宝付：基于安全运维的实践应用分享

分享

1 **资产**
资产的识别和准确性

2 **漏洞及补丁**
补丁及漏洞的管理

3 **端口扫描及弱点**
端口扫描及常见端口存在的安全问题

4 **日志的采集及审计**
如何利用日志服务器提高工作效率

我们到底有多少资产?

主机

网络

数据库

中间件

域名

资产不准确会面临哪些问题?

- 在安全运维中遗漏对资产的管理，造成潜在的安全隐患
- 无法准确定位资产的属性（物理位置/用途）
- 应对第三方审核机构的检查，成为不符合项

如何正确管理资产

- 有资产变动时及时更新资产信息
- 明确资产责任人
- 定期对资产进行清查，确保资产准确性
- 使用产品（联软/ forescout等）与日志服务器联动，或其他技术手段进行资产发现
- 对防火墙策略进行梳理，查看对应的映射策略/端口，并确认业务类型

漏洞及补丁

为什么要打补丁?

微软发布补丁的日期:

爆发日期：

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约172,000个 搜索工具

永恒之蓝时间：

2017年5月12日

永恒之蓝是指2017年5月12日起，全球范围内爆发的基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序... 详情>>

来自百度百科 | 报错

永恒之蓝_百度百科

永恒之蓝是指2017年5月12日起，全球范围内爆发的基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的...

事件经过 攻击方式 事件影响 病毒防范

baike.baidu.com/

OH,MY GOD。。。。。GAME OVER

如何管理补丁

- 定期对企业内部进行漏洞扫描（NESSUS/NEXPOSE/OPENVAS等）
- 建立统一的补丁管理工具（WSUS）
- 强制开发或运维人员更新补丁
- 建立版本标准，部署数据库/中间件都按照安全建议的版本安装，并每年更新一次版本标准
- 虚拟化部署，可利用模板化部署方式，免去打补丁所带来的困扰，并定期更新模板

端口扫描及弱点

为什么要进行端口扫描?

拒绝对外开放高危端口

保证自身端口安全

常见端口存在的安全风险

端口	对应服务	风险
22	SSH	弱口令探测
3389	RDP	弱口令探测/利用ms12-020攻击3389端口
3306	MySQL	弱口令探测/各种版本的漏洞
1521	ORACLE	弱口令探测/各种版本的漏洞
6379	Redis	未授权访问
80/8080	Apache/Tomcat	目录遍历/弱口令探测
11211	Memcached	未授权访问
445	Samba-NetBIOS服务	MS17-010漏洞
1443	MSSQL	弱口令探测/各种版本的漏洞
2049	NFS	未授权访问
9043	Websphere	密码爆破/JAVA反序列化
7001/7002	Weblogic	密码爆破/JAVA反序列化
161	SNMP	未授权访问

实际案例-1 弱口令探测

```
Starting Nmap 7.50 ( https://nmap.org ) at 2018-04-11 22:30 CST
Nmap scan report for 192.168.10.19
Host is up (0.000024s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
3306/tcp open  mysql   MySQL 5.1.73
MAC Address: 00:0C:29:9D:4D:79 (VMware)
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-11 22:35:33
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (l:1/p:7), ~2 tries per task
[DATA] attacking service mysql on port 3306
[ATTEMPT] target 192.168.10.19 - login "root" - pass "admin" - 1 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "superadmin" - 2 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "test" - 3 of 7 [child 2] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "123456789" - 4 of 7 [child 3] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "123456" - 5 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "1qaz@WSX" - 6 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.10.19 - login "root" - pass "root" - 7 of 7 [child 2] (0/0)
[3306][mysql] host: 192.168.10.19   login: root   password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-11 22:35:34
```

