OWASP

Open Web Application Security Project

安全服务与应急响应

启明星辰山西分公司-李忠仁

传统的攻击手段

- 1 DDOS攻击。
- 2 传统web攻击(sql注入,xss,上传漏洞等)。
- 3 传统黑帽seo手段(cloaking等)。
- 4 其他,如缓冲区溢出漏洞等。

传统攻击手段的特点

- 1 易检测
- 2 易排查
- 3 易封堵

针对传统攻击的防御手段

- 1 对处于公网的网站或者应用进行渗透测试，提前修复一些常规漏洞。
- 2 使用传统的安全设备，对一些攻击手段进行屏蔽，如sql注入，xss等。
- 3 使用日志审计，对每天日志中的攻击手段进行查看。

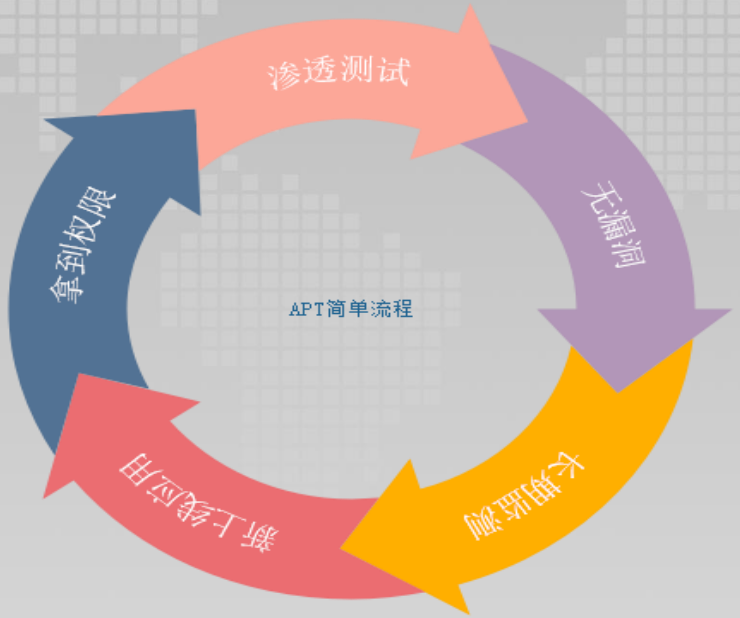
针对传统攻击的防御手段

- 4 关闭不必要的端口和高危端口，限制攻击者的攻击角度。
- 5 主机安装杀毒软件并实时更新。
- 6 定时检测网站源代码的完整性与安全性。
- 7 新应用上线前检测。

新的攻击手段

- 1 最近比较流行的恶意网站镜像
- 2 长期的可持续化攻击(APT)
- 3 随时可能会爆发的nday
- 4 攻击面的扩大(不再局限于传统的web)
- 5 更加针对性的攻击

