



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
(All Branches NBA Accredited)



Department of Information Technology

**Semester: V**  
**Academic Year: 2022-23**  
**Class / Branch: TE IT**  
**Subject: Security Lab (SL)**  
**Date: 07/11/2022**

**Name of Student: Atharv Sathe**  
**Student ID: 20104054 (32)**

**Aim: Implement ARP spoofing over a local area network**

```
root@worker01: /home/apsit# arpwatch --version
Version 2.1a15
usage: arpwatch [-dN] [-f datafile] [-F "filter" ] [-i interface] [-n net[/width]] [-r file] [-s sendmail_path] [-p] [-a] [-m addr] [-u username] [-Q] [-z ignorenet/ignoremask]
root@worker01: /home/apsit#
```

```
● arpwatch.service - arpwatch service
   Loaded: loaded (/lib/systemd/system/arpwatch.service; enabled; vendor preset:
   Active: active (exited) since Tue 2022-07-19 13:46:01 IST; 1min 26s ago
     Docs: man:arpwatch(8)
  Main PID: 7179 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 4915)
   CGroup: /system.slice/arpwatch.service

Jul 19 13:46:01 apsit-HP-280-G3-MT systemd[1]: Starting arpwatch service...
Jul 19 13:46:01 apsit-HP-280-G3-MT systemd[1]: Started arpwatch service.
```



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



```
Activities Terminal Mon 13:00
root@worker01: /home/apsit

File Edit View Search Terminal Help
root@worker01:/home/apsit# arpwatc --version
Version 2.1a15
usage: arpwatc [-dN] [-f datafile] [-F "filter" ] [-i interface] [-n net[/width]] [-r file] [-s sendmail_path] [-p] [-a] [-m addr] [-u username] [-Q] [-z ignorenet/ignoremask]
root@worker01:/home/apsit# arp -a
? (192.168.13.111) at c4:ac:59:ab:2a:68 [ether] on enp4s0
? (192.168.87.22) at 18:60:24:ac:32:50 [ether] on enp4s0
_gateway (192.168.192.193) at c8:4f:86:05:06:24 [ether] on enp4s0
root@worker01:/home/apsit#
```

## Changing MAC Address

```
Activities Terminal Mon 13:18
root@worker01: /home/apsit

File Edit View Search Terminal Help
root@worker01:/home/apsit# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:73:b5:30:b0 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.87.24 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 fe80::e412:8be5:68f1:3749 prefixlen 64 scopeid 0x20<link>
    ether 00:1a:ff:0a:e7:1d txqueuelen 1000 (Ethernet)
    RX packets 153106 bytes 51862620 (51.8 MB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 14199 bytes 2096098 (2.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2281 bytes 250255 (250.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2281 bytes 250255 (250.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@worker01:/home/apsit#
```

mac address is 00:1a:ff:0a:e7:1d



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



```
Activities Terminal Mon 13:19
root@worker01: /home/apsit
File Edit View Search Terminal Help
root@worker01: /home/apsit# ifconfig enp4s0 hw ether 00:1a:ff:0a:e7:1f
root@worker01: /home/apsit# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:73:b5:30:b0 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.87.24 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 fe80::e412:8be5:68f1:3749 prefixlen 64 scopeid 0x20<link>
    ether 00:1a:ff:0a:e7:1f txqueuelen 1000 (Ethernet)
    RX packets 154774 bytes 52112453 (52.1 MB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 14199 bytes 2096098 (2.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2293 bytes 252021 (252.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2293 bytes 252021 (252.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@worker01: /home/apsit#
```

