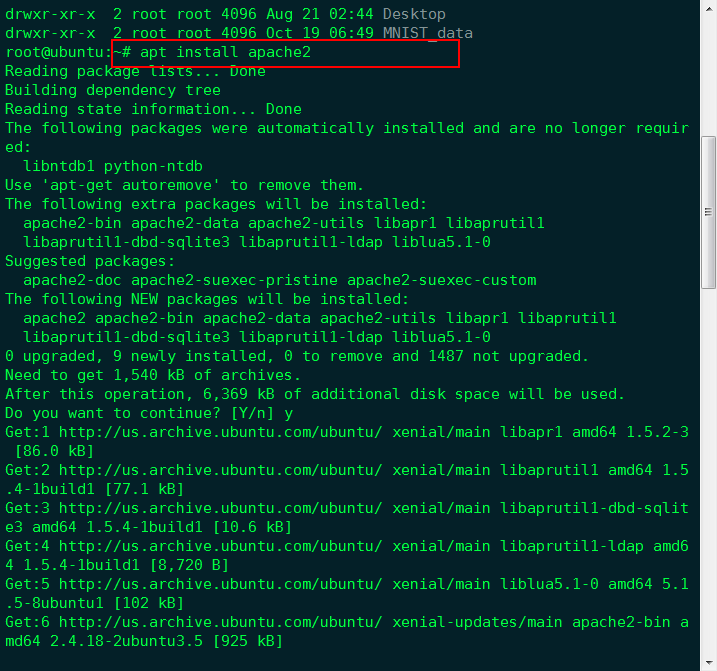
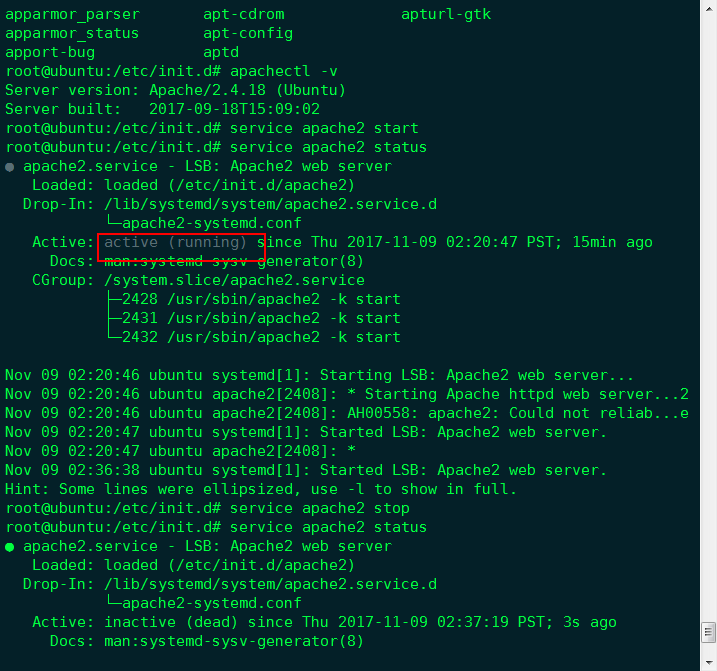
1. **搭建HTTP服务器**

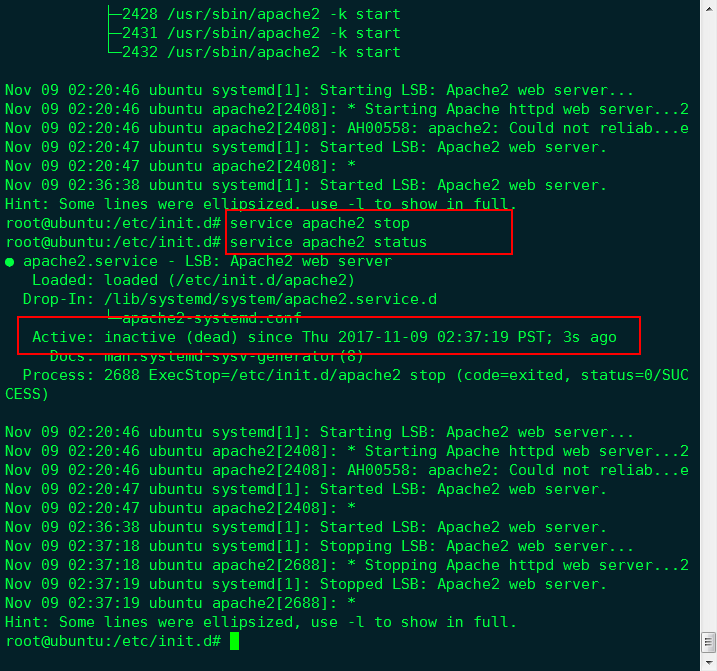
1) 实验准备：Linux虚拟机作为HTTP服务器，服务器软件选择Apache。

2) 安装apache2。



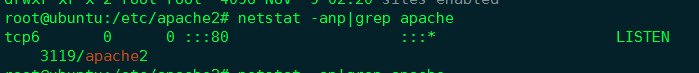
3) 如何查看apache2服务的状态？如何开启、停止、重启apache2服务？



