Standard Operation Procedure(SOP)

Team Hex

Objective

The objective is to understand and combat malware threats effectively. Through a combination of analyzing malware behavior and system activities, using tools like PEiD, Process Monitor, and Wireshark, we aim to strengthen cybersecurity defenses. By dissecting malicious code and network traffic, we protect computer systems from harm, ensuring a secure digital environment for users.

Tools Required:

1.Virtual Environment Setup:

- VirtualBox

2.Operating Systems:

- Kali Linux

- Windows 7
- Windows 10

3.Static Testing Software:

- Dependency Walker
- PEiD
- PEview
- Sysinternals Suite

4.Dynamic Testing Software:

- Regshot
- Process Monitor
- Process Explorer
- Process Hacker
- Apache DNS
- InetSim
- Reverse Engineering Software
- Ollydbg
- Wireshark

Procedure

1. **Download VirtualBox:** Go to the VirtualBox website, download the software, and follow the installation steps.
2. **Install Operating Systems:** Download Kali Linux, Windows 7, and Windows 10 ISO files from their respective websites. Install them on VirtualBox by creating new virtual machines and configuring settings.
3. **Install Required Software:** Download tools like Dependency Walker, PEiD, Sysinternals Suite, Regshot, Process Monitor, Process Explorer, and Apache DNS. Follow the provided links and instructions for installation.
4. **Start Virtual Machines:** Launch the virtual machines for the installed operating systems.
5. **Analyze Malware:** If your computer is infected with malware, disconnect it from the network and submit it for analysis. Malware analysts will investigate the issue using a combination of static and dynamic analysis tools.
6. **Stay Safe:** Learn about different types of malware, such as viruses, worms, Trojans, and ransomware, and how they spread. Use security best practices to protect your computer from future malware attacks.

Reporting

Malware, harmful software, can infect computers through emails, websites, or USB drives. Tools like PEiD and Process Monitor help detect malware by analyzing files and system activities. Malware comes in types like viruses and trojans, aiming to steal data or cause damage. Using tools like OllyDbg and Wireshark, experts can understand and stop malware, protecting computers from harm.

Conclusion

Understanding malware is crucial as it can harm computers and steal information. Tools like PEiD, Process Monitor, and Wireshark help analyze malware. Malware, like viruses and ransomware, spreads through emails and infected websites. Analyzing malware involves studying its code and behavior. By using these tools, we can understand how malware works and protect our computers better.