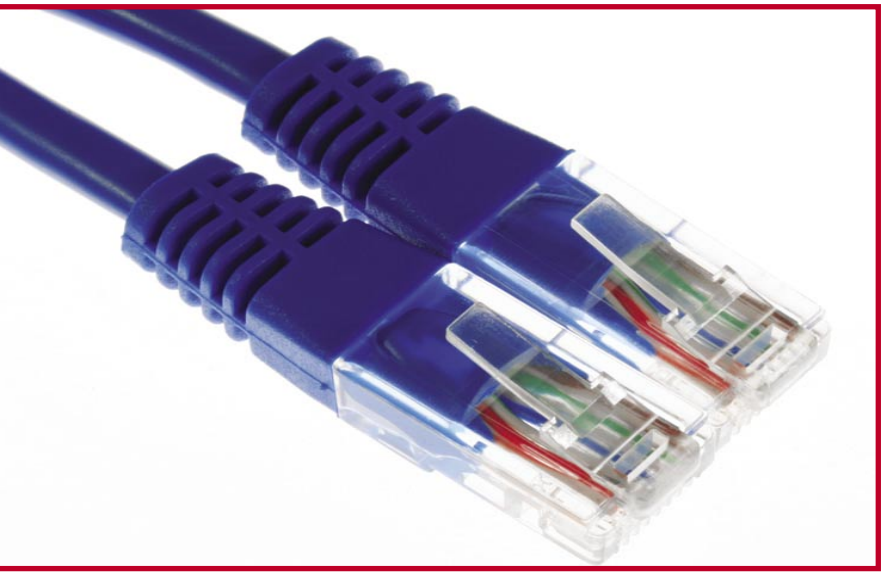
La sécurisation des points d'accès au réseau

Cédric Baillet



Les technologies de l'information sont aujourd'hui en plein BOUM. Tous la presse traitant des TIC parle désormais de convergence. Ce phénomène recoupe de nombreux items, mais pourra être schématisé rapidement en disant que l'on fait converger de nombreux services au sein d'un seul réseau et d'un minimum de périphériques utilisateurs.

Une bonne illustration pourrait être l'apparition de produits destinés à fournir un service de web conférence. Sous ce nom, les fonctionnalités de messagerie instantanée de conférences audio et vidéo, ou encore de partage de document se retrouveront sur le poste utilisateur fusionné au sein d'une seule interface.

Quel rapport avec le sujet de cet article ? Le réseau. Celui-ci est désormais mutualisé pour l'ensemble des applications et porte de plus en plus de services. Il est devenu un élément central du bon fonctionnement de l'entreprise. Il s'agit désormais d'un vecteur d'informations qu'il faut protéger pour éviter toute coupure de service, mais aussi d'un moyen permettant d'apporter de la sécurité de façon homogène à tous les utilisateurs de l'entreprise au travers de fonctions embarquées ou de périphériques spécialisés sur certains domaines comme les IPS.

S'il est certain que l'utilisation de périphériques spécialisés dans la sécurité a un coût important que tous ne peuvent se permettre, l'exploitation de l'ensemble des fonctions améliorant la sécurité contenues nativement sur les routeurs ou commutateurs est accessible dès l'achat. C'est donc un excellent moyen de diminuer un nombre important de risques tout en se plaçant au plus près de l'utilisateur (le port réseau auquel tout machine est connectée).

Nous vous proposons donc de regarder dans cet article comment sécuriser un périmètre utilisateur classique mettant en œuvre des protocoles couramment usités.

Les thématiques abordées dans cet article se retrouveront au sein du module SNRS du CCSP.

Cet article explique...

- Les différentes attaques utilisables pour détourner un point d'accès au réseau de ses fonctions initiales.
- Les contre mesures existantes pour s'en protéger.

Ce qu'il faut savoir...

- Connaître les commandes de base et le fonctionnement d'un IOS CISCO.
- Connaissance réseau Ethernet TCP/IP.

Les éléments de sécurisation du niveau 2

Le protocole DHCP (*Dynamic Host Configuration Protocol*) est un protocole LAN utilisé couramment dans la plupart des installations réseaux et devenu aujourd'hui un véritable standard. Grâce à lui, les imprimantes, ordinateurs ou téléphones IP peuvent acquérir dynamiquement une adresse IP sans intervention humaine systématique.

Ce protocole a été défini dans les RFC 2131 et 2132 et possède désormais de nombreuses extensions au travers de différentes RFC. On pourra se reporter au site web *http://www.dhcp.org/rfcs.html* pour en prendre connaissance.

Le fonctionnement du protocole DHCP est très simple. Un client se connectant au réseau émettra une requête pour obtenir une adresse IP sous forme de broadcast (donc à destination de tous les périphériques présents sur son subnet IP). Cette dernière sera traitée par le serveur DHCP s'il est présent dans le même subnet que le client, si ce n'est pas le cas, un agent tierce (un routeur le plus souvent) la transformera en unicast (donc à destination d'une seule machine) et la transmettra au serveur DHCP. On parlera dans ce dernier cas de DHCP relay. On pourra noter au travers de cette description sommaire que nous sommes clairement dans un mode de fonctionnement *client/serveur*.

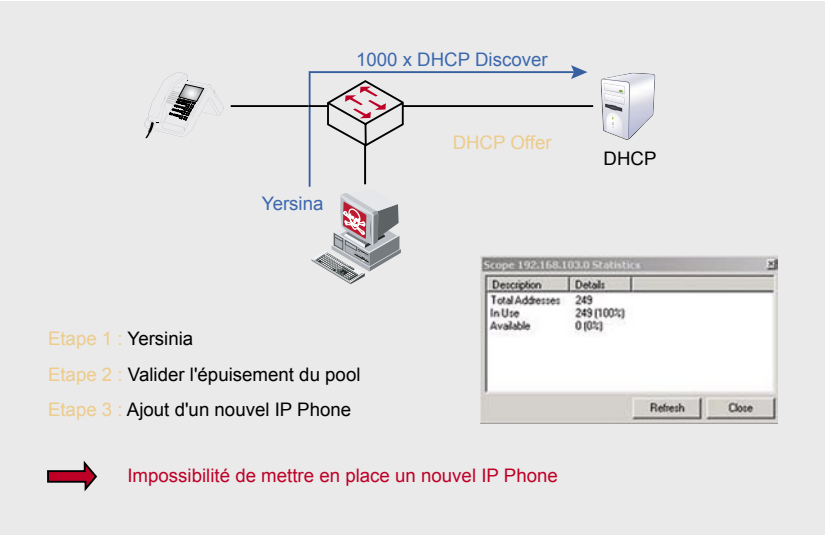
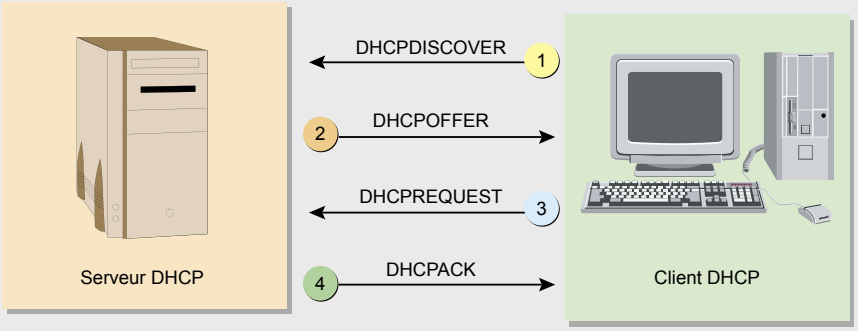


Figure 2. *Épuisement de pool DHCP*

Une fois a requête reçue, le serveur DHCP renverra une réponse au client avec une adresse IP et l'ensemble des informations nécessaires pour pouvoir communiquer sur le réseau. Il y a bien sur plusieurs échanges et confirmation pour arriver à ce résultat, mais le détail complet du protocole n'est pas le sujet de cet article.



1. Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau, du moins, en principe. Il envoie donc une trame "DHCPDISCOVER", destinée à trouver un serveur DHCP. Cette trame est un "broadcat", donc envoyé à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi sa "MAC Address".
2. Le, ou les serveurs DHCP du réseau qui vont recevoir cette trame vont se sentir concernés et répondre par un "DHCPOFFER".
   Cette trame contient une proposition de bail et la "MAC Address" du client, avec également l'adresse IP du serveur.
   Tous les DHCP répondent et le client normalement accepte la première réponse venue.
   Le "DHCPOFFER" sera un broadcast (Ethernet) ou non, suivant le serveur DHCP utillisé. Nous y reviendrons plus en détail sur l'example.
3. Le client rèpond alors par un DHCPREQUEST à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
4. Le serveur DHCP Concerné répond définitivement par un DHCPACK qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

Figure 1. *Synoptique d'échange du protocole DHCP avec un client*

Les attaques

Nous allons nous concentrer dans cette partie uniquement sur les attaques du protocole liées au réseau. Il est évident que le serveur DHCP lui même en tant que service est potentiellement faillible. Il sera donc nécessaire de suivre les règles de sécurité classiques en suivant les différentes failles publiées et en le mettant à niveau si nécessaire.

Il est désormais reconnu que le protocole DHCP est sensible essentiellement à deux grands types d'attaque:

- L'épuisement de pool DHCP,
- La mise en place d'un DHCP pirate.

L'épuisement de pool DHCP

Un serveur DHCP est constitué de différents ensemble d'adresses IP pour répondre aux requêtes de ses clients. Si l'ensemble des adresses IP de ces derniers ont déjà été attribuées, les nouveaux clients n'obtiendront pas de réponse du serveur DHCP et ne pourront utiliser le réseau. Le but d'une attaque par épuisement de pool est donc de réussir à arriver à cette situation de blocage. Il s'agit clairement d'une attaque par déni de service.

Pour arriver à ce résultat, les scripts (Yersinia, Gobbler, ...) que l'on peut trouver sur Internet génèrent des adresses MAC virtuelles et forges des paquets de type DHCP Discover qui sont envoyés sur le réseau à destination du serveur DHCP. Ces derniers répondront aux demandes des scripts jusqu'au moment ou l'ensemble des adresses IP auront été affectées (Figure 2).

L'insertion d'un serveur DHCP pirate

Le protocole DHCP fonctionne en mode concurrent. Il est ainsi possible qu'un client envoie un seul message DHCP Discover et reçoive des réponses des différents serveurs. La réponse sélectionnée par le client sera alors celle qui est arrivée le plus rapidement. Il est à noter que c'est ce mécanisme qui est utilisé pour assurer la redondance du service. Malheureusement, ce mode de fonctionnement est aussi une faiblesse du protocole. En effet, si aucun mécanisme de sécurité n'est en place, rien ne garantit que le premier serveur DHCP répondant à un client est bien un des serveurs officiels du LAN.

Cette faille pourra mener à deux grands types d'attaques :

- Un déni de service sur le réseau,
- À l'interception d'informations via un MITM (*Man In The Middle*).

Le déni de service sera réalisé en envoyant un message DHCP Offer contenant des informations réseaux sans aucun lien avec le contexte aux clients. Ces derniers auront alors paramétrés leurs cartes réseaux de façon cohérente vis à vis du protocole mais absolument pas sur le LAN. Le trafic qui sera émis à partir de ces postes ne pourra donc pas atteindre la cible espérée.

Dans le cas ou l'action souhaitée est l'interception de trafic, il sera nécessaire d'avoir pu prendre connaissance de la configuration du LAN (les informations nécessaires sont présentes sur un ordinateur dès que le serveur DHCP lui à attribué une adresse IP). Le serveur DHCP pirate sera alors configurée de manière à se positionner comme passerelle vis à vis des postes utilisateurs. Le trafic lui sera alors destinée dès qu'il faudra sortir du subnet IP et il suffira de mettre en place une redirection vers la passerelle officielle pour se rendre transparent et ne pas interrompre le service. Un simple sniffer permettra alors d'intercepter le trafic réseau.

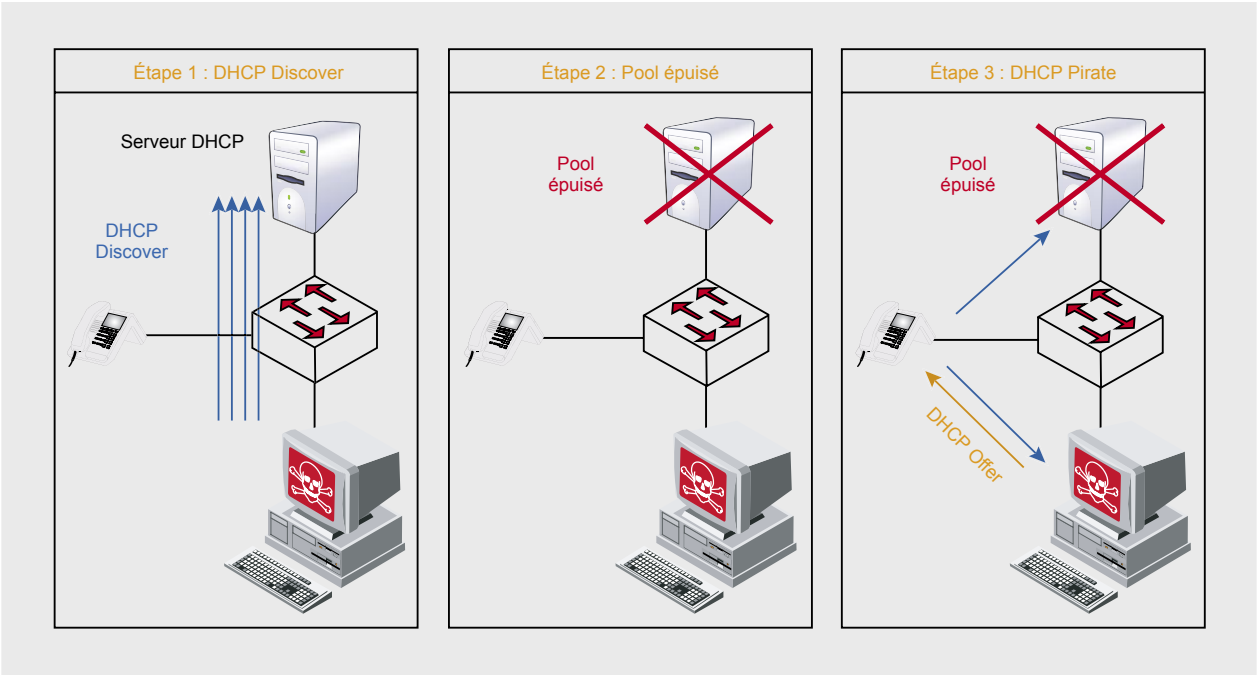


Figure 3. *Insertion d'un DHCP pirate*

En fonction de la façon dont cette attaque est exécutée, la perturbation d'un LAN pourra être partielle ou total. En effet, si l'attaque repose uniquement sur le mécanisme de concurrence entre serveurs DHCP pour que sa réponse soit acceptée, certains clients auront un paramétrage correcte et d'autres défectueux en fonction de la rapidité des réponses. Si au contraire un impact fort est souhaité, il faudra d'abord réaliser une attaque de type épuisement de pool pour ensuite inséré le serveur DHCP pirate. En effet, l'épuisement de pool sur le serveur DHCP officiel rendra celui-ci inactif sur le LAN et seules les réponses du serveur pirate pourront atteindre la cible.

Les contre mesures

La fonction *port-security.* Il existe différentes méthodes pour contrer les attaques visant à épuiser les pools d'adresses IP. Nous allons regarder ce qu'un périphérique réseau peut offrir comme possibilité, il sera néanmoins intéressant de ne pas forcément se limiter à cette seule possibilité et de regarder les fonctions d'authentification des messages existant sur certains DHCP.