新的攻击手段



1.首先对目标进行渗透测试

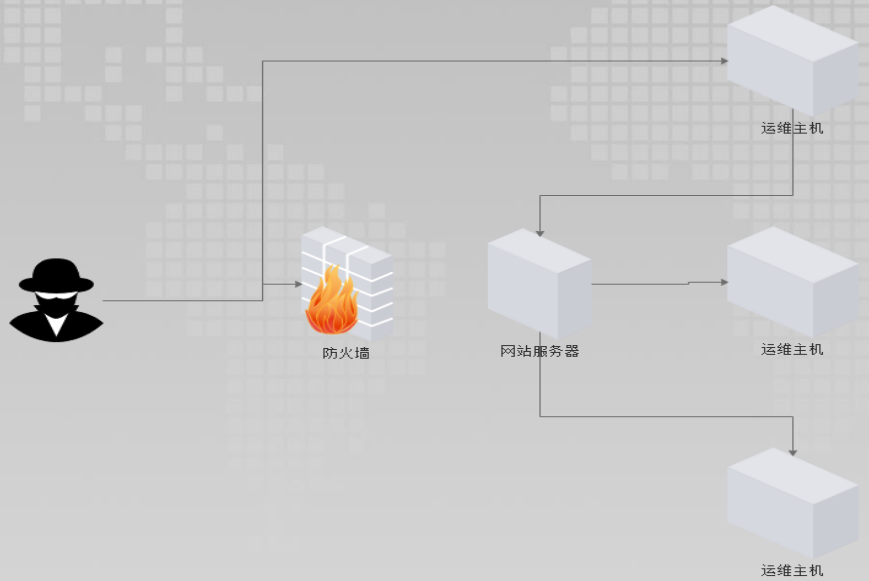
2.没有发现漏洞的情况下，使用网络环境监测脚本去长时间监测是否有新上线应用。

3.如果有就在加固新应用之前拿到权限。

新的攻击手段

2016-05-05	宜搜某站存在struts2命令执行	命令执行	路人甲
2016-03-14	中国电信某189.cn站点天翼对讲系统存在struts2任意命令执行漏洞	命令执行	nansss
2016-02-26	方正宽带多台服务器Struts2命令执行(可Getshell)	命令执行	几何黑店
2015-12-14	长沙广电某APP系统SQL注入/struts2远程执行/导致webshell	系统/服务运维配置不当	superbing
2015-12-09	看我如何绕过深信服NGAF的struts2防护规则（含过程）	设计不当	路人甲
2015-11-23	中信银行某系统struts2命令执行修复不当（root权限）	命令执行	撸撸侠
2015-11-19	兴业银行某站点Struts2修复不当造成命令执行	命令执行	路人甲
2015-11-02	搜狗某内网存在Struts2命令执行（discuz!应用实例）	系统/服务补丁不及时	Jannock
2015-10-15	深圳航空某站点Struts2命令执行漏洞	命令执行	路人甲
2015-10-10	中信银行某两站漏洞打包（弱口令/struts2/sql注入）	命令执行	路人甲
2015-09-23	某云盘Struts2远程命令执行S2-016打包	命令执行	路人甲
2015-09-14	神器而已证券系列之兴业证券某站struts2命令执行导致Getshell	命令执行	举起手来
2015-09-13	阳光保险主站Struts2命令执行漏洞	命令执行	路人甲

在漏洞爆发时，短时间内会制作出自动利用工具，并批量进行漏洞扫描和利用。



被防火墙阻断后，更换攻击目标。

新攻击手段防御难点

- 攻击者的攻击面不在只局限于web，通过多角度的攻击方式，让传统的安全设备如 waf ids ips等检测不到，阻断不了。
- 免杀技术的普及，通过加壳，混淆等手段，对木马进行免杀，同时绑定系统自带文件中或者利用powershell等系统功能留下后门造成传统杀毒软件无法及时查杀。

新攻击手段防御难点

- 利用wordhound等字典生成工具，针对目标生成弱口令字典，不在使用传统的弱口令字典导致爆破成功几率增大。
- 使用网站和端口监控手段，实时监控新上线的应用，导致在还未建立起防护机制时就被入侵。

