312-50V8^Q&As

Certified Ethical Hacker v8

Pass EC-COUNCIL 312-50V8 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-50v8.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

Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl

B. C++

C. Python

D. Java

Correct Answer: B

QUESTION 2

The configuration allows a wired or wireless network interface controller to pass all trafice it receives to thecentral processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. WEM

B. Multi-cast mode

C. Promiscuous mode

D. Port forwarding

Correct Answer: B

QUESTION 3

A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application

B. Layer 4 - TCP

C. Layer 3 - Internet protocol

D. Layer 2 - Data link

Correct Answer: B

QUESTION 4

In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user

accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

A. Full Blown Attack

B. Thorough Attack

C. Hybrid Attack

D. BruteDict Attack

Correct Answer: C

QUESTION 5

What is GINA?

A. Gateway Interface Network Application

B. GUI Installed Network Application CLASS

C. Global Internet National Authority (G-USA)

D. Graphical Identification and Authentication DLL

Correct Answer: D

QUESTION 6

Bob has been hired to perform a penetration test on XYZ.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information of have any technical details online.

Within the context of penetration testing methodology, what phase is Bob involved with?

A. Passive information gathering

B. Active information gathering

C. Attack phase

D. Vulnerability Mapping

Correct Answer: A

QUESTION 7

Which of the following ICMP message types are used for destinations unreachables?

A. 0

B. 3

C. 11

D. 13

E. 17

Correct Answer: B

QUESTION 8

You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn\\'t work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems. In other words you are trying to penetrate an otherwise impenetrable system.

How would you proceed?

A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank\\'s network

B. Try to hang around the local pubs or restaurants near the bank,get talking to a poorly-paid or disgruntled employee,and offer them money if they\\'ll abuse their access privileges by providing you with sensitive information

C. Launch DDOS attacks against Merclyn Barley Bank\\'s routers and firewall systems using 100,000 or more "zombies" and "bots"

D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank\\'s Webserver to that of your machine using DNS Cache Poisoning techniques

Correct Answer: B

QUESTION 9

A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true

B. false

Correct Answer: B

QUESTION 10

You are doing IP spoofing while you scan your target. You find that the target has port 23 open. Anyway you are unable to connect.

Why?

A. A firewall is blocking port 23

B. You cannot spoof + TCP

C. You need an automated telnet tool

D. The OS does not reply to telnet even if port 23 is open

Correct Answer: A

QUESTION 11

This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools. Which of the following tools is being described?

A. Wificracker

B. WLAN-crack

C. Airguard

D. Aircrack-ng

Correct Answer: D

QUESTION 12

Which of the following is the successor of SSL?

A. RSA

B. GRE

C. TLS

D. IPSec

Correct Answer: C

QUESTION 13

How do you defend against MAC attacks on a switch?

A. Disable SPAN port on the switch

B. Enable SNMP Trap on the switch

C. Configure IP security on the switch

D. Enable Port Security on the switch

Correct Answer: D

QUESTION 14

Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk.

B. Deny the risk.

C. Mitigate the risk.

D. Initiate the risk.

Correct Answer: C

QUESTION 15

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the network.

How can you achieve this?

A. There is no way to completely block tracerouting into this area

B. Block UDP at the firewall

C. Block TCP at the firewall

D. Block ICMP at the firewall

Correct Answer: A

Latest 312-50V8 Dumps 312-50V8 PDF Dumps 312-50V8 VCE Dumps