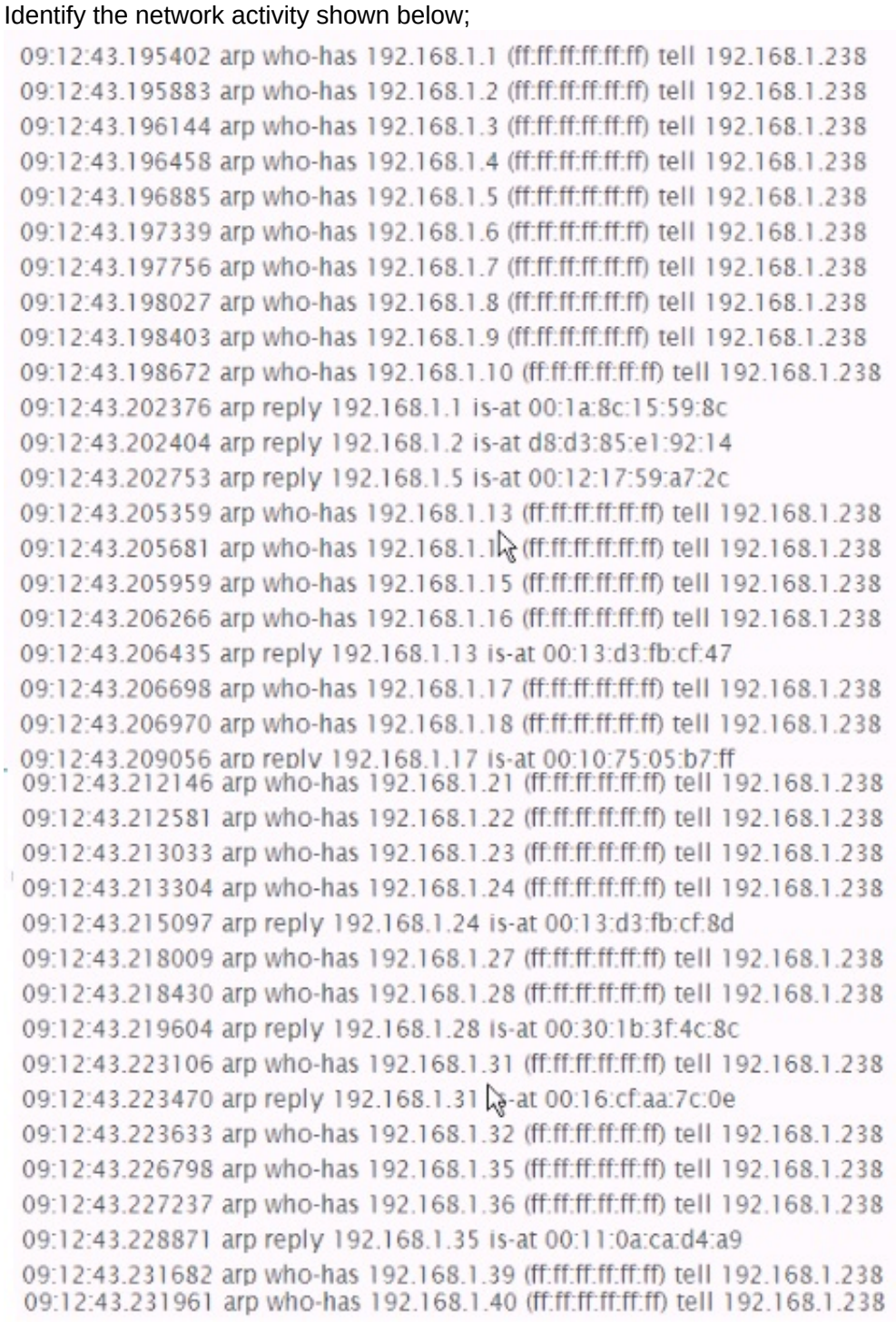
GIAC

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)
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 3
- (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 4
- (Topic 1)

You are done pen testing a Windows system and need to clean up some of the changes you have made. You created an account ‘pentester’ on the system, what command would you use to delete that account?

A. Net user pentester /del
B. Net name pentester /del
C. Net localuser pentester /del
D. Net account pentester /del

Answer: D

NEW QUESTION 5
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 6
- (Topic 1)
While performing a code audit, you discover a SQL injection vulnerability assuming the following vulnerable query, what user input could be injected to make the query true and return data?
select * from widgets where name = '[user-input]';

A. 'or 1=1
B. ‘or l=l…
C. 'or 1=1--
D. ‘or l=1’

Answer: D

NEW QUESTION 7
- (Topic 1)
ACME corporation has decided to setup wireless (IEEE 802.11) network in it's sales branch at Tokyo and found that channels 1, 6, 9,11 are in use by the neighboring offices. Which is the best channel they can use?

