



Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

Name of Student: visha
Student ID: 20104084

EXPERIMENT NO. 1

Aim: To Demonstrate IP Spoofing and ARP Spoofing in Local Area Network.

Demonstration of IP Spoofing:

```
pc2
--- Netkit phase 2 initialization terminated ---

pc2 login: root (automatic login)
Last login: Fri Jul 22 10:49:40 UTC 2022 on tty1
pc2:~# ifconfig eth0 192.168.1.12
pc2:~# tcpdump -i any
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
10:54:04.745813 IP 192.168.1.12 > 192.168.1.13: ICMP echo request, id 1282, seq 1, length 64
10:54:04.754866 arp who-has 192.168.1.12 tell 192.168.1.13
10:54:04.754880 arp reply 192.168.1.12 is-at 2e:18:cc:d4:8c:e7 (oui Unknown)
10:54:04.755027 IP 192.168.1.12 > 192.168.1.13: ICMP echo reply, id 1282, seq 1, length 64
10:54:04.765534 IP pc2.59814 > pc2.domain: 17891+ PTR? 13.1.168.192.in-addr.arpa. (43)
10:54:04.765546 IP pc2 > pc2: ICMP pc2 udp port domain unreachable, length 79
10:54:04.765655 IP pc2.52304 > pc2.domain: 17891+ PTR? 13.1.168.192.in-addr.arpa. (43)
10:54:04.765660 IP pc2 > pc2: ICMP pc2 udp port domain unreachable, length 79
10:54:04.765906 IP pc2.59161 > pc2.domain: 51142+ PTR? 12.1.168.192.in-addr.arpa. (43)

pc1
RX packets:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:100 (100.0 B) TX bytes:100 (100.0 B)

pc1:~# ping 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
64 bytes from 192.168.1.13: icmp_seq=1 ttl=64 time=2.54 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=64 time=0.603 ms
64 bytes from 192.168.1.13: icmp_seq=3 ttl=64 time=0.580 ms
64 bytes from 192.168.1.13: icmp_seq=4 ttl=64 time=0.545 ms
64 bytes from 192.168.1.13: icmp_seq=5 ttl=64 time=0.517 ms
^C
--- 192.168.1.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4050ms
rtt min/avg/max/mdev = 0.517/0.958/2.548/0.795 ms
pc1:~# iptables -t nat -A POSTROUTING -p icmp -j SNAT --to-source 192.168.1.12
pc1:~# ping 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
^C
--- 192.168.1.13 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8011ms
pc1:~#

pc3
Mounting kernel modules directory (/home/apsit/Documents/netkit/kernel/modules/1
ib/modules) on /lib/modules/ ...
Loading kernel modules...done.
Setting kernel variables (/etc/sysctl.conf)...done.
Setting up networking....
Configuring network interfaces...done.
Starting portmap daemon....
INIT: Entering runlevel: 2

--- Starting Netkit phase 1 init script ---
Mounting /home/apsit on /hasthome...
--- Netkit phase 1 initialization terminated ---

Starting system log daemon....
Starting kernel log daemon....

So we h
we will

--- Starting Netkit phase 2 init script ---
--- Netkit phase 2 initialization terminated ---

2.2
pc3 login: root (automatic login)
Last login: Mon Jul 25 10:51:00 UTC 2022 on tty1
pc3:~# ifconfig eth0 192.168.1.13
pc3:~#
```



Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

ARP TABLE:

```
apsit@apsit-HP-280-G3-MT:~$ arp -e
Address          HWtype  HWaddress      Flags Mask    Iface
gateway          ether    c8:4f:86:05:06:24 C              enp4s0
192.168.87.8      ether    18:60:24:a9:23:83 C              enp4s0
192.168.5.15      ether    10:62:e5:5c:62:9e C              enp4s0
apsit@apsit-HP-280-G3-MT:~$ arp -e
Address          HWtype  HWaddress      Flags Mask    Iface
gateway          ether    c8:4f:86:05:06:24 C              enp4s0
192.168.87.8      ether    02:42:eb:0c:ac:4d C              enp4s0
192.168.5.15      ether    10:62:e5:5c:62:9e C              enp4s0
```

Demonstration of ARP Spoofing:

```
root@apsit-HP-280-G3-MT:~# cat /var/log/syslog | grep 192.168.87.8
Jul 25 16:04:46 apsitt-HP-280-G3-MT arpwatrch: new station 192.168.87.8 02:42:eb:0c:ac:4e enp4s0
root@apsitt-HP-280-G3-MT:~# cat /var/log/syslog | grep 192.168.87.8
Jul 25 16:04:46 apsitt-HP-280-G3-MT arpwatrch: new station 192.168.87.8 02:42:eb:0c:ac:4e enp4s0
Jul 25 16:08:21 apsitt-HP-280-G3-MT arpwatrch: changed ethernet address 192.168.87.8 02:42:eb:0c:ac:4f (02:42:eb:0c:ac:4e) enp4s0
root@apsitt-HP-280-G3-MT:~# cat /var/log/syslog | grep 192.168.87.8
Jul 25 16:04:46 apsitt-HP-280-G3-MT arpwatrch: new station 192.168.87.8 02:42:eb:0c:ac:4e enp4s0
Jul 25 16:08:21 apsitt-HP-280-G3-MT arpwatrch: changed ethernet address 192.168.87.8 02:42:eb:0c:ac:4f (02:42:eb:0c:ac:4e) enp4s0
Jul 25 16:11:38 apsitt-HP-280-G3-MT arpwatrch: changed ethernet address 192.168.87.8 02:42:eb:0c:ac:1b (02:42:eb:0c:ac:4f) enp4s0
root@apsitt-HP-280-G3-MT:~#
```