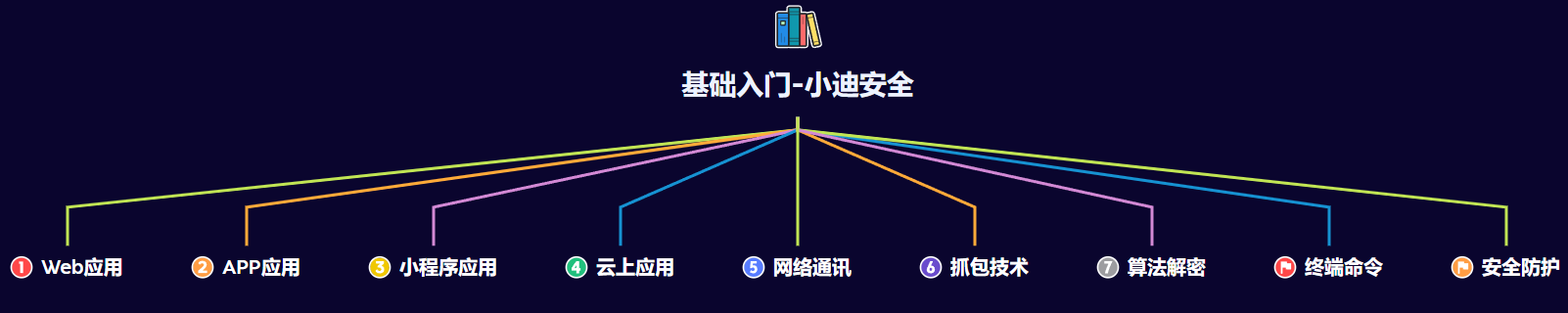
基础入门-系统命令&终端脚本&Shell编程&Bat批处理&文件属性权限&用户及组划分



#知识点：  
1、基础入门-Web应用-域名上的技术要点  
2、基础入门-Web应用-源码上的技术要点  
3、基础入门-Web应用-数据上的技术要点  
4、基础入门-Web应用-解析上的技术要点  
-----------------------------------------------------  
1、基础入门-Web应用-搭建架构上的技术要点  
2、基础入门-Web应用-源码类别上的技术要点  
-----------------------------------------------------  
1、基础入门-Web应用-防护产品-WAF保护  
2、基础入门-Web应用-加速服务-CDN节点  
3、基础入门-Web应用-文件托管-OSS存储  
4、基础入门-Web应用-通讯服务-反向代理  
5、基础入门-Web应用-运维安全-负载均衡  
-----------------------------------------------------  
1、基础入门-Web应用-蜜罐系统  
2、基础入门-Web应用-堡垒机运维  
3、基础入门-Web应用-内外API接口  
4、基础入门-Web应用-第三方拓展架构  
-----------------------------------------------------  
1、基础入门-APP应用-开发架构安全问题  
2、基础入门-小程序应用-开发架构安全问题  
-----------------------------------------------------  
1、抓包技术-Web应用-http/s-Burp&Yakit  
2、抓包技术-APP应用-http/s-Burp&Yakit  
3、抓包技术-PC端应用-http/s-Burp&Yakit  
4、抓包技术-WX小程序-http/s-Burp&Yakit  
5、抓包技术-软件联动-http/s-Proxifier  
6、抓包技术-通用方案-http/s-ReqableApi  
7、抓包技术-其他工具-http/s-Fiddler&Charles  
-----------------------------------------------------  
1、抓包技术-HTTP/S双层代理-扶墙环境  
2、抓包技术-HTTP/S上游下游-项目联动  
3、抓包技术-全局协议-WireShark&科来  
-----------------------------------------------------  
1、数据不回显原因和解决-带外延迟反弹写文件  
2、数据不出网原因和解决-出入站策略正反向连接  
-----------------------------------------------------  
1、反弹Shell-项目&命令&语言等  
2、系统渗透命令-网络&文件&操作等  
-----------------------------------------------------  
1、传输格式&数据-类型&编码&算法  
2、密码存储&混淆-不可逆&非对称性  
-----------------------------------------------------  
0、算法类型-单向散列&对称性&非对称性  
1、算法识别加解密-MD5&AES&DES&RSA  
2、解密条件寻找-逻辑特征&源码中&JS分析  
-----------------------------------------------------  
1、请求头&返回包-方法&头修改&状态码等  
2、数据包分析-红队攻击工具&蓝队流量研判  
3、数据包构造-Reqable自定义添加修改请求  
-----------------------------------------------------  
1、网站协议-http/https安全差异（抓包）  
2、身份鉴权-HTTP头&OAuth2&JWT&Token  
-----------------------------------------------------  
1、AI赋能-结合安全-ChatGPT4注册&使用&升级  
2、AI赋能-结合安全-ChatGPT4专业接口&安全插件  
-----------------------------------------------------  
1、Windows&Linux-脚本开发-Bat&Shell  
2、Windows&Linux-权限差异-文件&用户组  
  
