Le Guide du Maitre du Donjon
Maitriser la cybersécurité en créant des challenges CTF

Date : 14 avril 2023
Speakers : Adam Bertrand (Accenture)
Format : Quickie (15mn)
Présentation : https://hydragyrum.gitlab.io/dungeon-master-prez/1

Adam est contributeur du site TryHackMe permettant d'apprendre la sécu

Capture the Flag :

- Série de défis de cybersécurité
- Objectif : trouver les flags
- Formats plus ou moins complexes : Jeopardy, Boot2Root, Attack/Defend, King of the Hill

Comment créer un challenge ?

Adam parle de l'importance de raconter une histoire aux joueurs.
Comme dans Donjon et Dragon, il faut un scénario, un personnage, des éléments perturbateurs, un déroulement, un dénouement et une situation finale.

Chaine de frappe : comment arriver à l'objectif ?

Pour créer un challenge, il s'appuie sur la technique de storyboarding utilisée en animation.
Bob a écrit une page de login. Le hacker cherche le mot de passe. Il scanne la machine. Il trouve un .git exposé. Il télécharge le repo Git et fouille les logs (commits) de Git puis trouve le mot de passe.

Adam s'inspire de ce qui lui arrive dans la vraie vie (ex : repo git exposé sur le web …) et de sa propre expérience en tant que dév. Lorsque des failles CVE comme Log4Shell font parler d'elle, il monte un POC permettant d'exploiter cette vulnérabilité puis s'en sert pour un challenge. Comme tout développeur, Adam essaie régulièrement de nouvelles technos (ex : Quakus). A cette occasion, on

fait souvent des erreurs de paramétrage, ouvrant alors un pan béant pour tout hacker. On fait tous des erreurs.

Adam prend un autre exemple avec Docker et les réseaux
Container avec frontend et nginx. Une API sur le réseau Public.
Un conteneur de dév caché sur le réseau interne. On arrive au port TCP Docker. Possibilité de créer une machine avec accès root sur l'hote.

Pourquoi faire çà ?

- Pour apprendre : docker, réseau docker. Ce qu'il ne faut pas faire
- Aider les autres à apprendre. Tout le monde n'est pas forcément au courant de toutes les failles de sécu
- Pour s'amuser
- Ou pour voir le monde brûler : n'aime pas les attaques par brute force et met souvent en place un rate limiting, ce qui l'amuse ☺

Log4Shell : exploitation de JNDI pour exécuter du code
Adam a créé une application Kotlin acceptant du XML et loggant avec log4j. Exploit avec JNDI et LDAP accédant à la machine.

On arrive dans le container qui n'est pas root mais contient une JVM. Possibilité d'écrire un scanner Java qui scanne le réseau. Construction d'un serveur RMI.

Quelques conseils

- Trouve un thème et raconter une histoire
- Laisse libre recours à sa créativité
- Automatisez le plus possible la création de l'environnement
- Testez, testez, testez …
- Demandez une revue
- Ecrire un guide pour résoudre le défi

Quelques ressources

- Blog d'Adam Bertrand
- Vidéo Youtube « The Great Escape »
- Site TryHackMe pour apprendre la cybersécurité en toute sécurité
- Site HackTheBox contenant des défis plus complexes