

REEBUF

2017深圳站

FREETALK

构建全流量入侵检测平台

李 斌

About Me

✓10年以上安全从业经验，专注企业信息安全建设

安全厂商
2006-2013

- 设备部署
- 渗透测试
- 安全咨询

互联网公司
2014-2017

- SDL自动化系统
- 安全防护/检测/审计
- 安全体系建设

互联网公司
NOW

- 业务安全
- 风控系统
- 数据安全

议题引入

企业面临越来越多的安全挑战，如何能在攻防对抗中占主动地位？

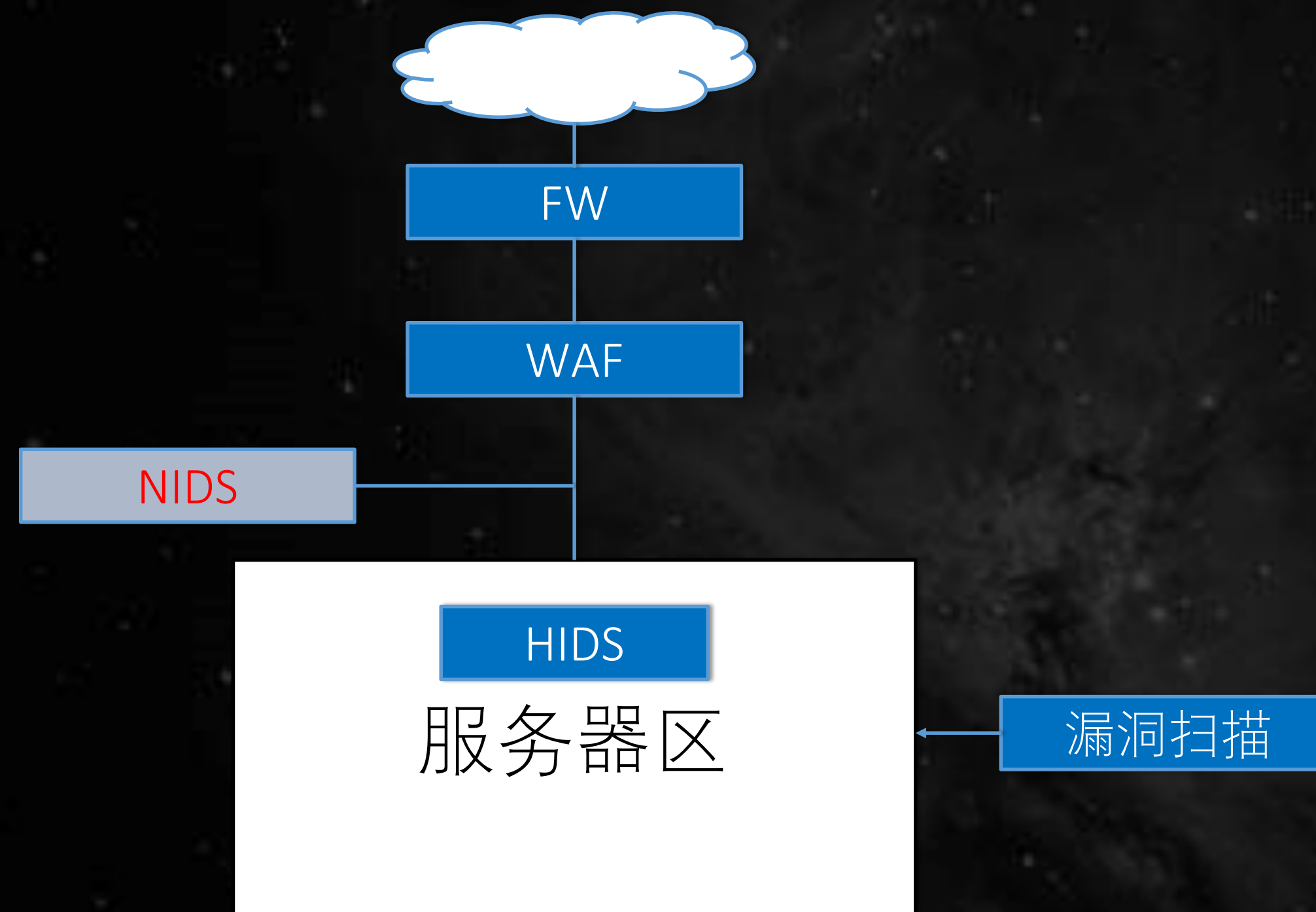
---需要全面掌控整体安全态势！

- 谁 什么时间 以什么方式发起攻击
- 攻击是否成功
- 如何快速响应和阻断攻击
- 全面排查和消除安全隐患

目录

- 安全威胁感知体系建设
- 全流量入侵检测平台
- 安全收益和平台扩展

安全威胁感知体系建设



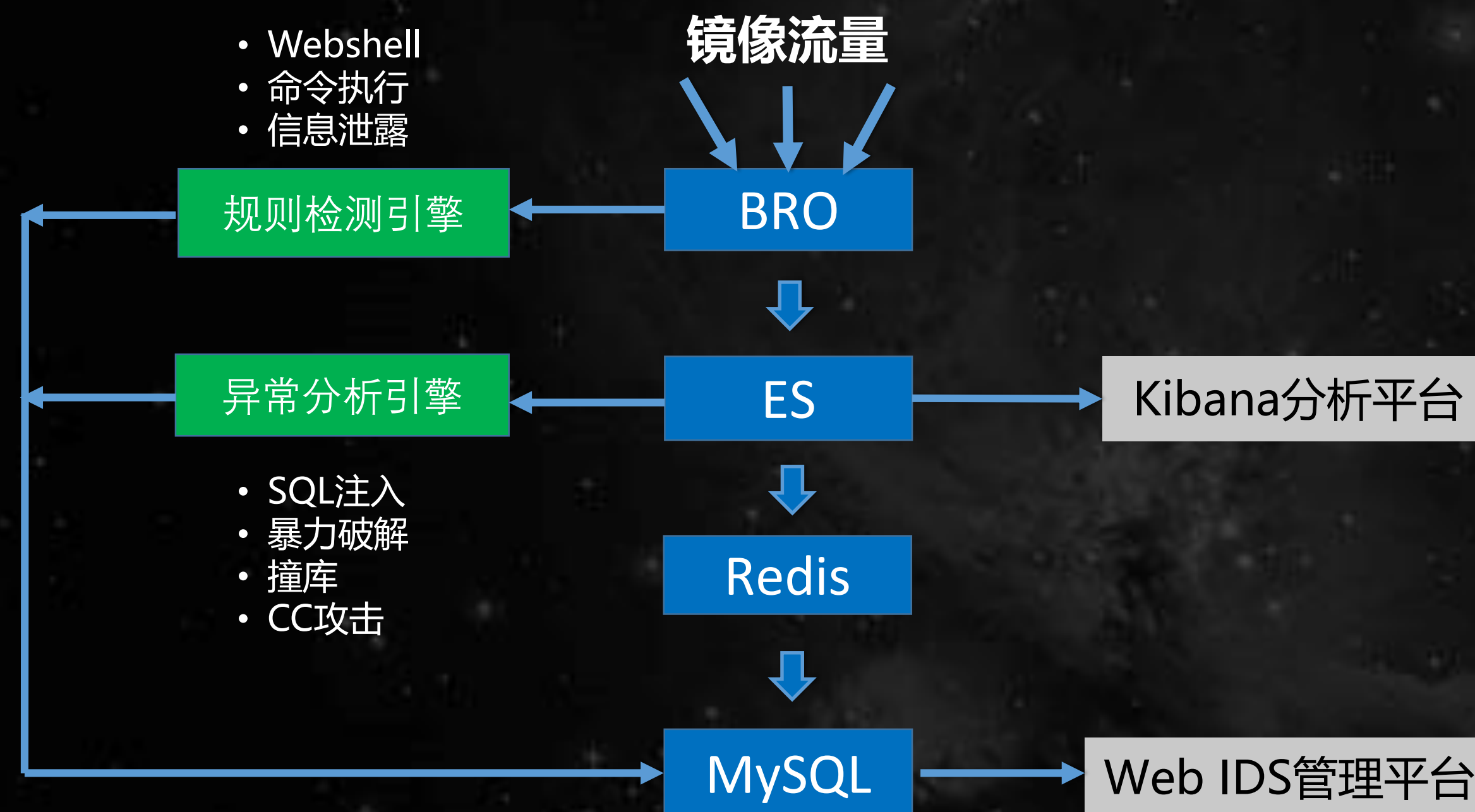
