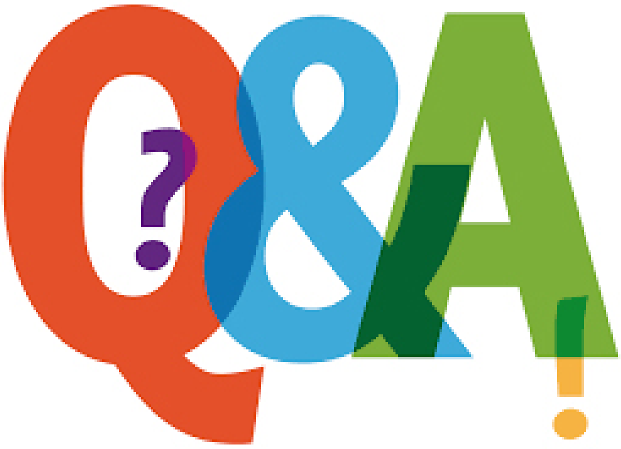


Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

killexams.com

EC-Council

312-38

EC-Council Certified Network Defender

Question: 371

Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?

A. IPS
B. HIDS
C. DMZ
D. NIDS

Answer: B

Explanation:
A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected.
Answer option D is incorrect. A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does.
Answer option A is incorrect. IPS (Intrusion Prevention Systems), also known as Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of "intrusion prevention systems" are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. An IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct CRC, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.
Answer option C is incorrect. DMZ, or demilitarized zone, is a physical or logical subnetwork that contains and exposes an organization’s external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization’s Local Area Network (LAN); an external attacker only has access to equipment in the DMZ rather than any other part of the network.

Question: 372

FILL BLANK
Fill in the blank with the appropriate term. The ______________is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions.

Answer: DCAP

Explanation:
The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

Question: 373

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:
It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.” Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd
B. Kismet
C. AirSnort

D. Cain

Answer: C

Explanation:

AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:

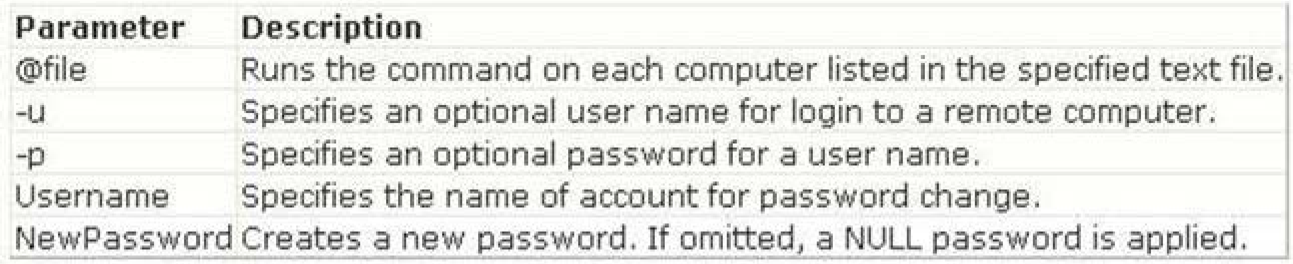
To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic

Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

Dictionary attack
Brute force attack
Rainbow attack
Hybrid attack

Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:

pspasswd [\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]



Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

Question: 374

Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?

A. Incident response
B. Incident handling
C. Incident management
D. Incident planning

Answer: A

Explanation:

Incident response is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference. One of the primary goals of incident response is to "freeze the scene". There is a close relationship between incident response, incident handling, and incident management. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Incident management manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred.

Answer option B is incorrect. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage.

Answer option C is incorrect. It manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option D is incorrect. This is an invalid option.

Question: 375

Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?

A. Sequence Number
B. Header Length
C. Acknowledgment Number
D. Source Port Address

Answer: D

Explanation:

Source Port Address is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment. Answer option C is incorrect. This is a 32-bit field that identifies the byte number that the sender of the segment is expecting to receive from the receiver.
Answer option B is incorrect. This is a 4-bit field that defines the 4-byte words in the TCP header. The header length can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 and 15. Answer option A is incorrect. This is a 32-bit field that identifies the number assigned to the first byte of data contained in the segment.

Question: 376

FILL BLANK
Fill in the blank with the appropriate term. ______________________ is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.

Answer: Network reconnaissance

Explanation:

Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

Question: 377

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.

Question: 378

In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

A. The router does not have a configuration file.
B. There is a need to set operating parameters.
C. The user interrupts the boot sequence.
D. The router does not find a valid operating system image.

