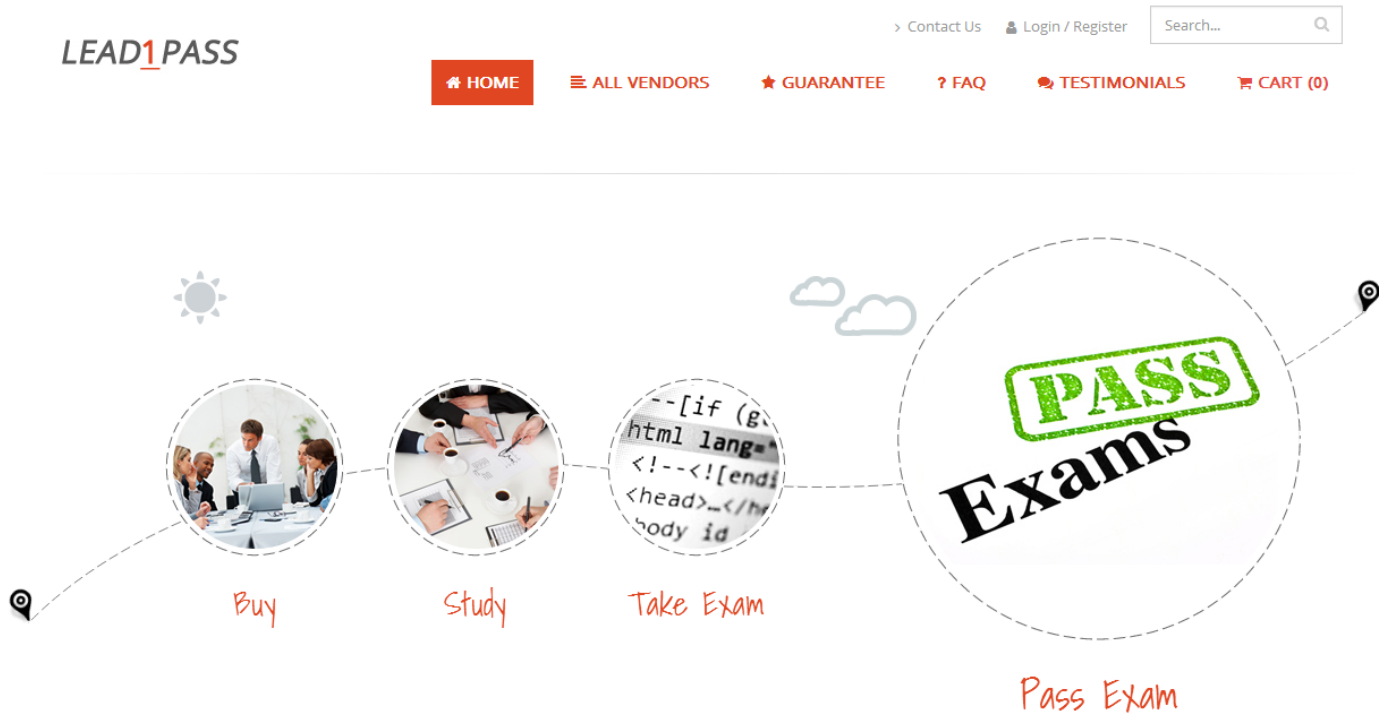
Lead1Pass



Try **PDF Demo** before you buy

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

http://www.lead1pass.com/

Latest Exam Guide & Learning Materials

Exam : **312-38**

Title : EC-Council Certified Network Defender CND

Vendor : EC-COUNCIL

Version : DEMO

NO.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.

NO.2 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.

NO.3 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.

NO.4 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.

NO.5 Drag and Drop Question

Drag and drop the terms to match with their descriptions.

	Terms	Description
Backdoor	Place Here	It is a 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 a 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.

NO.6 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: CD

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.

NO.7 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.

