

Documentation générale

Sommaire

Sommaire	1
Nos Objectifs.....	2
C'est quoi un Honeypot ?	3
Points positifs d'un honeypot	3
Points négatifs d'un honeypot :	3
Les Différents Protocoles	4
Le Protocole File Transfer Protocol (FTP) :	4
Le Simple mail Transfer Protocol (SMTP) :	4
Remote Desktop Protocol (RDP) :	5
Secure Socket Shell (SSH) :	5
C'est quoi PostgreSQL ?	6
Les Avantages.....	6
Les Inconvénients.....	6
Le Modèle ACID.....	7
C'est quoi Grafana ?	9
Avantages de Grafana :	9
Points négatifs de Grafana :	9
C'est quoi Apache2 ?	11
Avantages d'Apache2 :	11
Négatifs d'Apache2.....	11
C'est quoi Qeeqbox/Honeypot ?	12

Documentation générale

Nos Objectifs



Faire un honeypot à faible interaction qui va permettre de savoir l'adresse IP, l'identifiant, le mot de passe, l'origine (Russie, Israël, Iran, Ukraine) et le protocole utilisé venant de l'attaquant (FTP, SMTP, RDP, SSH). Ces informations seront stockées dans un fichier csv puis ouvrir sur Excel par exemple.

Documentation générale

C'est quoi un Honeypot ?

Un honeypot est un système informatique qui est configuré de manière à attirer les pirates informatiques et à les piéger. Il s'agit d'un leurre qui est utilisé pour détecter, surveiller et étudier les activités malveillantes sur un réseau informatique. Il y a deux type d'honey-pot ceux à forte interaction et ceux à faible interaction



Points positifs d'un honeypot

- Détection proactive des attaques.
- Collecte de renseignements sur les méthodes et motivations des attaquants.
- Amélioration de la sécurité grâce à l'identification des vulnérabilités.
- Possibilité d'apprentissage et de formation en matière de sécurité.
- Contribution à la recherche et à la compréhension des menaces actuelles

Points négatifs d'un honeypot :

- Risque de compromission et d'utilisation abusive par les attaquants.
- Coût élevé de déploiement, de configuration et de maintenance.
- Complexité technique et besoin de ressources spécialisées.
- Surcharge des équipes de sécurité due à la gestion des faux positifs.

Documentation générale

Possibilité de conflit avec les lois et réglementations en matière de cyber sécurité et de confidentialité.

Les Différents Protocoles



Le Protocole File Transfer Protocol (FTP) :

Le Protocole FTP est un Protocole de communication, destiné au partage de fichiers sur un réseau TCP/IP

Exemple : Il permet, depuis un ordinateur de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur l'ordinateur.

Le Simple mail Transfer Protocol (SMTP) :

Le Protocol SMTP est un serveur de messagerie capable d'envoyer et de recevoir des e-mails.

Exemple : Le client possédant un courrier électronique se connecte directement au serveur SMTP du fournisseur de messagerie pour démarrer le processus d'envoi d'un e-mail.

Documentation générale

Remote Desktop Protocol (RDP) :

Le Protocol RDP est un Protocole permettant d'utiliser un ordinateur de bureau à distance, il est le plus courant utilisé.

Exemple : Nous avons la possibilité de se connecter à un bureau à distance comme si nous étions réellement sur l'ordinateur en question.

Secure Socket Shell (SSH) :

Le Protocol SSH est un Protocole réseau, d'accéder à un ordinateur à distance, en toute sécurité, à l'aide d'une authentification forte et des données chiffrées.

Exemple : Un collègue va pouvoir accéder de manière sécurisée à distance sur votre bureau et limité les risques que présente-les instruisons, tel qu'internet.

Documentation générale

C'est quoi PostgreSQL ?



PostgreSQL, est un gestionnaire de base relationnelles (SGBDR) open source réputée pour sa fiabilité et sa conformité aux normes SQL.

Définitions : SGBDR est un logiciel qui stocke, gère et interroge des données organisées en tables avec des relations. Il utilise le langage SQL pour les opérations sur les données.

Les Avantages

Open source : Il permet de stocker, gérer et interroger des données structurées.

PostgreSQL : il est basé sur le modèle relationnel, où les données sont organisées en tables avec des relations définies entre elles.

Beaucoup de possibilité : Il offre une large gamme de fonctionnalités avancées, une grande stabilité et une communauté active de développeurs.

Les Inconvénients

Complexité : Riche en fonctionnalité, il est peut-être complexe à configurer et à gérer pour les utilisateurs novices en bases de données.

Documentation générale

Consommation de ressources : Il peut nécessiter un matériel et système plus conséquent, lors de charge de travail plus volumineuses

Apprentissage : il est nécessaire, d'apprendre pour comprendre ses nombreuses fonctionnalités avancées et sa configuration.

Le Modèle ACID



Atomicité : Les transactions sont traitées comme une unité indivisible. Toutes les opérations doivent réussir, sinon aucune modification n'est effectuée.

Exemple : Imaginez que vous transférez de l'argent d'un compte à un autre. Dans une base de données avec l'atomicité, la transaction est traitée comme une unité indivisible. Si le transfert échoue à mi-chemin pour une raison quelconque, toutes les opérations effectuées sont annulées, et les comptes restent dans leur état initial.

Cohérence : Les transactions maintiennent l'intégrité de la base de données, respectant les contraintes et les règles définies.

