STAGE 1ere année de Célia Baylet :

OKANTIS

4ème semaine du 17 au 21 juin 2024

17/06/2024

-Je remets au propre le rapport d'audit, pour les vulnérabilités trouvées, sous forme de plans présentés ainsi :

1-Comment je les ai découvertes

2-La vulnérabilité découverte

3- Les recommandations aux développeurs pour régler la vulnérabilité

Attention à ne pas utiliser la première personne mais :"Nous constatons que…"

Dans le rapport d'audit, il faut mettre seulement les 'NON'.

-Nous avons fait la réunion avec l'escouade sécurité.

-J'ai rédigé un mail avec les questions à poser aux développeurs lors d'une réunion vendredi pour pouvoir compléter mon audit.

-J'ai eu un accès au compte admin de l'application Lynksee pour voir les différences de droit entre chaque compte.

18/06/2024

-Ce matin j'ai ajouté les recommandations aux développeurs sur le rapport d'audit.

-J'ai aussi complété la partie de la ''méthode utilisée'' et celle de ''l'outillage utilisé''.

-Cet après-midi j'ai complété le rapport d'audit avec les réponses du développeur que j'ai contacté hier.

(voir annexe 1)

19/06/2024

-Aujourd'hui c'était une journée dédiée au CTF* CNSSIS 2024 (Congrès National de la Sécurité des Systèmes d'Information de Santé) avec Ange et Clément, nous avons passé la journée à rechercher à résoudre les (14) défis.

Le CTF a commencé hier, mardi 18 juin à 19h30 et se poursuit jusqu'au jeudi 20 juin à 11h30. Le lien vers le site : https://ctf.apssis.org/settings

* CTF = Capture the Flag (challenge du monde de la cybersécurité)

(voir annexe 2)

20/06/2024

-Ce matin on a continué le CTF (on est classé 4ème sur 13).

-Cette après-midi j'ai lu le document ci-dessous et fait un tableur pour Clément avec les 'recommandations docker de l'anssi' :

''RECOMMANDATIONS DE SÉCURITÉ RELATIVES AUX DÉPLOIEMENTS DE CONTENEUR DOCKER - FICHE TECHNIQUE'' :

https://cyber.gouv.fr/sites/default/files/2020/12/docker_fiche_technique.pdf

J'ai relevé quelques éléments que j'ai trouvé intéressants.(voir annexe 3)

-J'ai revu avec Clément les derniers points du rapport d'audit.

21/06/2024

-J’ai relu le rapport avec les modifications que Clément a fait.

-Nous avons passé toute l'après-midi en réunion :

-réunion avec les développeurs pour faire un point sur la sécurité lors des développements (d'application par exemple). C’était un point entre les 2 escouades.

-point audit avec un développeur sur Lynksee pour nos dernières questions.

(voir annexe 4)

Annexe 1

Vocabulaire :

-Un fournisseur d'identité est une entité système qui crée, conserve et gère les informations d'identité des principaux et fournit également des services d'authentification aux applications de confiance au sein d'une fédération ou d'un réseau distribué.

Identity provider : Un fournisseur d'identité (IdP) est un service qui stocke et vérifie l'identité des utilisateurs.

-WAF : Un Web Application Firewall (WAF) protège le serveur d'applications Web dans le backend des multiples attaques (phishing, ransomware, attaque DDOS, malware*). La fonction du WAF est de garantir la sécurité du serveur Web en analysant les paquets de requête HTTP / HTTPS et les modèles de trafic.

*L'hameçonnage (phishing) est une technique frauduleuse destinée à piéger l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance

*Les rançongiciels ou ransomwares sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

*Une attaque en déni de service (Distributed Denial of Service) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé ...

*Le terme « malware » est un terme générique qui désigne tout type de logiciel malveillant, conçu pour s'infiltrer dans votre appareil à votre insu, causer des dommages ou perturbations à votre système, ou encore voler des données.

Annexe 2

Le lien vers le règlement du CTF : https://ctf.apssis.org/rules

Article 4 : Thématiques

Les thématiques des quatorze challenges proposés cette année sont :

Crypto

Reverse

DFIR

Réseau

Défense

Web

Vocabulaire :

Reverse : Pourquoi faire du Reverse Engineering ? Le reverse engineering est souvent utilisé pour des raisons de sécurité, par exemple pour vérifier qu'un programme fait exactement ce qu'il est censé faire ou ce pourquoi nous l'avons acheté et qu'il ne contient pas de vulnérabilités

DFIR : DFIR intègre deux disciplines distinctes de cybersécurité : l'analyse contextuelle numérique, l'investigation des cybermenaces, principalement pour rassembler des preuves numériques et poursuivre en justice les cybercriminels, et la réponse aux incidents, la détection et l'atténuation des cyberattaques en cours.

