Rakib Mahmud Nadir

Penetration Tester | Web App & Network Security | AI/LLM Security Researcher
CRTP | CRTO (In Progress) | eJPTv2 | CRTA | CNSP
+880 1785029110 | sec.rakibnadir@gmail.com | LinkedIn | Portfolio | GitHub | Medium | Khulna, Bangladesh

PROFESSIONAL SUMMARY

Offensive security professional with hands-on experience in web and network penetration testing, Active Directory attack simulation and adversarial AI/LLM security research. Currently conducting VAPT engagements at Cyenetic Solutions Ltd, identifying high and critical vulnerabilities and delivering risk-rated remediation reports. Recognized by the World Bank Group, U.S. HHS, U.S. Courts, U.S. Dept. of Education, and U.S. Dept. of Justice for responsible vulnerability disclosure: 3× U.S. Federal Hall of Fame, 6+ acknowledged findings. Author of garak-report-to-excel, adopted by practitioners for structured LLM audit reporting. Ranked Top 1% on TryHackMe.

EXPERIENCE

Junior VAPT Engineer April 2026 – Present
Cyenetic Solutions Ltd, Dhaka, Bangladesh

- Conducted web and network penetration tests using Burp Suite Pro, Nmap, Nuclei, and Metasploit; identified and exploited XSS, IDOR, authentication bypass, and misconfiguration vulnerabilities across production environments
- Automated vulnerability triage and recon workflows using custom Nuclei templates and Python scripts, reducing manual review time by ~40% on recurring scopes
- Delivered CVSS-scored, risk-rated reports with proof-of-concept evidence and remediation roadmaps; findings accepted and remediated by clients including follow-up closure testing
- Performed OSINT-driven attack surface mapping using subfinder, amass, and crt.sh to enumerate exposed assets prior to each engagement

Assistant Mentor December 2025 – March 2026
Hack Secure, Remote

- Designed and delivered hands-on offensive security curriculum covering OWASP Top 10 exploitation (SQLi, XSS, IDOR), service enumeration with Nmap/Gobuster, and post-exploitation with Metasploit and hash cracking via Hashcat/John
- Reviewed intern penetration test reports and provided structured feedback on finding quality, CVSS scoring accuracy, and remediation recommendations; improved average report quality by cohort's end

Cyber Security Intern April 2025 – May 2025
Hack Secure, Remote

- Executed structured web and network penetration tests; documented vulnerabilities with steps-to-reproduce and mapped findings to OWASP Top 10 and CVE references
- Co-hosted two cybersecurity webinars on ethical hacking methodology, reaching 100+ participants

CERTIFICATIONS

Certified Red Team Professional (CRTP), Altered Security [verify]
Certified Red Team Operator (CRTO), Zero-Point Security *(In Progress)*
Junior Penetration Tester (eJPTv2), eLearnSecurity [verify]
Certified Red Team Analyst (CRTA), CyberWarfare Labs [verify]
Certified Network Security Practitioner (CNSP), The SecOps Group
Certified SOC & Endpoint Detection Professional (CSEDP), The SecOps Group
Practical Help Desk, TCM Security

HONORS & AWARDS

- Acknowledged Security Contributor, **World Bank Group** (VDP-2026-1027, Apr 2026)
- Hall of Fame, **U.S. Dept. of Health & Human Services** (HHS, Synack-powered) [ref]
- Hall of Fame, **The Federal Courts of the United States** (U.S. Courts, Synack-powered) [ref]
- Hall of Fame, **U.S. Department of Education** (Synack-powered, Jun 2026) [ref]
- **Critical-Severity Finding**, U.S. Dept. of Justice (report #13044 — unauthenticated deployment archive with plaintext credentials; formal acknowledgement in progress)
- Acknowledged Security Contributor, **Slapfive** (SL-10462, acknowledged by CTO Sean Langford, May 2026)
- Accepted findings pending formal acknowledgement: U.S. Dept. of Energy, WHO, UKG, Morgan Stanley, Trakonomics
- 1st Place, CTF War Homelab, Hack Secure
- CTF Hunter badge, Hack Secure Discord — awarded for consistent CTF performance and community contributions

SKILLS & TOOLS

Web App Pentesting: Burp Suite Pro, OWASP ZAP, SQLMap, ffuf, Gobuster, subfinder, amass, crt.sh, AlienVault OTX, Shodan, Censys, theHarvester — OWASP Top 10: SQLi, XSS, IDOR, CSRF, SSRF, Auth Bypass, Command Injection, File Inclusion, Business Logic Flaws

