



ENSA
ÉCOLE NATIONALE DES SCIENCES
APPLIQUÉES
KHOURIBGA



Rapport de projet de fin d'année

En vue de valider notre année universitaire

Spécialité : Ingénierie des Réseaux Intelligents et de la Cyber sécurité

Présenté par

AJAITE Houssam-eddine

EL MOUJAHID Maha

FDILI Houda

PEZONGO Mickael

WAHBI Mohamed

WebSecPi - Plateforme de tests d'intrusion sur Raspberry PI 4

Encadrants

Mr Nouredine ABOUTABIT

Mr Imade Fahd Eddine FATANI

RESUME

Ce projet consiste en la création d'une interface web permettant d'exécuter des commandes à distance sur un Raspberry Pi et d'utiliser des exploits via MSFConsole, dans le but de réaliser des tests d'intrusion à distance sur des cibles spécifiques.

La première partie du projet se concentre sur la présentation et la configuration de l'interface web, visant à offrir une expérience utilisateur conviviale et pratique. Des fonctionnalités telles qu'un shell distant et une intégration avec MSFConsole sont mises en place pour permettre une gestion à distance efficace du Raspberry Pi.

La deuxième partie du projet concerne l'implémentation de l'interface web pour les tests d'intrusion. Les utilisateurs peuvent exécuter des commandes à distance sur leur Raspberry Pi, ce qui leur offre une flexibilité et une mobilité accrues dans la gestion de leur appareil. De plus, l'intégration de MSFConsole permet l'utilisation de exploits avancés, ce qui est particulièrement utile pour les professionnels de la sécurité cherchant à évaluer la vulnérabilité des systèmes.

Enfin, une simulation complète d'une attaque est réalisée sur l'interface web. Cela permet de mettre en évidence les capacités de l'application pour mener des attaques ciblées à distance. Cependant, il est important de souligner que l'utilisation de cette application à des fins malveillantes est strictement interdite et que ce projet vise principalement à des fins éducatives et de recherche dans le domaine de la sécurité informatique.

En conclusion, ce projet offre une solution pratique, accessible et sécurisée pour la gestion à distance du Raspberry Pi et l'exécution de tests d'intrusion. Il représente un outil puissant pour les passionnés de Raspberry Pi et les professionnels de la sécurité cherchant à approfondir leurs compétences et connaissances en matière de sécurité informatique.

TABLE DES MATIERES

RESUSME.....	3
TABLE DES MATIERES.....	4
INTRODUCTION.....	6
CHAPITRE1 : Notre projet.....	7
I. Objectif de notre projet.....	7
1. Création d’une interface web.....	7
2. Utilisation de métasploit.....	7
3. Evaluation de la sécurité des systèmes cibles.....	7
II. Contexte du projet.....	8
CHAPITRE2 : Présentation et configuration.....	9
I. PRESENTATION DU RASPBERRY PI 4.....	9
II. INSTALLATION DU SYSTEME D’EXPLOITATION.....	10
III. CONFIGURATION RESEAU.....	12
1. CONFIGURATION DU SERVEUR DHCP.....	12
a. Présentation du dhcp serveur.....	12
b. Utilisation du DHCP Server pour le Raspberry Pi 4.....	12
2. CONFIGURATION DU RESEAU WIFI.....	16
3. CONFIGURATION DE VPN ZERO TIER.....	18
a. Présentation de zero tier.....	18
b. Installation et configuration de zerotier sur raspberry.....	18
4. INTERFACE GRAPHIQUE DU RASPBERRY.....	20
a. Présentation de VNC Server.....	20
b. Configuration de vnc server sur raspberry.....	21
c. Connexion à l’aide de vnc viewer.....	23
CHAPITRE3 : IMPLEMENTATION DE L’INTERFACE WEB ET TESTS D'INTRUSION	24
I. INSTALLATION DES PREREQUIS.....	24
1. INSTALLATION DE NODEJS.....	24
2. INSTALLATION DE NMAP.....	24
3. INSTALLATION DE MSFCONSOLE.....	26
II. PRESENTATION DE L’INTERFACE WEB.....	28
III. SIMULATION D’UNE ATTAQUE COMPLETE AVEC L’INTERFACE WEB.....	29
CONCLUSION.....	34

INTRODUCTION

Les cyberattaques sont devenues une menace croissante pour les systèmes informatiques et les réseaux. Les entreprises et les organisations doivent prendre des mesures pour évaluer et renforcer leur sécurité afin de protéger leurs données sensibles et leurs infrastructures. Les tests d'intrusion sont une méthode couramment utilisée pour évaluer la résistance d'un système aux attaques et identifier les vulnérabilités qui pourraient être exploitées par des attaquants malveillants.

Dans le cadre de ce projet, nous avons exploré les capacités du Raspberry Pi 4, une plateforme d'ordinateur monocarte abordable et polyvalente, pour créer une interface web permettant d'exécuter des tests d'intrusion et d'évaluer la sécurité d'un réseau. Notre objectif était de développer une solution pratique et portable, offrant une approche conviviale pour les tests d'intrusion, tout en étant abordable pour les petites entreprises et les passionnés de sécurité.

Chapitre 1 : Notre projet

I. Objectif du projet

1. Création d'une interface web

Notre premier objectif était de concevoir et développer une interface web conviviale qui permettrait aux utilisateurs de configurer et d'exécuter des tests d'intrusion sur des cibles spécifiques. L'interface devait être intuitive, offrant une expérience utilisateur fluide pour les personnes sans connaissances approfondies en sécurité informatique.

2. Utilisation de métasploit

Nous avons choisi d'utiliser Metasploit, une plateforme d'exploitation de vulnérabilités largement utilisée, comme outil principal pour les tests d'intrusion. Notre objectif était d'explorer les fonctionnalités de Metasploit et de l'intégrer dans notre interface web, offrant ainsi aux utilisateurs un accès facile à un large éventail de modules d'exploitation et d'outils de test d'intrusion.

3. Évaluation de la sécurité des systèmes cibles

Nous souhaitons évaluer la sécurité des systèmes cibles en exécutant des tests d'intrusion à l'aide de notre interface web. Notre objectif était de détecter les vulnérabilités potentielles, d'identifier les failles de sécurité et de fournir des recommandations pour améliorer la résistance aux attaques.

II. Contexte du projet

Le Raspberry Pi 4 est un choix idéal pour ce projet en raison de sa puissance de calcul, de sa flexibilité et de sa faible consommation d'énergie. Ces caractéristiques en font une plateforme de test d'intrusion compacte et économe en ressources, pouvant être facilement transportée et déployée dans différents environnements.

Les tests d'intrusion sont une pratique courante dans le domaine de la sécurité informatique, permettant de simuler des attaques et d'identifier les vulnérabilités avant qu'elles ne soient exploitées par des acteurs malveillants. L'utilisation de Metasploit, un outil open source populaire, nous a permis d'accéder à une vaste gamme de modules d'exploitation et d'exploiter des vulnérabilités connues pour évaluer la résistance des systèmes cibles.


Chapitre 2 : Présentation et configuration

I. Présentation du Raspberry Pi 4

Le Raspberry Pi 4 est un ordinateur mono carte de petite taille, conçu pour offrir une solution abordable et polyvalente pour les projets de développement et d'expérimentation. Il est doté d'un processeur ARM Cortex-A72 quadri cœur, de jusqu'à 8 Go de RAM, de ports USB, d'un port Ethernet, d'un slot pour carte microSD et de ports d'affichage HDMI.

La puissance de calcul du Raspberry Pi 4 en fait une plateforme idéale pour exécuter des applications et des logiciels gourmands en ressources, tels que Metasploit. Son faible coût et sa taille compacte en font également un choix populaire pour les projets de test de sécurité et les environnements de laboratoire.

The Raspbian with Desktop image contained in the ZIP archive is over 4GB in size, which means that these archives use features which are not supported by older unzip tools on some platforms. If you find that the download appears to be corrupt or the file is not unzipping correctly, please try using [7Zip](#) (Windows) or [The Unarchiver](#) (Macintosh). Both are free of charge and have been tested to unzip the image correctly.




Raspbian Buster with desktop and recommended software
Image with desktop and recommended software based on Debian Buster

Version: February 2020
Release date: 2020-02-13
Kernel version: 4.19
Size: 2530 MB

[Release notes](#)

[Download Torrent](#) [Download ZIP](#)

SHA-256: c9c352b659b9d94b8590cb9e2a00c2292a91a370286ab4642f23850451077662d




Raspbian Buster with desktop
Image with desktop based on Debian Buster

Version: February 2020
Release date: 2020-02-13
Kernel version: 4.19
Size: 1136 MB

[Release notes](#)

[Download Torrent](#) [Download ZIP](#)

SHA-256: ae2ed4139dfad31c3167e60e943bcbe28c404d1558f4713efe5830c08a419f50



Raspbian Buster Lite
Minimal image based on Debian Buster

Version: February 2020
Release date: 2020-02-13
Kernel version: 4.19
Size: 434 MB

[Release notes](#)

[Download Torrent](#) [Download ZIP](#)

SHA-256: 12ae6e17bf95b6ba53beca61e7394e7411b45eba7e6a520f434b0745ea7370e8

Note: Raspbian and NOOBS contain Java SE Platform Products, licensed to you under the Oracle Binary Code Licence Agreement available [here](#). Mathematica and the Wolfram Language are included in this release under license and with permission of Wolfram Research, Inc. and may be used for non-commercial purposes only. By using this software you agree to be bound by the Wolfram Raspberry Pi Bundle License Agreement available

II. Installation du système d'exploitation

Pour utiliser le Raspberry Pi 4, nous avons procédé à l'installation d'un système d'exploitation adapté. Nous avons opté pour Raspbian, une distribution Linux basée sur Debian spécialement conçue pour les Raspberry Pi.

Nous avons téléchargé l'image Raspbian officielle et l'avons écrite sur une carte microSD à l'aide d'un logiciel de gravure d'image.

