
腾讯安全
腾讯安全云鼎实验室
相约江夏
智汇攻防
腾讯安全沙龙（武汉站）

关于
About me

樊一博（keyi / 无尾熊）

- 长亭科技华北技术总监
- 红队建设/红蓝对抗/代码审计/应急响应
- 参与多次国家级、省级HW行动，获2023、2024第一名
- 多次挖掘例如某知名堡垒机反序列化RCE漏洞、某友NC命令执行等0day漏洞
- 多次对关键基础设施单位进行应急响应，处理多起勒索&APT攻击事件
- 输出《Fastjson黑盒盲测与白盒审计》、《CobaltStrike绕过流量审计》等文章
- 《无尾熊安全》创始人，运营《无尾熊安全》公众号、《无尾熊安全》知识星球

CONTENTS

魔鬼训练营

红队组成架构

武器平台

自动化渗透

前沿技战法

攻防案例

2022

01 红队魔鬼训练营

HW攻击准备工作

Red team attack preparation work

战略战术思想

- **特点**：“海量数据”“供应链”“动态权重”“核心专网”
- **目标**：各级基础设施、重点供应商、储存核心敏感数据业务系统
- **形式**：“窃密战”“零感知”“大流量攻击”

组织行动分工

- **情报组**：确保行动目标达成的基础条件，及时复现最新漏洞并工具化为EXP
- **打点组**：突防、窃取和瘫痪目标的工具，依托情报打击目标，根据漏洞装载攻击部（钓鱼、互联网突破、供应链）
- **内网组**：内部网络的横向蔓延（专网突破、重点系统、权限提升）
- **攻防利器**：自动化信息收集平台、ASM攻击面管理平台

阶段性工作
Phased work

攻击分阶段任务

- 距离HW攻击2-3月开始储备相关人员，并根据人员擅长领域进行分组技能提升；并同步研发各类免杀工具、域前置调试，等各类防溯源工作；
- 距离HW攻击1月开始准备各类Nday、1day、0day漏洞，并随时分析最新出现的各类通用型漏洞；
- 距离HW攻击1周此时已经拿到攻击方规则，可以开始着手研究攻击方的规则相较于往年是否存在变化，是否具备新的倾向性，决定本次攻防的攻击战术。

准备阶段				攻击阶段	
人员能力	漏洞储备	工具储备	技战法储备	规则分析	得分分析
依人员数量分组做专项技能准备	储备Nday、1Day以及0day	储备红队常用的各类工具	熟悉红队必须掌握的OPSEC	熟悉本次红队攻击中规则的倾向性	随时分析目前已经提交成果的报告
外网打点人员	通用系统漏洞	信息收集工具	关键信息识别	路径分上限	路径分
内网渗透人员	框架漏洞	漏洞利用工具	威胁分析	边界划分	突破边界分
代码审计人员	中间件漏洞	代理隧道工具	漏洞分析	靶标目标	靶标分
免杀对抗人员	CMS漏洞	内网渗透工具	风险评估	数据泄漏规则	重大成果分
武器开发人员	安全设备漏洞	社会工程学库	措施（防溯源）	漏洞发现与防溯源	0day分