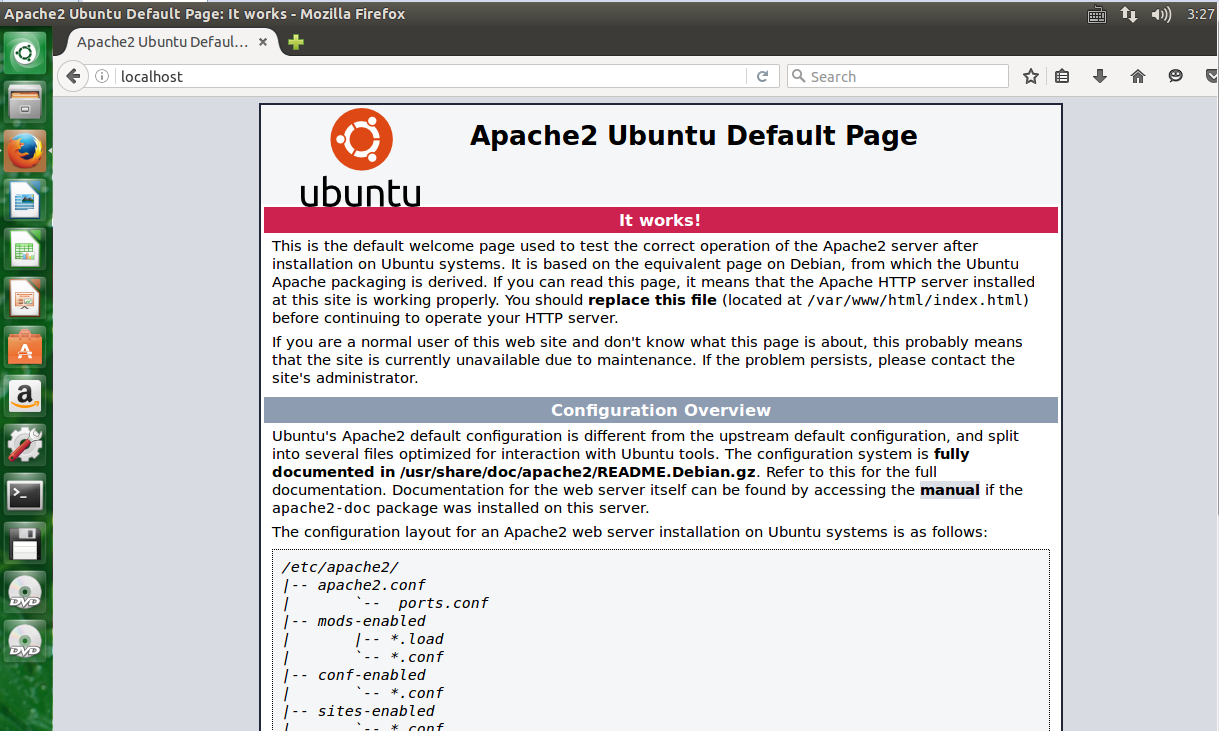


4) 开启apache2服务后，默认开放了哪个端口？

提示：nmap



5) 测试Apache。在Windows虚拟机上打开IE浏览器，访问：



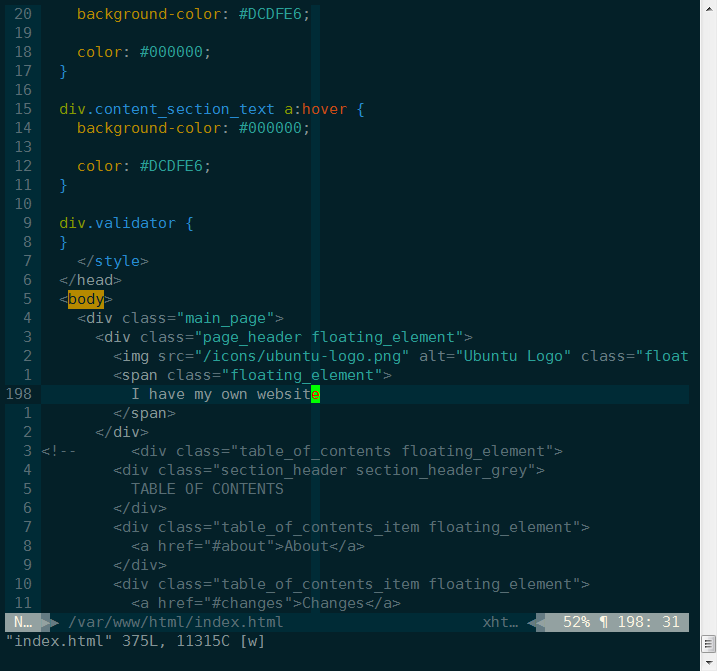
6) Apache常用的目录：

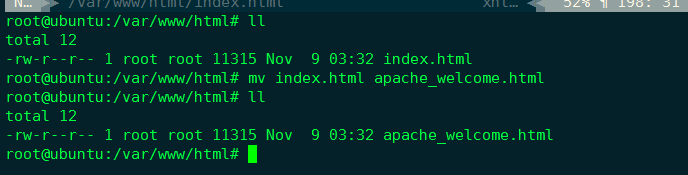
|  |  |
| --- | --- |
| Web目录 | /var/www |
| 安装目录 | /etc/apache2/ |
| 全局配置 | /etc/apache2/apache2.conf |
| 监听端口 | /etc/apache2/ports.conf |
| 虚拟主机 | /etc/apache2/sites-enabled/000-default.conf |

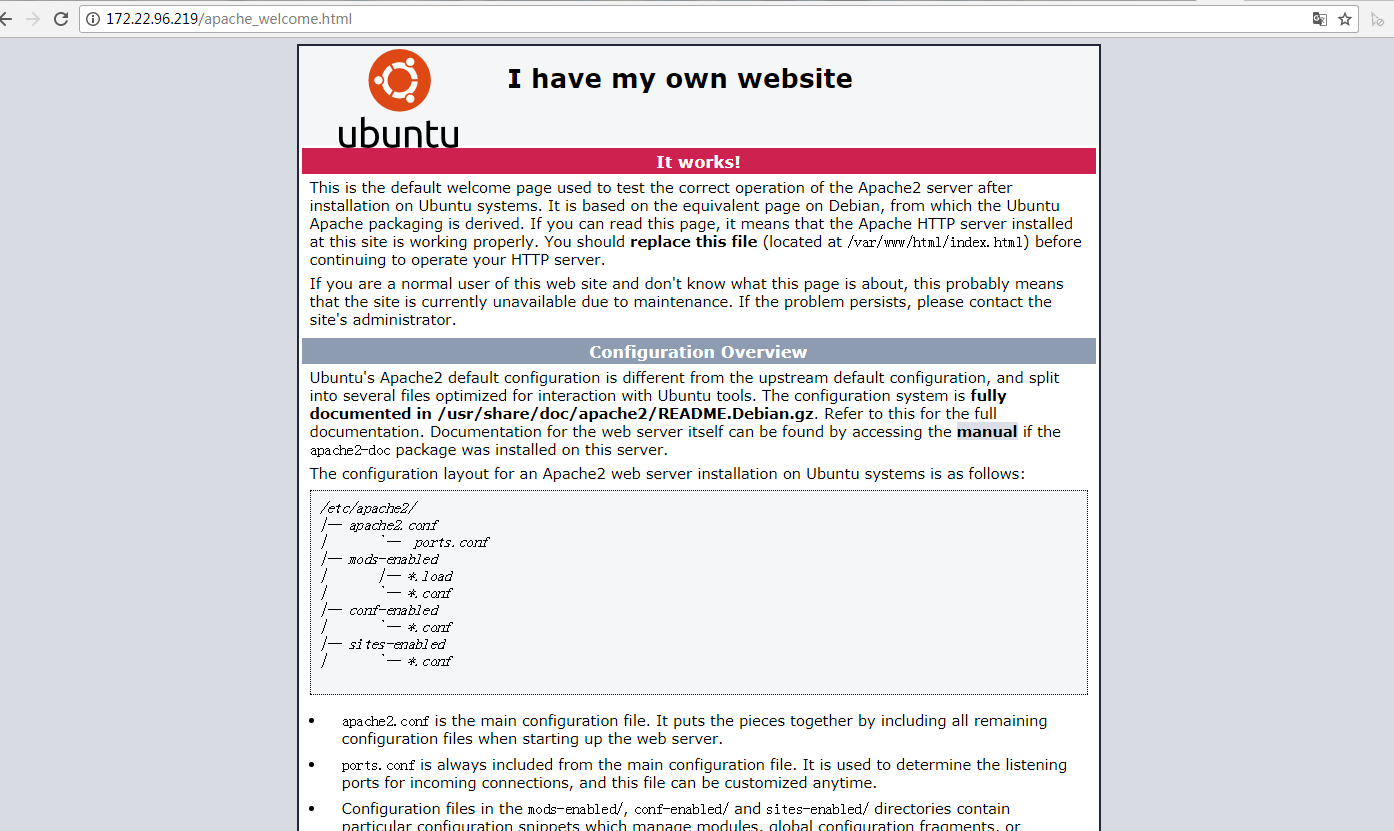
当浏览器访问服务器时，如果未指定所访问的资源名称，则默认寻找根目录下的index.html或default.html，视服务器类型而定。将/var/www/html/目录下的index.html重命名为apache\_welcome.html。在该目录下新建index.html，文件内容遵循HTML语法（不熟悉HTML语法结构的同学，可参考下图）。在Windows虚拟机上打开IE浏览器，访问：

