312-38 Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which of the following steps are required in an idle scan of a closed port? Each correct answer represents a part of the solution. Choose all that apply.

A. The attacker sends a SYN/ACK to the zombie.

B. The zombie\\'s IP ID increases by only 1.

C. In response to the SYN, the target sends a RST.

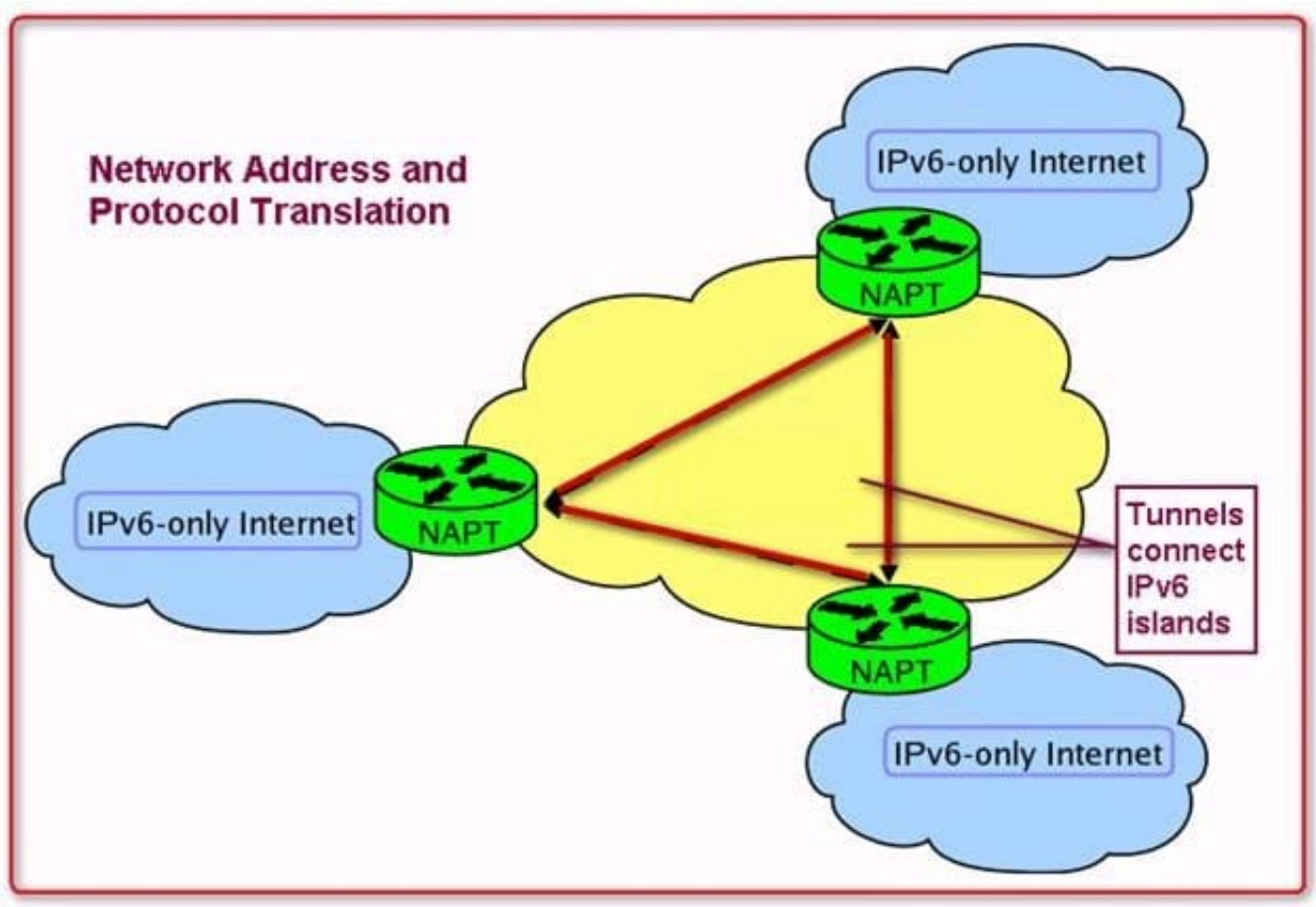
D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

