专项行动之高效攻击策略

演讲嘉宾：蔚(Yù)谛

目录

XCON®

HackingGroup

第一部分

[现状]

网络目标攻击现状与问题

网络目标攻击现状与问题

01

上帝视角

不能以上帝视角考虑问题，缺乏对目标全面的安全防御和技术认知，缺乏完善的行动和应对方案。

02

散兵游勇

关键岗位领导缺乏团队组织经验和分工协作安排，核心行动目的可行性不严谨、不评估，拍脑门式盲目工作。

03

意图暴露

具体任务执行人员工作技能不足、缺乏重要任务执行经验、拍脑门式盲目攻击轻易暴露攻击意图，造成攻击难度提升或丧失攻击可能性。

XCON®

HackingGroup

第二部分

[知彼]

攻击目标选择与情报收集

攻击面目标选择

01

识别关键资产

对网络目标进行扫描测绘和多方位收集目标系统信息，快速目标关键系统资产，按照重要性进行资产划分。

02

网络架构分析

整体分析攻击目标网络部署情况，确定攻击目标电信服务运营商、部署地域、网络结构，优化攻击目标选择。

03

攻击目标排序

分析获取的目标基本情况，对关键目标进行战术预案攻击排序，试探性优化攻击战术。

攻击面目标选择思路图


基本资产
网络地址
企业域名
企业证书
指纹管理
资产扫描
端口扫描
开放端口
指纹扫描
应用指纹
域名扫描
子域名
子域名+开放端口 网络地址+开放端口
响应标题
响应内容
状态码
组件指纹
应用指纹
服务指纹
WAF识别
运营商
漏洞库关联
应用漏洞
组件漏洞
服务漏洞
字典管理
资产管理
漏洞管理
漏洞推荐
漏洞发现时间
漏洞攻击类型
漏洞利用难度
漏洞危害程度
漏洞利用脚本
漏洞官方补丁
推荐列表

情报分析与漏洞挖掘

01

攻击薄弱目标

通过已有的情报分析，找出关键且薄弱的高价值目标，按照技战术预案优先对高价值目标进行攻击测试。

02

网络对抗感知

在攻击过程中，实时感知网络攻击中的对抗行为，采用假性攻击的模式，摸清目标网络中的深层防御部署情况。

03

漏洞挖掘与评估

对攻击目标进行试探性漏洞挖掘与利用评估，将发现的漏洞进行最大化攻击利用，并评估漏洞利用后的战术结果。

情报分析与漏洞挖掘思路图

第一序列 没有防护	网络地址	开放端口	有效域名	开放端口	数据服务	开放端口		
高价值目标	OA	邮箱	VPN	运维系统	核心业务系统	人力资源系统		
漏洞挖掘	越权访问	未授权访问	SQL注入	反序列化	文件上传	…	对抗感知	
漏洞评估	危害级别	攻击难度	攻击效果	漏洞管理	漏洞战术	制定攻击战术	汇总攻击成果	

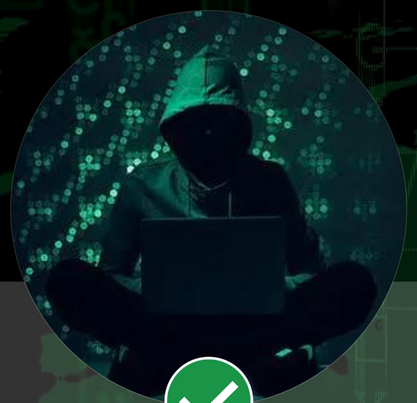
Xcon®

HackingGroup

目标防御能力整体评估

外部防御能力评估

通过采用假性攻击战术，全面获取目标网络中的外部攻击防御策略，评估目标外部网络的整体防御能力。



内部防御能力评估

通过获取薄弱目标权限，分析薄弱目标中的网络、应用、进程信息，评估目标内部网络中安全防御能力。

人工值守防御评估

通过有意识的进行多时段攻击模拟测试，评估目标系统的人工防御和响应、人工值守部署情况。

Xcon®

HackingGroup

目标防御能力评估思路图

第三部分

[战术]

