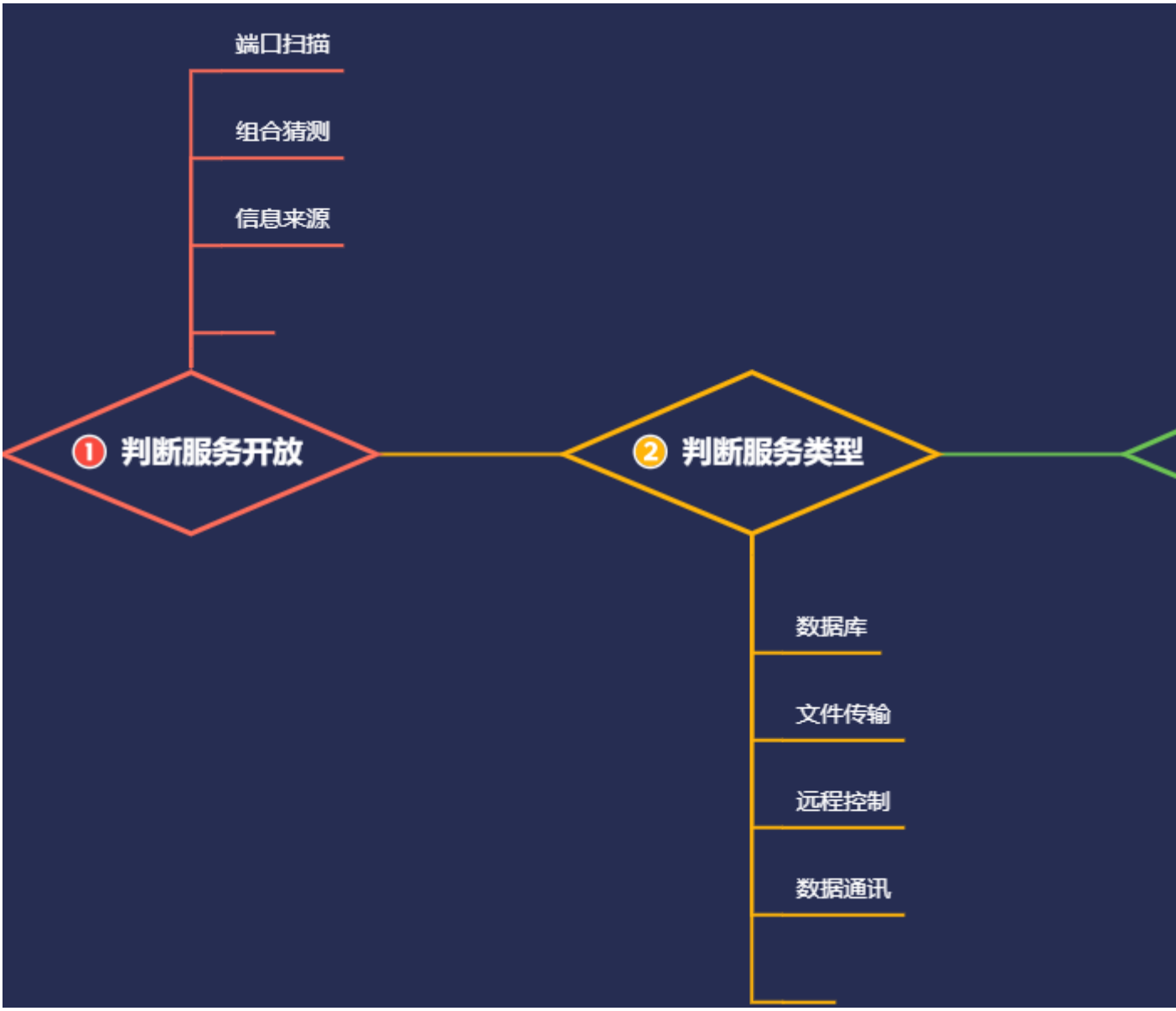
服务攻防-应用协议&Rsync&SSH&RDP&FTP&漏洞批扫&口令猜解

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
  - Influxdb
  - CouchD
  - Elastics
  - H2 Data
- FTP


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-远程控制&文件传输等

2、远程控制-RDP&RDP&弱口令&漏洞

3、文件传输-FTP&Rsync&弱口令&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：

- 口令猜解-Hydra-FTP&RDP&SSH
- 配置不当-未授权访问-Rsync 文件备份
- 高端课程-直接搜哈-MSF&Fofaviewer
- 协议漏洞-应用软件-FTP&Proftpd 搭建
- 协议漏洞-应用软件-SSH&libssh&Openssh

#口令猜解-Hydra-FTP&RDP&SSH

https://github.com/vanhauser-thc/thc-hydra

hydra 是一个自动化的爆破工具，暴力破解弱密码，

是一个支持众多协议的爆破工具，已经集成到 KaliLinux 中，直接在终端打开即可

-s PORT 可通过这个参数指定非默认端口。

-l LOGIN 指定破解的用户，对特定用户破解。

-L FILE 指定用户名字典。

-p PASS 小写，指定密码破解，少用，一般是采用密码字典。

-P FILE 大写，指定密码字典。

-e ns 可选选项，n：空密码试探，s：使用指定用户和密码试探。

-C FILE 使用冒号分割格式，例如"登录名:密码"来代替-L/-P 参数。

-M FILE 指定目标列表文件一行一条。

-o FILE 指定结果输出文件。

-f 在使用-M 参数以后，找到第一对登录名或者密码的时候中止破解。

-t TASKS 同时运行的线程数，默认为 16。

-w TIME 设置最大超时的时间，单位秒，默认是 30s。

-v / -V 显示详细过程。

server 目标 ip

service 指定服务名，支持的服务和协议：telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp 等等。

例子：

FTP：文件传输协议

RDP：Windows 远程桌面协议

SSH：Linux 安全外壳协议

```
hydra -L test -P 10top1K.txt 47.110.53.159 ftp -V
hydra -l root -P 10top1K.txt 47.110.53.159 ssh -V
hydra -l administrator -P 10top1K.txt 47.110.53.159 rdp -V
```

#配置不当-未授权访问-Rsync 文件备份

rsync 是 Linux 下一款数据备份工具，支持通过 rsync 协议、ssh 协议进行远程文件传输。其中 rsync 协议默认监听 873 端口，如果目标开启了 rsync 服务，并且没有配置 ACL 或访问密码，我们将可以读写目标服务器文件。

判断：rsync rsync://123.58.236.76:45854/

利用：

-读取文件：rsync rsync://123.58.236.76:45854/src/

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址