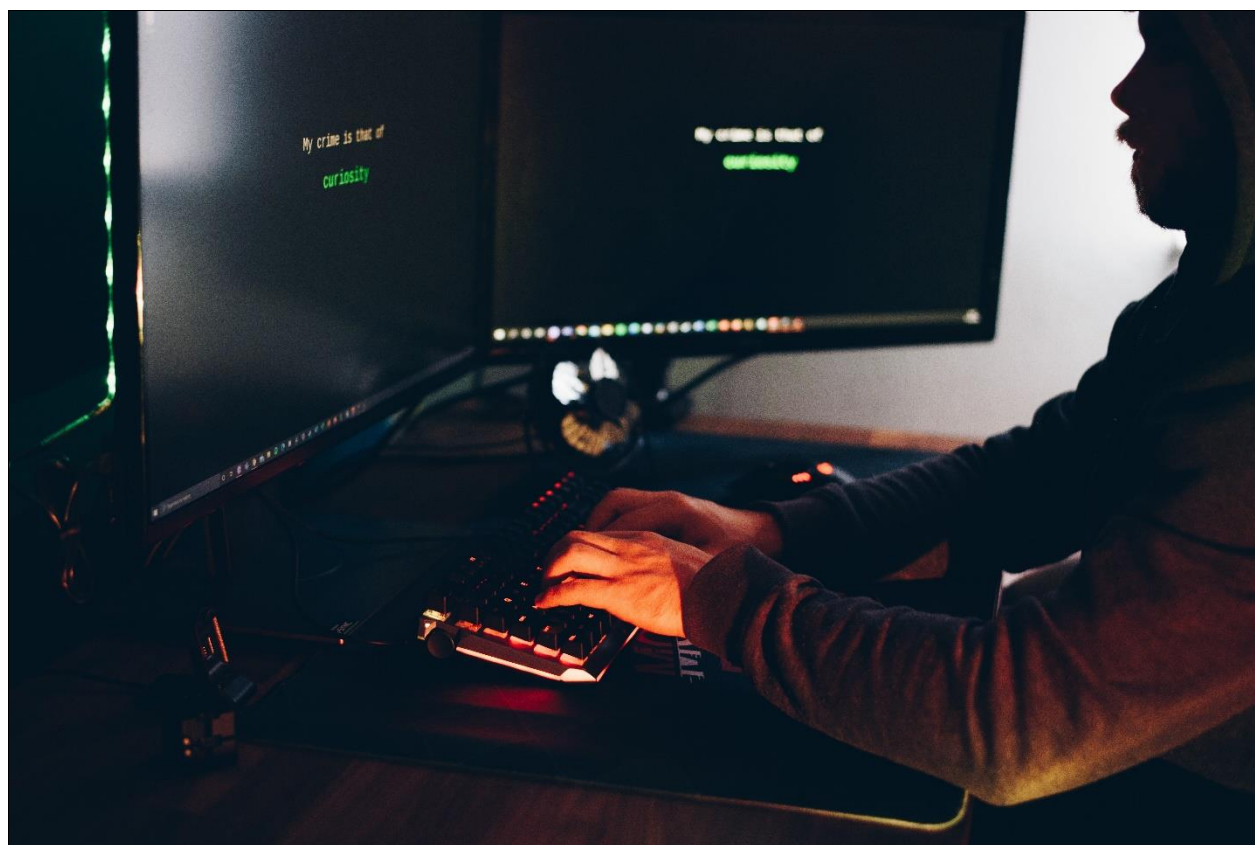


HardeningKitty Liaison Officer

Guide de l'utilisateur



Etudiant : Thomas Luyet

Professeur : Xavier Barmaz

SOURCE DE L'ILLUSTRATION DE LA PAGE DE TITRE

[Crop Hacker Silhouette Tapant Sur Le Clavier De L'ordinateur Tout En Système De Piratage · Photo gratuite \(pexels.com\)](#) (Auteur : Anete Lusina)

i. Table des matières

SOURCE DE L'ILLUSTRATION DE LA PAGE DE TITRE	ii
i. Table des matières.....	1
ii. Liste des figures	2
1. Avant propos	1
1.1 Contexte	1
1.2 Prérequis	1
1.3 Résumé conceptuel	1
1.4 Diagramme de séquence.....	2
1.5 Connaissances nécessaires.....	2
2. Mise en place.....	3
2.1 Activation de OpenSSH Server	3
2.2 Activation de l'exécution de Scripts	6
2.3 Connexion SSH avec authentification par clé (Optionnel)	7
3. Télécharger HardeningKitty Liaison Officer.....	13
4. Utilisation.....	15
4.1 Préparation.....	15
4.2 Connexion SSH.....	18
4.3 Menu	19
4.4 Nettoyage	26
4.5 Personnalisation	27

ii. Liste des figures

Figure 1 : Diagramme de séquence (Source : Auteur).....	2
Figure 2 : Configuration OpenSSH – Settings (Source : Auteur)	3
Figure 3 : Configuration OpenSSH – Apps (Source : Auteur)	3
Figure 4 : Configuration OpenSSH - Optional features (Source : Auteur)	4
Figure 5 : Configuration OpenSSH - Add a feature (Source : Auteur)	4
Figure 6 : Configuration OpenSSH – Install (Source : Auteur).....	4
Figure 7 : Configuration OpenSSH (Source : Auteur)	5
Figure 8 : Configuration OpenSSH - Validation (Source : Auteur)	5
Figure 9 : Activation Service OpenSSH (Source : Auteur)	6
Figure 10 : Autorisation des Scripts - Commande (Source : Auteur)	6
Figure 11 : Clé publique - .ssh (Source : Auteur)	7
Figure 12 : Clé publique - génération (Source : Auteur).....	8
Figure 13 : Clé publique - Transfert SCP (Source : Auteur)	8
Figure 14 : Clé publique - Connexion SSH (Source : Auteur).....	9
Figure 15 : Clé publique - Authorized Keys (Source : Auteur).....	9
Figure 16 : Clé publique - fermeture connexion SSH (Source : Auteur)	9
Figure 17 : Clé publique - Notepad admin (Source : Auteur)	10
Figure 18 : Clé publique - All Files (Source : Auteur)	10
Figure 19 : Clé publique - sshd_config (Source : Auteur)	10
Figure 20 : Clé publique - PubkeyAuthentication yes (Source : Auteur)	11
Figure 21 : Clé publique - Restart sshd (Source : Auteur)	11
Figure 22 : Clé publique - Passphrase (Source : Auteur).....	11
Figure 23 : Clé publique - PasswordAuthentication no	12
Figure 24 : Télécharger HardeningKitty Liaison Officer - GitHub (Source : Auteur)	13
Figure 25 : Télécharger HardeningKitty Liaison Officer - Extract All (Source : Auteur).....	13
Figure 26 : HardeningKitty Liaison Officer - Extract folder (Source : Auteur).....	14
Figure 27 : HardeningKitty Liaison Officer - Extract Files (Source : Auteur)	14
Figure 28 : Utilisation - répertoire HardeningKitty Liaison Officer (Source : Auteur).....	15
Figure 29 : Utilisation - load.ps1 (Source : Auteur)	15
Figure 30 : Préparation - Security Warning (Source : Auteur).....	16
Figure 31 : Préparation - Informations machine Slave (Source : Auteur)	16
Figure 32 : Préparation - Transfert de fichier (Source : Auteur)	16
Figure 33 : Préparation - Connexion SSH (Source : Auteur)	17
Figure 34 : Préparation - Prêt à l'utilisation (Source : Auteur).....	17
Figure 35 : Exécution - Connexion SSH (Source : Auteur)	18
Figure 36 : Menu - Script menu.ps1 (Source : Auteur).....	19
Figure 37 : Scan - liste de bonnes pratiques (Source : Auteur)	20
Figure 38 : Scan - Surligner list (Source : Auteur).....	20
Figure 39 : Scan - Sélection par click droit (Source : Auteur)	21
Figure 40 : Scan - Résultat (Source : Auteur)	21
Figure 41 : Harden – connexion annulée (Source : Auteur).....	21
Figure 42 : Audit – nom de l'audit et sélection liste (Source : Auteur).....	22
Figure 43 : Audit – log et rapport (Source : Auteur).....	23
Figure 44 : Backup – fichier de backup (Source : Auteur).....	23
Figure 45 : Backup – emplacement fichier backup (Source : Auteur).....	24
Figure 46 : Backup – backup ajouté aux listes (Source : Auteur)	24
Figure 47 : Export – exporter les fichiers (Source : Auteur)	25
Figure 48 : Export – répertoires backups et reports (Source : Auteur)	25
Figure 49 : Quit - quitter HardeningKitty Liaison Officer (Source : Auteur)	26
Figure 50 : Remove - Script Remove.ps1 (Source : Auteur).....	27
Figure 51 : Modification – Sélection d'une liste (Source : Auteur).....	28
Figure 52 : Modification - List (Source : Auteur).....	28
Figure 53 : Modification - User Rights (Source : Auteur).....	28

1. Avant propos

Ce guide a pour but de présenter la mise en place et l'utilisation de HardeningKitty Liaison Officer. Il regroupe l'intégralité des prérequis et des configurations nécessaires à son bon fonctionnement ainsi qu'un guide d'utilisation. HardeningKitty Liaison Officer est une solution Open Source et gratuite.

