NowExam

Higher Quality , Better Service !

Q&A

Exam : **312-38**

Title : Certified Network Defender

Version : DEMO

1.John works as a C programmer. He develops the following C program:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
char buffer1[10];
strcpy(buffer1, str);
return 1;
}
int main(int argc, char *argv[]) {
buffer (argv[1]);
printf("Executed\n");
return 1;
}
```

His program is vulnerable to a _____ attack.
A. SQL injection
B. Denial-of-Service
C. Buffer overflow
D. Cross site scripting
Answer: C
Explanation:
This program takes a user-supplied string and copies it into 'buffer1', which can hold up to 10 bytes of data. If a user sends more than 10 bytes, it would result in a buffer overflow.

2.DRAG DROP
Drag and drop the terms to match with their descriptions.

Terms		Description
Backdoor	Place Here	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Answer:

Terms		Description
Backdoor	Trojan horse	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Explanation:

Terms	Description
Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

A Trojan horse is a malicious software program that contains hidden code and masquerades itself as a normal program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard disk. An example of a Trojan horse is a program that masquerades as a computer logon to retrieve user names and password information. The developer of a Trojan horse can use this information later to gain unauthorized access to computers. Trojan horses are normally spread by e-mail attachments. Ping sweep is a technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. A ping is often used to check that a network device is functioning. To disable ping sweeps on a network, administrators can block ICMP ECHO requests from outside sources.
However, ICMP TIMESTAMP and ICMP INFO can be used in a similar manner. Spamware is software designed by or for spammers to send out automated spam e-mail. Spamware is used to search for e-mail addresses to build lists of e-mail addresses to be used either for spamming directly or to be sold to spammers. The spamware package also includes an e-mail harvesting tool. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

3.FILL BLANK
Fill in the blank with the appropriate term. _____ is the complete network

configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Answer:

NetRanger

Explanation:

NetRanger is the complete network configuration and information toolkit that includes the following tools: a Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

4.FILL BLANK

Fill in the blank with the appropriate term. A _____device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Answer:

biometric

Explanation:

A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits. Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided into two main classes:

Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent.

Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

5.Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

A. Wireless sniffer

B. Spectrum analyzer

C. Protocol analyzer

D. Performance Monitor

Answer: AC

Explanation:

Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications. Answer option D is incorrect. Performance Monitor is used to get

statistical information about the hardware and software components of a server. Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.