

Mohamed Boulanouar

55 rue du Château d'eau
45120, Châlette-sur-Loing

☎ +33 6 59 75 83 49

✉ mohamed.boulanouar@mbrobot.fr

CONSULTANT EN CYBERSÉCURITÉ

Présentation

Mohamed est un ingénieur en sécurité informatique avec 9 ans d'expérience dans les équipes offensives et défensives. Depuis son plus jeune âge, il est très passionné par le hacking éthique et les technologies de l'information en général. Au début de sa carrière, il a travaillé comme ingénieur en sécurité informatique dans une importante entreprise d'énergie algérienne où il a appris à sécuriser les systèmes industriels SCADA, à surveiller le réseau via une solution SIEM et à répondre aux incidents. Il a ensuite amélioré ses compétences en travaillant comme pentester dans un célèbre fournisseur de services français où il a effectué de nombreux tests d'intrusion et Red Teaming au sein de diverses technologies. Il a ensuite travaillé comme consultant en cybersécurité en freelance pendant plus de 7 ans, où il a eu l'opportunité de travailler sur différents secteurs comme l'industrie, sociétés de services, bijouterie et marques de luxes, construction et bâtiments et Industrie militaire entre la France et la Suisse, pour effectuer des tests d'intrusion sur des systèmes embarqués, Analyse de sécurité Web, réponse aux incidents et forensics. En Juin 2021, il a fondé sa propre entreprise de Sécurité Informatique. Mohamed est membre de diverses communautés White Hat comme Root-Me et Hack The Box, où il peut augmenter ses compétences et obtenir des certifications en sécurité informatique.

Diplômes Universitaires

- Juillet 2014 **Master 2 en Informatique**, *Université d'Avignon et des Pays de Vaucluse*, Avignon, Spécialité Réseaux Informatique et Sécurité.
- Juin 2012 **Licence en Informatique**, *Université d'Avignon et des Pays de Vaucluse*, Avignon, Spécialité Réseaux Informatiques et Systèmes Mobiles.

Diplômes Informatiques Supplémentaires

- Mars 2022 **Certified Red Team Professional, CRTP**.
Active Directory ATTACK and DEFENSE
- May 2020 **Offensive Security Certified Expert, OSCE**.
Advanced Exploitation, Anti-Virus Evasion, Backdoored Files, Debugging, Egghunter, Exploit Development, Network Attacks, Advanced Web Attacks
- Mars 2020 **Splunk Core Certified User**.
Splunk 7.x Fundamentals Part 1 (eLearning)
- Septembre 2018 **Offensive Security Certified Professional, OSCP**.
Antivirus Exploitation, Buffer Overflow Exploits, Client Side Attacks Exploitation, Information Gathering, Kali Linux, Metasploit, Network Vulnerability, Scanning Password Attacks, Pivoting, Port Scanning, Privilege Escalation, Web Exploitation.
- Mai 2013 **Cisco Certified Network Associate Niveau 4, CCNA 4**.
Technologie WAN et Sécurité.
- Janvier 2013 **Cisco Certified Network Associate Niveau 3, CCNA3**.
Notions de base sur la commutation et le routage intermédiaire.
- Mai 2012 **Cisco Certified Network Associate Niveau 2, CCNA 2**.
- Notions de base sur les routeurs et le routage.
- Janvier 2012 **Cisco Certified Network Associate Niveau 1, CCNA 1**.
- Notions de base sur les réseaux.

Expériences et Stages

Juin 2021 **Président-Fondateur**, CYBERDYN/MBROBOT, PARIS.
en cours

Ingénieur SecOps. Client : Groupe Duval - Novembre 2023 à Mars 2024

- Build d'un SIEM basé sur SEKOIA
- Déploiement d'agents NetSkope
- Configuration des journalisations détaillées sur l'environnement Windows (WinEvent)
- Mise en place et déploiement de SYSLOG/RSYSLOG sur les environnement Linux/UNIX
- Mise en place d'une machine de puits de logs sur le Cloud Azure
- Déploiement des agents Velociraptor via GPO et via Cloud Itune (Azure)
- Réalisation d'une mission de Threat Hunting
- Analyse d'incidents niveau 3 en se basant sur les outils : Microsoft Defender Endpoints, SentinelOne et Sekoia
- Développement d'alerte de détection sur SEKOIA
- Reverse Engineering sur des malwares reçus via phishing

