Free Questions for ECSAv10 by dumpshq

Shared by Jordan on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

Options:

A- Visit Google's search engine and view the cached copy

B- Crawl and download the entire website using the Surfoffline tool and save them to his computer

C- Visit the company's partners' and customers' website for this information

D- Use Way Back Machine in Archive.org web site to retrieve the Internet archive

Answer:

D

Question 2

Question Type: MultipleChoice

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contractfor the state government of Californi

a. Your next step is to initiate a DoS attack on their network. Why wouldyou want to initiate a DoS attack on a system you are testing?

Options:

A- Use attack as a launching point to penetrate deeper into the network

B- Demonstrate that no system can be protected against DoS attacks

C- List weak points on their network

D- Show outdated equipment so it can be replaced

Answer:

C

Question 3

Question Type: MultipleChoice

What is the target host IP in the following command?

```
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
```

Options:

A- Firewalk does not scan target hosts

B- 172.16.28.95

C- This command is using FIN packets, which cannot scan target hosts

D- 10.10.150.1

Answer:

A

Question 4

Question Type: **MultipleChoice**

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted.

Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

Options:

A- Paranoid

B- Sneaky

C- Polite

D- Normal

Answer:

C

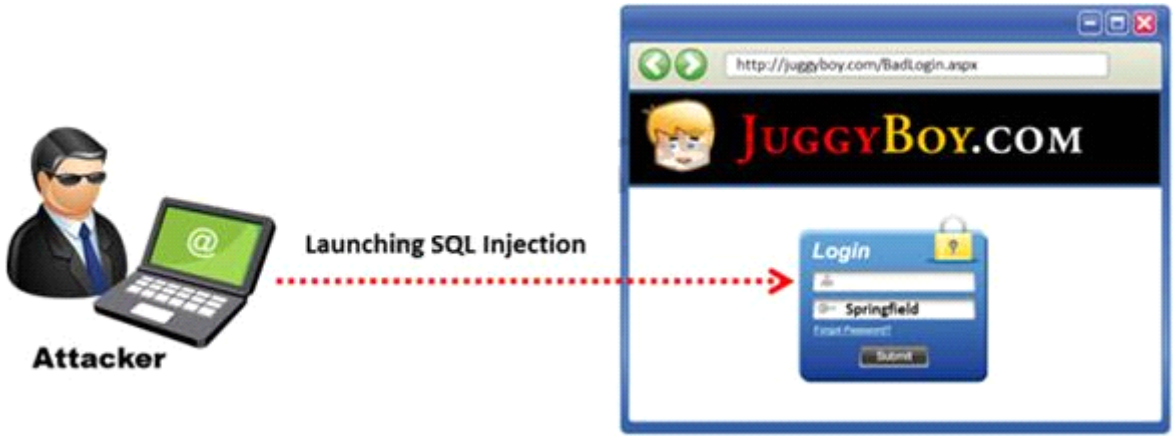
Question 5

Question Type: **MultipleChoice**

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.

This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database.

The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

Options:

A- Blah' "2=2 --"

B- Blah' and 2=2 --

C- Blah' and 1=1 --

D- Blah' or 1=1 --

Answer:

D

Question 6

Question Type: MultipleChoice

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utilitythat executes exploits against his system to verify the results of the vulnerability test. The second utilityexecutes five known exploits against his network in which the vulnerability analysis said were not exploitable.

What kind of results did Jim receive from his vulnerability analysis?

Options:

A- True negatives

B- False negatives

C- False positives

D- True positives

Answer:

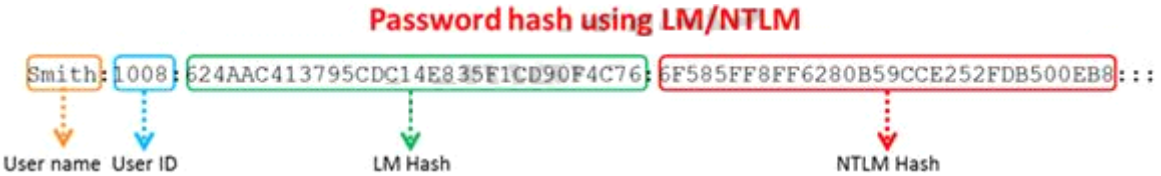
B

Question 7

Question Type: MultipleChoice

Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.

NTLM and LM authentication protocols are used to securely store a user's password in the SAM database using different hashing methods.



The SAM file in Windows Server 2008 is located in which of the following locations?

Options:

A- c:\windows\system32\config\SAM

B- c:\windows\system32\drivers\SAM

C- c:\windows\system32\Setup\SAM

D- c:\windows\system32\Boot\SAM

Answer:

D

Question 8

Question Type: MultipleChoice

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

Options:

A- unified

B- csv

C- alert_unixsock

D- alert_fast

Answer:

B

Question 9

Question Type: MultipleChoice

DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories.

Identify the attacks that fall under Passive attacks category.

Options:

A- Wardriving

B- Spoofing

C- Sniffing

D- Network Hijacking

Answer:

A