DUMPSARENA

GIAC Penetration Tester

GIAC GPEN

Version Demo

Total Demo Questions: 15

Total Premium Questions: 385

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	99
Topic 2, Volume B	97
Topic 3, Volume C	98
Topic 4, Volume D	91
Total	385

QUESTION NO: 1

You run the following PHP script:

$password = mysql_real_escape_string($_POST["password"]);?>

What is the use of the mysql_real_escape_string() function in the above script.

Each correct answer represents a complete solution. Choose all that apply

A. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

B. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".

C. It can be used to mitigate a cross site scripting attack.

D. It can be used as a countermeasure against a SQL injection attack.

ANSWER: A D

QUESTION NO: 2

Which of the following is the correct syntax to create a null session?

A. c:\>net view \\IP_addr\IPC$ "" /u: ""

B. c:\>net view \\IPC$\IP_addr "" /u: ""

C. c:\>net use \\IP_addr\IPC$ "" /u: ""

D. c:\>net use \\IPC$\IP_addr "" /u: ""

ANSWER: C

QUESTION NO: 3

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Brute Force attack

B. Dictionary attack

C. Hybrid attack

D. Rule based attack

ANSWER: A B C

QUESTION NO: 4

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com network. Now, when you have finished your penetration testing, you find that the weare- secure.com server is highly vulnerable to SNMP enumeration. You advise the we-are-secure Inc. to turn off SNMP; however, this is not possible as the company is using various SNMP services on its remote nodes. What other step can you suggest to remove SNMP vulnerability?

Each correct answer represents a complete solution. Choose two.

A. Close port TCP 53.

B. Change the default community string names.

C. Upgrade SNMP Version 1 with the latest version.

D. Install antivirus.

ANSWER: B C

QUESTION NO: 5

Which of the following statements are true about session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. It is used to slow the working of victim's network resources.

B. TCP session hijacking is when a hacker takes over a TCP session between two machines.

C. Use of a long random number or string as the session key reduces session hijacking.

D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

ANSWER: B C D

QUESTION NO: 6

Which of the following is NOT an example of passive footprinting?

A. Scanning ports.

B. Analyzing job requirements.

C. Querying the search engine.

D. Performing the whois query.

ANSWER: A

QUESTION NO: 7

Which of the following security protocols can be used to support MS-CHAPv2 for wireless client authentication?

Each correct answer represents a complete solution. Choose two.

A. PEAP

B. IPSec

C. HTTP

D. PPTP

ANSWER: A D

QUESTION NO: 8

Which of the following syntaxes is the correct syntax for the master.dbo.sp_makewebtask procedure?

A. sp_makewebtask [@inputfile =] 'inputfile', [@query =] 'query'

B. sp_makewebtask [@outputfile =] 'outputfile', [@query =] 'query'

C. sp_makewebtask [@query =] 'query', [@inputfile =] 'inputfile'

D. sp_makewebtask [@query =] 'query', [@outputfile =] 'outputfile'

ANSWER: B

QUESTION NO: 9

Which of the following describe the benefits to a pass-the-hash attack over traditional password cracking?

A. No triggering of IDS signatures from the attack privileges at the level of theacquired password hash and no corruption of the LSASS process.

B. No triggering of IDS signatures from the attack, no account lockout and use ofnative windows file and print sharing tools on the compromised system.

C. No account lockout, privileges at the level of the acquired password hash and useof native windows file and print Sharif tools on the compromised system.

D. No account lockout, use of native file and print sharing tools on the compromisedsystem and no corruption of the LSASS process.

ANSWER: D

QUESTION NO: 10

Which of the following are considered Bluetooth security violations?

Each correct answer represents a complete solution. Choose two.

A. Bluebug attack

B. SQL injection attack

C. Cross site scripting attack

D. Social engineering

E. Bluesnarfing

ANSWER: A E

QUESTION NO: 11

You successfully compromise a target system's web application using blind command injection. The command you injected is ping-n 1 192.168.1.200. Assuming your machine is 192.168.1 200, which of the following would you see?

A. Ping-n 1 192.168.1 200 on the compromised system

B. A 'Destination host unreachable' error message on the compromised system

C. A packet containing 'Packets: Sent - 1 Received = 1, Loss = 0 (0% loss) on yoursniffer

D. An ICMP Echo packet on your sniffer containing the source address of the target

ANSWER: A

QUESTION NO: 12

Which of the following techniques is used to monitor telephonic and Internet conversations by a third party?

