

# 企业安全的另一道门

内网安全 - 向红阳

# Who am I

- 向红阳
- 11年加入PPTV
- 信息安全从业7年，乌云白帽子。
- 擅长内网攻击与防御、应急响应、入侵检测、数据分析，
- 放荡不羁，爱自由。



向红阳

上海 浦东新区



# 企业安全的另一道门

- 议题介绍

网络是企业业务的基础。在网络安全层面，传统防护的侧重对象通常是外网，内网及其运行或容纳的服务往往由于糟糕的安全性，成了影响企业业务的关键因素；因此，增强内网安全可以视为完善企业安全的另一道门。

- 哪些被我们忽略而又严重的安全边界漏洞

- 实例

- 我的一些防御思路

# 企业内网安全重要性

- 办公网络
- 生产网络
- 其他





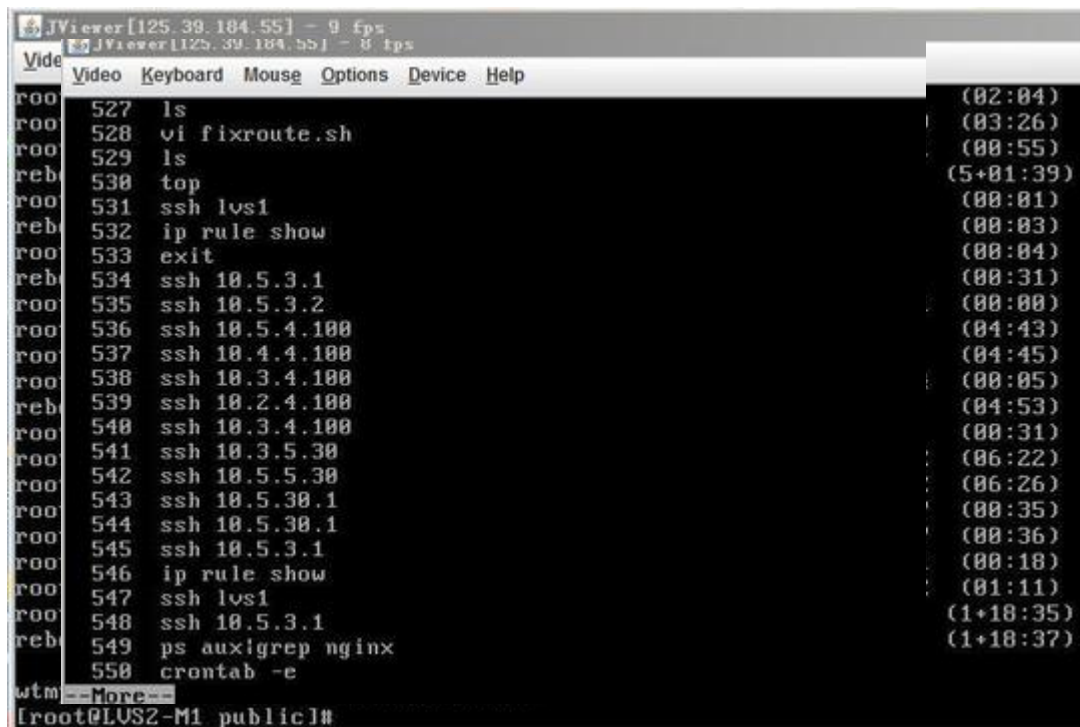
# 企业内网安全

那些严重的而且极易被忽略的

- 顽固的默认设置
- 缺失的安全边界
- 任性的代码实现
- 迟缓的事件处理
- 被动的日志审计

# D1 – 顽固的默认设置

## 默认口令——



The screenshot shows a JViewer window with a menu bar (Video, Keyboard, Mouse, Options, Device, Help) and a terminal window. The terminal displays a list of commands and their execution times, with a prompt at the bottom: [root@LUS2-M1 public]#

Command	Execution Time
527 ls	(02:04)
528 vi fixroute.sh	(03:26)
529 ls	(00:55)
530 top	(5+01:39)
531 ssh lvs1	(00:01)
532 ip rule show	(00:03)
533 exit	(00:04)
534 ssh 10.5.3.1	(00:31)
535 ssh 10.5.3.2	(00:00)
536 ssh 10.5.4.100	(04:43)
537 ssh 10.4.4.100	(04:45)
538 ssh 10.3.4.100	(00:05)
539 ssh 10.2.4.100	(04:53)
540 ssh 10.3.4.100	(00:31)
541 ssh 10.3.5.30	(06:22)
542 ssh 10.5.5.30	(06:26)
543 ssh 10.5.30.1	(00:35)
544 ssh 10.5.30.1	(00:36)
545 ssh 10.5.3.1	(00:18)
546 ip rule show	(01:11)
547 ssh lvs1	(1+18:35)
548 ssh 10.5.3.1	(1+18:37)
549 ps aux grep nginx	
550 crontab -e	

