HW行动必备防御手册

一. 整体思路分析

不知攻焉知防，如果了解白帽子的攻击手法和常规思路，针对性的做出防御措施，往往事半功倍，整个防御过程总结为技术层面的防御和管理层面应急响应处理，技术层面首先是确定对外提供服务的资产情况，然后在网络层面、主机层面和 web 应用层面进行整体技术加固。管理层面建立保障团队体系、应急解决方案、攻击流量监控等。只有各方面工作准备充分， 才能第一时间解决问题，话不多说进入正题。

二. 技术部分的防御手段

2.1 确定风险窗口

风险窗口是哪些提供对外服务的服务器，要知道自己的风险窗口有多大，就必须掌握整个系统对外的资产情况，因此需要梳理资产情况，清楚自己系统的风险窗口在哪里，那么梳理哪些资产呢？怎么去梳理呢？

2.1.1 梳理哪些资产？

系统资产往往涉及多个部门，一个完整的、准确的资产应该来自运维部门/系统管理员 、 开放测试人员和运维部门/网络管理员。具体如下：

- **服务器基础信息资产**

服务器基础信息表运维系统管理员提供，发现问题可以第一时间找出主机相关信息，并进行处理。

服务器名称	服务器IP地址	开放端口	操作系统	服务器类型
Secweb	10.1.1.200	TCP:80,22	Centos Sever 6.5	Web应用
Secdb	10.1.2.100	禁止全部	Centos Sever 6.5	数据库
SecFTP				
运维/系统工程师运维（提供）				

■ **应用系统信息资产**

此表由开发人员提供更加准确，包括了数据库、Web 中间件、域名、后台地址、使用框架和是否使用 CMS，敏感目录有公司安全部门同信息收集工具收集所得。

数据库	中间类型和版本	子域名	后台管理URL	框架	CMS	敏感目录
NA	Apache 2.4.39	zone.secevery.com	zone.secevery.com/admin	NA	WeCenter	
mysql	NA	NA	NA	NA	NA	
软件开发或者测试人员（提供）						自查

■ **网络策略管理**

运维部门的网络工程师需要对防火墙对主机策略进行统计，目前核心是网络设备为防火墙和 WAF 设备和开启策略进行统计。

A. 对外主机的端口策略

B. WAF 是否对业务网址进行保护

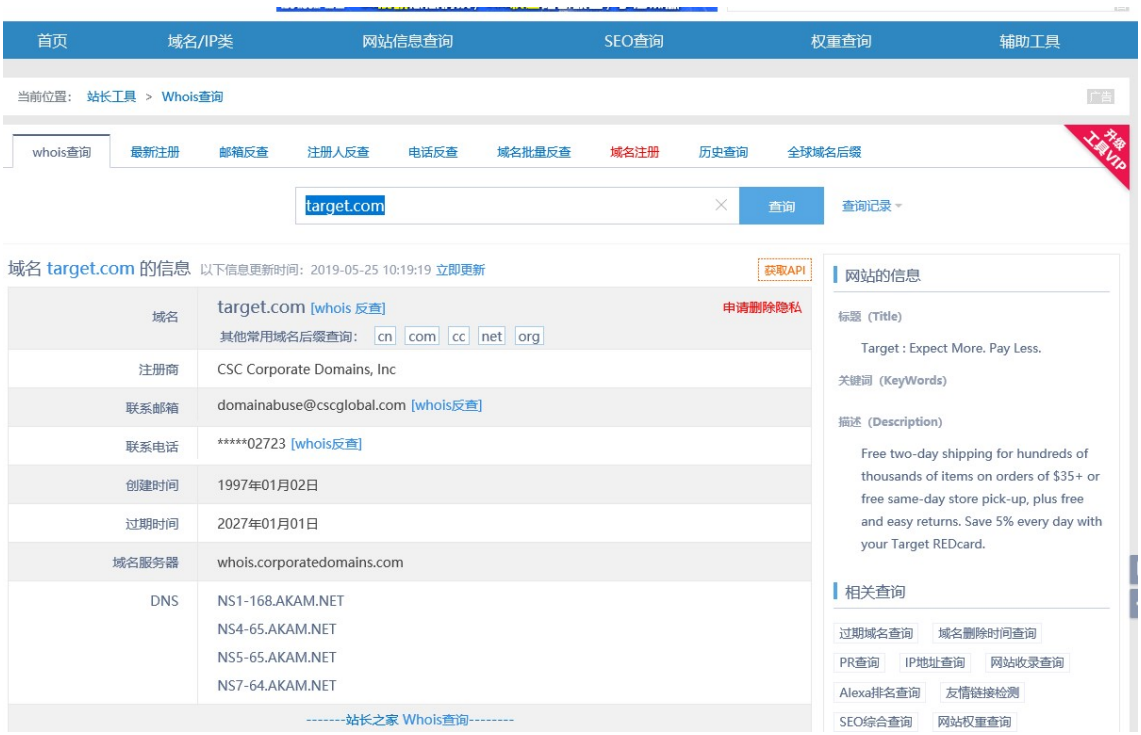
2.1.2 收集资产的方法

很大部分资产公司部门提供，但是也要通过黑盒方式，去获得一些资产，避免公司统计资产疏漏，资产收集可用如下方法：

- whois 信息: 站长之家、爱站、https://whois.aliyun.com/
- 子域名: 子域名挖掘机 Layer、subDomainsBrute、phpinfo.me
- 目标 IP : http://ping.chinaz.com/、nslookup
- 旁站C 段查询: http://www.webscan.cc/、Nmap、Zenmap
- 邮箱搜集: theharester
- CMS 类型: 云悉、BugScaner
- 敏感目录: 御剑、dirbuster、wwwscan、IIS_shortname_Scanner
- 端口信息: Nmap、masscan
- 服务器和中间件信息: Nmap、Zmap、whatweb

2.1.3 收集资产的工具和简单介绍

- 站长之家:在线 whois 查询网站



爱站: 在线 whois 查询网站

whois概况

域名	baidu.com
注册商	MarkMonitor Inc.
参照页	-
域名持有人/机构名称	Beijing Baidu Netcom Science Technology Co., Ltd. 反查注册人
域名持有人/机构邮箱	-
创建时间	1999-10-11
更新时间	2019-05-09
过期时间	2026-10-11
域名服务器	whois.verisign-grs.com
域名服务器	whois.markmonitor.com
DNS服务器	ns1.baidu.com - 202.108.22.220
DNS服务器	ns2.baidu.com - 220.181.33.31
DNS服务器	ns3.baidu.com - 112.80.248.64
DNS服务器	ns4.baidu.com - 14.215.178.80
DNS服务器	ns7.baidu.com - 180.76.76.92
域名状态	运营商设置了禁止删除保护 https://icann.org/epp
域名状态	运营商设置了禁止转移保护 https://icann.org/epp
域名状态	运营商设置了禁止更新保护 https://icann.org/epp

https://whois.aliyun.com/:在线 whois 查询网站