1.1 Contexte

Pour l'élaboration du présent guide, nous utilisons deux machines virtuelles Windows 10 Education version 21h2, avec anglais comme choix de langue du système. Oracle VirtualBox 6.1 fait office de gestionnaire de machines. Nous utilisons HardeningKitty v.0.8.0.

[HardeningKitty \(gitHub.com\)](https://github.com/HardeningKitty)

1.2 Prérequis

Chacune des machines doit disposer d'une connexion Internet.

1.3 Résumé conceptuel

HardeningKitty Liaison Officer est une solution inédite qui utilise HardeningKitty afin d'automatiser du Hardening sur une machine distante par le biais de Scripts PowerShell. HardeningKitty Liaison Officer se sert de protocoles SCP et SSH pour son fonctionnement.

Afin de faciliter la compréhension du lecteur, dans le cadre de ce guide nous utilisons les termes Master et Slave pour différencier respectivement la machine effectuant les commandes de Hardening et la machine qui fait l'objet du Hardening.

Trois Scripts constituent la solution HardeningKitty Liaison Officer.

- load.ps1, est un Script de préparation, met en place HardeningKitty Liaison Officer de la machine Master à la machine Slave.
- menu.ps1, le Script d'exécution, permet la réalisation de l'ensemble des opérations de Hardening sur la machine Slave.
- remove.ps1, le Script de nettoyage, supprime l'ensemble des éléments mis en place par le premier Script après l'application du Hardening.

1.4 Diagramme de séquence

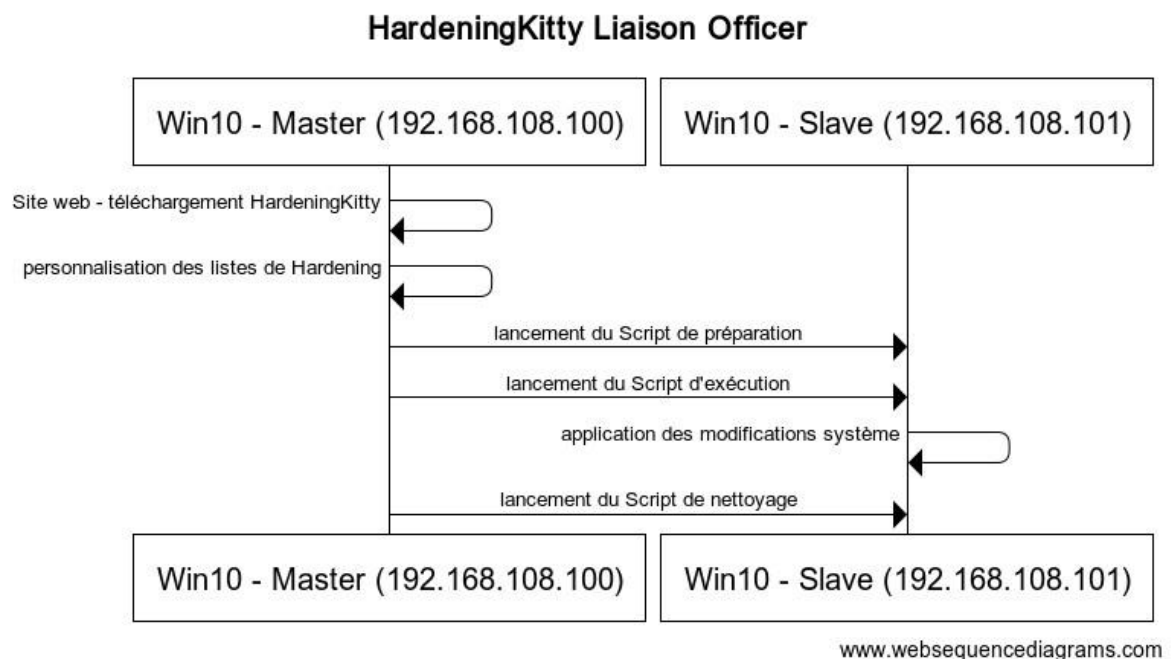


Figure 1 : Diagramme de séquence (Source : Auteur)

1.5 Connaissances nécessaires

HardeningKitty Liaison Officer se veut une solution facile d'utilisation à la complexité modérée. Des connaissances de base dans l'utilisation de PowerShell ainsi que la navigation en ligne de commande sont un plus.

L'utilisateur doit connaître le nom de compte, le mot de passe et l'adresse IP des machines Master et Slave.

2. Mise en place

Ce chapitre contient l'intégralité des démarches nécessaires afin de pouvoir utiliser HardeningKitty Liaison Officer.

*L'ensemble des démarches de ce chapitre sont à réaliser
sur la machine Master et sur la machine Slave.*

2.1 Activation de OpenSSH Server

1. Taper **Settings** dans la barre de recherche Windows

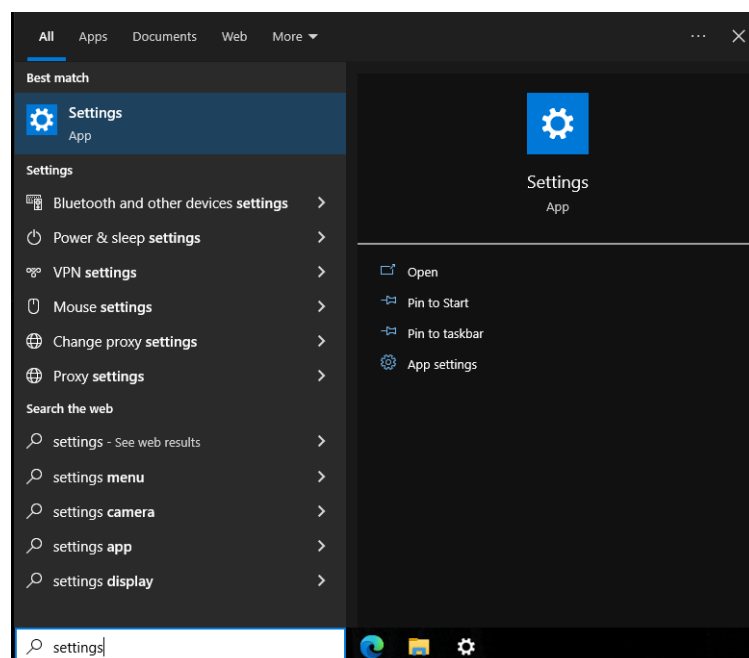


Figure 2 : Configuration OpenSSH – Settings (Source : Auteur)

2. Cliquer sur **Apps**

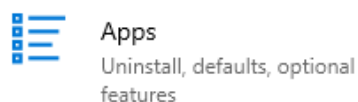


Figure 3 : Configuration OpenSSH – Apps (Source : Auteur)

3. Cliquer sur **Optional Features**

Apps & features

[Optional features](#)

Figure 4 : Configuration OpenSSH - Optional features (Source : Auteur)

4. Cliquer sur **Add a feature**

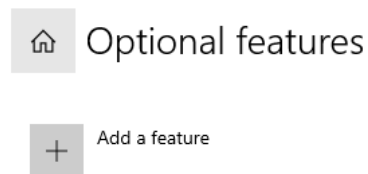


Figure 5 : Configuration OpenSSH - Add a feature (Source : Auteur)

5. Taper dans la barre de recherche **openssh**, sélectionner OpenSSH Server, cliquer sur **Install(1)**.



Figure 6 : Configuration OpenSSH – Install (Source : Auteur)

6. Dans la barre de recherche Windows taper **powershell**
7. Cliquer avec le bouton de droite de la souris sur l'icône Windows PowerShell et cliquer sur **Run as administrator**