整体组织架构

Overall organizational structure

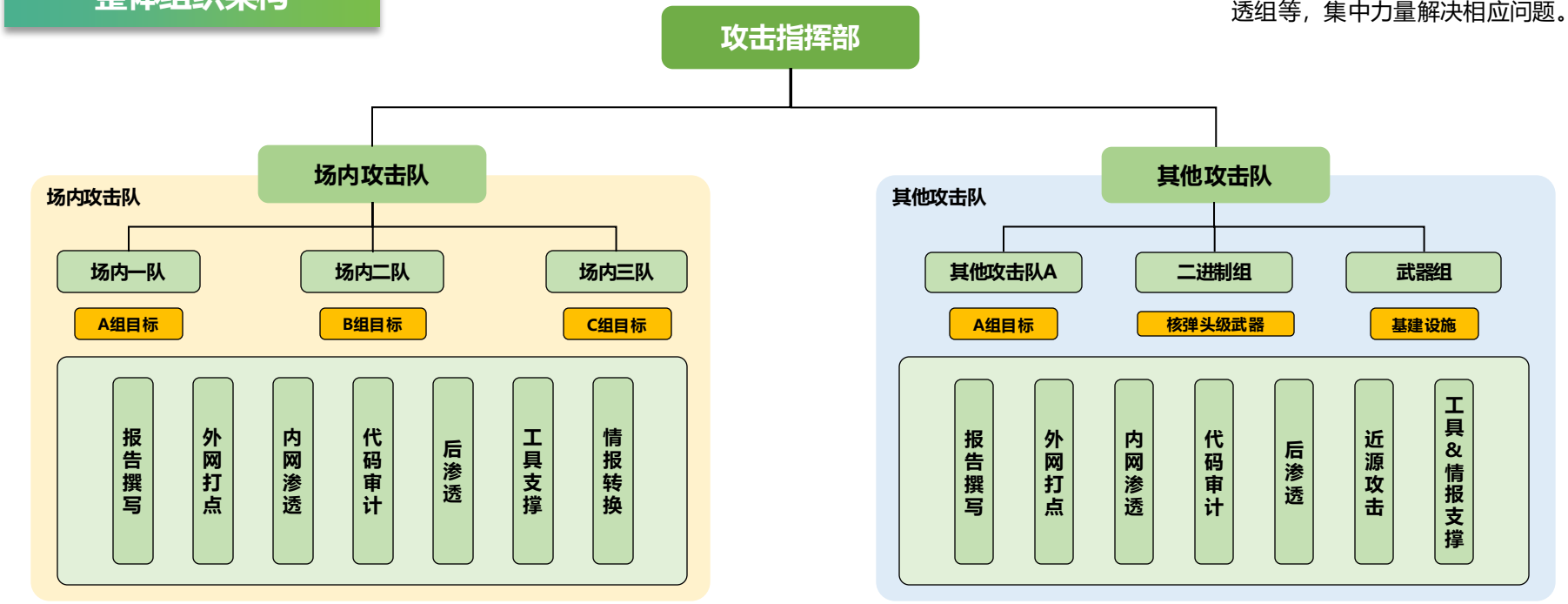
组织架构意义

- 定义HW攻击队的整体组织架构，包括各个部门和角色的划分。
- 确定HW攻击队的领导结构和指挥链条，确保任务的协调和决策的高效。
- 确定HW攻击队、二进制研究组、武器组的关系和沟通方式。

细分组织架构

- **攻击指挥部：**
  - 负责整体红队行动的策划和指导，协调场内和其他攻击队的工作。
- **场内攻击队：**
  - 负责场内攻击行动的直接执行，并随时将场内情报传递至其他后方大本营。
- **其他攻击队：**
  - 依据不同人员的不同技术能力，组建报告组、打点组、内网组、审计组、后渗透组等，集中力量解决相应问题。

整体组织架构



攻击职责划分

Division of attack responsibilities

外网打点组

- 负责对目标组织的外部网络进行侦查和攻击，获取入侵起点；
- 执行针对目标组织的漏洞扫描、漏洞利用和外部渗透测试等技术；
- 例子：端口扫描、漏洞利用、Web应用程序漏洞攻击。

内网渗透组

- 负责在目标组织的内部网络中寻找目标和敏感资产，并获取更高权限；
- 执行内部渗透测试、横向渗透和提权等技术；
- 例子：局域网扫描、密码破解、横向移动、提权攻击。

代码审计组

- 负责对目标组织的应用程序代码进行审计和漏洞挖掘；
- 分析代码的安全性和漏洞，发现潜在的安全问题，并挖掘0day；
- 例子：源代码审计、安全漏洞挖掘、漏洞验证。

权限维持组

- 负责在目标系统中维持长期访问权限，并隐蔽存在；
- 开发和使用后门、持久性攻击工具，以确保持续控制目标系统；
- 例子：后门开发、远程控制工具、持久性攻击技术。

