GIAC

Exam Questions GPEN

GIAC Certified Penetration Tester

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (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 2
- (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 3
- (Topic 1)
A penetration tester used a client-side browser exploit from metasploit to get an unprivileged shell prompt on the target Windows desktop. The penetration tester then tried using the getsystem command to perform a local privilege escalation which failed. Which of the following could resolve the problem?

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

Answer: B

NEW QUESTION 4
- (Topic 1)
Analyze the screenshot below. What type of vulnerability is being attacked?

```
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process
   LPORT     4444             yes       The local port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.116.5
RHOST => 192.168.116.5
msf exploit(ms08_067_netapi) > set LPORT 52525
LPORT => 52525
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Triggering the vulnerability...
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) >
```

A. Windows Server service
B. Internet Explorer
C. Windows Powershell
D. Local Security Authority

Answer: B

NEW QUESTION 5
- (Topic 1)
What is the main difference between LAN MAN and NTLMv1 challenge/responses?

A. NTLMv1 only pads IS bytes, whereas LANMAN pads to 21 bytes
B. NTLMv1 starts with the NT hash, whereas LANMAN starts with the LANMAN hash
C. NTLMv1utilizes DES, whereas LANMAN utilizes MD4
D. NTLMv1 splits the hash into 3 eight-byte pieces, whereas LAN MAN splits the hash Into 3 seven-byte pieces

Answer: A

NEW QUESTION 6
- (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. Un announced test
B. Tell response personnel the exact lime the test will occur
C. Test systems after normal business hours
D. Limit tests to business hours

Answer: C

NEW QUESTION 7
- (Topic 1)
How can a non-privileged user on a Unix system determine if shadow passwords are being used?

A. Read /etc/password and look for "x" or “II” in the second colon-delimited field
B. Read /etc/shadow and look for “x” or “II” in the second colon-delimited field
C. Verify that /etc/password has been replaced with /etc/shadow
D. Read /etc/shadow and look NULL values In the second comma delimited field

Answer: B

NEW QUESTION 8
- (Topic 1)
ACME corporation has decided to setup wireless (IEEE 802.11) network in it's sales branch at Tokyo and found that channels 1, 6, 9,11 are in use by the neighboring offices. Which is the best channel they can use?

A. 4

B. 5
C. 10
D. 2

Answer: D

NEW QUESTION 9
- (Topic 1)
As pan or a penetration lest, 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 websit
B. A competitor's employee's scanning the company's websit
C. Wireless "war driving" the company manufacturing sit
D. Running a Nessus scan from the sales department networ
E. B, C, and D
F. A,
G. and D
H. B and D
I. A and D

Answer: C

NEW QUESTION 10
- (Topic 1)
You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular
password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

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

Answer: C

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

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

Answer: C

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

NEW QUESTION 11
- (Topic 1)
Approximately how many packets are usually required to conduct a successful FMS attack onWEP?

A. 250.000
B. 20.000
C. 10.000,000
D. l (with a weak IV)

Answer: B

NEW QUESTION 15
- (Topic 1)
Which Metasploit payload includes simple upload and download functionality for moving files to and from compromised systems?

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

Answer: D

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

NEW QUESTION 20
- (Topic 1)
All of the following are advantages of using the Metasploitpriv module for dumping hashes from a local Windows machine EXCEPT:

A. Doesn't require SMB or NetBIOS access to the target machine
B. Can run inside of a process owned by any user
C. Provides less evidence for forensics Investigators to recover
D. LSASS related reboot problems aren't an Issue

Answer: B

Explanation:
Reference:
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/2012_Jan_ISOAG.pdf

NEW QUESTION 21
- (Topic 1)
Which of the following describe the benefits to a pass-the-hash attack over traditional password cracking?

A. No triggering of IDS signatures from the attack privileges at the level of theacquired password hash and no corruption of the LSASS proces
B. No triggering of IDS signatures from the attack, no account lockout and use ofnative windows file and print sharing tools on the compromised syste
C. No account lockout, privileges at the level of the acquired password hash and useof native windows file and print Sharif tools on the compromised syste
D. No account lockout, use of native file and print sharing tools on the compromisedsystem and no corruption of the LSASS proces

Answer: D

NEW QUESTION 24
- (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 26
- (Topic 1)
You have compromised a Windows workstation using Metasploit and have injected the Meterpreter payload into the svchost process. After modifying some files to set up a persistent backdoor you realize that you will need to change the modified and access times of the files to ensure that the administrator can't see the changes you made. Which Meterpreter module would you need to load in order to do this?