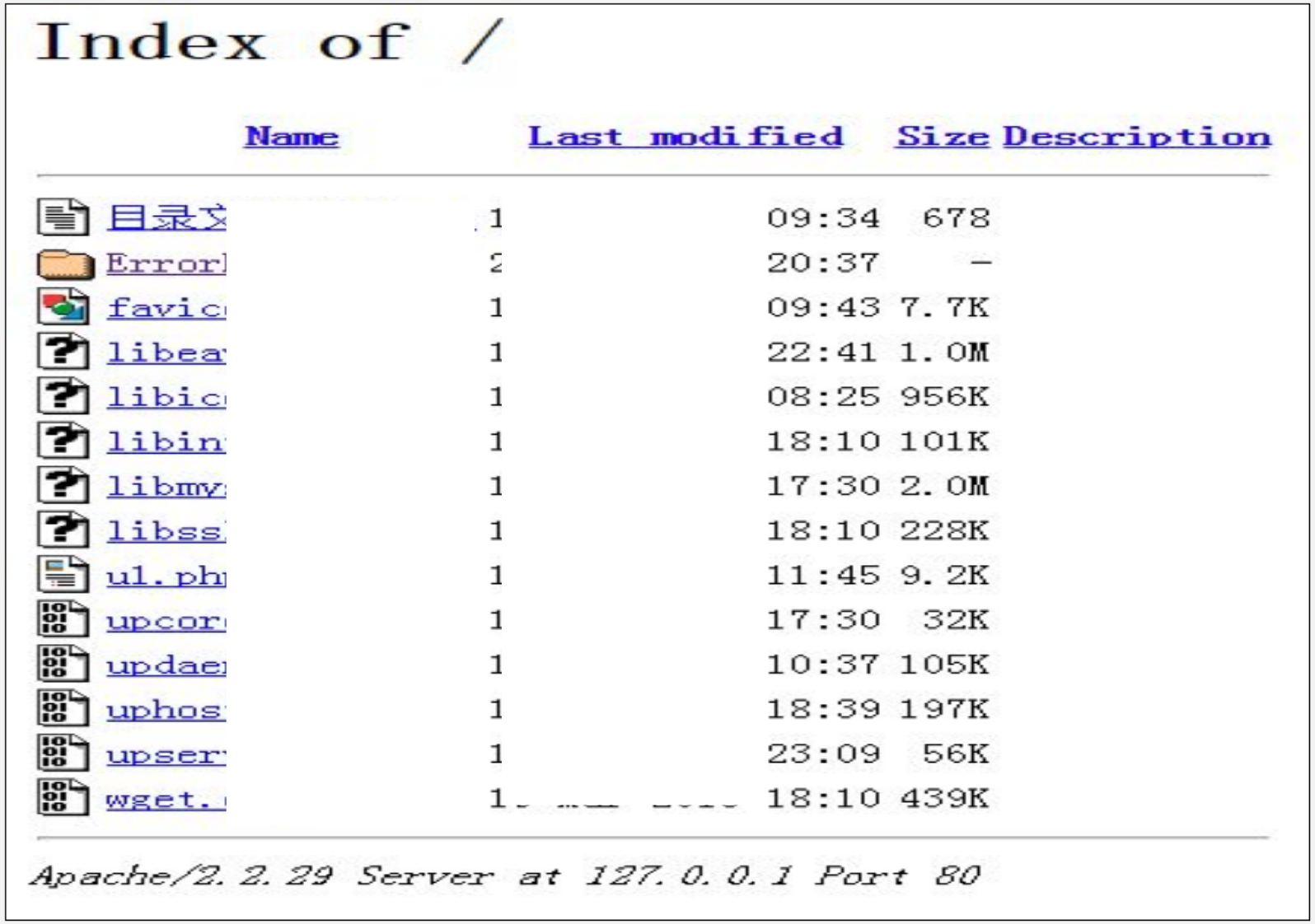
实际案例-2 Redis未授权访问

```
Nmap scan report for 192.168.10.73
Host is up (0.000054s latency).
Not shown: 29997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
6379/tcp open  redis   Redis key-value store 2.4.17
MAC Address: 00:0C:29:7F:FC:D3 (VMware)
```

