312-50

(Certified Ethical Hacker Exam)

Total Questions: 574
Last Updated: Apr 23, 2009
Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' 312-50 study guide is a comprehensive compilation of

Questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: **refund@techeXams.ws**. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: **feedback@techeXams.ws**

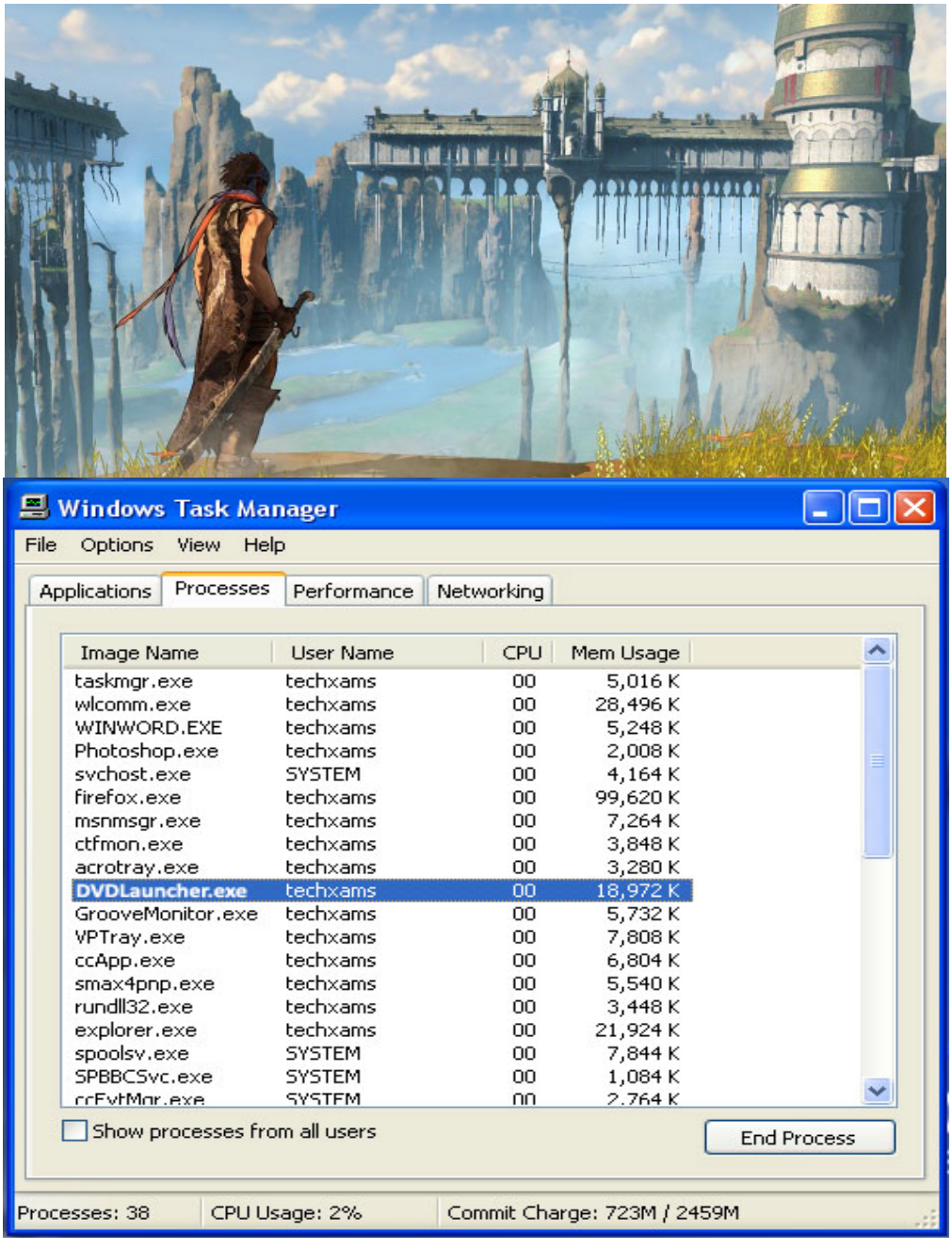
Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

© Copyright www.techeXams.ws 2008

Question 1:

John wants to try a new hacking tool on his Linux System. As the application comes from a site in his untrusted zone, John wants to ensure that the downloaded tool has not been Trojaned. Which of the following options would indicate the best course of action for John?



