Sécurité des systèmes d'exploitation

Introduction à la sécurité des annuaires Active Directory

Active Directory

- Introduit dans Windows 2000 Server en remplacement des domaines NT4 (type Samba <=3)
  - Déploiement *On Premise* ou *cloud* (Azure AD)
  - Renommé en *Active Directory Directory Services* (AD DS) depuis Windows Server 2008
- Regroupement administratif de ressources
  - Machines, utilisateurs, groupes, imprimantes, …
  - Ressources organisées dans un annuaire

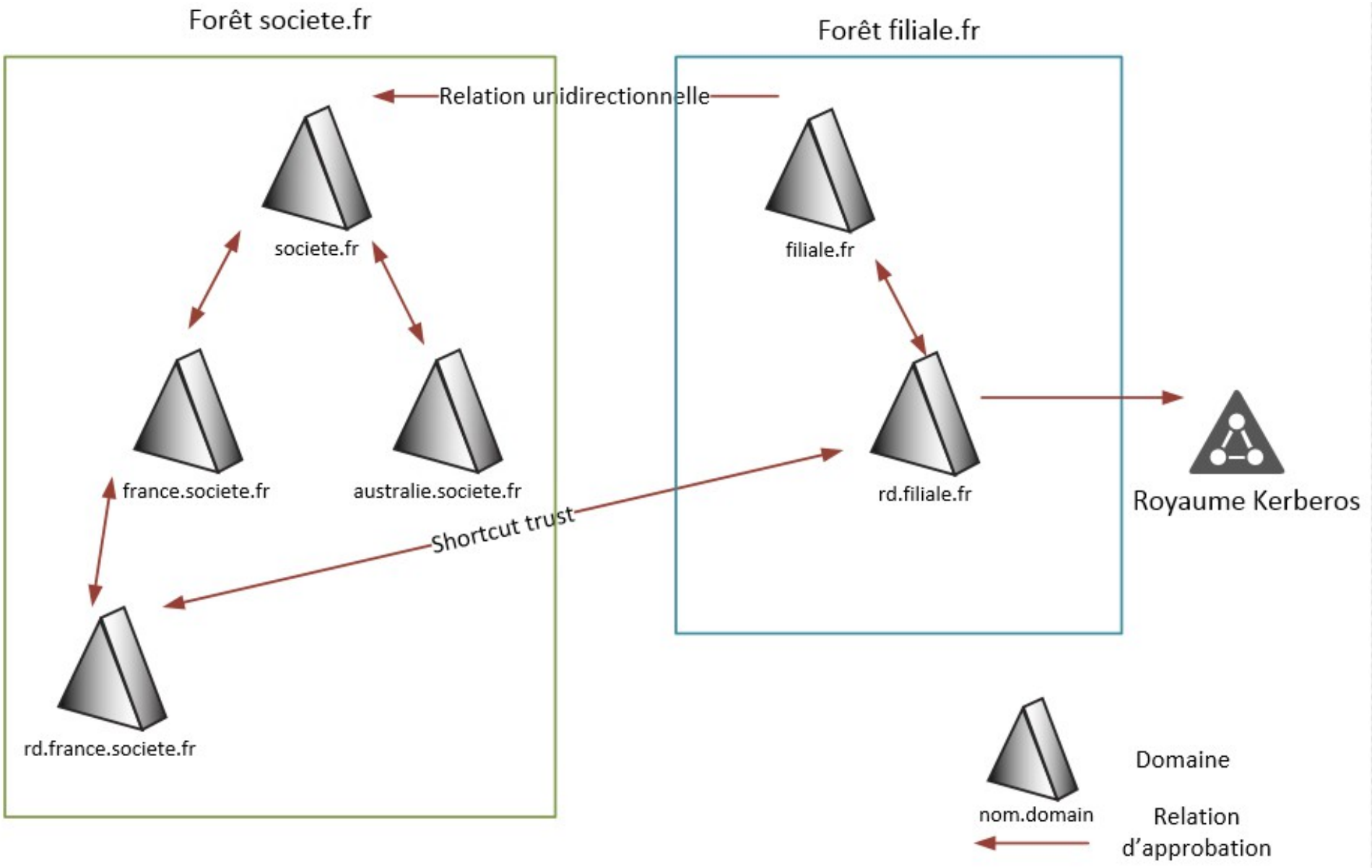
Active Directory

- Repose sur un ensemble de services qui utilisent a minima (liste étendue selon version)
  - des protocoles standards sur Internet
    - DNS : 53/TCP/UDP
    - SNTP : 123/UDP
    - LDAP (ou LDAPS): 389/TCP/UDP, 636/TCP, 3268/TCP, 3269/TCP
    - Kerberos v5 (avec des extensions) : 88/TCP/UDP et 464/TCP/UDP
  - mais pas uniquement
    - SMB/CIFS : 445/TCP
    - RPC Windows : 135/TCP, 49152-65535/TCP
    - NTLM (peut se désactiver sous certaines conditions)

Active Directory

- Un contrôleur de domaine (rôle « AD DS » depuis Windows Server 2008) héberge
  - l'annuaire Active Directory
    - Annuaire type LDAP
  - un serveur Kerberos (AS et KDC)
    - Authentification centralisée
    - Domaine AD <=> Royaume Kerberos
  - des fichiers (scripts et *Group Policy Objects*) partagés avec les membres du domaine
    - Utilisés pour l'administration et la configuration (y compris politique de sécurité) des machines membres
- Les contrôleurs de domaine se répliquent entre eux (réplication multi-maître)

