Group 7

Step 1: Research on Ransomware Techniques

Team Members:-

1. **Vamshi Krishna Bukka - 11693102 - vamshikrishnabukka@my.unt.edu**
2. **Sivabhavana Nelluri - 11702191 - sivabhavananelluri@my.unt.edu**
3. **Nithish Kumar Boggula -** 11559328 - nithishKumarBoggula@my.unt.edu
4. **Revanth Boddupalli - 11718089 - revanthBoddupalli@my.unt.edu**
5. **Vikram Reddy Allam - 11697684 - vikramallam@my.unt.edu**

Overview:-

The creation of file encryption ransomware is the main goal of this project, which will be studied and cybersecurity measures will then be implemented. Our project plan is below, including the techniques we will use at each stage.

1. Research on Ransomware Techniques:
   a. File Encryption Ransomware is the ransomware technique that we have selected. Typically, user files encrypted by this kind of ransomware demand payment to unlock or decrypt.
   b. This kind of ransomware encrypts some files on a computer, then demands money for the decryption key. It looks for important files, breaks into systems using a variety of methods, then encrypts data to render it unreadable using encryption. After being informed of the encryption, the victim is demanded to pay a ransom in order to receive the decryption key.

2. Action:-
   a. We will be using Python scripting language for encryption .
   b. PyCryptodome is a cryptographic library.
   c. For encryption we will utilize the AES encryption method.

3. Infection:-
    a. A malicious executable attachment will be used as the infection mechanism in a phishing email attack.

4. Monitoring:-
    a. We will utilize OSSEC Host IDS for file integrity monitoring. We will create a monitoring component to identify ransomware activity on the victims computer. (Will try to implement logging if possible)

5. Detection:-
    a. We will lay out the rules for file operations, outlining what can and cannot be done.
    b. We will make rules to identify policy violations, particularly when they point to the possibility of ransomware activity.

6. Mitigation:-
    a. When ransomware is discovered, we will take countermeasures and implement a defense-in-depth strategy that may involve stopping or eliminating the ransomware process.

Every team member made a significant contribution, ensuring complete participation and cooperation throughout the task.