EC1-349 Q&As

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.pass2lead.com/ec1-349.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

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times

B. a new log file is created everyday

C. a new log file is created each week

D. a new log is created each time the Web Server is started

Correct Answer: B

QUESTION 2

Jason is the security administrator of ACMA metal Corporation. One day he notices the company\\'s Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center

B. Local or national office of the U.S. Secret Service

C. National Infrastructure Protection Center

D. CERT Coordination Center

Correct Answer: B

QUESTION 3

What is a good security method to prevent unauthorized users from "tailgating"?

A. Pick-resistant locks

B. Electronic key systems

C. Man trap

D. Electronic combination locks

Correct Answer: C

QUESTION 4

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 211.185.125.124:3500 -> 172.16.1.108:111 TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF ***A**** Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772

=+= += 03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111 UDP TTL:43 TOS:0x0 ID:29733 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 ....

=+= +=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c............

00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....

3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost

=+= +=+=+

03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168

TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF

AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23679878 2880015

63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;

69 64 3B id;

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 5

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network

A. 16-bit address

B. 24-bit address

C. 32-bit address

D. 48-bit address

Correct Answer: D