Active Directory



Active Directory

- Un domaine fait toujours partie d'une forêt
  - La forêt porte le nom du domaine racine (le premier domaine créé)
- Une forêt contient un arbre de domaines
  - Cet arbre peut être constitué d'un seul domaine
- La forêt constitue une frontière de sécurité
  - Les domaines d'une même forêt sont liés automatiquement par des relations d'approbations bidirectionnelle
    - Racine/arbre
    - parent/enfant

Active Directory

- Les relations d'approbations sont des liens de confiance
  - elles permettent à un sujet d'un domaine A d'accéder à une ressource d'un domaine B
- Les relations d'approbation peuvent être constituées manuellement
  - Unidirectionnelle ou bidirectionnelle
  - Entre 2 domaines de forêts différentes
    - Entre 2 domaines racines de forêts différentes : relation de forêt
  - Entre 2 domaines issus de branches différentes au sein d'une même forêt ou issus de 2 forêts liées par une relation de forêt : *shortcut trust*

Active Directory

- Les objets contenus dans l'annuaire ont des attributs de sécurité :
  - ACL (contrôle d'accès et audit) et un propriétaire
    - les opérations possibles varient en fonction des objets, par ex. :
      - Mettre à jour le mot de passe d'un utilisateur
      - Lier une GPO à une unité d'organisation
  - Les principaux ont un identifiant de sécurité (SID)
- Modèle de contrôle d'accès par défaut : DAC
  - Complété par un modèle ABAC (*Attribute Based Access Control*) à partir de Windows Server 2012
- Délégation de droits via les ACL

