# ECSAV8$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA)

## Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.passapply.com/ecsav8.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

**QUESTION 1**

What information can be collected by dumpster diving?

A. Sensitive documents

B. Email messages

C. Customer contact information

D. All the above

Correct Answer: A

Reference: http://www.spamlaws.com/dumpster-diving.html

**QUESTION 2**

During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction

B. IPID State Number Prediction

C. TCP State Number Prediction

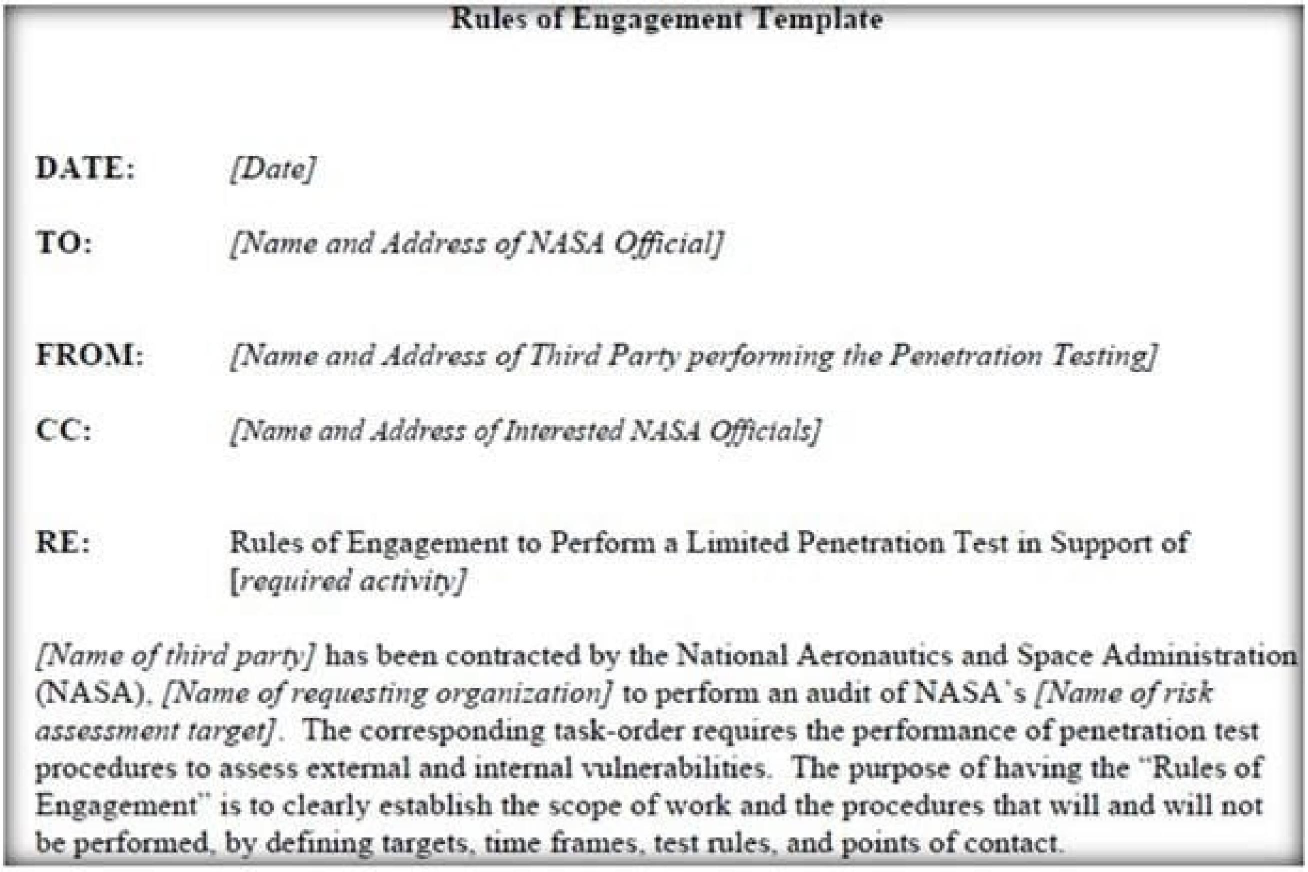
D. IPID Sequence Number Prediction

Correct Answer: A

Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration- Testing-NoRestriction (p.43)