NO.8 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

NO.9 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

NO.10 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

NO.11 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:

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd

B. Kismet

C. AirSnort

D. Cain

Answer: C

NO.12 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

NO.13 Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?
A. Fire sprinkler
B. Fire suppression system
C. Fire alarm system
D. Gaseous fire suppression
Answer: C

NO.14 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

NO.15 Which of the following types of VPN uses the Internet as its main backbone, allowing users, customers, and branch offices to access corporate network resources across various network architectures?
A. PPTP VPN
B. Remote access VPN
C. Extranet-based VPN
D. Intranet-based VPN
Answer: C

NO.16 Which of the following is a protocol that describes an approach to providing "streamlined" support of OSI application services on top of TCP/IP-based networks for some constrained environments?
A. Network News Transfer Protocol
B. Lightweight Presentation Protocol
C. Internet Relay Chat Protocol
D. Dynamic Host Configuration Protocol
Answer: B

NO.17 You are an Administrator for a network at an investment bank. You are concerned about individuals breeching your network and being able to steal data before you can detect their presence and shut down their access. Which of the following is the best way to address this issue?
A. Implement a strong password policy.
B. Implement a strong firewall.

C. Implement a honey pot.
D. Implement network based anti virus.
Answer: C

NO.18 Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.
A. E-mail spam
B. Junk mail
C. Email spoofing
D. Email jamming
Answer: AB

NO.19 Which of the following is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic?
A. Nmap
B. Hping
C. NetRanger
D. PSAD
Answer: D

NO.20 Which of the following is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing?
A. Logical Link Control
B. Token Ring network
C. Distributed-queue dual-bus
D. CSMA/CA
Answer: C

NO.21 Which of the following is a distributed application architecture that partitions tasks or work loads between service providers and service requesters?Each correct answer represents a complete solution. Choose all that apply.
A. Client-server computing
B. Peer-to-peer (P2P) computing
C. Client-server networking
D. Peer-to-peer networking
Answer: AC

NO.22 Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?
A. Website defacement
B. Zero-day attack
C. Spoofing

D. Buffer overflow
Answer: A

NO.23 Which of the following cables is made of glass or plastic and transmits signals in the form of light?
A. Coaxial cable
B. Twisted pair cable
C. Plenum cable
D. Fiber optic cable
Answer: D

NO.24 Which of the following is a network that supports mobile communications across an arbitrary number of wireless LANs and satellite coverage areas?
A. LAN
B. WAN
C. GAN
D. HAN
Answer: C

NO.25 Fill in the blank with the appropriate term. A_____ network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token- passing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.
Answer:
Token Ring

NO.26 Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?
A. Spamming
B. War driving
C. War dialing
D. Warchalking
Answer: D

NO.27 Which of the following is a standard protocol for interfacing external application software with an information server, commonly a Web server?
A. DHCP
B. IP
C. CGI
D. TCP
Answer: C

NO.28 Which of the following honeypots provides an attacker access to the real operating system without any restriction and collects a vast amount of information about the attacker?

A. High-interaction honeypot
B. Medium-interaction honeypot
C. Honeyd
D. Low-interaction honeypot
Answer: A

NO.29 Which of the following representatives of the incident response team takes forensic backups of systems that are the focus of an incident?
A. Technical representative
B. Lead investigator
C. Information security representative
D. Legal representative
Answer: A

NO.30 Which of the following devices allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards?
A. Express card
B. WAP
C. WNIC
D. Wireless repeater
Answer: B

NO.31 Which of the following protocols uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets?
A. PPTP
B. ESP
C. LWAPP
D. SSTP
Answer: A

NO.32 Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service, or unauthorized changes to system hardware, software, or data?
A. Cyber Incident Response Plan
B. Crisis Communication Plan
C. Disaster Recovery Plan
D. Occupant Emergency Plan
Answer: A

NO.33 Which of the following TCP commands is used to allocate a receiving buffer associated with the specified connection?
A. Send
B. Close

C. Abort
D. Receive
Answer: D

NO.34 You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. History folder
B. Temporary Internet Folder
C. Cookies folder
D. Download folder
Answer: ABC

NO.35 Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?
A. Transport layer
B. Link layer
C. Internet layer
D. Application layer
Answer: A