Introduction:

DNS logs play an important role in tracking how a network is being used and in spotting possible security risks. With the help of Splunk SIEM, these logs can be analyzed to identify unusual patterns, detect signs of cyberattacks, and improve overall visibility into network activity.Project Overview

In this project, I analyzed sample DNS logs using Splunk and created queries to extract important fields such as source IP, destination IP, and domain names. By studying the query patterns, I was able to identify unusual domains that might suggest network misconfigurations or tunneling activity. This hands-on work helped me strengthen my skills in SIEM log analysis, field extraction using regex, and detecting anomalies in a practical cybersecurity setting.

**Steps to Upload Sample DNS Log Files to Splunk SIEM**

1. **Data Preparation**

**Create or collect a sample DNS log file and ensure it includes relevant DNS event records**

1. **Importing**
2. **Data into Splunk**

* **In Splunk, go to Settings → Add Data → Upload, and upload the prepared DNS log file**A screenshot of a computer

  AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Select File**

* Choose your DNS log file or drag and drop it into the upload box.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Set Source Type**

* Once the DNS log is uploaded, click **Save As** and provide a meaningful name and description for easy identification

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Review Settings**

* Double-check important configurations such as **Host** and **Index** to ensure they are correctly set

A screenshot of a computer

AI-generated content may be incorrect.

1. **Submit and Upload Data**

* Do a final review of all settings, then click **Submit** to complete the data upload process into Splunk.

A screenshot of a computer

AI-generated content may be incorrect.

To confirm that your file has been uploaded successfully, run the following query:  
index=\* sourcetype=<your\_sourcetype>

1. Parsing Data

On the left side, you’ll see a table displaying your log data. In my case, I modified the fields to include additional details such as **dest\_ip** and **dest\_port**.  
You can do this by selecting **Extract New Fields** in Splunk to define and extract new custom fields from your logs.

A screenshot of a computer code

AI-generated content may be incorrect.

* I intend to add additional field as shown below, so we will add Query ID, Source IP, Source Port, Destination IP, Destination Port, Full Quality Domain Name and Record.

A screenshot of a computer

AI-generated content may be incorrect.

* From the event below, select any event and click next

A screenshot of a computer

AI-generated content may be incorrect.

* Select Regular Expression

A screenshot of a computer

AI-generated content may be incorrect.

Select the field **192.168.202.88**, which is the client IP address, and click **Add Extraction**. It will then be grouped and highlighted in a unique color as shown below.

A screenshot of a computer

AI-generated content may be incorrect.

This is how it looks after you finish grouping all the fields you want. In the **Events** panel below, you can see the names of your fields along with colors that indicate them.

A screenshot of a computer

AI-generated content may be incorrect.

* Validate your fields.

A screenshot of a computer

AI-generated content may be incorrect.

Finally, check the newly extracted field, and if everything is correct, click **Finish**.A screenshot of a computer

AI-generated content may be incorrect.

* It shows that you successfully extracted additional fields.

A screenshot of a computer

AI-generated content may be incorrect.

Now, additional fields have been added to the **Interesting Fields** section, including **dest\_ip**, **dest\_port**, and others.

A screenshot of a computer code

AI-generated content may be incorrect.

**Steps to Analyze DNS Log Files in Splunk SIEM**

1. **Search for DNS Events**

* Launch the Splunk interface and navigate to the search bar.
* Use the following query to pull all DNS-related events:

index=\* sourcetype="DNS"

Note: "DNS" is the sourcetype name you assigned when uploading the data.

A screenshot of a computer

AI-generated content may be incorrect.

* If you navigate to the fields, it shows you interesting information like top value count and more

A screenshot of a computer

AI-generated content may be incorrect.

**2. Extract Relevant Fields**

* Identify important fields in DNS logs, such as **source IP**, **destination IP**, **domain name**, **query type**, **response code**, and more.
* You can use a regex to search for common DNS-related keywords in the raw event data. For example:

| regex \_raw="(?i)\b(dns|domain|query|response|port 53)\b"

* Full example query:

index=\* sourcetype=dns\_sample | regex \_raw="(?i)\b(dns|domain|query|response|port 53)\b"

This helps isolate DNS-specific information from the raw logs for easier analysis.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

3. Identity Threat or Unusual Pattern

* - Analyze DNS activity to spot any unusual or suspicious patterns.
* Example query to highlight such events:

index=\* sourcetype="DNS" | stats count by full\_qualified\_domain\_name

This query counts the number of occurrences for each domain, helping to identify domains with abnormal or excessive query activity.

A screenshot of a computer

AI-generated content may be incorrect.

With this search, we see the anomalies in DNS activity

* \*\x00\x00\x00 look like encoded entries, it might be from corrupted DNS packet or malformed queries.
* 0.xxx.168.192 in-addr.arpa, this one is reverse DNS lookups, so it is when an IP address is queried to find its hostname. It is normal but the large number of these could indicate that malicious activity going on here.

A screenshot of a computer

AI-generated content may be incorrect.

Now we get the top queried domains and can see what stand out.

1.Random looking names

- Here, the example is HPE8AA67 which look like a random hostname or misconfigured local device but it is not a standard full qualified domain name

2. Extremely high query count

- in this case, teredo.ipv6.microsoft.com has 54850 queries. Teredo is a windows IPv6 tunneling protocol, but with so many queries like this could indicate automated or misconfiguration. Should check the source ip (10.10.117.210)

3. Reverse DNS lookups

- 44.206.168.192.in-addr.arpa, this is reversed lookup which is normal, but with the high count could indicate something.

4. Well known service

-The rest like [www.apple.com](http://www.apple.com), imap.gmail.com, or api.twitter.com are normal network activity from users.

So in this case, HPE8AA67 and teredo.ipv6.microsoft is suspicious and worth to investigate more.

Conclusion

Analyzing DNS (Domain Name System) logs with Splunk helps security teams quickly detect and investigate suspicious activity. By studying DNS traffic and spotting unusual patterns, organizations can improve their security and reduce the risk of cyber threats.