Communication WiFi par injection de trafic : Wifitap

Cédric BLANCHER

http://sid.rstack.org

cedric.blancher@eads.net
EADS Centre Commun de Recherche
DCR/SSI

sid@rstack.org
Rstack Team
http://www.rstack.org/

SSTIC 2005 Rump Session
http://www.sstic.org/

Agenda

EADS CCR

Plan

Motivation

2 points de départ

- Une discussion "argumentée" avec un avant-vente C***o sur l'inutilité de PSPF
- Un besoin sur les pentests sur hotspots WiFi commerciaux

Établir un canal de communication en outrepassant les restrictions imposées par l'AP

EADS CCR

Le problème

Communiquer

- avec les stations associées à un AP
- sans être soit-même associé

Solution

Écouter le trafic et injecter

- Injecter des trames de données en usurpant l'AP
- Écouter le trafic pour récupérer les réponses

Le WiFi permet cela de manière très simple

Plan

Wifitap : architecture générale

Wifitap est écrit en Python et s'appuie sur

- Un périphérique/interface tuntap en mode TAP (ethernet)
- Une carte 802.11 pour écouter et injecter
- Scapy[1]

C'est une preuve de concept...

[1] http://www.secdev.org/projects/scapy/

Wifitap : fonctionnement

Trafic sortant

- Récupérer de l'ethernet
- Ajouter les entêtes 802.11
- Ajouter BSSID et From-DS
- Injecter sur le WiFi

Trafic entrant

- Sniffer une trame 802.11
- Déchiffrer si WEP
- La transformer en ethernet
- L'envoyer à travers le tuntap

EADS CCR

Démo...

We Proudly R3wt

Download theses slides from `http://sid.rstack.org/`

EADS CCR