wtm --force--  
[root@LUS2-M1 public]#

## D2 – 缺失的边界和任性的实现 绕过ACL，从外网访问管理后台





## D3-我们熟悉的管理系统

名称	#	成员
admin servers	模板 (14) 主机 (3)	check http page, check ip_port, hardware, http80, infolist WEB, Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 10.4.10.27, 192.168.9.35, 192.168.9.35 test
check_ip_port	模板 (0) 主机 (18)	10.4.11.20, 192.168.11.11, 192.168.11.12, 192.168.11.21, 192.168.11.72, 192.168.11.79, 192.168.11.90, 192.168.11.97, 192.168.11.104, 192.168.11.172, 192.168.14.21, 192.168.14.208, 192.168.14.209, 192.168.14.210, 192.168.14.211
DBSERVER	模板 (4) 主机 (148)	Linux, Linux 2G mem, Linux 400processes, Linux 400processes 50load 10.3.11.11, 10.3.11.12, 10.3.11.13, 10.3.11.14, 10.3.11.15, 10.3.11.16, 10.3.11.17, 10.3.11.18, 10.3.11.19, 10.3.11.20, 10.3.11.21, 10.3.11.22, 10.3.11.23, 10.3.11.24, 10.3.11.25, 10.3.11.26, 10.3.11.27, 10.3.11.28, 10.3.11.29, 10.3.11.30, 10.3.11.31, 10.3.11.32, 10.3.11.33, 10.3.11.34, 10.3.11.35, 10.3.11.36, 10.3.11.37, 10.3.11.38, 10.3.11.39, 10.3.11.40, 10.3.11.41, 10.3.11.42, 10.3.11.43, 10.3.11.44, 10.3.11.45, 10.3.11.46, 10.3.11.47, 10.3.11.48, 10.3.11.49, 10.3.11.50, 10.3.11.51, 10.3.11.52, 10.3.11.53, 10.3.11.54, 10.3.11.55, 10.3.11.56, 10.3.11.57, 10.3.11.58, 10.3.11.59, 10.3.11.60, 10.3.11.61, 10.3.11.62, 10.3.11.63, 10.3.11.64, 10.3.11.65, 10.3.11.66, 10.3.11.67, 10.3.11.68, 10.3.11.69, 10.3.11.70, 10.3.11.71, 10.3.11.72, 10.3.11.73, 10.3.11.74, 10.3.11.75, 10.3.11.76, 10.3.11.77, 10.3.11.78, 10.3.11.79, 10.3.11.80, 10.3.11.81, 10.3.11.82, 10.3.11.83, 10.3.11.84, 10.3.11.85, 10.3.11.86, 10.3.11.87, 10.3.11.88, 10.3.11.89, 10.3.11.90, 10.3.11.91, 10.3.11.92, 10.3.11.93, 10.3.11.94, 10.3.11.95, 10.3.11.96, 10.3.11.97, 10.3.11.98, 10.3.11.99, 10.3.11.100, 10.3.11.101, 10.3.11.102, 10.3.11.103, 10.3.11.104, 10.3.11.105, 10.3.11.106, 10.3.11.107, 10.3.11.108, 10.3.11.109, 10.3.11.110, 10.3.11.111, 10.3.11.112, 10.3.11.113, 10.3.11.114, 10.3.11.115, 10.3.11.116, 10.3.11.117, 10.3.11.118, 10.3.11.119, 10.3.11.120, 10.3.11.121, 10.3.11.122, 10.3.11.123, 10.3.11.124, 10.3.11.125, 10.3.11.126, 10.3.11.127, 10.3.11.128, 10.3.11.129, 10.3.11.130, 10.3.11.131, 10.3.11.132, 10.3.11.133, 10.3.11.134, 10.3.11.135, 10.3.11.136, 10.3.11.137, 10.3.11.138, 10.3.11.139, 10.3.11.140, 10.3.11.141, 10.3.11.142, 10.3.11.143, 10.3.11.144, 10.3.11.145, 10.3.11.146, 10.3.11.147, 10.3.11.148, 10.3.11.149, 10.3.11.150, 10.3.11.151, 10.3.11.152, 10.3.11.153, 10.3.11.154, 10.3.11.155, 10.3.11.156, 10.3.11.157, 10.3.11.158, 10.3.11.159, 10.3.11.160, 10.3.11.161, 10.3.11.162, 10.3.11.163, 10.3.11.164, 10.3.11.165, 10.3.11.166, 10.3.11.167, 10.3.11.168, 10.3.11.169, 10.3.11.170, 10.3.11.171, 10.3.11.172, 10.3.11.173, 10.3.11.174, 10.3.11.175, 10.3.11.176, 10.3.11.177, 10.3.11.178, 10.3.11.179, 10.3.11.180, 10.3.11.181, 10.3.11.182, 10.3.11.183, 10.3.11.184, 10.3.11.185, 10.3.11.186, 10.3.11.187, 10.3.11.188, 10.3.11.189, 10.3.11.190, 10.3.11.191, 10.3.11.192, 10.3.11.193, 10.3.11.194, 10.3.11.195, 10.3.11.196, 10.3.11.197, 10.3.11.198, 10.3.11.199, 10.3.11.200, 10.3.11.201, 10.3.11.202, 10.3.11.203, 10.3.11.204, 10.3.11.205, 10.3.11.206, 10.3.11.207, 10.3.11.208, 10.3.11.209, 10.3.11.210, 10.3.11.211, 10.3.11.212, 10.3.11.213, 10.3.11.214, 10.3.11.215, 10.3.11.216, 10.3.11.217, 10.3.11.218, 10.3.11.219, 10.3.11.220, 10.3.11.221, 10.3.11.222, 10.3.11.223, 10.3.11.224, 10.3.11.225, 10.3.11.226, 10.3.11.227, 10.3.11.228, 10.3.11.229, 10.3.11.230, 10.3.11.231, 10.3.11.232, 10.3.11.233, 10.3.11.234, 10.3.11.235, 10.3.11.236, 10.3.11.237, 10.3.11.238, 10.3.11.239, 10.3.11.240, 10.3.11.241, 10.3.11.242, 10.3.11.243, 10.3.11.244, 10.3.11.245, 10.3.11.246, 10.3.11.247, 10.3.11.248, 10.3.11.249, 10.3.11.250, 10.3.11.251, 10.3.11.252, 10.3.11.253, 10.3.11.254, 10.3.11.255, 10.3.11.256, 10.3.11.257, 10.3.11.258, 10.3.11.259, 10.3.11.260, 10.3.11.261, 10.3.11.262, 10.3.11.263, 10.3.11.264, 10.3.11.265, 10.3.11.266, 10.3.11.267, 10.3.11.268, 10.3.11.269, 10.3.11.270, 10.3.11.271, 10.3.11.272, 10.3.11.273, 10.3.11.274, 10.3.11.275, 10.3.11.276, 10.3.11.277, 10.3.11.278, 10.3.11.279, 10.3.11.280, 10.3.11.281, 10.3.11.282, 10.3.11.283, 10.3.11.284, 10.3.11.285, 10.3.11.286, 10.3.11.287, 10.3.11.288, 10.3.11.289, 10.3.11.290, 10.3.11.291, 10.3.11.292, 10.3.11.293, 10.3.11.294, 10.3



