DNS ATTACKS AND SOC ANALYSIS

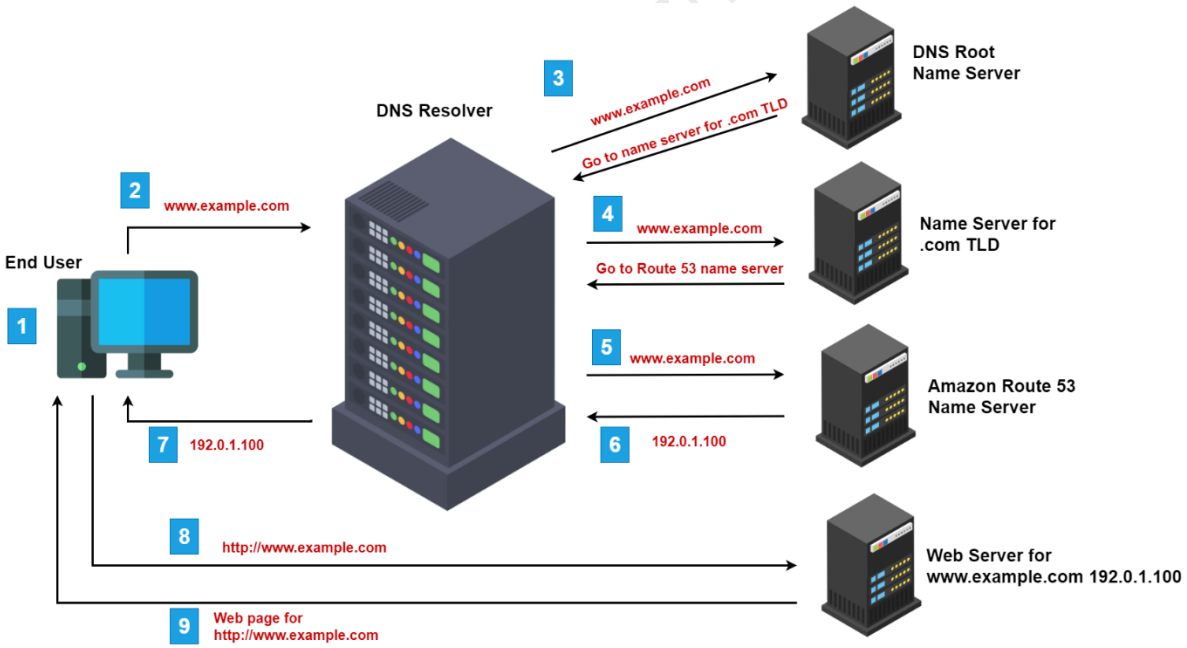
VAISHALI SHISHODIA

Introduction to DNS

The Domain Name System (DNS) is often referred to as the "phonebook of the internet." It translates human-readable domain names like www.google.com into machine-readable IP addresses such as 142.250.190.14. While DNS is a foundational service for internet communication, it is also a frequent target for cyberattacks. Understanding how DNS works and how it can be exploited is crucial for Security Operations Center (SOC) analysts.

