- Filename: eccouncil-ceh31250-v12-3-6-1-stealth-scan.md
- Show Name: CEHv12 (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 only a part of the TCP 3-way handshake
- Can you show us how to perform a Stealth scan with nmap?
    - `sudo nmap -sS 10.6.6.11`
    - `sudo hping3 -8 1-65535 -S 10.6.6.11`
        - Use *Wireshark* to see an open/closed port
            - `tcp.port == 8080`
- 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