Nguyen Van Hiep

Infomation Security Specialist

+84 973674820 hypnguyen1209@gmail.com https://www.linkedin.com/in/hypnguyen1209/ Thanh Xuan, Hanoi

OBJECTIVE

Capable of independently managing tasks and time effectively to achieve optimal results, while also adept at collaborating with teams when necessary. Proficient in both redteamming and penetration testing on diverse environments. Thrives on continual learning and deep-dive in vulnerable research. Guided by integrity, professionalism, and a collaborative spirit.

WORK EXPERIENCE

Military Commercial Joint Stock Bank 04/2023 - Present

Infomation Security Specialist

Pentesting / RedTeamming client/server assets, including internet-facing (both on-premises and cloud) infrastructures, web applications, software and source codes. Repoting to team leaders and management board:

- Familiar with commercial solutions: Metasploit, BurpSuite, Acunetix, IDA, Fiddler, Tenable Nessus, ...
- Deploying and customizing CVE and CNVD exploits.
- Fluent with VMware Vsphere and Jira for task performing and reporting.
- Target including exploiting servers, workstations, and containers.
- Golang/Dotnet/PHP/ASP/Java applications, API and business logic.
- Architectural consulting to ensure information security for a number of large infrastructure and service project boards.

Vulnerability Pentesting and RedTeamming:

- During Red Team engagements, vulnerable hosts within the client's ASN were identified. OSINT techniques were leveraged to obtain valid credentials for logging into systems and subsequently exploiting an ASPX web server. Defensive measures were circumvented to access a non-domain machine, employing lateral movement techniques to exploit MSSQL and gain control of domain-joined systems. Diverse methods were utilized to extract passwords and evade multiple EDR and AV (TrendMicro, Kaspersky, MS Defender) solutions.
- Research on AI or ML implementations can be used to develop automated malware, based on user behavior analysis to bypass intrusion detection (under research)
- Grey-box pentesting web application that handles real-time financial-related events using Java Spring Boot in k8s architecture. Using BurpSuite, Acunetix and Nessus to aid development team to migrate unrestricted file download and upload, SQL Injection, IDOR in customer eKYC, authentication bypass and bad design. Utilizing the customer's architecture to held 10x more concurrent users (upto 80k users/s).
- While reverse engineering an Dotnet/Java accountant software on Windows that have large enterprise userbase, found a critical vulnerable in its design leading to RCE as SYSTEM of the running server.
- During Red Team engagements, found an cloud contract management API was exposed to the Internet. One of its function was vulnerable to Local File Inclusion, which allows attackers to read files such as loaded DLLs on DotNet Linux application. Reverse engineering these DLLs using IDA revealed hard-coded keys and paths to config files. Examine these config files reveals contract signing and e-invoices private key, which could leads to potential financial loss and legal risk.
- Analysis some variety of Android malware written with Flutter, ReactNative, Kotlin and Java, using both statically and dynamically methods to study character of malware, its behavior and it's Command and Control server.

Security Mobile:

- Proficiency in tools: Jadx, Jeb, Frida,...
- Proficient in skills related to mobile hacking, hooking, tempering, rooting/jailbreaking, writing Frida scripts in custom hooking into native libraries.
- Participated in the role of consultant and developer of the enterprise's Mobile RASP solution, which has been used for apps of member companies in the group.
- Conduct assessment and POC of RASP solutions of service providers to ensure the safest banking app
- Incident response related to service failure and customer fraud on mobile apps
- Assess the security of the bank's EKYC/Onboarding service, thereby building appropriate checklists

Viettel Cyber Security 12/2021 - 04/2023

Cyber Security Engineer

- Gained a lot of knowledge through internship and training
- Analyzed 1-day vulnerabilities, wrote POC exploits
- Performed pentests for many service systems for large enterprises/banks in Vietnam and Japan

VNCS Global Solution Technology 04/2021 - 08/2021

Research And Development Engineer Internship

- Develop data analysis backend system with Apache Druid (incomplete).
- Develop some important features (frontend VueJS) of Security Information and Event Management (VSIEM).
- Contribute and brainstorm ideas for mechanisms to ensure the safety of the VSIEM.
- Deploy ticket system for SOC department (Rother Otobo).

EDUCATION

Academy of Cryptography Techniques - ACTVN 2019 - 2024

Information Security Engineering - GPA 2.8/4

Actively participate in the academy's movement activities related to the CTF competition, have achievements and awards from the academy
Github: https://github.com/hypnguyen1209

ACTIVITIES

KMA Cyber Security Club (KCSC) 2019 - Present

Advisor member

- Expert committee's member of KMA Cyber Security Club (KCSC)
- Author, advisor of KMACTF and KCSCCTF
- Self-developed WAF Rule-based system for CTF competitions, handle Nginx rules without using native Nginx library

Infomation Security PTIT Club (ISPCLUB) 2019 - Present

Member

- Training committee's member of Infomation Security PTIT Club (ISPCLUB)
- Author, advisor of PTITCTF and ISPCTF
- Deploy CTF training system and competitive programming

CERTIFICATIONS

Burp Suite Certified Practitioner	11/2022
Certified Mobile Pentester (CMPen-Android) with Merit	06/2024
Certified AI/ML Pentester (C-AI/MLPen)	05/2025
Certified Cybersecurity Educator Professional (CCEP)	12/2025
Certified Threat Hunting and Incident Response I (CTHIRI)	12/2025
Certified LLM Security Expert (CLLMSE)	07/2026
Certified Red Teamer (CRTeamer)	07/2026
HTB Certified Active Directory Pentesting Expert	09/2026

HONORS & AWARDS

First Prize - Finals round of Duy Tan University ISITDTU CTF 2022	12/2022

Third Prize - Quals round of Asean Student Contest on Infomation Security 2022 (ASCIS 2022)	10/2022
First Prize - Banking Information Technology Innovation and Improvement Competition	07/2024
Second Prize - Banking Information Technology Innovation and Improvement Competition	11/2024