# PRELUDE

BEFORE THE TEMPEST

CIKALA Frédéric
LATAIX Rémy
MARMECHE Samuel
Ingénieurs2000 - IR3

# Plan de la démonstration

I) Présentation de l'architecture de la démo

II) Présentation du framework IDS Prelude

III) Lancement des attaques

IV) Résultats obtenus

V) Conclusion

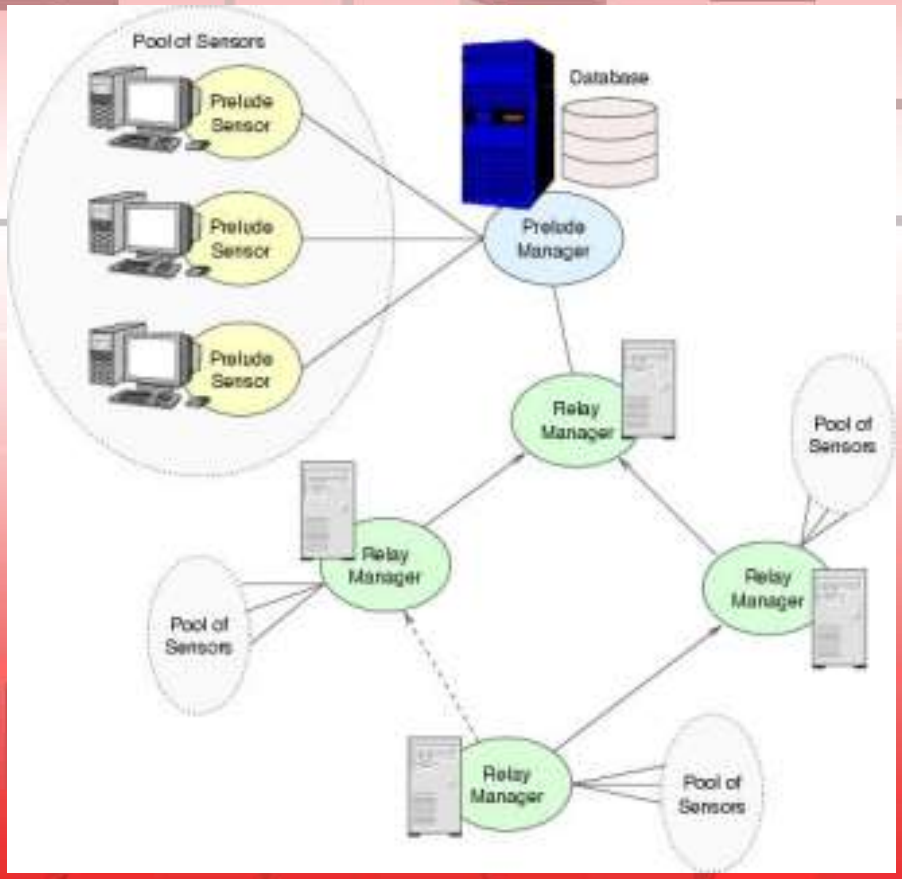
# Présentation de l'architecture

- Cible :
  - Server Web Apache
  - perl
  - Postgre
  - prelude (manager, nids, sensor, lml, lib)
- Assaillant :
  - netcat
  - hping2
  - nessus
  - nmap

# Présentation de Prélude

- Hybrid IDS = Host IDS + Net IDS
- Composants:
  - libprelude : fonctionnalités communes à tous les capteurs
  - prelude NIDS : capture et analyse des paquets en temps réel, « *network-based* »
  - prelude Manager : serveur gérant les capteurs
  - prelude LML : parti « *host-based* » de la détection

