INFORMATIQUE
TECHNIQUE

Expert

Réseaux informatiques

Guide pratique pour l'administration et la supervision

En téléchargement

Exemples de captures de trames réseau

+ QUIZ

Version numérique **OFFERTE !**
www.editions-eni.fr

Pierre CABANTOUS

eni

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
http://www.editions-eni.fr
Saisissez la référence ENI de l'ouvrage **EIRESAS** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

1. Introduction 11
2. Public concerné et démarche 13
3. Contenu 13
4. Organisation 16
5. Remerciements 16

Chapitre 1
Évolution des métiers autour des réseaux

1. Évolution de l'informatique et des réseaux 19
   - 1.1 Les premiers ordinateurs 19
   - 1.2 Réseaux à commutation de circuits 20
   - 1.3 Réseaux à commutation de paquets 21
   - 1.4 L'émergence des réseaux LAN et du protocole TCP/IP 23
   - 1.5 L'évolution vers les réseaux ATM 24
   - 1.6 L'émergence de la virtualisation de serveurs 25
   - 1.7 Développement de l'Internet et du WAN 26
   - 1.8 Le cloud computing 27
2. Le métier d'administrateur réseau 28
   - 2.1 Tâches et missions de l'administrateur réseau 28
   - 2.2 Extension et évolution du métier 28
   - 2.3 De nouveaux domaines à maîtriser 29
     - 2.3.1 Mouvance DevOps 29
     - 2.3.2 Le contexte de la virtualisation 30
     - 2.3.3 Certifications et outils d'autoformation 31
     - 2.3.4 Un métier purement technique? 35

Chapitre 2
Conception d'un réseau local

1. Ethernet et les liaisons physiques 37
1.1 Historique 37
1.2 Principaux standards Ethernet et évolutions 38
1.3 Du courant fort sur Ethernet : le PoE 41
1.3.1 Principes de la norme 41
1.3.2 Performances et utilisation en pratique 42
2. Segmentation d'un réseau 44
2.1 Pourquoi segmenter un réseau ? 44
2.1.1 Segmentation géographique 44
2.1.2 Segmentation fonctionnelle et sécuritaire 45
2.1.3 Segmentation pour raisons de performances 49
2.2 Segmentation réseau par la mise en place de VLANs 54
2.2.1 Principe des VLANs 54
2.2.2 Types de VLANs 54
2.2.3 Norme 802.1Q 56
2.2.4 Mise en place de liaisons interswitch et VLAN tagging . . 57
2.2.5 Gestion du tagging par les équipements réseau 59
2.3 Conception avancée de réseau à partir de VLANs 66
2.3.1 La norme QinQ ou 802.3ad : VLANs dans un VLAN . . . 66
2.3.2 Extension des VLANs avec VXLAN 70
2.3.3 Private VLAN 73

Chapitre 3
Gestion des actifs et haute disponibilité

1. Gestion des commutateurs et routeurs 79
1.1 Outils et interfaces d'administration 79
1.1.1 Interfaces CLI 79
1.1.2 Interfaces web 84
1.1.3 Autres possibilités de management 86

1.2 Gestion des configurations des éléments actifs 89
1.2.1 Mémoires d'un équipement et synchronisation 89
1.2.2 Synchronisation de la configuration 89
1.2.3 Sauvegarde et restauration de configuration 92
1.3 Gestion des systèmes d'exploitation des éléments actifs 94
1.3.1 Inventaire 94
1.3.2 Homogénéité du matériel. 96
1.3.3 Mise à jour des équipements réseau 99
2. Haute disponibilité 103
2.1 Introduction 103
2.2 Redondance des liens physiques et agrégation 103
2.2.1 Principe du spanning-tree 103
2.2.2 Protocoles d'agrégation d'interfaces. 106
2.3 Stacking de commutateurs 111
2.3.1 Stacking traditionnel 111
2.3.2 Capacité de commutation d'un commutateur 113
2.3.3 Particularités d'implémentation de stack 115
2.3.4 Vers un stack virtuel. 117
2.4 Redondance et clustering de niveau 3 118
2.4.1 Principe du clustering sur des routeurs 118
2.4.2 Le protocole VRRP et son fonctionnement 119
2.4.3 Solutions propriétaires 124
2.4.4 Redondance de liens opérateurs. 125

