Albania 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: Albania

- Download the ova file
https://mega.nz/#!Gk502Tob!Octl2yiiryjBXNLyzK8QsCtVm6gqw72rKQvEebGvMmk

- Import the ova file into your favorite hypervisor;

- Attach a DHCP enabled interface to the machine and run it

- Objective
Find the flags

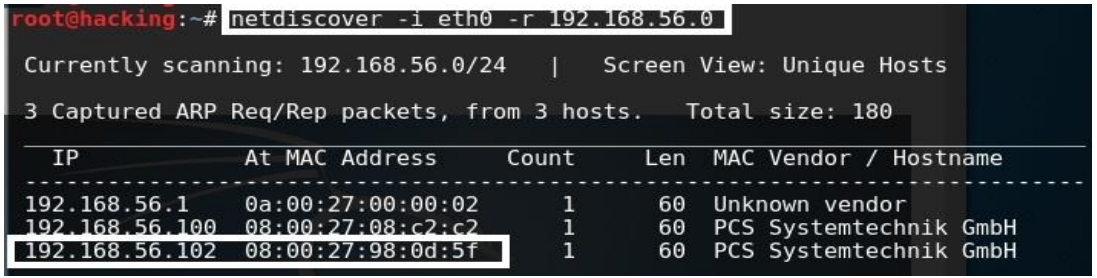
Test Setup

◎ Testing environment

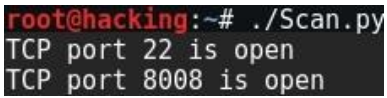
Linux Kali (attacker) >>> Firewall >>> D0Not5top (target vm)

Walkthrough

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

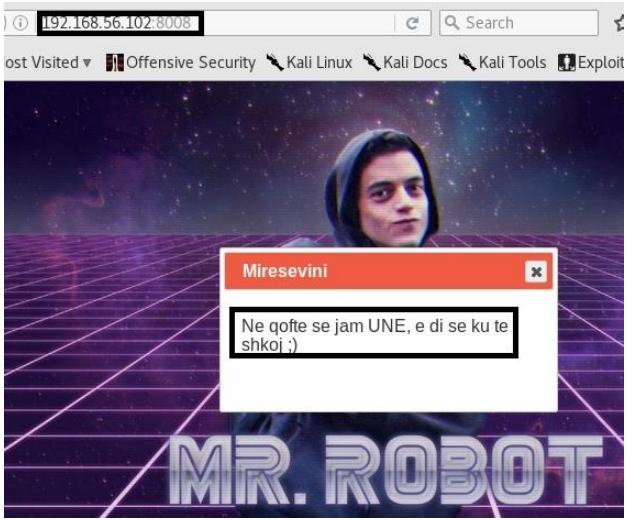


◎Scan the target machine IP (192.168.56.102)



Walkthrough

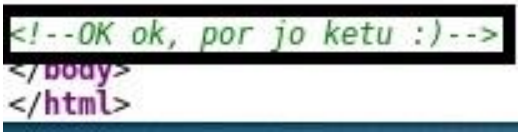
- Explore Port 8008 in a browser



- The message in the box translates to “if I am, I know where to go”

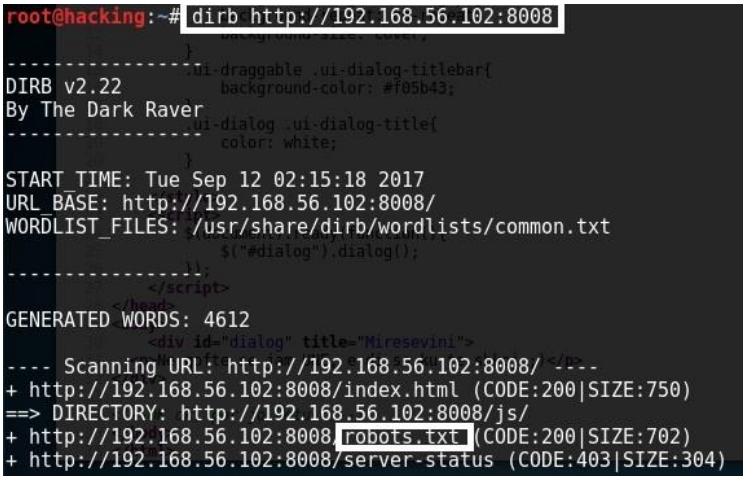
Walkthrough

◎ Page-source has a comment at the bottom which says “Ok ok, but not here” (translated using Google translate)



