CONTENTS

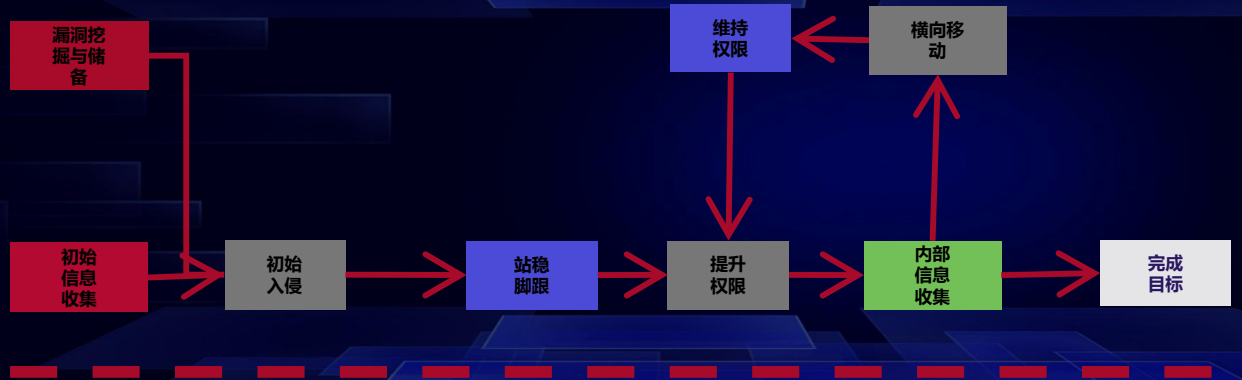
/01

攻防体系升级

攻击流程与核心要素剖析

卡亭科技 CHAITIN | ADCONF

攻击流程



核心要素

1. **信息** 是实战攻防的第一生产力，贯穿攻击的整个生命周期，优秀的情报能力可以令准备和攻击事半功倍；
2. **漏洞** 是撕开防线、扩大战果的重要武器，需要依靠信息进行精确制导；
3. **工具** 是潜伏敌线、刺探情报的间谍：主要包括远控，搜集、密码窃取等前后渗透工具。

攻击职责划分

卡亭科技 CHAITIN | ADCONF

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；

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。

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；
- 例子：钓鱼邮件制作、社会工程攻击、电话钓鱼攻击。

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。

甲方攻击方表现


第一梯队
三大运营商
01
第二梯队
头部能源、大型银行、部分金融机构
02
第三梯队
其他参演攻击方
03
• 模式
• “窃密战” “零感知” “新形势”
第一梯队
01
• 丰富的漏洞储备
• 定制化工具
• 成熟的组织与配合
第二梯队
05
• 投入人员较多
• 有一定漏洞储备
• 组织配合稍显不足
第三梯队
06
• 资源投入降低

/02

蓝军体系

网络空间安全人才能力框架

攻防演练服务常态化，效果与质量逐年下降

统一、结构化的演练活动（项目）管理手段，是提升红队攻防演练效果的重中之重，对红队高频使用的工具的整合是一个高级攻防专家的刚需。建设好攻防演练基础设施能力，才能最大化发挥红队潜在实力。

94%

依据长亭科技市场调研发现，以金融、通信、政企为主的行业至少94%的企业每年至少执行一次攻防演练，其中90%以上的客户认为他们从攻防演练中获得的效果不及预期。

5+

由于人的技术专项能力偏差导致各厂商发现的暴露资产不一致，导致企业和组织必须花费更多的资金投入来邀请至少5只攻击队伍才能收敛攻防演练目标的60%安全风险。

30+

红队队员擅长领域各不一样，所使用的工具数据结构不一，每个红队队员至少需要30种不同的脚本、工具，才能完成擅长领域的攻击动作。演练执行期间，98%以上的时间被应用于调试脚本、工具和变更部署环境，极为影响演练效果与实际产出。

