



# Introduction à la cybersécurité

CLUB DE SÉCURITÉ INFORMATIQUE (CSIUL)  
UNIVERSITÉ LAVAL  
HIVER 2025

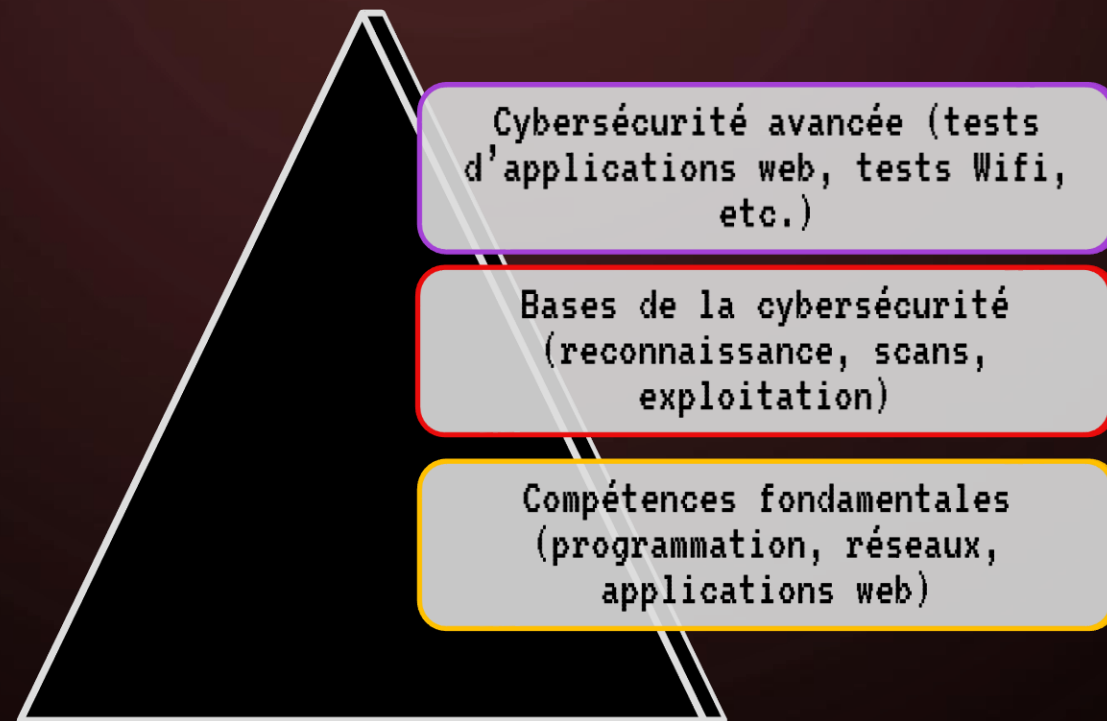
PRÉSENTATION PAR MARC-ANDRÉ BEAULIEU

MODIFIÉ PAR JEAN-NICOLAS TURBIS

# PLAN DE LA SÉANCE

- Apprendre la cybersécurité
- Suite de formations
- Le monde de la cybersécurité
  - Hackers, pentesters et analystes en cybersécurité
    - Script kiddie
  - Red team et blue team
  - Tests d'intrusion (pentests)
    - Phases d'un test d'intrusion
- Outils
  - Les outils en cybersécurité
  - Linux
  - Kali et ParrotOS
  - Les machines virtuelles
  - Installer kali ou parrotOS
- Pratique
  - Tutoriels, environnements de pratique et CTFs
  - Tutoriels
  - Environnements de pratique
  - CTFs
  - Projet lab hacking
  - CSIUL

# APPRENDRE LA CYBERSÉCURITÉ



# SUITE DE FORMATIONS DU CSIUL



>> Introduction à la cybersécurité

Les réseaux

Les applications web

La reconnaissance en cybersécurité

Les scanners de réseaux et de vulnérabilités

Les attaques web

Les attaques systèmes et réseaux

INTRODUCTION

COMPÉTENCES FONDAMENTALES

BASES DE LA CYBERSÉCURITÉ

The background features a dark, gradient field of concentric circles centered in the upper half. In the corners, there are stylized, glowing red circuit traces with small circular nodes, resembling a digital or network theme.

