Paradox07

Introduction to Host Discovery

- **Purpose**: Determine which systems are online within a network.
- **Methods**: Various Nmap options, primarily using ICMP echo requests to check if a target is alive.

Storing Scan Results

- **Importance**: Critical for documentation, comparison, and reporting. Different tools may produce different results, and it's beneficial to track which tool provides which results.

Scanning a Network Range

- **Command**: `sudo nmap 10.129.2.0/24 -sn -oA tnet`
  - **Options**:
    - `10.129.2.0/24`: Target network range.
    - `-sn`: Disables port scanning, focusing on host discovery.
    - `-oA tnet`: Stores results in all formats starting with 'tnet'.
- **Output Filtering**: Use `grep`, `cut`, etc., to process results.

Scanning from an IP List

- **Use Case**: When provided with a predefined list of IPs.
- **Command**: `sudo nmap -sn -oA tnet -iL hosts.lst`
  - **Options**:
    - `-iL hosts.lst`: Reads targets from the specified list

Scanning Multiple IPs

- **Direct Multiple IPs**:
  - Command: `sudo nmap -sn -oA tnet 10.129.2.18 10.129.2.19 10.129.2.20`
- **IP Range**:
  - Command: `sudo nmap -sn -oA tnet 10.129.2.18-20`

Scanning a Single IP

- **Basic Command**: `sudo nmap 10.129.2.18 -sn -oA host`
  - **Options**:
    - `10.129.2.18`: Target IP.
    - `-sn`: Disables port scanning.
    - `-oA host`: Stores results in all formats starting with 'host'.
- **Enhanced Options**:
  - `-PE`: Ensures ICMP Echo Requests are used.
  - `--packet-trace`: Displays all sent and received packets.
  - `--reason`: Shows why a host is marked as "up".

Dealing with Firewalls and ARP

- **ARP vs. ICMP**: Default behavior sends ARP pings. Use -PE to enforce ICMP Echo Requests.
- **Disabling ARP**: --disable-arp-ping to avoid ARP and use only ICMP.

Example Commands and Outputs

- **Basic Network Scan**:
  sh
  Copy code
  ```
  sudo nmap 10.129.2.0/24 -sn -oA tnet | grep for | cut -d" " -f5
  ```

1.
   - ○ Lists all active hosts in the network range.

- **Using IP List**:
  sh
  Copy code
  ```
  sudo nmap -sn -oA tnet -iL hosts.lst | grep for | cut -d" " -f5
  ```

2.
   - ○ Scans only the hosts listed in hosts.lst.

- **Multiple IPs**:
  sh
  Copy code
  ```
  sudo nmap -sn -oA tnet 10.129.2.18 10.129.2.19 10.129.2.20 | grep for | cut -d" " -f5
  ```

3.

- **Single IP with Packet Trace**:
  ```
  sudo nmap 10.129.2.18 -sn -oA host -PE --packet-trace
  ```

4.

- **Single IP with Reason**:
  ```
  sudo nmap 10.129.2.18 -sn -oA host -PE --reason
  ```

5.

- **Disabling ARP**:
  ```
  sudo nmap 10.129.2.18 -sn -oA host -PE --packet-trace --disable-arp-ping
  ```

Conclusion

Understanding Nmap's host discovery options is crucial for penetration testing and network mapping. Learners should familiarize themselves with various scanning techniques and options to effectively identify active hosts within a network. Detailed attention to scan results and documentation is essential for accurate analysis and reporting. For more strategies, refer to the Nmap book's host discovery strategies section: Host Discovery Strategies.