

Track Flaw

Full overall pentesting

ESGI

école supérieure de
génie informatique

Introduction à la sécurité informatique

2A ESGI

Année 2022/2023



Whoami

Whoami



Thibaud Robin

- 🧑‍💻 Auditeur/pentester chez Tracklaw
- 🧑‍🏫 Enseignant à l'ESGI
- 🐦 Twitter
- 🔗 LinkedIn



Au menu de ce cours

Sommaire



1

Définitions

2

Filière SI à l'ESGI

3

Métiers

4

Théories

5

Pratiques



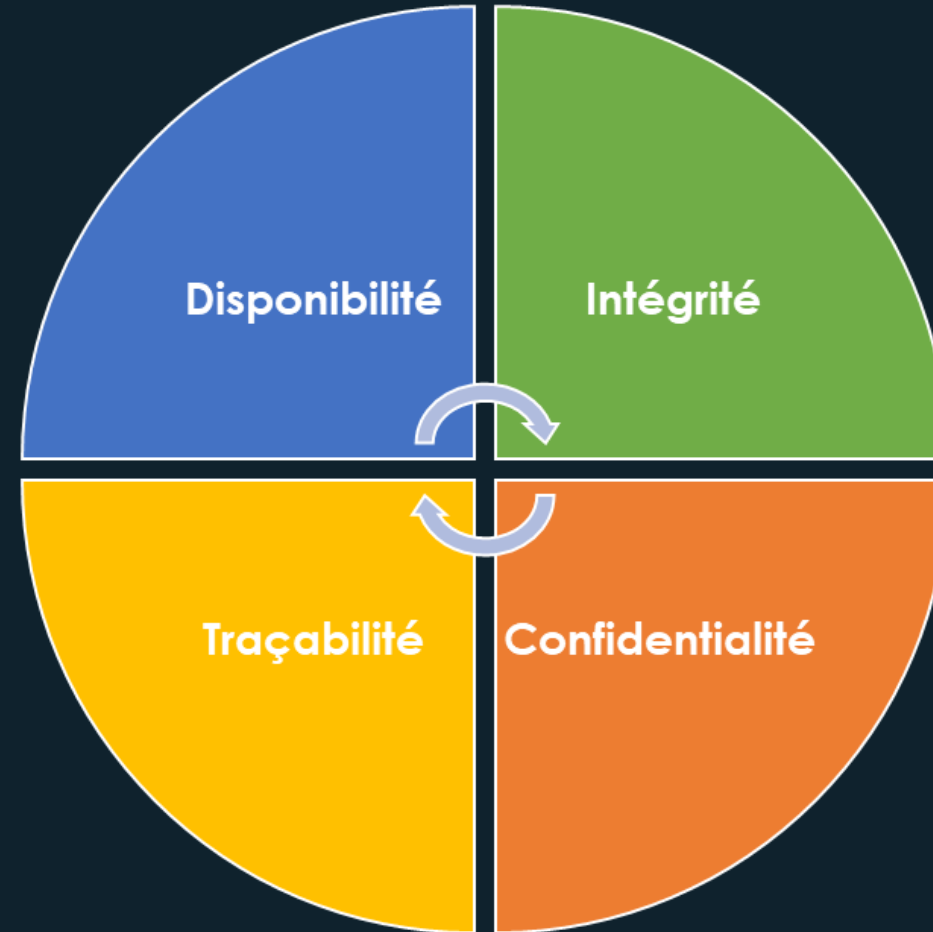
Définitions

Définitions

A decorative graphic in the top-left corner consisting of a network of small dots connected by thin lines, resembling a molecular or digital structure.

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.

Définitions



Définitions

A decorative graphic in the top-left corner consisting of a network of small dots connected by thin lines, resembling a molecular or digital structure.

Audit

- Évaluer le niveau de sécurité des applications/produits ou/et SI
- Détecter des vulnérabilités → traduire en risque métier
- Proposer des correctifs → aider le client à établir un plan d'action



Security Operation Center (SOC)

- Equipe en charge d'assurer la sécurité de l'information.
- Supervision et l'administration de la sécurité du SI au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.
- Le SIEM (Security Information Event Management) est l'outil principal du SOC → permet de gérer les évènements d'un SI.



Computer Emergency Response Team (CERT)

- Centre d'alerte et de réaction aux attaques informatiques.
- Destiné aux entreprises ou aux administrations.
- Vulgairement appelé "Pompiers" dans le métier.



Cyber Threat Intelligence (CTI)

- Issu du monde du renseignement.
- Collecte et surveillance d'informations publiques.
- Objectif :
 - Anticiper les attaques.
 - Faciliter la tâche du CERT et du SOC.

