漏洞扫描实施标准

2019护网专项培训

NSFOCUS

CONTENTS 目 录

02

怎么做 安全漏洞扫描

1. 扫描前计划准备
2. 按计划实施扫描
3. 扫描后收尾确认

工作流程

计划准备 → 扫描实施 → 收尾确认 → 报告分析

- 技术交流
- 确认扫描范围
- 准备扫描环境
- 确定扫描方案
- 申请实施授权

- 环境与网络配置
- 扫描策略确认与任务下发
- 扫描其间业务观察

- 异常任务处理
- 导出扫描报告
- 交付与汇报成果

2.1

扫描前计划准备

a. 沟通与技术交流
b. 确认范围、目标
c. 工具、环境准备
d. 扫描方案、授权

扫描前准备 – 沟通与技术交流

01

技术、原理沟通

- 沟通扫描原理
- 确定扫描方式
- **确定任务类型（按系统扫描漏洞、按网段探测存活、对全端口扫描开放的端口服务）**

02

客观风险的提示与告知

- 如占用部分带宽
- 触发告警
- 存在一定业务风险
- 可能造成宕机等
- **大批量网段扫描可能造成长时间占用扫描器以及网络有受影响的可能**
- **网段扫描可能涉及未知资产，存在一定风险**

03

沟通漏洞扫描的必要条件

- 如网络环境
- 接入点
- 配合人员等

04

沟通交付的成果

- 如扫描报告的要求等

扫描前准备 – 确认目标与范围

明确扫描范围，收集目标系统资产信息

已知系统漏洞扫描：IP地址、承载的应用、网络拓扑（电子版）

按网段存活扫描：涉及的网段

端口服务探测扫描：涉及的资产、需检查的端口清单

收集安全防护产品配备情况

当前已使用的防火墙、安全产品及使用情况，策略情况等，以方便确认开展漏洞扫描过程中是否有被误阻断情况。

收集以往漏洞扫描信息

是否进行过漏洞扫描、是否因扫描而造成设备异常。

其他信息

业务系统的重要程度、业务繁忙时期等（重要资产夜间扫描）、**网段扫描是否允许长时间挂扫。**

NSFOCUS

扫描前准备 – 工具、环境准备

扫描设备准备

- 确定漏洞扫描工具
- 漏洞库升级到最新、证书有效、设备/工具正常使用

目标网络接入环境准备

- 确定网络接入的方式和位置，以及电源的接入情况
- 提供漏洞扫描目标网段的空闲IP地址、网络掩码、网关等配置信息；
- 收集接入网络安全防护产品部署情况、安全策略配置情况；

扫描时间、地点和人员

- 扫描时间（是否指定时间、是否可长时间挂扫）。
- 进入机房流程等
- 机房配合人员、业务系统配合人员等

扫描前准备 – 确认扫描方案、申请授权

- **确定扫描方案，护网期间建议与护网方案结合，提前完成沟通准备**
- **在漏洞扫描实施，特别是按照网段扫描之前，制定单项扫描计划，通过邮件与安全接口人及系统负责人确认扫描时间，并获取相关的授权或审批**
  - 避免口头、电话沟通；

常见问题及风险规避

资产收集

- 基础资产表：资产属性一般包括：所属于系统、IP地址、承载业务、映射前地址、映射后地址、浮动IP、所属部门、责任人、联系方式等，如果该资产为WEB应用地址，需提供开发语言，URL、数据库地址、中间件地址等；
- 信息资产，禁止未授权分发，外泄。
- **PS.资产收集可参考《资产梳理》培训内容加强了解。**

扫描申请与授权

- 禁止对他人的资产或非授权站点进行扫描操作
- **禁止在非计划时间内，不告知客户进行任何扫描操作**

2.2

按计划实施扫描

a. 扫描环境与网络配置
b. 策略确认与任务下发
c. 常见扫描工具的实操

扫描实施 – 现场环境、网络配置

现场环境

- 扫描其间，维护人员全程配合观察业务系统运行状态；
- 涉及机房操作的，针对网线插拔、开关机柜等操作，由配合人员完成；
- 遵守客户场地要求：如机房严谨吸烟、吃东西、需要穿戴鞋套等要求；
- **佩戴通行证，不要出入非授权场所。**

