s(4)u for Windows

Aurélien Bordes – aurelien26 (at) free (dot) fr

SSTIC – 4 juin 2015

Pas de commande **su** sous Windows

- Il n'existe pas de commande native sous Windows permettant, à un utilisateur privilégié, de prendre l'identité de n'importe quel utilisateur

```
# whoami
root
# su user
$ whoami
user
```

- Même problématique pour passer SYSTEM ou vers un autre compte de service (LocalService, NetworkService)

Ce qui existe

- La commande **`runas`** permet de changer d'utilisateur, mais ceci nécessite son mot de passe
  - Problématique d'imputabilité des actions

- Divers outils, de type **`PsExec`**, permettent de passer SYSTEM, mais il subsiste plusieurs limitations :
  - « Bruyant » pour le système (installation de service)
  - Impossibilité de passer sous l'identité d'autres comptes de service (`S-1-5-19`, `S-1-5-20`, `S-1-5-80-…`, `S-1-5-87-…`)

- Autres solutions possibles :
  - Modification des *tokens* directement dans le noyau
  - Utilisation de l'API `CreateToken`

S4U - Service-for-User

- S4U est apparu avec Windows Server 2003 (*S4U2self* et *S4U2proxy*)

- Utilisé avec Kerberos, S4U permet de mettre en œuvre la délégation d'authentification
  - Obtention, par un service, de tickets de service au nom de n'importe quel utilisateur membre de l'Active Directory

- Ces tickets de service peuvent ensuite servir à générer, via l'*impersonation*, des *tokens*

S4U pour msv1_0 (NTLMSSP)

- S4U est également mis en œuvre par le SSP msv1_0
- S4U de msv1_0 permet :
  - de créer un *token* pour prendre l'identité de n'importe quel utilisateur
  - d'ajouter des SID arbitraires au jeton créé
- Très simple à mettre en œuvre
- DÉMO

Limitations

- Nécessite les privilèges :
  - SeTcbPrivilege
  - SeAssignPrimaryTokenPrivilege
- Ces privilèges ne sont pas, par défaut, accordés au groupe Administrateurs, mais ses membres peuvent modifier la politique de sécurité locale
- Aucun secret d'authentification (empreinte NTLM) n'est associé à la session d'authentification créée par s4u (pas de saisie de mot de passe)

Questions ?

https://github.com/aurel26/s-4-u-for-windows