HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

FRnOG release 9 (24/11/2006)

Sécurité des Hébergeurs

Raphaël Marichez
<Raphael.Marichez@hsc.fr>

Sommaire

- Introduction
- Les risques : pourquoi une politique de sécurité ?
  - Obligations contractuelles
  - Risques consécutifs à une compromission
  - Aspects juridiques
- Techniques d'intrusion
  - Client ou extérieur vers hébergeur
  - Client vers client
  - Extérieur vers client
- Les parades
  - Techniques passives
  - Techniques actives
  - Solutions organisationnelles

Sommaire

- Introduction
- Les risques : pourquoi une politique de sécurité ?
  - Obligations contractuelles
  - Risques consécutifs à une compromission
  - Aspects juridiques
- Techniques d'intrusion
  - Client ou extérieur vers hébergeur
  - Client vers client
  - Extérieur vers client
- Les parades
  - Techniques passives
  - Techniques actives
  - Solutions organisationnelles

Introduction : « héberger » ?

- Hébergement de serveur propriété du client (OVH, RedBus)
  - Location d'un emplacement
  - Fourniture électrique et connectique Internet
  - Accès physique possible
  - **Pas** de maintenance
- Hébergement de serveur « dédié » (dedibox, kimsufi)
  - Location d'un serveur
  - **Pas** d'accès physique
  - Maintenance physique uniquement
- Hébergement de service
  - Location d'une plate-forme web, SMTP, ...

Sommaire

- Introduction
- Les risques : pourquoi une politique de sécurité ?
  - Obligations contractuelles
  - Risques consécutifs à une compromission
  - Aspects juridiques
- Techniques d'intrusion
  - Client ou extérieur vers hébergeur
  - Client vers client
  - Extérieur vers client
- Les parades
  - Techniques passives
  - Techniques actives
  - Solutions organisationnelles

Obligations contractuelles

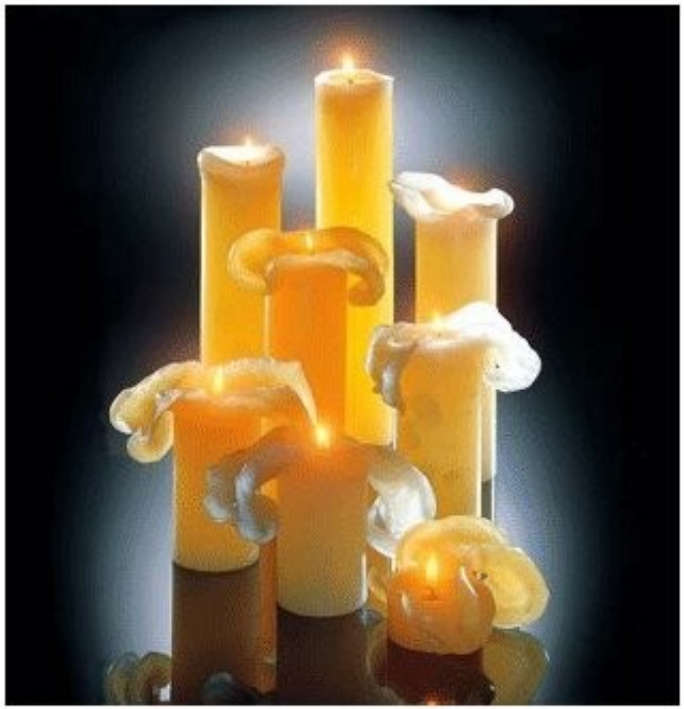
- Connectivité internet
  - Cause du FAI, ou déni de service (distribué) sur le lien réseau
  - Prévoir une clause contractuelle
- Alimentation électrique
  - Prévoir une clause contractuelle. Mais ne suffit pas.
  - Nécessité d'alimentation de secours **testée**
  - **Cas RedBus : 28 février puis dimanche 26 mars 2006 pendant 48h**
    - Image de marque, relations client.
    - Réactivité et transparence des clients hébergeurs (OVH, Agarik, AMEN...).
- Disponibilité du matériel; sauvegardes : selon le contrat
- Conclusion : spécifier une « obligation de moyens », mais pas de résultat

Le Cas RedBus : image de marque

OPERATION “NOIR TOTAL”

SOYEZ GENEREUX : ENVOYEZ LEUR UNE BOUGIE*

*déductible des impôts



MERCI D'ENVOYER VOS DONS A :

REDBUS INTERHOUSE

Redbus Interhouse (France) SA
9 Energy* Park
130-136 boulevard de Verdun**
92413 Courbevoie Cedex
Paris
France

*c'est vite dit...
**comme la bataille

MERCI POUR EUX !!!