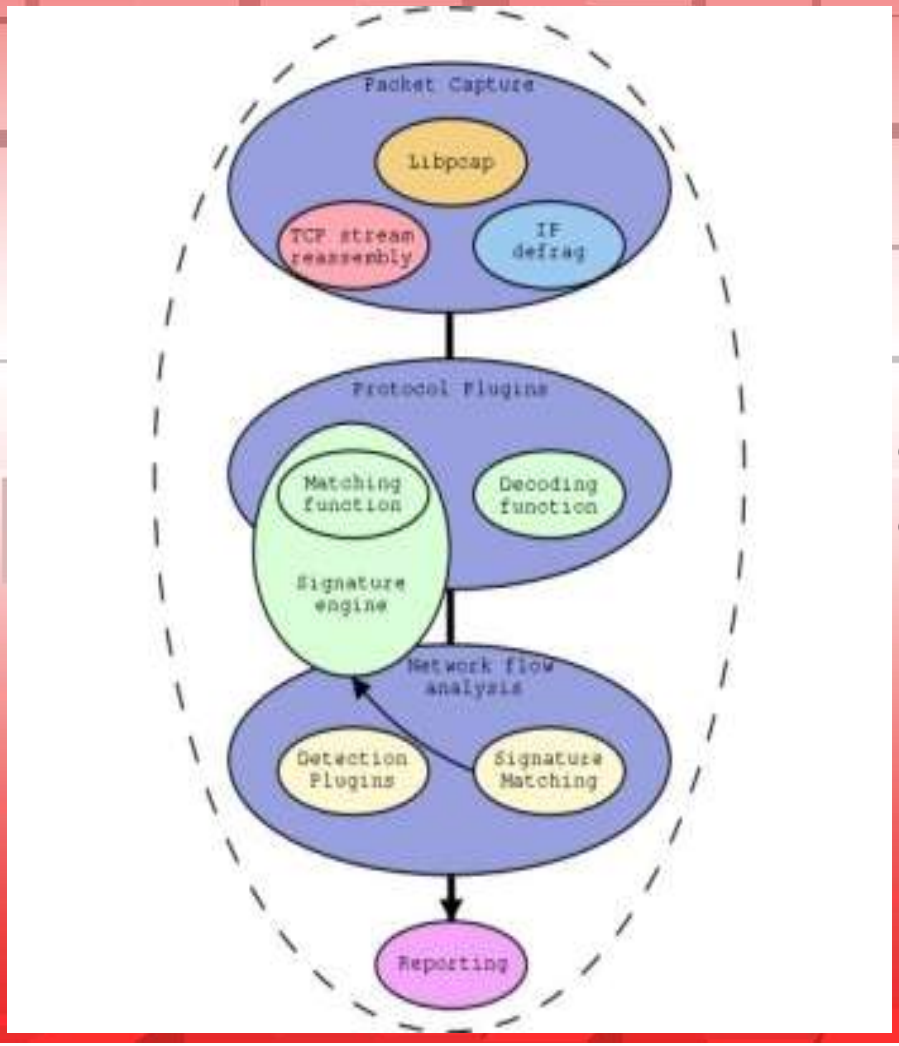
# Présentation de Prélude




**Prelude Network IDS :**

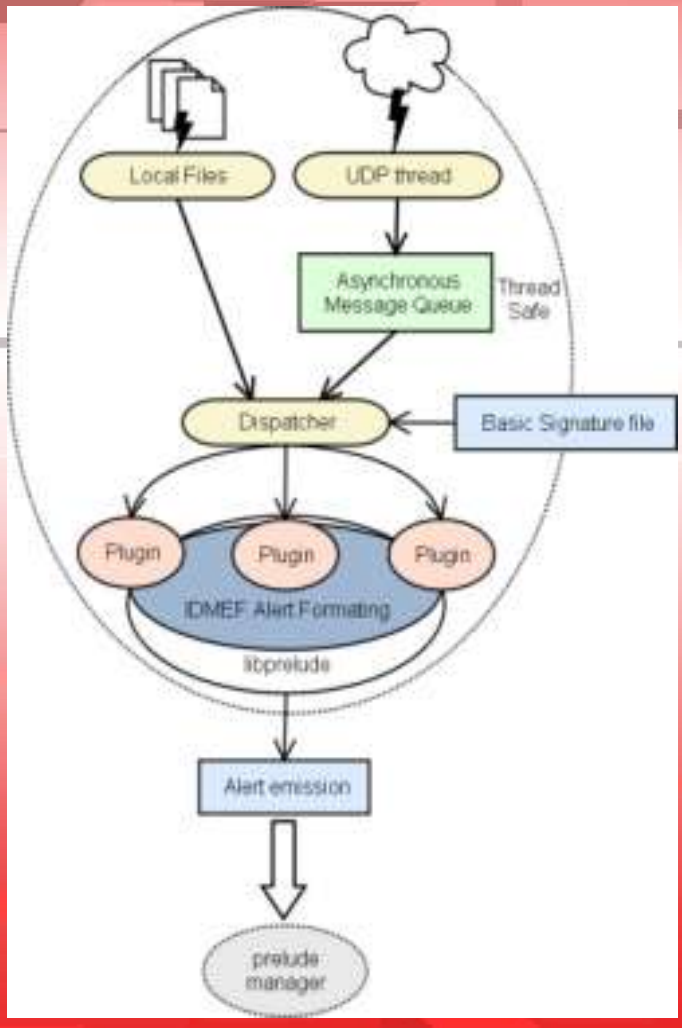
- **Prelude Manager**
- **Prelude Sensors**
- **Prelude nids**

# Présentation de Prélude




**Prelude HIDS:**

- **Prelude LML**
- **libPrelude**



# Lancement des attaques - Nessus

- architecture client / serveur
- lancement d'une rafale d'attaques
- couvre la plupart des OS et applications
- Interface graphique

# Lancement des attaques - Netcat

- Création de socket
- Synopsis
  - nc [-options] hostname port[s] [ports] ...
  - nc -l -p port [-options] [hostname] [port]

- Nombreuses options pour varier les paquets générés

# Lancement des attaques - Nmap

- Synopsis
  - nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>
- Exemple
  - -sT = TCP Connect : facilement détectable
  - -sS = TCP SYNScan (HalfOpen, sans ack)
  - -sF, -sX, -sN = Scan Stealth
  - -sU = UDPScan (parfois utile).

# Résultats - Piwi

- Projet récent, openSource, en cours de développement, «  customisable  »
- interface graphique exécutant des scripts perl liés à la base de donnée de prelude

# Conclusion

- Prelude est un framework efficace évolutif,
- il comporte des limites mais reste cependant très utile,
- prelude sera amené à évoluer de manière à tendre vers l'IPS

# Merci de votre attention =)