# LE MONDE DE LA CYBERSÉCURITÉ

# HACKERS, PENTESTERS ET ANALYSTES EN CYBERSÉCURITÉ

- **Hacker**
  - Quelqu'un qui aime comprendre comment l'informatique fonctionne et le modifier / briser
  - Malheureusement souvent péjoratif
  - Rarement utilisé au niveau professionnel
  - Souvent utilisé dans la communauté, loin des gestionnaires et des RH
- **Penetration tester (pentester)**
  - Hacker employé par une entreprise pour hacker leurs services et identifier leurs vulnérabilités
  - Synonymes : Testeur en cybersécurité, Testeur d'intrusion, Hacker éthique
- **Analyste en cybersécurité**
  - Inclus aussi les analystes en sécurité défensive

# SCRIPT KIDDIE

n. (Hacker Lingo) One who relies on premade exploit programs and files ("scripts") to conduct his hacking, and refuses to bother to learn how they work. The script kiddie flies in the face of all that the hacker subculture stands for - the pursuit of knowledge, respect for skills, and motivation to self-teach are just three of the hacker ideals that the script kiddie ignores. While anyone can be a script kiddie, generally they are teenagers who want the power of the hacker without the discipline or training involved. Obviously anyone who follows this route aspires to be a blackhat, but most refuse to even dignify them with this term; "blackhat" generally implies having skills of your own.

- Urban Dictionary

# RED TEAM ET BLUE TEAM DANS LES ENTREPRISES

## RED TEAM

### Cybersécurité offensive

- Pentesters
- Chercheurs en cybersécurité

## BLUE TEAM

### Cybersécurité défensive

- Détection d'incident
- Réponse aux incidents
- Développeurs DevSecOps

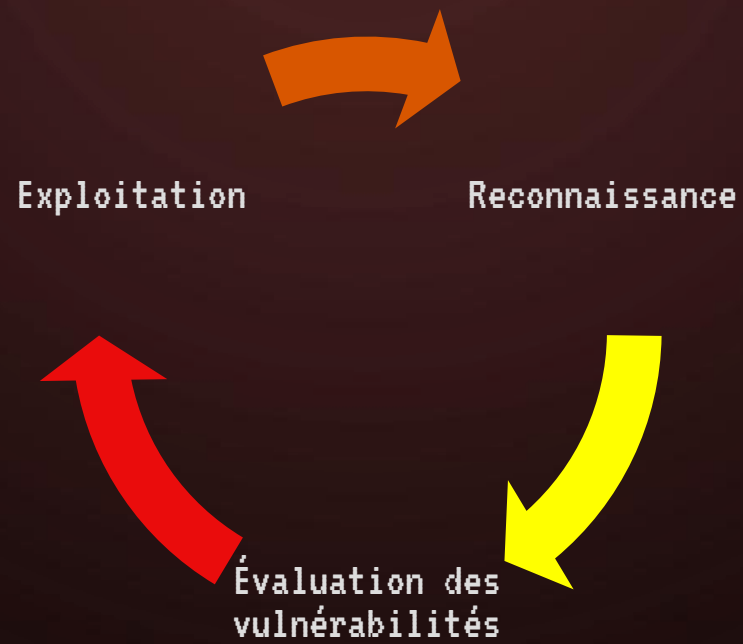
En général, il y a plus d'offres d'emploi de **blue team** que de **red team**



# TESTS D'INTRUSION (PENTESTS)

- Simulation de cyberattaque autorisée
- Évaluer la sécurité d'un système informatique
- Suivi par un rapport de test d'intrusion
- 3 phases

# PHASES D'UN TEST D'INTRUSION





OUTILS

## LES OUTILS EN CYBERSÉCURITÉ

- Script qui automatise une attaque qui pourrait souvent être faite à la main
- Rendre des tâches plus faciles et rapides
- Pas magique
- Ex.: *Hydra* est un outil qui permet d'attaquer, par force brute, une page d'authentification en envoyant des milliers de requêtes d'authentification par minutes

# LINUX

- Famille de systèmes d'exploitation (OS) (comme Windows)
  - Distributions
- Open Source
- Entièrement personnalisable
- Plusieurs distributions
  - Ubuntu
    - Desktop
    - Server
  - Mint
  - Kali
  - ParrotOS

# KALI ET PARROTOS



Distributions de linux



Axé sur la  
cybersécurité offensive



Plusieurs outils  
préinstallés

# MACHINES VIRTUELLES



- Système d'exploitation virtuel
- Exécuté sur votre système d'exploitation principal, sous forme d'application
- On n'est donc pas obligé de remplacer notre cher Windows !