免杀对抗组

- 负责对抗目标组织的安全防御系统和防病毒软件；
- 分析常见防御技术和免杀方法，开发和使用绕过技术；
- 例子：恶意代码免杀技术、反沙箱技术、免杀工具开发；

社工钓鱼组

- 负责通过社会工程和钓鱼攻击手段获取目标组织的敏感信息和访问权限；
- 发送钓鱼邮件、制作钓鱼网站、进行电话钓鱼等活动，欺骗目标用户并获取信息；
- 例子：钓鱼邮件制作、社会工程攻击、电话钓鱼攻击。

工具支撑组

- 负责红队攻击中使用的工具和系统的支持和维护；
- 管理和更新攻击工具、脚本和平台，以确保其可用性和效果；
- 例子：攻击平台管理、工具配置和维护、脚本编写和维护。

后勤支撑组

- 负责支持红队行动中的后勤和组织管理工作；
- 管理团队的资源、计划和进度，协调与其他小组的合作；
- 例子：资源管理、进度跟踪、团队协调。

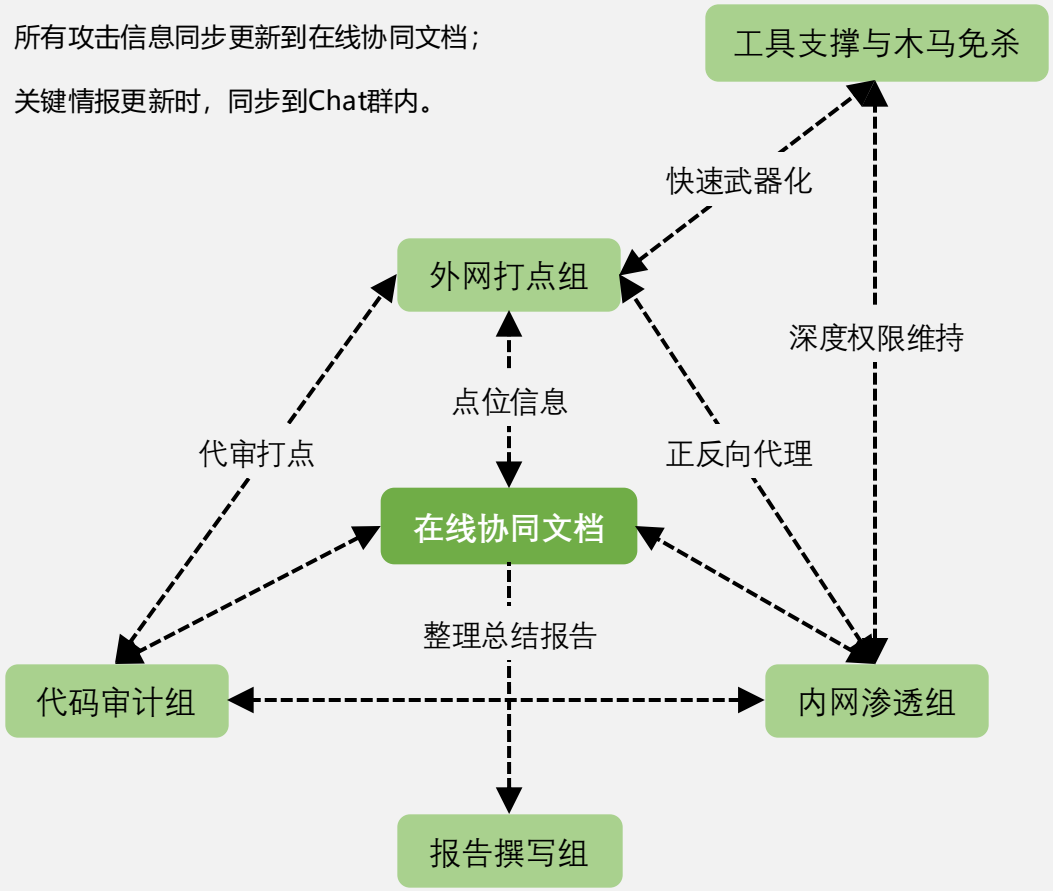
攻击协同机制

Attack coordination mechanism

场内/其他协同机制

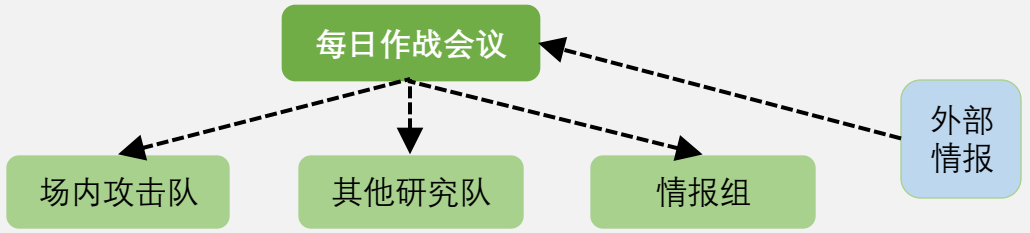
Rocket.Chat
即时聊天工具

- 根据不同靶标分别建立群聊；
- 所有攻击信息同步更新到在线协同文档；
- 关键情报更新时，同步到Chat群内。



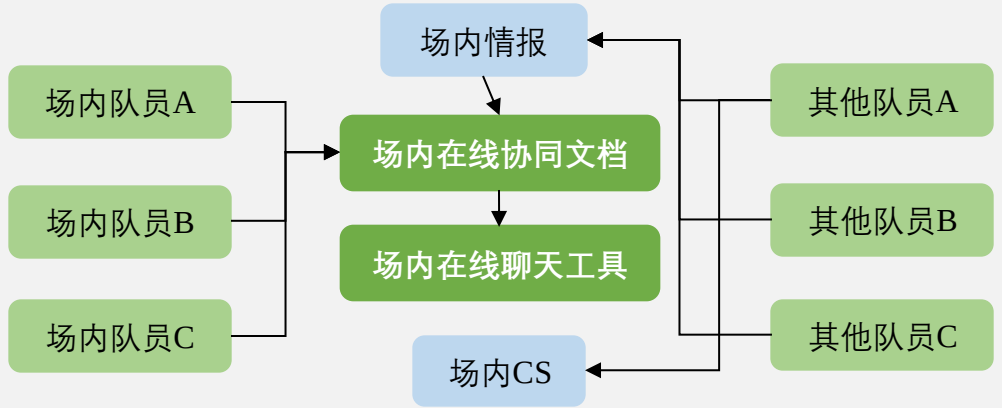
协同机制

场内外每日沟通



- 每日晚上非攻击时间，前后场对齐当日攻击进度、行业内进度、裁判尺度、情报信息等；
- 根据最新整体攻击情况，建立明日待办、攻击重点、攻坚重点。

场内外即时沟通



02 武器平台

Red team attack preparation work

红队一体化攻防渗透服务产品-自动化SaaS版