A. 4
B. 5
C. 10
D. 2

Answer: D

NEW QUESTION 8
- (Topic 1)
You are conducting a penetration test for a private company located in the UK. The scope
extends to all internal and external hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under the computer Misuse Act of 1990?

A. Sending crafted packets to internal hosts in an attempt to fingerprint the operatingsystems
B. Recovering the SAM database of the domain server and attempting to crackpasswords
C. Installing a password sniffing program on an employee's personal computer withoutconsent
D. Scanning open ports on internal user workstations and exploiting vulnerableapplications

Answer: B

NEW QUESTION 9
- (Topic 1)
You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular
password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

A. Use the getuid command to determine the user context the process is runningunder, then use the imp command to impersonate that use
B. use the getpid command to determine the user context the process is runningunder, then use the Imp command to impersonate that use
C. Use the execute command to the passmgr executabl
D. That will give you access to the fil
E. Use the migrate command to jump to the passmgr proces
F. That will give you accessto the fil

Answer: C

NEW QUESTION 10
- (Topic 1)
Which of the following is the JavaScript variable used to store a cookie?

A. Browsercookie
B. Windowcookie
C. Document cookie
D. Session cookie

Answer: C

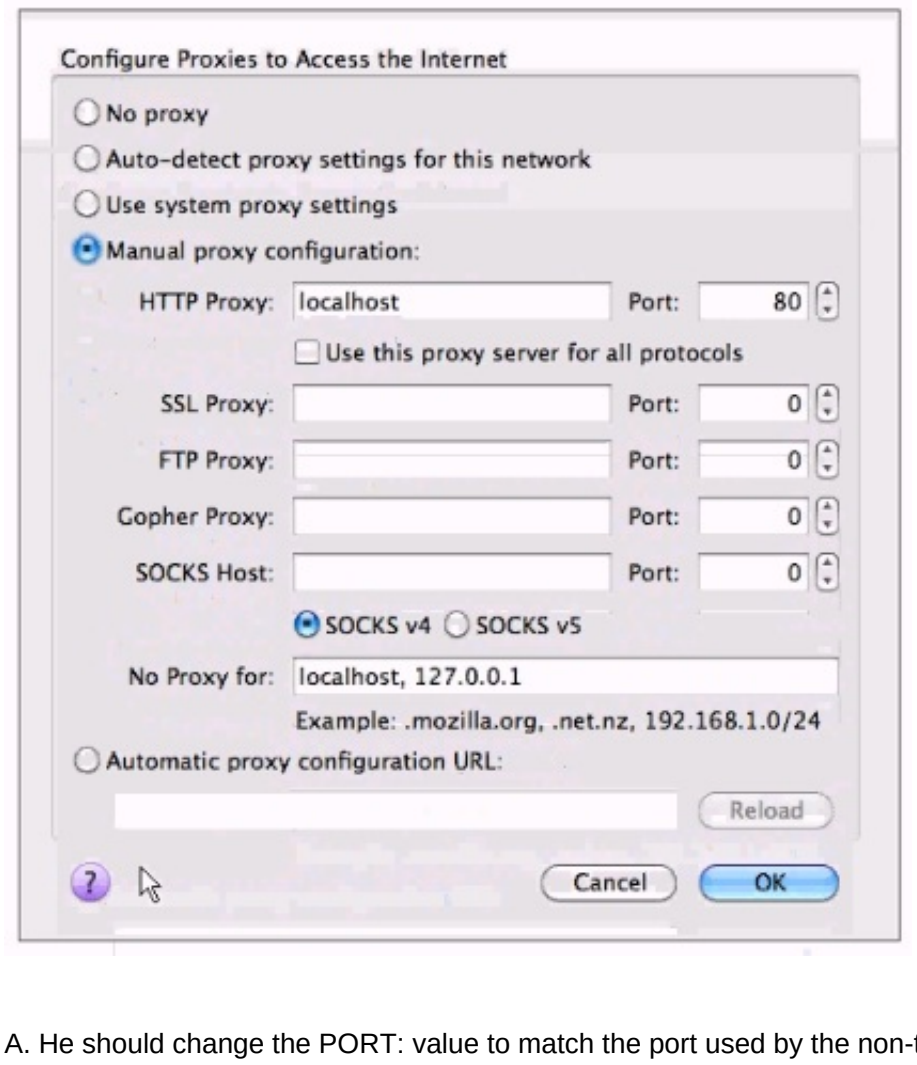
Explanation:
Reference: http://www.w3schools.com/js/js_cookies.asp

NEW QUESTION 10
- (Topic 1)
You are pen testing a system and want to use Metasploit 3.X to open a listening port on the system so you can access it via a netcat shell. Which stager would you use to have the system listen on TCP port 50000?