*http://*服务器的*IP*

*http://*服务器的*IP/apache\_welcome.html*



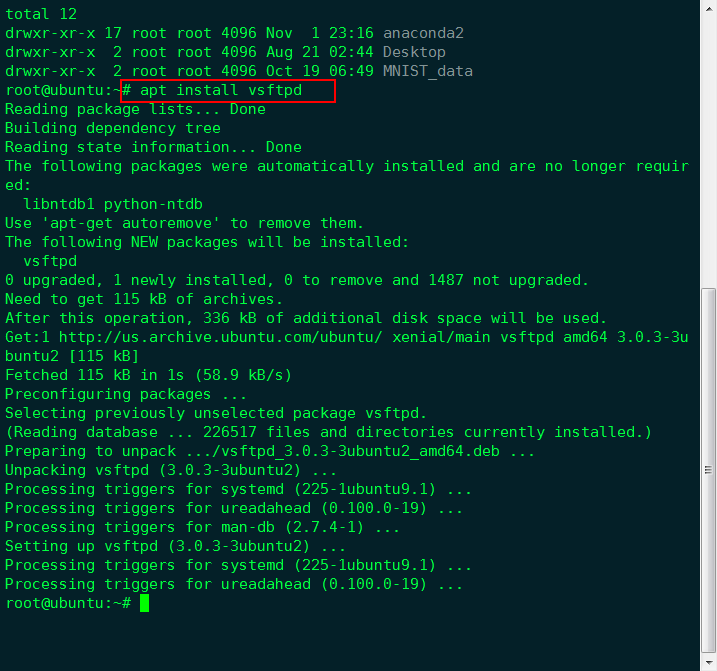




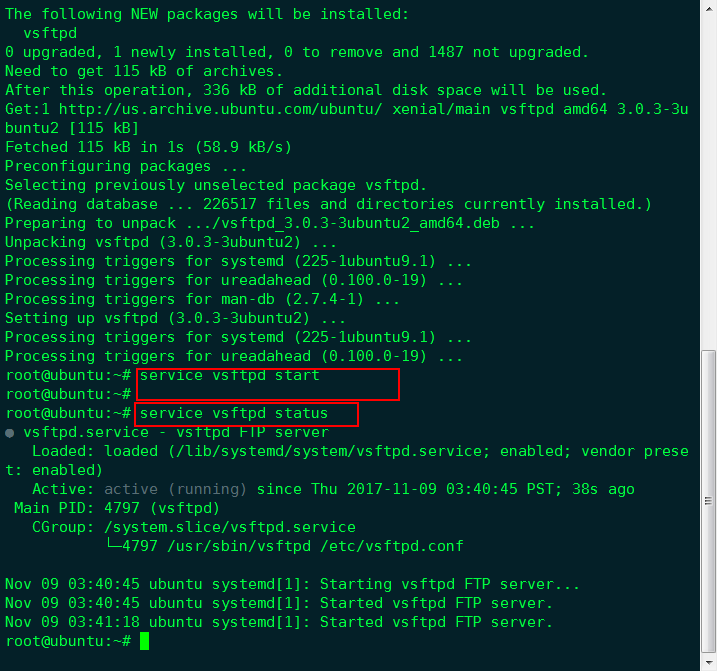
1. **搭建FTP服务器**

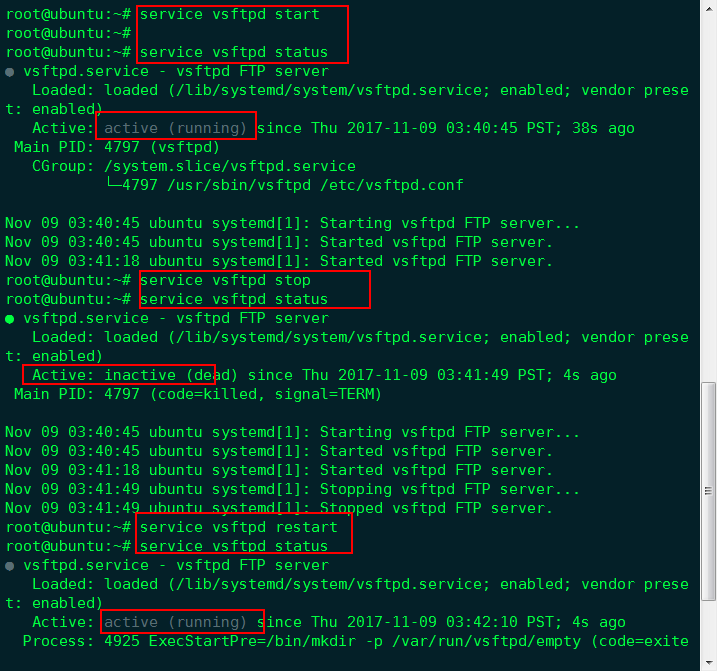
1) 实验准备：Linux虚拟机作为FTP服务器。

2) 安装vsftpd。

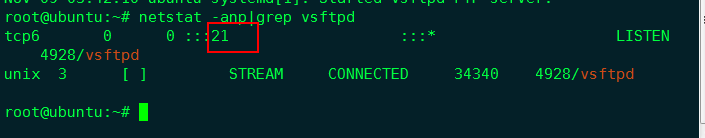


3) 如何查看vsftpd服务的状态？如何开启、停止、重启vsftpd服务？





4) 开启vsftpd服务后，默认开放了哪个端口？



5) 修改配置文件/etc/vsftpd.conf

【25行】将anonymous\_enable=YES 改为anonymous\_enable=NO（是否允许匿名ftp，若不允许选NO）

