Cybersecurity Institute
Université Grenoble Alpes

Reshaping technologies and social sciences

CALI-SSI: ChALlenge Interdisciplinaire en Sécurité des Systèmes d'Information

Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, 16-18 Décembre 2020, Nouan-le-Fuzelier.

Romain Xu-Darme
16 Décembre 2020
romain.xu@univ-grenoble-alpes.fr

financed by
IDEX Université Grenoble Alpes

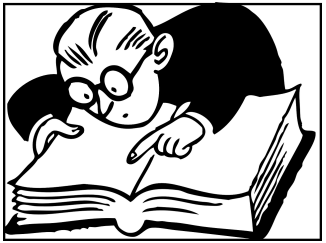
This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02).

Sommaire

- Problématique technique
  - Concevoir des briques de sécurité **robustes**
  - Concevoir des outils d'**évaluation** de sécurité
  - Améliorer la **résilience**
- Problématique juridique
  - **Réguler** le cyberespace
  - Protéger les **données privées** des citoyens
- Problématique sociétale
  - Quel impact des nouvelles technologies sur la société ?

La nécessité d'un langage commun

"En reversant le binaire du serveur avec Ghidra, j'ai identifié un buffer overflow dans la pile TCP/IP et écrit un *exploit* pour un DOS."



"L'obligation d'utilisation non-dommageable du territoire telle qu'exprimée par la Cour internationale de justice est une obligation dite de due diligence qui désigne ainsi une obligation de comportement et non une obligation de résultat."

K.Bannelier&T. Christakis, *Cyberattaques. Prévention-réactions : rôle des Etats et des acteurs privés/Cyberattacks. Prevention-Reactions*, Les Cahiers de la Revue Défense Nationale, 2017

Un challenge interdisciplinaire ?

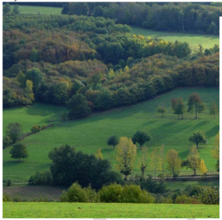
- CALI-SSI n'est pas (que) un CTF
- CALI-SSI n'est pas (que) un Strategy Challenge
- Compétition hybride entre challenge de sécurité et gestion de crise basée sur un scénario fictif.
- Des équipes mixtes entre étudiants en informatique et cybersécurité et étudiants en droit
- **Technique :** Investigation numérique afin d'analyser une cyberattaque
- **Juridique :** Proposer des solutions concrètes basées sur le droit national et international afin de sortir de la crise

- Introduit le scénario fictif de crise
  - Contexte géopolitique et relations internationales
  - Crise contenue à l'échelle locale (régionale, nationale)
- **Objectif** : Mettre en évidence l'étendue de la menace
- Les équipes ont 15 jours pour remettre un rapport écrit décrivant :
  - leur évaluation de la situation avec une analyse de risque à court/moyen/long terme
  - les preuves recoltées par l'investigation numérique
  - leurs recommandations sur les actions à mettre en place
  - les rapports écrits seront à destination du cabinet du Premier Ministre français.

Cybersecurity Institute
Université Grenoble Alpes

ZAD de Roybon – Le résultat du referendum contesté par les partisans du projet Middle Park

03 juin 2024



La tension monte entre les militants écologiste
partisans du projet de centre de vacances Middl
referendum organisé par la mairie de Roybon ce
publiés.

Date : 18/06/2024. 13:55
From : Magalie Vernom <magalie.vernom@ssi.gouv.fr>
To : ssi@eoila.fr
Subject : Découverte d'un fichier de mots de passe de votre SI

Monsieur,
à l'occasion d'une opération de veille effectuée sur le site Reddit le 17 juin 2024, nos équipes ont mis à jour un fichier contenant les identifiants et mots de passe de quelques utilisateurs de votre usine (voir ci-dessous). Ce fichier a pu permettre à des individus mal intentionnés de pénétrer dans votre système et de provoquer les dysfonctionnements parus récemment dans la presse. C'est pourquoi, nous ne saurions que trop vous conseiller de demander à l'ensemble de vos utilisateurs de changer leurs mots de passe immédiatement.