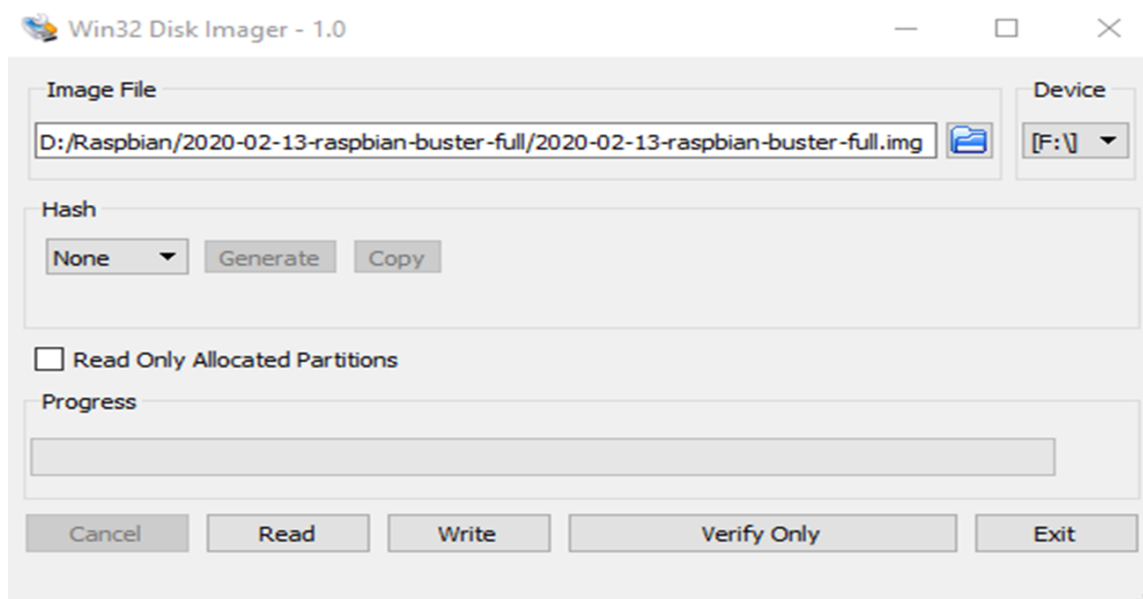
Nous avons besoin de télécharger un programme appelé: Win32 Disk Imager



Le processus d'installation de Raspbian a été guidé par une interface conviviale, nous permettant de sélectionner les options de configuration de base, telles que la langue, le fuseau horaire et les paramètres de réseau.

Exécutez d'abord le programme d'installation de Win32 Disk Imager, puis chargez le programme.

Cliquez ensuite sur "Write"



III. Configuration réseau

Une fois le système d'exploitation installé, nous avons configuré le réseau sur le Raspberry Pi 4 pour assurer la connectivité. Nous avons utilisé l'interface Ethernet pour connecter le Raspberry Pi 4 à notre réseau local, ce qui nous a permis d'accéder à l'interface web depuis d'autres appareils connectés.

1. Configuration du serveur dhcp

a. Présentation du DHCP Server

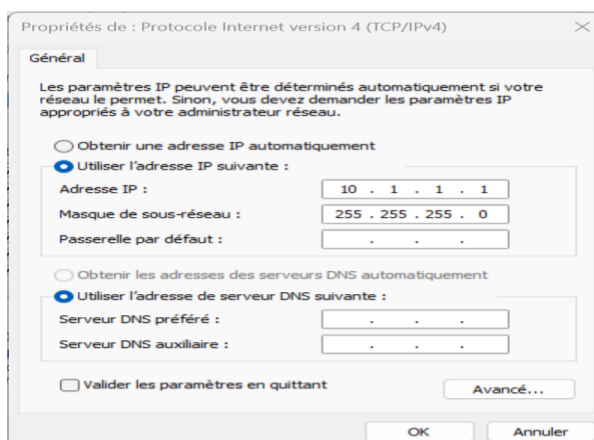
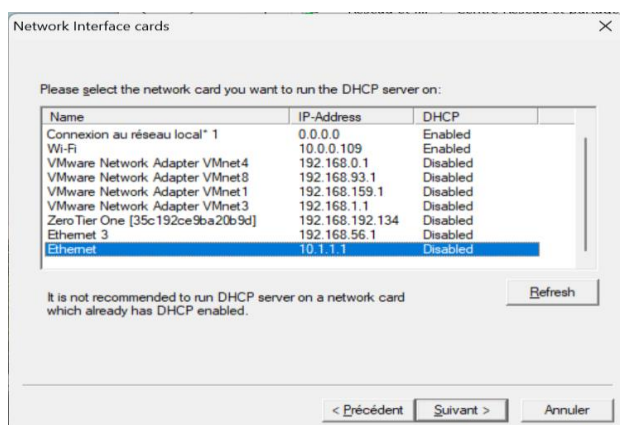
Le serveur DHCP est un composant logiciel qui joue le rôle de distributeur d'adresses IP dans un réseau. Il attribue automatiquement des adresses IP, ainsi que d'autres paramètres réseau tels que les adresses DNS et les passerelles par défaut, aux appareils qui se connectent au réseau.

b. Utilisation du DHCP Server pour le Raspberry Pi 4

L'utilisation d'un serveur DHCP offre plusieurs avantages lors de la configuration du Raspberry Pi 4 :

- Attribution automatique des adresses IP.
- Flexibilité dans les environnements de déploiement.
- Gestion centralisée des adresses IP.

D'abord on va attribuer à notre machine windows une adresse IP statique.

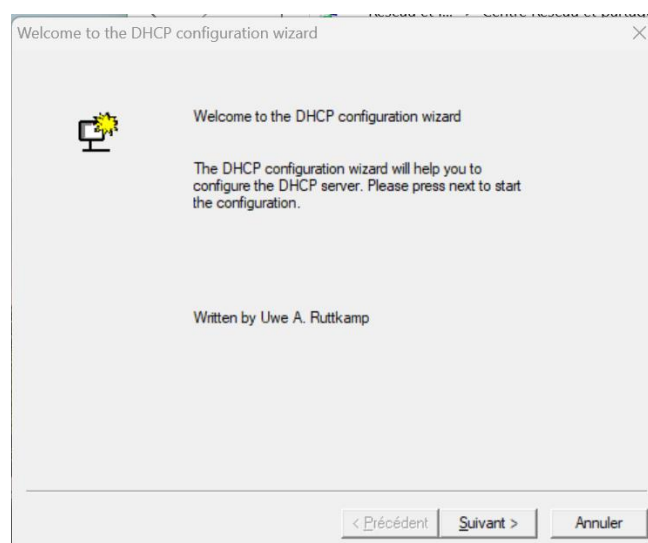
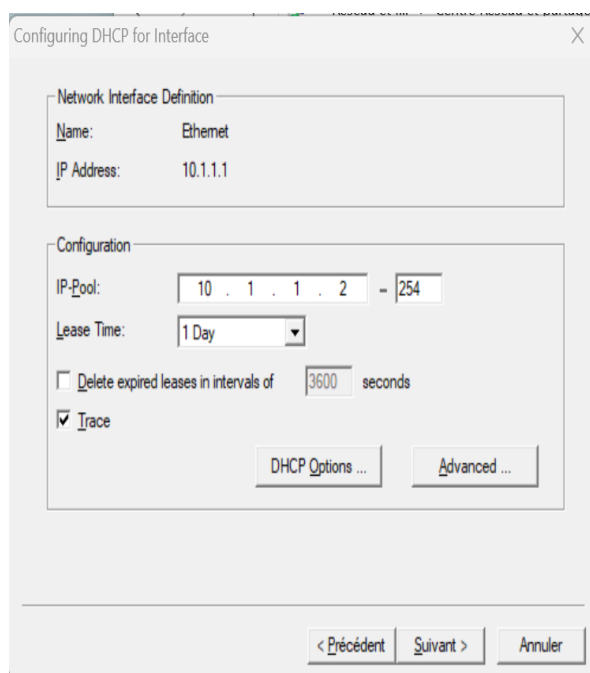


Maintenant on passe à la configuration du serveur dhcpwiz :

DHCPwiz est un outil de configuration du service DHCP (Dynamic Host Configuration Protocol) dans les environnements Windows. Le DHCP est un protocole réseau utilisé pour attribuer automatiquement des adresses IP, des paramètres de réseau et d'autres informations de configuration aux appareils connectés à un réseau.

DHCPwiz est spécifiquement conçu pour faciliter la configuration du service DHCP dans les systèmes d'exploitation Windows. Il offre une interface conviviale et des fonctionnalités avancées pour simplifier le processus de configuration et de gestion du service DHCP.

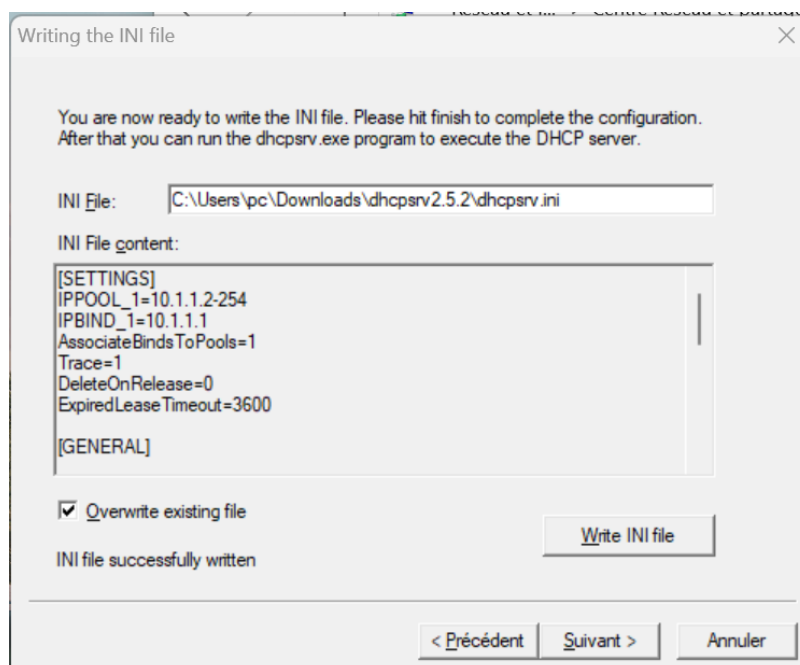
L'avantage de DHCPwiz réside dans sa simplicité d'utilisation, même pour les administrateurs réseau moins expérimentés. Il simplifie la configuration du service DHCP et permet de gagner du temps lors de la mise en place et de la maintenance des réseaux.



