Ibrahim Sharul

OSCP+, BSCP, CRT, BTL1, CIPT
+65 8714 2535 | ibrahimramos4@outlook.com | linkedin.com/in/ibrahimsharul | ibrahimisramos.github.io

PROFILE

Cyber Security Consultant with 16+ months of offensive security experience (web, API, mobile, thick client pentesting) and an earlier foundation in SOC operations across two government security operations centres. Actively building hands-on digital forensics and malware analysis capability through self-directed projects and lab work, with a strong interest in transitioning into incident response.

WORK EXPERIENCE

Vantage Point Security — Cyber Security Consultant **Feb 2025 – Present**

- Delivered over 30 projects across web applications, mobile apps, and APIs for clients including major banks, identifying vulnerabilities such as IDORs, SSRF, CSRF, and authentication bypasses
- Performed mobile application security testing, including bypassing RASP and anti-tampering controls (Frida detection, SSL pinning) on iOS/Android banking applications — building practical understanding of attacker evasion techniques at the endpoint level
- Built a custom Burp Suite extension to decrypt 3DES/AES-GCM end-to-end encrypted traffic for a banking application assessment, and a custom JOSE fuzzing framework for a payment gateway engagement
- Independently discovered and responsibly disclosed a systemic IDOR vulnerability affecting all major resource controllers in an open-source CRM platform, filed via responsible disclosure
- Assisted in Red Team preparation, including OSINT gathering and phishing email crafting

Straits Interactive — Data Protection and Governance Intern **May 2022 – Aug 2022**

- Conducted market research on SaaS pricing models and presented findings to senior management to inform pricing strategy for a new SaaS product
- Devised Python automation scripts to generate CIS Benchmark templates, increasing efficiency by over 50%

Ministry of Home Affairs SOC — Cyber Analyst **Jan 2019 – Aug 2020**

- Led a team of Tier 1 Operators in monitoring, analysing, and responding to security events
- Devised scripts in JavaScript and VBA to automate daily SOC tasks, improving productivity by over 50%
- Organized and promoted MHA NSF activities, increasing participation rate from 11% to 77%

Cyber Security Agency of Singapore (CSA) — SOC Intern **Nov 2017 – Feb 2018**

- Improved daily SOC operations through Python automation, reducing time spent by 70% and increasing accuracy by 20%
- Trialled a new SIEM product to assess feasibility for SOC deployment and presented findings to management, informing the deployment decision
- Developed Python scripts to automate OSINT gathering, such as identifying blacklisted websites

RELEVANT PROJECTS

Malware Analysis — Static & Dynamic Analysis Exercise **University Project**

- Performed static and dynamic analysis on a live malware sample in an isolated lab environment, identifying file structure, behaviour, and network/registry activity

Digital Forensics — Disk, Memory & Artifact Analysis **University Project**

- Conducted disk, memory, and browser artifact forensics, including recovery of encrypted/hidden data

FlareVM Malware Analysis Lab **In Progress**

- Building a dedicated FlareVM lab environment to extend malware analysis practice, with reverse engineering as a planned next area of focus

TOOLS & TECHNOLOGIES

- Security Operations / SIEM: Splunk (BTL1)
- Malware Analysis: PEView, PEiD, VirusTotal, Sysinternals Suite (Process Hacker, Process Explorer), Regshot, ApateDNS
- Digital Forensics: Autopsy, The Sleuth Kit, Volatility Framework, ChromeHistoryViewer, MZHistoryView, TrueCrypt, Image Steganography
- Offensive Security: Burp Suite (incl. custom extension development), Frida, Objection, JADX
- Scripting & Automation: Python, JavaScript, VBA

- Cloud Security: AWS (IAM enumeration, EBS snapshot exploitation, CloudTrail analysis) — via Pwned Labs

EDUCATION

National University of Singapore (NUS) **Aug 2020 – May 2024**

Bachelor of Computing (Information Security) + Minor in Science, Technology and Society (STS) + University Scholars Programme (USP) / NUS College — CAP: 4.25/5.00

- IMDA SG Digital Scholar (Cyber Security)
- Facilitators@NUS Vice-President (External); NUS College Residential Assistant & Pastoral Care Committee; Peer Mentor Coordinator (Computing)
- Summer School at Autonomous University of Barcelona on "Data Protection Legislation and Ethics" (GDPR, EU AI Act); Student Exchange at Utrecht University

CERTIFICATIONS

- Offensive Security Certified Professional+ (OSCP+)
- Burp Suite Certified Professional (BSCP)
- CREST Registered Tester (CRT)
- Blue Team Level 1 (BTL1)
- Certified Information Privacy Technologist (CIPT)
- Amazon Cloud Red Team Professional (ACRTP), Pwned Labs — In Progress

ADDITIONAL INFORMATION

- Blue Team Labs Online (BTLO): Completed 25+ Blue Team Investigations
- Languages: English, Tamil, Malay, Hindi
- CliftonStrengths: Connectedness, Input, Communication, Strategic, Individualisation