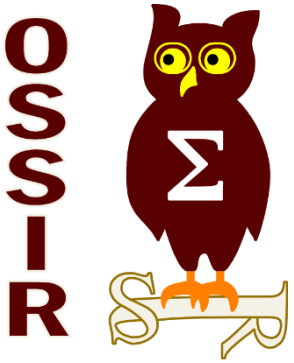


Pentest en environnement SAP

OSSIR Paris / 13 mai 2014

Emmanuel Mocquet – Consultant sécurité
Emmanuel.Mocquet@intrinsec.com

Plan

- Introduction
- Outillage
- Mots de passe
- Défauts de configuration
- Conclusion

Introduction / whoami

- Emmanuel Mocquet
  - → Consultant sécurité
    - ✓ Tests d'intrusion
    - ✓ Audits de code
  - → Travaux d'état de l'art sur SAP

- Intrinsec : acteur historique de la sécurité des SI (1995)
  - → Sécurité de l'information
    - ✓ Pentest / Audit / Conseil / SOC
  - → Hébergement et infogérance des SI

Introduction / SAP = ?

- SAP : Systems Applications and Products

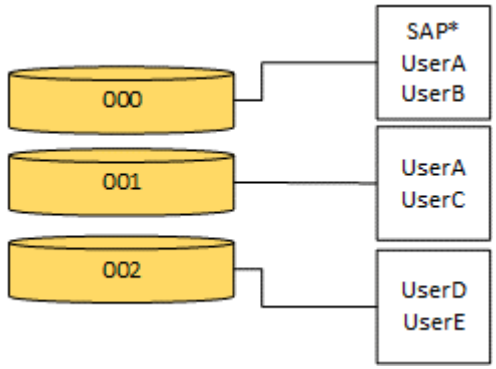
  ou Systeme, Anwendungen und Produkte…

  - → ERP, BI…
  - → Solution majeure sur le marché

- Objectifs
  - → Gérer les différentes fonctions d'une société
    - ✓ Modules spécialisés (« Treasury », « Sales & distribution », etc.)
  - → Automatiser la gestion des flux
    - ✓ Modification d'une donnée → Propagation sur l'ensemble des modules

Introduction / Clients & utilisateurs

- Les flux d'une société sont cloisonnés en « clients » (*mandants)*
  - Identifiant : 000-999
  - Chaque client dispose d'utilisateurs
  - Objectif : garantir l'étanchéité des comptes des corps de métier



- SAP dispose de clients et utilisateurs par défaut
  - Administrateurs (•_•)
  - Support
  - …

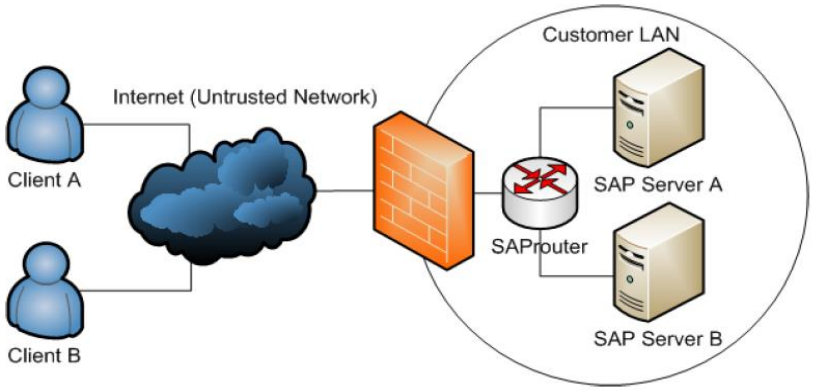
Introduction / Clients & utilisateurs

Utilisateurs	Description	Client	Mot de passe	Privilèges
SAP*	**Super-utilisateur**	000, 001, 066	06071992, PASS	Administrateur
DDIC	Dictionnaire de données ABAP (super-utilisateur)	000, 001	19920706	Appels distants à des programmes ABAP
EARLYWATCH	Utilisateur pour le service EarlyWatch	066	SUPPORT	Administrateur
SAPCPIC	Utilisateur dédié à la communication inter-programmes	000, 001	ADMIN	Modifications entre environnements SAP

- Pour les versions ultérieures à 2010, SAP* et DDIC disposent d'un mot de passe choisi à l'installation

- SAP* peut être automatiquement régénéré si supprimé
  - → avec un mot de passe par défaut

