PROPOSITION DE SUJET
PROJET TECHNIQUE DE FIN DE E3
2e SEMESTRE 2022/2023

Document word à remplir puis transmettre par mail à Christine LECLERC et au responsable ayant validé le sujet le 13 MARS 2023 AU PLUS TARD

NOMS DES ÉLÈVES (4 minimum obligatoirement) :

1. Théo Lefèvre
2. Camille Lefebvre
3. Valentin Lallier
4. Mathis Lasson

TITRE DU PROJET : Station de détection de menaces pour les dispositifs USB

MOTS-CLÉS : USB, cybersécurité, malware, station, interface, logiciel, script, scan, virus, signature, analyse heuristique, firewall USB

DESCRIPTION DU PROJET : Nous avons choisi comme projet, de réaliser une station de détection de menaces pour les dispositifs USB. La station consiste en un boîtier contenant un ou plusieurs ports USB permettant d'y brancher les périphériques à analyser ainsi qu'un écran pour visionner le résultat du scan et évidemment d'un ordinateur (format raspberry pi) pour effectuer le traitement logiciel. Concernant les dispositifs USB pris en charge, nous souhaitons limiter l'analyse aux clés USB ainsi qu'aux câbles USB ayant potentiellement la capacité d'exécuter des scripts sur une machine en usurpant un HID car ce sont généralement les périphériques les plus utilisés. En effet, nous avons identifié une liste d'équipements USB directement destinés à lancer des scripts malveillants, voler des données, … :

- Rubber Ducky
- Bash bunny
- BadUSB
- USBHarpoon
- OMG cable

Pour ce qui est de la partie logicielle, nous souhaitons que notre système puisse scanner les fichiers présents et qu'il détecte d'une part les virus et d'autre part l'exécution de scripts malveillants directement lancés lors de l'insertion du périphérique USB. En ce qui concerne la détection de virus, nous avons identifié une première technique pour la détection de virus via l'analyse de la signature des fichiers que l'on pourrait comparer avec celles contenues dans des bases de données de virus mises en ligne mais cette technique permettrait de détecter uniquement des virus "simples". Afin d'identifier des virus plus récents et complexes, nous avons pensé à l'analyse heuristique qui se base sur l'étude du code source et l'exécution du fichier dans un environnement virtuel pour ensuite détecter des actions suspectes. La technique la plus répandue

à l'heure actuelle est l'analyse comportementale utilisant le machine learning mais nous avons conscience que cela demande des connaissances et des compétences que nous n'avons pas et que donc cette idée serait explorée en dernier si le temps nous le permettait. Dans le cas des périphériques USB usurpant les certificats de périphériques comme les claviers pour lancer des scripts automatiques, une première approche est de détecter la vitesse de frappe des touches comme l'a fait Google avec son application UKIP (USB Keystroke Injection Protection). On pourrait aussi envisager de réaliser un firewall USB se basant sur des projets open-source disponible en ligne.

TRAVAIL À RÉALISER : Réalisation du boîtier physique avec implémentation du Raspberry pi (ou modèle équivalent). Détection de scripts (Rubber Ducky, Bash Bunny et autres). Mise en place de la détection des virus. Possibilité de rajouter du machine Learning pour améliorer la détection des menaces et un port de détection de dispositifs type USBKiller ce qui inclurait de devoir faire de la soudure.

OUTILS MATÉRIELS / LOGICIELS SUPPORT :

Raspberry Pi ou mini ordinateur équivalent avec les équipements associés (alimentation, carte SD),

Imprimante 3D pour le boitier, Ecran, Visual Studio, clé USB suspecte pour tester

URL DU PROJET LE PLUS PROCHE AUQUEL CETTE PROPOSITION DE PROJET PEUT ÊTRE COMPAREE :
Le SMX de Honeywell :
https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Brochure_SMX_Cybersecurity_Honeywell.pdf
L'ICSP Neural de Symantec : https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/endpoint-security-and-management/critical-server-protection-and-industrial-control-system-protection/generated-pdfs/ICSP_Neural_6.0.0_EN_US_Help.pdf

==========
Accord du responsable de projet de fin d'année du département :

Le / / 2023