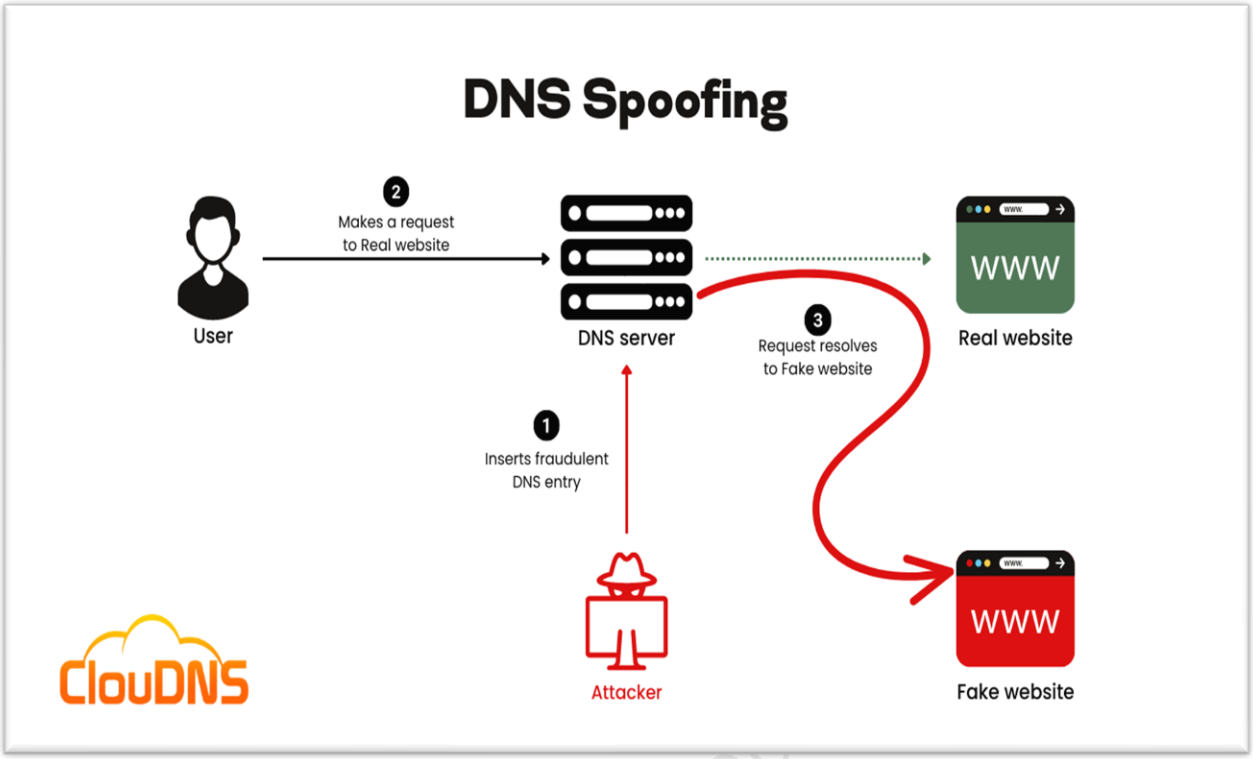
How DNS Works (Basic Flow):

1. You enter example.com into your browser.
2. Your device asks a **DNS resolver** (usually provided by your ISP or set manually, like Google's 8.8.8.8) to find the IP address.
3. If the resolver doesn't know it, it asks a **root DNS server**, which points to a **Top-Level Domain (TLD)** server (like .com).
4. The TLD server sends it to the **authoritative DNS server** for example.com.
5. That server gives back the IP address.
6. Your device can now connect to the site.