Pentest Automotive. Client : VALEO - Novembre 2023 à Février 2024

- Analyse de PCB, détection de GPIO
- Test de continuité pour détecter les ports UART ou JTAG
- Soudage et dessoudage sur PCB sur des petites composantes
- Connexion sur différents type de BUS série/parallèle
- Dump de mémoire flash qui utilise le protocole SPI
- Debuggage JTAG en utilisant OpenOCD
- Audit de code source C, C++ et Java Android
- Développement de script de fuzzing
- Reverse Engineering et Binary Exploitation x86/x64 et ARM
- Utilisation d'outils d'analyse du protocole CAN BUS
- Analyse de trame Bluetooth BLE

Gouvernance Sécurité SI. Clients :M1VH - Mai 2023 à Novembre 2023

- Pilotage d'un SOC managé, revue des analyses d'incidents critiques
- Suivi des alertes et corrections des faux positifs
- Planification de développement de nouveaux Uses Cases
- Revue des KPI hebdomadaire avec le SOC managé
- Suivi des SLA d'incidents traités par le SOC managé
- Pilotage de Test d'intrusion
- Réalisation des détections périodiques des vulnérabilités avec RAPID7
- Suivi de plan d'action de correction vulnérabilité
- Suivi de déploiement de solution de sécurité
- Audits d'architecture d'infrastructure et applicatif
- Suivi et validation de demandes d'ouverture de flux

Systèmes Embarqués - Client : ATOS-Avantix - Décembre 2022 à Avril 2023

- Conception et intégration de solutions technique respectant les recommandations de l'ANSSI
- Conception de solutions techniques en réponse des exigences du clients
- Développement d'applications de sécurité sur AOSP
- Intégration d'une solution VPN-IPSec le Noyau/Linux d'AOSP avec une architecture AARCH64/ARM
- Modification du framework AOSP
- Recherche de vulnérabilités ou backdoor sur le mobile utilisé
- Développement d'un noyau dédié à la gestion des périphériques utilisés
- Mise en place de serveurs VPN et firewall sur ESXi8

Offensif - Clients : Lulubuy, Lexfo, SG-Markets, Airliquid, OCD MGAS

- Test d'intrusion WEB
- Test d'intrusion REST API
- Test d'intrusion Mobile Android

- Test d'intrusion Infrastructures Windows
- Test d'intrusion Infrastructures Linux
- Test d'intrusion Active Directory
- Compagne de Phishing
- Missions Red Team

Défensif - Client : Technip Energies Octobre 2021 - Décembre 2022

- Gestion d'incidents de sécurité N2 et N3
- Analyse de malwares et de vulnérabilités
- Forensic et investigation
- Investigation Avancée avec Windows Defender
- Surveillance des emails/spams sur Office 365
- Filtrage des domaines indésirables sur le proxy ZScaler
- Automatisation de la gestion d'incidents avec Phantom SOAR
- Développement de playbook sur Phantom SOAR
- Détection et whitelisting des faux positifs
- Création de règles de détection sur Splunk
- Création de dashboards sur Splunk

Défensif - Client : Orange Cyberdéfense (Juin 2021 - Novembre 2022)

- Gestion d'incidents de sécurité N2 et N3
- Analyse de malwares et de vulnérabilités
- Revue de playbooks sur le SOAR Cotex
- Détection et whitelisting des faux positifs
- Création de règles de détection sur Splunk
- Création de dashboards sur Splunk
- Vérification journalière des dashboards Cortex et Splunk
- Nettoyage des alertes en backlog
- Responsable de comités techniques hebdomadaires
- Préparation des comités techniques avec les remontées de KPI
- Préparation des comités de pilotage mensuels
- Présentation des cas les plus pertinents et critiques (avec les détails technique) aux clients lors du comité opérationnel

Décembre 2020 Sécurité systèmes embarqués et mobiles, ATOS, PARIS (6 MOIS).

- Intégration les outils et solutions de sécurité sur les systèmes embarqués
- Intégration deux VPN simultanément (TLS et IPSec) dans différentes couches de l'environnement Android
- Sécurisation l'environnement du noyau Linux
- Reverse engineering sur environnement ARM/AARCH64
- Attaques hardware sur le SoC MediaTek
- Développement des programmes sur ARM TrustZone OS
- Développement de Trusted Applications sur Prove&Core OS en utilisant le langage C
- Analyse de code statique sécurisé sur des applications C
- Fuzzing des programmes binaires, développés en C sur des architectures ARM
- Exploitation de différentes vulnérabilités Overflow sur la Stack et sur la Heap
- Pentest sur les cartes RFID
- Audit de sécurité des infrastructures et architectures VoIP

Mars 2020 Analyste en Sécurité (SOC), SCRT, GENÈVE (6 MOIS).

