GIAC Penetration Tester

GIAC GPEN

Version Demo

Total Demo Questions: 15

Total Premium Questions: 385

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	99
Topic 2, Volume B	97
Topic 3, Volume C	98
Topic 4, Volume D	91
Total	385

QUESTION NO: 1

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.

ANSWER: A B

QUESTION NO: 2

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)

ANSWER: A

QUESTION NO: 3

Which of the following can be used to mitigate the evil twin phishing attack?

A. Magic Lantern

B. Obiwan

C. IPSec VPN

D. SARA

ANSWER: C

QUESTION NO: 4

Which of the following federal laws are related to hacking activities?

Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030

B. 18 U.S.C. 1028

C. 18 U.S.2510

D. 18 U.S.C. 1029

ANSWER: A C D

QUESTION NO: 5

Which of the following statements are true about NTLMv1?

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

A. It uses the LANMAN hash of the user's password.

B. It is mostly used when no Active Directory domain exists.

C. It is a challenge-response authentication protocol.

D. It uses the MD5 hash of the user's password.

ANSWER: A B C

QUESTION NO: 6

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.

ANSWER: B D

QUESTION NO: 7

You configure a wireless router at your home. To secure your home Wireless LAN (WLAN), you implement WEP. Now you want to connect your client computer to the WLAN. Which of the following is the required information that you will need to configure the client computer?

Each correct answer represents a part of the solution. Choose two.

A. WEP key

B. MAC address of the router

C. IP address of the router

D. SSID of the WLAN

ANSWER: A D

QUESTION NO: 8

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

A. IEEE 802.11b

B. IEEE 802.5

C. IEEE 802.3

D. IEEE 802.4

ANSWER: A

QUESTION NO: 9

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: B C D

QUESTION NO: 10

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?

A. intitle:index.of inbox dbx

B. intext:"outlook.asp"

C. allinurl:"exchange/logon.asp"

D. intitle:"Index Of" -inurl:maillog maillog size

ANSWER: C

QUESTION NO: 11

If the privacy bit is set in the 802.11 header, what does it indicate?

A. SSID cloaking is being used.

B. Some form of encryption is In use.

C. WAP is being used.

D. Some form of PEAP is being used.

ANSWER: C

QUESTION NO: 12

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

ANSWER: D

QUESTION NO: 13

You are using the Nmap Scripting Engine and want detailed output of the script as it runs. Which option do you include in the command string?

A. Nmap --script-output -script-SSH-hostkey.nse 155.65.3.221 -p 22

B. Nmap --script-trace --script-ssh-hostkey.nse 155.65.3.221 -p 22

C. Nmap -script-verbose --scrlpr-ssh-hostkey.nse 155.65.3.221 -p 22

D. Nmap -v --script=ssh-hostkey.nse 155.65.3.221 -p 22

ANSWER: C

QUESTION NO: 14

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.

ANSWER: A B D

QUESTION NO: 15

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