# Network security


Local security

**Antoine Puissant**

Enseignant : M. Rey

2014 - 2015

**Résumé**

Ceci est le résumé

# Table des matières

# 1 Introduction

Être compétant c'est savoir appliquer les notions, le savoir, les compétences. Être professionnel c'est être capable de mettre en œuvre ses compétences à un instant T durant une durée donnée plus le relationnel.

## 1.1 Plan du cours

## 1.2 Fonctionnement des labs

VM avec un simulateur de réseau français, *Marionnette*. La syntaxe est « à la *CISCO* ».

# 2 Rappels de réseaux

Taille de la trame Ethernet : 1500 octet. Ethernet est normée par IEEE.
Au dessus du niveau Ethernet, on retrouve la norme IP. Elle a un taille max de 65Ko.
TCP va être en charge de la découpe des paquets IP.
TCP demande à la carte quel est son MTU [1] puis il fait des segments dont la taille correspond au plus petit paquet. Il calcule par rapport à la taille des en-têtes qui vont être rajouter à la fin.
La trame Ethernet va avoir une partie qu'on ne peut pas voir en exécutant un analyseur logiciel, on va retrouver (en vert sur le schéma) des partie que seule a carte réseau va utiliser : une initialisation de l'horloge de la carte en fonction de l'horloge de la trame, jusqu'à un checksum.
Pour connaître de quel type d'équipement vient l'adresse MAC, on peut utiliser des *MAC manufacturer*.
Chaque constructeur a un code constructeur composé de 3 octets.
Adresse MAC de destination en premier car ça permet de ne pas avoir à attendre de lire la trame pour pouvoir commuter le plus rapidement possible.
On met le $R_x$ sur le $T_x$ de l'autre.
Un routeur est ordinateur avec deux cartes réseaux. Donc il faut un câble croisé entre les deux PC ou alors mettre un switch entre les deux pour que ce dernier croise en interne.
Auto négociation MDIX : la carte réseau sonde pour savoir si le câble est croisé ou pas. Si ce n'est pas le cas, la carte croise d'elle même. Le problème c'est que ça prend du temps tout le temps.

## 2.1 Câbles

Blindage (shield) ! = d'écrantage (folded). Ecrantage = protection des parasites basse fréquence $< 3000Hz$.
Blindage (on tresse autour du câble) = protection des parasites hautes fréquences de rentrer et empêche le signal de sortir du câble.
Extérieur blindé (shield) et chaque paire est écrantée (folded) est le meilleur rapport qualité.

1. Taille max que la carte réseau

Entre deux équipement réseaux, il ne faut pas dépasser 100m. Sinon le réseau n'est plus assuré.

## 2.2 Les offres Ethernet

Fast Ethernet = ? ? ?
Giga Ethernet = Gigabit
10 Giga Ethernet = 10 Gigabit

## 2.3 Matériel

### 2.3.1 Hub

C'est un répéteur.
Pour ne pas que tout le monde ne parle pas en même temps, on a une norme ( ? ? ?). Elle va permettre de mesurer le voltage pour voir s'il est supérieur à celui qu'on envoie. Si c'est le cas c'est que quelqu'un d'autre à parlé. On arrête la transmission. Une durée de temporisation est alors choisie aléatoirement avant de relancer le message.
Hub, acces point, bluetooth c'est de l'half-duplex.

### 2.3.2 Switch

C'est du full-duplex.
Pas de collision car auto-commutés par le switch.
Pas de norme car personne ne s'est mis d'accord.
Combien de switch peut-on mettre en casaque ? Entre deux switchs, pas plus de 100m déjà. On ne doit pas dépasser 3 bonds (hop). On prend une topologie en étoile. Il faut réduire le nombre de bonds pour augmenter la vitesse de transmission.
Fonctionnement interne du switch :

### 2.3.3 VLAN

Sert à cloisonner le réseau local sans avoir à dépenser beaucoup de switchs. On va alors indiquer au switch principal sur quelles VLAN sont les machines qu'il connaît.
Les VLAN sont à concevoir intelligemment.
802.1$q$

### 2.3.4 IP/Ethernet

Quelle est la différence entre le broadcast et le multicast MAC ?
De 224 à 255, c'est des adresses de multicast IP. Le multicast IP c'est envoyer en continu le/les flux à tous les utilisateurs. Les utilisateurs se calent ensuite sur un des flux.

