Week 9 Lab Assignment

1. **Aim:** Detect ARP spoofing using open source tool ARPWATCH.
2. **Objectives:** Objective of the module to find ARP spoofing using open source.
3. **Outcomes:** The learner will be able to: -

   - Identify network vulnerability with tool usage.
   - Also recognize the need of such tool to identify ARP spoofing, and an ability to engage in life-long learning to exploit gained skills and knowledge of contemporary issues.

4. Hardware / Software Required: ARPWATCH Tool
5. **Theory:**

   Arpwatch Commands and Usage:

   - To watch a specific interface, type the following command with _-i_ and device name. So, whenever a new MAC is plugged or a particular IP is changing his MAC address on the network, you will notice syslog entries at _/var/log/syslog_ or _/var/log/message_ file.

6. **Conclusion:**

   - Arpwatch is a software or program tool for monitoring Address Resolution Protocol traffic on a computer network. Its main goal is to detect arp poisoning attacks like (e.g. ARP Poisoning, Ettercap, and Netcut) also detect intruders in your network by sending an email to an administrator when new Ethernet MAC addresses.

- Arpwatch is an open-source computer software Links to an external site. program that helps you to monitor Ethernet traffic activity (like Changing IP and MAC Addresses) on your network and maintains a database of ethernet/ip address pairings.
- It produces a log of the noticed pairing of IP and MAC address information along with a timestamp, so you can carefully watch when the pairing activity appeared on the network. It also has the option to send reports via email to a network administrator when a pairing is added or changed.
- The Arpwatch tool is especially useful for Network administrators to keep a watch on ARP activity to detect ARP spoofing or unexpected IP/MAC address modifications.

Installing ARPWATCH on Linux

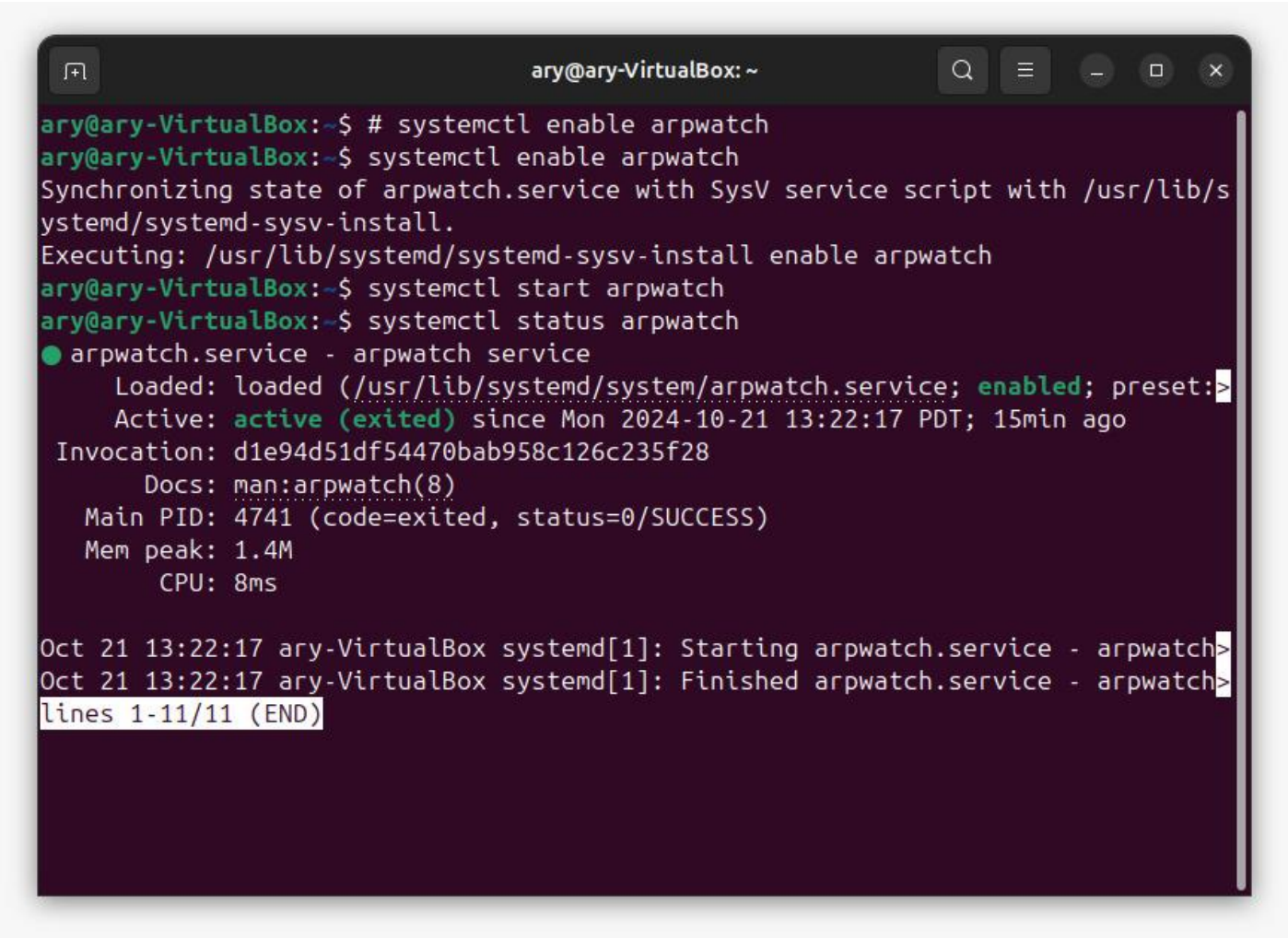
- The **Arpwatch** tool is not installed on Linux distributions, you need to use your default package manager to install it from the system repositories as shown.
- Use the following command to install Arpwatch on Ubuntu.

```
$ sudo apt install arpwatch
```