Chapitre 4
Principes de sécurité sur un réseau local

1. Sécurité au niveau des commutateurs. 133
1.1 Les faiblesses du protocole ARP. 133
1.2 Mécanisme de sécurité de port ou port-security 138
1.3 Sécurité autour des mécanismes d'adressage IP 140
1.3.1 Adressage statique ou dynamique via DHCP. 140
1.3.2 DHCP Snooping 141

1.4 Politiques d'accès au réseau 144
1.4.1 Principe du NAC : Network Access Control 144
1.4.2 Authentification 802.1x sur port de commutateur 145
1.5 Saut de VLANs : hopping 147
2. Les firewalls. 151
2.1 Caractéristiques d'un firewall 151
2.1.1 Fonction et positionnement dans un réseau. 151
2.1.2 Analyse jusqu'à la couche transport 154
2.1.3 Analyse jusqu'à la couche applicative 157
2.2 Les solutions du marché et comment faire son choix 158
2.2.1 Solutions commerciales NGFW (Next Generation Firewall) 158
2.2.2 Solutions libres 161
2.2.3 Critères de choix et métriques. 162
2.2.4 Firewall matériel ou virtuel? 165
2.3 Tester son firewall 167
3. Les attaques de déni de service 169
3.1 Principe de l'attaque 169
3.2 Dénis de services distribués 172
3.3 Moyens de protection 173
4. Gestion des accès distants 174
4.1 Connexion à distance sécurisée : VPN nomade 174
4.1.1 Principe 174
4.1.2 Solutions nomades libres 179
4.2 Connexion site à site : VPN IPSEC 182
4.2.1 Le principe. 182
4.2.2 Les phases et la négociation d'un tunnel VPN IPSEC . . 183
4.2.3 Les problématiques de NAT. 185
4.2.4 Problématiques d'adressage IP 187
4.2.5 Guide pour une configuration IPSEC site à site rapide et simple. 188
4.3 Autres types de VPN 189

Chapitre 5
Approche globale de la supervision avec SNMP

1. Définition de la supervision 191
   - 1.1 Contexte de la DSI 191
   - 1.2 Comment détecter un problème technique ? 192
   - 1.3 Comment traiter un problème technique ? 193
   - 1.4 Améliorer la disponibilité effective 194
2. Approche ISO 195
   - 2.1 Cahier des charges initial 195
   - 2.2 Gestion des incidents 196
   - 2.3 Gestion des configurations 197
   - 2.4 Gestion des performances 199
     - 2.4.1 Mesure de la performance 199
     - 2.4.2 Les politiques de qualité de service 200
   - 2.5 Gestion de la sécurité 202
   - 2.6 Gestion de la comptabilité 203
3. Entreprendre un projet de supervision 204
   - 3.1 Erreurs à éviter 204
   - 3.2 Que superviser au niveau réseau ? 206
     - 3.2.1 Disponibilité des actifs 206
     - 3.2.2 Variables à contrôler selon le type d'équipement réseau 208
4. Supervision réseau via le protocole SNMP 210
   - 4.1 Principes du protocole SNMP 210
     - 4.1.1 Caractéristiques du protocole SNMP 210
     - 4.1.2 Modélisation d'un élément actif : la MIB 211
     - 4.1.3 Première approche sur la structure de la MIB par un cas d'étude 213
   - 4.2 Les MIB publiques et privées 217
     - 4.2.1 Principe général de la MIB I et la MIB II 217
     - 4.2.2 Organisation de la MIB I 220
     - 4.2.3 Organisation de la MIB II 226

