# 网络安全实验FAQ

目录

[网络安全实验FAQ 1](#_Toc70701918)

[1. 在virtualbox中如何使多台虚拟机位于同一局域网? 2](#_Toc70701919)

[2. 多台虚拟机之间网络为什么不通？ 2](#_Toc70701920)

[3. 如何给虚拟机设置静态IP? 2](#_Toc70701921)

[4. 电脑内存不够，运行多台虚拟机卡顿很严重 2](#_Toc70701922)

[5. 虚拟机如何切换到字符界面启动？ 2](#_Toc70701923)

[6. 如何查看网卡的名称、ip地址、MAC地址等信息？ 2](#_Toc70701924)

[7. 电脑无法启动图形界面，如何在界面查看截包信息？ 3](#_Toc70701925)

[8. VirtualBox如何实现与主机之间的复制粘贴？ 3](#_Toc70701926)

[9. 用户机和服务器建立的TCP连接，为什么在攻击机器上截获不到该连接的报文？ 3](#_Toc70701927)

[10. 在做DNS攻击实验时，为什么客户机上无法解析域名？ 3](#_Toc70701928)

[11. 在做本地DNS攻击时，用netwox伪造了响应报文，wireshark也监听到了伪造报文，为什么客户机解析出来的还是原来的IP？ 4](#_Toc70701929)

[12. 远程DNS攻击时，在system调用dig命令之后，为什么伪造的第一个报文都比真实响应还慢？ 4](#_Toc70701930)

[13. 在vpn实验中，虚拟网卡选择工作在什么模式？ 5](#_Toc70701931)

[14. VPN实验中，可以只启用两个虚拟机，把自己的物理机也加入到实验环境中吗？ 5](#_Toc70701932)

[15. 为什么在tls例程运行时，tlsclient和tlserver的tcp连接不成功？ 5](#_Toc70701933)

[16. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示error:14094418:SSL routines:ssl3\_read\_bytes:tlsv1 alert unknown ca:s3\_pkt.c:1487:SSL alert number 48 的错误 6](#_Toc70701934)

[17. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示error:14094416:SSL routines:ssl3\_read\_bytes:sslv3 alert certificate unknown:s3\_pkt.c:1487:SSL alert number 46 的错误 6](#_Toc70701935)

[18. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示error:14094415:SSL routines: ssl3\_read\_bytes: sslv3 alert certificate expired:s3\_pkt.c:1487:SSL alert number 45 的错误 6](#_Toc70701936)

[19. 在demo\_openssl\_api.zip中怎么只有.crt文件，没有.pem文件？.crt文件和.pem文件有什么差别 7](#_Toc70701937)

[20. VPN实验中，最后支持多客户端那个部分，内网主机返回的报文到达VPN服务器以后，tun0中的数据应该向哪个隧道转发？怎么区分？ 7](#_Toc70701938)

## 1. 在virtualbox中如何使多台虚拟机位于同一局域网?

解决方法：<https://jingyan.baidu.com/article/948f5924ee2a5dd80ff5f9e4.html>

## 2. 多台虚拟机之间网络为什么不通？

解答：因为多台虚拟机是复制的，可能出现了IP地址、MAC地址相同的情况，ifconfig命令可以虚拟机的IP地址、MAC地址。如果有相同的情况，参考问题1的解决方案进行解决。

## 3. 如何给虚拟机设置静态IP?

解决办法：<https://www.cnblogs.com/IcarusYu/p/10967537.html>

## 4. 电脑内存不够，运行多台虚拟机卡顿很严重

解决办法：1）虚拟机可以字符界面方式启动，尽量减少内存的使用；

1. 网络配置成功以后，可以用secureCRT这样的远程终端管理软件来通过网络管理，不用在虚拟机之间切换（连接地址为要管理的虚拟机地址，连接端口为22）。
2. 将自己的机器作为实验环境的一部分，减少虚拟机的台数，整个实验环境包括一台电脑+2台虚拟机，虚拟机网卡可以设为桥接模式，这样2台虚拟机就和自己的电脑位于同一个局域网，IP地址也是同一网段。

## 5. 虚拟机如何切换到字符界面启动？

解决办法：1）sudo systemctl set-default multi-user.target，重启系统就进入字符界面

2）快速在字符界面和图形界面切换命令：

init 3 切换到字符界面

init 5 切换到图形界面

## 6. 如何查看网卡的名称、ip地址、MAC地址等信息？

解答： “ifconfig” 查看所有的网卡信息

“ifconfig 网卡名”查看指定网卡的信息

## 7. 电脑无法启动图形界面，如何在界面查看截包信息？

解答：tcpdump命令

典型的使用方法：

tcpdump -i 接口名 协议(tcp/udp/icmp) [ port 端口号] [host 主机地址] [-vv]