A. Reverse.tcp
B. Bind.tcp
C. Fincltag.ord
D. Passivex

Answer: B

NEW QUESTION 15
- (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

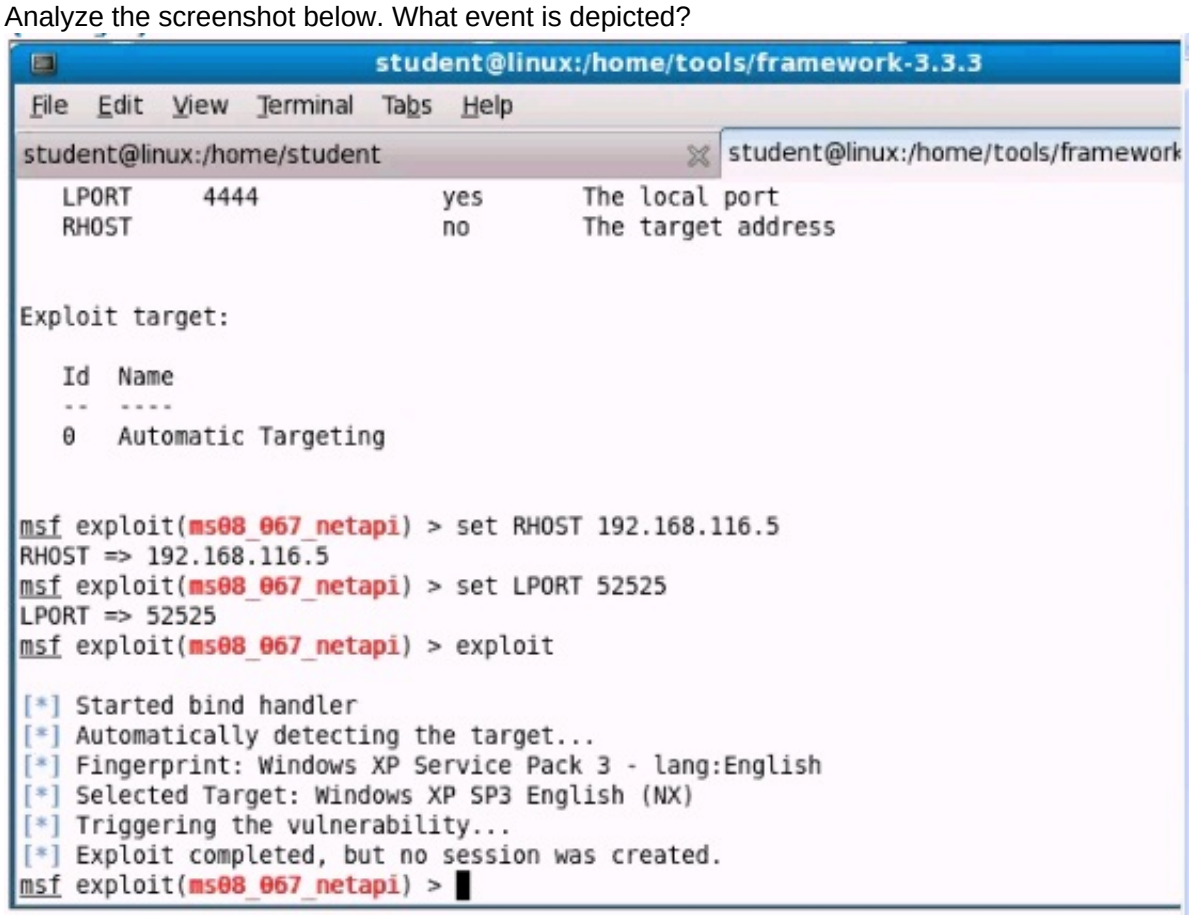
NEW QUESTION 16
- (Topic 1)
Which Metasploit payload includes simple upload and download functionality for moving files to and from compromised systems?

A. DLL inject
B. Upexec
C. Meterpreter
D. Vncinject

Answer: D

Explanation:
Reference:
http://www.opensourceforu.com/2011/02/metasploit-meterpreter-payload/

