RemTeam攻击技巧和安全防御

wing / 2019-04-01 09:39:00 / 浏览数 5441 渗透测试 渗透测试 顶(1) 踩(0)

0X00 前言

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

0X01 我所理解的RedTeam

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，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
所以，红队的存在可以说就是为了弥补这些缺陷，我们也要证明我们自己存在的意义，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

0X02 RedTeam And Pentesting ?

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嗦就完事，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
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
我们的目的是为了制定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
- ...and so on

总之，需要红蓝双方共同配合，一起行动。

0X03 RedTeam常用的攻击手法是什么？

侦察

利用nmap，masscan，EyeWitness，邮箱探测工具等对目标执行周期性检查，监控Web
Application，github上寻找敏感信息，架设找到一个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)，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

Web Application

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。
  可以参考一下我翻译的Web程序测试指南

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.

我在公众号分享过一篇译文，Extracting NTLM Hashes from keytab files
linux上也可以设置与域通信，这个keytab文件里面就有hash，它的作用我就不多说了。

ATTACK

找到一个立足点之后，就得想办法攻击网络了。
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

文章目录 站点概览

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

linux下我熟悉的就是内核直接提权，SUID，高权限文件或者文件夹的利用，符号链提权，服务提权等

这里我放一个具体的案例

■■■■■■■■RCE
`https://mp.weixin.qq.com/s?timestamp=1553699733&src=3&ver=1&signature=qNtvRWkWNZ35M9uXeWqVZZgxlzt0w4iTPoag28c5K5GZBeiBwTDblY*g`

Lateral movement

在没有任何凭据的情况下可以考虑WPAD攻击，目的就是抓到hash值，有些系统可能不会验证SMB签名，以及最近看到的无约束委派攻击。

可以看一下我复现一些案例。
一篇域攻击文章的复现
目录：

- Bloodhound
- Kerberoasting攻击 | Tool: GetUserSPNs.py
- ASEPRoasting | tool：Rubeus
- SILENTTRINITY
- 无约束的 Kerberos
- RBCD攻击
- MS14-025，GPP
- 查找权限高的用户|CrackMapExec
- PowerTools
- PowerUp
- Get-ExploitableSystem
- GetSystem

- ADAPE

除了这些还有很多，但是大体上就是这些了。

很多大家都了然于心，不必过多赘述。

我们要明确目标是什么，尽量在每台机器上搜集好必要的信息，留着后用。

linux下的横向移动，做好代理，进行资产探测常规的手法。

免杀

现在的防御机制越来越严格，常规的木马被杀的体无完肤，简单的说一下常规的免杀方法，我在圈子也分享过不下10篇Bypass AV的文章了。
以AMSI为例：

- 尝试禁用AMSI
- 定位AMSI查杀的是哪一行代码，加以混淆
- 白名单绕过
- 自己定制对应工具
- 重新编译msf payload
- 写自己的加载器
- sharpshooter
- psh混淆
- NoPowershell
- battoexe，不加upx壳
- 将恶意代码放到bmp中，再调用powershell下载，再将powershell加密放到hta，hta放入html中。
- ...

社工

现在的钓鱼都是比较高级，最有特点的就是双因子钓鱼，你完全不知道自己已经上钩了。
我还是照样用一个栗子说明。
Red Team Techniques-通过钓鱼攻击获得访问权限

物理攻击

badusb，dropbox，WIFI，等等，快捷而有效。

权限维持

我推荐个ppt，有兴趣的自行参阅

总之，猥琐至上。

0X04 如何隐藏自己

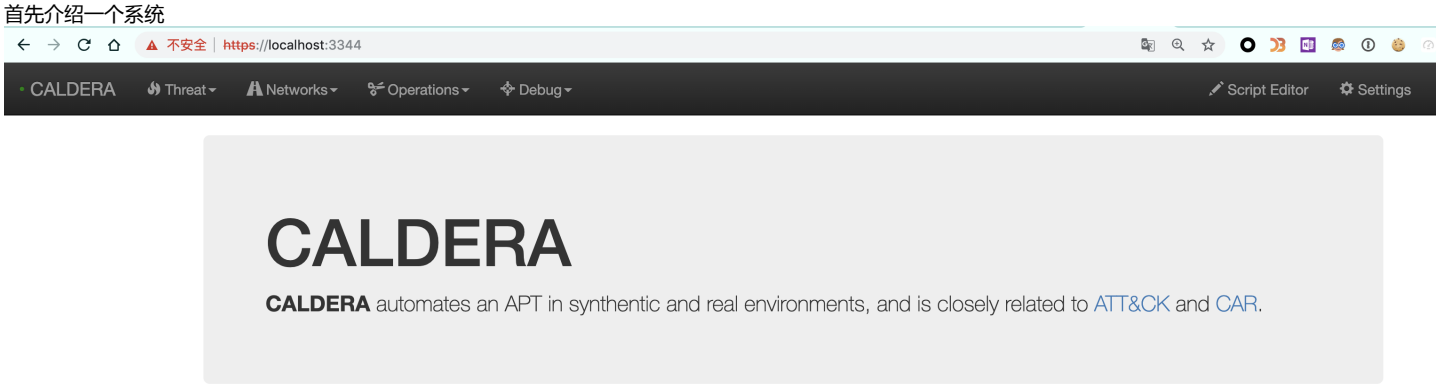
隐藏自己主要其实就是攻击者本身和我们的C2服务器。
前者的话可以通过代理或者肉鸡来实现。
后者的话就有很多细节
我只列举我自己用过的技术，其余还有很多。

