- Filename: eccouncil-ceh31250-v11-4-5-1-ntp-enumeration.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: NTP Enumeration
  ==

NTP Enumeration

Objectives:

- Explain the function of the NTP service
- Describe the common attributes of the NTP service
- Employ NTP commands and tools to reveal NTP service versioning, hostname, and IP address

---

- What does NTP do for us?

  - Sync time/date settings

    - Why is this important?

      - Many network services utilize time as a metric for admin/security

- What are some of the attributes of NTP that we need to be aware of?

  - UDP port 123

    - `sudo nmap -sU -n -Pn -p 123 target_IP`

  - Maintain time within 10ms
  - Can achieve time accuracy of 200 micro seconds

- Enough of the pleasantries, how do we enumerate NTP?

- *shodan search for NTP for good target(s)*

  - ntpdate

    - `-d` (debug info)

  - ntptrace

    - Trace NTP servers to source

      - Could help map out network resources

  - ntpdq & ntpdc

    - `host target_IP`
    - `version`
    - `peers`