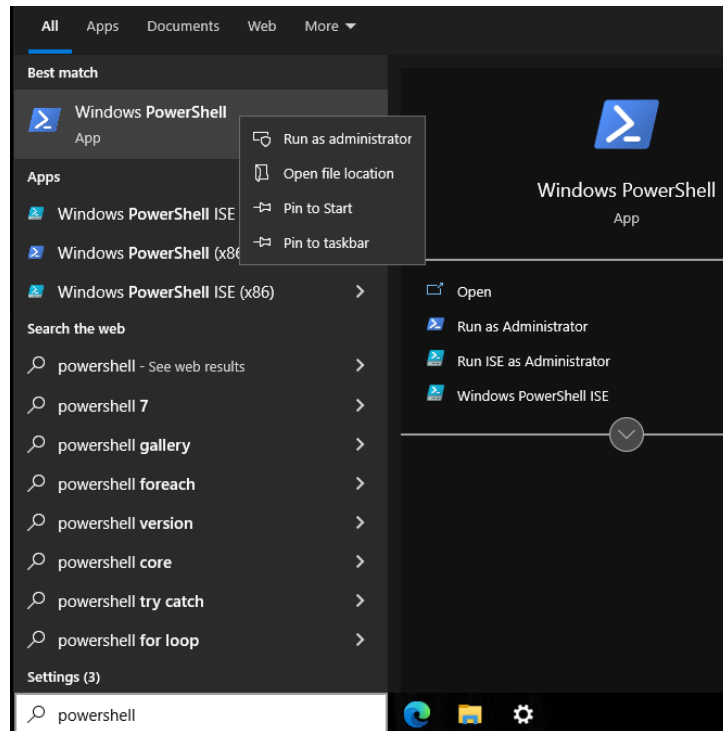


Figure 7 : Configuration OpenSSH (Source : Auteur)

8. Cliquer Yes pour la demande d'autorisation

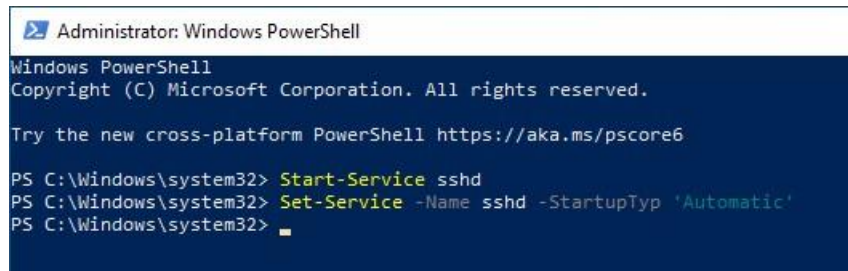


Figure 8 : Configuration OpenSSH - Validation (Source : Auteur)

9. Dans Windows Powershell taper les commandes suivantes :

Start-Service sshd

Set-Service -Name sshd -StartupType 'Automatic'



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Start-Service sshd
PS C:\Windows\system32> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Windows\system32>
```

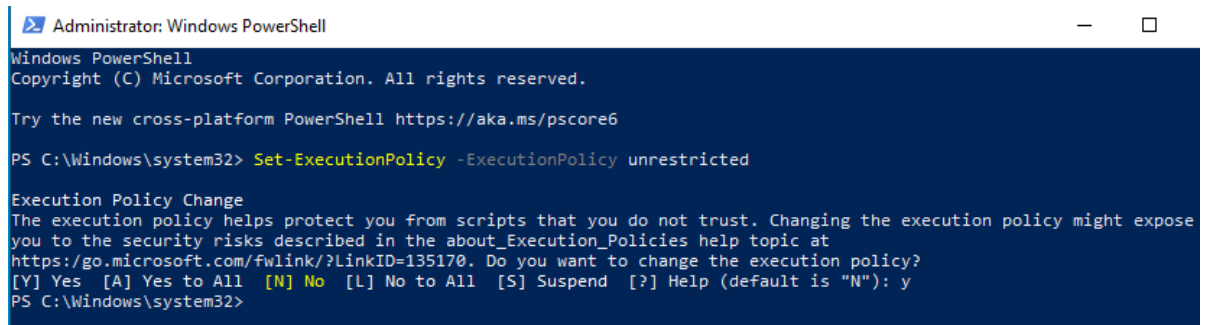
Figure 9 : Activation Service OpenSSH (Source : Auteur)

2.2 Activation de l'exécution de Scripts

1. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**
2. Dans Windows Powershell taper la commande suivante :

`Set-ExecutionPolicy -ExecutionPolicy unrestricted`

Puis taper Y



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32>
```

Figure 10 : Autorisation des Scripts - Commande (Source : Auteur)

2.3 Connexion SSH avec authentification par clé (Optionnel)

HardeningKitty Liaison Officer utilise le protocole SSH pour se connecter de la machine Master à la machine Slave. Initialement ce protocole requiert trois éléments, le nom de compte de la machine, le mot de passe respectif ainsi que son adresse IP.

Il est tout à fait possible d'utiliser HardeningKitty Liaison Officer en se basant sur ces trois prérequis. Néanmoins, nous conseillons pour des raisons de sécurité de favoriser une authentification par clé.

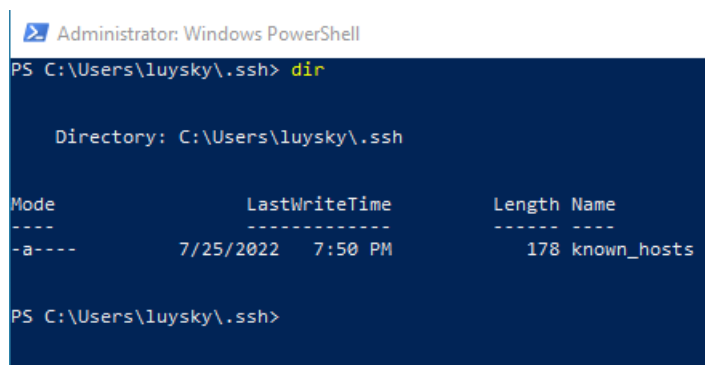
Le fonctionnement de HardeningKitty Liaison Officer reste pour l'utilisateur, visuellement très similaire. Au lieu de demander le mot de passe de l'utilisateur, le programme demande la phrase de sécurité de la clé.

Depuis la machine Master

1. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**
2. Taper `cd C:\Users\luysky\.ssh`

Remplacer **luysky** par votre nom d'utilisateur Master

3. Taper `dir`



```
Administrator: Windows PowerShell
PS C:\Users\luysky\.ssh> dir

Directory: C:\Users\luysky\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----             7/25/2022   7:50 PM           178 known_hosts

PS C:\Users\luysky\.ssh>
```

Figure 11 : Clé publique - .ssh (Source : Auteur)

4. Taper `ssh-keygen`

Pour la question relative au file taper uniquement la **touche Enter**

Saisir **deux fois** son **passphrase**

Taper `dir`

```

PS C:\Users\luisky\.ssh> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\luisky\.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\luisky\.ssh/id_rsa.
Your public key has been saved in C:\Users\luisky\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:uzgdQ9t32lZ0w0dc53W40o2ZobwS6hsVgIWhuLm+69w luisky@Master
The key's randomart image is:
+---[RSA 3072]---+
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
|      .o        |
+---[SHA256]-----+
PS C:\Users\luisky\.ssh> dir

Directory: C:\Users\luisky\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----             7/26/2022   2:41 PM          2655 id_rsa
-a----             7/26/2022   2:41 PM           568 id_rsa.pub
-a----             7/25/2022   7:50 PM           178 known_hosts
PS C:\Users\luisky\.ssh>

```

Figure 12 : Clé publique - génération (Source : Auteur)

5. Taper

scp id_rsa.pub luisky@192.168.108.101:%programdata%/ssh

Remplacer **luisky** et **l'adresse IP** par le nom et l'adresse IP de la **machine Slave**

6. Taper le mot de passe de la machine distante

```

PS C:\Users\luisky\.ssh> scp id_rsa.pub luisky@192.168.108.101:%programdata%/ssh
luisky@192.168.108.101's password:
id_rsa.pub                                100% 568    45.5KB/s   00:00
PS C:\Users\luisky\.ssh>

```

Figure 13 : Clé publique - Transfert SCP (Source : Auteur)

7. Taper ssh luisky@192.168.108.101

Remplacer **luisky** et **l'adresse IP** par le nom et adresse IP de la **machine Slave**

```
PS C:\Users\luysky\.ssh> ssh luysky@192.168.108.101
luysky@192.168.108.101's password:
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

luysky@SLAVE C:\Users\luysky>
```

Figure 14 : Clé publique - Connexion SSH (Source : Auteur)

8. Taper

```
cd %programdata%/ssh
```

```
type id_rsa.pub >> administrators_authorized_keys
```

```
icacls administrators_authorized_keys /inheritance:r /grant "Administrators:F" /grant
"SYSTEM:F"
```

```
luysky@SLAVE C:\ProgramData\ssh>type id_rsa.pub >> administrators_authorized_keys
luysky@SLAVE C:\ProgramData\ssh>icacls administrators_authorized_keys /inheritance:r /grant "Administrators:F" /grant "SYSTEM:F"
processed file: administrators_authorized_keys
Successfully processed 1 files; Failed processing 0 files
luysky@SLAVE C:\ProgramData\ssh>
```

Figure 15 : Clé publique - Authorized Keys (Source : Auteur)