- Once installed, you can view the most important arpwatch files, the locations of the files are slightly different based on your operating system.
  - /usr/lib/systemd/system/arpwatch – The arpwatch service for starting or stopping the daemon.
  - /etc/sysconfig/arpwatch – This is the main arpwatch configuration file.
  - /usr/sbin/arpwatch – Binary command to starting and stopping tool via the terminal.
  - /var/lib/arpwatch/arp.dat – This is the main database file where IP/MAC addresses are recorded.
  - /var/log/messages – The log file, where arpwatch writes any changes or unusual activity to IP/MAC.

- Now run the following command to start the **arpwatch** service.

```
# systemctl enable arpwatch
# systemctl start arpwatch
# systemctl status arpwatch
```



How to Use Arpwatch Commands in Linux

- To watch a specific interface, type the following command with -i and device name.
- Use the following command to know the interface.

```
# arpwatch -i eth0
```

// not working this command

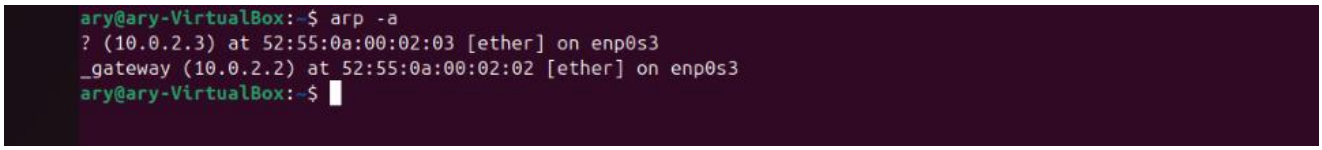
- So, whenever a new MAC is plugged in or a particular IP is changing his MAC address on the network, you will notice syslog entries in the '**/var/log/syslog**' or '**/var/log/message**' file using the tail command

```
# tail -f /var/log/messages
```

// not working this command

- You can also check the current **ARP** table, by using the following command.

```
# arp -a
```

