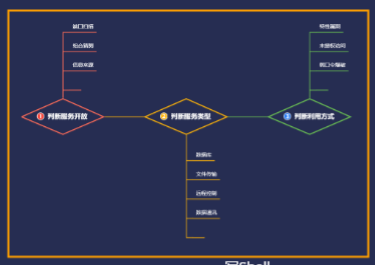
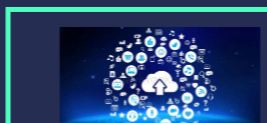
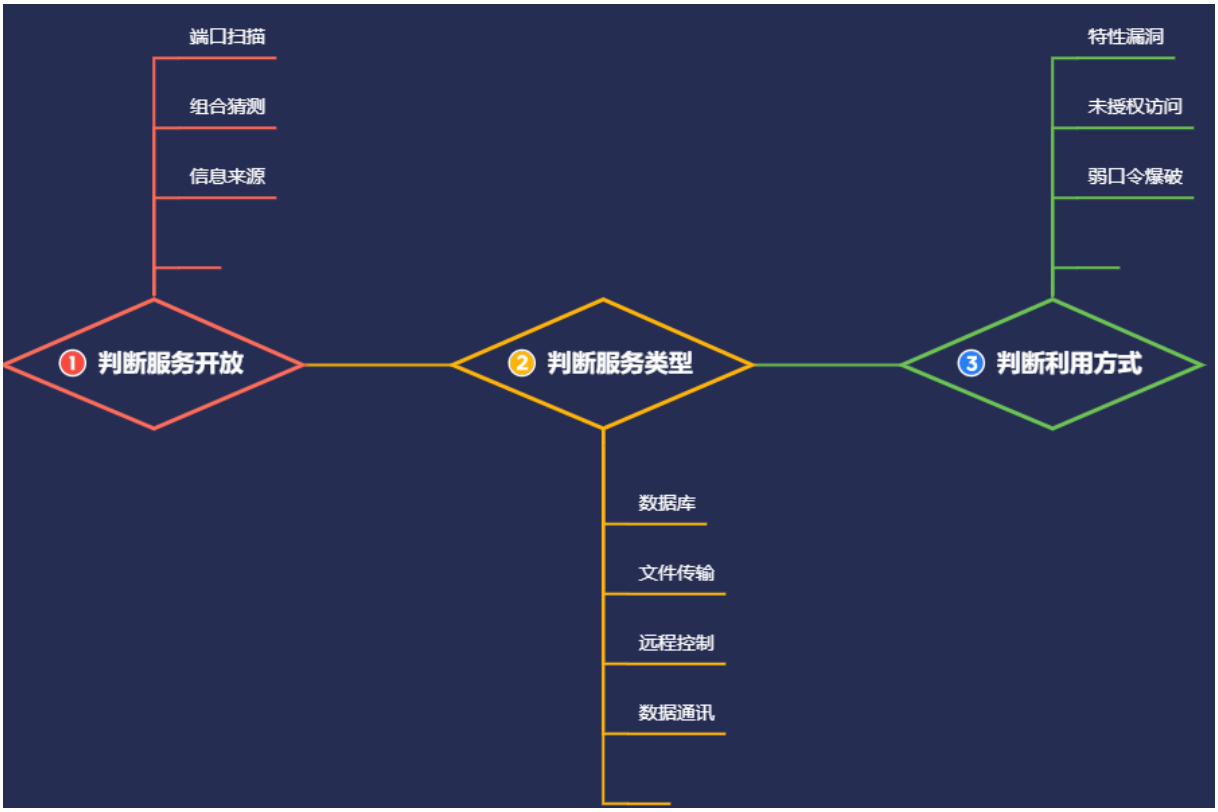
服务攻防-中间件安全&CVE 复现

&K8s&Docker&Jetty&Websphere

- 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
- 
  - IIS
    - 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
    - 1、后缀解析 文件名解析


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，K8s，Weblogic，JBoos，WebSphere，Jenkins ，GlassFish，Jetty，Jira，Struts2，Laravel，Solr，Shiro，Thinkphp，Spring，Flask，jQuery 等

0、中间件-K8s 安全

1、中间件-Jetty 安全

2、中间件-Docker 安全

3、中间件-WebSphere 安全

#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-K8s-搜哈
- 中间件-Jetty-搜哈
- 中间件-Docker-搜哈

- 中间件-WebSphere-搜哈
- 配合下-Fofa_Viewer-搜哈

#中间件-K8s-搜哈

kubernetes 简称 k8s，是一个由 google 开源的，用于自动部署，扩展和管理容器化应用程序的开源系统。在 B 站内部，k8s 在管理生产级容器和应用服务部署已经有较为广泛和成熟的应用。通过 k8s，可跨多台主机进行容器编排、快速按需扩展容器化应用及其资源、对应用实施状况检查、服务发现和负载均衡等。

https://blog.csdn.net/w1590191166/article/details/122028001

#中间件-Jetty-搜哈

Elipse Jetty 是一个开源的 servlet 容器，它为基于 Java 的 Web 容器提供运行环境。

CVE-2021-28164

http://123.58.236.76:63126/%2e/WEB-INF/web.xml

CVE-2021-28169

http://123.58.236.76:63126/static?/WEB-INF/web.xml

CVE-2021-34429

http://123.58.236.76:63126/%u002e/WEB-INF/web.xml

#中间件-Docker-搜哈

Docker 容器是使用沙盒机制，是单独的系统，理论上是很安全的，通过利用某种手段，再结合执行 POC 或 EXP，就可以返回一个宿主机的高权限 Shell，并拿到宿主机的 root 权限，可以直接操作宿主机文件。 它从容器中逃了出来，因此我们形象的称为 Docker 逃逸漏洞。

1、容器判断：

-是否存在.dockerenv 文件

ls -alh /.dockerenv

-查询系统进程的 cgroup 信息：

cat /proc/1/cgroup

2、容器逃逸漏洞：权限提升

-由内核漏洞引起 ——Dirty COW(CVE-2016-5195)

-由 Docker 软件设计引起——CVE-2019-5736、CVE-2019-14271，CVE-2020-15257

-由配置不当引起——开启 privileged（特权模式）+宿主机目录挂载（文件挂载）、功能（capabilities）机制、sock 通信方式

-CVE-2016-5195

https://github.com/gebl/dirtycow-docker-vdso

https://www.ichunqiu.com/experiment/catalog?id=100295

使用本地 1234 端口连接 docker 的 1234 端口运行 dirtycow 镜像，并将其临时命名为 test

其中 test 为临时名称，可以自定义填写，-p 第一个端口为本机的端口，第二

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址