Brainpan

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Sat Jun  6 14:54:51 2020 as: nmap -sC -sV -oN portscn 10.10.6.5
Nmap scan report for 10.10.6.5
Host is up (0.22s latency).
Not shown: 998 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=7.80%I=7%D=6/6%Time=5EDB3DC6%P=x86_64-pc-linux-gnu%r(NUL
SF:L,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\
SF: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\x2
SF:0\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\x
SF:20\x20\x20_\|_\|_\|\x20\x20_\|_\|_\|\x20\x20\n_\|\x20\x20\x20\x20_\|\x2
SF:0\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_\|\x2
SF:0\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\x2
SF:0_\|\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_\|\n_\|_\|_\|\x20\x2
SF:0\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\x2
SF:0_\|_\|_\|\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
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\x2
SF:0\x20\x20\x20\x20\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_\|\n\n\[_____\x20WELCOME\x20TO\x20BRAINPAN\x2
SF:0_____\]\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\x20ENTER\x2
SF:0THE\x20PASSWORD\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\n\n\x
SF:20\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");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun  6 14:55:47 2020 -- 1 IP address (1 host up) scanned in 56.37 seconds
```

Targets

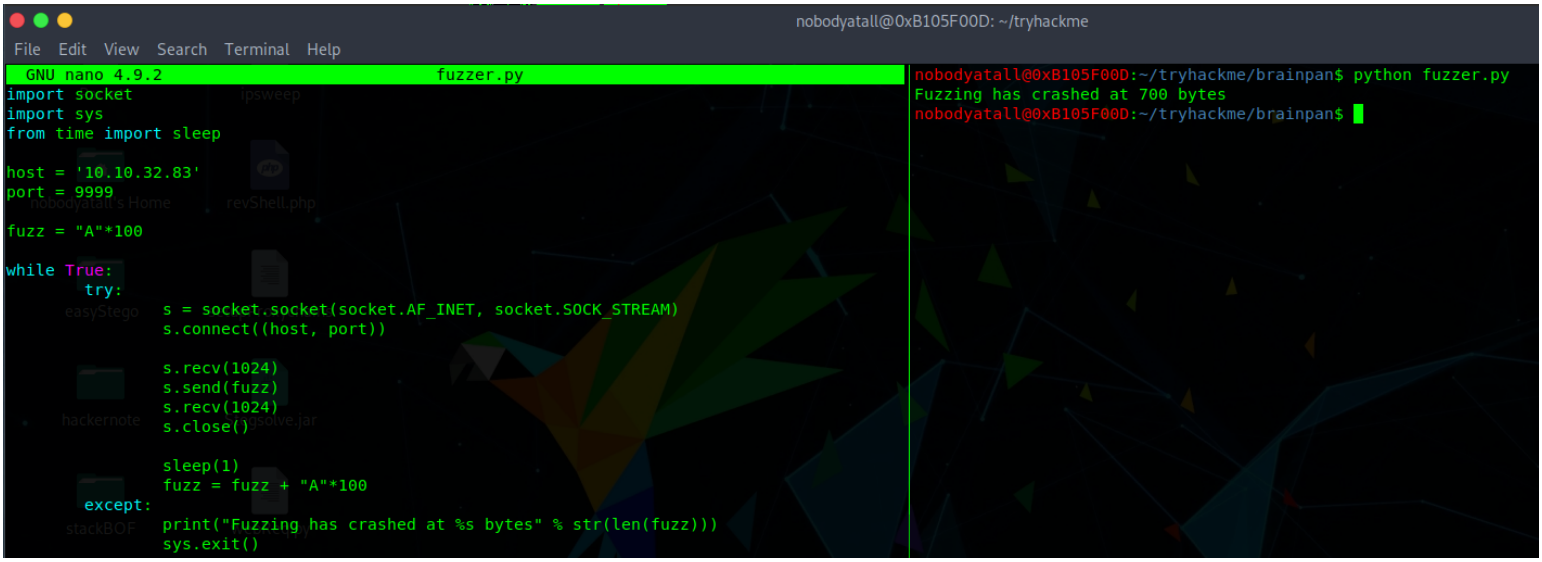
port 9999

running a binary program
==========
-tried to send bunch of string and it caused the program to crash