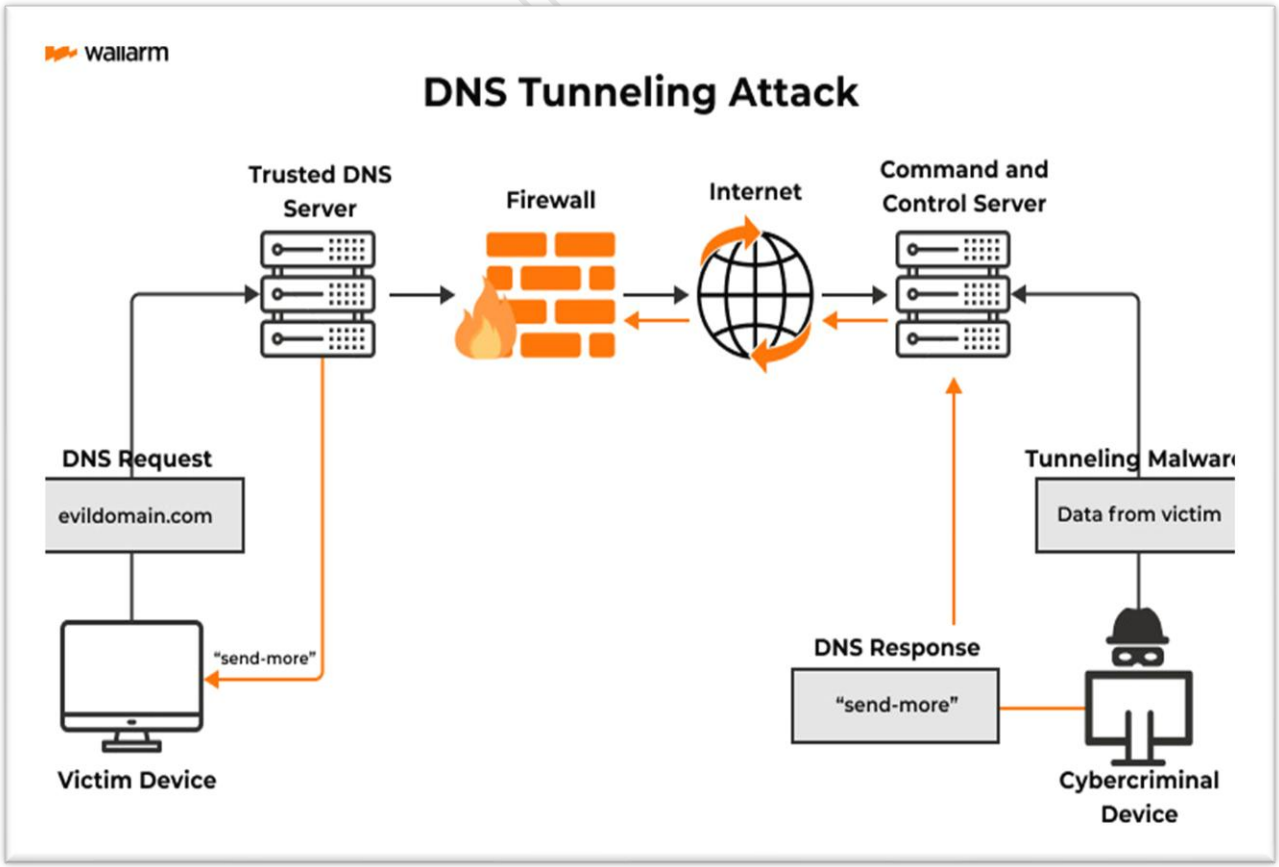


Common Types of DNS Attacks

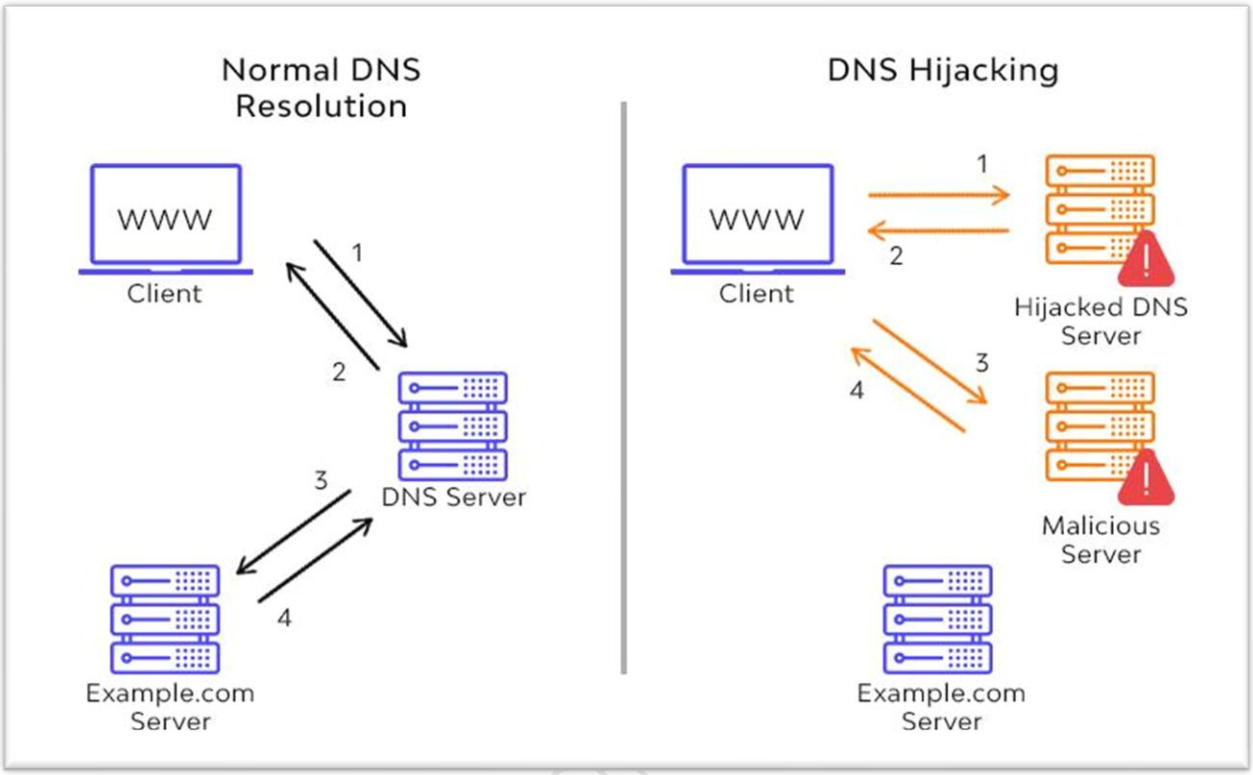
1. **DNS Spoofing / Cache Poisoning**
    - Attackers send fake DNS responses to a resolver, redirecting users to malicious websites.



