**Nmap Live Host Discovery**

1. **Introduction:**

1. Targets Enumeration

2. Discovering Live Hosts

3. Reverse DNS Lookup

4. Scan Ports

* Nmap Scan Steps

5. Detect Versions

6. Detect OS

7. Traceroute

8. Scripts

9. Write Outputs

1. **Subnetworks**
2. **Enumerating Targets**
3. **Discovering Live Hosts:**

* ARP from Link Layer
* ICMP from Network Layer
* TCP from Transport Layer
* UDP from Transport Layer

1. **Nmap Host Discovery Using ARP:**

<http://www.royhills.co.uk/wiki/index.php/Main_Page>

-I Interface -l Localhost

1. **Nmap Host Discovery Using ICMP**
2. **Nmap Host Discovery Using TCP and UDP:**

masscan MACHINE\_IP/24 ‐‐top-ports 100

1. **Using Reverse-DNS Lookup**
2. **Summary:**

ARP Scan 🡪 sudo nmap -PR -sn MACHINE\_IP/24

ICMP Echo Scan 🡪 sudo nmap -PE -sn MACHINE\_IP/24

ICMP Timestamp Scan 🡪 sudo nmap -PP -sn MACHINE\_IP/24

ICMP Address Mask Scan 🡪 sudo nmap -PM -sn MACHINE\_IP/24

TCP SYN Ping Scan 🡪 sudo nmap -PS22-25 -sn MACHINE\_IP/30

TCP ACK Ping Scan 🡪 sudo nmap -PA22,80 -sn MACHINE\_IP/30

UDP Ping Scan 🡪 sudo nmap -PU53,161 -sn MACHINE\_IP/30