Exemple : Supposons que vous ayez une base de données d'un site de commerce électronique. Lorsqu'un client passe une commande, la cohérence garantit que toutes les contraintes et règles définies sont respectées. Par exemple, si un client a déjà atteint son quota d'achat pour un produit, une nouvelle commande ne sera pas acceptée pour ce produit.

Documentation générale

Isolation : Les transactions s'exécutent de manière isolée les unes des autres, évitant les interactions et les dépendances entre elles.

Exemple : Considérons une situation où deux utilisateurs essaient de réserver la même place dans un cinéma en même temps. L'isolation garantit que chaque transaction s'exécute de manière isolée, sans affecter l'autre. Ainsi, même si les deux transactions sont exécutées simultanément, elles ne se gêneront pas mutuellement et ne causeront pas de conflits.

Durabilité : Les modifications apportées par une transaction confirmée sont permanentes et résistent aux pannes ultérieures.

Exemple : supposons que vous insérez des données dans une base de données. Une fois que la transaction est confirmée et que les données sont enregistrées, elles doivent être durables. Même en cas de panne du système, redémarrage ou tout autre problème, les données doivent rester enregistrées et accessibles lorsque le système est rétabli.

Le modèle ACID garantit la fiabilité et la cohérence des transactions dans PostgreSQL, ce qui en fait une base de données fiable pour les applications nécessitant des opérations transactionnelles sûres et cohérentes.

Documentation générale

C'est quoi Grafana ?



Grafana est une plateforme open-source de visualisation et de monitoring utilisée pour surveiller les systèmes, applications et services. Ses avantages clés sont les suivants :

Avantages de Grafana :

Interface conviviale : Une interface utilisateur intuitive facilite la création de tableaux de bord personnalisés et interactifs sans compétences avancées en programmation.

Large écosystème de plugins : Grafana dispose d'une grande variété de plugins permettant l'intégration avec de nombreuses sources de données, offrant ainsi une flexibilité maximale dans la visualisation des données.

Visualisations puissantes : Grafana propose une gamme étendue d'options de visualisation, permettant aux utilisateurs de représenter leurs données de manière claire et significative.

Points négatifs de Grafana :

Configuration complexe : La configuration initiale peut être complexe, en particulier pour l'intégration de multiples sources de données ou des tâches avancées de personnalisation.

Documentation générale

Besoin d'expertise en données : Une compréhension solide des données est nécessaire pour tirer pleinement parti de Grafana et modéliser efficacement les données.

Gestion des ressources : Grafana peut consommer des ressources importantes lorsqu'il est utilisé pour collecter et afficher de grandes quantités de données en temps réel, nécessitant une gestion prudente des ressources.

D'autres outils similaires à Grafana incluent Kibana et Prometheus. En résumé, Grafana est une plateforme puissante et flexible pour la visualisation et le monitoring des données, offrant une interface conviviale, un écosystème de plugins étendu, mais nécessitant une configuration complexe, une expertise en données et une gestion prudente des ressources.

Documentation générale

C'est quoi Apache2 ?



Apache2 est un serveur web open-source largement utilisé pour héberger des sites web et fournir des services web.

Avantages d'Apache2 :

Fiabilité et stabilité : Apache2 est réputé pour sa fiabilité et sa stabilité, ce qui en fait un choix populaire pour les sites web à fort trafic.

Flexibilité : Apache2 offre une grande flexibilité grâce à sa prise en charge d'une vaste gamme de modules et d'extensions. Il permet ainsi de personnaliser les fonctionnalités et les performances du serveur en fonction des besoins spécifiques.

Sécurité : Apache2 propose des fonctionnalités de sécurité avancées telles que la prise en charge du protocole HTTPS (HTTP sécurisé) et la possibilité de configurer des règles de sécurité personnalisées pour protéger les sites web contre les attaques.

Négatifs d'Apache2

Configuration initiale complexe : La configuration initiale d'Apache2 peut être complexe, en particulier pour les utilisateurs novices. Il peut nécessiter une certaine expertise pour optimiser les performances et la sécurité du serveur.

Documentation générale

Consommation de ressources : Apache2 peut consommer des ressources système importantes, en particulier lorsque le serveur doit gérer un grand nombre de connexions simultanées. Une planification et une gestion appropriées des ressources sont nécessaires pour éviter les problèmes de performance.

Maintenance : La maintenance continue d'Apache2, y compris les mises à jour de sécurité et les correctifs, nécessite une attention régulière pour assurer la sécurité et la stabilité du serveur.

Apache2 est un serveur web fiable et flexible, offrant une large gamme de fonctionnalités et une bonne sécurité. Cependant, il nécessite une configuration initiale complexe, peut consommer des ressources importantes et nécessite une maintenance régulière d'autres outils sont similaire-t-elle que Nginx, Microsoft IIS ,Lighttpd, Caddy , Tomcat.

C'est quoi Qeeqbox/Honeypot ?

Qeeqbox/Honeypot est un outil open source de déploiement de honeypots conçu pour attirer et piéger les attaquants afin d'étudier leurs méthodes et de mieux comprendre les tactiques utilisées dans les cyberattaques, développé par Qeeqbox Security. Qeeqbox/Honeypot permet de déployer facilement différents types de honeypots, tels que des honeypots rdp, SSH, smtp et ftp qui simulent des services vulnérables pour attirer les attaquants.

Avantages	Inconvénients	Outils similaires
Étude des attaques en temps réel	Complexité de configuration	Cowrie (https://github.com/cowrie/cowrie)
Permet de prévenir les attaques	Risques de sécurité supplémentaires, si les Honeypots ne sont pas correctement configuré et surveiller	Dionaea (https://github.com/DinoTools/dionaea)