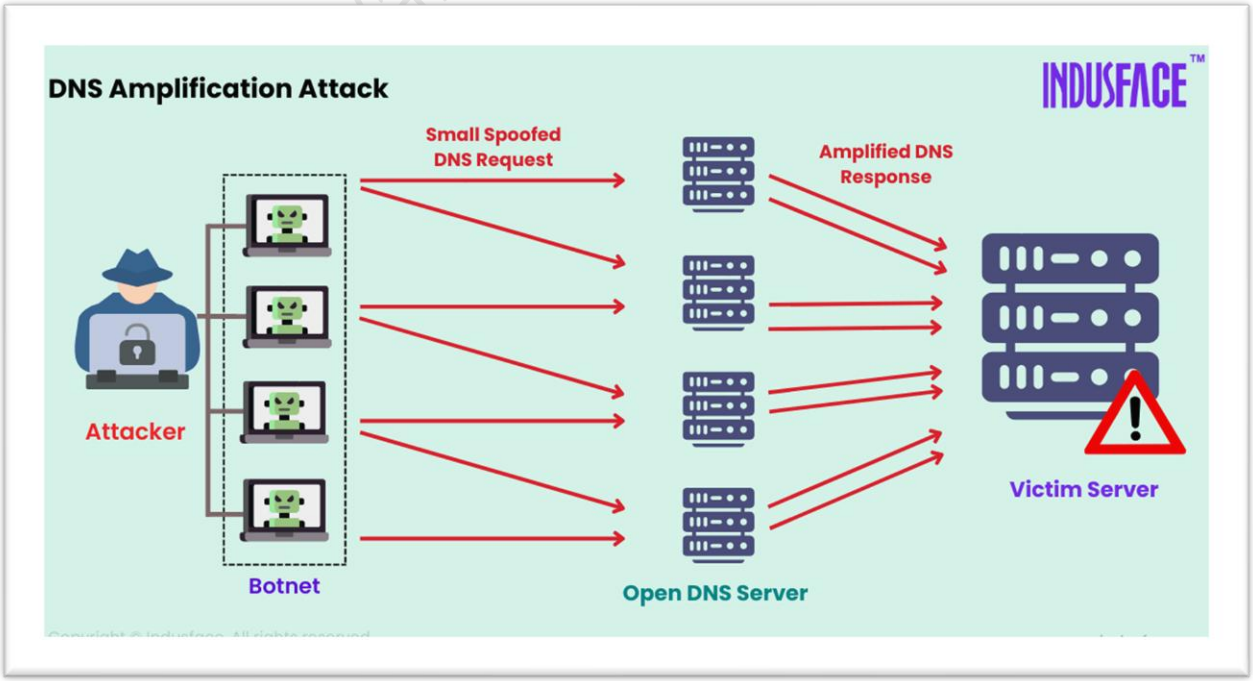
2. **DNS Tunneling**
    - Exfiltration of data or command-and-control communication via DNS queries, often bypassing firewalls.



3. **DNS Hijacking**
    - Modifies DNS settings or records to redirect traffic to malicious sites.



4. **DNS Amplification (DDoS)**
    - Attackers send forged DNS requests to open resolvers, overwhelming a target with amplified traffic.



5. **NXDOMAIN Attack**
    - Floods DNS resolvers with queries for non-existent domains to exhaust server resources.

SOC Analyst Workflow: Detection and Mitigation Steps

1. Log Collection and Monitoring

- **Tools**: SIEM (Splunk, ELK, QRadar), DNS server logs, endpoint logs
- **Indicators**:
    - High DNS query volume
    - Strange or rarely seen domain names
    - Repeated NXDOMAIN errors
    - Responses from unexpected IP addresses

2. Anomaly Detection

- **DNS Spoofing**: Identify mismatched IPs in responses
- **DNS Tunneling**: Look for long, encoded subdomains
- **DNS Amplification**: Unusual spikes in outbound DNS traffic
- **DNS Hijacking**: Unauthorized DNS server usage

3. Threat Intelligence Correlation

- Match observed domains and IPs with known threat intelligence feeds like VirusTotal, AlienVault OTX, and Cisco Talos.

