**PCAP comparison**

Results against **Aposemat IoT-23**

**CTU-IoT-Malware-Capture-20-1 (Torii)**

**Labels Distribution**

|  |  |
| --- | --- |
| **Label** | **Flows** |
| Benign | 3,193 |
| C&C-Torii | 16 |

A screenshot of a computer

AI-generated content may be incorrect.

**CTU-IoT-Malware-Capture-34-1 (Mirai)**

**Labels Distribution**

|  |  |
| --- | --- |
| **Label** | **Flows** |
| Benign | 1,923 |
| C&C | 6,706 |
| DDoS | 14,394 |
| PartOfAHorizontalPortScan | 122 |

**Link to this dataset files:**

<https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/IndividualScenarios/CTU-IoT-Malware-Capture-34-1/>

****

**Port**

**TRUE** **POSITIVES (TP)**

**LIVE CAPTURES**

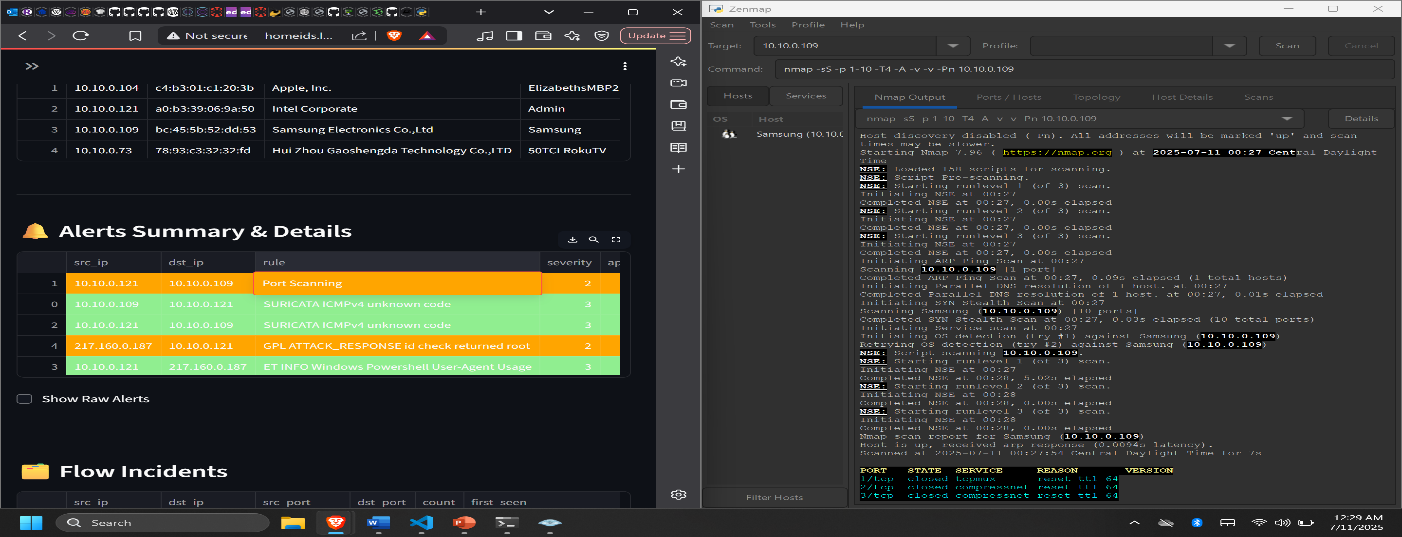
**Powershell curl** <http://testmyids.com> - Detected

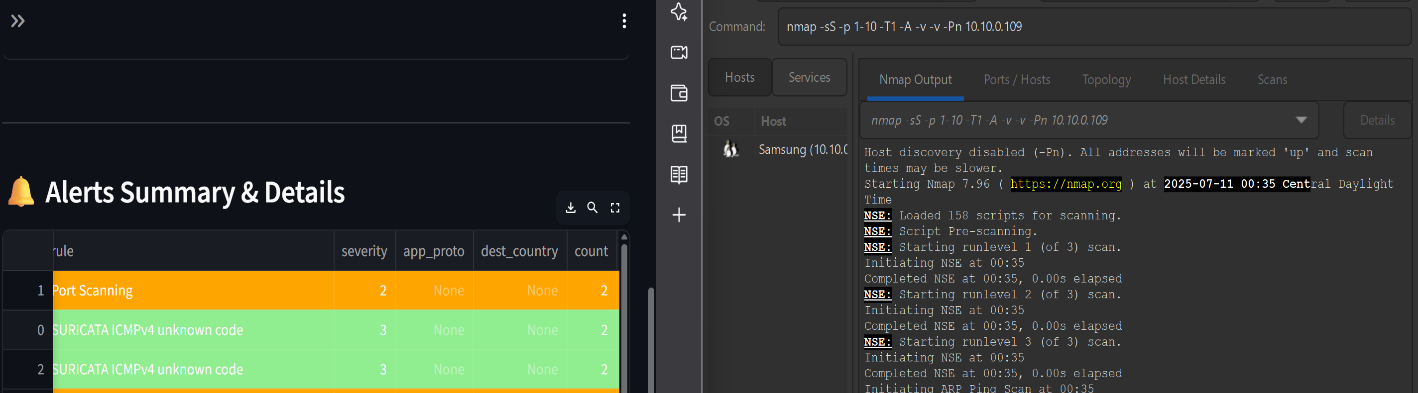
A screenshot of a computer

AI-generated content may be incorrect.

