Achievements

- Completed 15+ cybersecurity labs simulating real-world attacks.
- Conducted Vulnerability Assessment & Penetration Testing (VAPT) on isolated lab systems, authored formal reports with risk ratings and remediation steps.
- Analyzed phishing emails & malware samples using Wireshark, VirusTotal, and Hybrid Analysis.

PROFESSIONAL ATTRIBUTES

- Analytical Thinking & Problem Solving
- Teamwork & Communication
- Self-Learning & Discipline
- Report Writing & Documentation

Languages

Khmer - Native

English – Intermediate (Read, write and Speaking)

NIN KANONG

IT Security Trainee | Ethical Hacking | Network Security

☎ 0978297806 | ✉ ninkanong200620@gmail.com | 🔗 linkedin.com/in/nin-kanong/
🔗 github.com/Nin-Kanong/pentest-writeups | 📍 Phnom Penh, Cambodia

Professional Summary

Motivated IT Security Trainee with hands-on experience in log analysis, vulnerability scanning, and network exploitation using Nessus, Wireshark, and Nmap. Skilled in documenting findings and automating tasks with Python. Passionate about identifying and mitigating cyber threats through offensive and defensive security practices. Eager to contribute to SBI Ly Hour Bank's security team by assisting with SIEM monitoring, log source integration, and vulnerability assessments.

Technical Skills

Security Tools: Metasploit, Burp Suite, Hydra, Wireshark, Nmap, Hydra, Nessus.
Monitoring & Defense: Learned theoretical concepts of Firewall configuration, IDS/IPS, and Log Analysis.
Log & SIEM Analysis: Learned theoretical concepts of SIEM, IDS/IPS, Log Analysis (Wireshark, Nmap).
Vulnerability Assessment: Scan VA, track new CVEs, patch management basics.
Programming: Python, Bash, C/C++, HTML/CSS (for web development and Testing).
Networking: TCP/IP, DNS, DHCP, VLANs, Wireshark Analysis, Firewall configuration (theoretical).
Concepts: MITRE ATT&CK, OWASP Top 10, Network Security, Post-Exploitation, Defense Evasion.
Operating Systems: Linux(Kali Linux, Ubuntu), Windows.

Experience & Labs

Network & Vulnerability Analysis: Performed reconnaissance and vulnerability scanning using Nmap, Nessus and Metasploit on isolated lab systems. Identified and documented critical flaws such as MS17-010 (EternalBlue).
Exploitation & Post-Exploitation Practice: Executed remote code execution exploits, deployed reverse shells over SMB, and practiced privilege escalation.
Traffic & Log Analysis: Captured and inspected network traffic using Wireshark to analyze protocols (TCP, SMB, SSH), detect anomalies, and understand attacker behavior.
Security Automation: Developed a Python script to automate SSH login attempts, demonstrating foundational scripting skills for security tasks.
Technical Documentation: Authored detailed lab reports covering methodology, findings, risk impact, and remediation.

Education

Bachelor of Network Engineering and Security

Norton University | Expected Graduation: 2027

Cybersecurity Certification Program

SalaCyber Academy

Certifications & Training

SalaCyber Network and Cybersecurity Foundation – SalaCyber | (December/22/2024)
SalaCyber IT Security Essential – SalaCyber | (June/08/2025)
SalaCyber Ethical Hacking Essential – SalaCyber | (October/16/2025)
Complete Ethical Hacking MasterClass – Udemy | (Augus/27/2025)