DUMPS ARENA

ECCouncil Computer Hacking Forensic Investigator

ECCouncil EC0-349

Version Demo

Total Demo Questions: 10

Total Premium Questions: 304
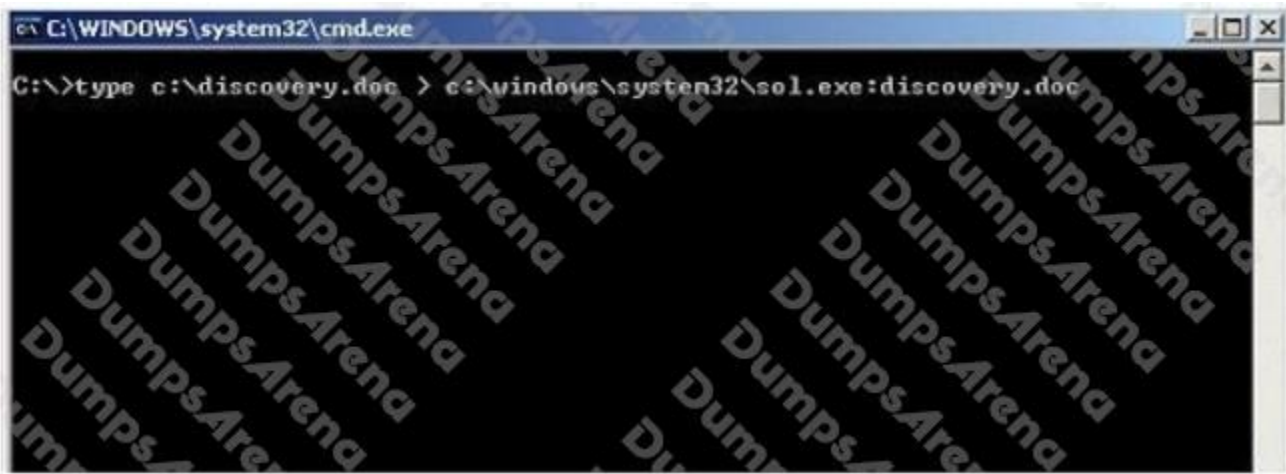
Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

dumpsarena.com

QUESTION NO: 1

What feature of Windows is the following command trying to utilize?

```
C:\WINDOWS\system32\cmd.exe                                    _ □ ×
C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

A. White space

B. AFS

C. ADS

D. Slack file

ANSWER: C

QUESTION NO: 2

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

QUESTION NO: 3

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

QUESTION NO: 4

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

A. File signatures

B. Keywords

C. Hash sets

D. Bookmarks

ANSWER: B

QUESTION NO: 5

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

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename 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 /Development/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 /Development/css/olcstyle.css - 80 - 17
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 /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 w3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 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 /Development/images/index_01.jpg - 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 /Development/images/index_02.jpg - 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 /Development/images/index_03.jpg - 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 /Development/images/index_04.jpg - 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 /Development/images/index_06.jpg - 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 /Development/images/index_07.jpg - 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 /Development/images/index_08.jpg - 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 /Development/script/dhtml.js - 80 - 172
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 /Development/images/greenArraw.jpg - 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 /Development/images/board_01.jpg - 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 /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

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

A. UTC

B. GMT

C. TAI

D. UT

ANSWER: A

QUESTION NO: 6

A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?

A. Root Internet servers

B. Border Gateway Protocol

C. Gateway of last resort

D. Reverse DNS

ANSWER: C

When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

A. 202

B. 404

C. 505

D. 909

ANSWER: B

Using Linux to carry out a forensics investigation, what would the following command accomplish?

dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file

B. Backup a disk to an image file

C. Copy a partition to an image file

D. Restore a disk from an image file

ANSWER: D

Why should you never power on a computer that you need to acquire digital evidence from?

A. When the computer boots up, files are written to the computer rendering the data nclean

B. When the computer boots up, the system cache is cleared which could destroy evidence

C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence

---

D. Powering on a computer has no affect when needing to acquire digital evidence from it

ANSWER: A

QUESTION NO: 10

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media

B. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence

C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media

D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

ANSWER: B