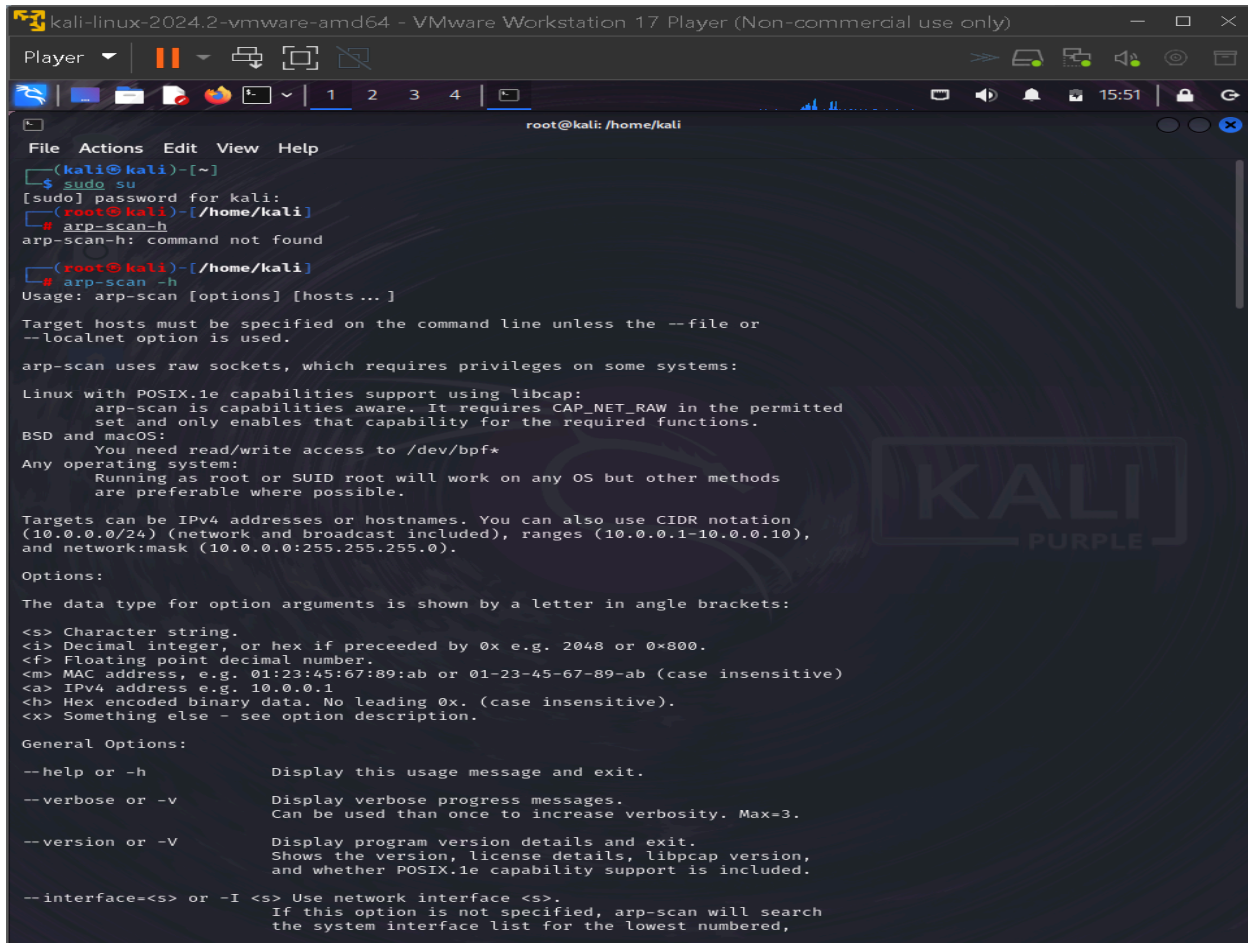


USING ARP COMMAND FOR NETWORK RECONNAISSANCE

Tools: kali linux

The **Address Resolution Protocol (ARP)** is a fundamental network protocol used in local area networks (LANs) to resolve or map an IP address to a MAC address (Media Access Control).