9. Taper Exit

```
luysky@SLAVE C:\ProgramData\ssh>exit
Connection to 192.168.108.101 closed.
PS C:\Users\luysky\.ssh>
```

Figure 16 : Clé publique - fermeture connexion SSH (Source : Auteur)

Depuis la machine Slave

10. Taper notepad dans la barre de recherche Windows et Run as administrator

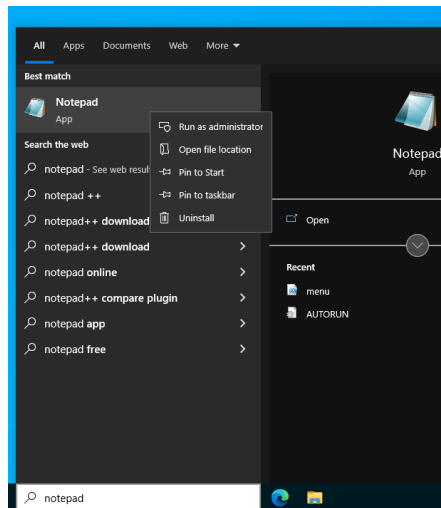


Figure 17 : Clé publique - Notepad admin (Source : Auteur)

11. Cliquer **File** et **Open** puis dans la **barre de recherche** taper

`%programdata%/ssh`

12. Changer le type de Text Documents à **All Files**

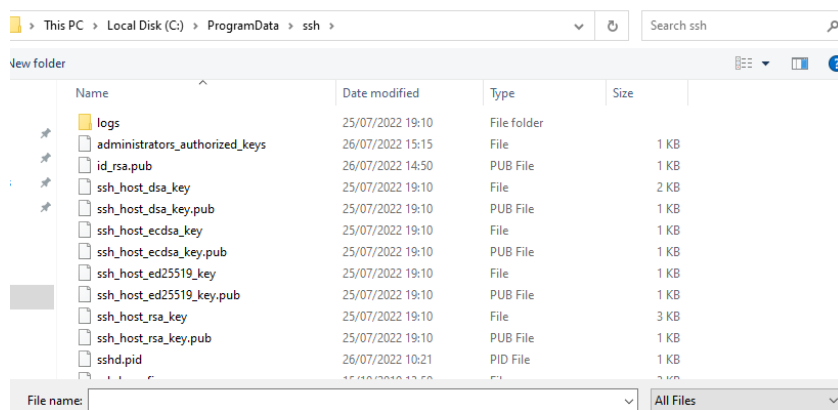


Figure 18 : Clé publique - All Files (Source : Auteur)

13. Sélectionner dans la liste le fichier **sshd_config** et cliquer **Open**

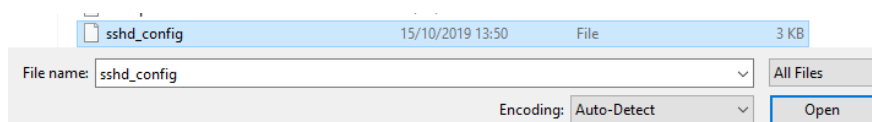


Figure 19 : Clé publique - sshd_config (Source : Auteur)

14. Enlever le commentaire # devant PubkeyAuthentication yes

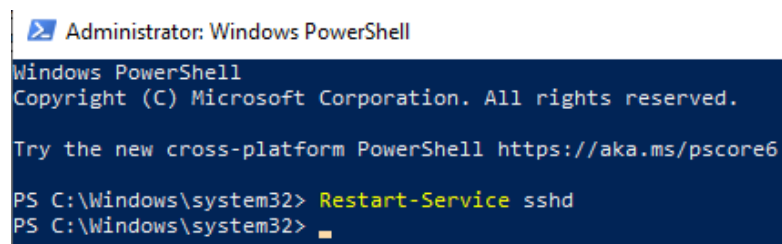
```
PubkeyAuthentication yes
```

Figure 20 : Clé publique - PubkeyAuthentication yes (Source : Auteur)

15. Cliquer **File** puis **Save** mais **ne pas fermer la fenêtre** sshd_config

16. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**

17. Taper **Restart-Service sshd**



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Restart-Service sshd
PS C:\Windows\system32>
```

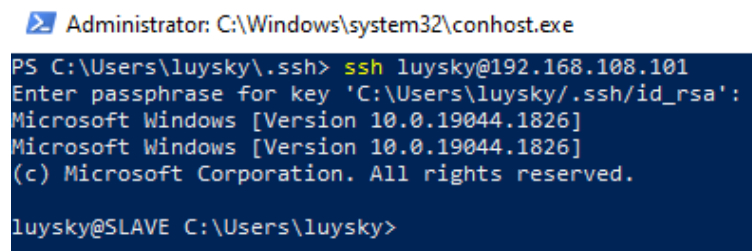
Figure 21 : Clé publique - Restart sshd (Source : Auteur)

Retourner sur la machine Master

18. Dans la console Powershell taper ssh **luysky@192.168.108.101**

puis taper le **passphrase** d'identification de la clé publique

Remplacer **luysky** et l'**adresse IP** par le nom et adresse IP de la **machine Slave**



```
Administrator: C:\Windows\system32\conhost.exe
PS C:\Users\luysky\.ssh> ssh luysky@192.168.108.101
Enter passphrase for key 'C:\Users\luysky\.ssh/id_rsa':
Microsoft Windows [Version 10.0.19044.1826]
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

luysky@SLAVE C:\Users\luysky>
```

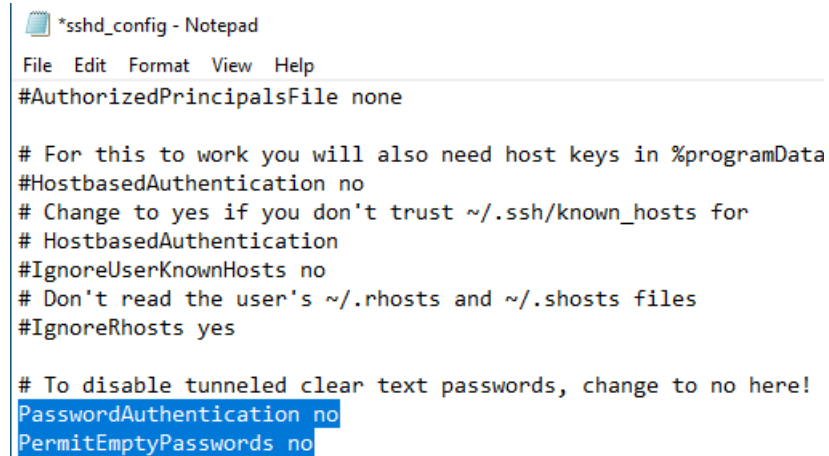
Figure 22 : Clé publique - Passphrase (Source : Auteur)

19. Taper exit

Retourner sur la machine Slave

20. Dans le fichier `sshd_config`, retirer les commentaires `#` aux lignes `PasswordAuthentication` et `PermitEmptyPasswords`

21. Modifier `yes` en `no` pour `PasswordAuthentication`



```
*sshd_config - Notepad
File Edit Format View Help
#AuthorizedPrincipalsFile none

