Cronos

nmap

```
┌──(kali㉿kali)-[~/htb/Cronos]
└─$ cat nmap/initial.txt
# Nmap 7.93 scan initiated Tue Jun 20 07:12:05 2023 as: nmap -sC -sV -oN nmap/initial.txt 10.10.10.13
Nmap scan report for 10.10.10.13
Host is up (0.088s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18b973826f26c7788f1b3988d802cee8 (RSA)
|   256 1ae606a6050bbb4192b028bf7fe5963b (ECDSA)
|_  256 1a0ee7ba00cc020104cda3a93f5e2220 (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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 20 07:12:23 2023 -- 1 IP address (1 host up) scanned in 17.91 seconds
```

- Simple Apache web server, let's investigate port 80

dig

Attempting to view http://10.10.10.13, we see the default Apache page

We can identify the domain name with the following command:

```
┌──(kali㉿kali)-[~/htb/Cronos]
└─$ nslookup 10.10.10.13 10.10.10.13
13.10.10.10.in-addr.arpa        name = ns1.cronos.htb.
```

Now that we know the domain name, we can add it to /etc/hosts
Then, we want to reveal subdomains using dig:

```
└─$ dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.18.12-1-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: 84 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (TCP)
;; WHEN: Tue Jun 20 07:27:54 EDT 2023
;; XFR size: 7 records (messages 1, bytes 203)
```

Navigating to admin.cronos.htb (after adding to /etc/hosts of course) we see a login panel

SQL Injection

SQL Injection vulnerability on username

With a valid username, we can comment out the rest of the authentication with the following:
username: admin'-- -

This bypasses the login panel

www-data

Simple command injection to get a reverse shell

priv esc

Interesting finding while running LinEnum:
* * * * * root php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1

cron is running this command as root periodically, and www-data has write permissions.
We can edit the file to contain a php reverse shell.

easy root!!