SAMIP POKHAREL

Offensive Security Specialist · Red Team Operator · OSCP · OSEP

Kathmandu, Nepal · sameepx2@gmail.com · samipp.com.np · github.com/maskop9 · linkedin.com/in/samip-pokharel

PROFESSIONAL SUMMARY

Offensive security specialist with 7+ years of experience across penetration testing, red team operations, exploit development, malware analysis, and adversary emulation. OSCP and OSEP certified, with hands-on experience delivering enterprise assessments, developing custom offensive tooling, and communicating complex attack paths to technical and executive stakeholders. Engagements span banking, fintech, healthcare, government, and corporate environments.

EXPERIENCE

Offensive Security Consultant | *StickmanCyber · Australia (Remote)* Jul 2024 – Present

- **Led full-scope web, network, and Active Directory penetration tests** for enterprise clients, covering scoping, threat modeling, exploitation, post-exploitation, reporting, and executive debriefs.
- **Designed and operated authorised red team infrastructure** including C2 servers, redirectors, payload delivery workflows, and phishing infrastructure for adversary emulation engagements.
- **Developed authorised red team tooling in C/C++ and C#/.NET** for endpoint-control validation, including syscall-based execution, ETW-aware tradecraft, PPID spoofing, and process injection techniques.
- **Executed end-to-end adversary emulation engagements** (initial access, lateral movement, privilege escalation, persistence) against APT-style scenarios to validate detection and response capabilities.
- **Authored technical and executive deliverables** and led client debriefs translating complex attack chains and risk impact for both engineering teams and C-suite stakeholders.

Security Analyst II | *Cotiviti · Kathmandu (Remote)* Aug 2021 – Jul 2024

- **Performed vulnerability assessments and Active Directory security reviews** across enterprise environments, identifying critical misconfigurations, kerberoasting paths, and exploitable trust relationships.
- **Conducted secure code review** and triaged Veracode SAST findings, validating exploitability and prioritizing remediation work for development teams.
- **Drove purple team exercises** against SOC detections and the enterprise security stack (CrowdStrike, Splunk SIEM, Imperva WAF, ZScaler, Proofpoint, DarkTrace, Digital Guardian DLP), producing actionable detection-tuning guidance.
- **Partnered with the blue team** to strengthen SOC playbooks, detection coverage, and incident response workflows.

Penetration Tester | *Eminence Ways · Kathmandu* Dec 2018 – Jul 2021

- **Delivered VAPT engagements** for clients in banking, fintech, government, and corporate sectors, covering both web applications and network infrastructure.

- **Led offensive security research and development initiatives,** building internal tooling, evaluating emerging techniques, and improving team capability across web, network, and exploit-focused assessments.
- **Performed incident response and malware analysis** investigations for client environments under tight time constraints.
- **Mentored junior testers and trainees** and delivered technical security training programs to government and corporate staff.

TECHNICAL SKILLS

Languages & Scripting: C, C++, C#/.NET, Python, PowerShell, Bash

Offensive Security: Web, Network, and Active Directory penetration testing; red team operations and adversary emulation; purple teaming; phishing campaign design

Red Team Tooling & Development: Custom C#/.NET tooling, PInvoke wrappers, reflective loaders, Cobalt Strike BOFs, Aggressor scripts, payload delivery workflows, post-exploitation modules

Tradecraft & Evasion: Direct and indirect syscalls (SysWhispers), process injection, ETW-aware execution, PPID spoofing, AMSI and AppLocker bypass, signed-binary abuse, sleep-mask techniques

Exploit Dev & RE: x86/x64 reverse engineering, Windows/Linux exploit development (ASLR, DEP/NX, stack cookies, RELRO bypass), shellcoding

C2 & Adversary Tooling: Cobalt Strike, Mythic, Sliver, Havoc, Metasploit, Evilginx, Gophish

Post-Exploitation: BloodHound, Rubeus, Impacket, NetExec, Evil-WinRM, Responder, mitm6

VAPT Tooling: Burp Suite Pro, Nmap, Nessus, Acunetix, OpenVAS

Security Operations: Splunk SIEM, CrowdStrike EDR, Imperva WAF, ZScaler, Proofpoint, DarkTrace, Digital Guardian DLP, Veracode

CERTIFICATIONS

- **OSEP**, Offensive Security Experienced Penetration Tester, OffSec, May 2026, *ID 183305438*
- **OSCP**, OffSec Certified Professional, OffSec, Mar 2024, *ID 100121114*
- **eWPTXv2**, Web Application Penetration Tester Extreme, INE Security, Nov 2022, *ID 7755815*
- **eCXD**, Certified Exploit Developer, INE Security, Jul 2022, *ID 1444671*
- **CAP**, Certified AppSec Practitioner, The SecOps Group, Jan 2023, *ID 6910103*
- **CSA**, Certified SOC Analyst, EC-Council, Apr 2021, *ID ECC1973260845*
- **ISO/IEC 27001**, Information Security Associate, SkillFront, May 2021, *ID 02781930917511*

EDUCATION

B.E., Computer Science · Siddaganga Institute of Technology, Tumkur · CGPA 7.1 2014 – 2018

RECOGNITION & COMMUNITY

- **CTF:** Runner-Up, ThreatCon CTF (2023, 2022, 2019); Winner, NepHack CTF 2020.
- **Bug Bounty:** Acknowledged by Facebook, Xiaomi, Microworld Technologies.
- **Speaking & Community:** Co-Leader & Speaker, Hack The Box Nepal; speaker at OWASP Kathmandu and Pentester Nepal; active in ThreatCon, BSides Ahmedabad, NepHack, Bounty Bash.