- Filename: eccouncil-ceh31250-v11-3-6-1-nmap-tcp-connect-scan.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: TCP Connect Scan
  ==

Nmap: TCP Connect Scan

Objectives:

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

- What is a TCP Connect scan?
  - Utilizes the TCP 3-way handshake in an attempt to verify whether a port is open or closed
  - Useful for scans run by users without administrative Privilege
- Is there a way for us to see that process? (The 3-way handshake)
  - Use Wireshark to capture the 3-way handshake of the scan
- Are there any advantages and/or disadvantages to using this type of scan?
  - Advantage
    - Relatively certain of port state
    - No need for admin privs
  - Disadvanages
    - Noisy, prone to detection
    - Slow
    - Slight possibility of crashing services