- Filename: eccouncil-ceh31250-v11-3-11-1-nmap-udp-scan.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: UDP Scan
  ==========

Nmap: UDP Scan

Objectives:

- Describe the process of an UDP scan
- Use nmap to perform an UDP scan to enumerate ports states and service detail
- Explain the pros and cons when utilizing this type of scan

- Kathy
  - Connection-less protocol
    - No 3-way handshake
      - Target response is different than TCP
- So how so we determine OPEN and CLOSED ports with a UDP scan?
  - CLOSED
    - Target responds with *ICMP Port Unreachable* message
  - OPEN
    - Target DOESN'T RESPOND!
- Time for a demo!
  - `sudo nmap -sU -p 22,69 <metasploitable-IP> --packet-trace`
    - See the SENT packets
    - See the *Port Unreachable* message for port 69
    - See the Resend to port 69
- What are our Pros/Cons with this type of scan?
  - It's slow
  - Needs root privs
  - That said, you may catch malicious traffic of an attacker using UDP