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

Answer: D

NEW QUESTION 27
- (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 32
- (Topic 1)
You have been contracted to penetration test an e-mail server for a client that wants to know for sure if the sendmail service is vulnerable to any known attacks. You have permission to run any type of test, how will you proceed to give the client the most valid answer?

A. Run all known sendmail exploits against the server and see if you can compromisethe service, even if it crashed the machine or service
B. Run a banner grabbing vulnerability checker to determine the sendmail version andpatch level, then look up and report all the vulnerabilities that exist for that

versionand patch level
C. Run all sendmail exploits that will not crash the server and see if you cancompromise the service
D. Log into the e-mail and determine the sendmail version and patch level, then lookup and report all the vulnerabilities that exist for that version and patch level

Answer: C

NEW QUESTION 35
- (Topic 1)
You have been contracted to perform a black box pen test against the Internet facing servers for a company. They want to know, with a high level of confidence, if their servers are vulnerable to external attacks. Your contract states that you can use all tools available to you to pen test the systems. What course of action would you use to generate a report with the lowest false positive rate?

A. Use a port scanner to find open service ports and generate a report listing allvulnerabilities associated with those listening service
B. Use a vulnerability or port scanner to find listening services and then try to exploitthose service
C. Use a vulnerability scanner to generate a report of vulnerable service
D. Log into the system and record the patch levels of each service then generate areport that lists known vulnerabilities for all the running service

Answer: B

NEW QUESTION 38
- (Topic 1)
You have been contracted to map me network and try to compromise the servers for a client. Which of the following would be an example of scope creep' with respect to this penetration testing project?

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

Answer: B

NEW QUESTION 41
- (Topic 1)
Which of the following is the feature that separates the use of Rainbow Tables from other applications such as Cain or John the Ripper?

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

Answer: B

NEW QUESTION 46
- (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 51
CORRECT TEXT - (Topic 2)
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 54
- (Topic 2)
You execute the following netcat command:
c:\target\nc -1 -p 53 -d -e cmd.exe
What action do you want to perform by issuing the above command?

A. Capture data on port 53 and performing banner grabbin
B. Capture data on port 53 and delete the remote shel
C. Listen the incoming traffic on port 53 and execute the remote shel
D. Listen the incoming data and performing port scannin

Answer: C

NEW QUESTION 55
- (Topic 2)
You work as an Administrator for Bluesky Inc. The company has 145 Windows XP Professional client computers and eighty Windows 2003 Server computers. You want to install a security layer of WAP specifically designed for a wireless environment. You also want to ensure that the security layer provides privacy, data integrity, and authentication for client-server communications over a wireless network. Moreover, you want a client and server to be authenticated so that wireless transactions remain secure and the connection is encrypted. Which of the following options will you use to accomplish the task?

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

Answer: C

NEW QUESTION 58
- (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 63
- (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 65
CORRECT TEXT - (Topic 2)
Fill in the blank with the appropriate tool.
____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

A.

Answer: NBTscan

NEW QUESTION 67
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following pre-attack phases while testing the security of the server:
Footprinting Scanning Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 71
- (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