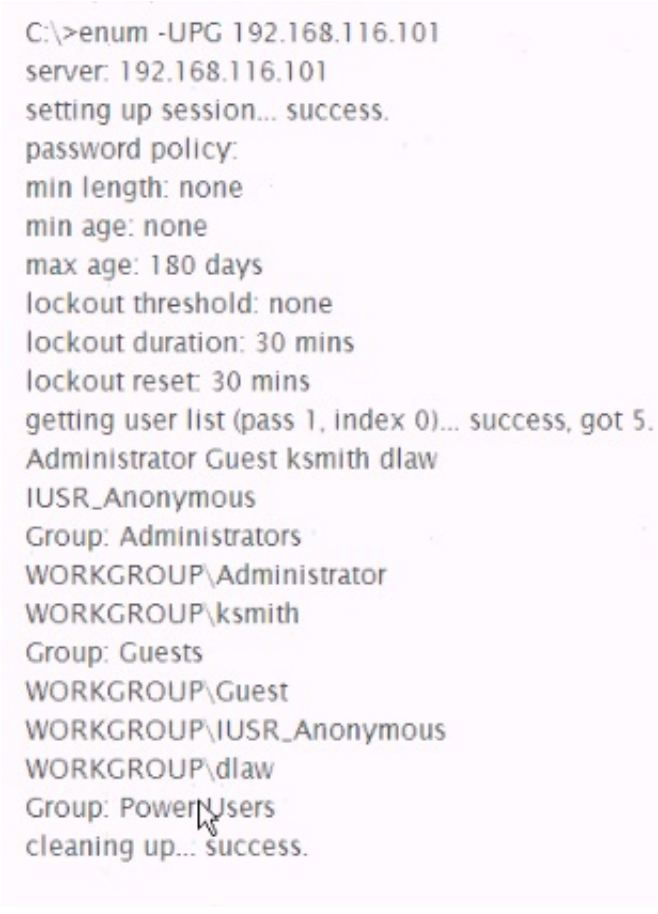
NEW QUESTION 19
- (Topic 1)
Analyze the screenshot below. What event is depicted?



A. An exploit that was attempted does not work against the target selecte
B. A payload was used that is not compatible with the chosen exploi
C. The exploit is designed to work against the local host onl
D. The payload Is designed to create an interactive sessio

Answer: D

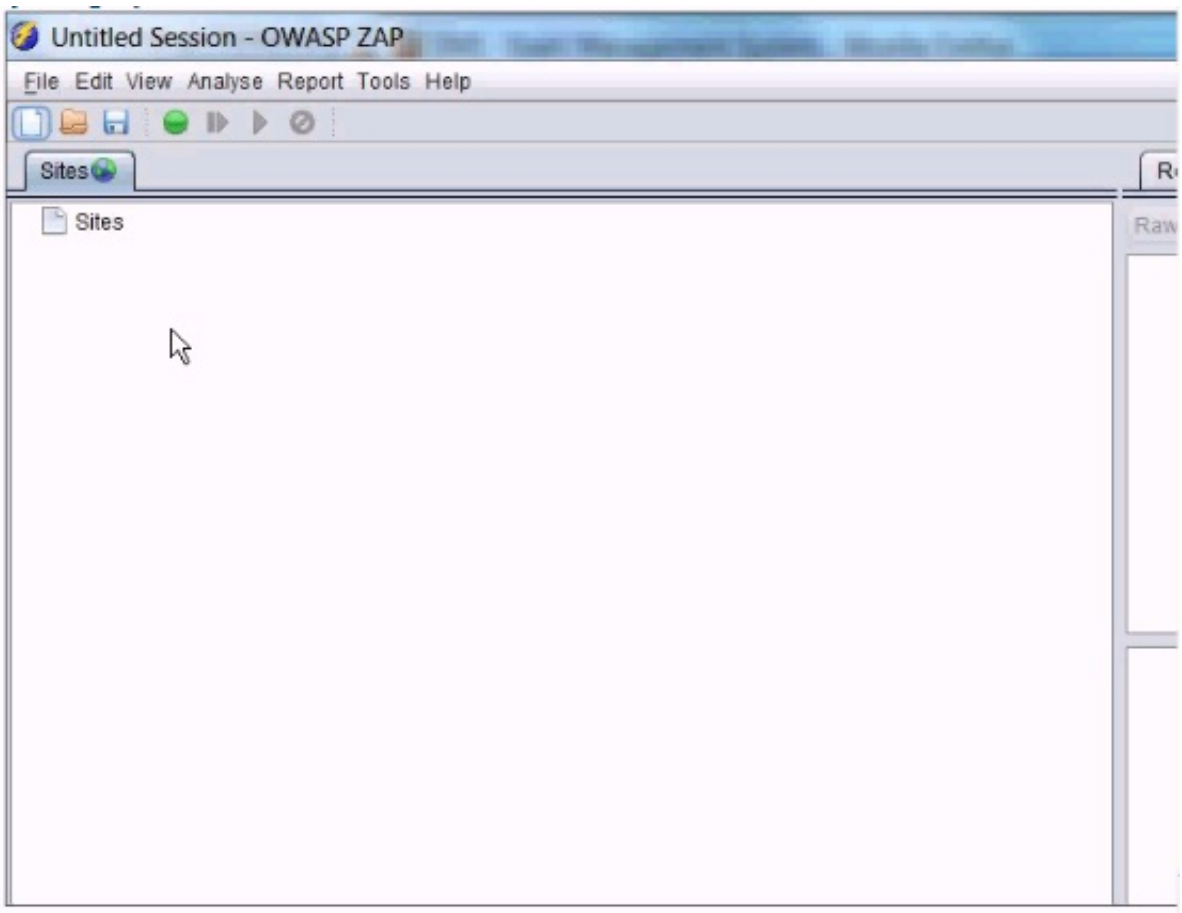
NEW QUESTION 20
- (Topic 1)
Analyze the command output below. What information can the tester infer directly from the information shown?