```
nobodyatall@0xB105F00D:~/tryhackme/brainpan$ python -c 'print "a"*1000' | nc -v 10.10.6.5 9999
10.10.6.5: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.6.5] 9999 (?) open
_|                      _|
_|_|_|    _|  _|_|    _|_|_|      _|_|_|    _|_|_|      _|_|_|  _|_|_|
_|    _|  _|_|      _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
_|    _|  _|        _|    _|  _|  _|    _|  _|    _|  _|    _|  _|    _|
```

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

[_____________________________ WELCOME TO BRAINPAN _____________________________]
                        ENTER THE PASSWORD

                        >> nobodyatall@0xB105F00D:~/tryhackme/brainpan$ python -c 'print "a"*1000' | nc -v
10.10.6.5 9999
10.10.6.5: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.6.5] 9999 (?) : Connection refused
```

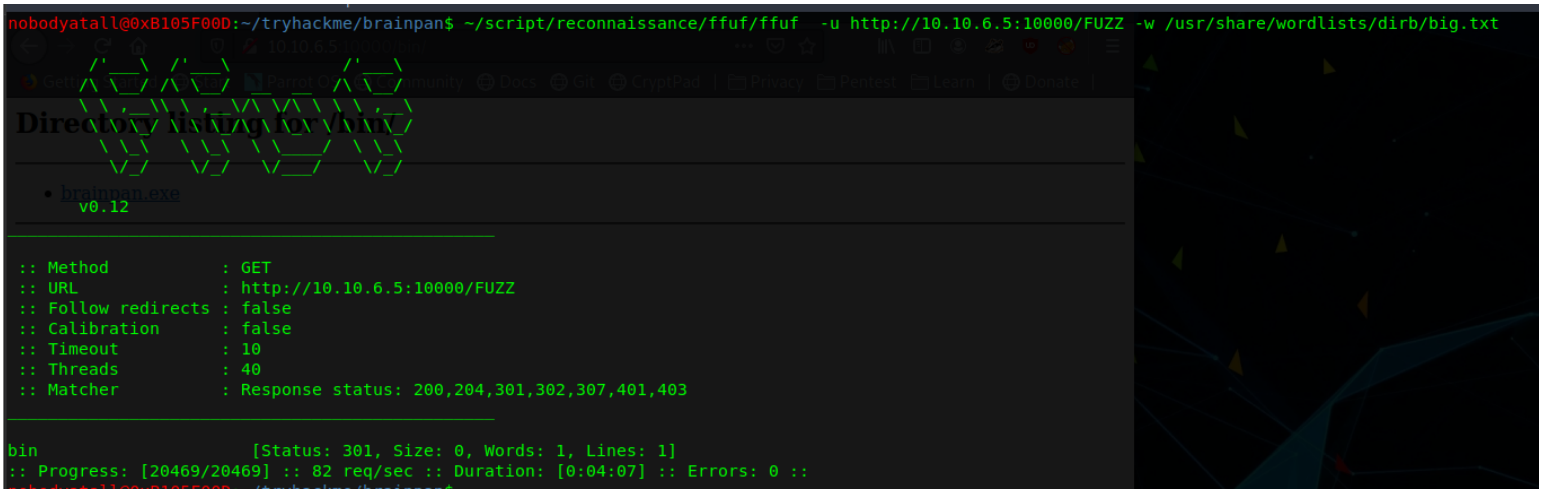
//it's vulnerable to buffer overflow

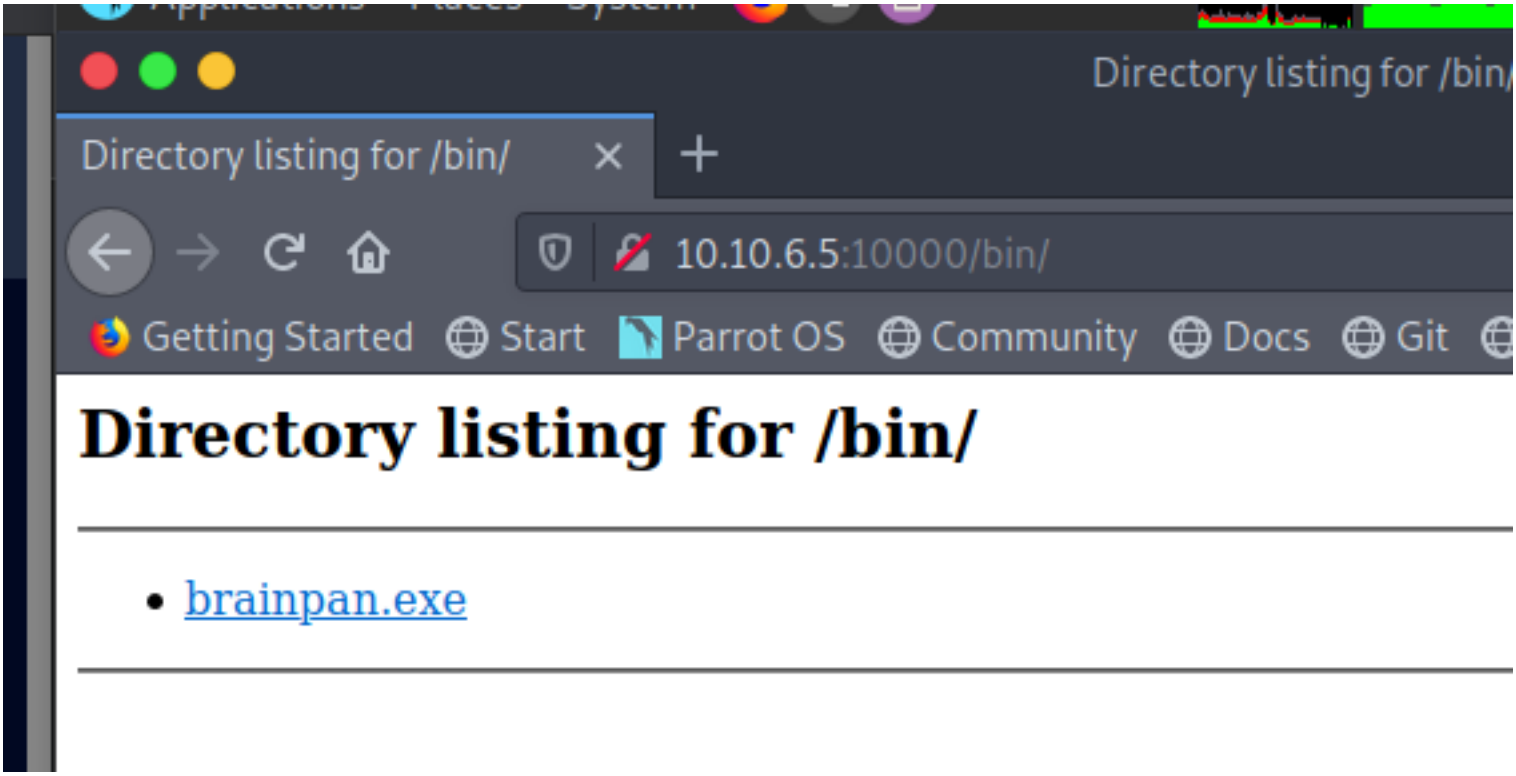


//program crashed

port 10000 (SimpleHTTPServer)

