

GPEN Dumps

GIAC Certified Penetration Tester

<https://www.certleader.com/GPEN-dumps.html>



NEW QUESTION 1

- (Topic 1)

If the privacy bit is set in the 802.11 header, what does it indicate?

- A. SSID cloaking is being use
- B. Some form of encryption is In us
- C. WAP is being use
- D. Some form of PEAP is being use

Answer: C

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 to examine the web server
- B. Trapping and changing response values is beneficial for web site testing but using the same cached values in your browser will prevent you from being able to change those values
- C. Trapping and changing response values is beneficial for web site testing but will cause browser instability if not cleared
- D. Values trapped and changed in the proxy, such as a cookie, will be stored by the browser and may impact further testing

Answer: D

NEW QUESTION 3

- (Topic 1)

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

- A. The proxy is likely hung and must be restarted
- B. The proxy is configured to trap responses
- C. The proxy is configured to trap requests
- D. The site you are trying to reach is currently down

Answer: C

NEW QUESTION 4

- (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-force password attack
- B. There isn't an advantage as Nessus will ultimately discover this information
- 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 5

- (Topic 1)

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

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

Answer: C

NEW QUESTION 6

- (Topic 1)

You are running a vulnerability scan on a remote network and the traffic is not making it to the target system. You investigate the connection issue and determine that the traffic is making it to the internal interface of your network firewall, but not making it to the external interface or to any systems outside your firewall. What is the most likely problem?

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

Answer: C

NEW QUESTION 7

- (Topic 1)

You suspect that system administrators in one part of the target organization are turning off their systems during the times when penetration tests are scheduled, what feature could you add to the 'Rules of engagement' that could help your team test that part of the target organization?

- A. Unannounced test
- B. Tell response personnel the exact time the test will occur
- C. Test systems after normal business hours
- D. Limit tests to business hours

Answer: C

NEW QUESTION 8

- (Topic 1)

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (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 1=1...
- C. 'or 1=1--
- D. 'or 1=1'

Answer: D

NEW QUESTION 10

- (Topic 1)

When DNS is being used for load balancing, why would a penetration tester choose to identify a scan target by its IP address rather than its host name?

- A. A single IP may have multiple domains
- B. A single domain name can only have one IP address
- C. Scanning tools only recognize IP addresses
- D. A single domain name may have multiple IP addresses

Answer: C

Explanation:

Reference: <http://www.flashcardmachine.com/sec-midterm.html>

NEW QUESTION 14

- (Topic 1)

What section of the penetration test or ethical hacking engagement final report is used to detail and prioritize the results of your testing?

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

Answer: C

NEW QUESTION 19

- (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 22

- (Topic 1)

As part of a penetration test, your team is tasked with discovering vulnerabilities that could be exploited from an inside threat vector. Which of the following activities fall within that scope?

- A. SQL injection attacks against the hr intranet website
- B. A competitor's employee scanning the company's website
- C. Wireless "war driving" the company manufacturing site
- D. Running a Nessus scan from the sales department network
- E. B, C, and D
- F. A,
- G. and D
- H. B and D
- I. A and D

Answer: C

NEW QUESTION 24

- (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 28

- (Topic 1)

Which of the following is the JavaScript variable used to store a cookie?

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

Answer: C

Explanation:

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

NEW QUESTION 30

- (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 35

- (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 39

- (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 42

- (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)

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

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

Answer: A

NEW QUESTION 48

- (Topic 1)

Which of the following is possible in some SQL injection vulnerabilities on certain types of databases that affects the underlying server OS?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 50

168.116.9 is an IP address for www.scanned-server.com. Why are the results from the two scans, shown below, different?

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

Answer: C

NEW QUESTION 53

- (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 57

- (Topic 1)

What command will correctly reformat the Unix password copy and shadow copy files for input to John The Ripper?

