

# Kali linux渗透测试

苑房弘 FANGHONG.YUAN@163.COM



# 第八章 漏洞扫描



# 发现弱点

- 发现漏洞
  - 基于端口服务扫描结果版本信息（速度慢）
  - 搜索已公开的漏洞数据库（数量大）
  - 使用弱点扫描器实现漏洞管理

# 从信息的维度定义漏洞管理

- 信息收集：
  - 扫描发现网络IP、OS、服务、配置、漏洞
  - 能力需求：定义扫描方式内容和目标
- 信息管理
  - 格式化信息，并进行筛选、分组、定义优先级
  - 能力需求：资产分组、指定所有者、向所有者报告漏洞
- 信息输出
  - 向不同层级的人群展示足够的信息量
  - 能力需求：生成报告、导出数据、与SIEM集成

# 弱点扫描类型

- 主动扫描
  - 有身份验证
  - 无身份验证
- 被动扫描
  - 镜像端口抓包
  - 其他来源输入
- 基于Agent的扫描
  - 支持平台有限

# 漏洞基本概念

- CVSS (Common Vulnerability Scoring System)

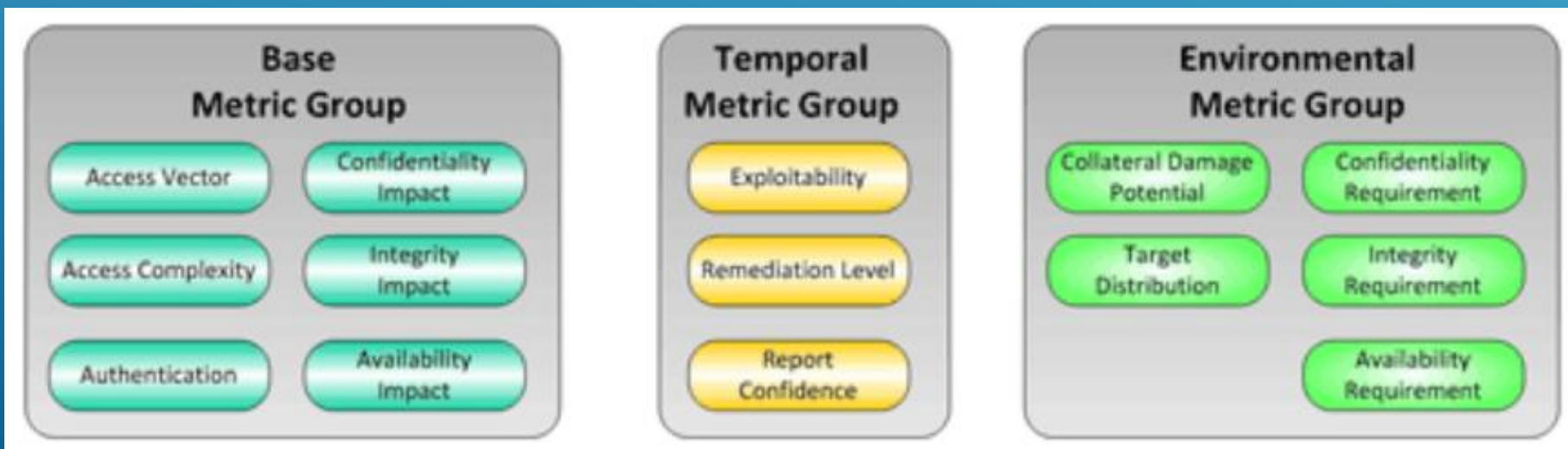
- 通用漏洞评分系统——工业标准
- 描述安全漏洞严重程度的统一评分方案
- V 3版本——2015年6月10日
- Basic Metric：基础的恒定不变的弱点权重
- Temporal Metric：依赖时间因素的弱点权重
- Enviromental Metric：利用弱点的环境要求和实施难度的权重



