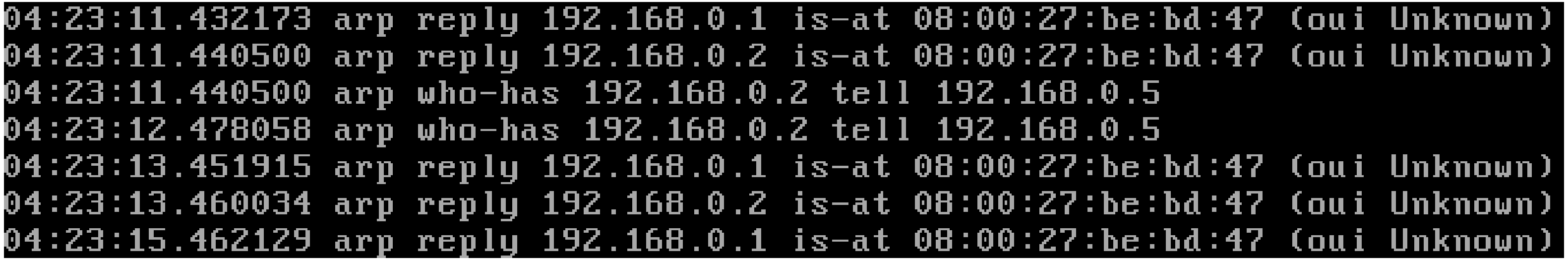
ARP poisoning and Man-In-The-Middle attacks

Stuck in the middle with you

Address Resolution Protocol (ARP)

- A way of finding the mapping between IP -> MAC addresses
- Is meant to be a request and response
  - But most machines listen in on anyone’s responses
- A computer says that it is the machine to contact about <IP>
  - “Hey everyone, I’m 192.168.0.3! Please send that traffic to me!”



```
04:23:11.432173 arp reply 192.168.0.1 is-at 08:00:27:be:bd:47 (oui Unknown)
04:23:11.440500 arp reply 192.168.0.2 is-at 08:00:27:be:bd:47 (oui Unknown)
04:23:11.440500 arp who-has 192.168.0.2 tell 192.168.0.5
04:23:12.478058 arp who-has 192.168.0.2 tell 192.168.0.5
04:23:13.451915 arp reply 192.168.0.1 is-at 08:00:27:be:bd:47 (oui Unknown)
04:23:13.460034 arp reply 192.168.0.2 is-at 08:00:27:be:bd:47 (oui Unknown)
04:23:15.462129 arp reply 192.168.0.1 is-at 08:00:27:be:bd:47 (oui Unknown)
```

Seeing is believing

/demoScripts/arpSpoofing/demo.sh

- Ubuntu box: access the metasploitable instance webpage
- Kali Box: Start the ARPSpoof demo script
- Ubuntu box: Refresh the metasploitable webpage
  - Notice that all instances of “msfadmin” now reads “Hacked”

What happened?

- When ARP spoof starts it begins flooding the network with ARP responses to claim control of IPs
  - You can see them in TCP dump if you want
  - It takes routing for both the metasploitable box (for capturing traffic) and the ubuntu box (to capture returned traffic)
- You can see the current cached MAC address of an IP using `arp` command

What happened? (cont)

- Kali acted as an intercepting proxy
  - Traffic modification: look for “msfadmin”, replace with “HACKED”
- When Ubuntu wanted to contact “192.168.64.2” it thought it should send the packet to the MAC address of the Kali instance.
- When metasploit wanted to reply to “192.168.64.4”, it thought it should address the packet to the MAC address of the Kali instance

ARP spoofing limitations

- Both machines must be on the same LAN
  - No external router between them
- Loud
  - Floods LAN with ARP replies

Another method: ARP sniping

- Listen for an ARP request for target machine and reply as fast as possible
- An ARP caches the first response it hears
  - If you can be first to respond, you'll be cached for some amount of time

What should I do about ARP spoofing?

- Have Dynamic ARP Inspection (DAI) on your routers/switches
  - Drops invalid ARP packets before they route anywhere else
- Logging and Intrusion Detection Systems (IDS)
  - ARP spoofing is obvious and traceable

Extra mitigations

- Higher layer machine authentication (such as HTTPS)
  - My Kali wouldn’t have the certificate for the metasploitable instance
  - Obviously only applicable to higher layer use cases.
- Hard coded network addresses for essential networking infrastructure
  - Messy and doesn’t scale

Information on ARP

- Wikipedia
  - https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- A worked example of ARP protocol in packet transmission across 2 subnets
  - https://www.juniper.net/documentation/en_US/junose13.1/information-products/topic-collections/swconfig-ip-ipv6/index.html?topic-65026.html