



# 对抗思路及常用手法解析

绿盟科技版权所有

2019护网专项培训



# CONTENTS 目录 >>>

- 01 护网行动规则解析
- 02 常见攻击思路及防护
- 03 攻击案例分享



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、防火墙等其他设备，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**

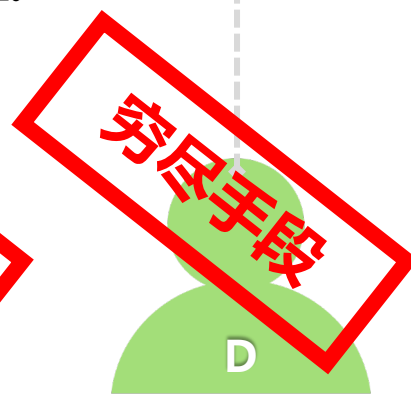
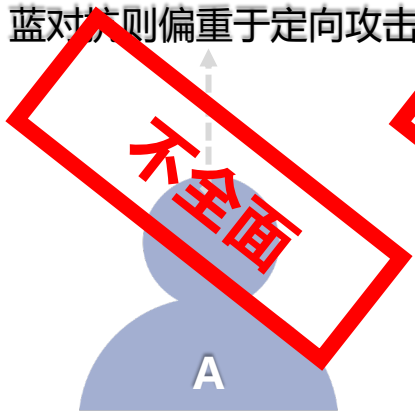


区别2：安全测试往往会根据提供的账号，对内部功能进行全面测试。红蓝对抗如果无法获取内部账号，可能发现不了内部的风险，也就不一定能攻击成功。

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

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。







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

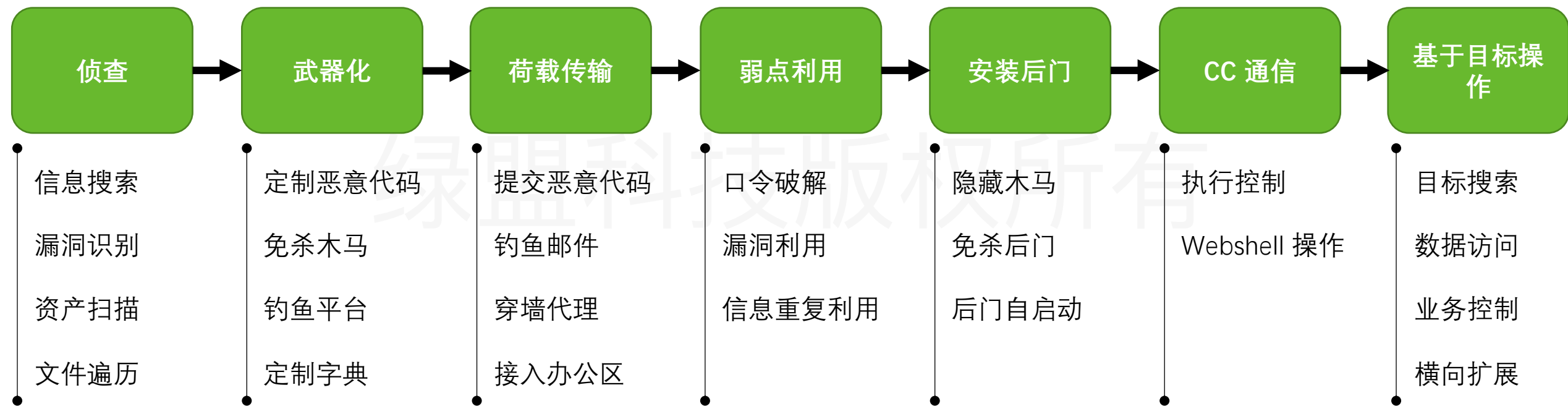
工作方式

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。



子域名爆破

https证书

搜索引擎

...

子域名收集

业务系统所在ip段的c段

扫描

搜索引擎关键字

Github搜索

端口扫描

AWVS扫描初筛

Poc扫描器

Web扫描

App资产收集

微信及小程序信息收集

APP及微信

# 子域名收集

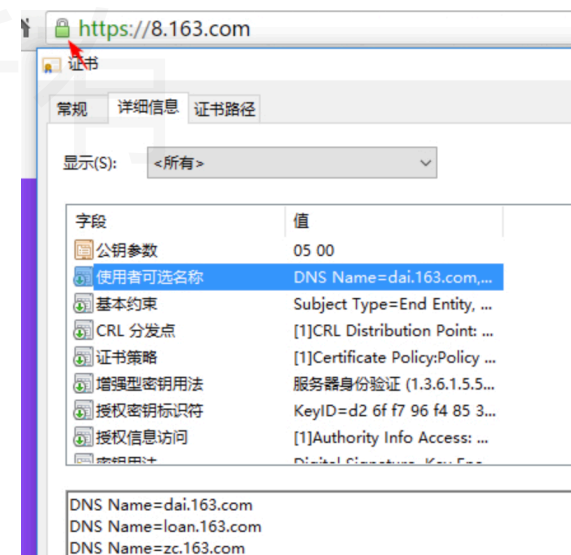
子域名爆破

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



绿盟科技版权所有

# ▶▶ 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

## CMS识别

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
- ✓ ...

