

智能安全领航者

企业安全短板和智能威胁感知

—— 安赛linx

www.aisec.com

Artificial Intelligence Security Co.,Ltd

AI 安赛 **AISEC**

个人介绍：

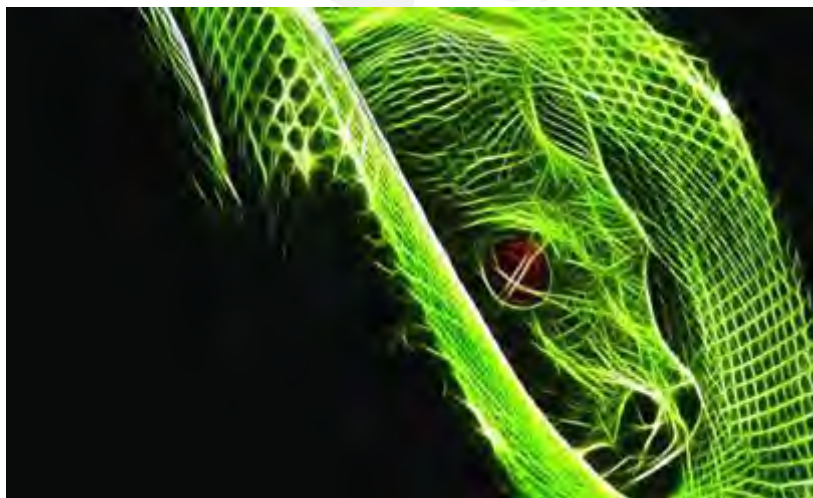
- 安赛CEO：linx
- 智能安全、Web安全
- Web2.0漏洞扫描产品：AIScanner安全检测系统
- WebIDS产品：Web入侵检测与漏洞感知系统

- 目前70%以上的应用系统都存在中高危漏洞，安全风险几乎无法避免。应对各种已知漏洞、通用漏洞已是非常困难，要面对各种动态变化的0Day漏洞及不断升级的黑客攻击手段更是难上加难。
- 本议题以分析漏洞的成因、现状和变化趋势，提出一种智能的漏洞挖掘及威胁感知方法，能够较好地解决目前漏洞挖掘的局限性，具备较高的实用价值，能真实有效地降低企业的安全风险。

目录 contents

- 1 议题目的
- 2 企业安全短板：网络攻防角度
- 3 新的漏洞挖掘和威胁感知技术
- 4 实际使用效果

- 无差别地识别Nday、0Day；收集BUG
- 面向群体：电商金融行业、安全运维团队
- 作用：发现漏洞、识别入侵、实时响应



2. 企业的安全短板（网络攻防的视角）

智能安全领航者

业务、资产、网络划分、系统架构、人员意识、攻防等
两个动态：



2.1 漏洞动态增加



2.2 攻击技术动态进化

2. 企业的安全短板（网络攻防的视角）

智能安全领航者

2.1 漏洞动态增加

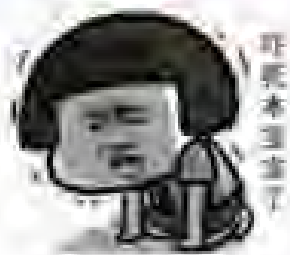


2.1 漏洞动态增加

(2.1.1) 每一项新产品、新技术的升级迭代，都会引进新的安全漏洞。

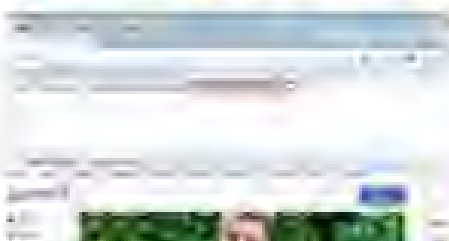
- 如：xml、nosql、Struts2每一次产品升级，都带来了新的安全风险。

[Apache struts2漏洞血洗中国互联网 系统安全如何保障?](#)



2016年4月28日 - (原标题:Apache struts2漏洞,安全如何保障?) 到年末做盘点时,没有人会忘记在这一天,Apache Struts2官方又发布...
[money.163.com/16/0428/...](#) - - 百度快照 - 26

[Struts2被曝重要漏洞,波及全系版本 - 企业架构 - ITeye资讯](#)



Apache Struts团队6月底发布了Struts 2.3.15版存在重要的安全漏洞,因此该团队今天发布了S版本。该版本修复的主要安全...