Answer: DC

Explanation:

The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic tests. Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup mode when the user switches it on. Setup mode creates an initial configuration. Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

Question: 379

Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?

A. IGMP
B. ICMP
C. EGP
D. OSPF

Answer: C

Explanation:

EGP stands for Exterior Gateway Protocol. It is used for exchanging routing information between two gateways in a network of autonomous systems. This protocol depends upon periodic polling with proper acknowledgements to confirm that network connections are up and running, and to request for routing updates. Each router requests its neighbor at an interval of 120 to 480 seconds, for sending the routing table updates. The neighbor host then responds by sending its routing table. EGP-2 is the latest version of EGP.

Answer option B is incorrect. Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.

Answer option A is incorrect. Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks.

Answer option D is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

Question: 380

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.*

Question: 381

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.

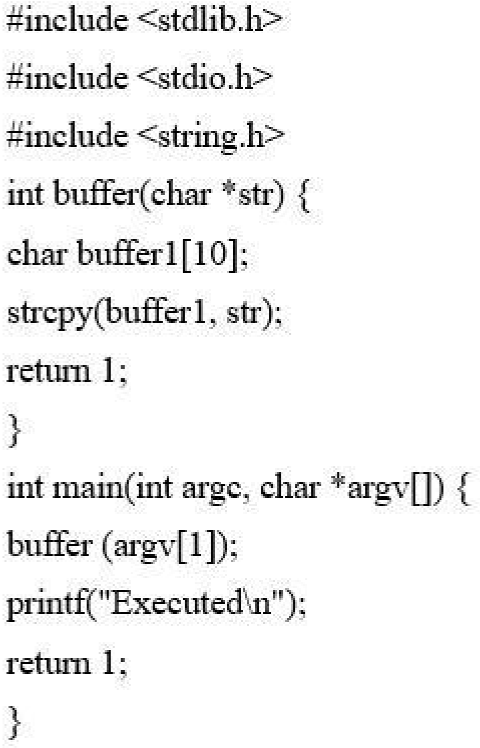
Answer: biometric

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:
1. 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.
2. Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

Question: 382

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

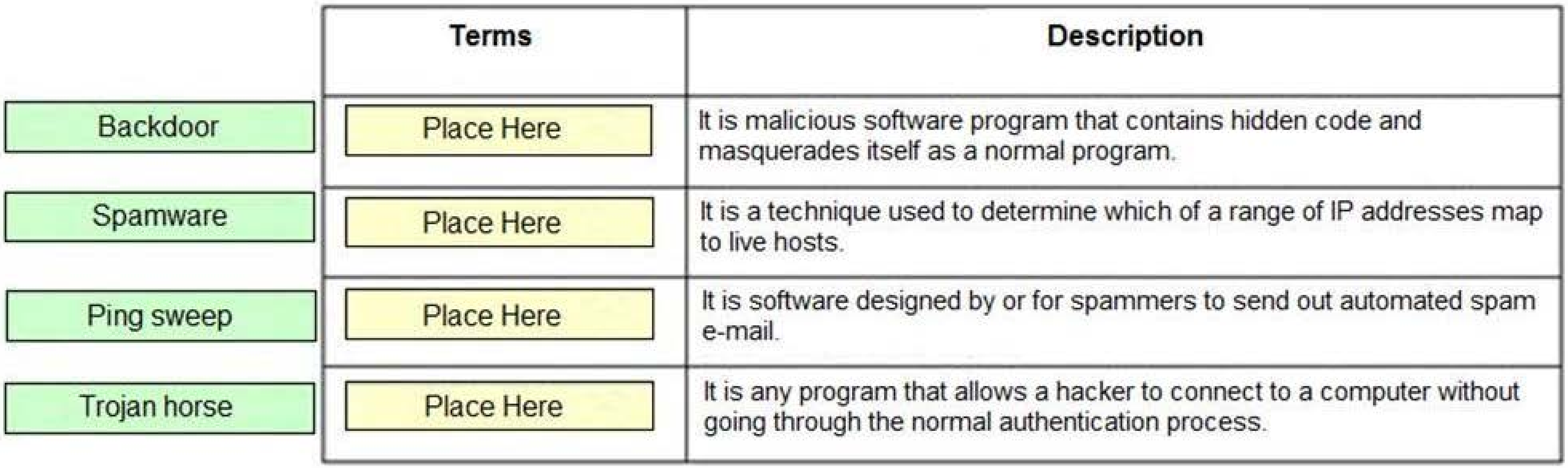
Answer: C

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.