## POC扫描

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

### 内部使用app

部分内部管理使用的app安全措施较为松懈，容易找到突破口

### 测试微信号

除正常服务的微信公众号外，为方便开发，一般存在一些测试微信号，通常一般配置有免登陆等功能

### 测试小程序

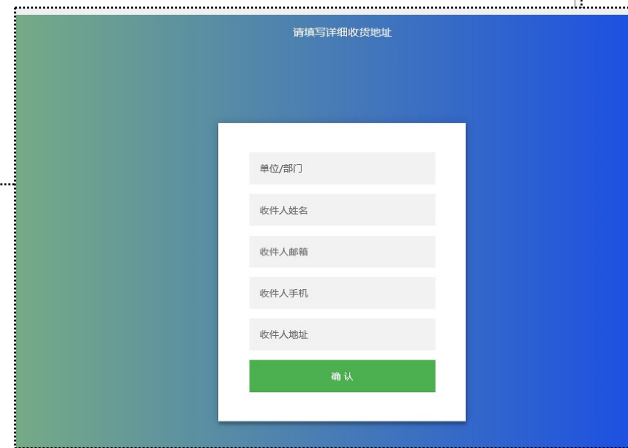
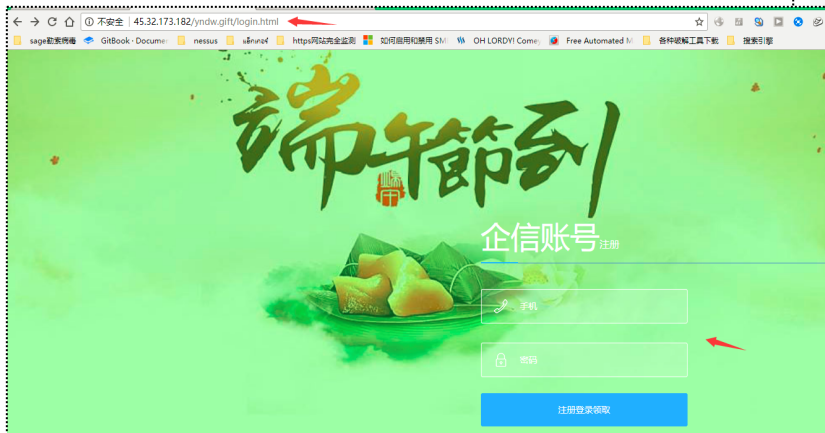
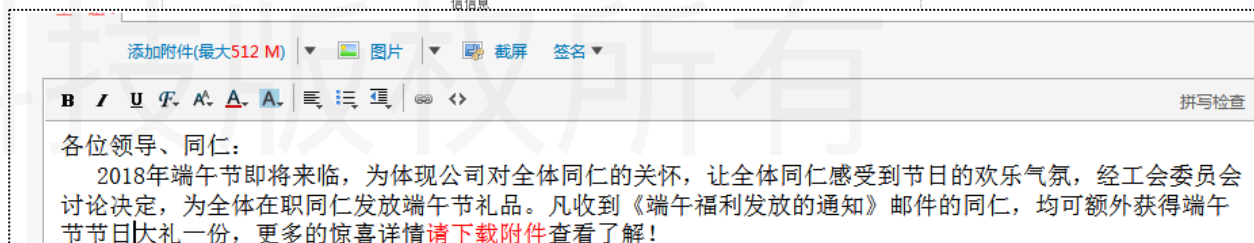
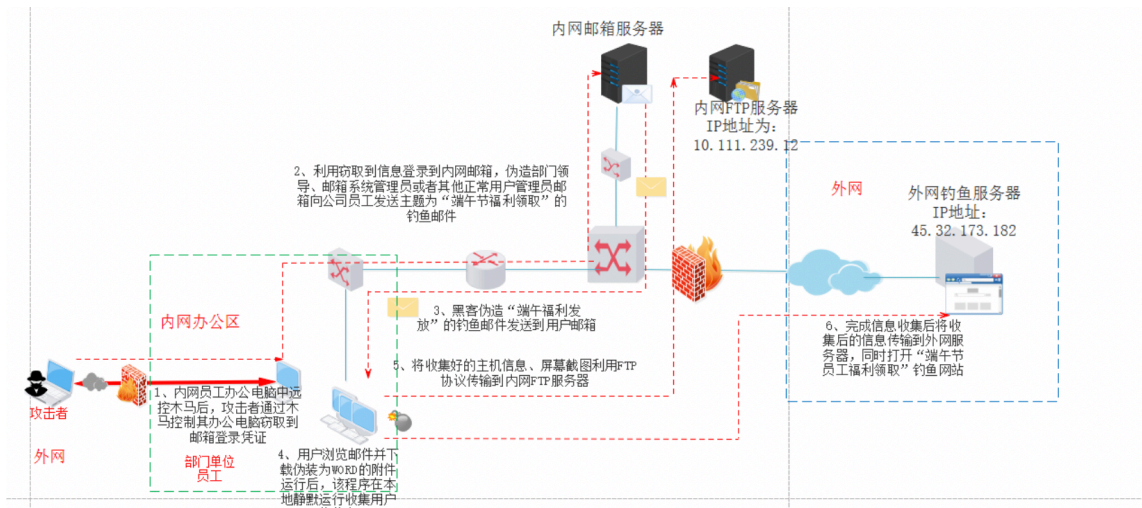
同测试微信号，一般包含测试账号

