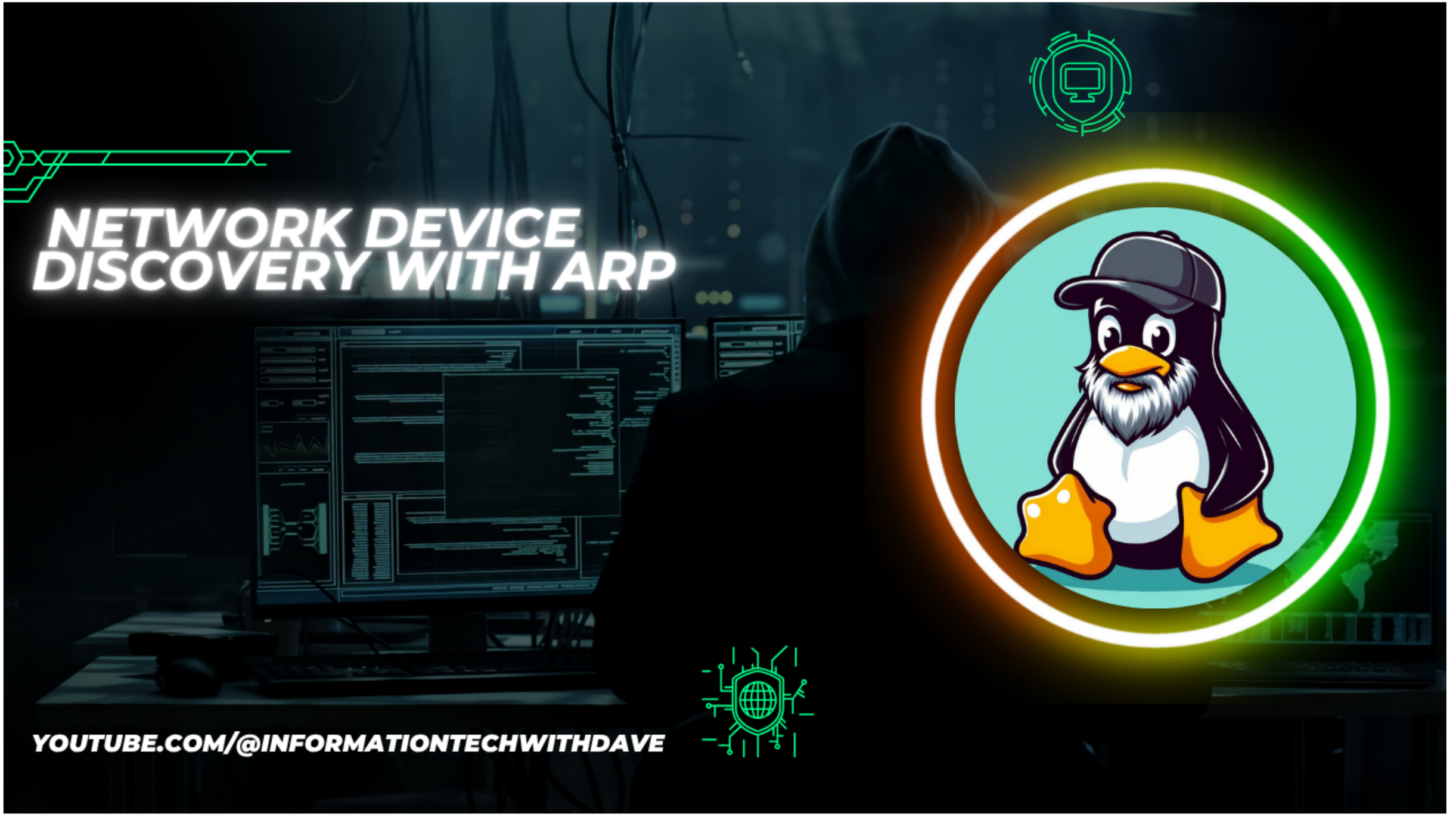

NETWORK DEVICE
DISCOVERY WITH ARP
YOUTUBE.COM/@INFORMATIONTECHWITHDAVE

Can’t this knowledge be used by 3v1l h4XX0rz?

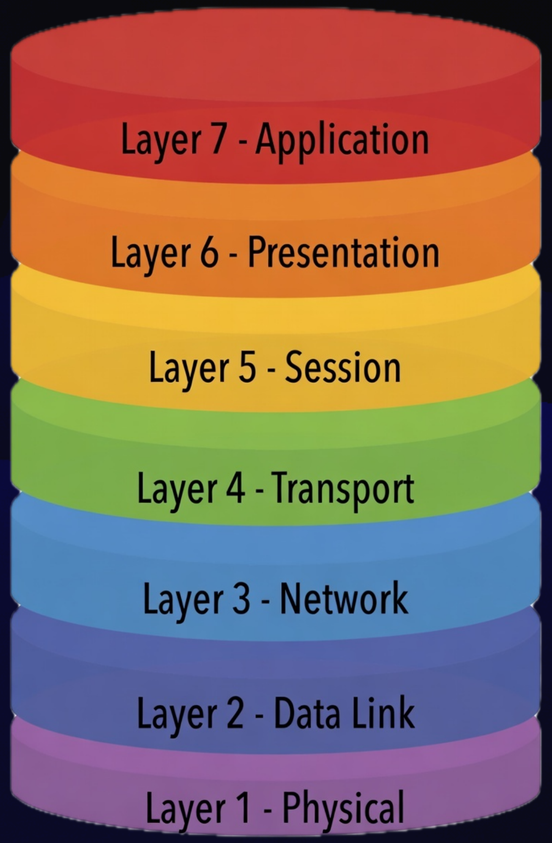
- YES. Unauthorized hackers can use arp tools to discover hosts to target on a network.
- Some of these tools are installed by default on systems, so hackers that like to “live off the land,” especially APTs (Advanced Persistent Threats) will rely on them.
- So, network administrators and Blue Team operators need to understand them, and can also use them to discover unauthorized hosts connected to their networks.
- Sun Tzu noted in The Art of War:
  - “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”
- As with any tool, intent matters!

