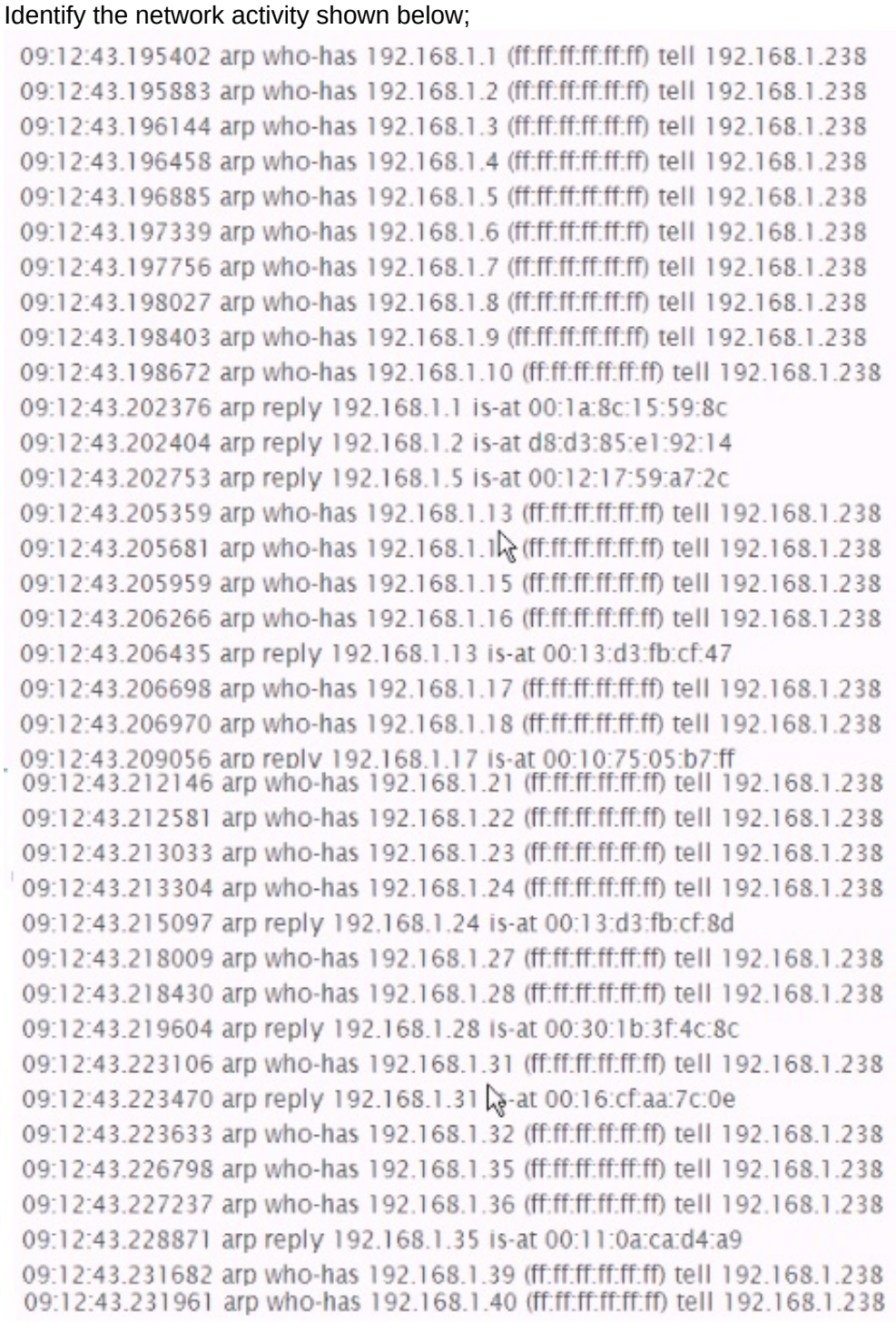
GIAC

Exam Questions GPEN

GIAC Certified Penetration Tester

NEW QUESTION 1
- (Topic 1)
Identify the network activity shown below;



A. A sweep of available hosts on the local subnet
B. A flood of the local switch's CAM tabl
C. An attempt to disassociate wireless client
D. An attempt to impersonate the local gateway

Answer: D

NEW QUESTION 2
- (Topic 1)
You've been asked to test a non-transparent proxy lo make sure it is working. After confirming the browser is correctly pointed at the proxy, you try to browse a web site. The browser indicates it is "loading" but never displays any part the page. Checking the proxy, you see a valid request in the proxy from your browser. Checking the response to the proxy, you see the results displayed in the accompanying screenshot. Which of the following answers is the most likely reason the browser hasn't displayed the page yet?

A. The proxy is likely hung and must be restarte
B. The proxy is configured to trap response
C. The proxy is configured to trap request
D. The site you are trying to reach is currently dow

Answer: C

NEW QUESTION 3
- (Topic 1)
During a penetration test you discover a valid set of SSH credentials to a remote system. How can this be used to your advantage in a Nessus scan?

A. This information can be entered under the 'Hydra' tab to launch a brute-forcepassword attac
B. There isn't an advantage as Nessus will ultimately discover this informatio
C. The "SSH' box can be checked to let Nessus know the remote system is running
D. This information can be entered under the 'credentials' tab to allow Nessus to log into the system

Answer: C

NEW QUESTION 4
- (Topic 1)
What is the main difference between LAN MAN and NTLMv1 challenge/responses?

A. NTLMv1 only pads IS bytes, whereas LANMAN pads to 21 bytes
B. NTLMv1 starts with the NT hash, whereas LANMAN starts with the LANMAN hash
C. NTLMv1utilizes DES, whereas LANMAN utilizes MD4
D. NTLMv1 splits the hash into 3 eight-byte pieces, whereas LAN MAN splits the hash Into 3 seven-byte pieces

Answer: A

NEW QUESTION 5
- (Topic 1)
You are pen testing a Windows system remotely via a raw netcat shell. You want to get a listing of all the local users in the administrators group, what command would you use?

A. Net account administrators
B. Net user administrators
C. Net localgroup administrators
D. Net localuser administrators

Answer: C

NEW QUESTION 6
- (Topic 1)
You are running a vulnerability scan on a remote network and the traffic Is not making It to the target system. You investigate the connection issue and determine that the traffic is making it to the internal interface of your network firewall, but not making. It to the external Interface or to any systems outside your firewall. What is the most likely problem?

A. Your network firewall is blocking the traffic
B. The NAT or pat tables on your network based firewall are filling up and droppingthe traffic
C. A host based firewall is blocking the traffic
D. Your ISP Is blocking the traffic

Answer: C

NEW QUESTION 7
- (Topic 1)
Raw netcat shells and telnet terminals share which characteristic?