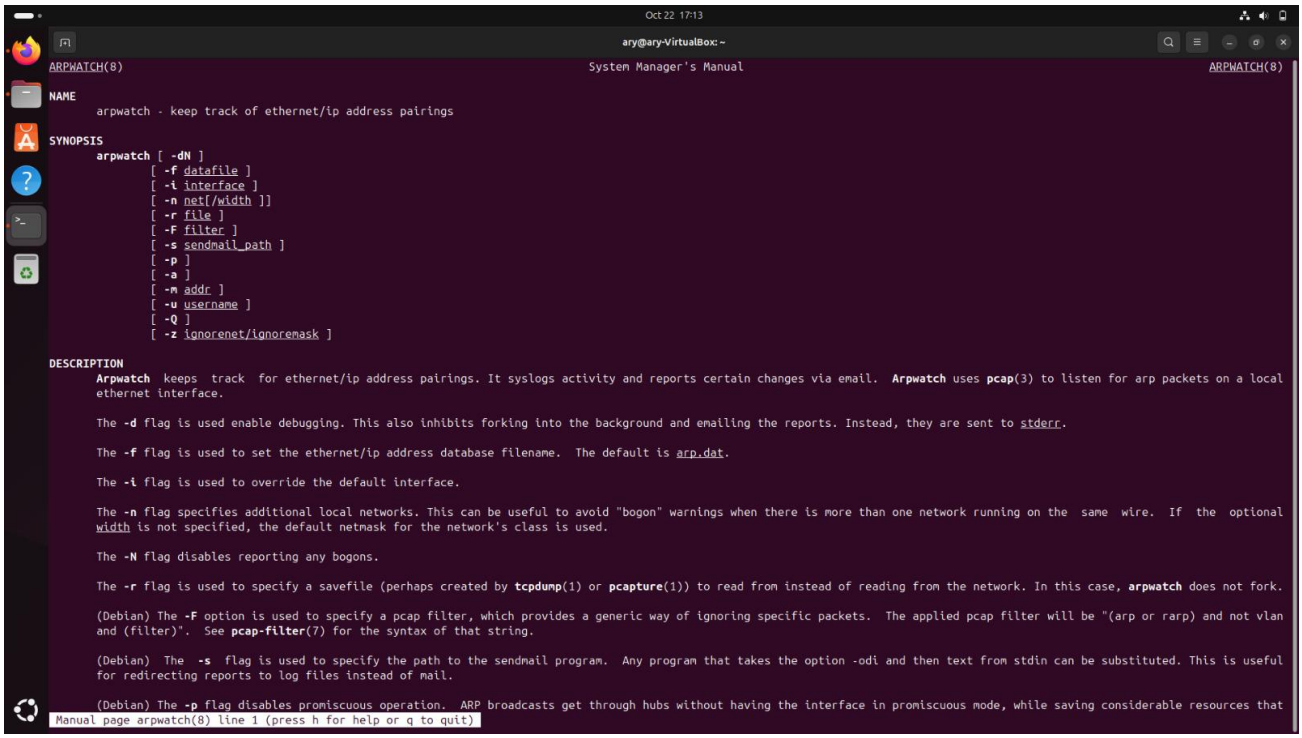


- If you want to send alerts to your custom email id, then open the main configuration file '**/etc/sysconfig/arpwatch**' and add the email as shown below.

```
# -u <username>: defines with what user id arpwatch should run

# -e <email>: the <email> where to send the reports

# -s <from>: the <from>-address

OPTIONS="-u arpwatch -e admin@tecmint.com -s 'root (Arpwatch)'"
```

- For more information, see the arpwatch man page by hitting 'man arpwatch' on the terminal.

```
# man arpwatch
```



7. **What is ARP Spoofing?**

ARP spoofing, also known as ARP poisoning, is a cyberattack where an attacker sends fake ARP messages over a local network to link their MAC address with the IP address of a legitimate device. This allows them to intercept, alter, or block data intended for that device.

In an ARP spoofing attack, the attacker sends out falsified ARP responses to trick devices on the network into associating the attacker's MAC address with the IP of another device, such as a router. As a result, any data meant for the legitimate IP gets sent to the attacker.

• Fake ARP Response: The attacker sends ARP messages mapping their MAC address to a trusted IP.
• Victims Update ARP Tables: Network devices store this incorrect information in their ARP tables.
• Traffic Interception: Data meant for the legitimate device is now routed to the attacker.
• Manipulation or Forwarding: The attacker can either read and modify the data or forward it to the intended destination to avoid detection.

➢ Consequences of ARP Spoofing

• Man-in-the-Middle Attacks: The attacker can secretly intercept and possibly alter the communication between two parties.
• Denial of Service (DoS): By disrupting or misrouting traffic, the attacker can cut off network access for the victim.
• Data Theft: Sensitive information, such as passwords or personal data, can be captured.
• Session Hijacking: By stealing session tokens, attackers can impersonate legitimate users.

What is IP Spoofing?

IP Spoofing is a type of cyberattack where an attacker disguises their computer's IP address to impersonate another device on a network. By doing this, the attacker can trick systems into thinking they're communicating with a trusted source when in reality, they're interacting with the attacker. This deception is often used to bypass security measures, gain unauthorized access, or flood a target with unwanted traffic in distributed denial-of-service (DDoS) attacks.

Here's how it works:

When devices communicate over the internet, they exchange information using unique IP addresses. These addresses are like mailing addresses, helping data packets find their way to the correct destination. In IP spoofing, the attacker alters the "sender" IP in a data packet to mimic the IP of another device. The receiving device, believing the packet is from a legitimate source, responds as if it's talking to the trusted device.

➢ Arpwatch is an open-source computer software Links to an external site. program that helps you to monitor Ethernet traffic activity (like Changing IP and MAC Addresses) on your network and maintains a database of ethernet/ip address pairings.
➢ The Arpwatch tool is especially useful for Network administrators to keep a watch on ARP activity to detect ARP spoofing or unexpected IP/MAC address modifications.