FAHIM SHAHRIAR

Junior Penetration Tester | Offensive Security | Web Application & Network Security

Pallabi, Dhaka-1206, Bangladesh | +8801701-728769 | fahimonlinux@gmail.com

LinkedIn | TryHackMe | Hacktolive Academy | Github | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity student and Junior Penetration Tester with hands-on experience in web application security, network penetration testing, and offensive security tooling. Completed 200+ TryHackMe rooms and multiple VulnHub machines covering OWASP Top 10, Windows/Linux privilege escalation, and OSINT. Maintains a personal homelab (Proxmox, Wazuh SIEM, AdGuard Home, Tailscale) as a continuous learning environment. Currently preparing for eWPTv2; targeting CPTS and OSCP next. Experienced in vulnerability assessment, exploit chaining, and penetration test report writing.

TECHNICAL SKILLS

Pentesting Tools	Burp Suite Professional, Metasploit Framework, Nmap (NSE), sqlmap, Nuclei, ffuf, Nessus,Amass, Hashcat, and tools across the Kali Linux arsenal.
Web App Security	OWASP Top 10, SQL Injection, XSS, RCE, Authentication Bypass, CMS Exploitation, Directory Fuzzing
Exploitation	EternalBlue (MS17-010), PrintSpoofer, SUID Abuse, UAC Bypass, Privilege Escalation (Linux & Windows)
Operating Systems	Kali Linux, Ubuntu, Windows (SMB, RDP, WMI, Service Enumeration), OpenWrt, Proxmox VE
Networking & Privacy	TCP/IP, DNS, HTTP/HTTPS, SSH, SMB/RPC, Subnetting, Tailscale (overlay VPN, ACL, subnet routing, private DNS)
Recon & OSINT	Google Dorking, SOCMINT, Passive Reconnaissance, Subdomain Enumeration, Hash Cracking
Homelab & Infra	Proxmox VE, Docker, Wazuh SIEM, AdGuard Home (DoH), Tailscale, OpenWrt, Ollama (local LLM), Samba
AI & Automation	Ollama (local LLM deployment, privacy-first), OpenClaw AI agent, n8n workflow automation, OpenRouter/Gemini API
Scripting	Bash (automation, hardening, WAN monitoring), Python (basic scripting), PowerShell (Windows administration)
Reporting	Wazuh SIEM alert triage and dashboard reporting, vulnerability documentation, penetration test findings write-up (scope, impact, remediation), Markdown-based technical notes

PRACTICAL EXPERIENCE & LABS

Penetration Tester (Self-Directed) . *TryHackMe & VulnHub* *2025 – Present*

Vulnerability Assessment	Completed 200+ lab challenges on TryHackMe and VulnHub targeting Linux and Windows machines, covering enumeration, service fingerprinting, and manual exploitation from initial access to root.
Web Application Security	Identified and exploited SQL injection, XSS, RCE, and broken authentication against intentionally vulnerable CMS platforms using Burp Suite for proxy interception, repeater-based testing, and payload delivery.
Windows Privilege Escalation	Leveraged unpatched services, misconfigured local permissions, and token impersonation techniques including PrintSpoofer and EternalBlue (MS17-010) to achieve full system compromise.
Linux Privilege Escalation	Escalated to root via SUID binary abuse, misconfigured sudo rules, and kernel-level exploits; uncovered credential exposure through improperly secured network shares and service misconfigurations.
Reconnaissance & OSINT	Used Google dorking, SOCMINT, and subdomain enumeration to map targets before active engagement, building a clearer picture of the attack surface going in.
Black-Box Lab Practice	Solved multiple VulnHub machines cold, without walkthroughs, working through enumeration, chaining vulnerabilities, and getting to root from nothing.

