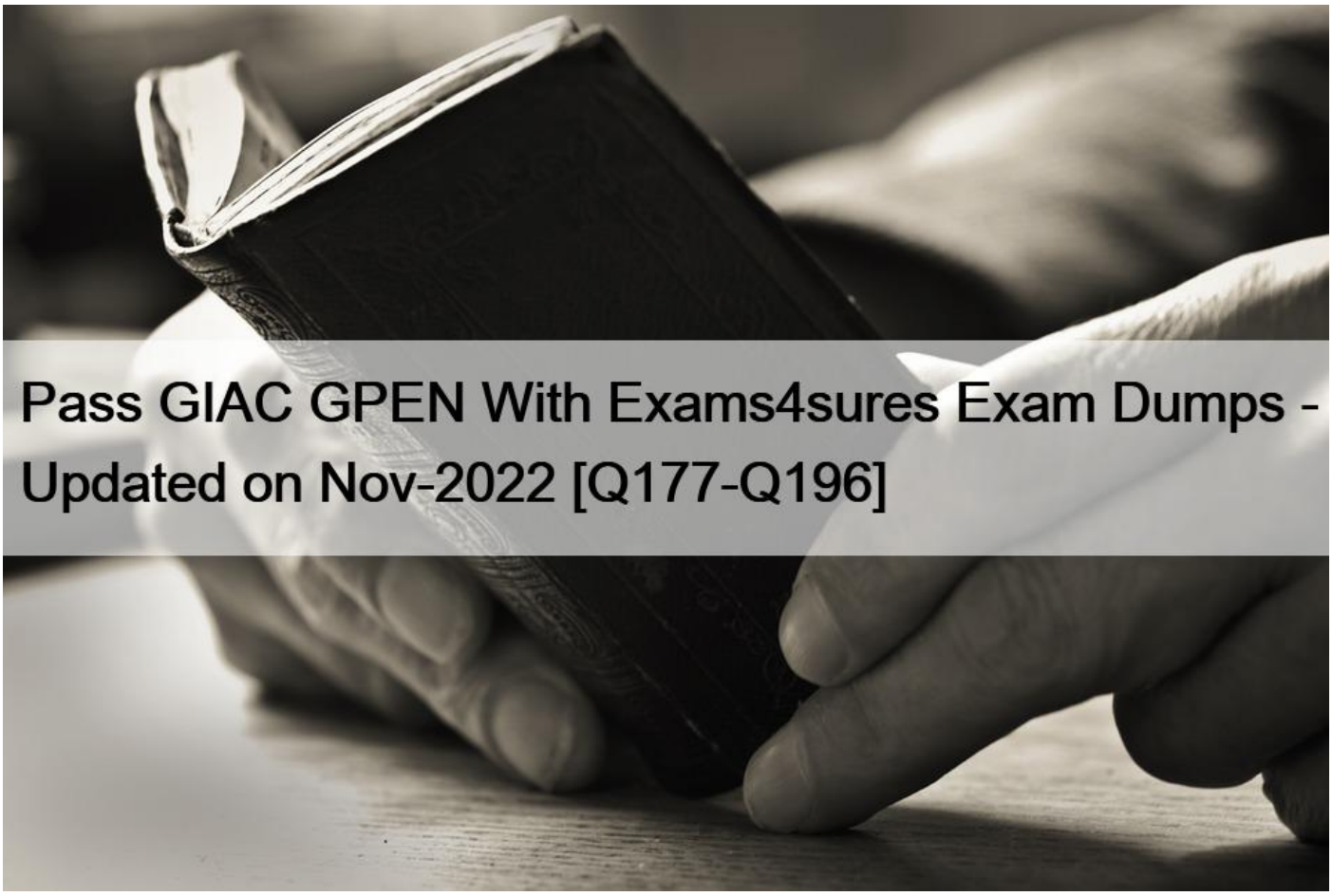
Pass GIAC GPEN With Exams4sures Exam Dumps - Updated on Nov-2022 [Q177-Q196



