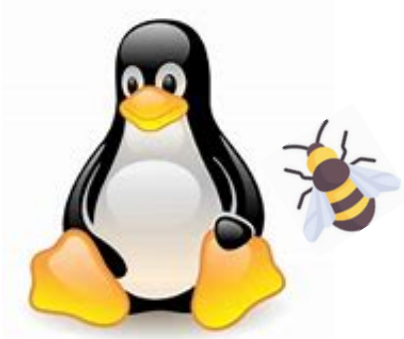
PAUL-ANDRE LE MOUEL
BTS SIO
OPTION SISR

HONEYTRAP

SERVICE DE SECURITÉ

KALI LINUX



2024 - 2025

Introduction

HONEYTRAP

Projet consistant a mettre en place un honeypot Cowrie sur un serveur SSH pour reproduire un environnement vulnérable et recueillir des données sur les tentatives d'intrusion en vue d'analyser les comportements malveillants.

Contexte de l’entreprise

L'organisme FAC est constitué d'une équipe de cinquante employés dont le principal objectif est de fournir une assistance financière aux familles en situation de précarité.

Il opère à l'échelle nationale pour apporter son soutien aux individus faisant face à des difficultés.

Son siège social est établi à Pontivy, d'où il supervise et coordonne ses initiatives et ses programmes visant à améliorer la qualité de vie des bénéficiaires à travers le pays.

Un honeypot tel que Cowrie permet à l'organisation de détecter et d'analyser les attaques potentielles sur des services vulnérables, comme SSH, sans compromettre ses systèmes réels.

Ce type de projet est essentiel pour renforcer la sécurité informatique en fournissant des informations sur les attaques potentielles, en améliorant les mesures de défense et en testant les systèmes de détection en conditions réelles.

Cela permet à l'entreprise d'anticiper et de réagir de manière plus efficace aux menaces.

Conception du projet

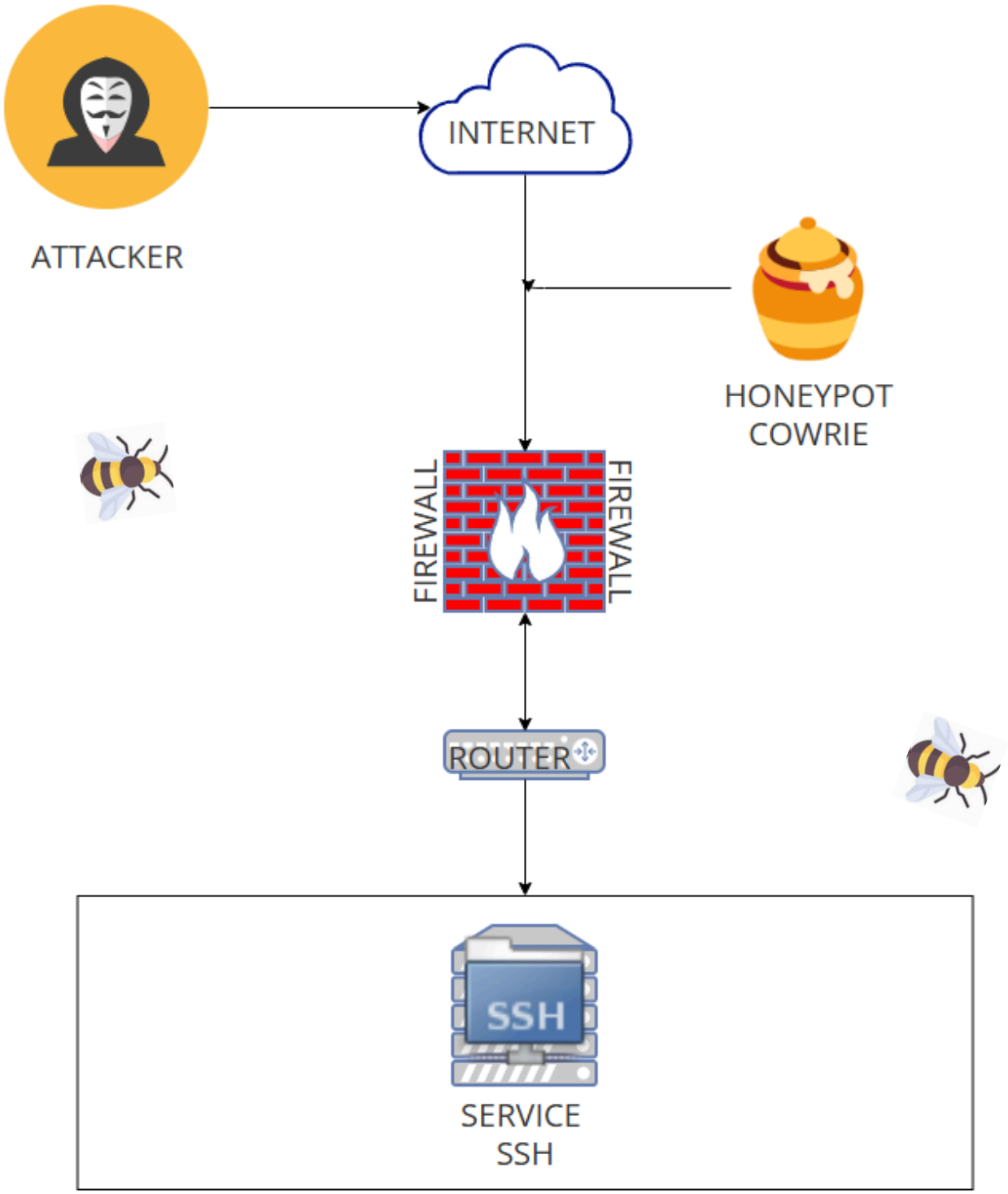
Au sein de l'organisation, de nombreux dossiers contenant des données à caractère personnel circulent dans nos systèmes.

