对抗思路及常用手法解析

2019护网专项培训

NSFOCUS

CONTENTS

目 录

01

护网行动规则解析

1. 攻击方规则
2. 防守方规则
3. 规则要点
4. 护网行动与安全测试差别

护网行动规则-攻击方

- 发现漏洞不得分，利用漏洞获取权限、数据才能得分，得分范围包括：
  - ✓系统层权限（域控、web 服务器、邮件服务器、数据库服务器、终端机等操作系统权限）
  - ✓设备、应用管理权限（路由器、交换机、防火墙其等他设备，web 后台管理）
  - ✓业务网账号密码（邮箱、ftp、vpn、数据库等）
- 限定攻击目标系统，不限定攻击路径，攻击路径上的资产权限均有得分
- 指定 5 个生产业务类系统，获取控制权限将得到 **10000** 分
- 明确规定了演习过程中严禁使用，谨慎使用和允许使用的攻击方式
  - 禁用一定会造成业务异常的行为：DoS，ARP、DHCP 欺骗，DNS 劫持，收买目标人员，物理攻击等
  - 慎用可能影响业务正常运转的操作：提权，远控，篡改

护网行动规则-防守方

减分项

类型	分类	赋值	备注
获取权限	被获取终端计算机权限	10 分/台	累计不超过 200 分
	被获取 webshell 权限	20 分/个，特别重要的附加 20 分	累计不超过 300 分
	被获取业务内网邮箱、FTP 应用、WEB 应用系统、数据库远程访问、互联网VPN 接入系统的账号密码	普通权限 20 分/个 管理员 60 分/个 特别重要的，附加 60 分	同一设备两种权限扣分取高值，累计不超过 800 分
	被获取 WEB 应用系统服务器、邮件服务器、数据库服务器等权限	普通权限 60 分/个 管理员 100 分/个 特别重要的，附加 100 分	两种权限扣分取高值，累计不超过 1200 分
	被获取域控服务器权限	管理员 300 分，特别重要的，附加 300 分	累计不超过 3000 分
	被获取路由器、交换机、防火墙等网络设备权限	接入层：50 分 汇聚层：100 分 特别重要的，附加 100-200 分	累计不超过 1000 分
	被获取其他设备权限	/	由裁判组核定

护网行动规则-防守方

加分项

工作阶段	得分标准	赋值	备注
发现攻击	发现木马攻击	50 分/个	得分累计不超过 500 分，提交拦截证据截图
	发现钓鱼邮件	20 分/个	得分累计不超过 200 分，提交分析报告和 eml 格式文件
	发现漏洞攻击	50 分/个	得分累计不超过 500 分，提交分析报告和攻击负载附件
	发现其他攻击（工控系统等）	/	由裁判组核定给分
消除威胁	处置 webshell 木马或主机木马程序	50 分/个	得分累计不超过 500 分，提交分析报告，包括木马样本及分析报告、控制流量证据等
	处置 web 系统、FTP 等异常新增账号，处置被爆破账号密码	20 分/个	得分累计不超过 200 分，提交分析报告，包括账号异常登陆源 IP、审计日志证据、异常登陆流量证据等。
	处置主机异常新增账号，处置被爆破账号密码	50 分/个	得分累计不超过 500 分，提交分析报告，包括账号异常登陆源 IP、系统审计日志证据、异常登陆流量证据等。
	消除其他威胁（工控系统等）	/	由裁判组核定给分
配合应急处置	积极配合应急组工作，根据线索能快速准确定位受害系统，能提供充分的日志记录，配合执法机关固定证据完成勘验	高效完成：+300 一般：+200 差：-100	最高 300 分，最低 -100 分

