ECSAV10$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

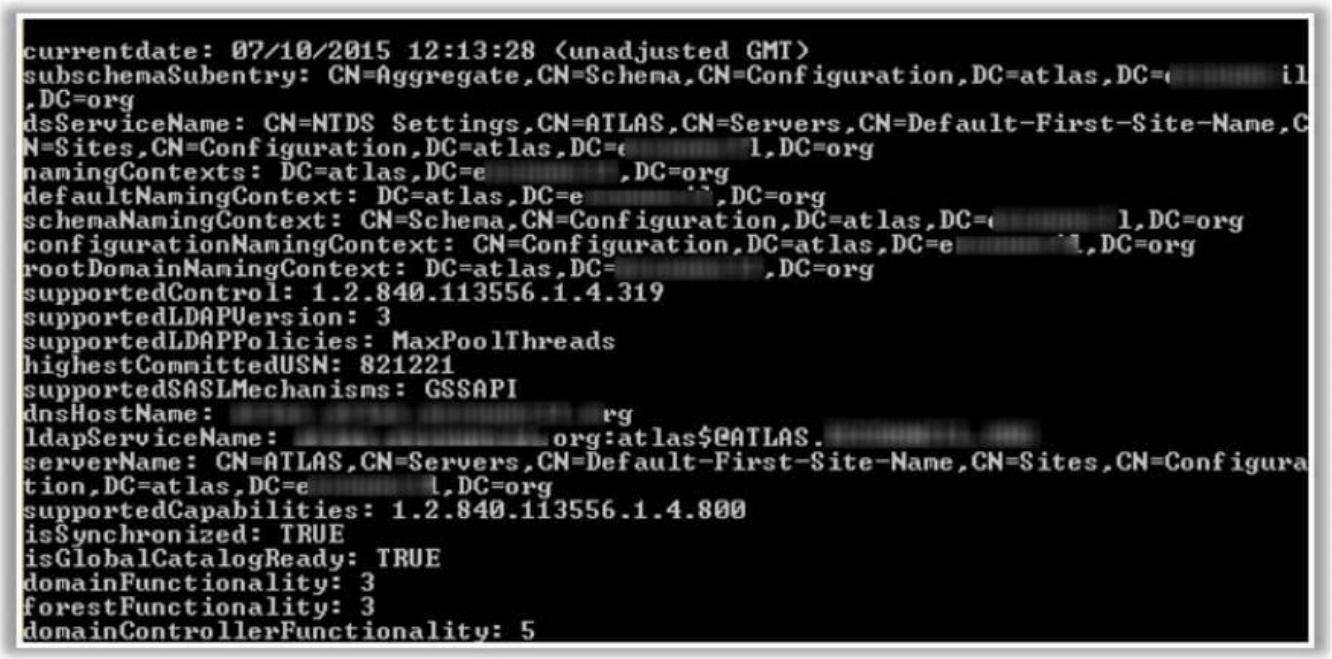
https://www.geekcert.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are enumerating a target system. Which of the following PortQry commands will give a result similar to the screenshot below:



A. portqry -n myserver -p udp -e 389

B. portqry -n myserver -p udp -e 123

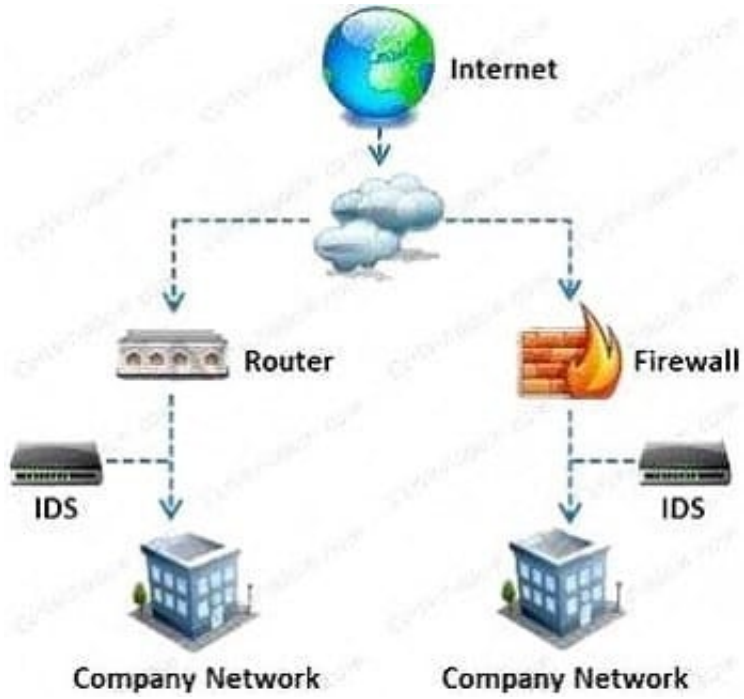
C. portqry -n myserver -p TCP -e 389

D. portqry -n myserver -p TCP -e 123

Correct Answer: C

QUESTION 2

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.