#章节点：(待补充)  
Web架构，App架构，小程序架构，前后端分离，容器技术，云产品服务，  
数据加解密算法，数据包抓取，数据包解析，正反向网络通讯，内外网通讯，  
防火墙出入站，Windows&Linux渗透命令，WAF产品，负载均衡，加壳保护等  
  
#具体点：(待补充)  
架构：WEB,APP,小程序,前后端,容器化等  
服务：OSS存储,CDN加速,云数据库,负载均衡等  
网络：不回显,反向代理,防火墙出入站,内外网,正反向连接等  
算法：MD5,Base64,AES,DES,Salt,自定义,代码加密算法等  
命令：Windows&Linux,文件下载,网络查看,反弹权限,用户等  
防护：WAF防护,蜜罐系统,CDN加速,权限设置,加壳加密反调试等

演示案例：

* Windows&Linux-脚本开发-Bat&Shell
* Windows&Linux-权限差异-文件&用户

#系统命令集合  
在线参考：https://book.shentoushi.top/  
  
#Windows Cmd&PowerShell  
CMD命令终端:  
VBS BAT格式文件  
echo  
@字符放在命令前将关闭该命令回显，无论此时echo是否为打开状态  
@echo off  
@echo on  
echo "hello"  
echo "hello" "world"  
  
常见：  
pause 将dos界面暂停关闭  
:: 注释  
chcp 65001 乱码解决  
  
变量  
set x=hello  
set y=world  
echo %x% %y%  
set /p input=请输入：  
%cd%  打印当前路径  
  
函数 :fun\_main  
start 调用其他程序，如可执行文件exe  
goto 用于函数跳转，其中特别的是goto :eof 可用于停止往下继续执行命令行  
call 用于调用函数，也可以调用别的bat脚本  
  
for  
dir /b 指定目录 这个语法可以用于获得指定目录下的所有文件和文件夹  
for /f 遍历指定目录下所有的文件和文件夹  
for /d 遍历指定目录下所有的文件夹  
for /r 遍历指定目录下所有的文件和子文件夹中的文件  
for /l 是Windows批处理脚本中的一种循环语句，用于按数字范围和步长进行循环  
%%i 则是声明的变量，可以是任意的变量名，但变量名前面必须加上两个百分号%%  
for 进阶 delims（分隔符），读取的字符串会以这些分隔符进行拆分成多个子字符串  
  
FIND  
/V 显示所有未包含指定字符串的行。  
/C 仅显示包含字符串行的次数。  
/N 显示行号。  
/I 搜索字符串时忽略大小写。  
/OFF[LINE]：不要跳过具有脱机属性集的文件。  
"string"：指定要搜索的文本字符串。  
[drive:][path]filename：指定要搜索的文件  
  
bat中 比较符号  
EQU - 等于  
NEQ - 不等于  
LSS - 小于  
LEQ - 小于或等于  
GTR - 大于  
GEQ - 大于或等于  
  
常用特殊符号  
命令管道符 |  
转义字符 ^  
&、&&、||   
&符号：允许在一行中使用2个以上不同的命令，如果第一个命令执行失败时，并不会影响到后面的命令执行，执行顺序是从左到右  
||符号：与&&符号一样，可以同时执行多条命令，但是不同的是，当第一条命令执行失败才执行第二条命令，当碰到执行正确的命令将不执行后面的命令，如果没有出现正确的命令则一直执行完所有命令  
， 逗号相当与空格  
  
