Experiment No. 9

Aim: Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark.Use arping tool to generate gratuitous arps and monitor using wireshark.

Objectives:

- Understand ARP spoofing.
- Understand ARPWATCH and use it to detect ARP spoofing.

Outcomes: The learner will be able to
Understand ARP spoofing and its detection using wireshark and other tools.

Hardware / Software Required: Unix/Linux, ARPWATCH, wireshark

Theory:

Arpwatch is an open source computer software 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 noticed pairing of IP and MAC addresses information along with a timestamps, so you can carefully watch when the pairing activity appeared on the network. It also has the option to send reports via email to an network administrator when a pairing added or changed.

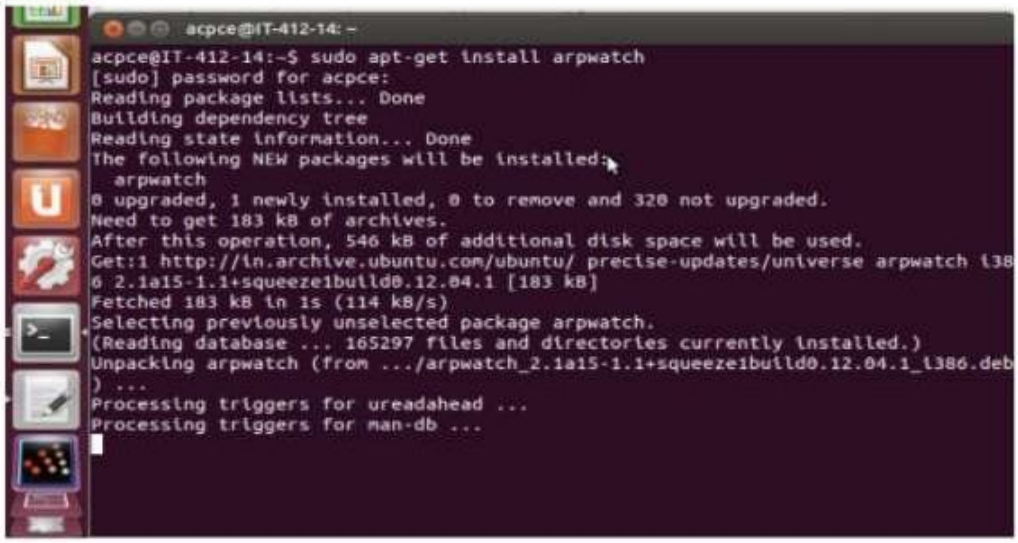
This tool is especially useful for Network administrators to keep a watch on ARP activity to detect ARP spoofing or unexpected IP/MAC addresses modifications.

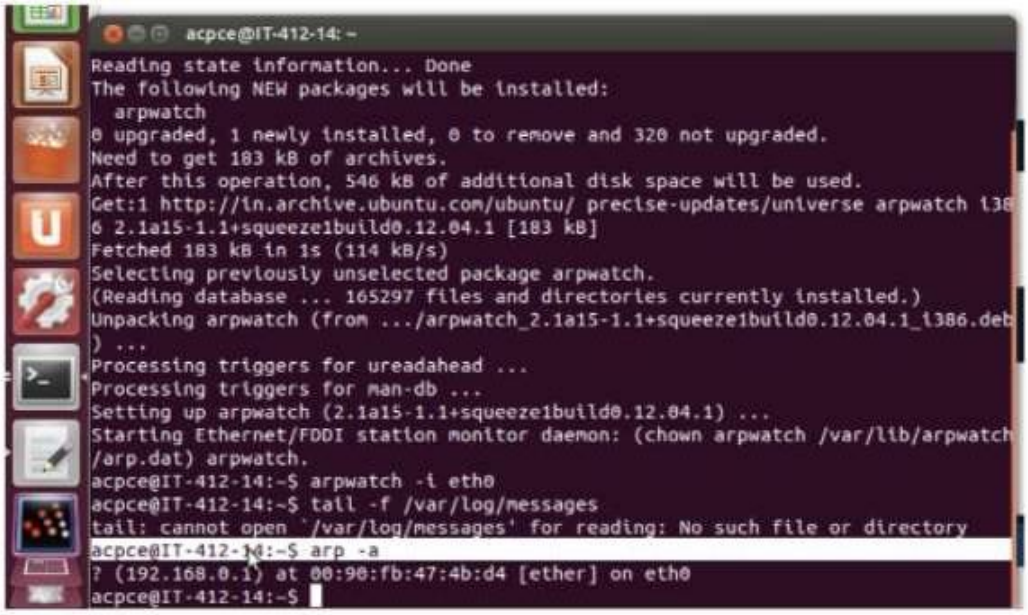
Installing Arpwatch in Linux

To watch a specific interface, type the following command with -i and device name. **#arpwatch -i eth0**

So, whenever a new MAC is plugged or a particular IP is changing corresponding toMAC address on the network, you will notice syslog entries at **/var/log/syslog** or **/var/log/message** file.

Output:





Conclusion: ARPWatch is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network.. An ARP spoofing, also known as ARP poisoning, isa Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices**.**