- A. `/usr/share/wordlists/rockyou.txt shadowcopy > johnfile`
- B. `/usr/share/wordlists/rockyou.txt shadowcopy > johnfile`
- C. `/usr/share/wordlists/rockyou.txt shadowcopy passwordcopy > johnfile`
- D. `/usr/share/wordlists/rockyou.txt shadowcopy > johnfile`

Answer: C

Explanation:

Reference:

<https://books.google.co.in/books?id=SC-tAwAAQBAJ&pg=PA286&lpg=PA286&dq=/Unshadow+shadow+copy+passwd+copy+%3Ejohn+file&source=bl&ots=OnZK9atlc1&sig=co7EM5EHye96vO74W3wZxky3sXU&hl=en&sa=X&ei=FBuoVPLHDc-cugSDxYGYBA&ved=0CCwQ6AEwAg#v=onepage&q=%2FUnshadow%20shadow%20copy%20passwd%20copy%20%3Ejohn%20file&f=false>

NEW QUESTION 59

- (Topic 1)

Analyze the command output below. What information can the tester infer directly from the Information shown?

- A. Usernames for the domain tesrdomain.com
- B. Directory indexing is allowed on the web server
- C. Vulnerable versions of Adobe software in use
- D. Naming convention for public documents

Answer: D

NEW QUESTION 62

- (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 67

- (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 this is happening?

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

Answer: D

NEW QUESTION 68

- (Topic 1)

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

- A. Salts increase the time to crack the original password by increasing the number of tables that must be calculated
- B. Salts double the total size of a rainbow table database
- C. Salts can be reversed or removed from encoding quickly to produce unsalted hashes
- D. Salts have little effect because they can be calculated on the fly with applications such as Ophcrack

Answer: B

NEW QUESTION 72

- (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 74

- (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 is required

Answer: C

NEW QUESTION 79

- (Topic 1)

You have been contracted to map a 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 80

- (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 comparison
- B. Applications take advantage of 64-bit CPU processor and multithread the cracking process
- 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 83

- (Topic 2)

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a 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 84

- (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?

- 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 87

- (Topic 2)

Which of the following is the frequency range to tune IEEE 802.11a network?

- A. 1.15-3.825 GHz
- B. 5.15-5.825 GHz
- C. 5.25-9.825 GHz
- D. 6.25-9.825 GHz

Answer: B

NEW QUESTION 88

- (Topic 2)

You run the following bash script in Linux:

for i in 'cat hostlist.txt' ;do nc -q 2 -v \$i 80 < request.txt done where, hostlist.txt file contains the list of IP addresses and request.txt is the output file.

Which of the following tasks do you want to perform by running this script?

- A. You want to perform port scanning to the hosts given in the IP address lis

- B. You want to transfer file hostlist.txt to the hosts given in the IP address lis
- C. You want to perform banner grabbing to the hosts given in the IP address lis
- D. You want to put nmap in the listen mode to the hosts given in the IP address lis

Answer: C

NEW QUESTION 92

- (Topic 2)

Analyze the output of the two commands below:

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 94

- (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 99

- (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 100

- (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 102

- (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 107

- (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 108

- (Topic 2)

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services? Each correct answer represents a complete solution. Choose all that apply.

- A. Cheops
- B. Fport
- C. Elsave
- D. Cheops-ng

Answer: AD

NEW QUESTION 112

- (Topic 2)

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. Use macoff to change MAC addres
- C. Guess the sequence number
- D. Use brutus to crack telnet passwor

Answer: C

NEW QUESTION 116

- (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 121

- (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 125

- (Topic 2)

Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

- A. Whishker
- B. Nmap
- C. Nessus
- D. SARA

Answer: C

NEW QUESTION 127

- (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 132

- (Topic 2)

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value. What may be the reason?

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

Answer: B

NEW QUESTION 134

- (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 137

- (Topic 2)

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

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

Answer: D

NEW QUESTION 139

- (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 141

- (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 144

- (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 password
- B. It is mostly used when no Active Directory domain exist
- C. It is a challenge-response authentication protocol
- D. It uses the MD5 hash of the user's password

Answer: ABC

NEW QUESTION 145

CORRECT TEXT - (Topic 2)

Write the appropriate attack name to fill in the blank.

In a _____ DoS attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields.

A.

Answer: land

NEW QUESTION 149

- (Topic 2)

Which of the following tools uses exploits to break into remote operating systems?

- A. Nessus
- B. Metasploit framework
- C. Nmap
- D. John the Ripper

Answer: B

NEW QUESTION 151

- (Topic 2)

Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

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

Answer: A

NEW QUESTION 153

- (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 '=' 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 154

- (Topic 3)

You work as a Network Administrator for Tech-E-book Inc. You are configuring the ISA Server

2006 firewall to provide your company with a secure wireless intranet. You want to accept inbound mail delivery through an SMTP server. What basic rules of ISA Server do you need to configure to accomplish the task.