A. Ability to send commands to a target machin
B. Ability to adapt output to the size of display window
C. Shells and terminals are exactly the sam
D. Ability to process standard output control sequence

Answer: D

Explanation:
Reference:
http://tartarus.org/~simon/putty-snapshots/htmldoc/Chapter3.html

NEW QUESTION 8
- (Topic 1)
You suspect that system administrators In one part of the target organization are turning off their systems during the times when penetration tests are scheduled, what feature could you add to the ' Rules of engagement' that could help your team test that part of the target organization?

A. Un announced test
B. Tell response personnel the exact lime the test will occur
C. Test systems after normal business hours
D. Limit tests to business hours

Answer: C

NEW QUESTION 9
- (Topic 1)
Which type of Cross-Sire Scripting (XSS> vulnerability is hardest for automated testing tools to detect, and for what reason?

A. Stored XS
B. because it may be located anywhere within static or dynamic sitecontent
C. Stored XS
D. because it depends on emails and instant messaging system
E. Reflected XS
F. because It can only be found by analyzing web server response
G. Reflected XSS: because it is difficult to find within large web server log

Answer: A

NEW QUESTION 10
- (Topic 1)
You suspect that a firewall or IPS exists between you and the target machine. Which nmap option will elicit responses from some firewalls and IPSs while being silently dropped by the target, thus confirming the existence of a firewall or IPS?

A. –Traceroute
B. –Firewalk
C. –Badsum
D. --SF

Answer: B

NEW QUESTION 10
168.1 200, which of the following would you see?

A. Ping-n 1 192.168.1 200 on the compromised system
B. A 'Destination host unreachable' error message on the compromised system
C. A packet containing 'Packets: Sent - 1 Received = 1, Loss = 0 (0% loss) on yoursniffer
D. An ICMP Echo packet on your sniffer containing the source address of the target

Answer: A

NEW QUESTION 13
- (Topic 1)
Which of the following modes describes a wireless interface that is configured to passively grab wireless frames from one wireless channel and pass them to the operating system?

A. Monitor Mode
B. Promiscuous Mode
C. Managed Mode
D. Master Mode

Answer: C

Explanation:
Reference:
http://www.willhackforsushi.com/books/377_eth_2e_06.pdf

NEW QUESTION 16
- (Topic 1)
What section of the penetration test or ethical hacking engagement final report is used to detail and prioritize the results of your testing?

A. Methodology
B. Conclusions
C. Executive Summary
D. Findings

Answer: C

NEW QUESTION 18
- (Topic 1)
Your company has decided that the risk of performing a penetration test Is too great. You would like to figure out other ways to find vulnerabilities on their systems, which of the following is MOST likely to be a valid alternative?

A. Network scope Analysis
B. Baseline Data Reviews
C. Patch Policy Review
D. Configuration Reviews

Answer: A

NEW QUESTION 23

- (Topic 1)
Which of the following is the number of bits of encryption that 64-bit Wired Equivalent Privacy (WEP) effectively provides?

A. 64
B. 40
C. 60
D. 44

Answer: A

Explanation:
Reference:
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

NEW QUESTION 25
- (Topic 1)
Approximately how many packets are usually required to conduct a successful FMS attack onWEP?

A. 250.000
B. 20.000
C. 10.000,000
D. l (with a weak IV)

Answer: B

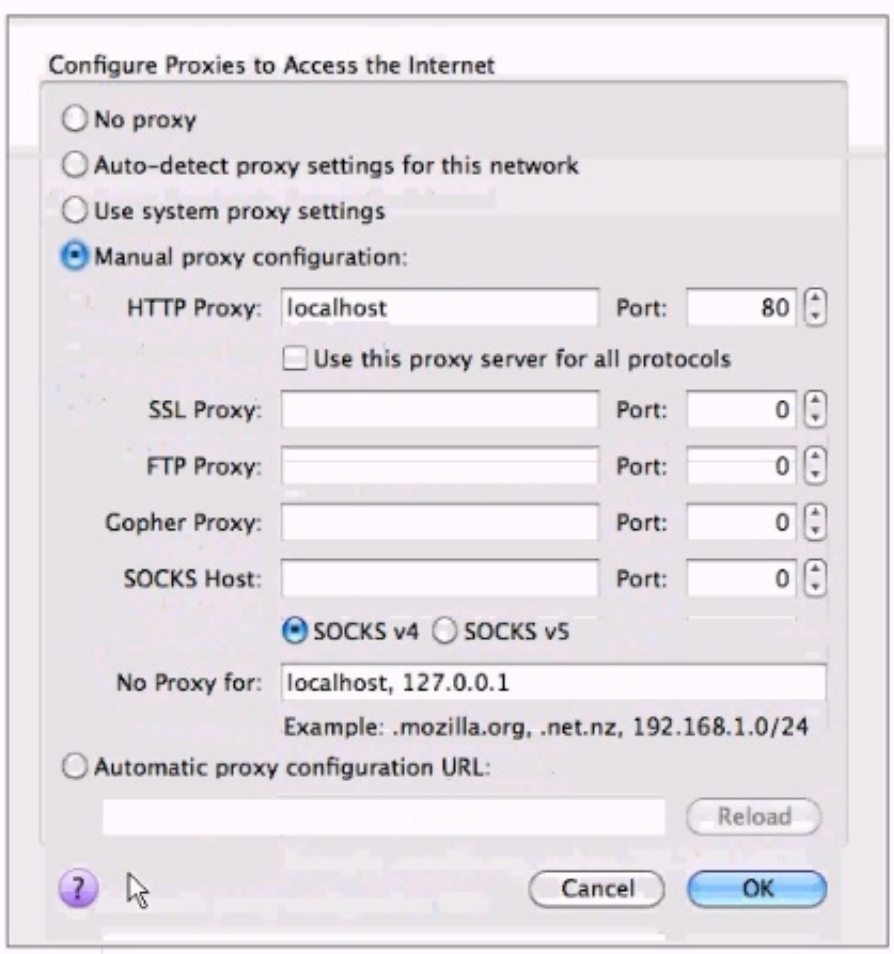
NEW QUESTION 28
- (Topic 1)
A customer has asked for a scan or vulnerable SSH servers. What is the penetration tester attempting to accomplish using the following Nmap command?

```
# nmap -n -sV --script=sshv1.nse 10.10.10.60 -p 22
```

A. Checking operating system version
B. Running an exploit against the target
C. Checking configuration
D. Checking protocol version

Answer: D

NEW QUESTION 29
- (Topic 1)
A junior penetration tester at your firm is using a non-transparent proxy for the first time to test a web server. He sees the web site In his browser but nothing shows up In the proxy. He tells you that he just installed the non-transparent proxy on his computer and didn't change any defaults. After verifying the proxy is running, you ask him to open up his browser configuration, as shown in the figure, which of the following recommendations will correctly allow him to use the transparent proxy with his browser?



