Day 17

Exploitation Analyst

NTP Protocol:

YouTube:

https://youtu.be/BAo5C2qbLq8?si=rNvP42wgATdm7IV2

What is NTP?

NTP (Network Time Protocol) is a protocol used to synchronize the clocks of computers and network devices over a network (usually the internet). It ensures that all systems in a network agree on the same time.

- Port: UDP 123
- Use Case: Accurate timestamps for logs, authentication, encryption, and scheduling.

What if it is not present?

1. Clock Drift: System clocks will slowly drift out of sync over time.
2. Authentication Errors: Time-sensitive protocols (like Kerberos, SSL/TLS, JWT tokens) may fail if clocks differ.
3. Log Confusion: Logs from different systems will have mismatched timestamps — making investigation, auditing, and correlation difficult.
4. Cron/Scheduled Jobs: May run at wrong times.
5. Certificate Validation Issues: SSL certs may appear "expired" or "not yet valid" if time is wrong.

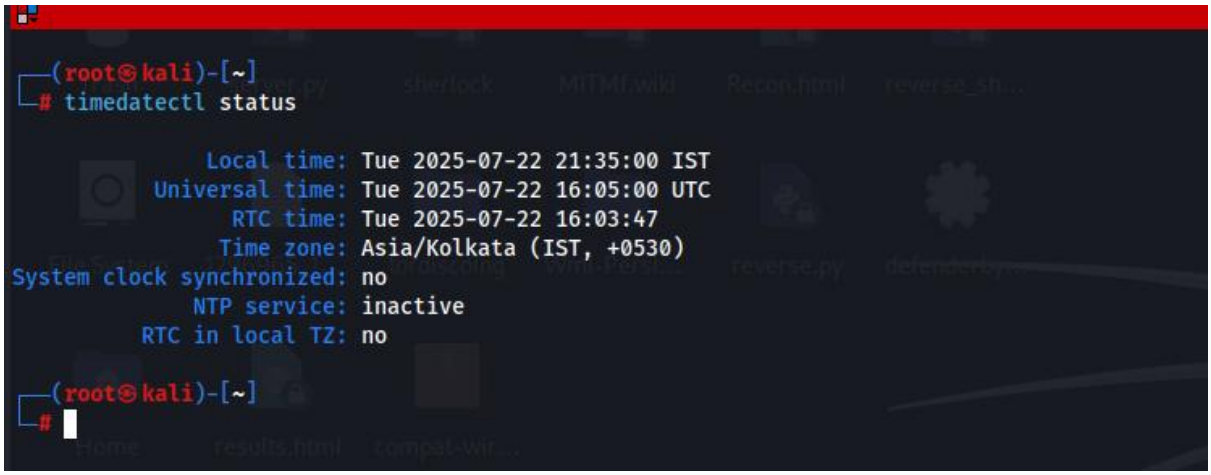
How it works?

1. Uses a Hierarchical System (Stratum Levels)
    a. NTP uses a layered structure.
    b. Stratum 0: High-precision reference clocks (atomic, GPS).
    c. Stratum 1: Primary time servers directly connected to Stratum 0.
    d. Stratum 2+: Secondary servers sync from above levels.
    e. Lower stratum = more accurate.
2. Clients Connect to Higher Stratum Servers
    a. Each client or device syncs with a server of lower (closer to 0) stratum level.
    b. Stratum value increases by 1 for every level away from the reference clock.
3. Accuracy Decreases Down the Hierarchy
    a. A Stratum 3 server syncing from a Stratum 2 will be slightly less accurate.
    b. This minimizes load on top-tier servers and keeps the network scalable.
4. NTP Uses UDP Port 123 (Not 23)
    a. Devices communicate over UDP port 123 to exchange time info.
    b. It's connectionless and lightweight, ideal for frequent time updates.
5. Router or Local Server Can Act as NTP Relay
    a. Your router can sync with an internet NTP server (e.g., Stratum 2 or 3).
    b. Then it acts as a local NTP server (Stratum 4) for LAN devices.
6. LAN Devices Sync with the Router

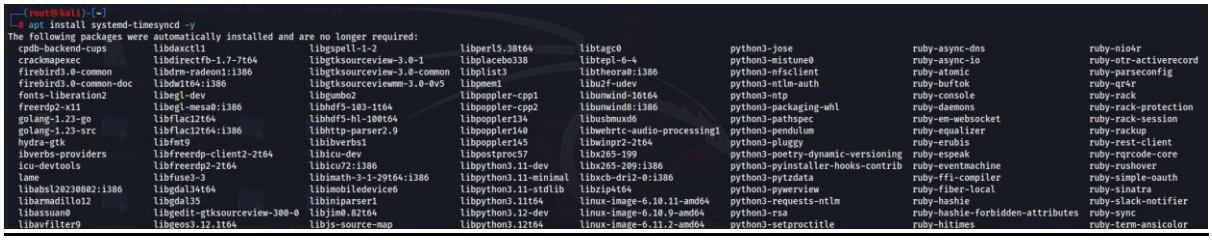
a. Devices on your network get their time from the router (or local NTP server), avoiding direct internet dependency.

Check if your Kali Linux has NTP active or not?

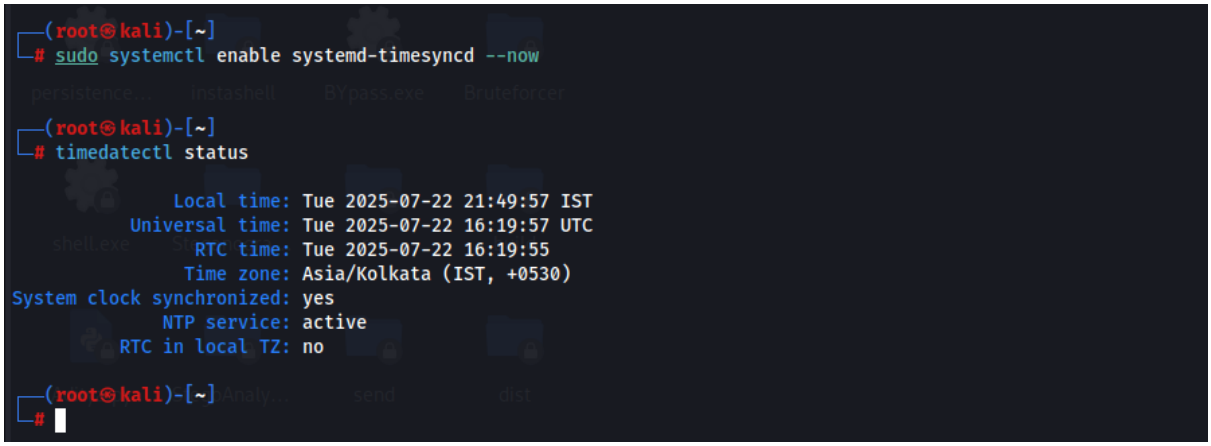
Following command will help in do so: timedatectl status. Clearly, NTP is not active.



So how will we activate it? We will first install: incase it is not installed.



Then,



We can see that it is active again.

--The End--