可攻击性分析与策略制定

XCON®

HackingGroup

预渗透攻击策略制定

01

合法身份获取

分析目标现有的系统登录管理方式，通过技术手段获取主机或系统合法登录或管理权限。

02

低感知度评估

采用低感知度管控技术长期维持目标系统登录会话，合理评估身份暴露的可能性大小。

03

横向目标选择

谨慎分析目标系统中网络连接关系，确定资产属性后进行攻击性评估，选择性对第二目标进行横向攻击。

预渗透攻击策略制定思路图

预渗透防守策略分析

拓扑弱点分析

按照制定的攻击性策略，在内部横向过程中，绘制网络拓扑结构，定位网络防守的薄弱区。

防御弱点分析

按照制定的攻击性策略，在内部横向过程中，重点分析主机和网络中的防御优势和缺陷。

运维弱点分析

按照制定的攻击性策略，在内部横向过程中，分析运维人员习惯，定位关键运维人员。

Xcon®

HackingGroup

预渗透防守策略分析思路图

预渗透人员安全意识评估

01

目标人员安全意识

通过在攻击过程中获取的员工信息，根据员工岗位职能有意识的选择对网络安全认识薄弱的员工进行意识评估。

02

高度仿真意识评估

通过对目标系统进行高度仿真，采用高度仿真或反向代理的形式植入攻击脚本，面向全体员工进行精心策划的安全意识评估。

03

社会工程意识评估

通过在攻击过程中获取的员工信息，通过采用社会工程学的方式，准备不同场景下的诱导话术进行意识评估。

XCON®

HackingGroup

预渗透人员安全意识评估思路图

预渗透安全意识

特定人员评估

- 销售部门
- 人资部门
- 财务部门
- 审计部门
- 法务部门
- 运营部门
- 运维部门
- 市场部门

全体人员评估

- 高管角色
- 安全部门
- 运维部门
- 其他全部部门

社会工程评估

- 历史账号
- 历史密码
- 历史手机
- 历史邮箱
- 运维部门
- 研发部门
- 运营部门
- 市场部门

预渗透意识评估

- 邮件钓鱼
- 水坑攻击
- 社交钓鱼
- 工单钓鱼
- 短信钓鱼
- …
- 高度仿真
- 恶意代码植入
- 恶意后门投送
- 话术后门植入
- 话术后门植入

预渗透战术选择

XCON®

HackingGroup

第四部分

[侦查]