新攻击手段防御难点

- 病毒的传播力度加大，出现了新型无法破解的勒索病毒，同时感染方式增强，不再局限于利用传统的漏洞，爆破等。
- 实时跟踪目标员工信息，收集信息。

针对新型攻击手段的防御策略

- 网站安全监控
- 渗透测试服务
- 网络安全评估
- 安全巡检服务

针对新型攻击手段的防御策略

- 安全加固服务
- 应急响应服务
- 新系统入网安全评估
- 重要时期安全保障

网站安全监测服务

- 网站漏洞扫描
- 网站挂马检测
- 可用性监测
- 网页篡改监测
- 敏感内容监测
- 域名解析监测
- 钓鱼网站监测
- 安全通告服务

网站安全监控

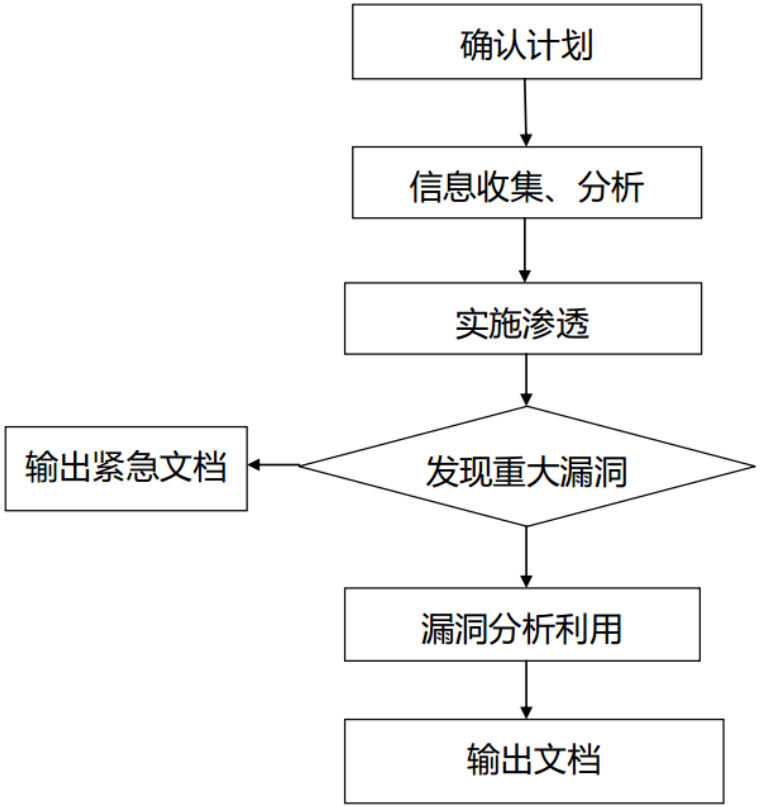
- 监控网站页面内容完整、不被篡改；
- 监控网站存在的SQL注入、XSS、非法访问、信息泄露等应用层漏洞，从而提前解决潜在风险；
- 监控网站，防止网站挂马。

网站安全监控

- 监控网站是否存在敏感信息，对于网站的敏感信息内容自行配制告警功能，方便管理者及时了解到发生的安全事件，可根据量化的标准，对网站的安全事件严重程度进行不同形式的告警。
- 监控网站是否被钓鱼，是否被镜像。