A. He should change the PORT: value to match the port used by the non-transparentprox
B. He should select the checkbox "use this proxy server for all protocols" for theproxy to function correctl
C. He should change the HTTP PROXY value to 127.0.0.1 since the non-transparentproxy is running on the same machine as the browse
D. He should select NO PROXY instead of MANUAL PROXY CONFIGURATION as thissetting is only necessary to access the Internet behind protected network

Answer: C

NEW QUESTION 30
- (Topic 1)
You are performing a vulnerability assessment using Nessus and your clients printers begin printing pages of random text and showing error messages. The client is not happy with the situation. What is the best way to proceed?

A. Enable the "Skip all primers" option and re-scan
B. Ensure Safe Checks is enabled in Nessus scan policies
C. Remove primer IP addresses from your target list
D. Verify primers are in scope and tell the client In progress scans cannot be stopped

Answer: B

NEW QUESTION 32
- (Topic 1)
When sniffing wireless frames, the interface mode plays a key role in successfully collecting traffic. Which of the mode or modes are best used for sniffing wireless traffic?

A. Master Ad-hoc
B. RFMON
C. RFMO
D. Ad-hoc
E. Ad-hoc

Answer: A

Explanation:
Reference:
http://www.willhackforsushi.com/books/377_eth_2e_06.pdf

NEW QUESTION 37
- (Topic 1)
What is the most likely cause of the responses on lines 10 and 11 of the output below?

```
<pre>
C:\>tracert -d 66.35.45.201

Tracing route to 66.35.45.201
over a maximum of 30 hops:

1 1 ms 1 ms <1 ms 192.168.1.1
2 10 ms 7 ms 8 ms 10.4.192.1
3 7 ms 11 ms 9 ms 68.12.8.94
4 15 ms 11 ms 21 ms 68.12.8.58
5 16 ms 11 ms 11 ms 68.12.14.0
6 17 ms 13 ms 14 ms 68.1.0.142
7 34 ms 35 ms 37 ms 206.222.119.58
8 33 ms 32 ms 31 ms 66.35.46.50
9 39 ms 35 ms 49 ms 66.35.46.62
10 * * * Request timed out.
11 * * * Request timed out.
</pre>
```

A. The device at hop 10 silently drops UDP packets with a high destination por
B. The device at hop 10 is down and not forwarding any requests at al
C. The host running the tracer utility lost its network connection during the scan
D. The devices at hops 10 and II did not return an "ICMP TTL Exceeded in Transit" messag

Answer: D

NEW QUESTION 40
- (Topic 1)
You are using the Nmap Scripting Engine and want detailed output of the script as it runs. Which option do you include in the command string?

A. Nmap --script-output -script-SSH-hostkey.nse 155.65.3.221 -p 22
B. Nmap --script-trace --script-ssh-hostkey.nse 155.65.3.221 -p 22
C. Nmap -script-verbose --scrlpr-ssh-hostkey.nse 155.65.3.221 -p 22
D. Nmap -v --script=ssh-hostkey.nse 155.65.3.221 -p 22

Answer: C

NEW QUESTION 41
- (Topic 1)
What is the purpose of die following command:
nc.exe -I -p 2222 -e cmd.exe

A. It is used to start a persistent listener linked to cmd.exe on port 2222 TCP
B. It is used to start a listener linked to cmd.exe on port 2222 TCP
C. It is used to start a listener linked to cmd.exe on port 2222 UDP
D. It is used to start a persistent listener linked to cmd.exe on port 2222 UDP

Answer: C

NEW QUESTION 45
- (Topic 1)
You have been contracted to penetration test an e-mail server for a client that wants to know for sure if the sendmail service is vulnerable to any known attacks. You have permission to run any type of test, how will you proceed to give the client the most valid answer?

A. Run all known sendmail exploits against the server and see if you can compromisethe service, even if it crashed the machine or service
B. Run a banner grabbing vulnerability checker to determine the sendmail version andpatch level, then look up and report all the vulnerabilities that exist for that versionand patch level
C. Run all sendmail exploits that will not crash the server and see if you cancompromise the service
D. Log into the e-mail and determine the sendmail version and patch level, then lookup and report all the vulnerabilities that exist for that version and patch level

Answer: C

NEW QUESTION 48
- (Topic 1)
You have gained shell on a Windows host and want to find other machines to pivot to, but the rules of engagement state that you can only use tools that are already available. How could you find other machines on the target network?

A. Use the "ping" utility to automatically discover other hosts
B. Use the "ping" utility in a for loop to sweep the networ
C. Use the "edit" utility to read the target's HOSTS fil
D. Use the "net share" utility to see who is connected to local shared drive

Answer: B

Explanation:
Reference:
http://www.slashroot.in/what-ping-sweep-and-how-do-ping-sweep

NEW QUESTION 49
- (Topic 1)
Analyze the command output below, what action is being performed by the tester?

```
C:\>enum -UPG 192.168.116.101
server: 192.168.116.101
setting up session... success.
password policy:
min length: none
min age: none
max age: 180 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest ksmith dlaw
IUSR_Anonymous
Group: Administrators
WORKGROUP\Administrator
WORKGROUP\ksmith
Group: Guests
WORKGROUP\Guest
WORKGROUP\IUSR_Anonymous
WORKGROUP\dlaw
Group: Power Users
cleaning up... success.
```

A. Displaying a Windows SAM database
B. Listing available workgroup services
C. Discovering valid user accounts
D. Querying locked out user accounts

Answer: C

NEW QUESTION 54
- (Topic 1)
You are pen testing a network and have shell access to a machine via Netcat. You try to use ssh to access another machine from the first machine. What is the expected result?

A. The ssh connection will succeed If you have root access on the intermediate machine
B. The ssh connection will fail
C. The ssh connection will succeed
D. The ssh connection will succeed if no password required

Answer: C

NEW QUESTION 55
- (Topic 2)
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Man-in-the-middle
B. ARP spoofing
C. Port scanning
D. Session hijacking

Answer: B

NEW QUESTION 59
- (Topic 2)
You want to find out what ports a system is listening on. What Is the correct command on a Linux system?

