312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

QUESTION 1

What type of cookies can be generated while visiting different web sites on the Internet?

A. Permanent and long term cookies.

B. Session and permanent cookies.

C. Session and external cookies.

D. Cookies are all the same, there is no such thing as different type of cookies.

Correct Answer: B

There are two types of cookies: a permanent cookie that remains on a visitor\\'s computer for a given time and a session cookie the is temporarily saved in the visitor\\'s computer memory during the time that the visitor is using the Web site. Session cookies disappear when you close your Web browser.

QUESTION 2

What will the following command produce on a website\\'s login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email = \\'someone@somewhere.com\\'; DROP TABLE members; --\\'

A. This code will insert the someone@somewhere.com email address into the members table.

B. This command will delete the entire members table.

C. It retrieves the password for the first user in the members table.

D. This command will not produce anything since the syntax is incorrect.

Correct Answer: B

QUESTION 3

Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

A. Spoof Attack

B. Smurf Attack

C. Man in the Middle Attack

D. Trojan Horse Attack

E. Back Orifice Attack

Correct Answer: DE

To compromise the data, the attack would need to be executed before the encryption takes place at either end of the tunnel. Trojan Horse and Back Orifice attacks both allow for potential data manipulation on host computers. In both cases, the data would be compromised either before encryption or after decryption, so IPsec is not preventing the attack.

QUESTION 4

On wireless networks, SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless networks?

A. The SSID is only 32 bits in length.

B. The SSID is transmitted in clear text.

C. The SSID is the same as the MAC address for all vendors.

D. The SSID is to identify a station, not a network.

Correct Answer: B

The SSID IS constructed to identify a network, it IS NOT the same as the MAC address and SSID\\'s consists of a maximum of 32 alphanumeric characters.

QUESTION 5

Why would an ethical hacker use the technique of firewalking?

A. It is a technique used to discover wireless network on foot.

B. It is a technique used to map routers on a network link.

C. It is a technique used to discover the nature of rules configured on a gateway.

D. It is a technique used to discover interfaces in promiscuous mode.

Correct Answer: C

Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker\\'s host to a destination host through a packet-filtering device. This technique can be used to map `open\\' or `pass through\\' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.