Activité d'Intégration 1

Comment savoir qu'on est attaqué et qu'est-ce qu'il faut faire comme mesures de premiers secours?

Dr.-Ing. Austin Waffo Kouhoué, PhD

UNITECH-DESS TI- 2025 - austin.waffo@gmail.com

Comment savoir qu'on est attaqué ?

Performances anormales

- Ralentissements soudains et inexpliqués
- Blocages fréquents ou redémarrages intempestifs
- Augmentation excessive de l'utilisation du CPU, de la RAM ou du disque dur.

Comment savoir qu'on est attaqué ?

Performances anormales

- Ralentissements soudains et inexpliqués
- Blocages fréquents ou redémarrages intempestifs
- Augmentation excessive de l'utilisation du CPU, de la RAM ou du disque dur.

Activité réseau suspecte

- Connexions Internet plus lentes que d'habitude.
- Transferts de données inhabituels, même lorsque vous ne faites rien.
- Présence de connexions inconnues ou suspectes dans le gestionnaire de tâches (**netstat -ano** sous Windows ou **lsof -i** sous Linux).

Comment savoir qu'on est attaqué ?

Activité réseau suspecte(suite et fin)

- Présence de connexions inconnues ou suspectes dans le gestionnaire de tâches :
  - **Trouver le processus associé** `tasklist /FI "PID eq 1234"`

Comment savoir qu'on est attaqué ?

Activité réseau suspecte(suite et fin)

- Présence de connexions inconnues ou suspectes dans le gestionnaire de tâches :
  - **Trouver le processus associé** `tasklist /FI "PID eq 1234"`
  - **Détection d'un Port Occupé**
  - Syntaxe : `netstat -ano | findstr :PORT`
  - Exemple : Par exemple, pour vérifier le port 80 `netstat -ano | findstr :80`

Comment savoir qu'on est attaqué ?

Programmes et fichiers inhabituels

- Apparition de nouveaux fichiers ou applications que vous n'avez pas installés.
- Modifications inexpliquées de fichiers existants.
- Applications qui se ferment ou se lancent sans votre intervention

Comment savoir qu'on est attaqué ?

Programmes et fichiers inhabituels

- Apparition de nouveaux fichiers ou applications que vous n'avez pas installés.
- Modifications inexpliquées de fichiers existants.
- Applications qui se ferment ou se lancent sans votre intervention

Messages ou comportements anormaux

- Pop-ups intempestifs ou messages d'alerte inhabituels.
- Transferts de données inhabituels, même lorsque vous ne faites rien.
- Demandes de rançon ou messages indiquant un chiffrement de vos fichiers (ransomware)
- Amis ou collègues recevant des e-mails étranges de votre part

Comment savoir qu'on est attaqué ?

Changements dans les paramètres système

- Le pare-feu ou l'antivirus désactivé sans raison
- Modifications des paramètres réseau (ex. : serveur proxy modifié)
- Comportements anormaux du navigateur (ex. : redirections inattendues, moteur de recherche modifié)

Comment savoir qu'on est attaqué ?

Changements dans les paramètres système

- Le pare-feu ou l'antivirus désactivé sans raison
- Modifications des paramètres réseau (ex. : serveur proxy modifié)
- Comportements anormaux du navigateur (ex. : redirections inattendues, moteur de recherche modifié)

Que faire si vous suspectez une attaque ?

Opérations

- 1 Déconnectez votre ordinateur d'Internet pour limiter les dégâts
- 2 Analysez votre système avec un antivirus ou un antimalware (ex. : Malwarebytes, Windows Defender, ClamAV).
- 3 Vérifiez les processus actifs (Gestionnaire des tâches sous Windows, htop sous Linux)
- 4 Regardez les programmes qui se lancent au démarrage (msconfig sous Windows, systemctl list-units –type=service sous Linux)

Que faire si vous suspectez une attaque ?

Opérations

1. Regardez les programmes qui se lancent au démarrage (msconfig sous Windows, systemctl list-units –type=service sous Linux)
2. 5 Mettez à jour votre système et vos logiciels pour corriger d'éventuelles failles de sécurité
3. 6 Changez vos mots de passe si vous pensez qu'ils ont été compromis.
4. 7 Consultez un expert en cybersécurité si l'attaque est grave.