CertBus.com

CERTBUS

# GPEN Q&As

## GIAC Certified Penetration Tester

**Pass** GIAC GPEN **Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**http://www.CertBus.com/GPEN.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **80000+** Satisfied Customers

**Vendor:** GIAC

**Exam Code:** GPEN

**Exam Name:** GIAC Certified Penetration Tester

**Q&As:** Demo

**QUESTION 1**
Which of the following commands can be used for port scanning?

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

**Correct Answer:** A

**QUESTION 2**
Which of the following tools allows you to download World Wide Web sites from the Internet to a local computer?

A. Netcraft
B. HTTrack
C. Netstat
D. Cheops-ng

**Correct Answer:** B

**QUESTION 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 SSID.
B. Changing keys often.
C. Using the longest key supported by hardware.
D. Using a non-obvious key.

**Correct Answer:** BCD

**QUESTION 4**
Adam is a novice Internet user. He is using Google search engine to search documents of his interest.

Adam wants to search the text present in the link of a Website.

Which of the following operators will he use in his query to accomplish the task?

A. inanchor
B. info
C. link
D. site

**Correct Answer:** A

**QUESTION 5**
You want to retrieve the default security report of nessus.

Which of the following google search queries will you use?

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

**Correct Answer:** C

**QUESTION 6**
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 Nikto.
B. Seting Nikto for network sniffing.
C. Port scanning.
D. Using it as a proxy server.

**Correct Answer:** C

**QUESTION 7**
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the preattack phase successfully:

Information gathering
Determination of network range
Identification of active systems
Location of open ports and applications

Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.
B. Map the network of We-are-secure Inc.
C. Fingerprint the services running on the we-are-secure network.
D. Install a backdoor to log in remotely on the We-are-secure server.

**Correct Answer:** A

**QUESTION 8**
Which of the following statements are true about session hijacking? Each correct answer represents a complete solution. Choose all that apply.

A. TCP session hijacking is when a hacker takes over a TCP session between two machines.
B. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
C. Use of a long random number or string as the session key reduces session hijacking.
D. It is used to slow the working of victim's network resources.

**Correct Answer:** ABC

**QUESTION 9**
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 though 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

**Correct Answer:** B

**QUESTION 10**
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

**Correct Answer:** ABC

**QUESTION 11**
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

**Correct Answer:** C

**QUESTION 12**
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

**Correct Answer:** B

**QUESTION 13**
Which of the following password cracking tools can work on the Unix and Linux environment?

A. Brutus
B. Cain and Abel
C. Ophcrack
D. John the Ripper

**Correct Answer:** D

**QUESTION 14**
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 names.

C. Upgrade SNMP Version 1 with the latest version.
D. Install antivirus.

**Correct Answer:** BC

**QUESTION 15**
Which of the following tools can be used to enumerate networks that have blocked ICMP Echo packets, however, failed to block timestamp or information packet or not performing sniffing of trusted addresses, and it also supports spoofing and promiscuous listening for reply packets?

A. Nmap
B. Zenmap
C. Icmpenum
D. Nessus

**Correct Answer:** C

**QUESTION 16**
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 names.
C. Upgrade SNMP Version 1 with the latest version.
D. Install antivirus.

**Correct Answer:** BC

**QUESTION 17**
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

**Correct Answer:** BCD

**QUESTION 18**
You work as a Network Administrator in the Secure Inc. Your company is facing various network attacks due to the insecure wireless network. You are assigned a task to secure your wireless network. For this, you have turned off broadcasting of the SSID. However, the unauthorized users are still able to connect to the wireless network.

Which of the following statements can be the reason for this issue? Each correct answer represents a complete solution. Choose all that apply.

A. You have forgotten to turn off DHCP.
B. You are using WPA2 security scheme.
C. The SSID is still sent inside both client and AP packets.
D. You are using the default SSID.

**Correct Answer:** ACD

**QUESTION 19**
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

**Correct Answer:** A

**QUESTION 20**
Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Stalking Amendment Act (1999)
B. Malicious Communications Act (1998)
C. Anti-Cyber-Stalking law (1999)
D. Stalking by Electronic Communications Act (2001)

**Correct Answer:** A

**QUESTION 21**
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

**Correct Answer:** C

**QUESTION 22**
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

**Correct Answer:** D

**QUESTION 23**

Which of the following are the drawbacks of the NTLM Web authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

A. It can be brute forced easily.
B. It works only with Microsoft Internet Explorer.
C. The password is sent in clear text format to the Web server.
D. The password is sent in hashed format to the Web server.

**Correct Answer:** AB

**QUESTION 24**
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 overloaded.
B. John's computer is behind a firewall that blocks incoming ICMP error messages.
C. There is no route to the we-are-secure server.
D. The we-are-secure server is down and is not connected to the Internet.

**Correct Answer:** ABCD

**QUESTION 25**
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 telnet session is being affected by the stateful inspection firewall.
B. The telnet service of we-are-secure.com has corrupted.
C. The we-are-secure.com server is using a TCP wrapper.
D. The we-are-secure.com server is using honeypot.

**Correct Answer:** C

**QUESTION 26**
Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access.

Which of the following addresses is a valid MAC address?

A. A3-07-B9-E3-BC-F9
B. F936.28A1.5BCD.DEFA
C. 1011-0011-1010-1110-1100-0001
D. 132.298.1.23

**Correct Answer:** A

**QUESTION 27**
You want to search the Apache Web server having version 2.0 using google hacking.

Which of the following search queries will you use?