La méthode la plus classique pour limiter les effets d'une attaque par épuisement de pool est de travailler sur le vecteur impactant directement le serveur DHCP, c'est à dire les DHCP Discover générés à partir d'adresses MAC virtuelles. En effet, il existe une fonction appeler *port-security* sur les commutateurs Cisco permettant de limiter le nombre d'adresses MAC que l'on peut avoir sur un port. Ainsi, en limitant le nombre d'adresses MAC à trois sur un port utilisateur, on autorisera un téléphone IP et l'ordinateur branché derrière à fonctionner correctement. Le commutateur prendra connaissance dynamiquement des adresses MAC au démarrage des périphériques et supprimera ensuite le trafic réseau ayant des adresses MAC différentes.

La fonction *port-security* des commutateurs Cisco possède un paramétrage très riche. Elle permet bien sur de paramétrer un apprentissage *dynamique* et/ou *statique* des adresses MAC (l'utilisation du mode statique dans un environnement de production n'est pas recommandé, sauf pour durcir le plus possible la sécurité, l'impact sur les équipes d'administration étant important), mais permet aussi, et surtout, de gérer la façon de réagir lorsqu'une violation des règles paramétrées survient. L'administrateur pourra ainsi choisir :

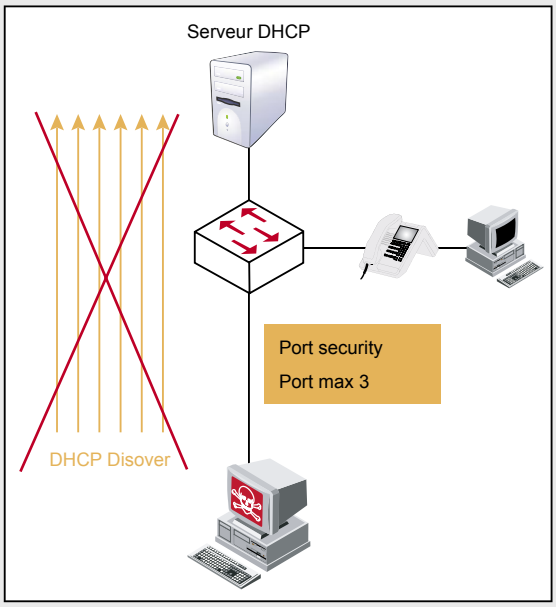
- De faire tomber le port pour un temps donné et le faire remonter sans intervention ou de le fermer définitivement,
- De paramétrer l'envoi d'une trap SNMP lors d'une violation.

Un exemple de configuration est présent dans l'encart de la Figure 4. La Figure 5 permettra de voir l'ensemble

```
6K-1-720(config)# interface g1/1
6K-1-720(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>

6K-1-720(config-if)# switchport port-security violation ?
  protect    Security violation protect mode
  restrict   Security violation restrict mode
  shutdown   Security violation shutdown mode
```

Figure 5. *La paramétrage de la commande port-security*




```
S_DEMO#sh run int g1/0/6
23:20:09: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...

Current configuration : 296 bytes
!
interface GigabitEthernet1/0/6
   switchport access vlan 2
   switchport mode access
   switchport port-security
   switchport port-security maximum 3
   switchport port-security aging time 2
   switchport port-security violation restrict
   switchport port-security  aging type inactivity
   no mdix auto
end
```

- Restriction du nombre d'adresse MAC autorisé par port.
- Configuration de comportement dynamique.
- Envoire automatique de traps.

Figure 4. *Mise en place des contre mesures visant à éviter l'épuisement de pool*

des possibilités de la commande `port-security`.

La commande `port-security` se révèle efficace pour lutter contre les attaques de type MAC flooding et donc contre une attaque d'épuisement de pool. Cependant, une forme plus évoluée existe permettant de contourner cette protection en gardant une seule adresse MAC physique sur l'en tête de niveau 2 des paquets réseaux et introduisant des adresses MAC virtuelles uniquement au niveau applicatif du paquet DHCP. Cette approche nécessitera la mise en place d'une protection complémentaire pour pouvoir être bloquée. Cette dernière se nomme *DHCP Snooping* dans le monde Cisco.

Rappelons pour conclure sur ce sujet que la famille d'attaque *MAC flooding* comprend ce que l'on appelle un *CAM Table overflow*. Il s'agit d'une attaque dédiée aux commutateurs et permettant de les faire basculer dans un mode dégradé proche du fonctionnement d'un hub, ce qui donne accès au trafic réseau puisqu'il est répliqué sur les différents ports de la machine. Le CAM flooding est réalisé en saturant la table CAM d'un commutateur (table contenant l'ensemble des adresses MAC connues par ce dernier) via l'envoi de requête ARP avec des adresses MAC virtuelles (Figure 6). La fonction port-security est donc toute indiquée pour l'éviter.

La fonction DHCP Snooping

La fonction DHCP Snooping a pour but de permettre de travailler sur le protocole DHCP au niveau applicatif et d'introduire les concepts de zone de confiance/méfiance sur un réseau donné. Elle aura donc trois grandes fonctions:

- Indiquer les zones de confiance,
- Créer une table de référence comportant les couples d'adresses MAC/IP,
- L'analyse des paquets DHCP.

La mise en place de zones de confiance se fera au travers d'un tag placé sur certains ports pour indiquer que le trafic DHCP transitant par ces derniers est légitime. Par défaut, tous les ports ne seront pas dans la zone de confiance et demanderont une intervention de l'administrateur pour basculer d'une zone à l'autre. Ce paramétrage permet d'éviter la mise en place d'un DHCP tiers inattendu, voir pirate. En effet, ce dernier ne pourra qu'être placer sur un port client n'appartenant pas à la zone de confiance et s'il pourra voir passer les requêtes DHCP qui se font en mode broadcast, toutes les réponses qu'il fera partir sur le réseau seront systématiquement supprimées au niveau du port.

Une fois que les circuits des paquets DHCP ont été sécurisés via l'établissement des zones de confiance, le DHCP Snooping permettra d'analyser les différents échanges entre le client et le serveur pour construire une table de correspondance entre les adresses MAC des clients et les adresses IP attribuées par le serveur DHCP. Cette table sera utilisée lors de l'analyse applicative des paquets puis au travers de fonctions de plus haut niveau du commutateur. On pourra se reporter à la Figure 7 pour visualiser de façon pratique la table de correspondance.

L'analyse des paquets DHCP nous apportera tout d'abord la validation de la syntaxe des messages puis la validation du contenu au travers de l'analyse applicative. Cette dernière comprendra les éléments suivants :

- 1- Les messages DHCP provenant normalement d'un serveur sont supprimés.
- 2- Les messages avec l'option 82 paramétrée sont supprimés (sauf paramétrage spécifique).
- 3- Les messages de type DHCP Release/DHCP Decline sont

