资产梳理实战指导

2019护网培训

NSFOCUS

CONTENTS 目 录

NSFOCUS

01

为什么要做资产梳理

1. 资产梳理的目的和重要性

1.1

资产梳理的目的和重要性

a. 资产表的重要性及作用

b. 资产梳理做什么

资产表的重要性及作用

资产梳理的目的

- 主机漏洞、弱口令、Web应用漏洞、基线配置的目标
- 排查“三无七边”资产
- 排查开放端口服务，作为关闭非必要端口及加强端口访问策略的依据
- 梳理重点资产，作为有限防护资源分配重点参考

✓ 确保检查无遗漏，处理无主资产，标记重点防护资产，为后续防护决策等提供部分基础信息。

资产梳理做什么

资产分类

- 内网、互联网资产、接口清单、服务器、网络设备、安全设备等

梳理内容

- 收集明确归属的系统资产信息：IP、系统归属、责任人归属
- 发现未明确（未知）资产，并明确其归属
- 梳理资产对应的开放端口/服务，并明确其用途
- 梳理与攻击目标相连接口/资产
- 梳理存在用户数据的资产
- 梳理防护资源等

CONTENTS 目 录

02

怎么做 资产梳理

1. 资产表的基本信息
2. 基本收集方法
3. 资产梳理流程
4. 资产梳理示例
5. 工作难点及解决建议

2.1

资产表的基本信息

a. 资产表类型及关键信息组成

资产表的基本信息 – 关键信息组成

类型

- 内网、互联网资产、接口清单、服务器、网络设备、安全设备，根据需要可选择不同角度资产表

常规信息

- 归属域、归属系统、IP（主备及浮动地址标记）、类型（服务器、路由交换设备、安全设备等）、功能（应用服务器、数据库服务器、华为路由器、防火墙、IDS等）、操作系统（如AIX 5.3.07）、安装应用软件及版本、 Web URL、可访问位置（内网、互联网）

扩展信息

- 开放端口/服务、可访问位置及授权（是否访问限制、是否VPN、是否堡垒机、是否双因素认证）、是否存放用户数据、是否与集团/地市分公司互联、覆盖的防护手段（ACL、IPS、WAF、ADS等）

2.2

资产梳理流程

资产梳理流程

- 向管理员收集原始资产表
- 安全管理平台录入的资产信息作为补充

- 网段资产存活探测
- 资产开放端口服务探测
- 监控设备/平台目标补充
- 站点探测补充

- 确认发现的未知资产归属
- 调研完善其他信息（可访问位置及授权、防护手段、接口及互联情况等）

2.2

基本收集方法

a. 基础资产表收集

b. 扫描手段补充信息

c. 监控手段补充信息

d. 其他信息补充

基本收集方法 – 基础资产表收集

向管理员收集

- 原始资产表，主要包括已知系统、资产的常规信息
- 通过基本调研补充扩展信息

安全管理平台资产信息导出

- 通过导出如SOC平台等安全管理平台中的资产信息，收集初步资产表

基本收集方法 – 扫描手段补充信息

扫描目的

- 梳理未知资产
- 梳理开放的端口/服务

扫描方法

- 收集和梳理资产网段：互联网网段、内网资产所属网段
- 按照网段进行存活扫描
- 按照网段进行全端口服务探测

基本收集方法 – 扫描手段补充信息

结果处理

- 存活列表与资产列表进行对比，筛选无归属资产，与管理员确认资产用途
- 将开放端口/服务信息与资产匹配，重点筛选标记http、https、FTP、SMTP、POP3、RADIUS、RDP、NTP、数据库端口，与管理员确认端口用途
- 开放Web相关端口的资产，向管理员进行站点确认，补充Web资产信息