- SAPRouter est un proxy applicatif développé par SAP AG
  - → Réguler et rediriger les requêtes entre l'externe et l'interne



  - → Basé sur des ACLs

Envoyé en clair ☺

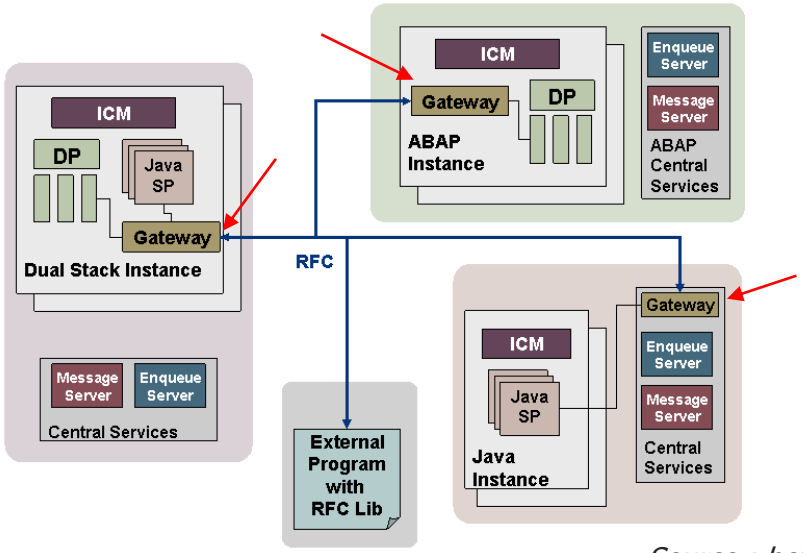
```
P|S|D[0-9]* <source> <destination> <service> [<mot de passe>]
```

  - ✓ Configuration trop permissive ⇔ Rebond interne

Introduction / SAPGateway

- Gateway SAP
  - Permet la communication entre instances ou programmes SAP externes
  - Configuration
    - ✓ Statique : le service démarre avec des options prédéfinies
    - ✓ Dynamique : les programmes ou serveurs externes peuvent s'enregistrer eux-mêmes.

Intéressant !