# 3 Le switch

Une matrice de commutation = une connexion à l'instant T. Le maximum c'est le $\frac{nombre\ de\ ports}{2}$ matrices.

Pour améliorer les performances d'un switch, on va pouvoir faire du *switch trunking*. On fait de deux switch un seul. Cela va permettre d'augmenter le nombre de ports ou de faire de la redondance.
On peut aussi mirrorer un port. Cela va permettre d'avoir un accès à un autre port pour faire de l'audit.
En sécurité, on va pouvoir réaliser certaines choses :

- Désactiver les ports qui ne sont et ne seront pas utilisées
- faire du MAC learning : Lors du premier branchement, on apprend l'adresse MAC et on bloque sur celle la. On ne pourra pas recevoir des messages d'autres adresses MAC. On pourra aussi lever des trappes SNMP afin de relever une intrusion.

Un commutateur c'est un HUB à mémoire. Cette mémoire est appelée la *CAM Table*.
In va avoir l'*aging time* aka le temps d'usure d'une adresse MAC. On fixe cette valeur. Durant cette durée, si l'adresse MAC n'a pas été vue, le switch va alors l'oublier de sa mémoire.
Les prises backbone vont permettre de faire une architechture en étoile.
Mode de Fonctionnement normal d'un switch bas de gamme : *Store and forward*.
Cependant, prend du temps car on fait une vérification du CRC de la trame.
Un switch plus intelligent va envoyer et chercher des erreurs aléatoirement. Si le switch détecte une erreur il passe alors en *store and forward*.

# 4 VLAN

On veut cloisonner dans un seul ou peu d'équipement réseaux.

## 4.1 VLAN de niveau 1

Dans la couche 1 du modèle OSI. C'est un filtre par ports. Les ports mis dans le VLAN1 n'auront pas accès aux autres VLAN des autres ports.
On ne peut pas alors pas bouger, pas de mobilité. C'est quelque-chose de figé.

## 4.2 VLAN d3 niveau 2

On va pouvoir faire de l'adressage dynamique. On va alors choisir les VLAN en fonction de l'adresse MAC. Quand le switch rencontre une adresse MAC qu'il connaît, il la positionne dans son bon VLAN.
Cependant, il faut rentrer les adresse MAC à la main, ce qui est long.

## 4.3 VLAN de niveau 3

Les machines ne vont pas utiliser les mêmes protocoles. Elles ne vont pas pouvoir communiquer entre elles. Par exemple, deux Russes dans une salle vont discuter entre eux. Les français ne vont pas discuter avec eux car ils ne parlent pas Russes.
La norme 802.1$Q$ va pouvoir permettre de tagger la trame. La partie du tag la plus utilisé est le VLAN ID. Le champs tagué est utilisé entre deux ports particuliers entre deux ports $TAG$ des deux switchs.
Pour un serveur qui doit être joignable par plusieurs VLAN, on peut :

— mettre ce serveur dans tous les VLAN
— faire un lien tagué jusqu'à ce serveur. Le tag comprend les VLAN de ceux qu'il devra tester (c.f. *router on the stick*).

# 5 Protocol SMB

SMB vient de IBM NETBIOS et à été repris et modifié par Microsoft.
Il est dédié uniquement aux réseaux LAN car les paquets font environ 50 octets. Cela va permettre d'être super réactif sur les LAN. Sur un WAN ça ne va pas fonctionner d'une bonne manière car les petits paquets vont surcharger les routeurs. Les prestataires (opérateurs) vont alors bloquer le protocole.
Le projet de portage de SMB sur Linux s'appelle SAMBA.
Le nom de SMB est aussi cifs.

# 6 Infrastructure du réseau Internet

Cloud computing :
— IaaS = Achat de machines physique. Plus cher mais plus libre.
— PaaS = Achat d'un VM. On peut mettre l'OS que l'on veut mais on n'a pas l'infirmation du serveur.
— SaaS = Achat d'un service uniquement.

SDNL = débit montant = débit descendant
FTTH/FTTB = fibre.
Opérateurs satellitaires (hors de la législation Française)
Comment sécuriser un réseau d'entreprise comprenant un réseau non classifié (Internet) et un réseau confidentiel ?