YouTube.com/@InformationTechWithDave

We’re UNIX-Focused

- This presentation will be focused on UNIX and UNIX-like operating systems on servers and workstations, but be aware that network devices like routers and switches also rely on ARP and have their own implementations.
- We’re focusing on Linux, macOS, and BSD-based systems.
- If you’re on Windows, check out the Windows Subsystem for Linux, or install a Linux virtual machine in VirtualBox.

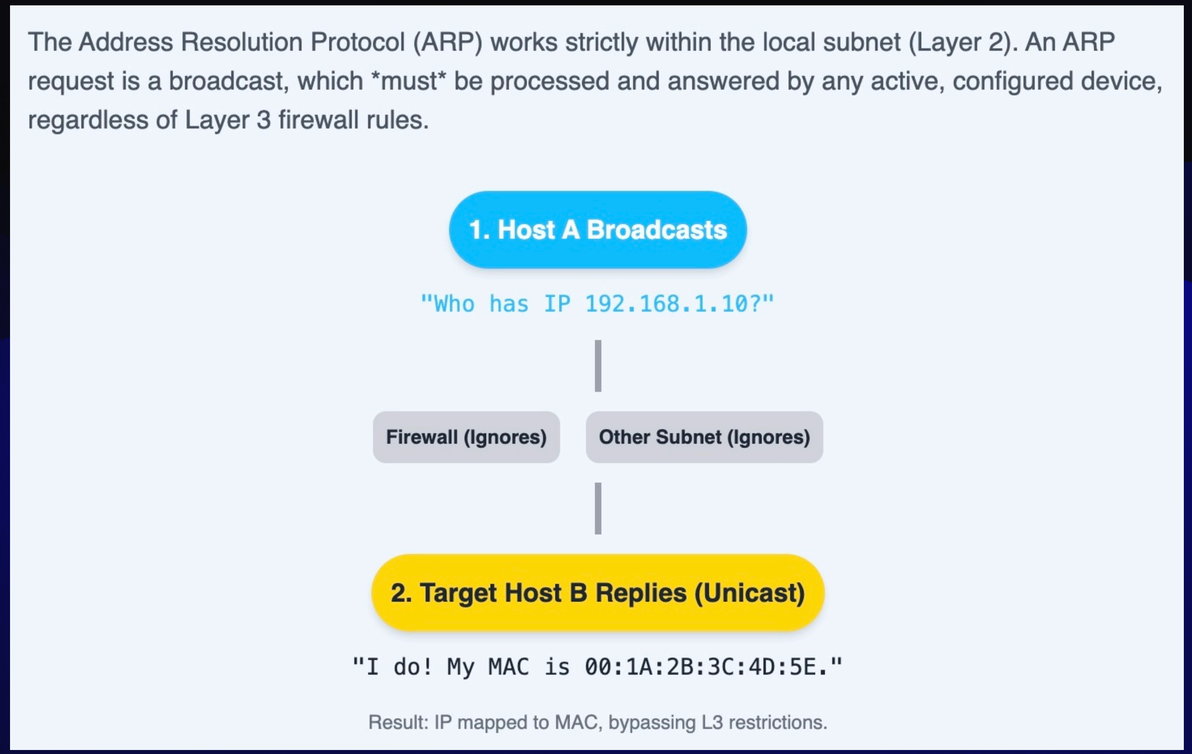
ARP - Address Resolution Protocol



- ARP is a networking protocol that works at Layer 2 of the OSI Model.
- Built-in on all network-capable operating systems.
- Maps physical (MAC) addresses to IPv4 addresses.
  - NOTE: IPv6 uses other protocols like Neighbor Discovery Protocol and Neighbor Advertisement Messages instead of ARP.
- Since it works at Layer 2, ARP resolution is confined to a single broadcast domain. I.e., subnets and VLANs.
- ARP packets do not traverse routers.

How ARP Maps a Physical Address to an IP

- Before diving into how to scan with ARP we need to understand how it works.
- It’s a simple two-step process.
- Step 1: Host A sends an ARP broadcast request for the physical address associated with an IPv4 address.
- Step 2: Host B with that IP replies with its MAC address.



