examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.examunion.com

Exam : **JK0-022**

Title : CompTIA Academic/E2C Security+ Certification Exam

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.

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.

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.

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.

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.