1. Les 2 réseaux sont séparés physiquement. Même pas de VLAN. Les deux réseaux n'ont aucuns lien.
2. Pour le réseau NP, on va mettre une sécurité (firewall)
3. Mise en place d'une station blanche pour transférer des données du NP au P.
4. Mise en place d'un DHCP snooping pour sécuriser le DHCP. Il va permettre en configurant le switch, de lui dire sur quels ports doivent aller les réponse DHCP (sur le port du serveur DHCP). Il faut alors un switch intelligent pour qu'il puisse aller sur la couche IP.
5. Chiffrer les Wi-Fi avec des clés primaires simples.
6. Limiter la puissance du Wi-Fi pour ne pas rayonner la où on n'en à pas besoin.
7. Cacher le SSID pour le réseau d'entreprise (visible pour le guest)

Vulnerabilités du DHCP :
— DDoS : on fait des requêtes jusqu'à que le DHCP n'aura plus d'adresses disponibles.
— Faire un serveur DHCP autre qui répondra plus rapidement que le vrai. Ainsi, les machines vont passer par le faux serveur DHCP.

## 6.1 Obligations légales

Toute personne physique ou morale qui propose un accès aux services de communication ou au stockage, au public, doivent conserver toutes les infos permettant d'identifier toutes les infos (dates, durée, identité ; ...) des utilisateurs.
La CNIL dit qu'un utilisateur est composé d'un nom et un prénom.
Il faut mettre en place un NAC [2]. On le place en coupure (pas en dérivation, si lui tombe, tout le réseau tombe pour pas qu'il loupe des informations).
Trois solutions :
— Louer un produit qui fait cela (il faut que ça soit écrit sur le contrat)
— Acheter une Appliance [3] (Utopia, StormShield, DSCbox, etc...)
Il faut contrôler la solution pour être sur que cela fonctionne correctement !

2. *Network Access Derivation*
3. OS modifié pour une application particulière puis monté

— Réaliser la solution en interne.
Il faut aussi contrôler ! Soit par le RSSI soit par un audit externe.

Pour le contrôle,

— Il faut tout loguer, tous les ports ! Que ça soit de l'IRC, de la VoIP, du HTTP, etc...

Autres NAC :

— IPCOP
— PFSense

Le problème des NAC « génériques » sont qu(ils vont logguer de manière simpliste. Il faut, pour la loi française pouvoir associer une personne à un moment donné.

# 7 Sécurité du LAN

Sécurité de l'accès aux médias.
Il faut connaître le MTBF [4]. Cela permet de prévoir quand une panne du système risque d'arriver, dans son créneau de panne. Il faut ainsi prévoir de changer ce matériel quand on va arriver au MTBF. En moyenne pour des équipements ont un MTBF de 5 ans. Pour les PC constructeurs professionnels, le MTBF est de 3 ans.
Il faut aussi prévoir la charge afin de pouvoir la répartir de manière adéquate.
Il faut prendre en compte tous les risques en compte (risque de tremblement de terre, de chute de météorites, inondation, etc...).
Il faut chiffrer le coût de la connectivité. Savoir en combien de temps il faut pour remettre le système en place après un problème.
Il faut aussi prévoir la consommation. Si le compteur n'est pas assez compétant, le courant sera insuffisant. Prévoir aussi des systèmes d'onduleurs en cas de coupure temporaire de courant. Peut-être un groupe électrogène en cas de coupure plus longue.
Il ne faut pas oublier la température : les sondes, les climatiseurs, etc...
Le sol doit pouvoir être capable de supporter la charge qui lui est imposée.
Enfin, plus logiciel, il faut prendre en compte des systèmes de sauvegarde et d'archivage. On va avoir des problèmes avec les archives magnétiques (dérèglement des champs magnétiques). On va préférer les systèmes d'archivages magno-optique : écriture en magnétique et lecture en optique. On va aussi pouvoir archiver sur des supports tels que les DVD et Bluray. Cependant ces systèmes s'usent avec la lumière. On passe alors sur des DVD ou Bluray en verre.
Dans une entreprise, on va trouver le RSSI [5] secondé par l'Officier de Sécurité.
Il existe 3 protocoles d'impression :

- LPR (orienté Unix)
- CUPS (orienté Windows)
- RAWPRINTIG, sur le port 9100 (propriétaires)
- Postscript. Cela va imprimer au format natif de l'imprimante. On se passe du spool (intégré à l'imprimante ou à un AD ou un serveur d'impression). Cela va imprimer directement.
  Pour cela, il faut attaquer l'imprimante en FTP : ftp :@IP_imprimante put fichierpostscrip. Ne fonctionne que sur les imprimantes laser.

