Lab. 2

Scanning, analyse et exploitations de vulnérabilités

Poste client

Objectifs :

Dans ce laboratoire, vous apprendrez à utiliser Metasploit pour accéder à une machine distante. L'objectif est de vous enseigner les bases du pentest pratique.

Le Metasploit Framework (MSF) contient une collection d'exploits. Il s'agit d'une infrastructure sur laquelle vous pouvez. Cela vous permet de vous concentrer sur la mise en place de vos environnements d'exploitation et de ne pas avoir à réinventer la roue. MSF est l'un des outils les plus populaires auprès des professionnels de la sécurité qui mènent des études pratiques du haking et du pentesting. Il contient un grand nombre d'outils d'exploitation et d'environnements de travail. De plus, il est disponible gratuitement.

Nous utiliserons deux machines virtuelles Linux : L'une est un Kali Linux avec le framework Metasploit installé ; et l'autre est un Linux intentionnellement vulnérable. Nous utiliserons le framework Metasploit sur Kali Linux pour accéder à distance à la machine Linux vulnérable.

Outils :

- The VirtualBox Software ;
- The Kali Linux, Penetration Testing Distribution ;
- Metasploit: Penetration Testing Software ;
- Metasploitable2: Vulnerable Linux Platform.

Architecture du Lab. :

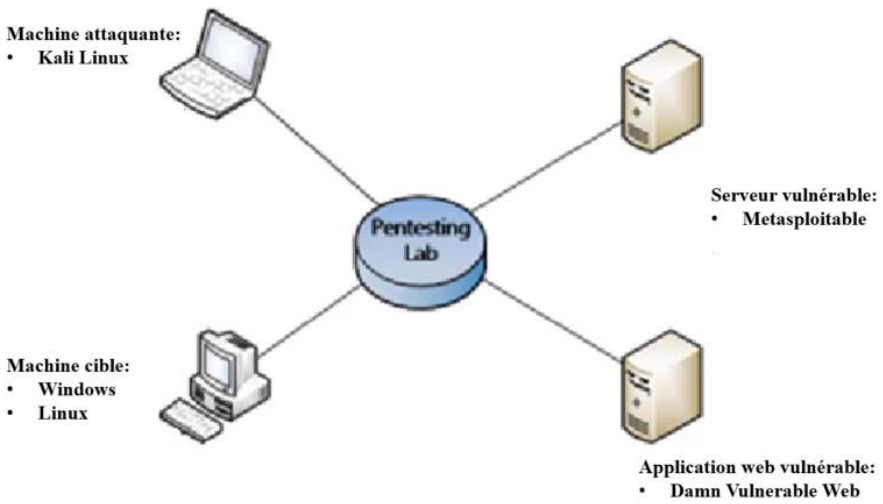

Figure 1 : Architecture globale du lab

Etape 1 : Configuration des machines :

Sur une machine virtuelle (VM), configurer la machine de l'attaquant sous Kali linux et sur une autre VM configurer le serveur cible (metasploitable). Après, spécifier les adresses des 2 machines, et assurez-vous qu'elle aient accès à internet (.

Etape 2 : Recherche des vulnérabilités :

- **Nmap : Scan de ports et vulnérabilités**

Sur la machine de l'attaquant, lancer nmap : **nmap –sV –O @IP victime** (voir figure ci-après) :

Nmap liste tous les ports ouverts et les services associés.

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

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

Explorer les options de nmap suivantes et expliquez les.

Nmap @réseau/masque
Nmap -sN -p 22,25 @ip cible
Nmap -sU @ip cible -p 53,161
Nmap -A @ip cible

```
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 rexecd
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)
```

Figure 2 : ports des services ouverts sur la machine victime

Etape 3 : Exploitation des vulnérabilités :

Metasploit :

Est un outil de Pentesting qui permet le développement et l'exécution d'exploits contre une cible. Il est développé en ruby. Metasploit est intégré à kali.

