SEYHA MEAS

seyha3788@gmail.com
0713992905
Phnom Penh
github.com/seyha3788-collab

SUMMARY

Cybersecurity student specializing in network security, penetration testing fundamentals, and security monitoring. Hands-on experience building virtual lab environments and performing reconnaissance, vulnerability assessment, exploitation, and intrusion detection analysis.
Skilled in Linux systems, networking fundamentals, and security tools including Nmap, Metasploit Framework, Wireshark, Snort, and Suricata. Actively developing offensive and defensive cybersecurity skills through Hack The Box learning paths and personal lab environments.

EDUCATION

Passed Grade 12 National Exam - Cambodia
Bati High School
Graduated :2023
Bachelor of Network Cybersecurity
BELTI University, Toul Sleng Campus – Cambodia
2024 – Present (3th Year)

SECURITY PROJECT EXPERIENCE

Home Penetration Testing Lab (Kali Linux & Metasploitable)

- Built a realistic virtual penetration testing environment using Kali Linux and Metasploitable to simulate real-world attacks
- Successfully executed the full attack lifecycle: reconnaissance, enumeration, exploitation, and privilege escalation to gain root access on multiple vulnerable machines
- Demonstrated practical skills in using Nmap for scanning, Metasploit for exploitation, and Wireshark for traffic analysis
- Strengthened understanding of Linux vulnerabilities commonly exploited in enterprise environments

Intrusion Detection Lab (Snort IDS)

- Designed and deployed a functional Network Intrusion Detection System using Snort in a virtual environment
- Developed and implemented 10+ custom detection rules to identify suspicious network activity and common attack patterns
- Monitored live traffic and successfully detected simulated attacks through detailed alert analysis
- Gained practical experience in signature-based threat detection and security monitoring

Cybersecurity Notes Repository

- Created a well-organized cybersecurity knowledge base using Obsidian and GitHub, documenting lab walkthroughs and key concepts
- Covered important topics including SIEM, Active Directory, Enumeration, Privilege Escalation, and Incident Response
- GitHub: github.com/seyha3788-collab/Cyber-Security

Hack The Box – Cybersecurity Learning Path

- Actively completing structured learning path focusing on networking, enumeration, exploitation, and privilege escalation
- Applied Nmap for advanced service detection and Metasploit Framework for payload delivery and shell access

CERTIFICATIONS

- CCNA (Cisco Certified Network Associate) – Cisco, April 2026
- Penetration Testing Engineer Certificate – Alison, April 2026
- Ethical Hacking Certificate – Cisco Networking Academy, April 2026
- Introduction to Cybersecurity – Cisco Networking Academy, April 2026

TECHNICAL SKILLS

Cybersecurity & Tools

- Network Scanning & Enumeration (Nmap)
- Exploitation Frameworks (Metasploit)
- Intrusion Detection & Monitoring (Snort, Suricata)
- Vulnerability Assessment & Analysis
- Network Traffic Analysis (Wireshark)
- Linux Privilege Escalation

Operating Systems

- Linux (Kali Linux, Ubuntu)
- Windows

Networking

- TCP/IP, DNS, HTTP/HTTPS
- Network Traffic Analysis

Programming & Scripting

- Python (Basic)
- C++ (Basic)

Tools & Technologies

- VirtualBox
- Git & GitHub

LANGUAGE

- Khmer: Native
- English: English: Intermediate (Professional reading, writing, and technical documentation)