# For this to work you will also need host keys in %programData
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
PermitEmptyPasswords no
```

Figure 23 : Clé publique - `PasswordAuthentication no`

22. Effectuer l'intégralité des démarches 1 à 21 en intervertissant le nom des machines.

3. Télécharger HardeningKitty Liaison Officer

1. Aller sur la page **GitHub** :

[GitHub - Luisky/HardeningKitty-LiaisonOfficer](https://github.com/Luisky/HardeningKitty-LiaisonOfficer)

2. Cliquer sur **Code** puis **Download ZIP**

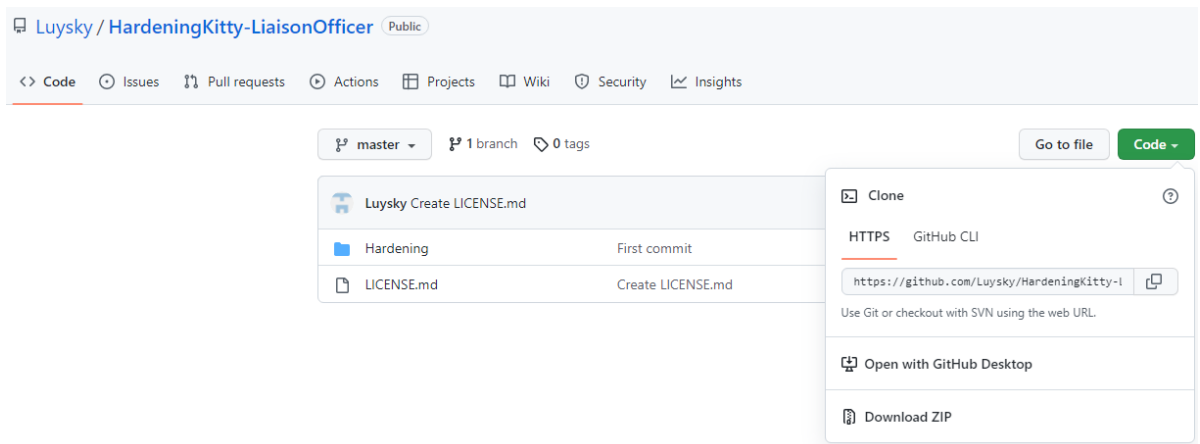


Figure 24 : Télécharger HardeningKitty Liaison Officer - GitHub (Source : Auteur)

3. Aller sous Downloads, cliquer avec le bouton de droite de la souris sur HardeningKitty-LiaisonOfficer-master, sélectionner **Extract All..**

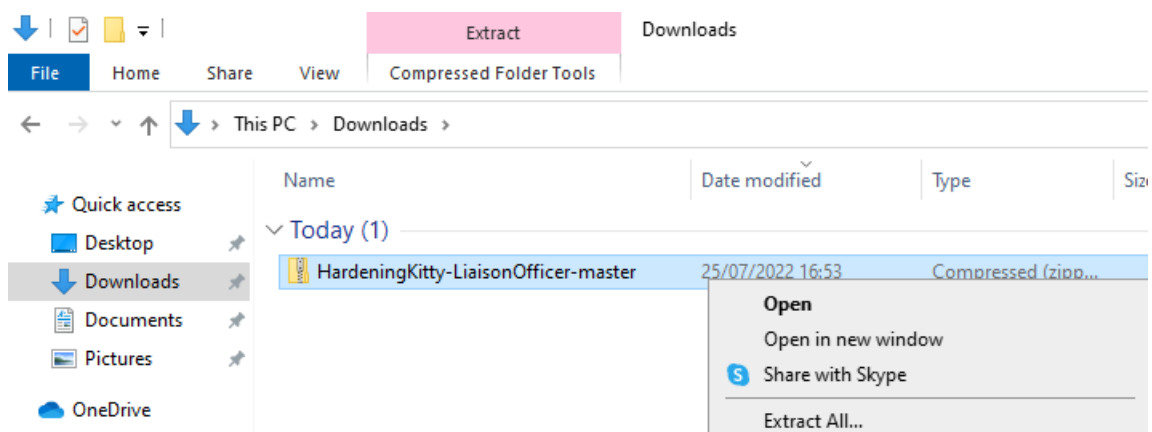


Figure 25 : Télécharger HardeningKitty Liaison Officer - Extract All (Source : Auteur)

4. Sélectionner **Browse...**, puis dans la barre de destination taper le chemin d'accès du nom d'utilisateur Master.

Remplacer Luisky par le nom d'utilisateur Master

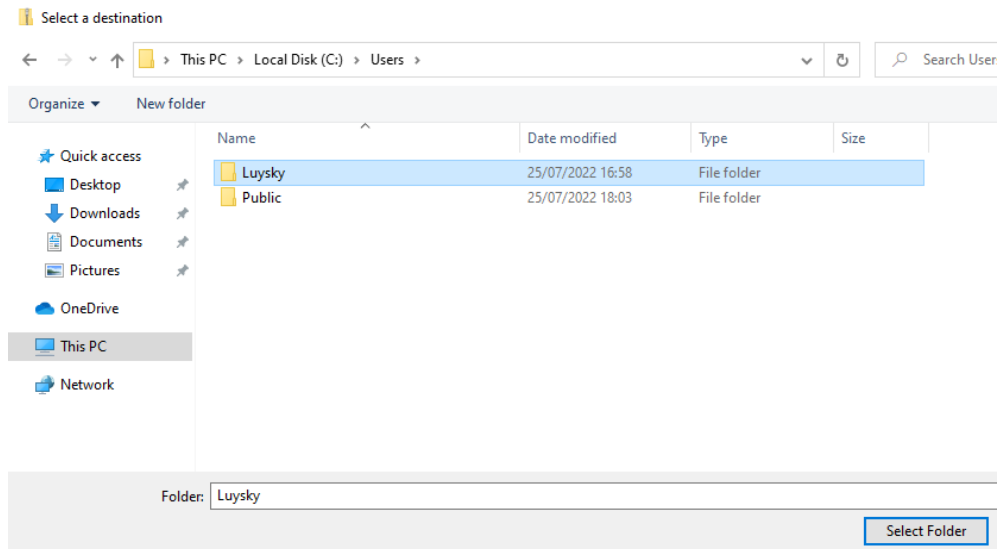


Figure 26 : HardeningKitty Liaison Officer - Extract folder (Source : Auteur)

5. Cliquer sur **Extract**

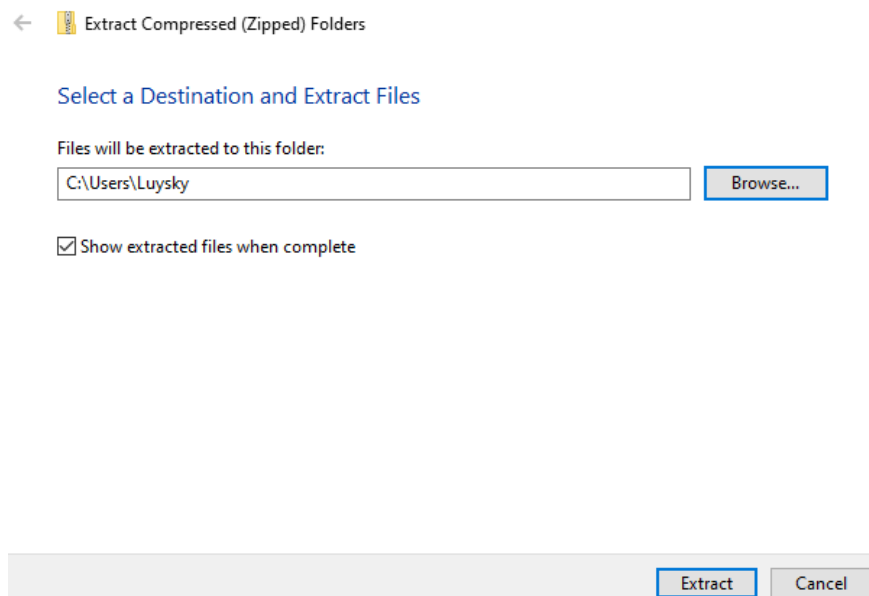


Figure 27 : HardeningKitty Liaison Officer - Extract Files (Source : Auteur)

4. Utilisation

Ce chapitre contient l'intégralité des commandes liées à l'utilisation de HardeningKitty Liaison Officer.

Toutes les démarches de ce chapitre sont à réaliser depuis la machine Master.

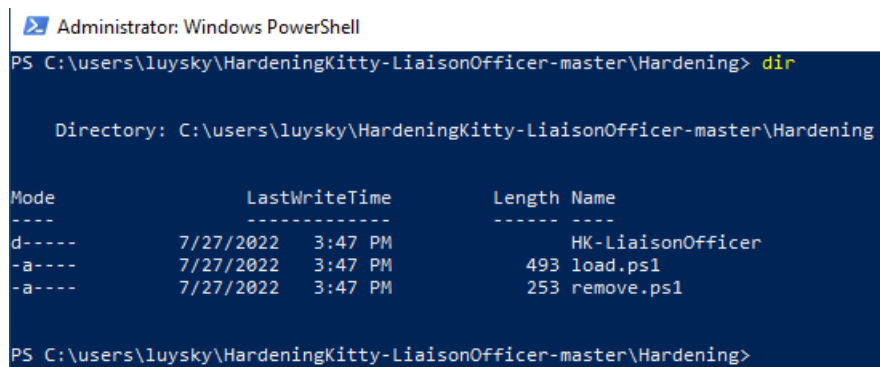
4.1 Préparation

La première étape, le Script de préparation, consiste à transférer HardeningKitty et le Script d'exécution de la machine Master à la machine Slave.

1. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**
2. Taper `cd C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening`

Remplacer **luysky** par le nom d'utilisateur Master

3. Taper `dir`



```
Administrator: Windows PowerShell
PS C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> dir

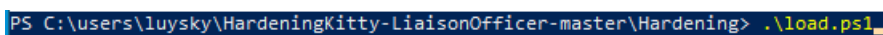
Directory: C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening

Mode                LastWriteTime         Length Name
----                -
d-----          7/27/2022   3:47 PM             HK-LiaisonOfficer
-a-----          7/27/2022   3:47 PM             493 load.ps1
-a-----          7/27/2022   3:47 PM             253 remove.ps1

PS C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening>
```

Figure 28 : Utilisation - répertoire HardeningKitty Liaison Officer (Source : Auteur)

4. Taper `.\load.ps1`. Il s'agit du Script de préparation.