传统IDS

- 1、基于规则检测，可检测攻击类型有限
- 2、关注检测过程，不关注结果，误报率高
- 3、没有保留全部原始流量数据，不便于事后追溯
- 4、扩展性不高

全流量入侵检测必要性

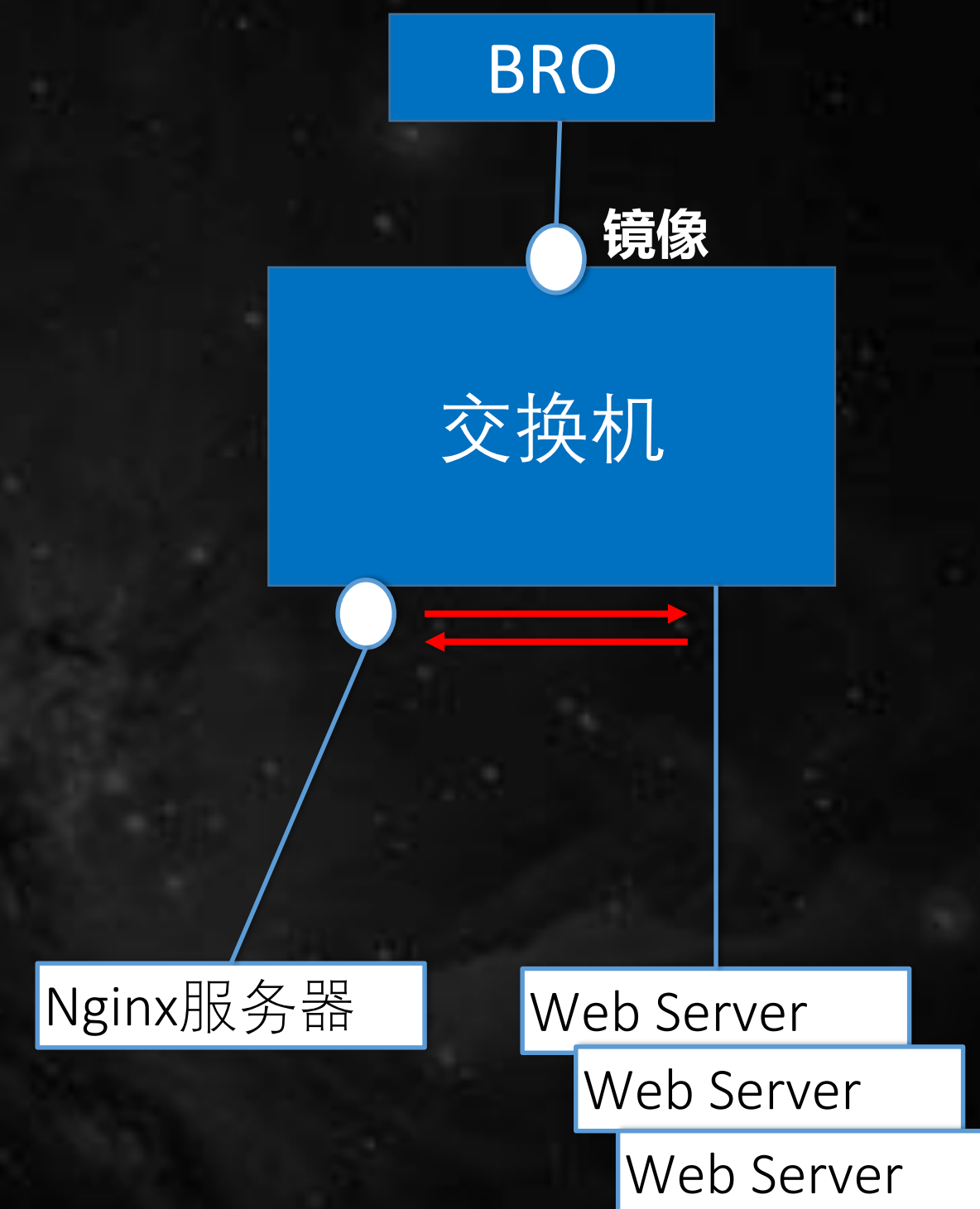
- 1、异常行为分析
 - CC攻击（基于统计）
- 2、响应结果判断
 - 撞库、爆破（高登录失败率）
- 3、攻击回溯和取证需要
 - 攻击路径、影响分析
 - APT攻击