## INSTALLER KALI OU PARROTOS

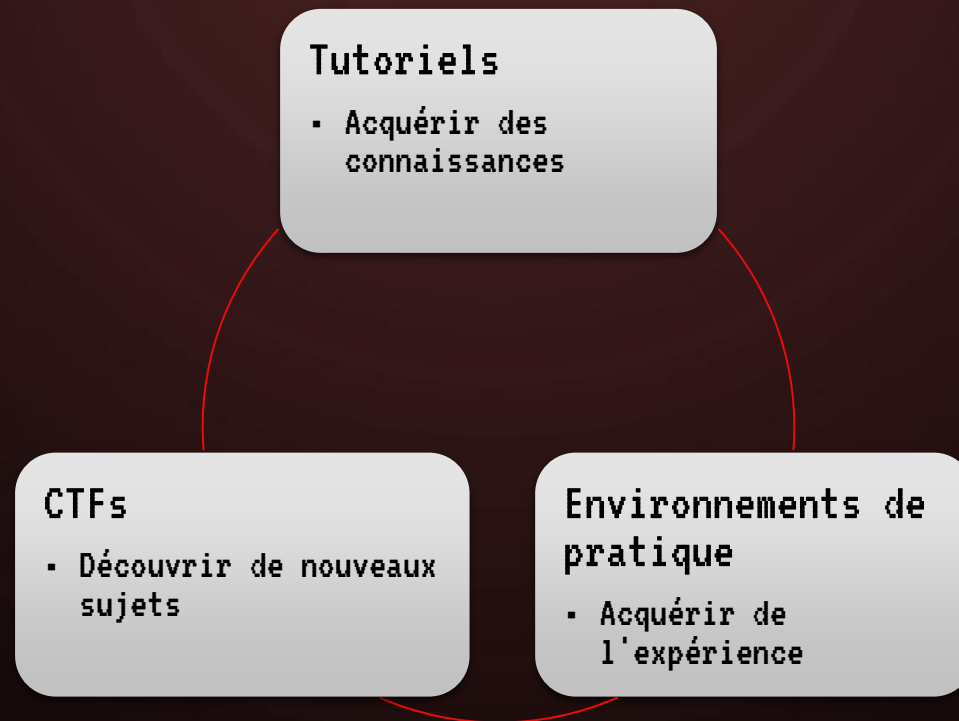
1. Installer VMware Workstation Player ou VirtualBox
  - VMware : <https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>
  - VirtualBox : <https://www.virtualbox.org/>
2. Télécharger Kali ou ParrotOS en fichier .iso
  - Kali : <https://www.kali.org/get-kali/>
  - ParrotOS : <https://parrotsec.org/>
3. Importer le fichier de machine virtuelle téléchargé dans VMware / VirtualBox



The background features a dark, reddish-brown gradient. In the center, there are several concentric circles of varying shades of red, creating a tunnel-like effect. The corners of the image are decorated with stylized, glowing red circuit lines and small circular nodes, resembling a digital or technological theme.

PRATIQUE

# TUTORIELS, ENVIRONNEMENTS DE PRATIQUE ET CTFs



# TUTORIELS

- Programmation :

- W3Schools : <https://www.w3schools.com/>

- Cybersécurité :

- HackTheBox Academy :

<https://academy.hackthebox.com/> recommandé pour  
débutants

- PortSwigger Web Security

Academy <https://portswigger.net/web-security>

## ENVIRONNEMENTS DE PRATIQUE

- Services clé-en-main
  - TryHackMe : <https://tryhackme.com/> recommandé pour débutants
  - HackTheBox : <https://www.hackthebox.com/>
- Laboratoire d'expérimentation à monter vous-même
  - Metasploitable : <https://www.rapid7.com/resources/test-metasploit-with-metasploitable/>
  - VulnHub : <https://www.vulnhub.com/>