网络配置

- 扫描器接入前需确认扫描口IP地址配置，避免发生IP地址冲突问题；
- 如网络不通，需要进行扫描设备故障排查、和网络环境故障排查（配合人员负责网络故障的排查）。

扫描实施 – 扫描策略确认

事先确认服务器性能，业务重要性、扫描类型等，根据不同情况调整扫描策略：

- 现网业务生产环境，未获取用户文件或邮件授权，禁止弱口令扫描;
- 如果没有指定要求，尽量避免登录扫描，避免开启Oracle深度扫描（RSAS），需与客户沟通是否开启;

  （开启Oracle深度扫描结果更为准确，但影响扫描效率，且有一定风险）
- 对于未进行过漏洞扫描的设备或重要系统，可采取以下方式降低扫描风险：

  1）单个IP逐个扫描；

  2）主备机分开扫描；

  3）同一设备不同IP地址（如浮动地址）分开扫描；
- 根据前期收集到信息，排除因扫描出现异常的设备，以及扫描存在较高风险的设备（如老旧设备、负荷较高设备，以及其他特殊情况）

扫描实施 – 扫描策略确认【演示】

01

漏洞扫描

- 按照前述注意事项及历史扫描策略进行

02

网段存活扫描

- 拆分为几个适当的子任务
- 选择“存活主机扫描”

03

全/特定服务端口开放探测

- 端口扫描策略 – 指定端口范围：1-65535
- 端口扫描策略 – 指定端口范围：配置为特定的端口，以“,”分隔

04

指定漏洞扫描

- 新建漏洞模板（如一系列重点关注漏洞：struts2、反序列化、远程命令执行等）
- 选择新建的漏洞模板后，正常调整其他策略

NSFOCUS

扫描实施 – 扫描任务下发

扫描任务下发

- 任务开始前，可通过扫1-2个地址，进行网络承载、路由通路等测试；
- 每个扫描任务IP地址不易太多，IP及网段较多的，建议分批扫描（防止设备卡死、扫描中断等意外情况）；
- 扫描的资产应以业务系统为单位，当无法确认业务系统时，应以部门单位进行扫描，方便历史数据统计分析；
- **若涉及某部门按网段进行扫描，应将网段拆分为多个子任务进行；**
- 扫描任务命名时明确部门、系统等关键信息，例如【部门名称+系统名称+任务类型+其他】，能够有效的区分不同的扫描任务 。
- 扫描其间，配合人员需要全程关注业务运行情况，观察是否出现异常；
- 在扫描其间一旦出现系统瘫痪、宕机等情况，根据提前准备的应急预案，立即配合进行处置和恢复。并根据现场情况决定业务恢复后是否还继续进行扫描任务。

常见扫描工具操作演示【演示】

操作演示

- RSAS
- WVSS

2.3

扫描后收尾确认

a. 异常任务排查
b. 导出扫描报表
c. 报告整理汇报

扫描实施 – 异常任务排查

异常现象

- 扫描任务失败
- 扫描结果无任何漏洞
- 扫描资产减少
- 扫描进度0%

发生原因

- 网络不可达或网络波动
- 有安全防护设备或配置安全策略
- 扫描工具故障

处置措施

- 排查扫描工具故障
- 排查网路环境故障
- 确认目标资产防护情况
- 重新配置扫描任务

漏洞扫描收尾

扫描收尾工作

- 配合人员对系统运行状态、业务运行状态进行确认，如有异常按照应急措施进行处置；
- 扫描人员并关闭扫描器，断开网线，恢复扫描前状态；
- 经确认无误后扫描人员离场。