Obligations contractuelles

- Connectivité internet
  - Cause du FAI, ou déni de service (distribué) sur le lien réseau
  - Prévoir une clause contractuelle
- Alimentation électrique
  - Prévoir une clause contractuelle. Mais ne suffit pas.
  - Nécessité d'alimentation de secours **testée**
  - **Cas RedBus : 28 février puis dimanche 26 mars 2006 pendant 48h**
    - Image de marque, relations client.
    - Réactivité et transparence des clients hébergeurs (OVH, Agarik, AMEN...).
- Disponibilité du matériel; sauvegardes : selon le contrat
- Conclusion : spécifier une « obligation de moyens », mais pas de résultat

Risques techniques consécutifs à une compromission

- Se protéger contractuellement n'est pas suffisant...
  - Rebonds
  - Relayage de mails : mise en listes noire du domaine ou du réseau IP
  - IRC bots
  - Hébergement et distribution de contenu illicite
  - Dénis de services sur le LAN
- Autres risques : image de marque, usurpation d'identité (dont phishing), ...

Aspects juridiques

- En cas d'activité illicite consécutive ou non à une compromission (phishing, IRC...) et quel que soit le contrat :
- Loi pour la Confiance dans l'Economie Numérique
  - Article 6 : le prestataire technique n'est pas responsable si :
    - **Il n'a pas connaissance** du « caractère illicite » « des activitées ou des informations stockées », ou si :
    - Dès le moment où cette connaissance est acquise, il **« agit promptement »** pour retirer les données ou en rendre l'accès impossible
- A cela s'ajoute l'obligation d'informer les autorités :
  - Décret n°2006-358 du 24/03/2006 relatif à la conservation des données des communications électroniques, article 1er :
    - Obligation de conserver **un an** les informations permettant d'identifier l'utilisateur, les destinataires des communications, etc. (en aucune façon le contenu ne doit être enregistré)

Sommaire

- Introduction
- Les risques : pourquoi une politique de sécurité ?
  - Obligations contractuelles
  - Risques consécutifs à une compromission
  - Aspects juridiques
- Techniques d'intrusion
  - Client ou extérieur vers hébergeur
  - Client vers client
  - Extérieur vers client
- Les parades
  - Techniques passives
  - Techniques actives
  - Solutions organisationnelles

Intrusion client vers l'hébergeur

- Une séparation physique du réseau d'administration et des réseaux clients est obligatoire.

- Les « VLAN » n'offrent pas un niveau de sécurité suffisant : la sécurité repose alors sur la sécurité de l'administration à distance des commutateurs.