4. Incident Triage and Investigation

- Use WHOIS, passive DNS analysis, and sandboxing
- Identify the scope of affected systems
- Verify whether the activity is malicious or benign

5. Mitigation Actions

For DNS Spoofing/Poisoning

- Use DNSSEC (validates integrity).
- Flush poisoned DNS caches.
- Switch to trusted DNS servers (e.g., Google, Cloudflare).

For DNS Tunneling

- Block the malicious domain/IP on firewalls.
- Enforce DNS inspection via firewalls/UTM.
- Disable unnecessary outbound DNS traffic (only allow trusted resolvers).

- Use tools like Pi-hole, Zeek, or Suricata for deep DNS packet inspection.

For DNS Hijacking

- Revert DNS settings on affected systems.
- Change credentials if router/router DNS was modified.
- Patch vulnerabilities that allowed hijack.

For DNS Amplification

- Block open DNS resolvers (don't run public DNS unless necessary).
- Rate limit DNS queries per IP on network appliances.
- Use anycast DNS to absorb and mitigate attack traffic**.**

6: Reporting and Documentation

- Document IOCs (Indicators of Compromise).
- Write a detailed incident report with timeline, detection method, actions taken, and recommendations**.**

Logs to Review for DNS Attacks

1. DNS server logs

- Examples: BIND logs, Windows DNS logs, Unbound
- Look For:
    - High query volume to unknown domains
    - Long or strange subdomains (e.g., base64-like strings)
    - Repeated NXDOMAIN responses (non-existent domains)
    - Responses from unexpected IPs (spoofed replies)
- Use: Detect spoofing, tunneling, hijacking, and DDoS

2. Firewall Logs

- Look For:
    - Unusual outbound DNS traffic
    - DNS queries to public resolvers (e.g., 8.8.8.8) bypassing internal DNS
    - DNS over port 53, 443, or 80 (DNS over HTTPS/TLS tunneling)
- Use: Identify unauthorized or suspicious DNS communication

3. SIEM Logs (Correlated Events)

- Look For:
    - DNS alerts triggered by custom correlation rules

    - Queries to blacklisted domains
    - Enriched DNS logs (with threat intel correlation)
- Use: Centralized view for alerting, triaging, and historical search

4. **Endpoint Detection and Response (EDR) Logs**
    - Look For:
        - Processes generating DNS queries (e.g., powershell, cmd.exe)
        - Malware or scripts invoking DNS calls
    - Use: Detect DNS tunneling or malware using DNS as C2
5. **Proxy Logs / Web Gateway Logs**
    - Look For:
        - Domains queried that resolve to shady IPs but never visited by browser
        - DNS over HTTPS traffic (DoH)
    - Use: Detect stealthy DNS activity bypassing DNS monitoring
6. **Network Traffic Logs (PCAP / NetFlow / Zeek)**
    - Look For:
        - DNS queries/responses on unusual ports
        - High frequency DNS requests from single host
        - Large payloads in DNS queries (sign of tunneling)
    - Use: Deep packet inspection, tunneling and anomaly detection
7. **Threat Intelligence Logs / Feeds**
    - Look For:
        - Match between queried domains/IPs and known malicious indicators
    - Use: Confirm domain/IP is part of a known campaign or malware
8. **Router/Network Device Logs**
    - Look For:
        - DNS configuration changes (DNS hijacking)
        - Unexpected external DNS resolver usage
    - Use: Trace DNS changes and unauthorized traffic redirection
9. **System Event Logs (Windows/Linux)**
    - Look For:
        - DNS client configuration changes

    - Script execution or scheduled tasks making DNS queries
- Use: Detect compromise or misconfiguration that leads to DNS abuse

Key Indicators of DNS-Based Attacks

Indicator	Possible Attack Type
Long/randomized subdomains	DNS Tunneling
Sudden spikes in DNS traffic	DNS Amplification/DDoS
External DNS queries from hosts	DNS Hijacking/Tunneling
High NXDOMAIN response count	NXDOMAIN Attack
DNS responses from unexpected IPs	DNS Spoofing/Poisoning
DNS over non-standard ports	Tunneling or Evasion

Recommended Tools for DNS Monitoring and Defense

Tool	Use Case
Wireshark	Packet-level DNS inspection
Zeek (Bro)	DNS behavior analysis
Splunk	DNS log analysis via SIEM
Pi-hole	DNS-level blocklisting
Security Onion	DNS log correlation and detection
Cisco Umbrella	DNS-layer protection
Suricata	Detect DNS tunneling and anomalies