GIAC

Exam Questions GPEN

GIAC Certified Penetration Tester

NEW QUESTION 1
- (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 2
- (Topic 1)
Analyze the excerpt from a packet capture between the hosts 192.168.116.9 and 192.168.116.101. What factual conclusion can the tester draw from this output?

```
19:18:01.943630 IP 192.168.116.9.36155 > 192.168.116.101.135: S 3470088794:3470088794
(0) win
19:18:01.944019 IP 192.168.116.9.53541 > 192.168.116.101.139: S 3468017513:3468017513
(0) win 5840 <mss 1460,sackOK,timestamp 1133348468 0,nop,wscale 5>
19:18:01.944903 IP 192.168.116.101.139 > 192.168.116.9.53541: S 627552668:627552668(0)
ack 3468017514 win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0,nop,nop,sackOK>
19:18:01.944925 IP 192.168.116.9.53541 > 192.168.116.101.139: . ack 1 win 183
<nop,nop,timestamp 1133348468 0>
19:18:01.945122 IP 192.168.116.9.53541 > 192.168.116.101.139: R 1:1(0) ack 1 win 183
<nop,nop,timestamp 1133348468 0>
```

A. Port 135 is filtered, port 139 is ope
B. Pons 135 and 139 are filtere
C. Ports 139 and 135 are ope
D. Port 139 is closed, port 135 is open

Answer: C

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

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

Answer: C

NEW QUESTION 4
- (Topic 1)
Why is OSSTMM beneficial to the pen tester?

A. It provides a legal and contractual framework for testing
B. It provides in-depth knowledge on tools
C. It provides report templates
D. It includes an automated testing engine similar to Metasploit

Answer: C

Explanation:
Reference:
http://www.pen-tests.com/open-source-security-testing-methodology-manual-osstmm.html

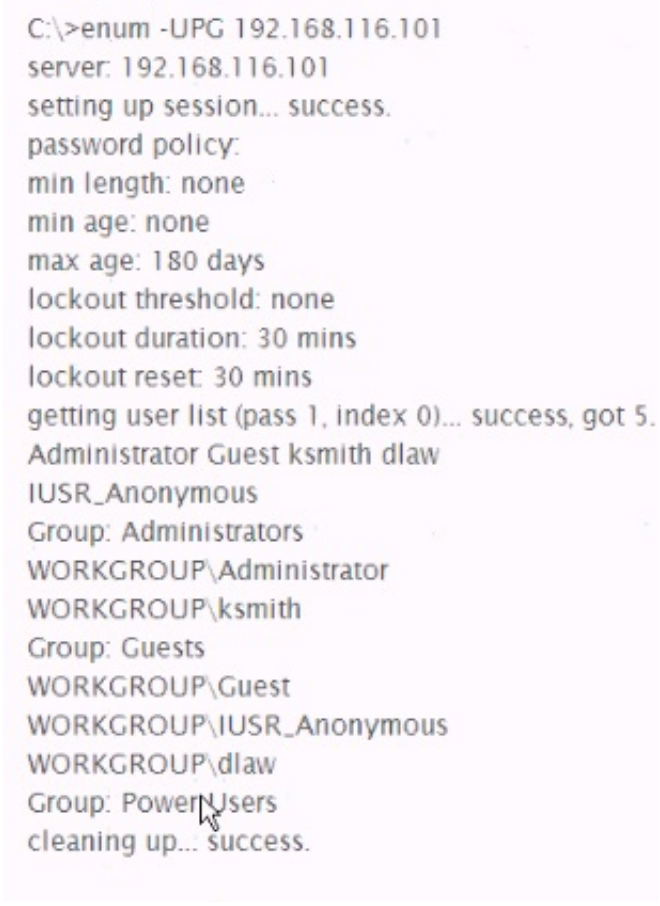
NEW QUESTION 5
- (Topic 1)
Your company has decided that the risk of performing a penetration test Is too great. You would like to figure out other ways to find vulnerabilities on their systems, which of the following is MOST likely to be a valid alternative?