A. The administrator account has no password
B. Null sessions are enabled on the target
C. The target host is running Linux with Samba services
D. Account lockouts must be reset by the Administrator

Answer: C

NEW QUESTION 25
- (Topic 1)
In the screen shot below, which selections would you need click in order to intercept and alter all http traffic passing through OWASP ZAP?



A. Trap response and continue
B. Set Break and Continue
C. Trap request and continue
D. Continue and drop

Answer: B

NEW QUESTION 30
000 and the loss of a high profile client. They ask you to perform a desktop vulnerability assessment to identify everything that needs to be patched. Using Nessus you find tens of thousands of vulnerabilities that need to be patched. In the report you find workstations running several Windows OS versions and service pack levels, anti-virus software from multiple vendors several major browser versions and different versions of Acrobat Reader. Which of the following recommendations should you provide with the report?

A. The client should standardize their desktop software
B. The client should eliminate workstations to reduce workload
C. The client should hire more people to catch up on patches
D. The client should perform monthly vulnerability assessments

Answer: C

NEW QUESTION 31
- (Topic 1)
A pen tester is able to pull credential information from memory on a Windows system. Based on the command and output below, what advantage does this technique give a penetration tester when trying to access another windows system on the network?

```
wce.exe -s
JoeArthur:WESTREGION:FD3C347788158CBBCCACBF972408D7DA:98ECC8D2E938A0016A2B3
262919C2E39

Username: JoeArthur
domain: WESTREGION
LMHash: FD3C347788158CBBCCACBF972408D7DA
NTHash: 98ECC8D2E938A0016A2B3262919C2E39
NTLM credentials successfully changed!
```

A. The technique is more effective through perimeter firewalls than otherauthentication attack
B. It allows the tester to escalate the privilege level of the account,
C. Access to the system can be gained without password guessing or crackin
D. Salts are removed from the hashes to allow for faster, offline cracking

Answer: A

NEW QUESTION 32
- (Topic 1)
Which of the following is possible in some SQL injection vulnerabilities on certain types of databases that affects the underlying server OS?

A. Database structure retrieval
B. Shell command execution
C. Data manipulation
D. Data query capabilities

Answer: A

Explanation:
Reference:
http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/

NEW QUESTION 33
- (Topic 1)
Where are Netcat's own network activity messages, such as when a connection occurs, sent?

A. Standard Error
B. Standard input
C. Standard Logfile
D. Standard Output

Answer: A

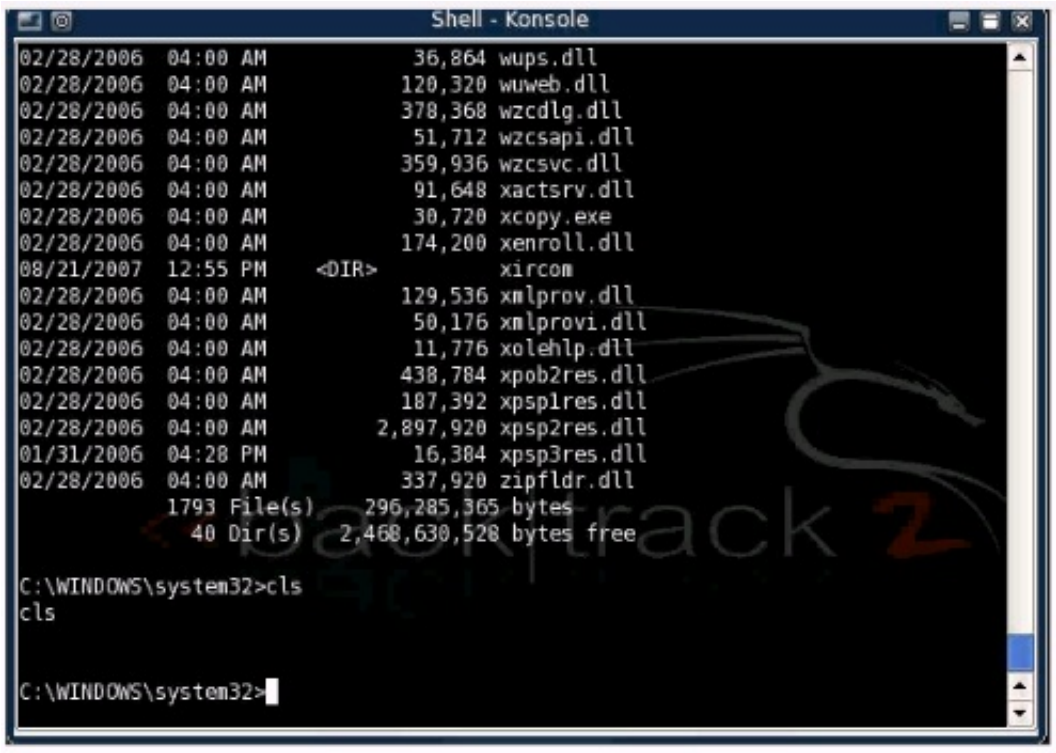
Explanation:
Reference:
http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

