- Filename: eccouncil-ceh31250-v11-3-5-1-port-and-service-scanning.md
- Show Name: CEHv11 (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
    - Service scan
        - Discover the service running on the open port
- 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?
    - Show scan of Metasploitable
    - 21:FTP
    - 22:SSH
    - 23:Telnet
    - 25:SMTP
    - 53:DNS
    - 80:HTTP
    - 110:POP3
    - 111:RPC
    - 137-139:NETBios
    - 143:IMAP
    - 161:SNMP (TCP/UDP)
    - 443:HTTPS
    - 445:SMB/CIFS (Server Message Block / Common Internet File System)
    - 3306:mysql
    - 8080:proxy
    - 6667:irc