规则要点

01

以获取权限数据为目的

- 获取主机、域控权限
- 获取内部数据
- 普通的xss或者sql注入基本不得分

02

社会工程结合使用

- 邮件钓鱼
- QQ群等测试账号获取

目的性的穿透攻击，非传统类的全面测试

03

横向渗透

- 内网扩大攻击
- 域控权限分数最高

04

定向攻击

- 定制爆破弱口令字典
- 获取内部系统定向数据

合理利用规则，扩大漏洞的影响面，最大化得分

与普通安全测试区别

- **安全测试目的是全面的发现企业的安全问题，红蓝对抗目的是穿透攻击，以获取目标为目的的攻击。**

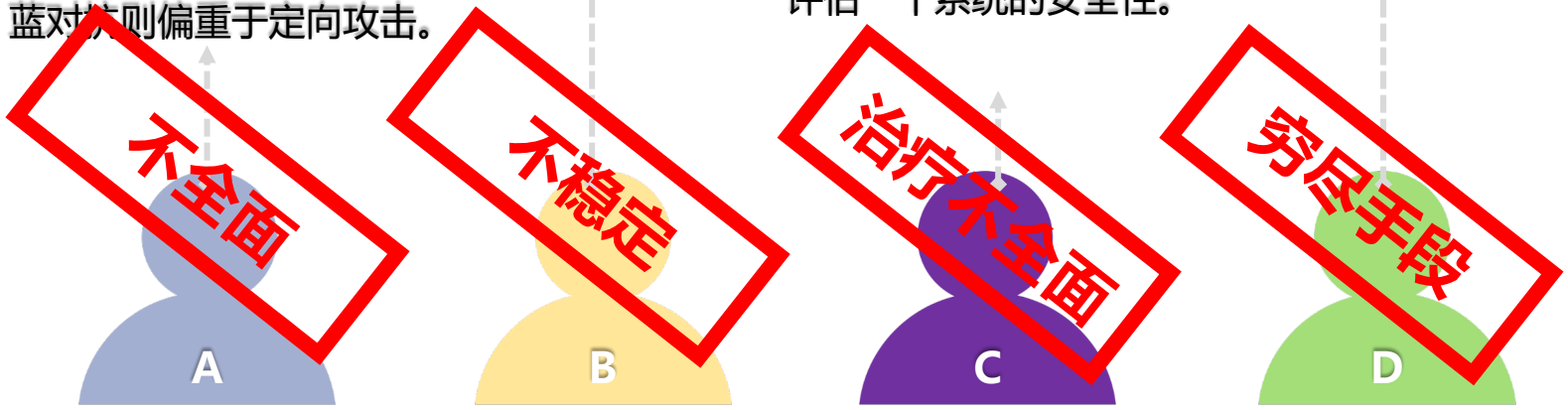
安全测试：点到为止，以此全面修复
红蓝对抗：千里之堤毁于蚁穴

区别1：安全测试侧重于尽量全面的发现系统问题，高中低危风险全覆盖，红蓝对抗则偏重于定向攻击。

区别2：安全测试往往会根据提供的账号，对内部功能进行全面测试。红蓝对抗如果无法获取内部账号，可能发现不了内部的风险，也就不一定能攻击成功。

区别3：红蓝对抗会将一个小漏洞尽量最大化利用， 获取最大的数据，往往无法全面的评估一个系统的安全性。

区别4：红蓝对抗会穷尽手段达到想要的目的，利用如钓鱼等社会工程学方式发起任何类型的攻击



02

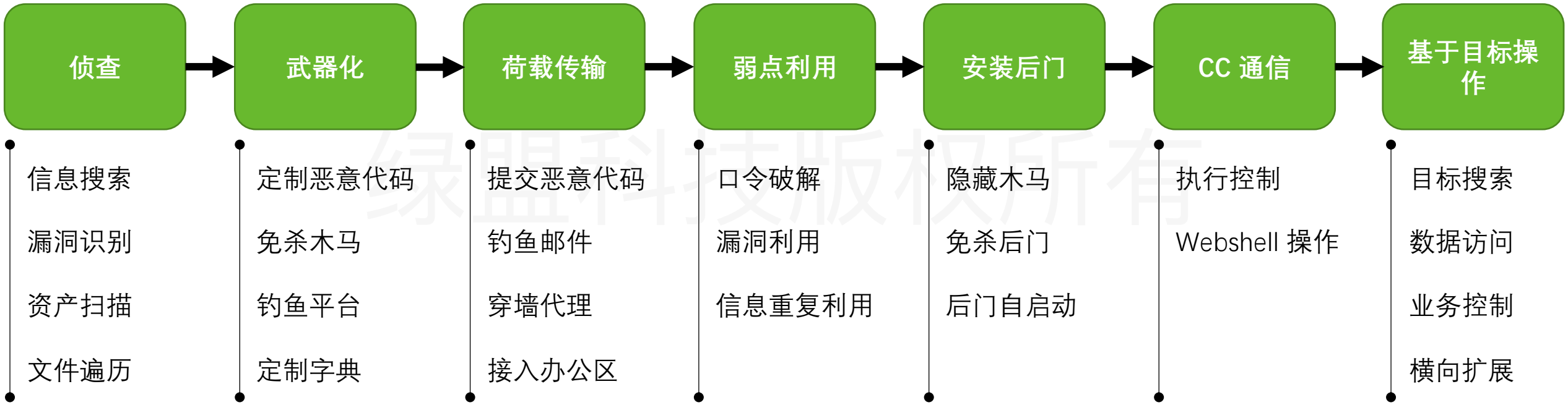
常见攻击思路及防护

1. 常见攻击思路
2. 常见防护方法

护网攻击工作开展方式

工作方式	每支队伍 出口 IP 全国变化，无明显规律
攻击方式	信息收集、扫描、漏洞利用、内网渗透等

攻击流程



攻击思路

APP

社会工程学

弱口令

注入攻击

入侵痕迹

Wi-Fi

NdayRCE

上传 getshell

VPN

子域名

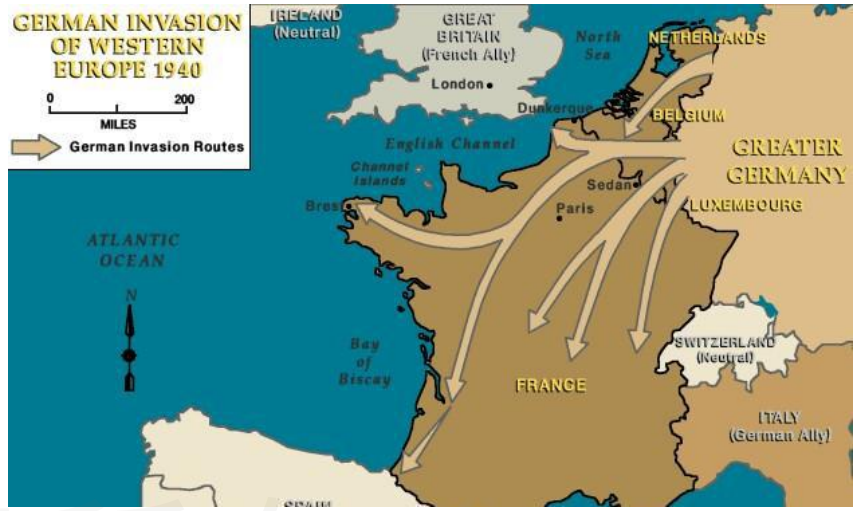
边角系统

数据库

废弃资产

侦查-扩大攻击面

攻击方在正面战场受阻的情况下，很有可能扩大攻击范围。通过入侵相邻或相关系统，绕过正面防御对目标系统进行攻击。

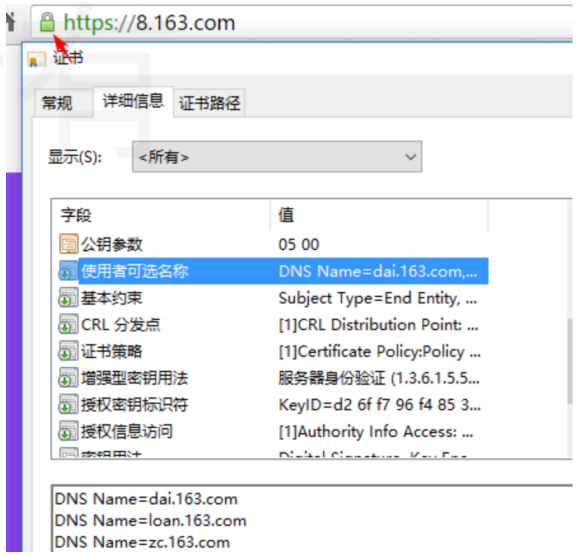


子域名收集	端口扫描	Web扫描	APP及微信
子域名爆破 https证书 搜索引擎 …	业务系统所在ip段的c段扫描 搜索引擎关键字 Github搜索	AWVS扫描初筛 Poc扫描器	App资产收集 微信及小程序信息收集

子域名收集

子域名爆破 → Subdomains，layer等工具

页面暴露子域名 → 查看网页源码



https证书泄露

DNS解析记录 → **nslookup** -qt=any bing.com

目的：扩大攻击面，寻找边缘系统

端口扫描

端口扫描

Telnet、SSH、RMI、DB

Web：80、443、8080、8443、7001 等

漏洞利用

信息复用

RCE

端口扫描-口令猜解

- 弱口令
  - 常见弱口令 top xxx
  - 测试账户
- 预测口令
  - 口令规律
    Hu%x(0@d241（IP 地址）
    dev@pdrs2013（年份）
  - 口令组合简单
    nsfocus@123
    nsfocus@*()
- 口令复用
  - 默认口令
    - huaweiadmin
  - 批量 SSH 口令一致
- 账户名
  - 常用管理账户名
  - 手机号
  - 人名相关
    - 中国人名拼音 top 100
    - Liyuan.ssd