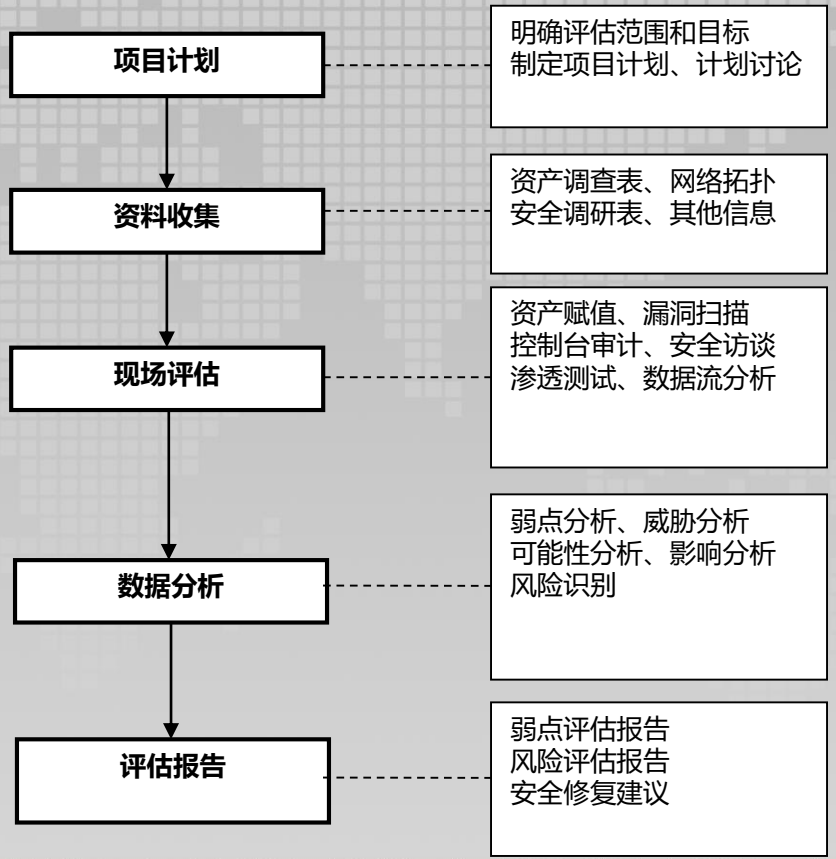
渗透测试

- 采用传统的渗透方式，包括:信息收集 → 寻找漏洞 → 利用漏洞 → 测评报告。
- 在授权的范围内，对网站和网络系统做完整的渗透测试。

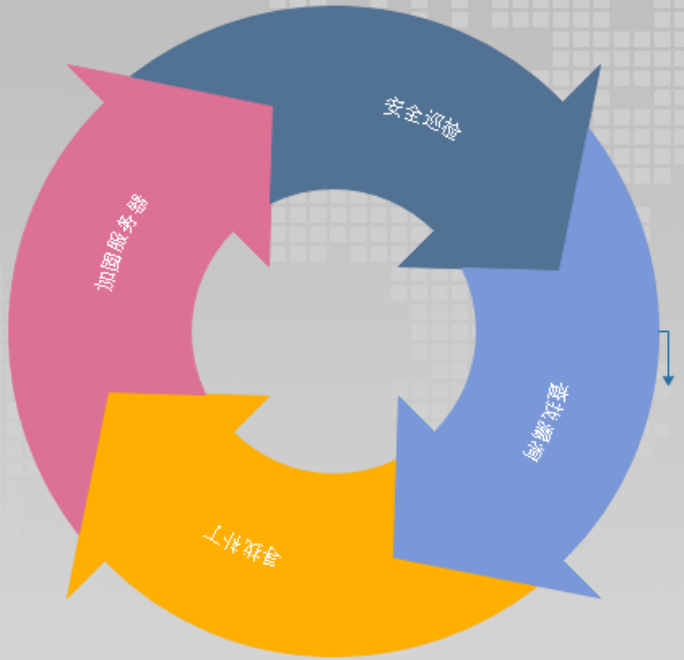


渗透测试工作流程。

网络安全评估



安全巡检服务



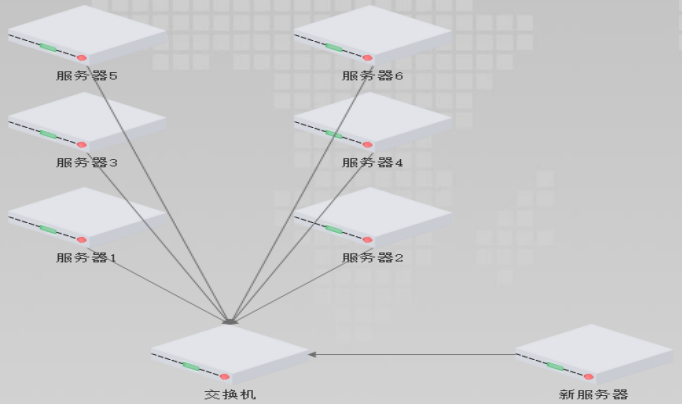
安全加固服务

- 为了有效保障网络的安全运行，在对操作系统、数据库、中间件、网络设备、安全设备进行安全检测后，，需要对发现的安全风险进行修复。
- 安全加固服务，是指根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。加固内容包括但不限于系统补丁、防火墙、防病毒、危险服务、共享、自动播放、密码安全。
- 安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、数据库、中间件、网络设备、安全设备，都需要进行安全加固。

应急响应服务

- 应急响应服务是为满足企业发生安全事件，需要紧急解决问题的情况而提供的一项安全服务。当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，启明星辰安全专家会在第一时间对安全事件进行应急响应处理，使企业的网络应用系统在最短时间内恢复正常运行，帮助企业查找入侵来源，为企业挽回或减少经济损失。
- 对安全事件进行应急响应处理后，我们将提供详细的应急响应报告，报告中将还原入侵过程，同时给出对应的解决方案。

新系统入网



谢谢！

OWASP
Open Web Application Security Project