Vendor:EC-COUNCIL

Exam Code:EC0-479

Exam Name:EC-Council Certified Security Analyst(ECSA)

Version: Demo

QUESTION 1

In Microsoft file structures, sectors are grouped together to form:

A. Clusters

B. Drives

C. Bitstreams

D. Partitions

Correct Answer: A

QUESTION 2

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command.

What is he testing at this point?

```
#include
#include
int main(int argc, char *argv[])
{
char buffer[10];
if (argc
{
fprintf(stderr, "USAGE: %s string\n", argv[0]);
return 1;
}
strcpy(buffer, argv[1]);
return 0;
}
```

A. Buffer overflow

B. Format string bug

C. Kernal injection

D. SQL injection

Correct Answer: A

QUESTION 3

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers clocks are synchronize D. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

Correct Answer: B

QUESTION 4

While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?

A. Keep the information of file for later review

B. Destroy the evidence

C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge

D. Present the evidence to the defense attorney

Correct Answer: C

QUESTION 5

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable

B. Port Unreachable

C. Protocol Unreachable

D. Administratively Blocked

Correct Answer: D

QUESTION 6

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

alert("This is a test.")

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS

B. Your website is not vulnerable

C. Your website is vulnerable to SQL injection

D. Your website is vulnerable to web bugs

Correct Answer: A

QUESTION 7

The MD5 program is used to:

A. wipe magnetic media before recycling it

B. make directories on a evidence disk

C. view graphics files on an evidence drive

D. verify that a disk is not altered when you examine it

Correct Answer: D

QUESTION 8

What operating system would respond to the following command?

A. Mac OS X

B. Windows XP

C. Windows 95

D. FreeBSD

Correct Answer: D

QUESTION 9

When cataloging digital evidence, the primary goal is to:

A. Make bit-stream images of all hard drives

B. Preserve evidence integrity

C. Not remove the evidence from the scene

D. Not allow the computer to be turned off

Correct Answer: B

QUESTION 10

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company\\'s network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Enumerate all the users in the domain

B. Perform DNS poisoning

C. Send DOS commands to crash the DNS servers

D. Perform a zone transfer

Correct Answer: D

QUESTION 11

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

What have you found?

A. Trojan.downloader

B. Blind bug

C. Web bug

D. CGI code

Correct Answer: C

QUESTION 12

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Open

B. Stealth

C. Closed

D. Filtered

Correct Answer: A

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: