Gildas COTTEN
4 avril 2017

Attaques réseaux - Bibliographie

Projet TWCS

Destination :
Daniel Bourget
Pascale Menard

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Sommaire

Liste de figures

Liste de tableaux

1. INTRODUCTION

1.1 SUJET

Ce projet devra dans un premier temps faire une étude bibliographique sur les mécanismes utilisés en cybercriminalité.

On s'intéressera uniquement aux aspects réseaux avec les outils utilisés.

La seconde partie sera consacrée à l'étude de deux ou trois types d'attaques en montrant explicitement comment les actions sont réalisées. Il faudra également en donner une ou plusieurs solutions permettant de limiter ce type d'attaques.

Les implémentations devront se faire aussi bien sur Linux que sur Windows. Le langage pour programmer ces attaques est laissé libre au choix du programmeur. Il faudra bien préciser les outils ainsi que leur version. Dans une large mesure il faudra travailler dans des machines virtuelles afin de faire les différents tests.

FIGURE 1– Logo de l'École

1.2 CONTEXTE EN 2016-2017

La sécurité informatique est de plus en plus médiatisée. Les derniers événements ultra médiatisés en 2016

Élections présidentielle USA : la possible cyberattaque perpétrée aux États-unis qui a rendu publique des e-mails confidentiels d'Hilary Clinton (qui a perdu l'élection présidentielle face à Donald Trump). Son directeur de campagne aurait répondu bien malgré lui à un e-mail frauduleux qui a permit à des hackers d'accéder à des centaines d'e-mails.

Les comptes piratés sur des sites très importants comme Yahoo (attaque de 2014 médiatisée en 2016), Linkedin, Dropbox, Twitter, DaylyMotion ...

Sécurité des objets connectés : les attaques réalisées par une vulnérabilité d'objets connectés. En septembre 2016, OVH a ainsi subi des perturbations suite à des attaques venant d'objets connectés. En octobre 2016, cela a permis a des personnes mal attentionnées d'attaquer le site "DYN" qui gère les noms DNS de plusieurs sites Internet aux USA. Certains sites ont été inaccessibles durant une journée (Amazon, CNN, Ebay, Netflix, Twitter, Spotify,...).

1.3 LES ATTAQUES

Le livre "Sécurité informatique Ethical Hacking" [1] décrit de nombreux types d'attaques possibles :

Attaques exploitant les failles humaines par exemple pour obtenir des informations sur une entreprise en se faisant passer pour un fournisseur ou client(directement sur place ou par téléphone)

Collecte d'informations : utiliser des outils et réseaux sociaux pour récupérer le maximum d'information sur une entreprise. Ceci avant de procéder éventuellement à une attaque plus intrusive. Si on connaît le nom des administrateurs réseaux et des dirigeants d'une entreprise, cela peut faciliter une attaque.

Les failles physiques exploitant des outils (logiciels ou CD/clé USB avec système bootable comme "Hiren's Bott CD") afin de s'authentifier sur un poste auquel on a accès physiquement.Exemples : outil de cassage de mot de passe "John The Ripper", OPHCRACK , ou logiciel de contournement d'authentification (KON-BOOT).

Les failles réseaux qui vont être détaillées dans ce rapport : "Man In The Middle"(MITM), vol de session TCP (hijacking), Usurpation d'adresse IP (spoofing d'IP).

Les failles réseaux spécifiques au WIFI comme le crackage de clé WEP ou WPA avec des outils comme airodump et aircrack présents dans la distribution Kali Linux (CD bootable).

Attaques sur la téléphonie su IP .

Attaques sur le Cloud Computing : cassage de clé pour casser les système d'authentification sur des solutions de cloud.

Les failles Web : exploiter les failles des serveurs web (faille de moins en moins exploitées car les serveurs web comme apache, nginx ou IIS sont de mieux en mieux protégés) ou des failles sur les sites web (injections SQL, de script JavaScript, de contournement des CATCHA ...).

Les failles Système : exploiter les faille du système d'exploitation ou de l'hyperviseur de virtualisation pour contourner les systèmes de sécurité (authentification ou droits d'accès).

Les failles applicatives

Ce document, tout comme l'article "Attaques des réseaux" des Techniques de l'Ingénieur [7] , présente tout d'abord les possibilités d'un attaquant pour cartographier le réseaux une fois qu'il peut y installer une sonde (donc il a accès physiquement ou à distance au réseaux attaqué). Ensuite sera présenté des attaques permettant d'écouter le réseaux afin d'obtenir des informations supplémentaires (login, mot de passe ...). Ce document terminera par un panel d'opérations permettant de perturber certains services pour gêner le bon fonctionnement du réseau (en provoquant ce qu'on appelle un Déni de Service).

2. CARTOGRAPHIE DU RÉSEAU INFORMATIQUE

Si un attaquant arrive à prendre le contrôle d'un poste informatique ou arrive à brancher son propre ordinateur dans le réseau d'une entreprise, il va chercher à connaître les différents services installés sur le réseau. Il existe de nombreuses possibilités pour cartographier le réseau informatique, c'est à dire recréer le plan du réseau avec le maximum d'information sur les adresses IP, les serveurs et leur rôle, les routeurs et si possible les connexions VPN avec d'autres sites.

2.1 RÉCUPÉRER LES INFORMATIONS DU POSTE

Il faut commencer par récupérer les informations du poste d'attaque.

ipconfig (Linux) ou ifconfig(Windows) pour obtenir l'adresse IP du poste.

arp -a pour lister les adresses MAC présentes actuellement dans le cache ARP du poste. cf [8]. exemple (sous Linux mais fonctionne aussi sous Windows) : arp -a ? (192.168.0.254) at 68 :a3 :78 :7c :4b :58 [ether] on eth0 ? (192.168.0.35) at 00 :d0 :b8 :20 :fb :aa [ether] on eth0

route -n(Linux en root) ou netstat -nr(Linux) ou route print (Windows) permet d'afficher les routes configurés sur le poste et ainsi de récupérer la passerelle par défaut. Exemple : netstat -nr Table de routage IP du noyau Destination Passerelle Genmask Indic MSS Fenêtre irtt Iface 0.0.0.0 192.168.0.254 0.0.0.0 UG 0 0 0 wlan0 192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0

nslookup ou dig pour connaître l'adresse du ou des serveurs DNS. Sous linux, on peut également visualiser le contenu du fichier /etc/resolv.conf. On peut également utiliser la commande hostname pour connaître le nom du poste (Linux et Windows).