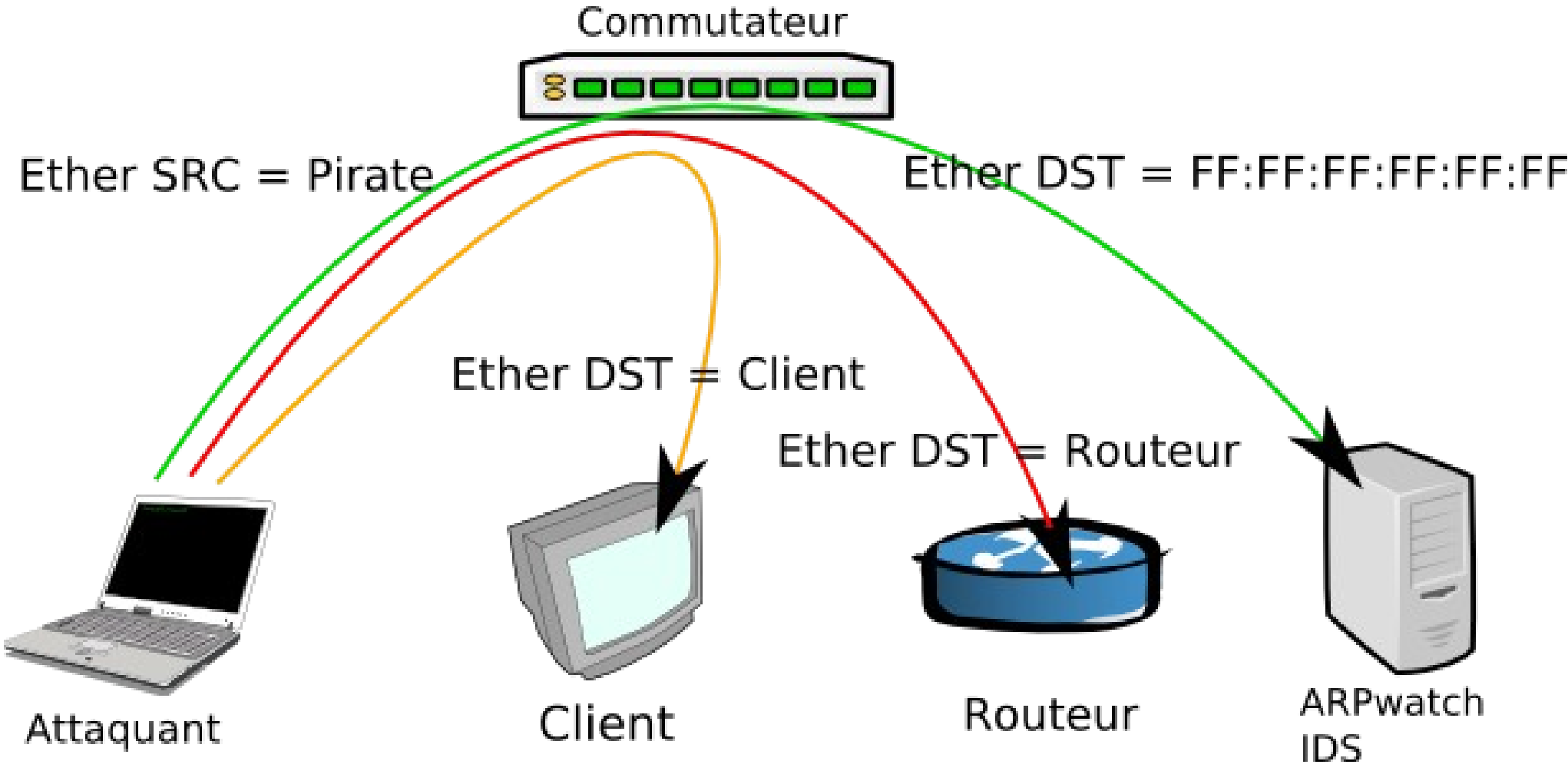
Client vers client sur un LAN switché

- Contrairement à l'xDSL, les clients d'un même sous-réseau IP sont sur le même LAN.

- Exemples de familles d'attaques :
  Innondations de cache ARP (« MAC flooding »)
  Tags VLAN (double-encapsulation, Cisco DTP...)
  Usurpation ARP (attaque « Man in the Middle »)
  Force brute

- Conséquences : usurpation, déni de service, écoute, modification...