Walkthrough

◎ Use dirb tool to scan the host on port 8008



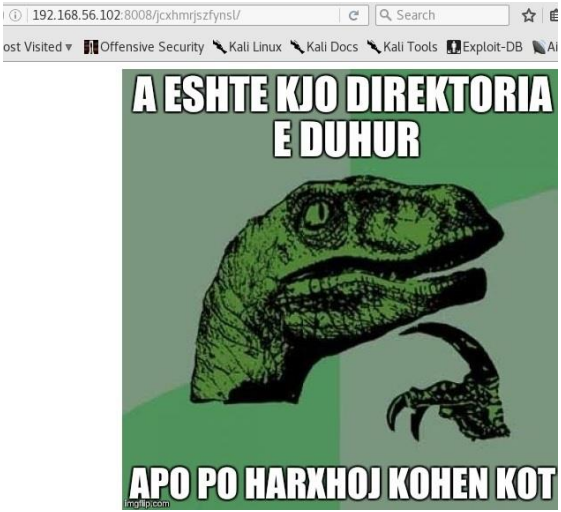
◎ robots.txt is available

Walkthrough

- Explore robots.txt

Walkthrough

◎ All but one directory give us the same result



◎ The message says “is this the right directory or I'm spending time in vain

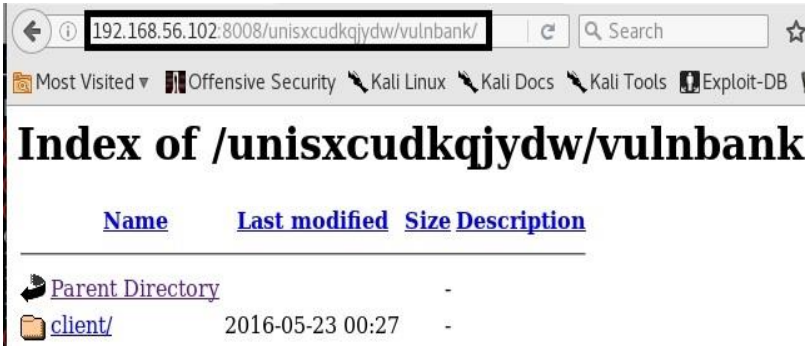
Walkthrough

◎ The directory that proves to be worth visiting is http://192.168.56.102:8008/unisxcudkqjydw/

◎ Found a new directory “vulnbank”

Walkthrough

◎ Explore the new found directory “vulnbank”



Walkthrough

◎ Click on the “client/” directory

◎ Found a login page of very secure bank

Walkthrough

◎ Try SQLi on the login form

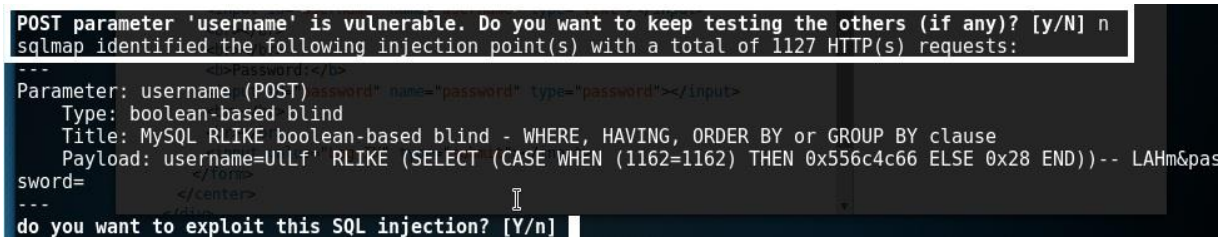
```
<form name="login" method="post" action="login.php">
    <b>Username:</b>
    <input id="username" name="username" type="text"></input>
    <br></br>
    <br></br>
    <b>Password:</b>
    <input id="password" name="password" type="password"></input>
    <br></br>
    <br></br>
    <input value="Log IN" type="submit"></input>
```

