安全小课堂第135期【RedTeam攻击技巧和安全防御】

JSRC 京东安全应急响应中心 4月1日

红队的起源是出现在军事领域方面，人们意识到，要做到更好的防守，就需要去攻击自己的防御，才能更好的找到防守的弱点。在国内，进攻方为蓝军，防守方为红军。蓝军我自己习惯称为RedTeam，红蓝对抗的意义在于帮助防守者更全面的意识到自己的薄弱之处。

JSRC **安全小课堂第135期**，邀请到**ATTCKWing**师傅就**RedTeam攻击技巧和安全防御**为大家进行分享。同时感谢白帽子们的精彩讨论。

RedTeam是什么?

京安小妹

ATTCKWing:

每个人对RedTeam的理解难免存在差异，但我觉得共同点是一样的——让防御方清楚的意识到自身的不足以及一起改进安全方案。

红队是使用真实的攻击技术来模拟攻击过程，以评估蓝队的安全防御是否做的到位。现在很多公司基本都有自己的安全防护程序和监控系统，软件程序的开发也遵循SDL等等一系列防护措施，但是每逢周五就应急这个梗其实蛮真实，因为新的漏洞总是在不断冒出来，而且你可能被入侵了，权限在别人手里控了几个月，几年，但是你却察觉不到。所以，红队的存在可以说就是为了弥补这些缺陷，我们也要证明自己存在的意义，这里的意义不是说你要挖到多么厉害的漏洞，也不是攻陷了多少系统，而是要发现目标的痛点，同时我们也要敢于挑战所有的目标，无论是人还是系统，都会有漏洞。

讲师

RedTeam常用的攻击手法是?

京安小妹

ATTCKWing:

我认知范围内的 RedTeam常用的攻击手法。第一步，侦察：利用nmap，masscan，EyeWitness，邮箱探测工具等工具对目标执行周期性检查，监控Web Application，github上寻找敏感信息。假设找到一个VPN账号，或者爆破到一个VPN账号，可能就直接杀入内部网络中。这里的爆破账号的技术老毛子叫做Password Sparying，域名监控方面鬼麦子的开源项目或者sublert，以及尝试对目标的云服务商或者云服务进行测试。

相关tools(部分)，url自行查找：

-emailsniper-7kb师傅

-EyeWitness，这个可以自己改进一下

-BloodHound，相关的不同版本fork的分支中有些加了些实用的功能

-x-patrol

-subfinder 建议使用多个工具，然后去重

-ssl

-zoomeye

-ip反查域名等

以及这几天出的根据SSL证书，去监控域名的变化，对喜欢挖src的朋友应该也有帮助。

然后就是**常规的web应用测试**，争取撕开一个口子：

-SQL

-XSS

-File Upload

-SSRF

-RCE

-CMS Vulnerability

-企业代理

-VPN等等

可以参考下Web程序测试指南https://evilwing.me/2018/12/13/web-fuzz/

一般能直接访问的机器都是linux，需要进行详细的信息收集，用户，进程，端口，各种密码，开放服务，是否要进行权限维持等。判断当前位于什么环境中，然后画出拓扑图。DMZ、生产网等等。我在公众号分享过一篇译文， Extracting NTLMHashes from keytab files，linux上也可以设置与域通信，这个keytab文件里面就有hash，它的作用不再赘述。找到立足点后，就到想办法测试内部网络。可能当前用户权限不足，iis权限或者www-data权限。关于windows提权，我有过一篇译文windows提权笔记，应该比较全面。

1. Windows提权笔记

1.1. Windows提权命令参考

1.2. Exploits

1.3. 服务配置错误

1.3.1. 不带引号的服务路径

1.3.2. 不安全的服务权限

1.3.3. 注册表

1.3.4. 不安全的文件系统权限

1.3.5. AlwaysInstallElevated

1.3.6. 组策略首选项漏洞

1.3.7. 凭证窃取(读书人怎么能叫窃呢)

1.3.8. 令牌权限

1.3.9. DLL劫持

1.3.10. 工具和框架

1.3.11. 最后的想法

1.3.12. 参考

1.3.13. END

讲师

RedTeam和Pentesting有什么区别?

