Réutilisez vos scripts d'audit avec PacketWeaver

https://github.com/ANSSI-FR/packetweaver

Sébastien Mainand, Florian Maury

Laboratoire sécurité des réseaux et des protocoles

9 juin 2017

Pourquoi PacketWeaver ?

Participation du LRP à des audits :

- mise en place de preuve de concept/démonstrations
- prototypage avec Python/Scapy, ArpSpoof, netfilter-queue, ebtables, iptables

Problématique :

- enchaînement complexe
- quid de la partie script ?

Capitaliser sur nos scripts d'audit

Besoins :

- base centralisée
- instrumenter les mécanismes de base : MITM, chaînage
- interface d'utilisation « à la Metasploit »

Script-ception

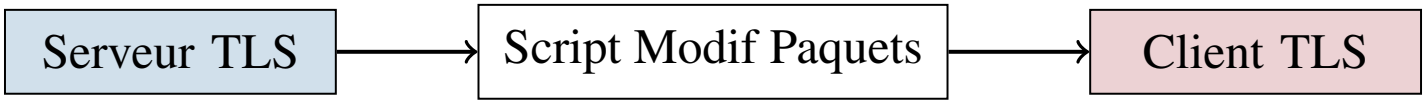
Chaînage de plusieurs scripts :

- **composition** de scripts

Script-ception

Chaînage de plusieurs scripts :

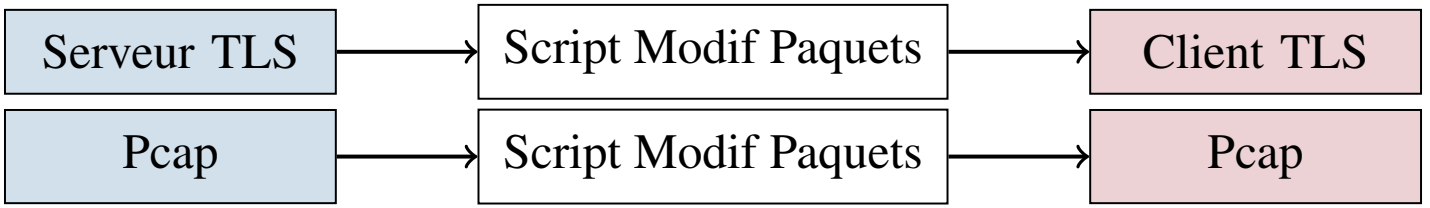
- **composition** de scripts
- syntaxe Pipe, comme en shell
  `script1 | script2 | script3`



Script-ception

Chaînage de plusieurs scripts :

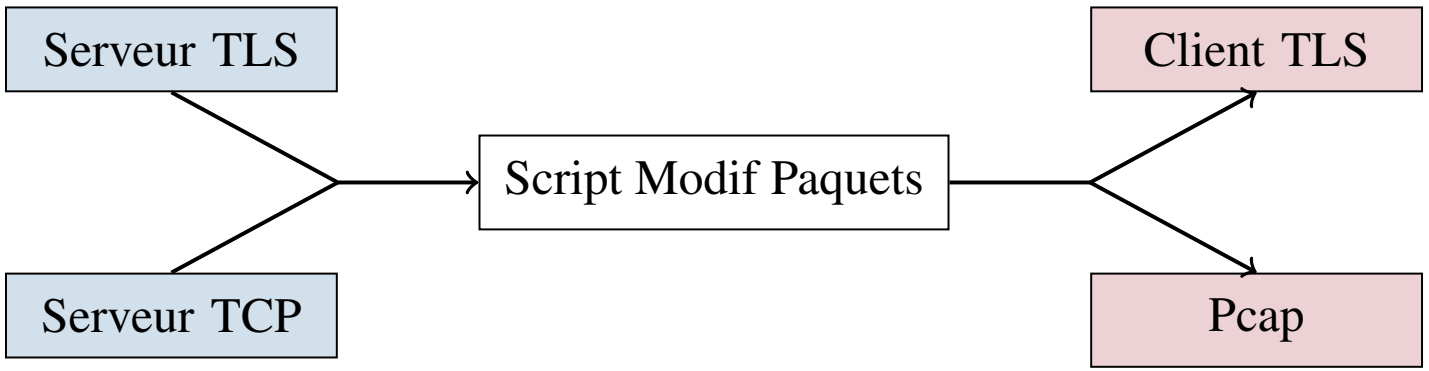
- **composition** de scripts
- syntaxe Pipe, comme en shell
  `script1 | script2 | script3`
- structure modulaire



Script-ception

Chaînage de plusieurs scripts :

- **composition** de scripts
- syntaxe Pipe, comme en shell
  `script1 | script2 | script3`
- structure modulaire
- gestion de **plusieurs entrées et plusieurs sorties**



Projets futurs

Développements futurs :

- amélioration de la robustesse du framework
- ajouter du contenu :
  - des **scripts pour l'audit**
  - des **exercices de formation**
  - des jeux de **tests d'équipements**
  - **automatiser/fiabiliser** des démonstrations

Merci pour votre attention
Questions ?

Testez ! Contribuez !

https://github.com/ANSSI-FR/packetweaver