## CTFs

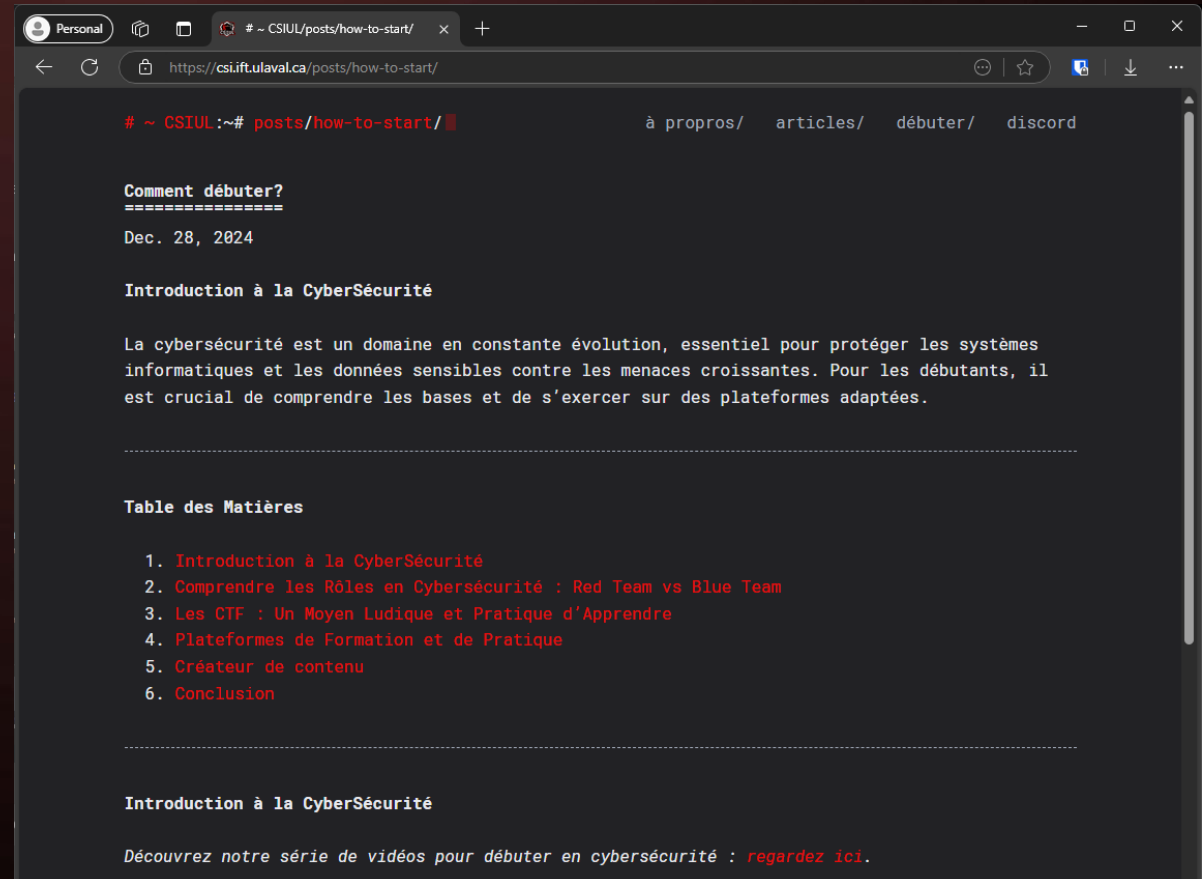
- PicoCTF : <https://play.picoctf.org/> recommandé pour débutants
- RingZeroCTF : <https://ringzer0ctf.com/challenges>
- CTFlearn : <https://ctflearn.com/>
- Hackfest Beginner CTF (Novembre) recommandé pour débutants
- UnitedCTF (Septembre) recommandé pour débutants

# SITE WEB DU CSI



<https://csi.ift.ulaval.ca/>

- Comment débiter
- Ressources
- Articles sur multiple domaine de la cybersécurité




CSIUL



- Tutoriels
  - Suite de formations d'initiation à la cybersécurité sur Youtube
  - Formations des années précédentes
  - Nouvelles formations à chaque session
  - Articles
- Rencontres
  - Plateforme d'apprentissage
  - Projet Lab Hacking
- CTFs
  - Participation aux CTFs
  - ULCTF 2025