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

Answer: B

NEW QUESTION 155

- (Topic 3)

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

- A. `nmap -O -p`
- B. `nmap -sS`
- C. `nmap -sU -p`
- D. `nmap -sT`

Answer: A

NEW QUESTION 157

- (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 161

- (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 164

- (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-are-secure server. Which of the following are countermeasures against a brute force attack?

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

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

Answer: BD

NEW QUESTION 165

- (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 170

- (Topic 3)

Which of the following tools can be used by a user to hide his identity?

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

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

Answer: ACE

NEW QUESTION 174

- (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 179

- (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 184

- (Topic 3)

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He uses a Windows XP operating system to do this. He enters the following command on the command prompt:

c:\tracert www.we-are-secure.com

However, he receives an incomplete traceroute result. What could be the reasons for getting an incomplete result for the tracert command?

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

- A. A router along the path is overloade
- B. John's computer is behind a firewall that blocks incoming ICMP error message
- C. There is no route to the we-are-secure serve
- D. The we-are-secure server is down and is not connected to the Interne

Answer: ABCD

NEW QUESTION 185

- (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 188

- (Topic 3)

Which of the following can be used to mitigate the evil twin phishing attack?

- A. Magic Lantern
- B. Obiwan

C. IPSec VPN
D. SARA

Answer: C

NEW QUESTION 189

- (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 193

- (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 198

- (Topic 3)

Which of the following ports must you filter to check null sessions on your network?

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

Answer: A

NEW QUESTION 202

- (Topic 3)

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company's security policy states that all users using laptops must use smart cards for authentication. Which of the following authentication techniques will you use to implement the security policy of the company?

A. IEEE 802.1X using EAP-TLS
B. IEEE 802.1X using PEAP-MS-CHAP
C. Pre-shared key
D. Open system

Answer: A

NEW QUESTION 204

- (Topic 3)

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

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

Answer: C

NEW QUESTION 209

- (Topic 3)

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

Each correct answer represents a complete solution. Choose two.

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

Answer: BC

NEW QUESTION 213

- (Topic 3)

What happens when you scan a broadcast IP address of a network?

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

- A. It leads to scanning of all the IP addresses on that subnet at the same tim
- B. It will show an error in the scanning proces
- C. It may show smurf DoS attack in the network IDS of the victi
- D. Scanning of the broadcast IP address cannot be performe

Answer: AC

NEW QUESTION 215

- (Topic 3)

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He has to ping 500 computers to find out whether these computers are connected to the server or not. Which of the following will he use to ping these computers?

- A. PING
- B. TRACEROUTE
- C. Ping sweeping
- D. NETSTAT

Answer: C

NEW QUESTION 217

- (Topic 3)

You run the following command while using Nikto Web scanner:

```
perl nikto.pl -h 192.168.0.1 -p 443
```

What action do you want to perform?

- A. Updating Nikt
- B. Seting Nikto for network sniffin
- C. Port scannin
- D. Using it as a proxy serve

Answer: C

NEW QUESTION 219

- (Topic 3)

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

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

Answer: A

NEW QUESTION 222

- (Topic 3)

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc.

Recently, John's company has got a project to test the security of a promotional Website

www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:

```
<script>alert('Hi, John')</script>
```

After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John."

Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

- A. XSS attack
- B. Replay attack
- C. Buffer overflow attack
- D. CSRF attack

Answer: A

NEW QUESTION 227

- (Topic 3)

You want to perform passive footprinting against [we-are-secure Inc.](http://www.we-are-secure.com) Web server. Which of the following tools will you use?

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

Answer: C

NEW QUESTION 228

- (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 231

- (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 236

- (Topic 3)

You have received a file named new.com in your email as an attachment. When you execute this file in your laptop, you get the following message:

'EICAR-STANDARD-ANTIVIRUS-TEST-FILE!'

When you open the file in Notepad, you get the following string:

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

What step will you take as a countermeasure against this attack?

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

Answer: B

NEW QUESTION 239

- (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 243

- (Topic 3)

You want to retrieve the default security report of nessus. Which of the following google search queries will you use?

