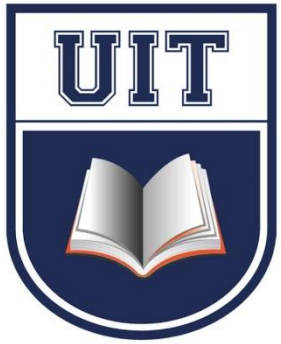

Cybersécurité

L3 RI

SECURITE DES SYSTEMES D'EXPLOITATION

Nizar Ben Neji
n.benneji@uit.tn

2020 / 2021

Protection des systèmes d'exploitation

- Protection des systèmes d'exploitation consiste à protéger les **objets** qu'il permet de manipuler:
  - Objets persistants tels que les fichiers, les périphériques, etc
  - Objets temporaires tels que les processus, les espaces de mémoire, etc
- Un objet (processus, fichier, segment mémoire) a un **propriétaire identifié**, généralement l'utilisateur qui l'a créé:
- Le propriétaire d'un objet peut avoir conféré à lui-même et à d'autres utilisateurs des **droits d'accès** à cet objet. Les types de droits possibles sont notamment :
  - droit d'accès en consultation (lecture)
  - droit d'accès en modification (écriture, destruction, création)
  - droit d'accès en exécution
- À chaque objet est donc associée une liste de **contrôle d'accès** (access control list) qui énumère les utilisateurs autorisés et leurs droits.
- Avant toute tentative d'accès à un objet par un utilisateur ou un processus, l'identité doit être authentifiée (serveur d'authentification).

Menaces sur les systèmes d'exploitation

- Risques lorsque l'accès physique à la machine est possible ou l'accès logique au système est possible (vol de la machine, de ses disques, installation de logiciels malveillants, modification des paramètres, …)
- Propagation et infection des machines par les logiciels malveillants (Virus, Ver, Cheval de Troie, Porte dérobée, Rançongiciel, …)
- Supports amovibles et les espaces de partage réseau non contrôlés,
- Intrusion et compromission d'une machine connectée
- Exploitation des erreurs de configuration de mises à jour non appliquées (Système ouvert, Administration à distance non sécurisée, …)
- Dénis de service (DoS ICMP, Smurf attaque (DDoS ICMP), …)
- Usurpation d'identité (IP/ARP Spoofing)
- Erreurs humaines (ne pas être root)
- Aspect multi-utilisateurs et partage de la machine (responsabilités en cas de problèmes)
- Pannes matérielles et bugs logicielles
- Saturation du disque et de certaines partitions
- …

Solutions et bonnes pratiques pour la sécurité système

- **Durcissement des systèmes** :
  - **Réduire la surface d'attaque physique**
    - Contrôle d'accès physique aux locaux
    - Attacher la machine
    - Empêcher l'ouverture de l'unité centrale pour empêcher le vol des éléments (ex. disques durs) ou retrait de la pile du BIOS pour supprimer le mot de passe.
    - Empêcher le redémarrage
    - Réduire la nuisance des périphériques
      - Limiter l'usage des clés USB et des disques amovibles
      - Désactiver les exécutions autoruns

Solutions et bonnes pratiques pour la sécurité système

- **Réduire la surface d'attaque système**
  - **Sécurité du système au démarrage**
    - **Sécurité du BIOS (Basic Input Output System):** système élémentaire d'entrée/sortie est un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère de l'ordinateur, lui permettant d'effectuer des opérations de démarrage de base et ce lors de la mise sous tension.
    - Installer/configurer un chargeur de démarrage ou chargeur système
  - **Sécurité de l'accès au système**
    - Mot de passe obligatoire et robuste pour l'accès au système
    - Ne pas proposer de noms d'utilisateurs
    - Ne pas afficher des étoiles (longueur plus difficile à connaitre)
    - Ouverture plus sécurisée de la session pour s'assurer qu'un virus ne crée pas un faux écran de connexion

