Mohamed Elsherbini

Junior Cybersecurity Analyst

Egypt • +20 106 608 2635 • sh3rb1n1@gmail.com • LinkedIn • github.com/N4P1x • n4p1.me

SUMMARY

Cybersecurity student with practical experience in penetration testing, threat intelligence, malware analysis, and vulnerability assessment. Built Night-Watch, a threat intelligence platform tracking ransomware leak sites and dark web forums, and Malware-Hunter, an ML-based PE file classifier. Competes internationally with N!ghtM4re, ranked #4 in Egypt and #90 worldwide on CTFtime. Co-author of an IEEE-accepted paper on embedded cryptographic security. Holds the OPSWAT ICIP certification; trained through ITI, IBM, and EFE-Global.

SKILLS

Offensive Security: Penetration Testing · Vulnerability Assessment · Web Application Security · Wireless Security · OSINT · Reverse Engineering

Defensive Security: Log Analysis · IOC Analysis · Malware Static Analysis (PE Headers, Opcodes) · Threat Intelligence · Dark Web Monitoring · Incident Documentation · MITRE ATT&CK

Tools: Splunk (home lab) · Nmap · Metasploit · Nessus · Wireshark · Shodan · Burp Suite · Python · Docker · Linux

Networking: TCP/IP · DNS · HTTP/S · Firewalls · VPN · Wireless (802.11) · CompTIA Network+

WORK EXPERIENCE

CTF Competitor & Analyst 05/2026 – Present

N!ghtM4re CTF Team

- Compete in international CTFs covering OSINT, network forensics, web exploitation, reverse engineering, and cryptography.
- ICMTC 2026 (Hack The Box): 16th out of 87 teams, 19/20 challenges solved, 7,525 pts.
- Team ranked #4 in Egypt and #90 worldwide on CTFtime. Published 19 writeups across GPN, HTB, and SecLeaf.

Penetration Testing Intern 06/2025 – 08/2025

Information Technology Institute (ITI), Egypt

- Performed network and web application security assessments using Nmap, Metasploit, and Nessus.
- Wrote structured pentest reports covering findings, risk ratings, evidence, and remediation steps.

.NET Developer Intern 08/2024 – 07/2025

Digital Egypt Pioneers Initiative (DEPI), Egypt

- Built REST APIs and backend services; gained working knowledge of application architecture relevant to web security testing and log analysis.

Software Engineer Intern 07/2023 – 12/2023

alx_africa, Egypt

Software Engineer Intern 05/2022 – 09/2023

School 21, Kazan, Russia

SECURITY PROJECTS

Night-Watch · **Threat Intelligence Platform** github.com/N4P1x/Night-Watch

- Monitors ransomware leak sites, dark web forums, and hacker communities; extracts IOCs automatically and sends real-time alerts.
- Stack: FastAPI · React · Docker · PostgreSQL · MongoDB · Redis · Tor.

Malware-Hunter · **ML-Based Malware Classifier** github.com/N4P1x/Malware-Hunter

- Classifies PE files as malicious or benign using Random Forest on PE headers and opcodes. Cross-validates results against VirusTotal.
- Stack: Python · Flask · Scikit-learn.

YoRHa-Deauther · **Wireless Security Research Tool** github.com/N4P1x/YoRHa-Deauther

- ESP32-based tool for studying 802.11 Wi-Fi deauthentication attack vectors. Stack: C++ · ESP-IDF.

CTF Writeups · **19 challenges — GPN CTF, Hack The Box, SecLeaf** github.com/N4P1x/Writeups

- Full write-up for each challenge: tools used, methodology, and lessons learned.

EDUCATION

Delta University for Science and Technology 2023 – 2027

B.Sc. Cybersecurity — Faculty of Artificial Intelligence, Gamasa, Egypt

Kazan Federal University 2021 – 2023

Cybersecurity — Kazan, Russia (transferred to Delta University)

CERTIFICATIONS

OPSWAT ICIP Introduction to Critical Infrastructure Protection Jun 2026 – Jun 2027

CompTIA Network+ (N10-009) Udemy course + practice exams

CompTIA A+ Core 1 & 2 (220-1101 / 220-1102) Udemy course + practice exams

ITI Ethical Hacking · Network Security · Computer Network Fundamentals · Red Hat System Administration I · Python Programming · Cybersecurity for Beginners (35 hrs)

Other IBM Cybersecurity Fundamentals · EFE-Global SkillsBuild Cyber Security · HP Cybersecurity Awareness

RESEARCH & PUBLICATION

Cyber-FIE: A Software-Induced Memory Fault Injection Framework for Evaluating AES-256 Resilience on ESP32

Accepted at ITC Egypt 2026 — To be published in IEEE Xplore

- Developed a post-exploitation SIFI framework using C++ volatile pointer arithmetic to corrupt the AES-256 key schedule on an ESP32, bypassing memory protections.
- 3,560 hardware trials; 12.3% critical fault rate (95% CI: 11.2–13.4%). Built the ‘Shield’ countermeasure: 94.2% state restoration, 1.5% overhead.