外围渗透与防御技术绕过

外围渗透

近源攻击

01

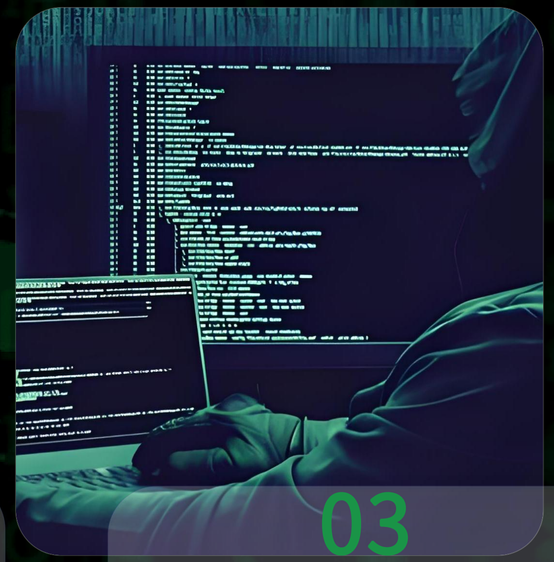
无线热点仿真攻击

通过前期踩点摸清攻击目标的无线热点分布和身份验证情况，模拟攻击目标无线认证过程进行无线热点攻击，窃取真实无线认证密码。

02

访客身份深入目标

通过以外部访客或面试者身份深入目标办公地点进行超近距离踩点，悄悄接入目标办公地点网络，无声无息的进行深层网络攻击。



03

快速进行网络攻击

通过控制好攻击手段，在不暴露自身位置的前提下做好攻击预案，用快和准的要求获取特定目标的管控权限和存放的敏感数据。

XCON®

HackingGroup

外围渗透近源攻击思路图

E WIFI网络

F USB接口

10-50米

G 物理接口

H 智能设备

A 仿冒热点

B 门禁攻击

50-200米

C 应用渗透

D 仿冒基站

Xcon®

HackingGroup

目标防御技术绕过

01

真实地址发现

通过借助互联网网络测绘平台，对目标系统进行真实IP发现，绕过CDN、云WAF等防御系统对目标进行攻击。

02

应用漏洞绕过

通过研究目标应用研究目标应用本身是否存在绕过防御技术的功能和漏洞。

03

防御系统绕过

通过摸清对方的防御系统或技术后，在测试环境中对防御产品进行防御技术绕过研究，形成攻击技术方法，达成在攻击过程中不被防御系统发现。

目标防御技术绕过

04

防御系统漏洞

通过摸清对方的防御系统后，在测试环境中对防御系统进行漏洞挖掘，形成攻击技术方法，达成在攻击过程中不被防御系统发现。

05

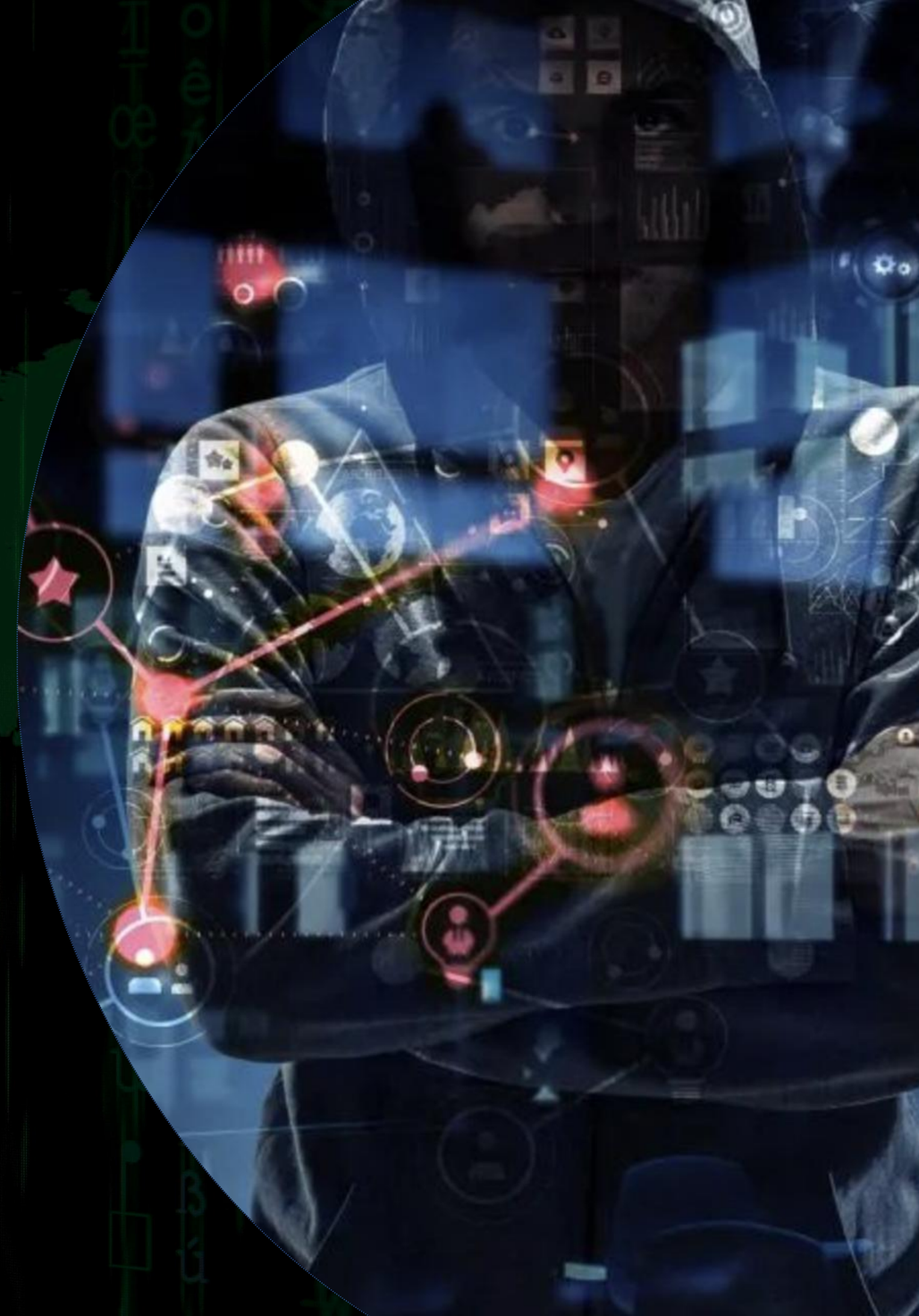
端口复用技术

利用端口复用技术实现隐蔽通道，隐藏对目标的真实网络攻击，同时绕过流量检测进行长期控制，实现数据传输而不被防御系统发现。

06

通信流量加密