特点

- 需要较多扫描资源、扫描时间长
- 相对完整

基本收集方法 – 监控手段补充信息

目的

- 发现和补充部分在用、无登记的资产

获取方法

- 在边界防护设备中获取被访问的目标IP、Web链接

结果处理

- 将其与现有资产表对比，筛选未登记资产
- 与管理员进行资产确认
- 完善资产信息

特点

- 作为补充手段，仅能发现在用但未登记资产信息

基本收集方法 – 其他信息补充

目的

- 完善资产信息，为后续防护策略提供参考
- 如：与其他系统的接口情况、数据接口、与集团/地市分公司连通情况

获取方法

- 网络拓扑分析
- 网络策略梳理
- 管理员访谈

结果处理

- 记录数据相关接口
- 记录与集团/地市分公司连通的资产IP和端口
- 上述接口资产进行重点标记

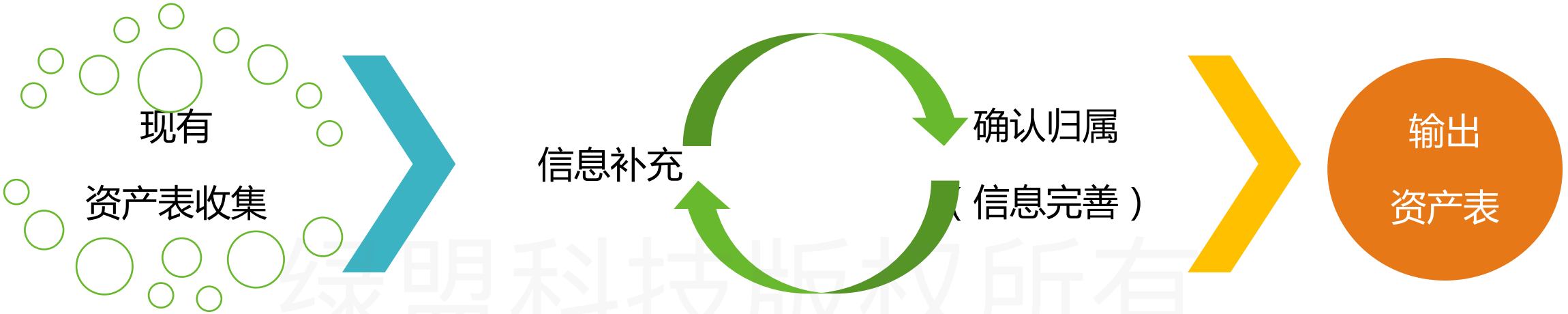
特点

- 需要大量人工参与
- 结果能突出防护重点

2.3

资产梳理示例

资产梳理示例



- 向管理员收集原始资产表
- 安全管理平台录入的资产信息作为补充

- 网段资产存活探测
- 资产开放端口服务探测
- 监控设备/平台目标补充
- 站点探测补充

- 确认发现的未知资产归属
- 调研完善其他信息（可访问位置及授权、防护手段、接口及互联情况等）

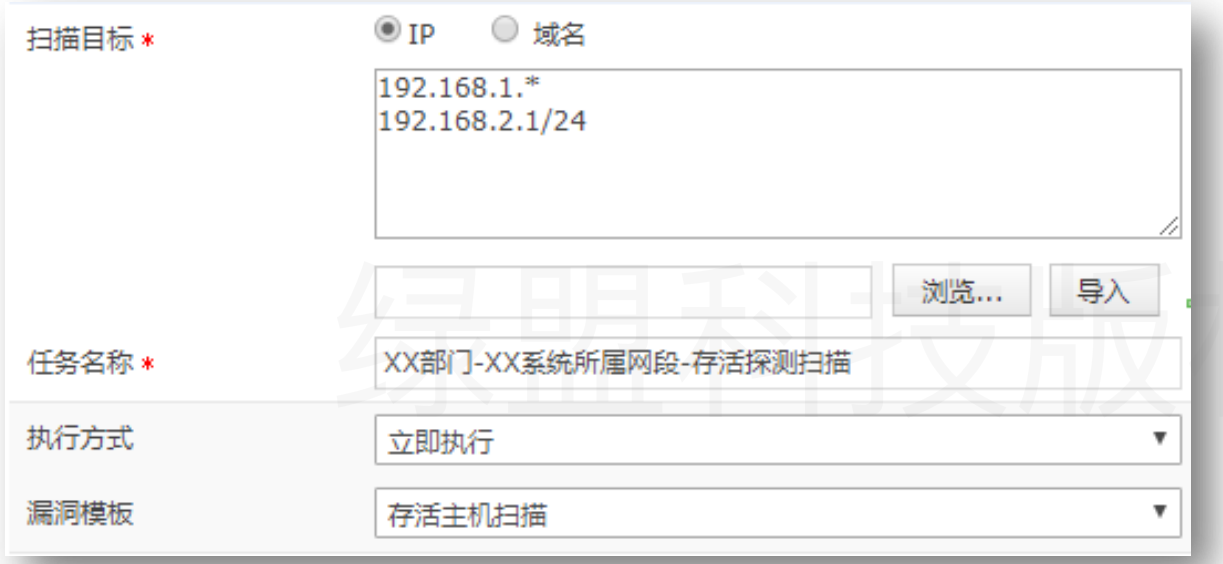
资产梳理示例 – 现有资产表收集

系统名称	设备名称	IP地址	设备类型	设备功能	操作系统	数据库	应用系统
短信中心	GX-XXXX-XXXX	192.168.1.1	核心服务器	业务处理机1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.2	核心服务器	业务处理机2	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.3	核心服务器	业务处理机3	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.4	核心服务器	计费服务器1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.5	核心服务器	计费服务器1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.6	核心服务器	qas服务器1	suse linux 11 sp3	sybase ase 1507	
短信中心	GX-XXXX-XXXX	192.168.1.7	核心服务器	qas服务器2	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.8	核心服务器	imsagent服务器1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.9	核心服务器	imsagent服务器2	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.10	核心服务器	SIPPROXY服务器1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.11	核心服务器	SIPPROXY服务器2	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.12	核心服务器	DCACHE服务器1	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.13	核心服务器	DCACHE服务器2	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.14	核心服务器	DCACHE服务器3	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.15	核心服务器	omm服务器	suse linux 11 sp3	sybase ase 1507	
短信中心	GX-XXXX-XXXX	192.168.1.16	核心服务器	网管服务器	suse linux 11 sp3	oracle 11g	
短信中心	GX-XXXX-XXXX	192.168.1.17	核心服务器	亿讯代理服务器	suse linux 11 sp3		
短信中心	GX-XXXX-XXXX	192.168.1.18	核心服务器	维护机器	windows2008		