Pass GIAC GPEN With Exams4sures Exam Dumps - Updated on Nov-2022
Fully Updated GPEN Dumps - 100% Same Q&A In Your Real Exam

GIAC GPEN Exam Certification Details:

Exam CodeGPENPassing Score75%Schedule ExamPearson VUESample QuestionsGIAC GPEN Sample QuestionsExam NameGIAC Penetration Tester (GPEN)Number of Questions82-115

How to book GPEN Exams

In order to apply for the GPEN, You have to follow these steps
Go to the GPEN Official Site- Read the instruction Carefully- Follow the given steps- Apply for the GPEN **NO.177** 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?
* Run all known sendmail exploits against the server and see if you can compromisethe service, even if it crashed the machine or service
* 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
* Run all sendmail exploits that will not crash the server and see if you cancompromise the service
* 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
Section: Volume A

Explanation

NO.178 How does OWASP ZAP function when used for performing web application assessments?
* It is a non-transparent proxy that sits between your web browser and the targetapplication.
* It is a transparent policy proxy that sits between Java servers and |SP web pages.
* It is a non-transparent proxy that passively sniffs network traffic for HTTPvulnerabilities.
* It is a transparent proxy that sits between a target application and the backenddatabase.

NO.179 Which of the following techniques are NOT used to perform active OS fingerprinting?

Each correct answer represents a complete solution. Choose all that apply.
* Analyzing email headers
* Sniffing and analyzing packets
* ICMP error message quoting
* Sending FIN packets to open ports on the remote system
Section: Volume C

NO.180 While performing an assessment on a banking site, you discover the following link:

hnps://mybank.com/xfer.aspMer_toMaccount_number]&amount-[dollars]

Assuming authenticated banking users can be lured to your web site, which crafted html tag may be used to launch a XSRF attack?
* <imgsrc-“java script alert (‘document cookie’):”>
* <scripi>alert(‘hnps:/’mybank.com/xfer.a$p?xfer_io-[attacker_account]&amoutn-[dollars]’)</script>
* <scripr>document.write(‘hTtp$://mybankxom/xfer.a$p?xfer_to-[attacker.accountl

& amount-[dollars)</script>
* <img src-‘https/mybank.com/xfer.asp?xfer_to=[artacker_account]&amount= [dollars]”>

NO.181 Given the following Scapy information, how is default Layer 2 information derived?

```
>>> packet=Ether()/IP(src="10.10.10.9",dst="10.10.10.10")/TCP(dport=80)/"GET / HTTP/1.1"
>>> packet.summary
<bound method="" ether.summary="" of="" type="0x800" frag="0" proto="tcp" src="10.10.10.9"
dst="10.10.10.10" dport="http" load="GET / HTTP/1.1">>>>> </bound>
```

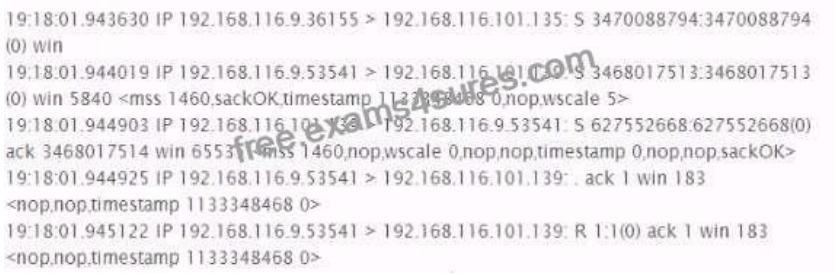

* The default layer 2 information is contained in a local scapy.cfg configuration fileon the local system.
* If not explicitly defined, the Ether type field value Is created using the hex value ofthe destination port, in this case 80
* If not explicitly defined, pseudo-random values are generated for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

NO.182 Which of the following is NOT a valid DNS zone type?