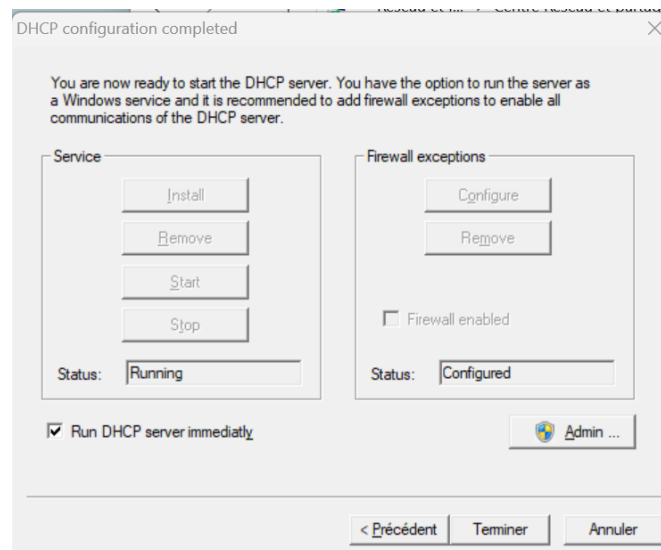
Dans DHCPwiz, vous pouvez spécifier l'interface réseau sur laquelle vous souhaitez que le serveur DHCP attribue des adresses IP. Cela vous permet de contrôler quelles interfaces réseau sont utilisées pour la distribution des adresses IP dans votre réseau. On définit le pool des adresses de 10.1.1.2 jusqu'à 10.1.1.254

Vous pouvez configurer le fichier INI pour définir et personnaliser les paramètres préétablis du serveur DHCP. Le fichier INI (Initialisation) contient les options de configuration du serveur DHCP, telles que les plages d'adresses IP, les options de bail, les options de configuration spécifiques, les réservations d'adresses IP, etc.

On configure le fichier ini qui se comporte des paramètres qu'on a déjà prédéfinis :



On démarre le serveur dhcp :



2. Configuration de réseau WIFI

Maintenant on connecte la carte raspberry au wifi pour qu'on aura accès à l'internet afin d'installer les dépendances qu'on va utiliser ultérieurement.

On accède a l'aide de SSH pour configurer la raspberry :

```
C:\Users\pc>ssh pi@10.1.1.2
pi@10.1.1.2's password:
Linux raspberrypi 5.15.84-v7l+ #1613 SMP Thu Jan 5 12:01:26 GMT 2023 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 25 20:46:30 2023
pi@raspberrypi:~ $
```

La commande raspi-config va nous aider a configurer la raspberry on va l'utiliser aussi pour l'affichage :

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 25 20:46:30 2023
pi@raspberrypi:~ $ sudo raspi-config
```

On va sélectionner System Options :

Raspberry Pi Software Configuration Tool (raspi-config)	
1 System Options	Configure system settings
2 Display Options	Configure display settings
3 Interface Options	Configure connections to peripherals
4 Performance Options	Configure performance settings
5 Localisation Options	Configure language and regional settings
6 Advanced Options	Configure advanced settings
8 Update	Update this tool to the latest version
9 About raspi-config	Information about this configuration tool
<div><Select> <Finish></div>	

Après on selectionne Wireless LAN :

Raspberry Pi Software Configuration Tool (raspi-config)	
S1 Wireless LAN	Enter SSID and passphrase
S2 Audio	Select audio out through HDMI or 3.5mm jack
S3 Password	Change password for the 'pi' user
S4 Hostname	Set name for this computer on a network
S5 Boot / Auto Login	Select boot into desktop or to command line
S6 Network at Boot	Select wait for network connection on boot
S7 Splash Screen	Choose graphical splash screen or text boot
S8 Power LED	Set behaviour of power LED
<div><Select> <Back></div>	

On entre le SSID et le passphrase du routeur :

Please enter SSID

Trevor

<Ok> <Cancel>

Please enter passphrase. Leave it empty if none.

<Ok> <Cancel>

3. Configuration de VPN Zerotier

a. Présentation du Zerotier

ZeroTier est un logiciel de réseau privé virtuel (VPN) qui permet de créer des réseaux locaux virtuels (LAN) sécurisés et décentralisés. Il permet aux utilisateurs de connecter des appareils sur différents réseaux physiques et de les faire fonctionner comme s'ils étaient tous sur le même réseau local.

ZeroTier utilise une technologie de réseau peer-to-peer, ce qui signifie que les appareils communiquent directement entre eux sans passer par un serveur central. Cela offre plusieurs avantages, notamment une latence réduite et une meilleure sécurité puisque les données sont chiffrées de bout en bout.

Pour utiliser ZeroTier, vous devez installer le logiciel sur vos appareils et les ajouter à un réseau ZeroTier spécifique. Chaque appareil se voit attribuer un identifiant unique appelé "adresse ZeroTier". Une fois les appareils connectés au même réseau ZeroTier, ils peuvent communiquer entre eux comme s'ils étaient sur le même réseau local physique.

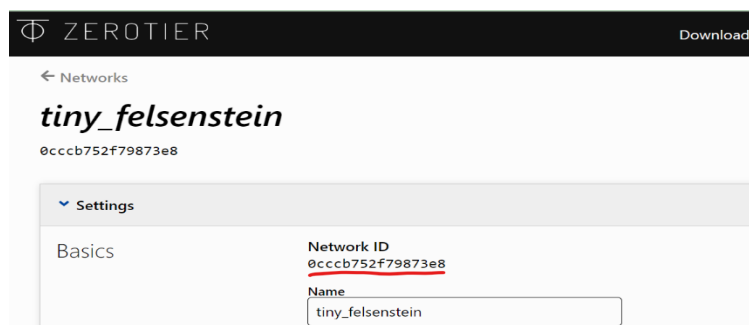
ZeroTier est utilisé dans de nombreux scénarios, tels que le travail à distance, les jeux en ligne, les réseaux d'entreprise distribués et les systèmes d'automatisation domestique. Il est compatible avec différents systèmes d'exploitation, y compris Windows, macOS, Linux, iOS et Android.

b. Installation et configuration de zerotier sur raspberry

On installe zerotier sur la carte avec la commande suivante

```
pi@raspberrypi:~$ curl -s https://install.zerotier.com | sudo bash
pi@raspberrypi:~$
```

On crée notre réseau vpn :





On exécute cette commande pour rejoindre le réseau :

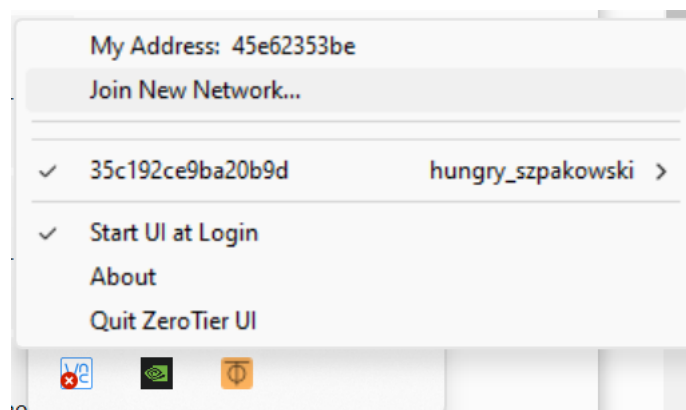
```
pi@raspberrypi:~ $ sudo zerotier-cli join 0cccb752f79873e8
200 join OK
```

Voici l'adresse IP obtenue par le vpn :

```
ztly5s6ii7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2800
    inet 10.242.61.202 netmask 255.255.0.0 broadcast 10.242.255.255
    inet6 fe80::e86f:3aff:fe5f:77c prefixlen 64 scopeid 0x20<link>
    ether ea:6f:3a:5f:07:7c txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 63 bytes 7150 (6.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

< 1-8 / 8 >						
	Address	Name/Description	Managed IPs	Last Seen	Version	Physical IP
	1ca2a855cb ea:6f:3a:5f:07:7c	(short-name)	 <u>10.242.61.202</u>	10 DAYS	1.10.3	105.66.0.117
		(description)	+ 10.242.0.x			

On rejoint le réseau d'après Windows



4. Interface graphique de Raspbian

a. Présentation de VNC Server

VNC (Virtual Network Computing) Server est un logiciel qui permet de partager et d'accéder à distance à un ordinateur ou à un environnement de bureau à travers un réseau. Il permet de contrôler un ordinateur distant comme si vous étiez assis devant lui, ce qui facilite la collaboration à distance, le dépannage technique et l'accès à des machines distantes et voici une présentation générale des fonctionnalités et du fonctionnement de VNC Server :

- Accès à distance : VNC Server permet d'accéder à distance à un ordinateur depuis un autre ordinateur, une tablette ou un smartphone. Vous pouvez visualiser et contrôler l'ordinateur distant en utilisant l'interface utilisateur de votre propre appareil.
- Partage de bureau : VNC Server permet de partager votre bureau avec d'autres utilisateurs, ce qui facilite la collaboration et la présentation à distance. Vous pouvez donner à d'autres personnes l'autorisation de voir votre écran et d'interagir avec votre ordinateur, ce qui est particulièrement utile lors de réunions en ligne ou de sessions de formation à distance.
- Plateformes supportées : VNC Server est disponible pour plusieurs plateformes, y compris Windows, macOS et Linux. Il est également compatible avec les appareils mobiles tels que les smartphones et les tablettes, ce qui permet d'accéder à distance à un ordinateur depuis ces appareils.
- Sécurité : VNC Server offre des fonctionnalités de sécurité avancées pour protéger les connexions à distance. Vous pouvez configurer des mots de passe forts et utiliser des méthodes d'authentification sécurisées pour vous assurer que seules les personnes autorisées peuvent accéder à votre ordinateur.
- Performance : VNC Server utilise des techniques de compression pour optimiser les performances lors de l'accès à distance. Cela permet de réduire la latence et d'améliorer la réactivité, même sur des connexions réseau lentes.
- Configuration et personnalisation : VNC Server offre des options de configuration et de personnalisation pour répondre aux besoins spécifiques de l'utilisateur. Vous pouvez définir des paramètres tels que la résolution d'écran, la qualité d'image, les autorisations d'accès, etc.