汇报与交付

漏洞扫描结果汇报与交付

整理漏洞扫描输出成果并交付。主要会涉及以下几方面的内容：

- 扫描数据整理：根据需求整理扫描数据；
- 报告输出与提交：根据漏洞分析结果撰写漏洞扫描报告；
- 结果沟通：漏洞扫描工作汇报；
- 扫描结果交付与工作确认。

CONTENTS 目 录

03

怎么评估 漏洞扫描结果

1. 漏洞扫描报告输出
2. 漏洞扫描误报分析
3. 风险分析

3.1

漏洞扫描报告输出

a. 关键信息提取
b. 漏洞信息检索
c. 常见加固方案
d. 报告整理输出

报告输出 – 关键信息提取

01

扫描目标存活数量

- 当次扫描可达的目标数量，与资产表对比发现是否有遗漏
- 遗漏的目标需检查原因补充扫描

02

目标主机漏洞分布情况

- 各风险等级漏洞在整体资产中的分布
- 哪些资产漏洞数量较多、风险等级较高

03

漏洞类型

- 应用类型：存在漏洞的主要是哪些系统、应用
- 哪些扫描原理类型发现的，存在误报可能性

04

漏洞信息

- 漏洞名称、漏洞描述、编号、受影响系统/版本/组件、风险等级、加固建议
- 为漏洞分析和加固提供参考

报告输出 – 关键信息提取 – 漏洞信息检索

基本漏洞信息检索 – 漏洞共享平台

- 检索方法：根据各类漏洞编号（CVE、CNVD、CNNVD等）在对应漏洞共享平台检索
- 获取信息：漏洞名称、描述、受影响通用应用版本范围、风险等级、部分官方补丁下载链接等

漏洞加固信息检索 – 操作系统/应用官方网站

- 在各类操作系统、应用软件官方网站通过漏洞编号检索官方漏洞公告、补丁编号
- 当前操作系统的哪些版本受影响，是否已有加固方案，具体加固方法及补丁下载链接

原理扫描型漏洞验证信息检索 – 互联网

- 通过BUGTRAQ编号，查找exploit
- 通过CVE编号，查找“CVE-XXXX-XXXX POC”或“CVE-XXXX-XXXX exploit”
- **验证有风险，需评估漏洞及验证风险，获取授权后开展**

NSFOCUS

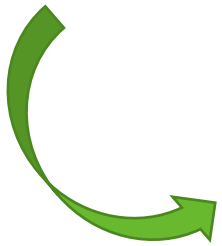
报告输出 – 关键信息提取 – 漏洞信息检索

- **CVE（Common Vulnerabilities & Exposures）**
  - CVE官网链接：http://cve.mitre.org/
- **CNVD（国家信息安全漏洞共享平台）**
  - CNVD官网链接：http://www.cnvd.org.cn/
- **CNNVD（中国国家信息安全漏洞库）**
  - CNNVD官网链接：http://www.cnnvd.org.cn/
- **SecurityFocus（根据Bugtraq ID检索漏洞）**
  - 官网链接：https://www.securityfocus.com
- **微软**
  - 安全公告：https://docs.microsoft.com/zh-cn/security-updates/securitybulletins/securitybulletins
  - 补丁检索链接（使用公告编号查询）：http://www.catalog.update.microsoft.com/home.aspx
- **各系统、应用官网**

报告输出 – 关键信息提取 – 基本加固方案

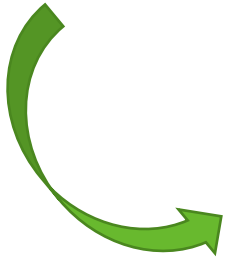
了解漏洞基本信息

- 漏洞描述
- 漏洞影响范围
- 漏洞风险等级



漏洞加固方案获取

- 扫描报告中的漏洞加固办法
- 漏洞检索获取的漏洞加固办法
- 通用的临时加固办法



加固方案选择

- 基于对漏洞基本信息的了解，根据漏洞存在的网络环境、业务/运维使用情况、加固办法可行性选择

报告输出 – 关键信息提取 – 基本加固方案

根本办法

- 升级应用版本，如openssh
- 安装安全漏洞补丁，如oracle CPU安全补丁
- 修改应用配置，如启用认证授权模块
- 更换更安全的其他应用/协议，如将Telnet更换为ssh
- 卸载应用，如非必要的运维应用

