M Christopher Arock

Cybersecurity Practitioner & Penetration Tester

christopherarock48@gmail.com | +91 9952834357 | Sivagangai, Tamil Nadu, India | LinkedIn: linkedin.com/in/christopher-arock | GitHub: github.com/arock-404 | TryHackMe: tryhackme.com/p/arock404 | Medium: medium.com/@christopherarock

PROFESSIONAL SUMMARY

Penetration Tester with hands-on experience in offensive security, Active Directory attacks, and web application vulnerability assessment. Every internship, project, and certification has been deliberately chosen to build towards a career in penetration testing — from understanding attacker techniques to gaining defender visibility through real SOC exposure. Ranked Top 2% globally on TryHackMe (200+ labs completed); currently pursuing OSCP.

WORK EXPERIENCE

Student Intern – Penetration Testing — Infoziant Security, Virudhunagar *09/2023 – 12/2023*

- Performed web **vulnerability testing & penetration assessments** on 3+ live systems, identifying XSS and SQL injection vulnerabilities.
- Built reconnaissance automation scripts, improving vulnerability discovery efficiency — laying the foundation for my offensive security focus.

Cybersecurity Intern — Max Conformance, Remote *06/2024 – 07/2024*

- Audited cloud security using AWS, Prowler, Powerpipe & Steampipe — building attacker-relevant insight into how cloud misconfigurations are identified and exploited.
- Built a Flask API to automate AWS compliance reporting, significantly improving audit efficiency.

SOC Intern — Ernst & Young (EY), Chennai *08/2025 – 10/2025*

- Used Splunk & Azure Sentinel for SIEM monitoring and use case tuning — deliberately gaining blue team visibility to better understand and anticipate defender detection during offensive engagements.

Freelance Penetration Tester — Self-Employed — Remote *2026*

- Conducted a grey-box penetration test on a Compliance-as-a-Service web application, with limited authenticated access provided by the client.
- Identified **2 critical vulnerabilities** — IDOR enabling unauthorized access to any user account, and an API response leaking MFA code — documented with CVSS risk ratings, proof-of-concept steps, and remediation guidance in a formal penetration test report.

EDUCATION

Higher Secondary Education *2022*

Kendriya Vidyalaya, Sivaganga, India | Grade: 89%

B.Tech in Computer Science & Engineering (Cyber Security) *2022 – 2026*

Kalasalingam Academy of Research and Education | GPA: 8.79 / 10.0

PROJECTS

Active Directory Home Lab (Offensive Security) *2024*

- Simulated enterprise AD environment; executed **Kerberoasting, LLMNR poisoning & Pass-the-Hash** using Mimikatz, CrackMapExec & BloodHound — directly aligned with OSCP exam scenarios and real-world red team engagements.
- Deployed AD DS with realistic users and GPOs; mapped full attack paths using **BloodHound**.

E-mailScanner: Phishing Detection System *2024*

- Built to understand **attacker-side phishing techniques** — strengthening web application security knowledge directly applicable to penetration testing engagements.
- Integrated **ClamAV, ML & VirusTotal API** for multi-layered phishing detection, reducing false positives in simulated datasets.

TryHackMe Labs & Challenges *2025 – Present*

- **Structured learning path deliberately chosen** to complement real-world internship experience and systematically prepare for OSCP — ranked **Top 2% globally** out of 200+ labs completed.
- Covered network exploitation, web vulnerabilities **(OWASP Top 10)**, privilege escalation; practiced **10+ tools**.

SKILLS

Focus: Offensive Security & Penetration Testing | Technical: Linux, Python, VAPT, Web App Security, AD Attacks, Network Security, Malware Analysis

Tools: Nmap, Burp Suite, Metasploit, BloodHound, Mimikatz, CrackMapExec, Netexec, Splunk, Azure Sentinel, Prowler, Steampipe, Flask

CERTIFICATIONS

AppSec Practitioner (CAP) – SecOps Group, Feb 2024 | **APIsec Certified Practitioner** – APIsec University, Oct 2025 | **CNSP** – SecOps Group, Dec 2025