Une image contenant texte

Description générée automatiquement

420-CFS-TT

CONCEPTION DE RÉSEAUX SANS FIL

Lab 3

Réaliser une attaque par DNS Spoofing

12 juin 2024

30 points

Nom:

* **NGANSOP NJANOU ULRICH SOSTAIRE**
* **Liberal Rose Tarline**
* **Bossambe Kong Valdez olivier**

Table des matières

[1 Introduction 3](#_Toc108553838)

[2 Matériel nécessaire 3](#_Toc108553839)

[3 Configuration du routeur sans-fil 4](#_Toc108553840)

[4 Attaque par DNS Spoofing 17](#_Toc108553841)

# Introduction

Dans ce projet vous aller apprendre à réaliser une attaque de type DNS spoofing dans le but de rediriger des utilisateurs de Facebook vers un site malicieux (qui ne l’est pas vraiment!).

# Matériel nécessaire

* Routeur sans-fil
* Station de travail
* Deux câbles réseaux RG-45

# Attaque par DNS Spoofing

L’interface web qui permet de configurer le routeur sans fil est accessible sans mot de passe.

Ceci est une vulnérabilité importante car elle donne la possibilité à n’importe quel utilisateur du réseau de se connecter à cette page et de modifier la configuration du réseau (à des fins potentiellement malicieuses).

Pour réaliser cette attaque nous allons changer la configuration DNS du routeur. Nous allons rediriger toutes les requêtes DNS vers un serveur configuré par un pirate informatique.

Ce serveur piraté retournera de fausses adresses IP pour certaine requêtes DNS faites par votre station de travail.

1. Faire un clone Alma Linux et le nommer Serveur WEB.

Installer le service Apache

Activer et démarrer le service Apache

Créer une page web index.html avec le contenu :

Ceci n’est pas Facebook !

Attention aux vols de vos identifiants !

Vérifier la configuration DNS de votre routeur !

