312-50V9 Q&As

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

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

https://www.certbus.com/312-50v9.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

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

A. PHP

B. C#

C. Python

D. ASP.NET

Correct Answer: C Section: (none)

QUESTION 2

An nmap command that includes the host specification of 202.176.56-57.* will scan _____ number of hosts.

B. 256

C. 512

D. Over 10, 000

Correct Answer: C Section: (none)

QUESTION 3

While conducting a penetration test, the tester determines that there is a firewall between the tester\\'s machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall

B. Application-level firewall

C. Circuit-level gateway firewall

D. Stateful multilayer inspection firewall

Correct Answer: C Section: (none)

QUESTION 4

While performing data validation of web content, a security technician is required to restrict malicious input. Which of the

following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.

B. Validate web content input with scanning tools.

C. Validate web content input for type, length, and range.

D. Validate web content input for extraneous queries.

Correct Answer: C Section: (none)

QUESTION 5

Which of the following is a preventive control?

A. Smart card authentication

B. Security policy

C. Audit trail

D. Continuity of operations plan

Correct Answer: A Section: (none)

QUESTION 6

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform

SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

Correct Answer: ABD Section: (none)

QUESTION 7

Which of the following parameters enables NMAP\\'s operating system detection feature?

A. NMAP -sV

B. NMAP -oS

C. NMAP -sR

D. NMAP -O

Correct Answer: D Section: (none)

QUESTION 8

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification

B. At least once every three years or after any significant upgrade or modification

C. At least twice a year or after any significant upgrade or modification

D. At least once every two years and after any significant upgrade or modification

Correct Answer: A Section: (none)

QUESTION 9

Which access control mechanism allows for multiple systems to use a central authentication server (CAS)

that permits users to authenticate once and gain access to multiple systems?

A. Role Based Access Control (RBAC)

B. Discretionary Access Control (DAC)

C. Windows authentication

D. Single sign-on

Correct Answer: D Section: (none)

QUESTION 10

Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Restrict Physical Access to Server Rooms hosting Critical Servers

D. Use Static IP Address

Correct Answer: A Section: (none)

A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn\\'t prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet\\'s payload so that all the sniffer sees is encrypted gibberish.

References: http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

QUESTION 11

Which of the following is the successor of SSL?

A. TLS

B. RSA

C. GRE

D. IPSec

Correct Answer: A Section: (none)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as \\'SSL\\', are cryptographic protocols that provide communications security over a computer network.

References: https://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 12

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

A. c:\compmgmt.msc

B. c:\gpedit

C. c:\ncpa.cpl

D. c:\services.msc

Correct Answer: A Section: (none)

QUESTION 13

What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

B. Manipulate format strings in text fields

C. SSH

D. SYN Flood

Correct Answer: A Section: (none)

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

QUESTION 14

An IT security engineer notices that the company\\'s web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company\\'s web server.

B. Determine the origin of the attack and launch a counterattack.

C. Record as much information as possible from the attack.

D. Perform a system restart on the company\\'s web server.

Correct Answer: C Section: (none)

QUESTION 15

In which phase of the ethical hacking process can Google hacking be employed? This is a technique that

involves manipulating a search string with specific operators to search for vulnerabilities.

Example:

allintitle: root passwd

A. Maintaining Access

B. Gaining Access

C. Reconnaissance

D. Scanning and Enumeration

Correct Answer: C Section: (none)

Latest 312-50V9 Dumps 312-50V9 Practice Test 312-50V9 Study Guide