

A. Spam filter
B. Protocol analyzer
C. Web application firewall
D. Load balancer

Answer: B

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.
Incorrect Answers:
A: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam). Spam is most commonly associated with email, but spam also exists in instant messaging (IM), short message service (SMS), Usenet, and web discussions/forums/comments/blogs. Because spam consumes about 89 percent of all email traffic (see the Intelligence Reports at www.messagelabs.com), it's essential to filter and block spam at every opportunity.
C: 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.
D: A load balancer is used to spread or distribute network traffic load across several network links or network devices.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 10, 18, 19

Question: 20

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

A. PSH
B. ACK
C. SYN
D. URG
E. FIN

Answer: B, C

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.
Incorrect Answers:

A: The PSH flag tells the TCP stack to flush all buffers and send any outstanding data up to and including the data that had the PSH flag set.
D: URG indicates that the urgent pointer field has a valid pointer to data that should be treated urgently and be transmitted before non-urgent data.
E: FIN is used to indicate that the client will send no more data.
References:
http://linuxpoison.blogspot.com/2007/11/what-are-tcp-control-bits.html

Question: 21

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

A. Spam filter
B. URL filter
C. Content inspection
D. Malware inspection

Answer: B

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: 22

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

A. 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 fi le 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.
Incorrect Answers:
A: The basic purpose of a firewall is to isolate one network from another. Firewalls are available as appliances, meaning they're installed as the primary device separating two networks.
B: Switches are multiport devices that improve network efficiency.
D: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam).
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 18, 19
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 96, 102

Question: 23

The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

A. The access rules on the IDS
B. The pop up blocker in the employee's browser
C. The sensitivity level of the spam filter
D. The default block page on the URL filter

Answer: D

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.
Incorrect Answers:
A: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.
B: Pop-up blockers prevent websites from opening further web browser windows without your approval.

C: A spam filter deals with identifying and blocking/filtering/removing unsolicited messages.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 18, 19, 21, 246

Question: 24

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

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

Answer: B

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.
Incorrect Answers:
A, C, D: These devices deal with controlling how devices in a network gain access to data and permission to transmit it, as well as controlling error checking and packet synchronization. It, therefore, operates at Layer 2 of the OSI model.
References:
http://en.wikipedia.org/wiki/Content-control_software#Types_of_filtering
http://en.wikipedia.org/wiki/OSI_model

Question: 25

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter
B. 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.
Incorrect Answers:

B: The basic purpose of a firewall is to isolate one network from another.
C: A proxy server is a variation of an application firewall or circuit-level firewall, and used as a middleman between clients and servers. Often a proxy serves as a barrier against external threats to internal clients.
D: The terms protocol analyzer and packet sniffer are interchangeable. They refer to the tools used in the process of monitoring the data that is transmitted across a network.
References:
http://en.wikipedia.org/wiki/Content-control_software
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 11, 96, 342

Thank You for trying SY0-401 PDF Demo

To try our SY0-401 practice exam software visit link below

https://www. braindumpscollection.com/SY0-401.html

Start Your SY0-401 Preparation

Use Coupon “20OFF” for extra 20% discount on the purchase of Practice Test Software. Test your SY0-401 preparation with actual exam questions.