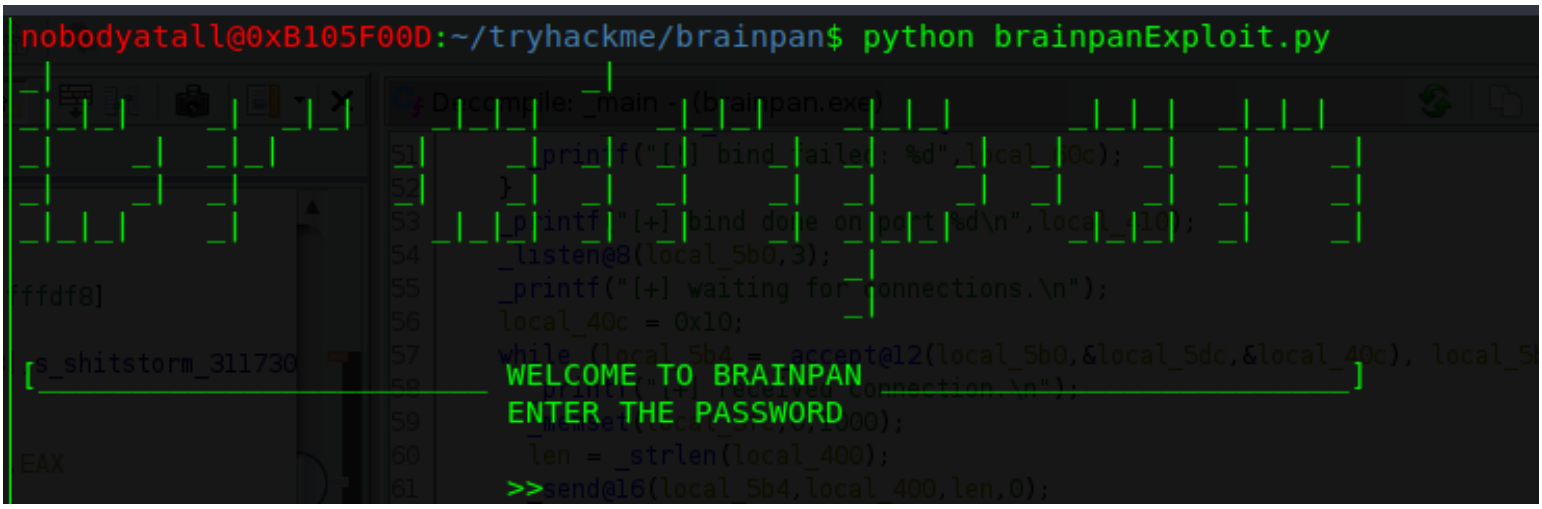
/bin found windows binary





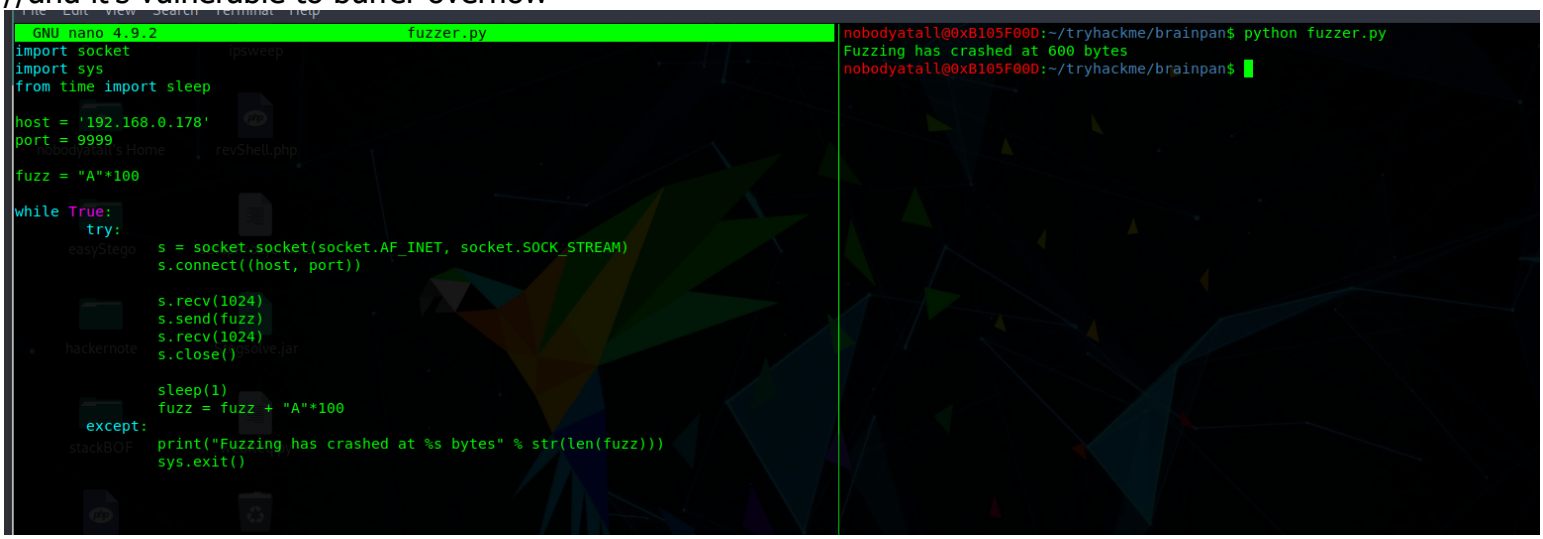
brainpan revEng

-seems like the same program listening in port 9999

