BTS SIO SISR

Situation professionnelle numéro 5

Mise en place et configuration d'un Honeypot

C'est lors de cette situation que je vais essayer de répondre à la problématique.

BTS SIO SISR CFA INSTA 75005

Léo LE CORRE

Plan de situation :

La demande

Dans le cadre du renforcement de sa stratégie de cybersécurité, l'entreprise KLLT Bank souhaite mettre en place un dispositif permettant de détecter précocement les activités malveillantes ciblant son infrastructure. En tant qu'établissement financier, KLLT Bank est particulièrement exposée aux menaces telles que les tentatives d'intrusion, la recherche de vulnérabilités, les attaques par force brute, ou encore les activités de reconnaissance réalisées par des attaquants avant une compromission.

Afin de mieux comprendre le mode opératoire des attaquants, d'anticiper les risques et de renforcer la posture de défense globale, l'entreprise exprime le besoin d'installer un honeypot de type T-Pot. Ce type de solution permet de :

- Attirer et isoler les activités malveillantes dans un environnement contrôlé et sans risque pour le système d'information ;
- Collecter des données réelles sur les attaques (adresses IP, techniques employées, outils, fréquences, types de scans, tentatives d'exploitation, etc.) ;
- Analyser les comportements des attaquants afin d'adapter les mécanismes de défense, les règles de pare-feu et les politiques de sécurité ;
- Évaluer la maturité de la sécurité du réseau et identifier d'éventuelles faiblesses ;
- Renforcer la surveillance sans exposer directement les actifs les plus sensibles de la banque.

La mise en œuvre d'un honeypot T-Pot répond donc à la volonté de KLLT Bank de développer une capacité proactive de détection et d'améliorer sa résilience face aux cybermenaces, dans un contexte où les établissements bancaires sont des cibles privilégiées.

C’est quoi un Honeypot ?

Un honeypot (ou “pot de miel”) est un système informatique volontairement vulnérable et isolé, conçu pour attirer les cyberattaquants.
Il imite des services réels (serveur web, base de données, SSH, RDP, API, etc.) afin de piéger, observer et enregistrer les comportements malveillants sans mettre en danger l’infrastructure de production.

Pourquoi ce choix ?

Solution	**Type**	**Limites**	**Avantages de T-Pot**
T-Pot	Plateforme multi-honeypots + dashboard	Plus lourd à déployer	Couverture très large + centralisation
Cowrie	SSH/Telnet honeypot	Très limité	T-Pot intègre Cowrie + d’autres services
Dionaea	Multi-protocoles, capture de malwares	Pas de gestion centralisée	Inclus dans T-Pot + dashboard complet
Honeyd	Simulation d’hôtes virtuels	Low-interaction, peu de détails	T-Pot offre des logs plus riches
OpenCanary	Honeypot léger et simple	Fonctionnalités limitées	T-Pot est plus complet et polyvalent
Thinkst Canary (payant)	Solution pro clé-en-main	Payant, peu flexible	T-Pot gratuit et personnalisable

Le choix de T-Pot s’explique par sa capacité à regrouper, au sein d’une seule plateforme, plusieurs types de honeypots couvrant différents protocoles et vecteurs d’attaque. Contrairement aux solutions plus limitées comme Cowrie ou OpenCanary, ou aux solutions commerciales comme Thinkst Canary, T-Pot offre une visibilité complète, une collecte de données unifiée et un tableau de bord centralisé grâce à la stack ELK. Cela permet d’obtenir un volume d’informations plus riche, plus exploitable et plus représentatif des menaces réelles, sans multiplier les installations.
Ce choix offre donc à l’entreprise une solution gratuite, polyvalente et plus réaliste pour analyser les attaques tout en restant simple à administrer.