**QUESTION 3**

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



**Rules of Engagement Template**

**DATE:** *[Date]*

**TO:** *[Name and Address of NASA Official]*

**FROM:** *[Name and Address of Third Party performing the Penetration Testing]*

**CC:** *[Name and Address of Interested NASA Officials]*

**RE:** Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

*[Name of third party]* has been contracted by the National Aeronautics and Space Administration (NASA). *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams

B. Decide the desired depth for penetration testing

C. Conduct a brainstorming session with top management and technical teams

D. Have pre-contract discussions with different pen-testers

Correct Answer: B

## QUESTION 4

Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts

B. References

C. Research

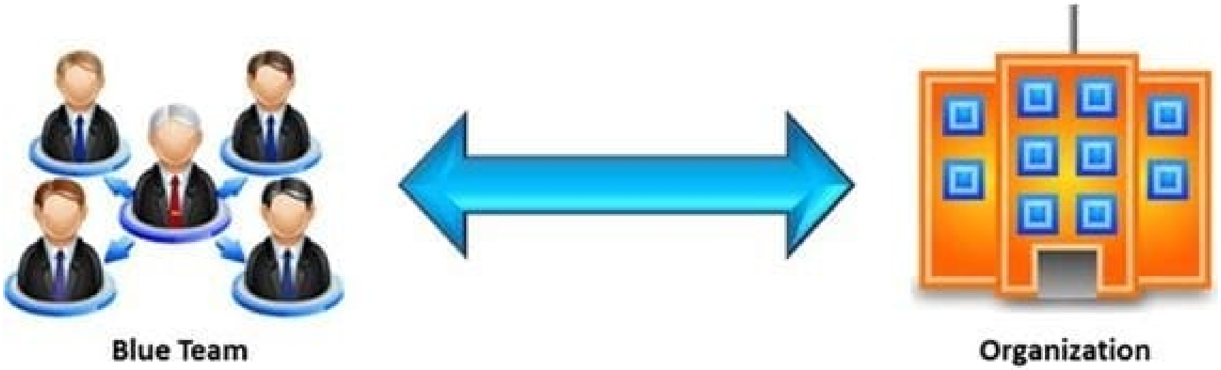
D. Glossary

Correct Answer: D

Explanation: Refere\\' http://en.wikipedia.org/wiki/Glossary

**QUESTION 5**

In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization\\'s IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization\\'s IT staff but with permission from upper management

Correct Answer: A

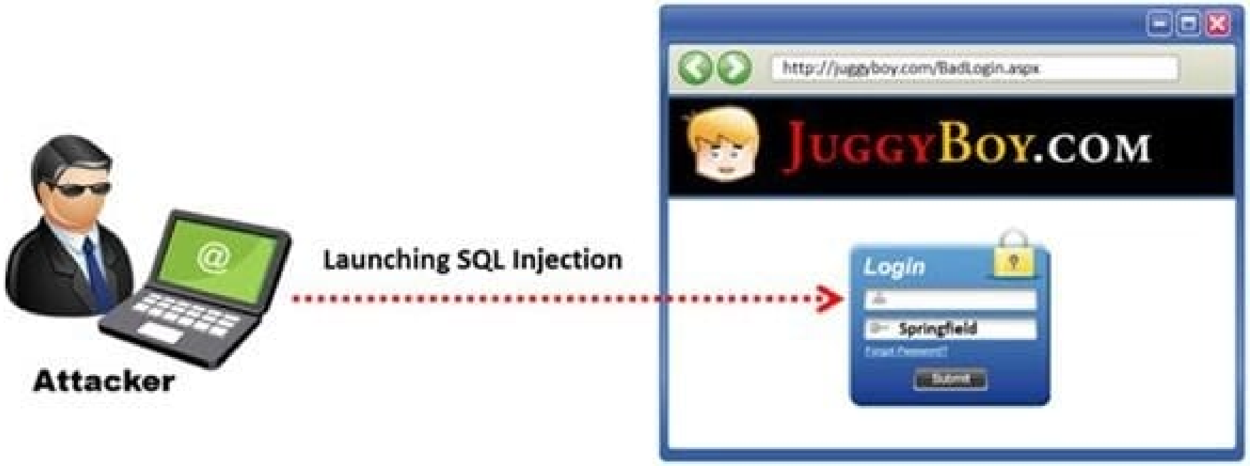
Reference: https://www.sypriselectronics.com/information-security/cyber-security- solutions/computernetwork-defense/

