

被动取证与主动取证

James Chen
陈虹宇
13568829980
chenhy@chengdu.gov.cn

> 内容简介

- 计算机取证新模型
- 被动取证
- 主动取证
- 案例分析
- 计算机取证实战中的注意事项

> FBI 公布2005年度计算机犯罪调查结果

1月18日美国联邦调查局发布了年度计算机犯罪调查(FBI Computer Crime Survey)结果, 调查范围涉及4个州, 2000多家企业和组织。

一些主要发现:

- 攻击频率. 九成企业遭受过计算机安全事件, 两成企业声称次数在20次以上.
- 攻击类型. 病毒 (83.7%) 和 间谍软件(79.5%) 为主.
- 经济损失. 超过六成的企业声称有经济损失, 病毒和蠕虫导致了1200万美金的损失, 是总共3200美元总损失的大头.
- 攻击来源. 来自36个不同的国家, 其中来自美国(26.1%)和中国(23.9%)的攻击约占了一半.
- 安全防范. 大多数企业都说已经安装了最新的安全补丁, 但是更高级的安全技术比如生物技术和智能卡认证等用的很少, 另外44%的入侵来自企业内部.

> 利用计算机犯罪的型类

- 盗取商业信息
- 职员利用职务之便进行犯罪
- 嫌疑人的私人电脑

> 计算机取证调查模型

> 计算机取证新模型

➤ 被动取证三步曲



➤ 识别证据

- 本地日志文件
- 被删除的文件
- 修复格式损坏的文件
- 被隐藏的信息
- 综合分析

➤ 提取证据

- 硬盘镜像
- 数据恢复
 - 包括文件属性
- 数据修复
 - 各种文件格式修复



➤ 保存证据

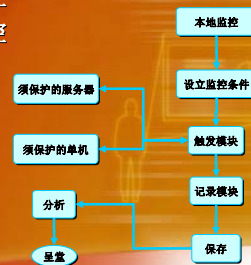
- 制成不可修改的存储介质
- 计算其HASH值
- 全过程实时录像

➤ 主动取证之本地记录

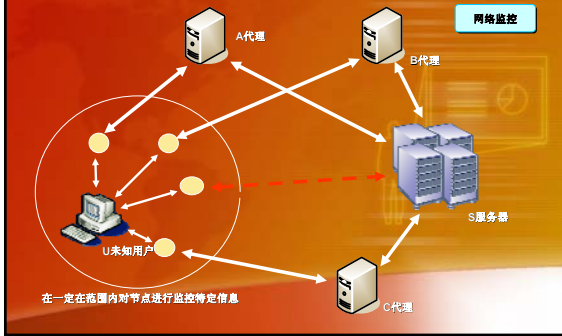
- 本机系统日志
- 本机操作日志
- 本机特定操作日志
- 预防性手段“蜜罐”

➤ 主动取证之本地监控

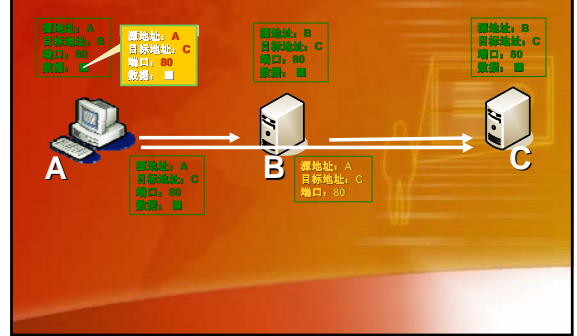
- 本地特定操作监控
- 特殊动作进行监控 (抓屏/截图)
- 任意指定监控
 - 邮件实时监控
 - 文件实时监控



> 主动取证之网络监控



> 代理基技术基本原理

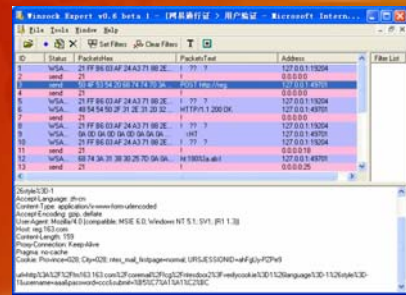


> 技术分析

- 使用代理前发送的数据包



- 使用代理后发送的数据包



- 正常情况

• `verifycookie=1&username=aaa&password=ccc&radtype=&login=%B5%C7%C2%BC%D3%CA%CF%E4&secure=on&style=-1`

- 代理情况

• `url=http%3A%2F%2Fm163.163.com%2Fcoremail%2Ffcg%2Fntesdoor%3Fverifycookie%3D1%26language%3D-1%26style%3D-1&username=aaa&password=ccc&submit=%B5%C7%A1%A1%C2%BC`



谢谢大家

James Chen
陈虹宇
13568829980
chenhy@chengdu.gov.cn