4.2.4 MIB privées et intégration dans le manager 228
4.3 Configurer SNMP 229
4.3.1 Les communautés et les droits 229
4.3.2 Les types de messages 231
4.3.3 Requêtes sur la MIB selon la communauté et les droits sur l'OID 235
4.3.4 Étapes de configuration minimale SNMP 237

Chapitre 6

Autres protocoles de supervision réseau

1. Gestion des journaux avec Syslog 239
1.1 Enjeux de la journalisation des événements 239
1.1.1 Fonctions initiales des logs 239
1.1.2 Enjeux juridiques 240
1.1.3 Besoin d'une gestion centralisée 242
1.2 Principes du protocole Syslog 243
1.2.1 Fonctionnement global 243
1.2.2 Classification des logs générés 245
1.2.3 Format de la trame 248
1.3 Configuration de Syslog 250
1.4 Solutions de collecte et d'analyse de logs 254
1.4.1 Critères de choix du collecteur 254
1.4.2 Les collecteurs basés sur de l'open source ou gratuits . . 256
1.4.3 Autres collecteurs 261
2. Les protocoles de supervision de flux réseau 264
2.1 Introduction à NetFlow 264
2.1.1 Origines du protocole 264
2.1.2 Cas d'utilisation 265
2.1.3 Caractéristiques et contenu d'un flux NetFlow 266
2.1.4 Fonctionnement et architectures 268
2.2 Configuration sur un actif réseau 270

2.3 Les collecteurs NetFlow et les applications d'analyse 273
2.3.1 Le marché 273
2.3.2 Les collecteurs basés sur de l'open source ou gratuits . . 274
2.3.3 Les solutions payantes 277
2.4 Le protocole sFlow 281
2.4.1 Principes de sFlow 281
2.4.2 NetFlow vs sFlow 282
2.5 Les sondes RMON 285
2.5.1 Principes de RMON 285
2.5.2 Fonctionnalités apportées par RMON 287
2.5.3 Exploration des MIB RMON 1 et 2 288
2.5.4 Configuration de RMON 293

Chapitre 7
Métrologie et mesure de performances

1. Métrologie et métriques réseau 295
1.1 Définition de la métrologie 295
1.2 Les métriques réseau 297
1.3 Méthodologie de tests de performances 299
2. Mesure de débit et optimisation 301
2.1 Débit brut et débit applicatif 301
2.2 Outils Iperf/Jperf 303
2.3 Ajuster les paramètres réseau pour augmenter le débit 306
2.4 Mesurer des débits au-delà du gigabit 309
2.5 Importance des performances dans un réseau SAN 313
2.6 Communication directe entre mémoire et carte réseau : le RDMA 317
2.7 Dimensionnement du débit applicatif 320
2.7.1 Caractéristiques des réseaux IP en matière de débit 320
2.7.2 Mesure de débit sur le serveur ou le poste utilisateur . . 321
2.7.3 Captures de trames et mesures via le SPAN 323

3. Mesurer les temps de réponse 325
3.1 Mesure de la latence et de la gigue 325
3.1.1 Ping 325
3.1.2 Traceroute 327
3.1.3 Calculer la gigue 328
3.2 Perte de paquets et disponibilité 329
3.2.1 Évaluation de la perte de paquet 329
3.2.2 Taux de disponibilité d'un service 329
3.2.3 Disponibilité d'un service en « nombre de neuf » 331
3.2.4 Analyse des services joignables 332
3.3 Temps de réponse applicatif 334
3.3.1 Notion d'Expérience Utilisateur (UX) 334
3.3.2 Scripts de surveillance 334
3.3.3 Monitoring des utilisateurs en temps réel (RUM) 336
3.4 Temps de réponse d'une application web 338
3.4.1 Introduction 338
3.4.2 Responsabilités techniques des performances d'une application web hébergée 338
3.4.3 Temps de réponse et montée en charge 342
3.4.4 Métriques spécifiques pour caractériser une application web 343
3.5 Performances d'un réseau de téléphonie IP 347
3.5.1 Gestion de la téléphonie par l'équipe réseau 347
3.5.2 Exigences des réseaux temps réel par rapport aux réseaux de données 348
3.5.3 Bande passante pour la téléphonie IP et codecs 350
3.5.4 Adaptation du réseau pour transmettre les flux VOIP . 352
4. Les outils de supervision spécialisés en métrologie 353
4.1 Stocker les mesures 353
4.1.1 Problématique de stockage des données de métrologie . 353
4.1.2 Outils répandus de stockage des données de métrologie 354