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

Answer: A

NEW QUESTION 6

- (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 7
- (Topic 1)
A client with 7200 employees in 14 cities (all connected via high speed WAN connections) has suffered a major external security breach via a desktop which cost them more than SI

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 8
- (Topic 1)
What is the purpose of the following command?
C:\>wmic /node:[target IP] /user:[admin-user]
/password:[password] process call create [command]

A. Running a command on a remote Windows machine
B. Creating a service on a remote Windows machine
C. Creating an admin account on a remote Windows machine
D. Listing the running processes on a remote windows machine

Answer: D

NEW QUESTION 9
- (Topic 1)
When a DNS server transfers its zone file to a remote system, what port does it typically use?

A. 53/TCP
B. 153/UDP
C. 35/TCP
D. 53/UDP

Answer: D

Explanation:
Reference:
http://www.networkworld.com/article/2231682/cisco-subnet/cisco-subnet-allow-both-tcp-and-udp-port-53-to-your-dns-servers.html

NEW QUESTION 10
- (Topic 1)

A. Mastered

B. Not Mastered

Answer: A

NEW QUESTION 10
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 11
- (Topic 1)
While performing an assessment on a banking site, you discover the following link:
hnps://mybank.com/xfer.aspMer_toMaccount_number]&amount-[dollars]
Assuming authenticated banking users can be lured to your web site, which crafted html
tag may be used to launch a XSRF attack?

A. <imgsrc-"java script alert (‘document cookie'):">
B. <scripi>alert('hnps:/'mybank.com/xfer.a$p?xfer_io-[attacker_account]&amoutn-[dollars]')</script>
C. <scripr>document.\write('hTtp$://mybankxom/xfer.a$p?xfer_to-[attacker.accountl &amount-[dollars)</script>
D. <img src-'https/mybank.com/xfer.asp?xfer_to=[artacker_account]&amount= [dollars]">

Answer: C

NEW QUESTION 16
- (Topic 1)
What is the MOST important document to obtain before beginning any penetration testing?

A. Project plan
B. Exceptions document
C. Project contact list
D. A written statement of permission

Answer: A

Explanation:
Reference:
Before starting a penetration test, all targets must be identified. These targets should be obtained from the customer during the initial questionnaire phase. Targets can be given in the form of specific IP addresses, network ranges, or domain names by the customer. In some instances, the only target the customer provides is the name of the organization and expects the testers be able to identify the rest on their own. It is important to define if systems like firewalls and IDS/IPS or networking equipment that are between the tester and the final target are also part of the scope. Additional elements such as upstream providers, and other 3rd party providers should be identified and defined whether they are in scope or not.

NEW QUESTION 21
- (Topic 1)
By default Active Directory Controllers store password representations in which file?

A. %system roots .system 32/ntds.dit
B. %System roots /ntds\ntds.dit
C. %System roots /ntds\sam.dat
D. %System roots /ntds\sam.dit

Answer: A

Explanation:
Reference:
http://www.scribd.com/doc/212238158/Windows-Administrator-L2-Interview-Question-System-Administrator#scribd

NEW QUESTION 25
- (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 29
- (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 31
- (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 36
- (Topic 1)
Analyze the command output below, what action is being performed by the tester?

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

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

Answer: C

NEW QUESTION 38
- (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 43
- (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 44
- (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 47
- (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 50
- (Topic 2)
In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?
Each correct answer represents a complete solution. Choose all that apply.

A. NSLookup
B. Host
C. DSniff
D. Dig

Answer: ABD

NEW QUESTION 55
- (Topic 2)
Analyze the output of the two commands below:

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

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

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

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

Answer: C

NEW QUESTION 58
- (Topic 2)
Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. snort_inline
B. EtherApe
C. Snort decoder
D. AirSnort

Answer: C

NEW QUESTION 59
- (Topic 2)
You are concerned about rogue wireless access points being connected to your network. What is the best way to detect and prevent these?

A. Site surveys
B. Protocol analyzers
C. Network anti-spyware software
D. Network anti-virus software

Answer: A

NEW QUESTION 64
- (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 68
- (Topic 2)
You configure a wireless router at your home. To secure your home Wireless LAN (WLAN), you implement WEP. Now you want to connect your client computer to the WLAN. Which of the following is the required information that you will need to configure the client computer?
Each correct answer represents a part of the solution. Choose two.