实际案例-3 Java反序列化

```
Nmap scan report for 192.168.10.132
Host is up (0.000081s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE           VERSION
80/tcp    open  http              Microsoft IIS httpd 7.5
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server     Microsoft Terminal Service
5060/tcp  open  sip               (SIP end point; Status: 503 Service Unavailable)
5061/tcp  open  ssl/sip-tls?
7001/tcp  open  http              Oracle WebLogic Server (Servlet 2.5; JSP 2.1)
7002/tcp  open  ssl/afs3-prserver?
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49156/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  msrpc             Microsoft Windows RPC
```

实际案例-4 Apache列目录



解决建议

系统配置账号复杂度策略

修改/etc/pam.d/system-auth文件

在password requisite pam_cracklib.so后追加以下参数

password requisite pam_cracklib.so retry=5 difok=3 minlen=8 ucredit=1 lcredit=1 dcredit=1 ocredit=1

difok：最少不同字符3

minlen：最小密码长度8

ucredit：大写字母个数1

lcredit：小写字母个数1

dcredit：数字个数1

ocredit：特殊字符个数1

系统配置账号锁定策略

编辑/etc/pam.d/password-auth

添加以下内容：

auth required pam_tally2.so onerr=fail even_deny_root deny=5 unlock_time=300

onerr=fail deny=5 unlock_time=300

登入失败次数超过5次，锁定时间300秒

系统配置账号锁定策略

编辑/etc/pam.d/password-auth

添加以下内容：

auth required pam_tally2.so onerr=fail even_deny_root deny=5 unlock_time=300

onerr=fail deny=5 unlock_time=300

登入失败次数超过5次，锁定时间300秒

Redis添加认证机制

编辑redis.conf

取消以下内容注释：

#requirepass foobared

修改后：

requirepass jdd#$DEW!5372

Requirepass后为自定义密码

重启redis服务

Apache目录遍历

编辑httpd.conf文件

方法1：将所有Options关键字后的Indexes去掉

方法2：在配置文件中将配置修改为如下所示：

Options –Indexes

重启Apache服务

日志的采集及审计

为什么要日志服务器?

合规需求

集中管理

日志审计

接入日志的准备工作

接入范围

日志级别

日志格式化

日志级别

emerg	系统不可用
alerts	必须立即采取措施
critical	致命错误
errors	错误状态
warnings	警告状态
notifications	一个平常的但重要的事件
informational	一个信息事件
debugging	debug信息

