- Filename: eccouncil-ceh31250-v11-3-8-1-nmap-inverse-tcp-xmas-and-maimon-scans.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: Inverse TCP and XMAS Scans
  ==

Nmap: Inverse TCP, XMAS, and Maimon Scans

Objectives:

- Use nmap to perform an Inverse TCP scan to enumerate port states and service details
- Use nmap to perform an XMAS scan to enumerate port states and service details
- Explain the pros and cons when utilizing these types of scans

---

- What is the concept behind an Inverse TCP scan? How does this work, theoretically?
  - 'Hacking' TCP
    - Firewalls/IPS can block SYN packets
      - How could we get around this?
        - Probe with other flags
          - FIN
          - URG
          - PSH
          - NULL
    - OPEN ports don't respond to FIN, URG, PSH, or NULL
    - CLOSED ports respond with RST
- How do we perform these types of scans?
  - `-sF` (FIN)
  - `-sN` (NULL)
  - `--scanflags URGACKPSHRSTSYNFIN`
  - SYN/ACK probe
- How about this 'Christmas' scan thing?
  - Scans using the FINURGPSH flags
    - You could also accomplish this with
      - `--scanflags URGPSHFIN`
- As if 'Christmas' scans weren't fun enough, we also need to be aware of 'Maimon' scans?
  - Basically the same trick, but with different flags
    - FIN/ACK probe
      - `-sM`
      - `--scanflags ACKFIN`
- Are there any issues with using these scans that we should take in to consideration?
  - Only works with BSD-Compliant Network Stacks

- Adherence to RFC 793
    - Windows and Linux will scoff