Lettre des "Lundi de la cybersécurité" n° 70

Bug Bounty
et Tests d'intrusion

Chercheur de faille = canaille ?

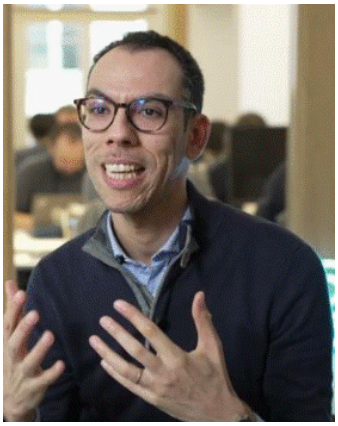
Tout dépend du côté où se place l'activité. Côté acteurs malveillants, chercher des vulnérabilités dans les applications de ses victimes pour les attaquer et en tirer profit, c'est le côté sombre de cette activité. Mais côté défenseurs chercher des vulnérabilités, en faire part au client et proposer des solutions, en étant rémunéré à la faille trouvée, le tout encadré par un contrat qui garantit le côté éthique et confidentiel de cette activité, c'est le **Bug Bounty**. En effet, un développeur n'est pas le mieux placé pour détecter des failles qu'il laisse, involontairement bien sûr, dans les applications qu'il conçoit. Le regard neuf d'un expert qui se penche sur le logiciel développé, pour en découvrir des failles, est bien plus efficace.

Et côté défenseurs des informations et des systèmes d'Information, un regard neuf et connaissant bien comment attaquer un système parce qu'il le connait ou bien découvrir comment le pénétrer parce qu'il ne le connait pas encore mais connait les méthodes pour le pénétrer, c'est le **Pentest** ou test d'intrusion.

Dans les organisations qui motivent leurs employés pour diminuer les surfaces d'attaques, on parle de trois équipes dont deux qui s'affrontent : La Red Team des attaquants, la Blue Team des défenseurs, et au milieu la Purple Team qui arbitre.

Bug Bounty et Pentests, voilà des métiers qui enthousiasmeront les plus techniques d’entre nous !

Je donne la plume à Yassir Kazar



Dans un monde où les cybermenaces évoluent à une vitesse vertigineuse, il est impératif pour les entreprises de repenser leurs stratégies de défense. Les méthodes traditionnelles ne suffisent plus face à des attaquants de plus en plus agiles et sophistiqués.

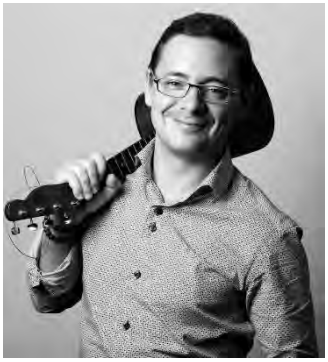
Ainsi, nous explorerons l'importance croissante des approches offensives et collaboratives telles que le Bug Bounty et le Continuous pentest. Ces méthodes permettent non seulement d'identifier les failles de sécurité avant qu'elles ne soient exploitées par des attaquants malveillants, mais aussi d'instaurer une culture de sécurité proactive au sein des organisations.

En encourageant la participation de chercheurs indépendants et en favorisant la collaboration entre experts en sécurité et équipes internes, les entreprises peuvent renforcer leur posture de sécurité de manière significative. Cette conférence sera l'occasion d'explorer les meilleures pratiques, les défis rencontrés et les bénéfices tangibles que ces approches offrent pour sécuriser les infrastructures numériques de demain.

Je reprends la plume

Yassir aurait dû être notre intervenant pour ce Lundi de la Cybersécurité du mois de mai, mais il a un empêchement pour le 13 mai, aussi il a demandé à Nicolas Kalmanovitz, Directeur des Opérations chez Yogosha, fin connaisseur, comme lui du sujet et excellent conférencier de le remplacer.

Qui est Nicolas KALMANOVITZ ?



Après 25 ans dans le software developments chez des acteurs innovants tels que Meetic et OCTO Technology, **Nicolas Kalmanovitz** est aujourd'hui COO de Yogosha, plateforme de tests de sécurité offensive.

C'est en assurant, jour après jour, l'évolution continue de leurs produits et services qu'il essaye de contribuer à la création d'un avenir numérique plus sûr.

Demande d'inscription pour le Lundi de la cybersécurité du mois de mai 2024

Lundi 13 mai, à partir de 18 h 00, par visio-conférence Zoom.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution de mes lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le nous.

Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés le lundi 13 mai, dès 18 h 00**.** La salle d'attente Zoom sera ouverte aux alentours de 17 h 00. Prévenez-nous, dès que possible si vous êtes inscrits mais avez un empêchement qui ne vous permet pas d'assister à ce webinaire.

Quelques minutes avec une organisation :

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

L'organisation sera l'initiative « **Kids Can Hack** » : une approche ludique pour faire découvrir la cybersécurité à tous, et en particulier aux jeunes enfants. C'est un site pour

apprendre le hacking avec les petits et les grands ». Allez sur **https://www.challenges-kids.fr/**, ce site vaut vraiment le coup d'œil !

A l'initiative de ce site **Sara Sellos**, chef de département à la DGA (Direction générale de l'armement), ancienne de l'ANSSI, nous dira comment faire de nos petits garnements et de nos petites filles pas toujours sages, des hackers et hackeuses, on espère éthiques, tout en s'amusant. Sara nous présentera la démarche, la plateforme et un projet d'ouvrage.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements et des comptes-rendus, écrits par Clarisse Véron, élève du master1 « Cybersécurité et e-Santé de l'université Paris Cité sur le web de l'ARCSI en **https://www.arcsi.fr/evt_passes.php.**

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos « Lundi ». Donc il est conseillé de les suivre par Zoom.

Le coin coin de l'IA Générative

Question posée à Gemini IA Générative de Google :

Le chercheur de failles est-il une canaille ?

Voici la réponse reçue :

« La question de savoir si un chercheur de failles est une canaille est complexe et dépend de plusieurs facteurs.

D'un côté, les chercheurs de failles jouent un rôle crucial dans la sécurité informatique. En découvrant et en signalant les failles de sécurité, ils permettent aux organisations de les corriger et de se protéger contre les attaques malveillantes.

D'un autre côté, certains chercheurs de failles peuvent exploiter leurs découvertes à des fins malveillantes. Ils peuvent par exemple vendre des informations sur les failles à des cybercriminels ou les utiliser pour lancer des attaques eux-mêmes.

En réalité, la plupart des chercheurs de failles sont des acteurs éthiques qui s'engagent à rendre Internet plus sûr. Ils travaillent souvent en étroite collaboration avec les organisations pour les aider à corriger les failles de sécurité.

Voici quelques éléments à prendre en compte pour déterminer si un chercheur de failles est une canaille :

- **L'intention du chercheur :** Est-ce qu'il cherche à rendre Internet plus sûr ou à exploiter les failles à des fins malveillantes ?
- **La manière dont il découvre et signale les failles :** Respecte-t-il les règles de divulgation responsable ?
- **Son passé :** A-t-il déjà été impliqué dans des activités malveillantes ?

En conclusion, il est impossible de répondre de manière générale à la question de savoir si un chercheur de failles est une canaille. Chaque cas est unique et doit être analysé individuellement.

Il est important de noter que la recherche de failles est une activité légale et protégée par la liberté d'expression. Cependant, il est important que les chercheurs de failles agissent de manière responsable et éthique. »

Gérard