Session 13 DNS Traffic Analysis

1. What is DNS?

Domain Name System (DNS) resolves domain names to IP addresses.
Acts like the internet's phonebook.

2. Why Analyze DNS Traffic?

Attackers misuse DNS for malicious activities:

Data exfiltration (hiding stolen data in DNS queries).
Command and Control (C2) communication.
DNS tunneling (covert channels inside DNS traffic).

Normal DNS is predictable → anomalies stand out.

3. Common DNS Query Types:

A Record → IPv4 address.
AAAA Record → IPv6 address.
MX Record → mail servers.
NS Record → authoritative name servers.
PTR Record → reverse lookup (IP → domain).
TXT Record → text data, often abused for hiding data.

4. Indicators in DNS Traffic:

Suspicious domains (random strings, long lengths).
High frequency queries to the same domain.
Excessive or uncommon record types (TXT, NULL).
NXDOMAIN responses (non-existent domains) → often from DGAs.

5. Tools for DNS Traffic Analysis:

Wireshark → filter with dns.
tcpdump → tcpdump -i eth0 port 53.
SIEM tools (Splunk, ELK, QRadar).
Threat intel + DNS logs from security providers.

6. Useful Wireshark Filters:

dns → all DNS traffic.
dns.flags.response == 0 → only queries.
dns.flags.response == 1 → only responses.
dns.qry.name == "example.com" → specific domain.

7. SOC Analyst Perspective:

Look for unusual query patterns and beaconing.
Check against threat intelligence feeds.
Pay attention to failed lookups (NXDOMAIN).
Correlate DNS activity with other logs (firewall, proxy).