通过使用目标的通信加密技术或使用自定义的加密技术实现攻击流量无法被正常检测，维持长期远程控制。



目标防御技术绕过思路图

预渗透 防御绕过	真实地址查找	应用漏洞绕过	防御系统绕过	防御系统攻击	通信隐蔽技术
	域名解析分析	请求加密	WAF防护检测	软件分发功能	通信协议加密
	历史解析查询	另类上传	主机防护检测	白名单功能	私有通信协议
	同站旁站分析	白名单接口	网络防护检测	防护策略关闭	端口复用技术
	全网测绘检索	逻辑漏洞	杀软能力检测	漏洞补丁下发	后门远程激活
预渗透 防御评估	真实地址评估	应用绕过评估	防御绕过评估	防御系统利用	隐蔽通信评估
					预渗透 战术选择

低感知攻击路径设计

隐蔽链路梳理

分析当前攻击需求，根据攻击过程中发现和研究的防御缺陷，梳理隐蔽链路，形成和制定攻击链路计划。

攻击时段划分

按照目标所在地域、作息时间、人员部署、工作内容、节假日等情况有计划性的进行攻击时段划分。

漏洞攻击策略

在对目标发起漏洞攻击前，应根据不同目标的防御程度采用不同的攻击策略，漏洞最小化攻击的同时考虑攻击产出。

Xcon®

HackingGroup

低感知攻击路径设计思路图

预渗透攻击梳理

隐蔽链路梳理

- 应用攻击缺陷隐蔽链路
- 后门基础功能模块设计
- 目标应用自身功能利用
- 知名厂商软件功能利用
- 安全防御缺陷隐蔽链路
- 通信协议加密隐蔽链路
- 防御系统自身功能利用
- 明文传输内容加密通信

攻击时段划分

- 所在国家区域
- 应急响应时间
- 国家劳动法律
- 非工作时间攻击反应
- 工作时间安排
- 防御系统反应时间
- 节假日时间安排
- 跨国公司安全值守

预渗透攻击策略

- 目标防护情况
- 攻击时间计划
- 攻击路径组合
- 攻击成本控制
- 攻击路径优化

预渗透攻击路径

第五部分

[利器]

特种工具与免杀技术应用

Xcon®

HackingGroup