YouTube.com/@InformationTechWithDave

Why ARP is useful for device discovery

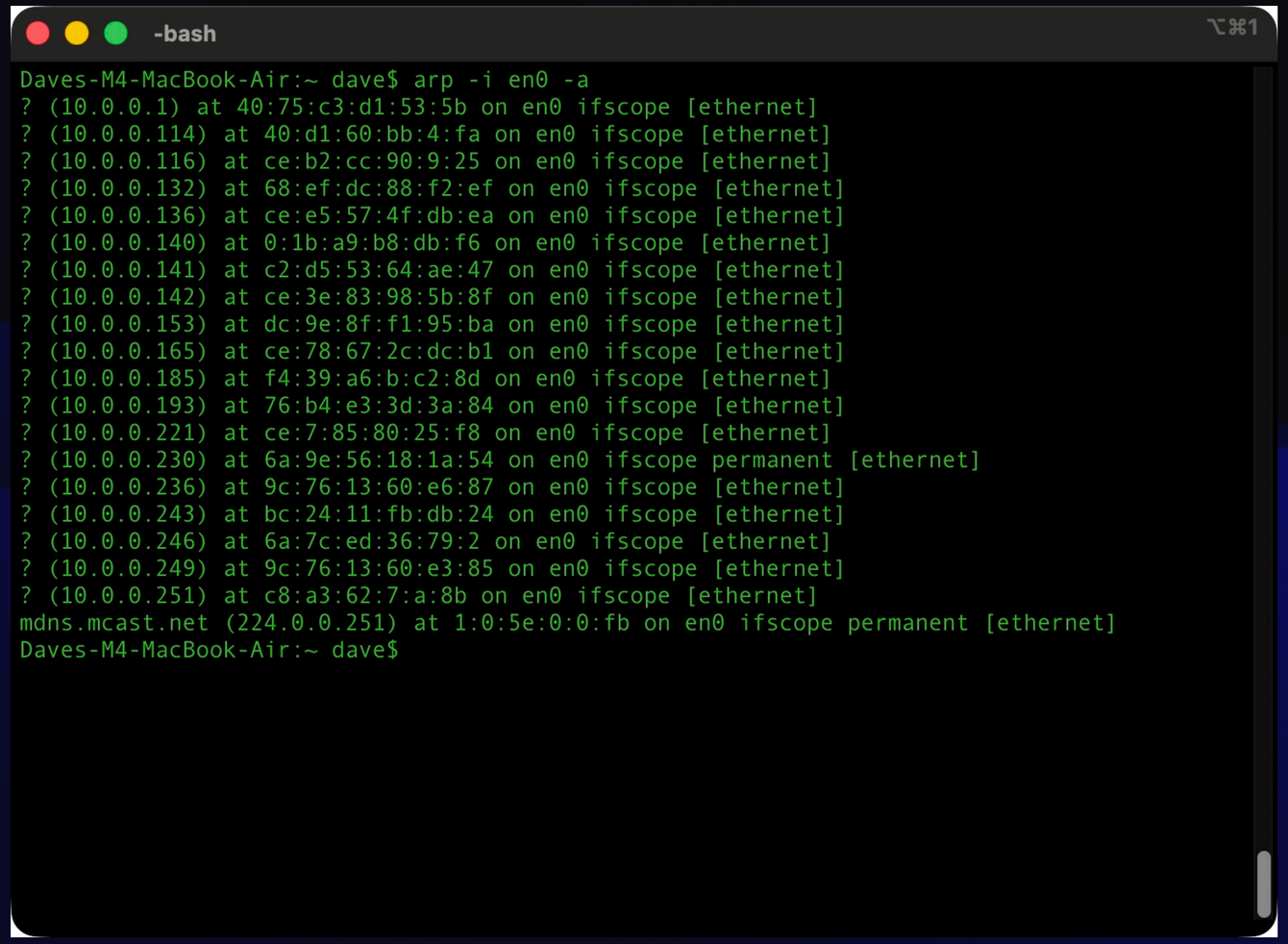
- Devices must respond to ARP to communicate on a LAN over IPv4.
- Many devices are configured to ignore ping requests. But even devices that don't respond to ping (ICMP packets) will respond to ARP queries.
- Local host firewalls that block all TCP, UDP, and ICMP packets will generally <u>not</u> block ARP.

YouTube.com/@InformationTechWithDave

Tools for Device Discovery with ARP

- arp - System command part of net-tools suite (deprecated on Linux but still used on macOS)
- ip neighbor - System command part of iproute2 suite
- arp-scan - https://github.com/royhills/arp-scan
- nmap - https://nmap.org/
- netdiscover - https://github.com/netdiscover-scanner/netdiscover
- tcpdump - https://www.tcpdump.org/
- oui.is - Look up device manufacturer based on MAC address