**扩大攻击面，找到突破口**

# 社会工程学

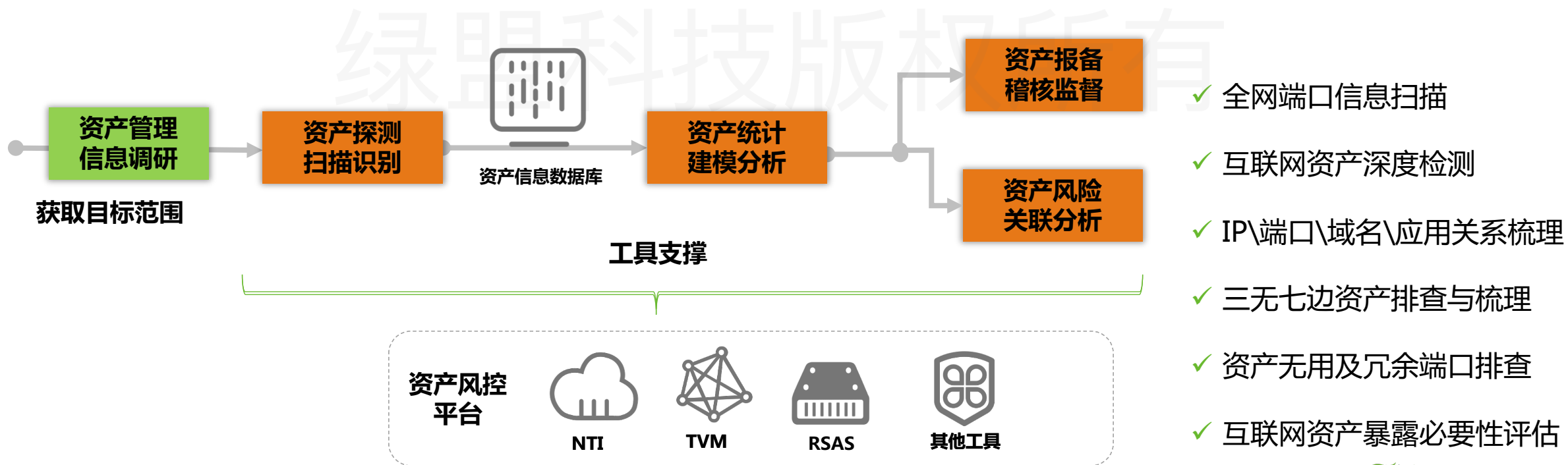
区别于传统安全测试，护网行动通常会包含红蓝对抗的社会工程学操作。

- 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。



## ▶▶ 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

邮件钓鱼

信息泄露



办公场所

陌生人员识别

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

### webllogic

- 反序列化漏洞
- 弱口令war包上传
- ssrf漏洞

### IIS

- 远程代码执行
- 解析漏洞

### Tomcat

- 弱口令war包部署
- PUT漏洞