产品定位：一款效力于红队攻防演练场景下外网打点&后渗透领域等多个阶段的综合服务产品。

洞鉴 X-RAY

快速、全面、精准

轻量便捷的SaaS化安全能力，蓝军的最佳选择

洞鉴SaaS专版是最佳实践与历年知识沉淀产生的安全服务产品，它内置了**项目管理，边界渗透、内网渗透、安全工具集（包含自研脚本）等**多个**红队高频利用的脚本与工具**。经历了内部**五年的研发迭代和规则优化**，洞鉴已经能够在攻防演练项目中大显身手，并被**广泛应用于重点攻防项目中**，协助安全服务团队多次在**实战演练中名列前茅。**

65% up
攻防打点效率

90%
红队工具集成

95% up
重复资产降噪

SaaS自动化发展史

除上述能力外，洞鉴还具备多个**领域自动化工具能力**，作为蓝军必备的神器，可以更好的辅助好人工在实战演练中**取得更好的名次和发挥更大的效果**。

2018

洞鉴框架封板

第一版本洞鉴开始使用，开始时仅有部分功能开发完成，扫描去重能力很差。

2019-2020

洞鉴工具能力集成

依据项目最佳实践，选取了多款高频工具进行集成，同时开始注重规则优化，洞鉴初步成型。

工具集成

内置了30多个脚本、工具提供给安全服务团队作为项目实践最好用的工具之一，已成为团队项目必备神器之一。

2023

精准扫描能力

基于通信、金融、电力多个行业的项目实践，PoC和识别能力已经成熟。协助服务团队多次获得实战演练的优异名次。

洞鉴-项目管理

在任务扫描过程中和已完成任务，结果通过根域名、IP、DNS记录、开放端口、Web服务、Web URL、可利用的漏洞等多个维度进行**分类展示**，用户通过筛选可快速找到可能存在安全风险的服务器，从而进行下一步攻击。对于扫描结果存在数量级比较多的情况，洞鉴还依据PoC可信度以及历史利用排名提炼了**重点关注模块**，**方便用户快速发现脆弱资产**。