A. Obtain the application via SSL
B. Obtain the application from a CD-ROM disc

2

© Copyright www.techeXams.ws 2008

C. Compare the files' MD5 signature with the one published on the distribution media
D. Compare the file's virus signature with the one published on the distribution media

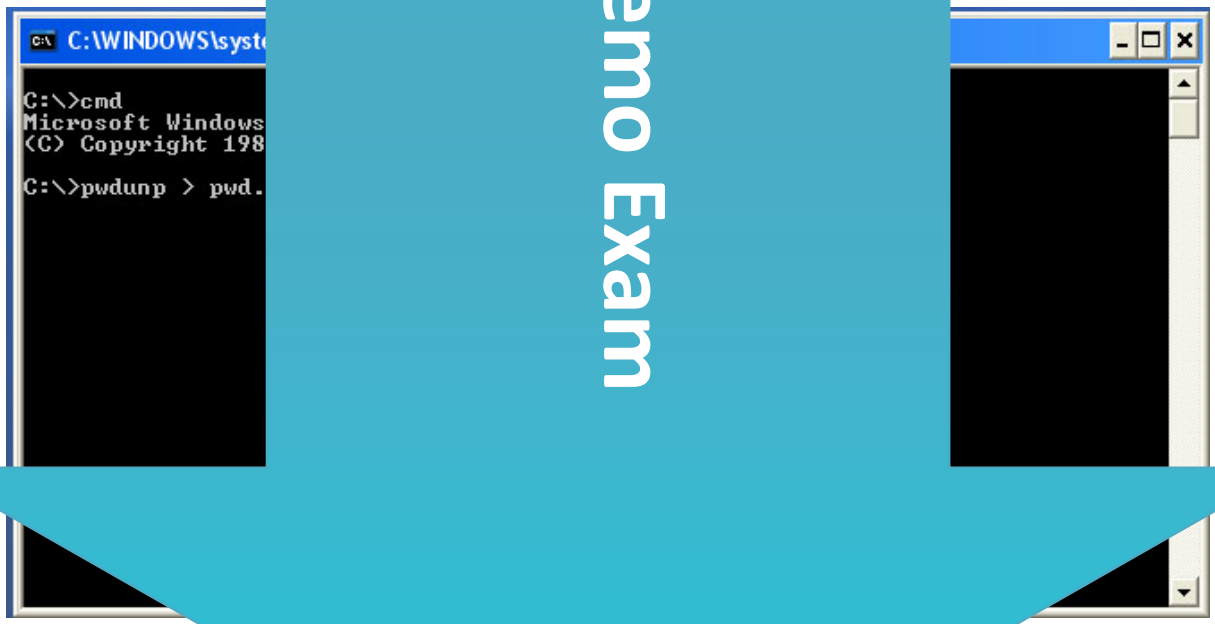
Answer: C

Explanation:

In essence, MD5 is a w … checksum and many other commonly used …

Question 2:

Michael is the secur … has been charged with strengthening … ord policies. Due to certain legacy applic … d group policy in Active Directory wit … company's employes, however … e must have complex passwords … e that everyone is using complex passw … nts. Michael has just logged on to on … to run the following command …



A. Dumps SAM pass…
B. Password history file is …
C. Dumps Active Directory pas…
D. Internet cache file is piped to pw…

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Answer: A

Explanation:

Pwdump is a hack tool … mote Windows computer. Pwdump > … e named pwd.txt

Question 3:

You have successful… Web Server using Brutus hacking tool. …ni@". You logon to the system using … rootkits. After downloading variou… …ine, you proceed to clear the log files … C:\Windows\system… …empts?

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

Answer: B

Explanation:

The Security Event log … against the system.

Question 4:

Spears Technology, … …os Angeles, California. They rep… …defenses has been do… Technol… intellectual p… …an employees home … …ic's corporate VPN network. The appli… …ttack to open a "Back Door" allowing the hackers … …each was discovered when customers complained about the … …ds without their knowledge. The hackers were traced back to Beijing Chi… …mail address evidence. The credit card information was sent to that same e-m… address. The passwords allowed the hackers to access Spears Technology's network from a remote location, posing as employees. The intent of the attacker was to steal the source code for their VOIP system and "hold it hostage" from Spears Technology, Inc exchange for ransom. The hackers had intended on selling

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

the stolen VOIP software source code to competitors. How would you prevent such attacks from occurring in the future at Spears Technology?