2.2 REQUÊTE ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

ICMP est utilisé par exemple pour "pinguer" les postes du réseau auquel appartient le poste et éventuellement les réseaux connexes.

2.2.1 Avantages

Les routeurs sont souvent configurés pour laisser passer le protocole ICMP (mais certains le bloquent).

La commande ping présente sur beaucoup de systèmes y compris les switchs ou routeurs manageables.

Possibilité d'écrire un script pour pinguer tous les postes d'un réseau.

Non détecté par la plupart des systèmes.

2.2.2 Inconvénients

N'obtient pas de détails sur les postes allumés mais uniquement leur adresse IP.

Ne scanne pas tout le réseau (notamment s'il y a des sous-réseau séparés par des routeurs).

2.2.3 Requête ICMP de découverte de routeurs

D'après [7], il est possible d'obtenir des informations des routeurs d'un réseau en émettant des requêtes de découverte de routeur (ICMP router discovery) ou des requêtes de protocoles de routage (OSPF, BGP...).

2.2.4 Requête ICMP traceroute(Linux) ou tracert(Windows

La commande **traceroute** envoie des paquets avec des champs TTL différents afin de déterminer les routeurs traversés pour une cible donnée. Les chemins pouvant être différents, il est parfois utile de lancer plusieurs fois la commande pour connaître tous les routeurs susceptibles d'être traversés. Exemple :

traceroute to google.fr (216.58.209.227), 30 hops max, 60 byte packets

1 192.168.0.254 (192.168.0.254) 1.046 ms 1.484 ms 2.207 ms

2 bre29-3-78-223-34-254.fbx.proxad.net (78.223.34.254) 28.054 ms 28.066 ms 28.068 ms

On voit ci dessus que le deuxième routeur est un routeur du Fournisseur d'Accès à Internet (F.A.I.). Une seul routeur semble être local au réseau de l'entreprise (192.168.0.254) pour atteindre Internet.

2.3 Scanner (balayer) les ports

Un attaquant pourra effectuer un balayage (scan) de plusieurs ports sur chaque IP du réseau. Pour cela, il faut utiliser des outils qui envoient un paquet SYN vers une adresse IP cible sur un port cible. Si le port est ouvert, le service sur le poste cible répond par un SYN,ACK (en TCP).

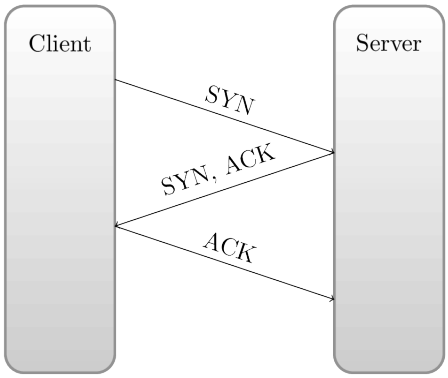

Figure 2– Poignée de main connexion TCP.

Schéma inspiré de [12].

2.3.1 nmap ou application graphique zenmap (Linux)

la commande nmap permet de scanner les ports d'une ou plusieurs machines. Pour plus de facilité, il est possible d'utiliser zenmap qui est dotée d'une interface graphique.