取消如下配置前的注释符号：

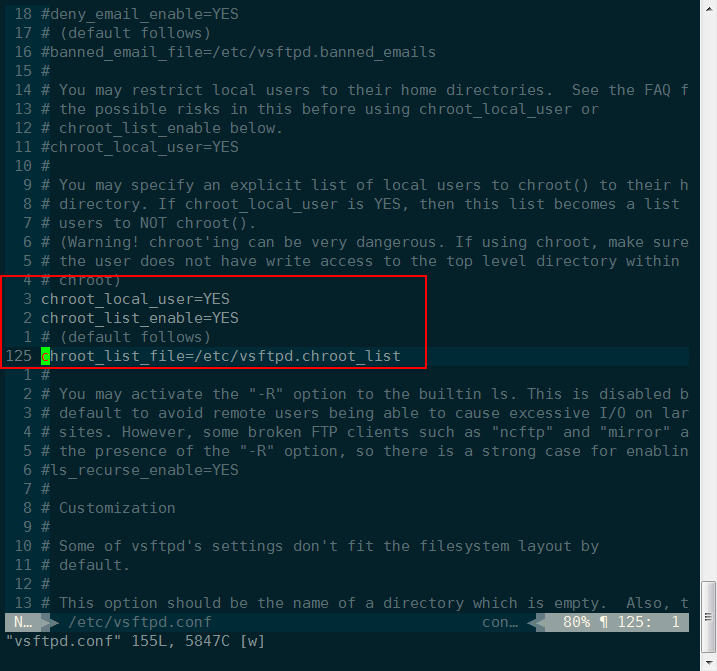
【28行】local\_enable=YES（是否允许本地用户登录）

【31行】write\_enable=YES（是否允许本地用户写的权限）

【122行】chroot\_local\_user=YES（是否将所有用户限制在主目录）

【123行】chroot\_list\_enable=YES（是否启动限制用户的名单）

【125行】chroot\_list\_file=/etc/vsftpd.chroot\_list（可在文件中设置多个账号）



6) 新建/etc/vsftpd.chroot\_list，文件内容为所有允许使用FTP协议访问服务器资源的用户。以换行作为不同用户的分隔符，如：

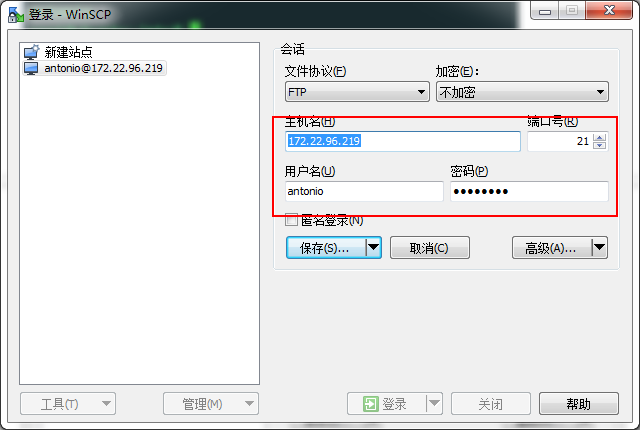


