Group – 3

Step 4: Monitoring

Memo: Monitoring Stage for Malicious PDF Exploit

Subject: Monitoring File Changes for Malicious PDF Exploit

Objective:

The purpose of monitoring during this stage involves tracking changes made through the malicious PDF exploit. Our system observes modifications to all files in the critical directory that occur through the execution or altering of the malicious PDF.

Overview:

During this stage the malicious PDF created through Metasploit exploitation of old PDF reader vulnerabilities (such as Adobe Reader) will be monitored. An opened file by a susceptible system will activate the programmed payload which produces remote system access for cyber attackers.

Monitoring Setup: During this stage the malicious PDF created through Metasploit exploitation of old PDF reader vulnerabilities (such as Adobe Reader) will be monitored. An opened file by a susceptible system will activate the programmed payload which produces remote system access for cyber attackers.

Creation: When the malicious PDF is copied or downloaded to the target system.

- **Modification**: When the file is opened or altered by the exploit.

- **Deletion**: If the malicious PDF is deleted after execution.

The script output will look like the following:

```
bash
Copy
Change detected: malicious.pdf in /home/kali/Desktop/critical/ with action
CREATE
```

This ensures that any interaction with the malicious PDF is logged and can be monitored in real-time.

Execution of the Malicious PDF: When the target directory contains the malicious PDF it becomes vulnerable to execution from an open PDF reader. A continuous script-based monitoring system maintains real-time logs whenever the following events occur. The system creates files whenever the malicious PDF enters the system during the introduction process. Such monitoring includes both the opening and execution of PDF files that will trigger the payload (file modification). The file deletion occurs following successful completion of the attack when the attacker's system access becomes confirmed.**Next Steps**:

1. **Test the Exploit**:

- ❖ Copy the malicious.pdf to the critical directory.
- ❖ Enable automated file logging service through the monitoring script.
- ❖ Check for logged changes inside vulnerable systems after opening a malicious PDF file.

2. **Review Monitoring Logs**:

An analysis of the terminal output from the monitoring script helps monitor how the exploit executes. The monitoring script output shows whether the PDF triggering the payload event thus confirming all execution activities.

Conclusion: Security assessments during the monitoring phase reveal the conduct of malicious PDFs as they affect a vulnerable system. The observation of file system changes allows us to monitor exploit actions along with system response patterns for appropriate system behavior. The phase captures crucial information required to evaluate the damaging effects of an attacker's PDF on targeted systems since it constitutes an important element for understanding vulnerabilities in ethical hacking research towards better defense practice.