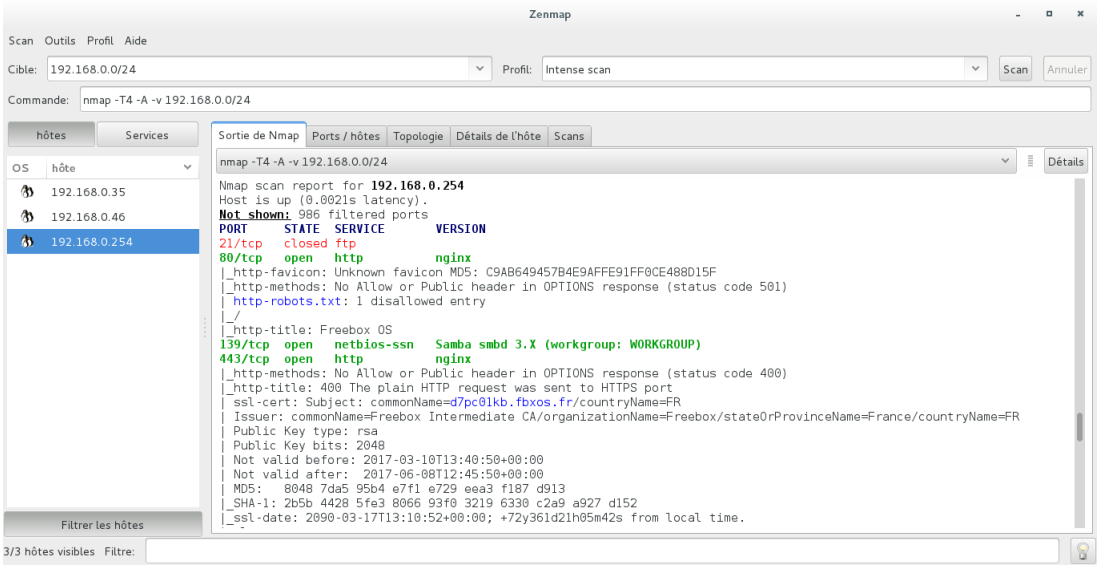

FIGURE 3– Zenmap

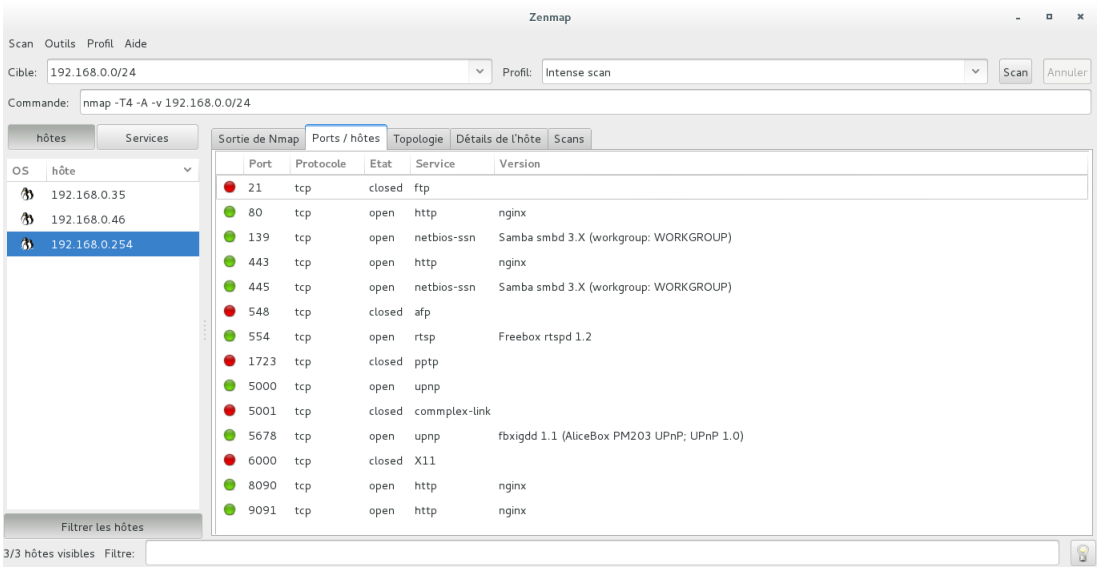

FIGURE 4– Zenmap : exemple de ports ouverts sur une freebox.

2.3.2 Outil scan réseau avancé

A ma connaissance, nmap permet de scanner le réseau à un instant T mais si un équipement n'est pas actif. Il faudrait relancer, par script ou à la main, plusieurs fois nmap pour fiabiliser la recherche d'équipements actifs.

Il existe des outils qui scannent en permanence le réseau pour réaliser cela. Par exemple, l'outil **look@Lan** sous windows envoie continuellement des requêtes ICMP et permet de découvrir des postes qui ne sont pas tout le temps allumés.

Un outil comme **The dude**, lui cartographie le réseau (et permet d'avoir automatiquement un plan graphique du réseau) à un instant T mais ensuite affiche un état des liens réseau de façon dynamique (on sait si un lien est ON ou OFF). Plusieurs autres outils sont listés dans le site internet [13].

2.3.3 Contre-mesures

Installer un IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System). Un IDS peut repérer un scan de port réseaux.

3. ECOUTE DU RÉSEAU

3.1 SNIFFERS RÉSEAU

Si l'attaquant se trouve dans le réseau, il peut mettre en place un système d'écoute du réseau. Pour cela il est possible d'utiliser des logiciel "renifleurs" ("sniffer" en anglais). Ces logiciels écoutent tous les paquets qui arrivent sur la carte réseau et offrent la possibilité de voir passer les mots de passes pour les protocoles qui ne sont pas sécurisés (par exemple FTP).

Par exemple les logiciels "tcpdump", "wireshark", "dsniff" qui comprend des logiciels pour "renifler" les mots de passe de certains protocoles, "ngrep", "etherape" (pour avoir un aperçu graphique des protocoles utililisés sur le réseau), Ettercap (qui contient en plus des outils d'attaques). Un logiciel comme "cain-abel" [9] permet même de capturer des mot de passe (en essayant de les craker s'ils sont chiffrés ce qui en fait un outil "actif"), il permet également d'enregistrer des conversations VoIP."KisMAC" et "KissMet" plus spécifique à la découverte des réseau WIFI.

3.2 CONTRE MESURES

L'écoute passive comme expliquée ci dessus ne permet pas de capturer tous les paquets circulant sur le réseau à-moins que l'attaquant ne réussisse à se brancher sur un hub auquel cas il pourra analyser tous les paquets qui circulent sur cet hub. Il est donc impératif de ne plus avoir de Hub dans le réseau mais uniquement des switchs (c'est souvent le cas , les hub n'existent plus en 2017 à part si une personne malveillante en installe).

De plus, il est possible de modifier le comportement d'un switch mannageable pour créer un port miroir (mirroring en anglais). Ce port miroir recopie tout le trafic d'un autre port. Il est donc impératif de bien sécuriser l'accès administrateur de tous les switchs (au minimum changer leur mot de passe par défaut).

Enfin, il faut privilégier les protocoles sécurisés comme SSH plutôt que telnet ou ftp. Avec des logiciel actif comme cain-abel, il vaut mieux utiliser des mots de passe complexes. L'Agence Nationale de la Sécurité de Systèmes d'Information (ANSSI) propose dans le document [3] l'utilisation de la méthode des premières lettres et indique : "Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A"

4. TRAVERSÉE DE ROUTEUR

L'attaquant n'a pas toujours la possibilité d'installer son propre matériel sur le site visé. Il a parfois recours à une attaque pour s'introduire sur le site. L'attaquant a également besoin de récupérer les informations récoltés ou de prendre la main à distance, une fois qu'il s'est introduit une fois sur le réseau d'une entreprise.

Un des problèmes pour un attaquant est de traverser les routeurs afin d'explorer et de cartographier l'ensemble du réseau. La méthode la plus efficace est d'aller sur place installer un mouchard mais une intrusion physique n'est pas toujours discrète. Le document [7] de Techniques de l'Ingénieur indique quelques méthodes possibles pour traverser un routeur équipé de pare-feu. La partie "routeur" redirige des paquets d'une interface à l'autre, la partie "pare-feu" est chargé de bloquer les paquets indésirables comme une attaque venant de l'extérieur par exemple (mais pouvant aussi bloquer des flux venant de l'intérieur). Le pare-feu est censé bloquer les paquets avec le drapeau (flag) SYN à 1 et ACK à 0 (paquet venant de l'extérieur avec une demande de connexion TCP). Schéma importé du site

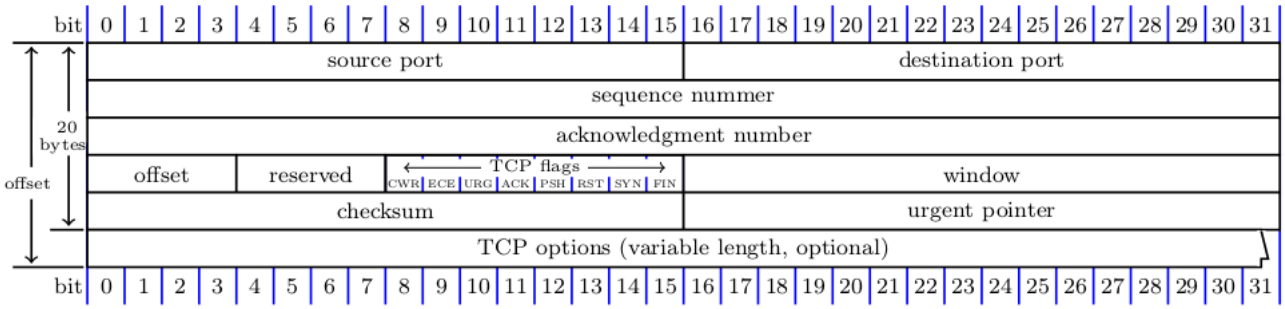

FIGURE 5– En-tête (header) du protocole TCP.

[12].

Exploiter un pare-feu peu performant uniquement basé sur les ports Le document [7] indique que certains routeur/pare-feu ne s'occupent que de regarder le port extérieur d'un paquet pour décider s'il le laisse passer ou pas. Dans ce cas il est possible d'émettre un paquet de l'extérieur à destination du réseau vers un serveur accessible. Par exemple un serveur de mail qui accepterait tout paquet provenant du port 25 d'un serveur externe.

Exploiter un pare-feu peu performant qui laisse passe les paquets SYN ACK A part pour certains serveurs internes, les routeurs pare-feu bloquent généralement les paquets venant du WAN avec le FLAG SYN (sans ACK) car cela signifie que c'est une demande de connexion de l'extérieur et non une réponse. L'idée est donc d'essayer d'envoyer un paquet à destination d'un serveur interne en demandant un SYN et en y ajoutant un ACK. Ce ACK ne correspond pas vraiment à un accusé puisqu'il n'y a pas eu réception. Sur certains systèmes le ACK ne sera pas compris mais le SYN aura tout de même sa réponse !

Fragmenter les paquets . Laurent LEVIER explique dans [7] et [8] 2 méthodes de fragmentation : elles sont également détaillés dans le document [2].

fragmentation par petits paquets (tiny fragments) qui consiste à envoyer un premier paquet avec les informations sur le port source et destination mais sans SYN ni ACK. Le pare-feu ne bloque pas ce paquet et en fera de même pour les suivants. Le 2eme paquet, lui, contiendra le SYN sans le ACK pour une demande de connexion. Les routeurs et pare feu actuels sont normalement parés contre cette attaque.

fragmentation par chevauchement idem à une fragmentation par petit paquets si ce n'est que le "offset" du 2ème paquet sera le même que le 1er et les donnée du 2ème paquet vont donc écraser celle du 1er paquet, ceci afin de berner les pare-feu.

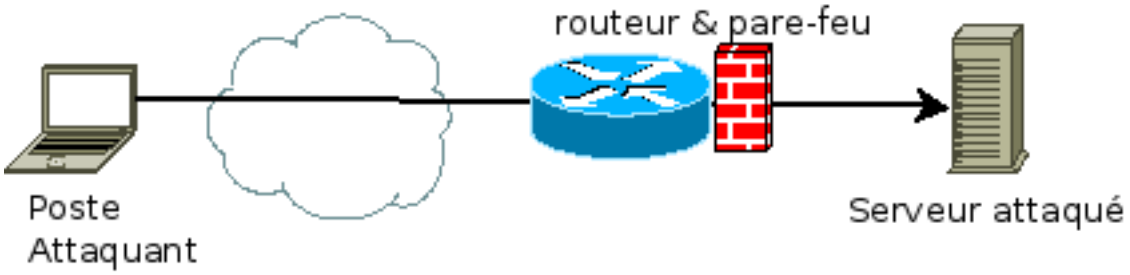

FIGURE 6– Traversée de routeur pare-feu

Paquet IP	
Fragment 0	Fragment 1
Auncun indicateur SYN ou ACK	Indicateur de connexion SYN sans ACK

TABLE 1– Chevauchements de fragments

4.0.1 Contre-mesures

Mise à jour régulière ou automatique des routeurs et pare-feu. Installer un IDS (Intrusion Detection System) comme "SNORT" qui est un NIDS (Network Intrusion Detection System) installable sous Windows ou Linux.

4.1 INSTALLER UN SYSTÈME DE PRISE DE CONTRÔLE À DISTANCE

Si l'attaquant arrive à s'introduire physiquement ou par traversée de routeur comme indiqué au chpitre précédent, il est amené à récolté des informations et à récupérer ces informations. le chapitre 6 faille réseau paragraphe 3.4 de [1] indique 2 méthodes pour prendre la main sur un hôte distant :

netcat nc, commande installable sous Windows ou Linux, permet de créer un serveur netcat sur le poste attaqué et un client sur le poste attaquant. nc permet d'exécuter des commande à distance et aussi de transférer des fichiers. nc permet de faire un bond par un serveur de la zone démilitarisée d'un réseau pour atteindre un poste du réseau privé (en installant nc sur chaque machine). Cryptcat est un clone de netcat avec des options de chiffrage.

ssh ssh permet d'établir une connexion sécurisée entre un client et un serveur. Openssh est installable sous windows et Linux. Un client SSH sous Windows est putty.

5. MAN IN THE MIDDLE (MITM)

Tous les documents traitants d'attaques réseaux décrivent l'attaque MITM. Lors d'une communication entre un poste A et un poste B, l'attaquant va essayer de capturer le maximum de flux qui transite entre A et B en se positionnant au milieu ("Middle"). Une bonne attaque MITM est telle que A et B communiquent très bien sans savoir que leur communication est capturée par l'attaquant qui capture les paquets venant de A et les redirige vers B. L'attaquant peut éventuellement modifier les paquets capturés.