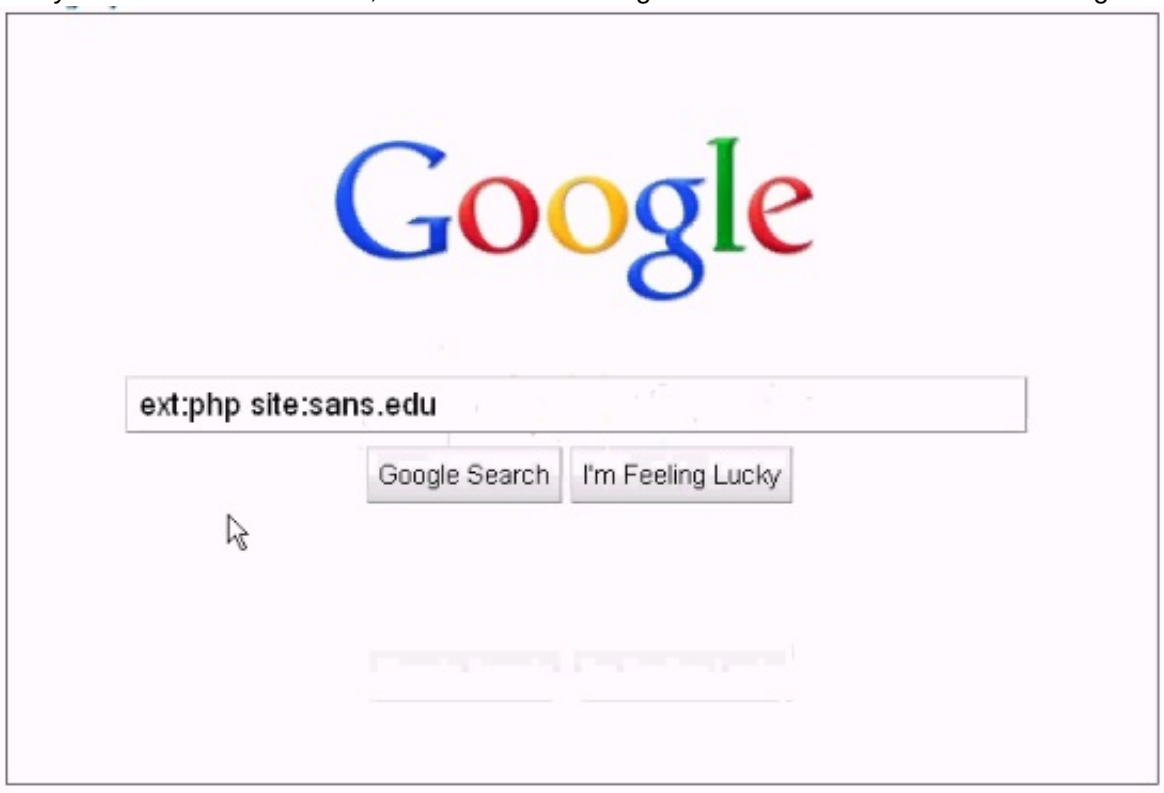
NEW QUESTION 72

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

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

Answer: C

NEW QUESTION 74
- (Topic 2)
Analyze the screenshot below, which of the following sets of results will be retrieved using this search?



A. Pages from the domain sans.edu that have external link
B. Files of type .php from the domain sans.ed
C. Pages that contain the term ext:php and slte.sans.ed
D. Files of type .php that redirect to the sans.edu domai

Answer: A

NEW QUESTION 78
- (Topic 2)
Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack
B. Cross-Site Scripting attack
C. Cross-Site Request Forgery
D. Code injection attack

Answer: D

NEW QUESTION 82
- (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 86
- (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 91
- (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 95
- (Topic 2)
Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Fragroute
B. Absinthe
C. Stick
D. ADMutate

Answer: B

NEW QUESTION 99
- (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 102
- (Topic 2)
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 105
- (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 110
- (Topic 2)
Joseph works as a Network Administrator for WebTech Inc. He has to set up a centralized area on the network so that each employee can share resources and documents with one another. Which of the following will he configure to accomplish the task?

A. WEP
B. VPN
C. Intranet
D. Extranet

Answer: C

NEW QUESTION 112
- (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 116
- (Topic 3)
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

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

Answer: A

NEW QUESTION 121
- (Topic 3)
Which of the following scanning methods is most accurate and reliable, although it is easily detectable and hence avoided by a hacker?

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

Answer: C

NEW QUESTION 124
- (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 127
- (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 130
- (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 133
- (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 138
- (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 143
- (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 148
- (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 153
- (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 154
- (Topic 3)
Which of the following are the countermeasures against WEP cracking? Each correct answer represents a part of the solution. Choose all that apply.

A. Using a 16 bit SSI
B. Changing keys ofte
C. Using the longest key supported by hardwar
D. Using a non-obvious ke

Answer: BCD

NEW QUESTION 155
- (Topic 3)
Which of the following tools automates password guessing in the NetBIOS session?

A. L0phtCrack

B. John the Ripper
C. Legion
D. NTInfoScan

Answer: C

NEW QUESTION 159
- (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 161
CORRECT TEXT - (Topic 3)
Fill in the blank with the appropriate word.
____is a port scanner that can also be used for the OS detection.