Walkthrough

- Trying manual SQLi on the login form (slqmap did not work)
  Trying a single ‘as the username, got an error page

Walkthrough

◎ The username parameter is vulnerable to SQL injection as shown by sqlmap



Walkthrough

◎ After trying a lot of manual SQLi (including a list from https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/)

found a working query /* **’%9#** */

Walkthrough

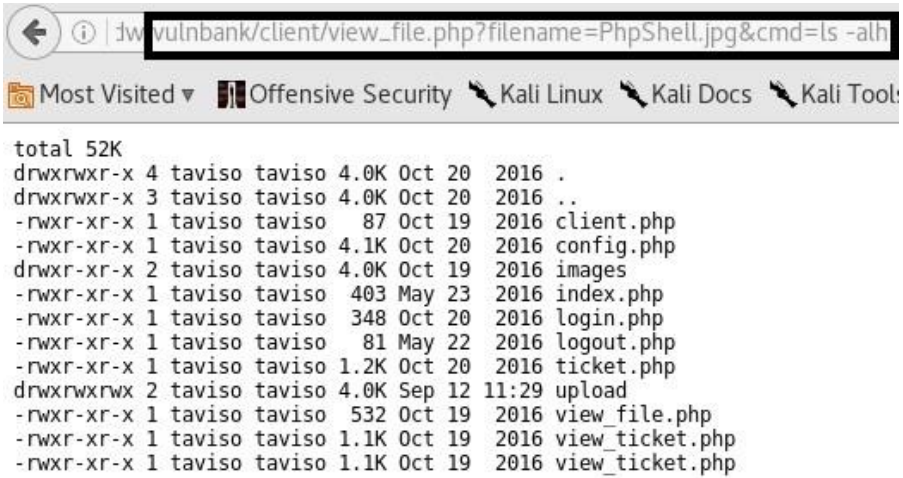
◎ The application allows the user to upload a file as part of a trouble ticketing system

Walkthrough

◎ Upload a php backdoor in a file with the extension “.jpg”