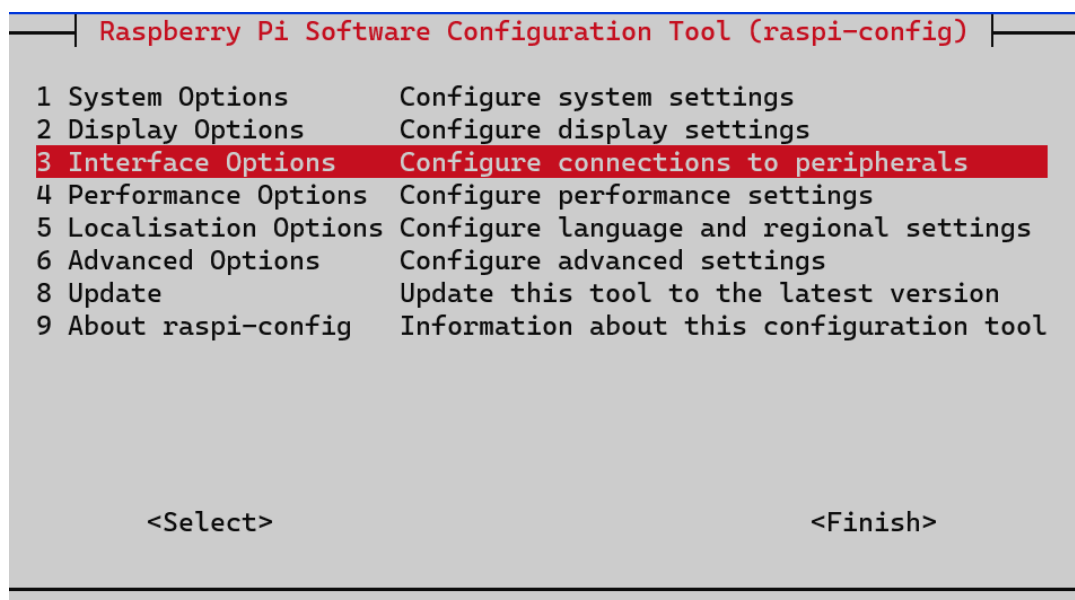
- Intégration avec d'autres logiciels : VNC Server peut être intégré à d'autres applications et systèmes de gestion à distance. Par exemple, il peut être utilisé avec des outils de gestion à distance, des systèmes de surveillance à distance ou des logiciels de support technique.

Il est important de noter que VNC Server nécessite l'installation d'un logiciel client VNC sur l'appareil à partir duquel vous souhaitez accéder à distance à un ordinateur. Le Logiciel client VNC permet d'établir la connexion avec VNC Server et d'afficher l'interface utilisateur de l'ordinateur distant.

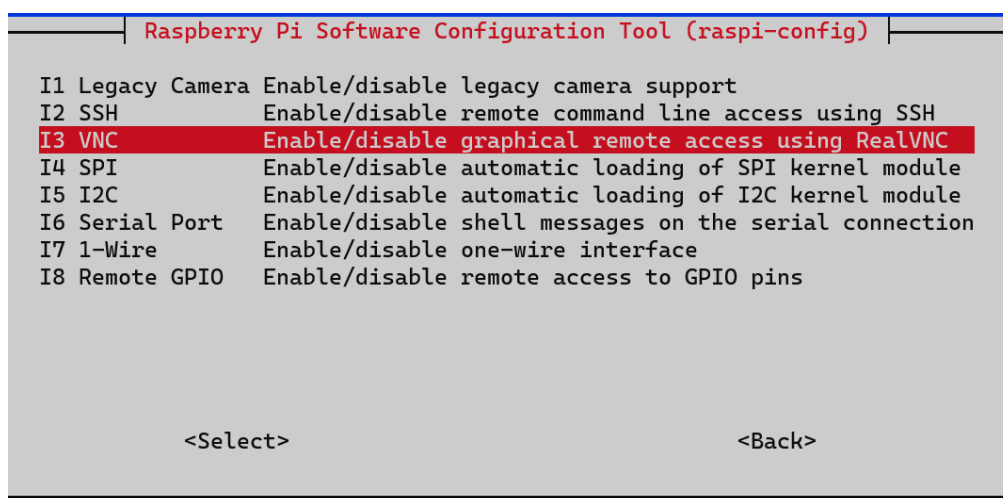
En résumé, VNC Server est un outil puissant et polyvalent pour l'accès à distance et le partage de bureau. Il facilite la collaboration à distance, le dépannage technique et l'accès à des machines distantes, le tout avec des fonctionnalités de sécurité avancées.

b. Configuration de vnc server sur raspberry

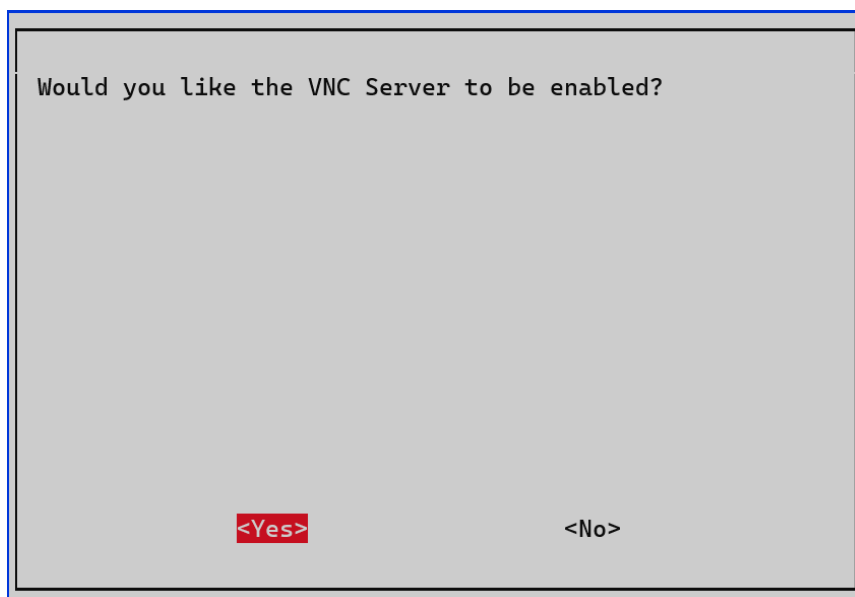
Par défaut, le serveur est installé sur le système Raspbian, donc il suffit juste l'activer afin de l'utiliser. Pour cela on accède à raspi-config et on choisit 3 les options d'interface pour configurer les connexions.



Ensuite on accède a VNC pour l'activer en utilisant RealVNC.



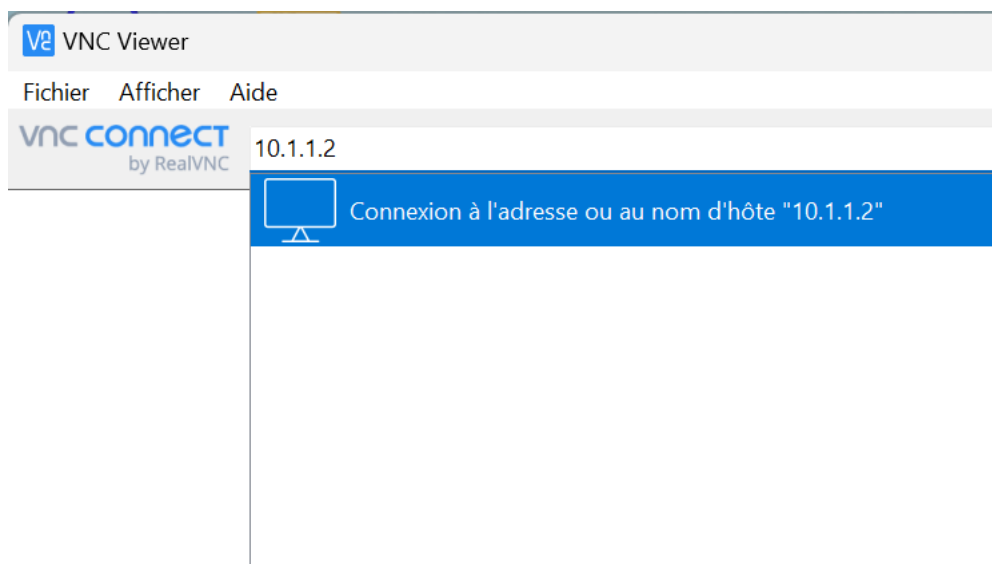
Puis on confirme l'activation de notre serveur VNC.