临时风险规避办法

- 官方提供的临时规避办法，如微软官方提供的缓解因素和变通办法
- 严格的端口访问控制策略，仅允许可信的有限源访问目标IP和端口
- 安全防护设备

报告输出 – 交付最终报告

- 漏洞扫描工作中，需根据实际需求输出经处理和分析的报告
- 评估目标与漏洞一一对应、漏洞状态追踪、漏洞对比分析等

漏洞扫描检查表

项目名称：		管理员：		检查人员：		检查日期：	
IP地址	计算机名	漏洞名称	风险程度	CVE	整改意见	整改情况	备注
		PHP '_php_stream_scandir()'缓冲区溢出漏洞	高	CVE-2012-2688	厂商补丁： PHP	未整改	
		PHP "crypt()" MD5 Salt安全漏洞	高	CVE-2011-3268	PHP 目前厂商已经发布了升级补丁以修复这个安全问	未整改	
		方程式组织后门DOUBLEPULSAR程序(SMB)【原理扫描】	高	CVE-2016-2842	更新微软最新补丁并联系绿盟科技安全服务人员	已整改	
		Samba未初始化指针释放远程代码执行漏洞(CVE-2015-0240)	高	CVE-2015-0240	临时解决方法： 在Samba 4.0.0和更高版本中，在smb.conf配置文	已整改	
		Samba 远程执行代码漏洞(CVE-2017-7494)	高	CVE-2017-7494	厂商补丁： Samba	已整改	
		PHP OS命令注入漏洞(CVE-2015-4642)	高	CVE-2015-4642	厂商补丁： PHP	未整改	

3.2

漏洞扫描误报分析

a. 常见误报原因
b. 常见误报场景
c. 误报案例解析

NSFOCUS

误报确认 – 误报原因

- 类型：漏洞误报、端口服务探测误报

误报确认 – 误报常见场景

01

获取信息异常

- OS识别错误
- 异常大量端口
- ……

02

获取信息不全

- 应用版本获取不全
- 获取到非当前在用的版本号
- ……

03

判断不准确

- 集成在某些操作系统中的应用与通用应用受影响情况差异
- 未开启存在漏洞的应用组件也报大量版本漏洞
- ……

04

其他

- 不同扫描器判断机制影响
- ……

误报确认 – 漏洞误报常见场景

- **资产信息获取错误**
- **示例：**网络设备报出大量其他OS漏洞
- **原因：**目标设备指纹信息识别出错，如网络设备识别为Linux，从而调用Linux相关扫描插件进行漏洞探测，导致大量漏洞误报
- **确认方法**
  - 与目标设备管理员确认设备类型
  - 通过远程访问/登录目标设备，人工查看返回信息。
  - 如Telnet开放端口，查看返回banner信息
- **规避方法**
  - 确认扫描链路上的防火墙情况，避免防护干扰
  - 确认扫描设备对目标设备类型的支持情况
  - 重新扫描

