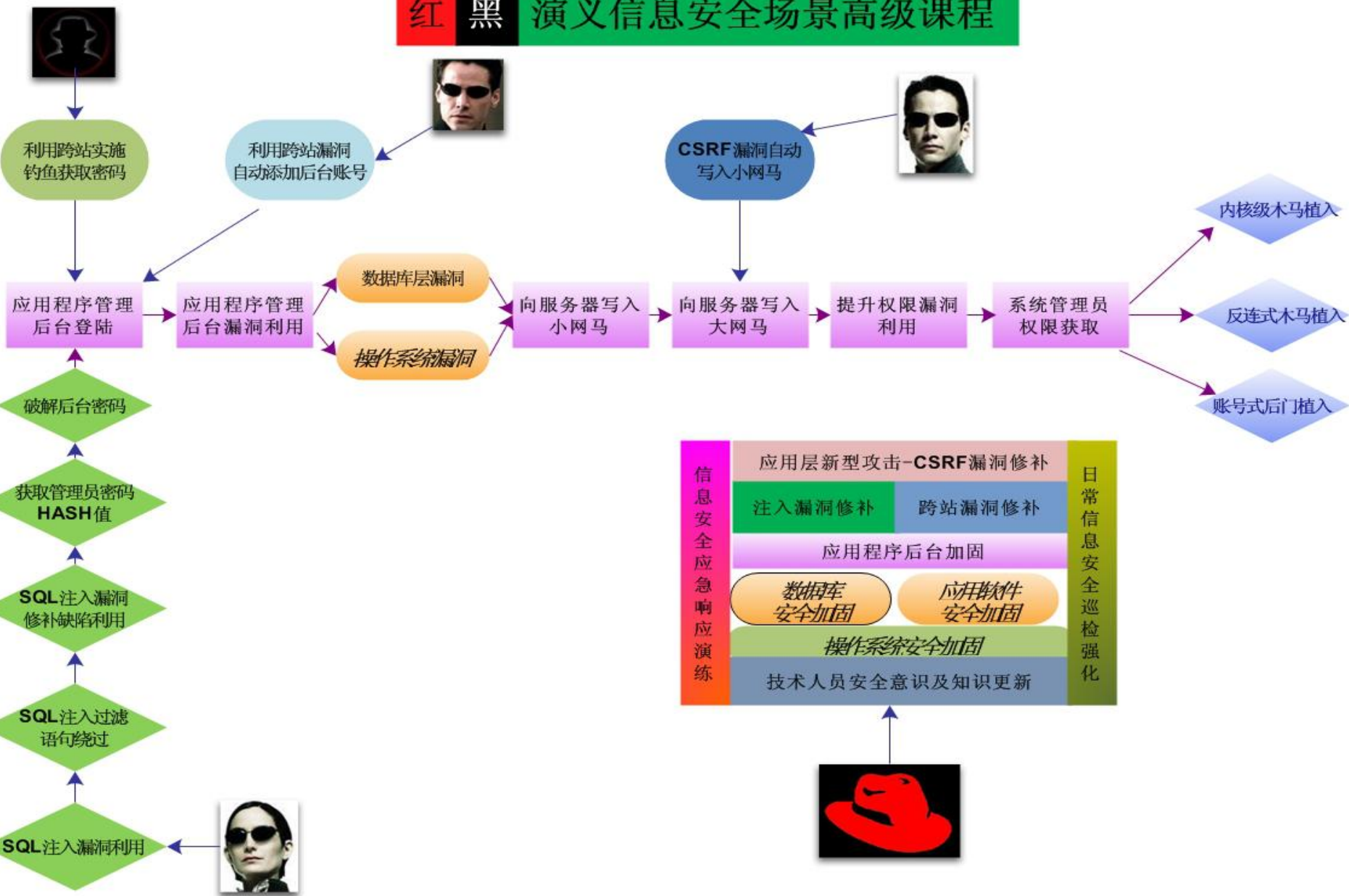


致力于中国安全国家发展，建设中国信息安全智库

红 黑 演义信息安全场景高级课程



致力于中国安全国家发展，建设中国信息安全智库


探讨部分

- *攻击者后续攻击路线分析

- *管理员深度防范对策与实践

论信息安全持久战


- 01-第一回 众里寻她千百度
- 02-第二回 知己知彼百战百胜
- 03-第三回 重金开发新网站
- 04-第四回 真真假假引君入瓮
- 05-第五回 最后的稻草
- 06-第六回 不入虎穴焉得虎子



徐漠
臭名昭著的商业黑客

黑客和网管的持久战

柯小玲
公司网站管理员



开展周密踩点
Whois查询、DNS信息查询

挖掘网站漏洞
上传webshell

利用自动化脚本成功挖掘发现
网站漏洞

进行CSRF攻击

进行ARP欺骗

利用XSS，获取管理员的公网
信箱的登录权限

利用管理员学习需求，引诱管
理员读取绑定木马的文档资料

进入该公司工作

发现敏感端口

第二次利用漏洞，攻击成功

进行SQL，XSS攻击

写入言论等非法信息

获取目标服务器的密码

寻找敏感信息

控制管理员的个人机器

获取大量价值信息，转手出售

安全设置防火墙
仅开放80和443端口

清除木马webshell
重新安全安装操作系统

去除SQL注入漏洞，修补跨站漏洞
建立专用的日志服务器

公司网站管理员下岗，后调查发
现为黑客攻击，重新回来工作

启用https和划分VLAN
进行IP+MAC+端口进行绑定

放弃公网原有信箱，采用gmail信箱

管理员使用虚拟机上网

发现人员异常，将该人送进监狱