arp command

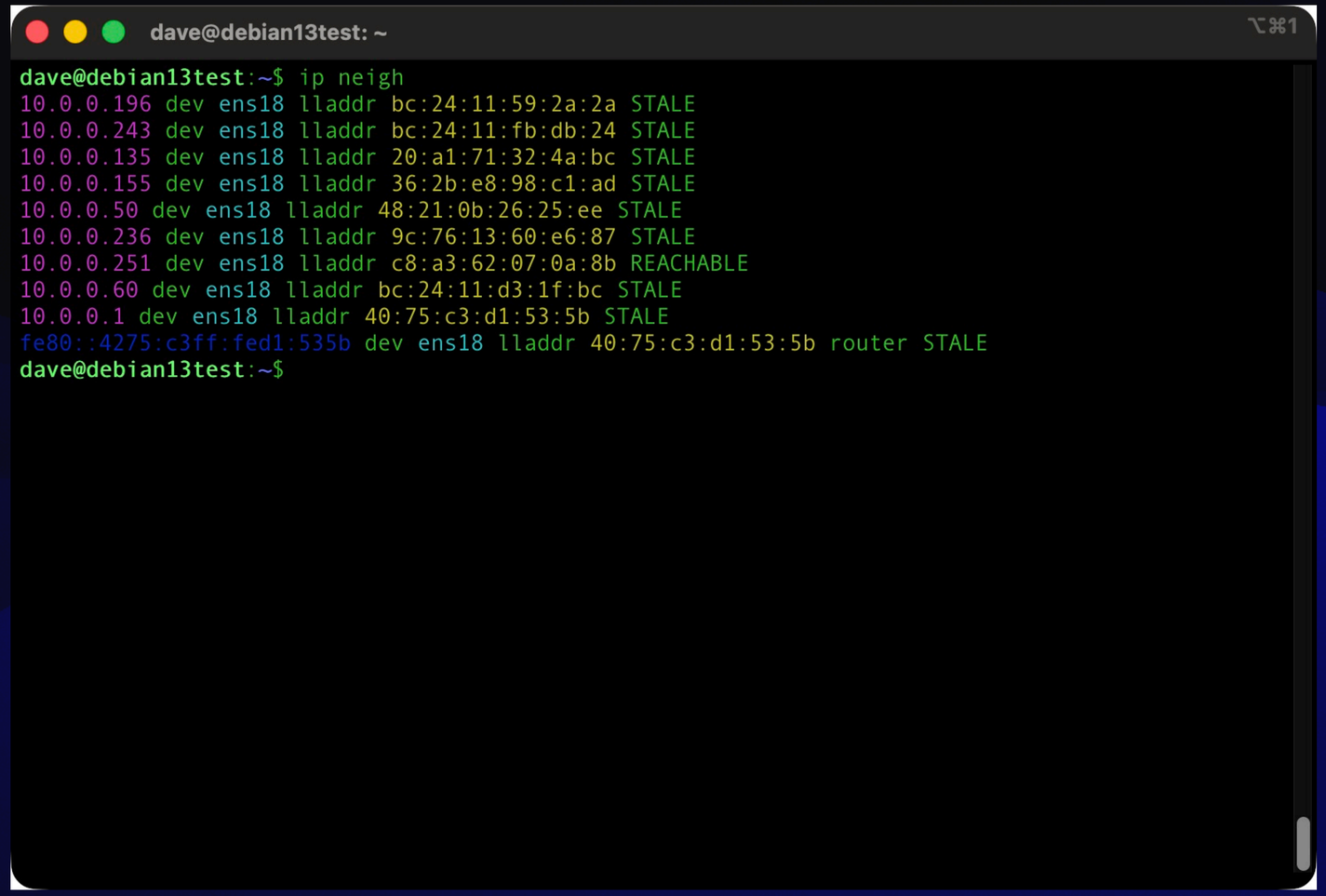


- Deprecated on Linux but still used on macOS.
- Quick and easy way to display your machines arp cache.
- $ arp -i en0 -a
- Shows host IPs, MACs, and which local interface they were seen on.
- If you don’t specify your machine’s interface (e.g., en0) it will use all of them, so you may get duplicates.