E. The zombie\\'s IP ID increases by 2.

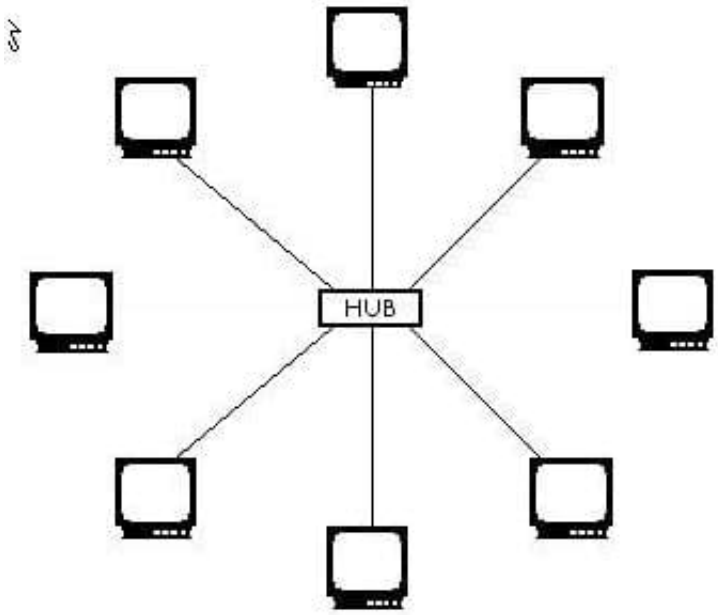
Correct Answer: ACDB

Following are the steps required in an idle scan of a closed port:

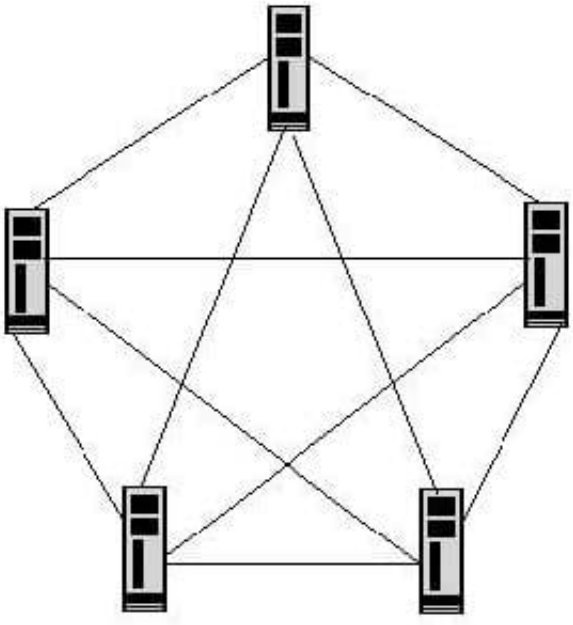
1.Probe the zombie\\'s IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ACK, sends back a RST, thus disclosing its IP ID.



2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.



3.Probe the zombie\\'s IP ID again: The zombie\\'s IP ID has increased by only 1 since step 1. So the port is closed.



QUESTION 2

Which of the following types of RAID offers no protection for the parity disk?

A. RAID 2

B. RAID 1

C. RAID 5

D. RAID 3

Correct Answer: D

QUESTION 3

Michael decides to view the _____ to track employee actions on the organization\\'s network.

A. Firewall policy

B. Firewall settings

C. Firewall log

D. Firewall rule set

Correct Answer: C

QUESTION 4

You work as the network administrator for uCertify Inc. The company has planned to add the support for IPv6 addressing. The initial phase deployment of IPv6 requires support from some IPv6-only devices. These devices need to access servers that support only IPv4. Which of the following tools would be suitable to use?

A. Multipoint tunnels

B. NAT-PT

C. Point-to-point tunnels

D. Native IPv6

Correct Answer: B

NAT-PT (Network address translation-Protocol Translation) is useful when an IPv4-only host needs to communicate with an IPv4-only host. NAT-PT (Network Address Translation-Protocol Translation) is an implementation of RFC 2766 as specified by the IETF. NAT-PT was designed so that it can be run on low-end, commodity hardware. NAT-PT runs in user space, capturing and translating packets between the IPv6 and IPv4 networks (and vice-versa). NAT-PT uses the Address Resolution Protocol (ARP) and Neighbor Discovery (ND) on the IPv4 and IPv6 network systems, respectively.

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
char buffer1[10];
strcpy(buffer1, str);
return 1;
}
int main(int argc, char *argv[]) {
buffer (argv[1]);
printf("Executed\n");
return 1;
}
```

NAT-Protocol Translation can be used to translate both the source and destination IP addresses.

Answer option D is incorrect. Native IPv6 is of use when the IPv6 deployment is pervasive, with heavy traffic loads.

Answer option C is incorrect. Point-to-point tunnels work well when IPv6 is needed only in a subset of sites. These point-to-point tunnels act as virtual point-to-point serial link. These are useful when the traffic is of very high volume. Answer

option A is incorrect. The multipoint tunnels are used for IPv6 deployment even when IPv6 is needed in a subset of sites and is suitable when the traffic is infrequent and of less predictable volume.

QUESTION 5

Fill in the blank with the appropriate term. The protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.

Correct Answer: Sliding Window

The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame sequences sent, and their respective acknowledgements received, by both the users. Its additional feature over a simpler protocol is that can allow multiple packets to be "in transmission" simultaneously, rather than waiting for each packet to be acknowledged before sending the next.In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgment is received or before a specified event occurs.An example of a sliding window is one in which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender "slides" the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes

called acknowledgment delay period.