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.geekcert.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

Lyle is a systems security analyst for Gusteffson and Sons, a large law firm in Beverly Hills. Lyle\\'s responsibilities include network vulnerability scans, Antivirus monitoring, and IDS monitoring. Lyle receives a help desk call from a user in the Accounting department. This user reports that his computer is running very slow all day long and it sometimes gives him an error message that the hard drive is almost full. Lyle runs a scan on the computer with the company antivirus software and finds nothing. Lyle downloads another free antivirus application and scans the computer again. This time a virus is found on the computer. The infected files appear to be Microsoft Office files since they are in the same directory as that software. Lyle does some research and finds that this virus disguises itself as a genuine application on a computer to hide from antivirus software. What type of virus has Lyle found on this computer?

A. This type of virus that Lyle has found is called a cavity virus.

B. Lyle has discovered a camouflage virus on the computer.

C. By using the free antivirus software, Lyle has found a tunneling virus on the computer.

D. Lyle has found a polymorphic virus on this computer

Correct Answer: C

QUESTION 2

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

A. Line number 31.

B. Line number 15

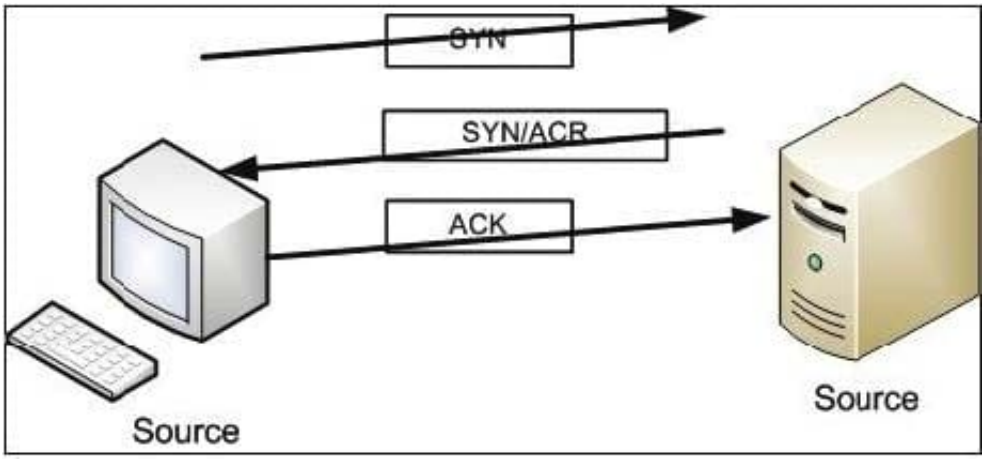
C. Line number 8

D. Line number 14

Correct Answer: B

QUESTION 3

Exhibit:



Please study the exhibit carefully.

Which Protocol maintains the communication on that way?

A. UDP

B. IP

C. TCP

D. ARP

E. RARP

Correct Answer: C

A TCP connection is always initiated with the 3-way handshake, which establishes and negotiates the actual connection over which data will be sent.

QUESTION 4

While footprinting a network, what port/service should you look for to attempt a zone transfer?

A. 53 UDP

B. 53 TCP

C. 25 UDP

D. 25 TCP

E. 161 UDP

F. 22 TCP

G. 60 TCP

Correct Answer: B

IF TCP port 53 is detected, the opportunity to attempt a zone transfer is there.

QUESTION 5

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency\\'s network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer\\'s manual but can\\'t find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency\\'s network is a switched network, which can\\'t be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency\\'s switched network?

A. ARP spoof the default gateway

B. Conduct MiTM against the switch

C. Launch smurf attack against the switch

D. Flood switch with ICMP packets

Correct Answer: A

ARP spoofing, also known as ARP poisoning, is a technique used to attack an Ethernet network which may allow an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether (known as a denial of service attack). The principle of ARP spoofing is to send fake, or \\'spoofed\\', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).