STAGE 1ere année de Célia Baylet :

OKANTIS

3ème semaine du 10 au 14 juin 2024

10/06/2024

-J’ai fait un point sur l'audit avec Clément pour savoir où j'en suis.

Il m’a expliqué qu’un identifiant qui est composé de 24 caractères est prédictible.

-Nous avons eu la réunion sécurité comme tous les lundis.

-J’ai continué le rapport d'audit en mettant les preuves.

-J'ai rajouté des titres aux points de l'audit, on doit pouvoir savoir de quoi on parle en lisant le rapport sans avoir le tableur sous les yeux.

(voir annexe 1)

11/06/2024

Pour plus d'information voir l'annexe.

(voir annexe 2)

J'ai assisté aux premières rencontres professionnelles de la cybersécurité, Okantis est un partenaire de cet événement.

J'ai tout d'abord assisté à un atelier qui était une "réunion du Club de la sécurité de l'information en réseau (CLUSIR)" avec Pierre VENOT et Gael LE DANTEC

Puis assisté à plusieurs conférences :

-"L'écosystème local vous accompagne" avec Anastasia SHINKAREVA, Olivier GRALL, Philippe ROCHES et Gilles ETIENNE

-"Cybersécurité & IA : amies ou ennemies" avec Pierre VENOT

-"OSINT : ce que le renseignement en source ouverte nous apprend" avec Yann PILPRÉ, Laurent FOURCADE et Damien TEYSSIER

-A la fin, nous avons participé à la remise des prix du "CTF OSINT MEDILEAK"

12/06/2024

-J'ai continué le rapport d'audit à mettre les preuves manquantes.

-Nous avons eu la réunion de l'escouade sécurité comme tous les mercredis.

-J'ai continué le rapport d'audit après avoir fait un point avec Clément.

(voir annexe 3)

13/06/2024

-attribution d'une carte professionnelle pour pouvoir rentrer dans l'établissement.

-J’ai avancé l’audit.

(voir annexe 4)

14/06/2024

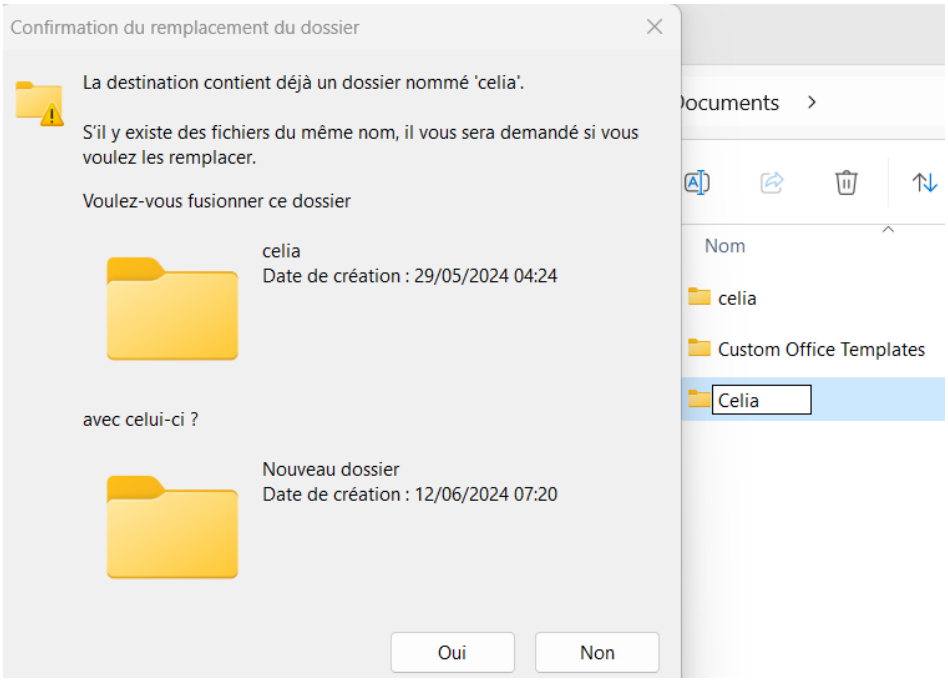
-Aujourd’hui j’ai refait un point sur l’audit de l’application Lynksee avec Clément, on a repris chaque question une à une.