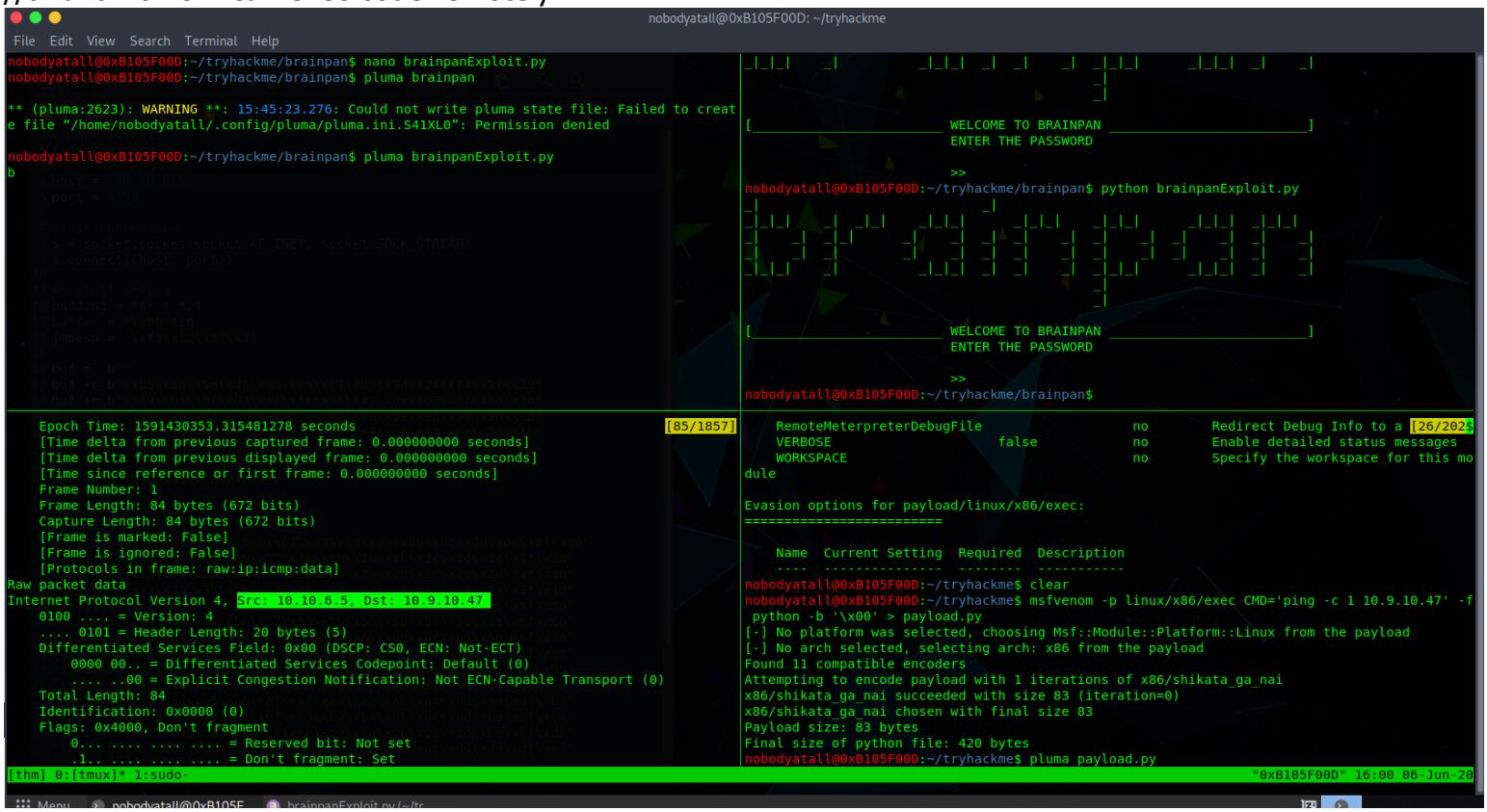


-password is shitstorm
//but seems useless even get the correct pw

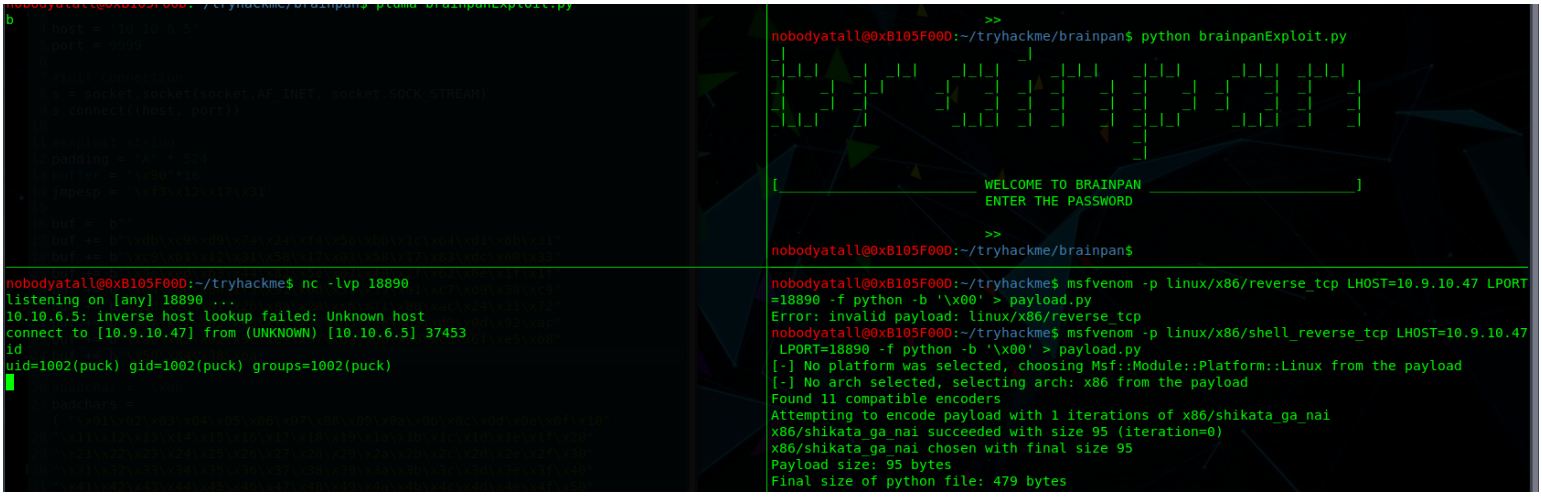
try fuzzing to see does it vulnerable to buffer overflow?
//and it's vulnerable to buffer overflow



//after done writing the exploit (try to exec ping back to my machine)
//and it works! i can exec code remotely



