Easy Peasy

POC

1- port 80 and 65524 are web servers ,6984 is ssh port :)
2- gobuster showed a hidden dir in 80 webs server
3- nothing interesting so again busted this url ;)(
4- found a /whatever directory so full url is ip/hidden/whatever
5- FOund the first flag flag{f1rs7_fl4g}
6- apache port showed had a perculiar robots.txt robots.txt
7- Found a encoded value on main source
8- found a secret dir on this port as /n0th1ng3ls3m4tt3r secret dir
9- got a encoded value
10- Got a possible password mypasswordforthatjob
11- this page had a image and it was named wierd so we downloaded it and it was wierd(hint)
12- Now this pic is not letting us steghide extraction from it so i used stegcracker to crack passphrase
13- the password we found above was same as what we found from cracking that hash on main page of apache web server mypasswordforthatjob Image on main page
14- got a secrettext.txt
15- got username and password in binary Johntheripper
16- credentials are boring:iconvertedmypasswordtobinary
17- user flag was decoded in rot13
18- Crontab showed a file in var /www Privesc
19- we had full write access so we wrote a bash reverse shell and got a shell Privesc
20- rooted

Enumeration

Nmap

```
nmap -p 80,6498,65524 -T4 -A 10.10.15.166
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-02 15:59 EDT
Nmap scan report for 10.10.15.166
Host is up (0.45s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.16.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx/1.16.1
|_http-title: Welcome to nginx!
6498/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 30:4a:2b:22:ac:d9:56:09:f2:da:12:20:57:f4:6c:d4 (RSA)
|   256 bf:86:c9:c7:b7:ef:8c:8b:b9:94:ae:01:88:c0:85:4d (ECDSA)
|_  256 a1:72:ef:6c:81:29:13:ef:5a:6c:24:03:4c:fe:3d:0b (ED25519)
65524/tcp open  http    Apache httpd 2.4.43 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.43 (Ubuntu)
|_http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   197.15 ms 10.4.0.1
2   ... 3
```

4 452.30 ms 10.10.15.166

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.65 seconds

Web port 80

Gobuster

```
gobuster dir -u 10.10.15.166 -w WordLists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.15.166
[+] Threads:        10
[+] Wordlist:       WordLists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/02 15:58:45 Starting gobuster
===============================================================
/hidden (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
===============================================================
2021/04/02 16:02:27 Finished
===============================================================
```

/Hidden directory busting

```
 gobuster dir -u 10.10.15.166/hidden -w WordLists/dirb/common.txt                                    130 ×
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.15.166/hidden
[+] Threads:        10
[+] Wordlist:       WordLists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/02 16:09:59 Starting gobuster
===============================================================
/index.html (Status: 200)
/whatever (Status: 301)
===============================================================
2021/04/02 16:13:32 Finished
===============================================================
```