# FORMATIONS

#  calendrier

Date	Heure	Nom
Mercredi 29 janvier	18h-19h	Introduction à la cybersécurité
Mercredi 12 février	18h-19h	Forensics
Mardi 11 mars	18h-19h	Analyse de malware

<https://www.youtube.com/@csiul>



# RENCONTRES

# 📅 calendrier

Date	Heure
Mercredi 5 février	18h-20h
Mercredi 19 février	18h-20h
Mercredi 5 mars	18h-20h
Mercredi 19 mars	18h-20h
Mercredi 26 mars	18h-20h
Mercredi 2 avril	18h-20h
Mercredi 9 avril	18h-20h
Mercredi 16 avril	18h-20h

- Plateforme apprentissage en ligne
    - TryHackMe
    - PicoCTF
    - HackTheBox
  - Collaboration et entraide
  - Socialiser
- 
- Projet lab hacking



# PROJET - LABORATOIRE DE HACKING



Attaque



Défense



Outils



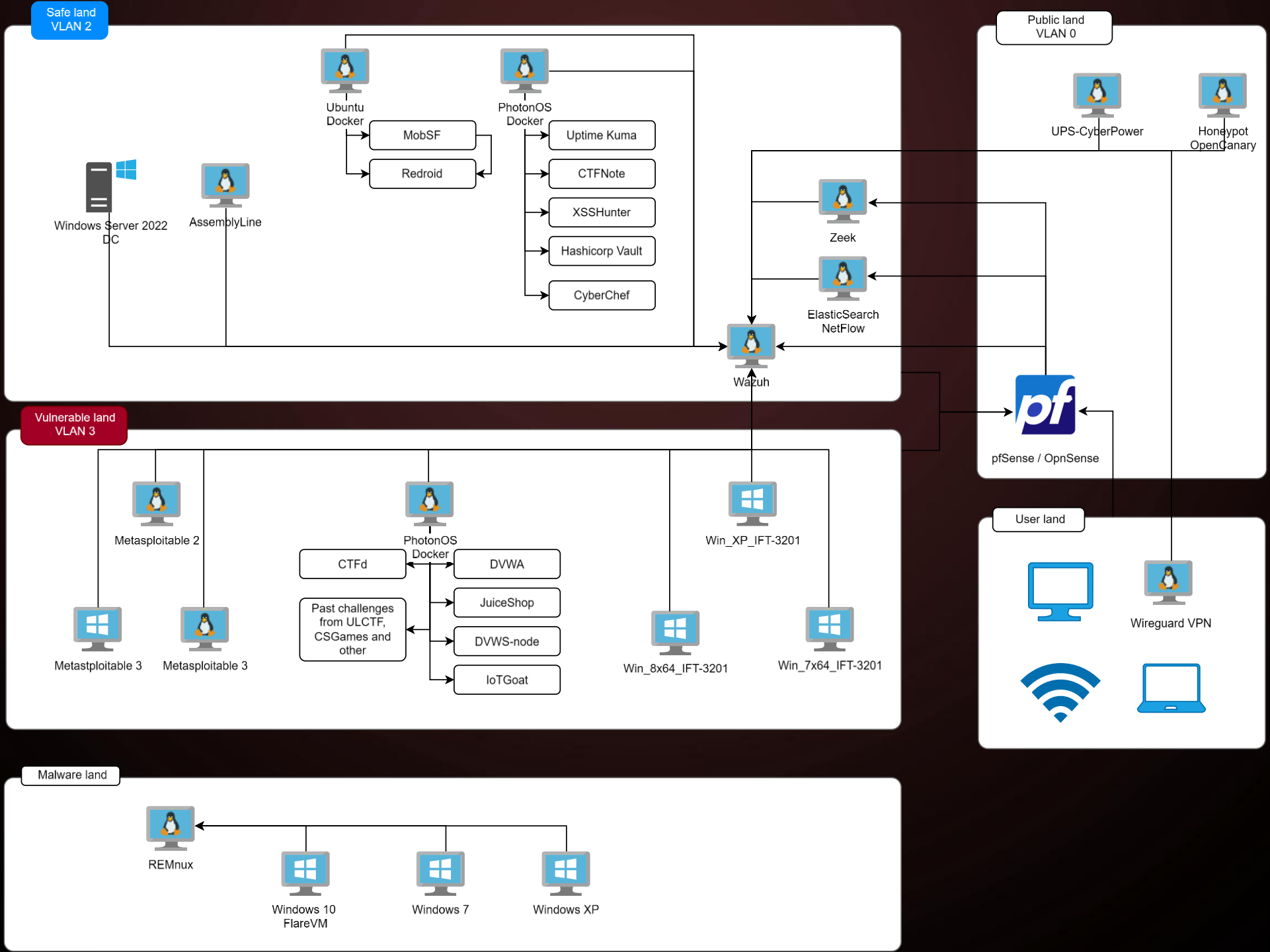
Malware

OBJECTIF : Créer un environnement qui permet l'attaque et la défense d'une infrastructure.

# SERVEUR

- Dell Precision T5610
- 2x Intel Xeon E5-2630 v2
- 64 GB RAM
- 2x 1TB SSD
- ESXi 7.0
- UPS CyberPower 1500VA

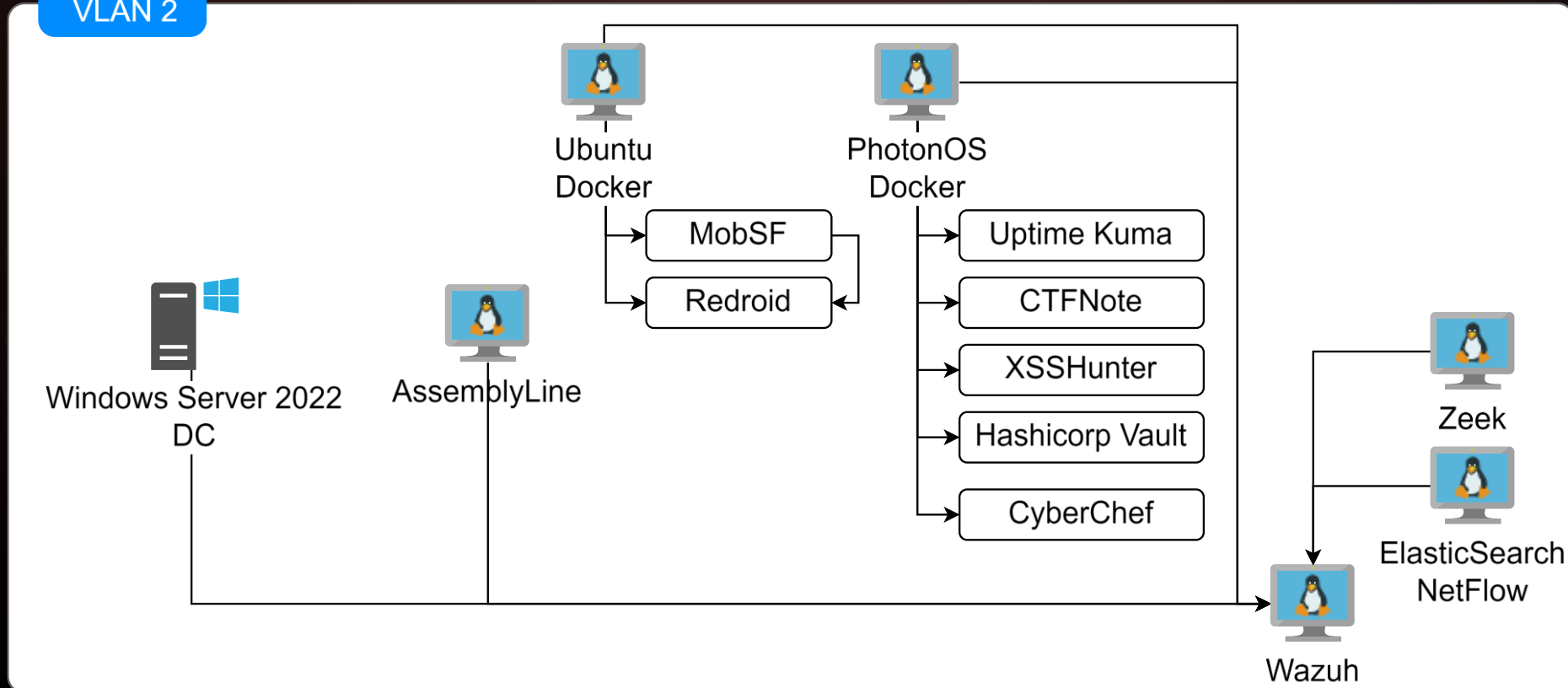




# SAFE LAND

- Outils
  - Sandbox malware
  - Reversing Android
  - Notes
- Surveillance Blue Team
- Gestion des comptes et des accès
- Surveillance de l'infrastructure