**Scanning**

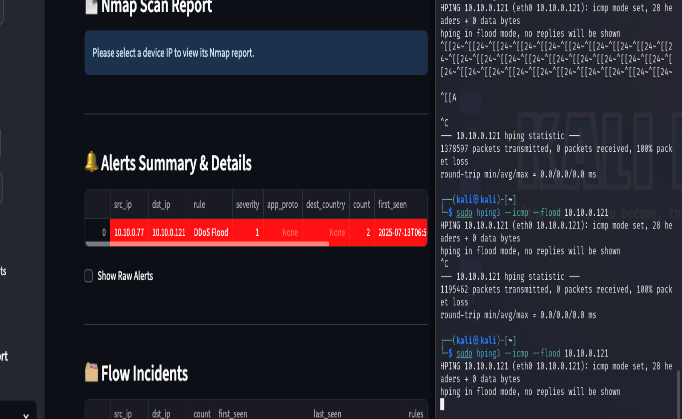
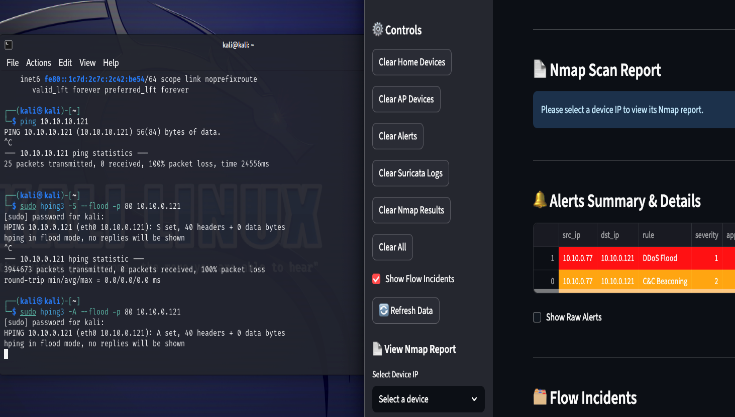
* Attacker IP:10.10.0.121 – Victim IP:10.10.0.109 - Detected
  + nmap -sS -p 1-10 -T1-4 -A -vv -Pn {IP}
  + failure occurs only when less than 10 ports are scanned per 5 seconds

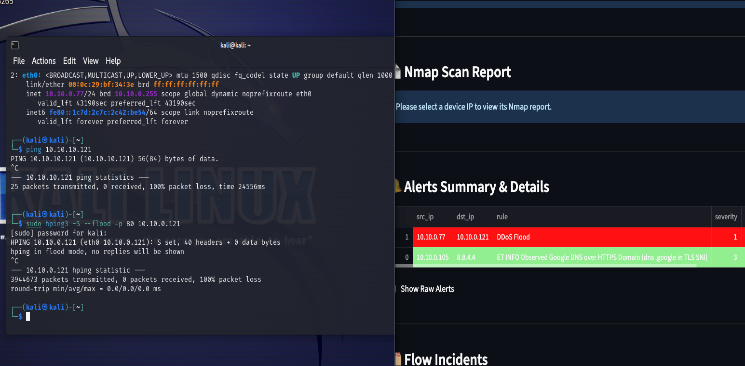
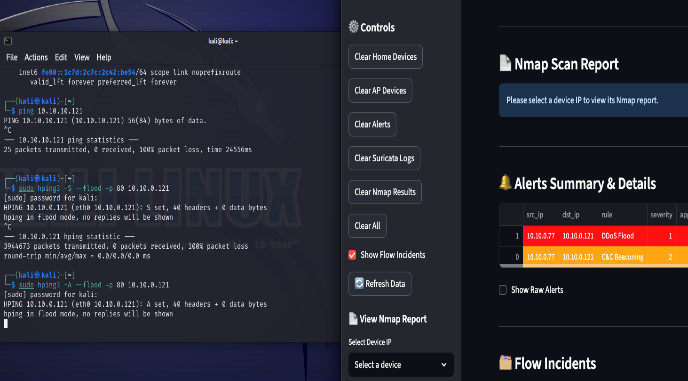




**DoS Attack**

* Attacker 10.10.0.77 – Victim 10.10.0.121
  + Sudo hping3 -S –-flood -p 80 10.10.0.121 – TCP SYN flood - Detected
  + Sudo hping3 -A –-flood -p 80 10.10.0.121 – TCP ACK flood - Detected
  + Sudo hping3 –-icmp –-flood 10.10.0.121 – ICMP PING flood – Detected
  + Sudo hping3 -udp –-flood -p ++1 10.10.0.121 – UDP flood – Detected
  + Sudo hping3 -S -i u90 -p 80 10.10.0.121 – TCP SYN flood w/ 199(pps) - limit





**BRUTE FORCE**

* Attacker 10.10.0.77 – Victim 10.10.0.104
  + hydra -l root -P /usr/share/wordlist/rockyou.txt ssh://10.10.0.104 - Detected

A screenshot of a computer

AI-generated content may be incorrect.