A. netstat nap
B. f port/p
C. tasklist/v
D. Isof -nao

Answer: A

Explanation:
Reference:
http://cbl.abuseat.org/advanced.html

NEW QUESTION 60
- (Topic 2)
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 lis
B. You want to transfer file hostlist.txt to the hosts given in the IP address lis
C. You want to perform banner grabbing to the hosts given in the IP address lis
D. You want to put nmap in the listen mode to the hosts given in the IP address lis

Answer: C

NEW QUESTION 63
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He enters the following command on the Linux terminal:chmod 741 secure.c
Considering the above scenario, which of the following statements are true?
Each correct answer represents a complete solution. Choose all that apply.

A. John is restricting a guest to only write or execute the secure.c fil
B. John is providing all rights to the owner of the fil
C. By the octal representation of the file access permission, John is restricting the group members to only read the secure.c fil
D. The textual representation of the file access permission of 741 will be -rwxr--rw-.

Answer: BC

NEW QUESTION 68
- (Topic 2)
Analyze the output of the two commands below:

```
user@desktop:~$ sudo traceroute -w 2 -n 10.63.104.1
1 192.168.116.1 1 ms 0 ms 0 ms
2 10.55.208.130 21 ms 23 ms 17 ms
3 10.55.208.129 16 ms 13 ms 14 ms
4 10.63.104.82 14 ms 14 ms 15 ms
5 10.63.104.206 16 ms 14 ms 16 ms
6 10.63.104.1 * * *

user@desktop:~$ ping -c2 10.63.104.1
PING 10.63.104.1 (10.63.104.1) 56(84) bytes of data.
64 bytes from 10.63.104.1: icmp_seq=1 ttl=251 time=20.8 ms
64 bytes from 10.63.104.1: icmp_seq=2 ttl=251 time=15.6 ms
```

Which of the following can be factually inferred from the results of these commands?

A. The router 192.16S.U6.1 is filtering UDP tracerout
B. The host 10.63.104.1 is silently dropping UDP packet
C. The host 10.63.104.1 is not issuing ICMP packet
D. The router 10 63.104 206 is dropping ICMP tracerout

Answer: C

NEW QUESTION 70
- (Topic 2)
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. Rick, your assistant, is configuring some laptops for wireless access. For security, WEP needs to be configured for wireless communication. By mistake, Rick configures different WEP keys in a laptop than that is configured on the Wireless Access Point (WAP). Which of the following statements is true in such situation?

A. The laptop will be able to access the wireless network but the security will be compromised
B. The WAP will allow the connection with the guest account's privilege
C. The laptop will be able to access the wireless network but other wireless devices will be unable to communicate with i
D. The laptop will not be able to access the wireless networ

Answer: D

NEW QUESTION 71
- (Topic 2)
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. Capture data on port 53 and performing banner grabbin
B. Capture data on port 53 and delete the remote shel
C. Listen the incoming traffic on port 53 and execute the remote shel
D. Listen the incoming data and performing port scannin

Answer: C

NEW QUESTION 76
- (Topic 2)
You work as a Web developer in the IBM Inc. Your area of proficiency is PHP. Since you have proper knowledge of security, you have bewared from rainbow attack. For mitigating this attack, you design the PHP code based on the following algorithm:
key = hash(password + salt)
for 1 to 65000 do
key = hash(key + salt)
Which of the following techniques are you implementing in the above algorithm?

A. Key strengthening
B. Hashing
C. Sniffing
D. Salting

Answer: A

NEW QUESTION 77
- (Topic 2)
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. Prepared statement
C. mysql_escape_string()
D. session_regenerate_id()

Answer: AB

NEW QUESTION 81
- (Topic 2)
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

NEW QUESTION 85
- (Topic 2)
Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. snort_inline

B. EtherApe
C. Snort decoder
D. AirSnort

Answer: C

NEW QUESTION 90
- (Topic 2)
You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?
Each correct answer represents a complete solution. Choose two.

A. MAC filtering the router
B. Using WPA encryption
C. Using WEP encryption
D. Not broadcasting SSID

Answer: BC

NEW QUESTION 92
- (Topic 2)
Which of the following Web authentication techniques uses a single sign-on scheme?

A. NTLM authentication
B. Microsoft Passport authentication
C. Basic authentication
D. Digest authentication

Answer: B

NEW QUESTION 94
- (Topic 2)
Which of the following Nmap commands is used to perform a UDP port scan?

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

Answer: D

NEW QUESTION 95
- (Topic 2)
Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Windows XP
B. Mac OS
C. MINIX 3
D. Linux

Answer: B

NEW QUESTION 99
- (Topic 2)
Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?
Each correct answer represents a part of the solution. Choose two.

A. WPA2 -EAP
B. WPA-PSK
C. WPA-EAP
D. WEP

Answer: BD

NEW QUESTION 102
- (Topic 2)
You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -B
B. tcpdump -dd
C. tcpdump -w
D. tcpdump –d

Answer: C

NEW QUESTION 103
- (Topic 2)
You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP
B. Implement MAC filtering
C. Don't broadcast SSID
D. Implement WPA

Answer: C

NEW QUESTION 104
- (Topic 2)
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 the Bluehill Inc. For this, you start monitoring the network traffic of the Bluehill Inc.
In this process, you get that there are too many FTP packets traveling in the Bluehill Inc. network.
Now, you want to sniff the traffic and extract usernames and passwords of the FTP server. Which of the following tools will you use to accomplish the task?

A. Ettercap
B. L0phtcrack
C. NetStumbler
D. SARA

Answer: A

NEW QUESTION 106
- (Topic 2)
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 attack
B. Deletes the entire members tabl
C. Deletes the rows of members table where email id is 'attacker@somehwere.com' give
D. Deletes the database in which members table reside

Answer: B

NEW QUESTION 107
- (Topic 2)
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. The remote server is dow
B. You have entered any special character in emai
C. Your internet connection is slo
D. Email entered is not vali

Answer: B

NEW QUESTION 112
- (Topic 2)
Anonymizers are the services that help make a user's own Web surfing anonymous. An anonymizer removes all the identifying information from a user's computer while the user surfs the Internet. It ensures the privacy of the user in this manner. After the user anonymizes a Web access with an anonymizer prefix, every subsequent link selected is also automatically accessed anonymously. Which of the following are limitations of anonymizers?
Each correct answer represents a complete solution. Choose all that apply.

A. Java applications
B. Secure protocols
C. ActiveX controls
D. JavaScript
E. Plugins

Answer: ABCDE

NEW QUESTION 117
- (Topic 2)
You want to run the nmap command that includes the host specification of 202.176.56-57.*.
How many hosts will you scan?