Walkthrough

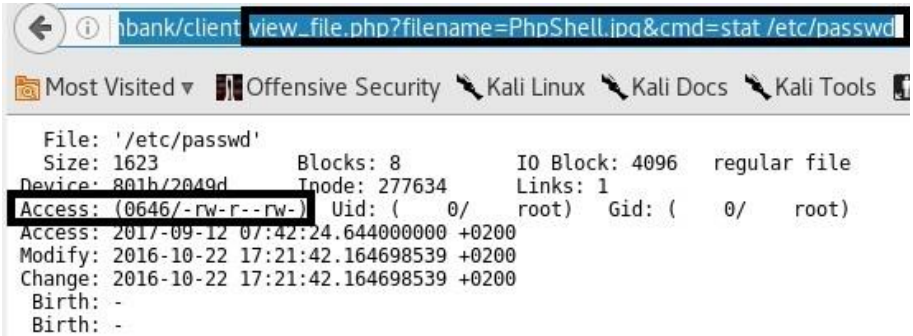
◎ Testing the PHP backdoor



◎ It works

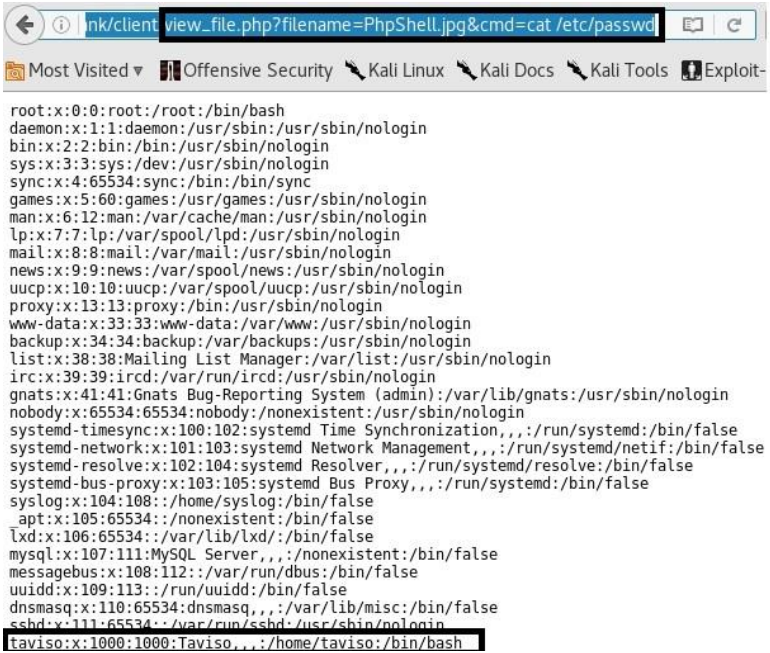
Walkthrough

- Passwd file has write permissions



Walkthrough

- Listing all users available



Walkthrough

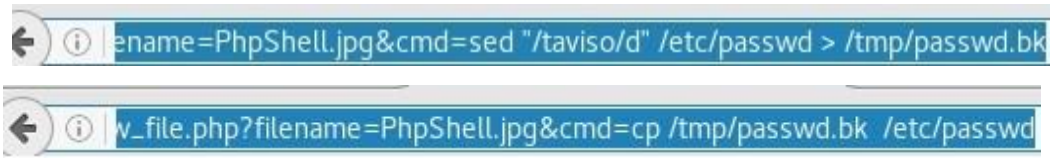
- Try to change "taviso" account to a known password
- First, simulating locally

Walkthrough

◎ Use the previous hash as support to create the new "taviso" entry

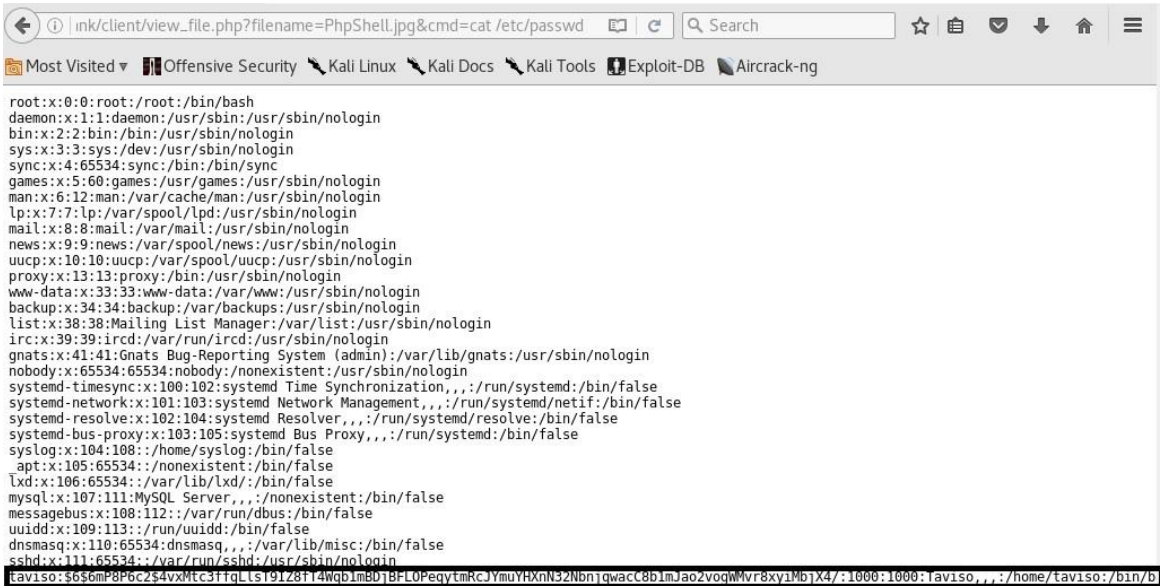
```
root@hacking:~# taviso:$6$6mP8P6c2$4vxMtc3ffgLlsT9IZ8fT4Wqb1mBDjBFLOPeqytmRcJYmuYHXnN32NbnjqwacC8b1mJao2vogWMvr8
xyiMbjX4/:1000:1000:Taviso,,,:/home/taviso:/bin/bash
```

