Splunk DNS Threat Hunting Portfolio

This project contains **Splunk SPL (`.spl`) queries**, a **custom DNS behavior dashboard**, and a **README guide** for detecting DNS-based anomalies, tunneling, and command & control (C2) activity.

📁Folder Structure

```
splunk-dns-threat-hunting/
│
├── detections/
│   ├── high_unique_subdomains.spl
│   ├── txt_query_anomalies.spl
│   ├── randomized_subdomain_patterns.spl
│   ├── high_nxdomain_rate.spl
│   └── suspicious_tlds.spl
│
├── dashboards/
│   └── dns_behavior_dashboard.xml
│
└── README.md
```

Objective

Develop SPL detections to identify DNS tunneling, data exfiltration, and other suspicious DNS behaviors. This project strengthens core SOC analyst skills in log analysis and threat detection.

🔍Detection Files

✂️`detections/high_unique_subdomains.spl`

```
sourcetype=dns_custom
| stats dc(qname) as unique_queries by src_ip
| where unique_queries > 50
| sort - unique_queries
```

Goal: Detect clients generating many unique DNS subdomains — common in tunneling or DGA malware.

🖋️ `detections/txt_query_anomalies.spl`

```
sourcetype=dns_custom
| where qtype_text="TXT"
| stats count by src_ip, dest_ip
| where count > 20
| sort - count
```

Goal: Identify excessive TXT record requests that could indicate data exfiltration over DNS.

🛏️ `detections/randomized_subdomain_patterns.spl`

```
sourcetype=dns_custom
| eval first_label=mvindex(split(qname, "."),0)
| where match(first_label, "^[A-Za-z0-9+/]{10,}$")
| stats count by src_ip, qname
```

Goal: Detect random or encoded subdomain strings that suggest tunneling or C2 communication.

🌂 `detections/high_nxdomain_rate.spl`

```
sourcetype=dns_custom
| where rcode="NXDOMAIN"
| stats count as nxd_count by src_ip
| where nxd_count > 30
| sort - nxd_count
```

Goal: Find hosts causing excessive NXDOMAIN errors, which may indicate DGAs or misconfigured applications.

🌡️ `detections/suspicious_tlds.spl`

```
sourcetype=dns_custom
| eval tld=lower(mvindex(split(qname, "."),-1))
| search tld IN ("xyz","top","tk","club","click","work","online")
| stats count by src_ip, qname, tld
| sort - count
```

Goal: Flag domains using unusual or low-reputation TLDs commonly abused in C2 campaigns.

📊Dashboard — `dashboards/dns_behavior_dashboard.xml`

The Splunk dashboard visualizes DNS behavior and anomalies.

Panels: 1. **Top 10 DNS Clients by Unique Queries**

```
sourcetype=dns_custom | stats dc(qname) as unique_queries by src_ip | sort -
unique_queries | head 10
```

2. **NXDOMAIN Counts per Client**

```
sourcetype=dns_custom | where rcode="NXDOMAIN" | stats count by src_ip, dest_ip
| sort - count
```

3. **TXT Query Activity**

```
sourcetype=dns_custom | where qtype_text="TXT" | stats count by src_ip | sort -
count
```

4. **Suspicious TLDs**

```
sourcetype=dns_custom | eval tld=lower(mvindex(split(qname,"."),-1)) | search
tld IN ("xyz","top","tk","work","club") | stats count by src_ip, tld
```

⚙️How to Use

1. Upload your DNS logs to Splunk → assign `sourcetype=dns_custom`.
2. Use Splunk's Field Extractor to extract:
3. `src_ip`, `dest_ip`, `qname`, `qtype_text`, `rcode`
4. Copy any `.spl` query into Splunk Search and run detections.
5. Save searches as alerts or add them to the dashboard.
6. Import the XML dashboard to visualize real-time DNS behavior.

🧰Tools Used

- Splunk Enterprise (Free / Local)
- Custom DNS logs (Zeek-like format)

- MITRE ATT&CK for detection mapping

🕑Learning Outcomes

- Built SPL queries for DNS anomaly detection
- Created a custom Splunk dashboard
- Practiced SOC triage workflow and field extraction
- Applied MITRE ATT&CK techniques to DNS threat detection

🧰MITRE ATT&CK Mapping

Technique	ID	Description
Application Layer Protocol: DNS	T1071.004	Use of DNS for C2 or tunneling
Exfiltration Over Alternative Protocol: DNS	T1048	Data exfiltration via DNS TXT records
Dynamic Resolution	T1568.002	DGAs and random subdomain lookups

---

📚References

- MITRE ATT&CK
- Splunk Documentation
- CyberDefenders Labs

Created by: *[Your Name]*
Role: SOC Analyst | Threat Hunter
Project: DNS Threat Hunting & Behavior Analysis using Splunk