cvss-v30-specification-v1.7.pdf



cvss-v30-preview2-metricvectorstring-december-2014.pdf

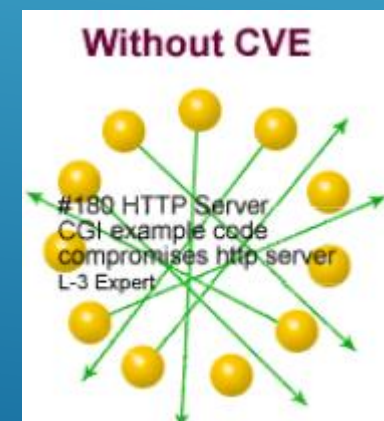
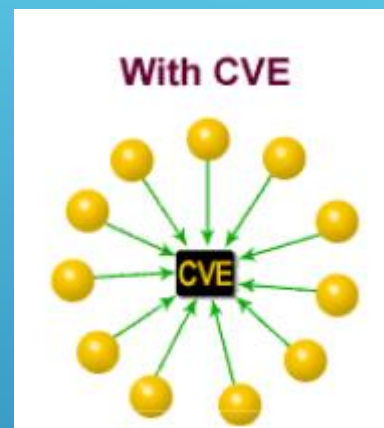


# 漏洞基本概念

- CVSS (Common Vulnerability Scoring System)
  - CVSS是安全内容自动化协议 (SCAP) 的一部分
  - 通常CVSS与CVE一同由美国国家漏洞库 (NVD) 发布并保持数据的更新
  - 分值范围：0 —— 10
  - 不同机构按CVSS分值定义威胁的中、高、低威胁级别
  - CVSS体现弱点的风险，威胁级别 (severity) 表示弱点风险对企业的影响程度
  - CVSS分值是工业标准，但威胁级别不是

# 漏洞基本概念

- Vulnerability Reference
- CVE ( Common Vulnerabilities and Exposures )
  - 已公开的信息安全漏洞字典，统一的漏洞编号标准
  - MITRE公司负责维护（非盈利机构）
  - 扫描器的大部分扫描项都对应一个CVE编号
  - 实现不同厂商之间信息交换的统一标准
- CVE发布流程
  - 发现漏洞
  - CAN负责指定CVE ID
  - 发布到CVE List —— CVE-2008-4250
  - MITRE负责对内容进行编辑维护





# 漏洞基本概念

- 很多厂商维护自己的Vulnerability Reference
  - MS
  - MSKB
- 其他Vulnerability Reference
  - CERT      TA08-297A
  - BID        31874
  - IAVM      2008-A-0081
  - OVAL      OVAL6093

# 漏洞基本概念

- OVAL (Open Vulnerability and Assessment Language)
  - 描述漏洞检测方法的机器可识别语言
  - 详细的描述漏洞检测的技术细节，可导入自动化检测工具中实施漏洞检测工作
  - OVAL使用XML语言描述，包含了严密的语法逻辑
- CCE
  - 描述软件配置缺陷的一种标准化格式
  - 在信息安全风险评估中，配置缺陷的检测是一项重要内容，使用CCE可以让配置缺陷以标准的方式展现出来，便于配置缺陷评估的可量化操作。
- CPE (Common Product Enumeration)
  - 信息技术产品、系统、软件包的结构化命名规范，分类命名
- CWE (Common Weakness Enumeration)
  - 常见漏洞类型的字典，描述不同类型漏洞的特征（访问控制、信息泄露、拒绝服务）

# 漏洞基本概念

- Security Content Automation Protocol (SCAP)
  - SCAP 是一个集合了多种安全标准框架
  - 六个元素：CVE、OVAL、CCE、CPE、CVSS、XCCDF
  - 目的是以标准的方法展示和操作安全数据
  - 由NIST负责维护
- SCAP主要解决三个问题
  - 实现高层政策法规等到底层实施的落地（如FISMA，ISO27000系列）
  - 将信息安全所涉及的各个要素标准化（如统一漏洞的命名及严重性度量）
  - 将复杂的系统配置核查工作自动化
- SCAP是当前美国比较成熟的一套信息安全评估标准体系，其标准化、自动化的思想对信息安全行业产生了深远的影响。

# 漏洞基本概念

- NVD (National Vulnerability Database)
  - 美国政府的漏洞管理标准数据
  - 完全基于SCAP框架
  - 实现自动化漏洞管理、安全测量、合规要求
  - 包含以下库
    - 安全检查列表
    - 软件安全漏洞
    - 配置错误
    - 产品名称
    - 影响度量
- <https://nvd.nist.gov/>