(voir fiche technique annexe 5)

Annexe 1

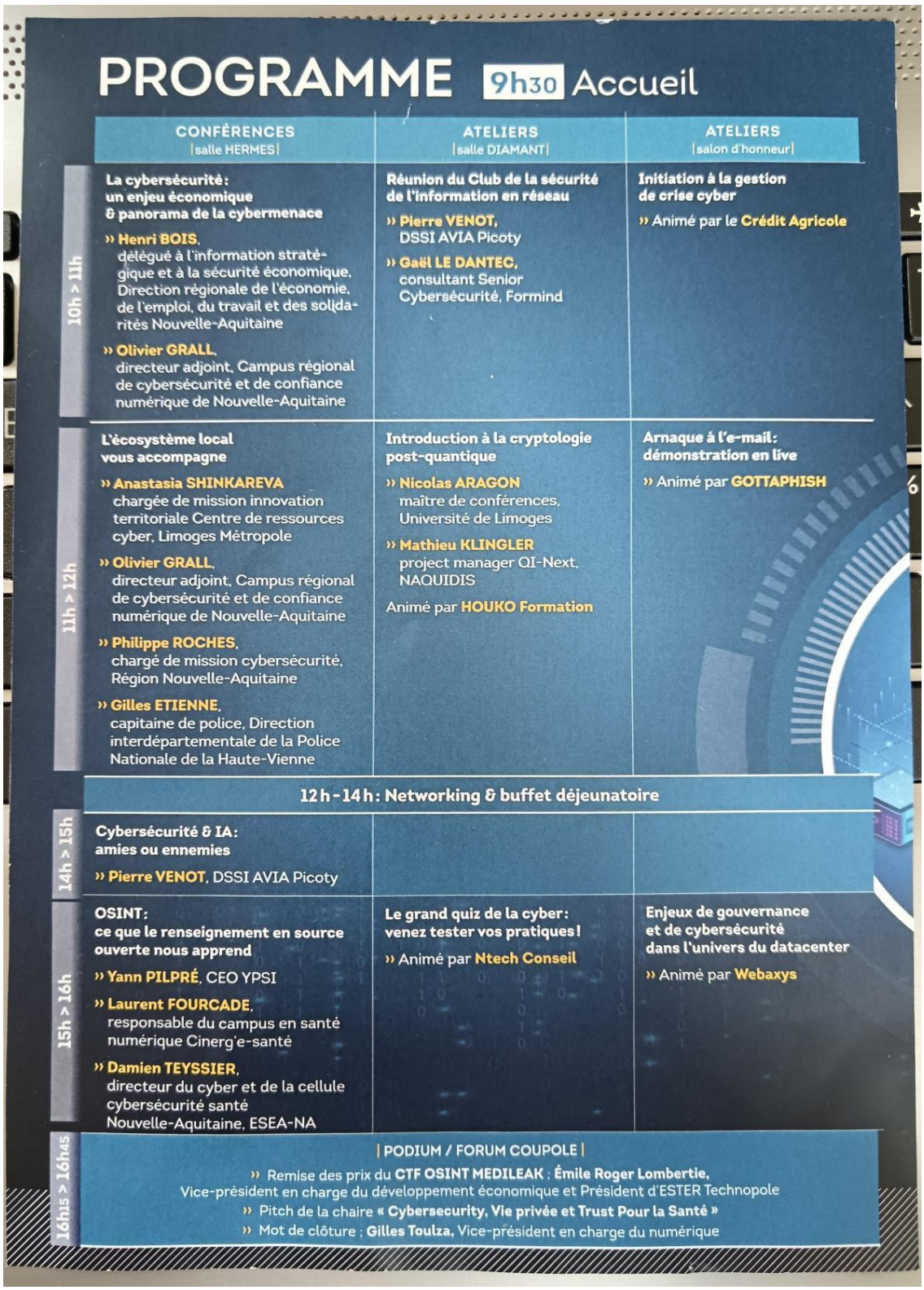
Définition sensible à la casse : se dit de tout programme qui fait une distinction entre les lettres majuscules et les lettres minuscules, et qui ne traite donc pas de la même façon les données ou les commandes selon qu'elles sont entrées en majuscules ou en minuscules.

--Windows n'est pas sensible à la casse parce que je ne peux pas créer ces dossiers par exemple malgré le fait que j'ai mis une majuscule sur le 2ème dossier :



Annexe 2

Premières rencontres professionnelles de la cybersécurité :



1-"réunion du Club de la sécurité de l’information en réseau (CLUSIR)" avec Pierre VENOT et Gael LE DANTEC

C’est une association de professionnels de la sécurité de l'information réunissant des personnes débutantes en informatique et des professionnels.

