软件安全入门

第三课 软件安全分析基础工具

目录
CONTENTS

主要内容包括常见的逆向反汇编工具IDA Pro、文本格式分析编辑工具PEiD、010Editor的介绍。

IDA Pro是一款交互式的反汇编工具，支持Windows、Linux、Mac OS等主流操作系统平台；支持Intel x86/x64、ARM、MIPS等数十种指令集的反汇编；支持exe、dll、elf、so、dex等文件类型程序的分析，被广泛应用于程序的静态分析。

□**反汇编功能**：IDA最基本的功能，将机器码转化为汇编语言代码。

□**反编译功能**：将汇编代码反编译成C/C++等高级语言代码。

□**导入表与导出表解析功能**：提取导入表的地址、函数名、动态库名等参数和导出表的地址、函数名等参数。

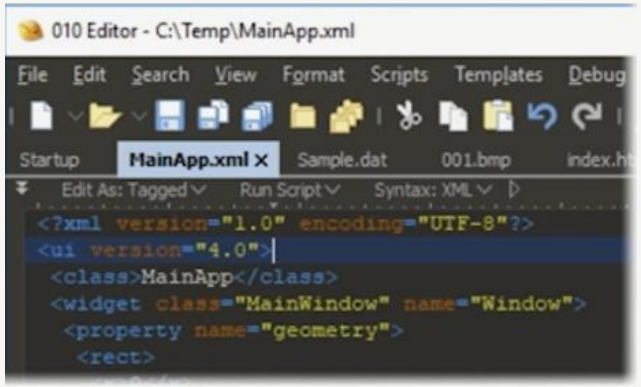
PEiD是Windows平台下常用的PE文件格式分析工具，用于提取exe、dll、sys等标准可执行程序的文件结构，也常用于检测程序加壳。但PEiD目前已停止更新，只支持32位程序，无法解析64位PE文件。

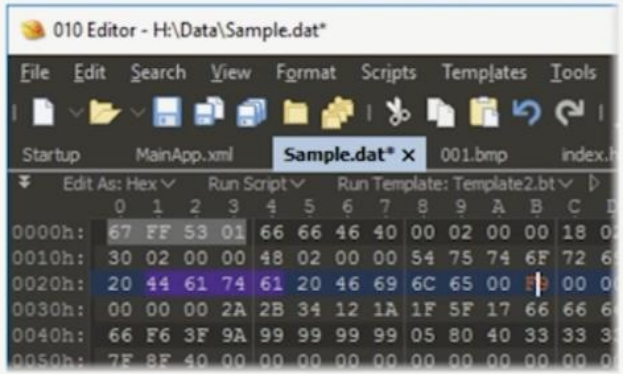
□ PE格式信息提取功能：PEiD最主要的功能，用于提取PE文件的程序入口点、EP节信息、连接器版本信息、子系统类型等。

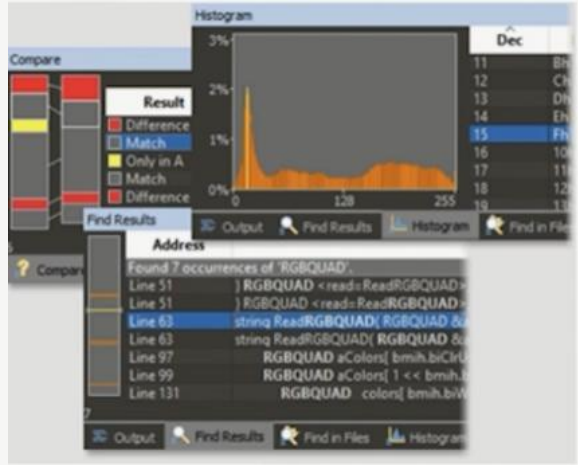
□插件扩展与脱壳处理：PEiD支持470种加壳特征信息的识别，支持数十种插件扩展，通过插件实现脱壳、修复CRC校验等功能。

010Editor是SweetScape公司推出的一款商业付费编辑器软件，支持32位和64位的Windows、Linux、Mac OS操作系统平台。

010Editor是一款功能齐全的文本编辑器，不仅支持文本文件和二进制文件的编辑，还具备磁盘编辑、进程内存编辑的能力，以及文件格式的范本分析，支持脚本分析等功能。







主要内容包括常见的外部观测类工具ProcessMonitor、Wireshark,常见的调试跟踪类工具OllyDbg等。

Process Monitor是一款Windows平台下的进程监控工具，主要用于进程行为监控与记录，包括文件操作行为、注册表操作行为、网络行为等。

□**进程监控功能**：用报表的形式列出了系统运行过和正在运行的进程，并以父子关系的进程树形式进行展示。

□**文件监控功能**：能够监控文件的打开、读、写、关闭等操作，同时获取操作是否成功的状态、文件路径、读写偏移量等参数。

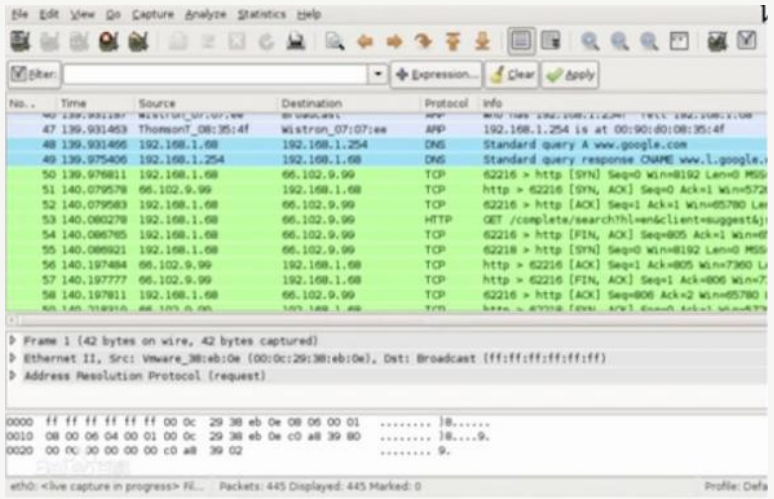
□**注册表监控**：能够监控注册表的创建、打开、读、写、关闭等操作，以及操作是否成功的状态、注册表路径等