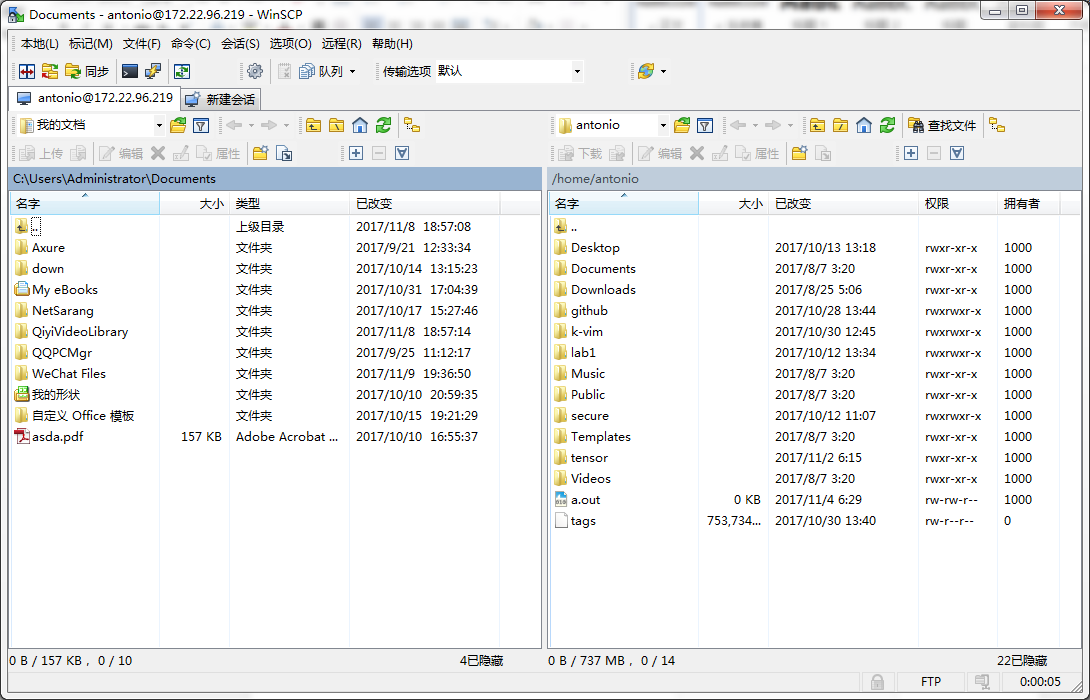
7) 重启vsftpd服务。



8) 测试FTP。在Windows虚拟机上，尝试使用以下四种方式，访问FTP服务器的资源：

工具，如WinSCP、FileZilla、XFTP。可在师大云盘-软件工具下载WinSCP。



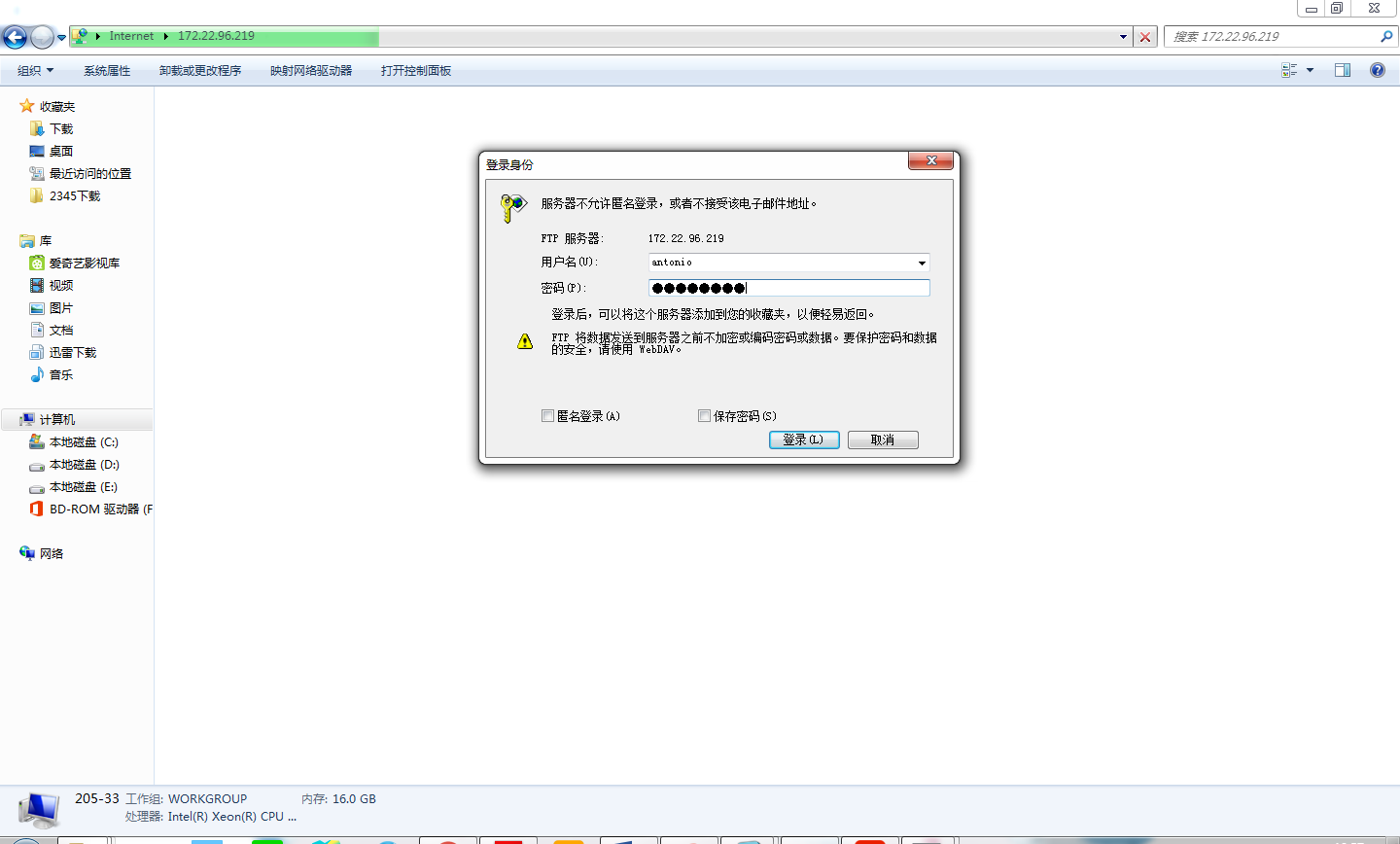


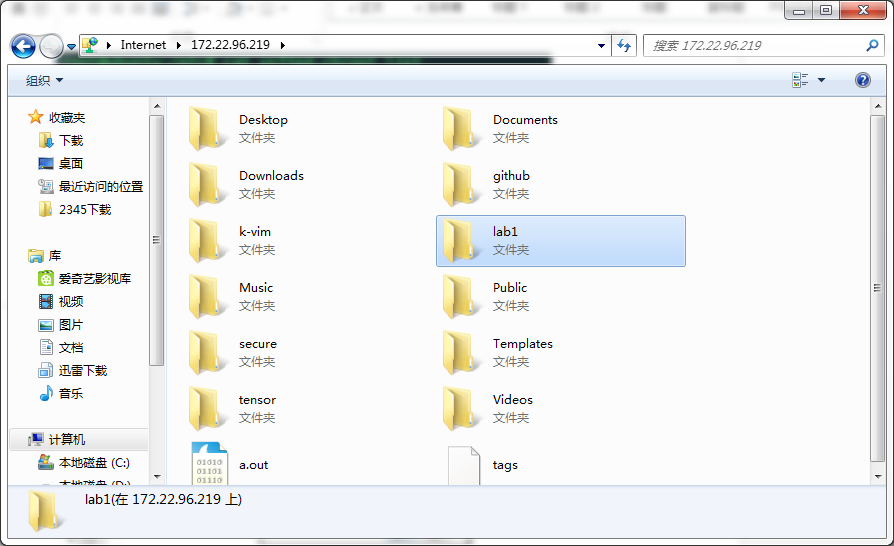
浏览器。地址栏访问：ftp://服务器的*IP*



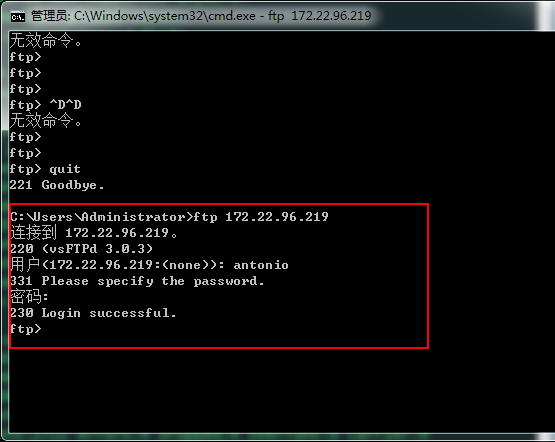


资源管理器/我的电脑/计算机。地址栏访问：ftp://服务器的*IP*





命令行/CMD。执行：ftp 服务器的*IP*

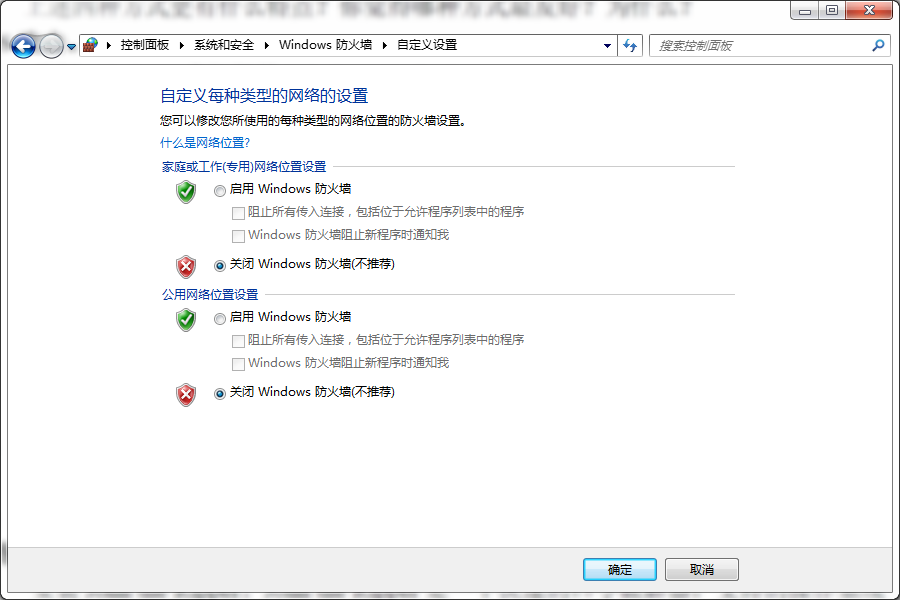


