312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

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

QUESTION 1

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) then it was intended to hold. What is the most common cause of buffer overflow in software today?

A. Bad permissions on files.

B. High bandwidth and large number of users.

C. Usage of non standard programming languages.

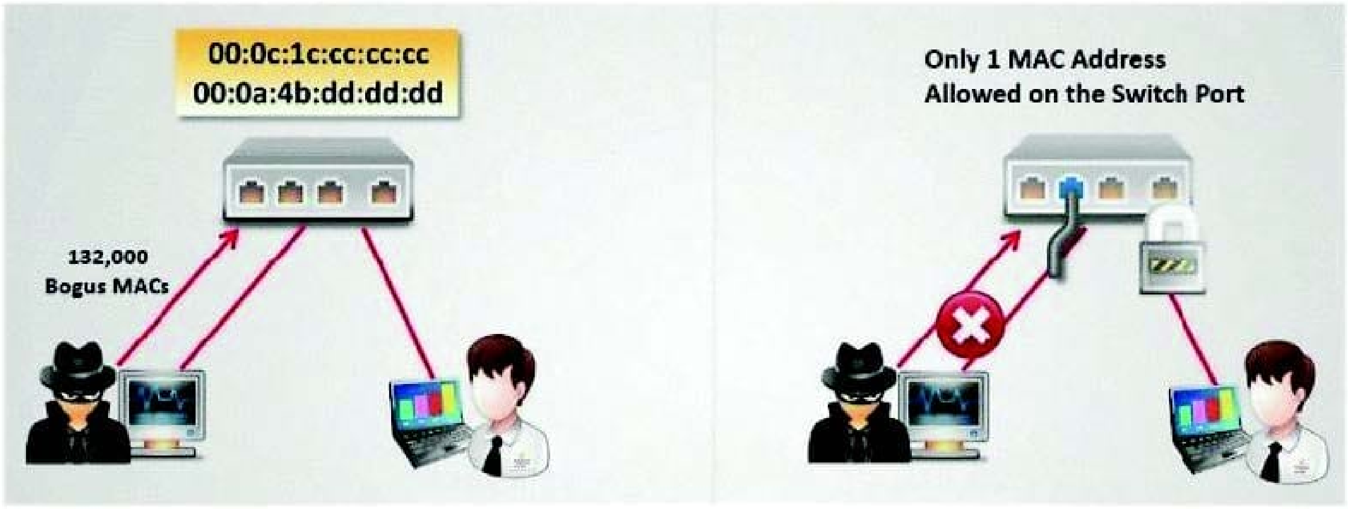
D. Bad quality assurance on software produced.

Correct Answer: D

Technically, a buffer overflow is a problem with the program\\'s internal implementation.

QUESTION 2

How do you defend against MAC attacks on a switch?



A. Disable SPAN port on the switch

B. Enable SNMP Trap on the switch

C. Configure IP security on the switch

D. Enable Port Security on the switch

Correct Answer: D

QUESTION 3

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption? Select the best answers.

A. PKI provides data with encryption, compression, and restorability.

B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.

C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.

D. RSA is a type of encryption.

Correct Answer: BD

PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public-key encryption WAS invented in 1976 by Whitfield Diffie and Martin Hellman. The famous hashing algorithm Diffie-Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

QUESTION 4

What does the term "Ethical Hacking" mean?

A. Someone who is hacking for ethical reasons.

B. Someone who is using his/her skills for ethical reasons.

C. Someone who is using his/her skills for defensive purposes.

D. Someone who is using his/her skills for offensive purposes.

Correct Answer: C

Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

QUESTION 5

Which type of hacker represents the highest risk to your network?

A. script kiddies

B. grey hat hackers

C. black hat hackers

D. disgruntled employees

Correct Answer: D

The disgruntled users have some permission on your database, versus a hacker who might not get into the database. Global Crossings is a good example of how a disgruntled employee -- who took the internal payroll database home on a hard drive -- caused big problems for the telecommunications company. The employee posted the names, Social Security numbers and birthdates of company employees on his Web site. He may have been one of the factors that helped put them out of business.

QUESTION 6

A denial of Service (DoS) attack works on the following principle:

A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.

B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.

C. Overloaded buffer systems can easily address error conditions and respond appropriately.

D. Host systems cannot respond to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).

E. A server stops accepting connections from certain networks one those network become flooded.

Correct Answer: D

Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service, such as a web site. This can be done by exercising a software bug that causes the software running the service to fail (such as the "Ping of Death" attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

QUESTION 7

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page can\\'t be reached. She contacts the website\\'s support team and they report that no one else is having any issues with the site. After handing the issue over to her company\\'s IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education\\'s server. Since Angela\\'s computer is behind a corporate firewall, her computer can\\'t ping the education website back.

What ca Angela\\'s IT department do to get access to the education website?

