- Filename: eccouncil-ceh31250-v11-3-12-1-nmap-sctp-init-and-cookie-echo-scans.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: SCTP INIT and COOKIE ECHO Scans
  ==========

Nmap: SCTP INIT and COOKIE ECHO Scans

Objectives:

- Describe the process of an SCTP INIT and COOKIE ECHO scans
- Use nmap to perform an SCTP INIT and COOKIE ECHO scans to enumerate port states and service detail
- Explain the pros and cons when utilizing these types of scans

---

NOTES for DANIEL
Can run an SCTP server with NCAT using `--sctp` switch
Capture SCTP traffic with Wireshark for demo

- Kathy
  - How SCTP works (*4-way handshake*)
    - Host1 >----INIT-----> Host2
    - Host1 <--INIT-ACK---< Host2
    - Host1 >-COOKIE-ECHO-> Host2
    - Host1 <-COOKIE-ACK--< Host2
- Now that we have the basics down, tell us about the INIT scan.
  - `-sY` option
  - Attacker >----INIT-Chunk----> Target
  - Attacker <--INIT+ACK-Chunk--< Target
    - Port is **OPEN**
  - Attacker >----INIT-Chunk----> Target
  - Attacker <---ABORT-Chunk----< Target
    - Port is **CLOSED**
    - Port is **FILTERED** if
      - No response
      - ICMP Unreachable
- COOKIE ECHO scan
  - `-sZ` option
    - "Stealthy"
      - Some non-stateful firewalls can't block
        - Advanced IDS/IPS *can* detect
      - Sends COOKIE ECHO Chunk to target
        - Target doesn't respond
          - Port is **OPEN**
        - Target responds with ABORT Chunk
          - Port is **CLOSED**