- 程序漏洞,反弹shell
- 程序漏洞,上传webshell,代理
- 扫描
- 服务器登录
- 后门

# 监控系统引发的内网入侵事件

Zenoss CORE						
DASHBOARD   EVENTS   INFRASTRUCTURE   REPORTS   ADVANCED						
Devices <b>Networks</b> Processes   IP Services   Windows Services   Network Map   Manufacturers						
Display: IP Addresses						
IPs Used/Free						
Address / Netmask   Device   Interface   MAC Address   Interface Desc.   Pi						
NETWORKS/24 (6966)						
1.1.1.0/24 (1)						
10.0.0.0/8 (4352)						
111.1.16.0/24 (54)						
112.117.209.0/24 (51)						
112.25.12.0/24 (0)						
112.25.32.0/24 (21)						
112.5.187.0/24 (0)						
113.105.173.0/24 (0)						
113.105.226.0/24 (52)						
113.105.227.0/24 (7)						
113.105.228.0/24 (30)						
113.105.251.0/24 (31)						
113.107.113.0/24 (16)						
113.17.168.0/24 (35)						
114.80.180.0/24 (11)						
114.80.184.0/24 (80)						
114.80.185.0/24 (13)						
114.80.186.0/24 (0)						
114.80.69.0/24 (8)						
115.238.229.0/24 (1)						
116.114.22.0/24 (0)						
1.1.1.1/32						
10.10.220.1/64						
10.10.220.18/24						
10.10.254.26/32						
10.102.1.1/24						
10.102.1.10/24						
10.102.1.100/24						
10.102.1.101/24						
10.102.1.102/24						
10.102.1.103/24						
10.102.1.104/24						
10.102.1.105/24						
10.102.1.106/24						
10.102.1.107/24						
10.102.1.108/24						
10.102.1.109/24						
10.102.1.11/24						
10.102.1.110/24						
10.102.1.111/24						
10.102.1.112/24						

# 他干了些什么

- 扫描
- 登录

10.10.65.92 "root/123456"

10.10.65.129 "root/111111"

10.10.65.133 "root/123456"

10.10.221.61 "root/123456"

10.10.221.63 "root/123456"

10.10.236.11 "root/123456"

# 系统日志

- 基于日志的防御体系

OSSEC HIDS Notification.