**QUESTION 6**

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.

This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back- end database.

The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah\\' "2=2 ?

B. Blah\\' and 2=2 -

C. Blah\\' and 1=1 -

D. Blah\\' or 1=1 -

Correct Answer: D

## QUESTION 7

By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry

B. Netstat

C. Telnet

D. Tracert

Correct Answer: A

Reference: http://support.microsoft.com/kb/832919

## QUESTION 8

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

A. Blue team

B. Tiger team

C. Gorilla team

D. Lion team

Correct Answer: B

**QUESTION 9**

In the example of a /etc/passwd file below, what does the bold letter string indicate?

nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid

B. Group number

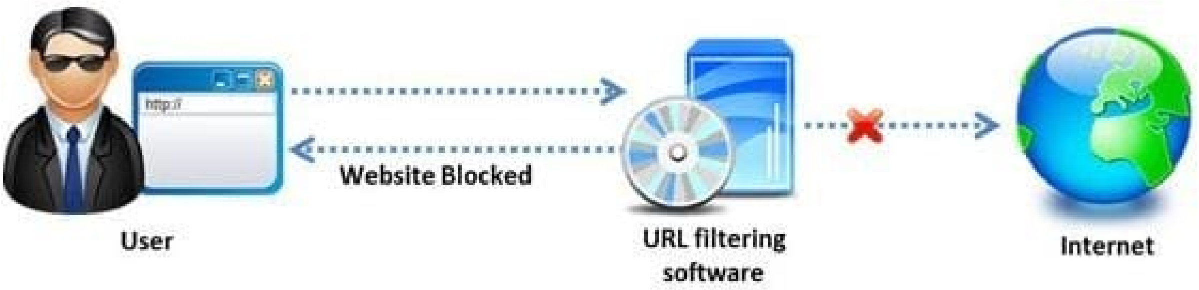
C. GECOS information

D. User number

Correct Answer: D

**QUESTION 10**

Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking

B. Using proxy servers

C. Using authentication

D. Using encryption

Correct Answer: B

QUESTION 11

What is the maximum value of a "tinyint" field in most database systems?

A. 222

B. 224 or more

C. 240 or less

D. 225 or more

Correct Answer: D

Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJandpg=SA3-PA3andlpg=SA3PA3anddq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+databa se +systemsandsource=blandots=NscGk-R5randsig=1hMOYByxt7ebRJ4UEjbpxMijTQsandhl=enandsa=Xandei=pvgeVJnTCNDkaI_fgugOandved=0CDYQ6AEwAw#v=onepageandq=maximum%20value%20of%20a%20%E2%80%9Ctin yint%E2%80%9D%20field%20in%20most%20database%20systemsandf=false

QUESTION 12

Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businessService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