4.2 Afficher les données mesurées 355
4.2.1 Représentation des données. 355
4.2.2 Outils répandus et conçus pour l'affichage de données métrologiques 356
4.3 Collecter les mesures 358
4.3.1 Moyens de collecte 358
4.3.2 Outils libres de collecte multiprotocoles. 359
4.4 Solutions complètes libres 360
4.4.1 Les fonctions à couvrir 360
4.4.2 InfluxDB/Telegraf/Graphana 361
4.4.3 ELK avec agents Beat 361
4.4.4 Cacti 362
4.4.5 LibreNMS 364
4.4.6 Graphite 364

Chapitre 8
Une nouvelle approche du réseau : SDN et NFV

1. Virtualisation du réseau 367
1.1 Virtualisation et cloud computing 367
1.1.1 Historique et principe de la virtualisation 367
1.1.2 Services de cloud computing proposés au sein des datacenters. 369
1.2 Cloud computing et réseaux des datacenters 372
1.2.1 Architecture réseau traditionnelle. 372
1.2.2 Modifications de l'architecture réseau des datacenters . 373
1.2.3 Ajout d'une couche virtuelle au sein du réseau. 375
1.3 Virtualisation des fonctions réseau : NFV 375
1.3.1 Technologies de virtualisation réseau 375
1.3.2 Problématiques des appliances matérielles 376
1.3.3 Avantages apportés par la NFV 376
1.3.4 Solutions proposées par éditeurs et équipementiers . . . 378
1.3.5 Performances des appliances réseau virtuelles 379

1.4 Gestion des actifs réseau d'un datacenter 379
2. Approche du SDN (Software Defined Network) 380
2.1 Architecture de commutation et routage 380
2.1.1 La commutation de paquets 380
2.1.2 Plans de données, de contrôle et de gestion 380
2.2 Caractéristiques du SDN 383
2.2.1 Définition du SDN 383
2.2.2 Technologies pionnières et analogies 385
2.2.3 Le standard OpenFlow 387
2.2.4 Le contrôleur SDN 390
2.2.5 Implémentations du SDN 391
2.3 Solutions du marché 392
2.3.1 Solutions libres 392
2.3.2 Solutions propriétaires 394
2.4 Le SD-WAN (Software-Defined WAN) 395
2.4.1 Les nouvelles attentes du WAN 395
2.4.2 Principes du SD-WAN 396
2.4.3 Les acteurs du marché 399

Glossaire 401
Index 411

Chapitre 4
Principes de sécurité sur un réseau local

1. Sécurité au niveau des commutateurs

1.1 Les faiblesses du protocole ARP

Le protocole ARP (*Address Resolution Protocol*) est indispensable au fonctionnement d'un réseau internet IPv4. Il assure en effet, la correspondance entre adresses IP des machines et adresses MAC. Ce protocole a été créé dès 1982, dans un contexte où la sécurité n'était pas encore une priorité.

ARP repose sur des broadcast, dans lesquels une machine voulant obtenir une résolution envoie une trame « ARP request » à l'ensemble du segment réseau. La machine concernée renvoie une requête « ARP Reply » où elle indique alors son adresse MAC. À partir de là, la machine émettrice peut constituer son paquet IP et envoyer la trame à son destinataire connaissant désormais son adresse physique.