A. Disable VPN ac
B. Allow VPN acce authentication
C. Replace the VP twork
D. Enable 25 chara e VPN network.

Answer: A

Explanation:

As long as there is a w n't be secure because you never know what workplace.

Question 5:

William has receive ramming class through email. Willi ame very well, but decides to install th William installs the game, he plays it fo Tetris game again and notices that his is Task Manager and sees the followi illiam just installed?

A. Remote Access
B. Zombie Zapper
C. Bot IRC Tunnel
D. Root Digger (RD

Answer: A

Explanation:

cont ns
such as Sy eration.
Intruders usua suspecting
users then execute c xecute the
malicious programs or are

Question 6:

What are the two basic types of attacks?(Ch se two.

A. DoS
B. Passive
C. Sniffing
D. Active

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

E. Cracking

Answer: B, D

Explanation:

Passive and active atta

Question 7:

You are footprinting visit the acme.com website for contact o not find it listed there. You know tha website 12 months ago but now it is no information from the website that is

A. Visit google sea
B. Visit Archive.or .
C. Crawl the entire
D. Visit the compa

Answer: B

Explanation:

The Internet Archive (an archive of Web and multimedia resou his archive includes "snapshots of the Wor points in time), software, movies, boo certs from bands that allow it). This site is fo

User whi mail scams and ma

A. 18 U.S.C 1029 Posse
B. 18 U.S.C 1030 Fraud and nputers
C. 18 U.S.C 1343 Fraud by wire,
D. 18 U.S.C 1361 Injury to Government
E. 18 U.S.C 1362 Government communicati tems
F. 18 U.S.C 1831 Economic Espionage Act
G. 18 U.S.C 1832 Trade Secrets Act

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Answer: B

Explanation:

http://www.law.corne ...000-.html

Question 9:

Which of the followi ...printing?

A. Go through the ... discarded.
B. Search on finan...
C. Scan the range ...
D. Perform multipl...

Answer: C

Explanation:

Passive footprinting is ... the target systems.
Scanning the range of ... contact to the
systems behind the IP ...

Question 10:

Which one of the fo... rrect Internet Protocol (IP) addres...

A. Network aliasin...
B. Domain Name S...
C. Reverse Addres...
D. Port scanning

E...

This referen... NS DOS
attack can occur. ... alter in this
fashion, which they sh... there server instead
of replacing the actual reco...

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Question 11:

You are footprinting … You visit the company's website … t do not find it listed there. You kn… their website 12 months ago but not… retrieve information from th…

A. Visit google's se…
B. Visit Archive.or… 's website.
C. Crawl the entir…
D. Visit the compa…

Answer: B

Explanation:

Archive.org mirrors w… ng on the crawl time. Archive.org dates bac… recent as the latest crawl, the cache is ove… iteis incorrect because that's the sar… osites is just bogus. The answer is then Fir…

Question 12:

A TecheXams securi… ystem log files. He notes the following… - Network log files a… At 14:00 hours, the … ened and what should he do about…

A. He should cont… nnection disconnected.
C. …
D. He s… e system problem.
E. He should disc… ized use, because an attack has taken place.

Answer: B

Explanation:

You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

312-50 Demo Exam

Question 13:

To what does "mess … n of email security?

A. Message repud … vers a message was passed through.
B. Message repud … e that damaged their reputation.
C. Message repud … sent from a particular person.
D. Message repud … sent from a certain host.
E. Message repud … d a particular message.

Answer: E

Explanation:

A quality that prevent … tion between two other parties ever too … communications to be traceable. Non-rep … at a communication between two other pa … to be able to trace your communications … ssage submission or delivery.

Question 14:

How does Traceroute … to point B?

C. … in transit …
D. It manipula … messages.

Answer: C

Explanation:

Traceroute works by increasing the "time-to-… of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the

© Copyright www.techeXams.ws 2008

sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

Question 15:

Snort has been used[illegible] packets, the penetration tester f[illegible] tester, why would you find this [illegible] ncept learnt during passive OS fingerpri[illegible] lity to read packet signatures from a sr[illegible] 337 -> 172.16.1.101:1 TCP [illegible] k: 0x53 Win: 0x400 ... 05/20-17:06:58.6[illegible] P TTL:44 TOS:0x10 ID:242 ***FRP Se[illegible] t this attack? (Choose the most a[illegible]**

A. This is not a spo[illegible] e three flags.
B. This is back orif[illegible]
C. The attacker wa[illegible] normally valid.
D. There packets v[illegible] rd IP stack.