**MAC changed to 00:1a:ff:0a:e7:1f**

**Detecting using tail -f var/log/syslog**





```
Activities Terminal Mon 13:51 ● root@worker01: /home/apslt  
File Edit View Search Terminal Help  
Nov 7 13:50:52 worker01 kubelet[23909]: Flag --container-runtime has been deprecated, will be removed in 1.27 as the only valid value is 'rem  
ote'  
Nov 7 13:50:52 worker01 kubelet[23909]: Flag --pod-infra-container-image has been deprecated, will be removed in 1.27. Image garbage collecto  
r will get sandbox image information from CRI.  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.327411 23909 server.go:200] "--pod-infra-container-image will not be pruned by the i  
mage garbage collector in kubelet and should also be set in the remote runtime"  
Nov 7 13:50:52 worker01 kubelet[23909]: Flag --container-runtime has been deprecated, will be removed in 1.27 as the only valid value is 'rem  
ote'  
Nov 7 13:50:52 worker01 kubelet[23909]: Flag --pod-infra-container-image has been deprecated, will be removed in 1.27. Image garbage collecto  
r will get sandbox image information from CRI.  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.334395 23909 server.go:413] "Kubelet version" kubeletVersion="v1.25.2."  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.334416 23909 server.go:415] "Golang settings" GOGC="" GOMAXPROCS="" GOTRACEBACK=""  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.334600 23909 server.go:825] "Client rotation is on, will bootstrap in background"  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.335852 23909 certificate_store.go:130] Loading cert/key pair from "/var/lib/kubelet/  
pki/kubelet-client-current.pem".  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.336318 23909 dynamic_cafile_content.go:157] "Starting controller" name="client-ca-bu  
ndle:/etc/kubernetes/pki/ca.crt"  
Nov 7 13:50:52 worker01 kubelet[23909]: I1107 13:50:52.358783 23909 server.go:660] "--cgroups-per-qos enabled, but --cgroup-root was not sp  
ecified. defaulting to /"  
Nov 7 13:50:52 worker01 kubelet[23909]: E1107 13:50:52.359016 23909 run.go:74] "command failed" err="failed to run Kubelet: running with sw  
ap on is not supported, please disable swap! or set --fail-swap-on flag to false." /proc/sys/containers: [Filename:\t\t\tType\t\tSize\tUsed\t  
Priority \dev\sdas partition\t0239996\t0\t0\t2-1]  
Nov 7 13:50:52 worker01 systemd[1]: kubelet.service: Main process exited, code=exited, status=1/FAILURE  
Nov 7 13:50:52 worker01 systemd[1]: kubelet.service: Failed with result 'exit-code'.  
Nov 7 13:50:53 worker01 snort[2015]: WARNING: No preprocessors configured for policy 0.  
Nov 7 13:51:02 worker01 snort[2015]: message repeated 372 times: [ WARNING: No preprocessors configured for policy 0.]  
Nov 7 13:51:02 worker01 systemd[1]: kubelet.service: Service hold-off time over, scheduling restart.  
Nov 7 13:51:02 worker01 systemd[1]: kubelet.service: Scheduled restart job, restart counter is at 411.  
Nov 7 13:51:02 worker01 systemd[1]: Stopped kubelet: The Kubernetes Node Agent.  
Nov 7 13:51:02 worker01 systemd[1]: Started kubelet: The Kubernetes Node Agent.  
Nov 7 13:51:02 worker01 kubelet[23954]: Flag --container-runtime has been deprecated, will be removed in 1.27 as the only valid value is 'rem  
ote'  
Nov 7 13:51:02 worker01 kubelet[23954]: Flag --pod-infra-container-image has been deprecated, will be removed in 1.27. Image garbage collecto  
r will get sandbox image information from CRI.  
Nov 7 13:51:02 worker01 kubelet[23954]: I1107 13:51:02.711295 23954 server.go:200] "--pod-infra-container-image will not be pruned by the i  
mage garbage collector in kubelet and should also be set in the remote runtime"  
Nov 7 13:51:02 worker01 kubelet[23954]: Flag --container-runtime has been deprecated, will be removed in 1.27 as the only valid value is 'rem  
ote'
```

**Conclusion: I understood the arpwatsh service and also how to spoof or change a MAC address of a existing system and perform arp spoofing.**