Design et implémentation d'une solution de filtrage ARP

Patrice Auffret – 8 Décembre 2009 – OSSIR B 0.2

THOMSON TECHNICOLOR

Qui suis-je ?

- GomoR (http://www.gomor.org/)
- Sinon, expert sécurité chez Thomson
  - http://www.thomson.net/
- 8 ans d'expérience en SSI
- Auteur d'outils de sécurité écrits en Perl
  - SinFP: http://www.gomor.org/bin/view/Sinfp
  - OSPF Attack Shell: http://www.gomor.org/bin/view/OspfAsh
  - SSL Capable NetCat: http://www.gomor.org/bin/view/GomorOrg/SslNetcat
- Des publications (des fois)
- Tant qu'on y est, mon CV
  - http://www.gomor.org/bin/view/GomorOrg/AboutCv

Plan

- Présentation du problème
- Solutions possibles
- Risques associés au DA et à l'AA
- Comment supprimer le DA et l'AA ?
- Architecture technique
- Liste des menaces à prendre en compte
- Menaces
- Scénario d'attaque
- Configuration de la passerelle
- Juste un dernier problème
- L'outil
- Conclusion

Présentation du problème

- **Accès restreint à Internet dans l'entreprise**
  - proxy HTTP avec authentification
  - filtrage des URL par listes noires, blanches, grises
  - aucun autre protocole ne passe
- **Certains métiers nécessitent un accès complet à Internet**
  - métiers de la sécurité (au hasard)

Solutions possibles

- **Solution 1 : Utilisation de comptes proxy privilégiés**
  - accès sans filtrage d'URL
  - mais donne toujours accès uniquement au Web (HTTP)
  - solution rejetée, ne satisfait pas au besoin métier
- **Solution 2 : Routage IP+NAT ?**
  - privilèges de routage pour certaines adresses IP
  - solution rejetée, beaucoup trop risquée
- **Solution 3 : Ajouter une connexion ADSL « à coté » du réseau de l'entreprise**
  - accès sans filtrage protocolaire
  - solution adoptée