红队一体化攻防渗透服务产品-自动化渗透工具SaaS版

卡亭科技 CHAITIN | ADCONF

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。**

除上述能力外，自动化扫描平台还具备多个**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**。

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。

2018

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。

2019-2020

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。

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。

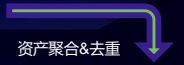
2023

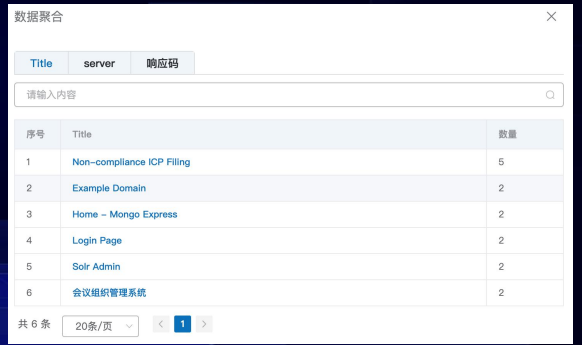
洞鉴-项目管理

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。

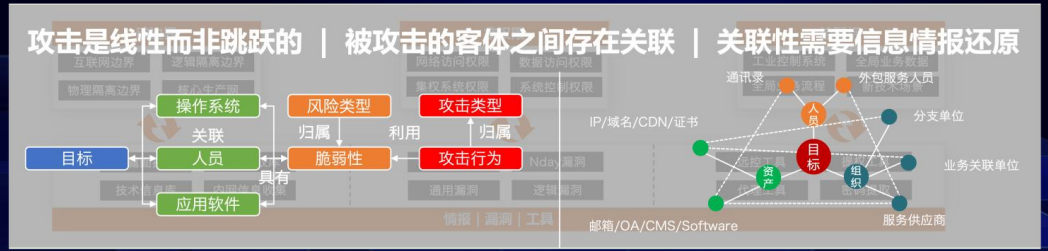




/03

实网案例


理论安全架构
HTTPS/TLS
加密传输
用户
边界安全
DDOS防护
防火墙
应用防火墙
应用与主机安全
身份鉴权
访问控制
API安全
基线核查
漏洞管理
入侵检测
数据安全
数据脱敏
数据备份
数据加密
凭证管理
研发安全
研发安全培训
安全需求分析
安全编码规范
业务上线评估
运维安全
双因素认证
运维操作审计
特权命令管控
运维


攻击是线性而非跳跃的 | 被攻击的客体之间存在关联 | 关联性需要信息情报还原
目标
关联
操作系统
人员
应用软件
具有
风险类型
归属
脆弱性
利用
攻击类型
归属
攻击行为
情报 | 漏洞 | 工具
通讯录
外包服务人员
分支单位
人员
目标
资产
组织
业务关联单位
服务供应商
IP/域名/CDN/证书
邮箱/OA/CMS/Software

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

- 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。

信创国产化

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

卡亭科技 CHAITIN | ADCONF

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）

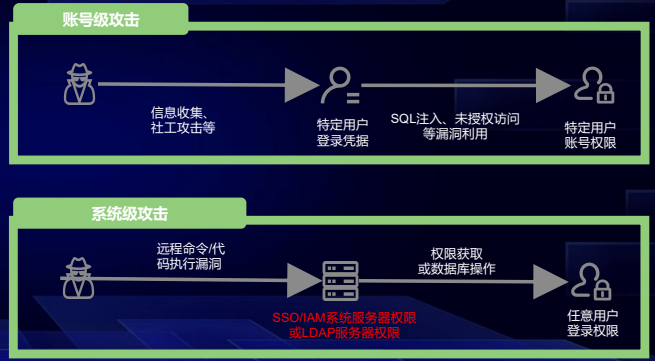
允许用户使用一组凭证（如用户名和密码）登录后访问多个应用和服务，而无需重复登录。

统一身份认证（IAM）

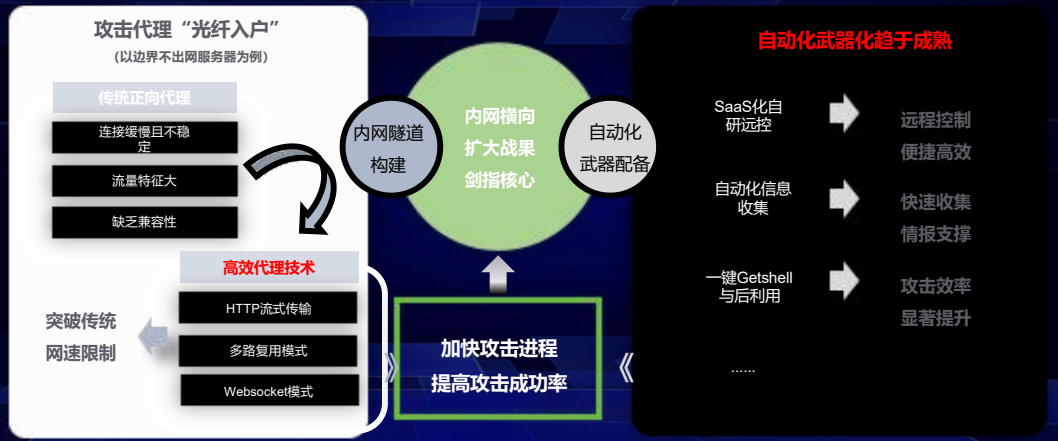
通过集中管理用户身份和访问权限，确保只有授权的用户才能访问特定资源。

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



攻击技战法5-被坚执锐，武器化强度升级



ADCONF

主场·见真章

THANKS