INTRODUCTION TO COMPUTER SECURITY-5550

PROJECT PLAN FOR RANSOMWARE RESEARCH AND MITIGATION

Team Mates: -

Pooja Peechara :11663887

Rachana Reddy Sunki :11709719

Mounika Nuchu :11653658

Lagadapati Kondarao :11661743

Yenugu Ruthiksha Reddy :11714976

- The following memo outlines the project plan for the study of ransomware attacks and the development of mitigation techniques, as per the provided guidelines. The memo was made after meticulously researching ransomware techniques.
- The literature survey included in-depth exploration of various ransomware variants, including CryptoWall, Petya and Mischa, Locky, Cerber, and WannaCry. The main focus is on their propagation methods, encryption

techniques, distribution channels, and impact on victims. In addition, the research examined case studies and research papers to understand evolving ransomware trends.

- In preparation for the project, specific components will be outlined. For the encryption and decryption aspect, Python will be used to develop the functionality. Cryptography libraries like PyCryptodome and AES encryption algorithms will be used because they are secure and efficient.
- On infection methods, the project will simulate real-world scenarios by implementing a phishing email campaign. This campaign will illustrate how ransomware infiltrates systems, emphasizing social engineering tactics and the importance of user awareness and security best practices.
- For monitoring, the approach will involve deploying OSSEC for real-time monitoring and configuring file integrity checks to detect unauthorized changes in the directory. Monitored data will be systematically logged into a structured database for analysis and forensic purposes.
- In terms of detection, the project will implement custom rules based on file access patterns and behavior analysis. Additionally, it will leverage machine learning algorithms such as clustering and anomaly detection to identify ransomware activities. Integration of YARA rules will help in detecting specific ransomware signatures and patterns.

- To mitigate ransomware attacks, the project will implement automated response mechanisms to isolate infected systems and block malicious processes promptly.. Furthermore, the project will explore network segmentation and access controls to contain ransomware outbreaks and limit lateral movement. The project plan provides detailed information on how the ransomware will be implemented and mitigated.