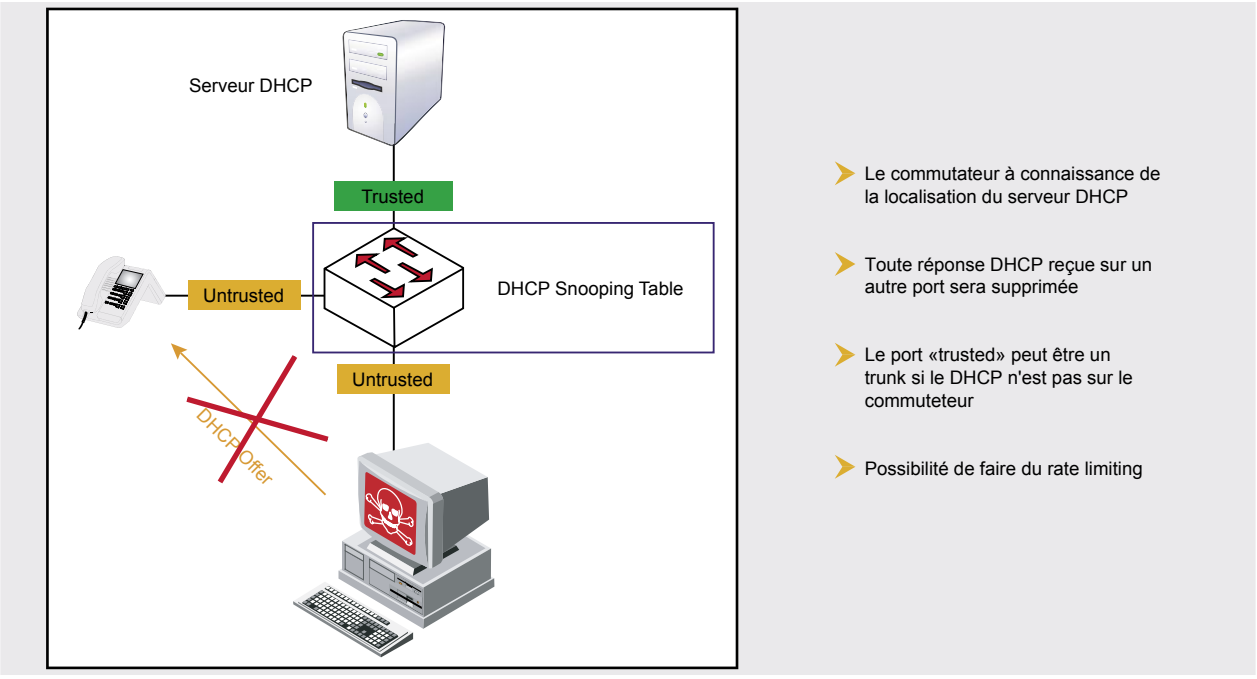


Figure 6. *Mise en place des zones de confiance.*

comparés à la table de correspondance construite par la fonction *DHCP Snooping* pour éviter qu'un ordinateur tierce puisse perturber le bon fonctionnement de la solution.

- 4- Les messages de type DHCP Discover dont l'adresse MAC de l'en tête de niveau 2 ne correspond pas à l'adresse MAC utilisée au niveau applicatif par le protocole DHCP seront supprimés – attention cependant, il est nécessaire d'activer une option spécifique dans le paramétrage pour que cette fonction soit active. Cette option répondra aux attaques évoluées visant à épuiser les pools d'adresses IP.

Une option plus restrictive encore de ce paramétrage consistera à mettre en place le *rate-limiting*. Cette fonction imposera un rythme de paquets par seconde maximum. Si la limite imposée est dépassée à cause d'un flux trop important, le port impacté sera coupé pour éviter un déni de service.

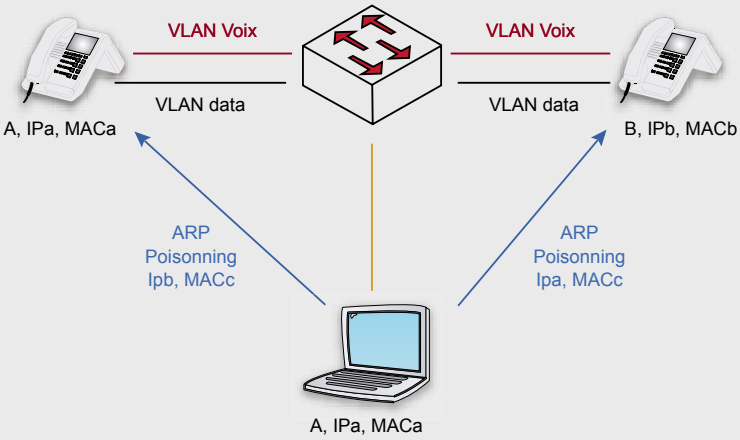
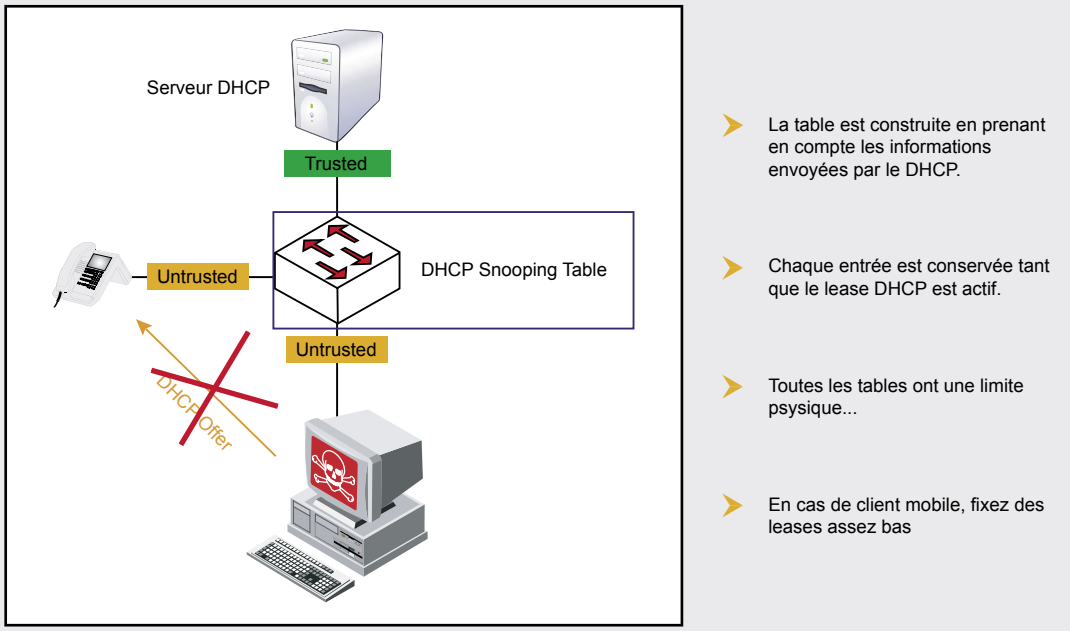


Figure 8. *Attaque de type ARP cache poisonning*

Le protocole ARP

Pour que deux ordinateurs connectés sur le même subnet puissent dialoguer, il est nécessaire que ces derniers connaissent leurs adresses MAC respectives pour pouvoir correctement adresser le trafic réseau. Le protocole ARP (*Address Resolution Protocol*) est là pour répondre à ce besoin.



- La table est construite en prenant en compte les informations envoyées par le DHCP.
- Chaque entrée est conservée tant que le lease DHCP est actif.
- Toutes les tables ont une limite psysique...
- En cas de client mobile, fixez des leases assez bas

```
S_DEMO#sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)     Type           VLAN  Interface
------------------  ----------      ----------     -------------  ----  ----------
00:12:79:BD:92:67   10.0.10.9       691184         dhcp-snooping  2     GigabitEth
ernet1/0/6
Total number of bindings: 1
```

Figure 7. *Construction de la table du DHCP Snooping*

Ainsi, lorsqu'un poste A (*IP_A*) souhaite communiquer avec un poste B (*IP_B*) sur un même LAN, il est obligé d'envoyer une requête ARP de type broadcast pour demander à qui appartient l'adresse IP_B et récupérer l'adresse MAC correspondante. Une fois en possession de ces deux informations, le poste A les places dans sa mémoire cache pour un temps donné et peut générer les trames réseaux avec les bons paramètres. ARP a par ailleurs été développé avec un mécanisme appelé Gratuitous ARP. Ce dernier est supposer permettre à un périphérique connecté sur le réseau d'informer l'ensemble des éléments actifs connectés d'un changement de son adresse MAC via une trame spéciale non sollicitée. L'ensemble des éléments actifs la recevant mettent alors leurs mémoires cache à jour.

ARP a été standardisé en 1982 au travers de la RFC 826 au tout début d'Internet lorsque les problématiques de sécurité que nous connaissons aujourd'hui n'étaient pas au cœur des préoccupations. Il n'a donc intégré aucun mécanisme de vérification d'intégrité ou encore d'authentification.

Les attaques

Le protocole ARP (et sa faible sécurité) a permis le développement d'une attaque de type MITM (*Man In The Middle*) au travers du mécanisme appelé ARP cache poisonning ou encore ARP *spoofing*.

