Identifying Hosts: DHCP, NetBios, and Kerberos

Identifying Hosts:

One of the Best methods is identifying the hosts and users on the network to decide the investigation's starting point and list the hosts and users associated with the malicious traffic/actively

Protocols that can be used in Host and Uses Identification.

- Dynamic Host Configuration Protocol (DHCP) traffic
- NetBIOS (NBNS) traffic
- Kerberos traffic

DHCP Analysis

What DHCP (Dynamic Host Configuration Protocol) is:

DHCP is how most devices automatically get:

- an IP address
- subnet mask (tells what is local vs remote)
- default gateway (our router's IP)
- DNS servers
- lease time (how long the device can keep that IP before renewing

How it automatically get these informations

- When our device joins a network, it usually doesn't know its IP yet.
  So it does 4 step conversation with DHCP server

  - DHCP Discover → Client Broadcast (Is there a DHCP I need address)
  - DHCP offer → DHCP server reply (give us IP, ...)
  - DHCP Request → Client requests offer
  - DHCP ACK → Server confirms

When we use DHCP

- Most of the time (for almost all networks)
- When there are many devices and don't want manual setup
- When devices come and go
- When we want to avoid IP conflicts

Where:

- Our routers are usually the DHCP server

what actually happens in DHCP:

1) User or Client joins the network (Wi-Fi)
   → at this point it may have no IP address
2) Client Broadcasts DHCP Discover
3) DHCP server sends an offer
4) Client Sends DHCP request
5) Server sends DHCP ACK

On the public Wifi, what DHCP does?

When we join the Wifi, the DHCP server on that network gives our device:

- Our local/private IP
- Subnet mask
- Default gateway (the router's local IP) ← this is the internet access
- DNS server
- Lease Time

So DHCP doesn't give us the internet IP. It gives us the settings that let us reach the internet through the gateway

After DHCP:

- Our device sends internet traffic
- Because those destinations are not local, our device forwards packets to the default gateway it got from DHCP
- The router uses NAT to translate our private IP into the router's public IP
- Website see the public IP of the router, not our private IP

Wireshark

Global search dhcp / bootp

DHCP Request : packet contain the host name info

dhcp.option.dhcp == 3

DHCP ACK : packet represent and accepted requests

dhcp.option.dhcp == 5

DHCP NAK: packet represent denial requests

dhcp.option.dhcp == 6

DHCP options :

Request
- Option 12 (Hostname) → the device name it reports
- Option 50 (Requested IP) → the IP it's asking for
- Option 51 (Lease Time) → how long it wants the IP
- Option 61 (Client ID) → includes MAC, or other

dhcp.option.hostname contain "keyword"

ACK
- Option 15 (Domain Name)
- Option 51 (Lease Time)

NAK Option 56 (Message)