Le Framework Metasploit utilise PostgreSQL comme base de données, vous devez donc le lancer en exécutant la commande suivante dans le terminal : **$ service postgresql start**

Vous pouvez vérifier que PostgreSQL fonctionne en exécutant la commande suivante :

$ service postgresql status

Avec PostgreSQL en marche, vous devez créer et initialiser la base de données msf en exécutant la commande suivante : **$ msfdb init**

Exploiter le service **vsftpd**, il possède une faille de sécurité exploitable par metasploit. Démarrer le Framework metasploit avec la commande **msfconsole**.

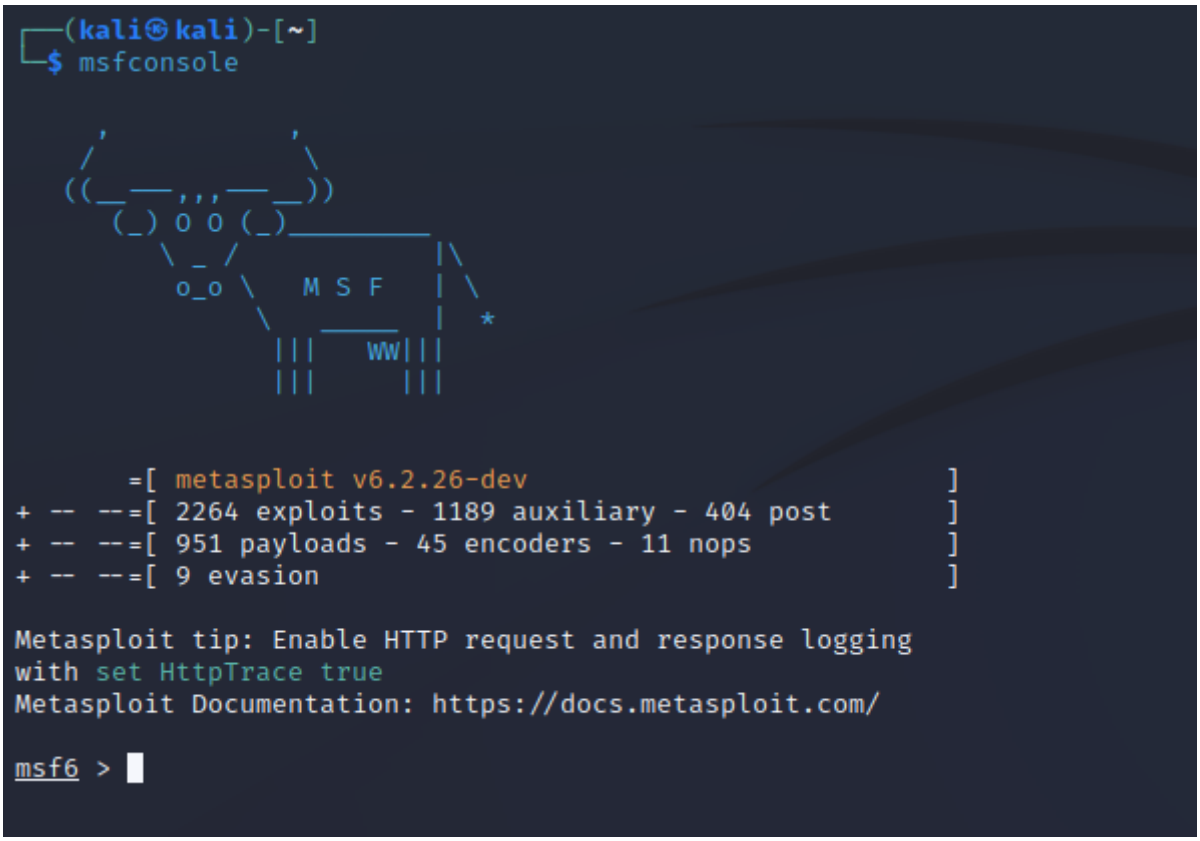

Figure 3 : Interface CLI de Metasploit

Préciser le nom et le chemin de la vulnérabilité (voir figure 4).

Remplir les options de cet exploit : pour voir les options disponibles taper la commande **show options :** Les paramètres à remplir : RHOST (adresse de la cible) et LPORT (port ciblé) (voir figure 5).