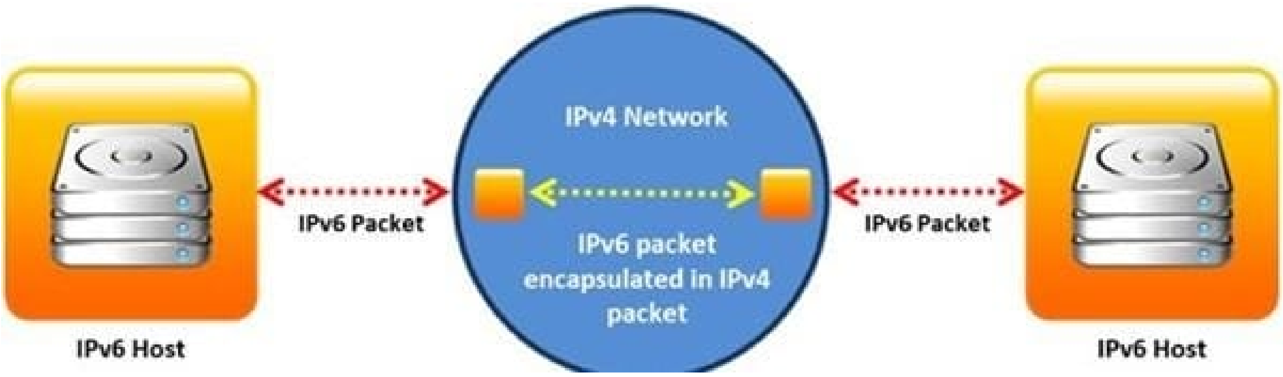
D. Inside Attacks

Correct Answer: A

Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web- Applications-pdf (page 99)

**QUESTION 13**

Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation

B. Tunneling

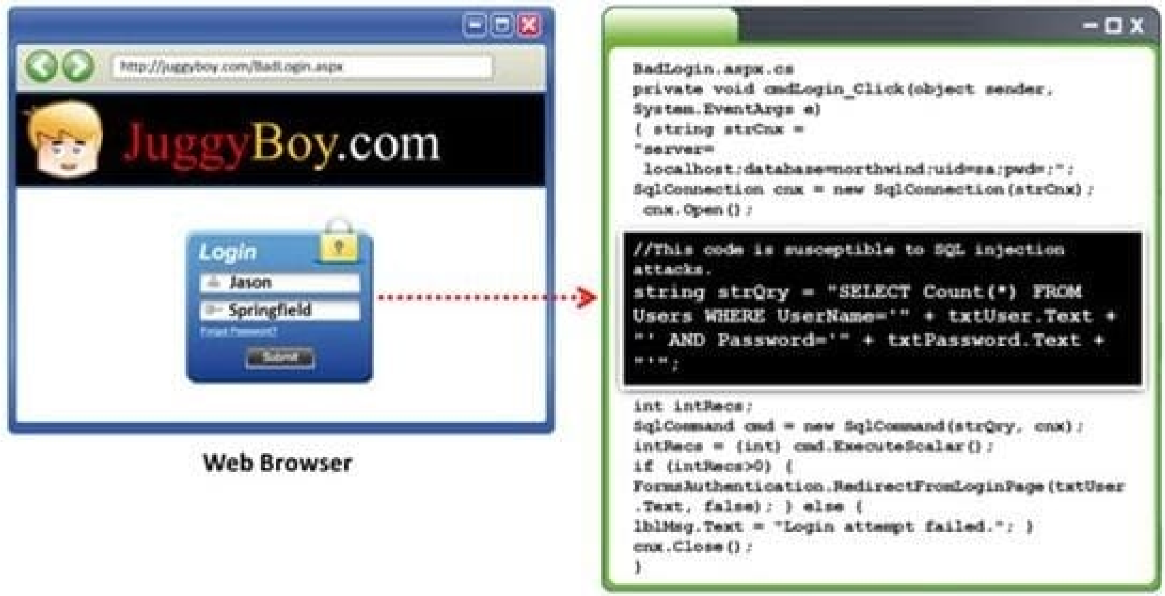
C. Dual Stacks

D. Encapsulation

Correct Answer: D

**QUESTION 14**

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.



```
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();
}
```

Web Browser

Server Side Code (BadLogin.aspx)

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

Correct Answer: D

**QUESTION 15**

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0 ?1023

Correct Answer: D

Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)