A. War driving

B. War dialing

C. Web ripping

D. Wiretapping

ANSWER: D

QUESTION NO: 13

A penetration tester used a client-side browser exploit from metasploit to get an unprivileged shell prompt on the target Windows desktop. The penetration tester then tried using the getsystem command to perform a local privilege escalation which failed. Which of the following could resolve the problem?

A. Load priv module and try getsystem again

B. Run getuid command, then getpriv command, and try getsystem again

C. Run getuid command and try getsystem again

D. Use getprivs command instead of getsystem

ANSWER: B

QUESTION NO: 14

Which of the following techniques are NOT used to perform active OS fingerprinting?

Each correct answer represents a complete solution. Choose all that apply.

A. ICMP error message quoting

B. Analyzing email headers

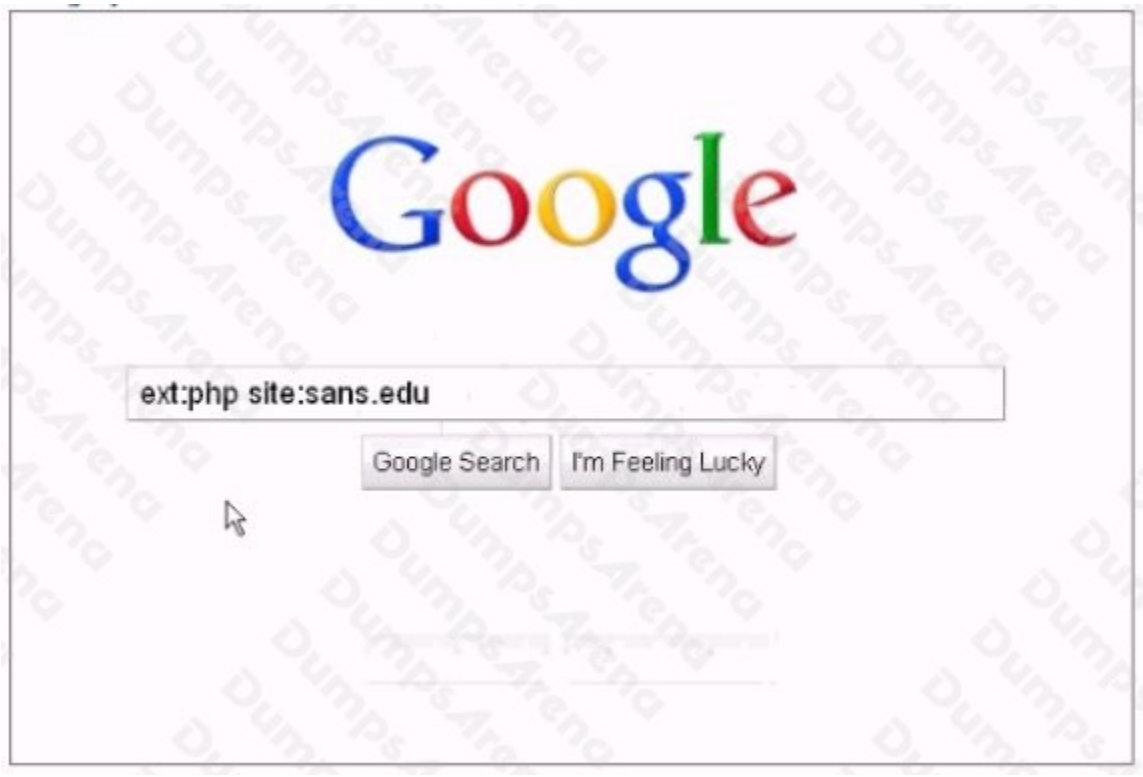
C. Sniffing and analyzing packets

D. Sending FIN packets to open ports on the remote system

ANSWER: B C

QUESTION NO: 15

Analyze the screenshot below, which of the following sets of results will be retrieved using this search?



A. Pages from the domain sans.edu that have external links.

B. Files of type .php from the domain sans.edu.

C. Pages that contain the term ext:php and slte.sans.edu.

D. Files of type .php that redirect to the sans.edu domain.

ANSWER: A