2. 企业的安全短板（网络攻防的视角）

2.1 漏洞动态增加

(2.1.2) 每一项新的业务类型，都需要建立新的风险模型

- 如：移动app漏洞、ATM漏洞、工控系统、钓鱼、反欺诈、

[XML实体注入漏洞安全警告 - 网站安全 - 红黑联盟](#)

2011年11月2日 - [漏洞介绍](#) 可扩展标记语言(Extensible Markup Language)电子文件使其具有结构性的标记语言,可以用来标记数据、定义数据
[www.2cto.com/Article/2...](#) - [百度快照](#) - 91条评价

[\[XML外部实体攻击\]XXE attack - About:Blank H4cking](#)

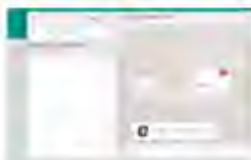
Pnig0sp.s:最近80Sec发表了一篇关于介绍XML实体注入漏洞的警告
可以发现XML外部实体攻击相关技术早在02年就在国外被提出
[www.pnig0s1992.blog.51cto...](#) - [百度快照](#) - 85%好评

[中国移动某处app缺陷getshell\(可内网\)](#)



2015年10月1日 - 国庆期间,套餐信息,|WooYun是平台,注重尊重,进步,与
[www.wooyun.org/bugs/...](#)

[那些APP身上出现的安全漏洞背后 - 站长](#)



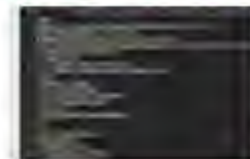
2015年9月14日 - 安全漏洞涉及到的操纵者包括 AF 某些不法创业团体等。
[www.chinaz.com/news/...](#)

[移动APP安全漏洞多 如何防护是关键](#)



2016年3月2日 - 在过去,对象是有一定用户基础和到位等,为此移动APP的

[Mongodb注入攻击](#)



php下操作mongodb的帖子国内mongodb的文章似乎还,PHP等
2016-02-26 15:24:58 学习了,谢
[drops.wooyun.org/tips/...](#) - [百](#)

[攻击MongoDB漏洞姿势之MongoDB注入 - 安](#)

2016年4月13日 - 现在,我几乎在我所有的项目中都使用,还是在开发我自己的项目,它都是一款非常优秀的数据库
[www.2cto.com/News/2016...](#) - [百度快照](#) - 91条评价

[MongoDB注入:如何攻击MongoDB? - 推酷](#)

2016年4月14日 - MongoDB注入,如何攻击MongoDB?8个未知用户输入时候产生的问题,为了说明,接下来我们
[www.tuicool.com/articl...](#) - [百度快照](#) - 77条评价

[MongoDB管理工具曝远程代码执行漏洞 - 网](#)

2015年3月19日 - MongoDB,IT界主流非关系型数据库(据,注入漏洞的利用和防范ASP注入漏洞全接触(最全的
[www.2cto.com/Article/2...](#) - [百度快照](#) - 91条评价

[MongoDB 远程命令执行漏洞:噩梦还是开眼?](#)

2013年3月28日 - 3月24日公开披露的 MongoDB 零日漏洞引起我们的关注,IT 安全和开发人员已经开始在热议这个话题。

2.1 漏洞动态增加

(2.1.3) 网络变更、业务变更、配置变更也有可能带进新的漏洞

[陌陌科技员工信息泄露导致内部运维信息泄露 |](#)



2014年10月11日 - 陌陌科技员工信息泄露 员工将账号密码信息泄露在了GitHub.png漏洞证明.为了防止贵上面打...

