

- Filename: eccouncil-ceh31250-v11-4-2-1-netbios-and-smb-enumeration.md
 - Show Name: CEHV11 (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 -t4 -n -Pn -p 445 target_IP`
 - net view
 - `net view \\target_IP /ALL`
 - `net view example.com`