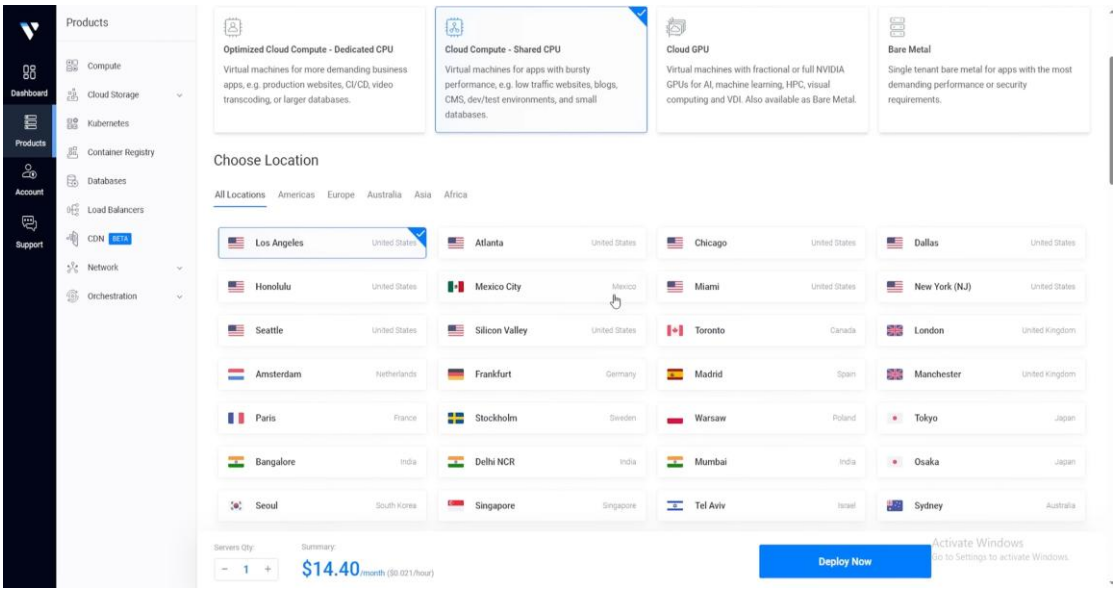
Le choix de l'hébergement

Le choix de Vultr comme cloud provider se justifie par plusieurs avantages pratiques pour la mise en place d'un honeypot T-Pot. Tout d'abord, Vultr propose un accès Internet public complet, indispensable pour exposer le honeypot et observer de vraies attaques extérieures. La plateforme offre également une grande simplicité de déploiement, avec la possibilité de créer rapidement une VM compatible avec T-Pot.
Un autre avantage majeur est la présence d'un crédit gratuit de 100 €, permettant de réaliser le projet sans coût pour l'entreprise pendant 2/3 mois. Vultr met aussi à disposition une interface intuitive, des performances stables, une facturation à l'usage et une bonne flexibilité dans le choix des ressources. Ces éléments font de Vultr un choix adapté, économique et pratique pour héberger un honeypot accessible depuis Internet.

Configuration du serveur

Pour le serveur, j'ai choisi d'utiliser le mode Cloud Compute – Shared CPU, étant le plus optimiser pour le type d'utilisations que nous aurons.

J'ai également choisi la localisation du serveur (Paris) pour de faibles latences.

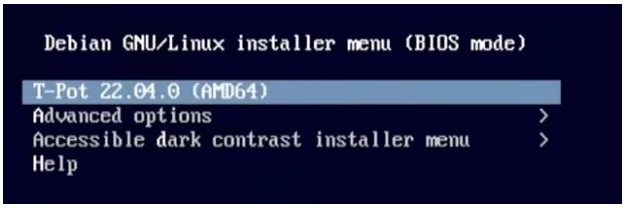


J'ai mis l'iso de T-Pot en cliquant sur l'upload personnalisé ISO. J'ai ensuite choisi les performances du pc, 160 GB SSD de disque, 4 cœurs CPU, 5 GB de mémoire instantané, et 4TB de bande passante (pour 40$). Enfin, je lui ai donné un nom.

J'ajoute un groupe de pare feux et j'autorise les port TCP/UDP de 1 à 65535 en provenance de mon ip uniquement, j'autorise le SSH pour tout le monde également.

Mise en place du serveur

Pour installer T-Pot, il faut suivre l'installation comme ceci :

