NTP Enumeration

The Network Time Protocol (NTP) is a widely used protocol for synchronizing time across networks. While NTP is essential for maintaining accurate timekeeping, it can also be a potential security risk if not properly configured.

As an Attacker we cam query NTP server to gather valuable information such as:

- List of hosts connected to NTP server
- Clients IP addresses in a network, their system names and OSs
- Internal IPs can also be obtained if NTP server is in the DMZ

NTP Enumeration with nmap

- Let us start NTP enumeration with nmap.

```
sudo nmap -Pn -sU -p 123 --script ntp-info,ntp-monlist <TARGET>
```

- Next we have ntpq and ntpdc command line tool through which we can monitor NTP daemon ntpd operations and determine its performance.

```
ntpq -c readlist <IP_ADDRESS>
ntpq -c readvar <IP_ADDRESS>
ntpq -c readvar <IP_ADDRESS>
ntpq -c associations <IP_ADDRESS>
ntpdc -c monlist <IP_ADDRESS>
ntpdc -c listpeers <IP_ADDRESS>
ntpdc -c sysinfo <IP_ADDRESS>
```

- Use NTPtrace to trace the chain of NTP servers back to the primary source.

```
ntptrace [-vdn] [-r retries] [-t timeout] [server]
```
