Complete SOC Project Report

Project Title

Network Traffic Analysis (PCAP)-Using Wireshark.

Author

Gourab Das

Target Role

SOC Analyst – Tier 1 / Junior SOC Analyst

---

1. Introduction

Network traffic analysis is a critical skill for SOC analysts and penetration testers. This project demonstrates how packet capture (PCAP) files can be analyzed to uncover indicators of compromise such as command-and-control communication and abnormal DNS behavior.

---

2. Environment Setup

- OS: Kali Linux (Virtual Machine)
- Tool: Wireshark
- Analysis Mode: Offline PCAP analysis
- Dataset: You Dirty RAT PCAP Pack

Wireshark was configured with proper columns, time format, and display filters to support efficient analysis.

---

3. Dataset Description

The PCAP files contain simulated malware traffic including:

- Repeated DNS queries
- Periodic HTTP requests
- External IP communication
- Low-volume but high-frequency traffic

These characteristics are commonly associated with malware beaconing.

---

4. DNS Traffic Analysis

Methodology

Filters used:

```
dns
udp.port == 53
```

Observations

- One internal host generated a high number of DNS queries
- Repeated resolution attempts to the same domains
- Spikes in DNS traffic visible in I/O Graph

Conclusion

The DNS behavior suggests **automated communication**, potentially related to malware command-and-control activity.

---

5. HTTP Traffic Analysis

Methodology

Filters used:

```
http
http.request
```

Observations

- Short and frequent HTTP requests
- Minimal payload size
- Repeated destination IPs

Conclusion

HTTP traffic patterns are consistent with **beaconing behavior**, often used by malware to check in with a C2 server.

---

6. Beaconing Behavior Analysis

Indicators Identified

- Fixed time intervals between packets
- Consistent packet sizes
- Repeated destination IP/domain

Interpretation

These indicators strongly suggest **malware beaconing**, where an infected host periodically contacts a remote server.

---

7. Suspicious IP Analysis

- External IPs observed communicating with internal host
- No evidence of normal user browsing behavior
- Communication pattern matches known malware traffic characteristics

These IPs should be flagged for further investigation and blocking.

---

8. MITRE ATT&CK Mapping Summary

Mapped techniques include:

- **T1071 – Application Layer Protocol**
- **T1071.004 – DNS**
- **T1571 – Non-Standard Port**
- **T1105 – Ingress Tool Transfer**

This mapping translates raw traffic findings into adversary behavior.

---

9. SOC Analyst Perspective

From a SOC Level 1 viewpoint:

- Traffic should be escalated as suspected C2 activity
- DNS, proxy, and firewall logs should be correlated
- Endpoint telemetry is recommended for confirmation

---

10. Limitations

- Analysis limited to PCAP data only
- No endpoint logs available
- Attribution of malware family not performed

---

11. Conclusion

This project demonstrates how **PCAP-based network traffic analysis** can uncover malicious communication patterns. By combining Wireshark analysis with MITRE ATT&CK mapping, the project reflects real-world SOC workflows and strengthens blue team detection capabilities.