京安小妹

ATTCKWing:

其实一开始我觉得渗透和红队好像没什么区别，不就都是为了拿下目标然后写报告么？现在我觉得最大的一个区别就是渗透的范围是有限的，而且大多数情况下基本商业扫描器一把梭就完事，因为你拿到的可能是一大堆目标，但只是单纯的website。红队需要对目标进行尽可能全面的情报收集，要配合蓝队的计划执行，比如：虽然我发给对方的邮件被对方识别到了，也就是说这个行动失败，触发了警报，这里就可以记录下来，它证明了蓝队的防御是有效的。分享一下今天面试官问我的问题：你怎么保证你的邮件能够被对方收到？我说了以下几点：远离黑名单、域名可信度、ip （一个ip发100封邮件很大几率会被系统拦截的）、域名是否有302、 域名是否有有效证书等。

渗透一般是定期的，红队活动有时候几周，有时候几个月，时间不固定。红队的活动是不规律的，有时候可能专注于社工，模拟窃取内部人员信息，在攻击方面对于渗透的话，可能我们去针对内网的时候，想着的时候怎么拿下DC，但是对于红队来说，除非必要，一般不去碰，因为这个动作有点大，除非能保证自己能够不被发现，因为活动中每一步都需要隐藏好自己，不去触发警报，否则SOC或者IDS发现了，就可能功亏一篑。也很少有入侵者直接发动大规模扫描，嗅探等等。我们的目的是什么？ 制造出更完善的安全方案，而不是无意义的攻击。

有时候目标就只是域内的某个开发人员，那么，怎么去判断呢？——DC里面的日志中去寻找，寻找命名规则， zhangsan.pentestlab.com类似这种，至关重要的Email系统，里面可能有大量内部人员信息，内部邮件钓鱼的几率成功率会很高。总之，需要红蓝双方共同配合，一起行动。

讲师

如何在RedTeam活动中隐藏自己?

京安小妹

ATTCKWing:

隐藏自己主要其实就是攻击者本身和我们的C2服务器。前者的话可以通过各种代理来实现，tor，vpn，等后者的话就有很多细节，我只列举我自己用过的技术，其余还有很多。Faction，最近出的，基于web的多人协作平台，dnscat2，支持win和linux，pentestlab的博客有很多，包括以下，ICMP、POWERSHELL、JAVASCRIPT、HTTP、HTTPS、DNS、GMAIL、TWITTER、COM、OFFICE、IMAGES、WMIAND SO ON。还有就是Domain Fronting技术。红队基础建设:隐藏你的C2server，但是蓝队一般会直接禁止合一开始Domain通信，虽然木马还在活动，但是CNAME失败就GG了。以及修改自己的c2工具特征，msf，empire，cs都被安排了。

讲师

BlueTeam如何进行全面的防御呢?

京安小妹

ATTCKWing：

这个是蓝队用来模拟红队攻击的系统。下面就是熟悉的ATT&CK矩阵图。就是当蓝队捕捉到相关的活动时，可以对比图中的技术，并进行标记。有三个平台的矩阵图Windows、Mac、Linux。我们将捕捉到的日志全部发送到splunk，在里面进行特征分析，提取，最后规划防御方案。像powershell有时候直接是被禁用的，你执行我就报警。可以通过.net去调用、跟进最新威胁情报，比如empire，cs，msf等工具的特征都有人公开了，就需要自己去更改相应的特征，防止被追查。TTP的手段是多样化的，需要红蓝双方共同合作才能找出不足，最后完善报告。蓝队需要进行安全审核、风险情报分析、DDOS测试、制定风险方案、PCAP、记录分析。跳跃性思维，红队的主要特点是跳出局限性思考，不断寻求新的工具和技术。深入了解系统，知己知彼，百战不殆。有组织，注重细节。在评估公司或组织的安全性时，你需要创建风险或威胁配置方案。牛x的威胁配置方案包含所有可能包含潜在威胁攻击者和现实威胁情景的数据，通过在前面的准备工作，为未来的任何攻击做好充分准备。强化系统，要真正为即将到来的攻击或破坏做好准备，需要对所有系统进行强化，减少黑客可能利用的攻击面。绝对必要的是强化DNS，因为它是强化策略中最容易被忽视的一个。了解入侵检测系统，熟悉网络方便查找任何异常和可能具有恶意活动的软件应用程序。过滤所有网络流量包，将更好地控制公司系统中的所有网络活动。

讲师

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，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：anquan@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