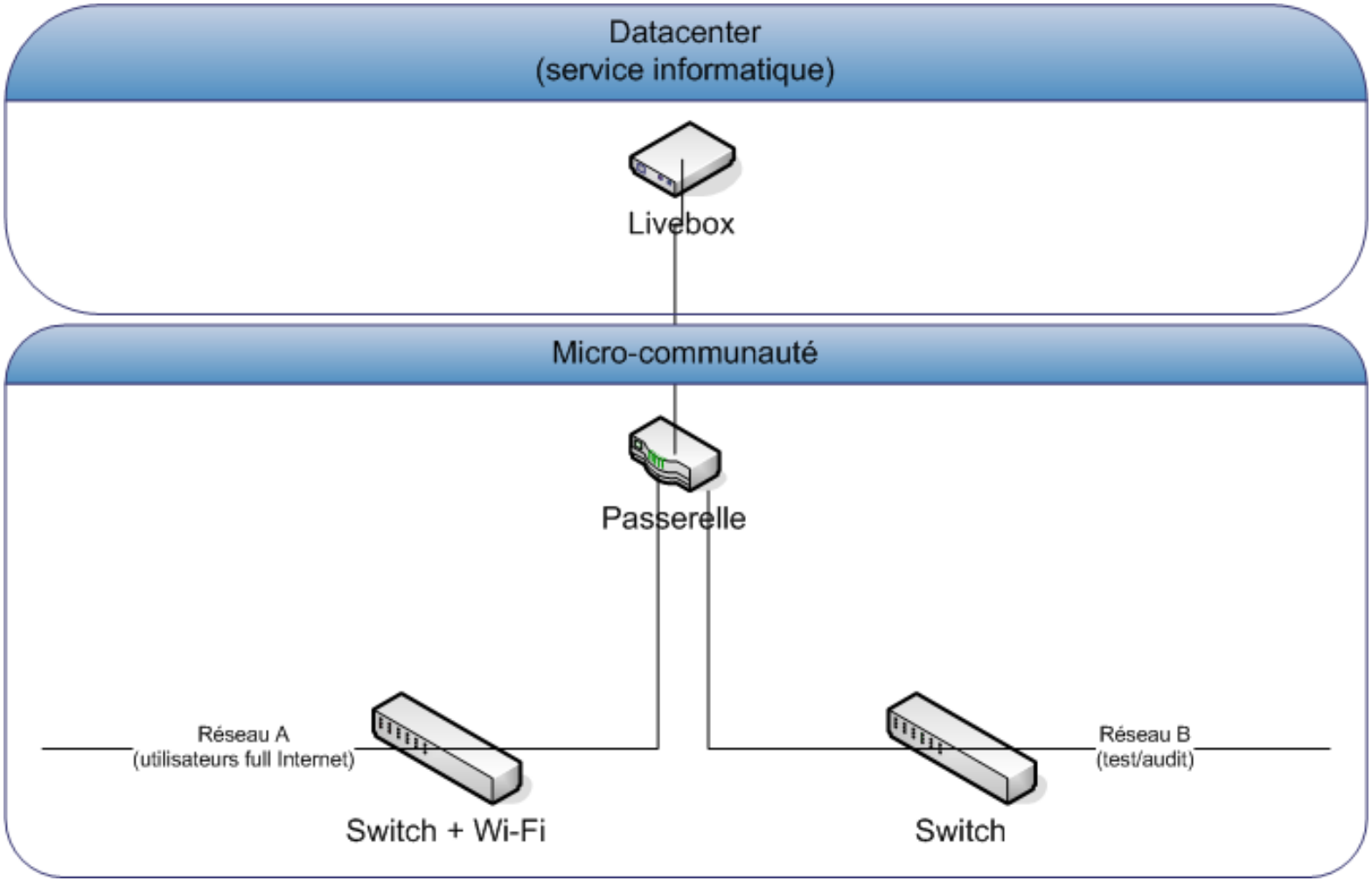
Risques associés au DA et à l'AA

- **Mais comment faire cohabiter deux connexions ?**
  - Pose les problèmes
    - du double attachement (DA)
    - et de l'attachement alternatif (AA)
- **Machine de l'entreprise est reliée au réseau de l'entreprise ainsi qu'à un accès « full Internet »**
  - si une compromission arrive sur l'interface « full Internet », le réseau de l'entreprise est compromis
  - facilite la fuite de documents
- **Plus généralement, permet de contourner la politique de sécurité de l'entreprise**
- **Même en AA !!**
  - c'est juste une attaque en 2 temps (remember slammer?)

Comment supprimer le DA et l'AA ?

- **De manière politique**
  - ne marche pas (même en menaçant de casser les jambes)
- **De manière technique**
  - marche un peu (y'a toujours quelqu'un de plus fort que nous)
- **De manière politique et technique, en ajoutant un soupçon de « trust »**
  - ne marche pas trop mal, en micro-communautées auto-gérées (qui a dit anarchie ?) (on peut aussi casser les jambes des plus faibles)

Architecture technique



Liste des menaces à prendre en compte

- **A/ 2 cartes réseaux (DA)**
- **B/ 1 carte réseau (AA)**
- **C/ accès non-autorisé à Internet**
  - C1: contournement filtrage MAC de la passerelle
  - C2: contournement filtrage IP de la passerelle
- **D/ accès non-autorisé sur le réseau de la passerelle**
  - D1: empoisonnement ARP de la passerelle
  - D2: empoisonnement ARP des clients
  - D3: autres attaques LAN

Menaces (1/2)

Menaces A et B (DA et AA)

- prise en compte politique
  - une personne souhaitant un accès « full Internet » subit un « audit »
  - pas de machine avec 2 cartes réseaux autorisée
  - une certaine confiance est accordée au propriétaire de la machine après un entretien
  - relevé de l'adresse MAC de la machine à connecter au « full Internet »
  - un responsable « filtrage MAC » par communauté
- prise en compte technique
  - l'adresse MAC est « désactivée » sur le réseau de l'entreprise
  - l'adresse est « activée » sur l'accès « full Internet »

Ni double attachement, ni attachement alternatif (à l'instant T de l'audit)

Menaces (2/2)

Menace C (C1, C2) (accès non-autorisé à Internet)

- prise en compte technique
  - désactivation de la résolution ARP de la passerelle
  - gestion statique du cache ARP de la passerelle
  - filtrage des adresses IP autorisées
  - NAT sur les adresses IP autorisées
  - couplage adresse MAC => adresse IP