A. intitle:Sample.page.for.Apache Apache.Hook.Function
B. intitle:"Test Page for Apache Installation" "It worked!"
C. intitle:test.page "Hey, it worked !" "SSl/TLS aware"
D. intitle:"Test Page for Apache Installation" "You are free"

**Correct Answer:** A

**QUESTION 28**
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 time.
B. It will show an error in the scanning process.
C. It may show smurf DoS attack in the network IDS of the victim.
D. Scanning of the broadcast IP address cannot be performed.

**Correct Answer:** AC

**QUESTION 29**
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-aresecure 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.

**Correct Answer:** BD

**QUESTION 30**
Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends 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 Spam
B. E-mail Storm
C. E-mail spoofing
D. E-mail bombing

**Correct Answer:** A

**QUESTION 31**
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 software.
B. It uses a public key certificate for server authentication.
C. It uses password hash for client authentication.
D. It provides a moderate level of security.

**Correct Answer:** AB

**QUESTION 32**
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

**Correct Answer:** A

**QUESTION 33**
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 laptop.
B. Do nothing.
C. Traverse to all of your drives, search new.com files, and delete them.
D. Clean up your laptop with antivirus.

**Correct Answer:** B

**QUESTION 34**
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 software.
B. It uses a public key certificate for server authentication.
C. It uses password hash for client authentication.
D. It provides a moderate level of security.

**Correct Answer:** AB

**QUESTION 35**
Which of the following statements are true about session hijacking? Each correct answer represents a complete solution. Choose all that apply.

A. It is used to slow the working of victim's network resources.

B. TCP session hijacking is when a hacker takes over a TCP session between two machines.
C. Use of a long random number or string as the session key reduces session hijacking.
D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

**Correct Answer:** BCD

**QUESTION 36**
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 the longest key supported by hardware.
B. Using a non-obvious key.
C. Using a 16 bit SSID.
D. Changing keys often.

**Correct Answer:** ABD

**QUESTION 37**
Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

A. Artistic license
B. Spam
C. Patent
D. Phishing

**Correct Answer:** C

**QUESTION 38**
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. Dictionary attack
B. Rule based attack
C. Hybrid attack
D. Brute Force attack

**Correct Answer:** ACD

**QUESTION 39**
Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively.

Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. MINIX 3
B. Linux
C. Windows XP
D. Mac OS

**Correct Answer:** D

**QUESTION 40**

Which of the following tools allows you to download World Wide Web sites from the Internet to a local computer?

A. Netstat
B. Netcraft
C. HTTrack
D. Cheops-ng

**Correct Answer:** C

**QUESTION 41**
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 fields.
B. The we-are-secure server cannot handle the overlapping data fragments.
C. The ICMP packet is larger than 65,536 bytes.
D. Ping requests at the server are too high.

**Correct Answer:** B

**QUESTION 42**
Which of the following is a tool for SSH and SSL MITM attacks?

A. Ettercap
B. Cain
C. Dsniff
D. AirJack

**Correct Answer:** C

**QUESTION 43**
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

**Correct Answer:** C

**QUESTION 44**
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

**Correct Answer:** C

**QUESTION 45**
Which of the following is the most common method for an attacker to spoof email?

A. Back door
B. Replay attack
C. Man in the middle attack
D. Open relay

**Correct Answer:** D

**QUESTION 46**
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 fields.
B. The we-are-secure server cannot handle the overlapping data fragments.
C. The ICMP packet is larger than 65,536 bytes.
D. Ping requests at the server are too high.

**Correct Answer:** B

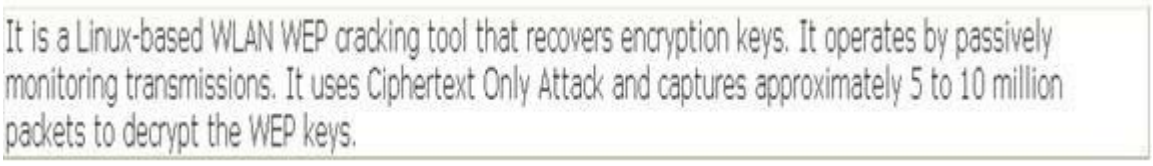
**QUESTION 47**
Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature.

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.

**Correct Answer:** A

**QUESTION 48**
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. Kismet
B. AirSnort
C. Cain
D. PsPasswd

**Correct Answer:** B

**QUESTION 49**
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

**Correct Answer:** B

**QUESTION 50**
Which of the following is NOT an example of passive footprinting?

A. Scanning ports.
B. Analyzing job requirements.
C. Querying the search engine.
D. Performing the whois query.

**Correct Answer:** A

# Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

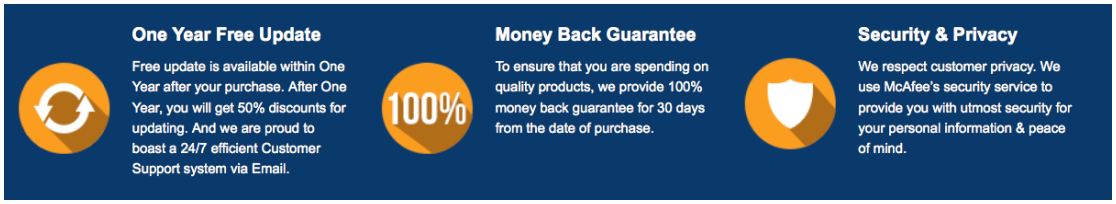
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:


**Guarantee & Policy | Privacy & Policy | Terms & Conditions**