A. 512
B. 64
C. 1024
D. 256

Answer: A

NEW QUESTION 122
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

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

A. AirSnort
B. PsPasswd
C. Cain
D. Kismet

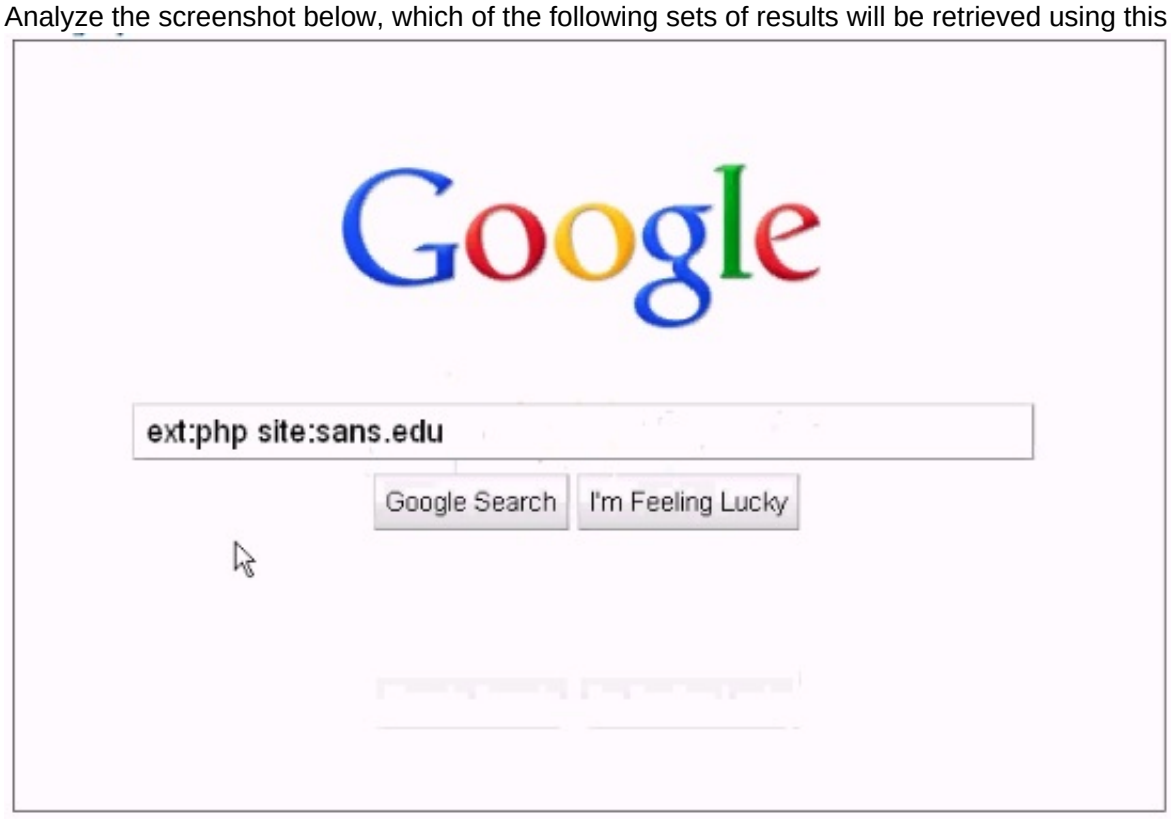
Answer: A

NEW QUESTION 124
- (Topic 2)
You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. History folder
B. Temporary Internet Folder
C. Cookies folder
D. Download folder

Answer: ABC

NEW QUESTION 125
- (Topic 2)
Analyze the screenshot below, which of the following sets of results will be retrieved using this search?



A. Pages from the domain sans.edu that have external link
B. Files of type .php from the domain sans.ed
C. Pages that contain the term ext:php and slte.sans.ed
D. Files of type .php that redirect to the sans.edu domai

Answer: A

NEW QUESTION 130
- (Topic 2)
Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack
B. Cross-Site Scripting attack
C. Cross-Site Request Forgery
D. Code injection attack

Answer: D

NEW QUESTION 135
- (Topic 2)
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-are-secure 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 session_regenerate_id() function
B. Use the escapeshellcmd() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellarg() function

Answer: C

NEW QUESTION 137
- (Topic 2)
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 zombie computer is not connected to the we-are-secure.com Web serve
B. The zombie computer is the system interacting with some other system besides your comp ute
C. Hping does not perform idle scannin
D. The firewall is blocking the scanning proces

Answer: B

NEW QUESTION 140
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network:
l Gathering information
l Determining the network range
l Identifying active systems
Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. APNIC
B. SuperScan
C. RIPE
D. ARIN

Answer: B

NEW QUESTION 142
CORRECT TEXT - (Topic 2)
Fill in the blank with the appropriate tool name.
_____is a wireless network cracking tool that exploits the vulnerabilities in the RC4 Algorithm, which comprises the WEP security parameters.

A.

Answer: WEPcrack

NEW QUESTION 143
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server.
The output of the scanning test is as follows:
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?
Each correct answer represents a complete solution. Choose all that apply.

A. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacke
B. The countermeasure to 'printenv' vulnerability is to remove the CGI scrip
C. This vulnerability helps in a cross site scripting attac
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious script

Answer: BCD

NEW QUESTION 148
- (Topic 2)

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

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

Answer: B

NEW QUESTION 150
- (Topic 2)
How many bits encryption does SHA-1 use?

A. 140
B. 512
C. 128
D. 160

Answer: D

NEW QUESTION 153
- (Topic 2)
The scope of your engagement is to include a target organization located in California with a /24 block of addresses that they claim to completely own. Which site could you utilize to confirm that you have been given accurate information before starting reconnaissance activities?

A. www.whois.net
B. www.arin.nei
C. www.apnic.net
D. www.ripe.net

Answer: B

NEW QUESTION 157
- (Topic 2)
Joseph works as a Network Administrator for WebTech Inc. He has to set up a centralized area on the network so that each employee can share resources and documents with one another. Which of the following will he configure to accomplish the task?

A. WEP
B. VPN
C. Intranet
D. Extranet

Answer: C

NEW QUESTION 162
- (Topic 2)
What will the following scapy commands do?

```
>>> packet=IP(dst="192.168.1/24")/TCP(dport=[80,8080],flags="SA")
>>> ans,unans=sr(packet)
```

A. Perform a SYN-ACK scan against TCP ports 80 and 3080 on host 192.168.1.24.
B. Perform a SYN scan against ports 80 through 8080 for all hosts on the192.168.1.0/24 networ
C. Combine the answered and unanswered results of a previous scan into the sr(packet)variabl
D. Perform a SYN-ACK scan against TCP ports 80 and 8080 for all hosts on the192.16S.1.0/24 networ

Answer: D

NEW QUESTION 163
- (Topic 2)
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: ABC

NEW QUESTION 164
- (Topic 3)
You work as a Network Administrator for Tech-E-book Inc. You are configuring the ISA Server
2006 firewall to provide your company with a secure wireless intranet. You want to accept inbound mail delivery though an SMTP server. What basic rules of ISA Server do you need to configure to accomplish the task.

