312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity

B. Key discovery

C. Bulk data encryption

D. Key recovery

Correct Answer: C

QUESTION 2

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe

B. g++ hackersExploit.py -o calc.exe

C. g++ -i hackersExploit.pl -o calc.exe

D. g++ --compile i hackersExploit.cpp -o calc.exe

Correct Answer: A

QUESTION 3

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm\\'s public facing web

servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

DatE. Mon, 16 Jan 2011 01:41:33 GMT

Content-TypE. text/html

Accept-Ranges: bytes

Last-ModifieD. Wed, 28 Dec 2010 15:32:21 GMT

ETaG. "b0aac0542e25c31:89d"

Content-Length: 7369

Which of the following is an example of what the engineer performed?

A. Cross-site scripting

B. Banner grabbing

C. SQL injection

D. Whois database query

Correct Answer: B

QUESTION 4

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator\\'s computer to update the router configuration. What type of an alert is this?

A. False positive

B. False negative

C. True positve

D. True negative

Correct Answer: A

QUESTION 5

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1

B. MD5

C. HAVAL

D. MD4

Correct Answer: A

QUESTION 6

A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.

B. The consultant may expose vulnerabilities of other companies.

C. The company accepting bids will want the same type of format of testing.

D. The company accepting bids will hire the consultant because of the great work performed.

Correct Answer: B

QUESTION 7

Which tool would be used to collect wireless packet data?

