Rabanov Protection contre DHCP Starvation Version <1.0>

HOTEL RABANOV



Protection contre DHCP Starvation

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

Historique des révisions

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

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

Table des matières

- 1. Introduction

 - 1.1 Contexte du projet1.2 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

Rabanov	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 veux protéger son DHCP contre une attaque connue appelée DHCP Starvation qui peut amener un serveur DHCP a ne plus émettre d'addresse (pool remplie).

1.1 Contexte du projet

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

1.2 Objectifs du document

Ce document a pour objectif de permettre la reconfigurzation 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 :

```
\label{tramedhcp} $$\operatorname{Ether}(\operatorname{src=RandMAC}(),\operatorname{dst="ff:ff:ff:ff:ff:ff:})/\operatorname{IP}(\operatorname{src="0.0.0.0"},\operatorname{dst="255.255.255.255"})/\operatorname{UDP}(\operatorname{sport=68},\operatorname{dport=67})/\operatorname{B00TP}(\operatorname{chaddr=RandString}(12,'0123456789abcdef'))/\operatorname{DHCP}(\operatorname{options=[("message-type","discover"),"end"])}
```

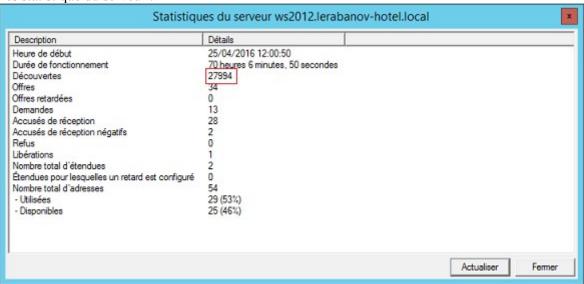
```
puis on l'envoi :
sendp (tramedhcp,loop=1)
```

les effets sur le réseau :

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

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

sur les statistique du serveur :



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

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 addresse IP par addresse 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

Rabanov	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 reçois 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