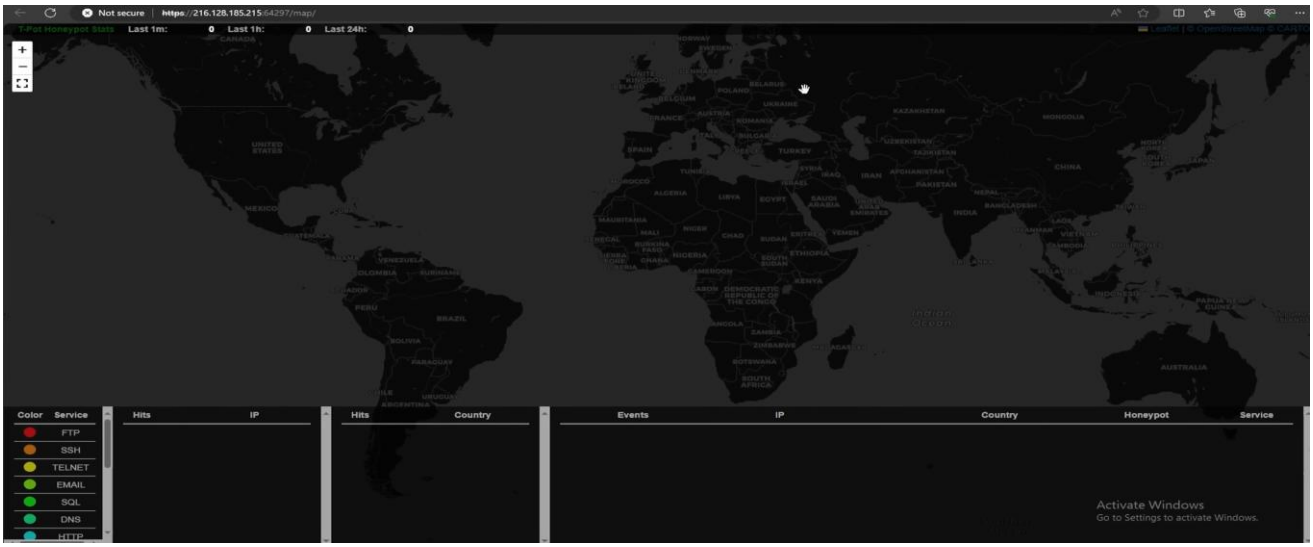


Cliquer sur T-Pot 22.04.0, puis choisir la localisation (France), le clavier, le mirroir par défaut, puis l'édition STANDART, le mot de passe, identifiant.

A partir de ce moment, on peut entrer dans l'interface web (https://(ip_fournit), et mettre les identifiants saisies précédemment.

Configuration de l'outil

Une fois dans l'outil, on peut cliquer sur T-Pot Attack Map dans le but de voir les attaques en temps réel et les provenances.



Rien n'apparait, c'est parce que le pare feu bloque toutes les attaques.

Configuration du pare-feu

Aussi contre intuitif que ça puisse paraître, le but vas être de ne pas sécuriser notre serveur. Pour cela, dans la console d'administration du serveur en ligne, nous allons mettre les règles du pare feu comme ceci :

- Autoriser TCP/UDP ports de 1 à 65535 any 0.0.0.0

Résultat après 2 jours

Après deux jours de fonctionnement, le honeypot a enregistré 6 583 tentatives d'attaques provenant de 1 485 adresses IP uniques. Ce volume important en si peu de temps montre que toute machine exposée sur Internet est immédiatement la cible de scans et de tentatives d'intrusion automatisées, même sans être référencée ou connue publiquement. L'analyse du volume global révèle que les attaques sont principalement générées par des bots, qui explorent en continu les plages d'adresses IP à la recherche de services vulnérables.

L'histogramme des attaques met en évidence un flux relativement constant au cours des 48 heures, avec des pics qui correspondent généralement aux cycles d'activité des botnets et aux campagnes de scans massifs. Cela confirme qu'il ne

s’agit pas d’attaques ciblées, mais d’une activité opportuniste visant tout service accessible.

La carte mondiale des attaques indique que les adresses IP sources sont réparties dans de nombreux pays, notamment les États-Unis, l’Europe, la Chine et l’Inde. Cette diversité géographique ne signifie pas que les attaquants se trouvent réellement dans ces pays, mais montre plutôt que les machines compromises utilisées par les botnets y sont hébergées.

L’analyse des ports les plus ciblés révèle que certains services sont beaucoup plus visés que d’autres. Le port 3389 (RDP) est largement attaqué, ce qui s’explique par son association fréquente aux attaques par force brute sur des environnements Windows. Le port 22 (SSH) fait également partie des cibles prioritaires, car il est l’un des services les plus exposés au monde. D’autres ports comme 8080, 8728, 3128 ou 9001 apparaissent aussi dans les statistiques, car ils correspondent souvent à des interfaces d’administration, des proxys ou des services mal protégés.

Enfin, la répartition des attaques par pays met en avant une forte contribution des États-Unis, de l’Europe et de certains pays asiatiques. Cette observation illustre la structure distribuée des botnets modernes, composés de milliers de machines compromises à travers le monde.

En conclusion, ces données démontrent que, même sur une période très courte, un honeypot reçoit un volume conséquent d’activités malveillantes. Cela souligne l’importance d’une protection rigoureuse des services exposés, d’un filtrage strict des accès, de pare-feux correctement configurés et de mécanismes de sécurité complémentaires comme l’authentification multifacteur ou la segmentation réseau.

Résumé

KLLT Bank souhaitait mieux comprendre les menaces qui ciblent son infrastructure afin de renforcer sa cybersécurité. Pour répondre à ce besoin, un honeypot T-Pot a été déployé sur une machine virtuelle Vultr, choisie pour son faible coût, sa simplicité et son accès Internet complet. T-Pot a été retenu car il centralise plusieurs honeypots et fournit un tableau de bord clair pour analyser les attaques.

Le serveur a été configuré avec l'ISO de T-Pot, puis volontairement exposé en ouvrant tout le trafic entrant afin d'observer de vraies tentatives d'intrusion. Après seulement deux jours, le honeypot a enregistré plus de 6 500 attaques provenant d'environ 1 500 IP uniques, confirmant qu'un système exposé est immédiatement ciblé par des scans automatisés. Les ports RDP et SSH sont apparus comme les plus attaqués, et les attaques provenaient de machines compromises du monde entier.

Ce projet apporte à KLLT Bank une vision concrète des menaces réelles présentes sur Internet. Les résultats permettent d'adapter les règles de sécurité, de mieux protéger les services critiques et de renforcer la stratégie globale de défense du système d'information.