**CVE-2014-6271 - Shellshock**

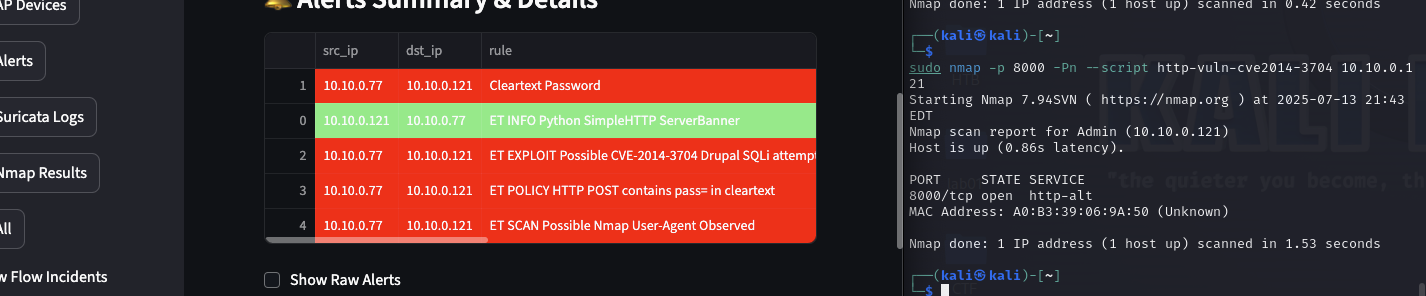
* Attacker 10.10.0.77 – Victim 10.10.0.121
  + Sudo nmap -p 8000 --script http-shellshock 10.10.0.121 – Detected

**A screenshot of a computer

AI-generated content may be incorrect.**

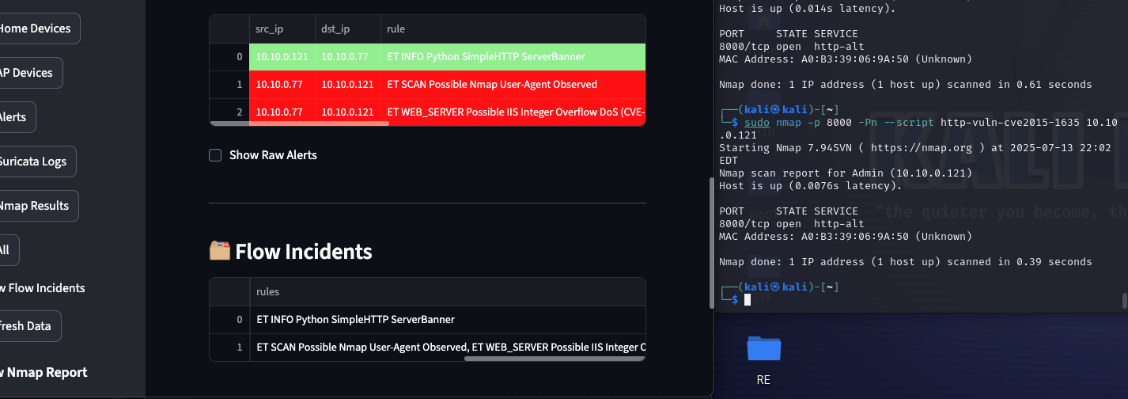
**CVE-2014-3704 – Drupal SQLi**

* Attacker 10.10.0.77 – Victim 10.10.0.121
  + Sudo nmap -p 8000 --script http-vuln-cve2014-3704 10.10.0.121 – Detected