Définitions



OSINT Open Source Intelligence : renseignement en source ouverte.

Cracking Déverouillage de logiciel.

White/Black/Gray hat Termes pour définir les volontés et les actions d'un attaquants.

Deface Action illégale destinée à vandaliser et dégrader l'image d'un site web.

Etc...



La sécurité informatique à l'ESGI

Programme



3e année

Cryptographie

Détection des vulnérabilités

Assembleur

Durcissement des OS

Sécurité WiFi

Sécurité physique

CEH

Forensic

Exploits

Programme



3e année

- Cryptographie, clé et certificats
- Détection de vulnérabilités
- Sécurité assembleur
- Hardening des OS / Sécurité des réseaux WiFi
- Sécurité Défensive et Sécurité périmétrique d'un SI
- Sécurité et intrusion physique
- Préparation et passage de la certification CEH (Certified Ethical Hacker)
- Kernel Windows, Volatilité et Analyse de RAM
- Gestion des exploits

Programme



4e année : NOUVEAUTE NEW

Filière technique ou Filière fonctionnelle

Programme



4e année : tronc commun

Durcissement des OS++

Shellcode

CTI

Audit ISO

Sécurité Python

Cryptographie++

Sécurité IOT

Programme



4e année : tronc commun

- Sécurité avancée des systèmes
- Sécurité Shellcode
- Détection des intrusions, Threat hunting
- Analyse Forensic
- Sécurité du système d'information
- Sécurité avec Python : Volatility, Modularité, Automatisation
- Cryptographie avancée
- Sécurité des IOT

Programme



4e année : spécialités

Fonctionnelle

Gouvernance Management SI

ISO 27001 EBIOS Risk Management

Sécurité cloud

Technique

Shellcode++

Reverse Audit mobile

Programme



5e année : tronc commun

Sécurité réseau

Forensic réseau

Analyse de malware

Audit et test d'intrusion

Sécurité SCADA

Sécurité RFID et radio

Droit informatique

Cryptographie+++

Programme



5e année : tronc commun

- Cryptanalyse
- Sécurité avancée des réseaux
- Network Forensic
- Analyse avancée de malwares
- Audit et Test d'intrusion
- Sécurité des systèmes SCADA
- Sécurité RFID et Radio
- Droit, éthique et cyber-criminalité

Programme



5e année : spécialités

Fonctionnelle

CISSP CISA

ISO 27001++ EBIOSRM / ISO27005

CERT Management

Technique

OSCP IAM RedTeam

Challenge CTF

Sécurité offensive

Programme



 Le choix de la spécialité débouche sur le même diplôme.

Elle permet de vous spécialiser et de vous préparer au mieux à votre futur métier.

Programme



Tous les jeudis après-midi : HACKLAB !!!



- Laboratoire de recherche.
- CTF, recherche de vulns et présentation.
- Aucun niveau requis.
- Tous les jeudis de 15h45 à 19h00.



Les métiers

Auditeur/Pentester



- 🕵️ La personne à capuche.
- Sécurité offensive.
- A pour mission de déceler des vulnérabilités.
- Souvent lié à un cabinet de conseil.
- Effectue des missions courtes variées de 1 à 2 semaines :
 - Audit de code
 - Test d'intrusion
 - Audit de configuration
 - Etc...

Analyste SOC



- 👁 L'oeil de Sauron.
- Surveille un système d'information.
- Maintient les dispositifs de surveillance.
- Effectue des actions de prévention.
- Travail pour un SOC interne ou externalisé.

Analyste CERT



- 🧑‍🚒 Le pompier.
- Effectue des analyses en cas de compromission ou de suspicion.
- Analyse les modes opératoires d'attaquants.
- Effectue de la veille informatique.
- Coordination avec d'autres entités.


Analyse CTI




- 🔍 Le détective numérique.
- Centraliser et analyser un maximum de données en accès public.
- Renforcer les protections de la structure.
- Infiltrer des groupes d'attaquants.
- Collecter et analyser des fuites de données.
- Communiquer sur les éléments critiques découverts.

Consultant sécurité



-  La personne à tout faire.
- Effectue de la gouvernance et de la gestion de risque.
- Assez peu technique.
- CISSP, ISO, etc.
- Formation et sensibilisation.
- Gestion de projet sécurité.
- Assistance au RSSI.



-  Le boss.
- Responsable de la Sécurité des Systèmes d'Information.
- Analyse de risques.
- Sensibilisation et formation aux enjeux de la sécurité.
- Étude des moyens et préconisations.
- Audit et contrôle.
- Veille technologique et prospective.



Un peu de théorie

Clause de non-responsabilité



ATTENTION !

