Dumps Planet
Your Partner in Success

EC-Council

ECSAV10 EXAM

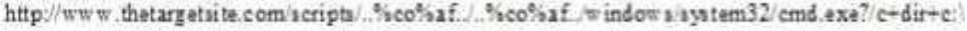
EC-Council Certified Security Analyst (ECSA) V10

Product: Demo File

For More Information:
https://www.dumpsplanet.com/ECSAV10-dumps

Question: 1

What will the following URL produce in an unpatched IIS Web Server?



http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of the C:\windows\system32 folder on the web server
D. Directory listing of C: drive on the web server

Answer: D

Question: 2

What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems
B. Man trap
C. Pick-resistant locks
D. Electronic combination locks

Answer: B

Question: 3

An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna
D. Directional Antenna

Answer: B

Question: 4

Software firewalls work at which layer of the OSI model?

A. Data Link
B. Network
C. Transport
D. Application

Answer: A

Question: 5

If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack

B. Sql injection attack
C. Session Hijacking
D. Cross-site request attack

Answer: D

Question: 6

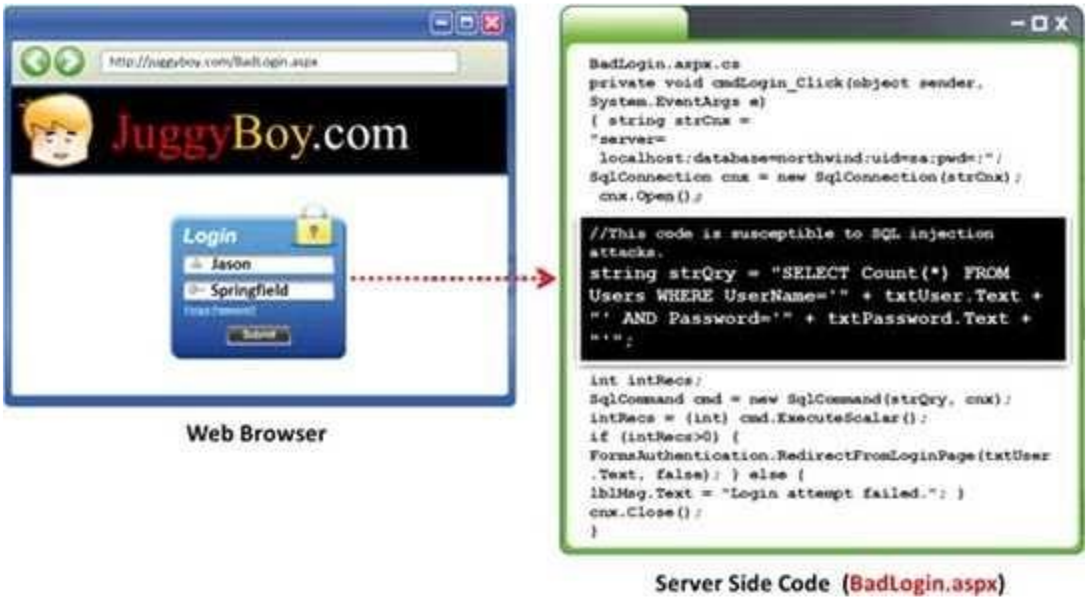
How many bits is Source Port Number in TCP Header packet?

A. 48
B. 32
C. 64
D. 16

Answer: D

Question: 7

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.


http://juggyboy.com/BadLogin.aspx
JuggyBoy.com
Login
Jason
Springfield
Web Browser
Server Side Code (BadLogin.aspx)

```
BadLogin.aspx.cs
private void cmdLogin_Click(object sender,
System.EventArgs e)
{ string strCnx =
"server=
 localhost;database=northwind;uid=sa;pwd=;";
SqlConnection cnx = new SqlConnection(strCnx);
 cnx.Open();
//This code is susceptible to SQL injection
attacks.
string strQry = "SELECT Count(*) FROM
Users WHERE UserName='" + txtUser.Text +
"' AND Password='" + txtPassword.Text +
"'";
int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx);
intRecs = (int) cmd.ExecuteScalar();
if (intRecs>0) {
FormsAuthentication.RedirectFromLoginPage(txtUser
.Text, false); } else {
lblMsg.Text = "Login attempt failed."; }
cnx.Close();
}
```

Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes. Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Answer: D

Question: 8

Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Answer: B

Question: 9

What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Answer: D

Question: 10

Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Answer: B

Question: 11

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Answer: C

Thank You for Trying Our Product