TD1 – Cybersécurité – Annexe
Définitions des termes principaux

I - Cybersécurité

Ensemble de techniques et de pratiques visant à protéger les ordinateurs, les réseaux, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

Exemple : Une entreprise installe un antivirus, configure un pare-feu, impose des mots de passe complexes et forme ses employés à ne pas cliquer sur des liens suspects pour se protéger contre les cyberattaques.

II - Hameçonnage (Phishing)

Technique utilisée par des fraudeurs pour tromper les gens et leur soutirer des informations sensibles (mots de passe, numéros de carte bancaire...) en se faisant passer pour une personne ou un service de confiance (par e-mail, SMS, etc.).

Exemple : Vous recevez un e-mail prétendant venir de votre banque, vous demandant de « vérifier votre compte » via un lien. En cliquant, vous tombez sur un faux site qui enregistre vos identifiants bancaires.

III - Attaque par force brute (Bruteforce Attack)

Méthode utilisée pour deviner un mot de passe ou une clé en essayant toutes les combinaisons possibles jusqu'à trouver la bonne.

Exemple : Un pirate essaie de deviner le mot de passe de votre compte en ligne en testant des milliers de combinaisons comme « 123456 », « azerty », ou « jean1975 » jusqu'à trouver le bon.

IV - Déni de service (DoS ou DDoS)

Une attaque par déni de service (**DoS** attack pour **Denial of Service** attack en anglais) est une attaque qui consiste à surcharger un serveur ou un site web avec énormément de requêtes pour le rendre lent ou totalement inaccessible aux utilisateurs. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (**DDoS** attack pour **Distributed Denial of Service** attack).

Exemple : Un groupe de pirates envoie des millions de requêtes à un site web gouvernemental ou commercial, le rendant indisponible pour les citoyens qui veulent y accéder normalement.

V - Attaque de l’homme du milieu (Man-in-the-Middle)

Une personne intercepte secrètement les communications entre deux parties pour espionner, modifier ou voler des informations sans que celles-ci ne s’en rendent compte.

Exemple : Dans un café, un pirate crée un faux réseau Wi-Fi appelé par exemple « CaféGratuit ». Vous vous y connectez, et il intercepte toutes vos communications, y compris vos mots de passe ou données bancaires.

VI - Rançongiciel (Ransomware)

Logiciel malveillant qui bloque l’accès à un ordinateur ou chiffre les fichiers, puis demande une rançon à la victime pour les débloquer.

Exemple : Vous ouvrez une pièce jointe dans un e-mail prétendument envoyé par un collègue. Un logiciel malveillant chiffre tous vos fichiers et affiche un message exigeant 500 € en bitcoins pour les déverrouiller.

VII - Authentification MultiFactorielle (AMF ou MFA)

C’est une méthode de sécurité qui demande plusieurs facteurs de vérification pour accéder à un compte ou un service. Les facteurs peuvent être :

- Quelque chose que vous connaissez : Comme un mot de passe ou un code confidentiel mémorisé ;
- Quelque chose que vous possédez : Comme un smartphone, ou une clé USB sécurisée ;
- Quelque chose que vous êtes : Comme une empreinte digitale ou la reconnaissance faciale.

Exemple : Pour vous connecter à votre boîte mail, vous entrez d’abord votre mot de passe, puis vous devez valider un code envoyé par SMS ou une notification sur une application (comme Google Authenticator).

VIII - IDS (Intrusion Detection System) – Système de Détection d’Intrusion

C’est un logiciel ou matériel qui surveille un réseau ou un système à la recherche de comportements suspects ou d’activités malveillantes, et qui alerte les administrateurs en cas de menace. Il ne bloque pas forcément l’attaque, mais il aide à la détecter rapidement.

Exemple : Une entreprise utilise un **IDS** pour surveiller le trafic réseau. L'IDS détecte une activité suspecte, comme une tentative de connexion répétée à un serveur depuis une adresse IP inconnue, et alerte les administrateurs système. Cela permet de prendre des mesures pour bloquer l'adresse IP et prévenir une éventuelle intrusion.