ISCAS 中国科学院软件研究所学术年会’2021
暨计算机科学国家重点实验室开放周

工具系统

# 二进制软件漏洞机理分析系统

闫佳、苏璞睿、黄桦烽、和亮、贾相堃

联系方式：闫佳、13426264127、yanjia@iscas.ac.cn

## 系统简介

二进制软件漏洞机理分析系统以硬件模拟技术为基础，构建完全可控的虚拟执行环境，实现漏洞利用攻击样本的自动化动态分析和交互式机理分析，该系统支持Office、Chrome、操作系统内核等大型软件系统的漏洞利用攻击样本的利用要素和代码特征抽取，支撑软件漏洞攻击检测和防御能力构建

## 典型分析流程

**漏洞样本分析环境构建和验证**

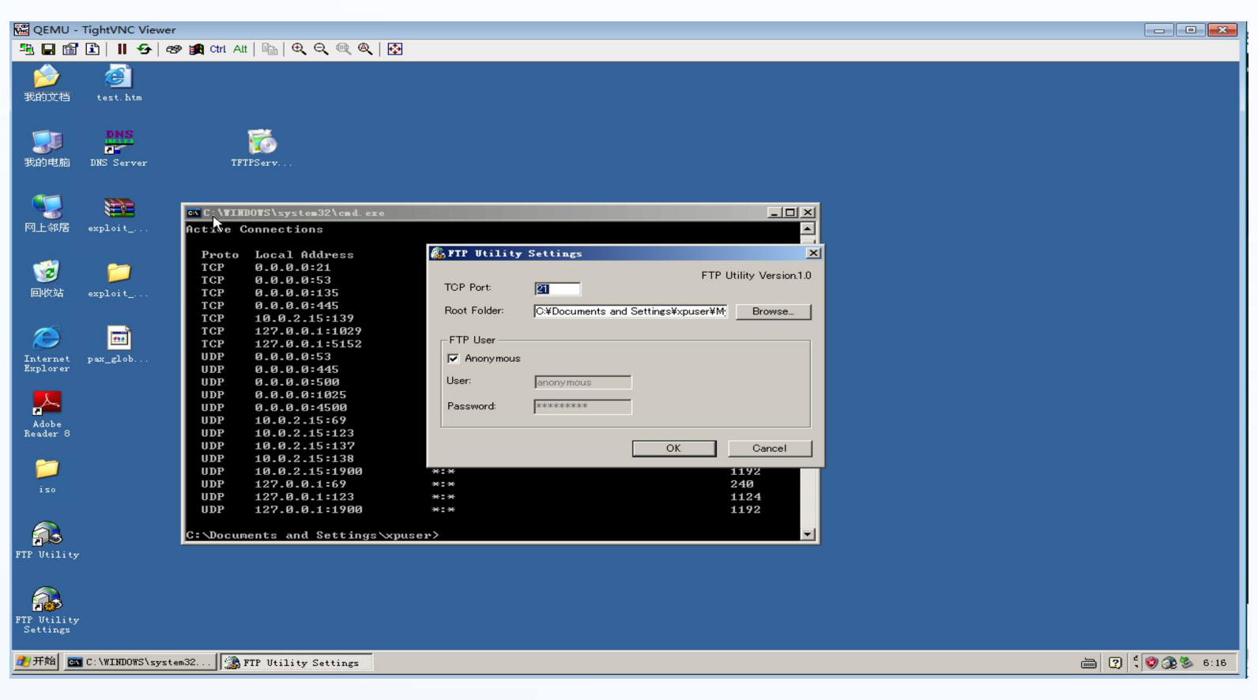
- 创建镜像
- 创建快照
- 漏洞利用行为验证

