Debjeet Banerjee

whokilleddb@protonmail.com
Github **LinkedIn** **Twitter**

Cyber Security professional with 2+ years of experience. Skilled in web application penetration testing, application security, binary exploitation, and network penetration testing. Currently focused on developing Red Team Tools, Malware Development, 0-Day/N-Day research while pursuing my Bachelors in Technology (CS).

PROFESSIONAL EXPERIENCE

FIRECOMPASS **BANGALORE, India**
Security Research Intern *October 2022–Present*

- Develop Red Teaming tools and exploits to be used in CART
- Develop Loaders and Payloads to bypass popular AV Engines and EDRs
- Document IOCs and TTPs for common exploitation techniques

PAYATU **PUNE, India**
Security Consultant Intern *February 2022–October 2022*

- Perform comprehensive web application and network penetration tests for clients along with comprehensive reporting on the same
- Design challenges for Capture the Flag events
- Write educational blogs on various security related topics'

CYBERPWN TECHNOLOGIES **BANGALORE, INDIA**
Security Analyst Intern *Nov 2021–Jan 2022*

- Carry out penetration testing activities across client web applications and networks to identify vulnerabilities and bugs in the application.
- Perform configuration reviews and static code analysis
- Develop automation scripts to enhance offensive security capabilities and provide hands-on training to development teams on secure code practices

CYBERFRAT **MUMBAI, INDIA**
Technical Project Intern *June 2021–August 2021*

- Design enterprise security posture and architecture
- Set up proper access management integration
- Setup endpoint management systems like UEM, EMM and MDM
- Compare services across various vendors to bring forth the most optimal solutions for clients

CERTIFICATIONS

- **Junior Penetration Tester | eLearnSecurity**
- **Red Team Operator Malware Development Essentials | Sektor7**
- **CNSS Certified Network Security Specialist | ICSI**
- **Splunk 7.x Fundamentals Part -1**
- **Splunk User Behavior Analytics**

PUBLISHED CVE(s)

- **CVE-2022-0845** : Code Injection in GitHub repository pytorchlightning/pytorch-lightning prior to 1.6.0.
- **CVE-2021-42192** : Konga v0.14.9 is affected by a privilege escalation vulnerability.
- **CVE-2022-2054** : Command Injection in GitHub repository nuitka/nuitka prior to 0.9.
- **CVE-2022-38258** : LFI in DLink consumer Routers, which can be escalated to Denial-of-Service
- **CVE-2022-40946** : Unauthenticated Denial of Service in DLink DIR-819 commercial router

PROJECTS

- **1s0lat3** : A Linux sandbox written from scratch using **C** which uses **Namespaces** to create a docker-like containerised environment.
- **Smoochum** : A **LD_PRELOAD** based rootkit inspired directly by the infamous **Jynx Rootkit**
- **Fake Stream** : Use **v4l2loopback** kernel modules and **ffmpeg** to create a shell script which takes a video as input and streams it on loop as your webcam output.
- **LazarusOS** : A **Rust-based** operating system written entirely from scratch.
- **Weaponizing OpenWRT** : Turn a **TP-MR3020** Router into a Linux computer with networking tools cross compiled for **MIPS** architecture.

OTHER FOSS CONTRIBUTIONS

- Contributed to security tools like **Metasploit** and **Social Engineering Toolkit**
- Contributor at **OWASP Pygoat**
- Fixed Security vulnerabilities in **Pytorch-lightning**
- Fix security vulnerabilities in **CommaAI, flairNLP, etc.**

PROGRAMMING LANGUAGES

- **Python**
- **C**
- **Bash**
- **ASM**
- **Rust**
- **Javascript**

EDUCATION

INSTITUTE OF ENGINEERING AND MANAGEMENT
Bachelor of Technology(CS),
CGPA: 9.63

ST XAVIER'S INSTITUTION
ISC Examination,
Percentage of Marks: 97.25%