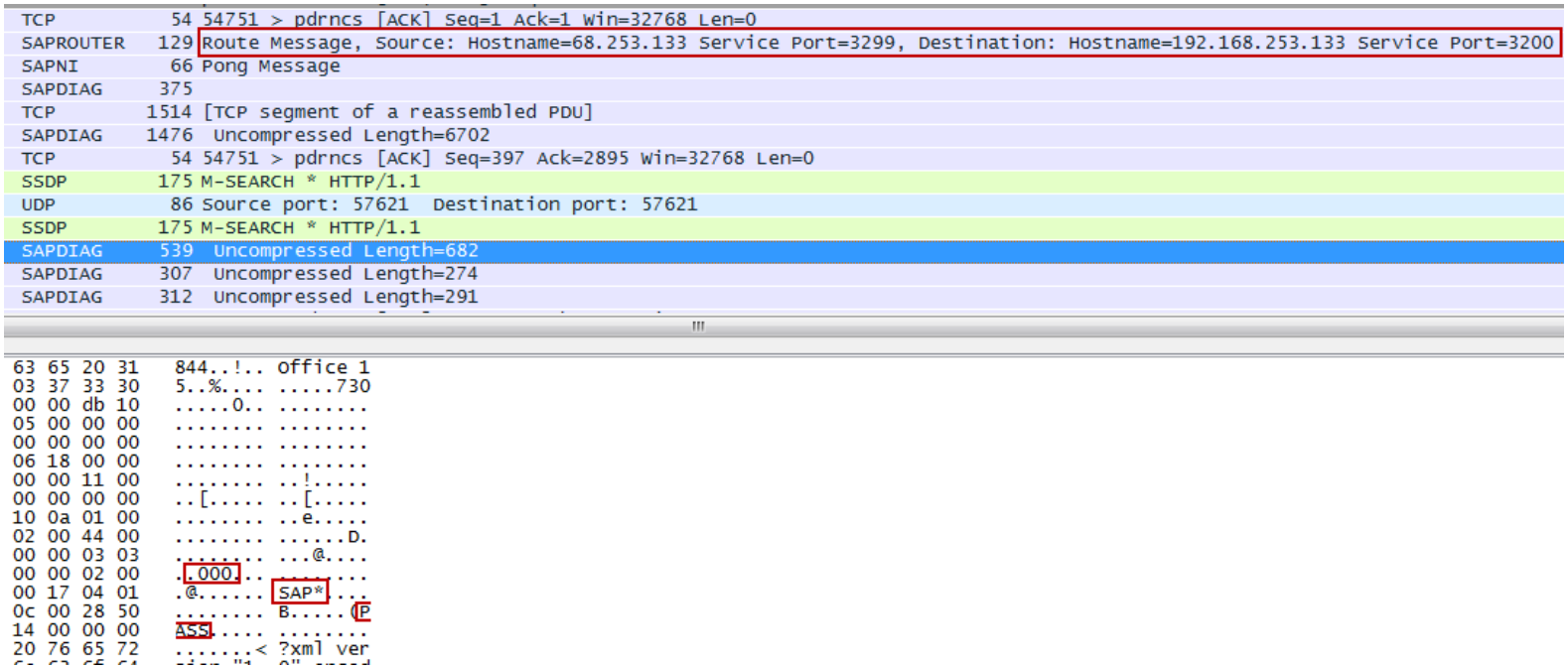
Source : help.sap.com

Plan

- Introduction
- Outillage
- Mots de passe
- Défauts de configuration
- Conclusion

Outillage

- Wireshark
  - Dispose d'un plugin permettant de « dissect » les trames SAP (NI, RFC, DIAG, etc.)
    - ✓ Très intéressant pour la capture de données sensibles (données métier, mots de passe…)



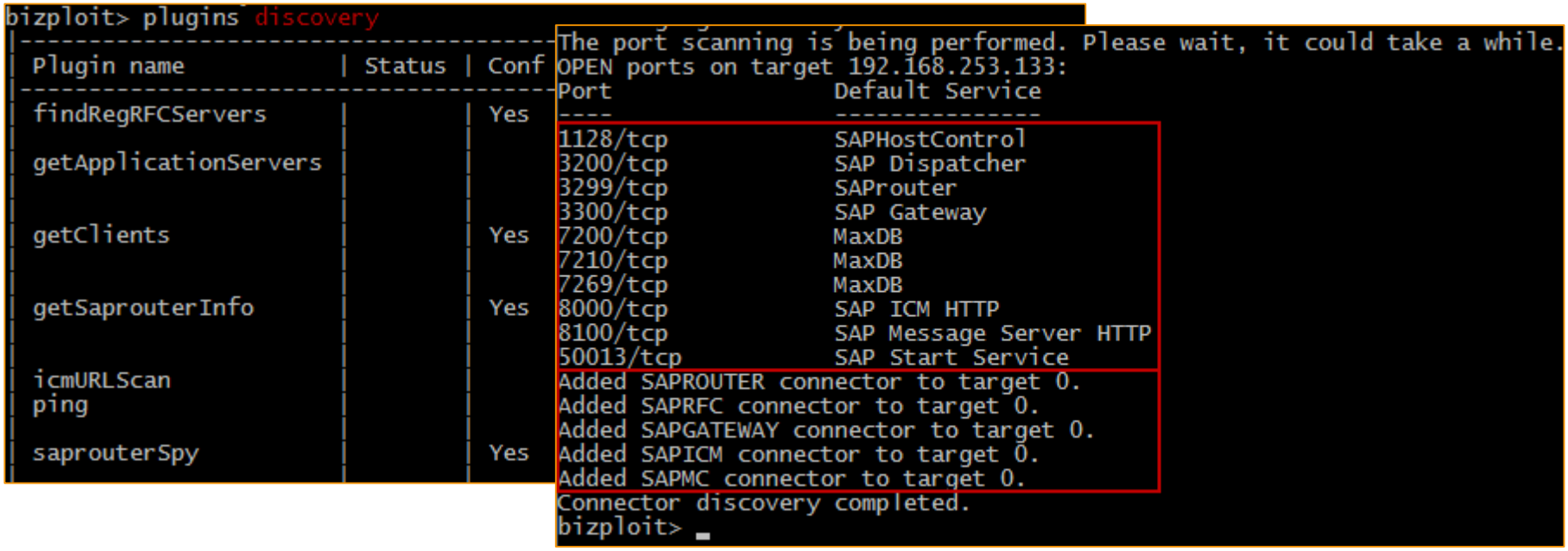
Outillage

- Cain & Abel
  - → Idem, surtout utile pour l'extraction de mots de passe (protocole DIAG)