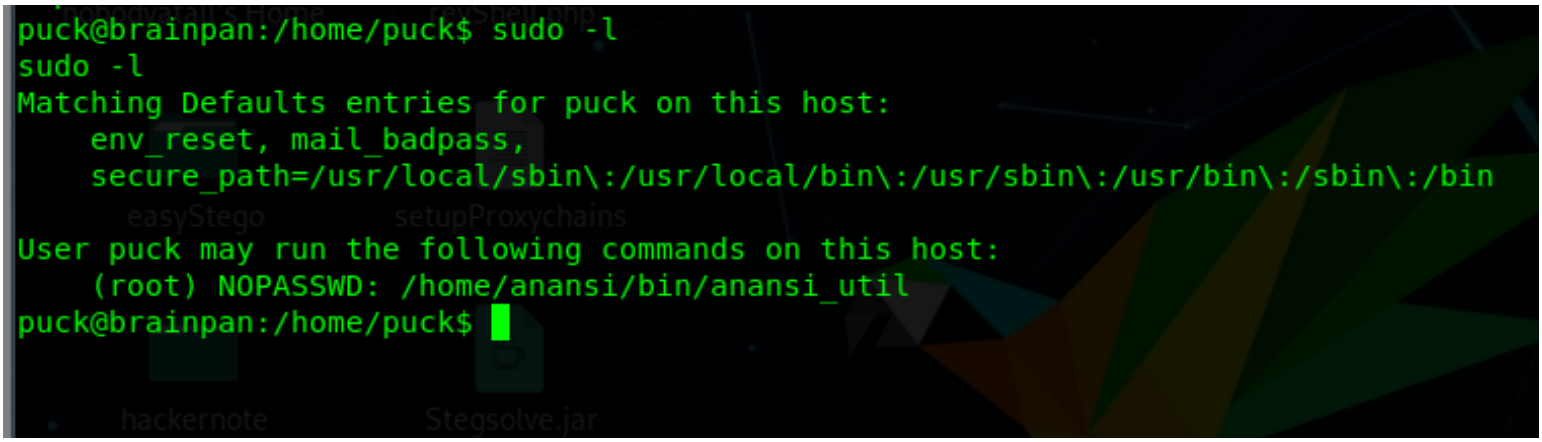
got initial foothold
//msfvenom shellcode payload: linux/x86/shell_reverse_tcp



Post Exploitation

Privilege Escalation

found sudo -l this binary can exec as root user without password
==========



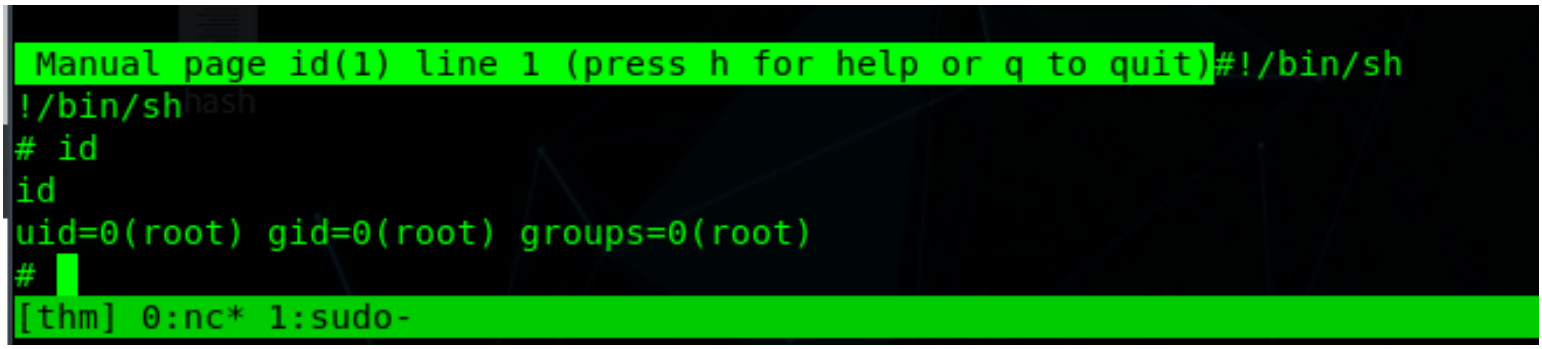
try to enumerate with the binary options (manual seems interesting)

```
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$
```

interesting it seems like this manual page exec as a root user now, let's try to escape it

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual id
sudo /home/anansi/bin/anansi_util manual id
No manual entry for manual
ID(1)                          User Commands                          ID(1)

NAME
       id - print real and effective user and group IDs

SYNOPSIS
       id [OPTION]... [USERNAME]

DESCRIPTION
       Print  user  and group information for the specified USERNAME, or (when
       USERNAME omitted) for the current user.

       -a     ignore, for compatibility with other versions

       -Z, --context
              print only the security context of the current user

       -g, --group
              print only the effective group ID

       -G, --groups
              print all group IDs

 Manual page id(1) line 1 (press h for help or q to quit)
[thm] 0:nc* 1:sudo-
```

escaping te man page(spawning shell)



root user now!!!

Creds

Flags

Write-up Images