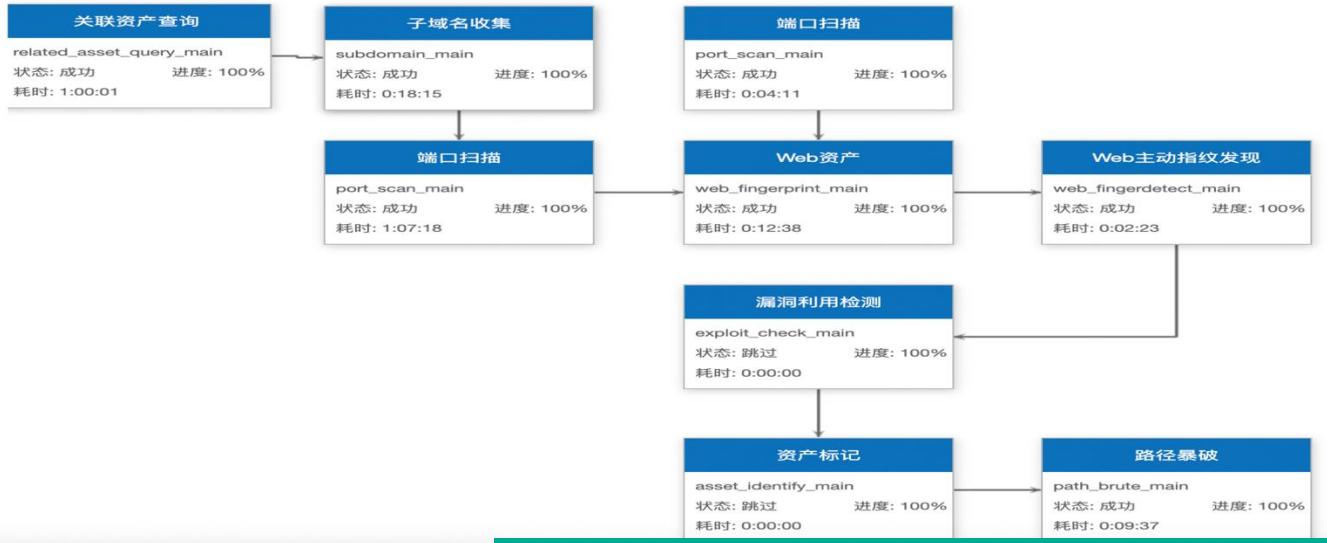
洞鉴-扫描管理

在扫描管理模块中，项目团队中的任一成员可通过扫描管理模块**灵活配置**扫描任务规则（遵循项目模板里配置的扫描策略），通过**黑名单机制、流量转发配置、唤醒时间配置**多个可选项来保证扫描在预期时间内进行，扫描过程中可编辑内置模板来配置扫描流量特征，同时还可设置漏洞通知。对于预期外的扫描任务和结果，洞鉴内置了任务管控模块来管理当前项目有效性，同时内置**资产聚合算法**来识别同一资产。