[www.wooyun.org/bugs/wo...](#) -- 百

[猎聘网运维不当导致内部共享信息人员架构可泄](#)



2015年6月11日 - 漏洞标题: 猎聘网架构可泄露 相关厂商: 猎聘网 漏洞时间: 2015-06-11 12:31公开时间:

[www.wooyun.org/bugs/wo...](#) -- 百

[某运维FTP未授权访问泄漏中国铁塔运维监控系统](#)



2015年6月14日 - 中国铁塔运维监控系统控制-设备远程开关机等|WooYun间的漏洞报告平台,注重尊重,进步:[www.wooyun.org/bugs/wo...](#) -- 百

[AuditSec运维操作审计-堡垒机密码的利用 | Woc](#)

[华安保险某系统配置不当导致getshell |](#)

2015年10月20日 - 缺陷编号: WooYun-2015-11致getshell可威胁内网 相关厂商: 华安保险 漏洞[www.wooyun.org/bugs/wo...](#) -- 百度快照 - 30

[汇通小贷某系统配置不当导致getshell |](#)

2015年12月11日 - 缺陷编号: WooYun-2015-11致getshell 相关厂商: 汇通小贷 漏洞作者: 路人E[www.wooyun.org/bugs/wo...](#) -- 百度快照 - 30

[华住酒店集团某关键配置错误导致大量](#)



2015年9月17日 - 华住;防爆破机制进行爆破,待配置好字典就开跑漏洞[www.wooyun.org/bugs...](#)

[TurboMail 设计缺陷以及默认配置导致](#)

2016年2月17日 - Tags标签: 设计缺陷/边界绕过...(ses, "getnextmsgid", jsonParam, ioRet);中的[www.wooyun.org/bugs/wo...](#) -- 百度快照 - 30

[远盟康健某系统配置不当可导致内网渗](#)



2015年1月4日 - 缺陷编号: 远盟康健某系统配置不当可导致内网渗透 路人甲提交时间: 2015-[www.wooyun.org/bugs...](#)

2. 企业的安全短板（网络攻防的视角）

智能安全领航者

2.1 漏洞的动态增加

2.2 攻击技术动态进化



2.2 攻击技术动态进化

黑客技术不断发展，每天都可能有新的攻击技术出现，给应用带来新的威胁。

如：

防火墙绕过技术

彩虹表

撞库

通过反射放大的DDOS



2. 企业的安全短板（网络攻防的视角）

2.2 攻击技术动态进化

- 技术壁垒：国外的技术更难以理解、研究
- 价格昂贵 + 禁售+，难以买到

Security AppScan Standard

版本 9.0.0.0

Licensed Materials - Property of IBM, 5724-T59 ©
Rights Reserved. U.S. Government Users Restricted
ADP Schedule Contract with IBM Corp. Watchfire, A
Corporation in the United States, other countries, c
<http://www.ibm.com/legal/copytrade.shtml>. Micro
trademarks of Microsoft Corporation in the United
service names may be trademarks or service mark



The logo for Nexpose, featuring the word 'nexpose' in white lowercase letters on a dark blue background.

The logo for Acunetix, featuring a red circular icon with a white 'a' and the word 'acunetix' in white lowercase letters on a black background.

The logo for CANVAS, featuring the word 'CANVAS' in white uppercase letters on a black background with a red, glowing, hexagonal pattern.

- “两个动态”：
- (1) 如何应对“漏洞动态增加”？
- (2) 如何应对“攻击技术动态进化”？

• 我们精力有限、知识范围有限：

不可能第一时间100%跟进所有漏洞和攻防技术。

需要一种技术，轻松地、便捷地、智能地、应对这些问题。

目标：

(1) 与漏洞同步感知，黑客发现了我的漏洞、利用了我的漏洞，不管是0Day还是Nday，我都能同步感知

(2) 黑客入侵了我们的网络，我们能够第一时间发现他所用的

漏洞



(2) 以往的技术和难题



(2.1) 漏洞动态增加



(2.2) 攻击技术持续进化

3. 新的技术：智能的漏洞挖掘和威胁感知

- 蜜罐、日志分析（日志审计）也是其中一种方式，
- 但是蜜罐风险高、效果不明显；日志分析的没有回包报文，线索太少；
- 通过分析旁路镜像的全流量数据，**全被动地**全面感知各种漏洞和网络攻击
- 人类用心念来诠释自己器官所接收的信号。称为：感知。
- 人之心念对刺激信号的解读与破译，并在内心产生各种的感觉。



