Introduction : (2 minutes)

Nassera

Bonjour à toutes et à tous,

Nous sommes ravis d'être ici aujourd'hui. **CyberSecurity Universe** est une école de formation passionnée par le domaine de la cybersécurité, qui est un sujet essentiel à l'ère numérique actuelle. Elle ne se limite plus à de simples mesures de prévention ; elle repose également sur l'observation active des menaces afin d'anticiper et de contrer les attaques de manière plus efficace.

Avant de commencer, permettez-moi de vous présenter notre équipe :

- OUAFI Omar – Expert et conseiller en cybersécurité.
- EREKYSY Anass – Expert en cybersécurité
- NAOUI Nassera – Analyste en cybersécurité

Aujourd'hui, nous allons vous donner une brève présentation des Honeypots, un outil stratégique en cybersécurité. Nous verrons comment ils fonctionnent ? leur rôle dans la détection des cyberattaques et comment ils peuvent aider à analyser les comportements pour renforcer la défense des systèmes informatiques.

Allons - y !

C'est quoi le concept du HoneyPot ? 30 sec

Anass

Un **honeypot**, c'est comme un pot de miel pour attraper les mouches.

Plus techniquement , Un **honeypot** est un faux système informatique créé pour attirer les cyber attaquants. Il imite des services et applications réels pour paraître vulnérable et inciter les pirates à s'y introduire. Une fois piégés, leurs actions sont discrètement surveillées et enregistrées. Cela aide les experts à analyser les techniques d'attaque utilisées et à renforcer la sécurité des vrais systèmes. Les honeypots sont souvent combinés à l'analyse comportementale pour mieux comprendre les menaces.

Les types des HoneyPots ? 1minute

Omar

Il existe plusieurs types de **honeypots** classés selon leur but et leur niveau d'interaction :

Selon l'objectif :

Honeypots de production :

- But : détecter les attaques en temps réel
- Exemple : ***KFSensor***
-

Honeypots de recherche :

- But **:** Étudier le comportement des attaquants et leurs techniques.
- Exemple : ***Honeyd***

Selon l'interaction :

Faible interaction :

- But **:** Simuler certains services sans offrir un véritable système d'exploitation.
- Exemple **: Dionaea**

Haute interaction :

- But ***:*** Fournir un véritable environnement où les attaquants peuvent interagir librement.
- Exemple ***:*** **Kippo**

Interaction moyenne :

- But ***:*** Simuler plus de services que les low-interaction sans offrir un accès complet.
- Exemple ***:*** **Cowrie**

L'analyse de l'existant ? 1 min

Nassera

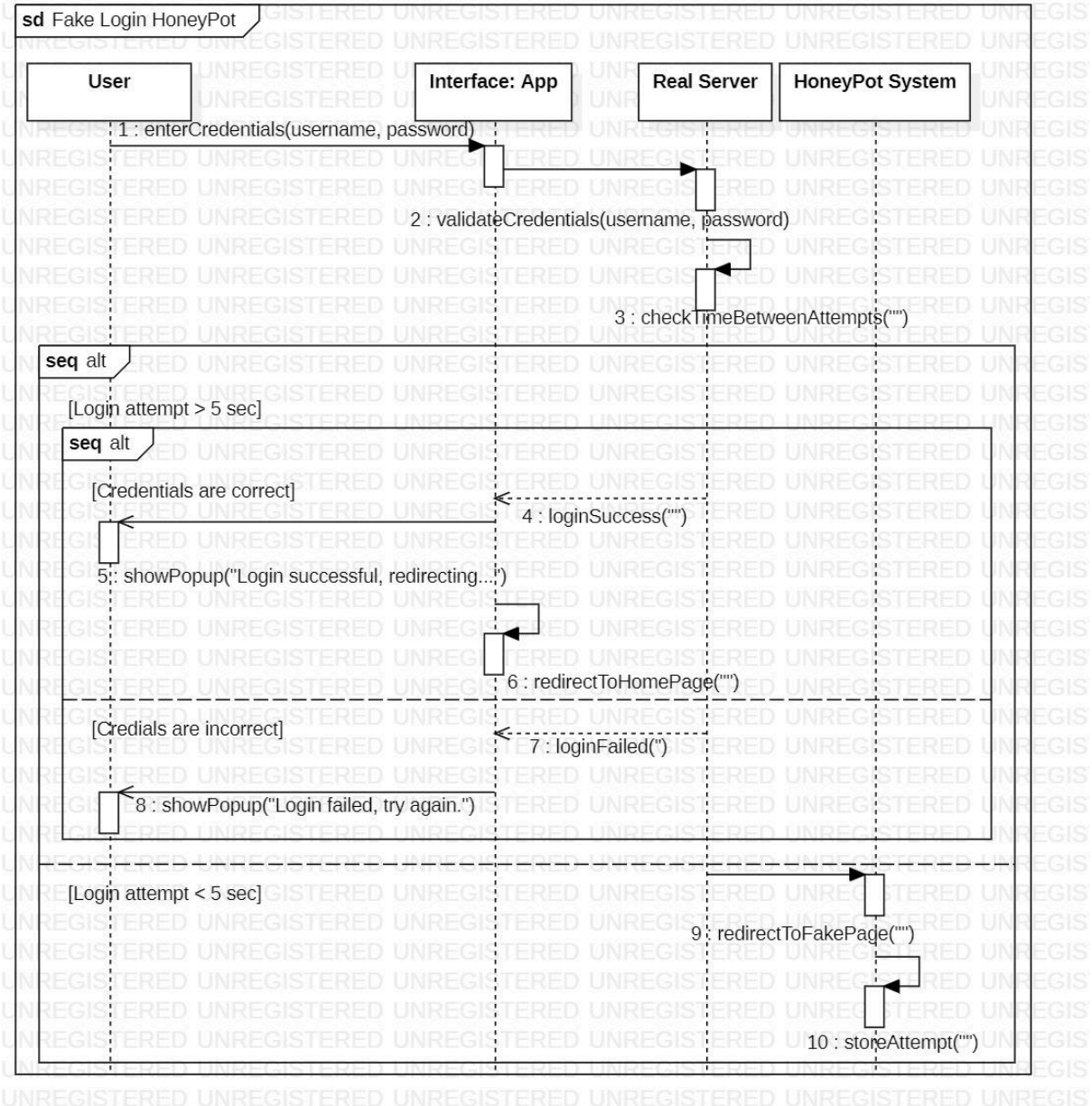
Vu L'utilité des HoneyPots ils existent pas mal je vais vous en citer quelque uns :

