- Filename: eccouncil-ceh31250-v12-3-4-1-port-and-service-scanning.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Port and Service Scanning

==

Port and Service Scanning

Objectives:

- Define port and service scans
- Describe the purpose of performing a port and service scan
- Identify the protocols commonly employed during a port/service scan

---

- What is a port scan? What is a service scan? How do they differ?
    - Port scan
        - Find ports that are open
            - Scan a single host
        - `nmap -T5 -n -Pn -p- 10.6.6.11 -o nmap_10.6.6.11.txt`
    - Service scan
        - Discover the service running on the open port
            - `-sV`
- What is the purpose of doing a port/service scan
    - Service may have vulnerability
- Are there any common ports and/or services that we should be familiar with when performing port/service scans?
    - Comprehensive list of ports/services @ `/usr/share/nmap/nmap-services`
        - `grep -v ^# nmap-services | grep tcp | less`