- SAP Pentesting Tool, par ERPScan
  - → Ensemble de scripts Perl
  - → Utiles pour un test d'intrusion en boîte noire
    - ✓ Exploitations de mauvaises configurations ou vulnérabilités

Outillage

- Bizploit (Sapyto) : « Metasploit-like »
  - Permet la collecte d'informations, de défauts de configuration ou vulnérabilités connues, exploitation
  - Automatisation
  - Génération de recommandations



Outillage

- Metasploit
  - « auxiliary/sap » : contient la majorité des scripts de Bizploit
  - Plus actif que Bizploit grâce à la communauté

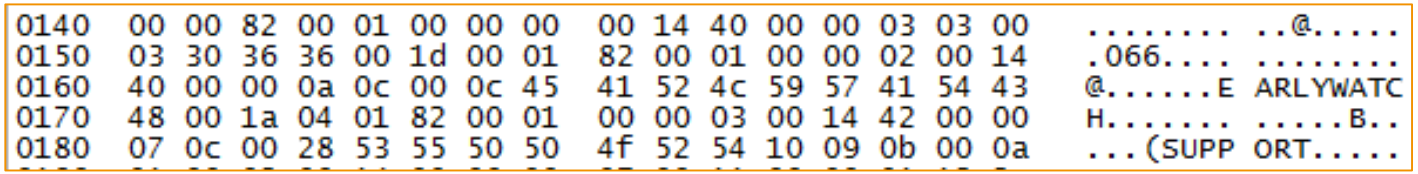
```
sf auxiliary(sap_router_portscanner) > show options

odule options (auxiliary/scanner/sap/sap_router_portscanner):

   Name         Current Setting            Required  Description
   ----         ---------------            --------  -----------
   CONCURRENCY  10                         yes       The number of concurrent ports to check per host
   INSTANCES    00-99                      no        SAP instance numbers to scan (NN in PORTS definition)
   MODE         SAP_PROTO                  yes       Connection Mode: SAP_PROTO or TCP  (accepted: SAP_PROTO, TCP)
   PORTS        1128,8000,3200,7200,50013  yes       Ports to scan (e.g. 3200-3299,5NN13)
   RESOLVE      remote                     yes       Where to resolve TARGETS (accepted: remote, local)
   RHOST        192.168.253.133            yes       SAPRouter address
   RPORT        3299                       yes       SAPRouter TCP port
   TARGETS      127.0.0.1                  yes       Comma delimited targets. When resolution is local address ran

sf auxiliary(sap_router_portscanner) > run

*] Scanning 127.0.0.1
!] Warning: Service info could be inaccurate

ortscan Results
===============

   Host       Port   State  Info
   ----       ----   -----  ----
   127.0.0.1  1128   open
   127.0.0.1  3200   open   SAP Dispatcher sapdp00
   127.0.0.1  50013  open   SAP StartService [SOAP] sapctrl00
   127.0.0.1  7200   open   LiveCache MaxDB (formerly SAP DB)
   127.0.0.1  8000   open   SAP ICM HTTP

*] Auxiliary module execution completed
```

Plan

- Introduction
- Outillage
- Mots de passe
- Défauts de configuration
- Conclusion

Mots de passe / Interception

- SAP DIAG
  - Protocole utilisé pour les connexions entre SAP et des clients lourds
  - Toutes les données sont compressées
    - ✓ Sécurité par l'obfuscation : des travaux de reverse engineering ont permis d'obtenir l'algorithme utilisé
- Même problématique qu'une authentification sur HTTP
  - Capture d'identifiants immédiate grâce à Wireshark et Cain



Mots de passe / Rétrocompatibilité

- Plusieurs méthodes de stockage de mots de passe

Version	Description
A	Algorithme propriétaire
B	MD5, tronqué à 8 caractères, insensible à la casse, ASCII
D	MD5, tronqué à 8 caractères, insensible à la casse, UTF-8
E	Version corrigée de D
F	SHA-1, 40 caractères, sensible à la casse, UTF-8
G	**CODVN B (MD5) et CODVN F (SHA-1)**
H	SHA-1, mot de passe salé aléatoirement
I	**CODVN B (MD5), CODVN F (SHA-1) et CODVN H (SHA-1)**

→ Mots de passe stockés plusieurs fois pour les versions G et I

- ✓ Souci de rétrocompatibilité
- ✓ Le niveau de sécurité du mot de passe correspond à la plus « faible » empreinte

