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 September 4th, 2024 Andrew Fletcher on DESKTOP-RNVO9AT was infected with a trojan, Koi stealer

Victim Details:

hostname: DESKTOP-RNVO9AT
IP address: 172[.]17[.]0[.]99
MAC address: 18:3d:a2:b6:8d:c4
User account name: afletcher
Full name: Andrew Fletcher

IOCs:

- 79[.]124[.]78[.]197