A. Network rules
B. Publishing rules
C. Mailbox rules
D. Access rules

Answer: B

NEW QUESTION 167
- (Topic 3)
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 -sS
C. nmap -sU -p
D. nmap –sT

Answer: A

NEW QUESTION 168
- (Topic 3)
You work as an IT Technician for uCertify Inc. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company's wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. MAC Filtering
B. SSID
C. RAS
D. WEP

Answer: A

NEW QUESTION 173
- (Topic 3)
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 Website. The we-are-secure.com Web server is using Linux operating system. When you port scanned the we-are-secure.com Web server, you got that TCP port 23, 25, and 53 are open. When you tried to telnet to port 23, you got a blank screen in response. When you tried to type the dir, copy, date, del, etc. commands you got only blank spaces or underscores symbols on the screen. What may be the reason of such unwanted situation?

A. The telnet session is being affected by the stateful inspection firewal
B. The telnet service of we-are-secure.com has corrupte
C. The we-are-secure.com server is using a TCP wrappe
D. The we-are-secure.com server is using honeypo

Answer: C

NEW QUESTION 176
- (Topic 3)
Which of the following attacks allows an attacker to recover the key in an RC4 encrypted stream from a large number of messages in that stream?

A. SYN flood attack
B. Rainbow attack
C. Zero Day attack
D. FMS attack

Answer: D

NEW QUESTION 177
- (Topic 3)
Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Stalking Amendment Act (1999)
B. Malicious Communications Act (1998)
C. Anti-Cyber-Stalking law (1999)
D. Stalking by Electronic Communications Act (2001)

Answer: A

NEW QUESTION 180
- (Topic 3)
You want to search the Apache Web server having version 2.0 using google hacking. Which of the following search queries will you use?

A. intitle:Sample.page.for.Apache Apache.Hook.Function
B. intitle:"Test Page for Apache Installation" "It worked!"
C. intitle:test.page "Hey, it worked !" "SSl/TLS aware"

D. intitle:"Test Page for Apache Installation" "You are free"

Answer: A

NEW QUESTION 182
- (Topic 3)
Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature. Which of the following statements is true in context with the above scenario?

A. Alternate Data Streams is a feature of Linux operating syste
B. Adam's system runs on Microsoft Windows 98 operating syste
C. Adam is using FAT file syste
D. Adam is using NTFS file syste

Answer: D

NEW QUESTION 186
- (Topic 3)
You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:

X-Apparently-To:	itzme_adee@yahoo.com via 209.191.91.180; Mon, 10 Aug 2009 07:59:47 -0700
Return-Path:	<bounce@vetpaintmail.com>
X-YahooFilteredBulk:	216.168.54.25
X-YMailISG:	lIOjjRIWLDshqPeX9g5WgzYv2NbqcgrXv47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmku96g9o8ggD
X-Originating-IP:	[216.168.54.25]
Authentication-Results:	mta251.mail.re3.yahoo.com from=vetpaintmail.com; domainkeys=pass (ok)
Received:	from 216.168.54.25 (EHLO mail.vetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SM
Received:	from vetpaintmail.com ([172.16.10.90]) by mail.vetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448
X-VirtualServer:	Digest, mail.vetpaintmail.com, 172.16.10.93
X-VirtualServerGroup:	Digest
X-MailingID:	1181167079::64600::1249057716::9100::1133::1133
X-SMHeaderMap:	mid="X-MailingID"
X-Mailer:	StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID:	itzme_adee@yahoo.com
X-SMFBL:	aXR6bWVfYWRIZUB5YWhvby5jb20=
DomainKey-Signature:	a=rsa-sha1; c=nofws; s=customer; d=vetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnpkJMsJ1F
Content-Transfer-Encoding:	7bit
Content-Type:	multipart/alternative; boundary="----=_NextPart_0F9_1F08_2109CDA4.577F5A4D"
Reply-To:	<no-reply@vetpaintmail.com>
MIME-Version:	1.0
Message-ID:	<1181167079.1133@vetpaintmail.com>
Subject:	The Ethical Hacking Weekly Digest
Date:	Mon, 10 Aug 2009 07:37:02 -0700
To:	itzme_adee@yahoo.com
From:	The Ethical Hacking <info@vetpaintmail.com>
Content-Length:	35382

What is the IP address of the sender of this email?

A. 172.16.10.90
B. 209.191.91.180
C. 141.1.1.1
D. 216.168.54.25

Answer: D

NEW QUESTION 191
- (Topic 3)
You are a Web Administrator of Millennium Inc. The company has hosted its Web site within its network. The management wants the company's vendors to be able to connect to the corporate site from their locations through the Internet. As a public network is involved in this process, you are concerned about the security of data transmitted between the vendors and the corporate site.
Which of the following can help you?

A. EAP
B. WEP
C. Smart card
D. VPN

Answer: D

NEW QUESTION 194
- (Topic 3)
Which of the following attacks can be overcome by applying cryptography?

A. Web ripping
B. Sniffing
C. DoS
D. Buffer overflow

Answer: B

NEW QUESTION 198
- (Topic 3)
Which of the following ports must you filter to check null sessions on your network?

A. 139 and 445
B. 111 and 222
C. 1234 and 300
D. 130 and 200

Answer: A

NEW QUESTION 201
- (Topic 3)
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. John has gained the access to the network of the organization and placed a backdoor in the network. Now, he wants to clear all event logs related to previous hacking attempts. Which of the following tools can John use if we-are-secure.com is using the Windows 2000 server?
Each correct answer represents a complete solution. Choose two.

A. elsave.exe
B. WinZapper
C. AuditPol
D. Blindside

Answer: AB

NEW QUESTION 202
- (Topic 3)
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. You install access points for enabling a wireless network. The sales team members and the managers in the company will be using laptops to connect to the LAN through wireless connections. Therefore, you install WLAN network interface adapters on their laptops. However, you want to restrict the sales team members and managers from communicating directly to each other. Instead, they should communicate through the access points on the network. Which of the following topologies will you use to accomplish the task?

A. Star
B. Ad hoc
C. Infrastructure
D. Mesh

Answer: C

NEW QUESTION 207
- (Topic 3)
You are concerned about war driving bringing hackers attention to your wireless network.
What is the most basic step you can take to mitigate this risk?