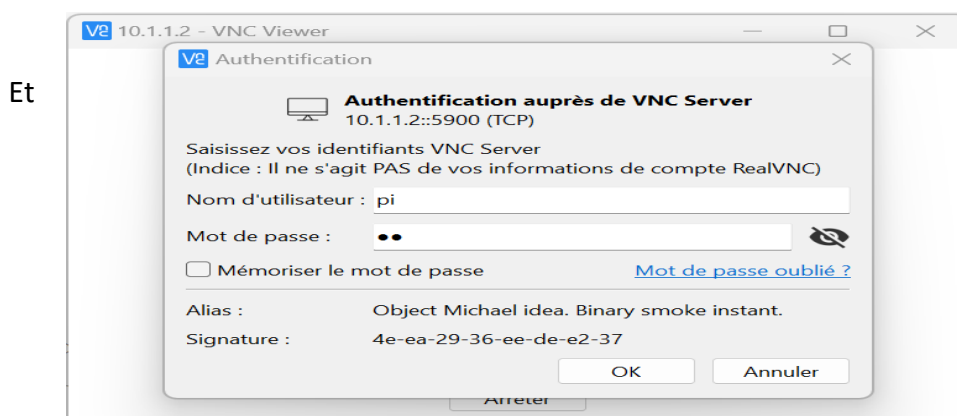
e. Connexion à l'aide de vnc viewer

VNC Viewer est un logiciel qui permet d'accéder à distance à un ordinateur contrôlé par VNC Server. Il fonctionne comme un client VNC et permet à l'utilisateur de visualiser et de contrôler l'ordinateur distant depuis son propre appareil.

Tout d'abord on installe le fichier vncviewer.exe sur notre machine Windows, qui se lance comme ci- dessous, et on écrit l'adresse IP de notre carte Raspberry.



Ensuite, VNC viewer nous demande d'entrer le nom d'utilisateur et le mot de passe pour réaliser une connexion SSH, pour notre carte le nom d'utilisateur est « pi » et le mot de passe est aussi « pi »



finalement, on peut visualiser l'interface graphique de notre système d'exploitation Raspbian qui est installé sur notre carte et cela nous facilite énormément l'utilisation de la carte et c'est plus pratique qu'une connexion SSH simple.

Chapitre3 : Implémentation de l'interface web et tests d'intrusion

I. Installation des prérequis

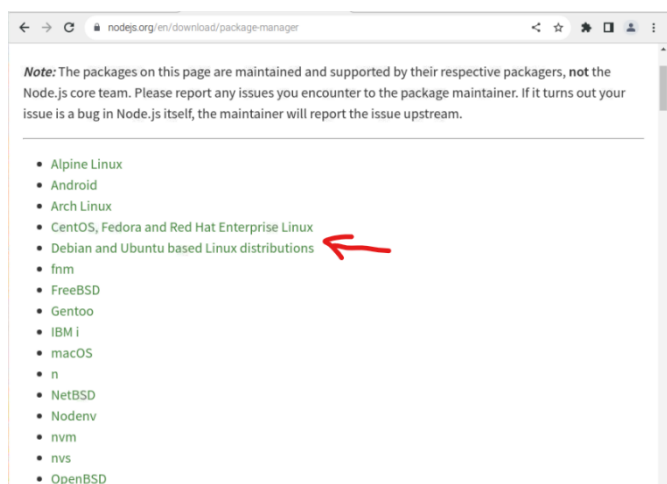
1. Installation de Node.js

Afin de réaliser notre propre interface Web qui nous permet de faire des tests d'intrusion a distance et attaquer des réseaux, on commence par faire une mise a jour de nos paquets qui sont déjà installé sur la carte.

```
pi@raspberrypi:~$ sudo apt update
Get:1 http://raspbian.raspberrypi.org/raspbian bullseye InRelease [15.0 kB]
Get:2 http://archive.raspberrypi.org/debian bullseye InRelease [23.6 kB]
Hit:3 http://download.zerotier.com/debian/bullseye bullseye InRelease
Get:4 http://raspbian.raspberrypi.org/raspbian bullseye/main armhf Packages [13.2 MB]
Get:5 http://archive.raspberrypi.org/debian bullseye/main armhf Packages [316 kB]
Fetched 13.6 MB in 38s (354 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
116 packages can be upgraded. Run 'apt list --upgradable' to see them.
pi@raspberrypi:~$
```

Ensuite on passe à l'installation de notre environnement d'exécution côté serveur qui est Node.js, ce dernier est basé sur le moteur JavaScript V8 de Google. Il permet d'exécuter du code JavaScript en dehors du navigateur, ce qui signifie que nous pouvons utiliser JavaScript pour créer des applications et des serveurs côté serveur.

Pour installer le package on visite le site officiel de nodejs.org ou on peut trouver les fichiers nécessaires pour l'installation de Node.js sur Debian.



Node.js v18.x:

Using Ubuntu

```
curl -fsSL https://deb.nodesource.com/setup_18.x | sudo -E bash -
sudo apt-get install -y nodejs
```

Using Debian, as root

```
curl -fsSL https://deb.nodesource.com/setup_18.x | bash - &&\
apt-get install -y nodejs
```


On lance la commande d'installation sur notre système.

```
root@raspberrypi:/home/pi# curl -fsSL https://deb.nodesource.com/setup_18.x | bash - &&\napt-get install -y nodejs\n\n## Installing the NodeSource Node.js 18.x repo...\n\n## Populating apt-get cache...\n\n+ apt-get update\nHit:1 http://raspbrian.raspberrypi.org/raspbian bullseye InRelease\nHit:2 http://archive.raspberrypi.org/debian bullseye InRelease\nHit:3 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid InRelease\nHit:4 http://download.zerotier.com/debian/bullseye bullseye InRelease\nReading package lists... Done\n\n## Confirming "bullseye" is supported...\n\n+ curl -sLf -o /dev/null 'https://deb.nodesource.com/node_18.x/dists/bullseye/Release'\n\n## Adding the NodeSource signing key to your keyring...\n\n+ curl -s https://deb.nodesource.com/gpgkey/nodesource.gpg.key | gpg --dearmor | tee /usr/share/keyrin
```

Et voici Node.js est installé avec succès.

```
root@raspberrypi:/home/pi# sudo node --version\nv18.16.0\nroot@raspberrypi:/home/pi# sudo npm --version\n9.5.1\nroot@raspberrypi:/home/pi# █
```

2. Installation de nmap

Nmap (Network Mapper) est un outil de sécurité informatique très populaire utilisé pour l'exploration de réseau et l'audit de sécurité. Il permet de scanner et d'analyser les hôtes, les ports ouverts, les services en cours d'exécution, les systèmes d'exploitation, les vulnérabilités et d'autres informations pertinentes sur un réseau. Nmap utilise des techniques de balayage avancées pour détecter et cartographier les ressources réseau, ce qui en fait un outil précieux pour les professionnels de la sécurité, les administrateurs système et les testeurs d'intrusion. Il peut être utilisé en ligne de commande ou avec une interface graphique. Nmap est open source et multiplateforme, disponible pour Windows, macOS, Linux et d'autres systèmes d'exploitation.

Pour l'installer on tape la commande suivante :

```
pi@raspberrypi:~ $ sudo apt install nmap\nReading package lists... Done\nBuilding dependency tree... Done\nReading state information... Done\nnmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2).\n0 upgraded, 0 newly installed, 0 to remove and 116 not upgraded.\npi@raspberrypi:~ $
```

3. Installation de msfconsole

Metasploit est un Framework de test de pénétration et d'exploitation largement utilisé dans le domaine de la sécurité informatique. Il fournit un ensemble d'outils, de modules et d'exploits prêts à l'emploi pour effectuer des tests d'intrusion, évaluer la sécurité des systèmes et des applications, et développer des contre-mesures.

Voici quelques points clés à retenir sur Metasploit :

1. Exploitation de vulnérabilités : Metasploit permet d'exploiter des vulnérabilités connues dans les systèmes cibles. Il fournit une large gamme d'exploits et de payloads (charge utile) pour exploiter des failles spécifiques dans différents services, applications ou systèmes d'exploitation.

2. Test de pénétration : Metasploit permet d'effectuer des tests de pénétration sur des infrastructures réseau, des systèmes et des applications. Il permet de simuler des attaques réelles pour identifier les failles de sécurité et évaluer la robustesse d'un système face à des attaques potentielles.

3. Modules et plug-ins : Metasploit dispose d'une vaste bibliothèque de modules et de plug-ins qui peuvent être utilisés pour effectuer des tâches spécifiques, tels que la découverte de réseau, l'analyse de vulnérabilités, le sniffing de paquets, la collecte d'informations, etc.

4. Facilité d'utilisation : Metasploit propose une interface en ligne de commande (msfconsole) et une interface graphique (Armitage) pour faciliter l'utilisation et la gestion des exploits. Il offre également des fonctionnalités de scripting pour automatiser les tâches et les scénarios d'attaque.

5. Intégration avec d'autres outils : Metasploit peut être intégré à d'autres outils de sécurité et de test d'intrusion, ce qui permet d'étendre ses fonctionnalités et d'améliorer la productivité des professionnels de la sécurité. Par exemple, il peut être utilisé en conjonction avec Nmap pour la découverte de réseau et l'identification de cibles potentielles.

6. Base de données de vulnérabilités : Metasploit dispose d'une base de données de vulnérabilités qui est constamment mise à jour avec de nouvelles failles de sécurité. Cela

permet aux utilisateurs de rechercher, d'importer et d'exploiter des vulnérabilités connues dans leurs tests de pénétration.

Il est important de noter que Metasploit doit être utilisé avec une autorisation appropriée et dans un cadre légal, de préférence avec le consentement du propriétaire du système ou de l'application testée. Il est conçu pour être utilisé par des professionnels de la sécurité qualifiés et éthiques dans le but d'améliorer la sécurité des systèmes et des réseaux.