特殊工具与隐蔽性提升

混淆加密

通过对敏感代码片段进行混淆和加密，使恶意代码难以被安全软件识别和分析，提高后门的隐蔽性。

进程注入

利用进程注入技术，将恶意代码注入到操作系统进程中，在用户不知情的情况下执行敏感操作。

无文件落地

通过利用系统自带对功能或将恶意代码注入到内存中执行，实现特殊工具在操作系统中进行良好的隐蔽。

XCON®

HackingGroup

特殊工具与隐蔽性提升思路图

预渗透 后门隐蔽	混淆加密	进程注入	无文件落地
	重要代码分片存储	动态链接库注入	恶意代码内存执行
	重要代码多重加密	远程线程注入技术	系统自带工具执行
	重要代码解密执行	HOOK注入技术	系统脚本权限反弹
	执行文件混淆加壳	PE注入技术	注册表篡改和劫持

预渗透 隐蔽策略	精心编写后门	服务自启动	启动优先加载	后门注入内存	无文件落地执行	预渗透 战术选择

免杀技术集成

使用网上泄露的合法软件签名证书对攻击工具进行软件签名，增强杀软对后门攻击程序的信任度，从而绕过查杀。

软件签名

利用隐藏驱动技术将后门攻击程序在操作系统中进行隐藏，避开防护软件的查杀和检测，使其在目标系统能够长期稳定运行。

隐藏驱动

采用线程注入加载技术，使得关键代码和功能模块与加载器进行分离，在加载器运行时远程加载后门代码及其他功能模块。

后门分离

Xcon®

HackingGroup

免杀技术集成思路图

防御检测与合法绕行

1

终端运维软件

通过技术手段获取目标服务器中运维软件使用的操作系统远程管理密码或凭证，使用远程运维软件对目标进行合法的远程控制。终端运维软件如：Xshell、Xftp、Puuty、SecureCRT等。

2

远程管理软件

通过技术手段获取目标服务器中远程管理软件中的认证密码或凭证，使用远程管理软件对目标进行合法的远程控制。远程管理软件如：RDP、Teamviewer、VNC、向日葵、ToDesk等。

