Free Questions for GPEN by ebraindumps

Shared by Wallace on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

A- Dictionary attack

B- Rule based attack

C- Hybrid attack

D- Brute Force attack

Answer:

A, C, D

Question 2

Question Type: MultipleChoice

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

Options:

A- Artistic license

B- Spam

C- Patent

D- Phishing

Answer:

C

Question 3

Question Type: MultipleChoice

Which of the following statements are true about session hijacking?

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

Options:

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.

Answer:

B, C, D

Question 4

Question Type: MultipleChoice

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.

Options:

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 5

Question Type: MultipleChoice

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?

Options:

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.

Answer:

B

Question 6

Question Type: **MultipleChoice**

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?

Options:

A- nmap -O -p

B- nmap -sS

C- nmap -sU -p

D- nmap --sT

Answer:

A

Question 7

Question Type: **MultipleChoice**

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?

Options:

A- E-mail Spam

B- E-mail Storm

C- E-mail spoofing

D- E-mail bombing

Answer:

A

Question 8

Question Type: **MultipleChoice**

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.

Options:

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 9

Question Type: MultipleChoice

What happens when you scan a broadcast IP address of a network?

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

Options:

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.

Answer:

A, C