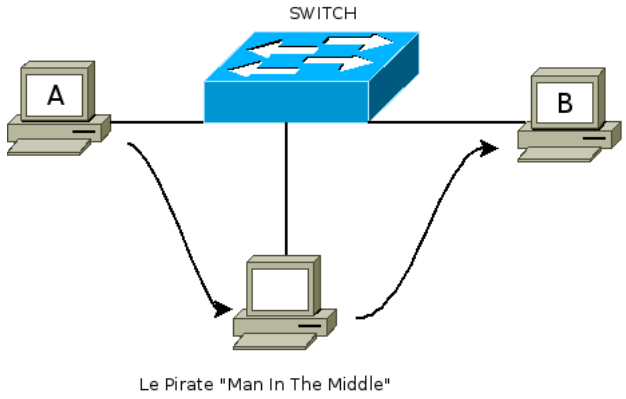

FIGURE 7– Exemple d'attaque Man In The Middle.

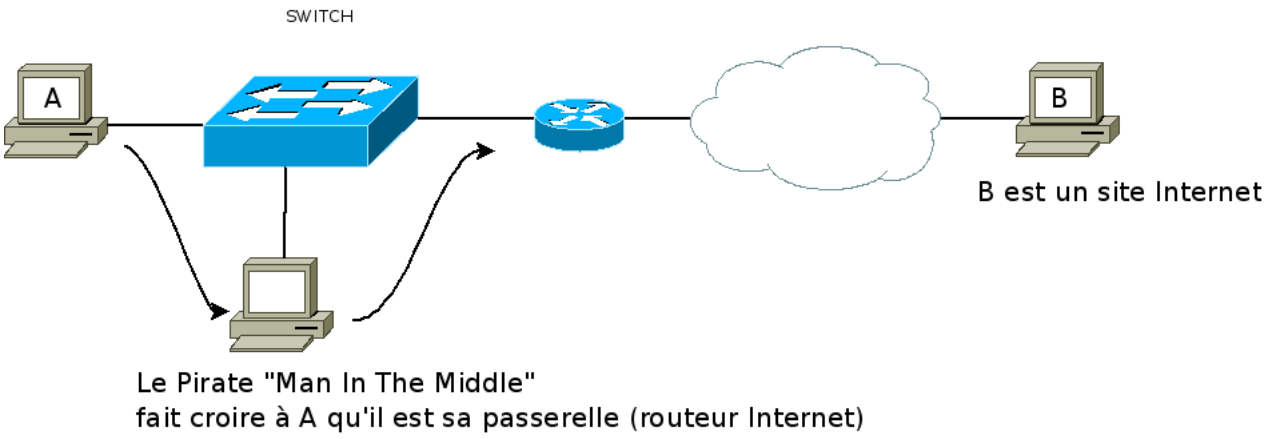

FIGURE 8– Exemple d'attaque Man In The Middle.

5.1 ARP POISONING (EMPOISONNEMENT) OU ARP SPOOFING (USURPATION)

5.1.1 Méthodes

L'attaque ARP poisoning permet une attaque MITM en perturbant les caches ARP des postes et la table ARP du switch. Pour cela on peut utiliser des logiciels come scapy (logiciel permettant de créer des trames avec des fausses information comme une fausse adresse MAC ou IP), arpoison, ARPSpoof, nemesis ou ethercap. L'idée est de modifier

le cache ARP de A pour lui faire croire que B (ou la passerelle pour le 2eme schéma) a pour adresse MAC celle de l'attaquant. Comme cela A mettra comme adresse MAC de destination l'adresse MAC de l'attaquant . Le switch redirigera donc tous les paquets vers l'attaquant. Il faut également effectuer une opération sur l'attaquant pour ensuite rediriger les paquets vers B (après les avoir capturés pour les analyser). On peut éventuellement en faire de même pour les réponses de B vers A pour les rediriger vers l'attaquant.

L'article de linuxfocus [2] explique l'utilisation de "ARPSpoof" dans le paragraphe "ARP Spoofing".

Le livre "Sécurité Informatique Ehical Hacking" [1], indique la démarche avec l'outil "Ettercap" sous Linux page 338. Ce livre page 346 propose d'utiliser le logiciel Cain & Abel [9] sous Windows qui contient de nombreux outils dont un pour de l'ARP poisoning.

Le livre "Techniques de Hacking" [4] page 250 détaille l'utilisation de script bash avec le logiciel nemesis ainsi que des explications sur le logiciel arpspoof (fourni avec dsniff).

5.1.2 Contre-mesures

Arpwatch : Sur un réseau, il faut éviter qu'un attaquant se fasse passer pour la passerelle car un flux important passe par la passerelle. Si la passerelle est sous Linux, il est possible d'installer l'utilitaire arpwatch qui repère l'ARP poisoning. Son utilisation est détaillée dans le document [10]. On peut aussi intaller arpwatch sur d'autres postes Linux qui peuvent être attaqués également. arpwach offre la possibilité d'envoyer un email en cas de changement de cache ARP suspect.

Adresse MAC statique : Le cache arp sur les postes réagit dynamiquement en fonction des réponses arp qu'il reçoit. Il est possible d'indiquer un couple "adresse MAC"-"adresse IP" statique dans le cache arp. Cela est possible Sous Windows, Linux ou même CISCO. Par exemple sous Windows et Linux : arp -s 192.168.0.254 00-0C-29-1F-62-43 . Cela peut être intéressant pour la passerelle et les serveurs. Pour des petits réseaux, on peut même imaginer inscrire les adresses MAC de tous les postes de façons statiques (éventuellement modifiable par un script de démarrage de poste) : cela aurait en plus de la sécurité l'avantage de diminuer le trafic ARP. Par contre, cela peut poser des problème lors d'évolution/changement d'éléments du réseau comme le changement de passerelle. Sur des gros réseau cela est rarement faisable.

Utiliser des protocoles sécurisés : utiliser ssh V2 plutôt que telnet ou ftp. Comme cela, même si un pirate réussit à créer une attaque ARP poisoning, il ne pourra pas capturer les login/mots de passe. Remarque : ssh V1 comporte des failles de sécurité, il faut installer la ssh V2 et vérifier que la V1 n'est pas disponible. (voir configuration ssh ici `http://virologie.free.fr/documents/openSSH/ssh_configurations.html`)

IPv6 Utiliser uniquement IPv6 qui n'utilise pas ARP. En général, les 64 bits de l'adresse IPV6 sont construits à partir de l'adresse MAC donc on ne peut pas dissocier aussi facilement adresse IPv6 et adresse MAC qu'en IPv4.

