Reliable GPEN Dumps Questions Available as Web-Based Practice Test Engine [Q79-Q102

Reliable GPEN Dumps Questions Available as Web-Based Practice Test Engine
Correct and Up-to-date GIAC GPEN BrainDumps

To sit for the GPEN exam, candidates must have a minimum of two years of work experience in the field of information security or an equivalent degree. GPEN exam is open to security professionals such as security consultants, network engineers, security architects, and system administrators, among others. Aspiring candidates must also possess a sound knowledge of TCP/IP networking, Linux, and Windows operating systems, and be proficient in using various penetration testing tools like Nmap, Metasploit, Burp Suite, and Wireshark.

NO.79 John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

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

Which of the following tools is John using to crack the wireless encryption keys?
* Kismet
* AirSnort
* Cain
* PsPasswd

NO.80 All of the following are advantages of using the Metasploitpriv module for dumping hashes from a local Windows machine EXCEPT:
* Doesn’t require SMB or NetBIOS access to the target machine
* Can run inside of a process owned by any user
* Provides less evidence for forensics Investigators to recover
* LSASS related reboot problems aren’t an Issue

Reference:

http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/201

2 _Jan_ISOAG.pdf

NO.81 A penetration tester obtains telnet access to a target machine using a captured credential. While trying to transfer her exploit to the target machine, the network intrusion detection systems keeps detecting her exploit and terminating her connection. Which of the following actions will help the penetration tester transfer an exploit and compile it in the target system?
* Use the http service’s PUT command to push the file onto the target machine.
* Use the scp service, protocol SSHv2 to pull the file onto the target machine.
* Use the telnet service’s ECHO option to pull the file onto the target machine
* Use the ftp service in passive mode to push the file onto the target machine.

NO.82 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.
* Public key certificate for server authentication
* Password hash for client authentication
* Strongest security level
* Dynamic key encryption

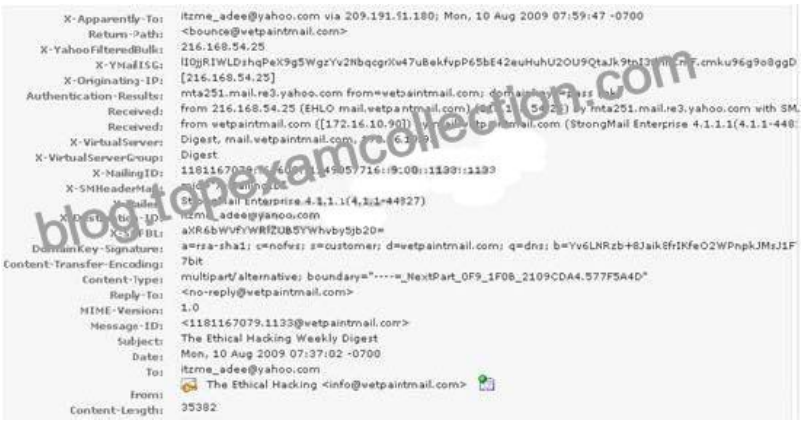
NO.83 You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. Rick, your assistant, is configuring some laptops for wireless access. For security, WEP needs to be configured for wireless communication. By mistake, Rick configures different WEP keys in a laptop than that is configured on the Wireless Access Point (WAP). Which of the following statements is true in such situation?
* The laptop will be able to access the wireless network but the security will be compromised
* The WAP will allow the connection with the guest account’s privileges.
* The laptop will be able to access the wireless network but other wireless devices will be unable to communicate with it.
* The laptop will not be able to access the wireless network.

Section: Volume B

NO.84 You want that some of your Web pages should not be crawled. Which one of the following options will you use to accomplish the task?
* Use HTML NO Crawl tag in the Web page not to be crawled

* Place the name of restricted Web pages in the private.txt file
* Place the name of restricted Web pages in the robotes.txt file
* Enable the SSL

NO.85 You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below: What is the IP address of the sender of this email?