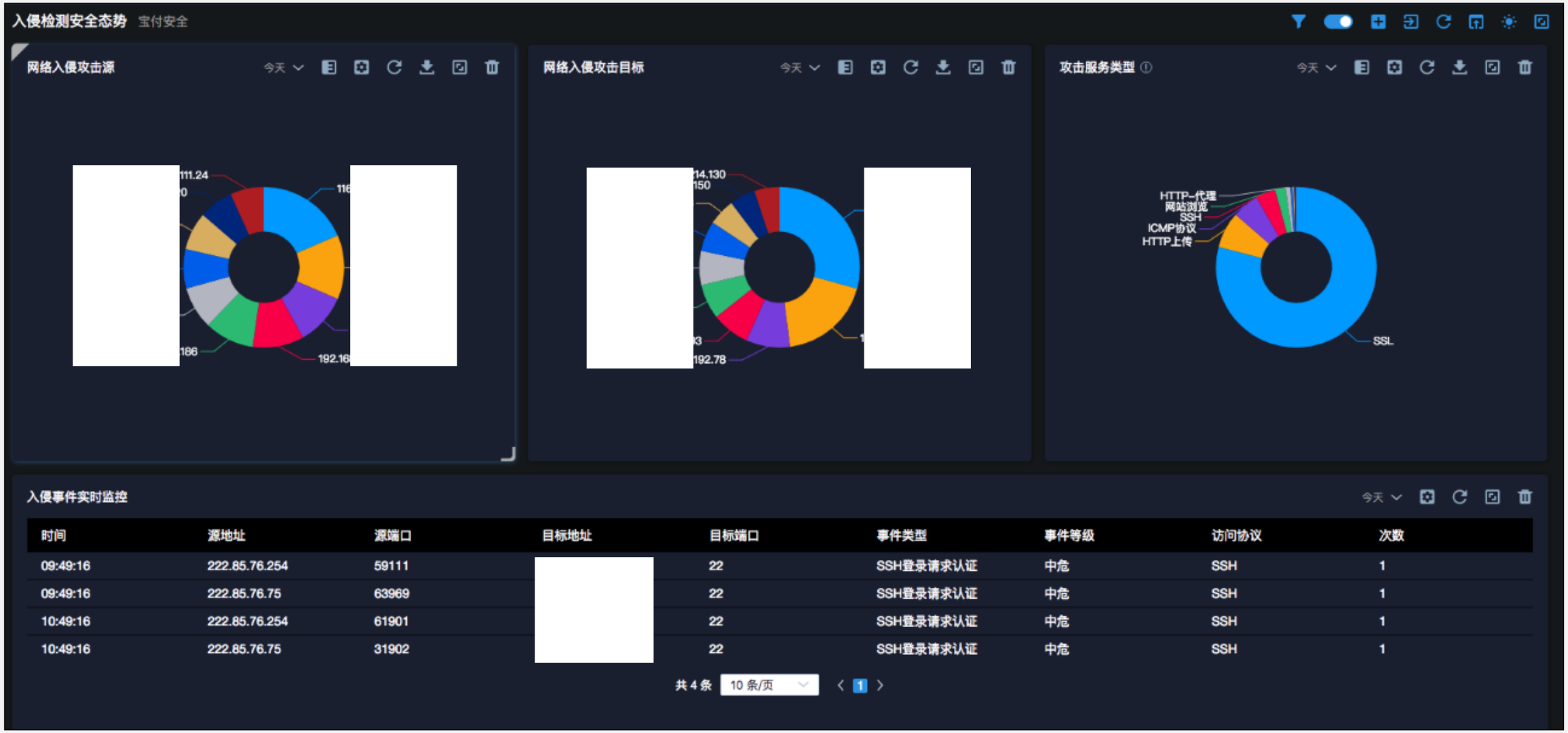
日志接入后的运维工作

日志查询

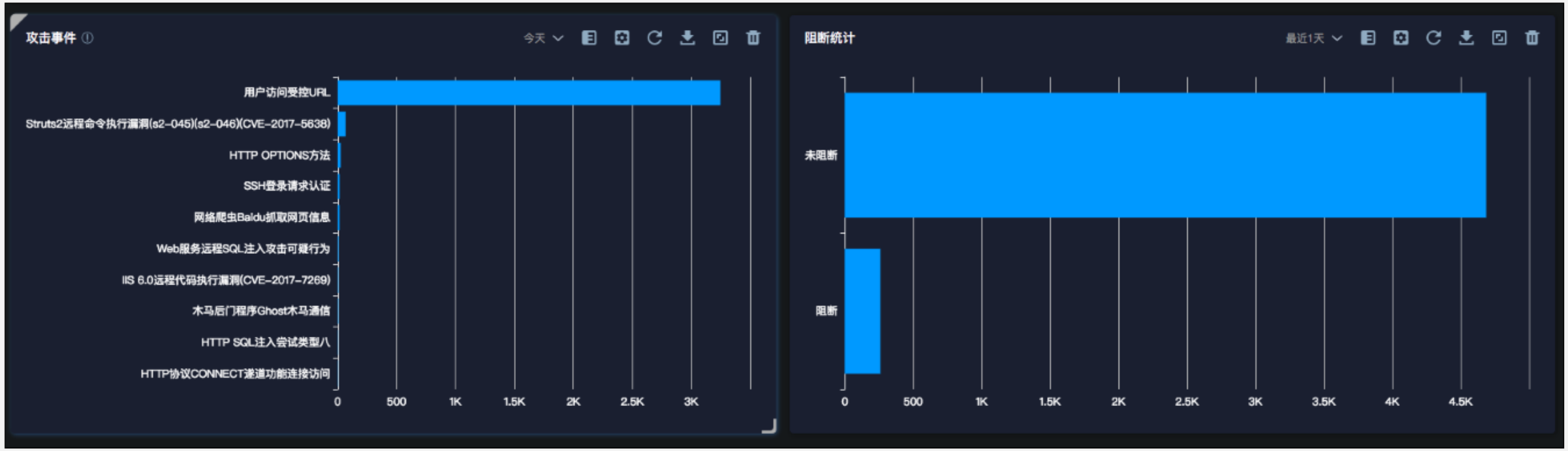
集中分析

仪表展示

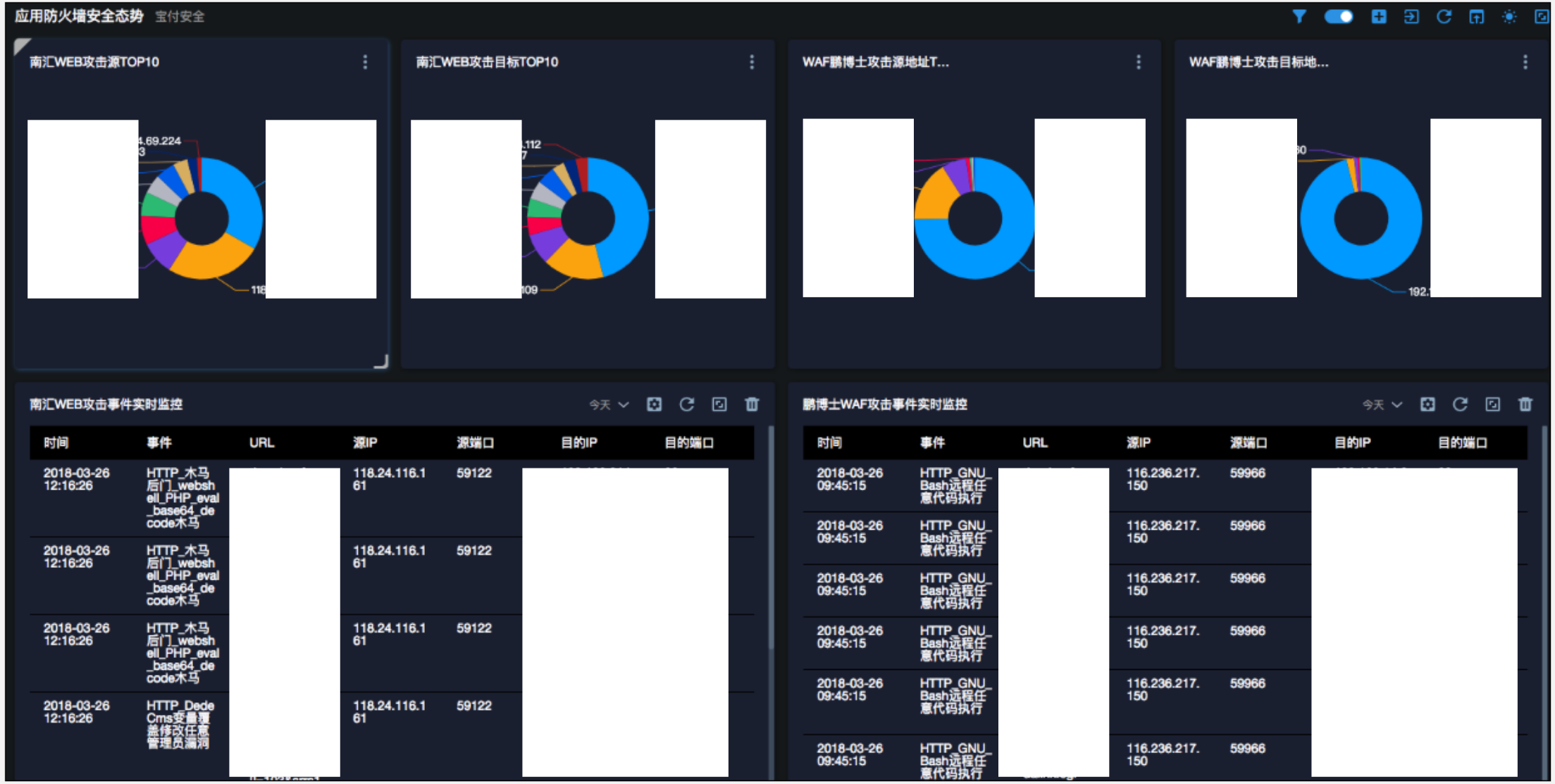
宝付案例-仪表盘大屏


入侵检测安全态势 宝付安全
网络入侵攻击源
今天
111.24
0
116
186
192.16
网络入侵攻击目标
今天
14.130
150
3
192.78
攻击服务类型
今天
HTTP-代理
网站浏览
SSH
ICMP协议
HTTP上传
SSL
入侵事件实时监控
今天
时间 源地址 源端口 目标地址 目标端口 事件类型 事件等级 访问协议 次数
09:49:16 222.85.76.254 59111 22 SSH登录请求认证 中危 SSH 1
09:49:16 222.85.76.75 63969 22 SSH登录请求认证 中危 SSH 1
10:49:16 222.85.76.254 61901 22 SSH登录请求认证 中危 SSH 1
10:49:16 222.85.76.75 31902 22 SSH登录请求认证 中危 SSH 1
共 4 条
10 条/页
1

宝付案例-仪表盘大屏


攻击事件
今天
用户访问受控URL
Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)
HTTP OPTIONS方法
SSH登录请求认证
网络爬虫Baidu抓取网页信息
Web服务远程SQL注入攻击可疑行为
IIS 6.0远程代码执行漏洞(CVE-2017-7269)
木马后门程序Ghost木马通信
HTTP SQL注入尝试类型八
HTTP协议CONNECT遂道功能连接访问
0
500
1K
1.5K
2K
2.5K
3K
阻断统计
最近1天
未阻断
阻断
0
500
1K
1.5K
2K
2.5K
3K
3.5K
4K
4.5K

宝付案例-仪表盘大屏


应用防火墙安全态势 宝付安全
南汇WEB攻击源TOP10
南汇WEB攻击目标TOP10
WAF鹏博士攻击源地址T...
WAF鹏博士攻击目标地...
南汇WEB攻击事件实时监控
今天
时间 事件 URL 源IP 源端口 目的IP 目的端口
2018-03-26 12:16:26 HTTP_木马后门_webshell_PHP_eval_base64_decode木马 118.24.116.161 59122
2018-03-26 12:16:26 HTTP_木马后门_webshell_PHP_eval_base64_decode木马 118.24.116.161 59122
2018-03-26 12:16:26 HTTP_木马后门_webshell_PHP_eval_base64_decode木马 118.24.116.161 59122
2018-03-26 12:16:26 HTTP_DedeCms变量覆盖修改任意管理员漏洞 118.24.116.161 59122
鹏博士WAF攻击事件实时监控
今天
时间 事件 URL 源IP 源端口 目的IP 目的端口
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966
2018-03-26 09:45:15 HTTP_GNU_Bash远程任意代码执行 116.236.217.150 59966

宝付案例-仪表盘大屏


WAF高危事件...
22 4.35%
WAF中危事件...
4 0%
WAF低危事件...
4419 3299.23%
IPS高危事件数
240 300%
IPS中危事件数
32 31.91%
IPS低危事件数
4586 3.74%
南汇专线防火墙TOP10...
南汇专线防火墙TOP10...
南汇外网防火墙访问源IP
南汇外网防火墙访问目...
南汇专线防火墙流量
最近30分钟
6
5
4
3
2
1
0
35:00
40:00
45:00
50:00
55:00
南汇公网防火墙流量
最近30分钟
4K
3K
2K
1K
0
35:00
40:00
45:00
50:00
55:00