### jBoss

- 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

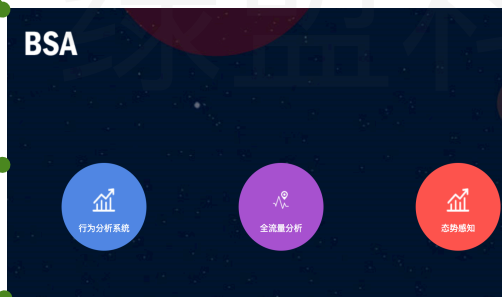
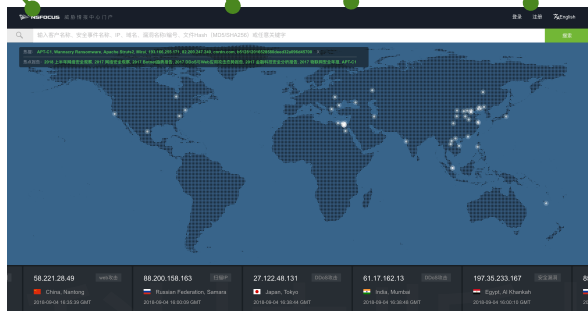
网络日志审计

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



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



HWA

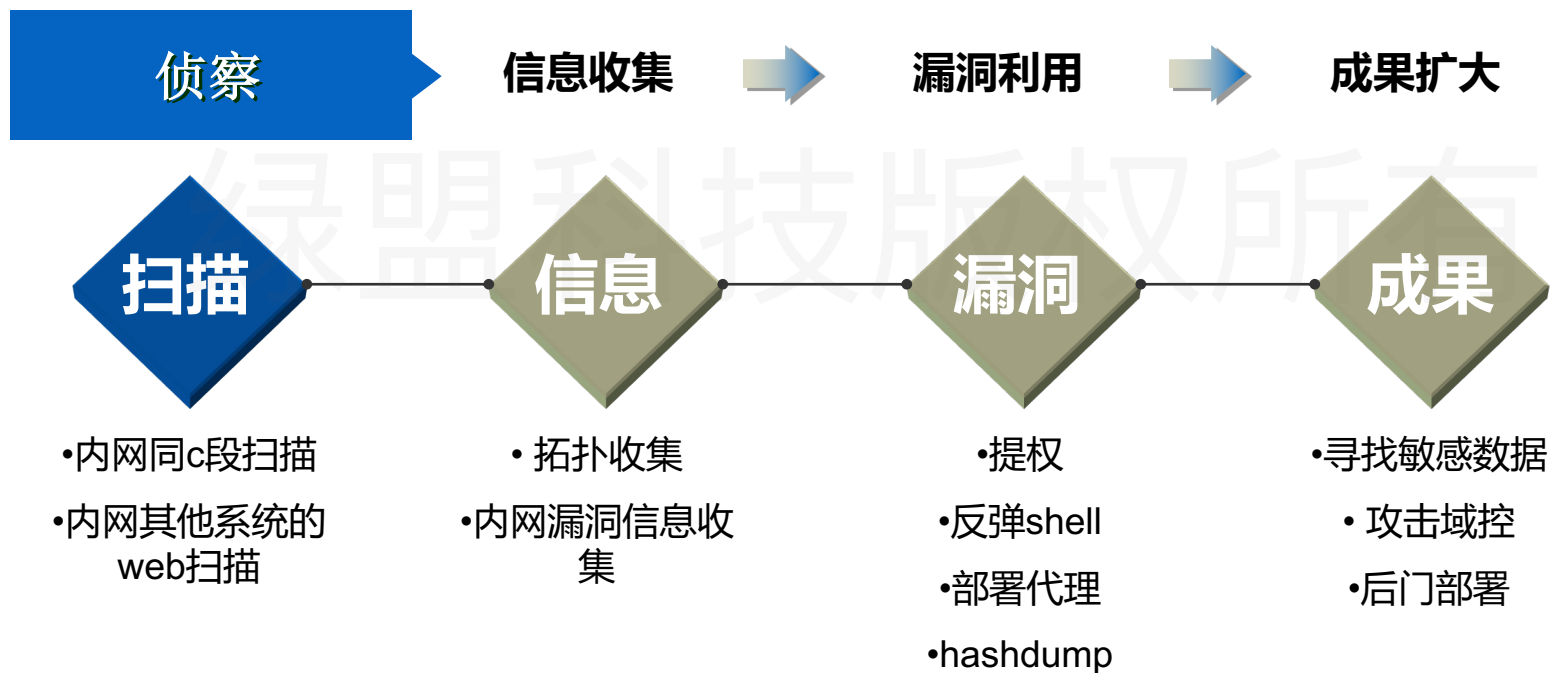
F

# 内网深入攻击

翻文件  
环境变量  
Bash\_history  
跳板选择  
网络连接  
访问历史  
部署代理  
权限提升  
主机发现  
内网漏洞挖掘  
后门部署  
Dumphash  
系统信息  
内网端口扫描  
文件上传  
攻击域控  
.ssh  
口令复用