Figure 4 : Nom et chemin de la vulnérabilité

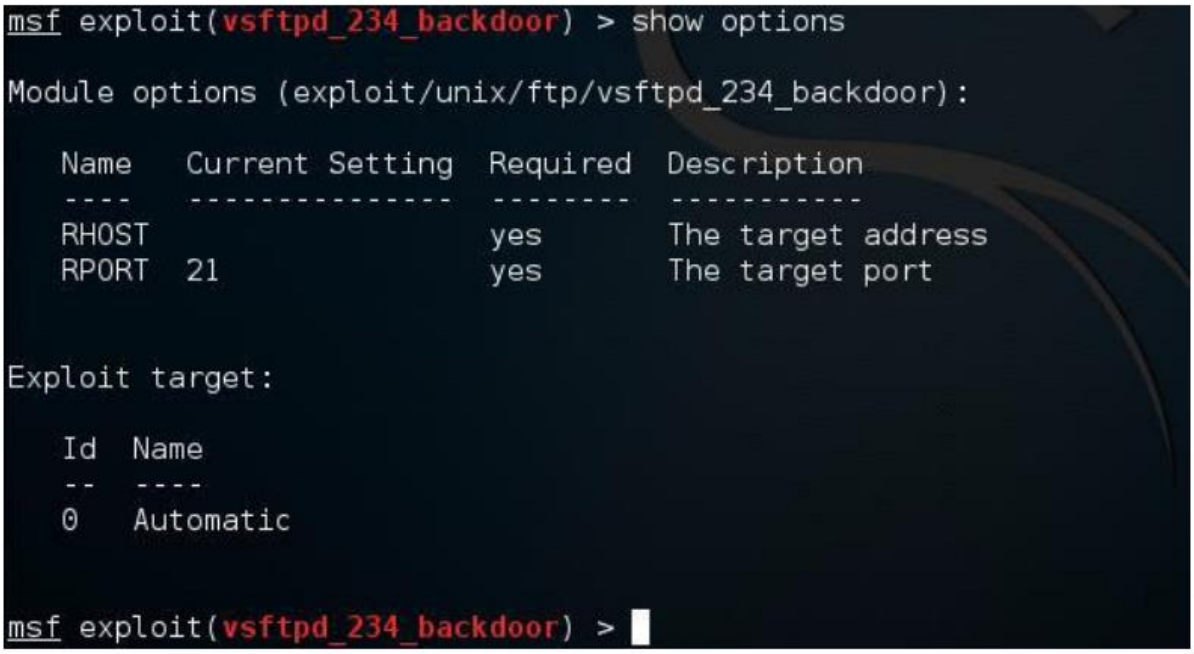

Figure 5 : Options de l'exploit

Taper :

set RHOST @ ip de la machine cible.

Pour lancer l'exploit utiliser la commande : **exploit**.

Etape 4 : Intrusion dans la machine cible :

Vérifier si l'intrusion a réussie.

Ouvrir un Shell dans la machine victime, ajouter un user ou toute action montrant que l'intrusion a réussie.

Etape 5 : Gestion des cyberattaques pour Metasploit - Armitage

1. Installer et configurer Armitage et exploiter la même vulnérabilité.
2. Lisez les instructions du laboratoire ci-dessus et terminez toutes les tâches.
3. Exploiter une autre vulnérabilité en utilisant à la fois msfconsole et Armitage. Montrez que vous avez placé un fichier dans la machine distante exploitée via des captures d'écran et en créant le fichier avec la commande "touch <yourname>" où <yourname> doit être remplacé par votre nom complet.

Etape : Explorer d'autres outils de scan de vulnérabilités

Nessus et OpenVAS

Installer, configurer et vérifier l'état de Nessus et OpenVAS sous kali linux.

Apt_get update
Apt-get install nessus
Service nessusd status
Lancer nessus avec ; https://localhost:Port

Explorer les différentes vulnérabilités découvertes par ces deux outils.

Exploiter des vulnérabilités et rédiger le rapport du pentest :

- Architecture du réseau cible ;
- Adressages ;
- Vulnérabilités découvertes avec les niveaux de criticités de chacune.
- Bonne pratiques techniques et organisationnelles à recommander pour y solutionner.

Il est essentiel de signaler que l'usage de tels outils est strictement INTERDIT en dehors d'un contexte pédagogique et d'apprentissage (et dans un réseau cloisonné et strict).