Aryan Gurung

+91 7477596692 | gurungaryan73@gmail.com | linkedin.com | heathen.in | Github1 | Github2

Summary

Highly skilled and experienced cybersecurity professional with expertise in conducting red-team attack simulations, penetration testing, and custom exploit and malware development. Possesses a strong technical background combined with exceptional client management and communication skills. Proven ability to identify and exploit vulnerabilities, providing valuable insights to enhance organizational security posture. Excels in collaborating with cross-functional teams to deliver effective solutions that meet client needs. A trusted advisor known for consistently exceeding expectations and delivering results in complex and dynamic environments.

Technical Skills

Programming Languages: C/C++, Rust, Python, Go, Java, NASM, JavaScript, TypeScript, C#, SQL, HTML/CSS

Networking: Fundamentals, protocols, packet capture and analysis using Wireshark

Technologies: Bash, PowerShell, Git, Docker. IDA Pro, Ghidra, Burp, Metasploit, Havoc, Wireshark

Writing: Technical Penetration Test Report, Techinical Documentations

Security: VAPT, Active Directory, Red Team, Incident Response, Reverse Engineering, Exploit development, Malware Development

Operating Systems: Linux, Windows, MacOS

Professionsl Experience

CyberSmithSecure Aug 2023 – May 2024
Red Team and Incident Response *Mumbai, IN*

- Conducted Red Teaming assessments by leveraging advanced post-exploitation frameworks and Command-and-Control tools
- Designed, deployed, and maintained reliable Red Team infrastructure to support continuous operations
- Developed Fully Undetectable (FUD) exploits to bypass modern detection mechanisms, ensuring successful simulations of sophisticated threat actor tactics
- Collaborated with teams to investigate and analyze security incidents, identifying root causes and mitigating threats

Subconscious Compute Jul 2022 – Sep 2022
System Security Engineering *Bangalore, IN*

- Designed and implemented a kernel-level security tool in Rust using the eBPF, focusing on anomaly and threat detection
- Developed efficient, low-level Rust code adhering to industry best practices, ensuring optimal performance and maintainability
- Solved complex system security challenges by leveraging Rust's memory safety and concurrency features
- Curated and optimized tool output for seamless integration into machine learning pipelines, enhancing automated threat analysis capabilities

VIKASANA Aug 2021 – Oct 2022
Presidency University R&D - Cybersecurity Division *Bangalore, IN*

- Participated in Capture The Flag (CTF) competitions, solving complex challenges to enhance practical cybersecurity skills
- Conducted interactive workshops on advanced cybersecurity concepts, tools, and techniques to educate peers and professionals
- Developed and delivered cybersecurity awareness programs, promoting best practices to mitigate digital threats
- Applied problem solving and critical thinking to address real-world cybersecurity scenarios during collaborative and independent research initiatives

GPCSSI2021 Jun 2021 – Jul 2022
Gurugram Police, Cyber Cell *Gurugram, IN*

- Investigated email based cybercrimes, including phishing and spoofing attacks, to identify perpetrators and mitigate risks
- Conducted investigations into financial frauds, employing advanced tools to trace illicit transactions and prevent recurrence
- Explored dark web activities, identifying illicit operations and gathering intelligence for law enforcement
- Analyzed social media platforms for cyber crimes and educated users about safe practices

Projects

Moox
GUI based Text Editor with Org Mode like features — *Rust, egui, eframes, GUI, Cross Platform*
• https://github.com/h3athen/moox

Hades
System level threat hunting tool — *Go, Windows, Threat Hunting*
• https://github.com/Threat-Olympus/hades

Syslog-ebpf
Log live syscalls over linux's kernel land using eBPF — *Rust, Aya, CLI, Linux, Threat Hunting*
• https://github.com/h3athen/syslog-ebpf

RAMP
A super fast port scanner in rust — *Rust, CLI, Unix, Networking*
• https://github.com/6Sixty6/ramp

Rrep
A simple grep implementation in rust — *Rust, CLI, Unix*
• https://github.com/0xlilith/rrep

Stivale2
A bare bone kernel implementation — *C, Shell, Make file, Kernel*
• https://github.com/0xlilith/stivale-two

Education

Presidency University, Bangalore — Bangalore, IN
B.Tech in Computer Engineering (Specialization in Cyber Security) — *Apr 2020 – Aug 2024*
Courses: OOP in C++, Compilers, Algorithms, Operating Systems, Data Structures, DBMS, Web Security, Java, System Architecture, Physics, Engineering Mathematics, Chemistry, Electronics, Ethical Hacking, Data Forensics

Certifications

ISO/IEC 27001 Information Security Associate — September 2, 2024
SkillFront — *https://www.skillfront.com/Badges/83073263326360*

OpenSecurityTraining2 Dbg1011: Beginner WinDbg — June 25, 2023
OpenSecurityTraining2 — *https://p.ost2.fyi/certificates/73249bd3588d467285f7c0f83d6b5aa7*

Foundation Level Threat Intelligence Analyst — June 25, 2023
OpenSecurityTraining2 — *https://arcx.io/verify-certificate*

Microsoft Rust — October 20, 2022
Microsoft — *https://learn.microsoft.com/en-us/users/aryangurung-3188/*

Web Hacking/Penetration Testing & Bug Bounty Hunting — June 2, 2020
Udemy — *https://www.udemy.com/certificate*

Awards

Hacktoberfest 2022
Digital Ocean

Hacktoberfest 2021
Digital Ocean