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 21
Snort

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

The TryHackMe “Snort” room provided an in-depth, hands-on experience with the Snort Intrusion Detection and Prevention System (IDS/IPS). The primary objective was to understand how Snort monitors network traffic, detects malicious activities, and generates alerts based on user-defined or pre-existing rules. Through this module, I explored different operational modes of Snort, such as sniffer mode, packet logger mode, and intrusion detection mode, along with rule creation and PCAP analysis.

The room offered a practical and interactive learning environment that simulated real-world cybersecurity monitoring tasks. It enhanced my understanding of how IDS/IPS systems play a crucial role in defending networks against attacks. Completing this module strengthened both my analytical and technical abilities to detect and respond to network-based threats efficiently.

Introduction

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential components of modern cybersecurity. They continuously monitor network traffic to detect unauthorized access, malicious activity, and policy violations. The TryHackMe Snort room serves as an introductory yet comprehensive guide to mastering Snort — one of the most widely used open-source IDS/IPS solutions maintained by Cisco Talos.

The room aimed to provide both theoretical and practical knowledge, helping learners to not only understand how Snort operates but also gain hands-on experience with real-time threat detection and packet analysis. Through guided exercises and interactive labs, I learned how to interpret alerts, write custom detection rules, and use Snort to analyse both live and recorded network data.

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

My primary role during the Snort training module was to complete all the assigned practical tasks and exercises while understanding how each component of Snort operates. This involved learning command-line operations for launching Snort in various modes, analyzing packet captures (PCAP files), and writing custom IDS rules to detect specific traffic patterns.

Additionally, I was responsible for documenting each step of the lab exercises, noting down observed alerts, rule matches, and anomalies detected during the analysis. I also explored Snort’s configuration files, rule syntax, and alert output to gain a complete understanding of its operation logic. This structured approach helped me bridge the gap between theoretical cybersecurity knowledge and real-time intrusion detection techniques.

Acomplishments

By completing this TryHackMe room, I successfully gained a foundational and practical understanding of how network intrusion detection systems function. I learned how to deploy Snort in different operational modes to monitor live traffic, log packets for later analysis, and actively detect intrusions based on defined rules.

One of my key accomplishments was writing and testing custom Snort rules capable of identifying suspicious packets and malicious behavior within simulated traffic. I also analyzed PCAP files to identify anomalies and practiced interpreting Snort alerts. Completing this module with 100% progress demonstrated my ability to apply cybersecurity tools effectively in both simulated and practical scenarios.

Skills Learned

Throughout the training, I developed several technical and analytical skills essential for network security monitoring. These include:

- **Snort Configuration and Usage:** Understanding operational modes such as Sniffer, Packet Logger, IDS/IPS, and PCAP Investigation.
- **Rule Writing and Analysis:** Crafting Snort rules to detect various attack signatures and recognizing malicious network patterns.
- **Network Traffic Analysis:** Interpreting network protocols, packet headers, and alert messages to identify anomalies.
- **Linux Proficiency:** Enhancing command-line navigation, file management, and system configuration skills while working within Snort’s environment.

In addition to technical growth, I improved my problem-solving, attention-to-detail, and documentation skills, which are vital for cybersecurity professionals handling live threat data.

Challenges Faced

One of the primary challenges encountered was understanding Snort’s rule syntax and operational modes. Initially, the configuration files and complex parameters were difficult to interpret. However, with continuous practice and referencing the TryHackMe learning materials, I became more comfortable with writing and modifying detection rules.

Another challenge was analyzing large volumes of packet data efficiently. Identifying relevant alerts among numerous log entries required patience, critical thinking, and familiarity with network protocols. Overcoming these difficulties enhanced my ability to manage real-world intrusion detection systems and improved my overall analytical capabilities.

Conclusion

The TryHackMe Snort module provided a valuable learning experience in network intrusion detection and prevention. It offered practical, hands-on exposure to one of the most important open-source tools used by cybersecurity professionals worldwide. Through this module, I developed a deeper understanding of how threats are detected, analyzed, and mitigated using rule-based systems.

Completing this room not only strengthened my technical skills in network monitoring and security analysis but also increased my confidence in working with enterprise-level cybersecurity tools. This experience marks a significant step toward becoming a proficient Blue Team analyst capable of identifying and responding to cyber threats in real time.

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.