- Filename: eccouncil-ceh31250-v12-3-5-1-tcp-connect-scan.md
- Show Name: CEHv12 (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?
  - aka "Full Open"
  - 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
- Run a TCP Connect Scan
  - `nmap -sT 10.6.6.11`
- What is the TCP 3-way handshake?
  - Proper establishment of a TCP connection
    - SYN --> SYN/ACK --> ACK --> CONNCETION ESTABLISHED!
- Is there any way to see the 3-way handshake process?
  - Wireshark
- 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