Aryan

Mob: +91-9430713067 | **Email:** aryantiwary10@gmail.com | **LinkedIn** | **GitHub** | **Website**

SUMMARY

Security-oriented Computer Science undergraduate with experience in securing and attacking enterprise-style systems, including Active Directory environments and networked infrastructure. Strong fundamentals in operating systems, networking, and Python automation, with hands-on exposure to SOC workflows, detection engineering concepts, and incident response.

PROJECTS

Splunk SIEM Home-lab:
- Deployed a multi-VM SIEM environment (Windows Server, Linux, attacker VM) to collect logs and simulate enterprise security workflows.
- Wrote custom SPL-based detection rules for PowerShell exploitation, privilege escalation, and brute-force attacks.

ML-Powered ICS Anomaly Detection System:
- Simulated power grid attacks by injecting abnormal Modbus sensor values into a virtualized ICS (OpenPLC, ModbusPal).
- Trained autoencoders + isolation forest on 50,000+ datapoints, achieving 92% anomaly detection accuracy with <500ms latency in SCADA dashboards.

Infrastructure & Network Exploitation (Hack The Box):
- Exploited OWASP Top 10 vulnerabilities including SQL injection, XSS, CSRF, SSRF, and authentication flaws in controlled lab environments
- Compromised Linux and Windows systems through service enumeration, misconfiguration abuse, and privilege escalation techniques

Active Directory Home-lab:
- Configured AD Domain Controller + Windows clients, with users, OUs, GPOs, and shared resources in a VMware lab.
- Simulated AD attacks (LLMNR poisoning, SMB/NTLM relay, IPv6 MitM) and applied hardening measures like SMB signing and LDAP channel binding.

EDUCATION

- **Manipal Institute of Technology,** **Sep 2023 - Present**
B.Tech in Computer Science Engineering | CGPA: 7.58/10

- **Rajendra Vidyalaya,** **Jul 2021 - Jun 2023**
Class XII (82%), Class X (89%)

SKILLS

Security & SOC:
- SIEM (Splunk concepts), SPL (Search Processing Language), Incident Response, MITRE ATT&CK, Log Analysis

Offensive & Defensive:
- Active Directory attacks, Privilege Escalation, Network Pentesting

Systems & Networking:
- Linux, Windows Server, TCP/IP, DNS, Active Directory

Programming & Automation:
- Python (automation, parsing), Bash, Java (OOP fundamentals), C

Cloud & DevOps:
- AWS fundamentals, IAM basics

CERTIFICATIONS

CompTIA Security+ | CompTIA CySA+ | IBM Cybersecurity Analyst Professional | IBM SOC in Practice

COMPETITION AND ACHIEVEMENT

- **Kaspersky Hackathon 2025** – Top 15 in India; collaborated with a team to design and deploy an ICS anomaly detection
- **Rakuten Hackathon 2025** – Finalist; FinTech AI Agent
- **Top 50 in India** on CTFtime platform.