Answer: B

Explanation:

Port 31337 is normally[illegible] of 'elite', meaning 'elite hackers'.

Question 16:

Your TecheXams tra[illegible] gional Internet Registry (RIR's)?

A. APNIC, PICNIC, [illegible]

D. [illegible]

Answer: B

Explanation:

All other answers includenon exist[illegible], LATNIC). See http://www.arin.net/library/internet_in[illegible]

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Question 17:

A very useful resource for passively gathering information about a target company is:

A. Host scanning
B. Whois search
C. Traceroute
D. Ping sweep

Answer: B

Explanation:

A, C & D are "Active" s

Question 18:

You receive an ema aving technical difficulty in restorin ur account data is corrupted. Please lo r password. http://www.supern gon.htm If you do not reset your passv ly disabled locking you out from our e- ailServices From this e-mail you susp e you have been using their e-mail se out an e-mail such as this. You also obs icion about 0xde.0xad.0xbde.0x ediately enter the following at Windov f You get a response with a vali ne e-mail URL?

A. 222.173.190.23
B. 233.34.45.64
C. 54.23.56.55
D. 199.223.23.45

: A

Explana

0x stands for hexad

Question 19:

Which of the following tools are used for fo inting?(Choose four.

A. Sam Spade
B. NSLookup C. Traceroute
D. Neotrace
E. Cheops

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Answer: A, B, C, D

Explanation:

All of the tools listed a

Question 20:

According to the CE ned after footprinting?

A. Enumeration
B. Scanning
C. System Hacking
D. Social Engineer
E. Expanding Influ

Answer: B

Explanation:

Once footprinting has anning should take place on two distinct

Question 21:

NSLookup is a good arget network. What does the follo ddress> > set type =any > ls -d <target

A. Enables DNS sp
B. Loads bogus er
C. Verifies zone se

Answer: D

Explanation:

If DNS has not been properly d above will perform a zone transfer.

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Question 22:

While footprinting a ... attempt a zone transfer?

A. 53 UDP
B. 53 TCP
C. 25 UDP
D. 25 TCP
E. 161 UDP
F. 22 TCP
G. 60 TCP

Answer: B

Explanation:

IF TCP port 53 is detect

Question 23:

Your lab partner is t... tors web site. The site has a .com exter... ols and look in one of the regional Inter... ks in first?

A. LACNIC
B. ARIN
C. APNIC
D. RIPE
E. AfriNIC

Answer: B

Explanation:

don... a
.com do...

Question 24:

Network Administrator Patricia is ... twork. Below are some of her findings concerning DNS. Which of the... ause for alarm? Select the best answer.

A. There are two external DNS Servers for Internet domains. Both are AD integrated.
B. All external DNS is done by an ISP.
C. Internal AD Integrated DNS servers are using private DNS names that are

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

A. unregistered.
D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server

Answer: A

Question 25:

Doug is conducting a ... lient target network has a web ... p and running. Doug has been swe... y response from the remote target. W... e behind this lack of response? Select

A. UDP is filtered b...
B. The packet TTL ...
C. The host might ...
D. The destination ...
E. The TCP windo...
F. ICMP is filtered ...

Answer: A, B, C, F

Explanation:

If the destination host ... t an answer and if TTL (Time To Live) is se... host because of too many hops between th... ndow size is the amount of received da... e sending host can send only that amount ... window update from the receiving host and ... ans.

Question 26:

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

312-50 Demo Exam

ata bytes

Joe Hacker runs the … quence numbers in one of the hacking … an? Select two.

A. The first colum…
B. The second col… sequence number
C. The second col…

…wer: A, B

Question 27:

While performing a ping sw… reply of Code 3/Type 13 for all the pings sent out. What i… mind this response?

A. The firewall is dropping the packets.
B. An in-line IDS is dropping the packets.
C. A router is blocking ICMP.
D. The host does not respond to ICMP packets.

