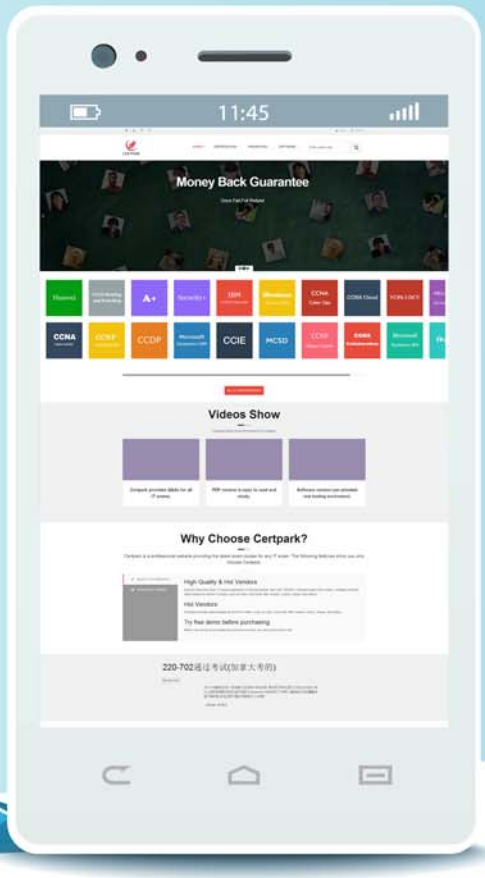
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **SY0-401**

Title : CompTIA Security+ Certification

Version : DEMO

1.Topic 1, Network Security
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

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|

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

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)

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