

- Filename: eccouncil-ceh31250-v11-3-15-1-target-os-identification-techniques.md
  - Show Name: CEHV11 (312-50)
  - Topic Name: Recon Techniques - Scanning
  - Episode Name: Target OS Identification Techniques
- =====

## Target OS Identification Techniques

### Objectives:

- Define OS Discovery/Banner Grabbing
  - Distinguish between Active and Passive Banner Grabbing techniques
  - Use nmap, wireshark, and unicornscan to identify target host's operating system using various techniques
- 

- Kathy
  - nmap
    - -O
      - Don't forget IPv6 (-6)
    - Services may reveal OS
      - port 445 open
        - `nmap --script smb-os-discovery.nse <targetIP>`
  - unicornscan
    - `unicornscan <targetIP> -iV`
  - Countermeasures
    - Disinformation Campaign
    - Turn off banners
    - Hide file extensions