- 挖掘：基于数据分析全被动式挖掘
- 感知：对攻击信号的同步感知



• 2014年ISC中国互联网大会《金融Web应用系统漏洞分析方法》，我们曾提出了三位一体的漏洞挖掘和分析方法，分别为：

(1) 基于**主动爬取（爬虫）**的漏洞扫描方法

(2) 基于代理或旁路抓url日志，再把url导入扫描器的**半被动漏洞扫描方法**

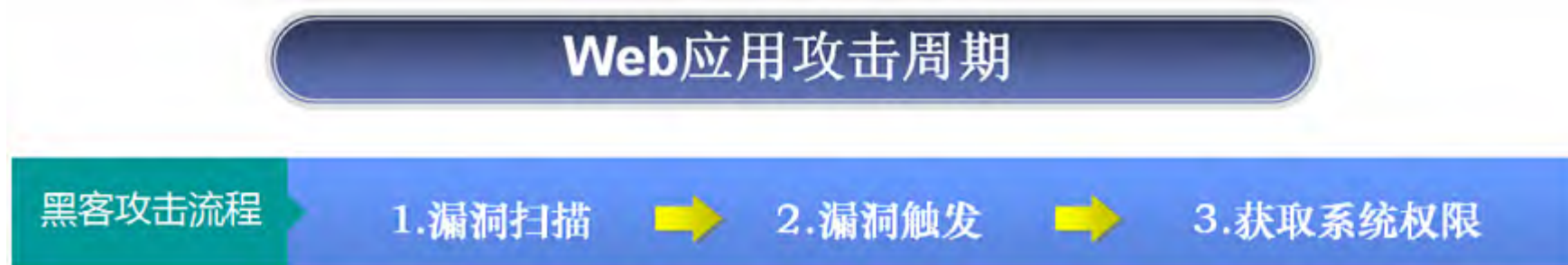
(3) 全被动的：基于旁路全报文分析，无发包的漏洞挖掘和威胁感知方法（PVS）

今天讨论很少被提及的全被动PVS



3.1 漏洞挖掘：对数据的挖掘

- 了解攻击者意图
- 识别数据包特征
- 数据包复用



AppScan漏洞感知/同步识别

- Appscan：Web2.0爬虫功能很强大，检出率高；误报率高；价格昂贵（几十到几百万）
- 像debug那样步步跟踪；**只用在镜像设备中添加几条规则就能和Appscan同步报警：**

描述： SQL 盲注：通过使用撇号并注释掉查询的余下部分，附加布尔 True/False 字符串表达式

差异：

以下更改已应用到原始请求：

已将参数“uname”的值设置为“' and 'f'='f' -- ”

已将参数“uname”的值设置为“' and 'b'='f' -- ”

已将参数“uname”的值设置为“' or 'f'='f' -- ”

已将参数“uname”的值设置为“' or 'b'='f' -- ”

WVS漏洞感知/同步识别

- WVS：大量黑客使用；检出率高；
- 准确率高；价格十几万到几十万
- 并没有使用随机特征，所以很容易识别
- 只用两条规则就能与其同步报警
- 像debug那样步步跟踪

wvs v9.5 201406

- $0+0+0+3 \Rightarrow \text{TRUE}$
- $0+645*640+3 \Rightarrow \text{FALSE}$
- $13-5-2-999 \Rightarrow \text{FALSE}$
- $13-5-2-3 \Rightarrow \text{TRUE}$
- $13-2*5+0+0+1-1 \Rightarrow \text{TRUE}$
- $13-2*6+0+0+1-1 \Rightarrow \text{FALSE}$
- $3 \text{ AND } 2+1-1-1=1 \text{ AND } 645=645 \Rightarrow \text{TRUE}$
- $3 \text{ AND } 3+1-1-1=1 \text{ AND } 645=645 \Rightarrow \text{FALSE}$
- $3 \text{ AND } 3*2=5 \text{ AND } 645=645 \Rightarrow \text{FALSE}$
- $3 \text{ AND } 3*2=6 \text{ AND } 645=645 \Rightarrow \text{TRUE}$
- $3 \text{ AND } 3*2*0=6 \text{ AND } 645=645 \Rightarrow \text{FALSE}$
- $3 \text{ AND } 3*2*1=6 \text{ AND } 645=645 \Rightarrow \text{TRUE}$

