EC0-349$^{\text{Q\&As}}$

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

QUESTION 1

What does the acronym POST mean as it relates to a PC?

A. Primary Operations Short Test

B. PowerOn Self Test

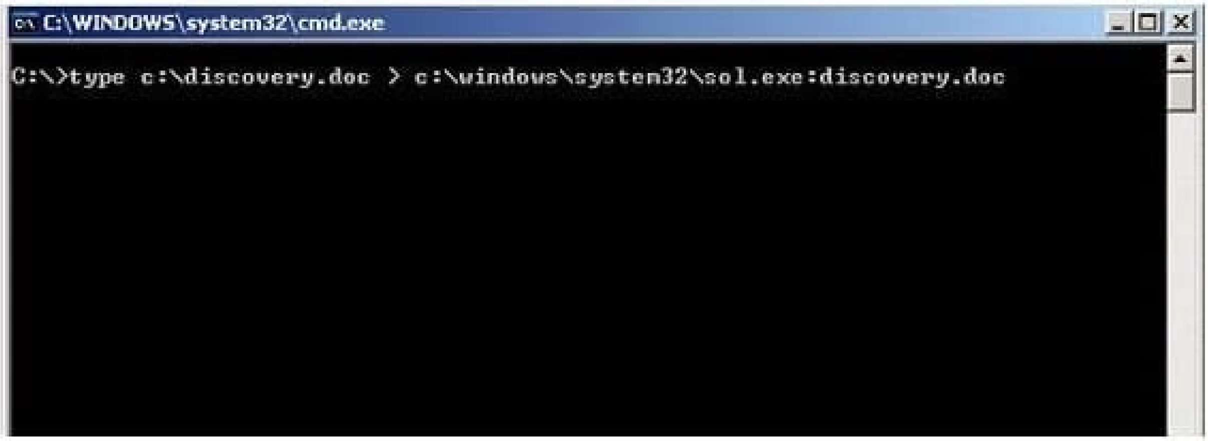
C. Pre Operational Situation Test

D. Primary Operating System Test

Correct Answer: B

QUESTION 2

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



```
C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

A. White space

B. AFS

C. ADS

D. Slack file

Correct Answer: C

QUESTION 3

You should make at least how many bit-stream copies of a suspect drive?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

QUESTION 4

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

A. create a compressed copy of the file with DoubleSpace

B. create a sparse data copy of a folder or file

C. make a bit-stream disk-to-image file

D. make a bit-stream disk-to-disk file

Correct Answer: C

QUESTION 5

Why should you note all cable connections for a computer you want to seize as evidence?

A. to know what outside connections existed

B. in case other devices were connected

C. to know what peripheral devices exist

D. to know what hardware existed

Correct Answer: A

QUESTION 6

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed

B. Open

C. Stealth

D. Filtered

Correct Answer: B

QUESTION 7

The following excerpt is taken from a honeypot log. The log captures activities across three days.

There are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

From the options given below choose the one which best interprets the following entry:

```
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
```

A. An IDS evasion technique

B. A buffer overflow attempt

C. A DNS zone transfer

D. Data being retrieved from 63.226.81.13

Correct Answer: A

QUESTION 8

Study the log given below and answer the following question:

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80 Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP53 in from outside to DNS server

B. Allow UDP53 in from DNS server to outside

C. Disallow TCP53 in from secondaries or ISP server to DNS server

D. Block all UDP traffic

Correct Answer: A

QUESTION 9

Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

A. The 10th Amendment

B. The 5th Amendment

C. The 1st Amendment

D. The 4th Amendment

Correct Answer: D

QUESTION 10

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware writeblocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

Correct Answer: D

QUESTION 11

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 12

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field

B. TCP header field

C. IP header field

D. UDP header field

Correct Answer: B

QUESTION 13

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A. 8

B. 1

C. 4

D. 2

Correct Answer: C

QUESTION 14

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

A. SD memory

B. CF memory

C. MMC memory

D. SM memory

Correct Answer: B

QUESTION 15

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk 80 heads/cylinder 63 sectors/track

A. 53.26 GB

B. 57.19 GB

C. 11.17 GB

D. 10 GB

Correct Answer: A