Afin de s'annoncer sur le réseau et également détecter d'éventuels conflits d'adresses IP, une machine se connectant physiquement sur le réseau émet une requête ARP appelée « ARP gratuit » dans laquelle elle s'annonce à tous les membres du segment réseau (`filtre wireshark : arp.isgratuitous == 1`). Ces derniers mettent alors à jour leur cache ARP dans lequel ils vont stocker l'adresse IP et l'adresse MAC correspondante, même s'ils n'ont jamais émis d'« ARP request » pour connaître la machine en question. Pour les communications futures, une machine du réseau consulte en premier lieu son cache ARP à la recherche d'une correspondance. Si et seulement si la correspondance n'existe pas, la machine émet une requête « ARP request ». On peut également placer statiquement des entrées permanentes dans le cache ARP (que l'on appelle table ARP) qui ne sont pas modifiables par le protocole.

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.17134.590]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>arp -a

Interface : 192.168.88.1 --- 0x21
  Adresse Internet      Adresse physique      Type
  192.168.88.255        ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  229.111.112.12        01-00-5e-6f-70-0c     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique

Interface : 192.168.1.56 --- 0x3c
  Adresse Internet      Adresse physique      Type
  172.31.141.122        00-ae-8c-79-1e-2d     dynamique
  192.168.1.76          f4-ca-e5-6b-ee-ac     dynamique
  192.168.1.89          08-2e-5f-f1-02-d8     dynamique
  192.168.1.90          3c-bd-3e-c4-4d-22     dynamique
  192.168.1.240         24-5e-be-0f-fe-e3     dynamique
  192.168.1.254         14-0c-76-95-c2-9a     dynamique
  192.168.1.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  226.178.217.5         01-00-5e-32-d9-05     statique
  229.111.112.12        01-00-5e-6f-70-0c     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Affichage de la table ARP sur une machine Windows 10

Partant du fait que n'importe quelle machine peut émettre des requêtes ARP sans vérification d'identité, il est tout à fait envisageable pour un attaquant d'émettre des requêtes ARP en usurpant une adresse IP. Concrètement, rien n'empêche d'annoncer à tout le segment réseau que l'adresse IP d'un poste, d'un serveur, de la passerelle par défaut par exemple, correspond à sa propre adresse MAC. Cela permet alors à l'attaquant d'intercepter du trafic qui ne lui est pas destiné.

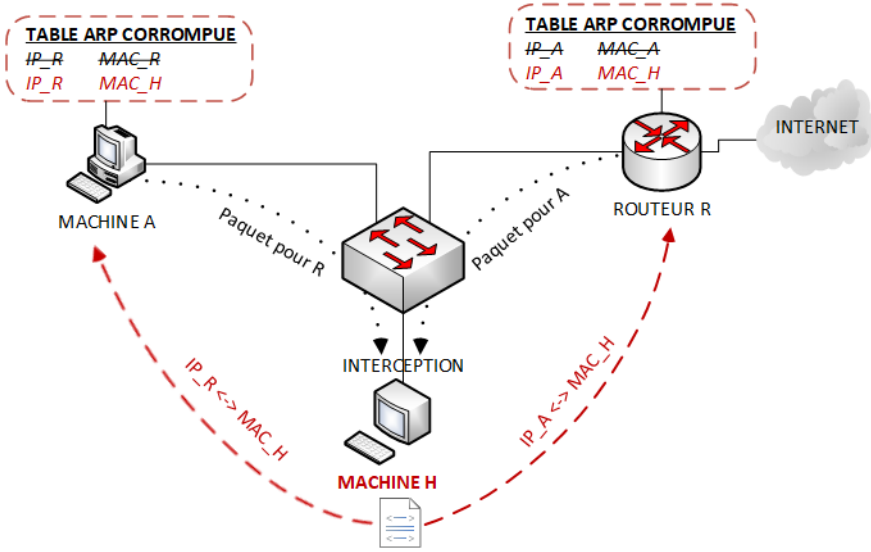
Voici en détail comment mettre en place ce type d'interception pour mieux comprendre le mécanisme d'attaque appelé « homme du milieu » ou « Man-in-the-Middle » :