Web扫描

快速找出cms类型
利用已公开的漏洞快速打开突破口

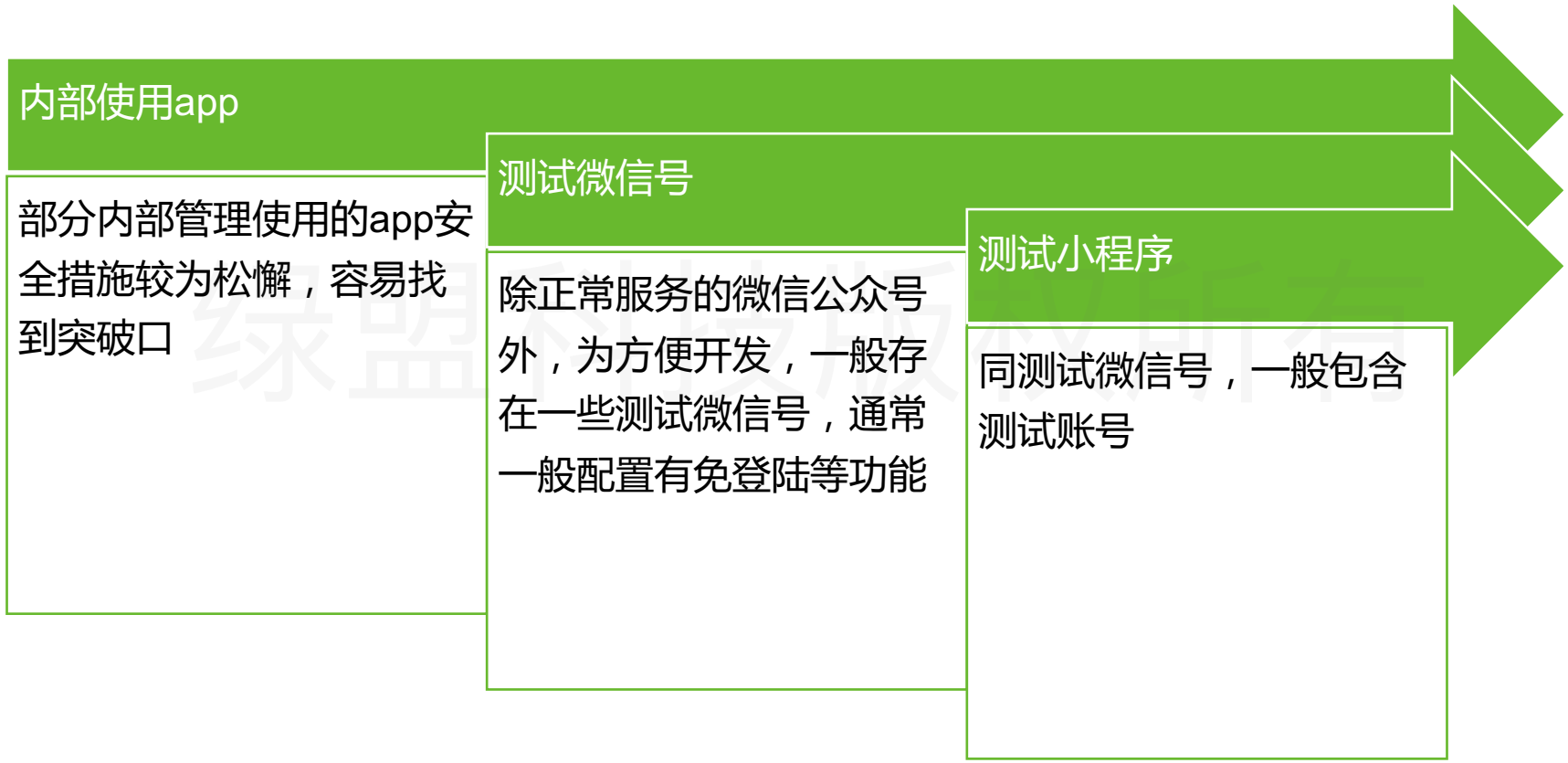
- ✓ discuz
- ✓ wordpress
- ✓ phpcms
- ✓ …

