412-79$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

QUESTION 1

Paula works as the primary help desk contact for her company.Paula has just received a call from a user reporting that his computer just displayed a Blue Screen of Death screen and he can no longer work.Paula walks over to the user s computer and sees the Blue Screen of Death screen.The user s computer is running Windows XP, but the Blue Screen looks like a familiar one that Paula had seen on Windows 2000 computers periodically. The user said he stepped away from his computer for only 15 minutes and when he got back, the Blue Screen was there.Paula also noticed that the hard drive activity light was flashing, meaning that the computer was processing something.Paula knew this should not be the case since the computer should be completely frozen during a Blue Screen. She checks the network IDS live log entries and notices numerous nmap scan alerts.

What is Paula seeing happen on this computer?

A. Paula s network was scanned using Floppyscan

B. There was IRQ conflict in Paula s PC

C. Paula s network was scanned using Dumpsec

D. Tools like Nessus will cause BSOD

Correct Answer: A

QUESTION 2

The offset in a hexadecimal code is:

A. The last byte after the colon

B. The 0x at the beginning of the code

C. The 0x at the end of the code

D. The first byte after the colon

Correct Answer: B

QUESTION 3

Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control

B. prove that the tools you used to conduct your examination are perfect

C. read your curriculum vitae to the jury

D. qualify you as an expert witness

Correct Answer: D

QUESTION 4

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

A. Globally unique ID

B. Microsoft Virtual Machine Identifier

C. Personal Application Protocol

D. Individual ASCII string

Correct Answer: A

QUESTION 5

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security

B. RestrictAnonymous must be set to "3" for complete security

C. There is no way to always prevent an anonymous null session from establishing

D. RestrictAnonymous must be set to "10" for complete security

Correct Answer: A

412-79 VCE Dumps 412-79 Study Guide 412-79 Braindumps