

Exam 312-49v9

ECCouncil Computer Hacking Forensic Investigator (V9)

Verson: Demo

[Total Questions: 10]

Topic break down

Торіс	No. of Questions
Topic 1: Exam Set A	2
Topic 2: Exam Set B	3
Topic 3: Exam Set C	5

Topic 1, Exam Set A

Question No : 1 - (Topic 1)

Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system

Network forensics can reveal: (Select three answers)

- A. Source of security incidents' and network attacks
- B. Path of the attack
- C. Intrusion techniques used by attackers
- **D.** Hardware configuration of the attacker's system

Answer: A,B,C

Question No : 2 - (Topic 1)

Which of the following file in Novel GroupWise stores information about user accounts?

A. ngwguard.dbB. gwcheck.dbC. PRIV.EDBD. PRIV.STM

Answer: A

Topic 2, Exam Set B

Question No : 3 - (Topic 2)

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

- A. He should search in C:\Windows\System32\RECYCLED folder
- **B.** The Recycle Bin does not exist on the hard drive

C. The files are hidden and he must use switch to view themThe files are hidden and he must use ? switch to view them

D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

Question No : 4 - (Topic 2)

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

- A. C:\Program Files\Exchsrvr\servername.log
- B. D:\Exchsrvr\Message Tracking\servername.log
- C. C:\Exchsrvr\Message Tracking\servername.log
- D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Answer: A

Question No : 5 - (Topic 2)

The following is a log file screenshot from a default installation of IIS 6.0.

```
WSoftware: Microsoft Internet Information Services 6.0
Wversion: 1.0
Poate: 2007-01-22 15:42:36
#Fields: date time s-strename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/index.asp = 80 - 172.16.28
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/cs/olcstyle.css = 80 - 172.16.28
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/cs/oltamber/set = 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/mages/index_01.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp = 80 -
Mozilla/4.0+(compatible:+MSIE+6.0;+windows+NT+5.1;+Sv1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /bevelopment/images/index_0.jp
```

What time standard is used by IIS as seen in the screenshot?

A. UTC **B.** GMT **C.** TAI **D.** UT

Answer: A

Topic 3, Exam Set C

Question No : 6 - (Topic 3)

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 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 lpLen:20 DgmLen:1104

Len: 1084

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

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

Answer: A

Question No : 7 - (Topic 3)

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

- A. Demonstrate that no system can be protected againstDoS attacks
- B. List weak points on their network
- C. Show outdatedeQuipment so it can be replaced
- **D.** Use attack as a launching point to penetrate deeper into the network

Answer: B

Question No : 8 - (Topic 3)

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 16

B. 32

C. 64

D. 48

Answer: B

Question No : 9 - (Topic 3)

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

- A. Something other than root
- B. Root
- C. Guest
- D. You cannot determine what privilege runs the daemon service

Answer: A

Question No : 10 - (Topic 3)

In a FAT32 system, a 123 KB file will use how many sectors?

A. 34 **B.** 25

C. 11

D. 56 **E.** 246

Answer: E

Explanation:

If you assume that we are using 512 bytes sectors, then $123 \times 1024/512 = 246$ sectors would be needed.