Comme évoqué précédemment, ARP n'a pas été conçu avec des mécanismes de sécurité intégrés. Cette absence de vérification va permettre de détourner la fonction Gratuitous ARP pour envoyer et faire accepter des informations falsifiées à des périphériques données. L'attaquant va donc générer un paquet *GARP* vers le poste A, Ipa, MACa l'informant que pour joindre le poste B,IPb,MACb il doit envoyer un paquet vers IPb, MACc. La même manipulation sera réalisée pour le poste B en lui envoyant le couple Ipa,MACc (voir Figure 8). Les postes vont alors mettre leurs caches ARP à jour avec ces informations et envoyer systématiquement les paquets vers la MACc, soit celle de notre attaquant, lorsqu'ils souhaitent communiquer entre eux. Le trafic réseau est détourné et peut alors être intercepté, puis interprété via un sniffer.

On notera que cette attaque vient briser le mythe de la commutation. En effet, lors de son apparition sur le marché, elle est apparue comme une technologie corrigeant l'un des gros défauts des hubs qui était de répliquer le trafic sur tous les ports. La capture de données sur le réseau était alors présentée comme impossible, le trafic étant véhiculé sur un mode proche du point à point entre les machines. Il est désormais simple de mettre en évidence que la sécurité d'un réseau n'est pas assurée par ce que ce dernier est intégralement en mode commuté.

De nombreux scripts automatisent aujourd'hui cette attaque et peuvent être facilement trouvés sur Internet. On pourra citer quelques exemples très connus et souvent décrit comme Ettercap, Dsniff ou encore Cain et Abel. La facilité de réalisation apportée par ces outils rend la nécessité de mettre en place les contre mesures disponibles sur le réseau d'autant plus importante. Cela fait désormais quelques années qu'il n'est plus nécessaire d'avoir des compétences poussées pour réaliser un MITM sur un LAN.

Suite à la description ci-dessus, il est intéressant de constater que nous avons déjà décrit deux attaques de types MITM. Cette famille d'attaques est particulièrement développée et repose sur l'exploitation de nombreux mécanismes différents. N'oublions donc pas que l'ARP cache poisonning n'est pas le seul permettant d'arriver à une redirection du trafic.

```
SwitchB# show ip arp inspection log
Total Log Buffer Size : 1024
Syslog rate : 100 entries per 10 seconds.
Interface   Vlan  Sender MAC      Sender IP  Num Pkts   Reason      Time
----------  ----  -------------   --------   ---------  ---------   ----
Gi3/31      100   0002.0002.0002  170.1.1.2     5       DHCP Deny   02:30:24 UTC
Fri Feb 4 2005
```

Figure 9. *Les logs générés par le DAI*

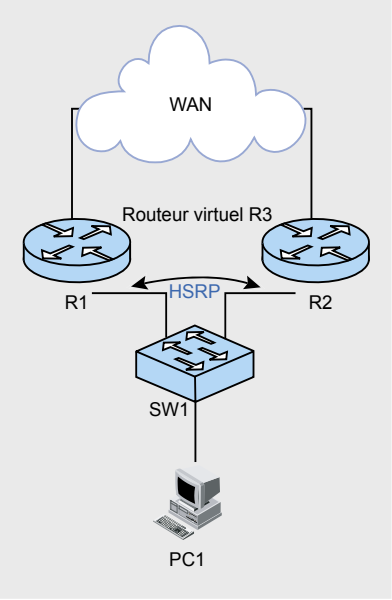


Figure 10. *Architecture réseau incluant le HSRP*

Les contre mesures

Les contre mesures existantes dans le monde Cisco reposent sur la table de correspondance décrite dans la partie DHCP Snooping. En effet, celle-ci nous garantit normalement d'avoir des couples de références identifiés et fiables. Il suffira donc d'activer un mécanisme allant comparer les couples MAC,IP des paquets transitant sur un commutateur avec cette table. La fonction permettant de mettre cette vérification en place se nomme *Dynamic ARP Inspector.* On la retrouvera souvent sous l'appellation DAI.

La configuration du DAI sur un commutateur Cisco est simple. Il suffit de passer la commande `ip arp inspection` en mode *config* en précisant le vlan sur lequel elle doit porter (il est naturellement possible de travailler sur de multiples VLAN). Une fois activée, tout paquet réseau ne respectant pas la table de référence se verra supprimé, aucun paquet falsifié ne pourra donc plus être émis sur le réseau.

Attention, dans le cas ou l'on devrait faire cohabiter un adressage fixe et un adressage dynamique dans le même VLAN avec la fonction DAI activée, il sera nécessaire d'effectuer un mapping manuel entre les adresses MAC et les adresses IP fixes à l'aide de la commande `ip dhcp snooping binding` Si ceci n'est pas réalisé, tout

le trafic à adressage fixe sera supprimé car non présent dans la table de correspondance et un déni de service aura été provoqué non intentionnellement vis à vis des utilisateurs...

Il est intéressant de constater que cette commande est capable de générer des logs lorsqu'une anomalie est détectée (Figure 9). Ces informations seront précieuses pour l'administrateur qui souhaiterait comprendre la provenance du problème et identifier les postes incriminés.

Dans le cas ou il serait impossible d'activer la fonction DAI sur un commutateur (obsolescence), il existe malgré tout d'autres solutions permettant d'identifier des attaques de type ARP Cache Poisonning. L'utilisation d'un script comme arpON permettra ainsi d'analyser le trafic réseau et d'identifier des anomalies.

Enfin, pour terminer sur ce point, rappelons que la commande DAI n'inspecte que les entêtes de niveau 2. L'inspection du niveau 3 et de l'adressage IP se fera à l'aide de la fonction ip source guard.

Le protocole spanning-tree

Le protocole spanning-tree est utilisé dans tous les environnements commutés pour créer des environnements redondés et éviter la création de boucles sur le réseau. C'est un protocole extrêmement important qu'il ne faut pas négligé car sa perturbation peut interrompre les transmissions d'un domaine de niveau 2 complet.

Ce sujet a déjà fait l'objet d'un article dans le HS1 2008 d'Hakin9 et ne sera donc pas à nouveau évoqué ici. Nous vous invitons cependant fortement à parcourir l'article le concernant pour bien comprendre les outils existants pour le sécuriser.

Les éléments de sécurisation du niveau 3

Le protocole HSRP (*Hot Standby Router Protocol*) est, comme tous les protocoles présentés jusqu'ici, régulièrement utilisé au sein des réseaux LAN. Il permet d'offrir une résilience des passerelles sur un LAN donné de façon totalement transparente pour l'utilisateur grâce à la création d'une entité virtuelle qui représentera plusieurs éléments physiques.

Les routeurs faisant tourner le processus HSRP seront inclus dans un groupe (Un groupe sera composé de deux routeurs ou plus) présentant une adresse IP unique aux utilisateurs. On parlera d'adresse IP virtuelle car elle représente l'ensemble des routeurs inclus dans le groupe. Cette adresse sera identifiée comme passerelle pour le LAN et distribuée via le DHCP. Une fois l'appartenance au groupe déclarée, un routeur sera choisi pour être l'élément actif vis à vis des utilisateurs et porter l'adresse IP virtuelle. L'ensemble des flux du LAN transiteront donc par ce dernier. Le choix du routeur actif est réalisé grâce à la comparaison du paramètre *priorité* renseigné dans la configuration. On se reportera à la Figure 10 pour voir la architecture réseau incluant le HSRP.

Périodiquement, les routeurs d'un groupe HSRP échangeront des messages Hello pour s'assurer que les routeurs du groupe sont encore joignables. Si le routeur actif devient inaccessible, ou si le lien tombe, un autre routeur sera élu. Tous les messages entre les routeurs sont échangés en utilisant l'adresse multicast *224.0.0.2* (qui correspond à tous les routeurs du lien local) via UDP sur le port 1985. Il suffira de se reporter à la RFC 2281 pour avoir tous les détails concernant le protocole.

