Nour El Houda Agrebi

Ingénieur Cybersécurité

En Master 2 Réseau

CONTACT
Mail: agrebinoor@gmail.com
Téléphone: +33 06 58 16 03 18
Linkedin: /in/agrebinoor/

PROFIL

Etudiante en Master 2 informatique à l'université Sorbonne mention Réseau. Je cherche un stage de fin d'études d'une durée de 6 mois à partir du 14 Février 2022. Intéressée principalement par le domaine de la sécurité des réseaux, je cherche à travailler sur des projets d'intégration des solutions Firewall, SIEM et Monitoring.

EDUCATION

Master 2 Mention Réseau (BAC+7)
Sorbonne Université – Paris / France
Septembre 2021
Septembre 2022

Diplôme d'Ingénieur en Télécommunications (BAC +5)
Ecole supérieure des communications de Tunis – Ariana / Tunisie
Option: Cybersécurité et défense
Septembre 2016
Septembre 2019

Diplôme de licence appliquée (BAC +3)
Institut Supérieur de l'Informatique de Tunis ISI – Ariana / Tunisie
Section : Réseaux et systèmes
Septembre 2013
Juin 2016

CERTIFICATIONS

Juin 2020 ICSI Certified Network Security Specialist
Mai 2020 Fortinet NSE1, NSE2 & NSE3

Décembre 2020 TCF SO : C1
2018 – 2019 CCNA CyberOps (Cisco)
2017 – 2018 CCNA Routing & Switching

2017 – 2018 TOEIC : 980/990
2016 – 2017 Qradar Security Intelligence Award

COMPÉTENCES

Compétences informatiques

- **Réseaux et Protocoles :** LAN, TCP/IP, IPv4, SSH, SSL/TLS, VLAN
- **Sécurité :** VPN ,IDS/IPS, Firewall, SIEM SOC, Pentest, Forensics, Réponse à Incident
- **Outils:** Elastic Stack, KALI, Metasploit, Nmap, Qradar, Splunk, Suricata, Tenable, Snort, Cisco Packet Tracer, MS Project, Wireshark.
- **Programmation:** C/C++, Python, Javascript

Compétences linguistiques

- **Arabe:** Langue Maternelle
- **Français :** Niveau Professionnel
- **Anglais:** Niveau Professionnel

EXPÉRIENCES PROFESSIONNELLES

Consultante Sécurité Informatique – Département Cybersécurité
SAMA PARTNERS– Tunis, Tunisie
Juin 2020
Juillet 2021

- Réalisation des tests d'intrusion (Pentest) externe et interne, web, infrastructure et des code reviews.
- Définition des besoins client et du périmètre d'audit conformément aux standards PTES/NIST.
- Rédaction des plans de remédiation des failles.
- Rédaction des Incident playbooks et Cyber incident response plans.
- Participation au déploiement du SIEM Qradar.

Projet Test d'intrusion Réalisation des tests d'intrusion applicatifs (architecture, code, configuration) pour les applications web de SAMA PARTNERS.

- Définition des besoins et du périmètre de test (blackbox, greybox ou whitebox)
- Collecte d'information et reconnaissance OSINT.
- Analyse statique et dynamique des vulnérabilités potentielles (selon la norme OWASP).
- Test des scénarios d'attaques sur les applications web en utilisant des outils d'attaques, de manière à imiter des tactiques, techniques et procédures réalistes.
- Rédaction des rapport contenant l'inventaire des vulnérabilités détectés, plan d'action et remédiations.
- Rédaction des documentations technique des attaques réalisés.

Environnement technique : KALI, Metasploit, Nikto, Nessus, Openvas, Nmap, droopescan, Burpsuite, ZAP OWASP.

<u>Projet Incident Response et Forensics:</u> Mise en place de service Incident Response & Forensics pour les clients de SAMA PARTNERS.

- Rédaction des guides pour les premiers répondant face au incidents cybersécurité.
- Création du plan de réponse aux incidents CSIRP (selon la norme NIST)
- Rédaction et spécification des prérequis fonctionnel et logistique pour la création du laboratoire Digital Forensics au sein de SAMA PARTNERS.
- Conception et Rédaction des Incident Playbooks (Malware, Ransomware, Phishing …)
- Rédactions des documents process nécessaires pour le service IR (SLA, Chain of custody …)

<u>Projet SOC Qradar</u>: Intégration des solutions d'évaluation des vulnerabilités, management des risques et Forensics avec Qradar SIEM Entreprise.

- Intégration et configuration des solutions externes avec Qradar SIEM.
- Priorisation des solutions d'évaluation des vulnérabilités selon les besoins
- Rédaction des documents techniques et guides d'utilisations.

Environnement technique : Qradar SIEM, Nessus, Openvas, Nmap, Rapid7, Qualys, IBM Vulnerability Manager

Stage de Fin d'Etudes d'ingénieur

Février 2019 - Aout 2019

Axians Eretel – Lyon, France

Construction de l'offre de RedTeam (Test d'intrusion offensive)

- Définition de la méthodologie de l'offre selon les normes ANSI/NIST o Définition et simulation des tactiques, des techniques et des procédures (TTP) d'attaque.
- Participation à la veille sur les nouveaux mécanismes d'attaque (zerodays).
- Documentation des killchains et des outils d'attaques et scan des vulnérabilités.
- Mission chez le client ville d'Annecy :
  - Définition de besoin et du périmètre de test.
  - Analyse des vulnérabilités et risque.
  - Reporting des résultats et proposition des remédiations.

Environnement technique : Kali, Metasploit, Openvas, Nmap, Scriptshell, PowerShell, Tenable.

Stage de fin d'études de licence appliquée

Février 2016 - Juin 2016

Orange – Tunis,Tunisie

Création d'une plateforme de pentest automatisée.

- Définition de la méthodologie du pentest
- Définition des besoin fonctionnels de plateforme.
- Développement de l'interface web contenant les différentes phases du pentest.
- Scripting des différentes taches de scan et exploitations
- Documentation

Environnement technique : Kali, Metasploit, Openvas, Nmap, Scriptshell, PHP, SQL, HTML

INTÉRÊTS

Peinture: J'ai un grand sens de créativité et un intérêt prononcé à la peinture qui m'a permis de monter mon propre projet de vente de mes créations.