- Filename: eccouncil-ceh31250-v12-3-14-1-ids-and-firewall-evasion.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: IDS and Firewall Evasion
  ==========

IDS and Firewall Evasion

Objectives:

- List common network scanning IDS/Firewall evasion techniques
- Demonstrate techniques using industry standard tools like nmap, hping3, ProxySwitcher, Tails, Whonix and VPNs

---

- How do we evade those pesky network security tools like firewalls and IDSs?
    - Packet Fragmentation
        - `nmap -f`
    - IP Address Decoy
        - `nmap -D <decoy1>,<decoy2> targetIP`
    - Source IP Address Spoofing
        - `nmap -S <SPOOF_IP>`
    - Source Port Modification
        - Use a port that's not being filtered by the target
            - i.e. 80,53,443,3389,etc
                - `nmap -g <PORT>`
    - SSRF attacks
    - Randomizing Hosts
        - `nmap --randomize-hosts`
    - Proxy Servers
        - `nmap --proxies`
    - Anonymizers
        - VPN
        - TOR
            - Tails
            - Whonix
        - https://www.proxyswitcher.com
        - https://www.torproject.org/download/
        - https://tails.boum.org
        - https://www.whonix.org