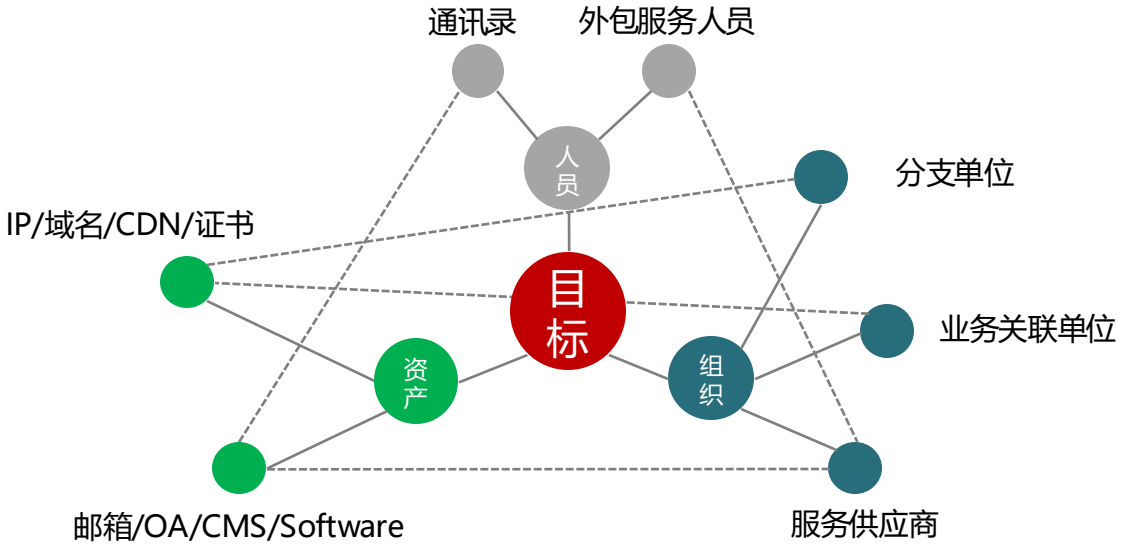
实战中的攻击自动化体系-信息收集自动化

自动化信息收集平台：

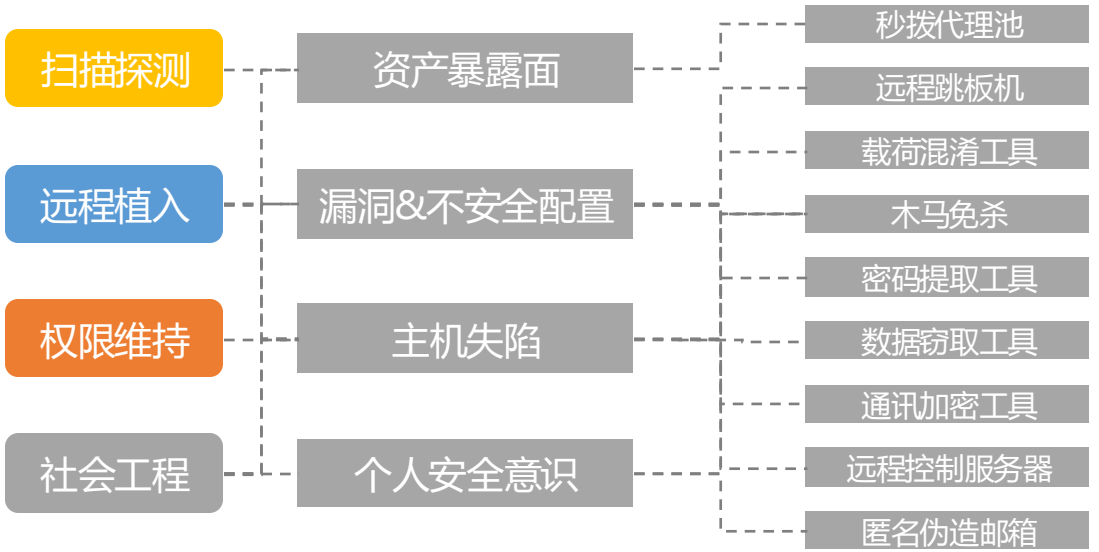
信息收集、风险发现、脆弱点扫描，资产聚集



组织-人员-资产



攻击战术-目标脆弱性-武器库



03 前沿技战法

Red team attack

preparation work

攻击技战法1：锚定信创国产化精准打击

主要对抗场景

目标单位在基础软件（操作系统，数据库，中间件）、基础硬件（整机，芯片，固件）、应用软件（办公、邮箱、社交、业务软件等）、信息安全（安全产品）等领域的信创国产化产品。

潜在突破口

信创国产化

- 发展时间较短，可能存在更多未发现或未修复的漏洞。
- 相比于市场中的成熟品牌，信创产品的安全研究和社区支持可能较少，导致漏洞披露相对延迟。
- 某些特定的信创环境配置可能使得常规攻击手段不易奏效，但同时也可能引入新的攻击向量。

