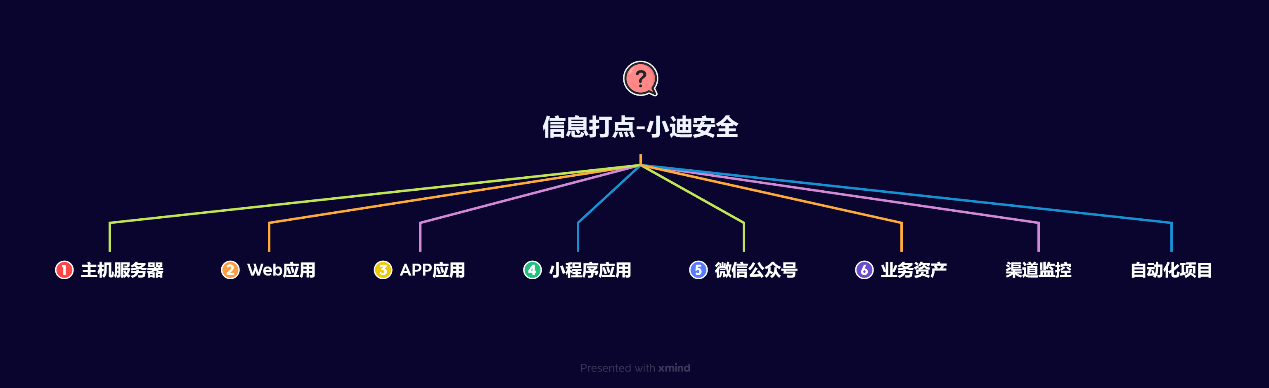
信息收集-项目系统&一键打点&资产侦察&企查产权&空间引擎&风险监测&利器部署



#知识点：  
1、信息收集-服务器系统-操作系统&IP资产  
2、信息收集-服务器系统-端口扫描&服务定性  
---------------------------------------------------  
1、信息收集-Web应用-机构产权&域名相关性  
2、信息收集-Web应用-DNS&证书&枚举子域名  
---------------------------------------------------  
1、信息收集-Web应用-架构分析&指纹识别  
2、信息收集-Web应用-架构分析&WAF&蜜罐  
3、信息收集-Web应用-架构分析&框架组件识别  
---------------------------------------------------  
1、信息收集-Web应用-源码获取-已知指纹&未知指纹  
2、信息收集-Web应用-源码获取-泄漏问题&发现指纹  
---------------------------------------------------  
1、信息收集-Web应用-JS提取分析-人工&插件\*项目  
2、信息收集-Web应用-JS提取分析-URL&配置&逻辑  
---------------------------------------------------  
1、信息收集-Web应用-CDN加速-如何识别  
2、信息收集-Web应用-CDN加速-绕过方法  
---------------------------------------------------  
1、信息收集-Web应用-开发框架-识别安全  
2、信息收集-Web应用-安全组件-特征分析  
---------------------------------------------------  
1、信息收集-APP应用-公开信息-知识产权&开发者定位  
2、信息收集-APP应用-资产信息-抓包&静态提取&动态调试  
---------------------------------------------------  
1、信息收集-小程序应用-公开信息-知识产权&平台搜索  
2、信息收集-小程序应用-资产信息-抓包&提取&动态调试  
---------------------------------------------------  
1、信息收集-项目推荐-自动化环境部署  
2、信息收集-项目推荐-自动化资产收集管理  
  
#章节点：(待补充)  
#具体点：(待补充)

演示案例：

* 自动化-环境部署-F8x
* 自动化-移动资产-ENScan\_Go
* 自动化-网络空间-Yakit&TScanPlus
* 自动化-综合管理-ARL&Nemo&TestNet

#自动化-网络空间-Yakit&TscanPlus  
项目地址：https://www.yaklang.com/  
项目地址：https://github.com/TideSec/TscanPlus  
集成Fofa、Hunter、Quake、Zoomeye、Shodan、censys、VT、0.zone、微步等接口查询  
  
#自动化-企查信息-ENScan  
项目地址：https://github.com/wgpsec/ENScan\_GO  
1、介绍：  
剑指HW/SRC，解决在HW/SRC场景下遇到的各种针对国内企业信息收集难题  
2、配置：  
ENScanGo在第一次使用时需要使用-v命令生成配置文件信息后进行配置  
3、使用：  
见项目文档  
  
#自动化-综合架构-ARL&Nemo&TestNet  
-ARL灯塔  
项目地址1：https://github.com/adysec/ARL（升级版）  
项目地址2：https://github.com/ki9mu/ARL-plus-docker  
1、介绍：  
旨在快速侦察与目标关联的互联网资产，构建基础资产信息库。 协助甲方安全团队或者渗透测试人员有效侦察和检索资产，发现存在的薄弱点和攻击面。  
2、配置：（docker搭建）  
安装环境：Aliyun HK服务器 Ubuntu20.04  
apt update  
apt install unzip wget docker.io docker-compose -y  
cd /opt/  
mkdir docker\_arl  
wget -O docker\_arl/docker.zip https://github.com/ki9mu/ARL-plus-docker/archive/refs/tags/v3.0.1.zip  
cd docker\_arl  
unzip -o docker.zip  
docker volume create arl\_db  
cd ARL-plus-docker-3.0.1  
docker-compose pull  
docker-compose up -d  
3、使用：见直播操作  
  
-Nemo\_Go  
项目地址：https://github.com/hanc00l/nemo\_go  
1、介绍：  
Nemo是用来进行自动化信息收集的一个简单平台，通过集成常用的信息收集工具和技术，实现对内网及互联网资产信息的自动收集，提高隐患排查和渗透测试的工作效率，用Golang完全重构了原Python版本。  
2、配置：（docker搭建）  
安装环境：Aliyun HK服务器 Ubuntu18.04  
https://github.com/hanc00l/nemo\_go/blob/main/docs/docker.md  
下载release的nemo\_linux\_amd64.tar后执行：  
mkdir nemo;tar xvf nemo\_linux\_amd64.tar -C nemo;cd nemo  
docker-compose up -d  
3、使用：见直播操作  
  
-Testnet  
项目地址：https://github.com/testnet0/testnet  
1、介绍：  
TestNet资产管理系统旨在提供全面、高效的互联网资产管理与监控服务，构建详细的资产信息库。 该系统能够帮助企业安全团队或渗透测试人员对目标资产进行深入侦察和分析，提供攻击者视角的持续风险监测，协助用户实时掌握资产动态，识别并修复安全漏洞，从而有效收敛攻击面，提升整体安全防护能力。2、配置：（docker搭建）  
2、配置：（docker搭建）  
安装环境：Aliyun HK服务器 Ubuntu22.04  
git clone https://github.com/testnet0/testnet.git  
cd testnet && bash build.sh  
3、使用：见直播操作  
  
#自动化-武器库部署-F8x  
项目地址：https://github.com/ffffffff0x/f8x  
1、介绍：  
一款红/蓝队环境自动化部署工具,支持多种场景,渗透,开发,代理环境,服务可选项等.  
2、配置：  
通过 CF Workers 下载 [推荐]  
wget : wget -O f8x https://f8x.io/  
curl : curl -o f8x https://f8x.io/  
3、使用：见项目文档

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