Lam Tan Thong | Blue Team Intern

☎ (+84) 877 233 971 | ✉ thongtan967@gmail.com | bruning-frighting | kaiz3n0512 | Notes and Blogs

Personal Summary

Junior college student majoring in Information Security at Posts and Telecommunications Institute of Technology (PTIT), seeking an internship in **Incident Response Intern** . Gained hands-on experience in IR workflows such as memory and network forensics, C2 decryption, and post-exploitation analysis.

Active participant in Capture-the-Flag (CTF) competitions with placements in **Blue Team and DFIR challenges**. Interested in learning from senior analysts and contributing to monitoring, incident triage, and forensic investigations.

Education

Posts and Telecommunications Institute of Technology (PTIT)

Engineering Degree. in Information Security *2023–Present*

GPA: 3.16/4.0

Coursework: Computer Networks, System Administration, Databases, Operating Systems, Algorithms and Data Structures, Object-Oriented Programming.

Projects

More projects & write-ups: **bruning-frighting**

C2 Traffic Decryption: Analyzed and decrypted command-and-control (C2) traffic from **Covenant**, **InsteallerC2**.

Discord Backdoor (Go): Developed a proof-of-concept backdoor using Discord as a C2 channel with remote command execution, file transfer, and screen capture to demonstrate C2 communication and data exfiltration techniques.

H7tex CTF Challenge: Digital Forensics Contributor – H7CTF International 2025

Technical Skills

Digital Forensics & Incident Response (DFIR)

Experienced DFIR practitioner with hands-on expertise in disk, memory, and network forensics; artifact extraction, timeline reconstruction, and automation for incident response.

- **Forensic Imaging & Evidence Collection:** Autopsy, FTK Imager — evidence acquisition and preservation ensuring chain-of-custody.
- **NTFS & File Activity:** Analysis of $MFT, NTFS journal, file carving, deleted file recovery, and timeline creation.
- **Windows Artifacts & Registry:** Extraction and parsing of NTUSER.DAT, SOFTWARE, SYSTEM, SAM, EVTX, Prefetch, LNK, Amcache, Jump Lists, and SQLite databases using Eric Zimmerman's toolset (CSV/JSON export).
- **Memory Forensics:** Acquisition with DumpIt (Windows) and LiME (Linux); analysis with Volatility and MemProcFS — process enumeration, code injection detection, VAD/heap/environment analysis, and YARA scanning (memory/pagefile).
- **Live / Endpoint Monitoring:** Sysinternals Suite (ProcExp, ProcMon), Process Hacker, API monitoring for process, API, and network behavior analysis.
- **Log Analysis:** Windows .evtx parsing; Linux /var/log (auth.log, btmp/utmp, access.log, crontab) for persistence and authentication tracing.
- **Network Forensics:** Wireshark, tshark, and NetworkMiner — packet/PCAP analysis, DNS query investigation, ARP cache inspection, and detection of C2/exfiltration activities.

Malware Analysis & Development

Skilled in static and dynamic malware analysis with practical experience reproducing attack techniques for detection and mitigation.

- **Static & Dynamic Analysis:** IDA Free, PE-bear, AnyRun, VirusTotal — sandbox-based behavioral analysis and runtime tracing.
- **API / DLL / Injection Analysis:** API call tracing, DLL load/unload observation, process injection, and thread hijacking investigation using Microsoft API documentation.
- **Reverse Engineering & Development:** Perform code review and static analysis on C/C++, .NET, Go, and Java applications; create PoCs and detection tooling to validate findings and automate detection.
- **Runtime Monitoring & Instrumentation:** Instrumentation with ProcMon, API hooking, and network behavior monitoring for telemetry collection.

- **Scripting & Automation:** Python, PowerShell, Bash — development of parsers, forensic automation, and lightweight analysis utilities.
- **Detection Engineering:** Author YARA rules and signatures derived from forensic artifacts and reverse-engineering findings.

Awards & Achievements

Google Cybersecurity Certificate Graduate: Coursera – Google (Completed February 6, 2024). Hands-on experience in network security, incident response; applied foundational Python scripting and threat modeling in labs.

CTF Participant – Forensics & Malware Analysis: Team f4n_n3r0 (2024–Present). Practical experience in memory forensics, log analysis, PCAP analysis, and basic malware reverse engineering with IDA. Notable rankings include:

- Top 7 – **HackTheOn Sejong Finals 2025**
- Top 2 – **Hola CTF2025**
- Top 23 – **DEADFACE CTF 2024**
- Top 42 – **HTB Sherlock Holmes - Blue Team only CTF2025**
- Top 7 – Kashi CTF 2025
- Top 7 – ACECTF 2025
- Top 23 – H7CTF international 2024
- Top 9 – VishwaCTF 2025
- Top 8 – BlitzCTF 2025
- Top 3 – CapturePoint 5353 3.0 CTF2025

More results on CTFtime: f4n_n3r0.