THALES

NATURE DU POSTE

POSTE : Analyse sécuritaire des drivers et de l'API VirtIO - F/H

TYPE DE CONTRAT : ☐ Alternance ☑ Stage ☐ VIE ☐ Thèse

DURÉE* : 6 mois

CONTEXTE DU POSTE (Enjeux, projet, taille de l'équipe)

Notre équipe Cybersécurité est amenée à architecturer des solutions reposant sur des mécanismes d'isolation. Dans ce contexte, nous assistons de plus en plus à la mise en place de mécanisme d'isolation logiciel reposant sur de la virtualisation afin de limiter l'effet d'attaques.

VirtIO est une spécification implémentée par de nombreuses solutions de virtualisation permettant aux environnements virtualisés d'accéder aux périphériques physiques de façon transparente. Pour cela, VirtIO définit une API standardisée et optimisée se basant sur des drivers afin d'échanger des données et de virtualiser des périphériques.

Il est donc primordial pour nous d'avoir une vision claire sur le fonctionnement de VirtIO et en particulier sur son aspect sécuritaire ainsi que de s'assurer qu'il ne mette pas en défaut l'isolation apportée par les solutions de virtualisation qui l'implémente.

DESCRIPTIF DES MISSIONS

Le candidat retenu devra réaliser une étude sécuritaire de la spécification VirtIO en étudiant les protocoles et mécanismes qu'il définit entre l'hôte et l'environnement virtualisé.
Dans un premier temps, à travers une étude documentaire et de la revue de code, le candidat retenu devra comprendre le fonctionnement de VirtIO et, en particulier, son aspect sécuritaire. Le candidat devra en parallèle mettre en place un environnement virtualisé lui permettant de tester et d'étudier les drivers de VirtIO. Le candidat devra sélectionner certaines parties de VirtIO pertinentes, par exemple, certaines "devices" (Crypto, GPU, Network...) et mettre en place des attaques et tests sécuritaires lui permettant de compléter sa connaissance du système et éventuellement trouver des faiblesses dans la conception ou l'implémentation de VirtIO. Enfin, le stage fera l'objet d'un rapport détaillé sur le fonctionnement de VirtIO et éventuellement les vulnérabilités découvertes.

THALES

COMPÉTENCES (Maximum 5 par onglet)

REQUISES	SOUHAITÉES
- Maitrise du langage C/C++ - Bonne capacité rédactionnelle - Connaissance des principaux vecteurs d'attaque et vulnérabilités (ex. buffer overflow) - Connaissance de l'environnement Linux	- Expérience en Debugging et/ou maitrise de GDB fortement appréciable - Expérience en pentest - Connaissances en virtualisation et/ou maitrise de QEMU - Connaissances en système d'exploitation (gestion de la mémoire, interruptions...)

SOFTSKILLS ATTENDUES (Maximum 5)

☐ Adaptabilité	☐ Dynamisme	☐ Force de proposition	☐ Proactivité
☑ Autonomie	☐ Ecoute	☐ Méthode	☐ Relationnel
☐ Communication	☐ Esprit critique	☐ Minutie	☑ Rigueur
☐ Créativité	☑ Esprit d'analyse	☐ Organisation	☐ Synthèse
☑ Curiosité	☐ Esprit d'équipe	☐ Ouverture d'esprit	
☐ Discrétion	☐ Force de persuasion	☐ Pédagogie	

Autres : Motivation

LANGUES REQUISES ET NIVEAU ATTENDU :

Langue 1	Francais	☐ Pratique orale	☑ Les deux
		☐ Pratique écrite	
Langue 2	Anglais	☐ Pratique orale	☑ Les deux
		☐ Pratique écrite	