2015 Apr 03 14:57:37

Received From: ~~shwgg@torontor-189-81~~ -> /home/logs/rsyslog/pplive\_sec.log

Rule: 5715 fired (level 7) -> "pplive user login"

Portion of the log(s):

2015-04-03T14:57:34+08:00 ~~shwgg@torontor-189-81~~ sshd[2313]: Accepted password for ~~blinchen~~ from 10.~~28.188~~.75 port 58247 ssh2

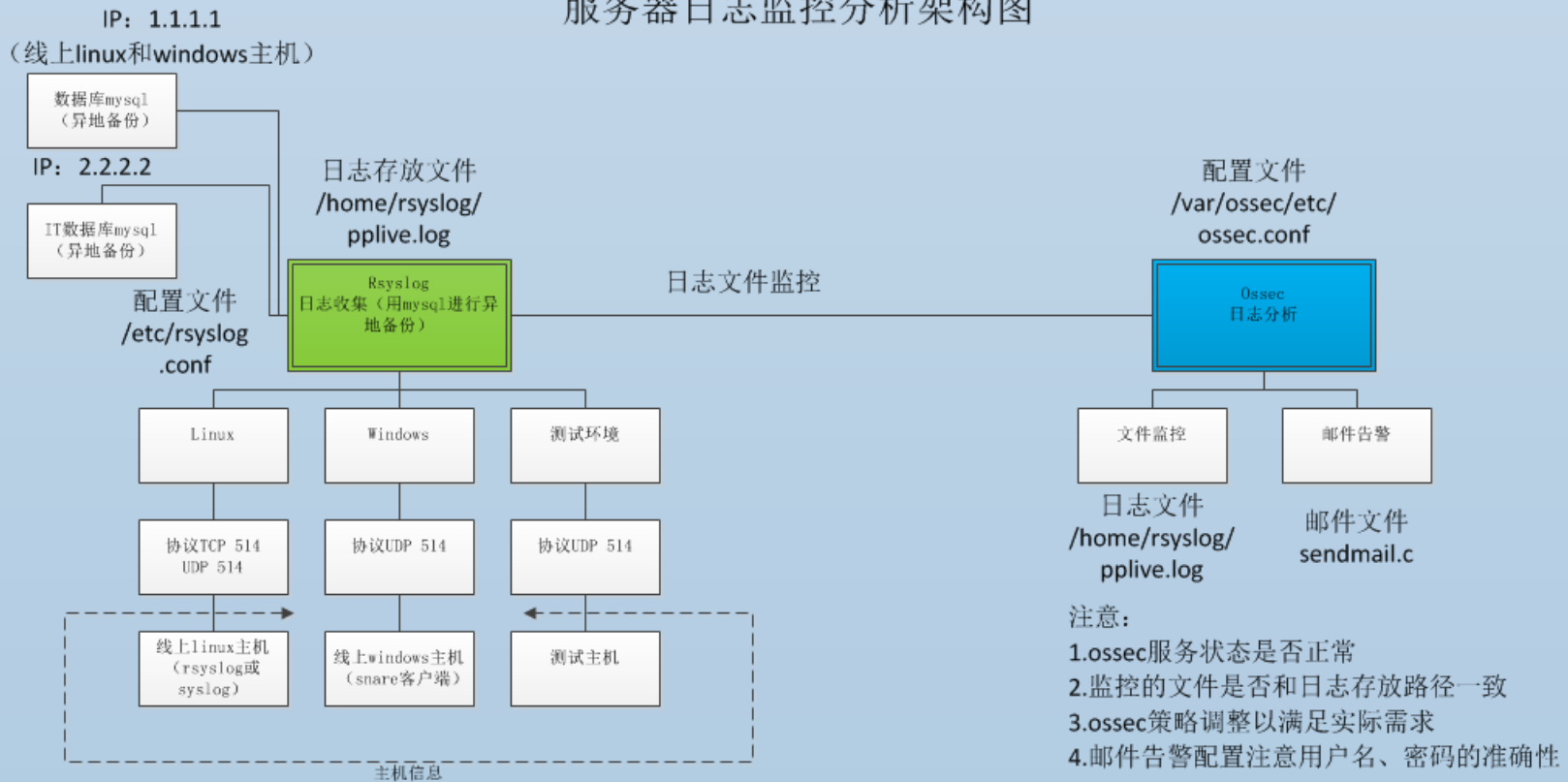
--END OF NOTIFICATION

# 怎么破？

- 如何做到

# Rsyslog+ossec

服务器日志监控分析架构图



注意:

- 1.主机的CPU、内存、磁盘使用率, 建议接入zabbix进行监控
- 2.主机端口链接是否正常 (TCP和UDP的514端口是否处于监听状态)
- 3.rsyslog服务状态是否正常
- 4.主机是否开启iptables

注意:

- 1.ossec服务状态是否正常
- 2.监控的文件是否和日志存放路径一致
- 3.ossec策略调整以满足实际需求
- 4.邮件告警配置注意用户名、密码的准确性



# 头疼的webshell

提交日期: 2015-03-12 作者: cd@zone

HostName: ~~bjch-mch-qclua.php-10-~~  
30.idc.pplive.cn; FileName: '~~/home/pplive/web/ms\_test/ms\_php1.php~~'; Feature: Rename:evalbackdoor; MatchRule: REpattern:eval\s\*(\s\*? \\\$\\\_POST;

#####

[浙江大学分站三个后台弱口令+SQL注入已getshell](#)

如题...第一个弱口令 http://www.cec.zju.edu.cn/wescms/index.php cgsoft kf1013 第二个弱口令 http://ipe.zju.edu.cn/manage/System\_main.asp admin admin 第三个弱口令+webshell

HostName: ~~shbun-mch-qclua.php-10-~~  
164.idc.pplive.cn; FileName: '~~/home/pplive/web/pplux/up/uploadlogmoddo.jsp~~'; Feature: REpattern:Runtime.\*\s\*exec\(| MatchRule: RawLine:Pro  
exec = Runtime.getRuntime().exec(cmd); ;