如：tcpdump -i enp0s3 tcp port 23 and host 1.2.2.4 -vv #监听1.2.2.4并且端口为TCP 23端口的所有报文，并在屏幕显示数据包细节

tcpdump -i enp0s3 tcp port 23 #监听TCP 23端口的所有报文，并在屏幕显示数据包细节

tcpdump -i enp0s3 icmp -s0 -w file.cap #监听所有的icmp报文，并写入file.cap文件

可以带过滤条件也可以不带，多个过滤条件之间用and连接。

其它的看帮助

## 8. VirtualBox如何实现与主机之间的复制粘贴？

解答： 设置->常规->高级->共享粘贴板->双向；

设置->常规->高级->拖放->双向。

## 9. 用户机和服务器建立的TCP连接，为什么在攻击机器上截获不到该连接的报文？

解答： 请确认攻击机上wireshark监听的网卡是跟其它两台机器配置同一网络IP的那个网卡，而不是any。

## 10. 在做DNS攻击实验时，为什么客户机上无法解析域名？

解答： 首先确认服务器上的域名服务是否正确启动

1）可以用sudo netstat -na查看监听端口，是否在udp 53号端口上监听（在任意地址监听，不是127.0.0.1)

2）也可以通过sudo ps aux|grep named查看named进程是否在运行；

3）以上过程发现域名服务没有启动的话，请启动域名服务

4）启动过程中如果出错，一般都是配置文件有问题；目前发现较多的问题是指导书上写的要在**/etc/bind/named.conf中增加的两个zone信息，需要添加到/etc/bind/named.conf.default-zones文件中**

|  |
| --- |
| zone "example.com" {  type master;  file "/etc/bind/example.com.db";  };  zone "0.168.192.in-addr.arpa" {  type master;  file "/etc/bind/192.168.0.db";  }; |

## 11. 在做本地DNS攻击时，用netwox伪造了响应报文，wireshark也监听到了伪造报文，为什么客户机解析出来的还是原来的IP？

解答：伪造的DNS响应需要比真实服务器的响应先到达客户机才能攻击成功。指导手册中真实服务器也在局域网，所以伪造的响应报文很难比真实服务器响应更快，建议选择外网的域名（比如baidu.com, 163.com等）进行测试，这样外网服务器返回响应的时间就要长一些，我们伪造的响应报文可以先于真实响应到达。

## 12. 远程DNS攻击时，在system调用dig命令之后，为什么伪造的第一个报文都比真实响应还慢？

解答：system("dig www.example.com");

sendto();

system语句是在执行完dig命令之后才会执行system之后的下一条sendto语句（system函数会阻塞在此），此时真实的响应报文已经到达apollo甚至是攻击主机了，后面再发送的伪造响应报文都肯定在真实响应之后。需要在dig命令之后加上 &符号，让dig命令放在后台运行，system立即返回,即改成system("dig [www.example.com](http://www.example.com) &");

## 13. 在vpn实验中，虚拟网卡选择工作在什么模式？

解答：为了不必要的麻烦，建议所有网卡全部选择工作在**网桥模式**下。网桥模式下，相当于所有的网卡接到了同一个交换机，利用ip地址来从逻辑上划分到不同的网络。

## 14. VPN实验中，可以只启用两个虚拟机，把自己的物理机也加入到实验环境中吗？

解答：可以。两个虚拟机分别做vpn客户端、VPN服务器，自己的物理机做内网主机。物理机作为实验环境的一部分，同时还可以上网的方法：

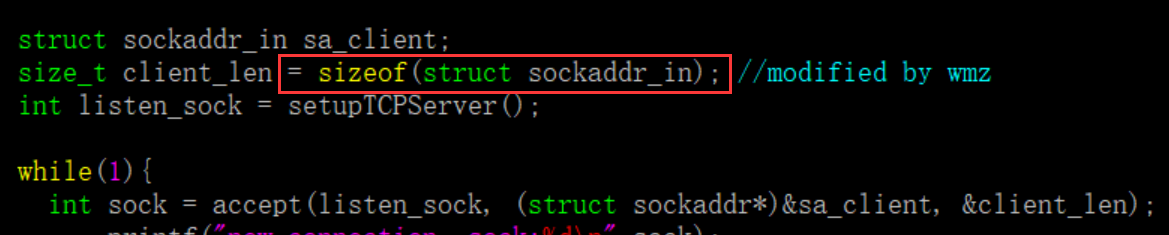
1）物理网卡上配置两个ip： 在物理网卡（上网的那个网卡）属性中将IP地址配置修改为静态配置方式（事先记下上网用的ip、掩码、网关、DNS配置），并且在高级设置里面增加一个内网ip地址

