FRED TEP

- OSCP certified Hack3r -

22 rue du camp de César - 24660 Chamiers
06 79 55 23 42 | fr3sh@fredtep.com
- https://fredtep.com -

WINDOWS - LINUX

Enumeration | Privilege escalation

ACTIVE DIRECTORY

LLMNR/NBT-NS Poisoning | Password Spraying | DCSync | Enumeration | Domain Trust | Kerberoasting | ACL Abuse

WEB / BUG BOUNTY

BurpSuite | SQL Injection | Command injection | JWT | File Upload | Server Side (SSRF, SSTI) | Login brute force | LFI | API | Broken auth | Session security | And More...

NETWORK

Enumeration | Traffic Analysis | VPN | WIFI | ManInTheMiddle

COOL ATTACK AND STUFF

Lock Picking | Wireless keyboard and mouse injection | Docker | Python Addict | Rasperry Pi dependent

Mon premier Hack

En CM2 j'ai écopé, avec toute la classe, d'une punition collective. Il fallait écrire 50 fois "je ne ferais plus blablabla". J'ai donc écrit mon premier code (qui ne faisait n'y avait que 3 lignes) sur un CPC 464 et j'ai envoyé le tout sur l'imprimante à aiguille.

Ou comment je suis devenu hacker

Après avoir installé quelques serveurs web pour héberger des sites Internet, je me suis vite retrouvé confronté au piratage informatique.

J'ai d'abord voulu comprendre comment les pirates s'y prenaient et je me suis pris au jeu. J'ai donc décidé de me spécialiser dans la sécurité informatique et plus précisément les tests d'intrusion.

ÉDUCATION & EXPÉRIENCE

- **1977** — NAISSANCE
- **1995** — BAC S
- **2001** — MAITRISE CHIMIE — Stage en Floride
- **2002** — DEA CHIMIE
- **2003-2006** — THÈSE — Loughborough UK
- **2007-NOW** — DÉVELOPPEUR & HACKER FREELANCE

CENTRES D'INTÉRÊT

lecture | cuisine | skate | champigon

LANGUES

Français [langue maternelle]
Anglais [bilingue]
Espagnol [intermédiaire]

TALKS

2022-11-25 > **Hack-it-n** [Bordeaux]
What hacker's tools for blue teamers

2022 décembre > **ATD24** [Dordogne]
Retex Red Teaming

2023-01-27 > **Campus Cyber** [Bordeaux]
Hacking with bloodhound

CERTIFICATION & TRAINING

Offensive security OSCP

Hack The Box Profile

CAPTURE THE FLAG & COMMITMENTS

28e/1000 au DGhAck 2022
34e au BreizhCTF 2023 avec les D4r0ns
1er au StarTrekDay CTF 2023
14e/1500 au DGhAck 2023

Membre du Campus-CyberNA - GT Cartographie

MÉTHODOLOGIE

L'objectif du test d'intrusion est de fournir une évaluation précise de la sécurité du système et des recommandations pour corriger les failles de sécurité. Dans ma pratique, j'oscille entre le red teaming et le pentest classique. Le but étant de trouver les failles les plus critiques en un minimum de temps afin d'élever le niveau de sécurité de l'infrastructure le plus rapidement possible.

LATEST HACK

Entreprise /// Audit externe et interne [Une trentaine de poste - 3 serveurs windows - 2 NAS]

Résultat de l'audit externe :
- Un wifi dont j'ai pu récupérer le mot de passe
- Un accès à un NAS depuis Internet - Bruteforced
- Un accès à un routeur qui utilisait le même mot de passe que le NAS

Résultat de l'audit interne :
- Les mots de passe utilisateurs ont tous été découverts (responder + brute force)
- Accès au poste de la direction via un RDP non sécurisé par un VPN
- Réseau non scindé

STARTUP /// Web App

Exploitation d'une mauvaise configuration de JSON Web Token (JWT) me permettant de rentrer dans le backoffice de l'application

EHPAD /// Audit externe [Point d'accès VPN - Site Internet - Serveur de mail]

L'audit a permis de découvrir une interface d'administration à un router ainsi qu'un serveur windows qui n'aurait pas dû être accessible depuis Internet.
Le wordpress n'était pas à jour mais ne présentait pas de faille majeure
Mauvaise configuration des DNS pouvait être exploité via la compromission d'un serveur tiers.

PME /// Web API on NodeJS

Exploitation d'une injection NoSQL me permettant de récupérer tous les hash des mots de passe