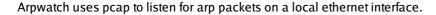# Table Of Contents

Home > Faq > CentOS

How to: Detect ARP Spoofing under UNIX or Linux

Posted by Vivek Gite <vivek@nixcraft.com>

Q. I would like to know - how do I detect ARP spoofing? I am using Debian Linux.

A. Use arpwatch command to keeps track for ethernet/ip address pairings. It logs message or activity to syslogs and reports certain changes via email.

Arpwatch uses pcap to listen for arp packets on a local ethernet interface.

[1]

Install arpwatch

Use apt-get command under Debian / Ubuntu Linux:

```
# apt-get install arpwatch
```

OR

```
$ sudo apt-get install arpwatch
```

arpwatch command examples

You can watch particular interface with command:

```
# arpwatch -i eth0
```

You will notice syslog entries as follows /var/log/syslog file (or /var/log/message file) when changes are made i.e MAC/IP address pair is changed:

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

Output:

```
Nov 10 15:59:34 debian arpwatch: new station 192.168.1.2 0:17:9a:a:f6:44 eth0
```

Above entry displays new workstation. If changes are made you should see something as follows:

```
Nov 10 15:59:34 debian arpwatch: changed station 192.168.1.2 0:17:9a:b:f6:f6
(0:17:9a:a:f6:44)
```

You can also use arp -a command to display current ARP table:

```
$ arp -a
```

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/how-to-detect-arp-spoofing-under-unix-or-linux/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/unix/**