A. NetStumbler

B. John the Ripper

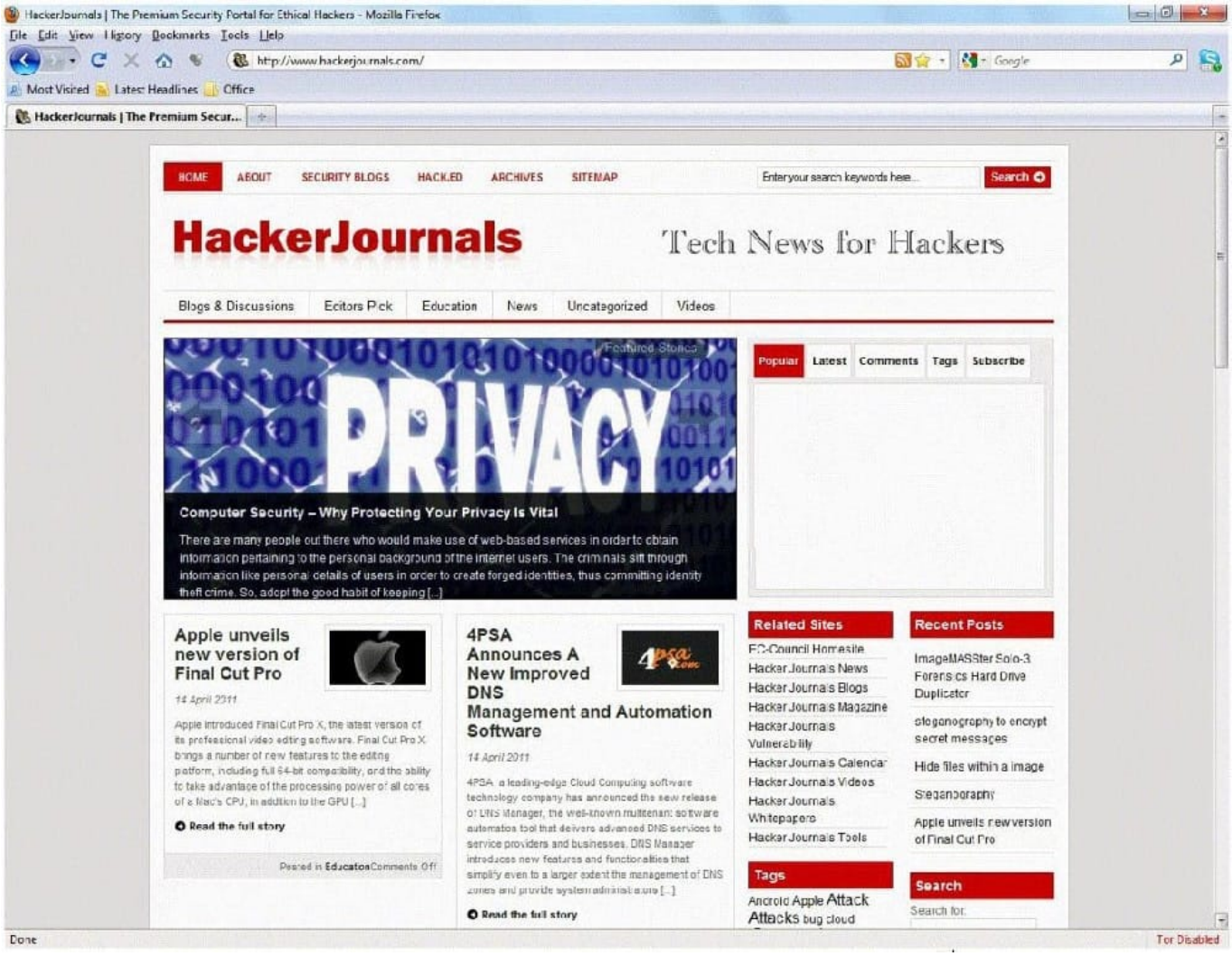
C. Nessus

D. Netcat

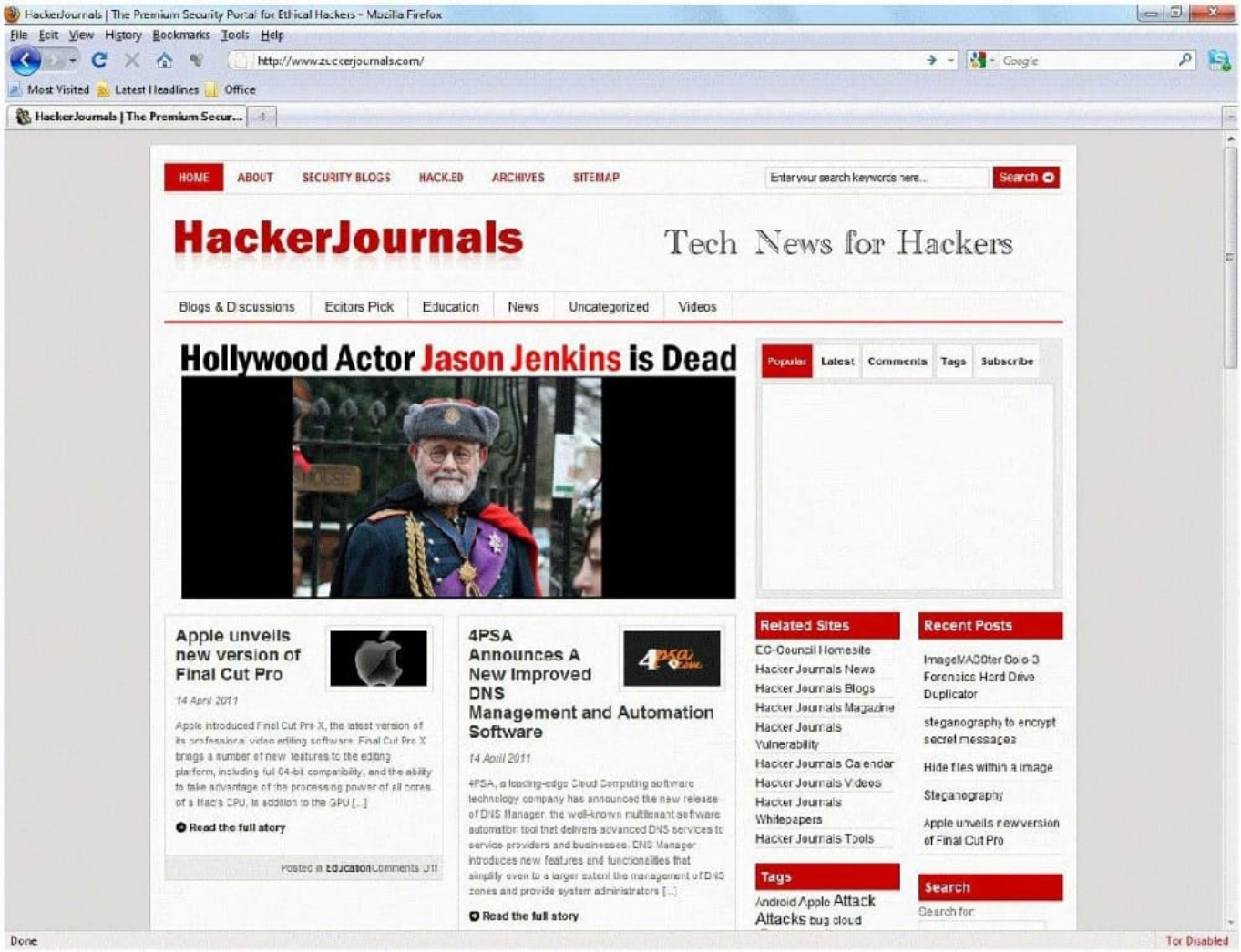
Correct Answer: A

QUESTION 8

An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker\\'s fake site shows up and dupes victims by the fake news.



This is another great example that some people do not know what URL\\'s are. Real website: Fake website: http://www.zuckerjournals.com



The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It\\'s the address that you enter into the address bar at the top your browser and this is clearly not legit site, its www.zuckerjournals.com

How would you verify if a website is authentic or not?

A. Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity

B. Navigate to the site by visiting various blogs and forums for authentic links

C. Enable Cache on your browser and lookout for error message warning on the screen

D. Visit the site by clicking on a link from Google search engine

Correct Answer: D

QUESTION 9

A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company\\'s internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL

B. Mutual authentication

C. IPSec

D. Static IP addresses

Correct Answer: C

QUESTION 10

Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl

B. C++

C. Python

D. Java

Correct Answer: B

QUESTION 11