B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.

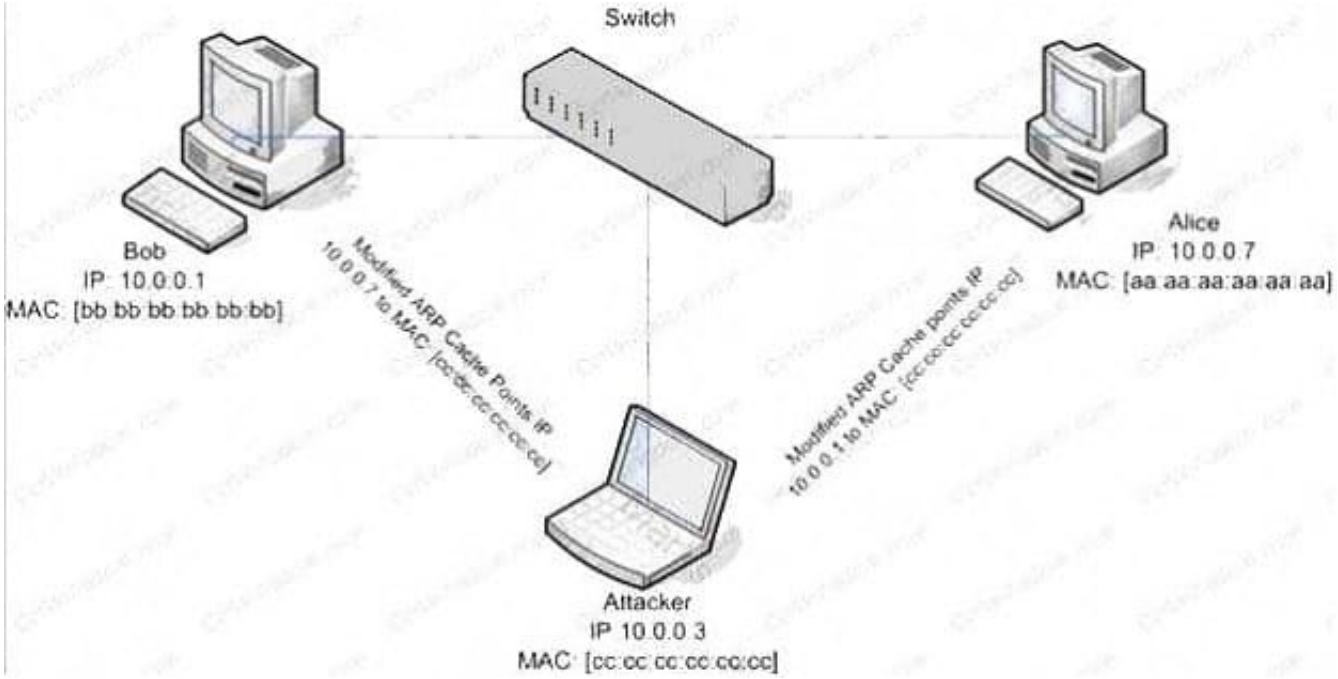
C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.

D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C

QUESTION 3

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker\\'s MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering

B. Social Engineering

C. Input Validation

D. Session Hijacking

Correct Answer: D

QUESTION 4

Identify the attack from the description below:

I. User A sends an ARP request to a switch

II. The switch broadcasts the ARP request in the network

III. An attacker eavesdrops on the ARP request and responds by spoofing as a legitimate user

IV.

The attacker sends his MAC address to User A

A.

MAC spoofing

B.

ARP injection

C.

ARP flooding

D.

ARP poisoning

Correct Answer: A

QUESTION 5

Which of the following shields Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested?

A. DNSSEC

B. Firewall

C. Packet filtering

D. IPSec

Correct Answer: A