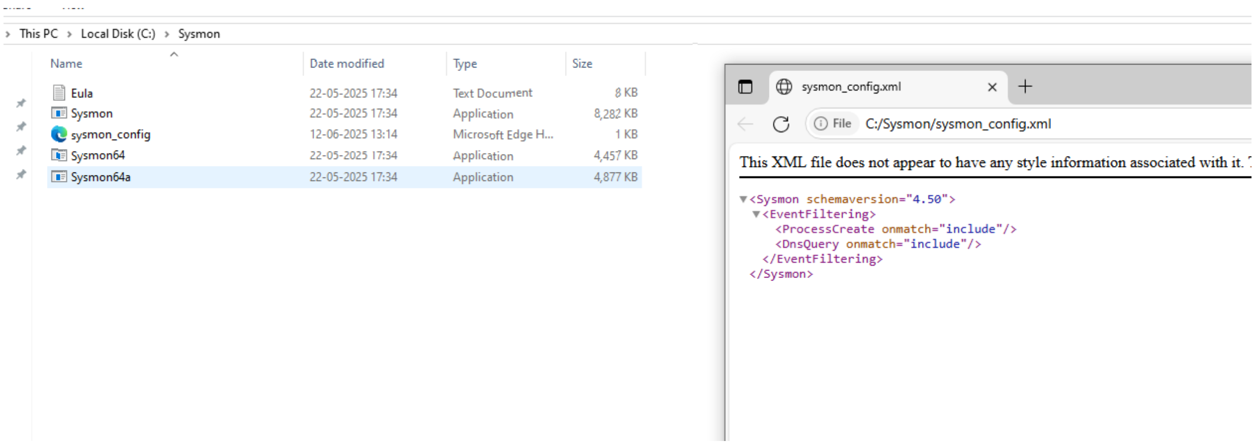
Scenario 4: DNS Tunneling (MITRE T1071.004)

In this scenario, we'll simulate **DNS tunneling**, where an attacker exfiltrates data through DNS requests by encoding data in subdomains. This is a stealthy technique often used by APTs to bypass firewalls and evade detection.

Step 1: Enable DNS Logging on the Windows Machine

- Use a Sysmon configuration that includes:
-
  - ○
    ```
    <Sysmon schemaversion="4.50">
    <EventFiltering>
    <ProcessCreate onmatch="include"/>
    <DnsQuery onmatch="include"/>
    </EventFiltering>
    </Sysmon>
    ```



This PC › Local Disk (C:) › Sysmon

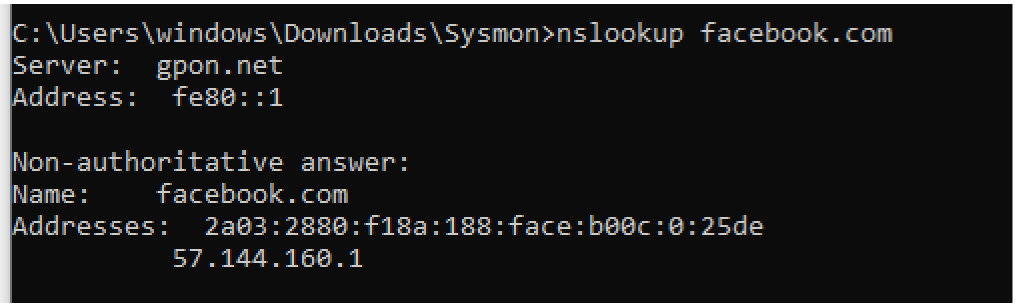
Name	Date modified	Type	Size
Eula	22-05-2025 17:34	Text Document	8 KB
Sysmon	22-05-2025 17:34	Application	8,282 KB
sysmon_config	12-06-2025 13:14	Microsoft Edge H...	1 KB
Sysmon64	22-05-2025 17:34	Application	4,457 KB
Sysmon64a	22-05-2025 17:34	Application	4,877 KB

sysmon_config.xml
File
C:/Sysmon/sysmon_config.xml

This XML file does not appear to have any style information associated with it.

```
▼<Sysmon schemaversion="4.50">
  ▼<EventFiltering>
      <ProcessCreate onmatch="include"/>
      <DnsQuery onmatch="include"/>
    </EventFiltering>
 </Sysmon>
```

Steop 2: run in CMD : nslookup google.com or facebook.com

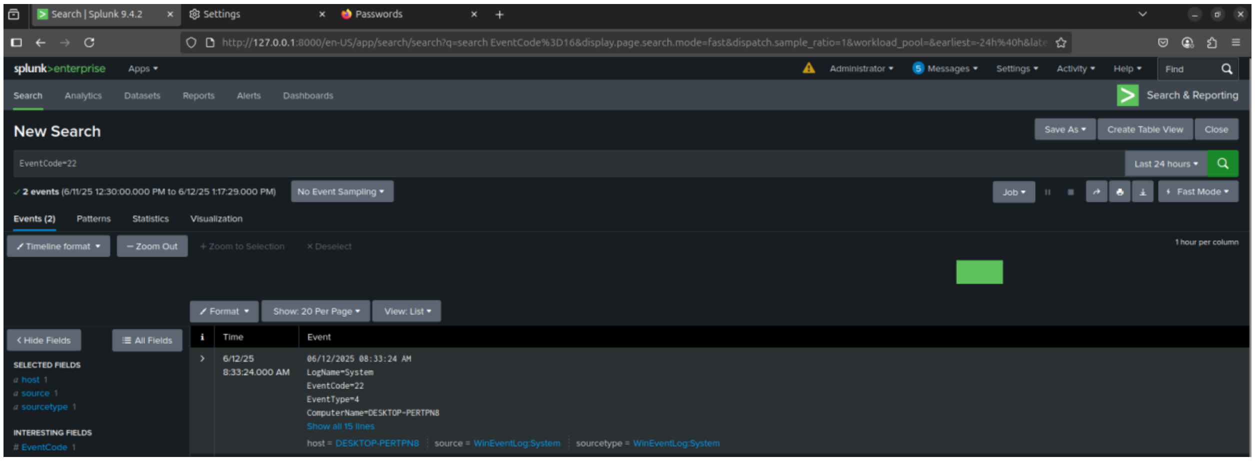
- 

```
C:\Users\windows\Downloads\Sysmon>nslookup facebook.com
Server:  gpon.net
Address:  fe80::1

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f18a:188:face:b00c:0:25de
          57.144.160.1
```

Step 3: Search and Analyze DNS Query Logs in Splunk

- EventCode=22
- **Event ID 22** is being logged by Sysmon,

- 

New Search

EventCode=22

✓ 2 events (6/11/25 12:30:00.000 PM to 6/12/25 1:17:29.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
EventCode 1

i	Time	Event

>	6/12/25
	8:33:24.000 AM
		06/12/2025 08:33:24 AM
		LogName=System
		EventCode=22
		EventType=4
		ComputerName=DESKTOP-PERTPN8
		Show all 15 lines
		host = DESKTOP-PERTPN8 source = WinEventLog:System sourcetype = WinEventLog:System