****

**CVE-2015-1635 – IIS Integer Overflow**

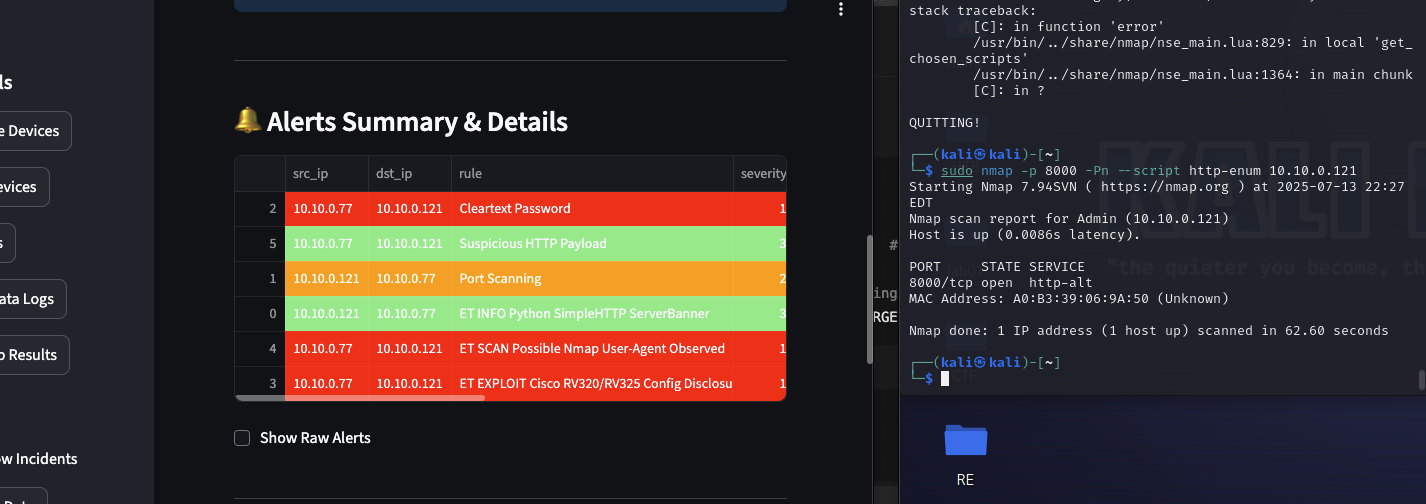
* Attacker 10.10.0.77 – Victim 10.10.0.121
  + Sudo nmap -p 8000 --script http-vuln-cve2015-1635 10.10.0.121 – Detected

****

**CVE-2019-1653 – Cisco RV320/RV325**

* Attacker 10.10.0.77 – Victim 10.10.0.121

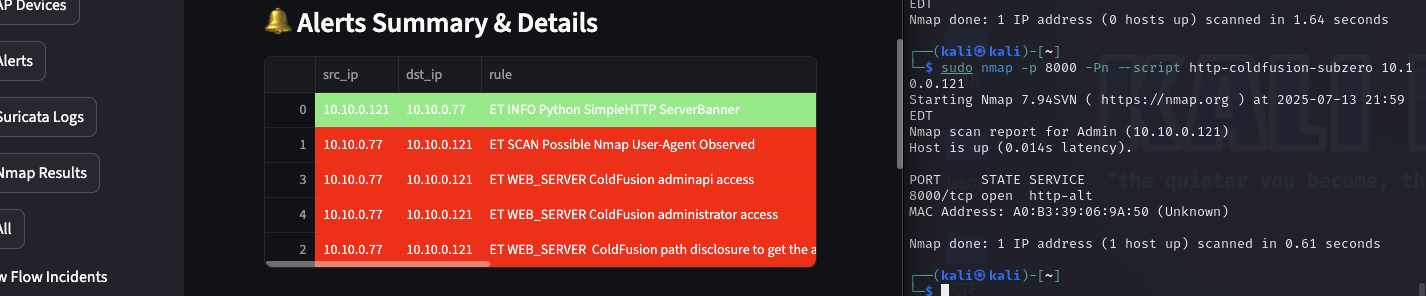
Sudo nmap -p 8000 --script http-enum 10.10.0.121 – Detected



**ColdFusion -**

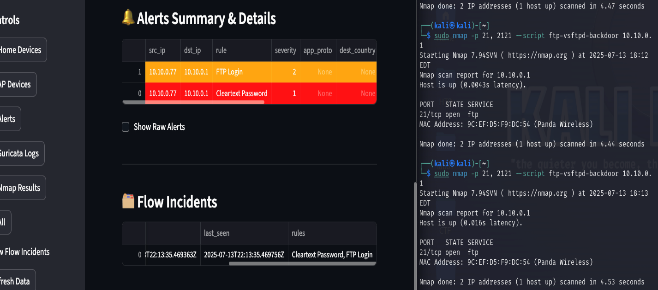
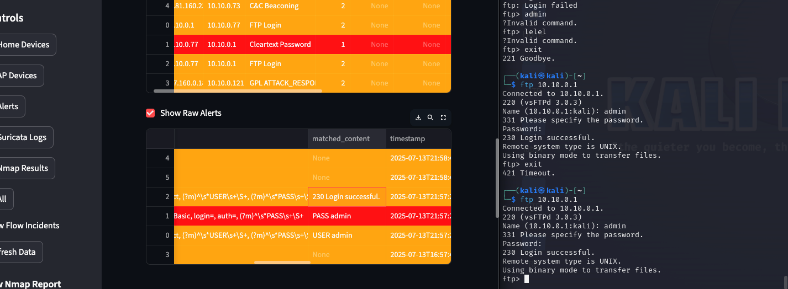
* Attacker 10.10.0.77 – Victim 10.10.0.121