L'installation de Metasploit se fait de la façon suivante :

```
pi@raspberrypi:~$ curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall
% Total    % Received % Xferd  Average Speed   Time    Time     Current
           Dload  Upload  Total   Spent    Left     Speed
100 6034 100 6034  0     0 14435    0 --:--:-- --:--:-- --:--:-- 14435
Switching to root user to update the package
Adding metasploit-framework to your repository list..Warning: apt-key is deprecated. Manage keyring files in trusted.gpg
.d instead (see apt-key(8)).
OK
Updating package cache..OK
Checking for and installing update..
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  metasploit-framework
0 upgraded, 1 newly installed, 0 to remove and 116 not upgraded.
Need to get 297 MB of archives.
```

Et voici l'interface que Metasploit génère en lançant la commande « msfconsole » :

```
pi@raspberrypi:~$ msfconsole

** Welcome to Metasploit Framework Initial Setup **
Please answer a few questions to get started.

Would you like to use and setup a new database (recommended)? yes
Clearing http web data service credentials in msfconsole

Running the 'init' command for the database:
Creating database at /home/pi/.msf4/db
Creating db socket file at /tmp
Starting database at /home/pi/.msf4/db...success
Creating database users
Writing client authentication configuration file /home/pi/.msf4/db/pg_hba.conf
Stopping database at /home/pi/.msf4/db
Starting database at /home/pi/.msf4/db...success
Creating initial database schema
Database initialization successful

** Metasploit Framework Initial Setup Complete **

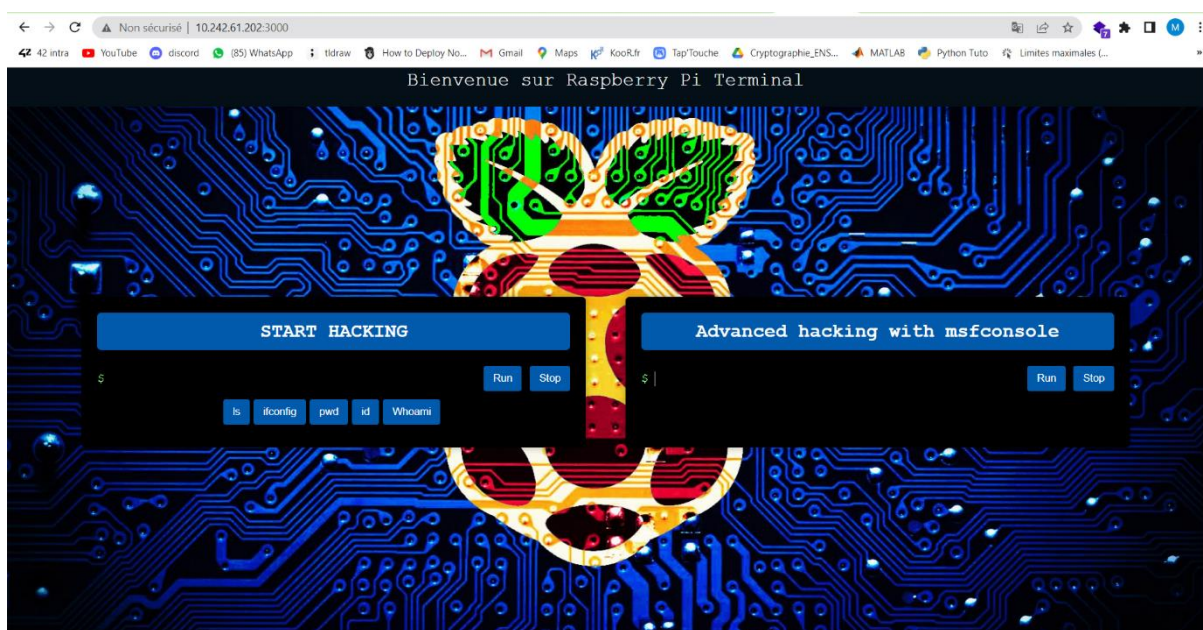

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMM                      MMMMMMMMMMMMMMMM
MMMN$                                vMMMMM
MMMMNl    MMMMM                    MMMMM   JMMMMM
MMMMNl    MMMMMMMM                NMMMMMMMMM JMMMMM
MMMMNl    MMMMMMMMMMMMmmmmMMMMMMMMMMMMMM JMMMMM
```

II. Présentation de l'interface web

L'interface web est conçu pour donner une expérience utilisateurs très satisfaisante. Elle permet à l'utilisateur d'interagir avec le raspberry puis d'exécuter des commandes basiques d'une part, puis des commandes plus avancées en utilisant msfconsole. Sur l'interface, on trouve une partie où on peut insérer des commandes puis les envoyer au serveur et récupérer les résultats. Aussi il y a des commandes prédéfinis et l'utilisateur a juste à cliquer sur un bouton pour les exécuter automatiquement.

Ensuite il y a une partie conçue pour exécuter les commandes de msfconsole afin de lancer des exploits sur les machines vulnérables qu'on aura trouvées sur le réseau.

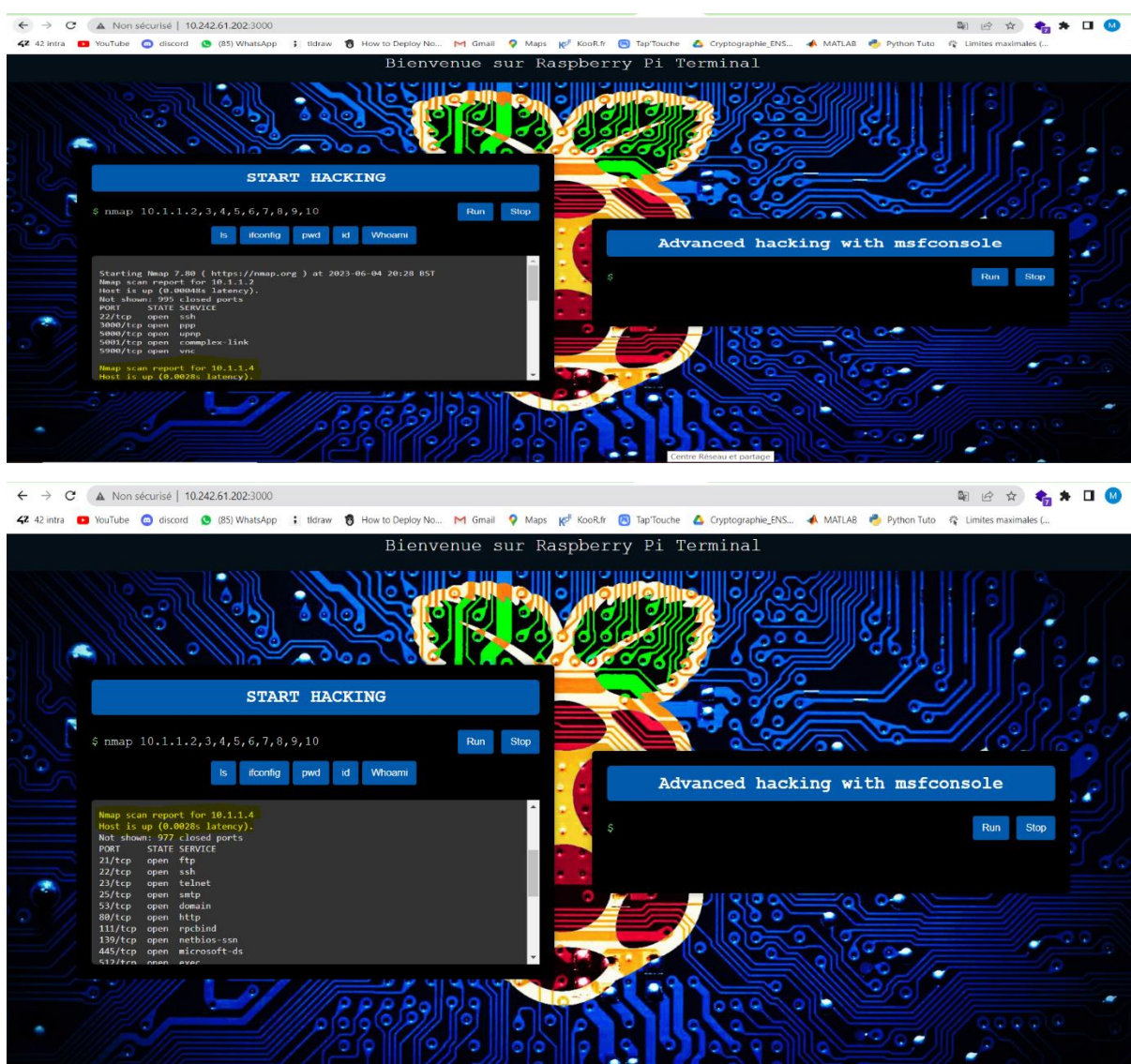
Voici une capture de l'interface web :



III. Simulation d'une attaque complète avec l'interface web

Maintenant nous allons simuler une attaque d'une machine qui se trouve dans le même réseau que le raspberry. Nous attaquerons cette machine qu'on n'a pas normalement accès grâce au raspberry en passant par le VPN.

