

---

---

**Rabanov**  
**Protection contre DHCP Starvation**  
**Version <1.0>**

HOTEL

RABANOV



**Protection contre DHCP Starvation**

<b>Rabanov</b>	Version: <1.0>
Protection contre DHCP starvation	Date: 25/04/2016

## Historique des révisions

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Auteur</b>
25/04/2016	<1.0>	Rédaction des configurations	Brice Harismendy

<b>Rabanov</b>	Version: <1.0>
Protection contre DHCP starvation	Date: 25/04/2016

## Table des matières

- 1. Introduction
  - 1.1 Contexte du projet
  - 1.2 Objectifs du document
  - 1.3 Portée
  - 1.4 Définitions, Acronymes et Abréviations
- 2. Éléments de configuration
  - 2.1 Tentative d'attaque
  - 2.2 Sécurisation
- 3. Conclusion

<b>Rabanov</b>	Version: <1.0>
Protection contre DHCP starvation	Date: 25/04/2016

# Configuration du Switch

## 1. Introduction

L'hotel Rabanov vient d'être construit et l'administrateur système et réseau veut protéger son DHCP contre une attaque connue appelée DHCP Starvation qui peut amener un serveur DHCP a ne plus émettre d'adresse (pool remplie).

### 1.1 Contexte du projet

Un groupe Hotelier international a lancé sur la cote vendéenne la construction d'un nouvel hotel 4 étoile de luxe « Le Rabanov »

### 1.2 Objectifs du document

Ce document a pour objectif de permettre la reconfiguration rapide de la protection anti DHCP Starvation de l'hotel

### 1.3 Portée

Cette documentation s'adresse a l'équipe technique de l'hotel Rabanov

### 1.4 Définitions, Acronymes et Abréviations

DHCP : Dynamic Host Configuration Protocol

## 2. Éléments de configuration

### 2.1 Tentative d'attaque

Nous allons commencer par vérifier la vulnérabilité de notre réseau, pour cela il faut utiliser la bibliothèque scapy sous kali-linux:

pour commencer entrez cette commande : `conf.checkIpAddr = False`

on construit le paquet a présent :

```
tramedhcp = Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/
IP(src="0.0.0.0",dst="255.255.255.255")/UDP(sport=68,dport=67)/BOOTP(chaddr=R
andString(12, '0123456789abcdef'))/DHCP(options=[("message-
type","discover"),"end"])
```

puis on l'envoi :

```
sendp (tramedhcp, loop=1)
```

les effets sur le réseau :

cette attaque fait une découverte des DHCP en boucle avec une adresse mac aléatoire ce qui donne ceci

<b>Rabanov</b>	Version: <1.0>
Protection contre DHCP starvation	Date: 25/04/2016

sur les statistique du serveur :

Statistiques du serveur ws2012.lerabanov-hotel.local	
Description	Détails
Heure de début	25/04/2016 12:00:50
Durée de fonctionnement	70 heures 6 minutes, 50 secondes
Découvertes	27994
Offres	34
Offres retardées	0
Demandes	13
Accusés de réception	28
Accusés de réception négatifs	2
Refus	0
Libérations	1
Nombre total d'étendues	2
Étendues pour lesquelles un retard est configuré	0
Nombre total d'adresses	54
- Utilisées	29 (53%)
- Disponibles	25 (46%)

ce grand nombre de découverte est problématique, en effet chaque découverte entraine la réservation d'une ip ce qui fait que si un utilisateur légitime tente de se connecter toutes les ip sont déjà réservé, message d'erreur en cas d'ipconfig /renew :

```

Carte Tunnel isatap.rabanov.local :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.lerabanov-hotel.local :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\Administrateur>ipconfig /renew

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion au réseau local 2 lorsque
son média est déconnecté.
Une erreur s'est produite lors du renouvellement de l'interface Connexion au rés
eau local :
Impossible de contacter votre serveur DHCP.
Le délai d'attente de la demande a expiré.
Une erreur s'est produite lors de la libération de l'interface Loopback Pseudo-I
nterface 1 : Le fichier spécifié est introuvable.

C:\Users\Administrateur>_

```

On voit ici que la demande de bail DHCP n'aboutit pas car le seul DHCP en place n'a plus d'adresse IP à distribuer

## 2.2 Sécurisation

Sur tout les ports on veut une adresse IP par adresse MAC (une ip par appareil)  
sur le switch on fait les commandes suivantes :

```
Switch_Rabanov01#conf t
```


```
Switch_Rabanov01(config)#int range fa0/1-24
```

```
Switch_Rabanov01(config-if-range)#switchport port-security maximum 1→1 pour une ip par mac
```

```
Switch_Rabanov01(config-if-range)#end
```

<b>Rabanov</b>	Version: <1.0>
Protection contre DHCP starvation	Date: 25/04/2016

quand on relance l'attaque les ip sont affecté aux hôtes alors que le serveur reçoit pleins de discover

 192.168.125.99      android-f043cdfea1...    29/04/2016 02:18:58      DHCP      c43abeb5...

notre DHCP est maintenant totalement sécurisé.

### 3. Conclusion

Notre switch est maintenant sécuriser contre les attaques DHCP starvation