- Filename: eccouncil-ceh31250-v12-3-10-1--udp-scan.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: UDP Scan
  ==========

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

- How is UDP differnet from TCP?
    - 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
    - `sudo hping3 -2 10.6.6.23 -p 80`
- 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