Menace D (D1, D2, D3) (accès non-autorisé sur le réseau)

- prise en compte technique
  - désactivation de la résolution ARP de la passerelle
  - gestion statique du cache ARP de la passerelle
  - si empoisonnement ARP, il ne sera possible que contre les clients
    - un seul sens de la communication est écoutable
  - pas d'attribution automatique d'adresse (faible obscurité)
  - « IDS » résolution ARP

Scénario d'attaque

Attaquant se branche

- il n'aura pas d'adresse IP attribuée par le DHCP (MAC non autorisée)
- il configure manuellement
  - son adresse IP sera refusée au niveau filtrage IP (ni NATée)
  - son adresse MAC n'étant pas autorisée, il ne pourra résoudre l'adresse MAC de la passerelle (en considérant qu'il a trouvé l'adresse IP de la passerelle)
- il vole une adresse IP autorisée
  - elle sera refusée, le lien entre adresse IP et adresse MAC n'étant pas correct
  - il doit en plus résoudre l'adresse MAC de la victime
- il connait déjà l'adresse MAC de la passerelle
  - il lui faudra tout de même un couple adresse MAC/IP autorisé
  - et que cette machine soit éteinte

Configuration de la passerelle

- **Connexion simple pour les utilisateurs**
  - Pas de gestion statique cache ARP
  - Pas de gestion statique IP
- **Configuration DHCP**
  - Statique: ajout du couple adresse MAC => adresse IP
  - Si une adresse MAC n'est pas reconnue, pas d'attribution d'IP
- **Configuration ARP statique (passerelle sous FreeBSD)**
  - ifconfig –arp INTERFACE
  - arp –f ARP_STATIC.file
- **Configuration filtrage IP**
  - Seule une liste d'adresses IP est autorisée
  - Cette liste est aussi autorisée à être NATée

Juste un dernier problème

- **Pas de résolution ARP sur la passerelle**
  - Comment les clients vont-ils connaître l'adresse MAC ?

- **Utilisation d'un outil de résolution ARP en « userland »**
  - Ecrit en Perl
  - Utilisation de Net::Frame, un framework de construction de paquets réseaux
  - Moins de 100 lignes

L'outil

- **load_arp_entries(): chargement du fichier des couples adresse MAC => adresse IP autorisés**
  - consultation des clients autorisés à résoudre l'adresse MAC de la passerelle
- **send_arp_reply(): envoie de la réponse ARP pour l'adresse MAC de la passerelle uniquement**
  - seulement si le couple adresse MAC/IP faisant la requête est autorisé (la fonction authorized_mac() gère l'autorisation)
  - sinon, on trace la tentative de résolution
  - aussi, si une tentative est faite pour résoudre l'adresse MAC d'une autre machine que la passerelle, on trace. Des fois que ce soit une tentative d'attaque sur le lien local
- **arp_reply_gw(): boucle d'écoute sur le réseau**
  - lance send_arp_reply() si les conditions sont réunies

Exemples de traces « IDS »

- Requête de résolution autorisée pour un client

```
Found authorized mac/ip pair: [MAC|IP]
Arp reply sent to [MAC|IP]
```

- Un client non autorisé tente un accès

```
WARNING: Found NOT authorized mac/ip pair:
   [MAC|0.0.0.0]
```

- Un client tente une résolution pour un autre client

```
WARNING: Found ARP request for non GW IP (IP)
   from: [MAC|IP]
```

Conclusion

- **Difficilement passable à l'échelle**
  - fonctionne pour les petites communautés
- **Fonctionne bien quand toutes les machines autorisées sont allumées**
  - sinon, la connaissance d'un couple MAC/IP permet la connexion
- **Ne protège pas complètement les clients**
  - exemple de l'empoisonnement ARP
- **Nécessite un minimum de confiance envers les clients**
- **L'outil pourrait être simplifié**
  - nécessité de modification dans différents fichiers pour ajouter un client autorisé

Derniers mots

- L’outil sera disponible sur mon blog
  - http://www.protocol-hacking.org/
- Non, je ne sais pas quand
- C’est une licence BSD ^^
- En attendant, amusez-vous avec Net::Frame:
  - http://search.cpan.org/~gomor/

Merci. Questions ?

THOMSON TECHNICOLOR