YouTube.com/@InformationTechWithDave

ip neighbor / ip neigh command on Linux

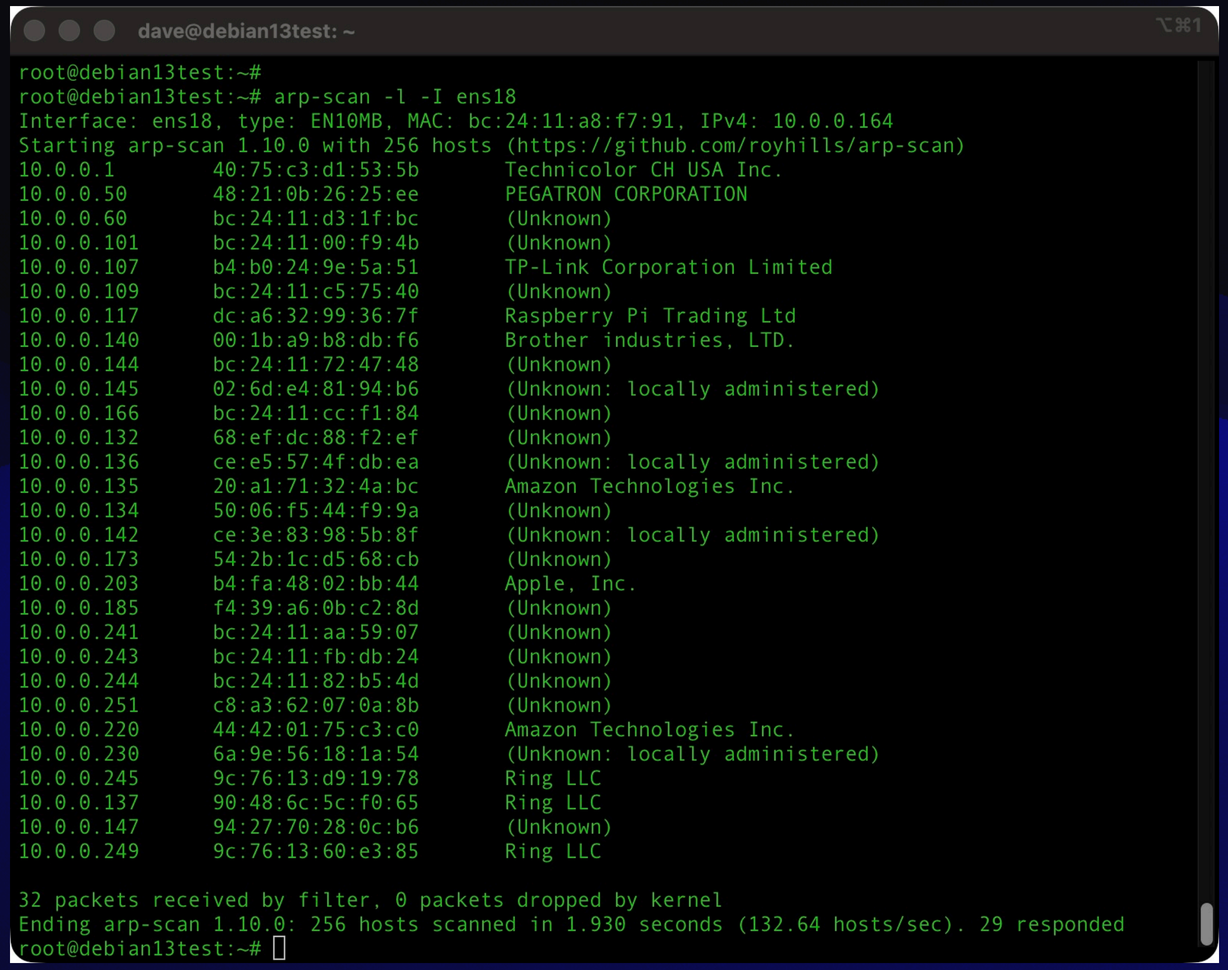
- Linux still supports arp but that is being deprecated, and it may not be installed by default.
- ip neighbor, or ip neigh for short, is the newer way to display the system's arp cache.
- Displays host IPs, which local interface they are seen on, MAC, and status of the cache entry.



YouTube.com/@InformationTechWithDave

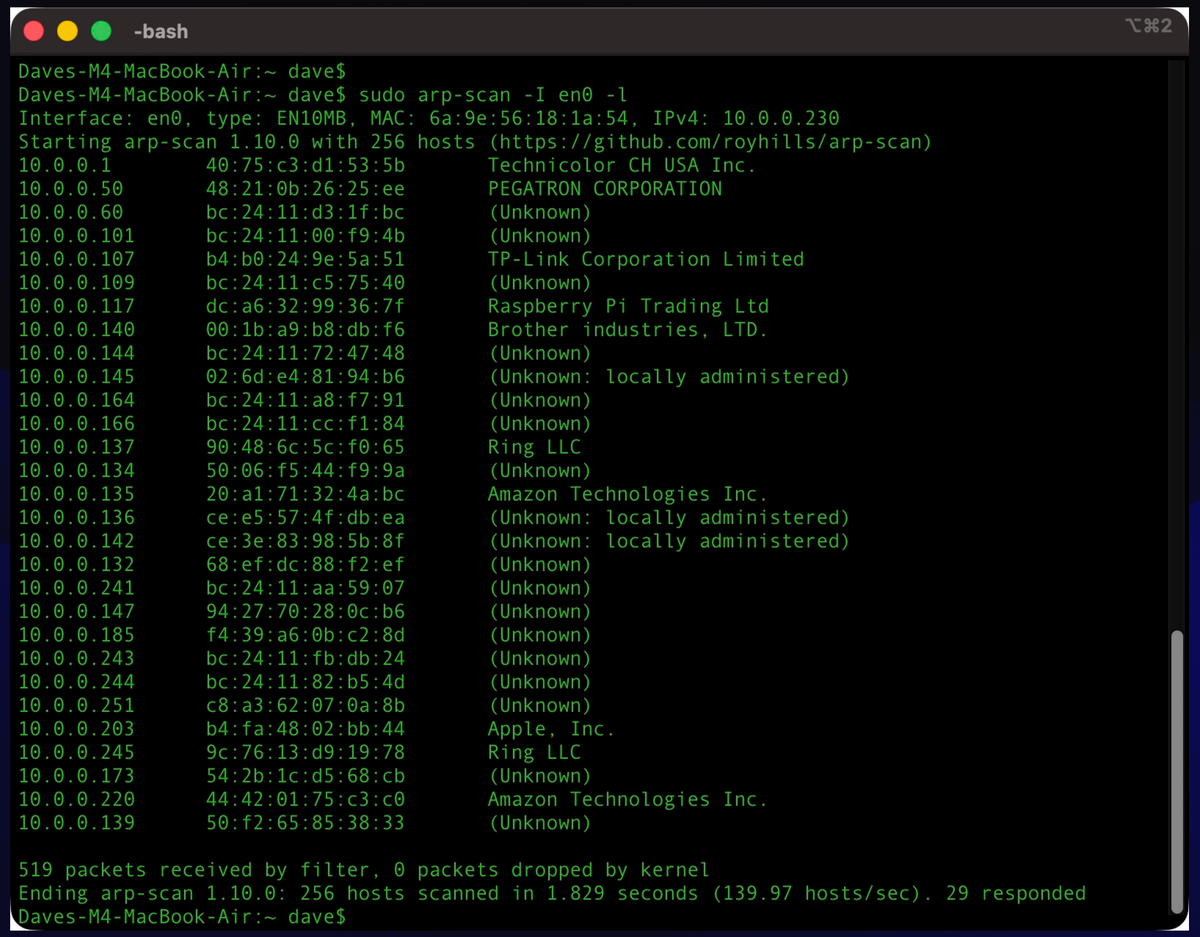
Host Discovery Using arp-scan (1 of 2)