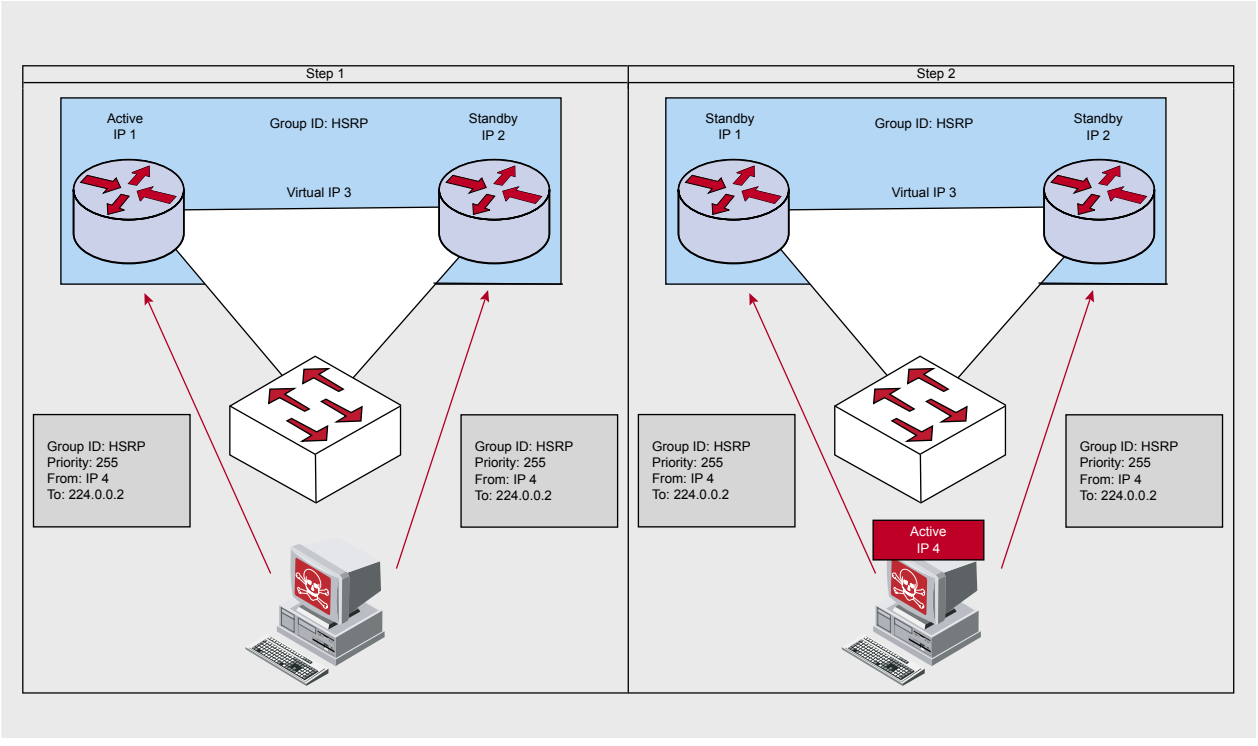


Figure 11. *Préemption du rôle de routeur actif*

Les attaques

Une machine sur le LAN sera susceptible d'intercepter les messages multicast générés par les routeurs HSRP et de prendre ainsi connaissance de certains paramètres du groupe existant. Le protocole HSRP est alors susceptible d'être attaqué au travers de son processus d'élection.

L'attaque qui va être décrite ci-dessous peut mener à deux résultats très différents en fonction des intentions initiales :

- un déni de service total sur le LAN,
- un MITM permettant d'intercepter des informations.

Une fois qu'un attaquant connait les paramètres du groupe HSRP, il lui est désormais facile de générer des messages pour s'insérer dans le groupe et récupérer le rôle de routeur actif en jouant sur le paramètre *priorité*. En effet, ce dernier peut varier de 1 à 255. Il suffira donc de générer des messages avec la valeur 255. Dans le cas ou deux routeurs auraient la même priorité, la plus haute adresse IP permettra de désigner le routeur actif (Figure11).

Une fois devenu routeur actif, l'attaquant pourra soit se transformer en *trou noir*, ce qui coupera l'ensemble du trafic du LAN (nous nous trouverons donc dans le cas du déni de service), soit rediriger le trafic qu'il reçoit en tant que porteur de l'adresse virtuelle vers l'adresse IP d'un des routeurs physique. Ce dernier cas transformera l'attaque sur le HSRP en MITM et permettra d'intercepter les données des utilisateurs. Des scripts comme IRPAS ou Yersinia permettent de réaliser l'attaque décrite ci-dessus très simplement.

Les contre mesures

L'attaque du protocole HSRP qui vient d'être décrite repose sur deux piliers fondamentaux :

- La possibilité de comprendre les informations des trames HSRP,
- La possibilité de générer des trames qui seront acceptées par le processus HSRP en cours.

Ces deux problématiques sont généralement résolues via l'utilisation du chiffrement et de l'authentification dans des situations comparables pour d'autres protocoles.

Seul le concept d'authentification à finalement été retenu pour sécuriser le HSRP. Avant l'introduction du MD5 dans l'IOS 12.2.(25)S, le HSRP ne proposait la mise en place d'une authentification qu'au travers d'une simple chaine de caractère, qui pouvait donc être contourner. L'utilisation de l'algorithme de hashing MD5 permet désormais d'éviter la transmission en claire de la chaine d'authentification et propose donc une sécurité plus importante. On se souviendra cependant que le MD5 possède désormais quelques failles connues et reste donc à surveiller.

Une fois l'utilisation du MD5 validée dans la configuration chaque groupe possédera désormais un mot de passe qui lui sera propre et qui permettra de signer les messages à l'aide d'un hash (Figure 12).

Enfin, si nous avons vu qu'il existait un mécanisme propre à HSRP pour augmenter la sécurité, il ne faut pas oublier les autres possibilités offertes par un routeur. Ainsi, la mise en place d'une access-list n'autorisant que les *messages multicast* (*224.0.0.2*) des membres du groupe HSRP permettra d'éviter toute réception de message HSRP générés par un éventuel attaquant.

Exemple d'access-list filtrant les messages HSRP entrant :

```
access-list 101 permit udp
      host192.168.0.7 host 224.0.0.2
      eq 1985
access-list 101 permit udp host
      192.168.0.9 host 224.0.0.2
      eq 1985
access-list 101 deny udp any any eq
      1985 access-list 101 permit
      ip any any !
interface FastEthernet0/0
   ip access-group 101 in
```

Le routage dynamique

Le routage est le processus permettant à un routeur de transmettre un paquet vers sa destination finale.

À chaque arrivée d'un paquet, ce dernier regardera les informations des entêtes IP, cherchera dans sa table de routage (table contenant l'ensemble des routes connues par le processus de routage) la route correspondant à la destination, et retransmettra le paquet sur la bonne interface.

Le routage se décline en deux grandes familles dans les périphériques réseau :

- Routage statique,
- Routage dynamique.

Le routage statique nécessite d'entrer manuellement toutes les routes sur un routeur. C'est donc un processus lourd et qui demande de reconfigurer l'ensemble des routeurs à chaque changement de topologie du niveau 3.

Les protocoles de routage *dynamique* introduisent une souplesse beaucoup plus grande dans la gestion du routage. En effet, on ne configurera initialement que les *subnet IP* directement connectés à un routeur donné. Celui-ci échangera ensuite ces informations avec les différents voisins (routeurs faisant tourner le même protocole de *routage dynamique*) qu'il aura identifié pour construire petit à petit une table de routage contenant toutes les routes du réseau.

À chaque changement de topologie, le routeur concerné mettra à jour sa table de routage et l'information se propagera sur l'ensemble du réseau au travers de messages périodiquement échangés par les routeurs et sans aucune intervention de l'administrateur.

Les protocoles couramment rencontrées sur le LAN sont les suivants :

- RIP V1,2,
- EIGRP,
- OSPF.

Les attaques

Un attaquant s'intéressera généralement aux protocoles de routage dynamique pour trois raisons essentielles :

- récolter des informations,
- réaliser un déni de service,
- détourner un flux de données.