SQLMap漏洞感知/同步识别

- SQLMap：开源，被广泛使用，漏洞验证、漏洞利用、窃取数据（脱库）的首选工具；
- SQLMap发现漏洞后，会自动进入漏洞校验“数据库指纹采集”环节，进入到这个环节就说明漏洞一定存在。把下图的几个特征加到旁路设备，就可以接近100%检出率和100%准确率去同步感知黑客使用的漏洞。

- 漏洞触发报文

```
sqlmap 指纹

if conf.direct:
    result = True
else:
    result = inject.checkBooleanExpression("SQUARE([RANDNUM])=SQUARE([RANDNUM])")

if result:
    infoMsg = "confirming %s" % DBMS.MSSQL
    logger.info(infoMsg)

for version, check in (("2000", "HOST_NAME()=HOST_NAME()"), \
                        ("2005", "XACT_STATE()=XACT_STATE()"), \
                        ("2008", "SYSDATETIME()=SYSDATETIME()"), \
                        ("2012", "CONCAT(NULL, NULL)=CONCAT(NULL, NULL)")):
    result = inject.checkBooleanExpression(check)
```

3.2 威胁感知：对数据的挖掘

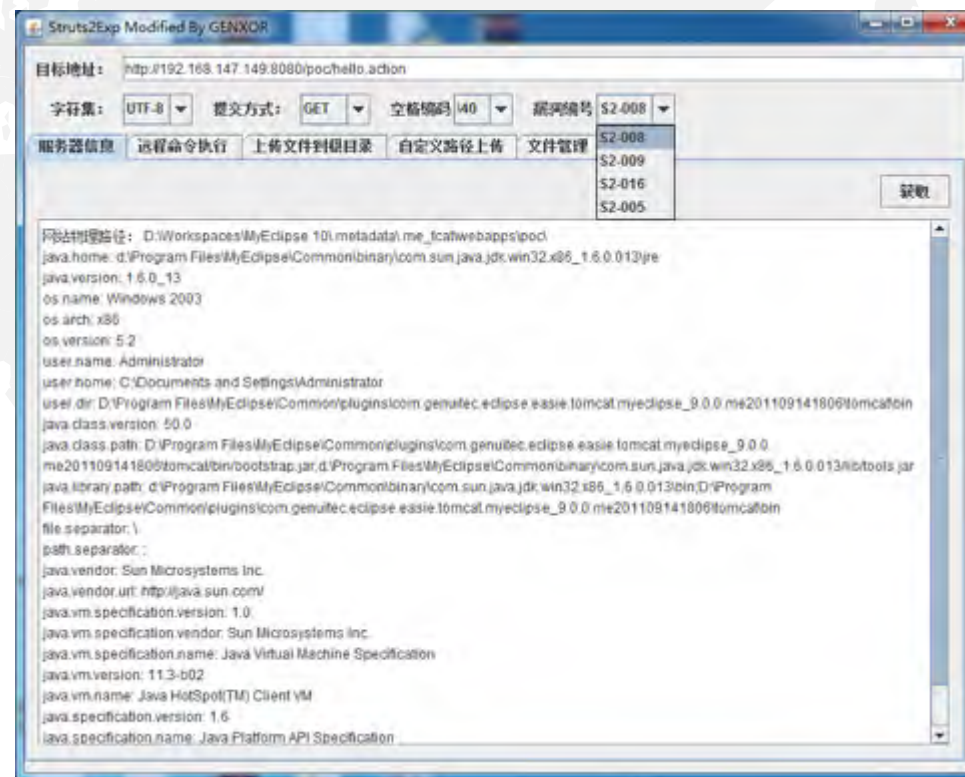
- **威胁的共性特征：**
 - 1) 命令执行：ifconfig、uname
 - 2) 数据泄漏（SQL注入、文件穿越等）：泄漏管理员帐号、密码/哈希、邮箱
 - 3) 系统异常：505错误页面、debug信息、sql报错语句
 - 4) 后门的共性特征：文件管理器、简单孤岛页面
- 一般情况下，Nday和0Day的影响是“无差异”的，需要“一样”漏洞确认页面作为信号反馈：**要么是返回数据库指纹，要么是命令执行结果、要么是页面延迟或页面出错**