A. Change the IP on Angela\\'s Computer to an address outside the firewall

B. Change the settings on the firewall to allow all incoming traffic on port 80

C. Change the settings on the firewall all outbound traffic on port 80

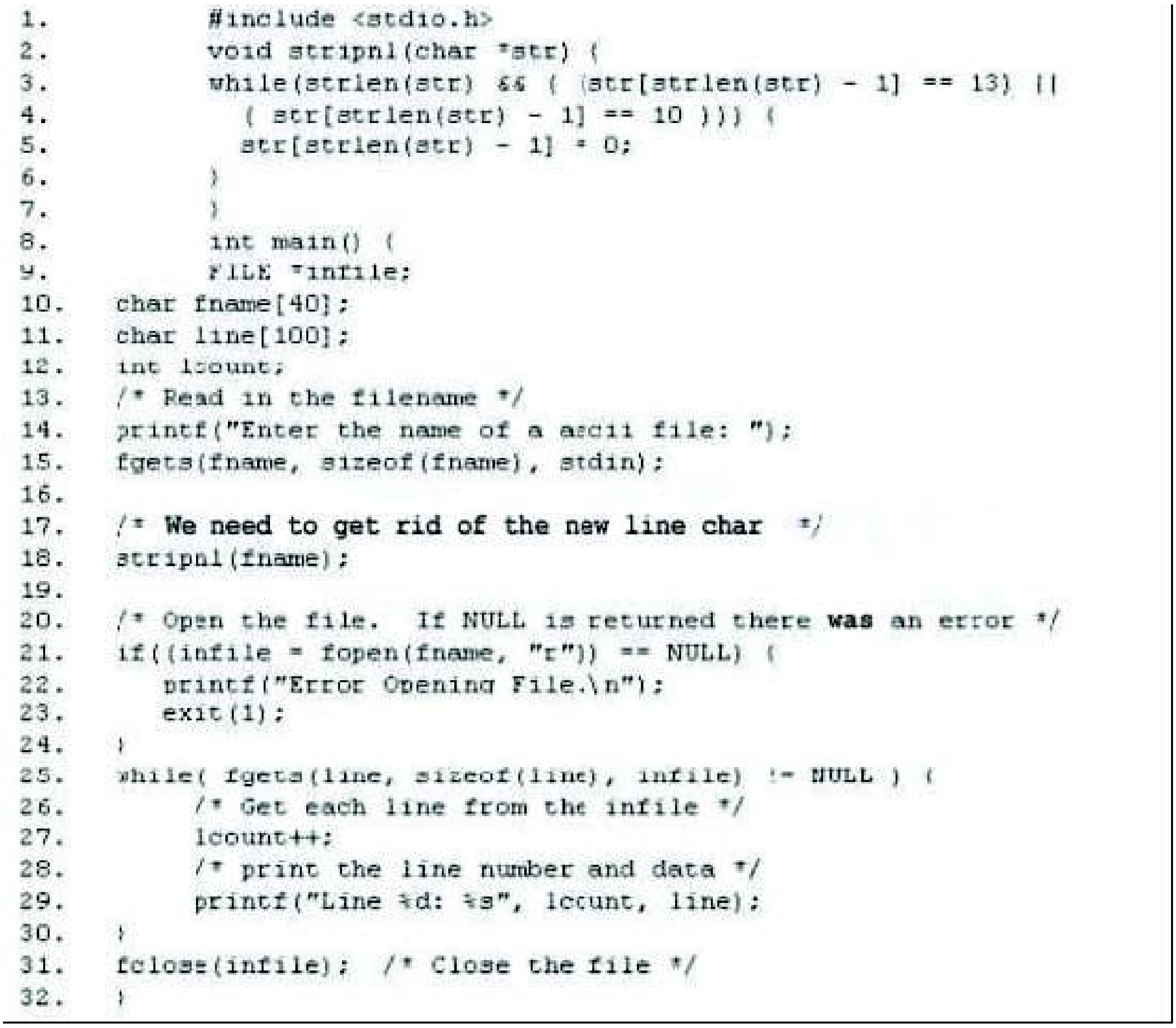
D. Use a Internet browser other than the one that Angela is currently using

Correct Answer: A

Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

QUESTION 8

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", lcount, 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 9

Bob is going to perform an active session hijack against company. He has acquired the target that allows session oriented connections (Telnet) and performs sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network.

So, what is Bob most likely to do next?

A. Take over the session.

B. Reverse sequence prediction.

C. Guess the sequence numbers.

D. Take one of the parties\\' offline.

Correct Answer: C

QUESTION 10

You want to perform advanced SQL Injection attack against a vulnerable website. You are unable to perform command shell hacks on this server. What must be enabled in SQL Server to launch these attacks?

A. System services

B. EXEC master access

C. xp_cmdshell

D. RDC

Correct Answer: C

QUESTION 11

While examining audit logs, you discover that people are able to telnet into the SMTP server on port

25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

A. Block port 25 at the firewall.

B. Shut off the SMTP service on the server.

C. Force all connections to use a username and password.

D. Switch from Windows Exchange to UNIX Sendmail.

E. None of the above.

Correct Answer: E

Blocking port 25 in the firewall or forcing all connections to use username and password would have the consequences that the server is unable to communicate with other SMTP servers. Turning of the SMTP service would disable the email function completely. All email servers use SMTP to communicate with other email servers and therefore changing email server will not help.