Honeypot	Type	Function
KFSensor	Honeypots de production	Placé dans le réseau de l'entreprise, ce type attire les pirates pour détecter les menaces avant qu'elles n'atteignent les véritables systèmes. Il est simple à gérer et axé sur la sécurité pratique.
Honeyd	Honeypots de recherche	Ces honeypots sont déployés principalement pour la recherche en cybersécurité. Ils offrent des données détaillées sur les méthodes utilisées par les cybercriminels afin d'améliorer les stratégies de défense globale.
Dionaea	Faible interaction	Ces honeypots sont faciles à configurer et présentent moins de risques, car les attaquants ont un accès très limité. Ils sont utiles pour détecter des tentatives simples d'intrusion
Kippo	Haute interaction	Ces honeypots offrent un environnement complet, augmentant les risques d'évasion, mais permettent d'obtenir des informations précieuses sur les comportements d'attaque complexes.
Cowrie	Moyenne interaction	Va être présenté Par mon collègue Omar

Scénario : Technique du Fake login ? 1 min

Nassera

Je vous mets dans la peau d'un pirate :



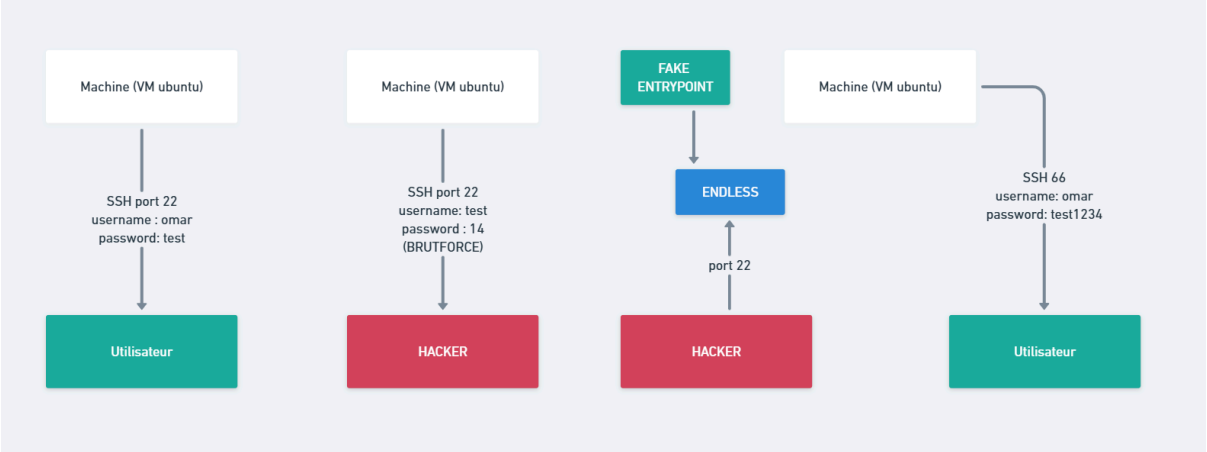
Explication et demonstration du Fake login technique ? 2 min

Anass

A ce niveau tu vas expliquer en même temps de la démonstration ce que ton code fait et les différents tests unitaires que tu as implémenter.