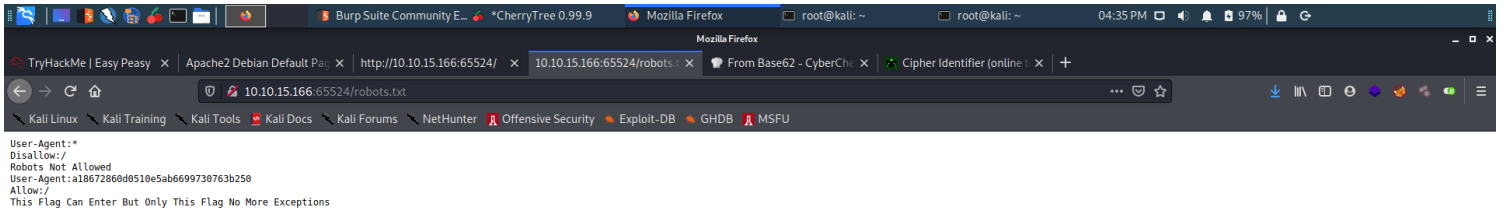
ssh port 6498

Apache web server port 65524

The main page had our Flag3 inside it

robots.txt

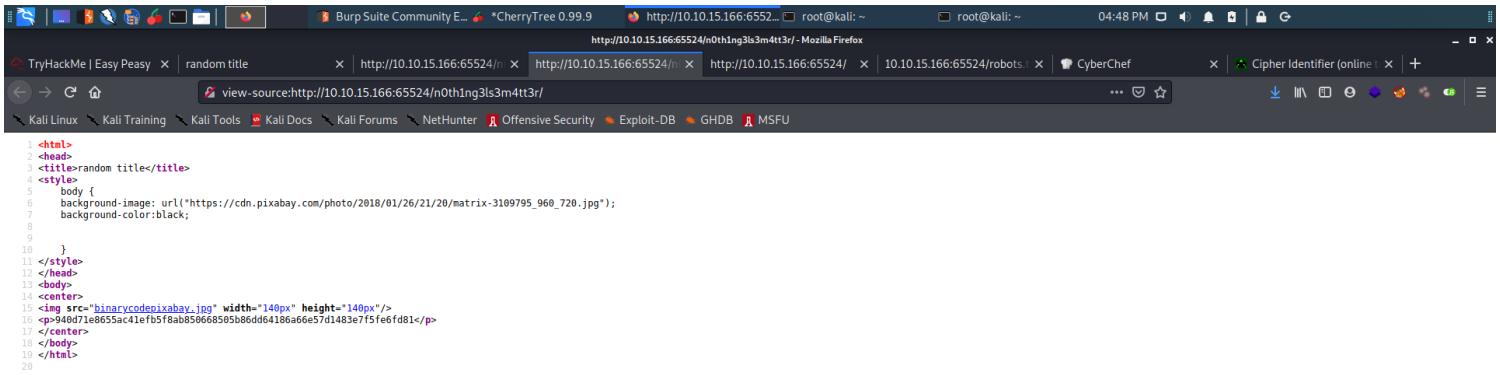
Found an interesting robots.txt file on this port



