Brim

## **Brim - Notes**

### **Task 1: Introduction**

* Brim is a **GUI tool** used for analyzing **Zeek** logs and **PCAP** files.
* It’s fast, intuitive, and helpful for **threat hunting**, **network forensics**, and **incident response**.

### **Task 2: What is Brim?**

* Brim integrates **Zeek**, **Suricata**, and **Zed lake** for seamless network data analysis.
* It allows you to:
  + Import PCAPs or Zeek logs.
  + Search/filter large data sets.
  + View connection metadata quickly.

### **Task 3: The Basics**

* **Search Bar**: For filtering logs (e.g., id.resp\_p=443).
* **Timeline**: Visual representation of traffic over time.
* **Logs Viewer**: Displays parsed Zeek logs (conn.log, dns.log, etc.).
* **Details Panel**: Shows detailed record info (e.g., source IP, ports, protocols).

### **Task 4: Default Queries**

* Brim provides **default queries** (filters/snippets) like:
  + HTTP
  + DNS
  + Conn
  + SSL
* Useful for quick insights into protocol-specific data.

### **Task 5: Use Cases**

* Brim is used in:
  + **Incident Response**: Quick identification of malicious connections.
  + **Threat Hunting**: Detecting command & control (C2), crypto mining, data exfiltration.
  + **Forensics**: Deep packet investigation over time.
* Integration with **Wireshark** for packet-level analysis.

### **Task 6: Exercise – Malware C2 Detection**

* Load a PCAP into Brim.
* Use queries to:
  + Identify long connections.
  + Look for odd ports or IPs.
  + Filter by protocol (conn, dns, etc.).
* Analyze suspicious patterns (e.g., beaconing behavior, strange hostnames).

### **Task 7: Exercise – Crypto Mining Detection**

* Load a crypto mining PCAP.
* Use filters:
  + Ports used by miners (e.g., 3333, 14444).
  + Long-lived connections.
  + Check conn.log and ssl.log for C2 connections.
* Look for signs of **Monero/XMRig mining** or pools.

### **Task 8: Conclusion**

* Brim simplifies network log analysis.
* Great for **SOC analysts**, **forensics investigators**, and **threat hunters**.
* Supports Zeek logs and PCAPs natively.
* Allows pivoting between metadata and full packets (via Wireshark).