3

开源项目植入

利用知名的开源项目，对目标服务器进行远程控制或植入二次开放的后门组件替换原有功能，实现长期控制。开源项目如：Openssh、Apache、Openssl、Pip、Npm、Jar等。

防御检测合法绕行思路图

预渗透
合法绕行

终端运维软件

- XShell&XFtp
- Puuty
- SecureCRT
- Mobaxterm
- ……

远程管理软件

- Teamviewer
- VNC
- 向日葵
- ToDesk
- ……

开源项目植入

- Python&Pip
- Java&Jar
- Nodejs&Npm
- Golang
- ……

预渗透
合法路径

获取连接凭证 → 运管软件登录 → 开源后门植入 → 后门服务隐藏 → 横向合规绕行

预渗透
合法选择

第六部分

[用兵]

通信安全与攻击时间管理

网络攻击通信安全

攻击流量加密

使用多重加密算法确保攻击指令在传输过程中的安全性，防止被监控发现和阻断。

确保加密安全

启用主控端和被控端双向验证；传输数据中进行数据签名确保请求唯一性；

网络攻击通信安全思路图

网络攻击时间窗口利用

01

攻击窗口选择

通过分析目标防护团队的工作时间窗口，选择在无人值守期间或防守相对薄弱对时期发起攻击。

02

节省攻击时间

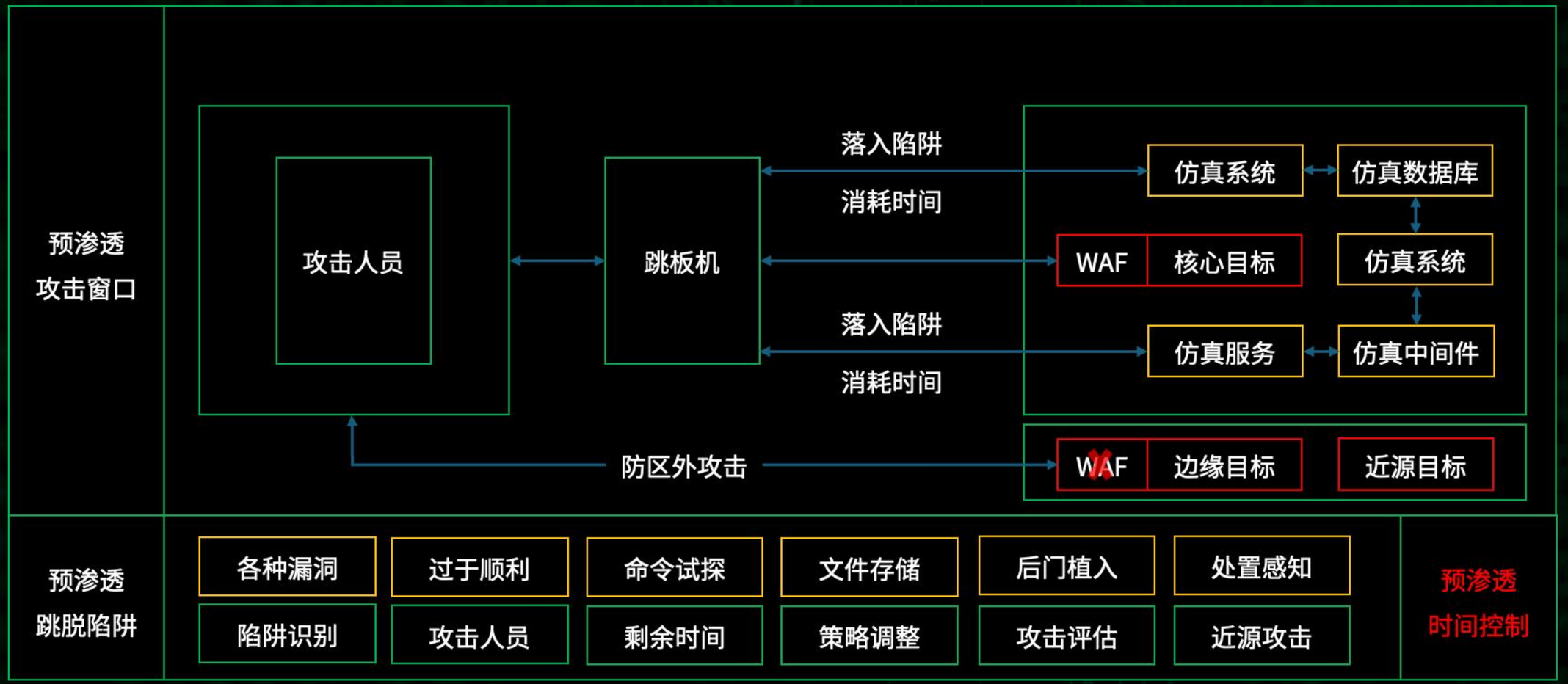
攻击过程中切勿掉入攻击陷阱，进入自嗨模式，理性研判攻击成果，尽快跳脱防御者精心设计的攻击陷阱。

