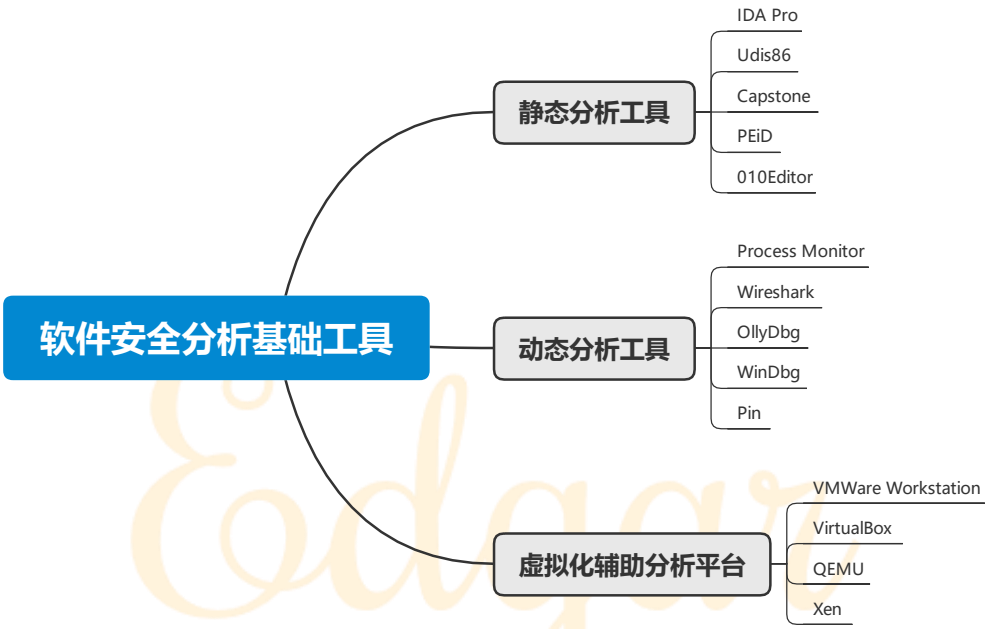
第三章 软件安全分析基础工具

一. 章节主要内容



二. 详细内容

3.1 静态分析工具

3.1.1 IDA Pro

✓ 常用功能:

✧ 反汇编功能

✧ 反编译功能

- ✧ 导入表与导出表解析功能
- ✧ 函数符号表功能
- ✧ 查找功能
- ✧ 插件功能

3.1.2 Udis86

- ✓ Udis86 提供一套反汇编的第三方库，用户可自行编写代码进行扩展
- ✓ Udcli 是基于 Udis86 的反汇编工具，可通过命令行实现反汇编

3.1.3 Capstone

Capstone 基于 C 语言开发，提供 C/C++、Python、Java、Perl 等接口，具备开放接口好、轻量级、性能高等特点，是一款多平台、多架构的反汇编框架

3.1.4 PEiD

- ✓ 常用功能：
  - ✧ PE 格式信息提取功能
  - ✧ 插件扩展与脱壳功能(需辅助插件)

3.1.5 010Editor

✓ 常用功能：

- ✧ 文件编辑功能
- ✧ 范本分析功能
- ✧ 脚本分析功能
- ✧ 磁盘编辑功能
- ✧ 进程内存编辑功能

3.2 动态分析工具

3.2.1 Process Monitor

✓ 常用功能：

- ✧ 进程监控功能
- ✧ 文件监控功能
- ✧ 注册表监控
- ✧ 网络监控

3.2.2 Wireshark

✓ 常用功能：

- ✧ 流量采集功能
- ✧ 协议分析功能

3.2.3 OllyDbg

- ✓ 常用功能：
  - ✧ 调试功能
  - ✧ Trace 功能

3.2.4 WinDbg

- ✓ 常用功能：
  - ✧ 符号功能
  - ✧ 调试功能
  - ✧ 命令：
    - ❑ 反汇编
    - ❑ 内存编辑
    - ❑ 内存搜索
    - ❑ 断点设置
    - ❑ 符号表加载
  - ✧ 内核调试

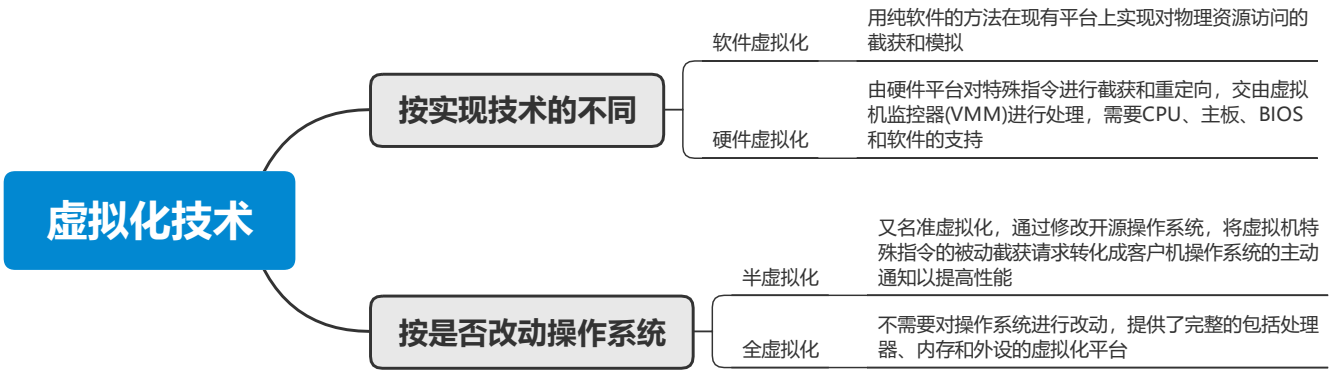
3.2.5 Pin

Pin 是一款二进制代码插桩分析框架，提供四种粒度的代码插桩模式：INS 级别、TRACE 级别、RTN 级别和 IMG 级别

类似的插桩工具有：Valgrind, DynamoRIO。

3.3 虚拟化辅助分析平台

虚拟化具有兼容性、隔离的优良特征，在恶意代码与漏洞分析过程中国经常使用虚拟化平台进行辅助分析



3.3.1 VMWare Workstation

✓ 主要功能：

- ✧ 虚拟机管理
- ✧ 数据交互
- ✧ 快照功能
- ✧ 内核调试

3.3.2 VirtualBox

与 VMWare Workstation 类似

3.3.3 QEMU

✓ 主要功能：

- ✧ 虚拟机的维护管理
- ✧ 数据交互
- ✧ 基于 QEMU 的扩展平台

3.3.4 Xen

Xen 坏境由两个组成部分：虚拟机监控器；虚拟机

运行在 Xen 上的虚拟机通常被称为 domain，可以有多台，但是有一个管理者 domain0，其他的虚拟机 domainU 需要 domain0 的协助