

网络空间安全中的红蓝对抗实践

晁巍



目录

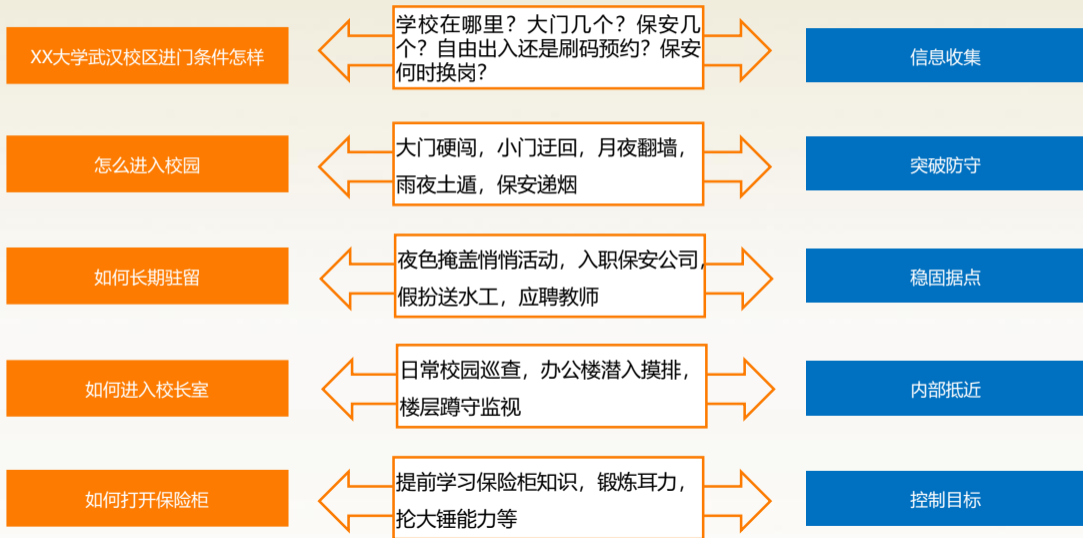
Contents

- 1 一个身边的场景
- 2 真实的红蓝对抗
- 3 红蓝对抗的一般流程
- 4 攻防矩阵与知识技能
- 5 社会需求

- XX校区校长室有一个保险箱
- 里面存了一个比特币钱包的私钥助记词
- 价值1024个比特币

怎么搞定它?

实施方案





蓝方：攻击方，内部蓝军、商业黑客、国家队

红方：防守方，监测预警、应急响应、情报溯源等

目标：争夺某家单位某个IT实体（系统、服务器、数据库）的控制权

- 中国国家XX集团，XX调度系统控制权
- 中国XX公司，XX调度数据
- 中国YY集团，全量YY信息

通过**模拟真实的攻防演练场景**，帮助国家**关键基础设施单位提升安全水位**，我们曾经帮助

- 某快递单位，发现可以**(省略)**的攻击路径
- 某大型航空公司，发现可以获取**(省略)**的攻击路径
- 某一线城市，发现可以取得**(省略)**的攻击路径
- 多个智能汽车品牌，发现**(省略)**的攻击路径

以及其他众多**涉及国家基础设施安全**的案例

现实的网络攻防不是小偷小摸，是没有硝烟的真实战斗 而且每天都在发生

- 阿里云高防日均防护云上DDoS攻击
2500次
- 阿里云WAF日均拦截5亿次Web攻击，
累计监测的全网活跃恶意IP达到60万
以上
- 阿里云安全中心监测到2023年的勒索
病毒家族比2022年增加了81%



展开一次网络入侵的关键步骤



ATT&CK攻防矩阵及知识技能

图引自: https://blog.csdn.net/qq_40216188/article/details/123106969



代码知识

- 后端代码审计能力
- 远控研发能力
- 前端相关代码分析能力
- 漏洞利用能力
- 日常自动化工具开发
- 逆向分析能力

运维知识

- Linux系统常规运维
- Windows系统常规运维
- 安全/网络设备运维
- 数据库运维
- Webserver运维

网络知识

- 网络通信七层模型
- HTTP/DNS/FTP协议标准
- 路由交换知识
- 网络架构体系
- 网络抓包工具使用

漏洞知识

- Web通用漏洞
- 组件专属漏洞
- 系统底层漏洞
- 移动端漏洞
- 漏洞挖掘及利用

密码知识

- SSH/SSL/TLS/HTTPS
- 对称密码/非对称密码
- 签名/哈希/加密
- PKI数字证书体系
- 区块链相关 (零知识证明/拜占庭容错等)

玄学加持：灵性和运气！

安全攻防岗位招聘情况及能力要求

安全攻防专家 [北京-大兴区-亦庄]

30-50K-16薪 3-5年 本科 杨女士 招聘经理

Java C/C++ 攻防 漏洞源 逆向

京东集团

电子商务 已上市 10000人以上

五险一金, 补充医疗保险, 带薪年假, 交通补贴, 股票期权...