Dynamic ARP Inspection Le document [10] indique que certains switch, notamment certains switch Juniper, disposent d'un mécanisme appelé Dynamic ARP Inspection (DAI). Ce mécanisme réduit les problèmes d'ARP poisoning en analysant les baux

DHCP et en repérant les requêtes ARP venant de port non fiable une IP qui n'aurait pas préalablement obtenu une adresse IP du serveur DHCP ne peut pas émettre de requête ARP.

pare-feu activé et à jour : Le logiciels pare-feu des postes et serveurs peuvent bloquer au moins le scan de ports.

5.2 Corruption de DNS (DNS spoofing)

Les documents [2] et [6] expliquent 2 méthodes pour perturber le cache DNS d'un poste : l'usurpation d'identifiant DNS ("DNS ID spoofing") et l'empoisonnement du cache DNS ("DNS cache poisoning"). Remarque, sous Windows : la commande ipconfig /displaydns affiche le cache DNS.

5.2.1 DNS ID Spoofing

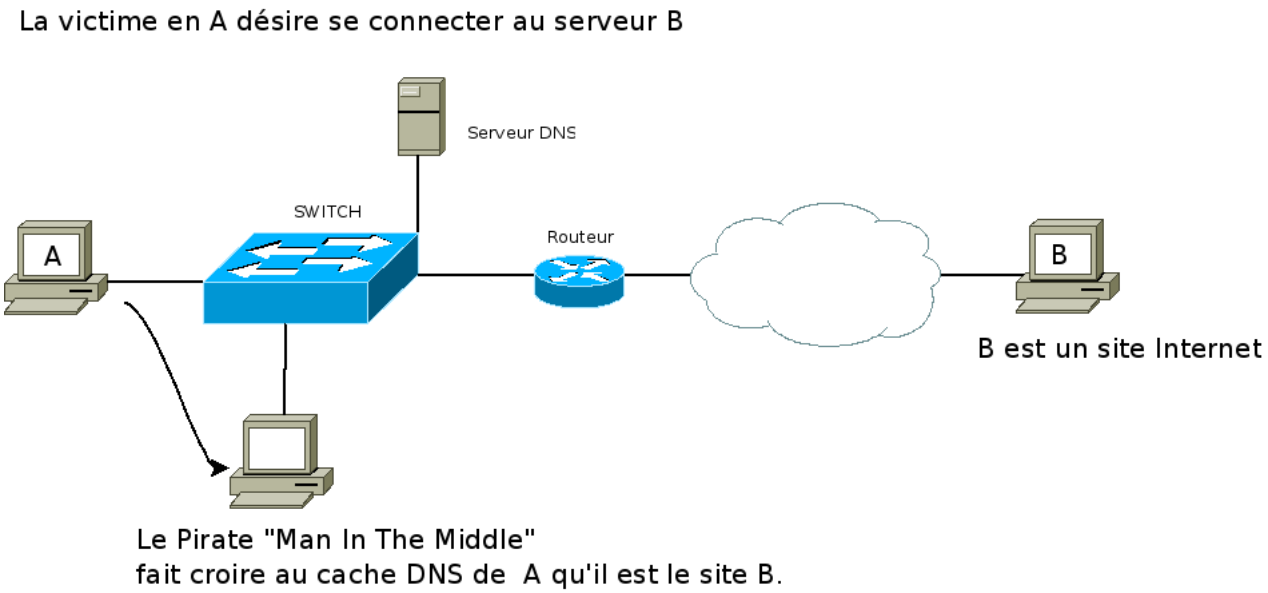

FIGURE 9– Exemple d'attaque MITM par DNS spoofing

Le pirate désire se faire passer pour le serveur B. Tout d'abord, il crée une copie du serveur B (par exemple la page de connexion du serveur Web se trouvant sur B).

Ensuite, le pirate effectue une attaque de type DNS ID SPOOFING pour que la victime A qui va se connecter au serveur B se connecte, sans le savoir, à la copie de B sur le poste du pirate.

Il est possible de générer des réponses DNS, soit pour empoisonner le cache du serveur DNS, soit pour empoisonner le cache DNS du poste A (voir exemple figure ci dessous).

La difficulté du pirate est de répondre plus vite que le serveur DNS et avec le bon ID présent dans la requête. Donc il faut capturer la requête DNS et répondre plus vite que le vrai serveur DNS.

Une autre difficulté est qu'il faut voir passer la requête DNS de la victime, ce qui selon moi rend cette attaque peu exploitable.

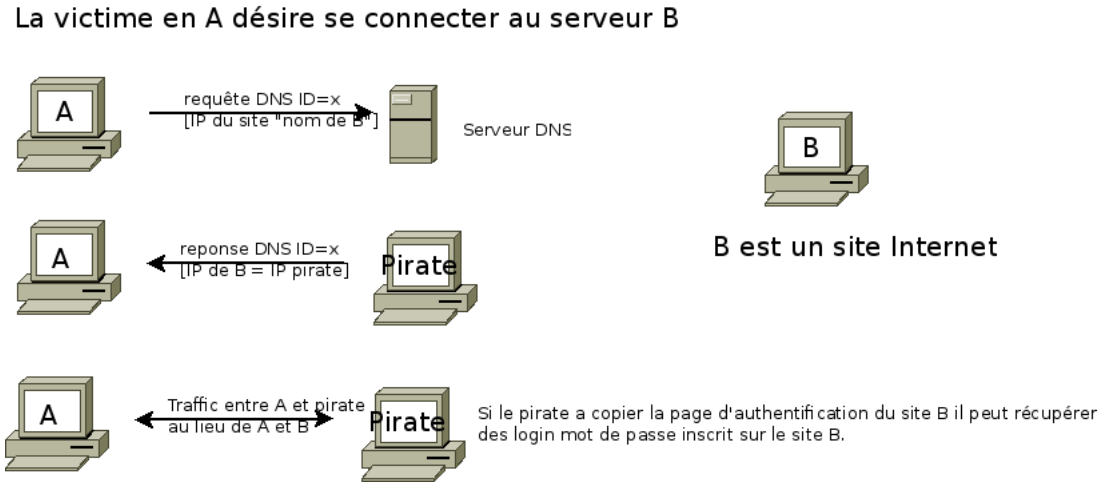

FIGURE 10– Méthode attaque DNS

5.2.2 DNS cache poisoning

Pour réaliser cette attaque, l'attaquant doit avoir son propre serveur DNS. Disons que le nom de domaine de l'ataquant est attaque.com .

