TestpassportQ&A

Bessere Qualität , bessere Dienstleistungen!

We offer free update service for one year

Http://www.testpassport.ch

Exam : **CEH-001**

Title : Certified Ethical Hacker (CEH)

Version : DEMO

1.Consider the following code:
URL: http://www.certified.com/search.pl?
text=<script>alert(document.cookie)</script>
If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.
What is the countermeasure against XSS scripting?
A. Create an IP access list and restrict connections based on port number
B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts
C. Disable Javascript in IE and Firefox browsers
D. Connect to the server using HTTPS protocol instead of HTTP
Answer: B

2.Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network.
How can she accomplish this?
A. Jayden can use the commanD. ip binding set.
B. Jayden can use the commanD. no ip spoofing.
C. She should use the commanD. no dhcp spoofing.
D. She can use the commanD. ip dhcp snooping binding.
Answer: D

3.TCP SYN Flood attack uses the three-way handshake mechanism.
1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called _____
A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"
Answer: B

4.You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.
A. New installation of Windows should be patched by installing the latest service packs and hotfixes
B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed
C. Install a personal firewall and lock down unused ports from connecting to your computer

D. Install the latest signatures for Antivirus software
E. Configure "Windows Update" to automatic
F. Create a non-admin user with a complex password and logon to this account
G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.
Answer: A,C,D,E,F

5.What is the problem with this ASP script (login.asp)?

```
strsql = "SELECT * FROM Users where where Username='" + Login1.UserName
+ "' and Pass='" + password + "'
try
{
OleDbConnection con = new OleDbConnection(connectionstring);
con.Open();
OleDbCommand cmd = new OleDbCommand(strsql, con);
OleDbDataReader dr = cmd.ExecuteReader();
if (dr.HasRows)
{
If (dr.Read())
{
Session["username"] = Login1.UserName;
Response.Redirect("Mainpage.aspx", false);
else
{
Response.Redirect("Login.aspx", false);
}
}
}
dr.Dispose();
con.Close();
}
catch (Exception ex)
{
ClientScript.RegisterStartupScript(this.GetType(), "msg",
"<script>alert('" + ex.Message + "')</script>");
```

A. The ASP script is vulnerable to Cross Site Scripting attack
B. The ASP script is vulnerable to Session Splice attack
C. The ASP script is vulnerable to XSS attack
D. The ASP script is vulnerable to SQL Injection attack
Answer: D