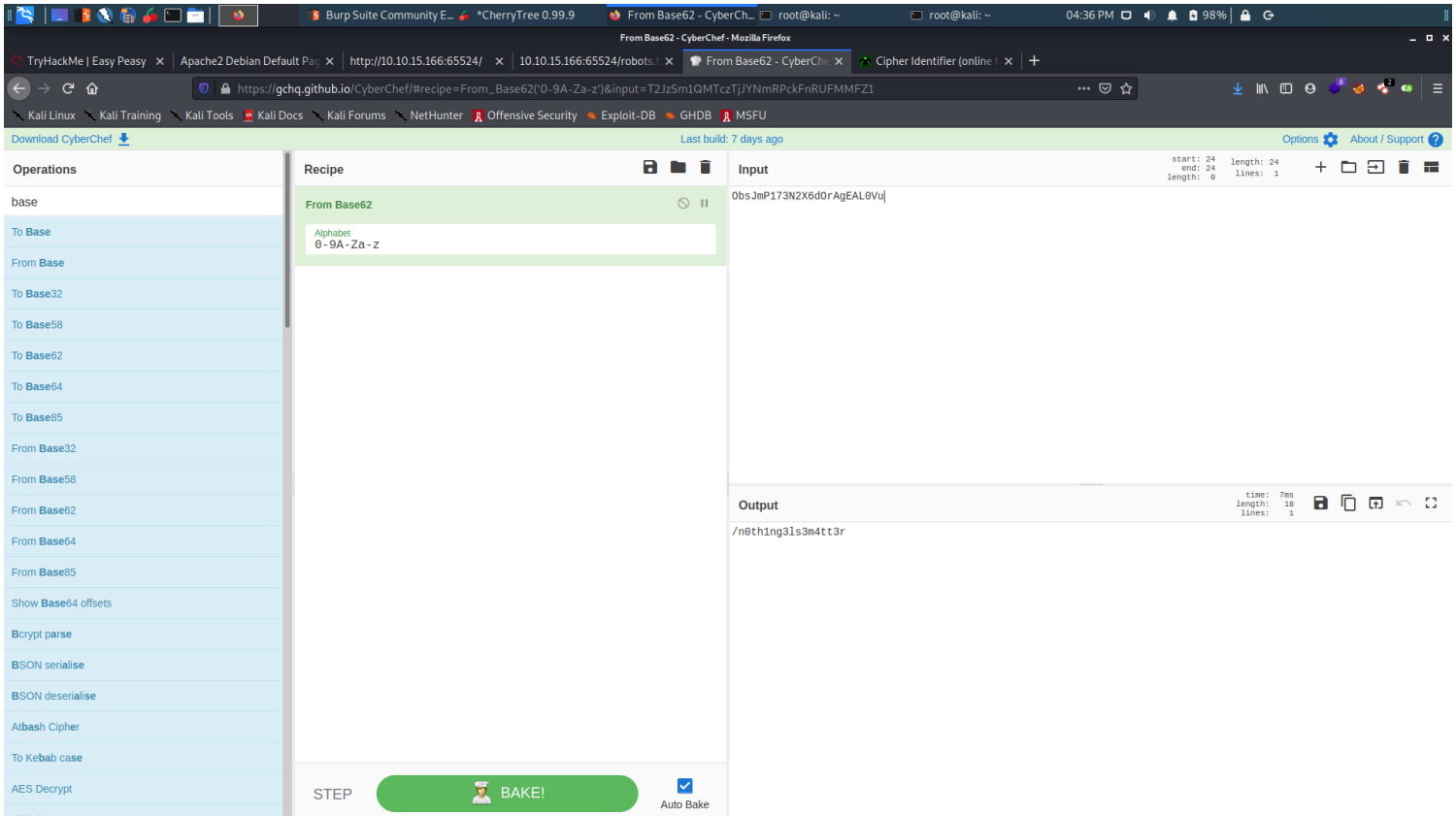
##

secret dir

1-



2- This code was base62 and was converted to /n0th1ng3ls3m4tt3r



Johntheripper

Got a cracked password from that encoded value found on this secret dir

mypasswordforthatjob

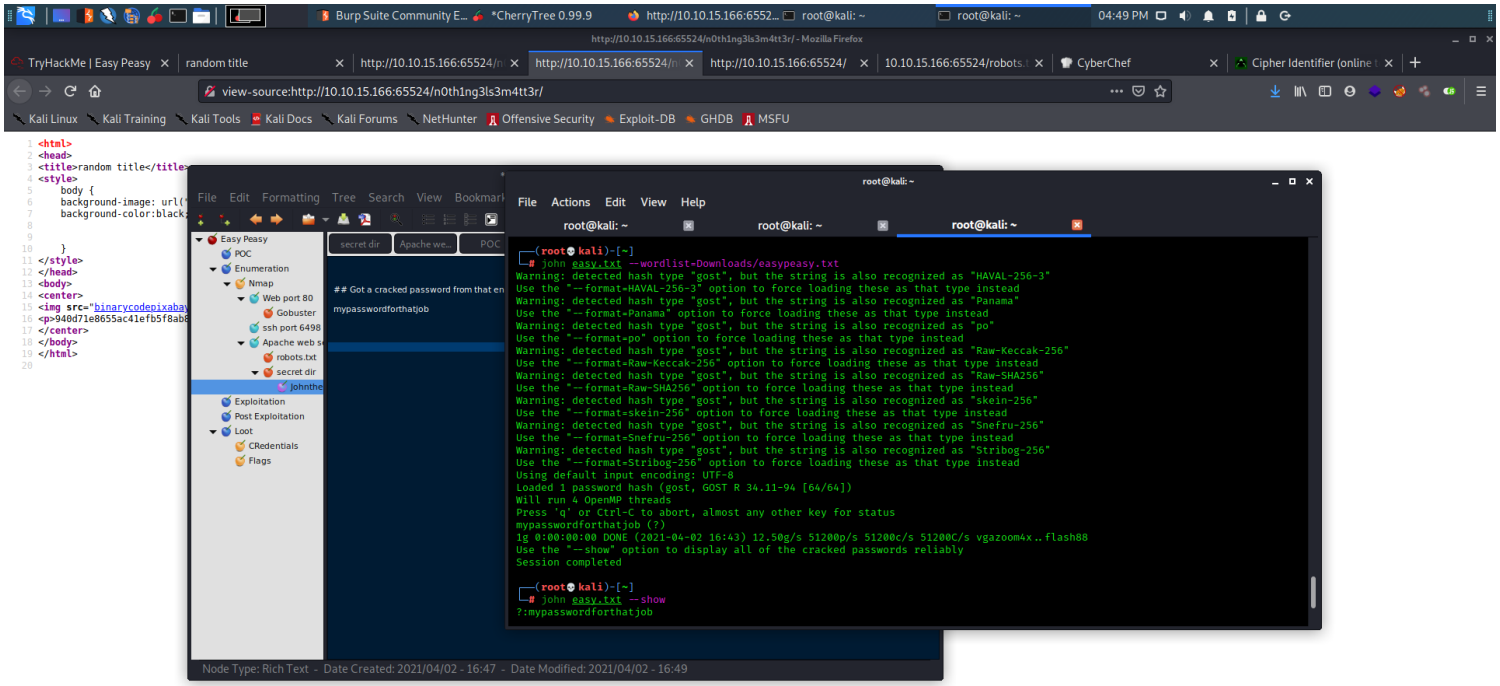


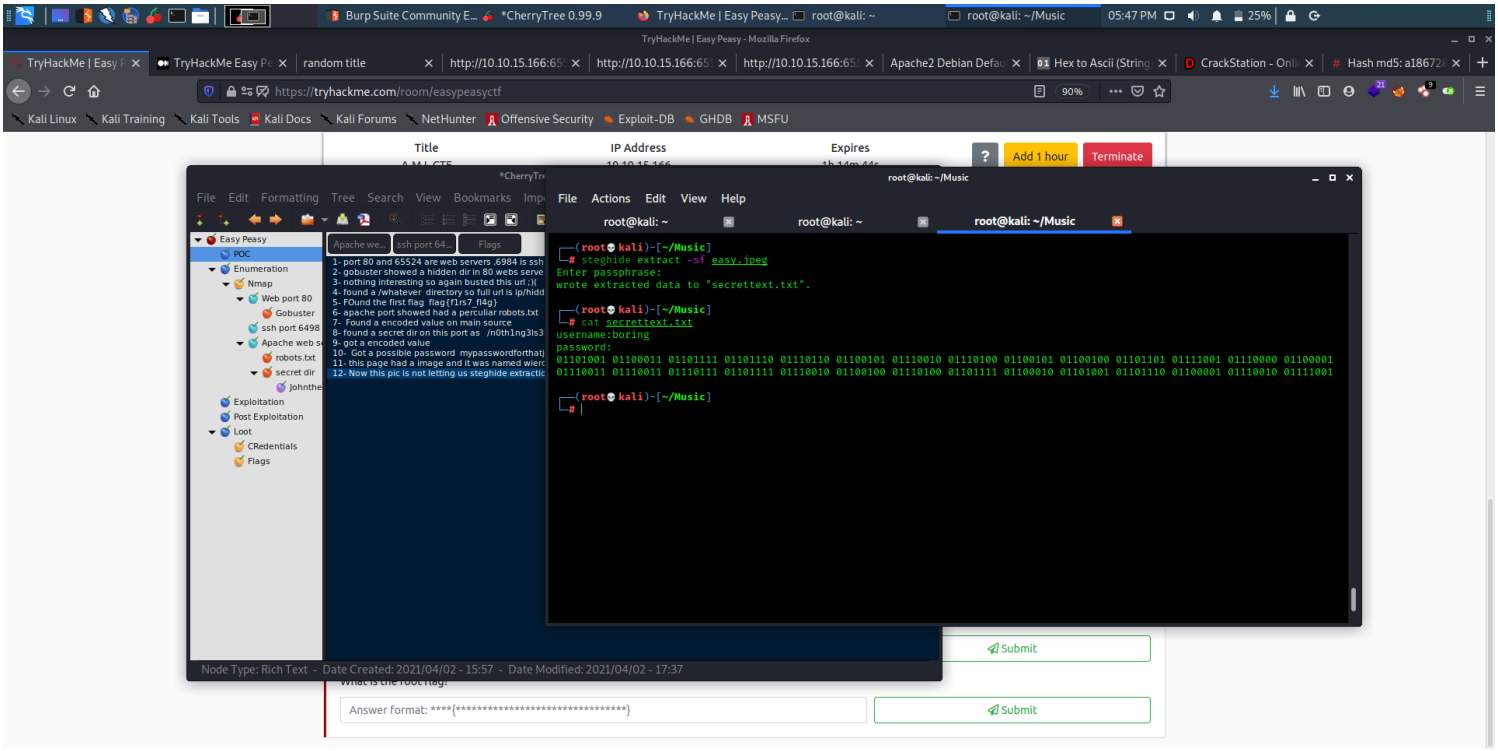
Image on main page