Il est **totalelement illégal** d'utiliser les connaissances et les compétences acquises durant ce cours sur une cible **sans son autorisation explicite**.

La peine encourue est de **3 ans d'emprisonnement** et **45 000€ d'amende**.

Les différents domaines



Sécurité Web

Sécurité Linux

Ingénierie inverse

Exploitation de binaire

Cryptanalyse

Forensique

Stéganographie

Sécurité réseau

Programmation et automatisation

Sécurité web



- Evaluer la sécurité d'une application web : OWASP
- Détecter des vulnérabilités applicatives.
- Analyser un code source.

Pratiques



Root - Me

<https://root-me.org>



HackTheBox

<https://www.hackthebox.com/>

Sécurité Linux



- Analyser des configurations systèmes.
- Analyser des scripts.
- Analyser les vulnérabilités d'un système d'exploitation.

\$ Outils

Linpeas

LinEnum

LSE

\$ Pratiques

OverTheWire

Root - Me

HackTheBox

Ingénierie inverse



Pratique qui consiste à analyser un produit fini (comme un logiciel d'application ou une puce) pour connaître la manière dont celui-ci a été conçu ou fabriqué.

\$ Outils

IDA

Ghidra

WinDBG

GnuDBG

\$ Pratiques

Analyse de malware

Pentest de client lourd

Crackme

Exploitation de binaire



Exploitation d'un programme informatique à travers des failles logiques dans son code source.

\$ Outils

IDA

Ghidra

WinDBG

GnuDBG

PwnTools

Python

\$ Pratiques

- Très peu d'utilité dans la vraie vie (hormis recherche de vulnérabilités).
- CTF et plateformes de challenge.

Cryptanalyse



La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement.

\$ Outils

Mathématiques

Langages de programmation

\$ Pratiques

- Utilisé parfois en analyse forensique.
- Débouche sur le métier de cryptologue.

Forensique



L'analyse scientifique de cas, appelée la forensique, regroupe l'ensemble des différentes méthodes d'analyse fondées sur les sciences afin de servir au travail d'investigation de manière large.

\$ Outils

Volatility

Linux

Foremost

Autopsy

Wireshark

Cellebrite

\$ Pratiques

- Métier d'analyste forensique (ex: police judiciaire).
- CTF et plateformes de challenge.

Stéganographie



La stéganographie est une forme de dissimulation (ou d'offuscation) d'information dans le but de transmettre un message de manière inaperçue au sein d'un autre message.

\$ Outils

StegHide

Aperisolve

Audacity

Exiftool

Stegsolve

Zsteg

\$ Pratiques

- Très peu d'utilité dans la vraie vie.
- CTF et plateformes de challenge.

Sécurité réseau



Analyser et manipuler les différents protocoles et services les plus courants pour les exploiter et les compromettre.

\$ Outils

Scapy

Wireshark

Python

\$ Pratiques

- Nécessite de bonnes connaissances en réseau.
- Parfois utilisé en intervention CERT et en analyse forensique.
- CTF et plateformes de challenge.

Programmation et automatisation



Programmez et automatisez des tâches de plus en plus complexes pour résoudre des problèmes techniques.

\$ Outils

Langages de programmation au choix

Python

C/C++

\$ Pratiques

- Très courant dans tous les métiers de la sécurité informatique.
- Développement d'application web ou mobile.
- CTF et plateformes de challenge.



Ouf... Trop d'infos...



Vite de la pratique !

Avoir les bases de Linux



overthewire.org/wargames/bandit/

Wargames Information ^{updated}

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

Donate! Help?

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. **If you notice something essential is missing or have ideas for new levels, please let us know!**

Note for beginners

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidemenu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. **Don't panic! Don't give up!** The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information. If you've never used the command line before, a good first read is this [introduction to user commands](#).

There are several things you can try when you are unsure how to continue:

- First, if you know a command, but don't know how to use it, try the **manual** (man page) by entering **man <command>**. For example, **man ls** to learn about the "ls" command. The "man" command also has a manual, try it! When using **man**, press **q** to quit (you can also use **/** and **n** and **N** to search).
- Second, if there is no man page, the command might be a **shell built-in**. In that case use **help <command>**.

OverTheWire

<https://overthewire.org/wargames/bandit/>

- Démarrer avec le level 0.
- Objectif level 34 ! 🚀



Surprise pour la suite !

Examen

A decorative graphic in the top-left corner consisting of a network of small grey dots connected by thin, light-grey lines, forming a complex web-like structure.

1 TP au choix noté.

1 QCM final sur papier.

Au boulot !



Track Flaw

Full overall pentesting