A. WEP key
B. MAC address of the router
C. IP address of the router
D. SSID of the WLAN

Answer: AD

NEW QUESTION 73
- (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 74
- (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 79
- (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 80
- (Topic 2)
You want to run the nmap command that includes the host specification of 202.176.56-57.*.
How many hosts will you scan?

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

Answer: A

NEW QUESTION 81
- (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 84
- (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 88
- (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 89
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server.
The output of the scanning test is as follows:
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 94
- (Topic 2)
Which of the following methods will free up bandwidth in a Wireless LAN (WLAN)?

A. Implement WE
B. Disabling SSID broadcas
C. Change hub with switc
D. Deploying a powerful antenn

Answer: B

NEW QUESTION 95
- (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 97
- (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 100
- (Topic 2)
The scope of your engagement is to include a target organization located in California with a /24 block of addresses that they claim to completely own. Which site could you utilize to confirm that you have been given accurate information before starting reconnaissance activities?

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

Answer: B

NEW QUESTION 102
- (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 104
- (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 109
- (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 114
- (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 116
- (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 119
- (Topic 3)
John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Brute Force attack
B. Dictionary attack
C. Hybrid attack
D. Rule based attack

Answer: ABC

NEW QUESTION 121
- (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 126
- (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 130
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 134
- (Topic 3)
You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com network. Now, when you have finished your penetration testing, you find that the weare- secure.com server is highly vulnerable to SNMP enumeration. You advise the we-are-secure Inc. to turn off SNMP; however, this is not possible as the company is using various SNMP services on its remote nodes. What other step can you suggest to remove SNMP vulnerability?
Each correct answer represents a complete solution. Choose two.

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

Answer: BC

NEW QUESTION 139
- (Topic 3)
Which of the following are the drawbacks of the NTLM Web authentication scheme?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: AB

NEW QUESTION 144
- (Topic 3)
You work as an IT Technician for uCertify Inc. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company's wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

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

Answer: A

NEW QUESTION 147
- (Topic 3)
Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?

A. Application layer
B. Link layer
C. Internet layer
D. Transport Layer

Answer: B

NEW QUESTION 150
- (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 153
- (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 154
- (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 155
- (Topic 3)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-aresecure server. Which of the following are countermeasures against a brute force attack?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: AB

NEW QUESTION 157
- (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 159
- (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 161
- (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 164
- (Topic 4)
Which of the following syntaxes is the correct syntax for the master.dbo.sp_makewebtask procedure?

A. sp_makewebtask [@inputfile =] 'inputfile', [@query =] 'query'
B. sp_makewebtask [@outputfile =] 'outputfile', [@query =] 'query'
C. sp_makewebtask [@query =] 'query', [@inputfile =] 'inputfile'
D. sp_makewebtask [@query =] 'query', [@outputfile =] 'outputfile'

Answer: B

NEW QUESTION 166
- (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 168
- (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 172
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

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

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

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

Answer: C

NEW QUESTION 175
- (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 178
- (Topic 4)
Which of the following is an open source Web scanner?

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

Answer: A

NEW QUESTION 181
- (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 186
- (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 188
- (Topic 4)
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. A virus
B. Spam
C. Blue jacking
D. Blue snarfing

Answer: C

NEW QUESTION 190
- (Topic 4)
Which of the following nmap switches is used to perform ICMP netmask scanning?

A. -PM
B. -PB
C. -PI
D. -PS

Answer: A

NEW QUESTION 193
- (Topic 4)
Which of the following tools is an example of HIDS?

A. Anti-Spector
B. Auditpol.exe
C. Elsave
D. Log File Monitor

Answer: D

NEW QUESTION 198
- (Topic 4)
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. Kismet
B. NetStumbler
C. Ettercap
D. Tcpdump

Answer: B

NEW QUESTION 199
- (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 200
- (Topic 4)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 205
- (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 210
- (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 213
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network:
Gathering information
Determining the network range
Identifying active systems
Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

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

Answer: B

NEW QUESTION 216
- (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 218
- (Topic 4)
Which of the following options holds the strongest password?

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

Answer: B

NEW QUESTION 219
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 222
- (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 224

.....

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