Steghide the image and use the foundeed passphrase

got a secret.txt file disclosing credentials

secret.txt

Contents



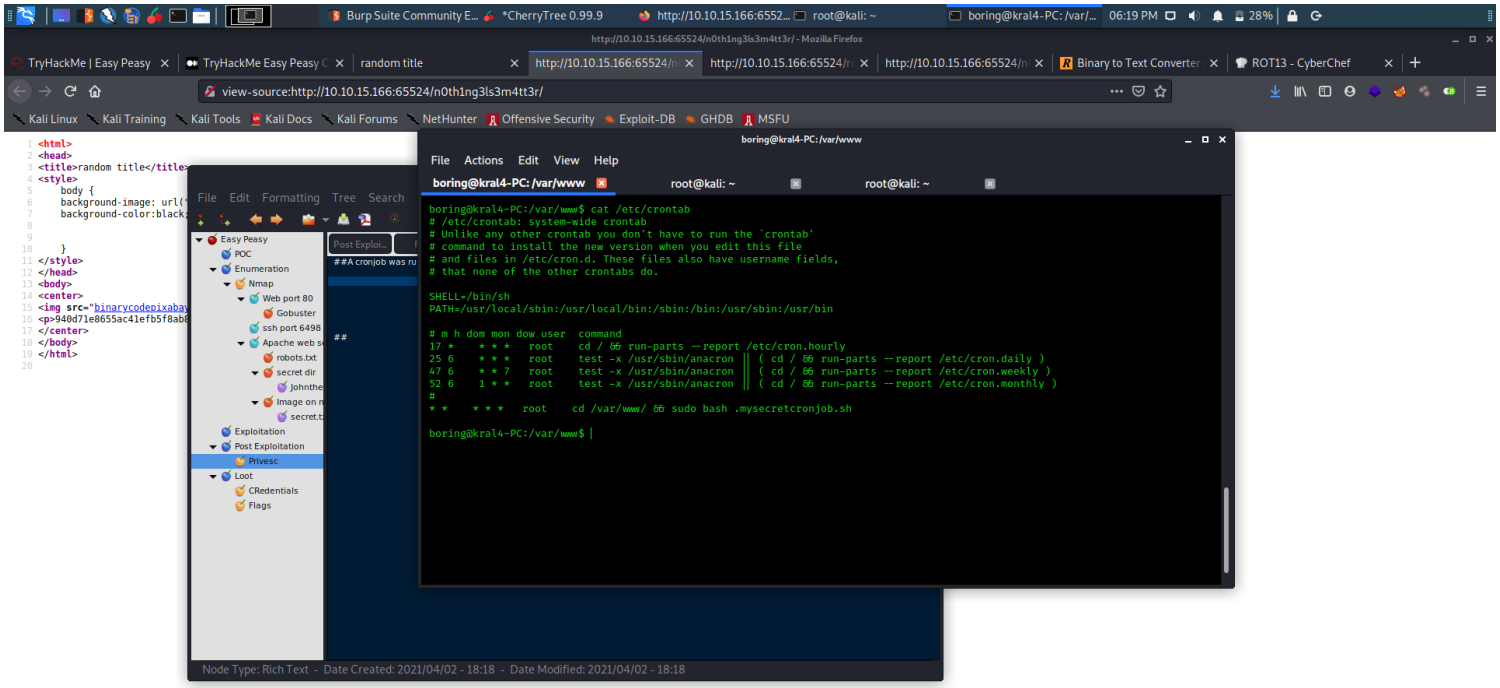
##

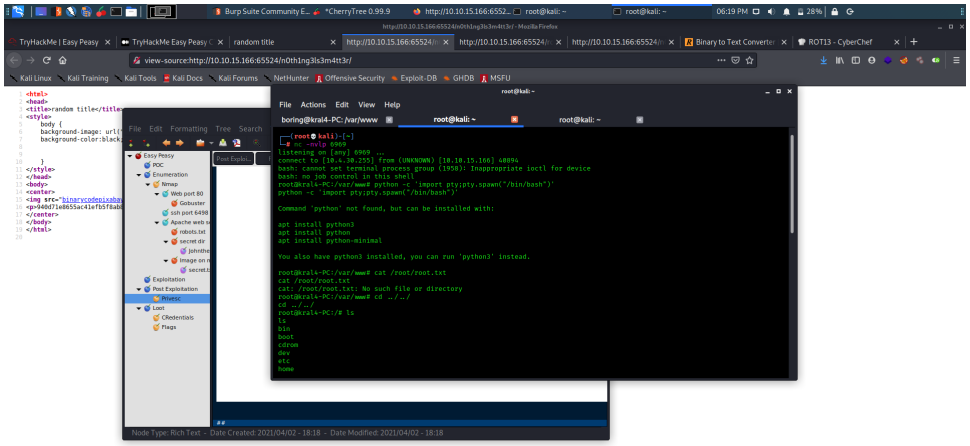
Exploitation

Post Exploitation

Privesc

##A cronjob was running





##wrote abash reverse shell in file and got root

Loot

CRedentials

A password for the downloaded image from apache main page giving us ssh password access

mypasswordforthatjob

##SSH
binary:iconvertedmypasswordtobinary

Flags

##Flag 1 $ip/hidden/whatever

flag{f1rs7_fl4g}

##Flag2

flag{1m_s3c0nd_fl4g}

##Flag3

flag{9fdafbd64c47471a8f54cd3fc64cd312}

##USer

flag{n0wits33msn0rm4l}

##Root
flag{63a9f0ea7bb98050796b649e85481845}