TP Analyse

Tout d'abord nous avons Josiane de la comptabilité qui nous contacte à propos de ralentissement, elle mentionne une charte informatique ce qui est notable. Elle nous explique qu'elle a de gros ralentissements sur sa machine (réseau ou système). Ensuite elle nous mentionne un message contenant « Conflit d'IP détecté ». Elle redémarre son ordinateur (ce qui est aussi notable, tous les utilisateurs ne pensent pas forcément au redémarrage). Elle nous fait part de son hypothèse sur « le petit jeune » qui aurait installé le photocopieur (quelqu'un d'interne à la société ou alors quelqu'un d'externe ?).
Sa collègue de travail Corinne, est-elle aussi impactée. Elles sont inquiètes car c'est la compta de fin d'année (celle qui semblerait très importante donc elle nous presse un petit peu).

D'autre part elle nous dis qu'elle est parfois redirigée vers des sites internet étranges.

Pour donner suite à cet échange nous pouvons émettre des hypothèses :

- Ce fameux jeune qui est venu installer le photocopieur. S'il fait parti de l'entreprise et du service informatique il y a peu de chance que ce soit lui qui a introduit un malware en installant le photocopieur. S'il n'est pas de la société je ne comprendrais pas pourquoi il viendrait installer un photocopieur, le service informatique est doté des compétences pour le faire normalement.
- Pour les ralentissements de l'ordinateur : cela peut être dû à un logiciel malveillant visant à interrompre le travail et perturber le réseau.
- Pour le conflit d'IP : cela peut venir d'un appareil qui a réussi à s'introduire dans le réseau et qui cherche à avoir une IP pour contacter d'autres machines ou serveurs pour les infecter à leur tour.
- Pour la redirection vers des sites bizarres : cela vient sûrement d'un fichier ou d'une pièce jointe qui a été ouverte et qui contenait sûrement un malware.

Différentes solutions pour régler les potentiels problèmes détectés :

Audit Complet du Réseau : Procéder à une évaluation exhaustive pour repérer toute activité anormale qui pourrait indiquer une intrusion ou un dysfonctionnement. Révision de la Configuration Réseau : Examiner en détail les paramètres DHCP et rechercher l'existence de dispositifs connectés au réseau sans autorisation. Réaction en cas d'Attaque : En cas de découverte d'une attaque active, agir rapidement pour isoler les dispositifs compromis et neutraliser la menace.

Pour les Ralentissements de l'Ordinateur :

- Scan Antivirus Approfondi → Utiliser un logiciel de sécurité fiable pour scanner le système à la recherche de tout type de logiciel malveillant.

- Inspection du Matériel : Contrôler le bon fonctionnement du matériel, en mettant l'accent sur l'état du disque dur, pour identifier d'éventuelles défaillances matérielles.

Face aux Redirections de Navigateur Indésirables :

- Utilisation d'Antimalware : Déployer des solutions antimalware robustes pour détecter et supprimer tout logiciel malveillant affectant le navigateur.
- Contrôle et Réinitialisation des Paramètres : Examiner minutieusement et réinitialiser les paramètres DNS et du navigateur pour garantir qu'ils n'ont pas été altérés malicieusement. En mettant en œuvre ces solutions, l'objectif est de rétablir la sécurité et le bon fonctionnement des systèmes informatiques, tout en s'attaquant à la racine des problèmes identifiés pour prévenir de futures occurrences.

Voici les différents points qui sont pour ma part à voir et à vérifier par rapport aux informations fournies en début de TP.

Stcherbinine Mattéo SIO2