宝付案例-操作行为审计

时间	用户名	动作	操作内容	信息
2018-03-20 18:51:22		Add	""	Add router.access-list hulinatong
2018-03-20 16:45:56		Add	""	Add router.ospf:area 0.0.0.0
2018-03-20 18:51:47		Add	""	Add router.route-map huliantong
2018-03-20 18:51:21		Add	prefix[	Add router.access-list:rule hulinatong:4
2018-03-20 17:18:56		Add	prefix[	Add router.ospf:network 5
2018-03-20 18:50:54		Add	prefix[	Add router.access-list:rule hulinatong:2
2018-03-20 17:18:03		Add	prefix[	Add router.ospf:network 3
2018-03-20 18:50:30		Add	prefix	Add router.access-list:rule hulinatong:1
2018-03-20 17:17:37		Add	prefix	Add router.ospf:network 2
2018-03-20 18:51:08		Add	prefix	Add router.access-list:rule hulinatong:3
2018-03-20 17:18:30		Add	prefix[	Add router.ospf:network 4
2018-03-20 17:24:34		Add	gateway[priority[40]device[port30]	Add router.static 33
2018-03-20 16:39:20		Add	interface[port30]	Add system.zone huliantong
2018-03-20 18:37:48		Add	interface[port30]ip[ ]cost[80]dead-interval[40]hello-interval[10]	Add router.ospf:ospf-interface 1
2018-03-20 16:46:33		Add	interface[port30]ip[ ]dead-interval[40]hello-interval[10]	Add router.ospf:ospf-interface huliantong
2018-03-20 16:45:19		Add	ip[ ]	Add system.interface:secondaryip port30:4
2018-03-20 16:45:19		Add	ip[ ]	Add system.interface:secondaryip port30:2
2018-03-20 16:45:19		Add	ip	Add system.interface:secondaryip port30:1
2018-03-20 19:38:26		Add	ip[	Add system.interface:secondaryip port30:6
2018-03-20 16:45:19		Add	ip[ ]	Add system.interface:secondaryip port30:3

宝付案例-操作行为审计

日期时间	目标IP	操作命令	用户名	源IP
2018-03-24 02:51:14		copy running-config tftp:		
2018-03-24 02:51:09		write		
2018-03-24 02:50:33		copy running-config tftp:		
2018-03-24 02:50:29		write		
2018-03-23 13:04:39		show processes cpu platform sorted		
2018-03-23 13:04:22		show processes cpu platform sorted		
2018-03-23 13:04:09		show processes cpu platform sorted		
2018-03-23 12:08:18		ip access-list extended preauth_ipv4_acl		
2018-03-23 12:08:09		do-exec show ip acces		
2018-03-23 12:08:06		no ip access-list extended preauth_ipv4_acl		
2018-03-23 12:08:01		no ip access-list extended preauth_ipv4_ac~l		
2018-03-23 12:07:33		do-exec show ip acces		
2018-03-23 12:07:24		no ip access-list extended preauth_ipv4_acl		
2018-03-23 12:07:07		no ip access-list extended CISCO-CWA-URL-REDIRECT-ACL		
2018-03-23 12:06:55		do-exec show ip acces		
2018-03-23 12:06:44		show running-config		
2018-03-23 12:06:44		do-exec show running-config		
2018-03-23 12:06:34		show running-config		
2018-03-23 12:06:34		do-exec show running-config		
2018-03-23 12:06:26		do-exec show ip acces		