Soit une machine A sur le réseau, naviguant sur Internet par l'intermédiaire du routeur passerelle par défaut R. H est un attaquant, il est connecté sur le même segment réseau qu'A et R. Son but est d'intercepter l'intégralité du trafic, entrant et sortant, entre A et R et donc l'intégralité de la navigation internet de la machine A.

La machine attaquante va dans un premier temps générer un paquet ARP dans lequel elle va annoncer que l'adresse IP du routeur « IP_R » correspond à son adresse MAC « MAC_H » (on parle d'« ARP poisoning »). La machine A va donc physiquement envoyer les trames à destination de l'IP de R sur l'adresse MAC de H. H recevra alors les paquets à destination de R contenant le trafic à destination d'Internet.

L'attaque ne peut s'arrêter là : dans un second temps, afin d'obtenir les paquets de réponse correspondant à la requête initialement interceptée, l'attaquant doit faire en sorte d'usurper l'identité de A par rapport au routeur. Il va annoncer alors avec une requête ARP, que l'adresse MAC correspondant à l'adresse IP de la machine A « IP_A » est la sienne : « MAC_H ». Le routeur enverra désormais toutes les réponses concernant logiquement la machine A à l'adresse physique de l'attaquant « MAC_H ». H se trouve donc en situation complète de MiM (Man In the Middle) et est capable d'intercepter le trafic dans les deux sens. Il ne lui reste plus qu'à transmettre les paquets sortants ou entrants aux deux intéressés pour ne pas interrompre la communication.

L'attaquant n'a cependant pas la possibilité d'empêcher A ou R d'envoyer leurs trames ARP sur le réseau. Ainsi, il est obligé d'envoyer des requêtes falsifiées à intervalles de temps régulier pour maintenir l'interception.