4. Mean Time Between Failures
5. Responsable de la Sécurité des Systèmes d'Information

# 8 Intranet : interconnection security

On se place dans plusieurs cas de figures :
- Réseaux de l'entreprise séparés physiquement du réseau internet (réseaux militaire, de la Défense).
- Réseaux Internet et entreprise lié (entreprises privées).

Ici, on va se placer dans le cadre d'une entreprise privée. 90% des entreprises sont protégées d'internet par...rien.
Pour mettre de la sécurité, il faut qu'il y ai un besoin de sécurité ; qu'il y ai une politique de sécurité.
Il faut demander au patron ce qu'il veut, quel est son besoin en terme de sécurité (de manière générale le serveur ERP [6]).
Il faut contrôler la sûreté de ce qui vient d'Internet.
Par rapport à ces problèmes, il n'y a qu'une seule règle : on fait passer les paquets dans un « sas ». On va donc cloisonner (*partitionning of flux*). On fait cela dans des DMZ [7].
En sécurité, le lien direct d'internet vers l'entreprise n'existe plus. On passe par les « zones de sécurité ». Généralement, on va mettre dans une zone les serveurs internet (serveurs web, de courrier, les serveurs publiques, ...). On va ainsi mettre une autre zone pour les données allant directement sur l'entreprise.
Pour découper le réseau internet en fonction de l'architecture de l'entreprise, on peut configurer les switchs avec des VLAN.
On va mettre 2 équipements pour rediriger les flux :
- Un pare-feu qui va empêcher les accès illégaux (pare-feu bastion)
- Un second pare-feu qui va permettre de faire de la redirection. Il est possible de rendre ce pare-feu plus intelligent avec un proxy (pare-feu = couche 3 et proxy = couche 4).

En général on ne met pas les mêmes marques pour les pare-feux interne et externe. Ainsi, Si celui qui est externe a une faille, il ne faut pas que le second ai la même.
On va vouloir vérifier si les protocoles autorisés sont bons. Pour cela, il nous faut une application de la couche 4 : le proxy. Il va falloir un proxy par protocole. Aucun proxy ne sait faire plusieurs protocoles.
Si l'on veut accélérer la vitesse de consultation de la navigation web des utilisateurs on va mettre un cache (un par protocole) dans le « sas ». Cela va permettre de ne pas charger la bande passante. Cela permet aussi d'anonymiser la connexion. De faire un NAT sur le routeur de sortie (MASKRADING).
On va donc avoir des règles de proxies :
- Contrôler
- Filtrer les protocoles en fonctions de plein de critères
- Anonymisation de la connexion. On se met en frontal. La sortie des clients (proxy cache, reverse proxy [8] ou de masquerading)
- Accélérer la connexion avec des proxy cache.

Pour détecter les intrusions ou comportements étrange, on va pouvoir avoir différentes solutions :
- NIDS : Network base Intrusion Detection System
- HIDS : Host based Intrusion Detection System

6. Enterprise Resource Planning
7. Demilitarized Zone
8. Devant les serveurs

— DIDS : Distributed : Intrusion Detection System
— WIDS : Wireles IDS

Un IPS, contrairement à l'IDS a un retour sur un pare-feu. Il va alors pouvoir donner des consignes au pare-feu.
CERT [9] va vendre des services de supervision pour récupérer les logs des IDS/IPS.
En plus de la détection réseau, on va aussi pouvoir faire de l'analyse machine. Cela va s'occuper des fichiers de configuration, des processus, comparer les processus en cours d'exécution par rapport à ceux d'hier, etc...Par exemple, PreludeIDS[5].
Les DIDS sont, de manière générale, conçut de manière interne et ne sont vendu quasiment qu'à des États, ou organisation gouvernementale.
Pour les WIDS, ils vont analyser le spectre de la bande Wi-fi pour analyser les flux sur les différentes bandes de fréquences.