© Copyright www.techeXams.ws 2008

Answer: C

Explanation:

Type 3 message = Dest nication
Administratively Prohi

Question 28:

The following excerp tivities across three days. There ar ccessful. Study the log given below and e of this Questions is to test gerprinting (which should tell them the attack signature; can they infer if a us they can read plain source - destination

"

Apr 24 14:46:46 [4 .169
Apr 24 14:46:46 [4 .107:482
Apr 24 14:46:46 [4 72.16.1.107:53
Apr 24 14:46:46 [4 -> 172.16.1.107:21
Apr 25 08:02:41 [5 .53
Apr 25 02:08:07 [5 72.16.1.107:53
Apr 25 02:08:07 [5 72.16.1.101:53
Apr 25 02:38:17 [5 .1.107:111
Apr 25 19:37:32 [5 21 ->
172.16.1.107:80
Apr 26 05:45:12 [6 2.16.1.101:53
Apr 26 06:43:05 [6 07:53
Apr 26 06:44:25 vic simple by (uid=0)

Apr
Apr 26 06 :4558

"

What can you infer from the above log?

A. The system is a windows system which is being scanned unsuccessfully.

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

B. The system is a web application server compromised through SQL injection.
C. The system has been compromised and backdoored by the attacker.
D. The actual IP c

Answer: A

Question 29:

Bob has been hired … He begins by looking at IP addre… main name registration. He the… ee if they are leaking any sensitiv… Within the context of penetration test…

A. Passive inform…
B. Active informa…
C. Attack phase
D. Vulnerability M…

Answer: A

Explanation:

He is gathering inform… f the targets systems he is considered gath…

Question 30:

Which of the follov… MTP message to an address that does …

A. To create a de…
B. To verify infor…

Answer: C

Explanation:

The replay from the emai… t will also give you some information about the name of… so on.

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Question 31:

You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and a show port 21 in closed state. What s med?

A. Connect to oper
B. Perform a ping s .
C. Perform a SYN s ght be up.
D. Rescan every co

Answer: C

Explanation:

As ICMP is blocked you running by using a ping sweep. As all the closed, probably any additional, previou nning a SYN scan on port 21 over the target

Question 32:

Ann would like to pe s not concerned about being stealth a ould be the most accurate and reliabl

A. A half-scan
B. A UDP scan
C. A TCP Connect s
D. A FIN scan

Answer: C

Explanation:

me
port sca e of a
three-way ha
[192.168.0.8] [192. 5840
[192.168.0.10] [192.168. 8695210 LEN=0
WIN=65535
[192.168.0.10] TCP: D=80 S=49389
[192.168.0.10] TCP: D=80 S=49389 RST 2=5840

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Question 33:

What type of port scan is shown below?

312-50 Demo Exam

A. Idle Scan
B. Windows Scan

Answer: C

Explanation:

An Xmas port scan is variant ain information about the state of a target port by sending a s set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, UR s to confuse and bypass simple firewalls. Some stateless firewalls only chec y policy those packets which have the SYN flag set (that is, packets that te connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

© Copyright www.techeXams.ws 2008

312-50 Demo Exam

Question 34:

War dialing is a very ... years ago. Why would a modem sec...

A. It is cool, and if ...
B. It allows circumv... al network.
C. It allows circumv...
D. A good security ...

Answer: B

Explanation:

If you are lucky and fin... etwork, it usually is less protected (as only ...ce connected you don't need to take eva...

Question 35:

An attacker is attem... MZ. The attacker doesn't want to get ... us tries he remains unsuccessful in conn... e target system is actually listening on ...g2. He is still unable to connect to ...on?

A. The firewall is b...
B. He cannot spoof...
C. He needs to use...

...wer: B

Explanation:

Spoofing your IP will on... get system. In this case the answer (login promp... "real" location of the IP address that you are showing as th...

© Copyright www.techeXams.ws 2008

Question 36:

You are scanning ir ry few conventional ports open. When y ation by connecting to the open ports, i re of which protocols are being ocols as possible. Which kind of scan swer)

A. Nessus scan w
B. Nmap scan wit
C. Netcat scan wi
D. Nmap with the

Answer: D

Explanation:

Running Nmap with t can is a bit different than the other nmap rotocols in use by the remote station, such P protocols such as EGP or IGP may be id

Question 37:

What are twp type ?

A. It uses types 0
B. It uses types 1
C. It uses types 1
D. The ping comn

Answer: A

Explanation:

Question 38:

You are having problen port scanning during internal testing. You verify t between you and the target system. When both stealth and c work, you decide to perform a NULL scan with N few systems scanned shows all ports open. Which one of the following statement is probably true?

A. The systems have all ports open.
B. The systems are running a host based IDS.
C. The systems are web servers.
D. The systems are running Windows.