Network Pentesting: Nmap, Netcat, Metasploit, Wireshark, Nuclei, enum4linux — service enumeration, credential attacks, misconfiguration exploitation

Active Directory: BloodHound, Impacket (ntlmrelayx, secretsdump), Mimikatz, Rubeus, PowerView, CrackMapExec, certipy-ad, PetitPotam — enumeration, lateral movement, privilege escalation, ADCS/ESC8 NTLM relay, DCSync, Kerberos abuse (Overpass-the-Hash, Pass-the-Ticket), multi-forest trust attacks

AI / LLM Security: Garak, Ollama, LLMmap — prompt injection, guardrail bypass, adversarial probing, model fingerprinting; OWASP Top 10 for LLM Applications

Reporting: Risk-rated findings, CVSS scoring, executive summaries, technical remediation recommendations, PoC documentation

COMMUNITY & LEADERSHIP

- Offensive Security Wing Lead, KUET Cyber Security Club, Khulna University of Engineering & Technology — organizing internal CTFs, workshops, and peer skill-sharing sessions
- Speaker, Hack Secure cybersecurity webinar series (two sessions, remote, 100+ attendees) — topics: ethical hacking methodology and responsible disclosure
- Top 1% on TryHackMe; active competitor in HackTheBox and Hack Smarter Lab CTFs and simulation labs
- Technical writer on Medium (@rakib_nadir): lab walkthroughs, vulnerability analysis articles, and LLM pentesting research

PROJECTS

Passive Subdomain Parser [GitHub]

- Tools: Python 3, asyncio, aiohttp, Rich, subfinder. Queried 7 passive sources (crt.sh, AlienVault OTX, urlscan.io, HackerTarget, RapidDNS, ThreatCrowd, SecurityTrails) with optional subfinder integration
- 80-concurrent async alive-checking via aiohttp; color-coded Rich terminal UI with live output; JSON/CSV export. Reduced subdomain discovery time ~60% vs sequential tools on comparable scopes

Adversarial LLM Security Assessment

- Tools: Garak v0.14, Ollama, LLMmap, Python. Ran 768 automated adversarial probes against 5 local models (Mistral, Qwen, Gemma, Granite, LLaMA); Mistral:7b rated DC-2 with 70.70% prompt injection success rate
- Fingerprinted a live RAG chatbot's hidden model (Mistral-7B-Instruct-v0.3) via LLMmap response-pattern analysis with no internal access; mapped findings to OWASP Top 10 for LLM Applications
- Published garak-report-to-excel, a Python utility converting Garak .jsonl reports to structured Excel spreadsheets, adopted by practitioners for structured LLM audit reporting

Multi-Forest Active Directory Lab & Credential Harvesting

- Tools: BloodHound, Impacket (ntlmrelayx), Mimikatz, Rubeus, PowerView, certipy-ad, PetitPotam. Designed a 4-segment enterprise AD environment (primary forest, child domain, secondary forest, DMZ)
- Executed full ESC8/ADCS NTLM relay chain: PetitPotam → ntlmrelayx → certipy-ad certificate abuse → DCSync; achieved Domain Admin via ADCS privilege escalation
- Demonstrated cross-forest trust attacks, Kerberos ticket replay (Overpass-the-Hash / Pass-the-Ticket), and credential harvesting via Mimikatz DCSync; mapped full attack chain from external access to Domain Admin

Web Application Penetration Test, Grey Box

- Tools: Burp Suite Pro, OWASP WSTG methodology (INFO-01 through INFO-10), custom Python scripts. Identified weak JWT leading to account takeover, stored XSS session hijacking, IDOR, and insecure transport
- Delivered a formal penetration test report with CVSS scores, exploit PoC evidence, and OWASP/PTES-aligned remediation; all findings acknowledged and prioritized by the client

Endpoint Persistence Analysis & Phishing Forensics

- Tools: Metasploit (Meterpreter), WMIC, TCPView, PSAutoRun, VirusTotal, PhishTool, URLVoid. Deployed and detected Meterpreter persistence via malicious service + registry run key; traced C2 traffic; payload flagged 58/71 on VirusTotal
- Performed phishing email header inspection, SPF/DKIM/DMARC verification, and IOC documentation; confirmed credential-harvesting portal via VirusTotal and URLVoid

EDUCATION

B.Sc. Urban and Regional Planning Jan 2023 – Dec 2027 (Expected)

Khulna University of Engineering and Technology (KUET), Khulna, Bangladesh