

# ARYAN PAREEK

+91 99504 00005 • aryanpareek311072004@gmail.com • Jaipur, Rajasthan 302019

## Personal Summary

Certified Ethical Hacker with four years of progressive experience in cybersecurity, specializing in both offensive and defensive security operations. Proven expertise in penetration testing, cybercrime investigation, and security consultancy, contributing to projects in government and private sectors. Holds a Bachelor of Computer Applications in Cybersecurity and advanced certifications including CompTIA Pentest+ and Certified Ethical Hacker. Skilled in developing security measures, conducting risk analysis, and integrating security within DevOps pipelines, with a focus on protecting critical information systems. Focused professional with extensive knowledge of threat detection, prevention and analysis. Leverages expertise in security software and products to build solid IT security infrastructure. Detail-oriented leader and proactive communicator dedicated to safeguarding against threats.

## Profiles

- <http://www.linkedin.com/in/aryan-pareek-597a0b218>
- <https://github.com/Aryanpareek3/>

## Skills

- Vulnerability assessment and penetration testing
- Risk analysis and incident response
- Cybersecurity policy development
- Operating system hardening
- Ethical hacking principles
- Threat modeling and intrusion detection
- Network security testing
- Security information and event management
- Web application security testing
- Vulnerability scanning tools
- Cloud security testing
- Cyber threat intelligence
- Problem-solving skills
- Network protocol analysis
- Cross-site scripting techniques

## Experience

10/2023 - Current

Cyber Volunteer, **Rajasthan Police**, Jaipur, Rajasthan

- Developed and implemented policies to enhance cyber awareness among various audiences.
- Maintained clear standard operating procedures to improve overall operational effectiveness.
- Conducted targeted analyses on specific cases and technologies to address emerging threats.

12/2024 - 03/2025

Cyber Security Intern, **Rajasthan Police**, Dhaulpur, Rajasthan

- Conducted full-time cybersecurity consulting with an emphasis on criminal investigations and security development.
- Handled cybercrime cases through thorough analysis and strategic interventions.
- Traced cybercriminals using advanced investigative techniques and tools.
- Gathered evidence to support legal proceedings and enhance case outcomes.
- Developed security measures to fortify systems against future threats.

02/2024 - 10/2024

Cyber Security Engineer, **Skyee Pvt Ltd**, Jaipur, Rajasthan

- Executed risk analysis to identify and recommend security countermeasures.
- Developed strategies to protect computer files from unauthorized modification, destruction, or disclosure.
- Enhanced system security by implementing targeted improvements based on analysis findings.
- Focused on continuous evaluation of security measures to mitigate risks effectively.

---

## Education

06/2025

**BCA**, Cybersecurity and Cyber Forensics

**Parul University**, Jaipur, Rajasthan

---

## Projects

- Identification of fraudulent websites**- developed a sophisticated machine-learning-based fraud detection tool, meticulously designed to identify and flag both phishing attempts and counterfeit websites effectively. This innovative system assists law enforcement agencies in the crucial task of identifying malicious websites, providing invaluable support for comprehensive cybercrime investigations, and proactively preventing the rapid spread of online scams, thereby significantly enhancing internet safety. The core of this tool lies in its robust analytical capabilities, leveraging key features such as thorough URL analysis, rigorous domain verification processes, and meticulous scrutiny of SSL certificates. Through rigorous testing and continuous optimization, the system consistently achieves an impressive accuracy rate exceeding 95% in accurately categorizing websites, clearly differentiating between legitimate online platforms and those posing malicious or fraudulent threats.
- Automated Web Reconnaissance and Web Toolkit**, 2025, Jaipur: Developed ENUMO, an automated web reconnaissance and exploitation toolkit. This tool is designed for penetration testers, bug bounty hunters, and CTF enthusiasts, accelerating enumeration and exploitation phases by automating the discovery of open ports, web technologies, directories, subdomains, potential XSS vulnerabilities, and known exploit.
- Traverser**: A high-speed, Bash-based directory traversal scanner equipped with parallelism, URL encoding, and null byte bypass capabilities. This lightweight command-line tool is designed to identify path traversal vulnerabilities in web applications, leveraging its portability through Bash implementation and features such as parallel execution, URL encoding, null byte injection, and file extension evasion.

