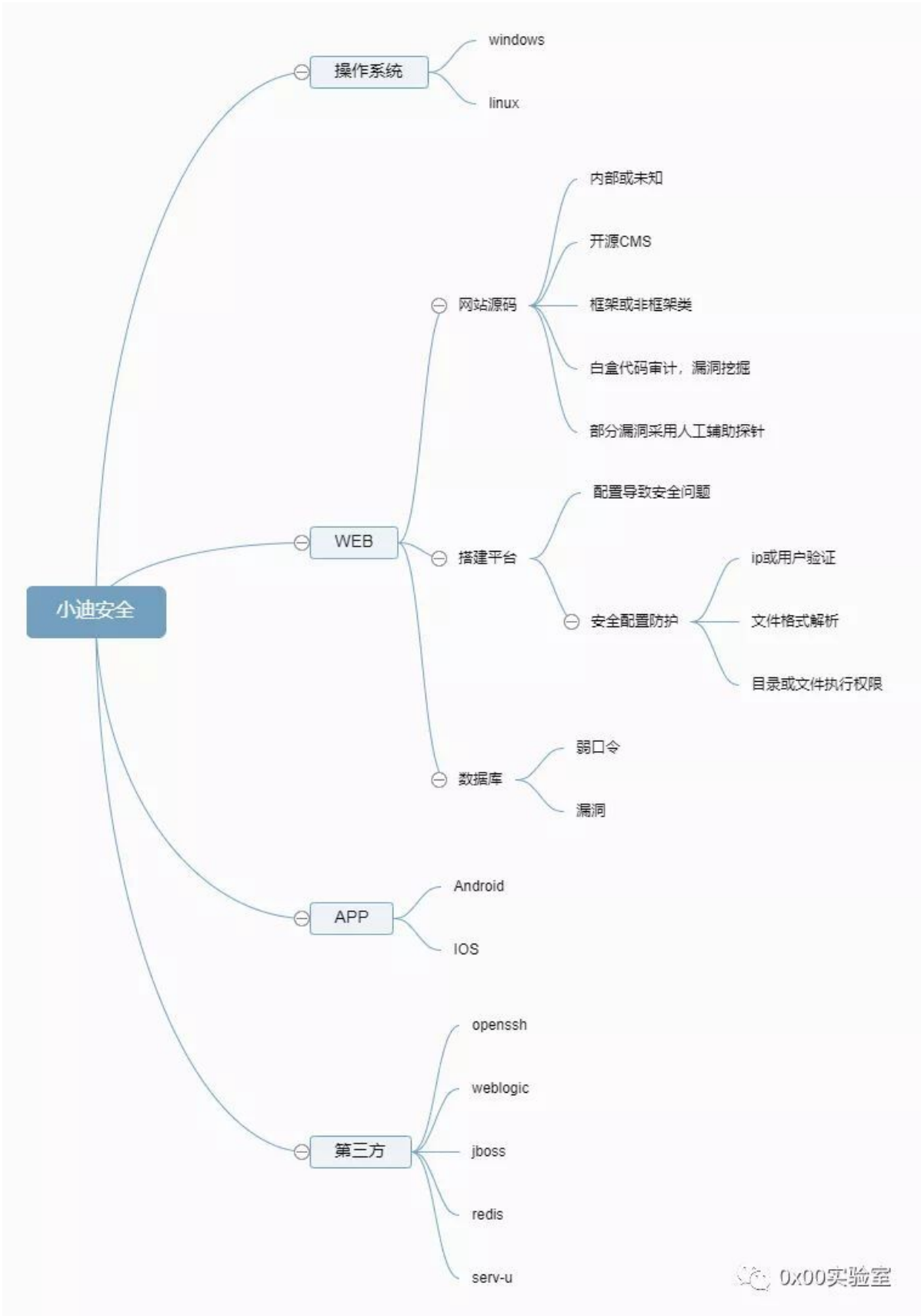
# Day05　基础入门–系统及关系库等



## 5.1 操作系统层面

### 5.1.1识别操作系统常见方法

1. 看字母大小写，windows对大小写不敏感，Linux敏感
2. 看ping值 --TTL在64左右Linux --TTL在128左右windows
3. NMAP -O IP

### 5.1.2简要两者区别及识别意义情况

- 可以帮助我们明确思路
- 可以筛选掉不符合系统的情况

### 5.1.3操作系统层面漏洞类型对应意义

- 覆盖面广
- 获取的权限高
- 危害性大

---

## 5.2 数据库层面

### 5.2.1识别数据库类型常见方法

- nmap -O ip
- nmap ip -p 端口，通过端口开放反推数据库

### 5.2.2数据库类型区别及识别意义

- 数据库的漏洞和类型相性很强
- 不同数据库漏洞爆发点不太一样
- 能确定数据库类型、版本，会对渗透有很大帮助

### 5.2.3数据库常见漏洞类型及攻击

- 弱口令
- SQL注入

### 5.2.4简要数据库层面漏洞影响范围

- 要参考数据库的重要程度来判断影响范围

### 5.2.5常见的数据库结构

ASP+Access
PHP+MySQL
Axpx+MSSQL JSP+MySQL,Oracle
Python+Mongodb

### 5.2.6服务器端口

关系型数据库： MySQL:3306 SqlServer:1433 Oracle:1521
NOSQL数据库： MongoDB:27017 Redis:6379 memcached:11211

### 5.2.7第三方

- 如何判断那些有第三方平台或软件 -- 端口扫描 -- 特征匹配
- 简要为什么要识别第三方平台或软件 -- 可以提供额外的攻击面
- 常见第三方平台或软件漏洞类型及攻击 -- 弱口令
- 简要第三方平台或软件安全测试的范围

> 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!

---

### 资源

```
https://nmap.org/
https://www.kali.org/downloads/
https://github.com/hellogoldsnakeman/masnmapscan-v1.0
https://pypi.tuna.tsinghua.edu.cn/simple-------清华大学python镜像
https://pypi.tuna.tsinghua.edu.cn-------清华大学python镜像
```