A. Implement WEP
B. Implement WPA
C. Don't broadcast SSID
D. Implement MAC filtering

Answer: C

NEW QUESTION 209
- (Topic 3)
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 network. Now, when you have finished your penetration testing, you find that the weare- secure.com server is highly vulnerable to SNMP enumeration. You advise the we-are-secure Inc. to turn off SNMP; however, this is not possible as the company is using various SNMP services on its remote nodes. What other step can you suggest to remove SNMP vulnerability?
Each correct answer represents a complete solution. Choose two.

A. Close port TCP 53.
B. Change the default community string name
C. Upgrade SNMP Version 1 with the latest versio
D. Install antiviru

Answer: BC

NEW QUESTION 213
- (Topic 3)
Which of the following are the drawbacks of the NTLM Web authentication scheme?
Each correct answer represents a complete solution. Choose all that apply.

A. It can be brute forced easil
B. It works only with Microsoft Internet Explore
C. The password is sent in clear text format to the Web serve
D. The password is sent in hashed format to the Web serve

Answer: AB

NEW QUESTION 216
- (Topic 3)

You work as an IT Technician for uCertify Inc. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company's wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. MAC Filtering
B. SSID
C. RAS
D. WEP

Answer: A

NEW QUESTION 220
- (Topic 3)
Which of the following are the countermeasures against WEP cracking? Each correct answer represents a part of the solution. Choose all that apply.

A. Using a 16 bit SSI
B. Changing keys ofte
C. Using the longest key supported by hardwar
D. Using a non-obvious ke

Answer: BCD

NEW QUESTION 225
- (Topic 3)
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. XSS attack
B. Replay attack
C. Buffer overflow attack
D. CSRF attack

Answer: A

NEW QUESTION 230
- (Topic 3)
Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?

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

Answer: A

NEW QUESTION 231
- (Topic 3)
You have received a file named new.com in your email as an attachment. When you execute this file in your laptop, you get the following message:
'EICAR-STANDARD-ANTIVIRUS-TEST-FILE!'
When you open the file in Notepad, you get the following string:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
What step will you take as a countermeasure against this attack?

A. Immediately shut down your lapto
B. Do nothin
C. Traverse to all of your drives, search new.com files, and delete the
D. Clean up your laptop with antiviru

Answer: B

NEW QUESTION 235
- (Topic 3)
Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?

A. FTK Imager
B. FAU
C. Device Seizure
D. Galleta

Answer: C

NEW QUESTION 240
- (Topic 3)
Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?

A. A3-07-B9-E3-BC-F9
B. F936.28A1.5BCD.DEFA
C. 1011-0011-1010-1110-1100-0001
D. 132.298.1.23

Answer: A

NEW QUESTION 245
- (Topic 3)
In which of the following scanning methods does an attacker send SYN packets and then a RST packet?

A. TCP SYN scan
B. XMAS scan
C. IDLE scan
D. TCP FIN scan

Answer: A

NEW QUESTION 248
- (Topic 3)
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 task do you want to perform?

A. Perform buffer overflow attac
B. Perform DDoS attac
C. View the directory list of c driv
D. Perform DoS attac

Answer: C

NEW QUESTION 253
- (Topic 3)
Which of the following are the countermeasures against WEP cracking?
Each correct answer represents a part of the solution. Choose all that apply.

A. Using the longest key supported by hardwar
B. Using a non-obvious ke
C. Using a 16 bit SSI
D. Changing keys ofte

Answer: ABD

NEW QUESTION 255
- (Topic 3)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-aresecure server. Which of the following are countermeasures against a brute force attack?
Each correct answer represents a complete solution. Choose all that apply.

A. The site should use CAPTCHA after a specific number of failed login attempt
B. The site should restrict the number of login attempts to only three time
C. The site should force its users to change their passwords from time to tim
D. The site should increase the encryption key length of the passwor

Answer: AB

NEW QUESTION 257
- (Topic 3)
Which of the following security protocols can be used to support MS-CHAPv2 for wireless client authentication?
Each correct answer represents a complete solution. Choose two.

A. PEAP
B. IPSec
C. HTTP
D. PPTP

Answer: AD

NEW QUESTION 259

- (Topic 3)
Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends large number of unsolicited commercial e-mail (UCE) messages on these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail Spam
B. E-mail Storm
C. E-mail spoofing
D. E-mail bombing

Answer: A

NEW QUESTION 263
- (Topic 3)
Which of the following tools can be used to enumerate networks that have blocked ICMP Echo packets, however, failed to block timestamp or information packet or not performing sniffing of trusted addresses, and it also supports spoofing and promiscuous listening for reply packets?

A. Nmap
B. Zenmap
C. Icmpenum
D. Nessus

Answer: C

NEW QUESTION 265
- (Topic 3)
Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?
Each correct answer represents a complete solution. Choose two.

A. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain acces
B. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain acces
C. Attacker can use the Ping Flood DoS attack if WZC is use
D. It will not allow the configuration of encryption and MAC filterin
E. Sending information is not secure on wireless networ

Answer: AB

NEW QUESTION 267
- (Topic 3)
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 network. Now, when you have finished your penetration testing, you find that the weare- secure.com server is highly vulnerable to SNMP enumeration. You advise the we-are-secure Inc. to turn off SNMP; however, this is not possible as the company is using various SNMP services on its remote nodes. What other step can you suggest to remove SNMP vulnerability?
Each correct answer represents a complete solution. Choose two.

A. Change the default community string name
B. Install antiviru
C. Close port TCP 53.
D. Upgrade SNMP Version 1 with the latest versio

Answer: AD

NEW QUESTION 271
- (Topic 3)
GSM uses either A5/1 or A5/2 stream cipher for ensuring over-the-air voice privacy. Which of the following cryptographic attacks can be used to break both ciphers?

A. Man-in-the-middle attack
B. Ciphertext only attack
C. Known plaintext attack
D. Replay attack

Answer: B

NEW QUESTION 275
- (Topic 3)
Which of the following statements are true about the Enum tool?
Each correct answer represents a complete solution. Choose all that apply.

A. It is capable of performing brute force and dictionary attacks on individual accounts of Windows NT/2000.
B. One of the countermeasures against the Enum tool is to disable TCP port 139/445.
C. It is a console-based Win32 information enumeration utilit
D. It uses NULL and User sessions to retrieve user lists, machine lists, LSA policy information, et

Answer: ABCD

NEW QUESTION 278

- (Topic 3)
Which of the following methods can be used to detect session hijacking attack?

