DNS Log Analysis Summary – Splunk SIEM

Environment:

- **Log Source:** `dns.log.gz`
- **Host:** `kali`
- **Index:** `dns_logs`
- **Sourcetype:** `DNS_Logs`
- **Total Events Analyzed:** 422,130
- **Time Range Covered:** Up to May 28, 2025, 2:45:10 PM

Key Findings

1. DNS Activity Volume

- A single timechart query showed **422,130 DNS events** occurred within the hour of **2:00 PM to 3:00 PM**, indicating a high concentration of DNS traffic during that period.
- This could suggest a scripted or automated process, possibly a software update check, service heartbeat, or even scanning/malicious behavior.

---

2. Top Source IPs

Using `| top src_ip`, the top 10 IP addresses generated over 45% of total DNS queries. Notably:

- `10.10.117.210` alone generated **75,943 queries** (~18%) — a significant outlier that warrants further inspection.
- Multiple internal IPs from `192.168.202.x` range are heavily represented, suggesting multiple internal clients or virtual machines contributing to DNS activity.

Rank	IP Address	Queries	Percentage
1	10.10.117.210	75,943	17.99%
2	192.168.202.93	25,934	6.14%
3	192.168.202.103	17,872	4.23%
…	…	…	…

Recommendation: Investigate the activity and role of `10.10.117.210`. High query volume could indicate a misconfigured host, DNS tunneling, or malware beaconing.

---

3. Most Queried Domain

- `teredo.ipv6.microsoft.com` accounted for **9% of all DNS queries (39,118)**.
- This domain is linked to Microsoft's Teredo service — used for IPv6 tunneling over IPv4.

---

4. NXDOMAIN Responses

- A search for NXDOMAIN responses returned **zero results**, suggesting:
    - All DNS queries resolved successfully
    - Logs may not contain DNS response codes
    - Possible filtering or logging limitation

Good Sign: No failed resolutions might indicate clean, well-functioning DNS behavior — or it could indicate logging gaps.

Summary

DNS log analysis revealed high traffic from a small group of internal IPs, with a major share of queries targeting Microsoft's IPv6 tunneling service. While no immediate signs of NXDOMAIN or known malicious domains appeared, the **query volume** and **Teredo usage** are red flags worth reviewing.

Next Steps

- **Investigate** high-traffic IPs like `10.10.117.210` — check process logs or outbound connections.
- **Audit** Teredo service usage across the network; consider disabling it on systems where not needed.
- **Enhance field extraction** to include DNS response codes, query types, and TTLs for deeper threat hunting.
- **Correlate** DNS logs with endpoint, proxy, or firewall logs to confirm normal vs. suspicious behaviors.