Solutions et bonnes pratiques pour la sécurité système

- **Verrouillage**
  - Verrouillage automatique après un temps d'inactivité (pas trop long)
  - Réactivation ne doit se faire que avec mot de passe comme la nouvelle connexion
  - Rabattre l'écran d'un ordinateur portable permet de le verrouiller
- **Comptes/Connexions/Autorisations**
  - Privilèges minimaux pour l'usage demandé
  - Limitation des connexions à certains moments et de certaines zones
  - Désactiver les comptes inactifs
  - Pas de comptes partagés
  - Prévoir une politique de mots de passe pour la gestion des comptes systèmes (Périodicité, Passation, Interdire des mots de passe faibles et par défaut, …)

Solutions et bonnes pratiques pour la sécurité système

- **Réduire la surface d'attaque réseau**
  - Activer et configurer le pare-feu local de la machine, en cohérence avec les services et applications exécutées: Le parefeu du système contrôle les connexions réseaux et le trafic entrant et sortant sur la machine et ce pour bloquer les ouvertures de connexions suspectes de et vers le système en question
  - Limiter au juste besoin les services en écoute pour chaque interface réseau.
  - Accès distant sécurisé et limité dans le temps et dans l'espace (adressage): VPN, SSH, etc

Solutions et bonnes pratiques pour la sécurité système

- **Réduire la surface d'attaque applicative**
  - Désactivez les services inutiles et limitez au juste besoin les services lancés.
  - Désinstaller les programmes inutiles et limiter au juste besoin les outils de gestion à distance.
  - Contrôler l'installation des nouveaux programmes (ne pas donner aux utilisateurs simples les droits d'installation, Installer et mettre à jour les logiciels nécessaires & autorisés de manière centralisée, et avec les sources officielles, etc)
  - Principe du moindre privilège pour les comptes de service associés aux logiciels.
  - Privilégier les applications web aux clients lourds.
  - Sécurité par l'obscurité: Configurer tous les systèmes, applications et services de façon à ne pas divulguer aucune information relative aux types et aux versions utilisées.

Solutions et bonnes pratiques pour la sécurité système

- **Contrôle d'intégrité:** Le contrôleur d'intégrité surveille le système de fichiers et vérifie si les données et les métadonnées ont été altérées ou non. Le contrôleur d'intégrité est passif et il génère une alerte à chaque fois qu'un fichier est modifié, créé ou supprimé sur la machine en question. Le contrôleur d'intégrité doit être installé sur une machine réputée saine, il ne doit pas surveiller les fichiers de données utilisateur mais plutôt les propriétés des fichiers et les partitions du système. Les propriétés des fichiers à surveiller portent sur:
  - Contenu des fichiers (données/informations)
  - Contenant (enveloppe) ou encore les métadonnées (taille, droit d'accès, date de la dernière modification, propriétaires des fichiers, etc)
- **Supervision et surveillance système**
  - Eviter les arrêts de service et limiter toute perte de productivité
  - Détecter le plutôt possible les problèmes de disfonctionnement et prévenir même les pannes
  - Surveiller l'usage des ressources (CPU, mémoire, espace disque, etc)
  - Remonter des alertes en temps réel

Solutions et bonnes pratiques pour la sécurité système

- **Détection d'intrusion système (HIDS):**
  - Surveiller le trafic entrant et sortant
  - Surveiller les fichiers log du système, des services et des applications installées
  - Surveiller l'intégrité des fichiers systèmes et des fichiers de configuration
- **Solution anti-virus** pour la protection contre les malwares
- ..

Solutions et bonnes pratiques pour la sécurité système

- **Politique de Sécurité Système** est un document qui définit les règles à suivre pour la sécurisation des systèmes d'exploitation. Elle est mise en place par l'Administrateur Système qui sera en charge de l'installation, du paramétrage, de la sauvegarde, de la restauration, de la planification, de la supervision, du support et de la veille technologique.
- **Politique des Mots de Passe** est un document englobant l'ensemble des règles de création, de changement, d'utilisation et d'annulation à appliquer pour la protection des mots de passe (Périodicité des changements, changement des mots de passe lors des passations, robustesse, …).
- **Charte informatique** pour rappeler le bon usage des ressources informatiques de l'entreprise.