# ▶▶ 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

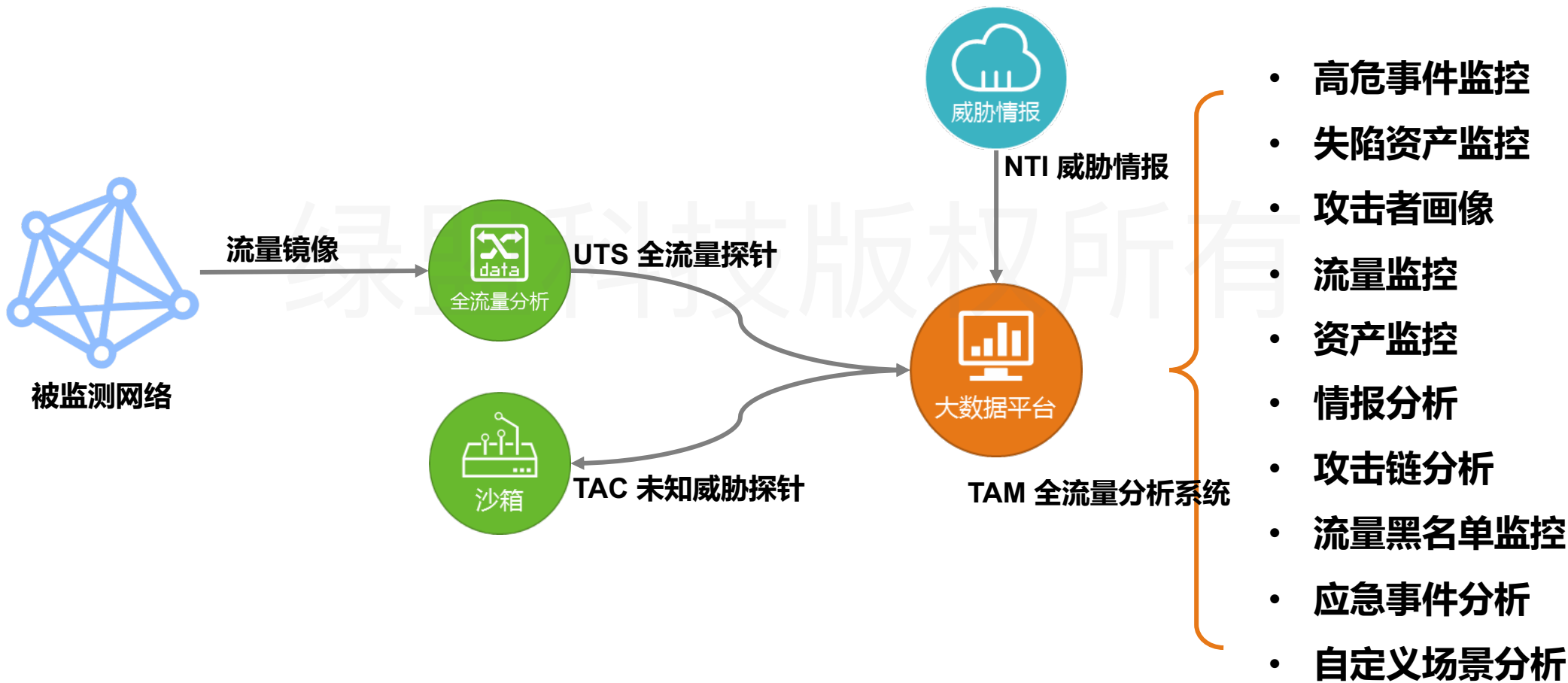


# ▶▶ 权限维持

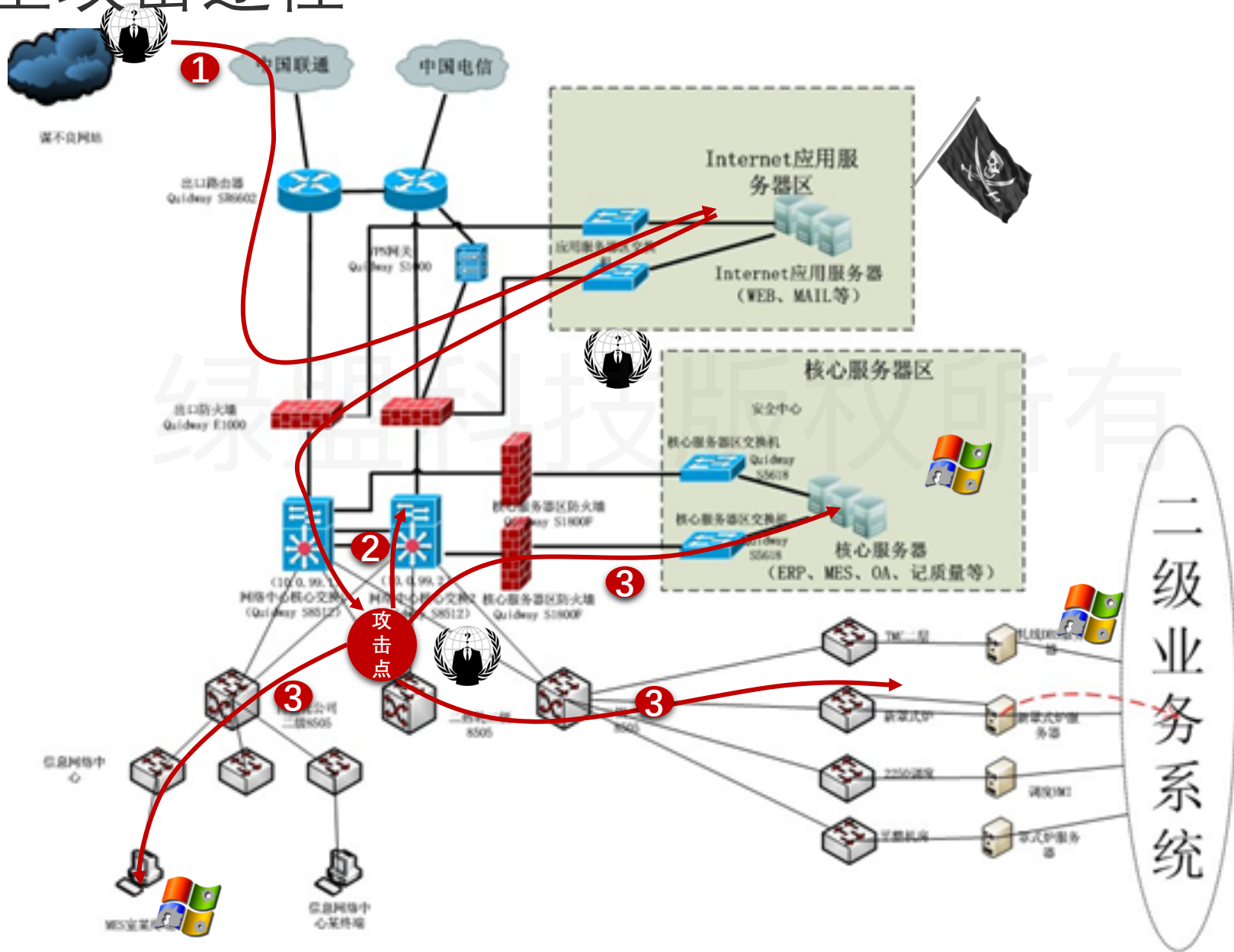
- C2阶段权限维持
  - Cs ( Cobalt Strike )
  - metasploit



# 全流量架构



# 典型攻击途径



# 护网防护工作整体流程及思路



# ▶▶ 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

绿盟科技版权所有

# 某学校域控攻击案例



# 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

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
26	26	200	<input type="checkbox"/>	<input type="checkbox"/>	355001	
27	27	200	<input type="checkbox"/>	<input type="checkbox"/>	216078	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	159960	
28	28	200	<input type="checkbox"/>	<input type="checkbox"/>	159960	
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	149823	
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	104140	
22	22	200	<input type="checkbox"/>	<input type="checkbox"/>	4843	
1	01	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
2	02	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
3	03	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
4	04	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
5	05	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
6	06	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
7	07	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	
8	08	404	<input type="checkbox"/>	<input type="checkbox"/>	3240	