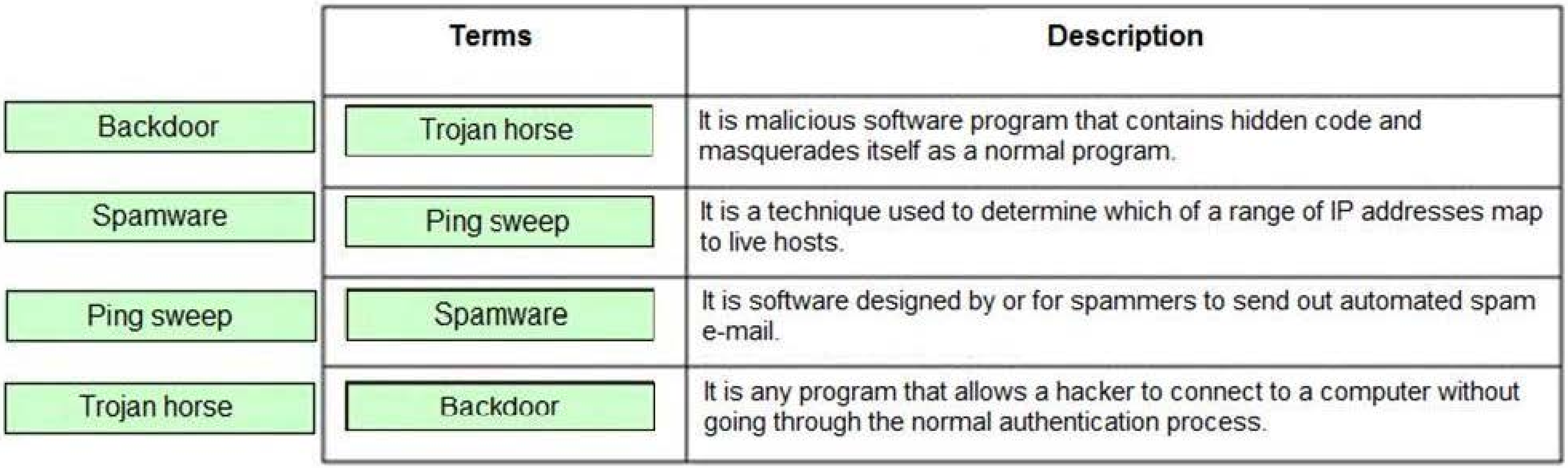
Question: 383

DRAG DROP
Drag and drop the terms to match with their descriptions.
Select and Place:



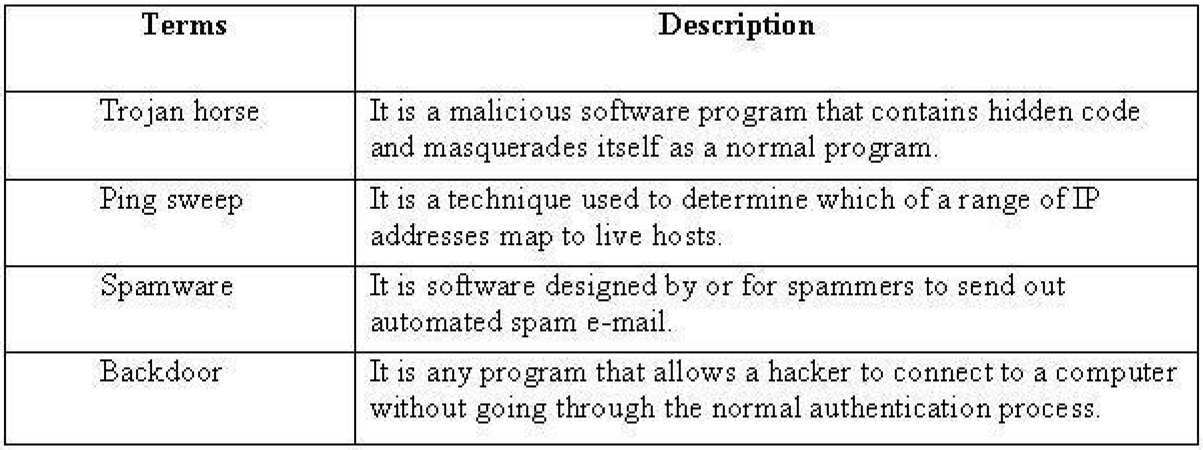
	Terms	Description
Backdoor	Place Here	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or 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:
Following are the terms with their descriptions:



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.