MD MAHBUBUL BASHAR CHOUDHURY (NEHAL)

nehalclickz@gmail.com +1 (443) 909-6725 Windsor Mill , MD , 21244

linkedin.com/in/nehal-choudhury08 github.com/Nehal-Choudhury

SUMMARY

Cybersecurity enthusiast with practical experience in offensive security, ethical hacking, and vulnerability assessment through hands-on labs, CTF challenges, and web security testing. Proficient in reconnaissance, enumeration, vulnerability exploitation, and privilege escalation across Linux and web environments. Comfortable using industry-standard tools including Nmap, Gobuster, Dirb, and Burp Suite, with strong interest in red teaming, OSINT, and real-world security assessment workflows.

PROFESSIONAL EXPERIENCE

Cyber Security and Ethical Hacker Intern 09/2025 – 02/2026
Creative IT Institute Remote

- Performed hands-on security assessments on Linux and web targets through boot-to-root labs, web exploitation exercises, and CTF-based problem solving.
- Conducted reconnaissance and vulnerability discovery using Nmap, Gobuster, Dirb, and Burp Suite.
- Exploited vulnerabilities including SQL injection, XSS, arbitrary file write, authentication bypass, and broken access control in controlled environments.
- Practiced privilege escalation through kernel exploit analysis, SUID binary analysis, credential recovery, and reverse shell access.
- Produced technical writeups for lab exercises and 40+ PicoCTF challenges covering web security, forensics, cryptography, and debugging.

SKILLS

Offensive Security — Penetration Testing, Vulnerability Analysis, Exploitation Basics, Privilege Escalation

Recon & OSINT — OSINT, Footprinting, Reconnaissance, Network Scanning, Enumeration

Network Security — Packet Sniffing, Wireless Network Security, IDS/Firewall Evasion, Threat Analysis

Web Security — Web Application Security, SQL Injection, Session Hijacking

Other — Malware Analysis, Cryptography Basics, Security Scripting, CTF Problem Solving

PROJECTS

MATRIX-BREAKOUT: 2 MORPHEUS 02/2026
Boot-to-Root CTF Challenge

- Compromised a vulnerable CTF machine through full boot-to-root exploitation.
- Performed reconnaissance and enumeration using Nmap and Gobuster to identify exposed services and hidden directories.
- Exploited an arbitrary file write vulnerability via Burp Suite to upload a PHP reverse shell and gain initial access.
- Escalated privileges to root using the Dirty Pipe (CVE-2022-0847) kernel exploit on a vulnerable Debian system.

The Planet: Earth Complete Vulnerability Report 01/2026
Boot-to-Root Security Lab

- Performed a full boot-to-root compromise of a custom Linux machine through enumeration, credential recovery, and privilege escalation.
- Used Nmap and Dirb to identify exposed services, hidden directories, and administrative portals.
- Decrypted an XOR-encoded payload to recover admin credentials and gained initial access by injecting a Base64-encoded Netcat reverse shell.

- Escalated privileges by analyzing a custom SUID binary with ltrace and exploiting its file-based logic to recover the root password.

Project Juice-Shop 12/2025
Web Application Security Assessment
- Conducted a hands-on security assessment of the OWASP Juice Shop application and identified/exploited 25+ web vulnerabilities.
- Performed manual SQL Injection, XSS, and access control exploitation to bypass authentication and escalate privileges.
- Used Burp Suite to intercept and manipulate HTTP requests, enabling API abuse and unauthorized access to restricted functionality.
- Applied OSINT and metadata analysis to recover sensitive information and bypass security questions.

PicoCTF Challenge Writeup 11/2025
CTF / Cybersecurity Lab
- Solved and documented 40+ PicoCTF challenges across web security, digital forensics, cryptography, and debugging.
- Exploited vulnerabilities including SQL Injection (SQLi), SSTI, and client-side authentication bypass using manual testing techniques.
- Performed forensic analysis, metadata extraction, cipher decoding, and hash cracking using industry-standard security tools.

VAPT Report on Metasploitable2 09/2025
Network and Web Reconnaissance Module
- Conducted end-to-end vulnerability assessment and penetration testing on a simulated target using OWASP, NIST SP 800-115, and PTES methodologies.
- Performed reconnaissance, vulnerability scanning, and manual exploitation using Nmap, Metasploit, Maltego, WHOIS, and DNS enumeration.
- Identified critical vulnerabilities including RCE, privilege escalation, weak cryptographic configurations, and the vsFTPd 2.3.4 backdoor (CVE-2011-2523).
- Achieved root access and prepared a technical report with risk assessment and remediation recommendations.

EDUCATION

Associate of Arts and Sciences - AAS, Cyber Security (Transferred) 01/2026 – Present
Community College of Baltimore County Baltimore, md, USA

Bachelor of Science in Computer Science & Engineering (Incomplete) 2021 – 2025
North South University Dhaka, Bangladesh

Higher Secondary Certificate (HSC) 2018 – 2020
Bangladesh Navy School & College Dhaka, Bangladesh

Secondary School Certificate (SSC) 2016 – 2018
Monipur High School & College Dhaka, Bangladesh

CERTIFICATES

Certified Ethical Hacker (CEH) — Creative IT Institute

Google Cybersecurity — Google

Ethical Hacker — Cisco

LANGUAGES

Bengali — Native/Bilingual

English — Fluent

Hindi — Conversational

Urdu — Conversational