ALI RAZA

Security Researcher

+92-305-738-1431 | elirazamumtaz@gmail.com | locus-x64.github.io

alirazamumtaz | locus-x64 | locus_x64

Lahore, Punjab - 53000, Pakistan

Professional Experience

- **Ebryx (Pvt.) Ltd. [🌐]** *Mar 2023 - Current*
  Security Researcher Lahore, Pakistan
  - Mitigating attacks by performing interpreter & runtime hardening
  - Designed kernel-level technique using Linux netfilters to detect path traversal attacks on a Linux system
  - Designed userland agent using JVMTI to detect Java deserialization attacks on a Linux system
  - Designed kernel-level technique using LKMs to detect ASLR brute force attacks on a Linux system
  - Discovered a 0-day vulnerability (CVE-2024-22857) in the open-source logging library zlog using AFL++ fuzzing
  - Performed fuzzing on Linux kernel-specific syscalls using syzkaller, focusing on black-box security research
  - Conducted n-day research on Linux Kernel Exploitation, improving security assessments and attack strategies
  - Formalized a Linux kernel exploitation attack matrix, uncovering exploitable kernel objects and refining pre/post-exploitation techniques
- **University of the Punjab [🌐]** *Oct 2022 - Feb 2023*
  Teaching Assistant Lahore, Pakistan
  - Designed material and coursework for the newly introduced lab component of the subject
  - Designed exam papers for the lab
  - Assisted students in the lab + other TA responsibilities

Research Experience

- **n-day ("Call of Death" in Shannon Baseband) - CVE-2020-25279 [🌐]**
  - Looked into Samsung's Exynos modem chip that uses Shannon RTOS
  - Used IDA Python and Ghidra scripts combined to load the firmware file for reversing
  - Analysed the PAL memory allocation mechanism in Shannon
  - Found the vulnerable code for the CVE mentioned above statically
  - Used FirmWire to emulate the firmware
  - Tools used: FirmWire, IDA Pro 9-beta, Ghidra
- **0-day in Zlog: CVE-2024-22857 [🌐]**
  - Conducted fuzzing of zlog, leading to the discovery of a critical 0-day vulnerability (CVE-2024-22857)
  - Successfully identified and reported the vulnerability, which allowed arbitrary code execution
  - Developed proof-of-concept (PoC) exploit to demonstrate the feasibility of the attack and assisted in proposing mitigations
  - Collaborated with the vendor to ensure a timely patch and public disclosure of the vulnerability
  - Tools used: AFL++, elixir, gdb, git
- **n-day (Dirty Pipe) - CVE-2022-0847 [🌐]**
  - Explored different data-only attacks in Linux kernel
  - Looked into the in-memory buffer management inside kernel
  - Following the source of pipe IPC in Linux kernel using elixir.bootlin, wrote a PoC for the CVE-2022-0847
  - Tools used: Elixir Bootlin, GDB with bata24/gef, QEMU

- **Vulnerability Research & Exploit Development for Android Kernel [🌐]**
  - Final Year Project (FYP) during Bachelor
  - Supervised by Dr. Muhammad Arif Butt (arif.phd)
  - Started binary exploitation from Linux user-land and completed with kernel-land exploitation
  - Conducted n-day research on CVE-2019-2215

Skills

- **Programming:** ANSI C, Assembly x86-64/ARM, Bash, Python
- **Research:** Linux Kernel, Mobile Baseband, Android Kernel, Linux Runtime, Python Interpreter, JVMTi
- **Tools:** QEMU, VMWare Workstation, IDA Pro (ost2 certified), Ghidra, GDB with gef, AFL++, elixir, CodeQL, Kali Toolchain, FlareVM Toolchain
- **Operating System:** Linux (Ubuntu), Android
- **Open Source Contributions:** zlog(vulnerability patch), Elixir Core Reference, Havoc (C2) Framework, pwncollege, Hacktoberfest contributor

Education

- **PUCIT, University of the Punjab** *Oct 2019 - July 2023*
  Bachelor of Computer Science Lahore, Pakistan
  - GPA: 3.58/4.00
  - Campus Lead by Google Developer Student Clubs [🌐]
  - President of PUCon23 (National Tech Event by University of the Punjab) [🌐]
- **Punjab Group of Colleges** *Aug 2017 - Oct 2019*
  Intermediate of Computer Science (ICS) Okara, Pakistan
  - Grade: 90.54%
  - Board Topper [🌐]

University Projects

- **Unix Shell]**
  Tools: C, gdb, Makefile, Linux Syscalls []
  - An effort to write the *nix-based shell to gain an understanding of how the shell works and how OS creates and handles processes and allows processes to communicate with each other through its IPC interface
- **Exploit Scripts**
  Tools: C, Python, x86-64 Assembly []
  - Basic scripts that I have written to solve some exploitation challenges
- **Hack Assembler**
  Tools: C++, gdb []
  - A 16-bit machine language assembler for the 16-bit Hack Assembly Language. It was done as part of building a complete 16-bit computer during the Computer Organization Assembly Language Course