- Filename: eccouncil-ceh31250-v12-4-6-1-smtp-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: SMTP Enumeration
  ==

SMTP Enumeration

Objectives:

- Use common SMTP commands and tools to enumerate valid user accounts

---

- SMTP is used to send email, so how can that be leveraged for enumeration purposes?
  - Users
  - email addresses
- How?
  - SMTP server commands
    - VRFY
    - EXPN
    - RCPT TO
- How to we make use of these commands for enumeration?
  - Login directly
    - netcat
    - Telnet
  - `smtp-user-enum`
    - `-U/-u` User list / single user
    - `-t` Target mail server (IP)
    - `-M` Mode (VRFY,EXPN,RCPT TO)
      - `smtp-user-enum -U /usr/share/seclists/Names/names.txt -t <targetIP>`
  - Metasploit
    - `search smtp aux`
    - `auxiliary/scanner/smtp/smtp_enum`
  - Nmap
    - `ls /usr/share/nmap/scripts | grep smtp`
    - `sudo nmap -n -Pn -p 25 --script smtp-enum-users.nse <targetIP>`