

浅谈内网渗透—安全小课堂第二十三期

京东安全应急响应中心 2016-08-19

安全小课堂第二十三期

拿到企业或者公司的内网权限，然后从内网得到最有价值的战果，这就是内网渗透。其危害不言而喻，影响到公司内部代码泄露与重要信息泄露等。各种信息泄漏直接导致的后果是，可以给黑客留下更多的可趁之机，比如再次进入内网，长期控制等。本期我们来聊一聊内网渗透。

本期邀请到
安全白帽子沦沦
360安全专家 Mickey
360安全专家zxx
大家欢迎~



豌豆妹

请问，什么是内网渗透呢？



哆啦A梦

内网渗透就是拿到企业或者公司的内网权限，然后从内网得到最有价值的战果。



豌豆妹

内网渗透中常见的几个问题有哪些呢？

小新



最主要有：1、**防火墙穿透**；2、**木马免杀穿透**；3、**内网信息收集及目标定位**；4、**关于文件下载**。

柴可夫斯基



常见的问题就是，遇到**工作组**一般成功率就很低了，如果是域环境的话，还是有很多技巧可以用的。



豌豆妹

求分享内网渗透测试思路~~

小丸子



进入内网或者拿到服务器权限之后首先我会用nmap或者**IIS PUT Scanner**探测一下内网IP段开放的端口和服务，如果是WEB服务就通过常规的WEB渗透黑入系统，如果是数据库、FTP通地批量爆破弱口令进入（因为**内网都是最薄弱的地方**，而且开发人员的数据库都为了方便，设置为弱口令，一般扫描数据库成功率很大），**ARP欺骗**（这个动作会很大，一般不建议使用）等等。

葫芦娃



我的思路，就是多花费时间摸环境，比如看看域内的管理员有谁，最后登录时间，有

没有home dir里有脚本的，边界服务器都有哪些（那种可以通内网和外网的），然后找立足点，留后门等都做好了，再突破搞内网。扫端口是可以的，先net group找到服务器组（邮件/WEB/），然后扫那个段的常见端口。话说nmap可以命令行下安装，不过win下的nmap不好用呢，linux下比较顺手~nmap很容易引起管理员警觉的，特别是加了scripts。如果是工作组，你可以nbtscan扫下看机器名，或者netscan扫描开放的共享（图形界面）。



豌豆妹

能介绍下内网渗透信息获取途径么？



小新

通过域名暴破、搜索引擎、挖掘公司企业相关网站最终找到突破口、社工企业人员账号或QQ号等相关信息等等。



哆啦A梦

内网获取信息，我分2步。1个是人员，1个是机器，人员如果有domain，通过ldap很好收集，或者找oa系统，或者进入一个员工的邮箱，爬通信录，机器的话，domain也好弄，还是dsquery命令取，或者其他类似的工具。工作组nbtscan，看机器名，有的机器名就是员工名，有的机器名会标出该机器的作用哦~



豌豆妹

推荐几个内网渗透小工具吧。

柴可夫斯基



这方面的小工具有，pstools、hijack、metasploit、nmap、IIS PUT Scanner、mysql与sqlserver弱口令爆破工具（通过python编写）、hydra（SSH爆破工具）、FTPscan（python脚本实现）、Ettercap（嗅探工具）等。

小丸子



win7 以后的我最常用的就 powerview、powerup、PowerEmpire 这些，PowerEmpire建议大家多看看哦，相当棒！



豌豆妹

能说说内网渗透的危害么？

哆啦A梦



危害当然就是影响到公司内部代码泄露与重要信息泄露等等啦~包括代码、数据库、人员、邮件、架构信息等信息都会泄漏，基本上公司裸奔了。可以参照一下hacking team。各种信息泄漏直接导致的后果是，可以给黑客留下更多的可趁之机。比如再次进入内网，长期控制等。



豌豆妹

那有哪些防御手段呢？

柴可夫斯基



防御手段，就是做好VLAN隔离，边界划分，安装有基于行为的入侵检测系统，终端做好防护。vpn/mail这种入口点做好防护，web最好托管到外面的云服务器，少跟内网有联系，把关好内部系统的安全性，定期扫描检查测试。提高人员安全意识培训，尽量少重用密码。wifi也别乱开乱用~公司的文档要DLP哦。加密好，备份好，别的就差不多了。



豌豆妹

好嘞~棒棒哒！谢谢小伙伴们的热烈讨论哟~咱们下期见！



安全小课堂往期回顾：

- 1、论安全响应中心的初衷；
- 2、安全应急响应中心之威胁情报探索；
- 3、论安全漏洞响应机制扩展；
- 4、企业级未授权访问漏洞防御实践；
- 5、浅谈企业SQL注入漏洞的危害与防御；
- 6、信息泄露之配置不当；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；
- 12、远程代码执行漏洞的探讨；
- 13、服务器安全管控的探讨；
- 14、畅谈端口安全配置；
- 15、谈一谈github泄露；
- 16、撞库攻击是场持久战；
- 17、url重定向攻击的探讨；
- 18、聊聊弱口令的危害（一）；
- 19、聊聊弱口令的危害（二）；
- 20、聊聊XML注入攻击；
- 21、聊聊暴力破解；
- 22、谈谈上传漏洞。





京东安全应急响应中心