ccharbonneau:$1$42388n45$65gK1VsOfHurgH5lWLY741
vbarrette:1W2Zcca8E$Jbdv8eYe2XVQiAPGr339r1
mpinette:1SWkhcIC8$20UjfvsTnLh7hrqJTf4vS0
laupry:1yH/XFTwo$b.AU3FTg6flSoXUSuM0nB.
fthivierge:1KlnjJKng$DjGkka46Hy36FIYAr6U8Q1
clafond:1J23ZOwEw$FPxHO9mIY637g8j3wfe89/
ltollmache:1GCTlDIg3$ZVmitfFPwjYgjFTRfaxcP.
acouet:1zBnUzWDG$ttHgV.YXG2BGabNFRWY6z0
ssicard:1m.T3gxyw$WpTkB6Duq8eTSijXOP4kv/
gflamand:1zz/.qC8s$KQdU47a95yaar4pFK847S1
mgadbois:1z9N9ROHg$jWnxSUXSgCceypKUwdoqM.
alaberge:1VuJxyjDK$ZTx1mBYUZz.bglqwm.6Ku.
adavis:1QBgZ.BmS$2X8Db8jfWLrbta76KgYc61
ebrault:1a8ubaar9$f6ypx8bF/4ncvJBmNf3Qj.
clagrande:1t5.uglKJ$FHUPfgCH4r8BVnjEBmOox.
aallaire:1uw70MDRw$AQrJb6F3uaNHUdYvn5Mj7.
ymathieu:1V6.ZWkc/$FbzS/UItDAeMKouwR7i.p/
mbegin:1.IMwqqoW$PD.gAT/cmusi/2CcOLcut1
rsevier:1QMiHvvcG$ficZ8CHT9oEJlyVbjtAr4/
nsouplet:1R56aAH/P$m2eoM4diJwR.LhQNJZYed1

Pour rappel, l'ANSSI met à votre disposition une note contenant des recommandations de sécurité relatives aux mots de passe.
Nous restons bien évidemment à votre disposition pour vous apporter toute l'aide nécessaire afin de renforcer votre infrastructure informatique.
Veuillez agréer, monsieur, l'expression de nos sentiments distingués
--
Magalie Vernom - Service relations industrielles
Agence Nationale de la Sécurité des Systèmes d'Information

Alerte sanitaire : présence a de chlore dans l'eau du robi plusieurs villes de l'agglom grenobloise

par Pauline Menat (Dauphiné Libéré) – 13 juin 2024 - 12h42

Les faits

- Depuis hier, la qualité de l'eau du robinet de l'agglomération gr fortement dégradée et plusieurs dizaines d'habitants se sont plaints au niveau de la gorge et des yeux
- Le bébé d'un couple de touristes américains a été admis à l'hôpit d' « urgence absolue »
- Des relevés ont mis en évidence une dose anormale de chlore dans l

President of the USA @POTUS
I am truly sorry having not met preachy @Miljodep expectations. Maybe I will when her fishy green friends are caught in the net of justice.
13.7K 7:01 PM - May 16, 2024
22.6K people are talking about this

Miljödepartementet @Miljodep
Despite his efforts, @POTUS didn't meet the world's expectations on his responsibilities as the second world polluter... #ParisAgreement
49.3K 2:26 PM - May 16, 2024
17.8K people are talking about this

President of the USA @POTUS
Despite our efforts to find a fair compromise, the #ParisAgreement remains invasive and too coercive. Our nation will NOT renounce freedom!
60.7K 2:17 PM - May 16, 2024
28.1K people are talking about this

- La crise a évolué en une catastrophe internationale.
- **Objectif :** Mettre un terme à la cyberattaque
- Les équipes finalistes ont 15 jours pour préparer une présentation orale de 10 min avec leurs recommandations

- Les rapports et présentations sont évalués par un jury d'experts en cybersécurité, géopolitique et droit international

Evaluation des risques	Capacité à déterminer les risques présentés dans le scénario et à évaluer leur gravité et leur probabilité d'occurrence
Investigation numérique	Capacité à résoudre les *challenges* techniques et à associer un niveau de confiance aux preuves numériques récoltées
Originalité des solutions	Capacité à innover dans les suggestions sur les actions à mettre en oeuvre
Qualité de synthèse	Capacité à rendre compte de la situation à un public non expert
Qualité de la présentation	Capacité à convaincre un décideur fictif de mettre en oeuvre les actions proposées (acte II uniquement).

Retours de l'édition 2019

- 13 étudiants répartis en 4 équipes lors de la première édition (octobre/novembre 2019)
- Retours très positifs quant à la pertinence de la compétition par rapport à leur formation
- Des échanges durables entre les étudiants même après la compétition

Vers une compétition annuelle ?

- Une édition 2020/2021 en cours de préparation
  - Scénario en cours d'écriture
  - 18 étudiants répartis en 5 équipes en lice pour la prochaine édition (janvier 2021)
  - Intégré à la formation CSI (Cybersécurité et Informatique Légale) de l'Université Grenoble Alpes
- Avec le soutien du Grenoble Alpes Cybersecurity Institute (Cyber@Alps), possibilité d'organiser une compétition annuelle

- CALI-SSI : Une compétition novatrice, interdisciplinaire de gestion de crise en cybersécurité
- Objectifs pédagogiques
  - Un travail collectif entre étudiants de formations hétérogènes
  - Un travail de synthèse de connaissances pour un public non expert
  - Un travail d'expression orale et écrite
  - Sensibilisation à la cybersécurité au sens large

Remerciements : J.Mercier, M.Becuywe, C.Bras, P.Lafourcade, F.Autréau, C.Castelluccia, K.Bannelier, P.Elbaz-Vincent, M.Kauffmann