DNS Attack Detection and Logging (Simple Lab Setup)

Setup Overview:

Machine A: Kali Linux (Attacker)

Machine B: Windows Server with DNS Role (Victim)

Step 1: Prepare DNS on Windows Server (Machine B)

- Install DNS role via Server Manager.

- Create a zone: example.lab (Primary Zone).

- Allow Zone Transfers (for testing only):

  Go to DNS Manager > Properties > Zone Transfers > 'Allow zone transfers'.

Step 2: Kali Linux (Machine A) - Launch Zone Transfer Attack

Use dnsrecon:

```
dnsrecon -d example.lab -t axfr
```

or dig:

```
dig @<Windows_Server_IP> example.lab AXFR
```

Expected: Full zone record dump (if allowed).

Step 3: Capture the Attack in Wireshark (Machine B)

- Start Wireshark on Windows Server.

- Filter with: dns or use:

```
ip.addr == <Kali_IP> and udp.port == 53
```

- Look for AXFR queries and responses.

Step 4: Enable DNS Logging in Windows Server

- Open Event Viewer > Applications and Services Logs > Microsoft > Windows > DNS-Server.

- Enable Analytical Logs (Right-click > Enable).

- Also monitor: C:\Windows\System32\Dns\dns.log (if logging enabled).

Step 5: Harden DNS on Windows Server (Post Test)

- Disable zone transfers (DNS Manager > Zone Properties).

- Enable recursion only for internal clients.

- Monitor logs regularly for suspicious queries.

Optional: Use Kali's Wireshark to sniff

- Run Wireshark on Kali.

- Capture outgoing queries.

- Useful for showing tool behavior like dnsrecon, dig, etc.