宝付案例-基线

检查项	说明	级别	修复建议	IIP
是否配置NTP服务器	日志应符合审计要求，存放在特定的日志服务器，且保存周期应大于等于半年	低	编辑/etc/ntp.conf 添加NTP服务器ip	192.168.101.81
是否配置日志服务器	日志应符合审计要求，存放在特定的日志服务器，且保存周期应大于等于半年	低	设置NTP服务器	192.168.101.81
UMASK值是否符合要求	当在创建新文件或目录时设置新建文件和目录的默认权限，控制用户缺省访问权限	中	在文件/etc/profile中设置umask 027	192.168.101.81
是否配置PAM su到root状态检查	避免任何人可以su为root，减少安全隐患	中	编辑/etc/pam.d/su,添加以下内容：auth sufficient /lib/security/pam_rootok.so auth required /lib/security/pam_wheel.so group=wheel	192.168.101.81
密码至少含一个特殊字母是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so ocredit=1	192.168.101.81
密码至少含三个小写字母是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so lcredit=3	192.168.101.81
密码至少含一个大写字母是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so ucredit=1	192.168.101.81
密码至少含三个数字是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so dcredit=3	192.168.101.81
密码最短长度是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so minlen=10	192.168.101.81
密码最少不同字符数是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so difok=3	192.168.101.81
密码尝试次数是否符合要求	口令应符合口令策略，要求包含数字、字符、大小写和特殊字符，且长度大于等于8位	中	设置/etc/pam.d/system-auth文件中password requisite pam_cracklib.so retry=5	192.168.101.81
未设置尝试和锁定策略	防止攻击者暴力破解系统账号	中	编辑/etc/pam.d/sshd 添加：auth required pam_tally2.so onerr=fail deny=6 unlock_time=1800 audit	192.168.101.81
是否配置口令过期前警告天数	口令过期前多少天，提醒用户更改口令，否则密码会失效	中	在文件/etc/login.defs中设置 PASS_WARN_AGE 不小于标准值	192.168.101.81
是否配置口令最小长度	口令长度应大于等于8位	中	在文件/etc/login.defs中设置 PASS_MIN_LEN 不小于标准值	192.168.101.81
是否配置口令生存周期	要求所有口令最长不超过3个月更改一次口令	中	在文件/etc/login.defs中设置 PASS_MAX_DAYS 不大于标准值	192.168.101.81

宝付案例-漏洞

时间	IP	CVE编号	漏洞名称	协议	端口	风险等级	解决建议
2018-03-28 14:22:43			nginx HTTP Server Detection	tcp	80	None	n/a
2018-03-28 14:22:43			Service Detection	tcp	80	None	n/a
2018-03-28 14:22:43			Traceroute Information	udp	0	None	n/a
2018-03-28 14:22:43			HTTP Server Type and Version	tcp	80	None	n/a
2018-03-28 14:22:43			nginx HTTP Server Detection	tcp	80	None	n/a
2018-03-28 13:29:57			nginx HTTP Server Detection	tcp	80	None	n/a
2018-03-28 13:29:57			Service Detection	tcp	80	None	n/a
2018-03-28 13:29:57			Traceroute Information	udp	0	None	n/a
2018-03-28 13:29:57			HTTP Server Type and Version	tcp	80	None	n/a
2018-03-28 13:29:57			nginx HTTP Server Detection	tcp	80	None	n/a
2018-03-28 13:29:57			Service Detection	tcp	80	None	n/a
2018-03-28 13:29:57		CVE-2007-3008	HTTP Reverse Proxy Detection	tcp	80	None	n/a
2018-03-28 13:29:57		CVE-2005-3498	HTTP Reverse Proxy Detection	tcp	80	None	n/a
2018-03-28 13:29:57		CVE-2005-3398	HTTP Reverse Proxy Detection	tcp	80	None	n/a
2018-03-28 13:29:57		CVE-2004-2320	HTTP Reverse Proxy Detection	tcp	80	None	n/a
2018-03-28 13:29:57			Traceroute Information	udp	0	None	n/a
2018-03-28 13:29:57			HTTP Server Type and Version	tcp	80	None	n/a

THANK YOU