**资源管理器/我的电脑/计算机** 这种方式更加方便，相当于本地一样

**3. DoS**攻击。

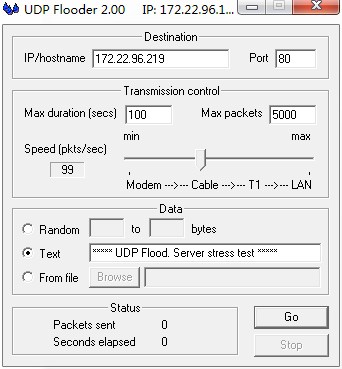
1) 关闭Windows虚拟机的Windows Defender。

提示：开始菜单——设置——更新和安全——Windows Defender

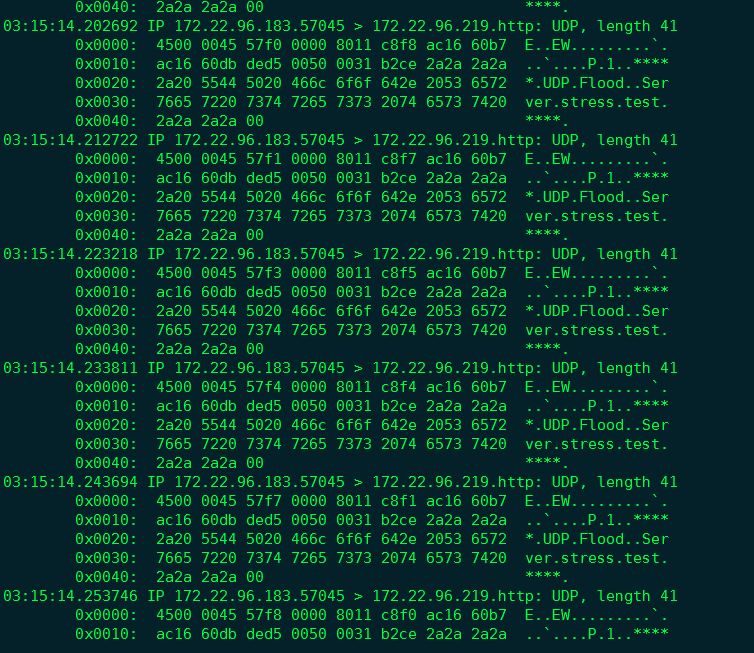


2) 对服务器的80端口做UDP洪水攻击。在Windows虚拟机上打开UDP Flood软件，做如下配置：

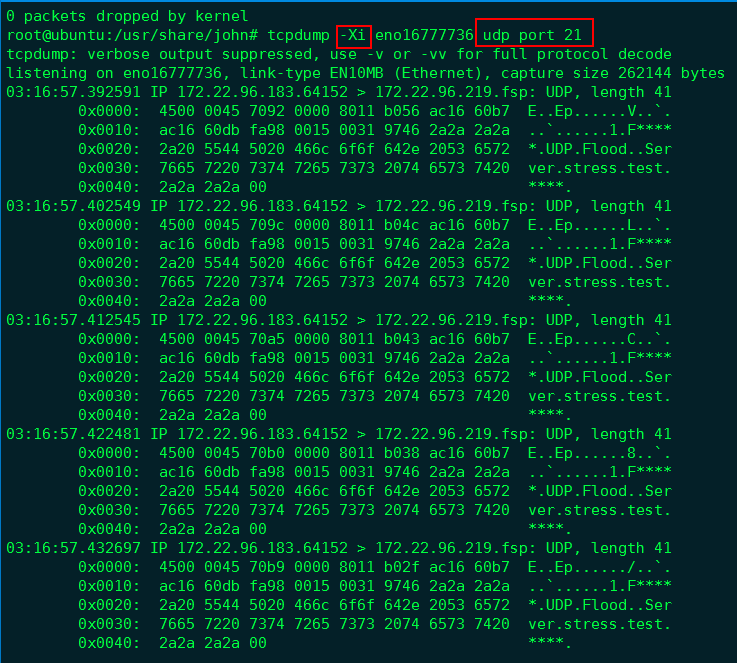
|  |  |
| --- | --- |
| IP/hostname | 服务器IP |
| Port | 80、21 |
| Max duration | 100 |
| Max packets | 5000 |
| Speed | 99 |



开始攻击后，在服务器端使用tcpdump抓包。数据包的内容是什么?