基于已知漏洞的poc，对目标进行扫描，
利用已知漏洞打开突破口

- ✓ struts2系列漏洞
- ✓ weblogic系列漏洞
- ✓ fastjson反序列化
- ✓ …

App及小程序

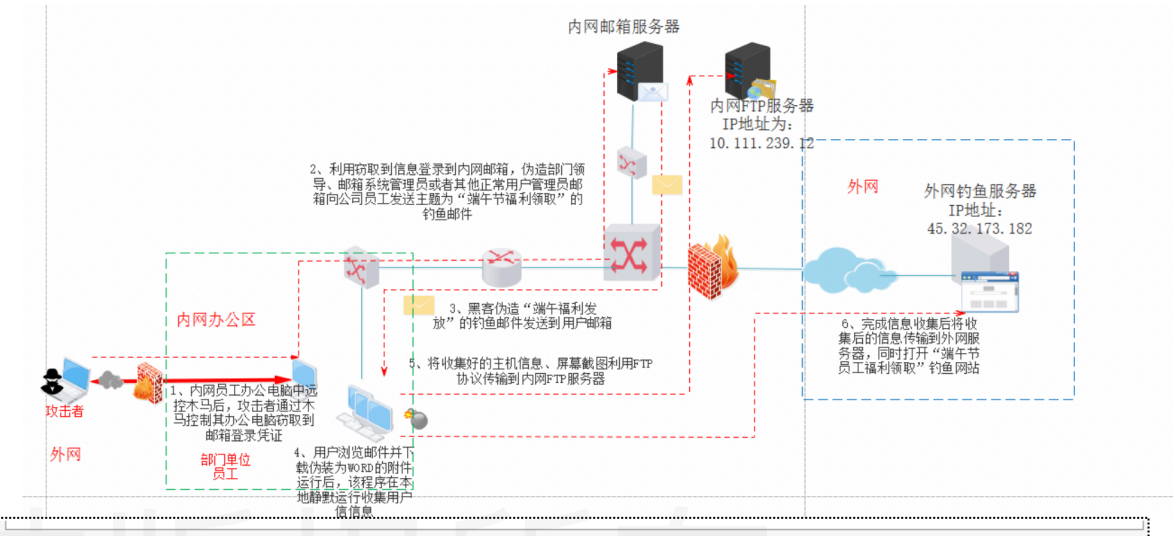
内部使用app

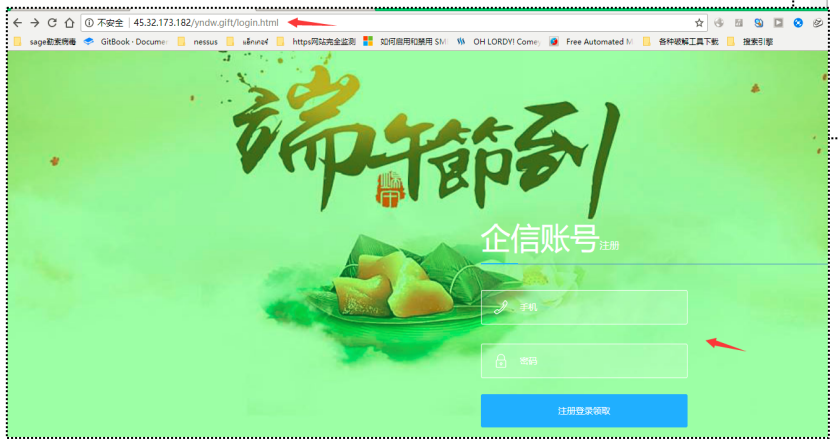


扩大攻击面，找到突破口

社会工程学

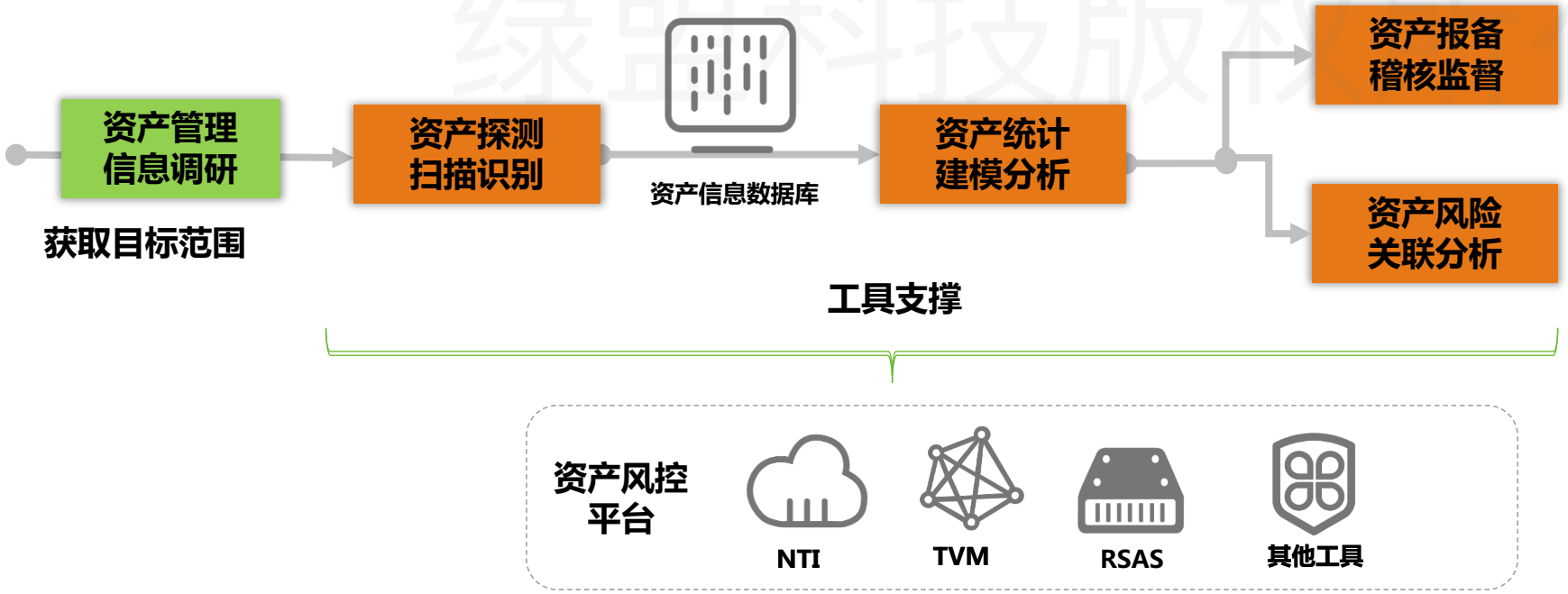
- 区别于传统安全测试，护网行动通常会包含红蓝对抗的社会工程学操作。
  - 邮件钓鱼
  - QQ群信息泄露





反侦察——互联网暴露资产自查

针对暴露在互联网的资产进行全面清查梳理工作，对于检测到所有暴露在互联网的端口及服务进行排查与检测等；梳理暴露在互联网上的网站/系统/平台，明确网站与系统的主管单位和具体责任人，形成详细清单。



- ✓ 全网端口信息扫描
- ✓ 互联网资产深度检测
- ✓ IP\端口\域名\应用关系梳理
- ✓ 三无七边资产排查与梳理
- ✓ 资产无用及冗余端口排查
- ✓ 互联网资产暴露必要性评估

NSFOCUS

安全域划分及安全策略调整

- 列入护网范围的业务系统必须独立进行安全域划分，禁止同其他业务系统混合部署
- 列入护网范围内的业务系统需要有独立的安全防护策略，安全策略必须遵守最小开放，全面覆盖的原则
- 列入护网范围内的业务系统与其关联系统的访问关系需要严格梳理，尽量减少周边业务系统的使用

反侦察——安全意识培训与评估

弱口令

办公场所

邮件钓鱼

陌生人员识别

信息泄露

废纸回收

突破——web

常见cms及框架

Discuz

- Discuz_ < 3.4_birthprovince_前台任意文件删除

DedeCMS

- DedeCMS_v5.7_shops_delivery_存储型XSS
- DedeCMS_v5.7_carbuyaction_存储型XSS
- DedeCMS_v5.7_友情链接CSRF_GetShell
- DedeCMS V5.7 SP2后台存在代码执行漏洞

Struts

- S2-048
- ...

ThinkPHP

- 远程命令执行
- 日志泄露

PHPCMS

- sql注入
- 命令执行
- ...

web通常为系统进入的大门，通过已知的漏洞快速找到撕破防御的突破口

快、狠、准

突破——RCE

中间件

weblogic	IIS	Tomcat	jBoss
• 反序列化漏洞 • 弱口令war包上传 • ssrf漏洞	• 远程代码执行 • 解析漏洞	• 弱口令war包部署 • PUT漏洞	• 反序列化漏洞 • war 后门文件部署