- arp-scan discovers and fingerprints hosts using ARP.
- Runs on Linux, BSD, and macOS (install on Mac with Homebrew).
- Like the other tools, results may vary depending on what switch port you're connected to.
- On Linux, you may also need to run as root rather than using sudo, to avoid permissions issues.



YouTube.com/@InformationTechWithDave

Host Discovery Using arp-scan (2 of 2)



- Here is the output from my Mac on a different switch port but on the same network as the Linux example on the previous slide.
- Note here that it ran properly when invoked via sudo.
- Output is nicely formatted into columns with the IP, MAC, and vendor (where known).

Nmap arp scanning

- Nmap can do arp scans of a subnet and return a list of connected hosts.
- Check out my other video, Exploring and Scanning with Nmap.

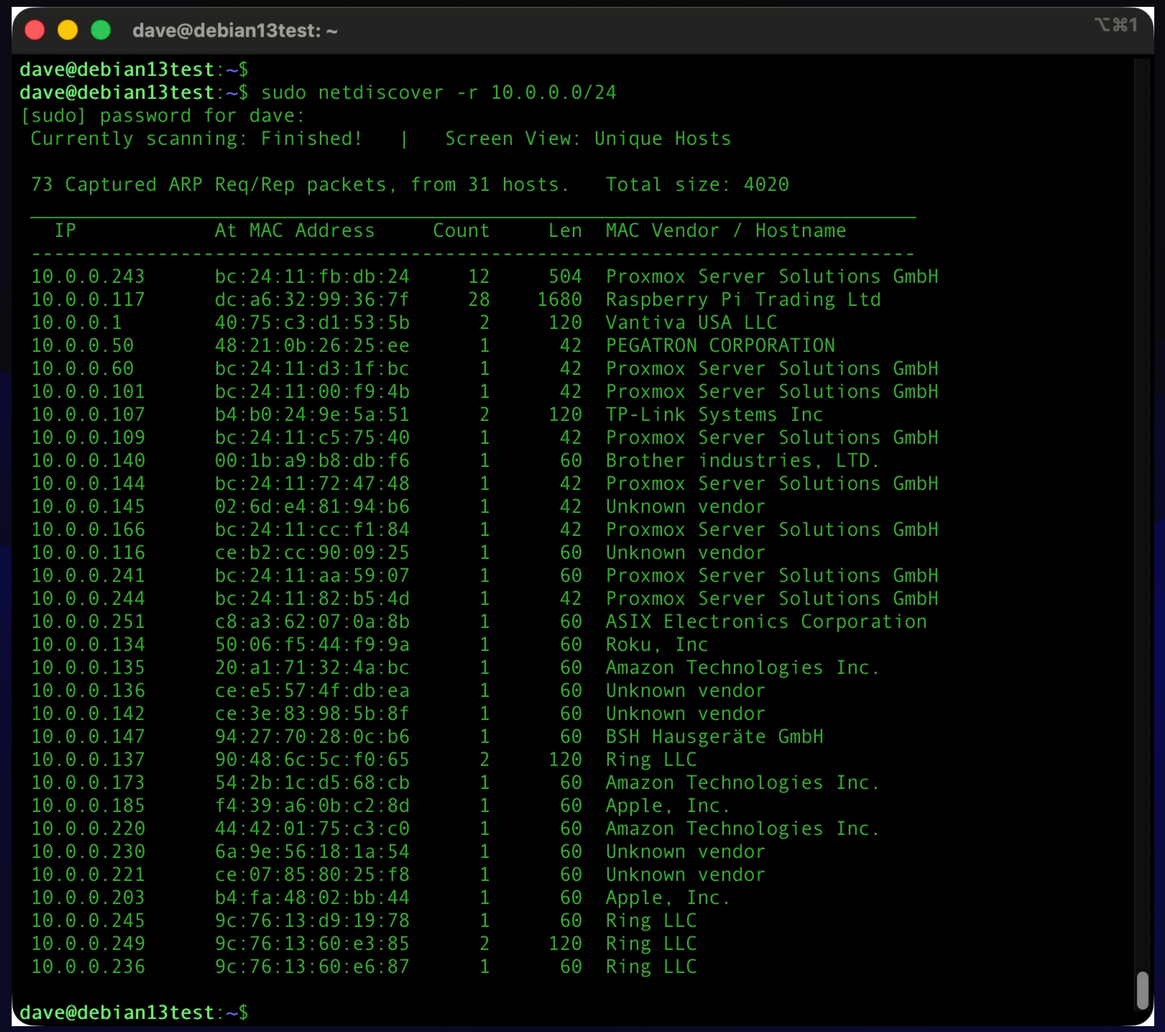
```
Daves-M4-MacBook-Air:~ dave$ sudo nmap -sn -PR 10.0.0.0/24
Password:

Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-15 17:42 -0500
Nmap scan report for 10.0.0.50
Host is up (0.00047s latency).
    MAC Address: 48:21:0B:26:25:EE (Pegatron)
Nmap scan report for 10.0.0.60
Host is up (0.00065s latency).
MAC Address: BC:24:11:D3:1F:BC (Proxmox Server Solutions GmbH)
Nmap scan report for 10.0.0.101
Host is up (0.00062s latency).
MAC Address: BC:24:11:00:F9:4B (Proxmox Server Solutions GmbH)
Nmap scan report for 10.0.0.107
Host is up (0.034s latency).
MAC Address: B4:B0:24:9E:5A:51 (TP-Link Limited)
Nmap scan report for 10.0.0.109
Host is up (0.00049s latency).
MAC Address: BC:24:11:C5:75:40 (Proxmox Server Solutions GmbH)
Nmap scan report for 10.0.0.117
Host is up (0.00042s latency).
MAC Address: DC:A6:32:99:36:7F (Raspberry Pi Trading)
Nmap scan report for 10.0.0.134
Host is up (0.19s latency).
MAC Address: 50:06:F5:44:F9:9A (Roku)

(Output deleted for brevity.)
```