ARP : usurpation IP sur un LAN switché



ARP : usurpation IP sur un LAN switché

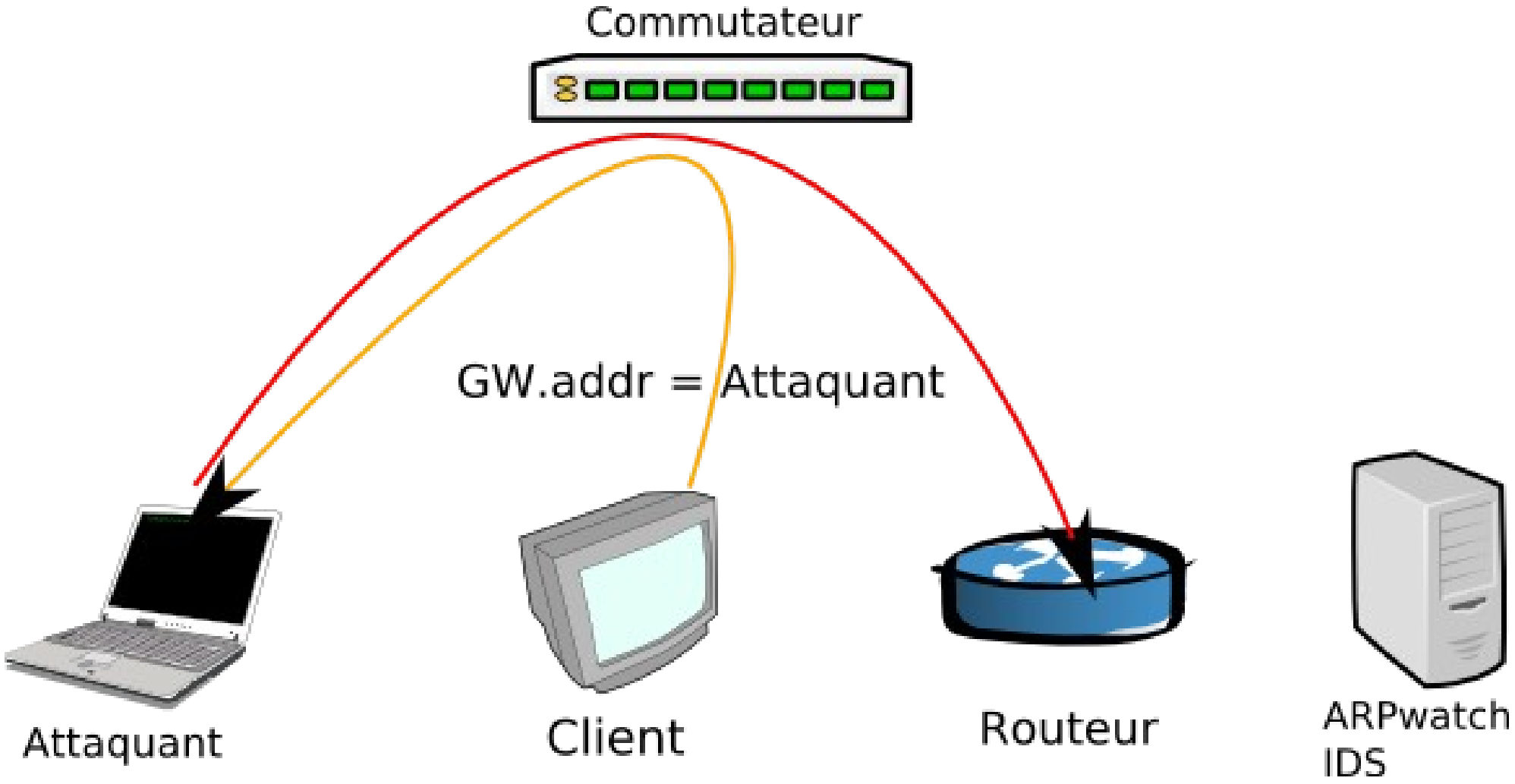
Ether SRC : Pirate	Ether DST : Client

OPCODE : ARP reply	
Sender HW@ : Pirate	Target HW@ : Client
Sender IP@ : Gateway	Target IP@ : Client