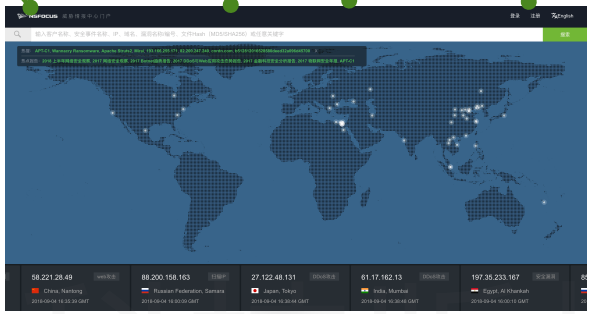
反突破——做好监测、防护

互联网资产类情报

互联网威胁类情报

漏洞情报

情报咨询



提供大量分散设备的异构日志进行集中采集、统一管理、存储、统计分析

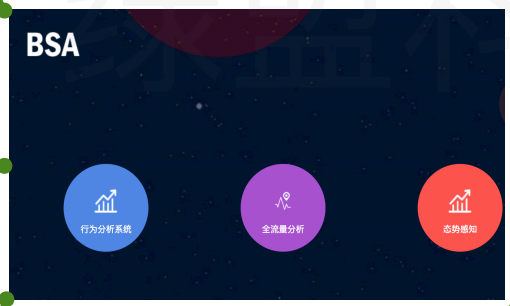
网络日志审计

流量存储、入侵检测、病毒检测及吸星等各类检测能力，提供安全威胁的检测能力，

全流量探针

转储并分析流量中的攻击行为，并提供事件追溯以往攻击

全流量分析



NTI

安全专家

BSA

ESPC

信誉库

对URL、IP、C&C、文件等进行信誉判断

威胁管理

接入自由检测和防护类设备，对各类攻击行为集中告警

资产管理

基于IP、名称、开放端口和应用对企业内部IT资产进行管理

设备管理

对安全设备的各类指标进行检测，集中展示安全产品的运行状态

日志审计

TAM

WAF

IDS/IPS

TAC

HWAF

内网深入攻击

翻文件

环境变量

口令复用

Bash_history

网络连接

跳板选择

.ssh

访问历史

部署代理

内网漏洞挖掘

后门部署

权限提升

Dumphash

主机发现

内网端口扫描

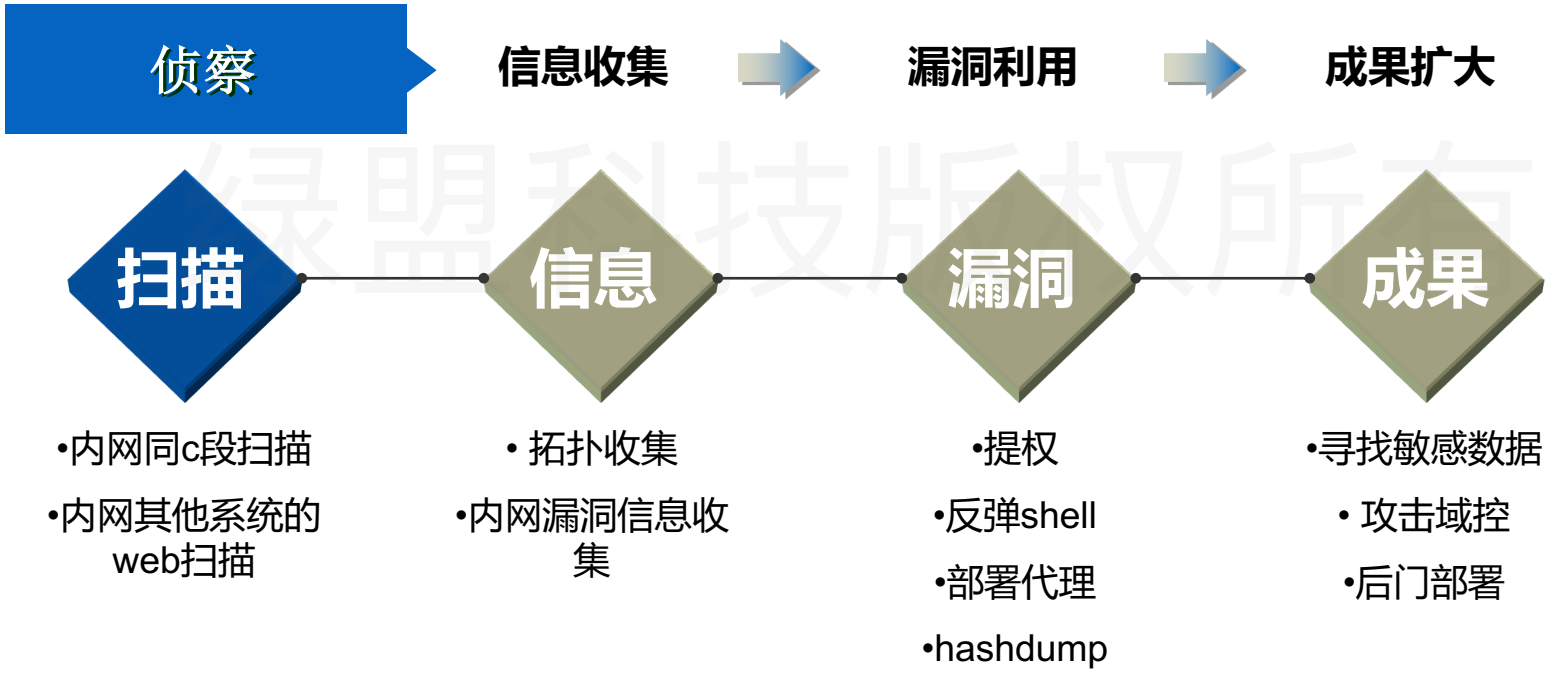