La récolte d'informations sur le réseau se fera essentiellement de façon passive en interceptant des messages échangés par les protocoles de routage *dynamique*. Cela permettra d'avoir une meilleure compréhension de la structure du réseau. Cette phase est d'autant plus facile que l'administrateur aura été laxiste dans sa configuration en autorisant, notamment, l'envoi des messages (*souvent multicast*) sur les LAN utilisateurs.

La réalisation d'un déni de service ou le détournement d'un flux sont nettement plus complexe. Il faudra tout d'abord que l'attaquant ait réussi à bien identifier le protocole de routage dynamique utilisé. Ceci devrait normalement avoir été réalisé dans la phase de reconnaissance évoquée ci-dessus. Une fois en possession de ces informations il sera nécessaire de pouvoir se faire reconnaître comme un nouveau voisin par les processus de routage des routeurs identifiés. Cette phase est obligatoire pour pouvoir envoyer des informations qui seront acceptées. Arrivé à ce stade, l'attaquant sera en mesure de générer des paquets contenant des informations de routage qui seront acceptées.

La suite IRPAS permettra de travailler sur le protocole *EIGRP* (Figure 13). Dans l'ensemble, les scripts permettant d'attaquer ou de détourner l'usage des protocoles de routage dynamique sont beaucoup moins présents sur Internet. Il faudra souvent avoir recours à des outils permettant de générer soi même des paquets arriver au résultat attendu (*Scapy* et *Nemesis* seront vos amis dans cette tache ardue).

L'envoi d'informations de routage n'ayant aucun sens sur le réseau provoquera un déni de service en perturbant le routage et donc l'acheminement des flux de données. Par ailleurs si un recalcule permanent des topologies du réseau est provoqué par l'attaquant, les ressources CPU et mémoires de routeurs pourront éventuellement être saturées au point de perturber les processus internes du périphérique.

Une étude plus approfondie permettra éventuellement à l'attaquant de rediriger certains flux vers sa machine ou vers une machine supervisant le réseau, lui donnant ainsi accès à des informations. Il sera bien sur nécessaire de mettre en place un processus ré-émettant les flux de données pour être le plus neutre possible vis à vis des utilisateurs. Avez vous remarqué que nous sommes à nouveau dans une situation de MITM ?

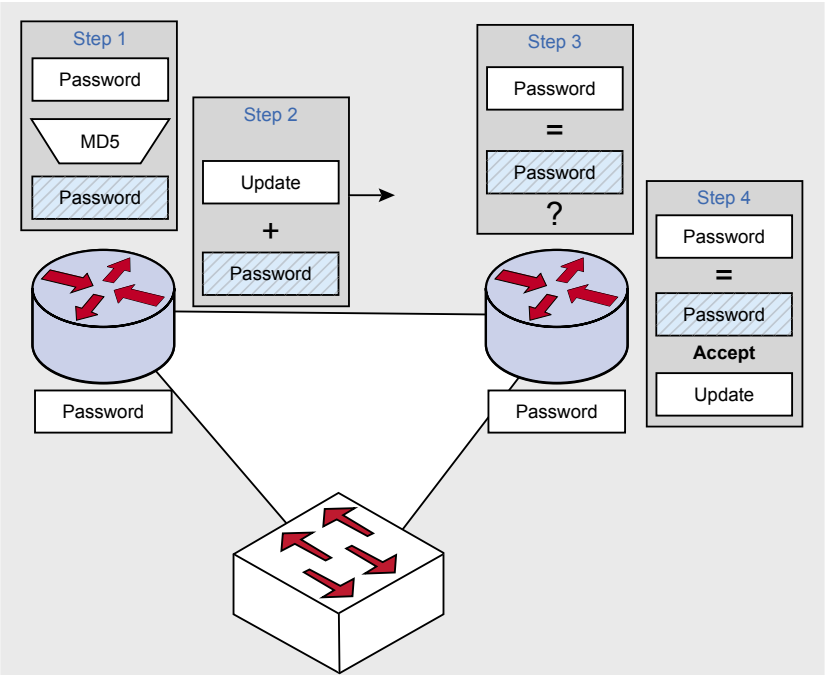


Figure 12. *Authentification via MD5*

Les contre mesures

Les protocoles de routage dynamique intègrent généralement deux grandes mesures permettant d'améliorer la sécurité du processus :

- L'authentification des routeurs partageant des mises à jour,
- La validation de l'intégrité des informations échangées.

La mise en place de l'authentification des routeurs et de l'intégrité des messages peuvent généralement être réalisées de deux façon :

- L'utilisation d'un mot de passe simple (chaîne de caractères) qui sera transmise entre voisins. Si la comparaison de la chaine reçue avec celle qui est gardée localement correspond, le voisin est authentifié et ses mises à jour acceptées. Comme toujours avec ce type de méthode, le mot de passe est envoyé en claire sur le réseau et peut donc être intercepté par une tierce partie. On lui préférera donc la deuxième option ci-dessous.
- L'utilisation des algorithmes de hashing MD5 ou HMAC permettant d'éviter la transmission en claire du mot de passe. En effet, le mot de passe sera utilisé avec le message pour produire un hash unique qui sera comparé par le voisin recevant la mise à jour avec le résultat qu'il produira en local à l'aide la clé pré-partagée (voir Figure 14).

On notera que la seconde méthode permet également de valider l'intégrité du message. Ainsi, même si un attaquant interceptait le message, il pourrait obtenir des informations complémentaires mais en aucun cas s'en servir pour modifier les

tables de routage des routeurs. En effet, n'ayant pas la clé, il ne pourra pas calculer le hash correct pour le message modifié.

Enfin, il ne faut pas oublier d'utiliser les commandes `passive-interface` et `distribute-list` qui permettent de mieux maitriser l'envoi des mises à jour sur le réseau, limitant ainsi les possibilités d'interception par un attaquant éventuel.

Sécurisation des périphériques réseaux eux mêmes

Nous avons examiné jusqu'ici comment sécuriser les protocoles couramment utilisés sur les réseaux LAN, mais sans à aucun moment nous pencher sur la problématique de la sécurisation du périphérique réseau lui même. Il est temps de réparer cet oubli.

Les périphériques Cisco travaillant sous IOS doivent subir un renforcement de leur sécurité de base, comme cela peut être pratiqué sur des serveurs Windows ou Linux. De nombreux éléments ne sont pas configurés de façon standard ou sont désormais obsolètes dans nos environnements modernes et sont susceptibles d'offrir des ouvertures à un attaquant potentiel. C'est d'ailleurs sans surprise que les mêmes titres de chapitres se retrouveront.

La première chose à réaliser sera de sécuriser correctement les moyens d'accès au périphériques. Il faudra donc travailler sur les accès console, auxiliaire et VTY essentiellement:

- Pour chacun de ces accès, il sera nécessaire de mettre en place une authentification. Une authentification locale est disponible, mais un véritable serveur d'authentification comme un *RADIUS* ou un *TACACS* sera toujours préféré. On veillera à mettre en place le système de détection des authentifications négatives pour pouvoir être alerté d'une attaque dictionnaire éventuelle.
- Seuls les administrateurs doivent pourvoir se connecter au périphérique pour le configurer. Il sera donc intéressant de mettre en place un filtrage (*access-list*) limitant l'accès aux seuls postes administrateurs.
- En cas de connections distantes, le protocole SSH devra toujours être préféré au protocole *TELNET*.
- Un mécanisme de timeout doit absolument être configuré sur ces interfaces de connexion pour éviter qu'une session puisse rester ouverte suite à un oubli et être réutilisée par une personne non habilité.
- Une bannière d'accueil doit être configurée, permettant de bien identifier le périphérique mais informant aussi que toute connexion non autorisée sera sanctionnée.