3.2 威胁感知

(3.2.1) 命令执行

- **Struts2的shellcode：代码是变化的，影响是一致的**
- **返回执行命令结果，或返回一个指定的字符串**

- **旁路设备中检测uname、ifconfig、ls命令的输出结果，一旦遇到struts2 0Day，就可以立刻抓获起样本**



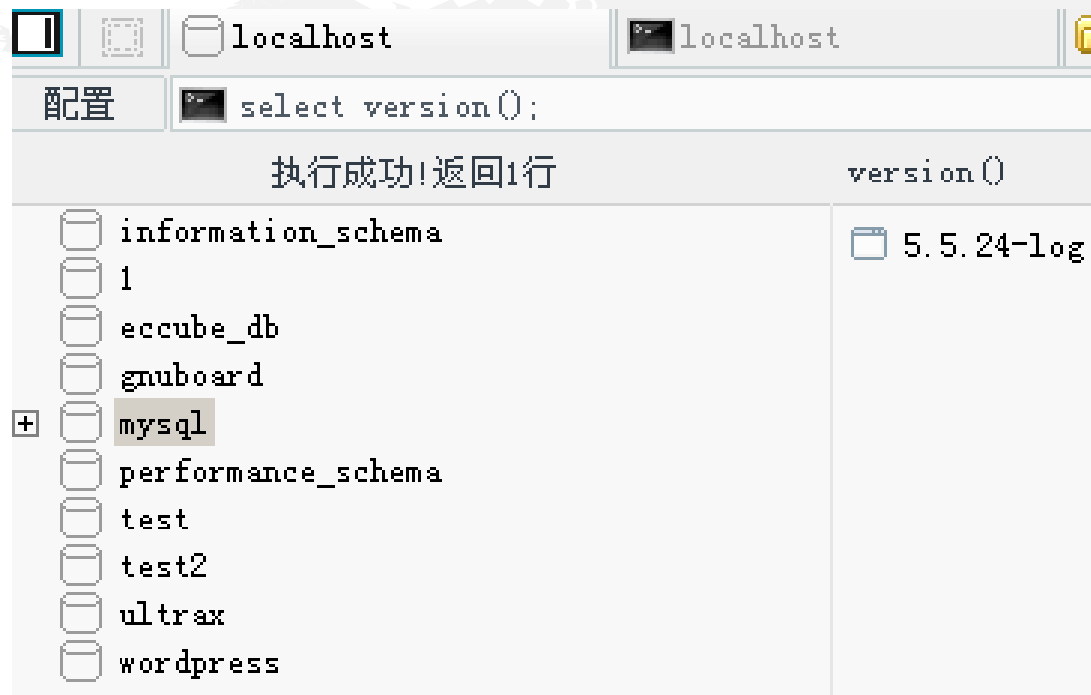
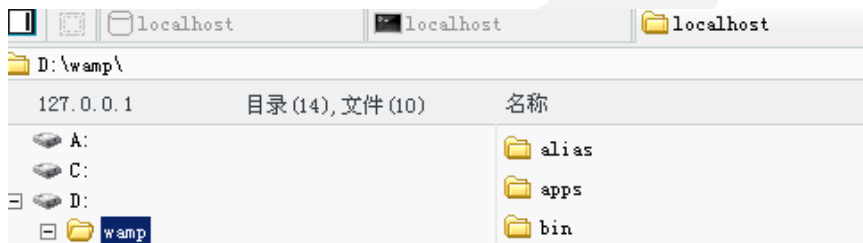
3.2 威胁感知