Sudo nmap -p 8000 --script http-coldfusion-subzero 10.10.0.121 – Detected



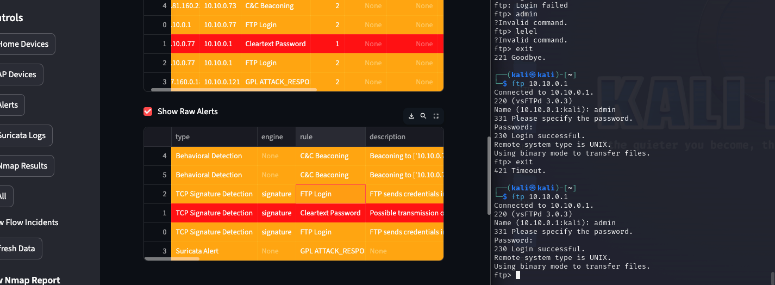
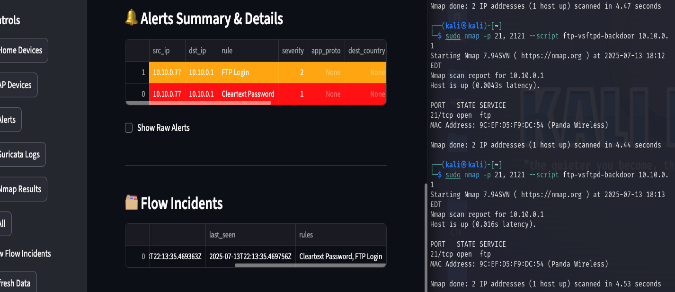
**Cleartext Password**

* Attacker 10.10.0.77 – Victim 10.10.0.1 - Detected
  + ftp 10.10.0.1 – admin:admin
* Attacker 10.10.0.77 – Victim 10.10.0.121
  + Sudo nmap -p 8000 --script http-vuln-cve2014-3704 10.10.0.121 – Detected

****

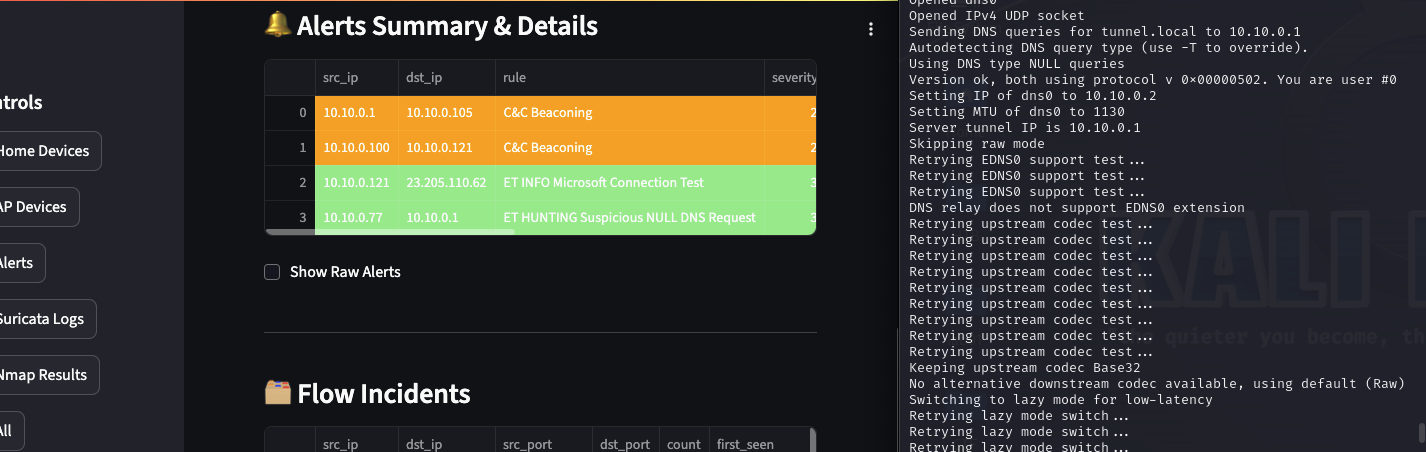
**FTP Login**

* Attacker 10.10.0.77 – Victim 10.10.0.1 - Detected
  + ftp 10.10.0.1
  + sudo nmap -p 21 –script ftp-vsftpd-backdoor - Detected

