

ABIR DEY

+91 7872918296 ◇ Gurugram, Delhi NCR

abirdey2011@gmail.com ◇ [linkedin.com/in/abirdey2011](https://www.linkedin.com/in/abirdey2011) ◇ github.com/AD2011

EDUCATION

Bachelor of Technology in Electronics and Electrical Engineering	2020 – 2024
Kalinga Institute of Industrial Technology, Bhubaneswar	CGPA: 9.04

SKILLS

Languages and Scripting	C, Python, Go, SQL, Bash, PowerShell, YAML, JSON
Tools	Linux, Git, Rubeus, Mimikatz, Nessus, Acunetix, Metasploit
Platforms	Azure, Entra, AWS, GCP
Security Solutions	SIEM(ArcSight, Sentinel, Chronicle), SOAR, WAF(CloudFlare, Imperva, Akamai) XDR(Sentinel One, CrowdStrike, Defender), DLP(NetSkope)

EXPERIENCE

Red Team Consultant	Jan 2024 – Present
PwC India	<i>Gurugram, Delhi NCR</i>

- Led comprehensive Red Team engagements simulating real-world cyberattacks to uncover critical vulnerabilities in clients' external and internal assets across Banking, Power, Petrochemical sectors
- Collaborated with Blue Teams to enhance detection and response strategies. Utilized SIEM and SOAR to create new rules and policies to proactively detect and stop attacks.
- Executed comprehensive social engineering assessments, including phishing, vishing, and physical intrusion simulations, to evaluate and improve clients' human-centric security defenses.
- Automated recon and attack processes to reduce mean time to report vulnerabilities by 25%
- Created custom C2 beacons and executables to evade XDR solutions using techniques such as Indirect Syscalls, Reflected DLL Loading and Obfuscation

Software Engineer (Data Science) Trainee	Jun 2023 – Dec 2023
HighRadius Corporation	<i>Bhubaneswar, Odisha</i>

- Built AI-enabled B2B invoice management platform with predictive capabilities.
- Designed algorithms to validate financial deductions and automate business logic.
- Improved algorithm efficiency by 15% in terms of time and memory.
- Collaborated with cross-functional teams to align models with client requirements.

CERTIFICATIONS

- Certified Red Team Professional (CRTP), Altered Security - 2025
- Certified AppSec Practitioner (CAP), The SecOps Group - 2024
- Cisco: CCNA-1, Cybersecurity Essentials – 2023

PROJECTS

Active Directory Attack Simulation and Malware Lab: Designed a virtual Active Directory environment to practice and demonstrate AD exploitation techniques and XDR evasion techniques using custom malware.

Distributed Network Latency Monitoring : Designed and deployed a distributed SmokePing environment utilizing a master-slave architecture to monitor global network latency across diverse environments.