全流量入侵检测技术架构



流量镜像和分析

- **镜像端口**
 - Nginx后端进出HTTP流量
- **Bro抓包**
 - Request/Header/Post/部分Response
- **分析**
 - 生成HTTP文件
 - Request和Response关联
 - Logstash-->ES



规则匹配检测

1、信息泄露

---响应 phpinfo、index of /、Directory , 响应为200

---请求 .bak .old .swp .sh .zip .rar .iso , 响应为200

2、命令执行 (POST、URI、Header检测)

---如struts2漏洞: Header会包含 ognl关键字

---命令执行:URI中会包含 ping 等字段

3、Webshell检测 (POST、URI、Header检测)

---eval.*base64_decode , 响应码为200

异常分析---SQL注入

- 1、ES API 检索敏感关键字如["select" , "ifnull" , "cast" , "union" , "sleep" , ascii " , " when " , " now "]等
- 2、单IP异常匹配次数到达阈值，将此IP的最近一段时间的访问记录从ES中取出来存入Redis中后续处理
- 3、匹配 .*schema_name.*from.*information_schema\schemata.*等模式，次数大于阈值，判定为SQL注入成功



异常分析---暴力破解/撞库/短信轰炸

- 1、监控url中含有login/captcha/register等关键字的url
- 2、ES API记录URL访问量
- 3、每五分钟抽取一次数据与前五分钟的数据对比，并且计算出下个五分钟的预估值并且计算出最大偏差量
- 4、下一次五分钟的访问量与上次的 预估值对比超过阈值就认为存在异常

PS：改进为匹配Response包，统计失败率

异常分析---CC攻击

- 1、ES API 获取 TOP 100 URL访问量
- 2、一定时间内，同UserAgent不同IP数量超过阈值判定异常
- 3、一定时间内，同B段IP，相同UserAgent数量超过阈值判定异常