- Mise en place d'un SIEM
- Mise en place d'une infrastructure SPLUNK
- Installation de WEC/WEF

- Déploiement de WinlogBeat, Sysmon et différentes applications SPLUNK
- Gestion d'incidents de sécurité (SOC)
- Mission purple et détection d'attaques en temps réels
- Étude de nouveaux usecases et intégration des règles SIGMA dans les alertes de SPLUNK

Mars 2019 **Analyste en Sécurité Web**, FREELANCER, GENÈVE (9 MOIS).

- Réponse aux incidents de sécurité sur le périmètre Digital
- Gestion d'incidents de sécurité (Failles WEB, Phishing, DOS)
- Investigation/forensic en utilisant Kibana
- Coordination et pilotage des audits de pentest
- Revue et correction des rapports de pentest, confirmation des vulnérabilités reportées
- Conseils et expertises dans plusieurs projets de développement de plate-forme e-commerce
- Gestion des solutions PKI (Symantec PKI, Digicert PKI et Richemont PKI)
- Gestion des demandes de certificats SSL
- Automatisation du processus de génération de certificat
- Automatisation de la gestion des tickets Jira
- Automatisation du processus d'audit de code source
- Gestion de la solution Checkmarx
- Intégration de Checkmarx avec l'ADFS et l'utilisation de l'authentification SAML
- Développement de scripts (Groovy) qui relie Checkmarx et Bitbucket afin de lancer les scans de code ressource à chaque PULL Request
- Audits de code source sur les sites d'e-commerce (PHP, Java EE, Javascript)
- Test d'intrusion et scan de vulnérabilité sur des site web e-commerce
- Accompagnement des développeurs à corriger les vulnérabilités
- Formation et sensibilisation des développeurs aux attaques WEB (OWASP)
- Développement de scripts python pour la gestion automatiques des incidents, en se basant sur les API de Jira
- Développement de scripts python pour la gestions des projets dans Sonarqube
- Développement de différents jobs Jenkins en langage Java/Groovy
- Gestion et validation des demandes VPN IPSec et SSL en respectant le politique de sécurité Richemont.
- Maintenance des accès VPN SSL et troubleshooting des problèmes liés au VPN IPSec

Décembre 2017 **Consultant en Cybersécurité**, FREELANCER, PARIS (1 ANS ET 3 MOIS).

- Mise en place de nouvelles procédures pour la gestion d'incidents
- Rédaction de rapport d'analyse d'incidents avec préconisation d'amélioration de procédures
- Présentation des actions des méthodes suivies lors de la réponse d'incidents
- Élaboration de processus d'industrialisation de tests d'intrusion
- Audit de sécurité applicatif (.NET, C, PHP, Oracle), Méthodologies : OWASP
- Audit de sécurité infrastructure (Active Directory, Compromission de serveurs, MITM, mouvement latéral, pivoting)
- Élaboration de modèle de rapports de tests d'intrusion
- Participation aux missions RED TEAMING
- Conception et élaboration d'attaques via le vecteur d'ingénierie sociale, OSINT, PHISHING, Phone Freaking, clé USB vérolée
- Conception d'un C2 en langage Python pour contourner les nouvelles protections d'antivirus
- Recherche d'information impactant le business de l'entreprise (Fiches de paies, documents de projets confidentiels)

Novembre 2016 **Ingénieur en sécurité SI, Pentesteur**, SFR, MARSEILLE (1 AN).

- Réalisation d'audits de sécurité suivant différentes méthodologies : PTES STANDARD, OWASP

- Étude des normes PASSI
- Réalisation de tests d'intrusion de tout type : boîte noire, boîte blanche, boîte grise.
- Test d'intrusion WEB (SQL injection, LFI, RFI, Attaques d'authentification , XSS, CSRF)
- Test d'intrusion VOIP (Déni service, interception, usurpation d'identité)
- Test d'intrusion sur Active Directory (Compromission de serveur, vol de session, mouvement latéral, pivoting)
- Test d'intrusion sur poste de travail sur Windows 10 (Injection de backdoor, Robber Ducky, Dump mémoire, dump mots de passes, élévation de privilèges)

Avril 2015 **Ingénieur Sécurité Réseaux et Systèmes**, ELIT, Sonelgaz, ALGER (1 AN ET 6 MOIS).

