contact@yann.cam

+33 6 XX XX XX XX (email first)

RENNES, FRANCE, *Remote*

https://yann.cam

Yann CAM (ycam)

ETHICAL HACKER / CYBERSECURITY CONSULTANT

AUDITEUR / PENTESTER / FORMATEUR

« *Passionné par la **CyberSécurité** et m'exerçant dans ce domaine depuis le début des années 2000 avec **plus de 15 ans** d'expériences professionnelles, j'interviens à présent en tant que **Hacker Ethique** au sein de **BZHunt**, ainsi que **consultant, formateur et auditeur** des systèmes d'information. Ces expériences m'ont permis de contribuer à la sécurisation de **plusieurs centaines d'entreprises** au travers de prestations d'**audits** ou de **Bug Bounty**, ainsi que de dispenser des **formations** auprès d'étudiants (écoles d'ingénieurs / collaborateurs d'entreprises).* »

EXPERIENCES PROFESSIONNELLES

HACKER ETHIQUE / INGENIEUR CYBERSECURITE (A TEMPS PARTIEL) — 2024+

BZHUNT – BREST/RENNES, FRANCE, *Remote*

BZHunt est la **1ère entreprise française à participer à des compétitions de BugBounty (LHE)**, où ses hackers éthiques ont fait de leur passion, un métier !

- **Hacker Ethique / Auditeur Cybersécurité** : réalisation d'audits offensifs de tests d'intrusion (TI) / Red Team (LAN/WAN, boîte-noire/grise/blanche) pour des cibles web, mobiles, clients-lourds, LAN/DMZ/Wifi, écosystème Active Directory…
- **Bug Hunter :** *Live Hacking Event* (LHE) et chasseur de vulnérabilités (Bug Bounty).

CONSULTANT CYBERSECURITE INDEPENDANT (A TEMPS PARTIEL) — 2018+

RENNES, FRANCE, *Remote*

Avec une polyvalence dans les domaines de la Cybersécurité, j'exerce également en tant que **Consultant Auditeur et Formateur Indépendant**.

- **Auditeur Cybersécurité :** Réalisation d'audits offensifs de tests d'intrusion (interne/externe, boîte-noire/grise/blanche, OSINT) et de configuration pour des cibles web, mobiles, clients-lourds, LAN/DMZ/Wifi, Active Directory, TI industriels (OT/IT)…
- **Formateur Cybersécurité :** Déroulement de formations de sensibilisation ou d'expertise offensive accompagnées de travaux-pratiques sous la forme de challenges / CTFs.
- **Bug Hunter :** chasseur de vulnérabilités sur des plateformes de Bug Bounty.

CONSULTANT CYBERSECURITE SENIOR — 2012-2022

SYNETIS – RENNES, FRANCE

Leader des cabinets de conseil indépendants en Cybersécurité français, SYNETIS propose une offre de services à 360° sur les différents domaines de la sécurité des systèmes d'information : GRC, habilitations, Gestion des identités et des accès, SecOps, Audit (PASSI), SoC, CSIRT/CERT.

Consultant Sécurité Senior : Lead-Tech / Responsable d'Audit / Formateur (2019-2022)

- Orchestration, suivi et réalisation d'audits techniques de tests d'intrusion, d'architecture, de configuration, de code source, *RedTeam*, *phishing*, cryptanalyse. Formations.

Consultant Sécurité Confirmé : Pentester / Lead-Auditor / Analyste (2014-2019)

- Audits de sécurité interne/externe, web, mobiles, clients-lourds, codes-sources, LAN, DMZ, wifi, Active Directory, etc. et interventions *forensic* post-incidents.

Consultant Sécurité : Expert Technique / Architecte Sécurité (2012-2014)

- Expertise et intégration de solutions d'IAM, SSO, MFA, DLP, chiffrement centralisé, fédération, SIEM, conformité des habilitations, gestion de mots de passe, annuaires…

FORMATEUR / ENSEIGNANT VACATAIRE – SECURITE OFFENSIVE — 2016+

ÉCOLE POLYTECHNIQUE DE L'UNIVERSITE DE NANTES – FRANCE

Interventions ponctuelles et récurrentes de formations en Sécurité Offensive auprès d'**étudiants de 5ème année** (BAC+5) du cycle d'Ingénieur en Informatique. Déroulement de **Cours Magistraux**, animation de **Travaux Pratiques** sous forme de challenges / énigmes / CTF de sécurité.