L'attaquant envoie une requête DNS au serveur DNS de la victime. Cette requête concerne son propre domaine. Le serveur DNS de la victime va donc faire une demande de résolution DNS au DNS de l'attaquant.

L'attaque consiste à faire une réponse DNS en y rajoutant des données falsifiées qui vont permettre à l'attaquant de rediriger des victimes uilisant le serveur DNS de la victime vers ses propres serveurs sans qu'ils le sachent.

C'est en fait le cache du serveur DNS de la victime qui est empoisonnée.

5.2.3 Contre-mesures DNS Spoofing

Configurer le serveur DNS du réseau local pour qu'il ne resolve directement que les noms de machines du réseau sur lequel il a autorité. Suivre les documents officiels sur la sécurité DNS comme par exemple le document du CERT (Computer Emergency Response Teams) "Securing an Internet Name Server" `http://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_52496.pdf`.

Par exemple sous Windows, suivre le document `http://blog.alphorm.com/howto-desacti` pour désactiver le cache DNS côté client (commande "Net stop DNSCache") et serveur (commande "SC Config DNSCache start= disabled").

6. ATTAQUES IP ET SESSION TCP

6.1 USURPATION (SPOOFING) D'ADRESSE IP (INTERNET PROTOCOL)

6.1.1 Méthodes

La méthode ressemble à du TCP Session Hijacking. L'idée est de créer une connexion TCP sur un serveur mais en envoyant un paquet SYN avec une fausse adresse IP (d'où le

terme IP spoofing). Pour cela, il est possible d'utiliser le logiciel "python-scapy" dans son propore script python afin d'envoyer des paquets avec une fausse IP source. Du coup on ne recevra pas les réponses du serveur mais on aura réussi à créer une connexion sans se faire voir. Ensuite on peut envoyer des commande par telnet même si on ne voit pas le résultat, les commandes sont effectuées. Le gros avantage est ici de ne pas se faire repérer.

6.2 Détournement de session TCP (TCP Session Hijacking)

Comme indiqué dans le livre "Sécurité Informatique Ehical Hacking" [1] page 348, plutôt que d'esssayer de "renifler" (sniff) login et mot de passe, il est intéressant de détourner une session TCP qui a déjà été initialisée. Par exemple une connexion telnet ou rlogin.

6.2.1 Repérer et imiter les numéros de ACK et SEQ pour prendre la main sur une connexion établie

L'établissement d'une session TCP entre un client A et un serveur B se fait par la poignée de main TCP en 3 temps (three handshake). Remarque : Le ACK, numéro d'accusé de réception (32 bits), correspond au numéro (d'ordre) du prochain segment attendu (d'où le "+1")

Le client A envoie une demande de connexion (SYN) avec un numéro de séquence que l'on appelera "SEQ-A"

Le serveur B répond avec un paquet (SYN+ACK). SYN est la réponse à la demande de connexion avec son numéro de séquence SEQ-B. ACK est l'accusé de réception pour le paquet du client et contient donc "SEQ-A + 1".

le client A répond avec un paquet (ACK) qui correspond à l'accusé de réception du paquet envoyé par B et contient donc "SEQ-B +1".

6.2.2 Méthodes

L'attaquant qui a reniflé la poignée de main TCP et repère les ACK et les SEQ peut créer un paquet avec les bons ACK et SEQ pour prendre la place de A qui lui, ne pourra plus communiquer car il aura un problème de ACK/SEQ.

Pour créer ce paquet, on peut utiliser le logiciel shijack [11] qui est un petit programme en C. Pour l'utiliser : ./shijack interface ipclient port-client ipserveur port-serveur

Il y a des logiciels plus simples comme HUNT, HJKSUITE, P.A.T.H. et Juggernaut.

Le livre "Techniques de Hacking" [4] page 270 détaille l'utilisation de rst-hijack pour injecter un paquet RST (ReSeT) pour réinitialiser une connexion et ainsi prendre la place du client A.

6.3 Contre-mesures

Ces attaques ne fonctionnent pas avec des protocoles sécurisés comme sshV2. Il ne faut pas utiliser ftp, telnet ou rlogin.

7. ATTAQUES DOS (DENY OF SERVICE)

Attaques par envoi massif de paquets réseau pour réaliser un déni de service (flooding for Deny Of Service) Le document "Protection contre les attaques de déni de service dans les réseaux IP" [5] décrit l'historique, les différente attaques DOS et DDOS ainsi que les contre-mesures pour essayer de les éviter. Ces attaques ont pour but de perturber les services des serveurs en les inondant de paquets réseaux ou en exploitant une faille dans ces services. Ces attaques sont souvent réalisées depuis Internet mais peuvent également être lancées à l'intérieur d'un réseau si le pirate y a accès. L'objectif n'est pas de voler ou détruire des informations mais d'empêcher au maximum l'accès à des serveurs ce qui peut nuire fortement à l'entreprise visée.

7.1 DOS

De très nombreuses méthodes permettent d'arriver à un DoS :

SYN flood : inondation de paquets TCP SYN à destination d'un serveur pour atteindre le maximum de connexions ouvertes possible et ainsi le faire tomber (ou ralentir).

UDP flood : inondation de datagrammes UDP à destination d'un serveur pour le faire tomber (ou ralentir). Les datagrammes UDP n'ont pas de mécanisme de contrôle de gestion donc sont souvent prioritaires par rapport aux flux TCP. Une inondation de datagrammes UDP peut faire tomber le réseau.

ping of death : envoi de paquets ICMP (protocole utilisé par la commande ping) volumineux pour attaquer des systèmes dont la pile TCP/IP n'est pas protégée (ancienne attaque)

smurfing Envoi de ping en grand nombre (en brodcast à destination de nombreux postes) et tous ont comme IP source le poste attaqué qui sera inondé de réponses à ces ping.

bombes email : envoi de mails volumineux.

Il existe plusieurs outils pour réaliser ce genre d'attaques : Hping, Slowloris, NKiller, Let-Down, Sockstress... On peut également développer ses propres outils en utilisant la libraire "scapy" sous python qui permet de créer des paquets en manipulant leurs en-têtes.

