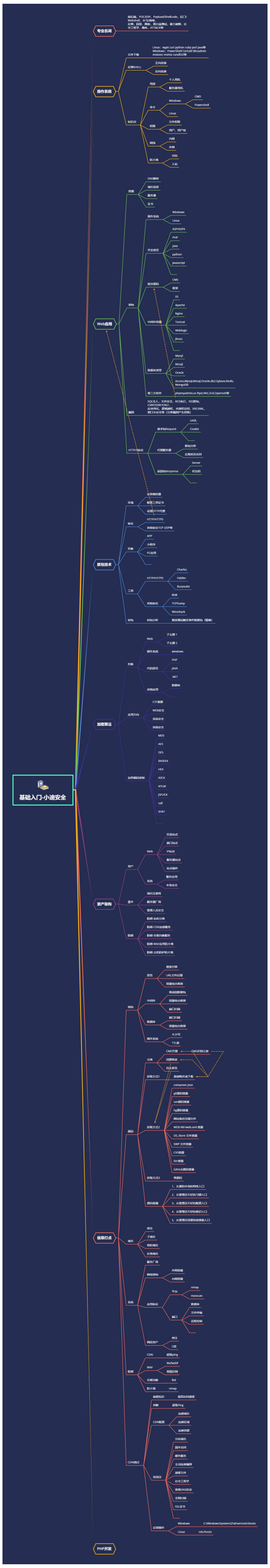
信息打点-CDN 绕过篇&漏洞回链&接口探针&全网扫描&反向邮件



基础入门-小迪安全
专业名词
前后端，POC/EXP，Payload/Shellcode，后门/Webshell，木马/病毒，
反弹，回显，跳板，黑白盒测试，暴力破解，社会工程学，撞库，ATT&CK等
操作系统
文件下载
Linux：wget curl python ruby perl java等
Windows：PowerShell Certutil Bitsadmin msiexec mshta rundll32等
反弹SHELL
正向连接
反向连接
知识点
用途
个人用机
服务器用机
命令
Windows
CMD
Powershell
Linux
权限
文件权限
用户、用户组
网络
内网
外网
防火墙
出站
入站
Web应用
搭建
DNS解析
域名选择
服务器
证书
架构
操作系统
Windows
Linux
开发语言
ASP/ASPX
PHP
java
python
javascript
程序源码
CMS
框架
中间件容器
IIS
Apache
Nginx
Tomcat
Weblogic
Jboos
数据库类型
Mysql
Mssql
Oracle
Access,Mysql,Mssql,Oracle,db2,Sybase,Redis,MongoDB
第三方软件
phpmyadmin,vs-ftpd,VNC,ELK,Openssh等
漏洞
SQL注入，文件安全，RCE执行，XSS跨站，CSRF/SSRF/CRLF，
反序列化，逻辑越权，未授权访问，XXE/XML，
弱口令安全等（分类漏洞产生层面）
HTTP/S协议
请求包Request
UA头
Cookie
代理服务器
抓包分析
实现转发访问
返回包Response
Server
状态码
抓包技术
环境
安装模拟器
配置工具证书
设置HTTP代理
协议
HTTP/HTTPS
其他协议TCP UDP等
对象
APP
小程序
PC应用
工具
HTTP/HTTPS
Charles
Fiddler
Burpsuite
其他协议
科来
TCPDump
Wireshark
封包
封包分析
整体测试触发事件数据包（精确）
加密算法
对象
Web
子主题 1
子主题 2
操作系统
windows
代码语言
PHP
JAVA
.NET
其他应用
数据库
应用方向
CTF赛题
WEB安全
系统安全
其他安全
加密编码进制
MD5
AES
DES
BASE64
HEX
ASCII
NTLM
JSFUCK
salt
SHA1
资产架构
资产
Web
目录站点
端口站点
IP站点
服务器站点
站点插件
系统
服务应用
本身安全
番外
域名注册商
服务器厂商
管理人员安全
阻碍
阻碍-站库分离
阻碍-CDN加速服务
阻碍-负载均衡服务
阻碍-WAF应用防火墙
阻碍-主机防护防火墙
信息打点
架构
语言
搜索引擎
URL文件后缀
搭建组合推算
中间件
看返回数据包
搭建组合推算
端口扫描
数据库
端口扫描
搭建组合推算
操作系统
大小写
TTL值
源码
分类
CMS开源
CMS识别云悉
闭源售卖
自主研发
获取方式1
直接购买或下载
获取方式2
composer.json
git源码泄露
svn源码泄露
hg源码泄漏
网站备份压缩文件
WEB-INF/web.xml 泄露
DS_Store 文件泄露
SWP 文件泄露
CVS泄露
Bzr泄露
GitHub源码泄漏
获取方式3
黑源码
源码泄漏
1、从源码本身的特性入口
2、从管理员不好的习惯入口
3、从管理员不好的配置入口
4、从管理员不好的意识入口
5、从管理员资源信息搜集入口
域名
旁注
子域名
相似域名
反查域名
系统
服务厂商
网络架构
外网搭建
内网搭建
应用协议
平台
nmap
masscan
端口
数据库
文件传输
远程控制
网段资产
旁注
C段
阻碍
CDN
超级ping
WAF
Wafw00f
看图识别
负载均衡
lbd
防火墙
nmap
CDN绕过
前置知识
提高访问速度
判断
超级Ping
CDN配置
加速域名
加速区域
加速资源
技战法
分站域名
国外访问
邮件服务
主动连接漏洞
遗留文件
社会工程学
查看DNS历史
全网扫描
SSL证书
后续操作
Windows
C:\Windows\System32\drivers\etc\hosts
Linux
/etc/hosts
PHP开发

#知识点：
0、CDN 知识-工作原理及阻碍
1、CDN 配置-域名&区域&类型
2、CDN 绕过-靠谱十余种技战法
3、CDN 绑定-HOSTS 绑定指向访问

演示案例：

- 真实应用-CDN 绕过-漏洞&遗留文件
- 真实应用-CDN 绕过-子域名查询操作
- 真实应用-CDN 绕过-接口查询国外访问
- 真实应用-CDN 绕过-主动邮件配合备案
- 真实应用-CDN 绕过-全网扫描 FuckCDN

#前置知识：
1.传统访问：用户访问域名–>解析服务器 IP–>访问目标主机
2.普通 CDN：用户访问域名–>CDN 节点–>真实服务器 IP–>访问目标主机
3.带 WAF 的 CDN：用户访问域名–>CDN 节点（WAF）–>真实服务器 IP–>访问目标主机

#CDN 配置：
配置 1：加速域名-需要启用加速的域名
配置 2：加速区域-需要启用加速的地区
配置 3：加速类型-需要启用加速的资源

#判定标准：
nslookup,各地 ping（出现多个 IP 即启用 CDN 服务）

#参考知识：
https://zhuanlan.zhihu.com/p/33440472
https://www.cnblogs.com/blacksunny/p/5771827.html
子域名，去掉 www，邮件服务器，国外访问，证书查询，APP 抓包
黑暗空间引擎，通过漏洞或泄露获取，扫全网，以量打量，第三方接口查询等

#案例资源：
超级 Ping：https://www.17ce.com/
接口查询：https://get-site-ip.com/
国外请求：https://tools.ipip.net/cdn.php
全网扫描：https://github.com/Tai7sy/fuckcdn

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址