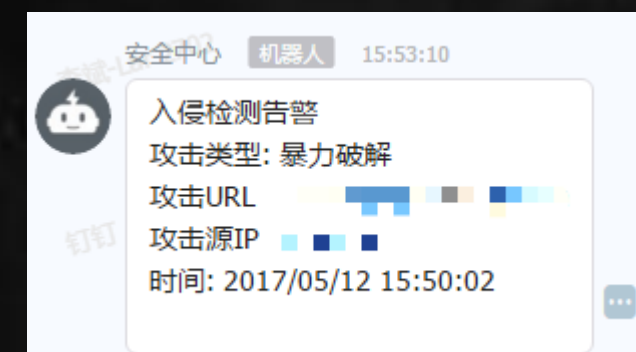
安全收益

全面入侵发现和威胁感知，攻防对抗处于主动地位！



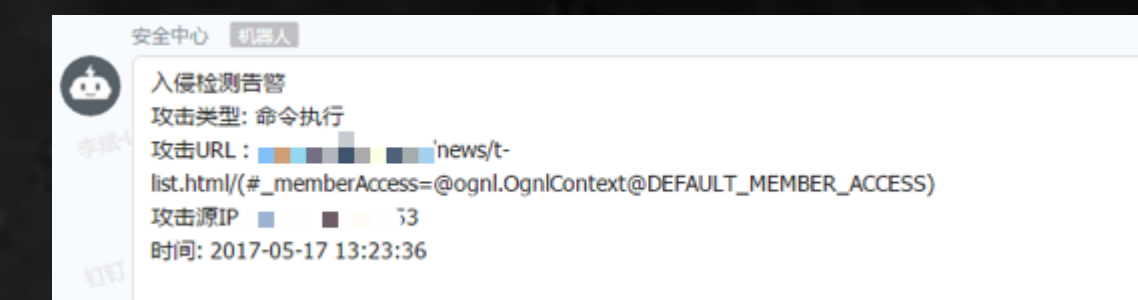
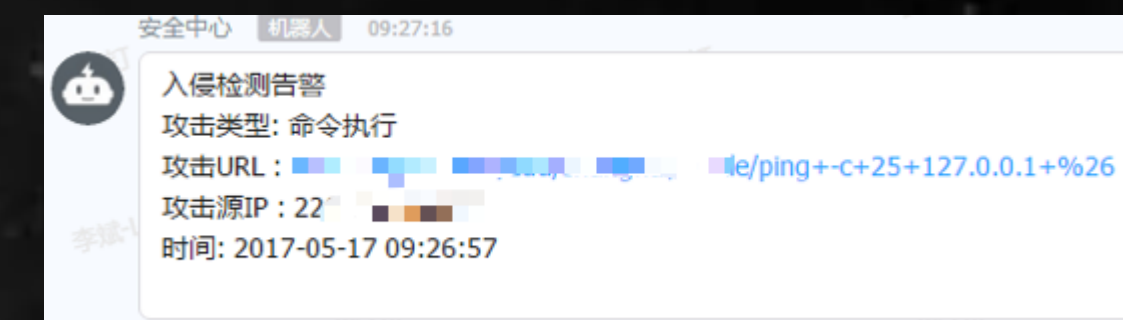
PHP Version	
System	Linux
Build Date	Feb 18 2017 15:55:44
Server API	PHP/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional ini files	/etc/php.d
Additional ini files parsed	/etc/php.d/imap.ini, /etc/php.d/bcmath.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/gmp.ini, /etc/php.d/igmp.ini, /etc/php.d/json.ini, /etc/php.d/mbstring.ini, /etc/php.d/mcrypt.ini, /etc/php.d/memcache.ini, /etc/php.d/mongo.ini, /etc/php.d/mysqli.ini, /etc/php.d/mysqlnd.mysqlini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/redis.ini, /etc/php.d/soap.ini, /etc/php.d/sockets.ini

信息泄露



May 12th 2017, 15:52:31.241	com	LoginForm\$Busername\$D=zhenzhihao&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login
May 12th 2017, 15:52:31.241	com	LoginForm\$Busername\$D=wangxueshu&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login
May 12th 2017, 15:52:31.241	com	LoginForm\$Busername\$D=wangkunoz&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login
May 12th 2017, 15:52:31.240	com	LoginForm\$Busername\$D=mlaobei&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login
May 12th 2017, 15:52:31.240	com	LoginForm\$Busername\$D=huangshun&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login
May 12th 2017, 15:52:31.237	com	LoginForm\$Busername\$D=01&LoginForm\$Bpassword\$D=11111111&LoginForm\$BrememberMe\$D=0&to=Login

暴力破解



命令执行

平台优势

1、易于扩展

- BRO、ES都可平行扩展
- 检测规则可扩展

2、应用场景广

- 生产、测试、办公

3、功能扩展

- 全流量数据可作为被动扫描器的数据源：全面发现安全漏洞
- MySQL数据包全流量分析：更精确判断SQL注入
- 对接威胁情报平台：实现攻击追根溯源

Q&A

