Protocoles réseau : grandeur et décadence

Pierre BETOUIN
Cédric BLANCHER
Nicolas FISCHBACH

SSTIC05, 2 Juin 2005

Intervenants

- Nicolas Fischbach, senior manager
  COLT Telecom
- Cédric Blancher, ingénieur chercheur
  EADS CCR - DCR/SSI
- Pierre Bétouin, padawan du président
  EADS CCR - DCR/SSI

Table des matières

Introduction (1/2)

Modèle OSI

- Antérieur à IP
- IP non conforme à OSI

Vieillissement des protocoles

- Standards anciens
- Peu de prise en compte de la sécurité
- Inadéquation par rapport au contexte acutel

Introduction (2/2)

Protocoles réseau

- Contexte d'élaboration relativement sûr
- "People never learn"(tm) : IPv6, WEP/WPA(2) vs WiMAX, attaque Land sous WinXP, etc.

Puissance des attaques

- Expérience et recul accru
- Augmentation de la puissance de calcul
- Augmentation de la bande passante disponible

Typologie des attaques sur le réseau

Notions clefs

- Source
- Destination
- Flux
- Échange *One-to-one*
- Échange *One-to-many*

Types d'actions

- Interruption
- Capture
- Injection
- Modification
- Usurpation

Types d'attaques

- Passives ou actives
- Directes / par rebond / aveugles

Redirection de trafic

Saint Graal de l'attaquant sur le réseau

- Permet de "voir" le trafic redirigé
- Interception uni/bidirectionelle
- Permet toutes les attaques possibles

L'action sur le trafic par l'attaquant devient exclusive et complète

Couche 1

- Liens filaires
  - "Pinces crocodile"
  - "Coupures" de liens
- Liens non filaires
  - Lien directionnel : insertion
  - Lien omnidirectionnel : station de base malicieuse

Note

Les liens non filaires sont très sensibles à l'injection

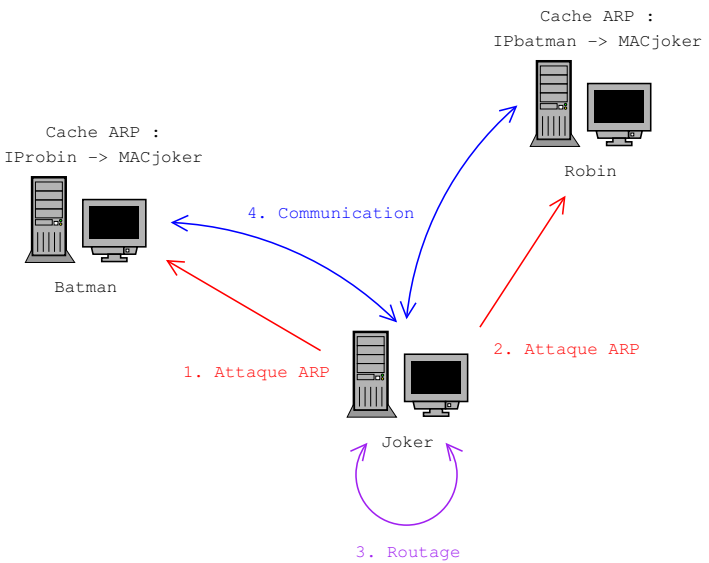
Couche 2

- CDP : protocole d'échange d'informations
- STP : calcul d'arbre couvrant sur typologie redondante
- DTP : protocole de négociation d'état de port
- VTP : protocole de gestion des VLANs

Outils : yersinia, irpas

ARP

- Envoi de réponses ARP non sollicitées
- Envoi de requêtes ARP
- Envoi de message ARP gratuits



Outils : arp-sk, scapy, arpspoof, ettercap, etc.

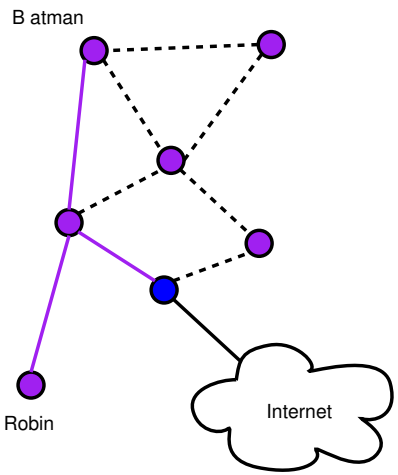
Couche 3 (1/2)

- Adressage
  - DHCP : serveur malicieux
- Routage dynamique
  - Redirection ICMP
  - HSRP
  - OSPF
  - BGP
  - MPLS

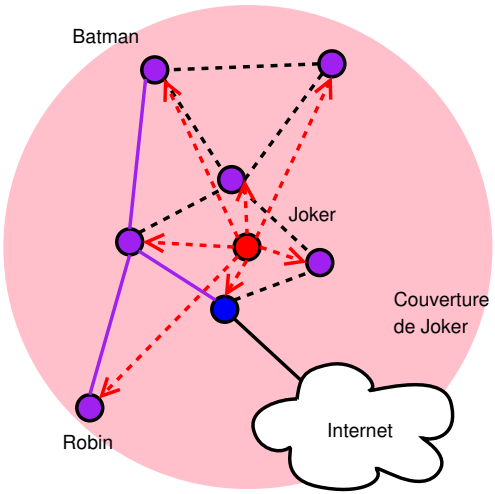
Outil : irpas

Couche 3 (2/2)