2）**物理机上增加到外网(10.0.2.0/24)和客户端虚拟网络的路由**，下一跳指向VPN服务器的内网接口IP

注意：物理机上可能有防火墙会阻挡掉来自VPN客户机的报文，可以考虑关闭防火墙或者修改规则。

## 15. 为什么在tls例程运行时，tlsclient和tlserver的tcp连接不成功？

解释: **tlsserver.c代码中有个错误**，client\_len需要初始化：



## 16. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示unknown ca错误

error:14094418:SSL routines:ssl3\_read\_bytes:tlsv1 alert unknown ca:s3\_pkt.c:1487: SSL alert number 48 的错误

解答：这是因为没有找到信任的证书链。

在客户机运行“c\_rehash 证书目录”，c\_rehash 为证书目录下的证书文件创建一个符号连接，并将此符号连接的名称设为文件的hash值，作用是让openssl在证书目录中能够找到证书。

## 17. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示:

error:14094416:SSL routines:ssl3\_read\_bytes:sslv3 alert certificate unknown:s3\_pkt.c:1487:SSL alert number 46 的错误

解答：

## 18. tlsclient和tlsserver建立ssl不成功，客户端验证服务器证书失败，服务器端提示error:14094415:SSL routines: ssl3\_read\_bytes: sslv3 alert certificate expired:s3\_pkt.c:1487:SSL alert number 45 的错误

解答：这个问题是因为**证书过期**了。如何查看证书的有效期：

windows下是可以双击证书，在详细信息里面看得到证书有效期

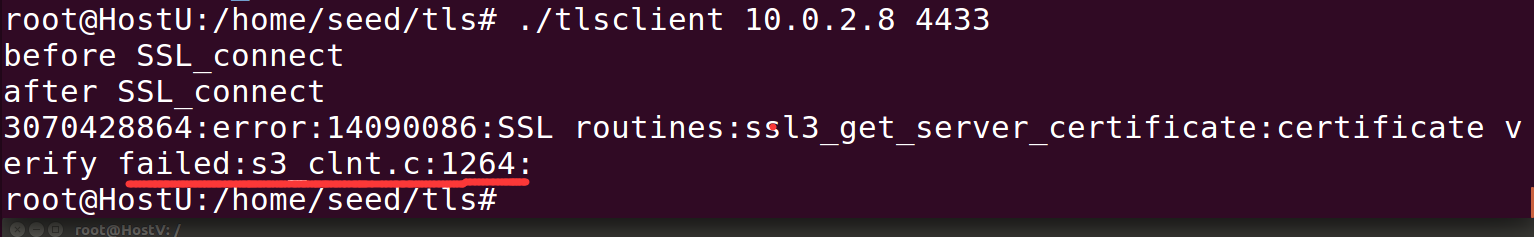
linux下可以用openssl命令查看：openssl x509 -in 证书文件名 -text 可以查看证书有效期。

解决办法1）懒人办法：将机器时间改到有效期之内

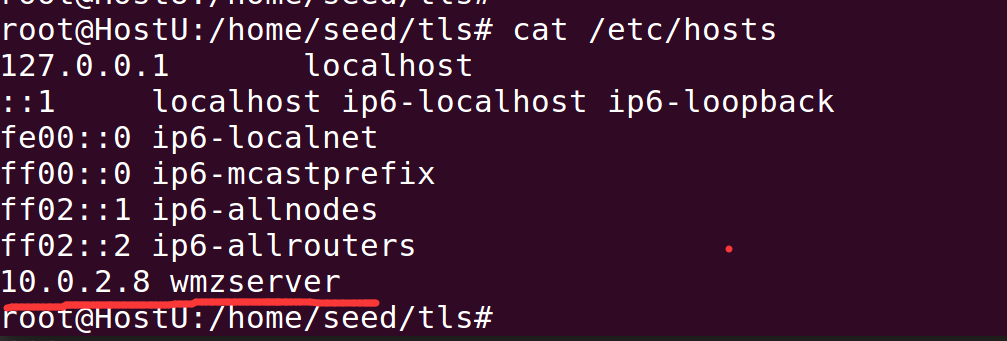
2） 重新生成证书，新生成的证书注意有可能因为时区的原因导致8小时候后才生效，也有可能及时生效。