Mots de passe / Rétrocompatibilité

- Exploitation
  - Si longueur (mot de passe) < 9
    - ✓ Casser l'empreinte MD5 suffit
      - SHA-1 devient inutile
  - Sinon
    - ✓ Casser l'empreinte MD5 permet d'obtenir les 8 premiers caractères (*p*)
    - ✓ Générer un dictionnaire de mots préfixés par *p*
    - ✓ *Bruteforcer* l'empreinte SHA-1

B	MD5, tronqué à 8 caractères, insensible à la casse, ASCII

F	SHA-1, 40 caractères, sensible à la casse, UTF-8
H	SHA-1, mot de passe salé aléatoirement

Mots de passe / Protections

- Ajouter une couche de chiffrement (« SNC »)
- Imposer des critères de complexité de mots de passe
  - ✓ login/min_password_lng
  - ✓ login/min_password_letters
  - ✓ login/min_password_specials
  - ✓ …
- Restreindre les accès à certaines tables
  - ✓ USR02
  - ✓ USH02
  - ✓ USRPWDHISTORY

Plan

- Introduction
- Outillage
- Mots de passe
- Défauts de configuration
- Conclusion

Défauts de configuration / SAPRouter

- Exemple de mauvaise configuration :

```
P  192.168.*   sapserver 3200
P  *           *         *
```

  - Toute connexion est autorisée vers tout service
    - ✓ Typique d'un environnement de test

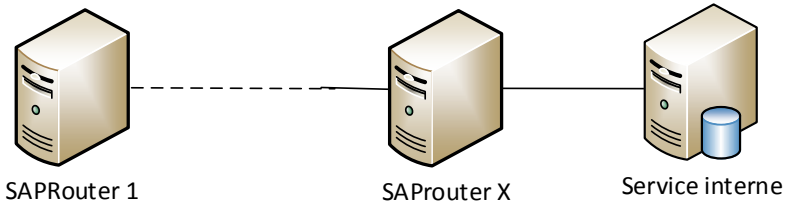
  - Risques :
    - ✓ Connexions illégitimes
    - ✓ Accès au SAPRouter (informations système, connexions actives)

```
msf auxiliary(sap_router_info_request) > run

[+] 192.168.56.101:3299 - Connected to saprouter
[+] 192.168.56.101:3299 - Sending ROUTER_ADM packet info request
[+] 192.168.56.101:3299 - Got INFO response
[+] Working directory   : C:\usr\sap\NSP\SYS\exe\uc\NTI386
[+] Routtab             : ./saprouttab

[SAP] SAProuter Connection Table for 192.168.56.101
==================================================

   Source        Destination     Service
   ------        -----------     -------
   192.168.56.1  192.168.56.101  sapdp00
```

auxiliary/scanner/sap/sap_router_info_request

Défauts de configuration / SAPRouter

- Si l'accès au SAPRouter est possible
  - → Exploitation du SAPRouter pour rebondir sur le réseau interne
    - ✓ Scan de ports
    - ✓ Recherche de vulnérabilités
    - ✓ …
- SAP impose une limitation :
  - → Accès refusé à tout service non-SAP implicitement autorisé (« * »)
    - ✓ Refus par le dernier SAPRouter sur la route



Défauts de configuration / SAPGateway

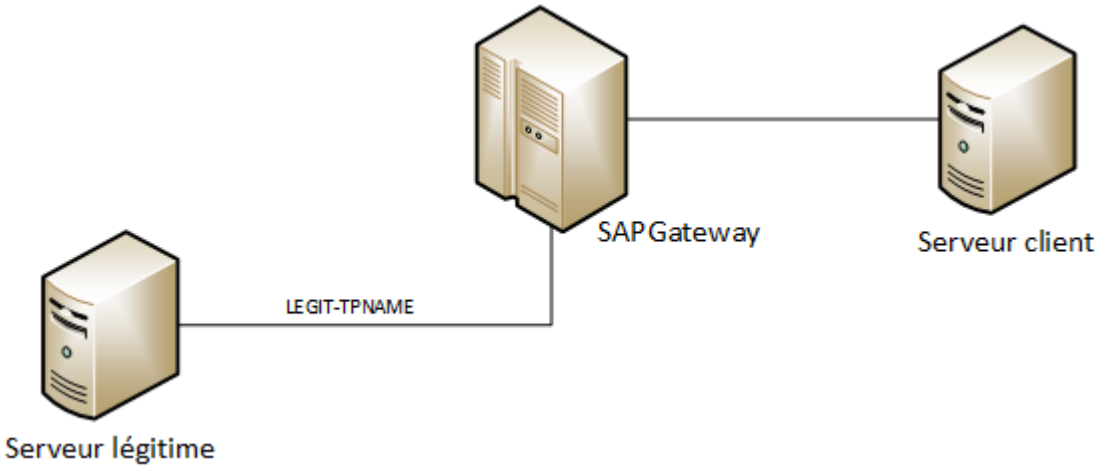
- *Register* mode
  - Permet aux serveurs ou programmes externes de s'enregistrer eux-mêmes auprès de la passerelle
  - Il suffit de fournir un identifiant de programme (« tpname »)
    - ✓ Pour chaque demande d'exécution du tpname X, le serveur sera contacté