7.2 DDOS

DDOS pour Distributed Denial Of Service attack. Les serveurs sont de plus en plus sécurisés et de plus en plus puissants pour palier à l'attaque d'un seul poste. Les attaques DOS se font désormais de façon distribuée afin d'inonder encore plus de paquets le serveur visé. Certains pirates ont par exemple réussi à utiliser des objets connectés pour réaliser une attaque DDOS sur les serveurs DNS de DYN en octobre 2016. Cela a paralysé de nombreux sites Internet aux USA. Il existe plusieurs outils permettant une attaque DDOS comme Trinoo (UDP flooding) , Tribe Flood Network (TFN) et TFN2k , Stacheldraht (UDP/TCP/TCP SYN flooding, Smurf) , Schaft (UDP/TCP/ICMP flooding) MStreamT (ACK fooding)

7.3 CONTRE-MESURE

Mise à jour des systèmes , des logiciels serveurs. Un serveur apache récent a plus de contre-mesure déjà intégré qu'une vieille version.

Pare-feu avoir un pare-feu réseau pour bloquer les attaques et aussi des pare-feu Logiciel à jour sur les serveurs.

IDS Système de détection d'intrusion par qui le flux réseau doit passer. L'IDS est capable de repérer des attaques DOS connues . Il faut donc lui aussi le mettre à jour si on veut qu'il soit performant. Exemple : le logiciel SNORT.

IPS Système de prévention d'intrusion qui analyse le comportement des applications du réseau et qui est capable de bloquer des comportements jugés suspects. Plus délicat à mettre en place que les IDS car un IPS peut éventuellement bloquer des flux réseaux qui en fait fait ne sont pas des attaques. Exemple : le logiciel SNORT avec "SNORT inline".

SYN Cookie à activer pour le serveur ne conservent pas les données de connexion mais les renvoie au cleient qui les renverra. Cela permet au serveur de moins saturer sa mémoire.

SYN Cache serveurs freebsd qui limitent la taille des données conservés par les serveurs en utilisant une table de hachage.

SYN Proxy par exemple installé sur le pare feu de l'entreprise : le SYN proxy se charge du threhand shke TCP à la place du serveur et ensuite le client accède au serveur.

8. CONCLUSION

Les attaques réseau en interne sont source d'attaques possibles avec des moyens relativement failes : un poste ou un accès à un poste suffit pour réaliser une attaque Man In The Middle par exemple. Il est important de privilégier des protocoles sécurisés et de ne pas installer de serveurs comme les serveurs FTP, telnet ou ssh V1 qui ne résiste pas à une attaque bien menée.

Concernant les attaques à distance à grande échelle, il est difficile de trouver un système qui permet de résister à une attaques venant de milliers de postes et générant ainsi des Gigabits de données qui arrivent dans un laps de temps très court. Et ce malgré la fait que les serveurs sont de plus en plus sécurisés et comportent de moins en moins de bugs. Il y a tellement de données qui arrive que c'est le réseau qui tombe. Des personnes de l'hébergeur OVH nous ont présenté leur nouveau système de détection d'intrusion (et de destruction des paquets malveillants). Il y a tellement de paquets à traiter qu'ils ne peuvent analyser que les paquets SYN et sont en train de développer leur propre solution à l'aide de cart FPGA capable d'effectuer beaucoup de calculs en parallèle.

La sécurité des systèmes nécessite une prévention accrue avec notamment l'installation systématique des mises à jours , de systèmes de détection d'intrusion et également par des tests d'intrusions.

Références

[1] Marion AGE, Robert CROCFER, Nicolas CROCFER, David DUMAS, Franck EBEL, Guillaume FORTUNATO, Jerome HENNECART, Sebastien LASSON et Laurent SCHALKWIJK : *Sécurité informatique, Ethical Haking, Apprendre l'attaque pour mieux se défendre*. Editions eni, 2015.

[2] Eric DETOISIEN : Les attaques externes. *Linuxfocus*, 2003. Available at `https://www.ibiblio.org/pub/Linux/docs/linux-doc-project/linuxfocus/Francais/Archives/lf-2003_03-0282.pdf`.

[3] CERT Fr Division assistance TECHNIQUE : Recommandations de sécurité relatives aux mots de passe, •. Available at `https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf`.

[4] Jon ERICKSON : *Techniques de Hacking*. Pearson, 2008.

[5] Marion HOTTE, Quentin Edouard LUTUN et Thomas ASCOET : Protection contre les attaques de déni de service dans les réseaux ip - snort. Available at `http://www.mi.parisdescartes.fr/~osalem/Projects/Hotte_LUTUN_ASCOET.pdf`.

[6] Philippe LATU et Alexandre VIARDIN : Un petit guide pour la sécurité, 2014. Available at `https://www.inetdoc.net/guides/tutoriel-secu/`.

[7] Laurent LEVIER : Attaques des réseaux. Rapport technique H5830 V1, Techniques de l'Ingénieur, avril 2005. Technologies de l'information | Sécurité des systèmes d'information.

[8] Laurent LEVIER : Attaques des systèmes - identifier les faiblesses du bastion. Rapport technique H5832, Techniques de l'Ingénieur, avril 2005. Technologies de l'information | Sécurité des systèmes d'information.

[9] MAO@OXID.IT : Cain-abel, 2014. Available at `http://www.oxid.it`.

[10] Guillaume PILLOT : Projet 8inf206 : Sécurité réseau informatique attaque de l'homme du milieu (mitm), 2012. Available at `http://www.guillaume-pillot.ca/static/fichier/projet_mitm_guillaume_pillot.pdf`.

[11] SPWNY : Shijack, •. Available at `http://www.securiteam.com/tools/5QP0P0K40M.html`.

[12] TABASCOEYE : Diagrams for latex using tikz, •. Available at `https://github.com/tabascoeye/TikZ-diagrams`.

[13] • : Site de téléchagement de logiciels réseau, •. Available at `http://www.commentcamarche.net/download/reseau-70`.

Technopôle Brest-Iroise
CS 83818
29238 Brest Cedex 3
France
+33 (0)2 29 00 11 11
www.telecom-bretagne.eu

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom