Sécuriser son exposition sur internet

Objectifs

La sécurisation de l'exposition sur internet vise à maitriser la diffusion d'information sur les systèmes connectés à Internet. Les bonnes pratiques mises en œuvre permettent de réduire la surface d'attaque et les tentatives de compromission du SI.

L'exposition sur internet concerne toutes les données et les traces laissées par les systèmes connectés et disponibles sur internet. Ces informations peuvent être directement issues du système d'information (de manière volontaire ou non), ou peuvent être relayées par des serveurs tiers.

Google Dorks

Le moteur de recherche Google peut être utilisé à des fins malveillantes via ce que l'on appelle les « *Google Dorks* ». Il s'agit de requêtes spéciales réalisées au moyen de certains mots-clés spécifiques et permettant de trouver des fuites d'informations sensibles ou des serveurs vulnérables.

Des sites publient des exemples de requêtes (ex : https://www.webrankinfo.com/commandes/google) et certains proposent même des listes de mots-clés permettant de faciliter la recherche de données sensibles (ex : Exploit-DB https://www.exploit-db.com/google-hacking-database/).

Shodan, Censys, Zoomeye

Il existe d'autres moteurs de recherche pouvant présenter un risque pour la sécurité de ses systèmes. Il s'agit de *Shodan*, *Censys* et *ZoomEye*. Ils répertorient et identifient les équipements connectés à Internet. Certains équipements et logiciels sensibles de son infrastructure (logiciels d'administration, base de données, routeurs, caméras IP…) peuvent se retrouver indexés et consultables. Les attaquants utilisent souvent ces services pour trouver des équipements et logiciels vulnérables.

Pour limiter son exposition

- **Durcir la configuration de ses serveurs web** exposés : suppression des fichiers installés par défaut, masquage des bannières logicielles, etc... (appliquer les recommandations de l'ANSSI pour la sécurisation des sites web)
- **Maintenir ses services à jour et appliquer les correctifs** de sécurité dès que possible (voir la fiche sur **la gestion des correctifs**)
- **Réaliser régulièrement des scans de vulnérabilité** des systèmes exposés sur Internet afin de détecter d'éventuelles erreurs de configuration, fuites de données sensibles, etc…
- **Utiliser les mêmes outils que les attaquants afin de détecter d'éventuelles vulnérabilités** sur ses serveurs. Attention, une version d'un fichier indexé sur Google peut être retrouvée même après sa suppression (visionnage du cache Google).
- **Effectuer régulièrement des recherches à partir de ces outils** afin de vérifier le maintien de la sécurité de son exposition. Attention, les résultats publiés par ces outils ne sont pas toujours à jour.

- **Ne rendre accessible sur Internet que les serveurs et les ports** pour lesquels cela est nécessaire (accès public, service à distance, etc.) et restreindre, si possible, aux ports 80 et 443. Les interfaces d'administration (SSH, RDP, etc) doivent être filtrées et uniquement accessibles depuis les réseaux internes et aux personnels dûment habilités.
- Il est aussi possible de **bloquer l'indexation de ses équipements** par la mise en place d'un filtrage :
  - **Censys** utilise les plages IP 141.212.121.0/24 et 141.212.122.0/24.
  - **Shodan** ne fournit pas les IP qu'il utilise pour ses scans mais il existe des scripts permettant de créer de manière dynamique une liste noire d'IP lors de tentatives de scan par ce service (https://github.com/romcheckfail/shodan-ip-block-list).
  - **ZoomEye** ne fournit pas d'adresse IP à bannir non plus. Le service met à disposition deux mécanismes permettant d'empêcher les scans (un premier pour les services web, et un second pour tous les autres appareils): https://www.zoomeye.org/about.