Ex:No:13

Date:

13.Demonstrate network forensics using PcapXray tool.

Aim

The aim of this exercise is to **rapidly analyze a suspicious Packet Capture (pcap) file** using PcapXray to visually map the network activity, identify communicating hosts, and quickly detect and triage potentially malicious or covert traffic flows.

Theory (How PcapXray Works)

Network forensics involves the collection and analysis of network traffic to investigate security incidents. PcapXray is a tool designed to expedite the initial analysis phase (triage) by converting raw packet data into an easy-to-digest visual format.

> **PCAP Parsing:** PcapXray reads the raw pcap file, extracts metadata from headers (e.g., source IP, destination IP, ports, protocols), and stores it in an internal database structure.
>
> **Visualization (Graph Theory):** It uses graph plotting libraries (like graphviz or NetworkX) to model the network.
>
> > **Nodes:** Represents individual hosts (devices), typically identified by their IP and/or MAC addresses.
> >
> > **Edges:** Represents communication flows or sessions between the hosts.
>
> **Triage & Highlighting:** The tool applies built-in heuristics and lookups to categorize and visually highlight traffic for the investigator:
>
> > **Malicious Traffic:** Heuristics look for connections to known bad reputation IPs, high-entropy traffic, or communication over non-standard/rarely used ports.

Tor Traffic: It checks destination IPs against a list of known Tor relay nodes to flag anonymization traffic.

Device Identification: It attempts to resolve MAC Organizationally Unique Identifiers (OUIs) to identify hardware vendors.

Payload Extraction: It automatically reassembles sessions (especially HTTP) to extract embedded files, which is critical for confirming malware or data exfiltration.

PcapXray works as a **triage accelerator**, providing a high-level visual summary and directing the investigator's attention to the most suspicious data points within a large pcap.

Observation (Expected Results from a Practical Scenario)

To demonstrate, assume the pcap file contains a malware infection that used HTTP to download a payload and Tor for Command and Control (C2).

PcapXray Feature	Expected Observation	Forensics Conclusion
Network Diagram	The main graph displays a node (Victim IP) with a high volume of connections.	Quickly identifies the **most active host** in the capture, likely the compromised system.
Traffic Highlighting	A specific connection flow is highlighted in a distinct color (e.g., red) labeled "Possible Malicious."	This connection, usually an HTTP request, is the probable **initial infection vector** (payload download).
Tor Traffic	A different connection from	Indicates that the malware is attempting

PcapXray Feature	Expected Observation	Forensics Conclusion
Identification	the Victim IP to an external IP is flagged as **"Tor Traffic."**	to establish covert **Command and Control (C2)** communication for exfiltration or remote instructions.
File/Payload Extraction	An extracted file named update.exe or a similar suspicious file is listed in the output report.	Confirms the type of **malware payload** downloaded. The file's hash can now be submitted to a service like VirusTotal for immediate threat intelligence.
Device Details	The victim's MAC address is resolved to a known vendor (e.g., "Dell Inc.")	Provides the necessary information to locate the **physical device** on the network for isolation and further host-based forensics.

Export to Sheets

Overall Observation:

PcapXray successfully reduced a large, complex pcap file into three key, actionable pieces of evidence (Malicious Download IP, Tor C2 IP, and Extracted Payload), allowing the incident responder to skip manual packet-by-packet analysis for the initial assessment.