On va vouloir aussi mettre en place des VPN [10] afin de pouvoir connecter les site distants ou des personnes en télétravail dans le réseau de l'entreprise. Le flux VPN doit arriver sur les pare-feu. Ainsi, cela permet de ne pas violer la première règle (pas de lien direct depuis l'extérieur de l'entreprise) mais aussi de faire de l'analyse comportementale afin de vérifier de ne pas avoir d'intrusion depuis une machine de l'entreprise.

9. Computer Emergency Response Team
10. Virtual Private Network

# 9 Correction du lab : Frame analysis

Le mode promiscuous donne un ordre au firmware de la carte réseau.
Il existe un mode « injection de trames » afin de pouvoir forger des trames Wi-Fi.
Le fichier faisait le lien entre le code carte mère et le nom de l'entreprise est le fichier « manuf ». Ce fichier se trouve au chemin suivant (sous Debian 8) :

```
/usr/share/wireshark/manuf
```

Pour capturer en ligne de commande, on peut utiliser « tcpdump » ou « tshark ».
Pour la résulution graohique des protocoles et services, Wireshark utilise respectivement les fichiers

```
/etc/protocols
```

et

```
/etc/services
```

Différences entre les paquets icmp d'ethernet (56 octets) : ICMP va alors gonfler la trame afin qu'elle fasse la taille minimale.
Sous Linux on charge la table ASCII depuis le début jusqu'à que la taille soit atteinte.
Sous Windows, la même chose est faite mais à partir de $0x41$ (caractère A).
Ainsi, il est possible de savoir, rien qu'en regardant un paquet ICMP, à partir de quel OS le ping a été réalisé. On appelle ça, l'OS Fingerprinting.
Pour forger des paquets, l'outil *SCAPI* est très performant et très proche du Python.
ARP Poisonning = ARP Flooding + ARP Spoofing
La bannière, c'est la partie dans laquelle le client WEB met des informations sur le système hôte. Pour ne plus afficher ces données, on va pouvoir installer des plugins ou choisir un navigateur le faisant de base[4].
Le Gratuitious arp (apr gratuite qui sert à savoir s'il n'y a pas sur le réseau une machine ayant la même IP). La source est donc 0.0.0.0
Windows, dans le cas d'une réponse positive (un PC disant que oui, l'adresse IP est prise) va alors se déconnecter du réseau en disant que l'IP est déjà prise. Il suffit de faire un paquet qui sera envoyé à tous les gratuitious arp répondant oui pour faire tomber tout un réseau (fausse MAC dans le paquet).
Sous Linux, la même chose est faite, mais on peut l'enlever. Il faut regarder le script de *ifup*. Vers la ligne 400, on peut voir qu'un *arping* est réalisé sur sa propre adresse IP. Il suffit de commenter cette partie pour que cela ne soit pas fait et ne pas avoir d'erreur.
Dans le fichier « capture4.cap », on va retrouver un mail comprenant une pièce jointe. Cette dernière, encodée en en Base64, n'est pas lisible par un humain. Pour avoir le mail complet, il faut, dans Wireshark, suivre le flux TCP [11] afin de voire le message. Dans la fenêtre, cliquer sur *enregistrer sous* puis donner l'extension « .eml » au fichier. En l'ouvrant, il est possible de retrouver la pièce jointe.

11. Follow TCP stream

# Références

[1] ALCASAR. *ALCASAR project*. ALCASAR. 2015. URL : www.alcasar.net/ (visité le 30/09/2015).

[2] ANTIDOTE. *Antidote - Druite*. Antidote. 2015. URL : http://www.antidote.info/ (visité le 01/10/2015).

[3] GLPI. *GLPI project*. GLPI. 2015. URL : http://glpi-project.org/ (visité le 30/09/2015).

[4] KONQUEROR. *Konqueror web browser*. Konqueror. 2015. URL : https://konqueror.org/features/browser.php (visité le 01/10/2015).

[5] PRELUDE. *Prelude SIEM*. PRELUDE. 2015. URL : www.prelude-siem.org (visité le 30/09/2015).

[6] SURICATA. *Suricata*. SURICATA. 2015. URL : http://suricata-ids.org/ (visité le 30/09/2015).

[7] XPLICO. *Open Source Network Forensic Analysis Tool (NFAT)*. Xplico. 2015. URL : http://www.xplico.org/ (visité le 01/10/2015).