03

优化攻击时间

脱坑后应立即根据剩余时间进行重新规划，可以将计就计的吸引目标火力，组织人员出其不意的从敌后发起攻击。

网络攻击时间窗口利用思路图



漏洞快速打点

攻击漏洞储备

通过前期储备的漏洞和建立漏洞生态圈，对互联网中流行的操作系统、应用漏洞进行提前储备。

时间窗口操作

根据前期获取的情报，在预设的时间窗口内执行关键操作，提高攻击的隐蔽性和效率。

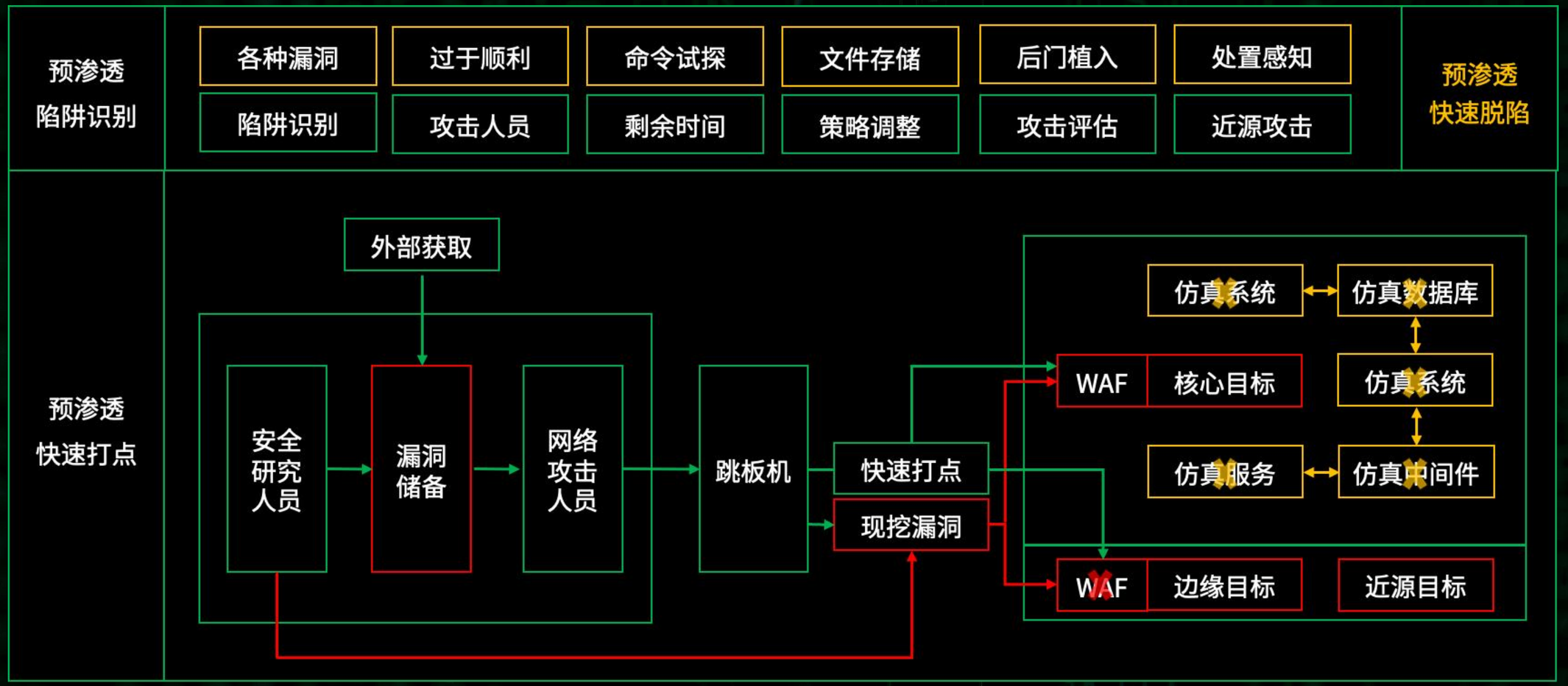
漏洞快速打点

通过指纹识别获取系统指纹类型，对识别指纹后的系统或组件使用特定的安全漏洞进行快速打点。

Xcon®

HackingGroup

漏洞快速打点思路图


预渗透
陷阱识别
各种漏洞
过于顺利
命令试探
文件存储
后门植入
处置感知
陷阱识别
攻击人员
剩余时间
策略调整
攻击评估
近源攻击
预渗透
快速脱陷
预渗透
快速打点
外部获取
安全
研究
人员
漏洞
储备
网络
攻击
人员
跳板机
快速打点
现挖漏洞
仿真系统
仿真数据库
仿真系统
仿真服务
仿真中间件
WAF
核心目标
WAF
边缘目标
近源目标

第七部分

[占领]

防御突破与目标全面掌控

XCON®

HackingGroup

强防御策略战术应对

01

遇强则弱

遇到防御策略较强或很强的目标时，故意对目标站点发起少量散点式攻击，迫使目标防御测发生重大变化，寻找攻击机会。

02

声东击西

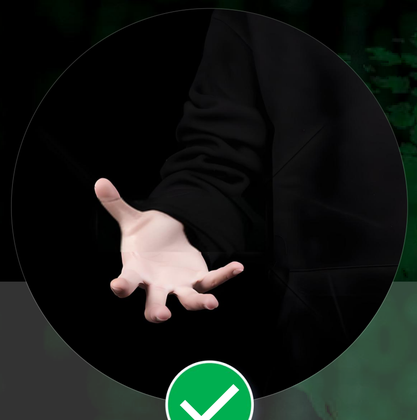
遇到防御策略较强或很强的目标时，突然对非真实目标发起大量扫描攻击，迫使目标抽调人员对攻击目标进行特别防守，产生决策失误。

03

敌疲我打

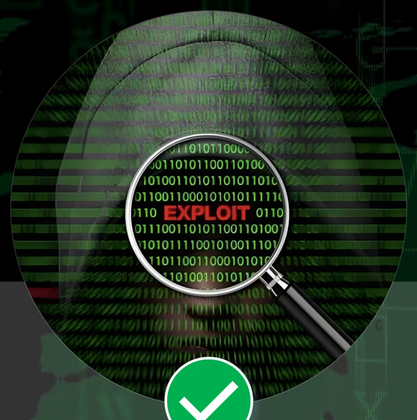
使用多战术混合攻击，造成攻击目标防守人员工作疲惫、重心转移，找准时机给予假性成果造成目标防守人员产生侥幸心理和错误认知。

