

412-79V10^{Q&As}

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

<https://www.leads4pass.com/412-79v10.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. Progressive IDS
- D. NIPS

Correct Answer: B

QUESTION 2

Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

- A. Anonymous Information Gathering
- B. Private Information Gathering
- C. Passive Information Gathering
- D. Active Information Gathering

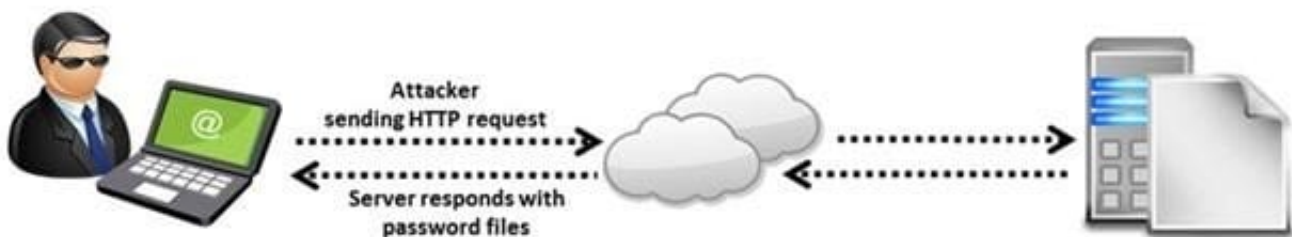
Correct Answer: D

Reference: <http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html>

QUESTION 3

A directory traversal (or path traversal) consists in exploiting insufficient security validation/sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs.

The goal of this attack is to order an application to access a computer file that is not intended to be accessible. This attack exploits a lack of security (the software is acting exactly as it is supposed to) as opposed to exploiting a bug in the code.



To perform a directory traversal attack, which sequence does a pen tester need to follow to manipulate variables of reference files?

- A. dot-dot-slash (../) sequence
- B. Denial-of-Service sequence
- C. Brute force sequence
- D. SQL Injection sequence

Correct Answer: A

Reference:

https://www.cs.ucsb.edu/~vigna/publications/2010_doupe_cova_vigna_dimva10.pdf (pae 7, directory traversal)

QUESTION 4

Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define meta-variables?

- A. "\$"
- B. "#"
- C. "*"
- D. "?"

Correct Answer: A

QUESTION 5

TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

- A. Simple Network Management Protocol (SNMP)
- B. Network File system (NFS)
- C. Internet Control Message Protocol (ICMP)
- D. Transmission Control Protocol (TCP)

Correct Answer: A

[Latest 412-79V10 Dumps](#)

[412-79V10 PDF Dumps](#)

[412-79V10 Exam Questions](#)