1. Faire un clone Alma Linux et le nommer Serveur DNS.

I

nstaller le service DNS

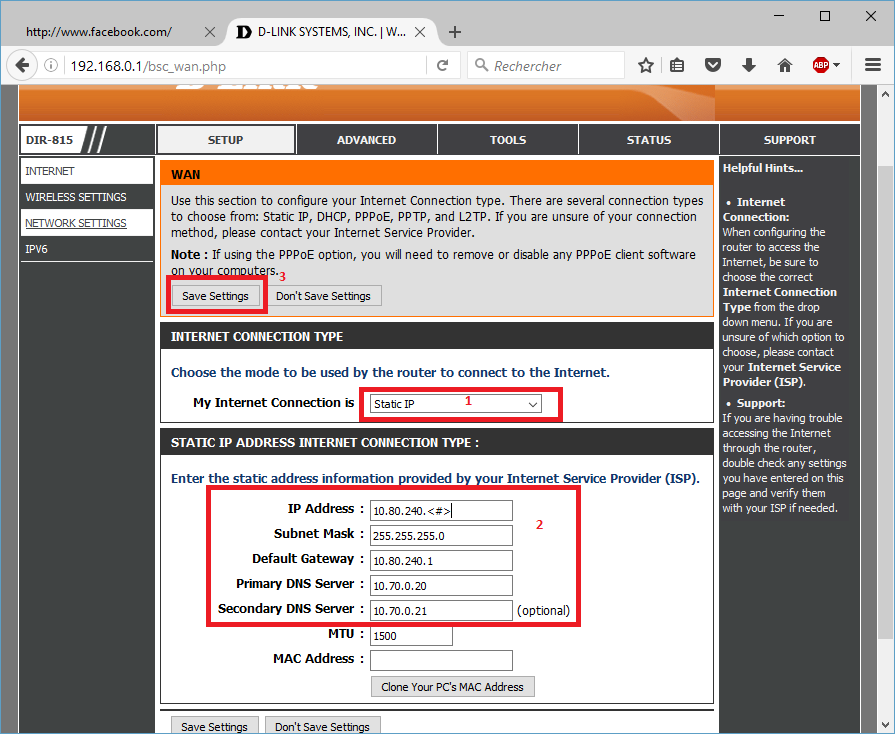
Activer et démarrer le service DNS

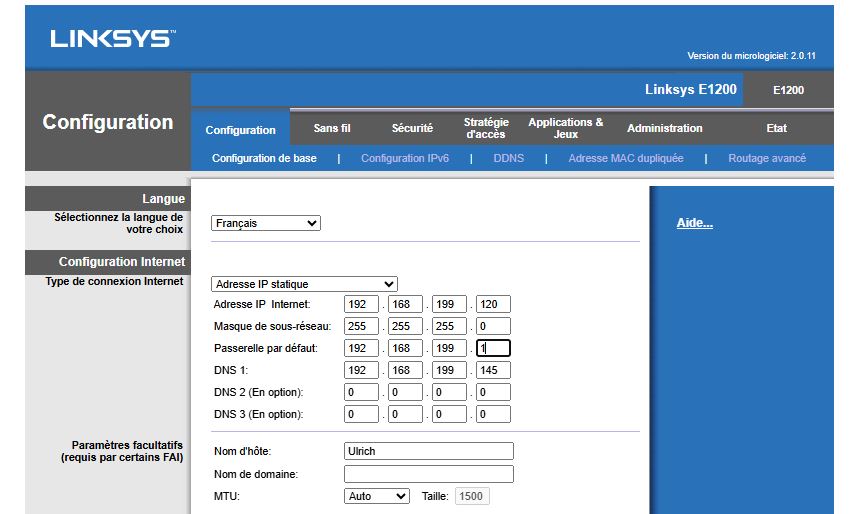
Ajouter une nouvelle zone nommée facebook.com

Ajouter un record [www.facebook.com](http://www.facebook.com) vers votre serveur web.

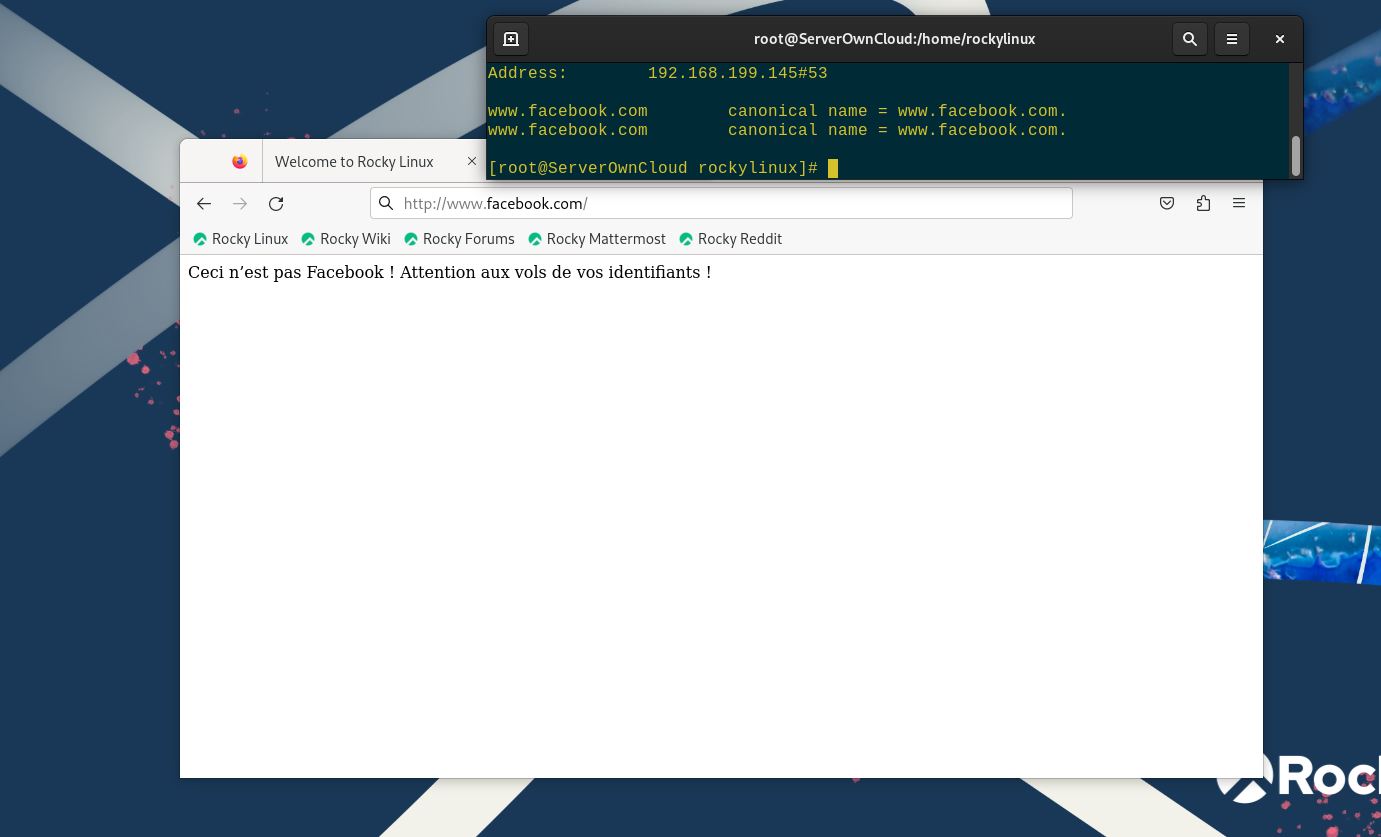
1. Modifiez la configuration IP de l’interface WAN de votre routeur sans-fil et donnez les paramètres IP suivants :