3) 对服务器的21端口做UDP洪水攻击。开始攻击后，在服务器端使用tcpdump抓包。数据包的内容是什么？



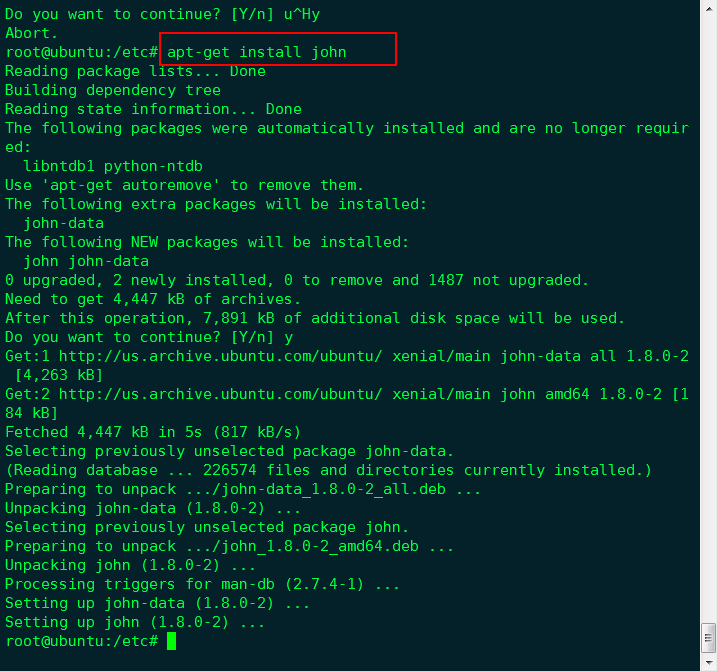
4) 通过实验，你对UDP洪水攻击有怎样的理解？

可以无限制的发送udp包，从而导致服务器崩溃。

**4.** 口令攻击。

1) 安装John the Ripper。John the Ripper是一个快速的口令破解器，支持的操作系统有UNIX、Linux、DOS、Windows等。

提示：*apt-get install john*



2) 在Linux虚拟机上，用户名/密钥方面的详细信息存储在下面这两个文件中：

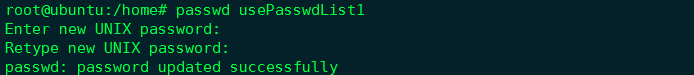
/etc/passwd

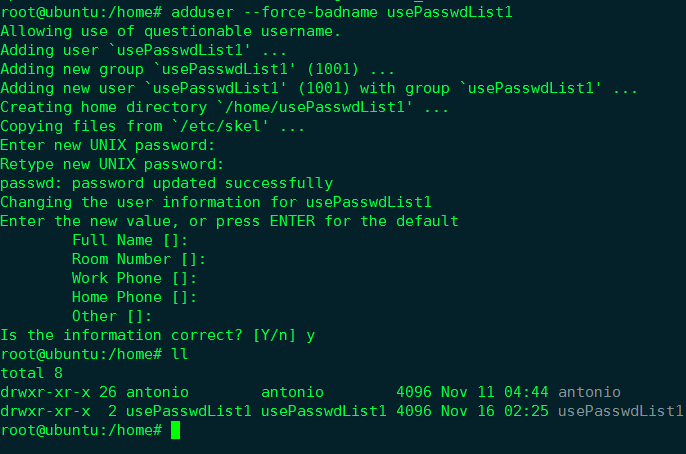
/etc/shadow

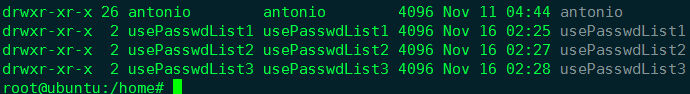
3) 使用密码列表做口令攻击。使用useradd、passwd命令，创建如下测试用户：

|  |  |
| --- | --- |
| 用户名 | 密码 |
| usePasswdList1 s | admin |
| usePasswdList2 | apple |
| usePasswdList3 | hello |



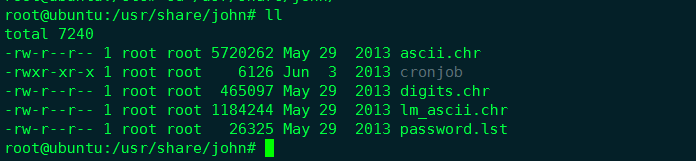


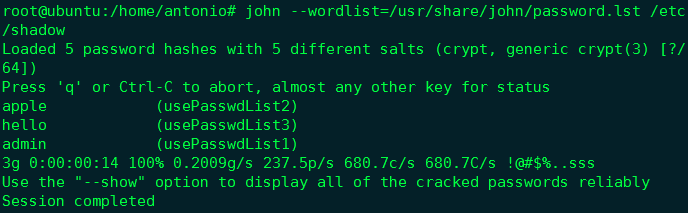




上述三个密码均存在于John自带的密码列表文件/usr/share/john/passwd.lst中。使用John对Linux虚拟机做口令攻击，能得到怎样的破解结果？

提示：*john --wordlist=*密码列表文件 /etc/shadow

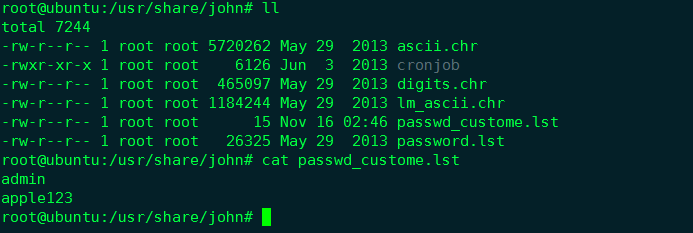


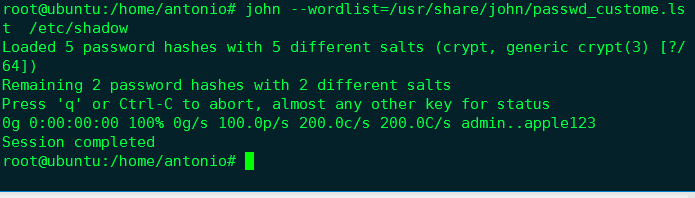


4) 使用自定义的密码列表做口令攻击。使用useradd、passwd命令，创建如下测试用户：

|  |  |
| --- | --- |
| 用户名 | 密码 |
| cusPasswdList1 | admin |
| cusPasswdList2 | apple |
| cusPasswdList3 | hello |