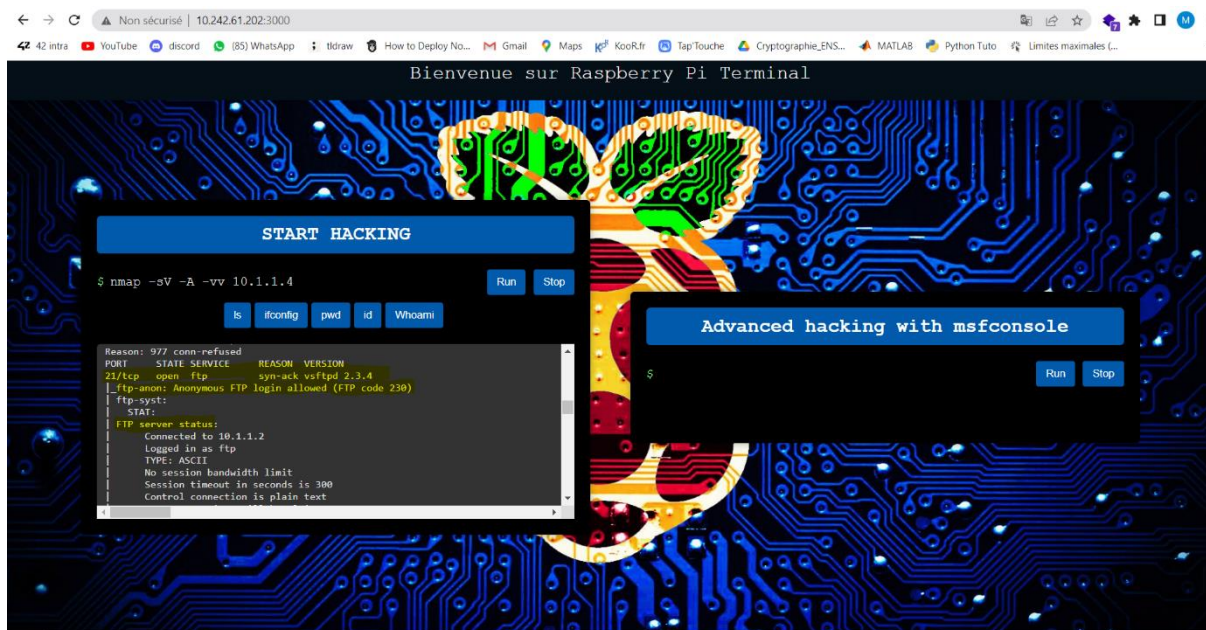
Tout d'abord vérifions les machine active et vulnérable (ici on va juste tester la plage d'adresse de 1 à 10 pour ne pas perdre beaucoup de temps) :



Chapitre3 :Implémentation de l'interface web et tests d'intrusion

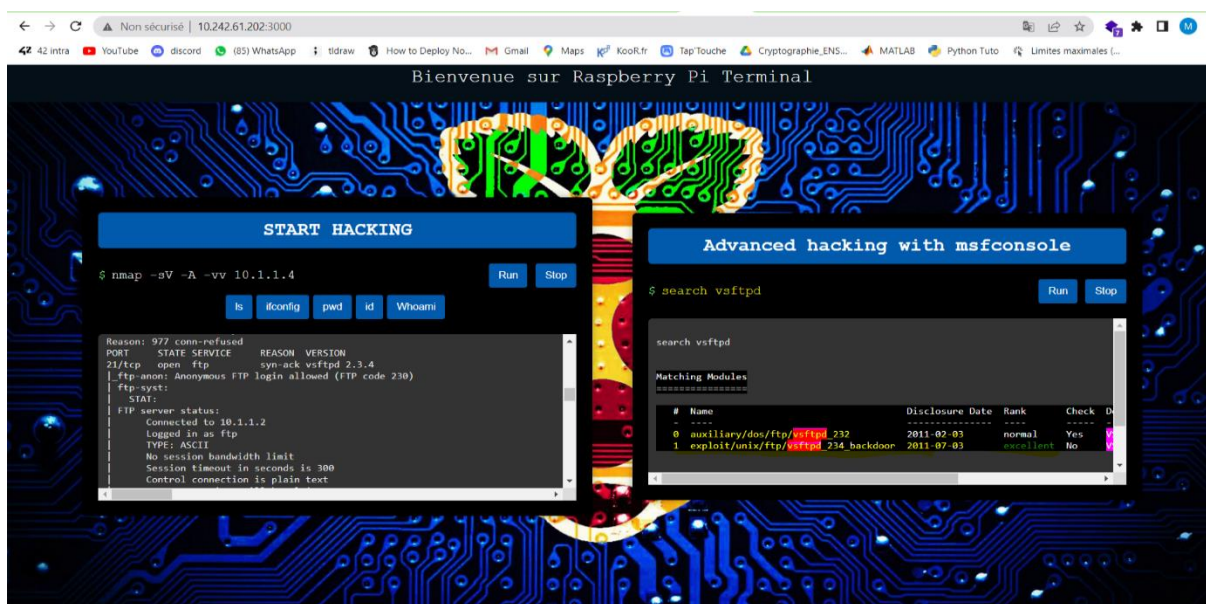
Comme on peut le voir, on 2 machines actives le 10.1.1.2 et le 10.1.1.4 et comme notre raspberry est le 10.1.1.2 nous allons essayer d'attaquer le 10.1.1.4.

Tout d'abord lançons la commande `nmap -sV -vv -A 10.1.1.4` pour voir les ports, les services qui y sont les versions afin de trouver des vulnérabilités :



Comme on peut le voir le port 21 est ouvert avec FTP dessus sur la version vsftpd 2.3.4.

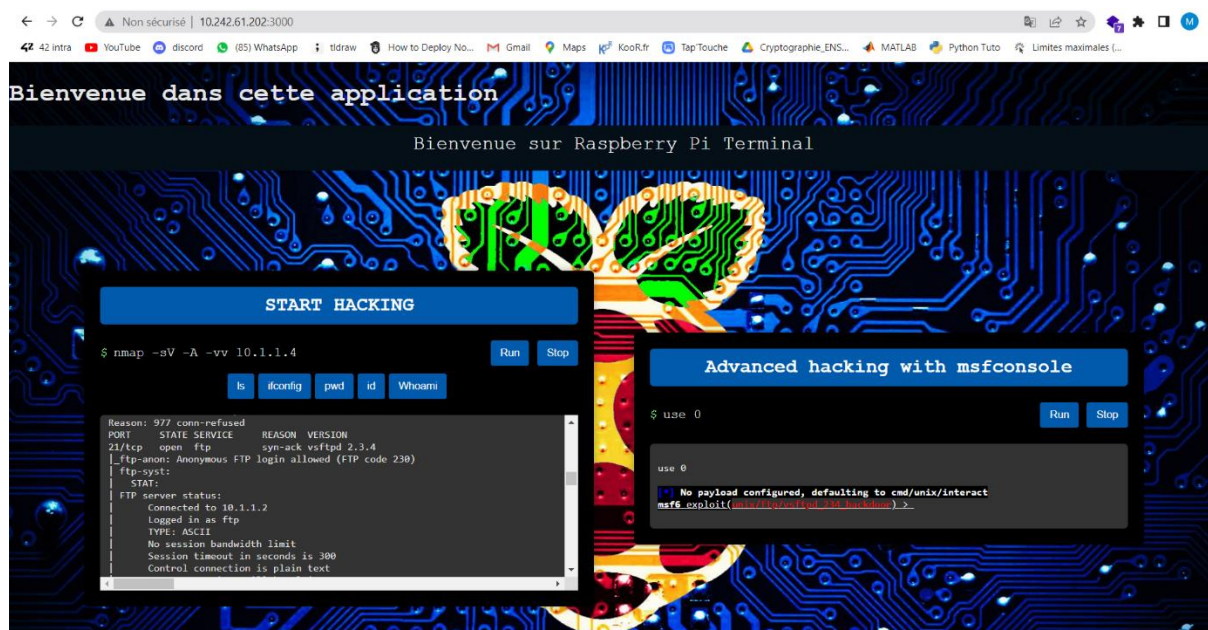
Vérifions sur msfconsole si cette version de ftp est exploitable avec la commande `search vsftpd 2.3.4` :



Chapitre3 : Implémentation de l'interface web et tests d'intrusion

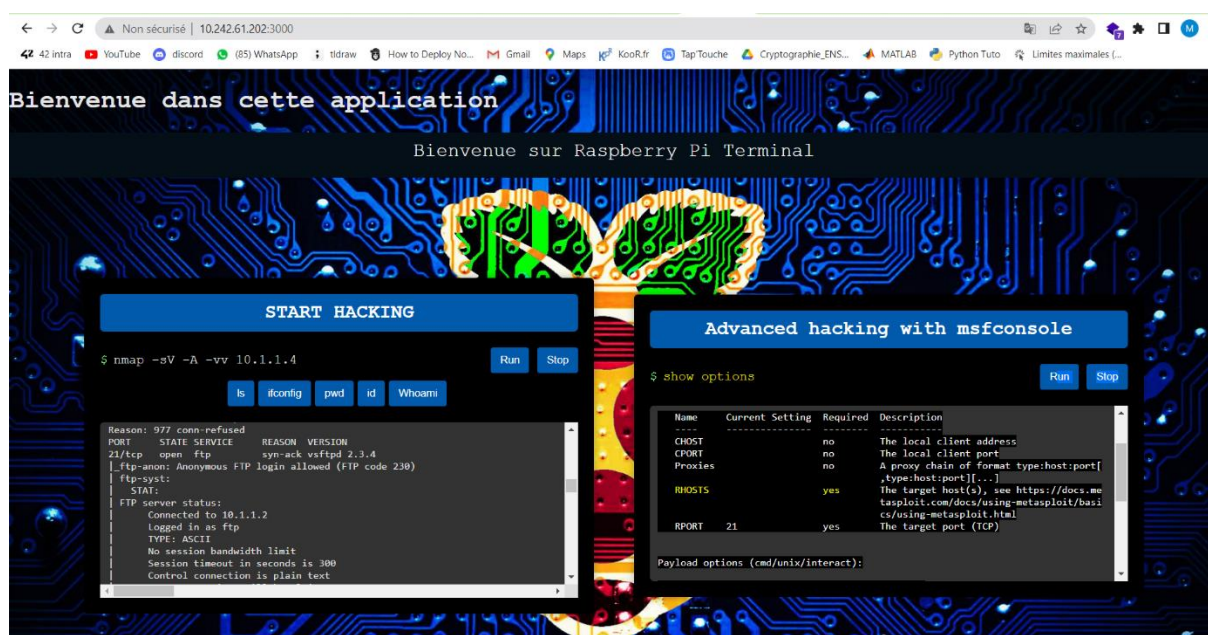
Comme on peut le voir il existe deux exploits possible de la version vsftpd 2.3.4. Nous allons exploiter cette vulnérabilité.

Lançons la commande use 0 pour load l'exploit sur msfconsole :



Maintenant que l'exploit est chargé, on va voir les options possibles.