YouTube.com/@InformationTechWithDave

netdiscover scanning

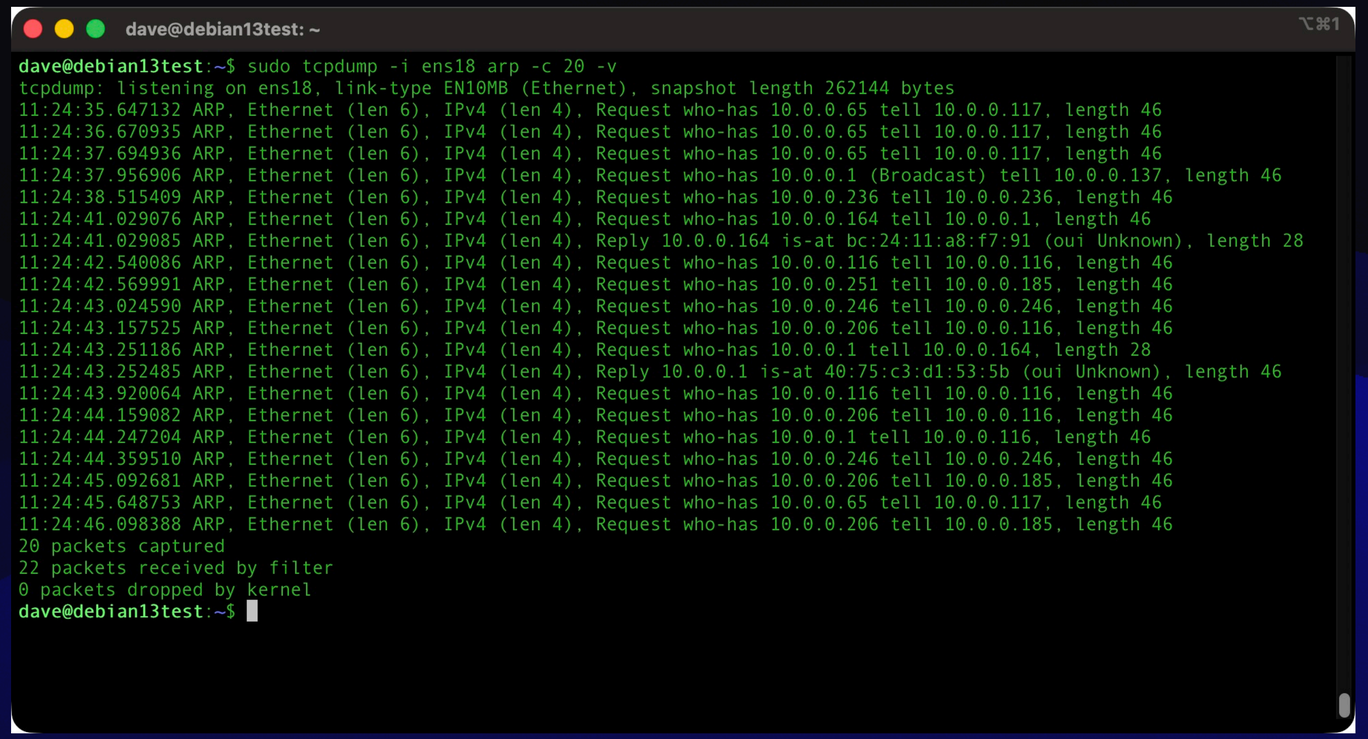


- netdiscover can be used actively or passively.
- Largely intended for use on WiFi networks but also works on wired networks.
- Can work on networks without a DHCP server.
- Use the “-r” option to specify scan range.
- Use the “-i” option to specify your network device if needed.