```
PS C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> .\load.ps1
```

Figure 29 : Utilisation - load.ps1 (Source : Auteur)

5. Taper **R** lors de l'avertissement de sécurité.

```
PS C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> .\load.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening\load.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

Figure 30 : Préparation - Security Warning (Source : Auteur)

6. Taper le nom d'utilisateur de la machine Slave

Taper l'adresse IP de la machine Slave

Taper le mot de passe ou la passphrase (en cas de clé publique) de la machine Slave

```
Input Username, please: luysky
Input IP Address, please: 192.168.108.101
Loading HardeningKitty Liaison Officer in progress
Enter passphrase for key 'C:\Users\luysky/.ssh/id_rsa':
```

Figure 31 : Préparation - Informations machine Slave (Source : Auteur)

HardeningKitty Liaison Officer transfère par protocole SCP l'ensemble des fichiers nécessaires à son utilisation de la machine Master à la machine Slave.

```
Enter passphrase for key 'C:\Users\luysky/.ssh/id_rsa':
.gitkeep 100% 0 0.0KB/s 00:00
Invoke-HardeningKitty.ps1 100% 103KB 28.6MB/s 00:00
LICENSE 100% 1064 59.1KB/s 00:00
finding_list_0x6d69636b_machine-L0.csv 100% 64KB 63.8KB/s 00:00
finding_list_0x6d69636b_machine.csv 100% 64KB 4.5MB/s 00:00
finding_list_0x6d69636b_user.csv 100% 8185 8.0KB/s 00:00
finding_list_bsl_sisyphus_windows_10_hd_machine.csv 100% 24KB 24.3KB/s 00:00
finding_list_bsl_sisyphus_windows_10_hd_user.csv 100% 1070 82.2KB/s 00:00
finding_list_bsl_sisyphus_windows_10_nd_machine-L0.csv 100% 64KB 63.9KB/s 00:00
finding_list_bsl_sisyphus_windows_10_nd_machine.csv 100% 64KB 64.1KB/s 00:00
finding_list_bsl_sisyphus_windows_10_nd_user.csv 100% 2546 183.5KB/s 00:00
finding_list_bsl_sisyphus_windows_10_ne_machine.csv 100% 58KB 58.0KB/s 00:00
finding_list_bsl_sisyphus_windows_10_ne_user.csv 100% 2546 143.4KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1809_machine.csv 100% 121KB 121.1KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1809_user.csv 100% 3562 219.5KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1903_machine.csv 100% 122KB 8.0MB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1903_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1909_machine.csv 100% 122KB 7.6MB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_1909_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_2004_machine.csv 100% 121KB 120.8KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_2004_user.csv 100% 3336 3.3KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_20h2_machine.csv 100% 122KB 6.9MB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_20h2_user.csv 100% 3336 3.3KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_21h1_machine-L0.csv 100% 117KB 116.7KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_21h1_machine.csv 100% 117KB 116.9KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_21h1_user.csv 100% 3336 237.1KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_21h2_machine.csv 100% 121KB 120.9KB/s 00:00
finding_list_cis_microsoft_windows_10_enterprise_21h2_user.csv 100% 3566 121.9KB/s 00:00
finding_list_cis_microsoft_windows_11_enterprise_21h2_machine.csv 100% 121KB 120.9KB/s 00:00
finding_list_cis_microsoft_windows_11_enterprise_21h2_user.csv 100% 3566 3.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2012_r2_2.4.0_machine.csv 100% 73KB 73.2KB/s 00:00
finding_list_cis_microsoft_windows_server_2012_r2_2.4.0_user.csv 100% 2624 2.6KB/s 00:00
finding_list_cis_microsoft_windows_server_2016_1607_1.2.0_machine.csv 100% 80KB 4.7MB/s 00:00
finding_list_cis_microsoft_windows_server_2016_1607_1.2.0_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2016_1607_1.3.0_machine.csv 100% 81KB 5.3MB/s 00:00
finding_list_cis_microsoft_windows_server_2016_1607_1.3.0_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.1.0_machine.csv 100% 86KB 85.8KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.1.0_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.2.0_machine.csv 100% 87KB 87.1KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.2.0_user.csv 100% 3562 3.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.2.1_machine.csv 100% 87KB 87.3KB/s 00:00
finding_list_cis_microsoft_windows_server_2019_1809_1.2.1_user.csv 100% 3562 203.6KB/s 00:00
finding_list_cis_microsoft_windows_server_2022_21h1_1.0.0_machine.csv 100% 91KB 91.5KB/s 00:00
finding_list_cis_microsoft_windows_server_2022_21h2_1.0.0_user.csv 100% 3566 3.5KB/s 00:00
finding_list_dod_microsoft_windows_10_stig_v2r1_machine.csv 100% 81KB 80.8KB/s 00:00
finding_list_dod_microsoft_windows_10_stig_v2r1_user.csv 100% 1090 1.1KB/s 00:00
```

Figure 32 : Préparation - Transfert de fichier (Source : Auteur)

Si un temps trop long s'écoule pour saisir le mot de passe ou la passphrase, la connexion se perd. Dans ce cas, un message d'information s'affiche. Si cela arrive, mettre un terme à la procédure en cours en tapant CTRL C puis relancer le Script load.ps1.

7. Taper le mot de passe ou la passphrase à nouveau.

```
finding_list_msft_security_baseline_windows_server_20h2_dc_machine.csv      100% 70KB 69.9KB/s 00:00
finding_list_msft_security_baseline_windows_server_20h2_member_machine.csv  100% 70KB 70.0KB/s 00:00
.gitkeep                           100% 0    0.0KB/s 00:00
README.md                          100% 11KB 10.7KB/s 00:00
menu.ps1                           100% 5155 5.0KB/s 00:00

*****
Welcome to HardeningKitty Liaison Officer!
*****
Enter passphrase for key 'C:\Users\luysky\.ssh\id_rsa':
Microsoft Windows [Version 10.0.19044.1826]
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

luysky@SLAVE C:\Users\luysky>
```

Figure 33 : Préparation - Connexion SSH (Source : Auteur)

Il s'agit cette fois de la connexion à la machine Slave par le biais d'un protocole SSH.

8. Taper cd Hardening

Taper dir

```
luysky@SLAVE C:\Users\luysky\Hardening>dir
Volume in drive C has no label.
Volume Serial Number is B8E4-9F0A

Directory of C:\Users\luysky\Hardening

27/07/2022  16:12    <DIR>          .
27/07/2022  16:12    <DIR>          ..
27/07/2022  16:12    <DIR>          HardeningKitty
27/07/2022  16:12                5'155 menu.ps1
               1 File(s)                5'155 bytes
               3 Dir(s)  28'197'773'312 bytes free

luysky@SLAVE C:\Users\luysky\Hardening>
```

Figure 34 : Préparation - Prêt à l'utilisation (Source : Auteur)

La phase de préparation prend fin. L'ensemble des fichiers sont sur la machine Slave. La connexion SSH est établie.

4.2 Connexion SSH

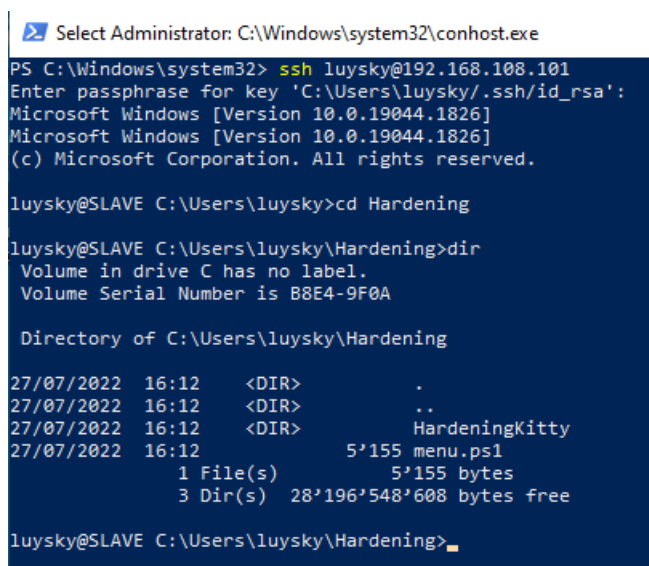
La phase d'exécution peut être réalisée directement à la suite de la phase de préparation ou n'importe quand lorsque la phase de préparation est déjà effective.