□**网络监控**：能够监控网络数据的发送与接收操作、协议类型，获取操作的进程名、PID、是否成功的状态、连接方、口、报文长度等参数。

Wireshark是一款开源的网络数据包采集与分析软件，具备数据包采集的数据报文协议解析的能力，支持32位和64位的Windows、Linux、Mac OS操作系统。

□**流量采集功能**：可以设置要采集的网卡、过滤规则，也可以指定协议、IP地址、端口号等，还支持逻辑符号组合。

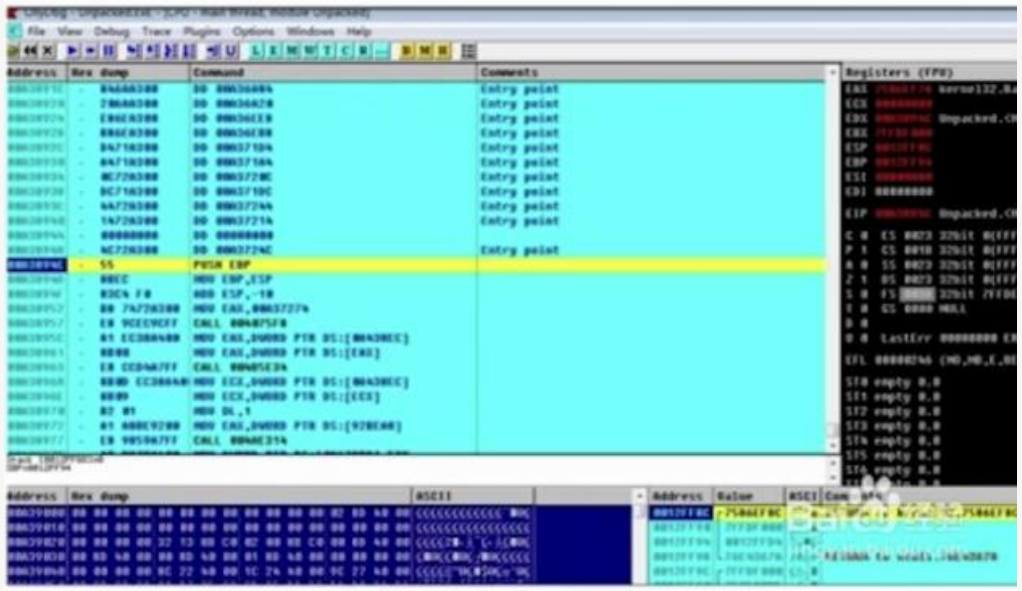
□**协议分析功能**：可以分析实时采集的数据，也可以分析离线存储的数据包。支持网络层的IP、IPv6,传输层的TCP、UDP、应用层的HTTP、FTP等协议。



OllyDbg是一款Windows平台反汇编动态调试追踪工具，只支持Ring3级别的用户态程序。

□**调试功能**：可启动新进程进行调试或附加到运行中的进程进行调试。在调试过程中能够提供指令、内存、寄存器、栈等基本信息。

□**Trace功能**：记录调试过程中执行的指令，用于分析前序执行指令。



主要内容包括支持硬件虚拟化技术的软件VMWare和纯软件虚拟化工具QEMU。

VMWare Workstation是一款常见的桌面虚拟化软件，支持在32位和64位的Windows、Linux、Mac OS平台上运行，支持虚拟Windows、Ubuntu、CentOS等多个版本的操作系统。

- **虚拟机管理**：包括虚拟机创建、安装、运行、管理。
- **数据交互**：指物理主机与虚拟机之间的数据双向传输，包括数据传入虚拟机和从虚拟机传出。
- **快照功能**：通过快照管理功能备份安装了不同软件或者同一软件不同版本的分析环境。
- **内核调试功能**：结合WinDbg可进行内核驱动调试。

QEMU是一款开源的虚拟化平台，通过自身的指令翻译模块模拟程序的执行。

支持x86、AMD64、MIPS、ARM等架构，可扩展和自定义新的指令集。作为模拟器时，可以在一种架构下运行另一种架构下的操作系统和程序。

作为虚拟机时，可进行虚拟机的维护管理，支持平台扩展：

□**虚拟机的维护管理**：QEMU以命令行的方式对虚拟机进行创建、维护和管理。

□**数据交互**：使用过程较为复杂，将物理主机文件复制到QEMU虚拟机内部的方法是将文件制作成iso,然后通过光盘加载到虚拟机。

课程小结

·1.静态分析工具

·主要内容包括：逆向反汇编工具IDA Pro、文本格式分析编辑工具PEiD、010Editor。

· 2.动态分析工具

·主要内容包括：常见的外部观测类工具ProcessMonitor、Wireshark,常见的调试跟踪类工具OllyDbg等。

·3.虚拟化辅助分析工具

·主要内容包括：支持硬件虚拟化技术的软件VMWare和纯软件虚拟化工具QEMU。

谢谢观赏