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.pass2lead.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

SATISFACTION GUARANTEED 100%

QUESTION 1

What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.

B. Has to be unforgeable, and has to be authentic.

C. Must be unique and have special characters.

D. Has to be legible and neat.

Correct Answer: B

QUESTION 2

Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

A. Out of band and boolean-based

B. Time-based and union-based

C. union-based and error-based

D. Time-based and boolean-based

Correct Answer: C

Union based SQL injection allows an attacker to extract information from the database by extending the results returned by the first query. The Union operator can only be used if the original/new queries have an equivalent structure Error-based SQL injection is an In-band injection technique where the error output from the SQL database is employed to control the info inside the database. In In-band injection, the attacker uses an equivalent channel for both attacks and collect data from the database.

QUESTION 3

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Multi-cast mode

B. Promiscuous mode

C. WEM

D. Port forwarding

Correct Answer: B

QUESTION 4

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company\\'s network. He

decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers

unencrypted traffic in port UDP 161.

what protocol is this port using and how can he secure that traffic?

A. it is not necessary to perform any actions, as SNMP is not carrying important information.

B. SNMP and he should change it to SNMP V3

C. RPC and the best practice is to disable RPC completely

D. SNMP and he should change it to SNMP v2, which is encrypted

Correct Answer: B

We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense. SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a `fire and forget\\' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link). There are two modes of operation with SNMP ?get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation. This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation. SNMP trapsSince SNMP is primarily a UDP port based system, traps may be `lost\\' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn\\'t listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know. The SNMP v2c specification introduced the idea of splitting traps into two types; the original `hope it gets there\\' trap and the newer `INFORM\\' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn\\'t get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

QUESTION 5

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with

firewalls and IPS systems.

What is the best security policy concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.

B. As long as the physical access to the network elements is restricted, there is no need for additional measures.

C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.

D. The operator knows that attacks and down time are inevitable and should have a backup site.

Correct Answer: A

QUESTION 6

in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 3.0-6.9

B. 40-6.0

C. 4.0-6.9

D. 3.9-6.9

Correct Answer: C

QUESTION 7

Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?

A. Known plaintext

B. Password spraying

C. Brute force

D. Dictionary

Correct Answer: C

A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password

protected, by golf shot technically each word in a very dictionary as a variety of password for that system.

This attack vector could be a variety of Brute Force Attack.

The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used

passwords and once combined with common character substitution with numbers, will generally be terribly

effective and quick.

How is it done?

Basically, it\\'s attempting each single word that\\'s already ready. it\\'s done victimization machine-controlled tools that strive all the possible words within the dictionary.

Some password Cracking Software:

John the ripper

L0phtCrack

Aircrack-ng

QUESTION 8

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

Correct Answer: BDE

QUESTION 9

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?

A. nmap -sn -pp

B. nmap -sn -PO

C. Anmap -sn -PS

D. nmap -sn -PA

Correct Answer: C

QUESTION 10

Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?

A. Advanced SMS phishing

B. Bypass SSL pinning

C. Phishing

D. Tap \\'n ghost attack

Correct Answer: A

QUESTION 11

What port number is used by LDAP protocol?

A. 110

B. 389

C. 464

D. 445

Correct Answer: B

QUESTION 12

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

A. MD4

B. DES

C. SHA

D. SSL

Correct Answer: B

QUESTION 13

Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 (content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111

B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet

C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the

192.168.1.0 subnet

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Correct Answer: D

QUESTION 14

Which of the following program infects the system boot sector and the executable files at the same time?

A. Polymorphic virus

B. Stealth virus

C. Multipartite Virus

D. Macro virus

Correct Answer: C

QUESTION 15

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp\\'s requirements?

A. Gateway-based IDS

B. Network-based IDS

C. Host-based IDS

D. Open source-based

Correct Answer: C

312-50V11 PDF Dumps 312-50V11 Practice Test 312-50V11 Study Guide