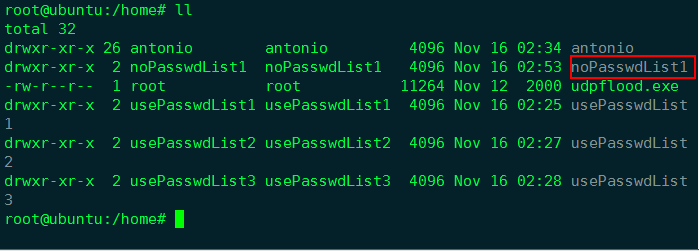
在/usr/share/john/目录中新建自定义的密码列表文件passwd\_custome.lst，文件格式可参考passwd.lst，文件内容包含如下两个密码：admin、apple123。使用John对Linux虚拟机做口令攻击，能得到怎样的破解结果？





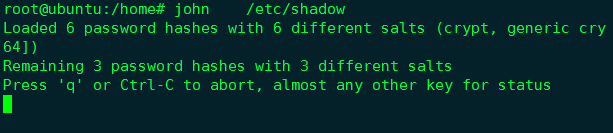
5) 不使用密码列表做口令攻击。使用useradd、passwd命令，创建如下测试用户：

|  |  |
| --- | --- |
| 用户名 | 密码 |
| noPasswdList1 | ad |



使用John对Linux虚拟机做口令攻击，能得到怎样的破解结果？

提示：*john /etc/shadow*



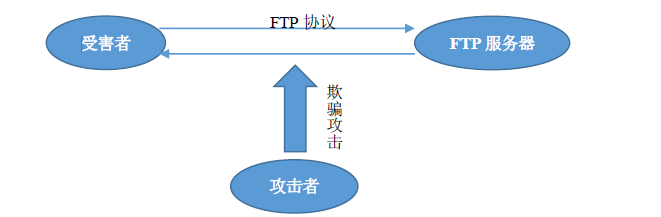
发现经过好久也没有破解密码

6) 通过实验，你对口令攻击有怎样的理解？

使用密码列表可以更快的破解密码

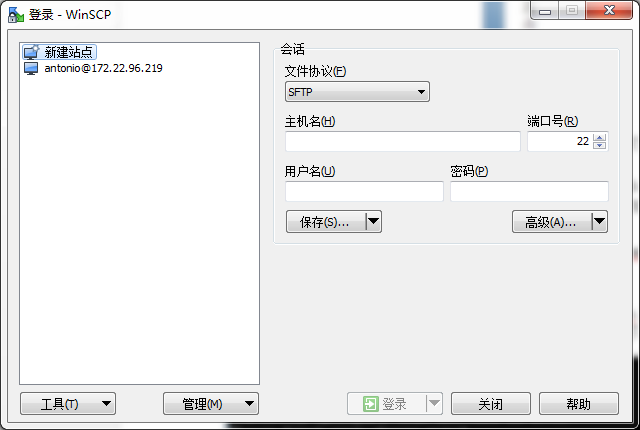
**5.** 欺骗攻击。

1) 演示ARP欺骗攻击，攻击者想得知受害者经常登录的FTP用户名和密码。攻击模型如下：



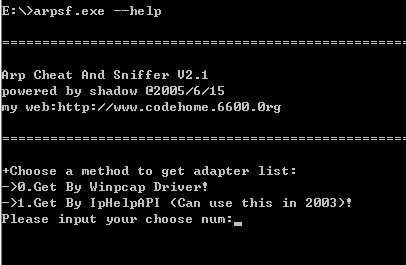
原Windows虚拟机作为攻击者，新建一个Windows虚拟机作为受害者，Linux虚拟机作为FTP服务器。

2) 【攻击者】安装WinPcap、Arp cheat sniff。Arp cheat and sniffer 是国内开源软件，它是一款Arp sniffer工具，可以通过Arp欺骗嗅探目标主机TCP、UDP和ICMP协议数据包。使用需要Winpacp支持。



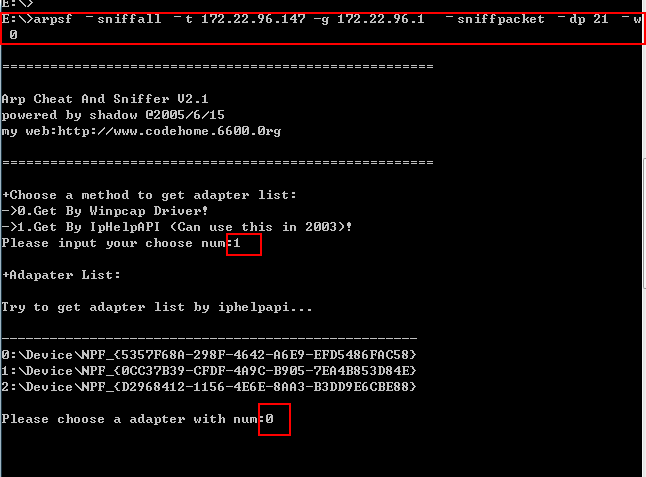
3) 【攻击者】打开CMD，进入arpsf.exe所在目录。查阅arpsf命令手册，使用Arp cheat sniff对受害者做欺骗攻击。





提示：*arpsf* –*sniffall* –*t* 受害者*IP* –*g* 网关*IP* –*sniffpacket* –*dp 21* –*w 0*

执行该命令后，会询问用户配置，分别选择1、0即可。如下：



4) 【受害者】打开IE浏览器，访问FTP服务器。

5) 【攻击者】当受害者计算机的用户登录了FTP后，攻击者的Arp cheat sniff就可以把受害者的操作记录下来。从中即可找到受害者经常使用的FTP用户名及密码。