* Stub zone
* Secondary zone
* AlterNet zone
* Primary zone

Section: Volume D

NO.183 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?



* Port 135 is filtered, port 139 is open.
* Pons 135 and 139 are filtered.
* Ports 139 and 135 are open.
* Port 139 is closed, port 135 is open

Section: Volume A

NO.184 What concept do Rainbow Tables use to speed up password cracking?

* Fast Lookup Crack Tables
* Memory Swap Trades
* Disk Recall Cracking
* Time-Memory Trade-off

Explanation/Reference:

Reference:

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

NO.185 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?

* intitle:index.of inbox dbx
* intext:”outlook.asp”
* allinurl:”exchange/logon.asp”
* intitle:”Index Of” -inurl:maillog maillog size

NO.186 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?

* www.whois.net
* www.arin.nei

* www.apnic.net
* www.ripe.net

Section: Volume B

NO.187 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 _____.

* 0xAAD3B435B51404EE
* 0xBBD3B435B51504FF
* 0xBBC3C435C51504EF
* 0xAAD3B435B51404FF

NO.188 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?

* Enable the “Skip all primers” option and re-scan
* Ensure Safe Checks is enabled in Nessus scan policies
* Remove primer IP addresses from your target list
* Verify primers are in scope and tell the client In progress scans cannot be stopped

Section: Volume A

NO.189 Which of the following is the second half of the LAN manager Hash?

* 0xAAD3B435B51404BB
* 0xAAD3B435B51404CC
* 0xAAD3B435B51404EE
* 0xAAD3B435B51404AA

Section: Volume D

NO.190 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?

* Updating Nikto.
* Seting Nikto for network sniffing.
* Port scanning.
* Using it as a proxy server.

Section: Volume C

NO.191 Which of the following statements are true about MS-CHAPv2?

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

* It is a connectionless protocol.
* It can be replaced with EAP-TLS as the authentication mechanism for PPTP.
* It provides an authenticator-controlled password change mechanism.
* It is subject to offline dictionary attacks.

NO.192 Analyze the command output below, what action is being performed by the tester?

* Displaying a Windows SAM database
* Listing available workgroup services
* Discovering valid user accounts
* Querying locked out user accounts

Section: Volume A

NO.193 Which of the following is a tool for SSH and SSL MITM attacks?

* Ettercap
* Cain
* Dsniff
* AirJack

NO.194 A client has asked for a vulnerability scan on an internal network that does not have internet access. The rules of engagement prohibits any outside connection for the Nessus scanning machine. The customer has asked you to scan for a new critical vulnerability, which was released after the testing started, winch of the following methods of updating the Nessus plugins does not violate the rules of engagement?

* Connect the scanning machine via wireless bridge and download the updateddirectly
* Change the routing and connect through an alternative gateway
* Proceed with the test and note the limitation of updating the plugins
* Download the updates on an alternative machine and manually load on scanningmachine

Section: Volume A

NO.195 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?

* AirSnort
* PsPasswd
* Cain
* Kismet

NO.196 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.
* It is supported by all manufacturers of wireless LAN hardware and software.
* It uses a public key certificate for server authentication.
* It uses password hash for client authentication.
* It provides a moderate level of security.

Section: Volume C

GPEN Test Structure

The GIAC GPEN certification exam includes 82 to 115 questions. The vendor doesn't give details on how the questions are structured. Thus, the applicants should be ready to solve variously-formatted inquiries. As for the time limit, the candidates will have 3 hours to answer a minimum of 75% of all questions. Also, this is a proctored exam. So, the test-takers will need to follow some rules before they can take it. In particular, they need to send an application to the vendor's site and wait for the evaluation team to check it. Once you get their reply, if you are accepted, you can proceed to pay the registration fee and take the final exam. Its value is $1,999.

Latest GPEN Exam Dumps - Valid and Updated Dumps:
https://www.exams4sures.com/GIAC/GPEN-practice-exam-dumps.html]