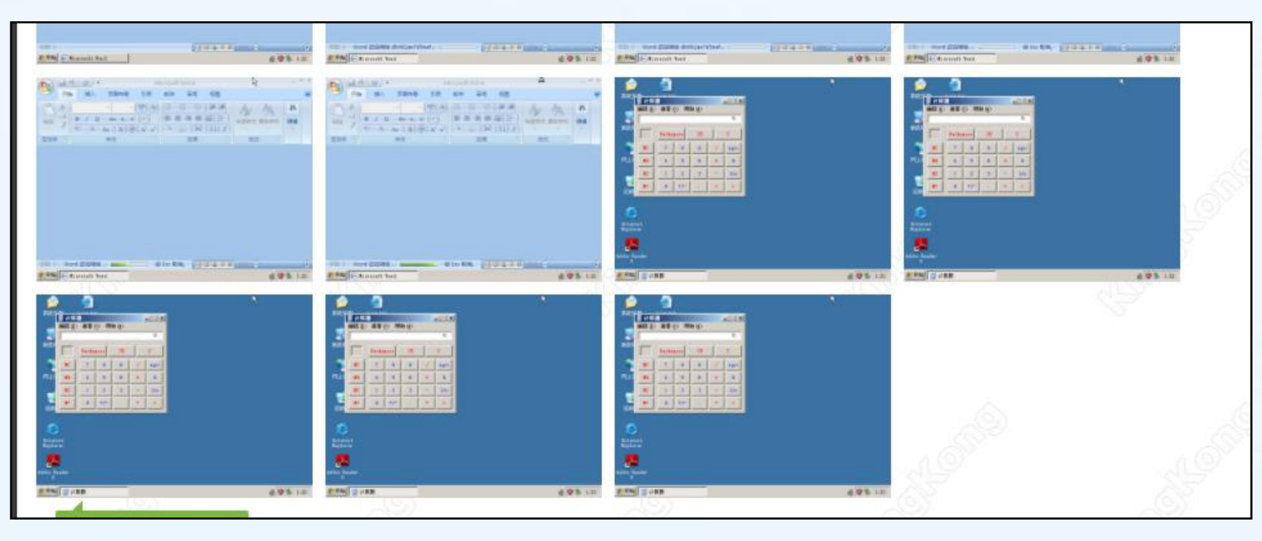
**漏洞利用样本动态机理分析**

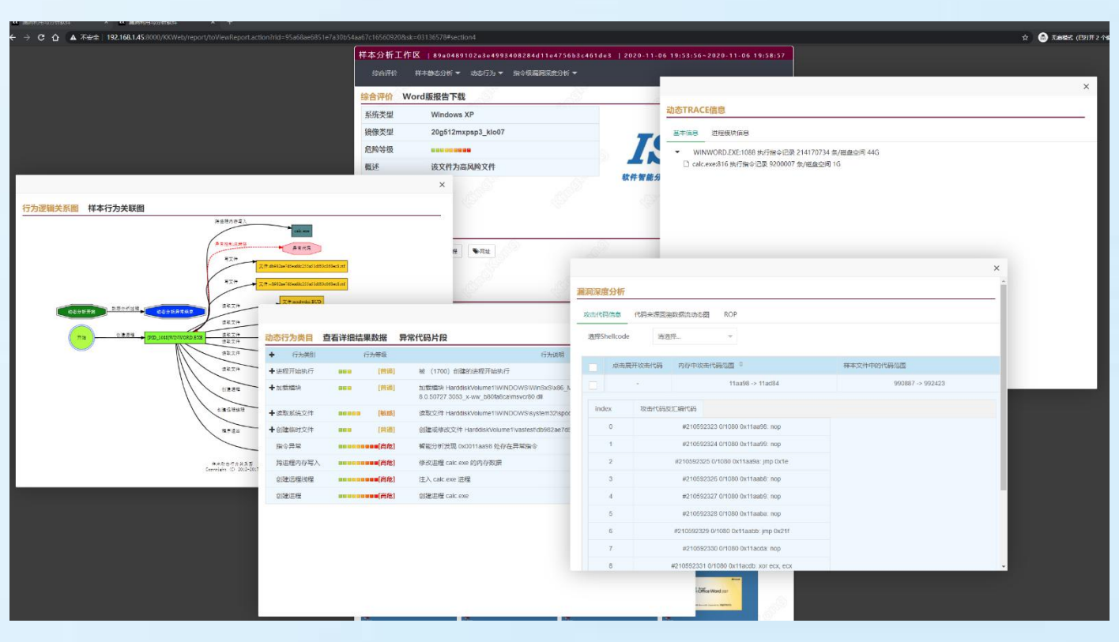
- 动态环境和参数设置
- Trace生成
- 动态行为分析
- 攻击代码识别

**交互式漏洞深度分析**

- Trace查询
- 污点分析
- 动态切片
- 内存布局分析







## 核心技术指标

- 漏洞样本Shellcode的自动化定位和攻击代码提取
- 漏洞样本Shellcode的加密、混淆、压缩、抗逆向分析等对抗手段的识别定位
- 漏洞样本代码注入、代码复用、代码喷射等典型漏洞利用行为识别
- 攻击代码中的敏感信息、控制流图等特征抽取分析
- 支持漏洞样本的离线污点分析和动态切片交互分析
- 支持Win7、Win10、Ubuntu等操作系统，支持x86和x64等指令架构