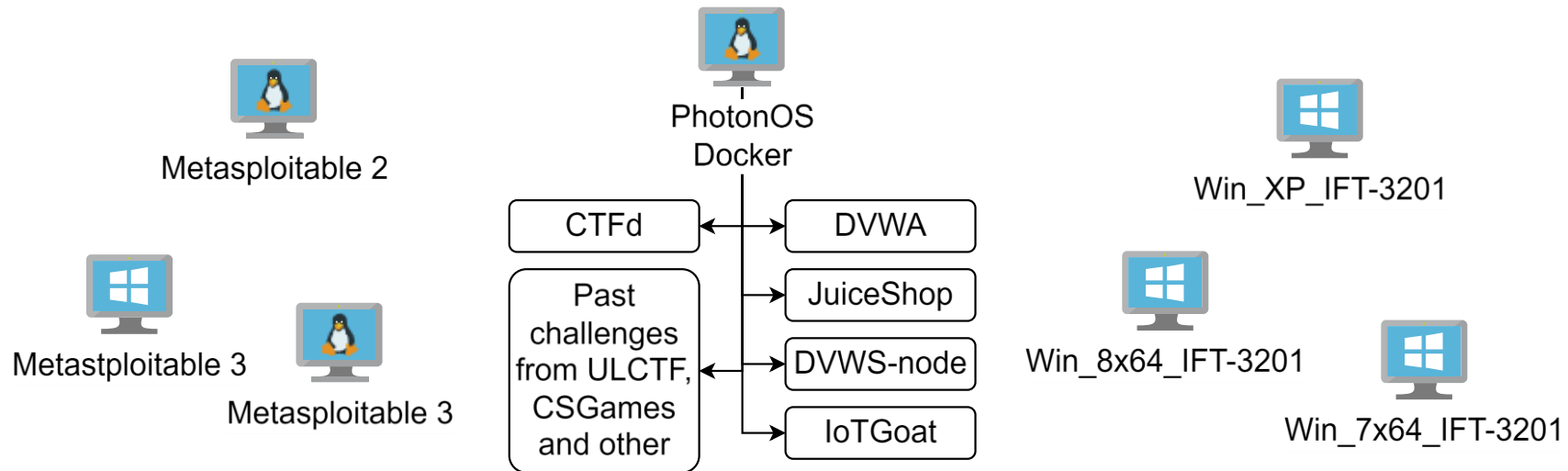
Safe land  
VLAN 2



# VULNERABLE LAND

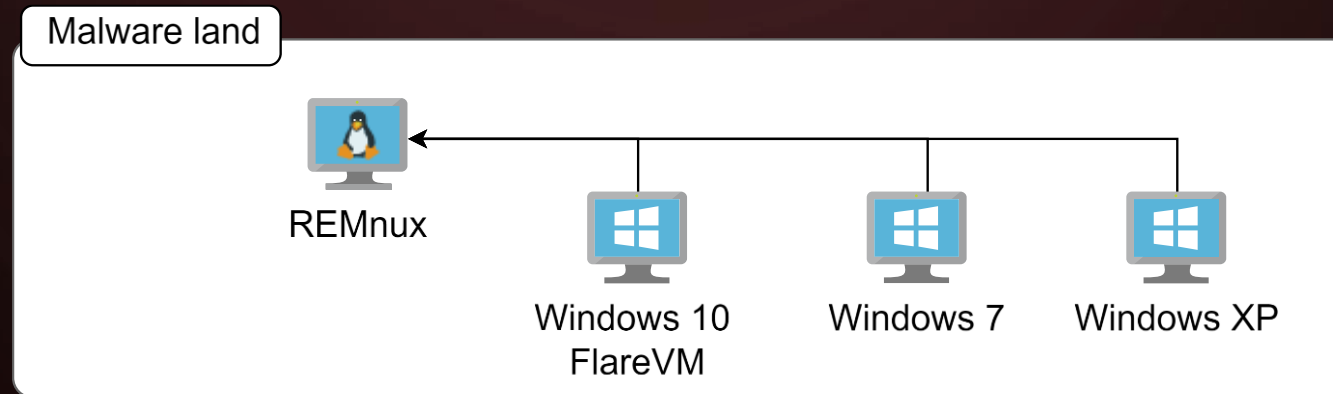
- Machines et conteneurs vulnérable
- Défis de compétitions passées
- CTF interne ULaval

