

HW防守

准备阶段

- 编制HW工作方案 根据用户现场实际情况编制工作方案，包括组织架构、工作分工与职责、工作计划、工作任务等
- 召开启动会 安全处与网络处、应用处、业务司局、第三方厂商达成一致共识
- 确定目标系统
 - 定目标系统建议：区域单一、业务连续性较低、单独物理机、上报数量
 - 目标关键链路、是否定级、安全检查、渗透测试，同区域、同网段业务系统等
- 全网资产梳理 目标系统资产，分析得知可能的攻击路径
- 安全设备了解 网络设备、主机系统（操作系统、数据库、中间件等梳理）、应用系统（访问地址、IP地址、开发语言）、集权类系统（OA、邮件、堡垒机）
- 安全厂商沟通 目前所有安全设备：防火墙、WAF、IPS、IDS等
- 安全厂商沟通 安全设备是否有厂家维护，HW期间是否现场支持
- 部署天眼 了解安全策略、访问控制如何做的，网络之间隔离措施
- 部署WAF 了解网络拓扑大体结构，知道目标系统拓扑位置
- 部署蜜罐 部署完成，确认旁路活串联，是否开启防护策略，全部或局部防护
- 部署主机加固 发布镜像系统，迷惑攻击方，发现攻击IP
- 部署主机加固 针对目标系统进行主机加固，提高防护和监测能力
- 内部集权系统梳理 邮件、域控、运维管理（ITSM、堡垒机）、运维终端（安全、网络、研发）
- 内部集权系统梳理 搜集内部IP地址，进行天眼分析查看与集权系统通信的IP地址是否正常
- 防守队伍沟通 建立即时通讯工作群，确定好监测、研判、封禁、配合整改、应急处置分组和具体责任人，包括用户谁负责牵头。客户、安全厂商、应用厂商、CND等

自查和整改阶段

- 应用系统梳理 根据前期准备工作形成资产清单，网络、安全设备、应用系统（系统名称、URL、内部地址（负载IP）、联系人等）
- 开展安全检查
 - 互联网资产扫描 发现未知资产和风险端口
 - 互联网暴露信息 搜索引擎、代码托管、网盘、漏洞平台
 - 安全基线检查 网络、安全、主机、应用等安全基线检查
 - 安全扫描 主机、应用安全漏洞扫描+验证
 - 渗透测试 漏洞验证、督促整改
 - 其他安全检查 运维终端安全检查、日志审计、备份有效性
 - 安全意识培训 关键岗位运维人员、管理人员安全意识
 - 安全加固 针对发现的安全漏洞、安全隐患及时跟进、验证修复情况
- 完善安全设备
 - 安全风险检查 弱口令、管理后台外部访问权限、内部访问IP范围、补丁更新、上传目录权限等
 - 设备完善 部署与测试WAF、IPS、IDS、蜜罐、主机加固等
 - 天眼检查 流量采集、规则更新、使用情况等
- 其他安全措施
 - 在攻防演习前，梳理业务连续性较低的、存在安全问题的系统下线或HW期间临时关停
 - HW期间是否可以每天定期修改关键应用、主机口令
 - 攻防演习前，对防守目标系统进行一次日志分析和失陷检测

攻防预演习阶段

- 通过预演习工作，发现安全漏洞隐患，验证防守方案可行性，进一步完善
- 预演习工作确认与用户确认攻击方式、时间、提交物，申请授权，确认攻击队资源与开始时间、攻击IP，提供应用系统列表
- 预演习工作开展：按照方案开展攻击和防守工作，模拟正式HW工作，安全监测、分析、处置
- 攻防预演习总结：与各方沟通总结不足，进行完善

正式演习阶段

- 分组工作职责
 - 领导小组：总体监督、协调、把控
 - 事件检测组 安全厂家监控各自安全设备，发现疑似攻击行为立即验证或上报
 - 威胁分析组 确认漏洞存在，通知相应资源处置
 - 事件处置组 安全工程师上机溯源分析、应用运维人员删除Webshell或下线系统，开发人员进行代码整改
 - 其他分组：邮件安全组、应急处突组、后勤保障组、外部资源协调组
 - 攻防演练平台上报 专人或兼职负责防守成果报告上报演练平台
- 安全设备监测 进行安全监测，发现后通知研判组进行验证
- 天眼监测 进行安全监测，发现后通知研判组进行验证
- 封禁IP 出口防火墙、CDN
- 失陷检测 每天针对目标系统进行Web日志检测，是否存在Webshell
- 日志、存储目录检查 应用系统进行日志查看、文件存储目录检查

注意事项

- 保密、个人安全、值守要求、关键行为、风险上报、工作要求、时间要求、漏洞上报