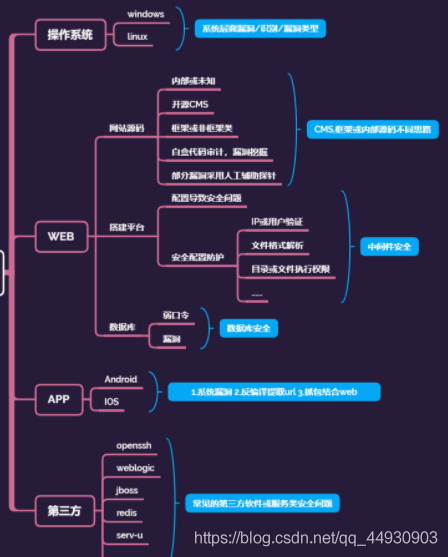
# 05 渗透基础入门-系统及数据库



操作系统层面

识别操作系统常见方法（nmap、windows大小写不敏感、linux大小写敏感(比如url大小写试探也可以判断出)，TTL值：linux一般64（<100），windows一般128(>100)）

简要两者区别及识别意义

操作系统层面漏洞类型对应意义(利用漏洞进行内网渗透、横向渗透等，如永恒之蓝等等)

简要操作系统层面漏洞影响范围(拿到服务器权限等)

数据库层面

识别数据库类型常见方法（nmap等工具扫描，对应端口开放）

数据库类型区别及识别意义

数据库常见漏洞类型及攻击

简要数据库层面漏洞影响范围

ASP+Access

php+mysql

aspx+mssql

jsp+mssql,oracle

python+mongodb

…

常见数据库对应的默认端口：

关系型数据库：

1.Oracle数据库默认端口号为，1521；

2.MySQL数据库默认端口号为，3306；

3.SQLServer数据库默认端口号为，1433;

NOSQL数据库：

1.MongoDB默认端口号为：27017；

2.Redis默认端口号为：6379；

3.memcached默认端口号为：11211；

其他：

1527　　Derby

5432　　pgsql

5000　　db2

9092　　pointbase

无默认　Informix

第三方层面

如何判断有那些第三方平台或软件

简要为什么要识别第三方平台或软件

常见第三方平台或软件漏洞类型及攻击

简要第三方平台或软件安全测试的范围

补充

除去常规WEB安全及APP安全测试外，类似服务器单一或复杂的其他服务（邮件，游戏，负载均衡等），也可以作为安全测试目标，此类目标测试原则只是少了WEB应用或其他安全问题。所以明确安全测试思路是很重要的！

案例演示：

✧ 上述涉及的基础知识演示

✧ 某操作系统层面漏洞演示（永恒之蓝等）

✧ 某数据库弱口令及漏洞演示

✧ 某第三方应用安全漏洞演示

涉及资源：

https://nmap.org/

https://www.kali.org/downloads/

https://github.com/hellogoldsnakeman/masnmapscan-V1.0