AET : signifie Advanced Evasion Techniques (Techniques d'Évasion Avancées). Ce sont des méthodes sophistiquées utilisées par les attaquants pour éviter la détection par les systèmes de sécurité, comme les pares-feux, les systèmes de détection d'intrusion (IDS), et les systèmes de prévention d'intrusion (IPS). Les AETs manipulent les données et le trafic réseau pour contourner ces systèmes et permettre aux attaques de réussir sans être repérées.

Les AET sont l'équivalent d'un passe-partout permettant aux cybercriminels d'ouvrir les portes de tout système vulnérable. Elles sont en effet capables de contourner les systèmes de sécurité réseau sans laisser aucune trace.

Une attaque DCSync : est une méthode que des acteurs malveillants peuvent utiliser pour usurper l'identité d'un DC en s'appuyant sur le protocole distant Directory Replication Services (DRS) pour demander des données de mot de passe à un DC ciblé.

DC : Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs des réseaux informatiques.

Fiche technique :

Quelques sites :

draw.io pour dessin réseau : https://app.diagrams.net/

try hack me plateforme d'entrainement CTF : https://tryhackme.com/

Autres sites utiles lors de mon stage :

https://www.dcode.fr/sha256-hash

https://www.base64decode.org/

Annexe 3

‘’RECOMMANDATIONS DE SÉCURITÉ RELATIVES AUX DÉPLOIEMENTS DE CONTENEUR DOCKER - FICHE TECHNIQUE’’ :

1
Préambule

1.1 Qu'est ce que Docker ?

Docker est une plateforme ouverte pour le développement, le déploiement et l'exécution d'applications. Il permet d'embarquer et d'exécuter une application dans un environnement cloisonné appelé conteneur. Ce cloisonnement permet d'exécuter plusieurs conteneurs simultanément sur un hôte donné. À la différence de la virtualisation où la machine virtuelle contient un système d'exploitation complet, les outils associés et l'application hébergée, le conteneur ne contient que les bibliothèques et les outils nécessaires à l'exécution de l'application, et il fonctionne directement dans le noyau de la machine hôte.

Un conteneur est une unité standard de logiciel, qui embarque le code et toutes ses dépendances, afin que l'application « conteneurisée » fonctionne normalement et de façon fiable, quelle que soit la machine hôte. L'image d'un conteneur, présente sur le système, devient un conteneur au moment de l'exécution. Dans le cas d'un conteneur *Docker*, l'image devient un conteneur lorsqu'elle fonctionne sur le *Docker daemon*, ou *Docker Engine*. L'application « conteneurisée » fonctionnera toujours de la même manière, quel que soit l'hôte. *Docker* peut s'exécuter soit sur un serveur, soit dans un *Cloud* privé, ou public, apportant une capacité de portabilité et de flexibilité dans le déploiement et l'exécution de l'application.

Docker repose sur une architecture client-serveur (figure 1.1). Un client *Docker* communique avec le *Docker daemon* pour gèrer la construction et le fonctionnement des conteneurs *Docker* ainsi que la distribution des images *Docker* issues d'un *Docker Registry*, public ou privé.

Les applications « conteneurisées » produisent au plus trois types de données :

■ les données non persistantes ou temporaires pouvant être supprimées à chaque arrêt du conteneur ;

■ les données persistantes devant être conservées après chaque arrêt ou destruction du conteneur ;

■ les données partagées avec l'hôte ou avec un ou plusieurs autres conteneurs.

Le Center for Internet Security (CIS) : est une organisation à but non lucratif américaine. La fonction du CIS est « d'aider les personnes, les entreprises et les gouvernements à se protéger contre les cybermenaces omniprésentes.

J'ai découvert la différence entre ERT et ERP :

-ERT (Établissements Recevant des Travailleurs)

-ERP (Etablissement Recevant du Public)

Un fichier ayant une extension '.pcap' est à ouvrir sur Wireshark.

Annexe 4

La sécurité des systèmes d'information (SSI) : ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information.