- Filename: eccouncil-ceh31250-v12-3-7-1-inverse-tcp-xmas-and-maimon-scans.md
- Show Name: CEHv12 (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?
    - FIN Scan
        - `-sF`
        - `sudo hping3 -8 8888-8890 -F 10.6.6.11`
    - NULL Scan
        - `-sN`
        - `sudo hping3 -c 2 -V -p 8888 -s 4444 -Y 10.6.6.11`
    - Custom Scan Flags
        - `--scanflags URGACKPSHRSTSYNFIN`
        - `sudo hping3 --scan 1-65535 -U -A -P -R -S -F 10.6.6.11`
    - SYN/ACK probe
        - `--scanflags ACKSYN`
        - `sudo hping3 -8 1-65535 -S -A 10.6.6.11`
- How about this 'Christmas' scan thing?
    - Uses the **FINURGPSH** flags, "lighting the packet up like a Christmas tree."
        - You could also accomplish this with
            - `--scanflags URGPSHFIN`
            - `sudo hping3 -c 2 -V -p 8888 -s 4444 -X 10.6.6.11`
- As if 'Christmas' scans weren't fun enough, we also need to be aware of 'Maimon' scans?
    - Named after discoverer, Uriel Maimon
        - RFC 793 states that FIN/ACK probe should force target to generate a RST for both open and closed ports
            - Uriel found that many BSD-derived systems drop the packet if port OPEN

  - Basically the same trick, but with different flags
    - FIN/ACK probe
      - `-sM`
      - `--scanflags ACKFIN`
      - `sudo hping3 --scan 1-1000 -F -A 10.6.6.11`
- 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
      - Some devices will scoff
    - Windows OS
    - Cisco OS
    - IBM OS/400