Request Response

Raw Headers Hex

```
SQL: SELECT `id` FROM `yn_column` [ RunTime:0.0003s ]
NOTIC: [8] Undefined index: auto /var/www/html/ThinkPHP/Library/Think/Model.class.php 第 1128 行.
SQL: SELECT `photo` FROM `yn_admin` WHERE `id` = 1 LIMIT 1 [ RunTime:0.0004s ]
SQL: UPDATE `yn_admin` SET
  `username` = 'yineng', `password` = 'b5f985dab87facc95c5ba2ec8d54508', `question` = '0', `answer` = '', `email` = '', `group_id` = '1', `department_id` = '0', `column_id` = '1,12,13,14,15,16,17,18,19,20,21,22,23,24,3,25,95,96,97,98,99,100,101,26,102,103,104,105,106,107,108,27,110,111,112,113,114,115,116,161,162,163,164,165,166,167,168,28,117,118,119,120,121,122,123,29,124,125,126,127,128,129,130,30,131,132,133,134,135,136,137,31,138,139,140,141,142,143,144,4,32,33,5,34,35,36,37,38,39,155,156,157,158,159,160,6,40,41,7,42,43,44,8,45,77,78,79,80,46,47,48,49,9,50,51,52,10,53,54,55,56,91,92,93,94,147,57,58,172,66,11,59,60,61,62,63,64,65,170,171,173,67,68,69,70,71,72,73,74,75,76,146,81,82,83,84,85,86,87,88,89,90,148,149,150,151,152,153,154,169,174,145,175,178,182,179,180,181,183', `style` = '0', `photo` = '/Uploads/Admin/Photo/yineng.png' WHERE `id` = 1 [ RunTime:0.0006s ]
SQL: SHO
SQL: INSE
```

查询结果:  
coursedev

# 突破

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

The screenshot displays a web management interface with a terminal window overlaid. The terminal shows the execution of the `ifconfig` command on a system with IP `10.0.200.104`. The output lists network interfaces `ens160`, `ens192`, and `lo` with their respective configurations and statistics. A red arrow points from the terminal output to the '保存' (Save) button in the background interface.

```
[/var/www/html/Uploads/Admin/Photo/]$ ifconfig
ens160: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
  inet 10.0.200.104 netmask 255.255.255.0 broadcast 10.0.200.255
  inet6 fe80::250:56ff:fe97:6c3d prefixlen 64 scopeid 0x20<link>
  ether 00:50:56:97:6c:3d txqueuelen 1000 (Ethernet)
  RX packets 290915617 bytes 8600757342 (8.0 GiB)
  RX errors 0 dropped 713823 overruns 0 frame 0
  TX packets 28229457 bytes 259889612459 (242.0 GiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens192: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
  ether 00:50:56:97:6c:3e txqueuelen 1000 (Ethernet)
  RX packets 62246 bytes 703140 (686.6 KiB)
  RX errors 0 dropped 290 overruns 0 frame 0
  TX packets 0 bytes 0 (0.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
  inet6 ::1 prefixlen 128 scopeid 0x10<host>
  loop txqueuelen 1000 (Local Loopback)
  RX packets 130160325 bytes 72982560015 (67.9 GiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 130160325 bytes 72982560015 (67.9 GiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## ▶▶ 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

Eternalblue Doublepulsar

NetworkTimeout: 60 TargetIP: 10.0.200.27 TargetPort: 445

VerifyTarget:  VerifyBackdoor:  MaxExploitAttempts:  ValidateOnly:

GroomAllocations:  OutConfig: stdout Target: WIN72K8R2

LogFile: C:\ProgramData\DoublePulsar\DoublePulsar\logs.txt

