**Lab 3: Ransomware**

**Objectives:**

* **To understand the thought process of an attacker and victim when dealing with ransomware.**
* **To use two machines to simulate a ransomware attack and its consequences.**
* **To identify preventive measures that could have been taken to avoid a ransomware attack.**

**Equipment:**

* Two virtual machines running on a host computer, such as VirtualBox or VMware
* A Ransomware program from Moriarty Matrix
* Basic knowledge of networking and Linux command line

**Steps:**

* Reconnaissance: Explain what reconnaissance means in the context of a cyber attack, and provide specific instructions on how to do it in this lab exercise.
* Phishing email: Provide specific instructions on how to create a phishing email that will serve as the attack vector for the ransomware.
* Victim VM: Explain what a Victim VM is and how it will be used in the lab exercise.
* Download and run ransomware: Explain how to download and run the ransomware on the Victim VM.
* Observe consequences: Provide instructions on how to observe and document the consequences of the ransomware attack, such as the inability to modify files.
* Send key to unlock files: Explain how to send the key to unlock the files, which will allow the Victim VM to regain access to their data.
* Prevention measures: Finally, instruct the students to write about the preventive measures that could have been taken to avoid a ransomware attack from the victim side.

**Rubric:**

* + Reconnaissance: Did the student demonstrate an understanding of reconnaissance techniques and effectively implement them in the lab exercise?
  + Phishing email: Did the student create a convincing phishing email that would effectively serve as the attack vector for the ransomware?
  + Victim VM: Did the student effectively use the Victim VM and follow the instructions for running the ransomware?
  + Consequences: Did the student effectively observe and document the consequences of the ransomware attack, such as the inability to modify files?
  + Key: Did the student successfully send the key to unlock the files and restore access to the data?
  + Prevention measures: Did the student effectively identify and explain preventive measures that could have been taken to avoid a ransomware attack from the victim side?
  + Overall: Overall, did the student demonstrate a thorough understanding of the objectives of the lab exercise and effectively complete all steps and requirements?