tasks

- Write an incident report based on malicious network activity from the pcap and from the alerts.
- The incident report should contains 3 sections:
    - ◇ **Executive Summary**: State in simple, direct terms what happened (when, who, what).
    - ◇ **Victim Details**: Details of the victim (hostname, IP address, MAC address, Windows user account name).
    - ◇ **Indicators of Compromise (IOCs)**: IP addresses, domains and URLs associated with the activity. SHA256 hashes if any malware binaries can be extracted from the pcap.

Executive Summary:

On November 26 of 2024, host DESKTOP-B8TQK49 with account oboomwald connected to malicious website modandcrackedapk[.]com. The C2 server commanded the infected host to connect with a different C2 server and await commands

Victim Details:

hostname: DESKTOP-B8TQK49
IP address: 10[.]11[.]26[.]183
MAC address: d0:57:7b:ce:fc:8b

User account name: oboomwald

Indicators of Compromise:

- 193[.]42[.]38[.]139 - modandcrackedapk[.]com
- 194[.]180[.]191[.]64
- 104[.]26[.]1[.]23