* 172.16.10.90
* 209.191.91.180
* 141.1.1.1
* 216.168.54.25

NO.86 Which of the following ports must you filter to check null sessions on your network?
* 139 and 445
* 111 and 222
* 1234 and 300
* 130 and 200

Section: Volume C

NO.87 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.
land

NO.88 Which of the following statements about Fport is true?
* It works as a process viewer.
* It works as a datapipe on Windows.
* It works as a datapipe on Linux.
* It is a source port forwarder/redirector.

NO.89 CORRECT TEXT

Fill in the blanks with the appropriate protocol.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE___ encryption protocol created to replace both TKIP and WEP.
802.11i

NO.90 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 tins is happening?

* Netcat cannot properly interpret certain control characters or Unicode sequences.
* The listener executed command.com instead of cmd.exe.
* Another application is already running on the port Netcat is listening on.
* TheNetcat listener is running with system level privileges.

Section: Volume A

NO.91 Which of the following methods can be used to detect session hijacking attack?
* ntop
* Brutus
* nmap
* sniffer

Section: Volume C

NO.92 Which of the following is the correct sequence of packets to perform the 3-way handshake method?
* SYN, ACK, ACK
* SYN, ACK, SYN/ACK
* SYN, SYN/ACK, ACK
* SYN, SYN, ACK

NO.93 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?
* Configuration of VPN access
* Setting up of monitoring on ISA Server
* Defining ISA Server network configuration

* Defining how ISA Server would cache Web contents

NO.94 Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails.

Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?
* /log/var/logd
* /var/log/logmail
* /log/var/mailog
* /var/log/mailog

NO.95 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?
* IEEE 802.1X using EAP-TLS
* IEEE 802.1X using PEAP-MS-CHAP
* Pre-shared key
* Open system

NO.96 You work as a Web developer in the IBM Inc. Your area of proficiency is PHP. Since you have proper knowledge of security, you have bewared from rainbow attack. For mitigating this attack, you design the PHP code based on the following algorithm:

key = hash(password + salt)

for 1 to 65000 do

key = hash(key + salt)

Which of the following techniques are you implementing in the above algorithm?
* Key strengthening
* Hashing
* Sniffing
* Salting

NO.97 Which of the following functions can you use to mitigate a command injection attack?

Each correct answer represents a complete solution. Choose all that apply.
* htmlentities()
* strip_tags()
* escapeshellarg()
* escapeshellcmd()

NO.98 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.
* Attacker can use the Ping Flood DoS attack if WZC is used.

* Attacker by creating a fake wireless network with high power antenna cause Victor’s computer to associate with his network to gain access.
* Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
* It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

NO.99 You have inserted a Trojan on your friend’s computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?
* HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionStart
* HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionAuto
* HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionStartup
* HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunServices

NO.100 Which of the following statements is true about the Digest Authentication scheme?
* In this authentication scheme, the username and password are passed with every request, not just when the user first types them.
* A valid response from the client contains a checksum of the username, the password, the given random value, the HTTP method, and the requested URL.
* The password is sent over the network in clear text format.
* It uses the base64 encoding encryption scheme.

NO.101 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?
* The byte length is different on the two machines
* End of-line characters are different on the two machines
* The file must have become corrupt during transfer
* ASCII character sets are different on the two machines
Section: Volume A

NO.102 You’ve been contracted by the owner of a secure facility to try and break into their office in the middle of the night. Your client requested photographs of any sensitive information found as proof of your accomplishments.

The job you’ve been hired to perform is an example of what practice?
* Penetration Testing
* Ethical Hacking
* Vulnerability Assessing
* Security Auditing
Section: Volume A

The GPEN exam is designed to test the candidate's knowledge of blue and red team methodologies, attack vectors, and exploitation techniques. It covers a wide range of topics, including password attacks, web application attacks, wireless attacks, network mapping

and reconnaissance, and malware analysis. GPEN exam is also hands-on, requiring the candidate to demonstrate their ability to apply their knowledge to real-world scenarios through practical exercises.

100% Reliable Microsoft GPEN Exam Dumps Test Pdf Exam Material:
https://www.topexamcollection.com/GPEN-vce-collection.html]