

Sécurité des systèmes d'informations

- Décrivez les types d'attaques 'ciblées' et non 'ciblées' ?

Attaques Ciblées :

1. **Attaques MITM (Man-in-the-Middle) :**
 - Ces attaques visent spécifiquement une communication entre deux parties. L'attaquant se positionne entre les deux parties et intercepte ou altère les données échangées sans que les parties ne le sachent.
2. **Attaques de phishing :**
 - Le phishing cible spécifiquement les utilisateurs en leur envoyant des emails ou des messages frauduleux dans le but de leur faire divulguer des informations sensibles comme des identifiants de connexion ou des informations financières.
3. **Attaques de spear-phishing ou harponnage :**
 - Ces attaques sont similaires au phishing mais sont plus ciblées. Les attaquants recherchent des informations spécifiques sur leurs cibles pour personnaliser les attaques et augmenter leurs chances de succès.
4. **Attaques de whale-phishing :**
 - Le whale-phishing vise spécifiquement des individus ou des entités de haut niveau au sein d'une organisation, comme des dirigeants ou des cadres supérieurs, dans le but d'obtenir un accès privilégié ou des informations sensibles.
5. **Ransomware :**
 - Les attaques de ransomware ciblent spécifiquement les systèmes informatiques en chiffrant les données et en demandant une rançon en échange de leur déchiffrement.
6. **Attaques par injection SQL :**
 - Ces attaques visent spécifiquement les applications web en insérant du code SQL malveillant dans les entrées des formulaires ou des paramètres de requête pour manipuler la base de données sous-jacente.
7. **Usurpation de DNS :**
 - Cette attaque cible spécifiquement les serveurs DNS en falsifiant les informations de résolution DNS pour rediriger le trafic vers des serveurs malveillants contrôlés par l'attaquant.
8. **Le détournement de session :**
 - Cette attaque cible spécifiquement les sessions utilisateur en usurpant l'identité d'un utilisateur légitime pour accéder à des ressources sensibles ou effectuer des actions frauduleuses.
9. **Attaques par force brute :**

- Ces attaques visent spécifiquement les identifiants de connexion en testant systématiquement toutes les combinaisons possibles de noms d'utilisateur et de mots de passe.

Attaques Non Ciblées :

1. Attaques par déni de service (DoS) et DDoS :

- Ces attaques ne ciblent pas spécifiquement une entité, mais visent à rendre un système ou un réseau indisponible en submergeant ses ressources avec un trafic excessif.

2. Attaques Web :

- Ces attaques ciblent les sites web en exploitant les failles de sécurité pour compromettre les données ou causer des dommages au système.

3. Menaces internes :

- Ces menaces proviennent d'acteurs internes tels que les employés ou les sous-traitants malveillants qui exploitent leur accès légitime aux systèmes de l'organisation.

4. Trojans ou chevaux de Troie :

- Ces programmes malveillants ne sont pas spécifiquement conçus pour une cible particulière mais sont distribués de manière générale pour infecter les systèmes et exécuter des actions malveillantes.

5. Attaques Drive-by :

- Ces attaques infectent les visiteurs d'un site web sans leur consentement en exploitant les vulnérabilités des navigateurs web ou des plugins.

6. Attaques XSS (Cross-Site Scripting) :

- Ces attaques injectent des scripts malveillants dans des sites web légitimes pour voler des informations ou prendre le contrôle du navigateur de l'utilisateur.

7. Attaques par écoute clandestine :

- Ces attaques interceptent passivement les communications réseau pour collecter des informations sensibles sans altérer les données.

8. Attaque d'anniversaire :

- Cette attaque est utilisée pour trouver des collisions dans les fonctions de hachage cryptographique en exploitant les mathématiques derrière la probabilité d'anniversaire.

9. Attaque de malware :

- Les attaques de malware impliquent la distribution de logiciels malveillants qui infectent les systèmes et exécutent des actions indésirables sans le consentement de l'utilisateur.

référence <https://www.fortinet.com/fr/resources/cyberglossary/types-of-cyber-attacks> :