弱点扫描

弱点扫描类型

主动类型和被动扫描指的是没有权限登入系统，只能通过猜测或扫描进行测试。
主动扫描也可以有系统登入权限，但是在渗透测试中这种情况不会怎么出现。
也有Agent扫描，但是这个系统不会在生产环境中出现。比如你能在网站服务器中安装Agent？所以Agent有局限性，虽然扫描出来的还算可靠

漏洞基本概念
CVSS
CVSS(Common Vulnerability Scoring System)通用漏洞等级评分系统，是一个工业标准。其作用是按照自己的评分方法进行评估，最低为0分，最高10分，根据威胁程度来评估。
CVSS分了三种的类别为Basic Metric（基础的恒定不变弱点权重）Temporal Metric（依赖时间因素的弱点权重）EnViromental Matric（利用弱点的环境要求和实施难度的权重）
CVSS与CVE一同由美国国家漏洞库（NVD）发布并保持数据的更新，不同机构按照CVSS分值分为中高低威胁级别

CVE
CVE(Common Vulnerabilities and Exposures)是一个统一漏洞编号的标准，木有由MITRE公司负责维护，而MITRE是一个非盈利机构统一了不同厂商的漏洞编号。

申请流程一般由CAN负责制定CVE ID格式你可以一般是CVE-年份-00000等。

MS
微软的漏洞定义了自己的漏洞编号是MS，通常格式是MS-年份-000等，对于补丁微软定义的编号就是MSKB

OVAL
OVAL（Open Vulnerability and Assessment Language）是一个开发的漏洞描述语言，是以XML语言描述和发布，用通用的描述方法对一个漏洞描述，这些会被漏洞扫描器中进行收入。之后这个扫描器就可以进行扫描或检测漏洞了。

CCE
CCE是用于来描述软件缺陷的一个格式，在信息安全风险管理的过程中，是由CCE进行规范标准来管理的。

CPE
CPE（Common Product Enumeration）是一个由信息技术产品、系统、软件包的结构化命名规范，分类命名

CWE
CWE（Common Weakness Enumeration）是一个通用弱点的描述，仅对弱点进行分类。

SCAP
SCAP (Security Content Automation Protocol）是一个集合了多个安全标准的框架，一共有CVE\CCE\CPE\CVSS\OVA\XCCDF是由NIST负责维护

SCAP主要解决是哪个问题
实现法规和底层企业的实施和落实
将信息安全所涉及的各个要素标准化
系统配置核查自动化

NVD

NVD（National Vulnerabillity Database）是一个美国政府的漏洞管理标准数据，完全基于SCAP框架，实现了自动化漏洞管理，安全测量、安全合规等要求。