误报确认 – 漏洞误报常见场景

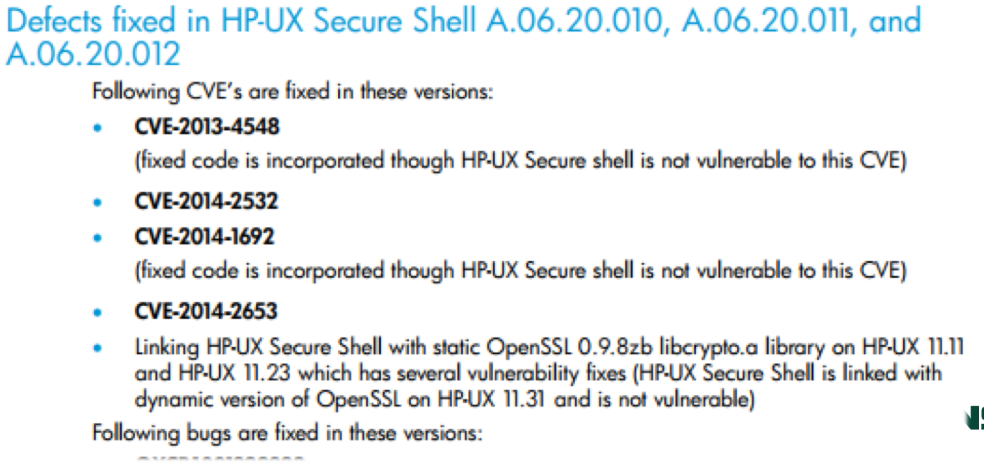
- **版本信息获取不全**
- **示例：**Oracle已打上最新安全补丁，扫描时仍报出大量漏洞
- **原因：**默认扫描时获取不到oracle完整版本号、补丁号
- **确认方法**
  - 手工登录查看oracle应用版本及补丁情况，
  - 与报告中获取版本对比
- **规避方法**
  - 使用具有system权限的oracle账户进行登录扫描
  - SSH登录扫描

误报确认 – 漏洞误报常见场景

- **获取的版本信息非当前在用版本**
- **示例：**目标系统已更新最新的openssh 7.9版本，却报出5.3版本下受影响的大量漏洞
- **原因：**目标系统升级到新版本时，未删除旧版本文件，导致扫描器获取到旧的文件信息
- **确认方法**
  - 远程探测端口确认回显banner信息
  - 手工登录系统，查看当前在用应用版本
  - 查找是否存在旧版本应用文件
- **规避方法**
  - 重新安装及更新应用时删除旧版本文件
  - 删除文件后重新扫描

误报确认 – 漏洞误报常见场景

- **特定操作系统中集成应用已修复，但版本与通用不一致**
- **示例：**扫描发现HP-UX中存在OpenSSH权限许可和访问控制漏洞（CVE-2014-2532），但实际HP-UX B.11.00 - B.11.31版本中集成的SSH已修复该漏洞
- **确认方法**
  - 根据漏洞的CVE编号查询目标系统的安全通告，如在redhat官方网站搜索CVE编号，确认redhat受到该漏洞影响的版本是否与目标系统一致
- **规避方法**
  - 人工确认漏洞与操作系统的关联性


Defects fixed in HP-UX Secure Shell A.06.20.010, A.06.20.011, and A.06.20.012

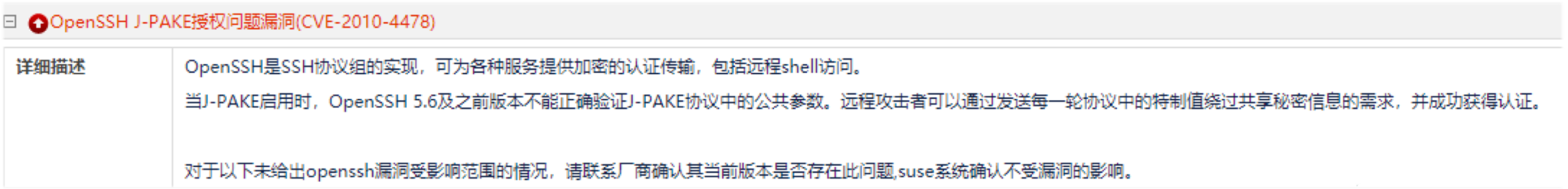
Following CVE's are fixed in these versions:

- **CVE-2013-4548**
  (fixed code is incorporated though HP-UX Secure shell is not vulnerable to this CVE)
- **CVE-2014-2532**
- **CVE-2014-1692**
  (fixed code is incorporated though HP-UX Secure shell is not vulnerable to this CVE)
- **CVE-2014-2653**
- Linking HP-UX Secure Shell with static OpenSSL 0.9.8zb libcrypto.a library on HP-UX 11.11 and HP-UX 11.23 which has several vulnerability fixes (HP-UX Secure Shell is linked with dynamic version of OpenSSL on HP-UX 11.31 and is not vulnerable)

Following bugs are fixed in these versions:

误报确认 – 漏洞误报常见场景

- **版本信息准确，但未使用受漏洞影响的模块、功能**
- **示例：**扫描发现存在OpenSSH J-PAKE授权问题漏洞(CVE-2010-4478)，但实际应用中并未启用J-PAKE
- **确认方法**
  - 确认漏洞基本信息，是否属于某版本下可独立选择开启的模块/功能
  - 确认目标系统中的应用，是否开启存在漏洞的模块/功能
- **规避方法**
  - 人工确认存在漏洞的模块及功能是否开启



误报确认 – 漏洞误报常见场景

- **不同扫描器结果差异**
- **示例：**使用两个不同品牌的系统扫描器对同一目标进行扫描，由于漏洞库差异、漏洞扫描插件差异等，导致扫描结果可能存在误报、漏报的情况
- **确认方法**
  - 对存在差异部分的漏洞进行分析，检查是否有通用的漏洞编号，如CVE、CNVD、CNNVD等，具有通用编号的漏洞普遍认可度较高
  - 存在差异部分的漏洞依据前述场景中的办法，验证是否误报

为保证漏洞扫描结果准确性，可考虑多种扫描器并用，并选择业界认可度较高的扫描器

误报确认 – 端口服务误报场景

- **扫描发现某目标IP开放了异常大量端口**
- **原因及确认方法**
  - 防火墙等防护设备代替目标设备，给扫描器回包应答，导致扫描器判断异常
- **规避方法**
  - 扫描时确认不经过防火墙等防护设备进行扫描

3.3

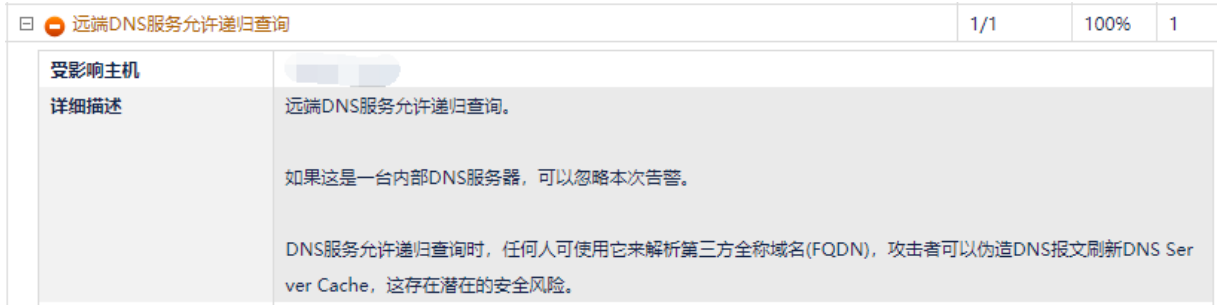
漏洞实例风险分析

a. 实际应用场景说明

漏洞风险定性分析 – 应用场景

- **实际评估中，应如何确定漏洞风险？**
  - 参考/定制权威漏洞风险评分定级方法；
  - 考虑业务、资产重要性/安全属性；
  - 结合时间维度、互联网公开信息考虑威胁赋值；
- **应用场景**
  - 不同扫描器扫描结果存在漏洞风险定级差异；
  - 某些漏洞在特定业务系统中的风险评定；
  - 漏洞加固优先级评定，指导漏洞修复工作。

风险较高（优先加固）：
- **重点资产**：核心系统、互联网系统、与防护目标相连接系统、有用户数据的系统
- **重点漏洞**：struts2系列、weblogic反序列化系列、远程命令执行系列等



FAQ

谢谢！

NSFOCUS