系统信息

文件上传

攻击域控

深入攻击

- **在找到内网突破口后，进入内容进行横向纵向上的攻击，扩大攻击成果**

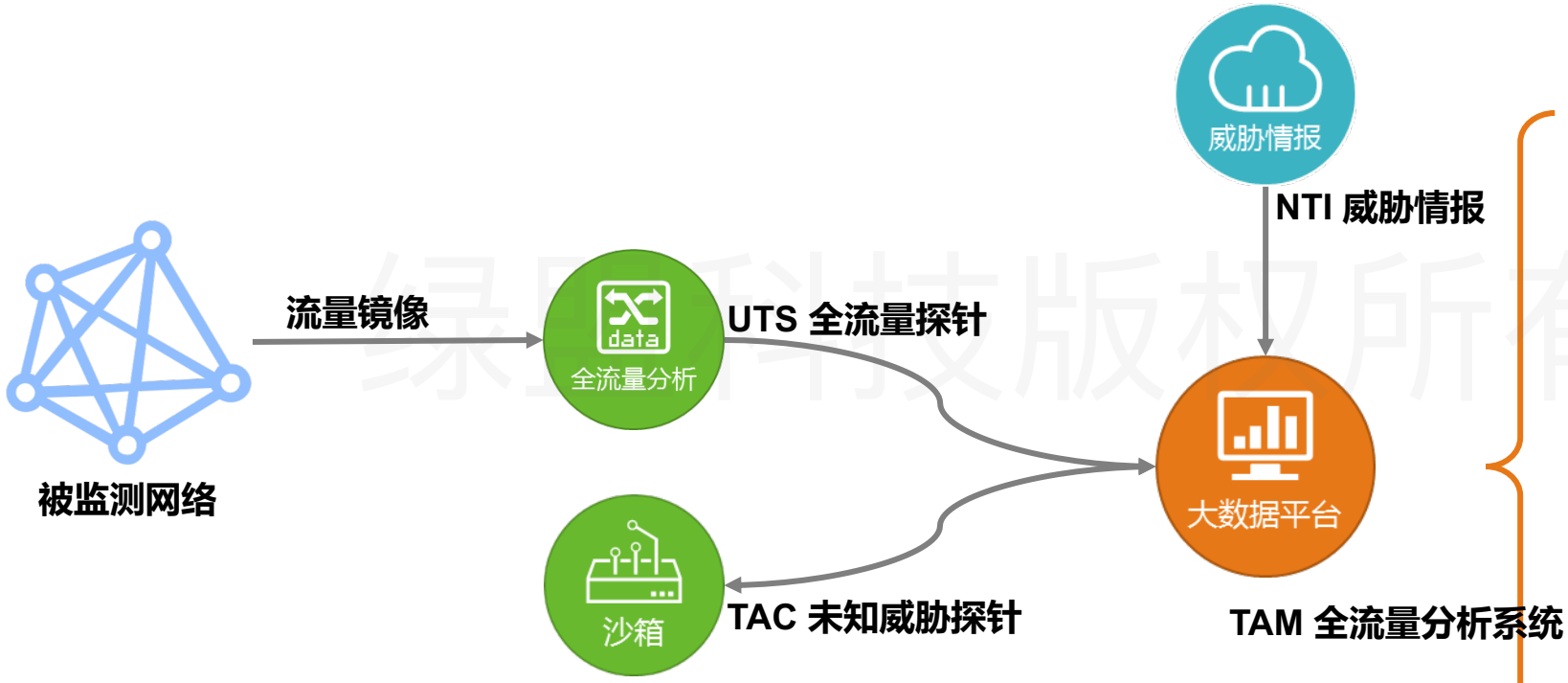


权限维持

- C2阶段权限维持
  - Cs（Cobalt Strike）
  - metasploit

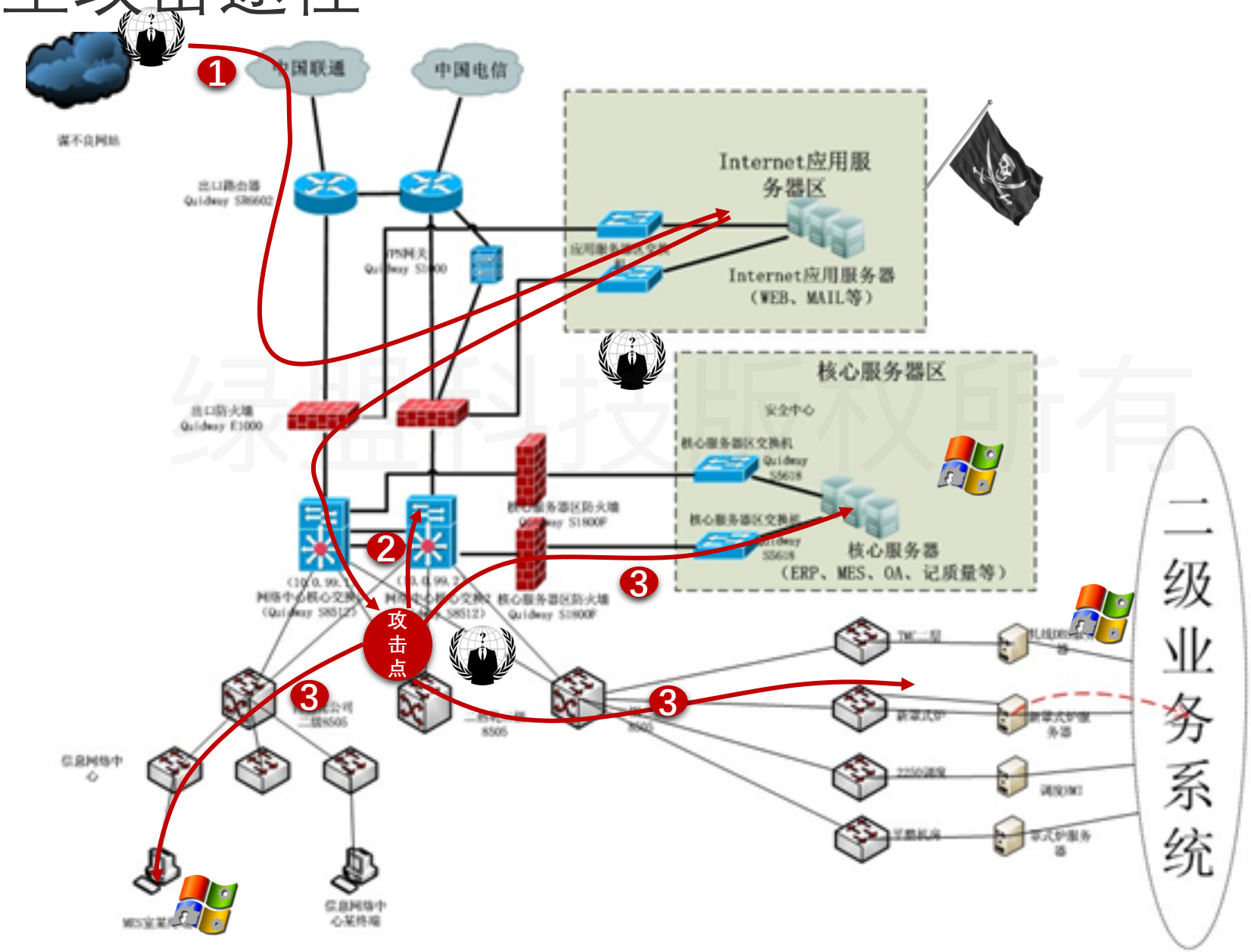
payload生成 → shell反弹 → 持续性控制

全流量架构



- 高危事件监控
- 失陷资产监控
- 攻击者画像
- 流量监控
- 资产监控
- 情报分析
- 攻击链分析
- 流量黑名单监控
- 应急事件分析
- 自定义场景分析

典型攻击途径



护网防护工作整体流程及思路

备战阶段	临战阶段	决战阶段	总结阶段
护网前2个月	护网前1个月	周期半个月	护网结束
减少攻击面	模拟演练	实时监测响应	应急防护总结
1、团队组建 2、减少攻击面 3、全面隐患自查 4、安全加固 5、策略优化 6、防护措施落地	1、安全宣贯培训 2、安全演练与总结	1、现场值守 2、威胁监测 3、分析研判 4、情报共享 5、协同处置 6、应急响应 7、防护策略优化	1、总结并沉淀知识 2、编制总结报告 3、攻击还原分析 4、应急防护优化