Homelab Enthusiast . *Self-Hosted Infrastructure* *2023 – Present*

Privacy-First DNS	Deployed AdGuard Home with DoH upstreams and integrated Tailscale so all devices, including mobile, resolve DNS privately through a personal encrypted server on any network, without relying on ISP or public resolvers.
Secure Remote Access	Configured Tailscale across all homelab nodes and personal devices, implementing ACL-based access control and subnet routing to connect securely without exposing any service to the public internet.
Local AI Deployment	Set up Ollama to run LLMs locally for coding assistance and research, keeping everything on-device rather than sending queries to external APIs.
SIEM & Threat Monitoring	Set up Wazuh SIEM with a Windows endpoint agent, built out detection dashboards, and kept log collection running to get real experience reading and triaging security alerts.
Network Engineering	Configured OpenWrt as the primary router with hardware flow offloading, DNS filtering, and custom Bash scripts for automated WAN health monitoring and system maintenance.
Workflow Automation	Set up n8n pipelines and connected OpenClaw AI agent with OpenRouter and Gemini API to automate repetitive research and documentation tasks.

EDUCATION

B.Sc. in Software Engineering, Major: Cybersecurity . *Daffodil International University, Dhaka* — *May 2024 – Expected May 2028*

Higher Secondary Certificate (HSC) . *Monipur High School and College, Dhaka* — *Completed 2023*

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- TryHackMe Junior Penetration Tester (PT1) — **Completed**
- eLearnSecurity Web Penetration Tester v2 (eWPTv2) — **In Progress**
- Hack The Box Certified Penetration Testing Specialist (CPTS) — **Expected 2027**
- Offensive Security Certified Professional (OSCP) — **Expected 2028**

Platform Activity:

- TryHackMe (profile: MaGnum): Completed 200+ rooms covering Windows exploitation, Linux privilege escalation, web application attacks, and OSINT reconnaissance.
- VulnHub: Solved multiple black-box machines independently, including ICA1, DC1, and HackMePlease, using full manual exploitation methodology without guided hints.

PROJECTS

Recon Automation Tool | *Python, Nmap, Amass, Subfinder, Nuclei, Bash*

- Built a modular Python-based recon pipeline that chains passive subdomain enumeration (Amass, Subfinder), live host discovery (Nmap), and automated vulnerability scanning (Nuclei) into a single CLI workflow with structured JSON/HTML output reports.
- Built scope filtering in from the start so enumeration stays within target bounds; results are saved per-target making it easy to pick back up or document findings later.

Vulnerable Web App: CTF Challenge Builder | *Python (Flask), SQLite, Docker, Burp Suite*

- Built a Flask web app with intentional OWASP Top 10 vulnerabilities (SQL Injection, stored XSS, broken authentication, IDOR) and Dockerized it so the Hacktolive Academy community could spin it up as a local training target.
- Wrote walkthroughs for each vulnerability so community members could understand not just how to exploit it, but why the code is vulnerable and how to fix it.

CVE Research & Exploit Analysis Reports | *Metasploit, Ghidra, Searchsploit, Markdown*

- Wrote technical breakdowns of real CVEs including MS17-010/EternalBlue and PrintSpoofer, covering the root cause, affected versions, how the exploit works, and patch analysis. Published these to the Hacktolive Academy community as reference material.
- Used Ghidra for basic binary inspection and Metasploit for controlled lab reproduction, with each report following a consistent format: summary, CVSS scoring, technical breakdown, PoC steps, and defensive recommendations.

COMMUNITY & ENGAGEMENT

Active Member . *Hacktolive Academy* — *2023 – Present*

- Active participant in Hacktolive Academy, working through lab challenges, sharing findings, and helping newer members get unstuck on recon, exploitation, and infrastructure tasks.
- Regularly join group discussions and knowledge-sharing sessions, talking through techniques, comparing approaches on boxes, and reviewing each other's work.

ADDITIONAL INFORMATION

Languages : English (Professional), Bengali (Native)
Availability : Open to full-time, part-time, and remote opportunities
Interests : CTF competitions, homelab infrastructure, local AI tooling, privacy-preserving technologies