Your company has blocked all the ports via external firewall and only allows port 80/443 to connect to the Internet. You want to use FTP to connect to some remote server on the Internet. How would you accomplish this?

A. Use HTTP Tunneling

B. Use Proxy Chaining

C. Use TOR Network

D. Use Reverse Chaining

Correct Answer: A

QUESTION 12

A security administrator notices that the log file of the company`s webserver contains suspicious entries:

```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.

B. SQL injection.

C. directory traversal.

D. LDAP injection.

Correct Answer: B

QUESTION 13

A security engineer is attempting to map a company\\'s internal network. The engineer enters in the following NMAP commanD.

NMAP n sS P0 p 80 ***.***.**.** What type of scan is this?

A. Quick scan

B. Intense scan

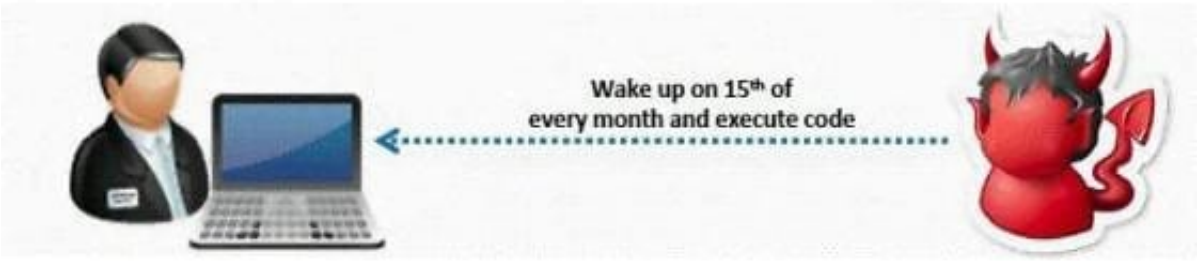
C. Stealth scan

D. Comprehensive scan

Correct Answer: C

QUESTION 14

What type of Virus is shown here?



A. Cavity Virus

B. Macro Virus

C. Boot Sector Virus

D. Metamorphic Virus

E. Sparse Infector Virus

Correct Answer: E

QUESTION 15

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.

B. Encrypt the data on the hard drive.

C. Use a strong logon password to the operating system.

D. Back up everything on the laptop and store the backup in a safe place.

Correct Answer: B