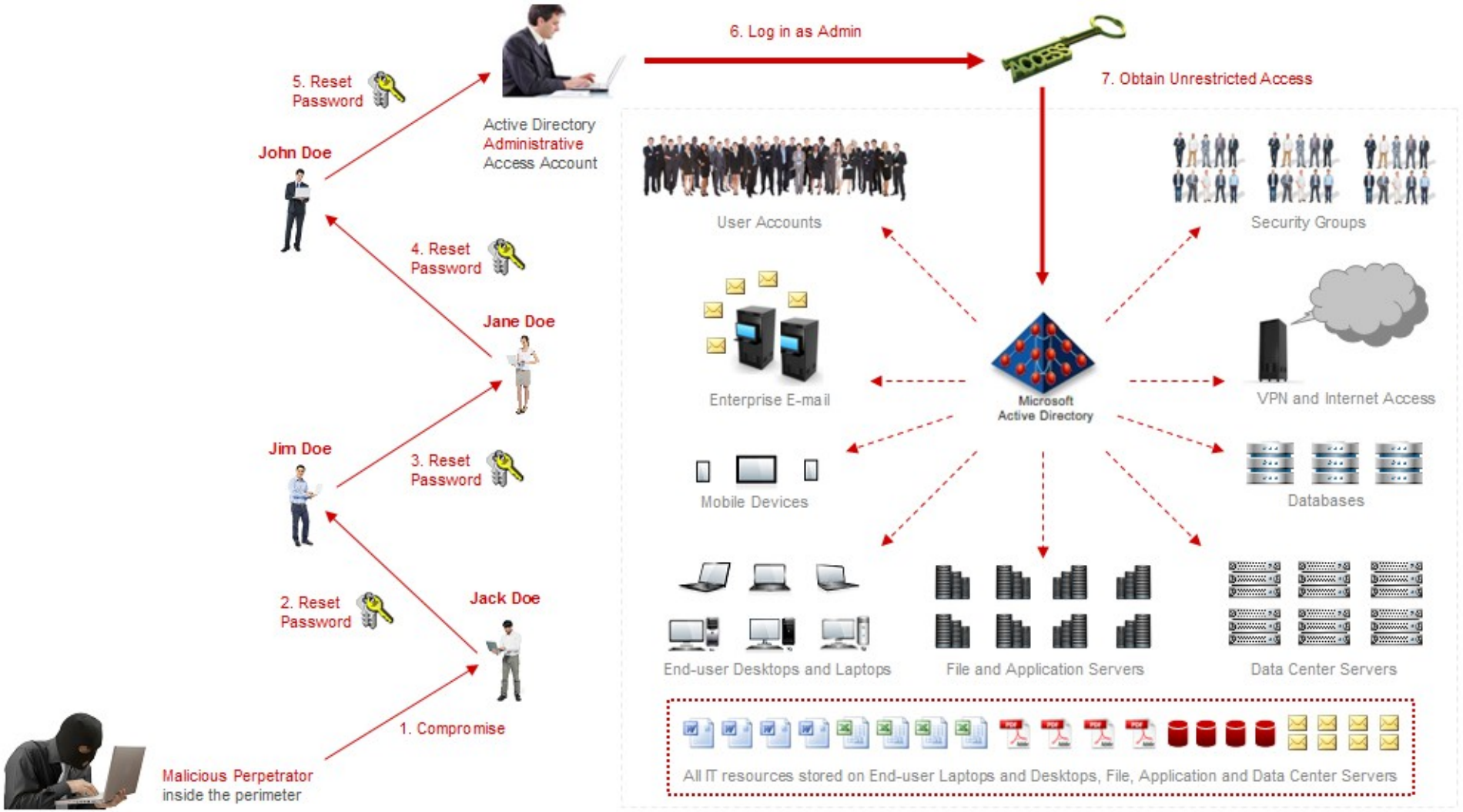
Impact sur la sécurité d'un système Windows

- Relation de confiance d'un membre du domaine envers le domaine
  - Utilisateurs et groupes
    - Y compris les comptes à privilèges
  - Configuration diffusée via les GPO
    - Politique de sécurité
      - Authentification, sécurisation de protocoles réseau, attribution des droits Windows, journalisation, filtrage réseau, configuration IPsec, contrôle applicatif,
    - Configuration de logiciels
    - Scripts (démarrage/extinction du poste, ouverture/fermeture de session)
    - Tâches planifiées

Impact sur la sécurité d'un système Windows

- Risque majeur : compromission d'un AD
  - Vol d'éléments d'authentification (*credentials*) jusqu'à obtenir un accès privilégié
    - Par ex., en cherchant dans la mémoire du processus LSASS d'une machine compromise
    - Un compte privilégié n'est pas nécessairement administrateur du domaine (furtivité)

Impact sur la sécurité d'un système Windows



Source : Paramount Defenses

Impact sur la sécurité d'un système Windows

- Quelques points d'attention sur la sécurité
  - Les contrôleurs de domaine
    - Y compris les services privilégiés présents sur ces machines : client AV, client de gestion (par ex., solution de télédéploiement), agent de sauvegarde
    - Compte krbtgt
  - Comptes et groupes privilégiés
  - Relations d'approbation
  - Stratégies de sécurité au sein des GPO
  - Canaux de communications entre les machines et les contrôleurs de domaine

Pour approfondir

- Active Directory Security, Sean Metcalf