Vulnérabilité + défauts de configuration

Usurpation serveur et/ou compromission client

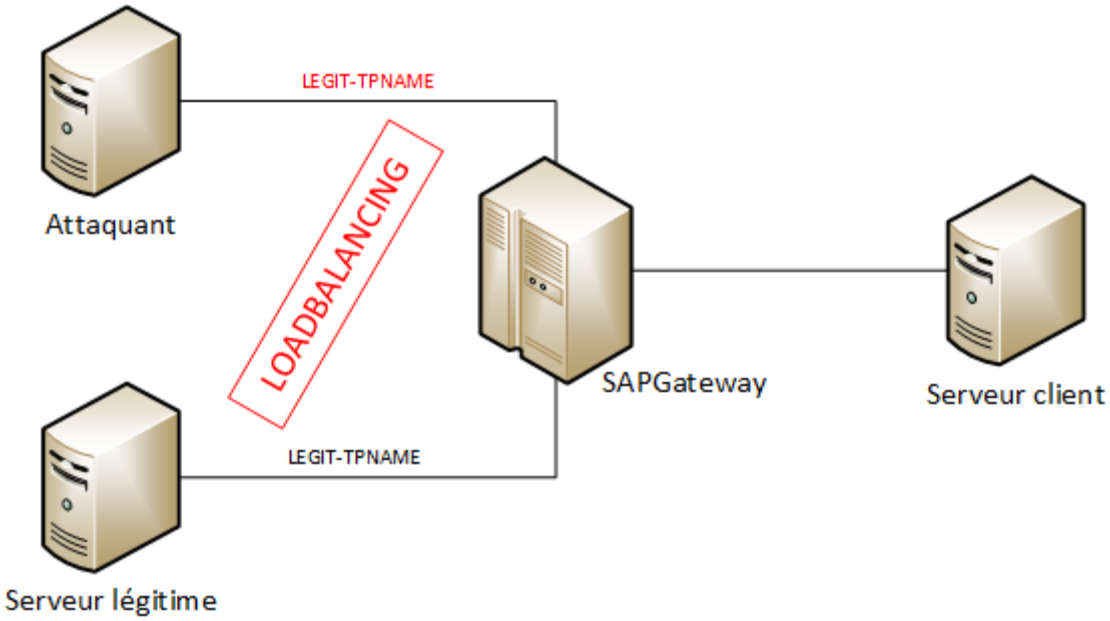
Défauts de configuration / SAPGateway

- Exploitation 1 : *Evil Twin*



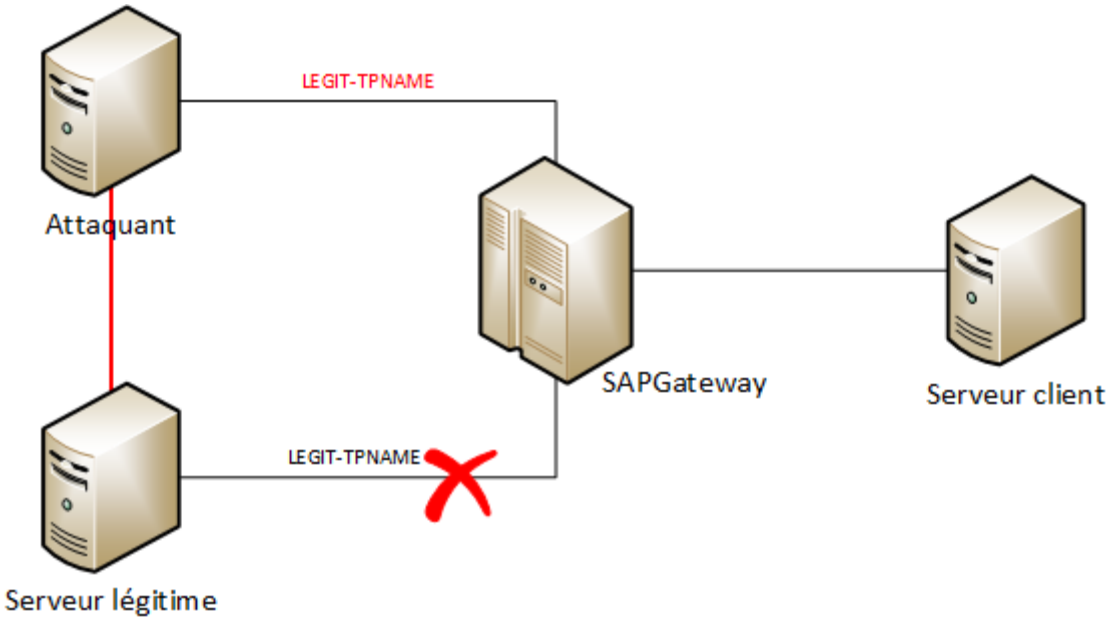
Défauts de configuration / SAPGateway

- Exploitation 1 : *Evil Twin*



Défauts de configuration / SAPGateway

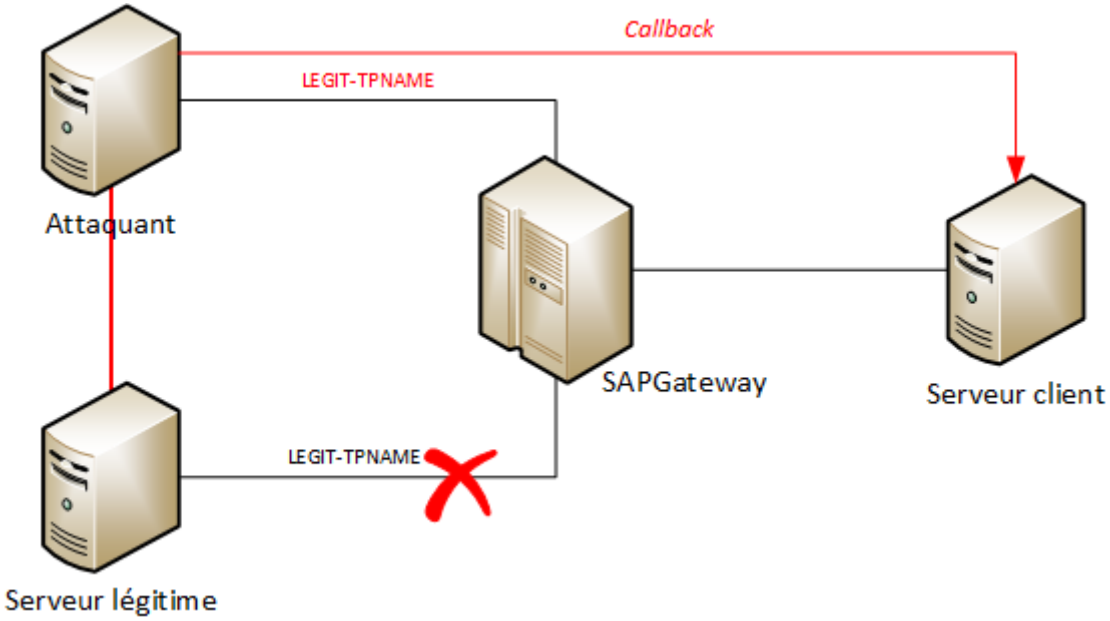
- Exploitation 1 : *Evil Twin*



- Divulgation de données

Défauts de configuration / SAPGateway

- Exploitation 2 : *Callback attack*
  - Le serveur peut demander l'exécution d'une commande post-traitement



Compromission du client

Défauts de configuration / SAPGateway

- Protections
  - Appliquer les « SAP Notes » (1003908, 1003910, 1004084, 1005397)
    - ✓ Application de *patches* de sécurité sur les serveurs SAP
  - Restreindre l'enregistrement des programmes externes

```
USER=*, HOST=*, TP=Prgm1
USER=*, HOST=host1, TP=Prgm2
```

Plan

- Introduction
- Outillage
- Mots de passe
- Défauts de configuration
- Conclusion