Une fois la préparation terminée, il est possible d'accéder à la machine Slave à tout moment en effectuant les démarches suivantes :

1. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**
2. Taper **ssh** puis **luisky@192.168.108.101**

Remplacer **luisky** et l'adresse IP par votre nom d'utilisateur et adresse IP Slave

3. Saisir le mot de passe ou la passphrase Slave.
4. Taper **cd Hardening**



```
Select Administrator: C:\Windows\system32\conhost.exe
PS C:\Windows\system32> ssh luisky@192.168.108.101
Enter passphrase for key 'C:\Users\luisky\.ssh\id_rsa':
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

luisky@SLAVE C:\Users\luisky>cd Hardening

luisky@SLAVE C:\Users\luisky\Hardening>dir
Volume in drive C has no label.
Volume Serial Number is B8E4-9F0A

Directory of C:\Users\luisky\Hardening

27/07/2022  16:12    <DIR>          .
27/07/2022  16:12    <DIR>          ..
27/07/2022  16:12    <DIR>          HardeningKitty
27/07/2022  16:12                5'155 menu.ps1
               1 File(s)                5'155 bytes
               3 Dir(s)  28'196'548'608 bytes free

luisky@SLAVE C:\Users\luisky\Hardening>
```

Figure 35 : Exécution - Connexion SSH (Source : Auteur)

4.3 Menu

Cette étape regroupe l'ensemble des opérations que l'utilisateur peut réaliser en utilisant HardeningKitty Liaison Officer. Le Script d'exécution, menu.ps1 peut se lancer soit à distance par connexion SSH depuis la machine Master soit directement depuis la machine Slave.

Pour exécuter le Script menu.ps1, il faut se trouver dans le répertoire Hardening de la machine Slave.

1. Taper `cd C:\Users\luysky\Hardening`

Remplacer **luysky** par le nom d'utilisateur de la machine Slave

2. Lors d'une utilisation à distance, taper **powershell.exe**
3. Taper **.\menu.ps1**
4. Taper le nom d'utilisateur de la machine Slave

```
> Administrator: C:\Windows\system32\conhost.exe - powershell.exe
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

luysky@SLAVE C:\Users\luysky>cd Hardening

luysky@SLAVE C:\Users\luysky\Hardening>dir
Volume in drive C has no label.
Volume Serial Number is B8E4-9F0A

Directory of C:\Users\luysky\Hardening

27/07/2022  16:12    <DIR>          .
27/07/2022  16:12    <DIR>          ..
27/07/2022  16:12    <DIR>          HardeningKitty
27/07/2022  16:12                5'155 menu.ps1
               1 File(s)                5'155 bytes
               3 Dir(s)  28'189'908'992 bytes free

luysky@SLAVE C:\Users\luysky\Hardening>powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\luysky\Hardening> .\menu.ps1
Input Username, please: luysky
```

Figure 36 : Menu - Script menu.ps1 (Source : Auteur)

4.3.1 Scan

La fonctionnalité Scan permet de tester le niveau de sécurité de la machine Slave en la comparant avec une liste de bonnes pratiques de Hardening.

L'utilisateur choisit la liste de Hardening qu'il veut utiliser comme référence. Il existe deux types de listes différentes : les listes machine et les listes user. Chacun correspond à un durcissement des infrastructures spécifiques basé sur les configurations de sécurité de la machine ou de l'utilisateur.

Au terme du Scan, un résultat s'affiche. Il s'agit d'une note allant de 1 à 6, 6 étant le meilleur résultat possible. Pour de plus amples informations relatives au Scan et aux résultats consulter la documentation de HardeningKitty.

1. Taper 1.

```
===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 1

SCAN
finding_list_0x6d69636b_machine-LO.csv
finding_list_0x6d69636b_machine.csv
finding_list_0x6d69636b_user.csv
finding_list_bsi_sisyphus_windows_10_hd_machine.csv
finding_list_bsi_sisyphus_windows_10_hd_user.csv
finding_list_bsi_sisyphus_windows_10_nd_machine-LO.csv
finding_list_bsi_sisyphus_windows_10_nd_machine.csv
finding_list_bsi_sisyphus_windows_10_nd_user.csv
finding_list_bsi_sisyphus_windows_10_ne_machine.csv
finding_list_bsi_sisyphus_windows_10_ne_user.csv
finding_list_cis_microsoft_windows_10_enterprise_1809_machine.csv
finding_list_cis_microsoft_windows_10_enterprise_1809_user.csv
finding_list_cis_microsoft_windows_10_enterprise_1903_machine.csv
finding_list_cis_microsoft_windows_10_enterprise_1903_user.csv
```

Figure 37 : Scan - liste de bonnes pratiques (Source : Auteur)

2. Au moyen de la souris surligner la liste choisie puis faire un clic droit

```
SCAN
finding_list_0x6d69636b_machine-LO.csv
finding_list_0x6d69636b_machine.csv
```

Figure 38 : Scan - Surligner list (Source : Auteur)


```

finding_list_msft_security_baseline_windows_server_2022_21h2_member_machine.csv
finding_list_msft_security_baseline_windows_server_20h2_dc_machine.csv
finding_list_msft_security_baseline_windows_server_20h2_member_machine.csv

Please write the name of the desired finding list followed by .csv
finding_list_0x6d69636b_machine.csv

```

Figure 39 : Scan - Sélection par click droit (Source : Auteur)

3. Taper **enter**
4. Visualiser le résultat du Scan

```

[*] 7/28/2022 9:07:53 AM - HardeningKitty is done
[*] 7/28/2022 9:07:53 AM - Your HardeningKitty score is: 3.19. HardeningKitty Statistics: Total checks: 329 - Passed: 63
, Low: 59, Medium: 206, High: 1.

```

Figure 40 : Scan - Résultat (Source : Auteur)

5. Taper **enter** pour retourner au menu.

4.3.2 Harden

La fonctionnalité Harden permet d'appliquer du Hardening sur la machine Slave. Il est à noter que la connexion par protocole SSH d'une machine distante à la machine Slave est considérée comme un risque par les bonnes pratiques de Hardening. C'est pourquoi après l'application d'un Hardening « machine » il n'est plus possible d'accéder depuis la machine Master à la machine Slave.

```

PS C:\Windows\system32> ssh luysky@192.168.108.101
Connection reset by 192.168.108.101 port 22
PS C:\Windows\system32>

```

Figure 41 : Harden – connexion annulée (Source : Auteur)

Afin d'éviter ce durcissement spécifique, nous fournissons quelques listes modifiées dont l'utilisation ne bloque pas ultérieurement l'accès par connexion SSH. Il s'agit des listes dont le nom se termine par LO. Pour plus d'informations sur comment modifier une liste voir le chapitre « personnalisation ».

1. Taper 2
2. Au moyen de la souris **surligner la liste** choisie puis faire un **clic droit**
3. Taper **enter** pour exécuter le Hardening
4. Taper **enter** pour retourner au menu

4.3.3 Audit

La fonctionnalité Audit est similaire à celle du Scan à la différence qu'elle conserve des logs et un rapport de l'exécution du Scan. Cet audit peut être récupéré ultérieurement sur la machine Master pour conservation et analyse. (voir chapitre Export Logs, Reports and Backups)

1. Taper 3
2. Taper un **nom de fichier** puis taper **enter**
3. Au moyen de la souris **surligner la liste** choisie puis faire un **clic droit**

```
===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 3

AUDIT
Input file name, please: myAudit
finding_list_0x6d69636b_machine-LO.csv
finding_list_0x6d69636b_machine.csv
```

Figure 42 : Audit – nom de l'audit et sélection liste (Source : Auteur)

4. Taper **enter** pour retourner au menu

Les fichiers de log et de rapport sont disponibles sur la machine Slave sous :

C:\Users\luysky\Hardening\HardeningKitty\logsNreports

Remplacer luysky par le nom d'utilisateur de la machine Slave

« Hardening > HardeningKitty > logsNreports Search logsNreports				
	Name	Date modified	Type	Size
ss	.gitkeep	27/07/2022 16:12	GITKEEP File	0 KB
ds	07-28-2022-0943-myAudit-log	28/07/2022 09:45	Text Document	38 KB
nts	07-28-2022-0943-myAudit-report.csv	28/07/2022 09:45	CSV File	29 KB

Figure 43 : Audit – log et rapport (Source : Auteur)

4.3.4 Backup

La fonctionnalité Backup est très importante. Elle permet de sauvegarder la configuration d'une machine avant d'appliquer du Hardening. De cette manière, il est possible après Hardening de revenir à une situation antérieure au durcissement de l'infrastructure. Ce fichier de Backup peut être récupéré ultérieurement sur la machine Master pour conservation. (voir chapitre Export Logs, Reports and Backups)

1. Taper 4
2. Taper le nom du fichier de Backup puis enter

```

===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 4

BACKUP
Input backup name, please: myBackup

    =^._.^=
    _ (      ) / HardeningKitty 0.8.0-1656567332

[*] 7/28/2022 10:23:49 AM - Starting HardeningKitty

```

Figure 44 : Backup – fichier de backup (Source : Auteur)