简易案例：  
1、获取目录下所有文件目录  
2、用Ping获取网段存活主机  
3、获取计算机信息筛选补丁  
  
#Linux Shell编程入门  
基础命令：首先，你需要熟悉一些基本的Linux命令，如ls、cd、cp、mv、rm等，这些是编写脚本的基础。  
文件系统：了解Linux文件系统结构和权限管理，知道如何使用chmod、chown等命令。  
环境变量：理解环境变量的概念和用法，以及如何使用export、echo $VAR\_NAME等命令。  
重定向和管道：学习如何使用输入输出重定向（>、<、>>）和管道（|）。  
脚本基础：脚本的创建和执行。  
脚本的第一行（shebang，如#!/bin/bash）。  
脚本的注释（以#开头）。  
变量：如何定义和使用变量。  
特殊变量（如$0、$1、$@、$#等）。  
条件语句：学习如何使用if、elif、else和fi来编写条件逻辑。  
循环：掌握for循环和while循环的用法。  
函数：了解如何定义和调用函数。  
文本处理：学习使用文本处理工具，如grep、sed、awk等。  
参考学习：https://mp.weixin.qq.com/s/qXZkKrF1vYtJv07L0-hkAA  
  
简易案例：  
1、统计登录日志中SSH爆破事件  
2、统计Web日志中的SQL攻击事件  
  
#Windows权限  
文件和目录权限  
完全控制，修改，读取和执行，列出文件夹内容，读取，写入，拒绝等  
完全控制（Full Control）：允许用户对文件夹、子文件夹、文件进行全权控制，包括修改资源的权限、获取资源的所有者、删除资源的权限等。  
修改（Modify）：允许用户修改或删除资源，同时拥有写入及读取和运行权限。  
读取和运行（Read & Execute）：允许用户拥有读取和列出资源目录的权限，另外也允许用户在资源中进行移动和遍历。  
列出文件夹目录（List Folder Contents）：允许用户查看资源中的子文件夹与文件名称。  
读取（Read）：允许用户查看该文件夹中的文件及子文件夹，也允许查看该文件夹的属性、所有者和拥有的权限等。  
写入（Write）：允许用户在该文件夹中创建新的文件和子文件夹，也可以改变文件夹的属性、查看文件夹的所有者和权限等。  
  
用户和用户组权限  
Windows用户组  
内置用户组：如管理员组（Administrators）、普通用户组（Users）、备份操作组（Backup Operators）等。这些组根据预设的权限执行任务。  
特殊权限用户：系统还设有如System、TrustedInstaller、Everyone等特殊权限用户，这些用户不属于任何内置用户组，具有独立的权限。  
  
#Linux权限  
uid分配原则  
0：管理员  
1-999：系统内部账号，维护系统服务  
1000-65534：普通账号，可以登录  
  
/etc/passwd文件解读  
root：登录的用户名  
x：登录该用户时是否需要输入密码，x表示需要使用密码，空代表不需要密码  
0：uid，用户ID，系统识别用户的唯一标识  
0：gid，组ID，  
root：用户描述信息，可以自定义  
/root：用户的家目录，存放个人文件，登录该用户时默认进入该目录  
/bin/bash：用户的登录shell，登录系统以后所执行的shell文件，登录此用户时默认打开的shell类型bash shell  
  
/etc/group文件解读  
erik：组名  
x：登录该组时是否需要密码，x表示需要密码，空表示不需要密码  
1000：组ID  
:erik 表示组内的成员erik  
  
某个文件或者目录的权限  
d：表示目录  
-：表示普通文件，二进制文件、文本文件、压缩包等  
l：表示链接文件，快捷方式  
c：表示字符设备，键盘鼠标等设备  
b：表示块设备，存数据的设备  
rwx：表示文件拥有人的权限  
r-x：表示文件拥有组的权限，即为组内用户的权限  
r-x：表示其他人的权限  
2：如果是文件则表示文件硬链接数量；如果是目录则表示该目录下有几个子目录  
root：表示文件的拥有人  
root：表示文件的拥有组  
  
文件的权限  
r：read，查看文件内容  
w：write，编辑文件内容  
x：execute，执行该文件  
  
目录的权限  
r：能够列出目录下面的文件  
w：能够在该目录下创建和删除文件（能否删除文件取决于用户对该文件所在目录的权限）  
x：能进入该目录

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)