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

Answer: D

Explanation:

The null scan turns off ur in the real world. If the port is closed, a ort results in no response. Unfortunate standard and do things their own way. Windows as they choose not to respons eing scanned is running Microsoft Win

Question 39:

John has scanned th ther enough information to help mote host accurately. What wo is being used on the remote web serv

A. Connect to the
B. Connect to the
C. Telnet to port 8
D. Telnet to an ope

Answer: D

Explanation:

Most people don't care stening to open ports and therefore yo anners from open ports with, for exampl

Question 40:

gues tp 23 telnet

A. This is a Windo
B. The host is not firew
C. The host is not a Linux o
D. Thehost is not properly patche

Answer: D

Explanation:

If the answer was A nmap would guess it, it holds the MS signature database, the host not being firewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not properly patched? That is the closest; nmaps OS

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN's or if your using a program tochange the ISN then OS detection will fail. If the TCP/IP IP ID's are modified then os detection could also fail, because the machine

Question 41:

What port scanning et system and then looking for adjustm

A. Blind Port Scan
B. Idle Scanning
C. Bounce Scannir
D. Stealth Scannir
E. UDP Scanning

Answer: B

Explanation:

from NMAP: -sI <zom d allows for a truly blind TCP port scan of om your real IP address). Instead, a u ntation ID" sequence generation on the zor e target.

Question 42:

What port scanning ctable?

A. Null Scanning
B. Connect Scanni
D. Idlescan Scanni
E. Half Scanning
F. Verbose Scanni

A TCP Conn ning method. If a port ake, and the port scanner immedia

Question 43:

What does an ICMP (Code 13) message normally indicates?

A. It indicates that the destination host is unreachable
B. It indicates to the host that the datagram which triggered the source quench message will need to be re-sent

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

C. It indicates that the packet has been administratively dropped in transit
D. It is a request to the host to cut back the rate at which it is sending traffic to the Internet destination

Answer: C

Explanation:

CODE 13 and type 3 is ...atively prohibited by filtering hence maybe ...ype 3 B - Type 4 C - Type 3 Code 13 D - Typ...

Question 44:

Because UDP is a co...

A. UDP recvfrom()...
B. It can only be us...
C. It can only be us...
D. There is no guar...
E. ICMP port unrea...

Answer: D, E

Explanation:

Neither UDP packets, r... so UDP scanners must ...be lost (or you will get a bunch of false po...

Question 45:

You are scanning int... few conventional ports open. When y... ion by connecting ... Which...

A. Nmap with...
B. Nessus scan wit...
C. Nmap scan with the -...
D. Netcat scan with the -u -e ...

Answer: A

Explanation:

Running Nmap with the -sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

Question 46:

What ICMP messag

A. Timestamp rec
B. Echo request (8
C. Echo request ((
D. Ping request (1

Answer: B

Explanation:

ICMP Type 0 = Echo R

Question 47:

Which of the follow **p XMAS scan?**

A. Windows 2000
B. Any Solaris ver
C. Any version of
D. RedHat Linux 8

Answer: A

Explanation:

When running a XMA closed, while no response means it is low RFC 793 to the letter. A number of sy ether the port is

Question 48:

home/root # traceroute getcorp.com> traceroute to www.targetcorp.com <http: 2.168.12.18), 64 hops may, 40 byte packets 1 router.anon.com (19 ms 1.123 ms 1.280 ms 2 192.13.133.121 (192.13.133.121) 3.680 m ms 4.583 ms 3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms 4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms 5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms 6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms 7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms 6 * * * 7 * * * 8

312-50 Demo Exam

© Copyright www.techeXams.ws 2008

www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392 ms 3.348 ms 3.199 ms Use the traceroute results shown above to answer the following Question: The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

A. True
B. False

Answer: A

Explanation:

As seen in the exhibit the ewall filters packets where the TTL ha es for TTL you will get an answer from the t

Question 49:

While attempting to di computer, you receive the following r PHA9 (www.insecure.org/nm g ports on 172.121.12.222: (The 1 e: filtered) Port State Service 21/tcp op tcp open http 443/tcp open https Re match to reliably guess the OS. I ned in 277.483 seconds What should I

A. Perform a firewalk
B. Perform a tcp trac
C. Run an nmap scan
D. Connect to the act

Answer: D

Explanation:

po
ports wi

312-50 Demo Exam

© Copyright www.techeXams.ws 2008