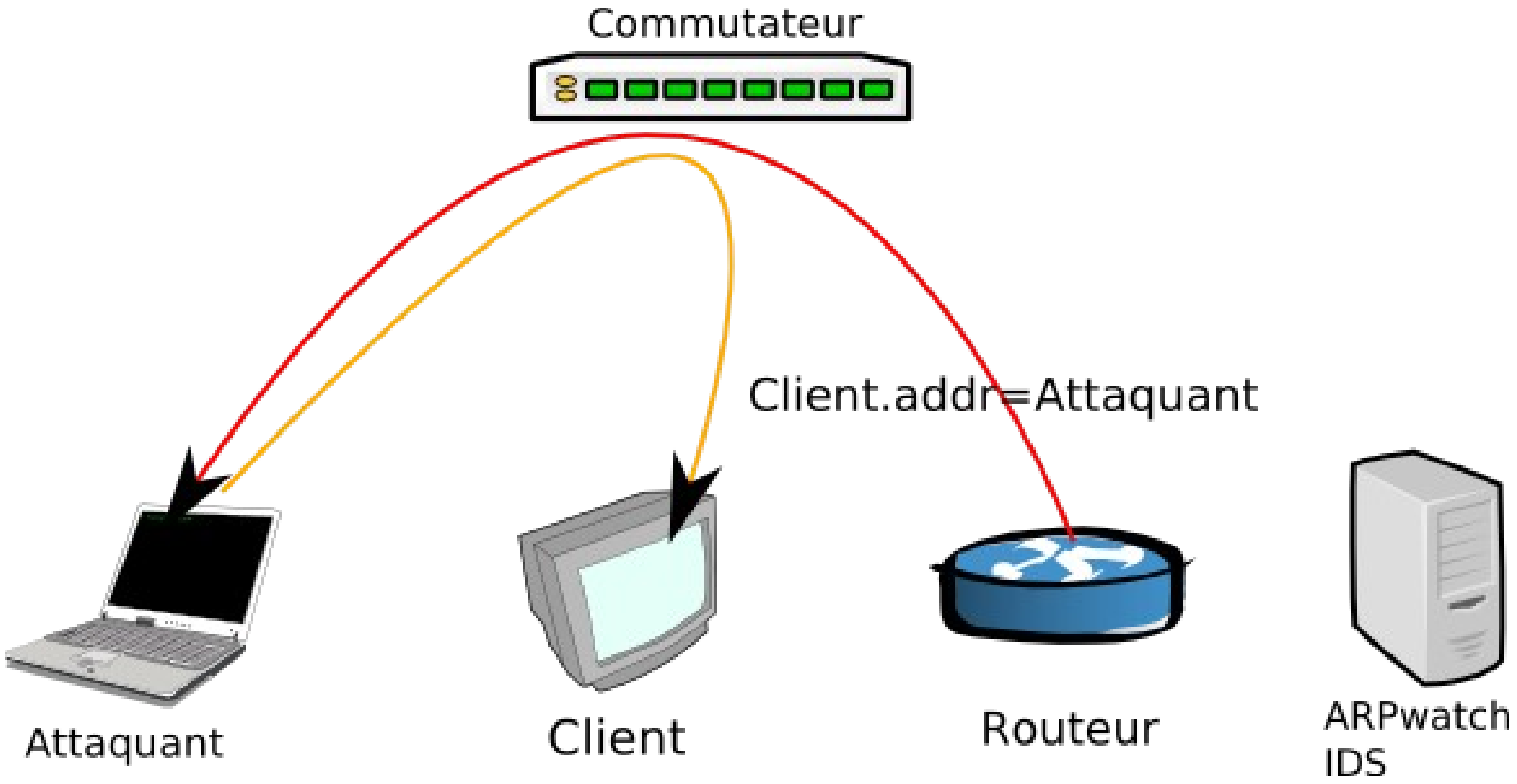
Ether SRC : Pirate	Ether DST : Gateway

OPCODE : ARP reply	
Sender HW@ : Pirate	Target HW@ : Gateway
Sender IP@ : Client	Target IP@ : Gateway

ARP : usurpation IP sur un LAN switché



ARP : usurpation IP sur un LAN switché



Attaque extérieur vers client

- Dénis de service (distribué)
  - Rien ne permet localement d'empêcher la saturation du lien descendant
- Scans d'IP (vers, virus, bots...)
  - Plus faciles à détecter (sauf techniques d'évasion avancées)
- Attaques ciblées
  - Serveurs dédiés : la protection est à la charge du client
  - Hébergement de services applicatifs (site web...) : la protection est à la charge de l'hébergeur
- Une attaque « extérieur vers client » réussie se transformera en attaque « client vers client » ou « client vers hébergeur »

Sommaire

- Introduction
- Les risques : pourquoi une politique de sécurité ?
  - Obligations contractuelles
  - Risques consécutifs à une compromission
  - Aspects juridiques
- Techniques d'intrusion
  - Client ou extérieur vers hébergeur
  - Client vers client
  - Extérieur vers client
- Les parades
  - Techniques passives
  - Techniques actives
  - Solutions organisationnelles

Parades passives

- Intrusion Detection Systems :
  - `Snort` (http://www.snort.org) :

    Machine dédiée qui reçoit tout le trafic transitant sur un routeur.
    Règles de remontées d'alertes nombreuses et nécessitant du travail.

