

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 a 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 to MAC address on the network, you will notice syslog entries at **/var/log/syslog** or **/var/log/message** file.

Output:

```
acpce@IT-412-14: ~$ sudo apt-get install arpwatc
[sudo] password for acpce:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  arpwatc
0 upgraded, 1 newly installed, 0 to remove and 320 not upgraded.
Need to get 183 kB of archives.
After this operation, 546 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/universe arpwatc 138
6 2.1a15-1.1+squeeze1build0.12.04.1 [183 kB]
Fetched 183 kB in 1s (114 kB/s)
Selecting previously unselected package arpwatc.
(Reading database ... 165297 files and directories currently installed.)
Unpacking arpwatc (from .../arpwatc_2.1a15-1.1+squeeze1build0.12.04.1_1386.deb
) ...
Processing triggers for ureadahead ...
Processing triggers for man-db ...
```

```
acpce@IT-412-14: ~$
Reading state information... Done
The following NEW packages will be installed:
  arpwatc
0 upgraded, 1 newly installed, 0 to remove and 320 not upgraded.
Need to get 183 kB of archives.
After this operation, 546 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/universe arpwatc 138
6 2.1a15-1.1+squeeze1build0.12.04.1 [183 kB]
Fetched 183 kB in 1s (114 kB/s)
Selecting previously unselected package arpwatc.
(Reading database ... 165297 files and directories currently installed.)
Unpacking arpwatc (from .../arpwatc_2.1a15-1.1+squeeze1build0.12.04.1_1386.deb
) ...
Processing triggers for ureadahead ...
Processing triggers for man-db ...
Setting up arpwatc (2.1a15-1.1+squeeze1build0.12.04.1) ...
Starting Ethernet/FDDI station monitor daemon: (chown arpwatc /var/lib/arpwatc
/arp.dat) arpwatc.
acpce@IT-412-14:~$ arpwatc -i eth0
acpce@IT-412-14:~$ tail -f /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
acpce@IT-412-14:~$ arp -a
? (192.168.0.1) at 00:90:fb:47:4b:d4 [ether] on eth0
acpce@IT-412-14:~$
```

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, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.