GAQM CPEH-001 Practice Questions

Shared by Ross on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

```
1. #include <stdio.h>
2. void stripnl(char *str) {
3. while(strlen(str) && ( (str[strlen(str) - 1] == 13) ||
4. ( str[strlen(str) - 1] == 10 ))) {
5. str[strlen(str) - 1] = 0;
6. }
7. }
8.
9. int main() {
10. FILE *infile;
11. char fname[40];
12. char line[100];
13. int lcount;
14.
15. /* Read in the filename */
16. printf("Enter the name of a ascii file: ");
17. fgets(fname, sizeof(fname), stdin);
18.
19. /* We need to get rid of the newline char. */
20. stripnl(fname);
21.
22. /* Open the file. If NULL is returned there was an error */
23. if((infile = fopen(fname, "r")) == NULL) {
24. printf("Error Opening File.\n");
25. exit(1);
26. }
27.
28. while( fgets(line, sizeof(line), infile) != NULL ) {
29. /* Get each line from the infile */
30. lcount++;
31. /* print the line number and data */
32. printf("Line %d: %s", lcount, line);
33. }
34.
35. fclose(infile); /* Close the file */
```

Options:

A- 9A.9
B- 17B.17
C- 20C.20
D- 32D.32
E- 35E.35

Answer:

B

Question 2

Question Type: MultipleChoice

What is a primary advantage a hacker gains by using encryption or programs such as Loki?

Options:

A- It allows an easy way to gain administrator rights
B- It is effective against Windows computers
C- It slows down the effective response of an IDS
D- IDS systems are unable to decrypt it
E- Traffic will not be modified in transit

Answer:

D

Explanation:

Because the traffic is encrypted, an IDS cannot understand it or evaluate the payload.

Question 3

Question Type: MultipleChoice

A company is using Windows Server 2003 for its Active Directory (AD). Whatis the most efficient way to crack the passwords for the AD users?

Options:

A- Perform a dictionary attack.
B- Perform a brute force attack.
C- Perform an attack with a rainbow table.

D- Perform a hybrid attack.

Answer:

C

Question 4

Question Type: MultipleChoice

A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program ina switched environmentnetwork. Which attack couldthe hacker useto sniff all of the packets in the network?

Options:

A- Fraggle
B- MAC Flood
C- Smurf
D- Tear Drop

Answer:

B

Question 5

Question Type: MultipleChoice

An engineer is learning to write exploits in C++ and is usingthe exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

Options:

A- g++ hackersExploit.cpp -o calc.exe
B- g++ hackersExploit.py -o calc.exe
C- g++ -i hackersExploit.pl -o calc.exe
D- g++ --compile --i hackersExploit.cpp -o calc.exe

Answer:

A

Question 6

Question Type: MultipleChoice

An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: netcat -l -p 1234 < secretfile

Machine B: netcat 192.168.3.4 > 1234

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

Options:

A- Machine A: netcat -l -p -s password 1234 < testfile
Machine B: netcat <machine A IP> 1234
B- Machine A: netcat -l -e magickey -p 1234 < testfile
Machine B: netcat <machine A IP> 1234
C- Machine A: netcat -l -p 1234 < testfile -pw password
Machine B: netcat <machine A IP> 1234 -pw password
D- Use cryptcat instead of netcat

Answer:

D

Explanation:

Netcat cannot encrypt the file transfer itself but would need to use a third party application to encrypt/decrypt like openssl. Cryptcat is the standard netcat enhanced with twofish encryption.

Question 7

Question Type: MultipleChoice

Which option best is not considered to be a part of active sniffing?

Options:

A- MAC Flooding
B- ARP Spoofing
C- SMAC Fueling
D- MAC Duplicating

Answer:

C

P2P exams

Question 8

Question Type: MultipleChoice

One way to defeat a multi-level security solution is to leak data via

Options:

A- a bypass regulator.
B- steganography.
C- a covert channel.
D- asymmetric routing.

Answer:

C

P2P exams

Question 9

Question Type: MultipleChoice

A developer for a companyis tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

Options:

A- if (billingAddress = 50) {update field} else exit
B- if (billingAddress != 50) {update field} else exit
C- if (billingAddress >= 50) {update field} else exit
D- if (billingAddress <= 50) {update field} else exit

Answer:

D

P2P exams

P2P exams

To Get Premium Files for CPEH-001 Visit

https://www.p2pexams.com/products/cpeh-001

For More Free Questions Visit

https://www.p2pexams.com/gaqm/pdf/cpeh-001

