安全小课堂第四十九期【网站安全检测之信息收集类工具】

京东安全应急响应中心 2017-03-17

网站安全检测的第一步是最大程度地收集目标系统的信息，这同样也是**网站安全检测**的关键性步骤。信息的收集和分析伴随着**网站安全检测**的每一个步骤。作为有着多年的网络安全经验的资深白帽子平时做渗透测试时会使用哪些信息收集类工具呢？JSRC 安全小课堂第四十九期，我们邀请到了**花开若相惜**、**沦沦**师傅为简单介绍一下他们常用的信息收集类工具。以及 JSRC 白帽子苦逼司马，DragonEgg，wadcl、 iDer、PX1624的讨论。

讲师：花开若相惜

讲师简介：

硬土壳安全CTO，Pax.Mac Team创始人之一，多年渗透测试、安全培训等经验。专注于安全开发、渗透测试、代码审计等领域。

讲师：沦沦

讲师简介：

安全白帽子,某甲方安全研究员，网络尖刀团队核心成员，具备渗透测试、漏洞挖掘等相关经验和技巧。

用于信息收集的工具有哪些?

京安小妹

subDomainsBrute、Layer子域名挖掘机、WebRobot、nmap、wyportma、python和一双勤劳的双手，常用到的东西都会自己会去用python实现自动化。

讲师：沦沦、花开若相惜

白帽子观点：matego

白帽子观点：跟Sublist3r类似，自动从各种搜索引擎搜索域名的子域名

白帽子观点：theharverster

白帽子观点：还有各种指纹识别的工具

白帽子观点：人员安全方面，在QQ群搜索，搜索企业名等，想办法混进去群里有可能有意想不到的发现

如果只能推荐三个工具会推荐哪三个？为什么？

京安小妹

seay写的Layer子域名挖掘机字典跟速度都挺不错，唯一缺点是每次都要打开虚拟机。
chrome插件 shodan ip的各种信息，端口信息 mysql redis等等能不能外连一目了然。
google，你懂的。
subDomainsBrute、WebRobot、nmap，试用了几个域名收集的还是感觉subDomainsBrute进行收集域名更精准一点重复的业务不会太多，WebRobot收集信息比较全面包含（百度、google和必应的搜索抓取、C段查询、域名暴破等）、nmap扫描端口指纹识别是比较好的。

讲师：沦沦、花开若相惜

请分别描述一下这三个工具的常见用法。

京安小妹

Layer子域名挖掘机 输入好域名，点开始，喝杯咖啡等结果。
shodan 点击图标view-hoste-detail 查看详情。
google ： 不会什么搜什么、想要什么搜什么，什么google hacker 域名收集啥的大家都懂。 subDomainsBrute的使用方法很简单在github下载完，直接写入
subDomainsBrute的执行文件都有相关的使用说明，比如：
python subDomainsBrute.py qq.com --full。
WebRobot比较简单看了都懂。
https://pan.baidu.com/s/1jGoxjqI。
nmap都是必备专用相信都会用 。

讲师：沦沦、花开若相惜

这三个工具在使用过程中存在什么问题？如何解决？

京安小妹

在使用过程过确实是有一些不足的地方，比如用subDomainsBrute进行扫描只收集了IP和域名但一些指纹就没进行识别，比如网站的标题和服务还有端口，可以在subDomainsBrute的前提上再进行编写把这几个功能增加上去就更加方便了。

讲师：沦沦、花开若相惜

企业是否有办法防御这三个工具？需要使用什么样的方法？

京安小妹

端口的话可以进行加防火墙规则进行处理，
然后域名的话一般公开到外网早晚都会被收集到最好的办法就是在上线前就进行全面的安全测试通过之后进行上线。

讲师：沦沦、花开若相惜

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂,如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

京东安全团队真诚招聘，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文