Ils ont parlé du renforcement des exigences expéditeurs, par exemple il est autorisé mais seulement sous certaines conditions d’envoyer plus de 5000 mails par jour.

Le deuxième point abordé est les JO (avec les menaces de cyber espionnage et hacktivisme).

On parle d'attaques pendant les JO, mais il n'y a pas d'attaques seulement à ce moment-là, c'est tous les jours qu'il faut sécuriser.

Le mot 'spam' a deux définitions : La définition principale est l’envoi répété d'un message électronique à un grand nombre d'internautes sans leur consentement, c’est aussi toute communication non sollicitée envoyée en masse (souvent envoyé par e-mail). Google et Yahoo définissent un spam comme étant un mail indésirable pour l’utilisateur.

2-"L’écosystème local vous accompagne" avec Anastasia SHINKAREVA, Olivier GRALL, Philippe ROCHES et Gilles ETIENNE

M. Grall nous a parlé de ‘mon aide cyber’. M. Roches de ‘neo terra’ qui travaille dans la transition sociale (égalité homme femme) et environnementale.

M.Etienne chef de l’OFAC (L'office anti-cybercriminalité) nous a expliqué que les américains sont les plus gros ‘lutteurs’ (avec le FBI). Un dépôt de plainte suite à une attaque cyber doit se faire dans les 72h, elle peut se faire en ligne. Les pirates mènent des attaques à l’international et pas seulement dans leur pays. ‘Europol’ est une agence européenne de police criminelle qui facilite l'échange de renseignements entre polices nationales au sein de l'Union européenne. ‘Eurojust’ est l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale.

‘RECYM’ propose, sur l'ensemble du territoire, des actions de sensibilisation aux risques cyber pour informer des bonnes pratiques, à Limoges des réservistes civiques s’en occupe.

Ils ont rappelé ces contacts :

https://www.cybermalveillance.gouv.fr/

Le numéro du Campus cyber : 0805292940

‘En cas d’attaque que faire ?’ : aller poser la première plainte, ne surtout pas éteindre les postes mais isoler le réseau. Ensuite prendre 2-3 semaines pour récolter les preuves utiles pour une enquête.

Il ne faut surtout pas se précipiter à tout re installer vite, car l’on risque de détruire les preuves et d’aggraver la situation car l’attaque peut donc avoir lieu à nouveau.

Ils ont aussi évoqué la rumeur des cyberattaques massives ce 13 juin. Ils ont rappelé que quoiqu’il en soit il est important d’avoir des sauvegardes immuables, car en ce moment les attaques sont effectivement déjà massives avec les JO qui vont arriver et la situation ukrainienne. Les cyberattaques ont le plus souvent lieu le vendredi soir (car c’est plus simple quand tout le monde est en week-end).

Ils ont expliqué que lorsqu’ils font des sensibilisations aux TPE (très petites entreprises), ce sont souvent celles qui ont une vraie prise de conscience, et qui appliquent bien les conseils et viennent demander conseil en cas de doute.

Les étudiants en médecine avaient jusqu’à présent seulement 1h de cybersécurité par an, ils souhaitent passer à 28h car ils sont concernés. Par exemple, ils travaillent avec les données sensibles des patients.

Les cyberattaques ont des conséquences physiques sur les personnes.

3-"Cybersécurité & IA : amies ou ennemies" avec Pierre VENOT

M. Venot a commencé par distinguer deux types d’intelligence artificielle. L’IA générative (comme chatgpt4 par exemple) et l’IA générale. Il existe aussi les LLM, mais j’en parlerai ultérieurement.

Il a évoqué l’attaque qui a eu lieu en février 2024 où un employeur a été piégé par les pirates ayant réussi une attaque au président avec un deepfake* usurpant le directeur financier du groupe lors d'une visioconférence. Comme les participants à la vidéoconférence ressemblaient à des personnes réelles, la victime a effectué 15

transactions sur cinq comptes bancaires locaux, pour un montant total de 24 millions d'euros.

Il a parlé du 'Worm gpt', qui est un 'faux chat gpt' qui peut nous écrire du code qui est 'dangereux' pour effectuer des attaques, c'est une arme des cyberattaquants pour nous piéger.

Il nous a parlé du guide de l'ANSSI sur l'IA : https://cyber.gouv.fr/sites/default/files/document/Recommandations_de_s%C3%A9curit%C3%A9_pour_un_syst%C3%A8me_d_IA_g%C3%A9n%C3%A9rative.pdf

LLM : ce sont des modèles d'apprentissage automatique capables de comprendre et de générer des textes en langage humain. Ils fonctionnent en analysant des ensembles de données linguistiques massives.