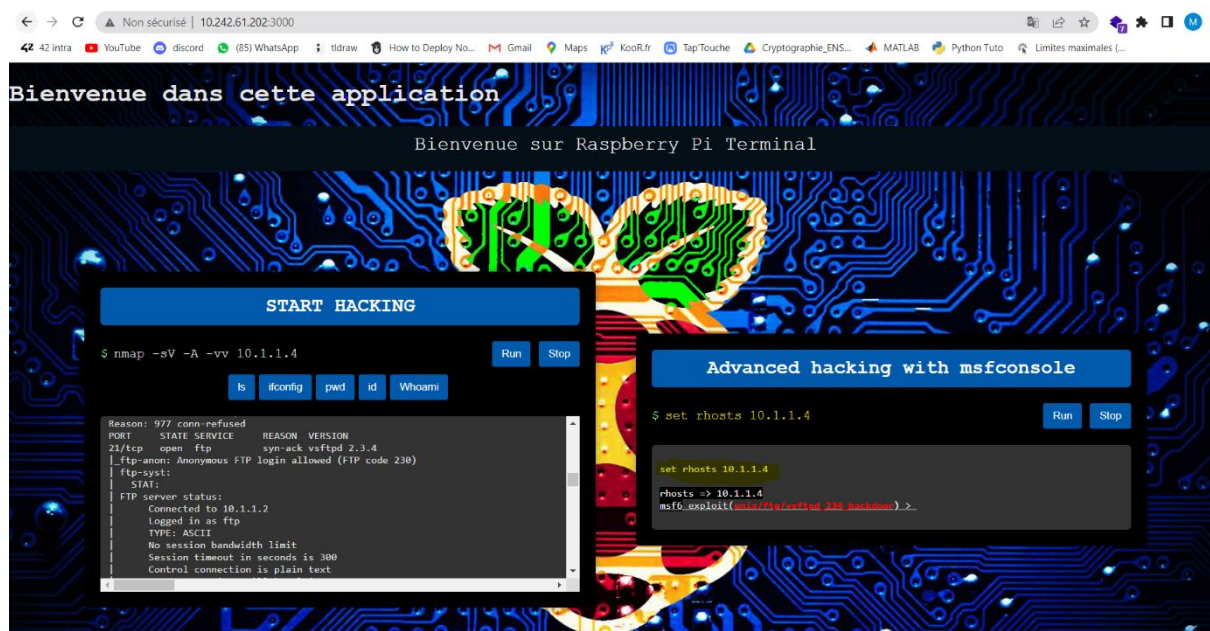
Lançons show options pour voir les options :



Comme on le voit, l'option rhosts est obligatoire. Ici notre RHOSTS est 10.1.1.4.

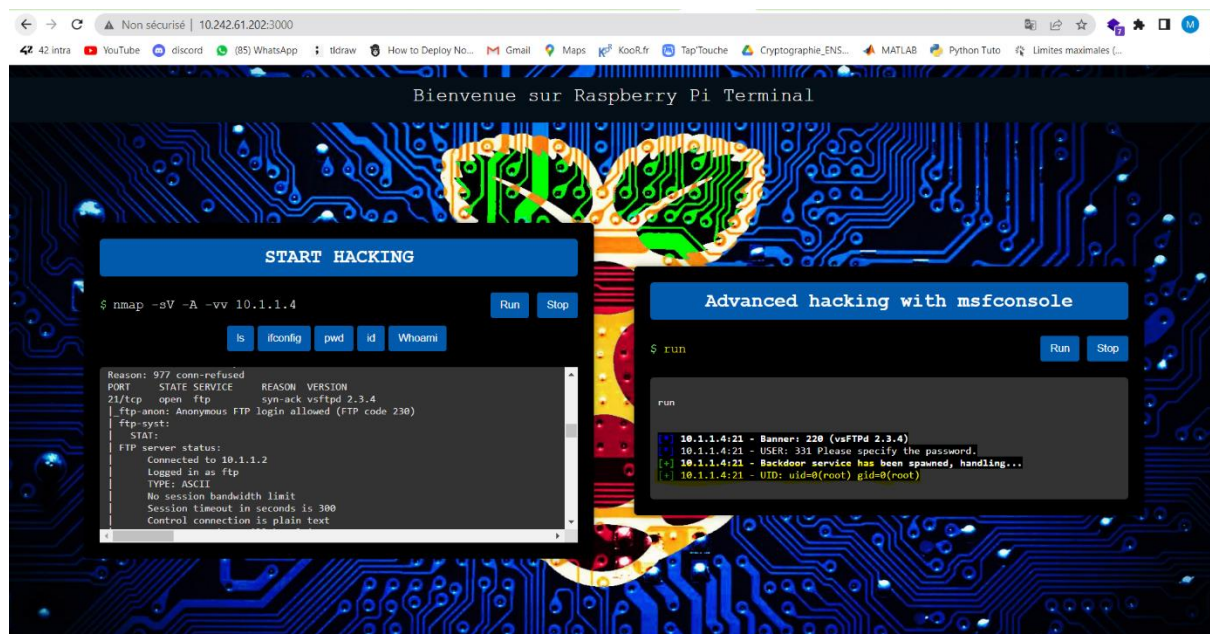
Chapitre3 :Implémentation de l'interface web et tests d'intrusion

Donner cette option à l'exploit avec la commande set rhosts 10.1.1.4 :



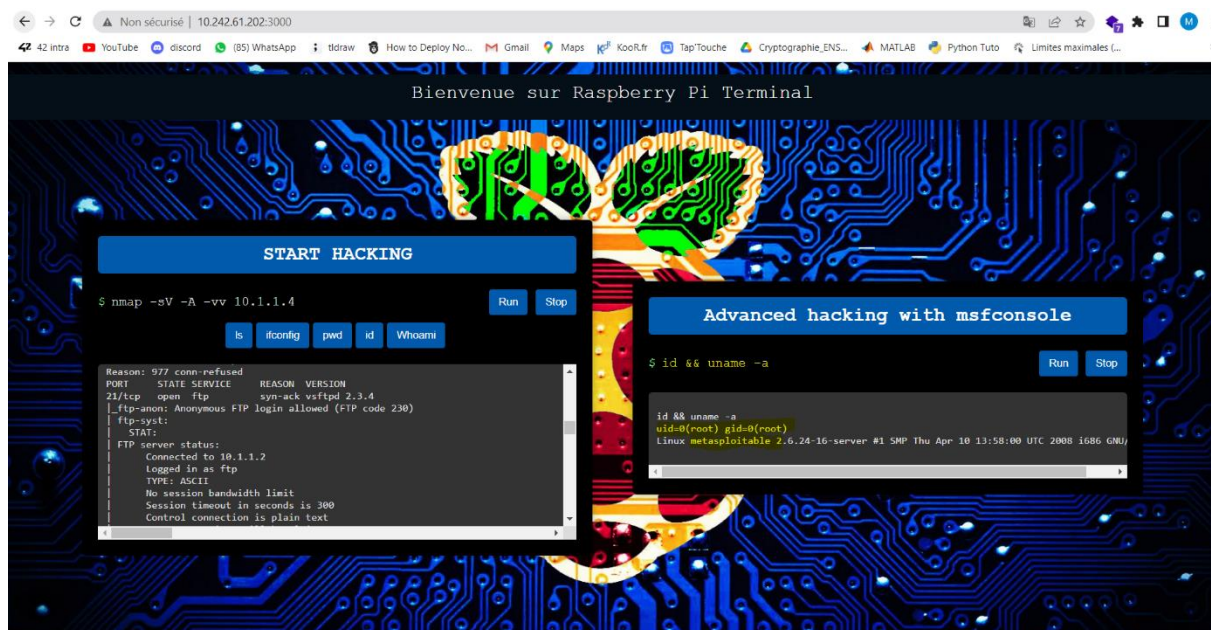
Maintenant l'exploit est prêt.

Lançons la commande run ou exploit pour essayer d'avoir un shell sur notre site :



On a eu un shell avec comme user le root ce qui montre qu'on a réussi à prendre le contrôle total de la machine depuis notre navigateur web.

Lançons la commande id puis uname -a pour vérifier qu'on est bien root et que c'est bien la machine metasploitable :



On est bien root et sur la machine mésploitable. Ce montre la puissance de notre plateforme web.

Ceci marque la fin de notre simulation d'attaque.

Conclusion

En conclusion, ce projet a permis de développer une interface web innovante qui offre une expérience utilisateur conviviale et pratique pour l'exécution de commandes à distance sur un Raspberry Pi, ainsi que pour l'utilisation de exploits via MSFConsole. L'objectif principal de cette application était de faciliter les attaques à distance sur des cibles spécifiques.

Grâce à cette interface web, il est possible d'accéder à un shell distant, offrant une flexibilité et une mobilité accrues. L'utilisateur peut ainsi exécuter des commandes à distance sur son Raspberry Pi, ce qui lui permet de gérer et de contrôler son appareil depuis n'importe quel endroit disposant d'une connexion Internet. Cette fonctionnalité s'avère particulièrement utile dans des scénarios où l'accès physique au Raspberry Pi est limité ou impossible.

De plus, l'intégration de MSFConsole dans l'interface web offre des possibilités d'exploitation avancées. Les utilisateurs peuvent tirer parti de la puissance de Metasploit Framework pour mener des attaques ciblées, tester la sécurité des systèmes, et effectuer des évaluations de vulnérabilités. Cette fonctionnalité est particulièrement pertinente pour les professionnels de la sécurité, les chercheurs en sécurité et les pentesteurs.

Cependant, il est essentiel de noter que l'utilisation de cette application à des fins malveillantes est illégale et fortement déconseillée. Ce projet vise à des fins éducatives et de recherche dans le domaine de la sécurité informatique. Il est primordial de respecter les lois et règlements en vigueur ainsi que d'obtenir l'autorisation appropriée avant de mener des tests de pénétration ou des attaques.

En conclusion, cette interface web avec un shell distant et l'intégration de MSFConsole représente un outil puissant pour la gestion à distance du Raspberry Pi et l'exécution d'attaques ciblées. Il offre une solution pratique, accessible et sécurisée pour les passionnés de Raspberry Pi et les professionnels de la sécurité cherchant à améliorer leurs compétences et à approfondir leurs connaissances dans le domaine de la sécurité informatique.