Input from kali :



```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# arp-scan-h
arp-scan-h: command not found

(root@kali)-[/home/kali]
└─# arp-scan -h
Usage: arp-scan [options] [hosts ...]

Target hosts must be specified on the command line unless the --file or
--localnet option is used.

arp-scan uses raw sockets, which requires privileges on some systems:

Linux with POSIX.1e capabilities support using libcap:
  arp-scan is capabilities aware. It requires CAP_NET_RAW in the permitted
  set and only enables that capability for the required functions.
BSD and macOS:
  You need read/write access to /dev/bpf*
Any operating system:
  Running as root or SUID root will work on any OS but other methods
  are preferable where possible.

Targets can be IPv4 addresses or hostnames. You can also use CIDR notation
(10.0.0.0/24) (network and broadcast included), ranges (10.0.0.1-10.0.0.10),
and network:mask (10.0.0.0:255.255.255.0).

Options:

The data type for option arguments is shown by a letter in angle brackets:

<s> Character string.
<i> Decimal integer, or hex if preceeded by 0x e.g. 2048 or 0x800.
<f> Floating point decimal number.
<m> MAC address, e.g. 01:23:45:67:89:ab or 01-23-45-67-89-ab (case insensitive)
<a> IPv4 address e.g. 10.0.0.1
<h> Hex encoded binary data. No leading 0x. (case insensitive).
<x> Something else - see option description.

General Options:
--help or -h          Display this usage message and exit.
--verbose or -v        Display verbose progress messages.
                       Can be used than once to increase verbosity. Max=3.
--version or -V        Display program version details and exit.
                       Shows the version, license details, libpcap version,
                       and whether POSIX.1e capability support is included.
--interface=<s> or -I <s> Use network interface <s>.
                       If this option is not specified, arp-scan will search
                       the system interface list for the lowest numbered,
```

Here we would learn how to use the ARP command for network reconnaissance.

Firstly we have to be a root user, we do that by typing **sudo su**.

To begin, we will first look at the help screen for this tool by typing the following: `arp-scan -h` This will tell us a bit about the tool and provide us with some common tags we can use.

We will now conduct a complete scan of our local network. We will need to run the `arp-scan` as “root” to do this. Type the following command: `arp-scan -localnet`

If you receive an error during this scan, double check that you are running it as root.

Let's take a look at the figure.

As a result of the scan, we detected 4 different network-capable devices. We can see their MAC addresses and their corresponding IP addresses in columns 2 and 3. The first 3 segments of MAC addresses are assigned to hardware manufacturers by IEEE. `arp-scan` creates vendor information in column 4 by comparison from its own database.

The last 3 segments in the MAC address are defined specifically for the interface card produced by that manufacturer. They are permanently written into interface cards. However, it is still possible to temporarily change these addresses at the software level. As a matter of fact, `arp-scan` has the option to change the MAC address for the selected card, which we will see later in this lab. The MAC address of the network card used for querying is indicated at number 5 in this figure. Since MAC addresses have to be globally unique, copying them can cause problems, so they are blurred.

To specify the interface and subnet which you want to scan the network with and for, use the “-I” option followed by the name of the interface you

want to use. Here is what that would look like: `arp-scan -I eth0 192.168.1.0/24`

In this scan, we have specified that we want to use the eth0 interface and we want to scan a specific subnet. The IP address assigned to the interface card does not have to be in the subnet to be scanned. It doesn't even need to be assigned an IP. See figure below:

-
- Find duplicate IP addresses.
- Isolate and localf the interface is configured as trunk, it is possible to scan on specific VLAN. Example for VLAN 10; If you find unknown devices as a result of an arp scan, they are not necessarily rouge devices. It simply means that the MAC adress is not in the arp-scan vendor databases. To identify these devices, you can use an online MAC finder site. You can also update the arp-scan databases by executing the following commands:

```
cd /usr/share/arp-scan
```

```
get-iab -v -u http://standards.ieee.org/develo/develop/regauth/iab/iab.txt
```

```
get-oui -v -u http://standards.ieee.org/develo/develop/regauth/oui/oui.txt
```

If there are cards in your network whose MAC addresses have been changed intentionally, you can manually add a line to “/usr/share/arp-scan/mac-vendor.txt” file to identify them. For our example:

```
060027    SPOOFED-NIC TECHNOLOGIES LLC
```

If we want to analyze the responses from the scanned devices later with analysis tools such as tcpdump, wireshark, it is possible to save them in a separate file.

```
arp-scan -localnet -W results.pcap
```

```
tcpdump -nr results.pcap
```

There are many things that an ARP scan can uncover, making it a very useful tool, including the following:

- Discovery of all IPv4 network-connected devices.
- Quickly identify and map IP addresses to MAC addresses to rogue devices.

Identify devices by NIC vendor.