312-50V11^{Q&As}

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v11.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

This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid

B. Linear

C. Symmetric

D. Brute Force

Correct Answer: A

QUESTION 2

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders

B. Using wget to perform banner grabbing on the webserver

C. Flooding the web server with requests to perform a DoS attack

D. Downloading all the contents of the web page locally for further examination

Correct Answer: B

QUESTION 3

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

A. Nmap

B. Cain and Abel

C. Nessus

D. Snort

Correct Answer: D

QUESTION 4

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA

B. -sX

C. -sT

D. -sF

Correct Answer: A

QUESTION 5

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. " Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

A. The -A flag

B. The -g flag

C. The -f flag

D. The -D flag

Correct Answer: D

flags -source-port and -g are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.