YouTube.com/@InformationTechWithDave

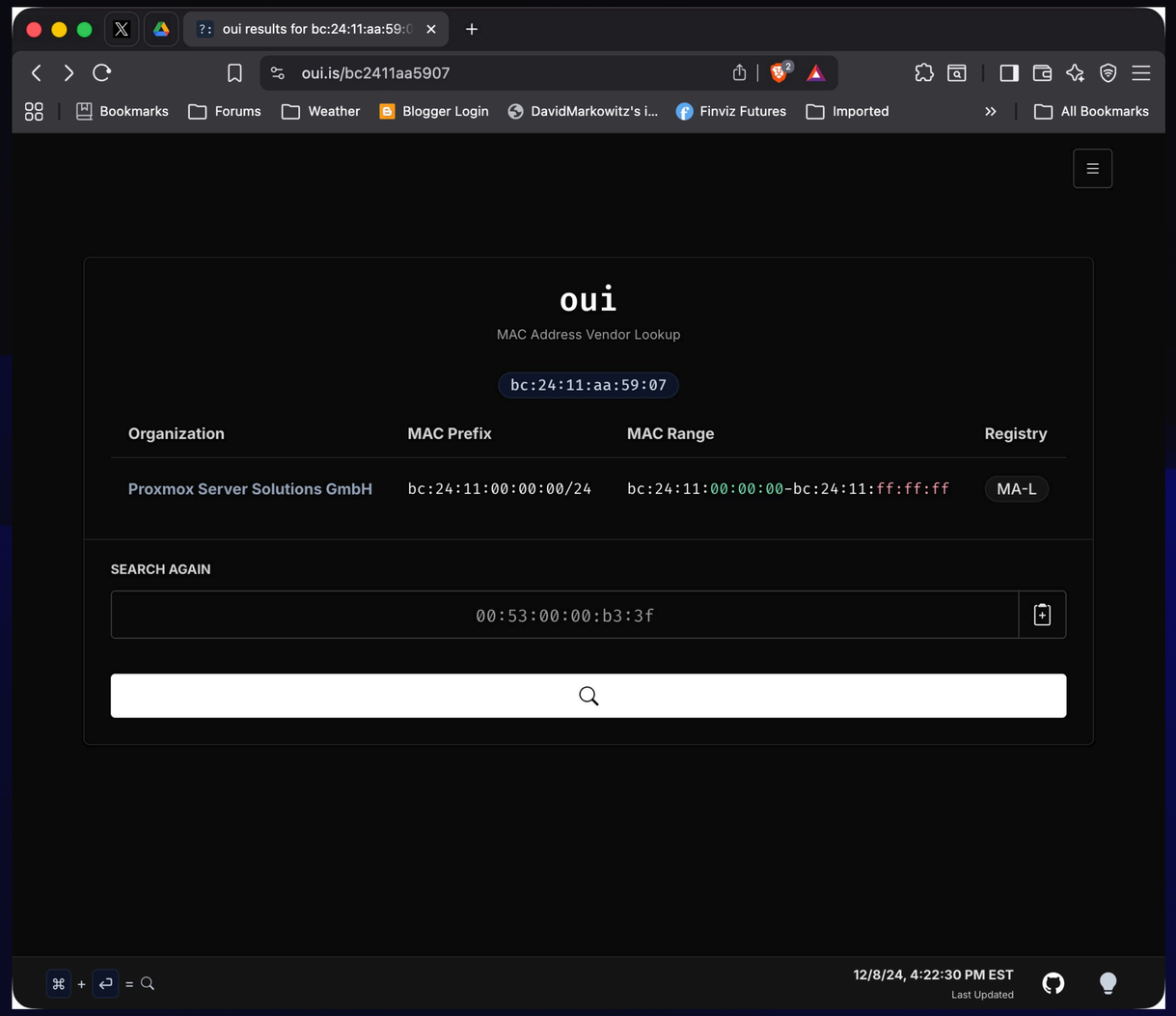
Using tcpdump to watch the wire

- tcpdump is a powerful commandline tool relied on by many other tools like Wireshark.
- It can be used on its own for live packet captures.
- Setup filters to limit captures to only what you're interested in.
- This example runs tcpdump, listening on interface ens18, only captures arp packets, and exits after 100 packets are captured. "-v" specifies verbose output.
  - sudo tcpdump -i ens18 arp -c 20 -v



YouTube.com/@InformationTechWithDave

Search for Device Manufacturers



- Each MAC address is globally unique.
- Device manufacturers are assigned prefixes by the IEEE.
- https://oui.is is one site that allows you to look up MAC addresses and find the manufacturer.

YouTube.com/@InformationTechWithDave

Conclusion

- Arp works at Layer 2 of the OSI network model, below most common networking protocols.
- There are several tools which you can use to discover network hosts via the ARP protocol.
- As shown in the previous examples, results can vary depending on the tool, whether you’re run it with admin rights, and depending on the switch port to which you’re connected. So, don’t rely on just one tool or just one network connection.
- Because MAC addresses are unique and ranges are assigned to device manufacturers you can research online who made them, which can help you track down devices on your network.
- Leveraging arp can facilitate you discovering hosts on your network that may escape other detection tools.

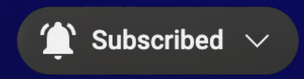
YouTube.com/@InformationTechWithDave

Thank you for watching!

Grab a copy of this slide deck from GitHub:

https://github.com/InformationTechWithDave

If you liked this video please hit the like button and subscribe. 

Don’t forget to click the notification button. 

Please share with anyone who would find this helpful. 

@InformationTechWithDave