阿里云 | 阿里云先知 Alibaba Cloud XianZhi | Alibaba Security Response Center

网络空间安全中的红蓝对抗实践

晁巍

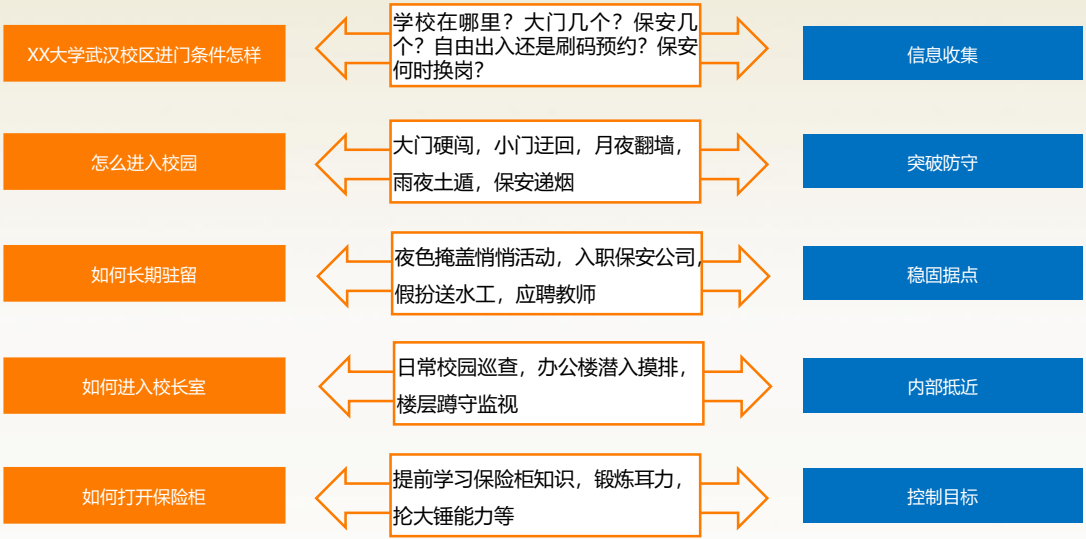
目录 Contents

思考这样一个场景

- 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


XX大学武汉校区进门条件怎样
学校在哪里？大门几个？保安几个？自由出入还是刷码预约？保安何时换岗？
信息收集
怎么进入校园
大门硬闯，小门迂回，月夜翻墙，雨夜土遁，保安递烟
突破防守
如何长期驻留
夜色掩盖悄悄活动，入职保安公司，假扮送水工，应聘教师
稳固据点
如何进入校长室
日常校园巡查，办公楼潜入摸排，楼层蹲守监视
内部抵近
如何打开保险柜
提前学习保险柜知识，锻炼耳力，抡大锤能力等
控制目标

网络空间安全中的红蓝对抗场景

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

红蓝对抗的实际意义

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

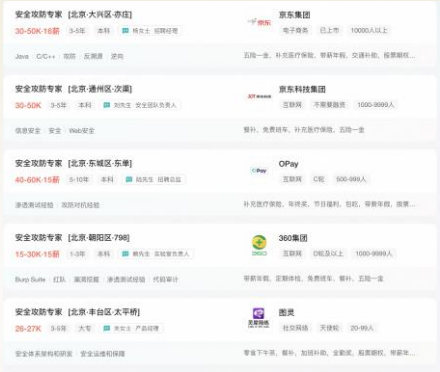
- Web通用漏洞
- 组件专属漏洞
- 系统底层漏洞
- 移动端漏洞
- 漏洞挖掘及利用

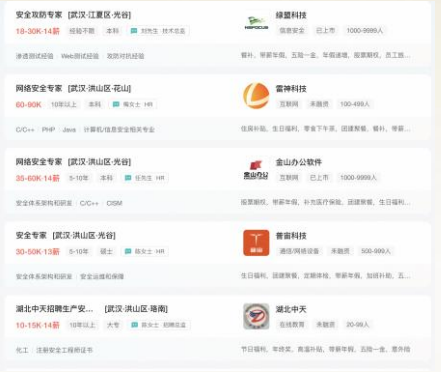
密码知识

- 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





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，实网攻防演练赛事，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漏洞原理，具有实际内网渗透攻防经验，熟悉常见内网渗透技巧，杀软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，并能根据需要进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，并转化为实际攻击手段。

5、具备良好的逻辑思维能力和团队合作精神，善于沟通和表达。

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 !