Une étude de l'université Cornell sur les agents LLM exploitant les failles 'One Day' de vulnérabilité simple.

Cette étude montre que les agents IA, peuvent exploiter de manière autonome des vulnérabilités de sécurité simple. Ces vulnérabilités, appelées "one-day", sont des failles de sécurité qui ont été divulguées publiquement, mais qui n'ont pas encore été corrigées.

L'IA est aussi utilisée de manière défensive (avec la connaissance du périmètre). L'usage utilisateur orchestre l'EDR et l'IDP.

EDR :(Endpoint Detection and Response) ou détection et réponse des terminaux surveille en temps réel la collecte des données et apporte une réponse automatique aux menaces.

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

Pour les sauvegardes, il faut penser au PRA (plan de reprise d'activité).

Moindre privilège : selon l'ANSSI, une tâche ne doit bénéficier que de privilèges strictement nécessaires à l'exécution du code menant à bien ses fonctionnalités.

*Deepfake : ou "hypertrucage" en français, est une technique utilisant l'intelligence artificielle pour créer des montages d'images, de vidéos et de sons. Bien que moralement répréhensible, il n'est pas nécessairement illégal.

4-"OSINT : ce que le renseignement en source ouverte nous apprend" avec Yann PILPRÉ, Laurent FOURCADE et Damien TEYSSIER

OSINT : Open Source INTelligent

Ce sont des données accessibles à tous. Il faut faire des liens, des corrélations entre les personnes et les actualités… L'information récupérée devient alors un renseignement. Pour pratiquer l'osint il faut avoir de la méthodologie et de la culture général.

Osint dans la santé :

Il faut faire attention au rapport à la loi et évaluer le périmètre. Ils nous ont expliqué la différence entre le sociogramme et l'organigramme.

Différence sociogramme organigramme : L'organigramme reflète en premier lieu les « preneurs de décision », le sociogramme reflète « comment elles sont mises en œuvre ». L'organigramme présente les flux d'information tels qu'ils sont conçus par la direction, le sociogramme reproduit les flux tels qu'ils s'organisent spontanément dans l'Entreprise.

Il faut récupérer des 'données blanches', car il faut pouvoir être capable de reproduire l'enquête.

Les données blanches : accessible et véracité de l'information

Les données grises : données qu'on ne peut pas reproduire (par exemple la conférence d'aujourd'hui, dans 3 mois, elle ne pourra pas être reproduite à l'identique). Autre exemple : un employeur va rechercher le profil LinkedIn d'un éventuel salarié.

Les données noires : données confidentielles, données médicales. C'est un secret professionnel, elles reflètent de la vie privée de la personne. Par respect, il faut faire comme si l'on n'était pas au courant de ce que l'on a vu / ce que l'on sait.

Avec de la collecte et de l'analyse de l'information cela devient un renseignement.

L'osint doit être réalisé dans un cadre éthique et juridique.

Même si une entreprise se protège pour ne pas fournir d'information (grise ou noire), le prestataire peut en donner.

L’osint peut permettre de trouver des faiblesses dans les centres hospitaliers. Par exemple, un plan 3D du bâtiment pour les patients peut être une source d’attaques faciles en connaissant où sont situé les salles d’administrations, de communication, d’hébergement.

Par exemple dans les hôpitaux aux services pédiatrie, il y a un problème avec les post-it, les disques durs, car les données sont grises et voir noires.

Il existe des campagnes de désinformation qui sont très faciles à réaliser avec un sociogramme. En donnant aux IA telle ou telle relation entre certaines personnes, elles peuvent générer de faux mails pour effectuer une attaque.

Les IA peuvent donc être offensives ou défensives.

Le problème reste toujours la personne et comment elle utilise l’outil, mais pas l’outil en lui-même.

Pour les soignants certains suivent des formations en cybersécurité à l’occasion des JO. Certaines entreprises veulent sensibiliser leur personnel avant les JO par rapport à différents types de risques.

5-A la fin nous avons participé à la remise des prix du "CTF OSINT MEDILEAK"

Une équipe de débutants dans l’osint ont fini premiers. La morale est que l’osint est accessible à tous.

Annexe 3

Vocabulaire :

-->La méthode de type POST sert notamment à envoyer des données de formulaire HTML, lorsqu'un internaute remplit un formulaire sur un site web. La méthode PUT, similaire, permet également de transmettre des données au serveur, pour ajouter ou remplacer une ressource sur le serveur.