◎ Remove taviso from /etc/passwd



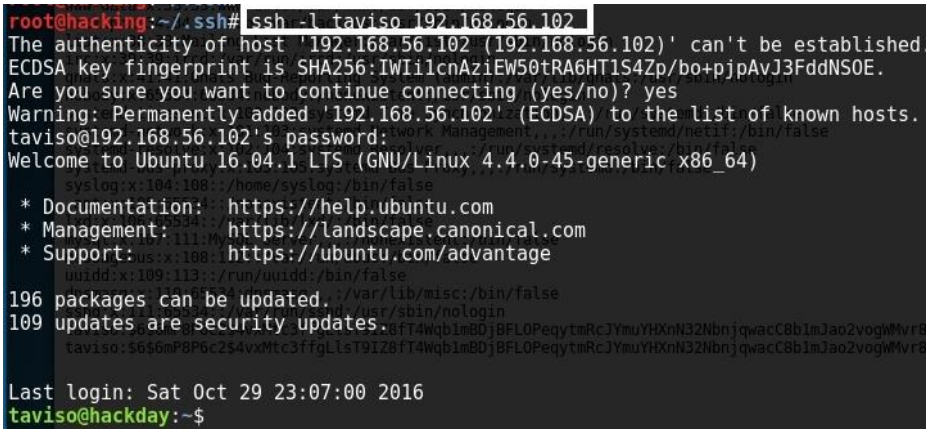
Walkthrough

◎ Add the new "taviso" created in previous step (echo “NewTaviso” >> /etc/passwd)



Walkthrough

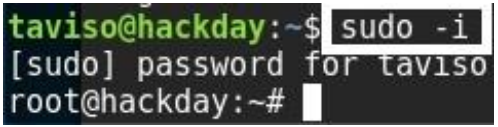
- Try to connect using ssh



- Success!

Walkthrough

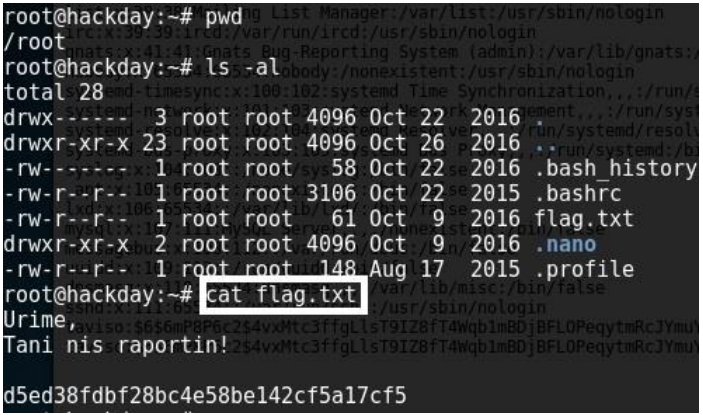
- Try see if taviso is on sudoers file



- BamBam! Got root

Walkthrough

◎ Try to see what root has on his home directory



◎ Captured the flag. Message says “Congratulations, Now begins the report!”

References

- Vulnhub website
https://www.vulnhub.com

- Vulnerable VM download
https://mega.nz/#!Gk502Tob!Octl2yiiryjBXNLyzK8QsCtVm6gqw72rKQvEebGvMmk

- Sqlmap
http://sqlmap.org/