## Vulnerable land VLAN 3



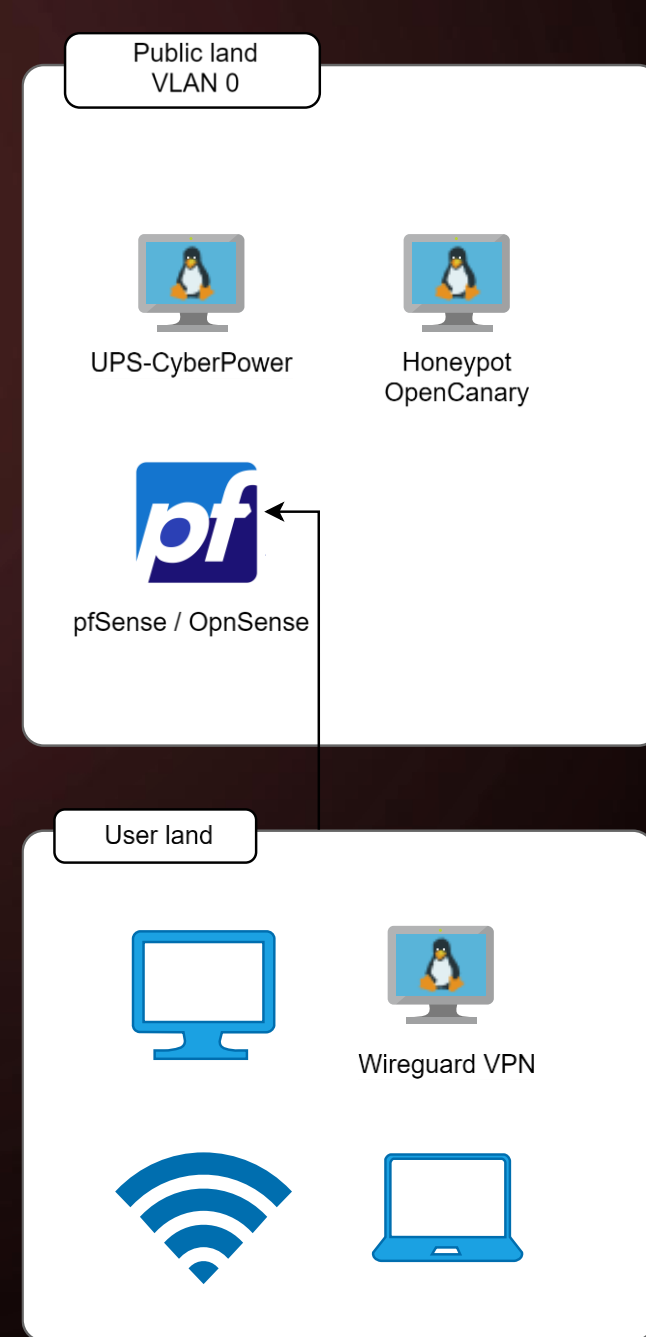
# MALWARE LAND

- Déploiement de virus
- **Environnement isolé**
- Snapshots



# PUBLIC LAND / USER LAND

- Accès VPN
- Point d'accès Wi-Fi (si possible)
- Pot de miel (HoneyPot)
- Routeur (point d'entrée unique)
  - Surveillance Blue Team





# ULCTF 2025

- Compétition organisée par les étudiants de l'université
- Accessible aux débutants
- Prix à gagner !
- Si vous êtes intéressé(e) par la création de défis, contactez @paradise14



Rejoignez le discord du  
ULCTF pour plus  
d'informations

CSIUL

<https://csi.ift.ulaval.ca>