- Mise en place d'un système de routage statique et dynamique.
- Configuration de plusieurs services : HTTP/S, PHP, DNS, Mail (SMTP, IMAP, POP), FTP/S, SSH, VPN, BackUp, Impression, Samba (CIFS, NTFS), Gestionnaire de quota.
- Recherche de différentes vulnérabilités dans les applications Web réalisées par les filiales du groupe de SONELGAZ.
- Recherche de différentes vulnérabilités dans les serveurs mis en service.
- Gestion de la plate-forme réseau informatique du groupe SONELGAZ en exploitant les différents équipements de supervisions et de sécurité (PRTG, E-mail gateway, SIEM).
- Test des performances et de la robustesse de l'antivirus Endpoint Protection mis en place.
- Étude et compréhension des systèmes S.C.A.D.A avec leurs différents domaines d'application.
- Étude des protocoles spécifiques au S.C.A.D.A appliqué aux systèmes électriques.
- Conception et réalisation d'un prototype de communication entre les postes de surveillance et le réseaux électrique avec une IHM simplifiée.
- Développement en C++ et en Java
- Etude du protocole IEC-62-443 qui est la référence de la sécurisation des systèmes S.C.A.D.A
- Installation et administration de serveurs et clients SVN
- Gestion des commits et conflits de code source
- Gestions des incidents via la plate-forme HelpDesk
- Rédaction de rapports détaillés des vulnérabilités détectées et les correctifs à appliquer
- Gestion des cas d'exceptions des restrictions des droits d'accès Proxy et Active Directory

Février 2014 **Ingénieur Chercheur**, LABORATOIRE INFORMATIQUE D'AVIGNON, AVIGNON (6 MOIS).

- Recherche de nouvelles méthodes pour optimiser l'allocation des ressources réseaux mobiles. (5G)
- Application de la Théorie des Jeux dans le domaine de la Téléphonie Mobile.
- Recherche de nouvelles méthodes d'allocation de ressources pour utiliser le spectre de manière optimale
- Adaptations et applications des récentes techniques d'utilisation de spectre, comme le scheduling en utilisant les algorithmes comme R.B (Round Robin) ou R.A (l'allocation aléatoire).
- Conception d'un système autonome avec une consommation d'énergie optimale.(Architecture CRAN)
- Développement de solutions mathématiques sous MATLAB

Compétences Techniques

Attaques Active Directory	Active Directory Enumeration, Local Privilege Escalation, Domain Privilege Escalation using Kerberoast, Kerberos delegation, Abusing protected groups, abusing enterprise applications, Domain Persistence and Dominance using Golden and Silver ticket, Skeleton key, DSRM abuse, AdminSDHolder, DCSync, ACLs abuse, host security descriptors, Forest privilege escalation using cross trust attacks, Inter-forest trust attacks
Attaques Réseaux	Arp poisoning, DHCP spoofing, IP spoofing, DNS spoofing, Scanne Zombie, Scanne over firewall, Packets sniffing, DOS/DDOS

Attaques Web	LFI, RFI, File upload, SQL injection, LDAP injection, Directory transversal, fichiers de sauvegardes, XSS, CSRF, javascript obfuscation
Attaques Système	Privileges escalations, SUID programme, Remote code execution, Malware obfuscation, Malware encoding, Packers
Outils de Sécurité	HTTrack, Google dork, The Harvester, Nmap, Nessus, Nexus, Metasploit, Veil-Evasion, Ettercap, Jhon The Ripper, Medusa, Hydra, WireShark, Macof, SET, Netcat, Cryptcat, NikTo, Sqlmap, Beef, Zed Attack Proxy, Burp, HackerDefender, Air-Crack, Reaver
Protocoles	Modèle OSI, TCP-IP, UDP, DNS, FTP, Telnet, SSH, SSL/TLS, NAT, PAT, SAMBA, SNMP, SMTP, DHCP, RIP, EIGRP, OSPF, IPSEC, VTP, STP, VPN, ARP, IPV4, IPV6, Ethernet, RS-232
Systèmes	Debian, Ubuntu, Kali Linux, Backtrack 5, IOS CISCO, Windows XP, Windows Server 2008, Window 7, Android
Langages Web	Avec concepts UML : JAVA, JAVA JEE, C++, C#, PL/SQL, SHELL, Python, MATLAB. HTML 5, CSS, PHP, javascript, Moodle

Langues

Français	Langue maternelle
Anglais	Très bonne maîtrise, oral et écrit