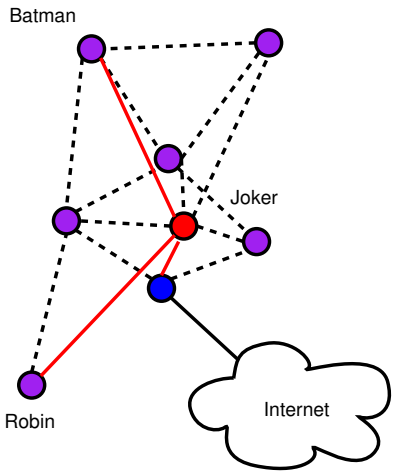
Routage en environnement WiFi maillé : OSLR



Le réseau MANET avec une route calculée entre Batman et Robin, et Internet



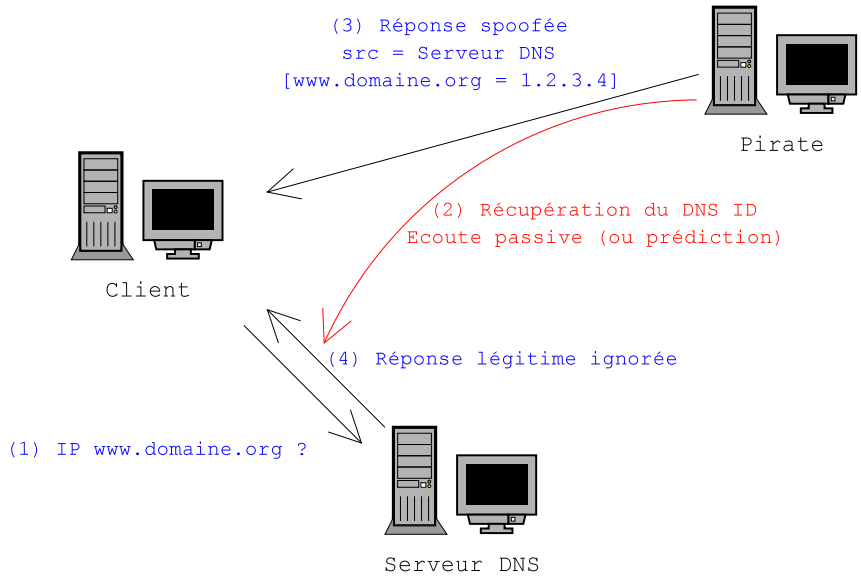
Joker entre dans le réseau et établit des liens forts



La reconfiguration du réseau permet à Joker de voir les flux entre Batman, Robin et Internet

Outil : une antenne avec du gain...

Attaques DNS : Prédiction de DNS ID



2 types d'attaques

- DNS ID Connu
- DNS ID Inconnu

Outil : dnsa

Attaques DNS : Corruption de cache DNS

Attaque toujours d'actualité (Cas *Symantec raptor* récent...) mais de moins en moins répandue

- Attaques du type *addRR* ou bugs logiciels
- Attaques via DNS ID *Spoofing*

Outil : dnsa

Attaques post-redirection : manipulation de trafic

Principales actions suite à une redirection :

- Écoute passive du trafic
- Redirection de trafic
- Déni de service (DoS)

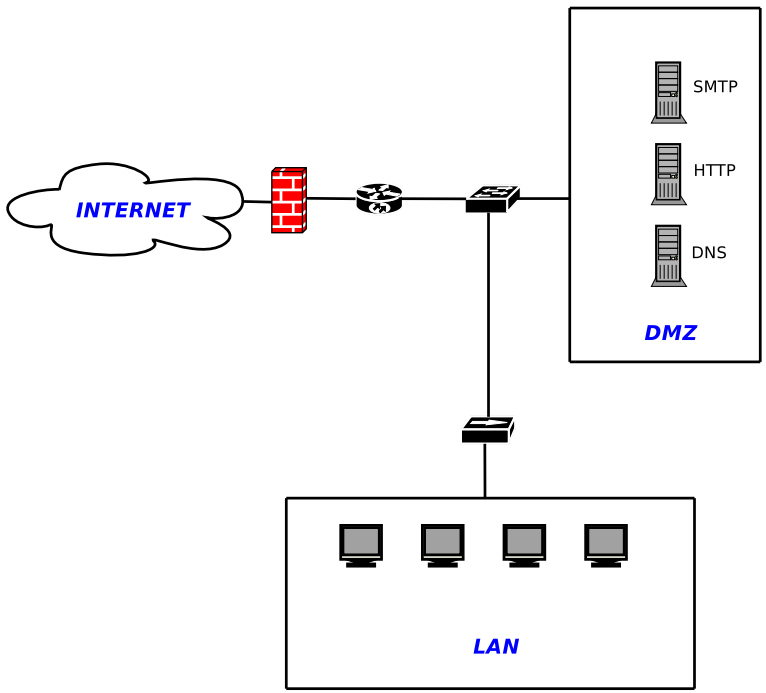
Attaques post-redirection

Action sur le contenu du flux :

- MiTM : *Man in the middle*
- Proxying transparent et redirection
- Tunneling (simple ou "furtif") et extraction

Compromission d'infrastructure

- Compromission du serveur HTTP
- ARP *cache poisoning*
- Redirection du flux DNS
- Compromission de l'ensemble des machines du LAN



VoIP Interne (Technique du pauvre...)

- CDP : identification du poste en téléphone VoIP
- ARP *cache poisoning*
- Identification de trafic RTP
- Écoute, Injection, DoS...

Cf. présentation de Nicolas Bareil

Conclusion

- Locales : simples et très efficaces
- Site : simple, bonne efficacité
- Multi-site : connaissance du réseau, fort risque de dommages collatéraux
- Internet-externe : relativement difficile mais pseudo-anonyme, surtout abus DNS

Greetings

- Securite.org
- French Honeynet Project
- Rstack

We Proudly R3wt