(3.2.2) 数据泄漏

Sql注入：影响是一致的

输出数据库版本、root密码、表的信息

ps：sql注入攻击属于多步攻击



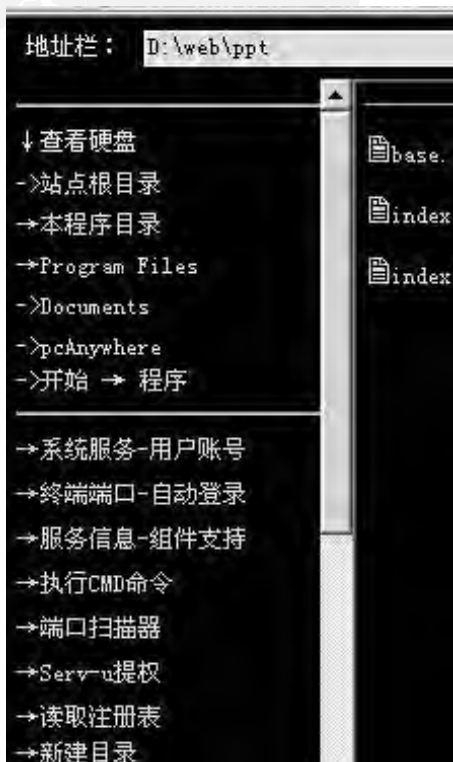
3.2 威胁感知

(3.2.3) 系统异常：50x、DBError、debug信息等

- 成功的fuzz也是搜集这些信息
- 我们等黑客来fuzz，看到页面出现出错信息后，回溯分析便能追溯到漏洞
- Web的异常不会导致应用发生影响

3.2 威胁感知

(3.2.4) WebShell：报文和返回都非常独特

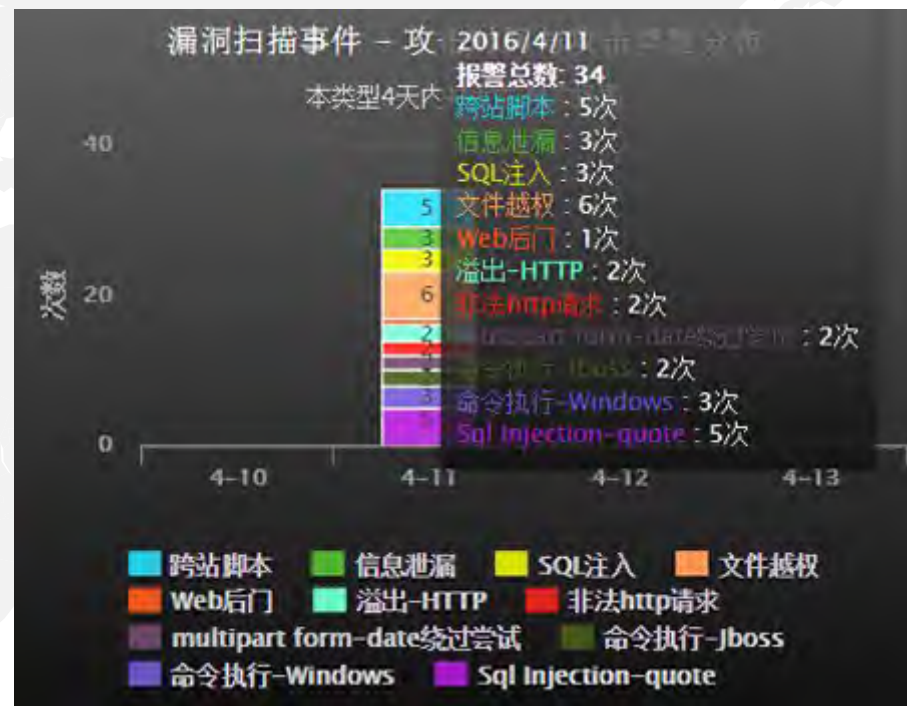


4.1 漏洞感知

- 研究各种漏洞扫描器的漏洞判断规则，提取确定漏洞的发包特征，形成同步判断规则。
- 黑客使用各种漏洞扫描器扫描用户网络时，系统可于各个扫描器同步发现各种漏洞。可与国外的扫描器IBM Appscan、HP Webinspect、Acunetix WVS、SQLMap、havij等漏洞扫描及漏洞利用工具同步发现漏洞
- 轻松应对Web通用攻击手段
-