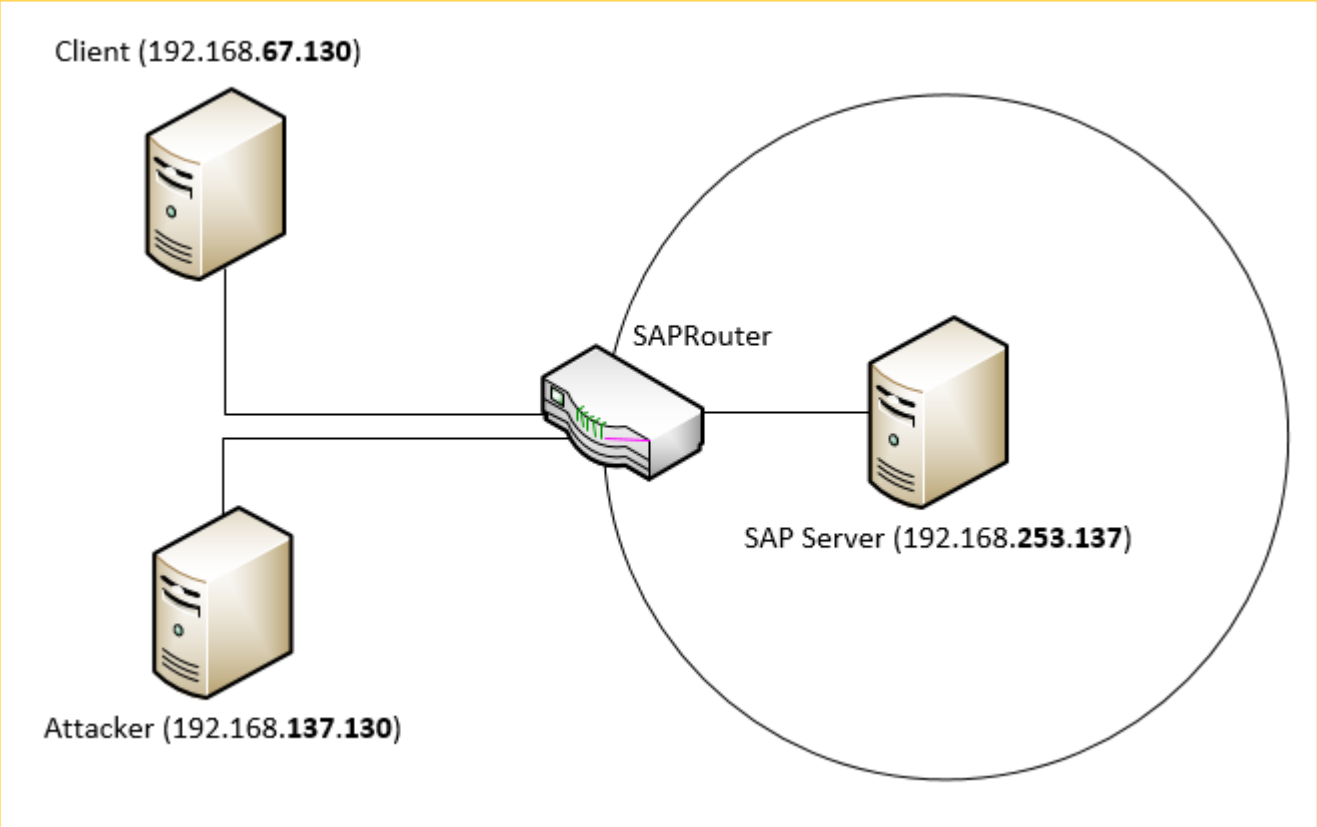
Conclusion

- Les points présentés ici ne représentent qu'une infime partie des vecteurs d'attaque
  - → Chaque module SAP peut apporter son lot de vulnérabilités
- Rapide correction des vulnérabilités par SAP AG
  - → Mais les patches tardent à être appliqués…
    - ✓ Appréhension de modifier une « configuration qui marche »
- Fonctions d'audit disponibles
  - → Ex. : présence de mots de passe faibles
  - → Utilisées ?

Conclusion

- Lectures recommandées :
  - Onapsis : http://www.onapsis.com/research-publications.php
  - ERPScan : http://erpscan.com/publications/the-sap-netweaver-abap-platform-vulnerability-assessment-guide/
  - MISC n°72 !

Démo !



Merci de votre attention
Questions ?