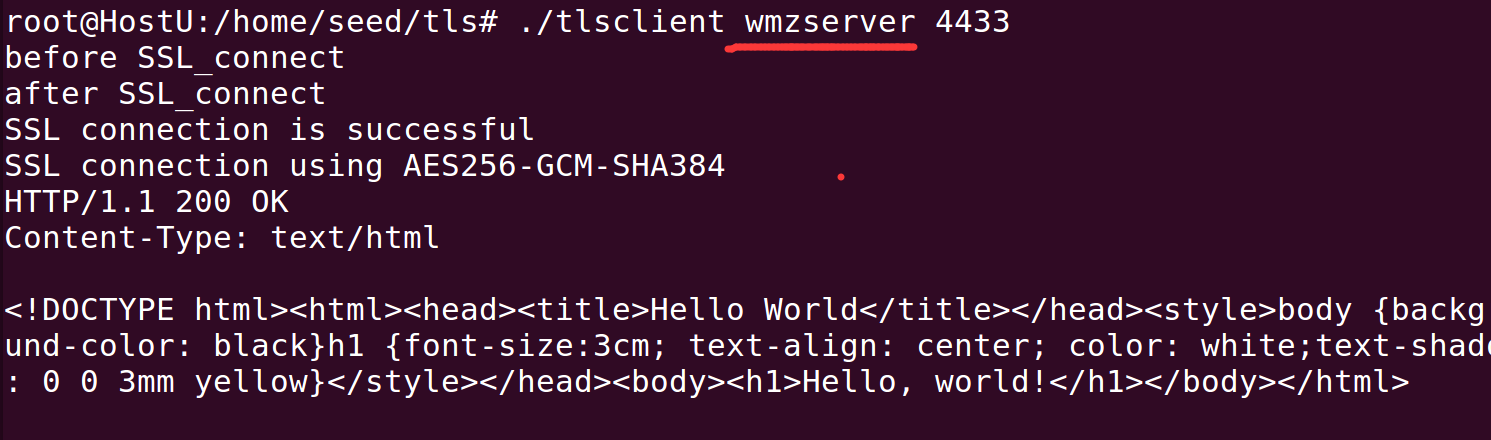
如果程序运行不再报45号错误，那说明这个问题解决了。

19. tlsclient和tlsserver建立不成功，客户端验证服务器证书失败：



解决办法：不能用服务器地址来进行访问，需要在/etc/hosts文件中增加服务器的域名，域名名字跟server证书主题（Subject）的CN（Common Name）字段名字一致





## 19. 在demo\_openssl\_api.zip中怎么只有.crt文件，没有.pem文件？.crt文件和.pem文件有什么差别

解答:.pem和.crt都是证书文件，只是文件名的不同而已，他们的格式都是PEM格式，在程序代码中都符合SSL\_FILETYPE\_PEM 格式。在windows下一般用.crt后缀，可以直接双击就可以解析证书文件内容。直接.pem文件的后缀改成.crt就能在windows下解析了。linux下证书文件可以用以下命令查看：

openssl x509 -in 证书文件 -text

## 20. VPN实验中，最后支持多客户端那个部分，内网主机返回的报文到达VPN服务器以后，tun0中的数据应该向哪个隧道转发？怎么区分？

解答：解决方式有多种:

1. 可以针对每个隧道做一个会话记录，记录客户端隧道ip（真实地址）、分配的虚ip地址、服务器端连接的套接字、跟客户端ssl会话的SSL指针等。那么就可以根据返回报文的目的地址（虚ip地址）来查会话表，从而确定跟客户端的SSL信息。也就是说最好在建立隧道的时候，服务器能有分配虚ip的机制，告诉客户端该虚ip地址信息，并且服务器在内存维护这样的一个会话表。（此方案服务器端适合采用单进程）  
  
  
2. 还有另一种实现方式，openvpn是一个开源的典型的sslvpn软件，它既有上面的这种模式，也有子网模式，每个客户端跟服务器建立隧道以后，服务器给每个客户端分配一个/30的虚拟子网（一个虚地址给客户端tun接口，一个地址给服务器端的虚接口）,服务器为每个隧道启动1个tun接口，这样服务器就会有多个tun接口，tun0、tun1....，每个tun接口上会有对应的虚拟子网路由，内网主机返回的报文，直接根据目的地址(虚IP地址）查找路由就可以找到对应的tun接口。（此方案服务器可以采用多进程，如下图所示，看蓝色手绘标注线）