```
[*] Connecting to target for exploitation.
[+] Connection established for exploitation.
[*] Pinging backdoor...
[+] Connection established for exploitation.
[+] Backdoor returned code: 10 - Success!
.
[+] Ping returned Target architecture: x64 (64-bit)
[+] Backdoor is already installed -- nothing to be done.
[*] CORE sent serialized output blob (2 bytes):
4-bit)
[+] Backdoor is already installed - nothing to be done.
0x00000000 08 01 ..
Backdoor is already installed -- nothing to be done.
[*] Received output parameters from CORE
```

# ▶▶ 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

10.0.200.27 - 远程桌面连接

RG-SAM安全计费管理系统

uc:00:21,601 INFO [ServerInfo] OS-system: windows server 2008 R2 6.1,amd64  
08:00:21,610 INFO [ServerInfo] VM arguments: -Dprogram.name=run.bat -Xrs -Djava.rmi.  
10.0.200.27 -Dsam.jms.address=10.0.200.27 -Dcom.sun.net.ssl.enableEC=fa...  
Duser.timezone=Asia/Shanghai -Xms1024m -Xmx2048m -XX:PermSize=128M -XX:MaxPermSize=256M  
Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Xloggc:  
+UseGCLogFileRotation -XX:NumberOfGCLogFiles=50 -XX:GCLogFileSize=100k -XX:+PrintGCDateStamps  
+PrintGCDateStamps -XX:+PrintGCTimeStamps -XX:-PrintTenuringDistribution -XX:  
+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=heap\_dump.bin -Dcom.sun.net.ssl.enableEC  
Djava.endorsed.dirs=.\lib\endorsed -Djboss.vfs.forceNoCopy=true -Djboss.vfs.forceCC  
08:00:21,659 INFO [MKKernel] Legacy JMX core initialized  
08:00:23,976 INFO [ProfileServiceBootstrap] Loading profile: ProfileKey@225c9404[don  
server=default, name=default]  
2019-03-19 08:01:00.059 SAM服务绑定的IP地址:10.0.200.27  
2019-03-19 08:01:19.135 认证服务器正在启动...  
2019-03-19 08:01:19.526 自助系统[/selfservice]启动成功!  
2019-03-19 08:01:20.183 认证服务器启动成功!  
2019-03-19 08:01:22.363 SAM兼容性组件正在启动...  
2019-03-19 08:01:22.372 SAM兼容性组件启动成功!  
2019-03-19 08:01:23.161 记账服务器正在启动...  
2019-03-19 08:01:23.179 记账服务器启动成功!  
2019-03-19 08:01:27.662 记账更新处理启动成功!  
2019-03-19 08:01:28.207 网关流量服务器启动成功!  
2019-03-19 08:01:28.423 日志处理启动成功!  
2019-03-19 08:01:29.401 管理系统[/sam]启动成功!  
2019-03-19 08:01:29.959 启动时日志记录成功, 花费434毫秒, 处理用户0个!  
2019-03-19 08:01:30.617 当前系统信息:RG-SAM V3.x企业版  
2019-03-19 08:01:30.673 系统使用人数限制:6000, 目前共有1486人使用!  
2019-03-20 02:00:00.104 只记账成功, 花费29毫秒, 处理用户0个!

10.0.200.41 - 远程桌面连接

Windows PowerShell

```
PS C:\Users\Administrator> Get-ADComputer -Filter * -Property * ! Select-Object Name,IPv4Address,OperatingSystem,OperatingSystemServicePack,OperatingSystemVersion,LastLogonDate>PasswordLastSet,CanonicalName ! Export-CSU adcomputer.csv -NoTypeInformation -Encoding UTF8  
无法将“Get-ADComputer”项识别为 cmdlet、函数、脚本文件或可运行程序的名称。请检查名称的拼写,如果包括路径,请确保路径正确,然后重试。  
所在位置 行:1 字符: 15  
+ Get-ADComputer <<<< -Filter * -Property * ! Select-Object Name,IPv4Address,OperatingSystem,OperatingSystemServicePack,OperatingSystemVersion,LastLogonDate>PasswordLastSet,CanonicalName ! Export-CSU adcomputer.csv -NoTypeInformation -Encoding UTF8  
+ CategoryInfo          : ObjectNotFound: (Get-ADComputer:String) [], CommandNotFoundException  
+ FullyQualifiedErrorId : CommandNotFoundException
```

```
PS C:\Users\Administrator> dsquery server  
"CN=ADSURI,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vmsldz,DC=com"  
"CN=ADSUR2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vmsldz,DC=com"  
PS C:\Users\Administrator> dsquery user  
"CN=Administrator,CN=Users,DC=vmsldz,DC=com"  
"CN=Guest,CN=Users,DC=vmsldz,DC=com"  
"CN=krbtgt,CN=Users,DC=vmsldz,DC=com"  
PS C:\Users\Administrator> dsquery site -o rdn  
"Default-First-Site-Name"  
PS C:\Users\Administrator> dsquery computer  
"CN=ADSURI,OU=Domain Controllers,DC=vmsldz,DC=com"  
"CN=ADSUR2,OU=Domain Controllers,DC=vmsldz,DC=com"  
"CN=UCENTER,CN=Computers,DC=vmsldz,DC=com"  
"CN=UDBSUR,CN=Computers,DC=vmsldz,DC=com"  
"CN=ESXISUR3,CN=Computers,DC=vmsldz,DC=com"  
"CN=ESXISUR2,CN=Computers,DC=vmsldz,DC=com"  
"CN=ESXISUR1,CN=Computers,DC=vmsldz,DC=com"  
PS C:\Users\Administrator>
```

时间戳	状态
2019/3/17 2:00:00	静态
2019/3/16 6:00:00	静态
2019/3/16 19:00:00	静态
2019/3/16 18:00:00	静态



# 谢谢！

绿盟科技版权所有