NEW QUESTION 38
- (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 42
- (Topic 1)
You have connected to a Windows system remotely and have shell access via netcat. While connected to the remote system you notice that some Windows commands work normally while others do not An example of this is shown in the picture below Which of the following best describes why tins is happening?



A. Netcat cannot properly interpret certain control characters or Unicode sequence
B. The listener executed command.com instead of cmd.ex
C. Another application is already running on the port Netcat is listening o
D. TheNetcat listener is running with system level privilege

Answer: D

NEW QUESTION 47
- (Topic 1)
A penetration tester wishes to stop the Windows Firewall process on a remote host running Windows Vista She issues the following commands:

```
C:\Documents and Settings\Owner>net use Z: \\fileserver\shared
/user:Administrator
The command completed successfully.

C:\Documents and Settings\Owner>Z:

Z:\>sc stop MpsSvc
[SC] ControlService FAILED 1062:

The service has been stopped.

Z:\>
```

A check of the remote host indicates that Windows Firewall is still running. Why did the command fail?

A. The kernel prevented the command from being execute
B. The user does not have the access level needed to stop the firewal
C. The sc command needs to be passed the IP address of the targe
D. The remote server timed out and did not complete the comman

Answer: C

NEW QUESTION 52
- (Topic 1)
A tester has been contracted to perform a penetration test for a corporate client. The scope of the test is limited to end-user workstations and client programs only. Which of die following actions is allowed in this test?

A. Attempting to redirect the internal gateway through ARP poisoning
B. Activating bot clients and performing a denial-of-service against the gatewa
C. Sniffing and attempting to crack the Domain Administrators password has
D. Sending a malicious pdf to a user and exploiting a vulnerable Reader versio

Answer: B

NEW QUESTION 54
- (Topic 1)
You are pen testing a Linux target from your windows-based attack platform. You just moved a script file from the windows system to the Linux target, but it will not execute properly. What is the most likely problem?

A. The byte length is different on the two machines
B. End of-line characters are different on the two machines
C. The file must have become corrupt during transfer
D. ASCII character sets are different on the two machines

Answer: A

NEW QUESTION 58
- (Topic 1)
Which of the following is the feature that separates the use of Rainbow Tables from other applications such as Cain or John the Ripper?

A. Salts are used to create massive password databases for compariso
B. Applications take advantage of 64-bit CPU processor and multithread the crackingproces
C. Data Is aligned efficiently in the rainbow tables making the search process quicker
D. Raw hashed passwords are compared to pre-calculated hash table

Answer: B

NEW QUESTION 60
- (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 61
- (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 63
- (Topic 2)
What difference would you expect to result from running the following commands;
(I). S dig .ns domain.com target.com -t AXFR
and
(2). S dig .ns.domain.com target.com -t IXFR=1002200301

A. Command (I) will display incremental information about a domain and command (2) Will provide only 1002200301 bytes of information
B. Command (1) will display all information about a domain and command (2) willprovide only incremental updates from SOA 1002200301
C. Command (I) will display all information about a domain and command (2) willprovide only incremental updates up to SOA 1002200301
D. Command (I) will display all information about a domain and command (2) willprovide only 1002200301 bytes of information

Answer: B

NEW QUESTION 67
- (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 69
- (Topic 2)
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. Replay attack
B. Buffer overflow attack
C. CSRF attack
D. XSS attack

Answer: D

NEW QUESTION 74
- (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 78
- (Topic 2)
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. Do nothin
B. Traverse to all of your drives, search new.com files, and delete the
C. Clean up your laptop with antiviru
D. Immediately shut down your lapto

Answer: A

NEW QUESTION 80
CORRECT TEXT - (Topic 2)
Fill in the blank with the appropriate tool.
____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

A.

Answer: NBTscan

NEW QUESTION 81
- (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 86
- (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 completed the following pre-attack phases while testing the security of the server:
Footprinting Scanning Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?
Each correct answer represents a complete solution. Choose all that apply.

A. PsFile
B. PsPasswd
C. UserInfo
D. WinSSLMiM

Answer: ABC

NEW QUESTION 90
- (Topic 2)
You are sending a file to an FTP server. The file will be broken into several pieces of information packets (segments) and will be sent to the server. The file will again be reassembled and reconstructed once the packets reach the FTP server. Which of the following information should be used to maintain the correct order of information packets during the reconstruction of the file?