Face à des cyberattaquants de plus en plus sophistiqués dans leurs méthodes d'attaque, nous avons observé une augmentation de la vulnérabilité et une insuffisance en matière de sécurité au sein de notre système d'information.

Objectifs du projet :

Le but du projet consiste à examiner toutes les techniques d'intrusion employées par les attaquants, dans le but de répondre de façon adéquate et de renforcer nos mécanismes de défense.

Architecture du système : Schéma réseau



Environnement de travail

- Serveur sur lequel est déployé Cowrie = Kali linux
- Outils de collecte de logs : Intégration avec Kibana pour l'analyse des logs

J'ai opté pour Cowrie comme honeypot en raison de sa capacité à simuler un serveur SSH vulnérable, permettant ainsi de détecter les tentatives d'accès non autorisées telles que les attaques par force brute et les commandes malveillantes.

L'utilisation de Kibana pour la visualisation des logs a été privilégiée en raison de son interface graphique intuitive et de sa capacité à analyser de manière approfondie les données collectées.

Par ailleurs, le service SSH a été choisi pour simulation en raison de sa fréquente ciblage par les attaquants cherchant à accéder à des serveurs distants, en faisant une cible pertinente pour l'observation des comportements malveillants.

Installation et Configuration

Mettre a jour le systeme

palm@pllkali-[/] sudo apt update && sudo apt upgrade -y

git clone *https://github.com/cowrie/cowrie.git*

Une fois installé, rentrer dans le dossier cowrie avec cette commande

palm@pllkali-[/] cd cowrie

installez toutes les dépendances nécessaires avec :

palm@pllkali-[/] pip install -r requirements.txt

Aller vers le repertoire bin

palm@pllkali-[/] cd bin

Lancez cowrie avec l'aide de cette commande

palm@pllkali-[cd] /cowrie/bin$ ./cowrie start

Tester depuis une autre machine de vous connecter en ssh avec l'ip de votre machine qui heberge le honeypot

C:\users\palm >ssh root@192.168.XX.XX -p 2222

Un mots de passe vous sera demandé

password

Peu importe le mots de passe renseigné l'accès sera autorisé et chaque commande entré sera enregistrer par le honeypot

Installation et Configuration

Elasticsearch

kibana fonctionne avec Elasticsearch

Ajout de la clé GPG et du dépôt Elasticserch

palm@pllkali-[/] wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list

Installation Elasticserch

palm@pllkali-[/] sudo apt install elasticsearch -y

Activation et démarrage

palm@pllkali-[/]sudo systemctl enable --now elasticsearch

Kibana

Installation

palm@pllkali-[/] sudo apt install kibana -y

Configuration

palm@pllkali-[/] sudo nano /etc/kibana/kibana.yml

Modifiez ou ajoutez les lignes suivantes :

```
server.port: 5601
server.host: "localhost"
elasticsearch.hosts: ["http://localhost:9200"]
```

Enregistrez avec CTRL+X, puis Y, et Entrée.

Démarrer et activer Kibana

sudo systemctl enable --now kibana

Accéder à Kibana sur votre navigateur

http://localhost:5601

Redémarrez Kibana

sudo systemctl restart kibana

Sécurité et précautions

1. Isolation du honeypot dans un réseau sécurisé :

Le honeypot est installé dans un réseau isolé de l'infrastructure principale afin de réduire les risques de diffusion d'attaques vers les systèmes de production. Ce réseau isolé est configuré de manière à empêcher toute communication directe avec d'autres ressources sensibles de l'entreprise.

2. Utilisation de machines virtuelles pour réduire les risques :

Le honeypot fonctionne sur une machine virtuelle dédiée, permettant de limiter les conséquences des attaques. En cas de compromission, l'environnement virtuel peut être rapidement isolé et réinitialisé sans impacter l'intégralité du système.

3. Surveillance des connexions réseau pour détecter les comportements suspects :

Une surveillance continue des connexions réseau est mise en place afin de repérer tout comportement inhabituel ou toute activité suspecte. Des outils de surveillance et des systèmes de détection d'intrusion (IDS) sont utilisés pour alerter l'équipe de sécurité en cas d'attaque ou de tentative de communication malveillante.

