Documentation Technique

Déploiement d’un Honeypot Cowrie

Infrastructure Sécurisée – Pingouin Hosting

BTS SIO – Option SISR
Projet E6

1. Présentation du projet

Dans le cadre du BTS SIO option SISR, ce projet consiste à déployer et sécuriser un honeypot Cowrie au sein d'une infrastructure réseau interne. L'objectif est de détecter et analyser les tentatives d'intrusion en simulant un serveur SSH vulnérable isolé du reste de l'infrastructure.

2. Objectifs

• Déployer un honeypot Cowrie
• Simuler un serveur SSH vulnérable
• Enregistrer les tentatives d'intrusion
• Sécuriser les accès via Port Knocking
• Isoler le honeypot du reste du réseau
• Superviser les connexions réseau

3. Architecture de l'infrastructure

L'infrastructure est composée des équipements suivants :

Équipement	Fonction
Proxmox	Virtualisation des machines
pfSense	Pare-feu et routage réseau
Cowrie	Honeypot SSH
Apache2	Serveur web du honeypot
Wireshark	Analyse du trafic réseau

4. Fonctionnement du Honeypot

Le serveur Honeypot Cowrie est isolé dans une zone spécifique afin d'éviter tout impact sur l'infrastructure principale. Le service simule un serveur SSH vulnérable permettant d'attirer les attaquants et d'enregistrer :

• les identifiants utilisés ;
• les commandes exécutées ;
• les tentatives de connexion.

5. Sécurisation de l'infrastructure

L'accès SSH du honeypot est protégé grâce à un mécanisme de Port Knocking mis en place via pfSense. Le port SSH n'est accessible qu'après l'envoi d'une séquence spécifique de connexions sur plusieurs ports. Le honeypot est totalement isolé du reste de l'infrastructure afin de limiter les risques de compromission.

6. Adressage réseau

Machine	Rôle	Adresse IP
PFSENSE	Routeur / Pare-feu	192.168.2.1
SRV WEB	Apache2 + DNS	192.168.2.2
SRV WEB HONEY-POT	Honeypot Cowrie + Apache2	192.168.2.4

7. Conclusion

Ce projet m’a permis de mettre en pratique les compétences acquises en cybersécurité, administration système et réseau dans un environnement virtualisé. Le déploiement du honeypot Cowrie a permis d’améliorer la surveillance des tentatives d’intrusion et de renforcer la sécurité de l’infrastructure.