

Eccouncil

312-39

Certified SOC Analyst (CSA)

Questions And Answers PDF Format:

For More Information – Visit link below:
<https://www.certsgrade.com/>

Version = **Product**



Latest Version: 7.0

Question: 1

Bonney's system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

- A. Complaint to police in a formal way regarding the incident
- B. Turn off the infected machine
- C. Leave it to the network administrators to handle
- D. Call the legal department in the organization and inform about the incident

Answer: B

Question: 2

According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

- A. Create a Chain of Custody Document
- B. Send it to the nearby police station
- C. Set a Forensic lab
- D. Call Organizational Disciplinary Team

Answer: A

Question: 3

Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

- A. Planning and budgeting → Physical location and structural design considerations → Work area considerations → Human resource considerations → Physical security recommendations → Forensics lab licensing
- B. Planning and budgeting → Physical location and structural design considerations → Forensics lab licensing → Human resource considerations → Work area considerations → Physical security recommendations
- C. Planning and budgeting → Forensics lab licensing → Physical location and structural design considerations → Work area considerations → Physical security recommendations → Human resource considerations

D. Planning and budgeting → Physical location and structural design considerations → Forensics lab licensing → Work area considerations → Human resource considerations → Physical security recommendations

Answer: A

Reference: <https://info-savvy.com/setting-up-a-computer-forensics-lab/>

Question: 4

Which of the following directory will contain logs related to printer access?

- A. /var/log/cups/Printer_log file
- B. /var/log/cups/access_log file
- C. /var/log/cups/accesslog file
- D. /var/log/cups/Printeraccess_log file

Answer: B

Explanation:

Mac Log Files



Log file	Location	Description
crashreporter.log	/var/log/crashreporter.log	Application usage history and application crash information written to this file
access_log	/var/log/cups/access_log	Printer access log information
error_log	/var/log/cups/error_log	Printer connection information and its error logs found here
daily.out	/var/log/daily.out	Network Interface History
log.nmbd	/var/log/samba/log.nmbd	Samba (Windows-based machine) connection information
Logs	~/Library/Logs	Home directory users and application-specific logs can found here
DiscRecording.log	~/Library/Logs/DiscRecording.log	Home users' CD & DVD media burning logs written to this file
DiskUtility.log	~/Library/Logs/DiskUtility.log	This file contains hard disk partitioning logs, CD/DVD burned media logs, ISO/DMG images files mount, unmount history, and file permission repair history
iChatConnectionErrors	/Library/Logs/iChatConnectionErrors	Log history of iChat connection attempts. Data such as username, IP address, and Date & Time of the attempt
Sync	/Library/Logs/Sync	This log file gives information on synchronized Mac systems and mobile devices such as cell phones and iPods, and their activities with date and time

Question: 5

Which of the following command is used to enable logging in iptables?

- A. \$ iptables -B INPUT -j LOG
- B. \$ iptables -A OUTPUT -j LOG

- C. `$ iptables -A INPUT -j LOG`
- D. `$ iptables -B OUTPUT -j LOG`

Answer: C

Explanation:

To enable logging in iptables, below command is used:

```
$ iptables -A INPUT -j LOG
```

In the above command, you can define the source IP or range in the following manner:

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG
```

You can also define the level of LOG to generate specific level of logs:

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG --log-level 4
```

You can also add some prefix to search the specific logs in the large file:

```
$ iptables -A INPUT -s 192.168.10.0/24 -j LOG --log-prefix '** SUSPECT  
**'
```

For More Information – **Visit link below:**
<https://www.certsgrade.com/>

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

16 USD Discount Coupon Code: NB4XKTMZ