****

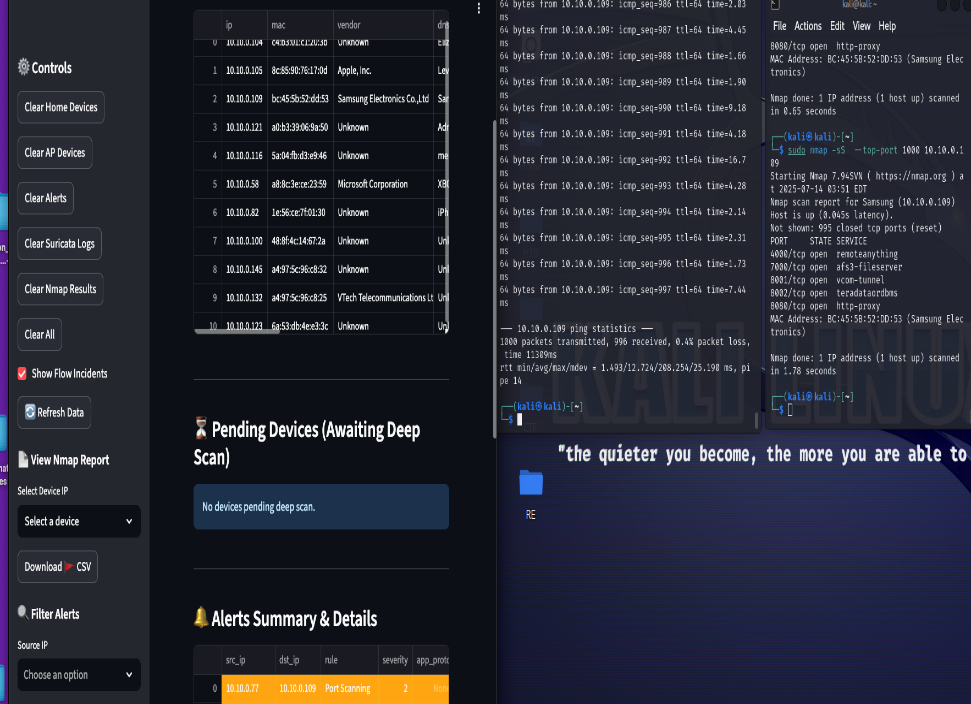
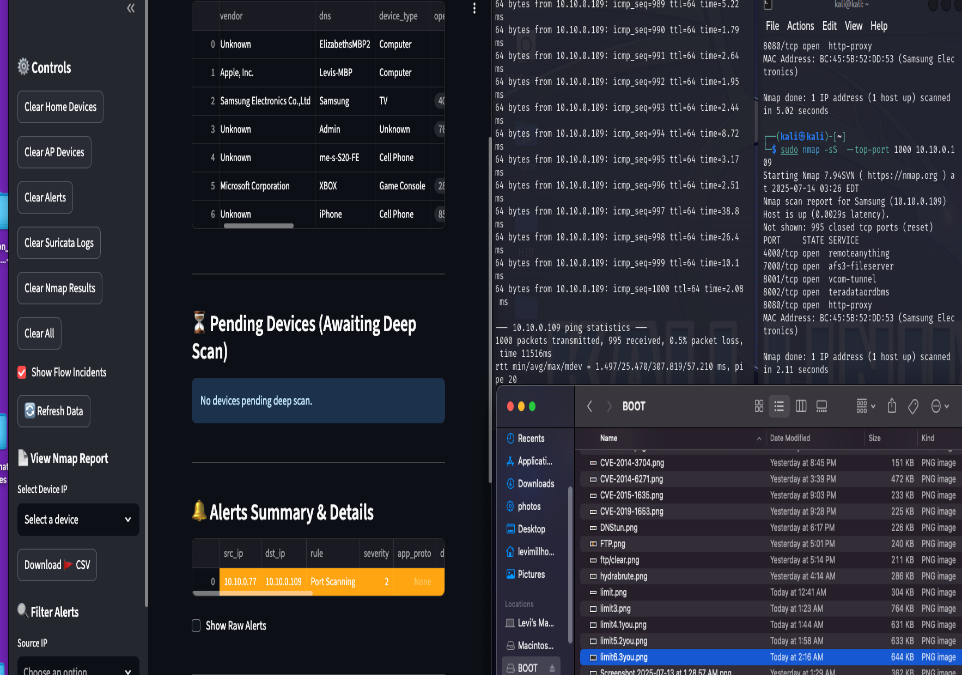
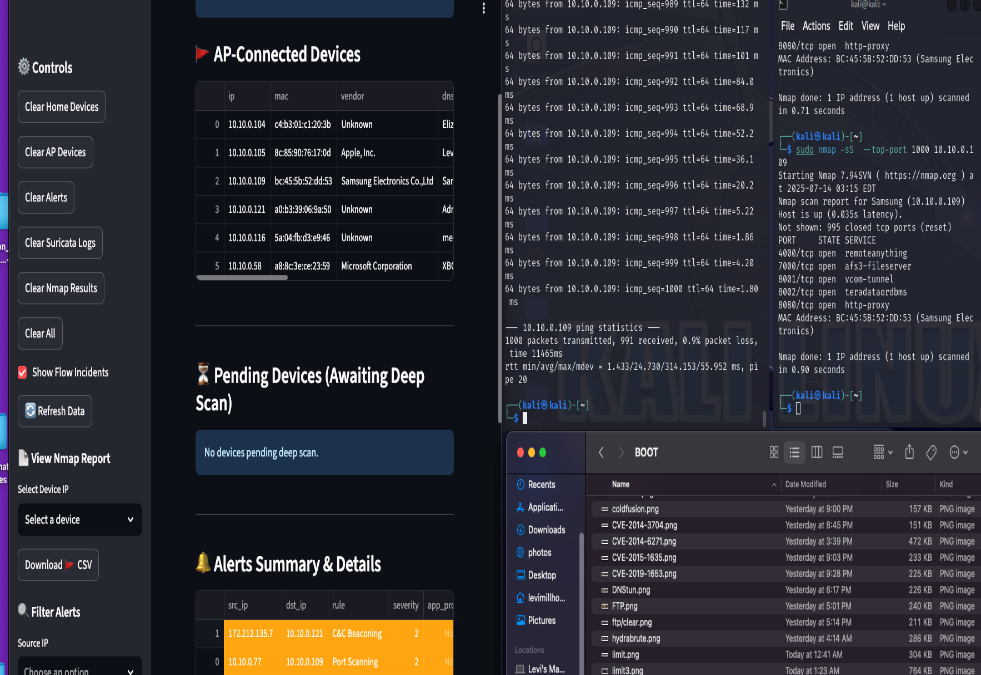
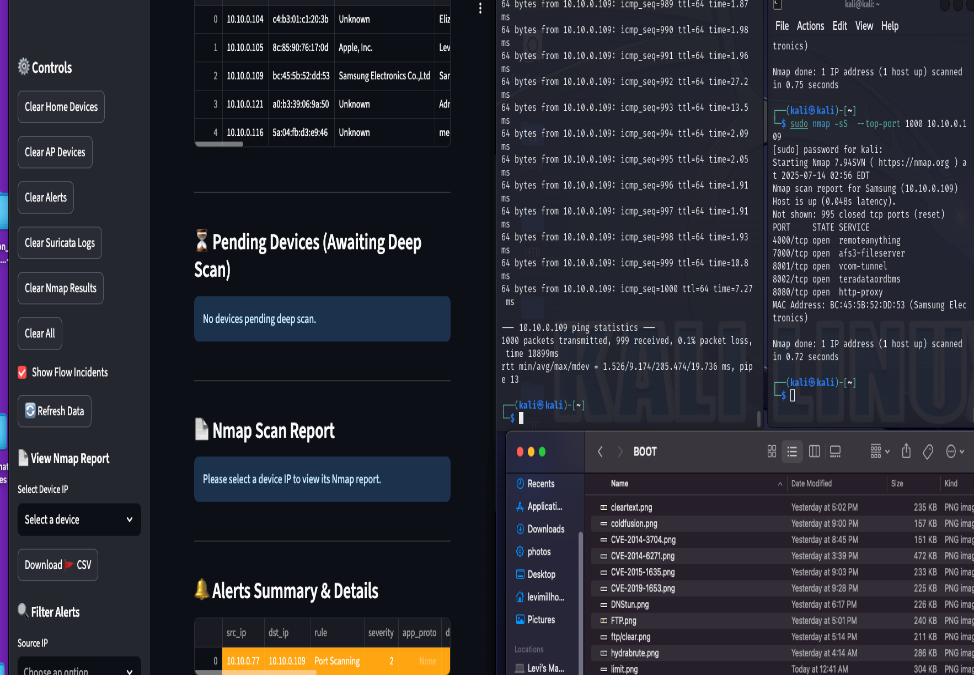