QUESTION 12

Yancey is a network security administrator for a large electric company. This company provides power for over 100,000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him. What would Yancey be considered?

A. Yancey would be considered a Suicide Hacker

B. Since he does not care about going to jail, he would be considered a Black Hat

C. Because Yancey works for the company currently; he would be a White Hat

D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Correct Answer: A

QUESTION 13

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company\\'s website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.

Where can Stephanie go to see past versions and pages of a website?

A. She should go to the web page Samspade.org to see web pages that might no longer be on the website

B. If Stephanie navigates to Search.com; she will see old versions of the company website

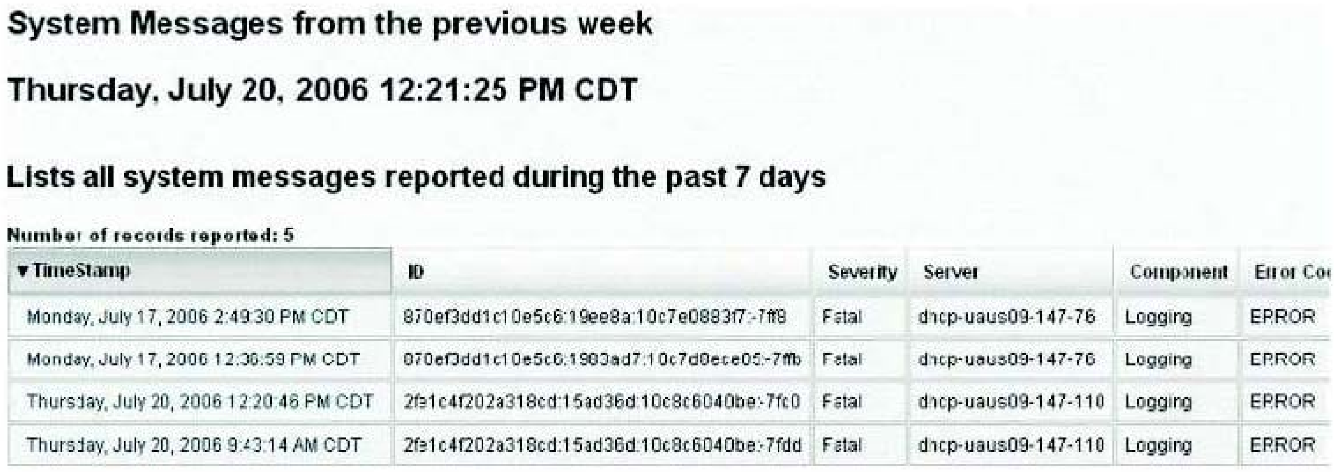
C. Stephanie can go to Archive.org to see past versions of the company website

D. AddressPast.com would have any web pages that are no longer hosted on the company\\'s website

Correct Answer: C

QUESTION 14

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to notify administrators of problems or performance.



System Messages from the previous week

Thursday, July 20, 2006 12:21:25 PM CDT

Lists all system messages reported during the past 7 days

Number of records reported: 5

▼TimeStamp	ID	Severity	Server	Component	Error Co
Monday, July 17, 2006 2:49:30 PM CDT	870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Monday, July 17, 2006 12:36:59 PM CDT	070ef3dd1c10e5c6:1983ad7:10c7d0ece05:-7ffb	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Thursday, July 20, 2006 12:20:46 PM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fc0	Fatal	dhcp-uaus09-147-110	Logging	ERROR
Thursday, July 20, 2006 9:43:14 AM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fdd	Fatal	dhcp-uaus09-147-110	Logging	ERROR

What default port Syslog daemon listens on?

A. 242

B. 312

C. 416

D. 514

Correct Answer: D

QUESTION 15

Theresa is the chief information security officer for her company, a large shipping company based out of New York City. In the past, Theresa and her IT employees manually checked the status of client computers on the network to see if they had the most recent Microsoft updates. Now that the company has added over 100 more clients to accommodate new departments, Theresa must find some kind of tool to see whether the clients are up-to-date or not. Theresa decides to use Qfecheck to monitor all client computers. When Theresa runs the tool, she is repeatedly told that the software does not have the proper permissions to scan. Theresa is worried that the operating system hardening that she performs on all clients is keeping the software from scanning the necessary registry keys on the client computers.

What registry key permission should Theresa check to ensure that Qfecheck runs properly?

A. In order for Qfecheck to run properly, it must have enough permission to read

B. She needs to check the permissions of the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates registry key

C. Theresa needs to look over the permissions of the registry key

D. The registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Microsoft must be checked

Correct Answer: B

Qfecheck check the registry HKLM\Software\Microsoft\Updates