Les fichiers de backup sont disponibles sur la machine Slave sous :

C:\Users\luysky\Hardening\HardeningKitty\backups

Remplacer luysky par le nom d'utilisateur de la machine Slave

<div> <div> <div><<</div> <div>Hardening</div> <div>></div> </div> <div> <div>HardeningKitty</div> <div>></div> </div> <div>backups</div> </div> <div> <div>Search backups</div> </div>				
	Name	Date modified	Type	Size
ss	.gitkeep	27/07/2022 16:12	GITKEEP File	0 KB
ls	07-28-2022-1023-myBackup.csv	28/07/2022 10:24	CSV File	72 KB

Figure 45 : Backup – emplacement fichier backup (Source : Auteur)

Il est désormais possible de sélectionner comme liste de Hardening le fichier de Backup récemment créé.

```

===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 2

HARDEN
07-28-2022-1023-myBackup.csv
finding_list_0x6d69636b_machine-LO.csv
finding_list_0x6d69636b_machine.csv
finding_list_0x6d69636b_user.csv

```

Figure 46 : Backup – backup ajouté aux listes (Source : Auteur)

4.3.5 Export Logs, Reports and Backups

La génération de fichiers d'Audit ou de Backup s'effectue sur la machine Slave. Afin de récupérer l'ensemble de ces fichiers, il est nécessaire de les transférer de la machine Slave à la machine Master. La fonctionnalité Export Logs, Reports and Backups effectue cette démarche.

1. Taper 5.
2. Taper le nom d'utilisateur de la machine **Master**
3. Taper l'adresse IP de la machine **Master**
4. Taper le mot de passe ou la passphrase de la machine **Master** (Transfère log et rapport)
5. Taper le mot de passe ou la passphrase de la machine **Master** (Transfère backup)

```

===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 5

EXPORT
Input MASTER Username, please: luysky
Input MASTER IP Address, please: 192.168.108.100
Loading HardeningKitty Liaison Officer in progress
Export logsNReports
Enter passphrase for key 'C:\Users\luysky\.ssh\id_rsa':
.gitkeep
07-28-2022-0943-myAudit-log.txt          100%    0    0.0KB/s    00:00
07-28-2022-0943-myAudit-report.csv      100%  38KB  2.6MB/s    00:00
Export backups
Enter passphrase for key 'C:\Users\luysky\.ssh\id_rsa':

```

Figure 47 : Export – exporter les fichiers (Source : Auteur)

Le transfert utilise un protocole SCP. L'ensemble des fichiers est désormais présent sur la machine Master sous :

C:\Users\luysky

Remplacer luysky par le nom d'utilisateur de la machine Master

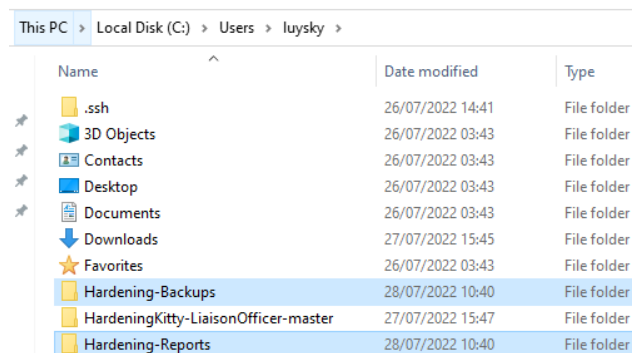


Figure 48 : Export – répertoires backups et reports (Source : Auteur)

4.3.6 Quitter HardeningKitty Liaison Officer

Cette fonctionnalité explique les démarches nécessaires afin de mettre un terme à l'utilisation de HardeningKitty Liaison Officer.

1. Taper 0 pour quitter le menu.

2. Taper exit pour quitter powershell.exe
3. Taper exit pour fermer la connexion SSH

```

===== HardeningKitty Liaison Officer =====
1: Scan.
2: Harden.
3: Audit.
4: Backup.
5: Export Logs, Reports and Backups.
0: Press '0' to quit.
Please make a selection: 0

=====
Type exit twice to end remote connection
=====

PS C:\Users\luysky\Hardening> exit

luysky@SLAVE C:\Users\luysky\Hardening>exit
Connection to 192.168.108.101 closed.
PS C:\Windows\system32>

```

Figure 49 : Quit - quitter HardeningKitty Liaison Officer (Source : Auteur)

4.4 Nettoyage

Cette fonctionnalité a pour but de retirer de la machine Slave l'intégralité des fichiers transférés de la machine Master et également ceux qui ont été générés par l'utilisation d'HardeningKitty Liaison Officer.

Avant d'effectuer ces démarches, s'assurer qu'aucun fichier ou répertoire d'HardeningKitty Liaison Officer ne soit ouvert. En cas de doute, redémarrer la machine Slave.

1. Dans la barre de recherche Windows taper **powershell** puis sélectionner **Run as administrator**
2. Taper `cd C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening`
Remplacer luysky par votre nom d'utilisateur Master
3. Taper `.\remove.ps1`
4. Taper **R**
5. Taper le **nom d'utilisateur** de la machine **Slave**
6. Taper l'**adresse IP** de la machine **Slave**
7. Taper **y**

```
PS C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> dir

Directory: C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening

Mode                LastWriteTime         Length Name
----                -
d-----          7/27/2022   3:47 PM             HK-LiaisonOfficer
-a-----          7/27/2022   3:47 PM           493 load.ps1
-a-----          7/27/2022   3:47 PM           253 remove.ps1

PS C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> .\remove.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening\remove.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r
Input Username, please: luysky
Input IP Address, please: 192.168.108.101
Enter passphrase for key 'C:\Users\luysky\.ssh\id_rsa':
C:\Users\luysky\Hardening, Are you sure (Y/N)? y
y
HardeningKitty has been fully removed.
PS C:\Users\luysky\HardeningKitty-LiaisonOfficer-master\Hardening> █
```

Figure 50 : Remove - Script Remove.ps1 (Source : Auteur)

4.5 Personnalisation

Ce chapitre a pour but d'expliquer comment personnaliser les listes de bonnes pratiques qui sont utilisées par HardeningKitty Liaison Officer. L'ensemble de ces démarches est à réaliser depuis la **machine Master** après téléchargement de HardeningKitty Liaison Officer.

Nous recommandons d'utiliser Visual Studio Code pour effectuer des modifications de listes.

[Visual Studio Code - Download](#)

Ce guide n'a pas vocation de montrer l'ensemble des modifications possibles qu'un utilisateur peut effectuer. Nous montrons ici comment modifier une liste afin d'en retirer le Hardening bloquant les connexions SSH entrantes :

1. Ouvrir Visual Studio Code en mode administrateur
2. Charger le répertoire HardeningKitty Liaison Officer Master
3. Aller dans le répertoire list

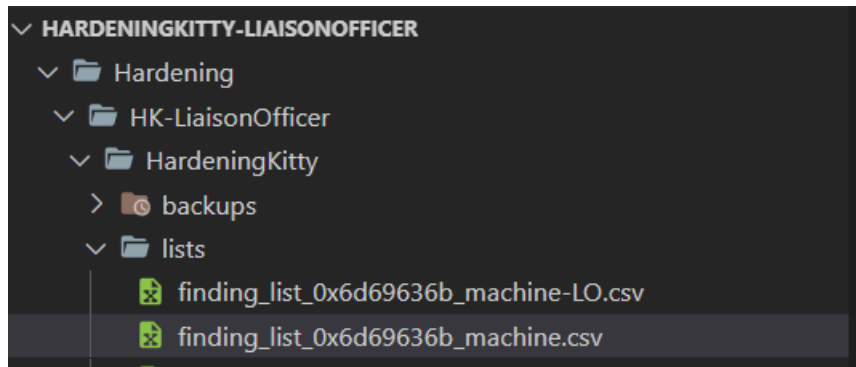


Figure 51 : Modification – Sélection d'une liste (Source : Auteur)

4. Double cliquer sur la liste choisie.



Figure 52 : Modification - List (Source : Auteur)

5. Repérer la ligne "User Rights Assignment","Deny access to this computer from the network"

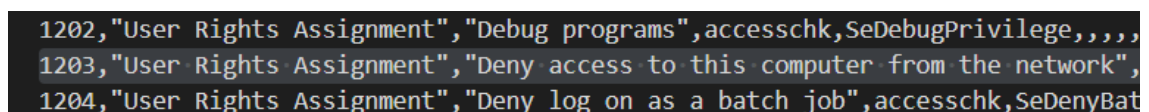


Figure 53 : Modification - User Rights (Source : Auteur)

6. Supprimer la ligne avec le bouton delete
7. Sauvegarder la liste modifiée dans le répertoire list. Nous conseillons d'enregistrer une liste modifiée en lui rajoutant les lettres LO à la fin pour Liaison Officer.