- A. site:pdf nessus "Assessment report"
- B. filetype:pdf nessus
- C. filetype:pdf "Assessment Report" nessus
- D. link:pdf nessus "Assessment report"

Answer: C

NEW QUESTION 244

- (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 245

- (Topic 3)

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

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

Answer: C

NEW QUESTION 247

- (Topic 3)

You enter the following URL on your Web browser:

`http://www.we-are-secure.com/scripts/..%co%af../..%co%`

`af../windows/system32/cmd.exe?/c+dir+c:\`

What task do you want to perform?

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

Answer: C

NEW QUESTION 248

- (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 252

- (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 253

- (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 255

- (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 firewall
- 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 256

- (Topic 3)

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

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

Answer: B

NEW QUESTION 260

- (Topic 3)

You have changed the RestrictAnonymous registry setting from 0 to 1 on your servers to secure your Windows 2000 system so that any malicious user cannot establish a null session on the server. However, when you test the security using userinfo tool, you got that you can still establish the null session. What may be its reason?

- A. You cannot disable establishing null session
- B. You need to disable the promiscuous mode of network Ethernet card
- C. You need to set the RestrictAnonymous key value to 2 instead of 1.
- D. You need to install a firewall

Answer: C

NEW QUESTION 261

- (Topic 3)

Which of the following commands can be used for port scanning?

- A. nc -z
- B. nc -t
- C. nc -w
- D. nc -g

Answer: A

NEW QUESTION 264

- (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 265

- (Topic 4)

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

Answer: A

NEW QUESTION 266

- (Topic 4)

Which of the following does NOT use a proxy software to protect users?

- A. Stateful inspection
- B. Packet filtering
- C. Application layer gateway
- D. Circuit level proxy server

Answer: D

NEW QUESTION 270

- (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 273

- (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 278

- (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 282

- (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 287

- (Topic 4)

How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 291

- (Topic 4)

Which of the following tools can be used to find a username from a SID?

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

Answer: C

NEW QUESTION 294

- (Topic 4)

What does APNIC stand for?

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

Answer: A

NEW QUESTION 295

- (Topic 4)

Which of the following is a web ripping tool?

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

Answer: D

NEW QUESTION 299

- (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 304

- (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 305

- (Topic 4)

Which of the following TCSEC classes defines verified protection?

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

Answer: C

NEW QUESTION 308

- (Topic 4)

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

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

Answer: D

NEW QUESTION 312

- (Topic 4)

Which of the following Penetration Testing steps includes network mapping and OS fingerprinting?

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

Answer: A

NEW QUESTION 313

- (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 314

- (Topic 4)

Which of the following is the correct sequence of packets to perform the 3-way handshake method?

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

Answer: C

NEW QUESTION 317

- (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 321

- (Topic 4)

Which of the following is NOT a Back orifice plug-in?

- A. BOSOCK32
- B. STCPPIO
- C. BOPeep
- D. Beast

Answer: D

NEW QUESTION 326

- (Topic 4)

Which of the following is the correct syntax to create a null session?

- A. c:\>net view \\IP_addr\IPC\$ "" /u: ""
- B. c:\>net view \\IPC\$\\IP_addr "" /u: ""
- C. c:\>net use \\IP_addr\IPC\$ "" /u: ""
- D. c:\>net use \\IPC\$\\IP_addr "" /u: ""

Answer: C

NEW QUESTION 328

- (Topic 4)

You want to run the nmap command that includes the host specification of 202.176.56-57.*. How many hosts will you scan?

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

Answer: C

NEW QUESTION 333

- (Topic 4)

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

- A. Scanning port
- B. Analyzing job requirement
- C. Querying the search engine
- D. Performing the whois query

Answer: A

NEW QUESTION 338

- (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 343

- (Topic 4)

In which of the following attacks does the attacker overload the CAM table of the switch?

- A. Mac flooding
- B. Man-in-the-middle attack
- C. Monkey-in-the-middle attack
- D. ARP poisoning

Answer: A

NEW QUESTION 344

- (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 345

- (Topic 4)

In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?

- A. Cross-site scripting
- B. Session sidejacking
- C. ARP spoofing
- D. Session fixation

Answer: B

NEW QUESTION 348

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GPEN Exam with Our Prep Materials Via below:

<https://www.certleader.com/GPEN-dumps.html>