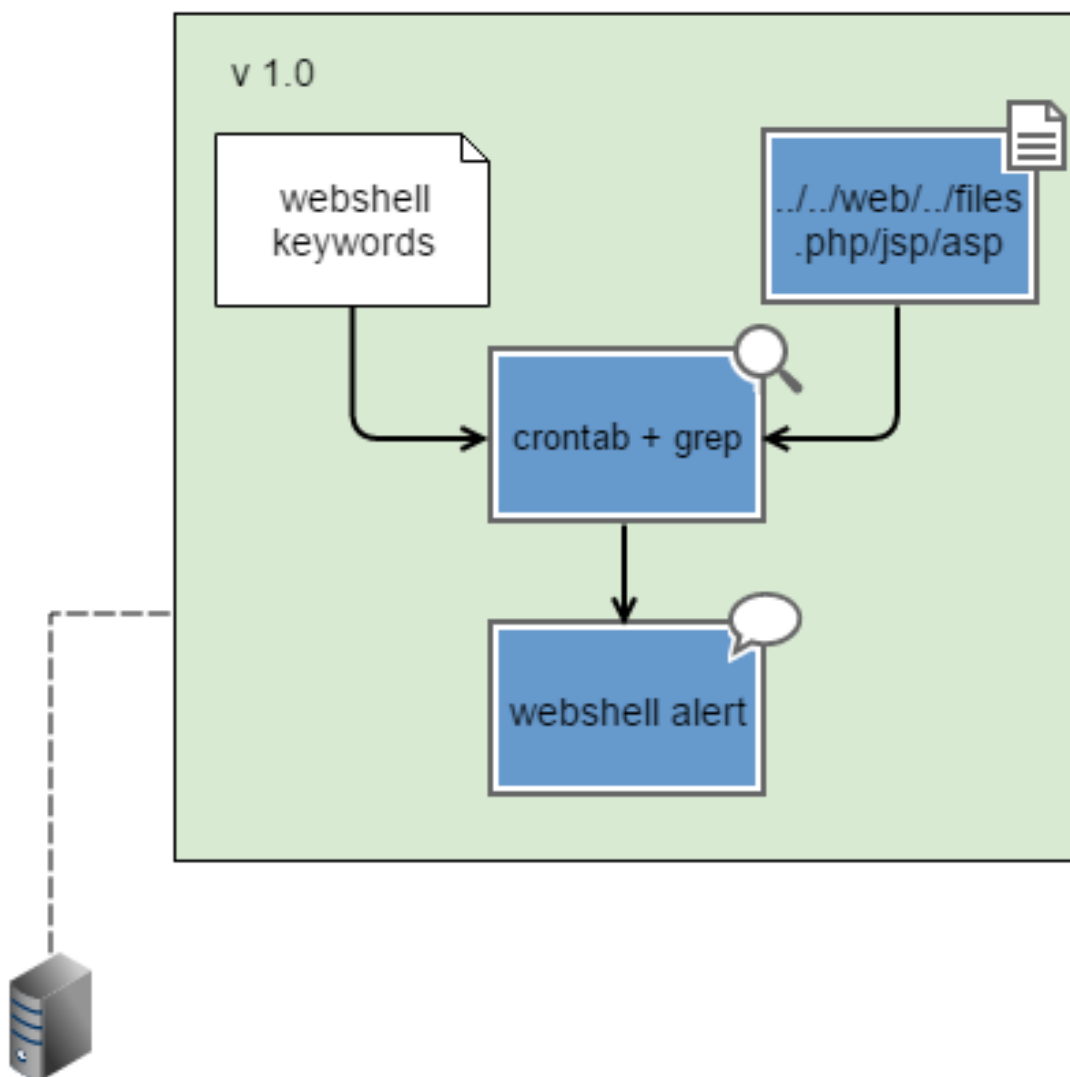
#####

未对数据进行任何破坏与修改 首先在浏览器里输入 http://yx.yiqifei.com 会提示你登录 这里随便注册一个帐号然后登录就行了 登录后会跳转到广告管理页面 这里其实就是越权了广告位只有管理员才能添加吧 网站信息一览无遗 当...

