- Filename: eccouncil-ceh31250-v10-4-1-1-enumeration.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Enumeration
- Description: In this episode, Daniel and Zach define and demonstrate performing enumeration during and engagement. Here they will explore the types of things you commonly target during enumeration as well as performing enumeration on services like NetBIOS, SMTP, and SNMP.

==========

Enumeration

- **What is enumeration?**
  - The active gathering of specific target info
    - Usernames/Groups
    - Network resources and shares
    - Services
- **How is this typically done?**
  - Scanning tools
  - Manually
- **What specific things are we targeting?**
  - Could be a myriad of things, but often includes...
    - NetBIOS
    - SNMP
    - LDAP
    - NTP
    - SMTP
    - DNS
- **Can you take us through some enumeration examples?**
  - SNMP
    - Management Information Base(MIBs)
      - OID (Object IDentifier)
    - `snmp-check 10.0.0.200` (Kali)
    - MIB Browser (WinServer)
  - NetBIOS
    - `net view \\srv2012`
    - `enum4linux -a -u administrator -p Eagle001Claw 10.0.0.200 > smbEnum.txt`
    - SysInternals
      - `psinfo`
      - `psfile`
      - `pslist`
      - `psloggedon`
  - SMTP
    - `VRFY`
    - `EXPN`
    - `RCPT TO:`
  - Other
    - `finger`
    - VoIP/SIP (Session Initiation Protocol)

- svmap
- auxiliary/scanner/sip/enumerator