- Filename: eccouncil-ceh31250-v12-3-9-1-ack-scan.md
- Show Name: CEHv12 (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

- What is an ACK scan?
    - Helps us answer the firewall questions
        1. Is there a firewall?
        2. What is the firewall filtering?
        3. Stateless or Stateful?
- How does it work??
    - `nmap -sA <targetIP>`
    - Send an ACK and random sequence number
        - Open|Closed should respond with RST
            - Scenario 1: No Firewall
        - Reports *100 unfiltered tcp ports (reset)*
            - Scenario 2: Stateless Firewall
                - Reports
            - *98 filtered ports (no-response)*
            - 2 *unfiltered* ports
                - Can't tell if ports are Open|Closed because both respond with RST
            - Scenario 3: Stateful Firewall
        - Reports *100 filtered tcp ports (no-response)*
- I understand there are some variations to this type of scan?
    - **TTL-based**
        - Determine TTL values of ACK scan with `--packet-trace`
            - Define ACK scan TTL value higher
                - If TLL values are lower than 64
                    - `nmap -sA --ttl 70 <targetIP>`
    - **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`
                    - `sudo nmap -sW -F <targetIP> --packet-trace`