- Filename: eccouncil-ceh31250-v11-3-7-1-nmap-stealth-scan.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: TCP Stealth Scan
  ==

Nmap: TCP Stealth Scan

Objectives:

- Use nmap to perform a TCP Stealth scan to enumerate ports states and service details
- Explain the pros and cons when utilizing this type of scan

- What is a Stealth scan?
  - AKA SYN Scan and Half-Open Scan
  - Utilizes part of the TCP 3-way handshake
- Can you show us how to perform a Stealth scan with nmap?
  - Demo
- Are there any advantages and/or disadvantages to using this type of scan?
  - Advantages
    - Much quieter than TCP Connect scans
    - Faster
  - Disadvanages
    - Now detectable by IDS/IPS
    - Requires admin privs