Suivi des modifications

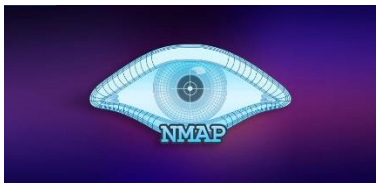
Version	Référence	Auteur	Date	Commentaires
A	D_20220205_AG	GREPILLOUX Antonin FRAIGNEAU Maxime	04/02/2022	Création

Moyen d'attaque :

Injection SQL :

L'injection SQL est une technique d'injection de code qui exploite une faille de sécurité dans la base de données d'une application. La vulnérabilité est présente lorsque la saisie de l'utilisateur n'est pas fortement typée. Cela permet d'altérer, par exemple, un lien hypertexte, ce qui entraînerait un faux résultat positif de la requête de la base de données et nous donnerait son accès.
L'utilisation du logiciel sqlmap sera privilégié dans notre cas.
sqlmap est un outil de test et d'exploitation d'injections SQL écrit en python.

Nmap :



Nmap est un scanner de ports open source. Il est conçu pour détecter les ports ouverts, les services hébergés et les informations sur le système d'exploitation d'un ordinateur distant.
L'utilisation de l'outils nmap sera important pour détecter les portes d'entré sur la machine victime, et identifié quel type t'attaque sera privilégié en premier.

Pour scanner les ports d'un ordinateur distant, Nmap utilise diverses techniques d'analyse basées sur des protocoles tels que TCP, IP, UDP ou ICMP.
Par défaut Nmap scanne les ports de 1 à 1024 et les ports indiqués dans le fichier nmap-services.
De même, il se base sur les réponses particulières qu'il obtient à des requêtes particulières pour obtenir une empreinte de la pile IP, souvent spécifique du système qui l'utilise. C'est par cette méthode que l'outil permet de reconnaître la version d'un système d'exploitation et aussi la version des services en écoute.

BruteForce :

Utilisation diverse de script Python et logiciel inclus dans Kali Linux.

L'attaque par force brute est une méthode de cryptanalyse qui consiste à trouver un mot de passe en essayant un par un tous les mots de passe possible : par exemple, si le mot de passe est « abc », il faudra d'abord essayer « a », puis « b », puis « c », jusqu'à « z ». Si le mot de passe n'est pas trouvé, il faut alors ajouter un nouveau caractère, donc il faut essayer « aa », puis « ab » et cela jusqu'à « zz » si le mot de passe n'est toujours pas trouvé. Puis nous ajoutons encore un nouveau caractère pour avoir « aaa », et nous continuons de tout essayer jusqu'à trouver le bon mot de passe, c'est-à-dire « abc » ici.

Cette méthode est simple à utiliser, dans un laps de temps défini. Néanmoins, le temps de calcul augmente considérablement selon la longueur du mot de passe (Plus le mot de passe sera long, plus la recherche de celui-ci prendra du temps). La durée de calcul du mot de passe dépend donc de 3 conditions : la puissance de calcul de la machine qui recherche le mot de passe, la longueur du mot de passe recherché et la bibliothèque de caractères exploitable (lettres majuscules, lettres minuscules et chiffres).

L'attaque par dictionnaire est une méthode utilisée pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si ce n'est pas le cas, l'attaque échouera.

Attaque dos ou DDOS :

Attaque DOS pour couper ou ralentir le serveur victime.

L'attaque par déni de service, ou DoS (en anglais Denial of Service), vise à perturber, ou paralyser totalement, le fonctionnement d'un serveur informatique en le bombardant à outrance de requêtes erronées.

Le but peut être d'affecter un service en ligne ou le réseau d'une entreprise en saturant une des ressources du système : la bande passante, l'espace de stockage, la capacité de traitement d'une base de données, les ressources de calcul des processeurs, la mémoire vive, etc.

Moyen de protection :

Fail2Ban :

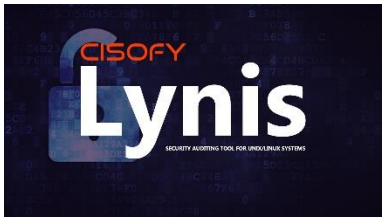
Fail2ban est une application qui analyse les logs de divers services (SSH, Apache, FTP…) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs.
Typiquement, fail2ban cherche des tentatives répétées de connexions infructueuses dans les fichiers journaux et procède à un bannissement en ajoutant une règle au pare-feu pour bannir l'adresse IP de la source.
Les objectifs de Fail2Ban sont d'éviter de surcharger les logs du système avec des milliers de tentatives de connexion et de limiter la portée des attaques répétées provenant d'une même machine.

Un serveur avec un accès SSH sur le port standard sera susceptible de recevoir très rapidement des centaines, voire des milliers de tentatives de connexions provenant de différentes machines, étant généralement des attaques par brute force lancée par des robots.
Fail2ban en analysant les logs permet de bannir les IP au bout d'un nombre de tentatives défini, ce qui limitera le remplissage des logs et l'utilisation de la bande passante.
Ceci va également rendre les attaques par brute force ou par dictionnaire beaucoup plus difficiles mais ce n'est pas une sécurité absolue contre ce type d'attaque.

Sécurisation Apache2 :

Mise en place d'une page erreur 404 si l'utilisateur essaye d'atterrir sur une page html inexistante.
Désactivation d'un message d'erreur si l'utilisateur essaye d'atterrir sur une page html inexistante. Des informations révélant la version d'apache2 et le type de machine.

Lynis :



Lynis est un outil de sécurité éprouvé pour les systèmes fonctionnant sous Linux, macOS ou des systèmes d'exploitation basés sur Unix. Il effectue un examen approfondi de la santé de vos systèmes pour soutenir le durcissement du système et les tests de conformité.

Honeypot :

Un honeypot (ou pot de miel) est dans le jargon informatique un mécanisme de sécurité.
Il permet aux administrateurs de tromper les pirates et ainsi de déjouer des cyberattaques.
Un honeypot simule des services de réseau ou des programmes d'application pour attirer les attaquants et ainsi les attirer à l'écart des serveurs de production pour éviter les dégâts.
Dans la pratique, les honeypots sont configurés en utilisant les technologies côté serveur et côté client.

-Côté serveur :
L'idée de base est d'attirer les attaquants dans des zones isolées d'un système informatique et de les éloigner ainsi des composants critiques du réseau.
Un honeypot permet également de suivre les actions d'un attaquant et d'étudier celui-ci.
Pour cela, il simule une application serveur qui mobilise un ou plusieurs services sur le réseau.
Si un attaquant est trompé par une manœuvre de diversion et commence une tentative d'attaque, le honeypot capture et enregistre toutes les activités, alerte l'administrateur et engage des contres mesures.

-Côté client :
Un honeypot côté client imite un logiciel d'application qui recourt aux services du serveur.
Un exemple récurrent serait la simulation d'un navigateur qui visite spécifiquement des pages Internet dangereuses afin de collecter des données sur les risques de sécurité.
En cas d'attaques en provenance de l'une de ces pages web, le processus de l'attaque est consigné.
Cela permet de recueillir des données permettant d'améliorer le logiciel simulé.

Sources :

https://www.ionos.fr/digitalguide/serveur/securite/honeypot-securite-informatique-via-des-leurres/

https://www.it-connect.fr/premiers-pas-avec-fail2ban/

https://doc.ubuntu-fr.org/fail2ban