- Filename: eccouncil-ceh31250-v12-3-12-1-scan-optimizations.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Scan Optimizations
  ==========

Scan Optimizations

Objectives:

- Customize nmap scan attributes in order to optimize or reduce scan completion times
- List common techniques for increasing scan efficiency

- Define what we mean when we say 'Optimized'
    - Running scan options that we need to run
    - Not running scans options that we don't need to run
    - Running scans as fast as possible
- How do we determine what scans we do/don't need to run?
    - Usually a 'reductionist' model
        - Start by casting the widest net, then increase focus
- Can you show us what that would look like?
    - Demo (scanme.nmap.org)
        - `-n`
        - `-Pn`
        - `-F`
        - `-p` (set a small port range, or ONLY look for specific ports)
        - `--disable-arp-ping` or `--send-ip`
- Are there any other 'speed' tricks with nmap?
    - `-T1-T5`