漏洞挖掘与全面目标掌控



全面掌控目标

按计划全面获取目标网络中的重要数据信息，包括：网络与应用配置信息、数据库、中间件、源代码、办公网权限、运维、供应链等。



持续漏洞挖掘

对目标获取的重要信息组织漏洞研究人员对目标进行全面漏洞分析和挖掘，设定漏洞攻击路径和场景，持续维持目标权限。

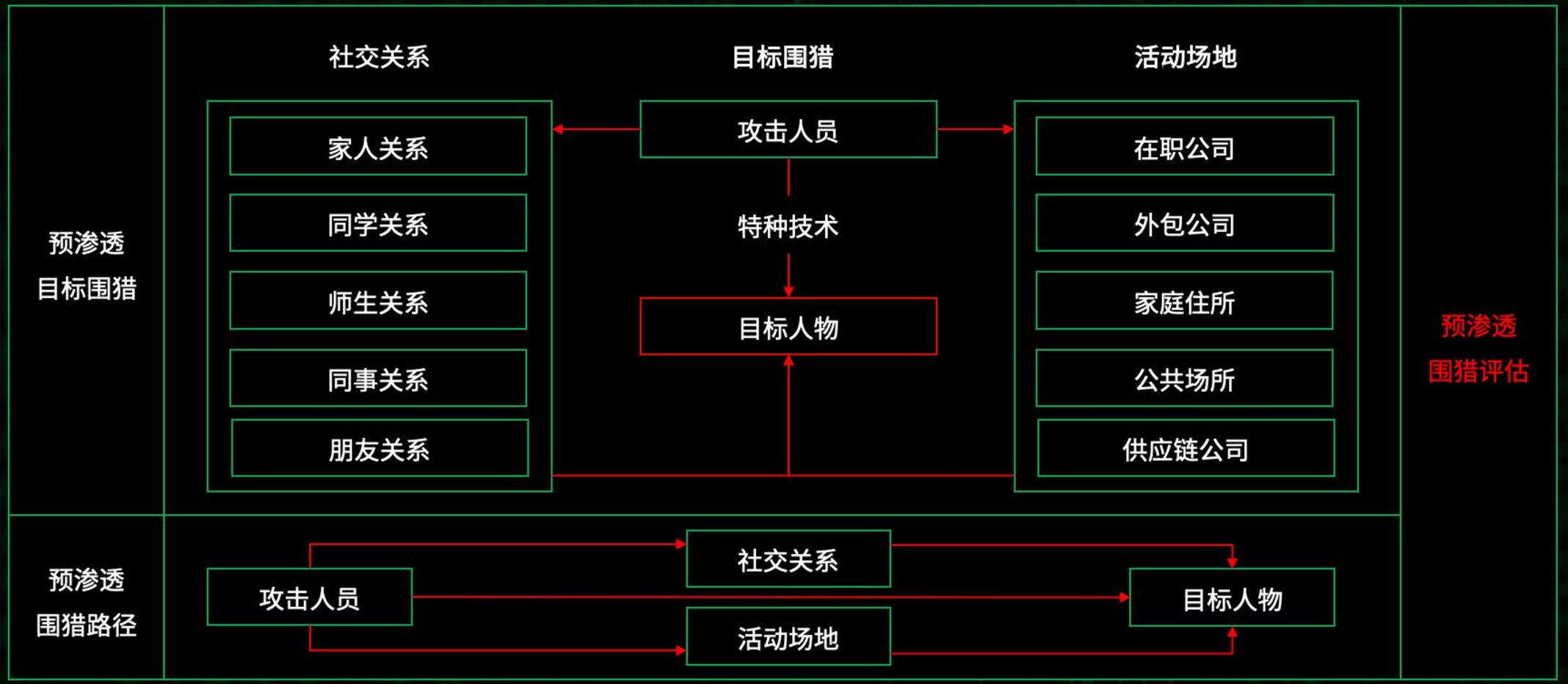
目标关系围猎

解决完漏洞的事情，接下来做的事情就是搞定目标的人，通过对目标数据进行分析，结合目标人际社交和合作关系对目标系统和人员进行围猎。

Xcon®

HackingGroup

社交关系围猎思路图


预渗透
目标围猎
社交关系
目标围猎
活动场地
家人关系
同学关系
师生关系
同事关系
朋友关系
攻击人员
特种技术
目标人物
在职公司
外包公司
家庭住所
公共场所
供应链公司
预渗透
围猎评估
预渗透
围猎路径
攻击人员
社交关系
活动场地
目标人物

第八部分

[持久]

新型威胁评估与持久控制

新型威胁下的风控策略调整

01

财力威胁评估

根据开源数据和商业数据，对评估目标整体财务状况评估，分析每年度安全领域的投入财务预算和引入的外部能力和服务预算。

02

人力威胁评估

根据目标的历史人力和招聘岗位数据，结合引入的外包团队人员进行岗位职能分析，综合评估目标安全能力现状。

03

物力威胁评估

根据目标现有的网络、安全防护和运维设备等，结合实际安全配置策略、网络配置策略进行整体安全防护力分析。

04

政策威胁评估

根据目标国家和地区出台的最新网络安全政策或其它信息领域政策进行涉安全领域威胁评估，并及时调整和制定应对计划。

新型威胁下的风控应对思路图

预渗透 威胁风控	财力威胁 目标工商数据 主营方向现状 投标招标情况 安全投入情况 商业情报分析	人力威胁 安全人员数量 安全人员能力 外包人员能力 安全招聘情况 安全领导能力	物力威胁 网络设备情况 网络防护情况 主机防护情况 WAF防护情况 安全基线配置	预渗透 威胁评估
预渗透 政策威胁	新出台法律	进出口管制	国家安全政策	实体黑名单 商业竞争打压	预渗透 威胁应对

Hacking Group

感谢聆听

正道网安 功德无量