Raphaël FRISCH
112 rue de Richelieu, Paris 75002
06 21 24 05 98
rfrisch@ethicalhackers.fr

Pentester indépendant

Parcours professionnel

Août 2020 – Aujourd'hui

PENTESTER INDEPENDANT

Recherche de vulnérabilités

Recherche de vulnérabilités et de mécanismes utiles aux exploitations en environnement Windows.

Tests d'intrusion

Réalisation de tests d'intrusion et d'audits de sécurité techniques.

Novembre 2016 – Août 2020

MANAGER DU POLE TEST D'INTRUSION A SECURIVIEW

Développement de l'offre « intrusion »

Création des propositions commerciales d'intrusion et de divers documents à destination de l'équipe marketing. Participation aux appels avec les prospects en tant qu'expert technique ou ingénieur avant-vente.

Management du pôle intrusion

Formalisation des méthodologies d'audit, et implémentation technique de leur suivi via l'outil Serpico. Formation des nouveaux arrivants. Participation au recrutement : évaluation des CV, interview des candidats.

Septembre 2015 - Septembre 2020

PENTESTER A SECURIVIEW

Tests d'intrusion

Réalisation d'une centaine de tests d'intrusion. En modes boîte noire, grise, et blanche, ces tests ont été de type : test d'intrusion externe, interne, d'application Web et d'application mobile

Campagnes de phishing

Plusieurs dizaines de campagnes de phishing, avec ou sans exploitation. Concernant les campagnes avec exploitation, un outil interne a été créé pour générer des documents Word contenant des macros VBA obfusquées, et dotées de défenses contre le sandboxing.

Audits de code source

Plusieurs audits de code source sur des applications Web. Les langages concernés ont été : C# (ASP.NET MVC), PHP, Ruby, Node.js.

Industrialisation des méthodologies d'intrusion et de rédaction

Contributeur important à l'outil de rédaction de rapport « Serpico ». Participation au développement de divers outils internes, les principaux étant : un outil d'aide au bruteforce, un générateur de dropper VBA, un analyseur basique de code source, un module Burp visant à exporter au format Excel les paramètres rencontrés lors du test d'une application Web.

Septembre 2014 - Septembre 2015

CONSULTANT SECURITE A HARMONIE TECHNOLOGIE

Audits techniques

Contrôle de la gestion des flux pour Thales, selon les aspects fonctionnels et opérationnels. Réalisation d'un audit de sécurité, focalisé sur la gestion de l'authentification de 6 applications du top 80 Natixis (suivi des exigences PCI-DSS et ISO 27000 ayant trait à l'authentification).

Tests d'intrusion

Tests de pénétration du système d'information de divers clients (CACF, Agirc-Arrco, etc.). Ces tests d'intrusions ont principalement suivi une méthodologie boîte noire, et ont été de type : test d'intrusion externe, test d'intrusion interne, test d'intrusion d'application Web, et test d'intrusion d'application mobile

Compétences

Intrusion interne	Metasploit, Empire, Covenant, SilentTrinity, escalade de privilèges
Intrusion externe	Nmap, Recon-NG, techniques d'énumération, password spraying
Intrusion applicative	Burp, AuthMatrix, XSS, SQL, XXE, CSRF, SSRF, RFD
Phishing	SET, HTA, Demiguise, ConfuserEx, macros Office, GoPhish
Développement	Ruby, Python, VBA, C#, PowerShell, Bash, XSLT, Gitlab, Git
Anglais	Courant **(915 TOEIC)**

Formation

2017 *Obtention de la certification **OSCP** (Offensive Security Certified Professional)*

2014 *Diplôme d'**ingénieur** suite au cycle Master de l'**Efrei, Majeure Sécurité et Réseaux***

2009 *Baccalauréat **scientifique**, lycée Camille Saint-Saëns*