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 24

History of Malware, Malware Intro, Basic Malware RE, Malware Researching

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This report combines insights from four TryHackMe modules—History of Malware, MAL: Malware Introductory, Basic Malware Reverse Engineering, and MAL: Researching—to present a holistic understanding of malware evolution, structure, analysis techniques, and research methodologies.

The journey begins with the early days of self-replicating programs like Creeper and moves through modern threats involving complex obfuscation, payload delivery, and stealth mechanisms. These modules collectively explore malware behavior, static and dynamic analysis, reverse engineering fundamentals, and the importance of cryptographic checksums in malware research.

Through practical labs and theoretical understanding, I developed critical analytical and investigative skills—learning not just what malware does, but how it operates, hides, and can be countered. This comprehensive study bridges the gap between historical knowledge and modern defensive analysis, preparing me for deeper malware research and incident response work.

Introduction

Malware, short for *malicious software*, has evolved from simple experiments into sophisticated cyber weapons. The study of malware is essential for cybersecurity professionals to understand threat actor tactics, analyze malicious payloads, and prevent large-scale compromises.

This combined TryHackMe learning path begins with the **origins of malware**—where programs like *Creeper* and *Elk Cloner* laid the groundwork for replication and infection concepts—and extends into **modern malware analysis**, including static inspection, reverse engineering, and checksum-based verification

By analyzing these stages, I gained a deeper appreciation for how threats matured alongside technological progress. This progression highlights why **malware analysis** remains a vital discipline within incident response, digital forensics, and threat intelligence.

Overview of the Company

TryHackMe provides an interactive cybersecurity learning environment where users gain real-world experience through guided labs, simulations, and challenges. In these rooms, I worked within sandboxed environments to safely analyze malware samples, generate checksums, identify obfuscation, and study their internal logic.

Each room followed a structured approach:

- **History of Malware** — Historical foundation and evolution of malicious software.
- **MAL: Malware Introductory** — Introduction to analysis techniques, campaign understanding, and detection methods.

- **Basic Malware RE** — Static reverse engineering to extract intelligence without executing the malware.
- **MAL: Researching** — Using checksums, online sandboxing tools, and public threat databases (e.g., VirusTotal).

TryHackMe's practical focus made it possible to apply both theoretical and investigative knowledge directly, which is crucial for future malware analysts and security researchers.

Description of Duties

Throughout this learning sequence, I engaged in the following activities:

- **Historical Analysis:** Studied early malware such as *Creeper, Elk Cloner, and Morris Worm* to understand original propagation methods.
- **Malware Campaign Assessment:** Investigated real-world infection vectors (spam attachments, trojans, backdoors).
- **Static Analysis:** Used techniques like *string analysis* and *import table inspection* to extract information without execution.
- **Checksum Generation:** Calculated MD5/SHA256 values to verify integrity and identify samples on VirusTotal.
- **Sandbox Research:** Uploaded samples to online sandboxes to observe behavioral indicators safely.
- **Obfuscation Identification:** Differentiated between packed and unpacked binaries to detect attempts at hiding malicious intent.

These tasks collectively built a foundation in malware reverse engineering and defensive research methodology.

Acomplishments

 Learned how early malware shaped today's threat landscape and the evolution from harmless experiments to cyber weapons.
 Gained proficiency in **static analysis tools and techniques**—identifying imports, strings, and sections within executable files.
 Successfully used **checksums** for malware identification, integrity verification, and community correlation via online platforms.
 Understood **obfuscation and packing** methods and their impact on antivirus evasion.
 Performed **safe sandbox investigations** to record malicious process behavior, registry modifications, and network calls.
 Developed the ability to **differentiate malware types** such as worms, trojans, viruses, and rootkits through behavior-based classification.

Skills Learned

Technical Skills:

- Static and basic dynamic malware analysis.

- Reverse engineering fundamentals (string and import analysis).
- Use of checksum and hash algorithms for malware tracking.
- Familiarity with online analysis tools like VirusTotal, Hybrid Analysis, and Any.Run.
- Recognition of obfuscation techniques and packed executables.

Analytical Skills:

- Tracing malware execution flow conceptually without direct execution.
- Correlating behavior patterns to malware families and indicators of compromise (IOCs).
- Evaluating attack campaigns and mapping infection chains.

Soft Skills:

- Improved technical reporting and incident documentation.
- Developed systematic problem-solving and research-oriented thinking.

Challenges Faced

- **Obfuscation Complexity:** Identifying packed binaries without execution was challenging since many samples hid imports or strings.
- **Checksum Collisions:** Understanding how similar files can produce different hashes due to even minor changes required careful verification.
- **Static Analysis Limitations:** Without dynamic testing, certain behaviors remained theoretical, demanding strong inference skills.
- **Data Overload:** Differentiating relevant strings or imports from benign noise needed patience and practice.

Despite these challenges, step-by-step practice within isolated environments enhanced my precision, caution, and analytical maturity.

Conclusion

The combined experience from these four modules provided a comprehensive understanding of malware—its origins, evolution, and analytical breakdown. I now grasp the historical foundation, behavioral mechanisms, and analytical procedures required for malware research.

From the Creeper program to modern packed binaries, malware has continuously evolved, adapting to technology and detection methods. Understanding this evolution empowers cybersecurity professionals to design better detection systems and response strategies.

Through these TryHackMe exercises, I have strengthened my investigative mindset and developed foundational skills necessary for future specialization in **malware reverse engineering, digital forensics, and threat hunting**.

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.