- Filename: eccouncil-ceh31250-v12-3-3-1-host-discovery.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Host Discovery

==========

Host Discovery

Objectives:

- Define host discovery and explain its function
- List host discovery techniques
- Describe the advantages and application of host discovery using ICMP, ARP, and UDP Ping scans
- Utilize common host discovery tools like nmap and Angry IP Scanner
- Identify and recall common security controls used to protect organizations against ping sweep scans
- Ascertain target network details such as IP range, internet-facing devices/servers, route path, and possible network-based security controls

---

- What is 'host discovery' and what is its function?
    - Discover live network connected devices
        - Both internal and external
- What are the common host discovery types/techniques?
    - ICMP ECHO
    - ARP
    - UDP
- Can you show us some common tools for performing host discovery?
    - Ping
        - https://github.com/daniellowrie/sweeper
    - Angry IP Scanner
    - nmap
        - `-sn`
    - Traceroute
        - ICMP
            - `tracert`
            - `traceroute -I`
        - TCP
            - `traceroute -T`
            - `tcptraceroute`
                - Any other traceroute-type tools?
                - Path Analyzer Pro
                - https://www.pathanalyzer.com
                - VisualRoute
                - https://www.visualroute.com
- Any other techniques we should be aware of?
    - ICMP Timestamp and Address Mask
        - ECHO (`-PE`)
        - Timestamp (`-PP`)
        - Address Mask (`-PM`)

    - SYN Ping (`-PS`)
    - ACK Ping (`-PA`)
    - Protocol Ping (`-PO`)
    - UDP Ping (`-PO`)

- Are there any security controls we can employ to protect us?
    - Firewall
    - IDS/IPS
    - Rate-limit hosts running more than X-number of ICMP ECHO requests
    - ACLs
    - DMZs