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.pass4itsure.com/312-50v11.html

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

QUESTION 1

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance

B. Maintaining access

C. Scanning

D. Gaining access

Correct Answer: D

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they\\'re Password cracking ?Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.?Password attacks ? Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 2

What is the role of test automation in security testing?

A. It is an option but it tends to be very expensive.

B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

C. Test automation is not usable in security due to the complexity of the tests.

D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D

QUESTION 3

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

] >

A. XXE

B. SQLi

C. IDOR

D. XXS

Correct Answer: A

QUESTION 4

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization\\'s OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p

B. nmap -Pn -sU -p 44818 --script enip-info

C. nmap -Pn -sT -p 46824

D. nmap -Pn -sT -p 102 --script s7-info

Correct Answer: B

QUESTION 5

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server\\'s access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server\\'s software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions

B. Privilege escalation

C. Directory traversal D. Brute force login

Correct Answer: A

QUESTION 6

By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember

B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

Correct Answer: B

QUESTION 7

What type of virus is most likely to remain undetected by antivirus software?

A. Cavity virus

B. Stealth virus

C. File-extension virus

D. Macro virus

Correct Answer: B

QUESTION 8

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. nessus

B. tcpdump

C. ethereal

D. jack the ripper

Correct Answer: B

QUESTION 9

Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed

B. It opens a security-delayed window based on the port being scanned

C. It doesn\\'t depend on the patches that have been applied to fix existing security holes

D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Correct Answer: D

QUESTION 10

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.

Why he cannot see the servers?

A. He needs to add the command ""ip address"" just before the IP address

B. He needs to change the address to 192.168.1.0 with the same mask

C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range

D. The network must be dawn and the nmap command and IP address are ok

Correct Answer: C

QUESTION 11

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux

B. Unix

C. OS X

D. Windows

Correct Answer: D

QUESTION 12

Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.

B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.

C. It is not ?a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.

D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Correct Answer: B

QUESTION 13

Which of these is capable of searching for and locating rogue access points?

A. HIDS

B. WISS

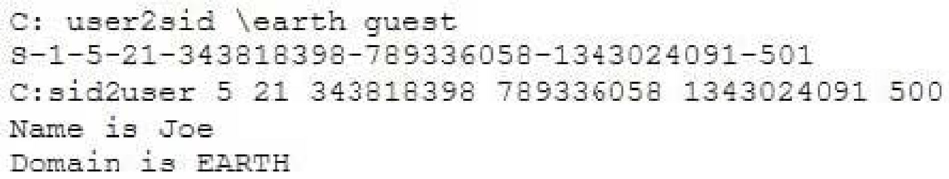
C. WIPS

D. NIDS

Correct Answer: C

QUESTION 14

What did the following commands determine?



```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. That the Joe account has a SID of 500

B. These commands demonstrate that the guest account has NOT been disabled

C. These commands demonstrate that the guest account has been disabled

D. That the true administrator is Joe

E. Issued alone, these commands prove nothing

Correct Answer: D

QUESTION 15

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP\\'s owned by XYZ (Internal) and private IP\\'s are communicating to a Single Public IP. Therefore, the Internal IP\\'s are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

A. Botnet Attack

B. Spear Phishing Attack

C. Advanced Persistent Threats

D. Rootkit Attack

Correct Answer: A

312-50V11 Study Guide 312-50V11 Exam Questions 312-50V11 Braindumps