- Filename: eccouncil-ceh31250-v12-4-2-1-netbios-and-smb-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: NetBIOS and SMB Enumeration
  ==

NetBIOS and SMB Enumeration

Objectives:

- Name the information details that can be obtained during NetBIOS Enumeration
- Perform NetBIOS Enumeration using the nbtstat CLI tool
- List other common NetBIOS Enumeration tools

- NetBIOS
  - Used by Windows for
    - File sharing
    - Printer sharing
  - nbtstat (Windows)
    - `-c` Cache
    - `-n` Names
  - nbtscan (Linux)
    - `-r target_IP`
    - `-v` for more output
  - nmap
    - `nmap -sV --script nbstat.nse <target_IP>`
- SMB
  - File sharing
  - CIFS (Common Internet File System)
  - Can use TCP directly
    - Port 445
  - Can use UDP/TCP
    - UDP 137,138
    - TCP 137,139
      - NetBIOS over TCP/IP
  - Tools
    - nmap
      - `nmap -A -T5 -n -Pn -p 445 <target_IP>`
    - net view
      - `net view \\target_IP /ALL`
      - `net view example.com`
    - smbclient
      - `smbclient -L //target_name|IP>`
    - enum4linux
      - `enum4linux -S <target_IP>`
    - `smblient //target/share`
      - We have read/write to this dir!
      - This could be useful for compromise later (web apps)