Module 1 Lab – Identify Host with Highest DNS Request Volume

Objective

In this lab, students will use Zeek DNS logs ingested into Elasticsearch and visualized in Kibana to identify the host that generates the highest number of DNS queries in the lab environment.

Step 1 – Generate DNS Traffic

On your Windows or Kali VM, generate DNS queries so that Zeek captures them:
- From Windows: Open a browser and visit multiple websites.
- From Kali: Run commands such as:

- dig example.com
- dig google.com
- for i in {1..20}; do dig test$i.example.com; done

Step 2 – Verify DNS Logs in Zeek

On the Zeek VM, confirm that DNS logs are being recorded:
ls /opt/zeek/logs/current/dns.log
head -5 /opt/zeek/logs/current/dns.log

You should see lines with fields such as id.orig_h (the client IP) and query (the domain).

Step 3 – Check Ingestion in Kibana

1. Log in to Kibana → Discover.
2. Select the filebeat-* data view.
3. Apply filter:
   event.dataset: "zeek.dns"
4. Confirm you see DNS queries with fields such as source.address and dns.question.name.

Questions:

- What are the statistics about the analysis on DNS

- How many destination IP addresses?

- What are the source IP addresses?

- Highest number of DNS query type and Which one is that?

- Are there any interesting DNS queries that are queried domain/subdomains?

Step 4 – Count DNS Requests Per Host

There are two approaches:

- Method 1 – Kibana Lens Visualization:

1. 1. Go to Visualize → Lens.
2. 2. Drag client.ip to Horizontal axis.
3. 3. Drag Records count to Vertical axis.
4. 4. Save chart as “Top DNS Requesting Hosts.”

Question: Provide the screen capture below:

- Method 2 – KQL Query (optional):

5. In Discover, apply the filter:
6. event.dataset: "zeek.dns"
7. Then click + Add field → client.ip and switch to “Top values” view.

Step 5 – Identify the Top Talker

The host with the highest count of DNS requests will be the most active DNS client.
Discuss:
- Is this behavior expected (e.g., normal browsing)?
- Or suspicious (e.g., malware beaconing, DNS tunneling)?

Step 6 – Wrap-up / Questions

- Which host made the most DNS requests?

- Which domains were queried most often?

- Could a high DNS request volume indicate scanning, tunneling, or malware activity?
- How would you distinguish normal vs abnormal DNS activity in your environment?

Deliverables

Students should provide:
- A screenshot of the Kibana visualization showing top DNS requesting hosts.
- A short written answer to the questions and result of the top DNS query host including the anomalous DNS query.