  - `Arpwatch` (http://www-nrg.ee.lbl.gov/)

    Permet de détecter les changements d'IP peu discrets (paquet ARP émis en broadcast).
    Utilisation plus avancée : l'arpwatch doit recevoir tout le trafic transitant sur le routeur.
    Rend détectable l'usurpation du client auprès du routeur mais pas l'usurpation du routeur auprès du client : le pirate voit toujours les paquets émis par le client.

Parades passives

- Fixer les adresses Ethernet
  - « `arp` » sous Unix comme sous Windows.
  - La corruption du commutateur reste possible (remplissage ou corruption des tables ARP pour aboutir à une diffusion du trafic), mais est plus difficile à réaliser (dépend du matériel).
  - Utiliser les « trusted ports » lorsque les commutateurs le permettent.
- Idéalement : comme certains points d'accès sans-fil, empêcher les clients de communiquer entre eux (sauf besoin légitime)
- Surveiller la charge machine, le trafic et la connectivité réseau, le nombre d'utilisateurs connectés, les connexions réseaux suspectes (rebond ou proxy IRC, ...)
  - `Nagios` (http://www.nagios.org), `Cacti` (http://www.cacti.net)
  - Outils de surveillance du réseau : MRTG (http://oss.oetiker.ch/mrtg/)

Parades actives

- Scans
  - L'adressage IP d'un hébergeur est souvent connexe : la détection de scans est plus aisée.
  - Mesures temps-réel de bannissement : boîtiers propriétaires ou logiciel libre :
    - `PortSentry` (http://sourceforge.net/projects/sentrytools/)
    - `Fail2ban` (http://fail2ban.sourceforge.net/)
    - `netfilter` et module « `recent` » (http://www.netfilter.org)
    - Attentions aux dénis de service induis par de telles mesures
- Veille active en vulnérabilités
  - Scanneurs de vulnérabilités, de versions
    - `Nessus` (http://www.nessus.org), Nmap (http://insecure.org/nmap)
  - Informer les clients

Solutions organisationnelles

- Réactivité et transparence
  - système public de gestion de tickets d'incidents (exemple : http://travaux.ovh.net)
- Les attaques sont majoritairement applicatives : s'assurer des mises à jour
  - Et si la tâche en incombe au client :
    - Prévenir le client et l'obliger contractuellement aux mises à jour de sécurité
    - Vérifier par un scanneur de versions, comme `Nmap` (http://www.insecure.org/nmap/)
- « La sécurité est un processus, pas un produit » (Schneier)
  - Cycle « Planifier - Réaliser - Vérifier - Réagir »

Solutions organisationnelles

- Politique de mot de passe client :
  - Personnel et incessible
  - Robustesse du mot de passe
    - Utilisation de casseur de mot de passe (`John the Ripper`) possible si le contrat le prévoit
- Homogénéité du parc :
  - Maîtrise du système d'exploitation
  - Simplifier les outils d'administration, de surveillance et de maintenance

Prochains rendez-vous

- **Formation ISO27001 Lead Auditor** :
  - Certification ISO27001 Lead Auditor par **LSTI**
  - **http://www.hsc.fr/services/formations/**

Paris : 4 - 8 décembre
Genève : 22-26 janvier
Toulouse : 5-9 février

- **Sécurité et journalisation : détection de machines Linux compromises**
  - Tutoriel en deux parties le 1er février 2007
  - **http://www.solutionslinux.fr/**

Questions ?

Raphael.Marichez@hsc.fr
www.hsc.fr