Comme un OS traditionnel, un IOS comporte un certain nombre de services qui sont inutiles la plupart du temps et peuvent donc être inactivés :

- ip source route,
- service tcp-small-servers,
- service udp-small-servers,

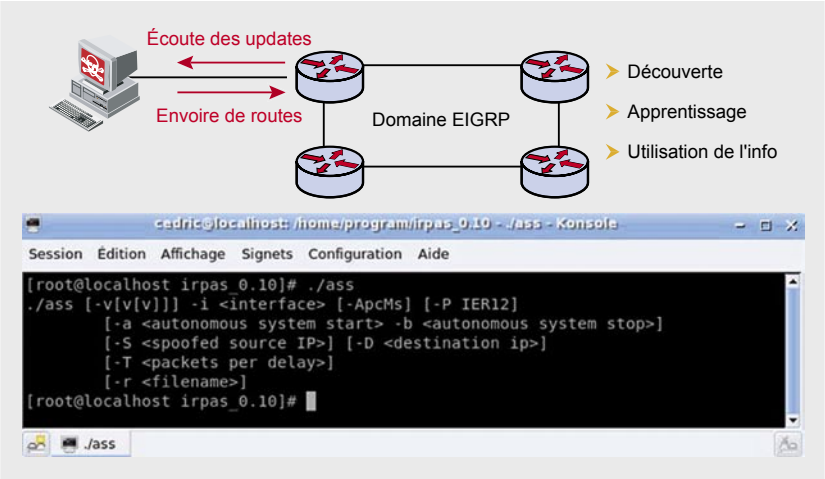


Figure 13. *IRPAS*

À propos de l'auteur

Après avoir travaillé pendant quatre années sur les technologies réseaux Cisco en tant qu'ingénieur de production, Cédric Baillet a été consultant sur les solutions de ToIP et les problématiques sécurité afférentes de 2004 à 2007. Il a aujourd'hui intégré une des équipes marketing d'Orange Business Services pour travailler sur les offres de services sécurité autour des nouvelles solutions de communications. L'auteur peut être contacté à l'adresse mail suivante: *cedric_baillet@yahoo.fr.*

Sur Internet

- Cisco – *www.cisco.com*,
- Guides NSA – *http://www.nsa.gov/snac/downloads_all.cfm*,
- RATS – *http://www.cisecurity.org/bench_cisco.html*,
- Nipper – *http://sourceforge.net/projects/nipper*,
- CCSAT – *http://freshmeat.net/projects/ccsat/*,
- ARCCIOS – *http://www.cedric-baillet.fr/spip.php?article12*,
- Yersinia – *www.yersinia.net*,
- irpas – *www.phenoelit.de*,
- arpON – *http://arpon.sourceforge.net*,
- Dsniff – *http://www.monkey.org/~dugsong/dsniff/*,
- Scapy – *http://www.secdev.org/projects/scapy/*,
- Nemesis – *http://www.packetfactory.net/projects/nemesis/*.

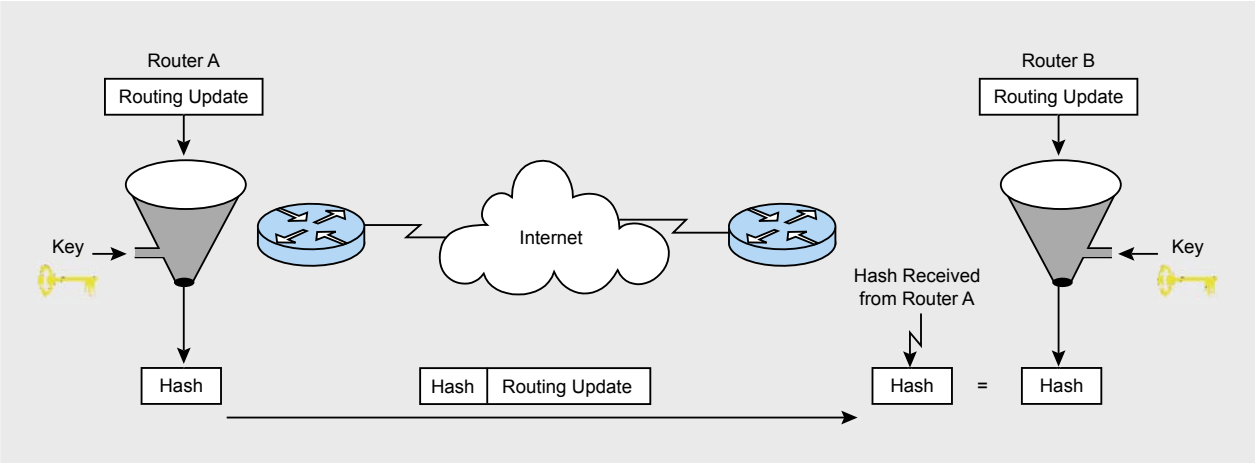


Figure 14. *Utilisation d'un algorithme de hashing pour sécuriser le routage dynamique*

- ip bootp server,
- ip finger,
- ip http server,
- service config,
- boot host,
- boot network,
- boot system,
- service pad.

Le listing ci-dessus reprend les plus connus mais n'est pas exhaustif. Seul un examen attentif de la documentation de l'IOS installé sur votre périphérique permettra d'aller jusqu'au bout de la démarche.

La gestion de la sécurité repose en grande partie sur l'examen des logs générés par les périphériques. C'est celui-ci qui permet de comprendre les évènements qui se sont produits, d'apporter d'éventuelles corrections, et surtout de pouvoir remonter vers la source ayant provoqué un comportement anormal. Il est donc absolument indispensable de les activer. Un niveau par défaut est présent localement. Un paramétrage plus fin et un transfert vers un syslog extérieur seront un plus indéniable dans la gestion de l'ensemble des messages qui seront générés.

Le protocole SNMP est généralement utilisé pour les opérations de supervision des périphériques et la génération de traps. L'utilisation de la version 3 sera préférée car plus sécurisée. Il sera par ailleurs nécessaire de ne pas laisser les *community string* privée et publique par défaut.

Il faudrait désormais détailler chaque point cité ci-dessus pour aller plus loin, ce qui n'est pas possible ici. Nous vous recommandons donc de lire le guide librement accessible de la NSA portant sur ce sujet (l'url est présente dans la rubrique lien web). Il est vrai qu'il a été rédigé depuis quelques années, mais toutes les bases sont présentes et le niveau de sécurité qui sera atteint sur vos périphériques si tout est respecté sera plus qu'honorable. Pour aller plus loin, il faudra se tourner vers les ouvrages spécialisés proposés par les grands éditeurs (Cisco Press, Syngress etc...).

Enfin, nous pensons qu'il est intéressant de finir en citant quelques scripts permettant de tester le niveau de sécurité des configurations. Les plus connus que l'on pourra trouver sur Internet sont les suivants :

- RATS,
- NIPPER,
- CCSAT.

Chacun à ses avantages et ses inconvénients. En tant qu'utilisateur, j'ai finalement opté pour le développement de mon propre script, Arccios, pour répondre à mes besoins spécifiques, à savoir:

- l'intégration des commandes récentes,
- la possibilité de gérer différents profils avec des jeux de tests différents,
- génération automatique d'une todo list,
- génération de fichiers csv pour une ré-intégration simple dans excel,
- la possibilité de modifier ou de créer de nouveaux jeux de tests assez simplement.

Il est souvent plus simple de créer et de maintenir son propre travail que de faire évoluer celui d'un autre... Dans ce domaine, seule votre propre expérience vous permettra de déterminer quel outil correspond le mieux à votre besoin.

Conclusion

Nous venons de voir qu'il était possible d'utiliser de nombreuses fonctions des routeurs et commutateurs Cisco pour améliorer la sécurité du réseau lui même et de l'environnement utilisateur par ailleurs.

Cet article ne présente que quelques briques de base traitant des éléments les plus couramment rencontrés. Le passage d'une certification comme le CCSP permettra d'avoir une vision beaucoup plus large des possibilités de sécurisation d'un environnement d'entreprise via son réseau et surtout de la façon d'architecturer l'ensemble à bonne escient.

Un réseau bien sécurisé ne passe pas forcément par une consommation immodérée de solution de sécurité, mais surtout par une architecture solide et une exploitation intelligente des fonctions présentes dans chaque périphériques déployé. ●