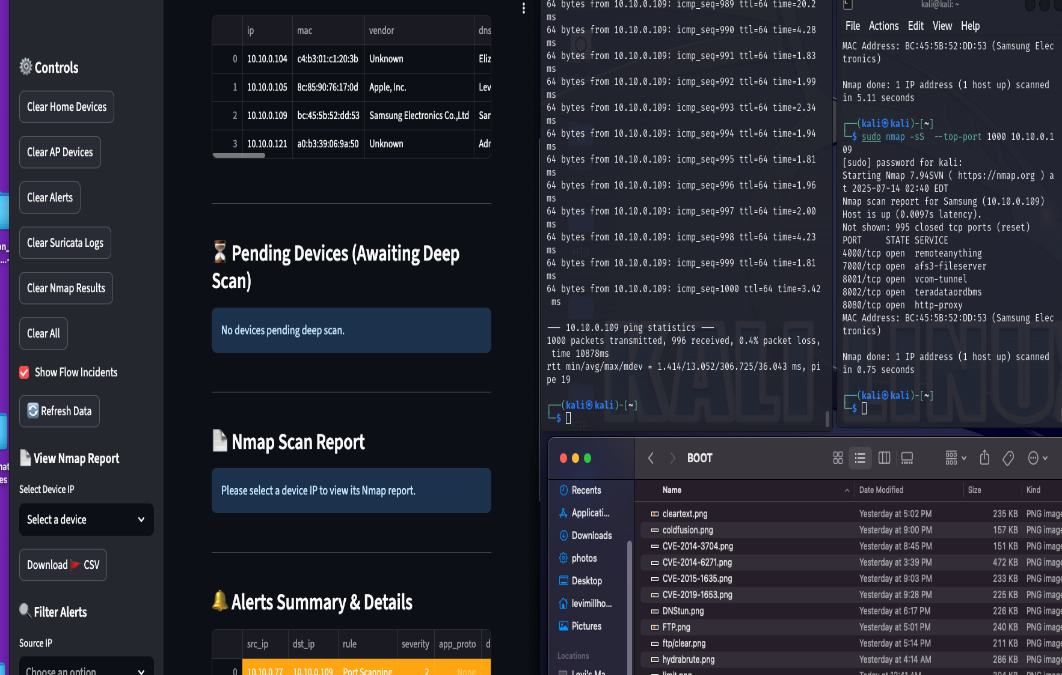
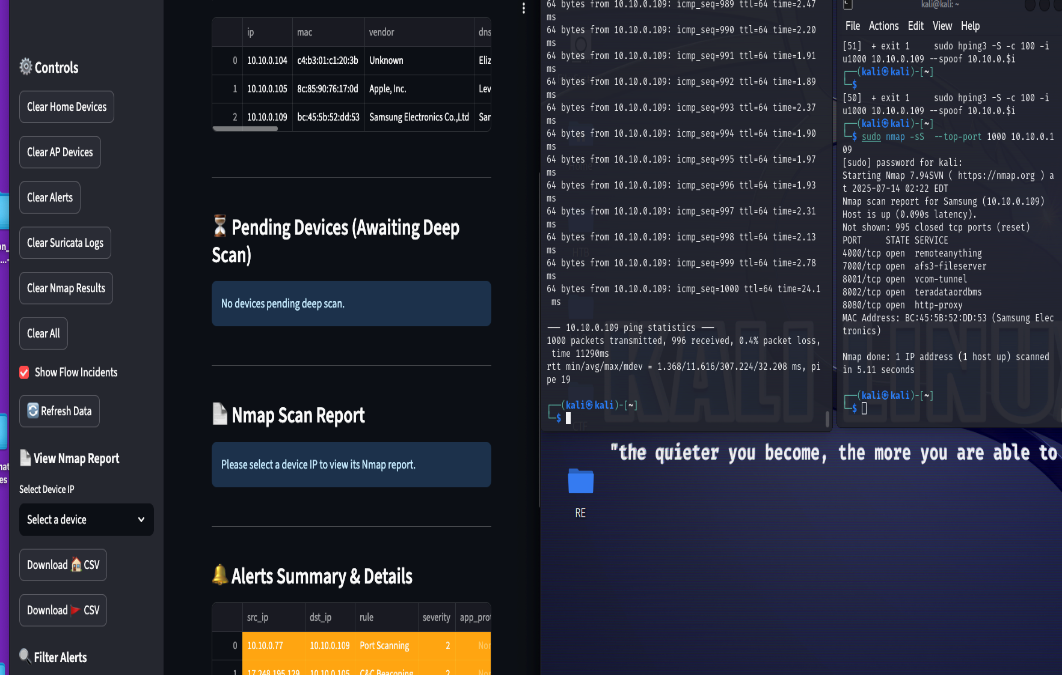
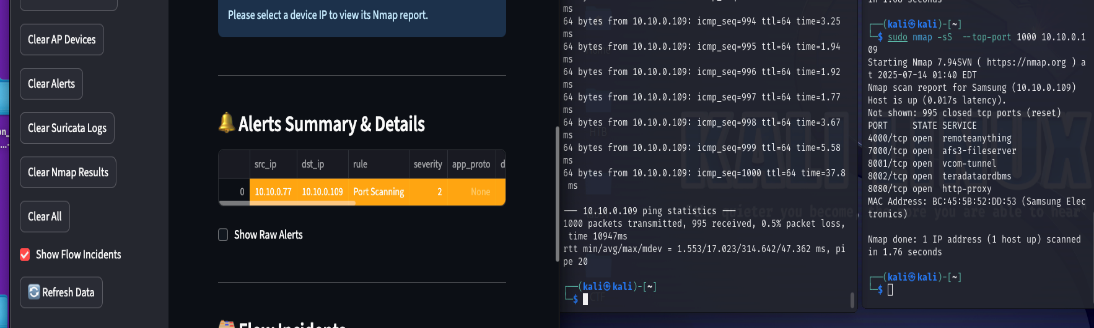
**DNS Tunnel**