---

## Certifications

- CompTIA PenTest+**, validated advanced skills in penetration testing, vulnerability assessment, and ethical hacking techniques used to identify, exploit, report, and manage network vulnerabilities. Demonstrated proficiency in planning and scoping penetration tests, performing active reconnaissance, exploiting network and application vulnerabilities, and producing comprehensive post-engagement reports.
- Certified AppSec Pentesting Expert**, a highly skilled and certified application security pentesting expert accredited by the SecOps Group, specializing in identifying and mitigating vulnerabilities within modern web and mobile applications. Experienced in conducting comprehensive security assessments, including threat modeling, static and dynamic analysis, and manual penetration testing to uncover risks that automated tools may overlook.
- Ethical Hacker, Cisco**, the Cisco Networking Academy Ethical Hacker certificate teaches you how to think and act like an ethical hacker. You learn the full penetration testing process—from reconnaissance to exploitation and reporting—using real-world tools in hands-on labs. It

covers web, system, network, and social engineering attacks, along with legal and ethical aspects. By the end, you're equipped to identify vulnerabilities, simulate attacks, and communicate findings professionally-making it a strong foundation for a career in offensive cybersecurity.

- **Foundations of Cybersecurity Certification — Google**

Successfully earned the Google Foundations of Cybersecurity Certification, which validates a comprehensive understanding of fundamental security principles, effective risk management strategies, efficient incident response procedures, and proactive threat detection methodologies, thereby providing a robust and essential foundation for a thriving career in the field of professional cybersecurity.

- **Cisco Cyber Security Fundamentals**, completed comprehensive training in foundational and intermediate cybersecurity concepts, including threat analysis, security monitoring, network defense, and incident response Gained practical skills in identifying and mitigating cyber threats using industry-standard tools and technologies Emphasized a layered security approach, aligning with real-world cybersecurity operations and best practices across enterprise and cloud environments.

- **CEHv13**: Demonstrated expertise in ethical hacking and offensive security practices, encompassing vulnerability assessment, penetration testing, network and application exploitation, and threat analysis. Proficient in utilizing tools and methodologies to identify and mitigate security risks in real-world environments.

- **DevSecOps**, This certification validates expertise in integrating security practices within the DevOps lifecycle, ensuring continuous security throughout software development and deployment. It covers the implementation of automated security testing, vulnerability scanning, and compliance checks within CI/CD pipelines.

- **Junior CyberSecurity Analyst**, Certified by **Cisco Networking Academy** for demonstrating practical understanding of network security, threat analysis, vulnerability management, and incident response within enterprise and SOC environments.

---

## **Extracurricular Activities**

- **Deloitte Australia Cyber Job Simulation** on Forage, 07/01/25 (Remote): Completed a job simulation involving the analysis of web activity logs. Assisted a client in a cybersecurity breach investigation by identifying suspicious user activities.
- **Mastercard Cybersecurity Virtual Experience Program**, Forage - September 2025: Conducted a job simulation as a Security Awareness Team Analyst. Responsibilities included identifying and reporting security threats, such as phishing attempts Additionally, analyzed business units to determine areas requiring enhanced security training, and implemented corresponding training programs and procedures.
- **Tata Cybersecurity Security Analyst Job Simulation** on Forage - September 2025: Conducted a job simulation focused on Identity and Access Management (IAM) for Tata Consultancy Services, collaborating with a Cybersecurity Consulting team. This experience provided expertise in IAM principles, cybersecurity best practices, and demonstrated strategic alignment with business objectives. Additionally, delivered comprehensive documentation and presentations, effectively communicating complex technical concepts.

---

## **References**

References available upon request.