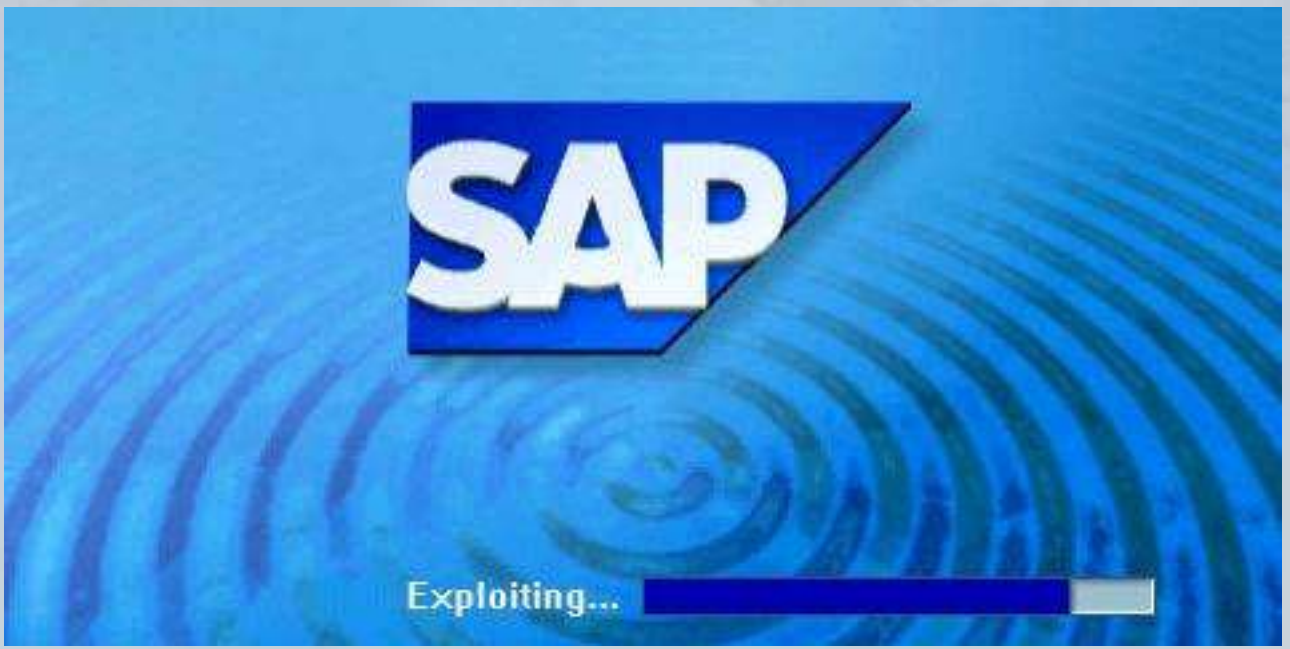
Exploiting SAP R/3



Nicolas Grégoire (ngregoire@exaprobe.com)

Introduction

- SAP : “Enterprise Resource Planning”
- Dave Aitel : “Tools such as SAP [...] typically hold a company's most valuable data, but for a variety of reasons have no public security record”
- Architecture “3 tiers” :
  - SGBD
  - Serveur applicatif
  - Présentation (ITS, SAPGUI, SAP RFC)

Attaquer les couches sous-jacentes

- L'OS n'est pas intégré au cycle d'application des mises à jour (si existant dans la structure) :
  - telnetd ou sadmin sous Solaris
  - RPC/DCOM sous Windows
- Le SGBD (typiquement Oracle) possède ses propres failles :
  - tnscmd.pl
  - bulletins NGS (“Unbreakable”)

Exploiter le frontal Web

- Sec-Consult vs. ITS :
  - XSS
  - divulgation de fichiers
- FX vs. ITS :
  - débordements de tampon
  - bugs de format

Pirater via la GUI

- Interception des mots de passe lors de l'utilisation de SAPGUI (selon les versions/OS)

- Utilisation des mots de passe par défaut :
  - SAP* / 06071992 (!)
  - DDIC / 19920706
  - SAPCPIC / ADMIN
  - EARLYWATCH / SUPPORT

- Exécution de commandes (transaction SM69)

API réseau : SAP RFC

- Implémentation par SAP des RPC
- Librement téléchargeable (Windows et Linux)
- Par design, certaines fonctions ne logguent pas les échecs de connexion :
  - RFC_PING
  - RFC_SYSTEM_INFO
  - RFC_LOGIN
  - ...

API réseau : SAP RFC (suite)

- Utilisation de RFC_SYSTEM_INFO :
  - “sapinfo” n'affiche pas tout
  - IP interne, versions du SGBD et du système d'exploitation récupérables
- Utilisation de RFC_LOGIN :
  - Pas de log en cas d'échec
  - Pas de blocage du compte
  - 1ère version publique : THC-Hydra 4.0

Futur

- Rétro-conception de l'algorithme d'encryption des mots de passe (champ BCODE dans USR02)
- Débordements de tampons exploitables via le réseau (fuzzing avec Spike ou SMUDGE)
- “I have a single UDP packet, which executes shell commands on a R/3 as NTAuthority SYSTEM or root depending on the platform.”

Liens

- Mots de passe par défaut
  - http://www.hoelzner.de/security/sap_default_passwords.php
- Failles ITS
  - http://www.websec.org/adv/sap.txt.html
  - http://www.phenoelit.de/whatSAP/
  - http://www.phenoelit.de/stuff/Phenoelit20c3.pdf
- Exécution de commandes (SM69)
  - http://www.tisc2001.com/newsletters/316.html

Liens (suite)

- THC-Hydra
  - http://www.thc.org/thc-hydra/
- SAP pour Linux (RFC API, documentation, ...)
  - http://www.sap.com/solutions/netweaver/linux/eval/index.asp
- SAPGUI
  - ftp://ftp.sap.com/pub/sapgui/java/