

Latest Version: 6.0

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: A

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: B

Reference: <https://tecmadmin.net/enable-logging-in-iptables-on-linux/>