# 漏洞管理

- 周期性扫描跟踪漏洞
- 高危漏洞优先处理
- 扫描注意事项
- 漏洞管理三要素
  - 准确性
  - 时间
  - 资源

# NMAP

- nmap 扫描脚本
  - 400+
  - 分类
- `cat /usr/share/nmap/scripts/script.db`
- `grep vuln /usr/share/nmap/scripts/script.db | cut -d "\"" -f 2`
- `cat /usr/share/nmap/scripts/smb-check-vulns.nse`
- `smb-check-vulns.nse`
  - `nmap -sU -sS --script=smb-check-vulns.nse --script-args=unsafe=1 -p U:137,T:139,445 1.1.1.1`
  - MS08-067

# NMAP

- smb-vuln-ms10-061.nse
  - Stuxnet蠕虫利用的4个漏洞之一
  - Print Spooler权限不当，打印请求可在系统目录可创建文件、执行任意代码
  - LANMAN API枚举共享打印机
  - 远程共享打印机名称
  - smb-enum-shares枚举共享
    - 身份认证参数——smbuser、smbpassword
    - `nmap -p445 --script=smb-enum-shares.nse --script-args=smbuser=admin,smbpassword=pass 1.1.1.1`
  - Windows XP, Server 2003 SP2, Vista, Server 2008, win 7
- 影响扫描结果的因素