A. Acknowledge number
B. TTL
C. Checksum
D. Sequence number

Answer: D

NEW QUESTION 92
- (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 97
- (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 98
- (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 101
- (Topic 2)
John works as an Ethical Hacker for uCertify Inc. He wants to find out the ports that are open in uCertify's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN
B. Xmas tree
C. TCP SYN/ACK
D. TCP SYN

Answer: D

NEW QUESTION 103
- (Topic 2)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 108
- (Topic 2)
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 Active Directory domain-based network. The domain consists of a domain controller, two Windows 2003 member servers, and one hundred client computers. The company employees use laptops with Windows XP Professional. These laptops are equipped with wireless network cards that are used to connect to access points located in the Marketing department of the company. The company employees log on to the domain by using a user name and password combination. The wireless network has been configured with WEP in addition to 802.1x. Mark wants to provide the best level of security for the kind of
authentication used by the company. What will Mark do to accomplish the task?

A. Use EAP-TLS
B. Use MD5
C. Use PEAP
D. Use IPSec

Answer: C

NEW QUESTION 110
- (Topic 2)
Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. Cain
B. L0phtcrack
C. Pass-the-hash toolkit
D. John the Ripper

Answer: A

NEW QUESTION 113
- (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 escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function

Answer: C

NEW QUESTION 116
- (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 121
- (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 increase the encryption key length of the passwor
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 use CAPTCHA after a specific number of failed login attempt

Answer: BD

NEW QUESTION 123
- (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 125
- (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:	lI0jjRIWLDshqPeX9g5WgzYv2NbqcgrXv47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.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:	aXR6bWVfYWRIZU85YWhvby5jb20=
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 126
- (Topic 3)
Which of the following tools can be used by a user to hide his identity?
Each correct answer represents a complete solution. Choose all that apply.

A. IPchains
B. Rootkit
C. Proxy server
D. War dialer
E. Anonymizer

Answer: ACE

NEW QUESTION 127
- (Topic 3)
John works as a Professional Ethical Hacker for we-are-secure Inc. The company is using a Wireless network. John has been assigned the work to check the security of WLAN of we-aresecure.
For this, he tries to capture the traffic, however, he does not find a good traffic to analyze data. He has already discovered the network using the ettercap tool.
Which of the following tools can he use to generate traffic so that he can crack the Wep keys and enter into the network?

A. ICMP ping flood tool
B. Kismet
C. Netstumbler
D. AirSnort

Answer: A

NEW QUESTION 128
- (Topic 3)
Adam is a novice Internet user. He is using Google search engine to search documents of his interest. Adam wants to search the text present in the link of a Website. Which of the following operators will he use in his query to accomplish the task?

A. inanchor
B. info
C. link
D. site

Answer: A

NEW QUESTION 131
- (Topic 3)
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_escape_string()
B. session_regenerate_id()
C. mysql_real_escape_string()
D. Prepared statement

Answer: CD

NEW QUESTION 136
- (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 137
- (Topic 3)
Which of the following tools can be used to automate the MITM attack?

A. Hotspotter
B. Airjack
C. Kismet
D. IKECrack

Answer: B

NEW QUESTION 140
- (Topic 3)
LM hash is one of the password schemes that Microsoft LAN Manager and Microsoft Windows versions prior to the Windows Vista use to store user passwords that are less than 15 characters long. If you provide a password seven characters or less, the second half of the LM hash is always _____.

A. 0xBBD3B435B51504FF
B. 0xAAD3B435B51404FF
C. 0xBBC3C435C51504EF
D. 0xAAD3B435B51404EE

Answer: D

NEW QUESTION 141
- (Topic 3)
You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring ISA Server 2006, which of the following is NOT necessary?

A. Configuration of VPN access
B. Setting up of monitoring on ISA Server
C. Defining ISA Server network configuration
D. Defining how ISA Server would cache Web contents

Answer: A

NEW QUESTION 146
- (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 149
- (Topic 3)
When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?

A. Closed
B. Open
C. Filtered

Answer: B

NEW QUESTION 150
- (Topic 3)
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. Nmap
B. Kismet
C. Sniffer
D. Nessus

Answer: A

NEW QUESTION 153
- (Topic 3)
Which of the following are considered Bluetooth security violations?
Each correct answer represents a complete solution. Choose two.

A. Bluebug attack
B. SQL injection attack
C. Cross site scripting attack
D. Social engineering
E. Bluesnarfing

Answer: AE

NEW QUESTION 157
- (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 161
- (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 162
- (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 164
- (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 168
- (Topic 3)
Which of the following tools allows you to download World Wide Web sites from the Internet to a local computer?