-Une requête PUT est une méthode HTTP utilisée pour créer ou mettre à jour une ressource sur le serveur.

-->L'en-tête « Access-Control-Allow-Origin » permet d'indiquer si l'origine est autorisée à accéder à la ressource demandée sur le serveur. Elle spécifie généralement un domaine ou une liste de domaines qui sont autorisés à effectuer des requêtes cross-origin vers cette ressource.

-Le CORS (ou Cross-Origin Resource Sharing) permet au navigateur du client de vérifier auprès des serveurs tiers si la requête est autorisée avant tout transfert de données.

<script type= “javascript”>alert(“test”)</script> j'ai utilisé cette commande pour observer si les entrées utilisateurs sont traités de manière sécurisée par le serveur pour proscrire tout type d'injection coté serveur.

-La falsification de demande intersite (CSRF) fait référence à une attaque qui fait que l'utilisateur final effectue des actions indésirables dans une application Web qui lui a déjà accordé l'authentification.

Annexe 4

Attaque csrf : https://kinsta.com/fr/blog/attaques-csrf/#questce-quune-attaque-csrf

Généralement, une attaque CSRF implique des requêtes de changement d'état, car l'attaquant ne reçoit pas de réponse. Parmi les exemples de ces requêtes, on peut citer la suppression d'un enregistrement, la modification d'un mot de passe, l'achat d'un produit ou l'envoi d'un message. Toutes ces actions peuvent se produire à l'insu de l'utilisateur.

L'attaquant malveillant utilise généralement l'ingénierie sociale pour envoyer à un utilisateur peu méfiant un lien par l'intermédiaire d'un tchat ou d'un e-mail.

Lorsque l'utilisateur clique sur le lien, il exécute les commandes définies par l'attaquant.

Par exemple, en cliquant sur un lien, l'utilisateur peut transférer des fonds de son compte. Il peut également modifier l'adresse e-mail d'un utilisateur, l'empêchant ainsi d'accéder à nouveau à son compte.

Le Dossier Médical Partagé (DMP) : est un carnet de santé numérique qui conserve et sécurise vos informations de santé : traitements, résultats d'examens, allergies

Si on avait déjà un DMP, son contenu a automatiquement été ajouté à notre profil Mon espace santé.

Les séquences d'échappement : permettent d'écrire des caractères dans des documents balisés en utilisant uniquement des points de code ASCII. Elles sont très pratiques quand vous ne pouvez pas saisir un caractère dont vous avez besoin ou quand vous souhaitez visualiser dans votre code un caractère invisible.

Annexe 5

Fiche technique :

Pour transférer un dossier de la VM à mon ordinateur Windows :

Sur la VM (installation ssh):

sudo apt install openssh-server

systemctl status ssh

systemctl start ssh

Puis taper (le nom d'utilisateur et l'adresse ip de la VM) :

ssh user@host

(user: utilisateur1 host : 10.X.X.X (ip vm))

Sur Windows (copié le dossier de la VM à un dossier sur l'ordinateur) :

C:\Users\cbaylet> scp -r utilisateur1@10.X.X.X:/home/utilisateur1/.ZAP/sessions/ZapAudit C:\Users\cbaylet\Documents\celia

scp de ssh et cp de copie

-r pour copier un dossier et pas un fichier

Si on a l'adresse https://lynksee-demo.okantis.io/api/auth/...

//FQDN(Fully Qualified Domain Name) : nom domaine

//api/auth : est appelé endpoint

//get post put delete

Vocabulaire :

La méthode GET passe les réponses saisies via l'URL tandis que la méthode POST passe les paramètres dans le corps de la requête. La méthode HTTP DELETE supprime la ressource indiquée.

put = Une requête PUT est une méthode HTTP utilisée pour créer ou mettre à jour une ressource sur le serveur.

Un Endpoint est ce qu'on appelle une extrémité d'un canal de communication. Autrement dit, lorsqu'une API interagit avec un autre système, les points de contact de cette communication sont considérés comme des Endpoints.

On a aussi fait un rappel des adresses privées :

10.0.0.0/8

172.16.0.0/12 101001100 00010000 00000000 00000000

192.168.0.0/16

Partie hôte et parti réseau

La partie réseau est commune à l'ensemble des hôtes d'un même réseau.

La partie hôte est unique à l'intérieur d'un même réseau.