Nofil Qasim

Blog: https://nofilqasim.info
Team: Kernelcide

Github: papadoxie
LinkedIn: nofil-qasim
Email: nofilqasim@gmail.com

Research Interests

My interests lie in the intersection of computer security and low-level systems. I am interested in the security vulnerabilities posed by system design flaws and their implementations, and how they can be exploited. In the past I have worked on flaws in the WebAssembly language specification, written malware for Windows, researched Linux Kernel vulnerabilities and found vulnerabilities in ZTNA (Zero Trust Network Architecture) applications. Currently I am working on introducing novel mitigations against low-level security issues found in cloud environments.

Education

PUCIT - University of the Punjab — September, 2019 – July, 2023
Bachelor of Science - Computer Science — Lahore, Punjab, Pakistan

Professional Experience

Senior Vulnerability Researcher — July, 2024 – Present
Ebryx F.Z.C. — Ajman, United Arab Emirates (Remote)

- Identified and demonstrated prevalent low-level attack vectors against cloud environments
- Formulated generic mitigation techniques to wipe out entire vulnerability classes at a low level
- Performed detailed research on enabling compile time mitigations, such as SHSTK and IBT, on precompiled binaries
- Designed alternatives to compile-time mitigations to be used at run-time
- Wrote agents to block execution of unknown code, by using low-level signals to verify origin, across JITed languages like Lua

Vulnerability Researcher — July, 2023 – July, 2024
Ebryx (Pvt.) Ltd. — Lahore, Punjab, Pakistan

- Lead a team in performing security assessments on a ZTNA (Zero Trust Network Architecture) solution and found more than 20 0-days
- Worked with a team to design architectural mitigations against those vulnerabilities
- Set up workflows for fuzzing a wide range of open-source projects including tar, zlog and xz-utils
- Set up a distributed environment for fuzzing the Linux Kernel on ESXi servers using syzkaller
- Researched Linux usermode and kernel (n-day & 1-day) exploits

Malware Researcher — November, 2021 – July, 2023
Ebryx (Pvt.) Ltd. — Lahore, Punjab, Pakistan

- Worked with a team on a fully featured RAT (Remote Access Trojan)
- Tested Windows (n-day) exploit PoCs for use in malware
- Researched and implemented initial access and malware deployment techniques for deployment against medium sized organizations
- Researched AV and EDR evasion techniques and successfully managed to evade major security products such as Crowdstrike EDR, Kaspersky AV, Windows Defender, etc.
- Worked on bypassing security mechanisms such as Applocker, etc.

Teaching Assistant (Operating Systems) — February, 2022 – October, 2022
PUCIT - University of the Punjab — Lahore, Punjab, Pakistan

Information Security Intern — July, 2021 – September, 2021
Systems Limited — Lahore, Punjab, Pakistan

- Performed Level 1 Security Operations Center (SOC) Analyst duties
- Used industry standard tools like HCL Appscan to perform real world vulnerability assessments
- Built a shared knowledge base of attack vectors and the cyber kill chain for future assessments
- Worked towards a Web Application Penetration Testing Certification

Teaching Assistant (Computer Organization and Assembly) — February, 2021 – June, 2021
PUCIT - University of the Punjab — Lahore, Punjab, Pakistan

Research Experience

A Novel Approach to Applying x86-64 Exploitation Techniques on WebAssembly Binaries
July, 2022 – July, 2023
PUCIT - University of the Punjab

- Formulated the idea and initiated the research project
- Discovered differences between WebAssembly Modules built from the same source
- Worked on WebAssembly binary fuzzing and the problems associated with it
- Working on identifying ways to reuse x86-64 exploitation techniques on WebAssembly binaries e.g. Return-to-libc, Return Oriented Programming (ROP) via WASM jump table overwrite, and, Heap Exploitation using Malloc Des-Maleficarum (House of Force, etc.) on emmalloc and dlmalloc

Salient Features of the MIPS32/64 Architecture and A Handy Guideline to its Assembly Programming
November, 2022 – July, 2023
PUCIT - University of the Punjab

- Worked on verifying claims and hypothesis of my team members
- Reviewed sources and references for correctness
- Prepared the paper for submission

Independent Projects

Python Debugger C, Python
https://github.com/papadoxie/pydbg

- A toy low-level debugger written in Python

OS Development C, x86-64 Assembly
https://github.com/papadoxie/Operating-System

- A hobby Operating System Kernal I work on in my spare time
- Multiboot compliant
- Custom linux-like kernel
- Custom libkernel implementation

Volunteering

Cyber Security Lead PUCIT - University of the Punjab
Google Developer Student Clubs 2020 – 2023
University Lead BSides Pakistan
2020 – 2023

Skills

Programming Languages: C, Python, Java, C#, x86-64 Assembly, LaTeX
Security: Binary Exploitation, Reverse Engineering, Malware Development
Tools: Ghidra, GDB, GNU/Make, Intel PIN, IDA Pro, FRIDA
OS: GNU/Linux, Windows + WSL