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

Answer: D

NEW QUESTION 279
- (Topic 4)
What does TCSEC stand for?

A. Trusted Computer System Evaluation Criteria
B. Target Computer System Evaluation Criteria
C. Trusted Computer System Experiment Criteria
D. Trusted Computer System Evaluation Center

Answer: A

NEW QUESTION 282
- (Topic 4)
Which of the following tools is used for SNMP enumeration?

A. SARA
B. Userinfo
C. Getif
D. Enum

Answer: C

NEW QUESTION 287
- (Topic 4)
Which of the following ports is used for NetBIOS null sessions?

A. 130
B. 139
C. 143
D. 131

Answer: B

NEW QUESTION 288
- (Topic 4)
Which of the following is an open source Web scanner?

A. Nikto
B. GFI LANguird
C. NetRecon
D. Internet scanner

Answer: A

NEW QUESTION 289
- (Topic 4)
How many bits encryption does SHA-1 use?

A. 128
B. 140
C. 512
D. 160

Answer: D

NEW QUESTION 290
- (Topic 4)
In which of the following attacks is a malicious packet rejected by an IDS, but accepted by the host system?

A. Insertion
B. Evasion
C. Fragmentation overwrite
D. Fragmentation overlap

Answer: B

NEW QUESTION 292
- (Topic 4)
Which of the following tools can be used to find a username from a SID?

A. SNMPENUM
B. SID
C. SID2User
D. SIDENUM

Answer: C

NEW QUESTION 294
- (Topic 4)
What does APNIC stand for?

A. Asia-Pacific Network Information Center
B. American-Pacific Network Information Center
C. American Private Network Information Center
D. Asian Private Network Information Center

Answer: A

NEW QUESTION 295
- (Topic 4)
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. Remoxec
B. Hk.exe
C. PSExec
D. GetAdmin.exe

Answer: C

NEW QUESTION 299
- (Topic 4)
Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. MINIX 3
B. Linux
C. Windows XP
D. Mac OS

Answer: D

NEW QUESTION 303
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

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

A. Kismet
B. AirSnort
C. Cain
D. PsPasswd

Answer: B

NEW QUESTION 308
- (Topic 4)
Which of the following TCSEC classes defines verified protection?

A. Class B
B. Class D
C. Class A
D. Class C

Answer: C

NEW QUESTION 312

- (Topic 4)
Which of the following techniques are NOT used to perform active OS fingerprinting?
Each correct answer represents a complete solution. Choose all that apply.

A. ICMP error message quoting
B. Analyzing email headers
C. Sniffing and analyzing packets
D. Sending FIN packets to open ports on the remote system

Answer: BC

NEW QUESTION 315
- (Topic 4)
Which of the following statements about Fport is true?

A. It works as a process viewe
B. It works as a datapipe on Window
C. It works as a datapipe on Linu
D. It is a source port forwarder/redirecto

Answer: A

NEW QUESTION 316
- (Topic 4)
Which of the following Web authentication techniques uses a single sign-on scheme?

A. Basic authentication
B. Digest authentication
C. NTLM authentication
D. Microsoft Passport authentication

Answer: D

NEW QUESTION 318
- (Topic 4)
Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

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

Answer: D

NEW QUESTION 322
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He performs a Teardrop attack on the we-are-secure server and observes that the server crashes. Which of the following is the most likely cause of the server crash?

A. The spoofed TCP SYN packet containing the IP address of the target is filled in both the source and destination field
B. The we-are-secure server cannot handle the overlapping data fragment
C. The ICMP packet is larger than 65,536 byte
D. Ping requests at the server are too hig

Answer: B

NEW QUESTION 324
- (Topic 4)
Which of the following is the most common method for an attacker to spoof email?

A. Back door
B. Replay attack
C. Man in the middle attack
D. Open relay

Answer: D

NEW QUESTION 326
- (Topic 4)
You want that some of your Web pages should not be crawled. Which one of the following options will you use to accomplish the task?

A. Use HTML NO Crawl tag in the Web page not to be crawled
B. Place the name of restricted Web pages in the private.txt file
C. Place the name of restricted Web pages in the robotes.txt file
D. Enable the SSL

Answer: C

NEW QUESTION 330
- (Topic 4)
Which of the following tools is a wireless sniffer and analyzer that works on the Windows operating system?

A. Void11
B. Airsnort
C. Kismet
D. Aeropeek

Answer: D

NEW QUESTION 333
- (Topic 4)
Which of the following nmap switches is used to perform NULL scan?

A. -sN
B. -sO
C. -sU
D. -sP

Answer: A

NEW QUESTION 337
- (Topic 4)
Which of the following is NOT a Back orifice plug-in?

A. BOSOCK32
B. STCPIO
C. BOPeep
D. Beast

Answer: D

NEW QUESTION 338
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network:
Gathering information
Determining the network range
Identifying active systems
Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. APNIC
B. SuperScan
C. ARIN
D. RIPE

Answer: B

NEW QUESTION 342
- (Topic 4)
Which of the following is NOT a Back orifice plug-in?

A. BOSOCK32
B. STCPIO
C. BOPeep
D. Beast

Answer: D

NEW QUESTION 347
- (Topic 4)
Which of the following options holds the strongest password?

A. Joe12is23good
B. $#164aviD^%
C. california
D. Admin1234

Answer: B

NEW QUESTION 349
- (Topic 4)

Which of the following is NOT an example of passive footprinting?

A. Scanning port
B. Analyzing job requirement
C. Querying the search engin
D. Performing the whois quer

Answer: A

NEW QUESTION 354
- (Topic 4)
The employees of CCN Inc. require remote access to the company's proxy servers. In order to provide solid wireless security, the company uses LEAP as the authentication protocol. Which of the following is supported by the LEAP protocol?
Each correct answer represents a complete solution. Choose all that apply.

A. Strongest security level
B. Dynamic key encryption
C. Password hash for client authentication
D. Public key certificate for server authentication

Answer: BC

NEW QUESTION 358
- (Topic 4)
Which of the following event logs contains traces of brute force attempts performed by an attacker?

A. SysEvent.Evt
B. WinEvent.Evt
C. AppEvent.Evt
D. SecEvent.Evt

Answer: D

NEW QUESTION 360
- (Topic 4)
Which of the following is the default port value of beast Trojan?

A. 6666
B. 2222
C. 3333
D. 1111

Answer: A

NEW QUESTION 365
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

GPEN Practice Exam Features:

* GPEN Questions and Answers Updated Frequently

* GPEN Practice Questions Verified by Expert Senior Certified Staff

* GPEN Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GPEN Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The GPEN Practice Test Here