A. Netcraft
B. HTTrack
C. Netstat
D. Cheops-ng

Answer: B

NEW QUESTION 171
- (Topic 3)
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. Collecting employees information
B. Gathering private and public IP addresses
C. Performing Neotracerouting
D. Banner grabbing

Answer: C

NEW QUESTION 173
- (Topic 3)
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He enters a single quote in the input field of the login page of the Weare- 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

NEW QUESTION 178

- (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 181
- (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 182
- (Topic 3)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the preattack phase successfully:
Information gathering
Determination of network range
Identification of active systems
Location of open ports and applications
Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure networ
B. Map the network of We-are-secure In
C. Fingerprint the services running on the we-are-secure networ
D. Install a backdoor to log in remotely on the We-are-secure serve

Answer: A

NEW QUESTION 186
- (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 188
- (Topic 4)
Which of the following is NOT a valid DNS zone type?

A. Stub zone
B. Secondary zone
C. AlterNet zone
D. Primary zone

Answer: C

NEW QUESTION 193
- (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 198
- (Topic 4)

_____ firewall architecture uses two NICs with a screening router inserted between the host and the untrusted network.

A. packet filtering
B. Screened host
C. Dual homed host
D. Screened subnet

Answer: B

NEW QUESTION 202
- (Topic 4)
You want to run the nmap command that includes the host specification of 202.176.56-57.*. How many hosts will you scan?

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

Answer: B

NEW QUESTION 204
- (Topic 4)
Which of the following statements about SSID is NOT true?

A. Default settings of SSIDs are secur
B. All wireless devices on a wireless network must have the same SSID in order to communicate with each othe
C. It acts as a password for network acces
D. It is used to identify a wireless networ

Answer: A

NEW QUESTION 207
- (Topic 4)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 209
- (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 211
- (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 216
- (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 219
- (Topic 4)
Which of the following tasks is NOT performed into the enumeration phase?

A. Discovering NetBIOS names
B. Obtaining Active Directory information and identifying vulnerable user accounts
C. Injecting a backdoor to the remote computer to gain access in it remotely
D. Establishing NULL sessions and queries

Answer: C

NEW QUESTION 224
- (Topic 4)
You want to perform an active session hijack against Secure Inc. You have found a target that allows Telnet session. You have also searched an active session due to the high level of traffic on the network. What should you do next?

A. Use a sniffer to listen network traffi
B. Guess the sequence number
C. Use brutus to crack telnet passwor
D. Use macoff to change MAC addres

Answer: B

NEW QUESTION 229
- (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 230
- (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 234
- (Topic 4)
Which of the following tools is based on the SATAN tool?

A. Retina
B. Internet scanner
C. GFI LANguard
D. SAINT

Answer: D

NEW QUESTION 236
- (Topic 4)
Which of the following tasks is NOT performed by antiviruses?

A. Activity blocking
B. Heuristic scanning
C. Integrity scanning
D. Session hijacking

Answer: D

NEW QUESTION 237
- (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 241
- (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 245
- (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 250
- (Topic 4)
Which of the following Penetration Testing steps includes network mapping and OS fingerprinting?

A. Gather information
B. Exploit
C. Verify vulnerabilities
D. Planning stage

Answer: A

NEW QUESTION 252
- (Topic 4)
Which of the following is the correct sequence of packets to perform the 3-way handshake method?

A. SYN, ACK, ACK
B. SYN, ACK, SYN/ACK
C. SYN, SYN/ACK, ACK
D. SYN, SYN, ACK

Answer: C

NEW QUESTION 255
- (Topic 4)
Which of the following is the second half of the LAN manager Hash?

A. 0xAAD3B435B51404BB
B. 0xAAD3B435B51404CC
C. 0xAAD3B435B51404EE
D. 0xAAD3B435B51404AA

Answer: C

NEW QUESTION 260
- (Topic 4)
You want to search Microsoft Outlook Web Access Default Portal using Google search on the Internet so that you can perform the brute force attack and get unauthorized access. What search string will you use to accomplish the task?

A. intitle:index.of inbox dbx
B. intext:"outlook.asp"
C. allinurl:"exchange/logon.asp"
D. intitle:"Index Of" -inurl:maillog maillog size

Answer: C

NEW QUESTION 262
- (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 264
- (Topic 4)
Which of the following options holds the strongest password?

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

Answer: B

NEW QUESTION 267
- (Topic 4)
Which of the following tools is used for port redirection?

A. SubSeven
B. Fpipe
C. NetBus
D. Loki

Answer: B

NEW QUESTION 271
- (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 276
CORRECT TEXT - (Topic 4)
Fill in the blank with the appropriate act name.
The ____act gives consumers the right to ask emailers to stop spamming them.

A.

Answer: CAN-SPAM

NEW QUESTION 280
- (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 284
.....

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