FORMATIONS

2009-2012 - **Polytech'Nantes I Ingénieur**
Diplôme d'ingénieur en Systèmes Informatiques, Logiciels, Réseaux et Sécurité - École Polytechnique de l'Université de Nantes 44000

2007-2009 - **DUT Informatique**
Diplôme Universitaire de Technologie Informatique - Institut Universitaire de Technologie de Nantes 44000

CONTRIBUTIONS / HoF

Google, Microsoft, moz://a, FORTINET, ebay, ORACLE, NASA, CERN, Java, Synology, cisco, CERT-EU, Hack4Values, redhat

YANN CAM / HTTPS://YANN.CAM / CONTACT@YANN.CAM

PUBLICATIONS

MISC n°133 (2024)
JS *Hoisting* : exploiter des XSS « inexploitables »

MISC n°128 (2023)
Shuck Hash before trying to Crack it

MISC n°125 (2023)
DisseXSSion d'un *payload* générique

JavaScript for Hackers (2022)
Mention dans les crédits de l'ouvrage de Gareth Heyes

Interview Télégramme (2022)
Sécurité offensive Manipulateurs et sans reproches

Interview de ZDNet (2020)
Bug bounty, peut-on en vivre ?

Conférence Min2Rien (2018)
Adoptez l'authentification-forte !

Interview de la plateforme de Bug Bounty Yogosha (2018)

MISC n°98 (2018)
Web authN & Password reset / Tour d'horizon de l'authentification forte

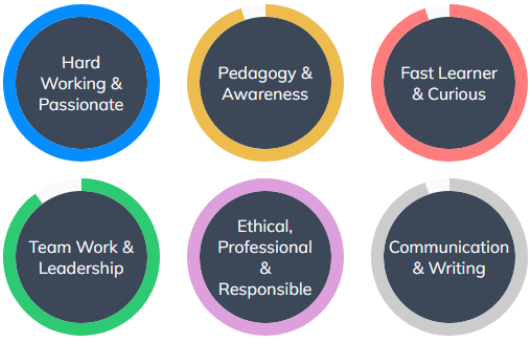
MISC n°94 (2017)
pfSense : obtention d'un reverse-shell root via une XSS

MISC n°89 (2017)
UnSHc : déchiffrer des scripts Shell protégés par SHc

GSMag n°34 (2016)
DarkWeb : Techniques d'anti-indexation et de camouflage

The Browser Hacker's Handbook (2015)
Citations de travaux personnels dans l'ouvrage

COMPÉTENCES PROFESSIONNELLES



CyberSecurity :

- Séduit par le modèle des Bug Bounty, tout en réalisant des missions de tests d'intrusion, *redteam*, *forensic*, sensibilisation (*phishing* / *USB-dropping* / formation), j'effectue une veille intensive (MSF, BeEF, Kali, fuff, Sulley, Nessus, Responder, Burp, Hashcat, BloodHound…).

Pedagogy & writing :

- Avec un fort attrait pour l'enseignement et le partage de connaissances, j'apporte une importance toute particulière à la qualité rédactionnelle des livrables, aux discours de restitution (managériale / technique) et à la vulgarisation / sensibilisation par l'illustration.

Hardening & configuration :

- Suivant une approche de durcissement de la sécurité constante, appuyée par des référentiels reconnus tels que le CIS / ANSSI, j'effectue des audits de configuration pour une multitude de technologies (OS Windows/Linux, services web, SGBD, progiciels, VPN, *firewall*, Active Directory, etc.).

Development / Scripting :

- Bash, Powershell, Python, PHP, Ruby, Go, Java, C/C++… avec de très bonnes bases dans de nombreux langages, je m'adapte de manière polyvalente aux divers développements pour la réalisation d'audits de codes sources et la recherche de vulnérabilités.

Identity & Access Management :

- Mes expériences m'ont amené à déployer, manipuler, comparer et auditer des solutions logicielles de sécurité telles que PingIdentity, ForgeRock, Apereo, PWM, Prim'X, Brainwave, LDAP, Symantec, ILEX, OIM, Wallix, O365, GSuite, etc. me permettant d'apporter conseils aux clients.

Advisories & CVEs :

Développement d'exploits, PoC, d'outils, d'articles et analyses de vulnérabilités :

- Jirafeau one-click-filesharing PHP project Stored-XSS (CVE-2024-12326, CVE-2025-7066)
- Stormshield Network Security firewalls Stored-XSS (CVE-2024-31946)
- pfSense 2.0.1 then 2.3.2 Remote root Command Execution (RCE)
- IPFire < 2.19 Update Core 101 XSS to CSRF to Remote Command Execution (RCE)
- IPCop 2.1.5 XSS and RCE (CVE-2013-7417, CVE-2013-7418)
- Smoothwall Express 3.1 (CVE-2014-9429, CVE-2014-9430, CVE-2014-9431)
- ZeroShell <=2.0.RC2 Local File Disclosure to Remote Command Execution (RCE)
- m0n0wall 1.33 CSRF to Remote root Command Execution (RCE)

Activités extra-professionnelles :

- Participation active sur les plateformes de Bug Bounty (YogoSha, YesWeHack, BugCrowd), d'évènements LHE/CTF/Wargame et de challenges (root-me : ycam).
- Arts du Cirque : jonglage (massues, balles, anneaux), bolas, monocycle…