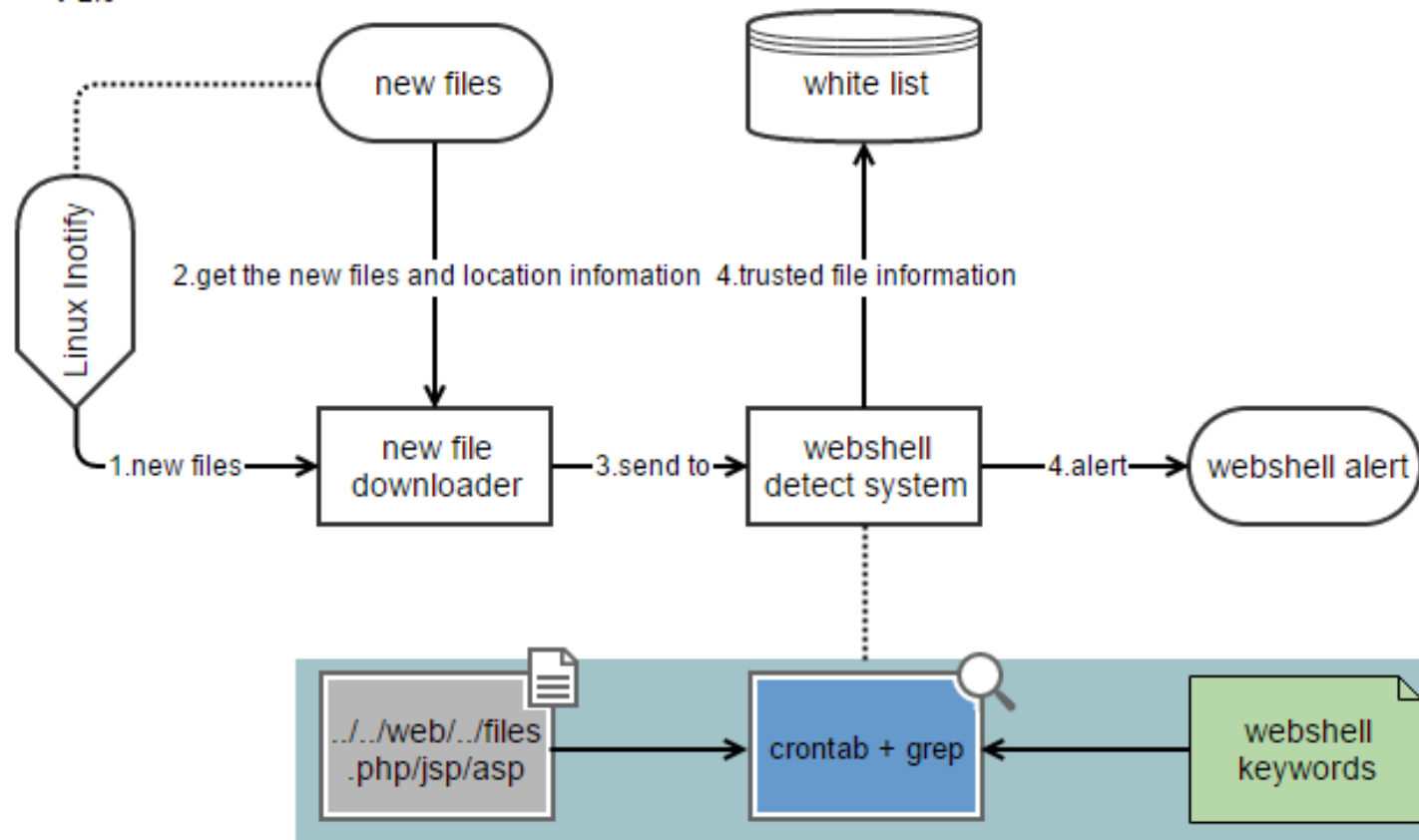
提交日期: 2015-03-05 作者: 天地不仁 以万物为刍狗

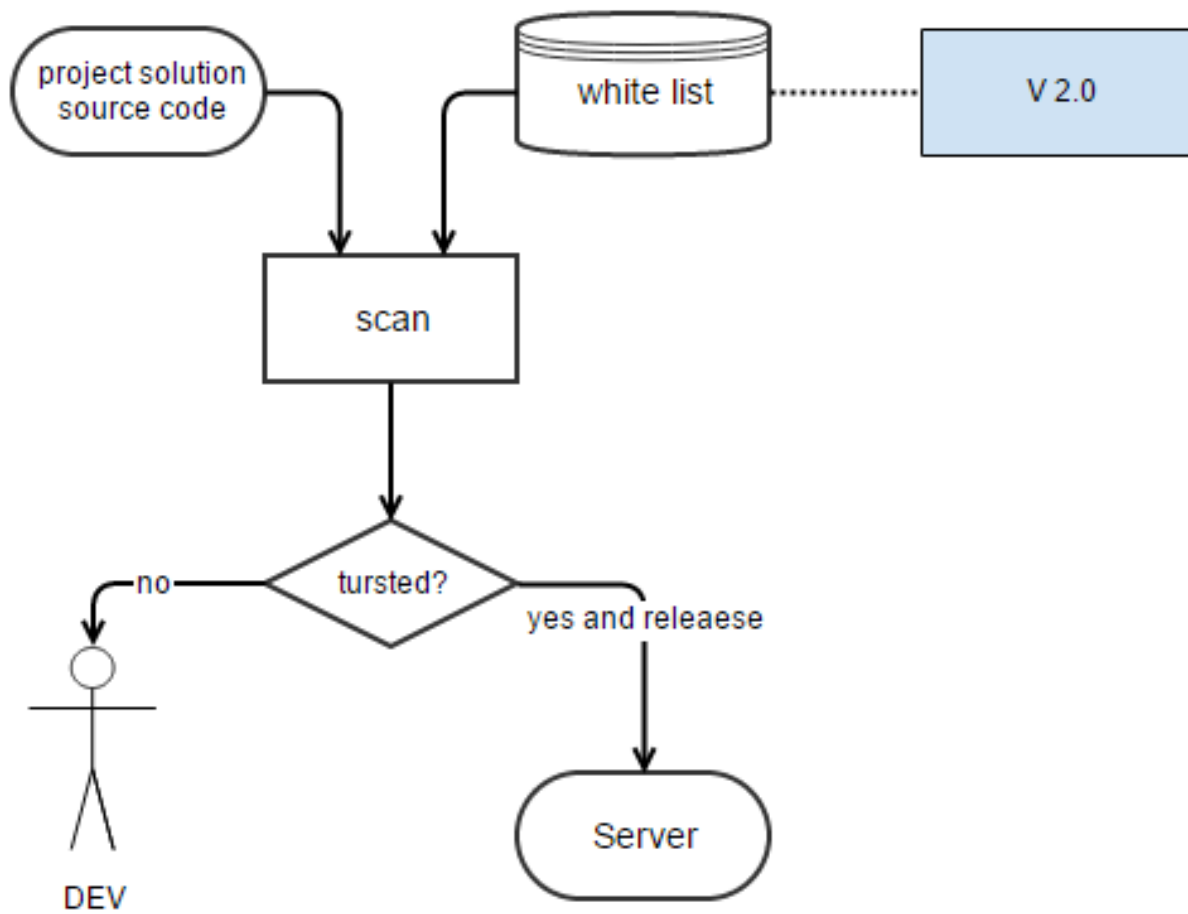


# 建立一个webshell查找响应



V 2.0





# 端口扫描的必要性

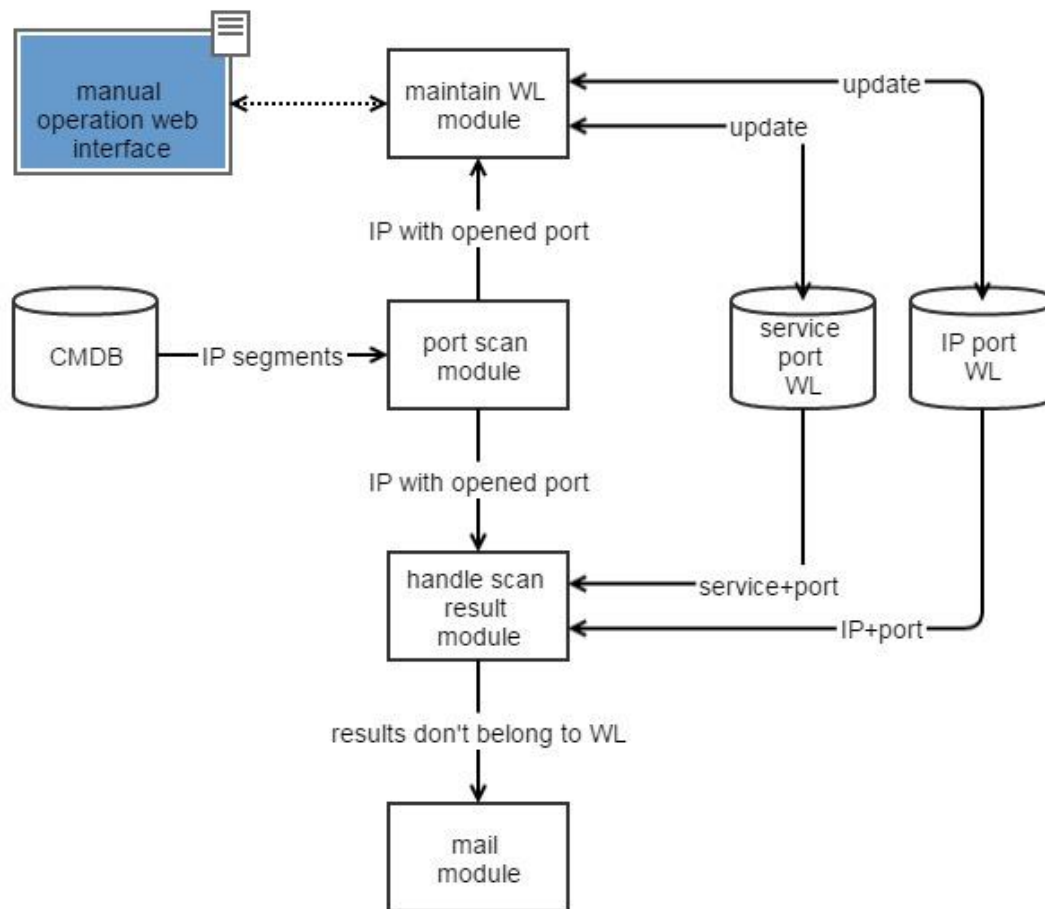
详细说明：

`http://114.80.121.203:8000/zabbix`

`admin admin` 不解释

漏洞证明：

10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13795	Too many processes running on {HOST.NAME}	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13802	{HOST.NAME} has just been restarted	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13799	Hostname was changed on {HOST.NAME}	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13792	Version of zabbix_agent(d) was changed on {HOST.NAME}	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13800	Lack of free swap space on {HOST.NAME}	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13796	Too many processes on {HOST.NAME}	
10 六月 14:48:50	sop	10.5.10.40	触发器	已添加	13803	/etc/passwd has been changed on {HOST.NAME}	
