412-79^Q&As

EC-Council Certified Security Analyst (ECSA)

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

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

https://www.passapply.com/412-79.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you

are required to infer only what is explicit in the excerpt. (Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

03/15-20:21:24.107053

A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP

TS: 23678634 2878772 =+= +=+=+=+=+=

IpLen:20 DgmLen:84 Len: 64

01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 .... 00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 .... 00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....

00 00 00 11 00 00 00 00 ....

=+=

IpLen:20 DgmLen:1104 Len: 1084 47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has conducted a network sweep on port 111

B. The attacker has scanned and exploited the system using Buffer Overflow

C. The attacker has used a Trojan on port 32773

D. The attacker has installed a backdoor

Correct Answer: A

QUESTION 2

Which of the following is NOT a graphics file?

A. Picture1.tga

B. Picture2.bmp

C. Picture3.nfo

D. Picture4.psd

Correct Answer: C

QUESTION 3

An Expert witness give an opinion if:

A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors

B. To define the issues of the case for determination by the finder of fact

C. To stimulate discussion between the consulting expert and the expert witness

D. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case

Correct Answer: A

QUESTION 4

What does the superblock in Linux define?

A. filesynames

B. diskgeometr

C. location of the firstinode

D. available space

Correct Answer: C

QUESTION 5

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

412-79 Study Guide   412-79 Exam Questions   412-79 Braindumps