A.
Answer: Nmap

NEW QUESTION 163
- (Topic 4)
Which of the following is a web ripping tool?

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

Answer: D

NEW QUESTION 167
- (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 170
- (Topic 4)
Which of the following tools allow you to perform HTTP tunneling?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 175
- (Topic 4)
Which of the following tools is used for SNMP enumeration?

A. SARA
B. Userinfo
C. Getif
D. Enum

Answer: C

NEW QUESTION 179
- (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 180
- (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

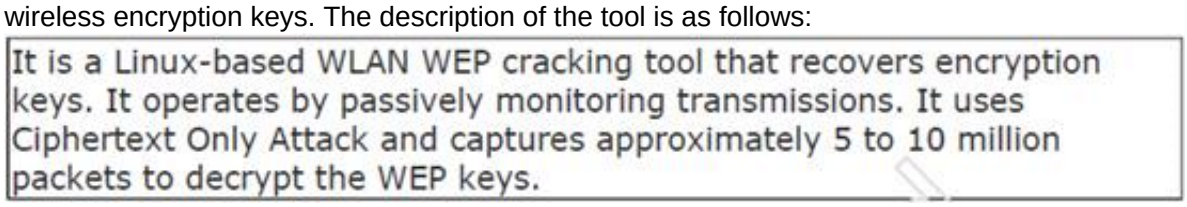
Answer: D

NEW QUESTION 183
- (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 186
- (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:



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 191
- (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 195
- (Topic 4)
Which of the following techniques are NOT used to perform active OS fingerprinting?
Each correct answer represents a complete solution. Choose all that apply.

A. ICMP error message quoting
B. Analyzing email headers
C. Sniffing and analyzing packets
D. Sending FIN packets to open ports on the remote system

Answer: BC

NEW QUESTION 196
- (Topic 4)
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He performs a Teardrop attack on the we-are-secure server and observes that the server crashes. Which of the following is the most likely cause of the server crash?

A. The spoofed TCP SYN packet containing the IP address of the target is filled in both the source and destination field

B. The we-are-secure server cannot handle the overlapping data fragment
C. The ICMP packet is larger than 65,536 byte
D. Ping requests at the server are too hig

Answer: B

NEW QUESTION 200
- (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 202
- (Topic 4)
You want to perform an active session hijack against Secure Inc. You have found a target that allows Telnet session. You have also searched an active session due to the high level of traffic on the network. What should you do next?

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

Answer: B

NEW QUESTION 203
- (Topic 4)
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. Internet layer
B. Application layer
C. Transport Layer
D. Link layer

Answer: D

NEW QUESTION 208
- (Topic 4)
Which of the following worms performs random scanning?

A. BugBear
B. SirCam
C. Code red worm
D. Klez

Answer: C

NEW QUESTION 209
- (Topic 4)
Which of the following tools is NOT used for wireless sniffing?

A. AirMagnet
B. Sniffer Wireless
C. AiroPeek
D. MiniStumbler

Answer: D

NEW QUESTION 210
- (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 215

- (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 216
- (Topic 4)
Which of the following tools is based on the SATAN tool?

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

Answer: D

NEW QUESTION 221
- (Topic 4)
Which of the following tools can be used for session splicing attacks?

A. ADMutate
B. APNIC
C. Whisker
D. ARIN

Answer: C

NEW QUESTION 223
- (Topic 4)
In which of the following attacks is a malicious packet rejected by an IDS, but accepted by the host system?

A. Insertion
B. Evasion
C. Fragmentation overwrite
D. Fragmentation overlap

Answer: B

NEW QUESTION 227
- (Topic 4)
Which of the following types of Penetration testing provides the testers with complete knowledge of the infrastructure to be tested?

A. White Box
B. Black Box
C. Grey Box
D. Water Fall

Answer: A

NEW QUESTION 229
- (Topic 4)
Which of the following tools is not a BlueSnarf attacking tool?

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

Answer: D

NEW QUESTION 230
- (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 231
- (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 234
- (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 237
.....

Relate Links

100% Pass Your GPEN Exam with Exambible Prep Materials

https://www.exambible.com/GPEN-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/