与传统攻击类似的攻击手法

SQL 注入	利用不安全的数据库查询参数，执行恶意SQL语句
文件上传	上传恶意文件至服务器，利用不当的文件过滤或权限设置
反序列化	通过发送特制的数据包，触发对象反序列化漏洞，执行任意代码
二进制漏洞	如缓冲区溢出、格式字符串漏洞，利用编译时或运行时错误
……	

攻击技战法2：奇兵出击，巧用IPv6攻关

对抗场景

信息安全强监管下的金融单位，攻击面充分收敛。

安全设备覆盖度较高，对外暴露的Web应用系统正面突破难度大。

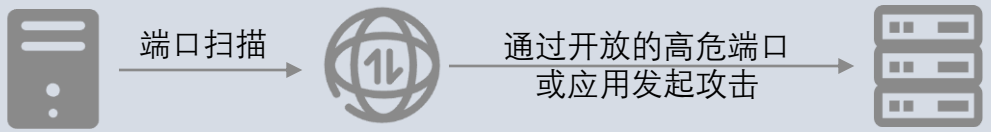
金融行业包括官网在内的核心业务系统已全面支持IPv6访问。

突破口

IPv6需单独设置安全策略以及在支持IPv6的网络下进行信息采集，可能很多IPv6地址未进行单独的安全防护以及日常的暴露收敛。

战术1：通过IPv6寻找潜在暴露点

若目标未在防火墙正确配置IPv6策略，可以通过对目标的IPv6地址进行**端口扫描**，查找开放的高危端口或应用，进而尝试发起攻击。



战术2：通过IPv6绕过安全设备拦截以及网络负载下代理稳定

- **IPv6安全策略缺失：**可利用IPv6流量绕过传统的IPv4防护设备；
- **IPv6流量特征利用：**IPv6日常访问流量较小，不易被检测，且多路负载均衡场景下，IPv6流量不易触发异常阈值。

攻击技战法3：单点登录与统一身份认证系统攻关

单点登录（SSO）

允许用户使用一组凭证（如用户名和密码）登录后访问多个应用和服务，而无需重复登录。

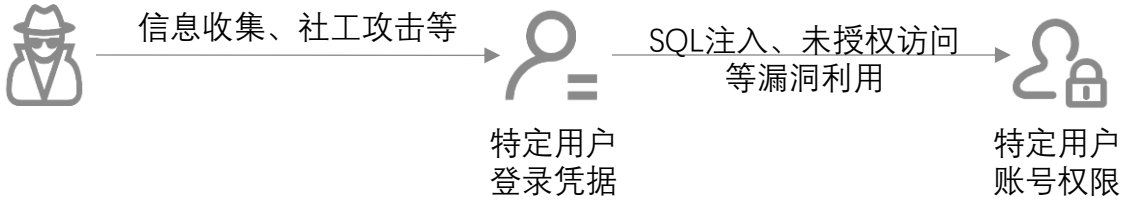
统一身份认证（IAM）

通过集中管理用户身份和访问权限，确保只有授权的用户才能访问特定资源。

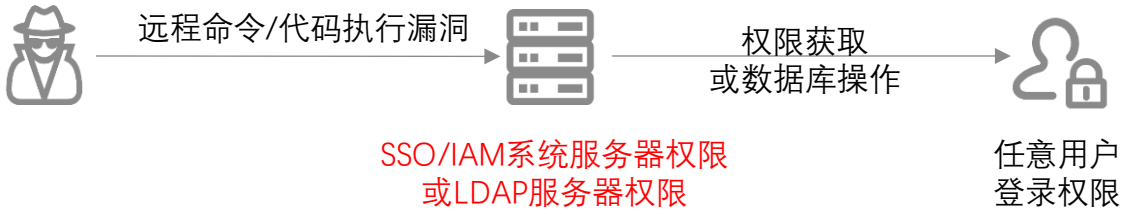
在减少潜在攻击点、降低因多个独立系统各自管理身份认证带来安全风险的同时，**集中化导致入侵收益和影响力进一步扩大。**

常用攻击手法

账号级攻击



系统级攻击



谢谢