- Filename: eccouncil-ceh31250-v11-3-9-1-nmap-ack-scan.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: ACK Scan
  ==========

Nmap: ACK Scan

Objectives:

- Describe the process of an ACK scan
- Use nmap to perform an ACK scan to enumerate ports states and map firewall rules
- Explain the pros and cons when utilizing this type of scan

- Kathy
  - Used in attempt to map firewall/filtering rules for target
- How is that done?
  - Send an ACK and random sequence number
    - NO RESPONSE = filtered
    - RST = not filtered
      - Only works on RFC 793 compliant stacks
  - `nmap -sA <targetIP>`
- I understand there are some variations to this type of scan?
  - TTL-based
    - If TLL values are lower than 64
    - `nmap -ttl 70 <targetIP>`
      - Learn target's TTL through packet inspection
        - `--packet-trace`
        - `--reason`
  - Window-based
    - All about the window size
      - If target returns
        - RST + Non-Zero Window = Port OPEN
        - RST + Zero Window = Port CLOSED
        - No Response = FILTERED
          - Can't really trust this scan as the OS may not be compliant
            - See `man nmap` and search for `-sW`