防护技巧

1. 非所属资产被扣分一定要上诉
2. 若攻击方提供的报告是内网资产，要求证明是我方资产。
3. 保持严谨态度，无确凿证据绝不承认

防扣分技巧

1. 关注文件沙箱告警日志，分析样本
2. 关注高危漏洞告警，例如反序列化，注入类漏洞，系统层获取权限类漏洞
3. 扫描事件上报不加分

拿分技巧

1. 善用IP封禁，境外IP一律封禁
2. 加强内网防护
3. 专职样本分析人员
4. 漏洞利用攻击和木马攻击避免失分

防护建议

1. 报告上报内容：源IP，事件类型，流量分析（全流量），有样本需分析样本并附上样本，切忌只截设备告警图
2. 内部沟通以微信为主，避免流程限制时效

内外部沟通

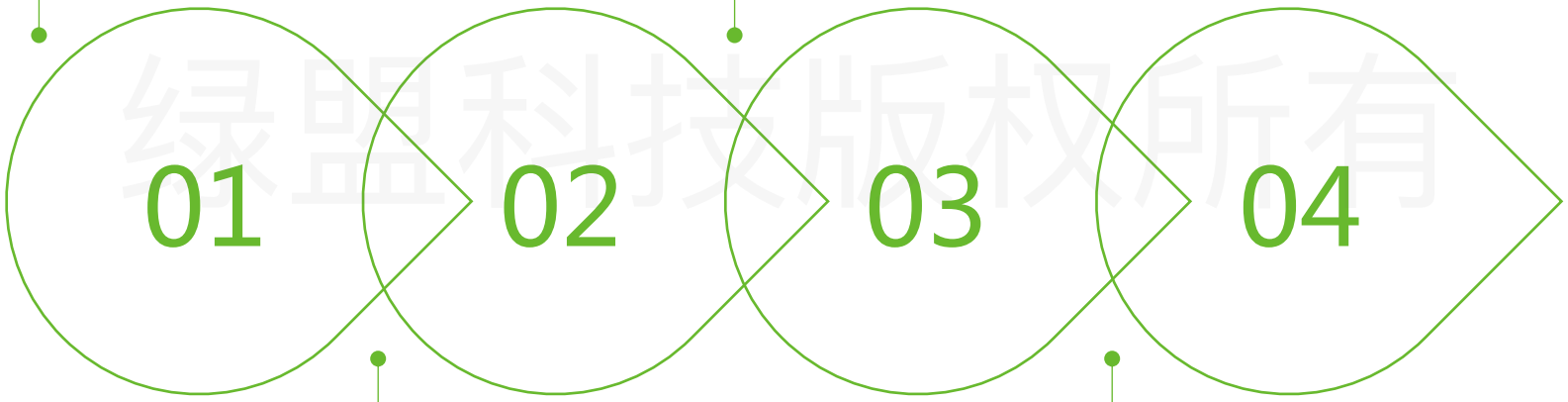
03

案例分享

某学校域控攻击案例

侦察：官网采用thinkphp框架默认配置，log日志发现后台用户名及密码

深入攻击：对内网所在C段进行深入扫描攻击，发现众多ms17010漏洞

