CHANDIGARH UNIVERSITY, GHARUAN

Department of Computer Science and Engineering

INTERNSHIP REPORT

Submitted in Partial Fulfilment of the Requirements for the
Degree of
Bachelor of Engineering (B.E.) in Computer Science and Engineering

Internship Program (20 Sep-25 Dec):

Cybersecurity Internship Program – Shentinelix Sphere Pvt Ltd

Task 19 & 20
Introduction to SAN and NAS Storage
, Windows x64 Assembly and Reversing ELF

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This internship focused on exploring three crucial domains of modern computing and cybersecurity — Storage Area Networks (SAN) and Network Attached Storage (NAS), Windows x64 Assembly (Reverse Engineering), and Reversing ELF (Executable and Linkable Format). The training provided a strong foundation in both infrastructure-level concepts like data storage systems and low-level binary analysis essential for software security.

Through this program, I gained hands-on exposure to how enterprise storage systems operate in data centers, how assembly language bridges software and hardware, and how reverse engineering techniques can be applied to dissect executable files. The sessions combined theoretical concepts with practical lab-based learning, enabling me to understand how real-world data communication and binary execution take place.

Overall, the internship offered valuable insight into both infrastructure management and cyber defense mechanisms, significantly enhancing my technical problem-solving, analytical thinking, and system-level debugging skills.

Introduction

The goal of this internship was to develop a deep understanding of three interconnected technological areas: enterprise data storage systems, low-level programming, and reverse engineering techniques. With the increasing importance of cloud computing, cybersecurity, and system optimization, understanding both the software and hardware layers has become essential.

The first module, *Introduction to SAN and NAS Storage*, covered how modern enterprises manage large-scale data efficiently through storage networks. The *Windows x64 Assembly* module explored how applications are executed at the instruction level, providing the foundation for debugging and exploit analysis. Finally, *Reversing ELF* introduced how Linux executables are structured and how they can be analyzed or decompiled for vulnerability assessment.

This combination of storage fundamentals and reverse engineering forms a well-rounded skill set, equipping me to pursue roles in cybersecurity analysis, penetration testing, and system engineering.

Overview of the Company

Shentinelix Sphere Pvt. Ltd. is a cybersecurity training and solutions provider that specializes in delivering practical exposure in information security, penetration testing, and cyber defense.

The company focuses on empowering students and professionals with real-world skills through structured labs, Capture-the-Flag (CTF) style challenges, and guided mentorship.

During the internship, I was assigned to the Cybersecurity Research and Training Department

The organization strongly emphasizes hands-on learning by offering lab environments, curated challenges, and continuous support from experienced security practitioners, ensuring that interns develop both technical competence and a strong research methodology.

Description of Duties

- Learned and configured SAN and NAS storage systems, including setting up CIFS (SMB), NFS, and iSCSI protocols.
- Explored Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) topologies and understood concepts like LUN Masking and Zoning.
- Conducted Windows x64 Assembly analysis using x64dbg and Ghidra to understand the flow of compiled programs at the instruction level.
- Understood registers, stack operations, calling conventions, and control flow in 64-bit assembly.
- Performed ELF (Executable and Linkable Format) reversing using Linux tools like objdump, readelf, and Ghidra.
- Analyzed program headers, sections, and symbol tables in ELF files to understand binary structure
- Documented procedures, findings, and key differences between Windows PE and Linux ELF executable formats.
- Participated in multiple quizzes, lab exercises, and assessments to validate theoretical understanding through practical applications.

Acomplishments

During this internship, I successfully:

- Completed all modules and quizzes with distinction, covering SAN/NAS theory, assembly-level debugging, and ELF analysis.
- Configured a basic SAN setup using simulated NetApp storage and established connections with Windows and Linux clients.
- Used x64dbg to trace program flow, inspect stack values, and analyze memory addresses.
- Identified function boundaries, loops, and conditions in assembly code by analyzing opcodes and call instructions.
- Reversed a Linux ELF binary to retrieve hidden strings, symbols, and execution logic, demonstrating a working understanding of static analysis.
- Developed comprehensive documentation that bridges storage architecture and cybersecurity, highlighting how data storage can be both optimized and protected from vulnerabilities.

- Strengthened my analytical reasoning by interpreting how compilers translate high-level code into assembly and machine code.

Skills Learned

- **Technical Skills:**
    - Deep understanding of **SAN, NAS, RAID, iSCSI, FCoE, and Fibre Channel** technologies.
    - Practical experience with **x64 Assembly**, including registers (RAX, RBX, RSP, RBP) and **stack management**.
    - Proficiency in using **Ghidra**, **x64dbg**, and **SysInternals** for reverse engineering and debugging tasks.
    - Knowledge of **ELF file internals**, including segments, sections, and linkage between compiled components.
    - Understanding of **data communication protocols** and **binary execution models** in both Windows and Linux.
- **Soft Skills:**
    - Improved **problem-solving** and **analytical thinking** through binary dissection tasks.
    - Enhanced **documentation** and **technical reporting** abilities.
    - Strengthened **time management** and **adaptability** while handling complex technical modules.

Challenges Faced

One of the main challenges was grasping the **complexity of assembly language syntax** and the compiler optimizations that make disassembled code difficult to interpret. Understanding how compilers handle loops, conditionals, and function calls required patience and practice. Another challenge was setting up **SAN/NAS environments** virtually and troubleshooting connectivity issues between client and storage systems. Configuring proper access controls and understanding LUN masking took several attempts before achieving stable connections. In the *Reversing ELF* section, analyzing stripped binaries (with missing symbols) was difficult, as it required understanding program behavior through pure control flow and pattern recognition. However, with persistence, I learned to use tools like strings, readelf, and objdump effectively to extract meaningful insights.

Conclusion

This internship provided an excellent balance between infrastructure-oriented knowledge and security-level technical depth. Learning SAN and NAS fundamentals helped me understand enterprise data management and cloud storage integration, while Windows x64 Assembly and Reversing ELF deepened my understanding of how programs operate at their lowest levels. Through this training, I gained the ability to analyze, configure, and secure systems across both the hardware and software spectrum. I am now more confident in approaching complex cybersecurity challenges, from identifying vulnerabilities in compiled software to ensuring secure and efficient data storage.

Overall, this internship served as a major step forward in my journey toward becoming a proficient cybersecurity professional and reverse engineer.

Acknowledgments

I would like to thank the team at Shentinelix Sphere Pvt. Ltd. for providing access to lab environments, learning resources, and a supportive environment that encouraged practical learning and skill development. Special thanks to the TryHackMe platform and the authors of the Research Methodology room for providing structured, hands-on lessons that significantly enhanced my research and problem- solving skills. Finally, I extend my gratitude to my peers and family for their continuous support and encouragement throughout the internship period.