4.1 漏洞感知

testasp.vulnweb.com:80	POST /Login.asp	192.168.1.152	Sql Injection-quote	200	5
open:80	/invoker/JMXInvokerServlet	192.168.1.152	命令执行-Jboss	404	1
testasp.vulnweb.com:80	/Search.asp?tfSearch=12345'\";]]*(< >...	192.168.1.152	非法http请求	500	3
open:n:80	/servlet/ Refresh:0?url=javascript:promp...	192.168.1.152	跨站脚本	404	1
testasp.vulnweb.com:80	POST /Register.asp	192.168.1.152	跨站脚本	500	9
testasp.vulnweb.com:80	POST /Register.asp	192.168.1.152	信息泄漏	302	4
op:n:80	/	192.168.1.152	溢出-HTTP	400	1
op:n:80	/util/barcode.php?type=../../../../...	192.168.1.152	文件越权	404	2
testasp.vulnweb.com:80	POST /Register.asp	192.168.1.152	信息泄漏	500	8



4.2 威胁感知

- Struts Nday、0Day
- 未知Webshell
- 数据泄漏
-

testasp.vulnweb.com:80	/Search.asp?tfSearch='+ (select convert(in...	192.168.1.152	SQL注入-Union
testasp.vulnweb.com:80	POST /Register.asp	192.168.1.152	SQL注入-Error
demo.aisec.cn:80	/demo/aisec/click_link.php?id=2-0 AND L...	192.168.1.54	SQL注入-SQLMap
222.209.252.8:80	POST /invoker/JMXInvokerServlet	192.168.1.80	命令执行
本地局域网-192.168.1.163:80	德国 POST /x.php	31.229.10.151	Web后门
本地局域网-192.168.1.70:80	POST /bWAPP/commandi.php	192.168.1.54	命令执行

设置“数据泄漏”响应规则：

当网页返回的报文流出了敏感数据，如：数据库的库名、管理员用户名、服务器的源代码，则发生报警，或者网页返回了“蜜罐服务器”中的“蜜”数据，则产生报警。

返回的敏感数据关键字：

下一步

返回的报文关键字：

(“蜜”的内容；可选参数)

下一步

4.2 威胁感知

利用
“全流量镜像分析技术”
定制入侵检测与漏洞感知引擎

示范1：触发页面出错 示范2：PHP信息泄漏 示范3：SQL注入尝试
示范4：黑名单 示范5：白名单 示范6：异常会话

事件分类 自定义-中危

攻击方式名称(自定义) PHP Information Leakage

域名关键字

URL包含以下关键字 phpinfo

文件名关键字

请求报文

回包部分：

返回结果包含以下关键字 <title>phpinfo()</title>&&>allow_url_fopen<

HTTP状态码

文件体积超过

源IP关键字

目的IP关键字

攻击描述(规则说明) 网页中泄露了phpinfo()的信息。

添加到规则库

- “两个动态”：漏洞动态增加、攻击技术动态进化
- 我们曾提出了三位一体的漏洞挖掘和分析方法，分别为：
 - (1) 基于**主动爬取（爬虫）**的扫描方法
 - (2) 基于代理或旁路抓url日志，再把url导入扫描器的**半被动扫描方法**
 - (3) 全被动的：基于旁路全报文分析，无发包的漏洞挖掘和威胁感知方法（PVS）**

基于旁路监听的全被动式入侵检测与漏洞感知系统，将会成为未来的技术趋势



- 技术交流: linx@aisec.com
- 安全智库 : <http://tt.aisec.com>
- 开放式引擎 : <http://ti.aisec.com>

An aerial photograph of a city at sunset. The sun is low on the horizon, casting a golden glow over the city. A wide river flows through the city, with a large bridge crossing it. The city skyline is visible in the background, and the foreground shows residential buildings and greenery.

Thanks.