10 六月 14:47:53	sop	10.5.10.40	主机	已添加	10115	b02.write.vpe.db.qd.tudou.com	
10 六月 14:47:16	sop	10.5.10.40	触发器	已删除	13768	MySQL slave lag more than 300 on {HOST.NAME}	
10 六月 14:47:16	sop	10.5.10.40	触发器	已删除	13775	Version of zabbix_agent(d) was changed on {HOST.NAME}	
10 六月 14:47:16	sop	10.5.10.40	触发器	已删除	13779	Too many processes on {HOST.NAME}	
10 六月 14:47:16	sop	10.5.10.40	触发器	已删除	13765	MySQL connections utilization {HOST.NAME}	
10 六月 14:47:16	sop	10.5.10.40	触发器	已删除	13786	/etc/passwd has been changed on {HOST.NAME}	



# Dns日志我们可以做什么

	尊敬的：各位领导及同仁
维护原因	公司办公自动化（OA）自运行以来，不断优化完善。为提高办公效率，实现无纸化办公，公司将全面推进办公自动化（OA）的使用。现对所有用户邮箱进行版本升级！由于您长期未验证邮件系统账号信息，导致系统无法识别信息，或超过三个月未登录！为保证正常使用（现需要对邮箱进行升级并需要重新采集用户信息）
维护时间	本次升级检测为期 7-15 天，为此给你带了不便的地方，敬请理解。
注意事项	为确保合理使用 OA 系统资源，若是收到此通知当天下班前没有前往升级或者校验用户信息，后台将自动识别此用户或是无人使用的邮箱，将被自动删除，感谢您的配合！
操作指示	<a href="#">请点击这里进行升级</a>

# Q&A

any questions?

谢谢大家！