安全攻防专家 [北京-通州区-次渠]

30-50K 3-5年 本科 刘先生 安全团队负责人

信息安全 安全 Web安全

京东科技集团

互联网 不需经验 1000-9999人

餐补, 免费班车, 补充医疗保险, 五险一金

安全攻防专家 [北京-东城区-东单]

40-60K-15薪 5-10年 本科 赵先生 招聘总监

渗透测试经验 攻防对抗经验

OPay

互联网 C轮 500-999人

补充医疗保险, 年终奖, 节日福利, 包饭, 带薪年假, 股票...

安全攻防专家 [北京-朝阳区-79街]

15-30K-15薪 1-3年 本科 魏先生 实验室负责人

Burp Suite 红队 漏洞挖掘 渗透测试经验 代码审计

360集团

互联网 C轮及以上 1000-9999人

带薪年假, 定期体检, 免费班车, 餐补, 五险一金

安全攻防专家 [北京-丰台区-太平桥]

26-27K 3-5年 大专 张女士 产品经理

安全体系架构和研发 安全运维和保障

图灵

社交网络 天使轮 20-99人

带薪年假, 餐补, 加班补贴, 年终奖, 股票期权, 带薪年假...

安全攻防专家 [武汉-江夏区-光谷]

18-30K-14薪 经验不限 本科 魏先生 技术总监

渗透测试经验 Web测试经验 攻防对抗经验

绿盟科技

信息安全 已上市 1000-9999人

餐补, 带薪年假, 五险一金, 年度体检, 股票期权, 员工旅...

网络安全专家 [武汉-洪山区-花山]

60-90K 10年以上 本科 曹女士 HR

C/C++ PHP Java 计算机/信息安全相关专业

雷神科技

互联网 未融资 100-499人

住房补贴, 生日福利, 带薪年假, 团建聚餐, 餐补, 带薪...

网络安全专家 [武汉-洪山区-光谷]

35-60K-14薪 5-10年 本科 任先生 HR

安全体系架构和研发 C/C++ OSM

金山办公软件

互联网 已上市 1000-9999人

股票期权, 带薪年假, 补充医疗保险, 团建聚餐, 生日福利...

安全专家 [武汉-洪山区-光谷]

30-50K-15薪 5-10年 硕士 杨女士 HR

安全体系架构和研发 安全运维和保障

普雷科技

通信/网络设备 未融资 500-999人

生日福利, 团建聚餐, 定期体检, 带薪年假, 加班补贴, 五...

湖北中天招聘生产安... [武汉-洪山区-珞南]

10-15K-14薪 10年以上 大专 张女士 招聘总监

化工: 注册安全工程师证书

湖北中天

在线教育 未融资 20-99人

节日福利, 年终奖, 高温补贴, 带薪年假, 五险一金, 餐补...

阿里云安全攻防专家 (杭州/北京)

主要方向

渗透测试与红蓝对抗

岗位职责

阿里云攻防服务交付, 实战攻防演练赛事, 阿里云蓝军武器库调优。

岗位要求

1、精通常见 Web 漏洞, 主机漏洞等高危漏洞的利用方式及溯源原理, 具有实际内网渗透攻防经验, 熟悉常见内网渗透技巧, 熟悉绕过策略及横向扩展手段。

2、熟练掌握各种渗透攻防工具, 如

Metasploit、CS、BP 等, 并能根据需要進行渗透攻防工具优化和开发。

3、精通 Rust、Java、Python、Shell、Go、C/C++ 中至少一种编程语言。

4、热爱安全攻防事业, 对安全研究兴趣浓厚, 能够持续关注国内外最新的安全发展动向和攻防技术, 并转化为实战攻击手段。

5、具备良好的逻辑思维能力和团队合作精神, 善于沟通与表达。

加分项 (不做必选, 但会优先考虑)

1、作为主力参加过国内大型攻防演练赛事, 并获取国家级 Top5 奖励

2、先知、补天、漏洞盒子、HackerOne、ASRC、TSRC 等平台 Top 白帽

3、有资产测绘、漏洞扫描、或远程控制等分布式安全平台开发经验

这个领域，有用，有趣，有钱，大有可为

搞定它！

问答环节

Q&A

Thanks !

The background is a traditional Chinese ink wash painting. It depicts a vast, misty landscape with rolling mountains and a body of water. In the distance, a modern city skyline is visible, blending with the natural elements. A lone figure in traditional attire stands on the shore in the foreground, looking out over the scene. The overall mood is serene and contemplative.