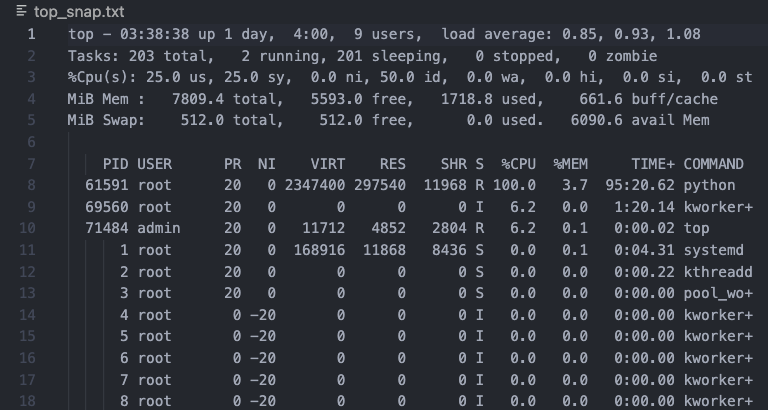
* Attacker 10.10.0.77 – Victim 10.10.0.121 – Partially. Failed to connect.
  + Sudo nmap -p 8000 --script http-vuln-cve2014-3704 10.10.0.121 – Detected

****

**LIMIT TEST**

**Throughput ceiling test - Detections under load - Device count scalability**

****

****