Gestion des données sensibles

Les journaux collectés, incluant des informations telles que les adresses IP des attaquants et les commandes malveillantes, sont traités avec précaution.

Ces données sont stockées de manière sécurisée dans des bases de données chiffrées, et seuls les analystes autorisés peuvent y accéder.

De plus, des mesures sont mises en place pour anonymiser certaines données sensibles, dans la mesure du possible, afin de préserver la confidentialité des individus concernés.

Conformité aux lois et à l'éthique

Ce projet est mené en respectant scrupuleusement les lois en vigueur concernant la collecte de données et la cybersécurité.

Les données collectées sont utilisées exclusivement à des fins d'analyse et de recherche dans le cadre d'une approche éthique.

Aucune utilisation malveillante ou à des fins commerciales n'est envisagée. De plus, des mesures sont prises pour assurer la conformité avec les réglementations telles que le RGPD (Règlement général sur la protection des données) afin de protéger les informations personnelles.

Captures et analyse des attaques

Exemples d’attaques capturées :

Montre quelques exemples de tentatives d’intrusion détectées par Cowrie. Tu peux inclure des captures d'écran des logs dans Kibana montrant les tentatives de connexion, les commandes exécutées, etc.

Analyse des attaques :

Analyse les attaques qui ont été détectées, comme les types d'attaques (brute force, tentatives d’injection de commandes, etc.), les méthodes utilisées par les attaquants, et leurs motivations possibles. Tu peux aussi discuter des outils utilisés par les attaquants.

Les résultats et analyse

Quantification des attaques :

Le nombre d’attaques détectées (par jour est d'en moyenne 10 a 15, ce qui revient a environ 400 par mois. Les attaques proviennent principalement d'Asie, en particulier de la Corée du Sud et de la Russie.

Les pics d'attaques peuvent survenir lors de périodes spécifiques comme les vacances, les mises à jour logicielles ou des événements géopolitiques.

Ces pics peuvent également être influencés par des événements propres au secteur de l'entreprise ou à la vulnérabilité d'un service particulier.

Les techniques d'attaque courantes sont les suivantes :

1. Brute force : Tentatives automatisées pour deviner les identifiants, souvent utilisées sur des services comme SSH ou RDP.

2. Phishing : Envoi d'emails ou messages frauduleux pour obtenir des informations sensibles.

3. Exploitation de vulnérabilités : Recherche de failles non corrigées pour accéder aux données ou exécuter des commandes malveillantes.

4. Malwares (virus, ransomware) : Infiltration de systèmes pour voler des données ou demander une rançon.

5. Attaques DDoS : Saturer les serveurs en envoyant un grand nombre de requêtes.

Évaluation de l'efficacité du honeypot :

1. Utilisation de Cowrie pour simuler un environnement vulnérable :

Cowrie a été efficace pour simuler un environnement vulnérable en capturant diverses attaques telles que les tentatives de force brute et les commandes malveillantes.

Ce honeypot SSH trompe les attaquants en leur offrant un faux serveur vulnérable, permettant ainsi de recueillir des données sur les tentatives d'intrusion sans compromettre la sécurité des systèmes réels.

Cependant, sa configuration et son isolation dans un réseau sécurisé sont essentielles pour maintenir son efficacité.

Évaluation de l'efficacité du honeypot :

2. Utilisation de Kibana pour l'analyse des attaques :

Kibana a facilité l'analyse des attaques en offrant une interface graphique intuitive pour visualiser les logs collectés.

Grâce à ses capacités de filtrage et de visualisation avancées, il a permis d'identifier facilement les tentatives de force brute, les adresses IP des attaquants, les commandes exécutées et de générer des rapports détaillés pour suivre l'évolution des attaques.

Évaluation de l'efficacité du honeypot :

3. Possibles améliorations :

- Diversification des services simulés : Ajouter la simulation d'autres services tels que HTTP ou RDP permettrait de capturer un plus large éventail d'attaques.

- Amélioration de l'analyse des attaques : L'intégration d'outils d'analyse automatisée, comme l'apprentissage automatique, pourrait améliorer la détection précoce des attaques.

- Gestion des alertes : L'intégration de systèmes d'alertes en temps réel pour réagir rapidement à des comportements suspects détectés dans les logs.

- Anonymisation des données : Mettre en place des systèmes d'anonymisation des données pour garantir la conformité avec les réglementations sur la protection de la vie privée, telles que le RGPD.

En résumé, Cowrie et Kibana ont été utiles, mais des améliorations telles que la diversification des services et l'amélioration de l'analyse des logs pourraient augmenter l'efficacité du système.

Conclusion

En conclusion,

ce projet a permis d'approfondir notre compréhension des techniques utilisées par les attaquants en simulant un environnement vulnérable avec Cowrie et en analysant les attaques via Kibana.

Cette expérience a été précieuse pour renforcer nos compétences et connaissances en matière de cybersécurité. En tant que passionnés de sécurité, nous avons grandement apprécié la réalisation de ce projet et le développement de nos capacités techniques.

Nous vous remercions pour votre attention portée à cette documentation.