

# 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.

```
(root@kali)-[~]
# timedatectl status

Local time: Tue 2025-07-22 21:35:00 IST
Universal time: Tue 2025-07-22 16:05:00 UTC
RTC time: Tue 2025-07-22 16:03:47
Time zone: Asia/Kolkata (IST, +0530)
System clock synchronized: no
NTP service: inactive
RTC in local TZ: no

(root@kali)-[~]
```

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

```
(root@kali)-[~]
# apt install systemd-timesyncd -y

The following packages were automatically installed and are no longer required:
cpdb-backend-cups libdirectfb-1.7-7t64 libgspell-1-2 libperl5.38t64 libtagc0 python3-jose ruby-async-dns ruby-nio4r
crackmapexec libdirectfb-1.7-7t64 libgtksourcview-3.0-1 libplacebo338 libtepl-6-4 python3-mistune0 ruby-async-io ruby-otr-activerecord
firebird3.0-common libdrm-radeon1:lib386 libgtksourcview-3.0-common libplist3 libtheora0:lib386 python3-nfsclient ruby-atomic ruby-parseconfig
firebird3.0-common-doc libdw1t64:lib386 libgtksourcviewmm-3.0-0v5 libplist3 libtheora0:lib386 python3-ntlm-auth ruby-buftok ruby-qtr
fontconfig libfontconfig2 libdw1t64:lib386 libgtksourcviewmm-3.0-0v5 libplist3 libtheora0:lib386 python3-ntp ruby-console ruby-rack
freerdp2-x11 libegl-mesa0:lib386 libhdf5-103-1t64 libpoppler-cpp1 libunwind-16t64 python3-packaging-whl ruby-daemons ruby-rack-protection
golang-1.23-go libflac12t64 libhdf5-bl-100t64 libpoppler-cpp2 libusbmuxd0 python3-pathspec ruby-em-websocket ruby-rack-session
golang-1.23-src libflac12t64:lib386 libhdf5-bl-100t64 libpoppler140 libwrtc-audio-processing1 python3-pendulum ruby-equalizer ruby-rackup
hydra-gtk libfontconfig2 libhdf5-bl-100t64 libpoppler145 libwinpr2-2t64 python3-pluggy ruby-erubis ruby-rest-client
ibverbs-providers libfreerdp-client2-2t64 libicu-dev libpostproc57 libx265-199 python3-poetry-dynamic-versioning ruby-espeak ruby-rqrcode-core
icu-devtools libfreerdp2-2t64 libicu72:lib386 libpython3.11-dev libx265-209:lib386 python3-pyinstaller-hooks-contrib ruby-eventmachine ruby-rushover
lame libfuse3-3 libmath-3-1-20t64:lib386 libpython3.11-minimal libx265-209:lib386 python3-pytda ruby-single-auth
libbss1202:lib386 libmath-3-1-20t64:lib386 libpython3.11-stdlib libzip4t64 python3-pyview ruby-sinatra ruby-sinatra
libarmadillo12 libgdal35 libbinparser1 libpython3.11t64 linux-image-6.10.11-amd64 python3-requests-ntlm ruby-hashie ruby-slack-notifier
libassuan libgdi1-gtksourceview-300-0 libjlm0.82t64 libpython3.12-dev linux-image-6.10.9-amd64 python3-rsa ruby-hashie-forbidden-attributes ruby-sync
libfilters libgdi1-gtksourceview-300-0 libjlm0.82t64 libpython3.12t64 linux-image-6.11.2-amd64 python3-setproctitle ruby-hlines ruby-term-ansicolor
```

Then,

```
(root@kali)-[~]
# sudo systemctl enable systemd-timesyncd --now

(root@kali)-[~]
# timedatectl status

Local time: Tue 2025-07-22 21:49:57 IST
Universal time: Tue 2025-07-22 16:19:57 UTC
RTC time: Tue 2025-07-22 16:19:55
Time zone: Asia/Kolkata (IST, +0530)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no

(root@kali)-[~]
```

We can see that it is active again.

--The End--