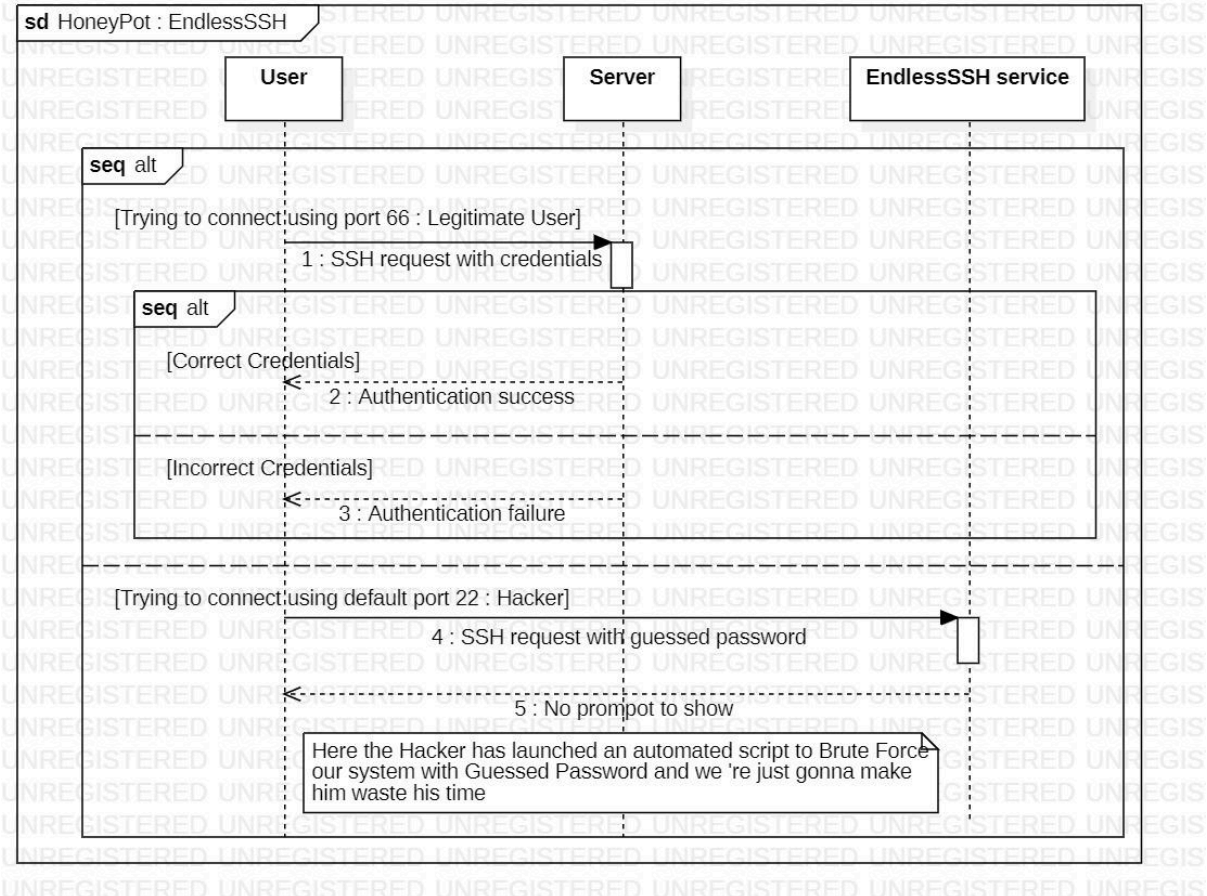
Architecture principale HoneyPot EndlessSSH ? 1 min

Nassera



Scénario : Technique du EndlessSSH ? 1 min

Nassera



Explication et démonstration du technique Cowrie? 2 min

Omar

A ce niveau tu vas expliquer en même temps de la démonstration ce que ton code fait et les différents tests unitaires que tu as implémenter.

Conclusion ? 15sec

Anass

En conclusion, les honeypots sont des outils puissants en cybersécurité, permettant non seulement de détecter les attaques, mais aussi de mieux comprendre les techniques utilisées par les cybercriminels. Ils jouent un rôle clé dans la protection proactive des systèmes informatiques. **CyberSecurity Universe** reste à votre disposition pour toute formation complémentaire dans ce domaine passionnant.

Merci pour votre attention et votre accueil chaleureux !