- 向管理员收集原始资产表
- 安全管理平台录入的资产信息作为补充
- **主要收集基础信息：**归属域、归属系统、IP、类型、功能、操作系统、应用软件、Web URL
- **输出物：**原始资产表

NSFOCUS

资产梳理示例 – 信息补充–网段存活资产探测



- 统计某系统资产归属192.168.1/2.*两个网段
- 将两个网段拆分为4个子任务
- 任务参数选择“存活主机扫描”
- **主要收集信息**：同网段其他存活资产、系统边界隔离情况
- **输出物**：①同网段未确认归属资产表

资产梳理示例 – 信息补充–开放端口服务探测

- 针对需探测资产（系统/按网段）
- 指定特定的一组端口，以“,”分隔统
- 或指定对全量的端口进行探测，1-65535
- **主要收集信息**：资产的开放端口及服务对应情况
- **输出物**：②资产对应的开放端口服务清单

资产梳理示例 – 信息补充–Web应用筛选

IP地址	端口	协议	服务	状态
192.168.1.2	5989	tcp	wbem-https	open
192.168.1.3	5800	tcp	vnc-http	open
192.168.1.4	8765	tcp	ultraseek-http	open
192.168.1.5	8088	tcp	radan-http	open
192.168.1.6	593	tcp	http-rpc-epmap	open
192.168.1.7	5988	tcp	wbem-http	open
192.168.1.8	5803	t		
192.168.1.9	808	t		
192.168.1.10	623	t		
192.168.1.11	6788	t		
192.168.1.12	5802	t		
192.168.1.13	7627	t		
192.168.1.14	8000	t		
192.168.1.15	16993	t		
192.168.1.16	16992	t		
192.168.1.17	80	t		
192.168.1.18	280	t		
192.168.1.19	8008	t		
192.168.1.20	1184	t		
192.168.1.21	443	t		
192.168.1.22	20002	t		

	URL	
新增	http://	[form1]
新增	http://	[form1]
前期已发现	http://	[管理系统 管理]
前期已发现	https://	[短信 管理]
新增	http://	[form1]
新增	http://	[form1]
新增	http://	[form1]
前期已发现	http://	[电信 短信 管理系统 管理
新增	http://	[form1]
新增	https://	[管理]
前期已发现	http://	[管理系统 管理]
前期已发现	https://	[管理]
前期已发现	https://	[form1 管理]
新增	http://	[form1]
新增	http://	[管理系统 管理]
前期已发现	http://1	[管理]
前期已发现	https://	[管理]
新增	http://	[form1]
新增	http://	[管理系统 管理]
新增	http://	[form1 管理]
前期已发现	https://	[管理]
新增	https://	[管理]
新增	https://	[管理平台 管理]
前期已发现	http://	[管理]
前期已发现	https://	[管理]
前期已发现	http://	[form1 管理系统 管理]
新增	http://	[集成 管理]

- 根据资产对应的端口服务开放清单进行端口筛选
- 其中筛选疑似Web应用端口进行站点排查
- 通过脚本探测页面存活及关键字情况，定位是否客户相关Web资产
- **主要筛选信息**：Web应用相关端口
- **输出物**：③Web端口清单、④可访问URL清单

资产梳理示例 – 确认归属（信息完善）

①同网段未确认归属的资产表

- 与管理员确认资产归属，扩充到原始资产表里
- 无归属资产评估进行处理：关停、下线等

②资产对应的开放端口服务清单

- 标记业务及运维必须开放的端口服务
- 其余端口评估进行关闭、严格限制

③Web端口清单

④可访问URL清单

- 确认Web应用站点归属及是否在用
- 关停已不使用的站点及Web端口

确认以上信息，完善资产表，输出完整资产表。

3.1

工作难点及解决建议

a. 资产不全

b. 资源不足

c. 沟通的重要性

工作难点及解决建议

- 资产及关键信息不全
  - 未知资产
  - 资产详情
- 资源不足
  - 扫描资源
  - 防护资源
- 归属不明
  - 归属部门、系统、责任人

沟通

- 扫描探测
- 监控输出
- 人工调研
- 划分重点任务优先处理
- 任务拆分提高效率
- 重要资产防护资源倾斜
- 与管理员、安全负责人等积极沟通
- 强制隔离后等待反馈

FAQ

谢谢！

NSFOCUS