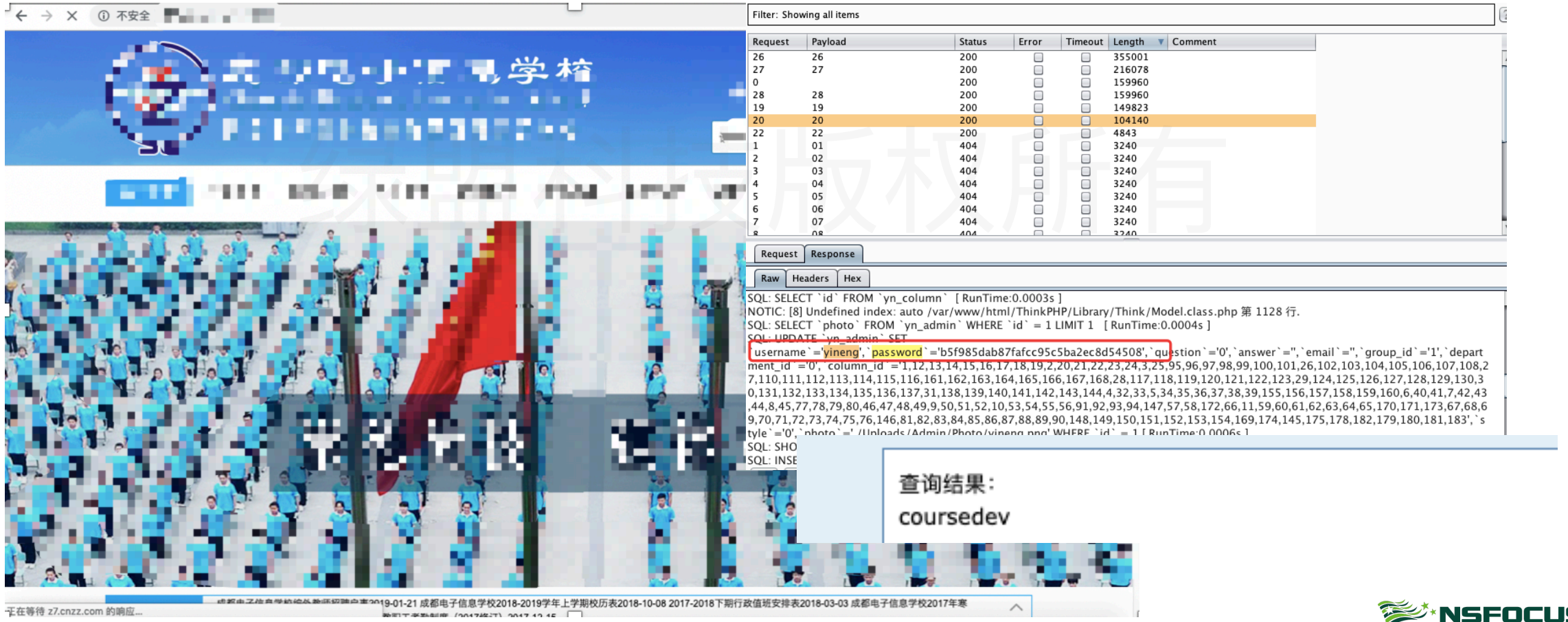


突破：后台文件上传拿到外网web服务器权限

权限维持、扩大战果：hashdump读取账户密码，对内网进行登录，发现域控机器

侦察

- 通过cms识别等工具，识别目标站点为thinkphp框架
- 同时存在log泄露，翻找log发现账号和密码

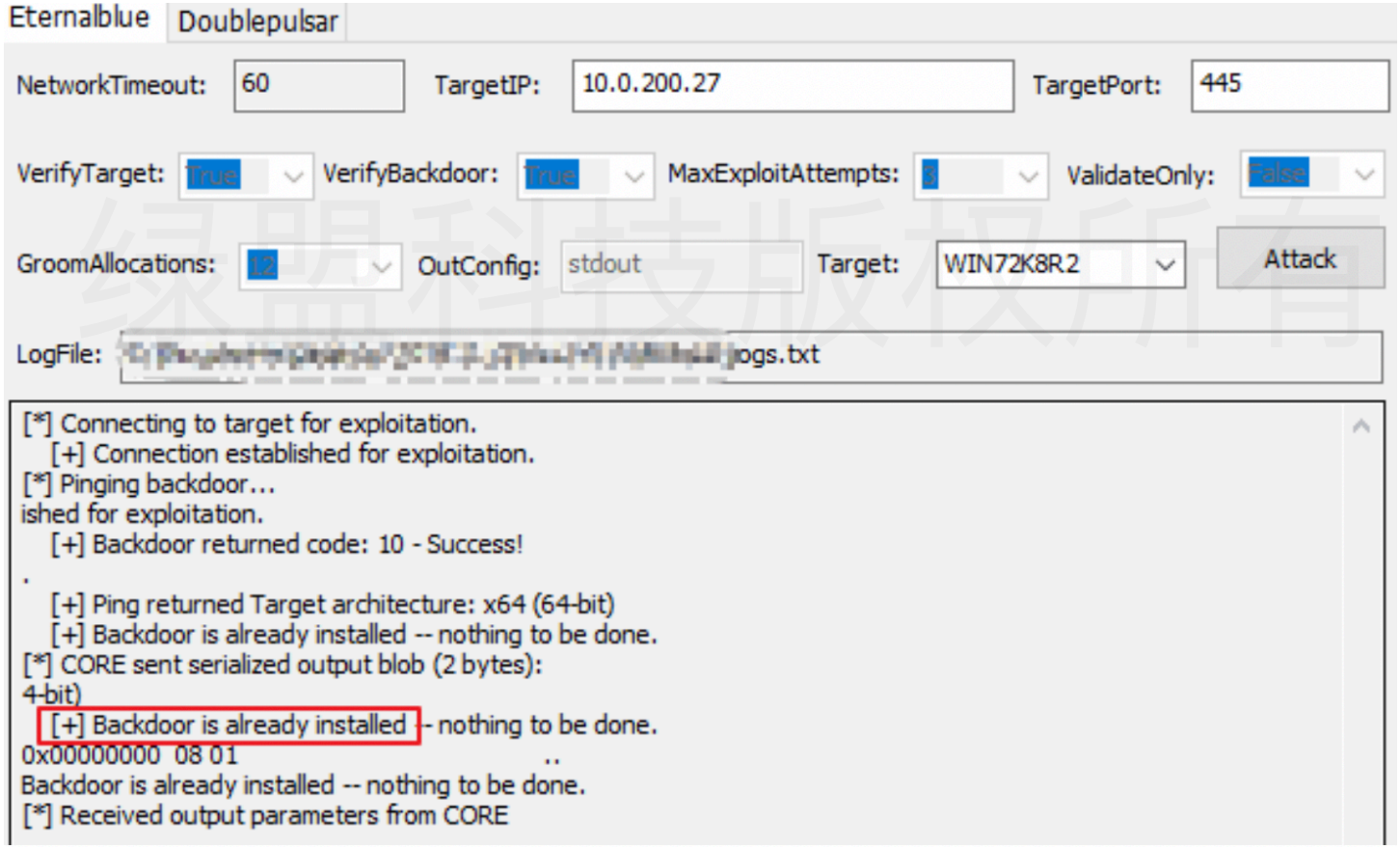


突破

- 登录后台添加php后缀为可上传文件
- 直接上传php后缀的webshell

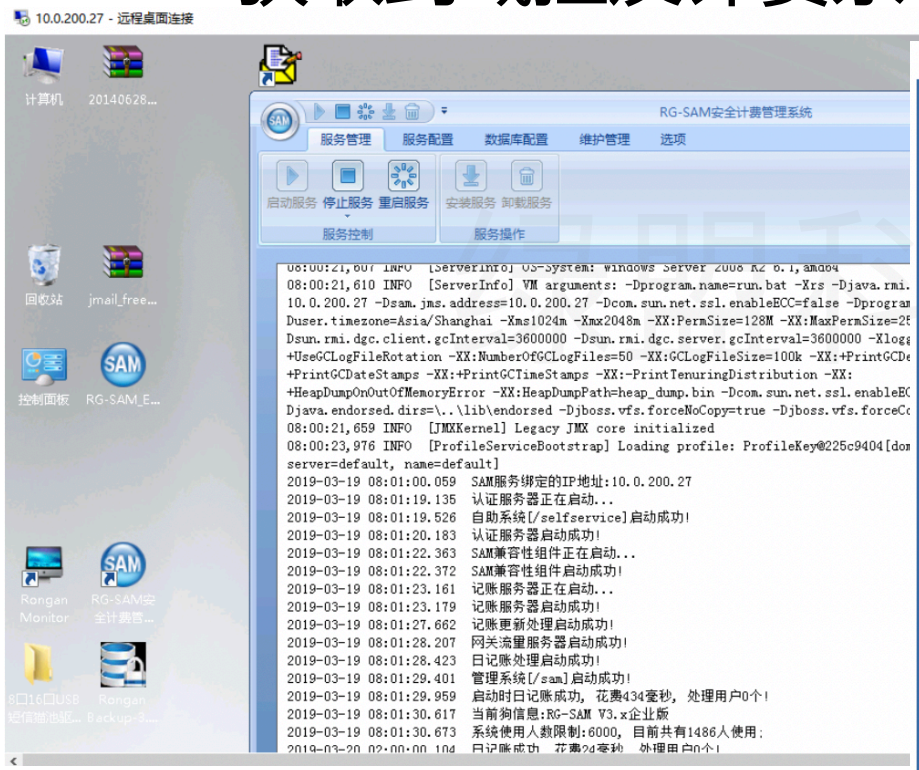
深入攻击

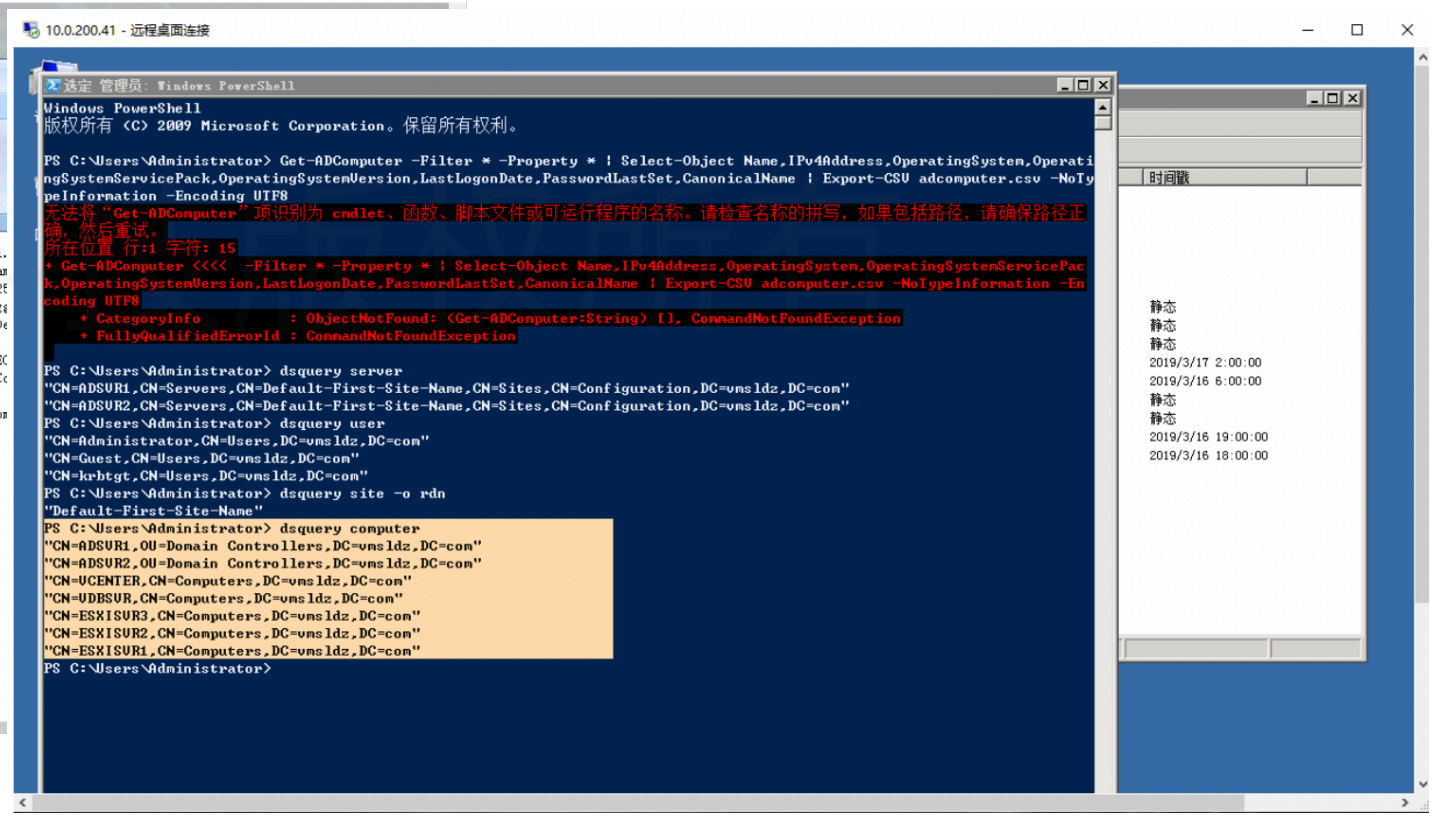
- 对服务器所在c段进行扫描，数台服务器存在MS17-010漏洞，直接获取服务器最高权限



扩大影响

- 对内网业务系统进行深入测试扩大影响
- 获取到域控及计费系统权限





谢谢！

NSFOCUS