# 扫描结果确认

- 目标系统版本
  - 补丁是否安装
  - 是否可被入侵
- 
- 有时很难说什么才是准确的扫描结果
  - 应综合的看待漏洞威胁

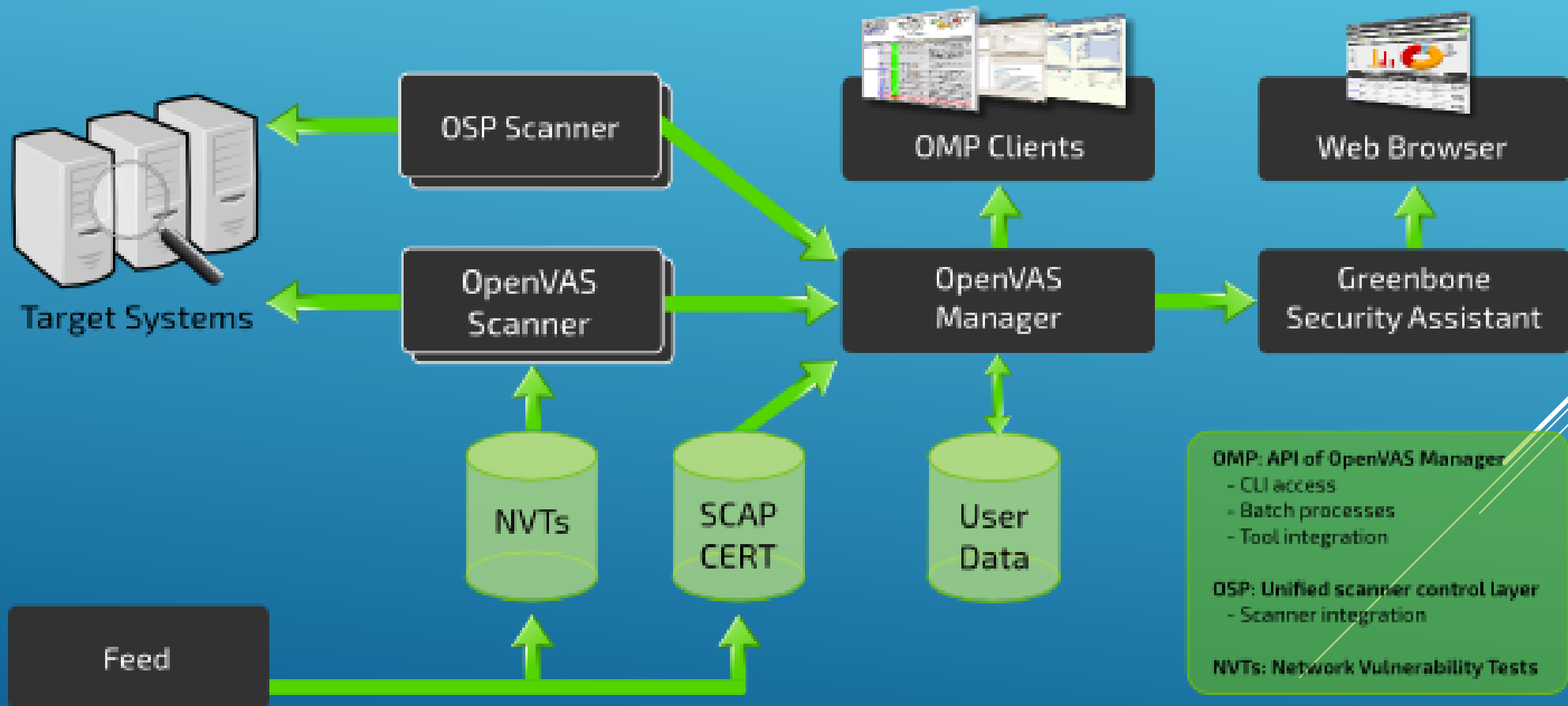


# OPENVAS

- Openvas
  - Nessus项目分支
  - 管理目标系统的漏洞
  - 免费开源
  - Kali默认安装，但未配置和启动

# OPENVAS

## Greenbone Security Manager: OpenVAS Framework Architecture




# OPENVAS

- OpenVAS Manager
  - 控制scanner和其他manager的中心组件
  - 控制中心数据库，保存用户配置及扫描结果
  - 客户端使用基于XML的无状态OMP协议与其通信
  - 集中排序筛选，使客户端获得一致展现
- OpenVAS Scanner
  - 具体执行Network Vulnerability Tests (NVTs)
  - NVTs 每天通过 Feed 更新
  - 受 Manager 控制

# OPENVAS

- OSP Scanner
  - 可以统一管理多个scanner
  - 将一组 scanner 作为一个对象交给manager管理
- Greenbone Security Assistant (GSA)
  - 提供 Web service
- OpenVAS CLI
  - omp 命令行工具，可实现批处理控制 manager
- 更新很快
  - 所有找得到的资料几乎都已不同程度的过时了

# OPENVAS

- 安装
  - 创建证书
  - 同步弱点数据库
  - 创建客户端证书
  - 重建数据库
  - 备份数据库
  - 启动服务装入插件
  - 创建管理员账号
  - 创建普通用户账号
  - 配置服务侦听端口
  - 安装验证
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

# OPENVAS

- 初始化安装
  - `openvas-setup`
- 检查安装结果
  - `openvas-check-setup`
- 查看当前账号
  - `openvasmd --list-users`
- 修改账号密码
  - `openvasmd --user=admin --new-password=Passw0rd`
- 升级
  - `openvas-feed-update`

# OPENVAS

- 不是秘笈是经验
- `vi /usr/bin/openvas-start`
  - Starting OpenVas Services
  - Starting OpenVAS Manager: `openvasmd`
  - Starting OpenVAS Scanner: `openvassd`
  - Starting Greenbone Security Assistant: `gsad`

# OPENVAS

- 扫描配置
    - 扫描windows
    - 扫描Linux
    - 扫描网络设备
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.



# OPENVAS

- 扫描目标
  - Windows
  - Linux
  - 路由器

# OPENVAS

- 扫描任务
  - 进度
  - 报告

# NESSUS

- 家庭版
  - 免费
- 专业版
  - 收费、无限的并发连接
- 下载
  - <http://www.tenable.com/products/nessus/select-your-operating-system>
- 安装
  - `dpkg -i`
  - 安装路径: `/opt/nessus`
- 启动服务
  - `/etc/init.d/nessusd start`

# NESSUS

- 管理地址
  - <https://127.0.0.1:8834>
- 注册激活码
  - <http://www.tenable.com/products/nessus-home>
- 管理账号
  - 更新插件
- 基本配置 (setting)
  - 升级
  - 账号
  - SMTP
  - 代理

# NESSUS

- 策略
- 扫描
- 扫描本机
- 扫描windows
- 扫描linux
- 扫描网络设备
- 扫描web server
- 报告
- 调度

CVSS score	Criticality
0	Info
<4	Low
<7	Medium
<10	High
10	Critical

# NEXPOSE

- Rapid 7
  - Nexpose
  - 完整的漏洞管理实现

# 扫描结果分析

- False positive:
  - 误报
- False negative
  - 漏报

# Q & A