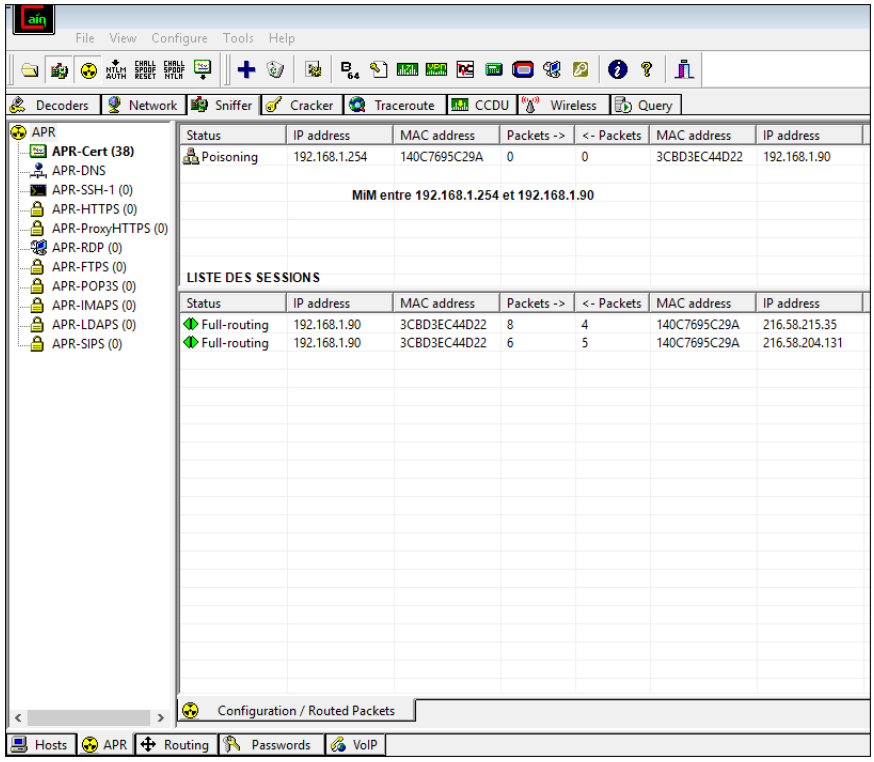


Attaque MiM ARP, la machine attaquante H émet des ARP request falsifiée et intercepte alors le trafic entre la machine A et le routeur R, et indirectement le trafic Internet

Il existe un certain nombre de programmes permettant de réaliser ce type d'attaque (en laboratoire uniquement) afin de mieux comprendre ces mécanismes. Il y a, par exemple, Cain&Abel sous Windows et ETTERCAP sous Linux pour les plus connus :

– http://www.oxid.it/

– https://www.ettercap-project.org/



Attaque MiM ARP via le logiciel Cain & Abel - interception de trafic entre 192.168.1.90 et le routeur 192.168.1.254

Le fichier C4_1_AttaqueARP_capture.pcapng est disponible en téléchargement sur le site des Éditions ENI.

La machine cible A peut-elle s'apercevoir que sa communication Internet est interceptée? Si le protocole de niveau applicatif n'a pas prévu une procédure d'authentification et de chiffrement, concrètement si la famille de protocoles SSL/TLS n'est pas utilisée, alors l'attaque reste imperceptible. Dans le cas de l'utilisation d'un protocole d'authentification comme SSH et dans notre cas présent HTTPS pour de la navigation web, la machine affichera un message d'avertissement de son application cliente (le navigateur), lui indiquant que la communication avec le serveur distant n'est pas sûre.

Pour améliorer l'attaque et la rendre plus discrète, l'attaquant devrait dans ce cas usurper le certificat du serveur de destination, en faisant en sorte qu'il soit reconnu par une autorité de certification (une CA), ce qui demande d'être en possession de la clé privée du serveur web de destination, ou d'avoir manipulé le navigateur web de la victime avant l'attaque, ce qui reste plus complexe, mais réalisable.

Une alternative plus simple consisterait à forcer l'utilisation par l'application cliente, d'un protocole non sécurisé, c'est-à-dire HTTP au lieu de HTTPS pour un navigateur, quitte ensuite à réencapsuler les requêtes en HTTPS pour la communication entre l'attaquant et le serveur web.

Les éditeurs de navigateurs, et en particulier Google avec son navigateur Chrome, ont été parmi les premiers à mettre en place une parade interdisant la consultation d'un site en HTTP, s'il existe une version HTTPS. C'est ce que propose le mécanisme HSTS (*HTTP Strict Transport Security*) dans la RFC 6797 imposant au navigateur l'utilisation du HTTPS.

Remarque

Dans une optique de mise en place de portail captif ou d'inspection de trafic web par un firewall, l'HSTS pose énormément de problèmes, car ces mécanismes reposent justement sur l'interception du trafic entre le client et le site web. Le renforcement de la sécurité sur les navigateurs, le durcissement des contraintes dans la génération d'un certificat TLS et les améliorations récentes autour du HSTS, deviennent alors contre-productives dans ces cas précis, et sont à l'origine de problèmes techniques rendant la navigation web impossible.

1.2 Mécanisme de sécurité de port ou port-security

Dans la section précédente était évoquée une attaque MiM sur un réseau local à partir d'une machine malveillante connectée sur le même segment réseau. Pourquoi ne pas endiguer une potentielle attaque en amont, en contrôlant les machines autorisées à se connecter sur un réseau local et donc un commutateur donné?