Cliquez sur **Internet** puis cliquez sur le bouton **Manual configuration**.





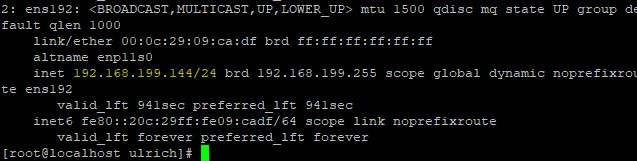
1. Débranchez le câble bleu de votre station de travail pendant 30 secondes, puis rebranchez le pour forcer une réinitialisation des paramètres IP.
2. Ouvrez maintenant Firefox et accédez à [www.facebook.com](http://www.facebook.com) . Vous devriez obtenir le résultat suivant signe que vous avez été redirigé vers un serveur qui n’est pas Facebook.

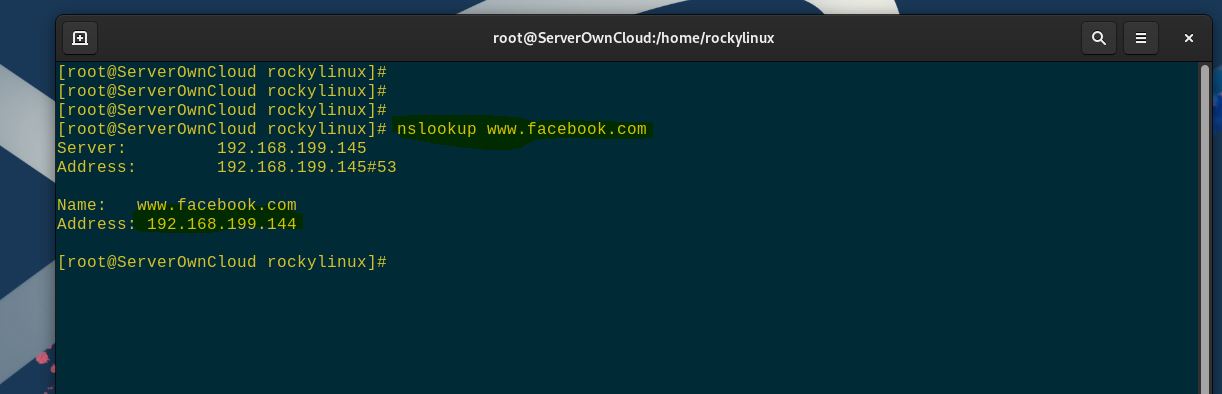


1. Décrivez cette attaque par « DNS Spoofing ».

L'objectif de cette 'attaque est de rediriger le trafic d'un site web légitime ([www.facebook.com](http://www.facebook.com)) vers un site malveillant ( Notre site crée ) sans que l'utilisateur en soit conscient. Cela permet aux attaquants ou hacker de voler des informations sensibles comme des identifiants de connexion, des numéros de carte de crédit ou autres …

1. À l’aide de la commande NSLOOKUP, demandez à votre serveur DNS quelle adresse IP correspond à [www.facebook.com](http://www.facebook.com). Lancez cette commande sur la station de travail connectée au routeur.





1. Comment auriez-vous pu prévenir cette attaque ?

**Pour prévenir cette attaque il est possible de :**

* **Configurer des ACL (Access Control Lists)** ;
* **Surveiller et analyser le trafic DNS ;**
* **Isoler les serveurs DNS ;**
* **Former le personnel ;**