Group – 3

Step - 3

Memo: Proposed Infection Method

Subject: Implementation of Malicious PDF Exploit for Victim Infection

Objective: The purpose of this method of infection is to find a way to infect a victim's system using the vulnerability in commonly used software (PDF readers) for the purpose of delivering malicious payload.

Infection Method:
To do that, we will create a malicious PDF that, when opened, will utilize known exploits in outdated PDF readers, including Adobe Acrobat Reader. This means it will be a 'zero click' infection method, i.e., the user does not need to interact with anything beyond opening the PDF.

Steps:

1. **Creation of Malicious PDF**:
    - Use an already existing exploit framework (e.g. Metasploit) to do your malicious PDF. In other words, this PDF will be constructed to hold a payload (like a reverse shell or trojan) which exploits some vulnerability in the victim's PDF reader.
    - The PDF will contain embedded JavaScript or exploit code, that executes the payload when the file is opened.
2. **Distribution of Malicious PDF**:
    - Once Metasploit had successfully created the malicious PDF, the following step was to send it to the target PC. We used SCP (Secure Copy Protocol) to transmit files directly. SCP was chosen for its safe and encrypted file transfers over SSH. It enables dependable delivery without requiring user intervention. It enables controlled testing in a secure environment with no external dependencies.
3. **Execution of Malicious Payload**:
    - If the victim opens the PDF, the exploit code will load, downloading and executing the payload on the machine.
    - The payload can act, by being designed, to open a backdoor for remote access or to steal sensitive information, for instance.
4. **Post-Infection Actions**:
    - If after executing successfully, the malware will establish connection with an attacker-controlled server and the attacker will be able to control the victim's machine.
    - With this access, the attacker can; perform reconnaissance, move laterally within the network or take data off.

Tools:

- **Metasploit Framework** for generating the exploit.
- **PDF Exploit Scripts** (or other relevant scripts) to craft the malicious PDF.

Security Measures:

For the simulation of the real-world scenario, the infected victim should have the vulnerable outdated PDF reader version. However, I want to point out that this attack would not work on up-to-date PDF readers or in systems with their security settings (like disabling JavaScript in PDFs) properly set.

Conclusion: This method demonstrates how trivial and straightforward it is to abuse software vulnerabilities, quintessence combined with social engineering. We introduce a tool to realize such an infection approach by using Metasploit and a PDF file on the specific technical vulnerabilities and human error, which can be powerful attack vector.