- 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
  - WMI
  - AND SO ON
    还有就是Domain Fronting技术，这个就这样叫吧，翻译我找不到合适的词。
    上次和lz1y讨论的时候有适用于国内的方法。
    [红队基础建设:隐藏你的C2 server]
    也可以找倾旋老哥讨论，他在OWASP大会上分享过email c2的思路。

以及修改自己的c2工具特征，msf，empire，cs都被安排了。

0X05 Blue Team如何全面的防御

首先介绍一个系统

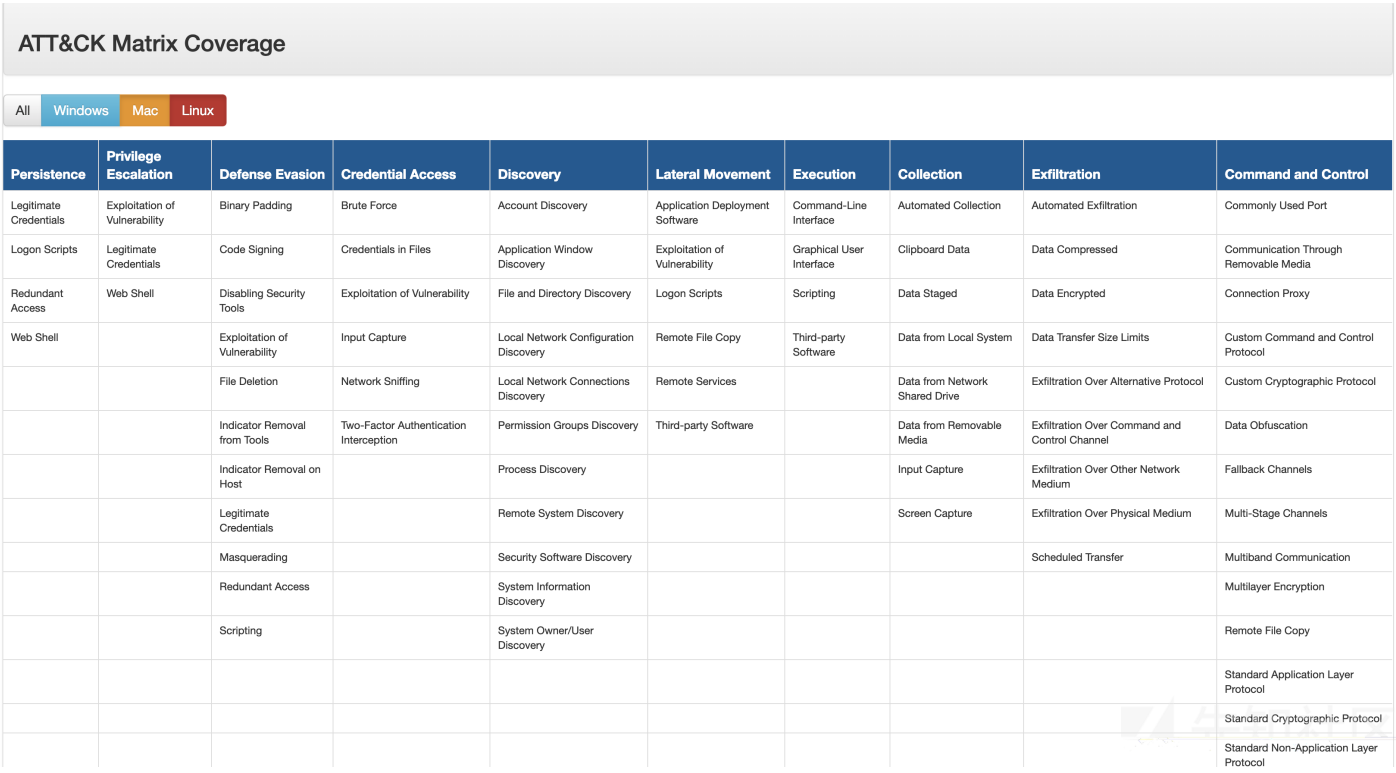


这个是蓝队用来模拟红队攻击的系统。
下面就是熟悉的ATT&CK矩阵图。
就是当蓝队捕捉到相关的活动时，可以对比图中的技术，并进行标记。
有三个平台的矩阵图
Windows

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Automated Collection	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Dumping	File and Directory Discovery	Logon Scripts	Graphical User Interface	Clipboard Data	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation
Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels
DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Email Collection	Exfiltration Over Physical Medium	Multi-Stage Channels
Hypervisor	New Service	Disabling Security Tools		Process Discovery	Replication Through Removable Media	Rundll32	Input Capture	Scheduled Transfer	Multiband Communication
Legitimate Credentials	Path Interception	Exploitation of Vulnerability		Query Registry	Shared Webroot	Scheduled Task	Screen Capture		Multilayer Encryption
Local Port Monitor	Scheduled Task	File Deletion		Remote System Discovery	Taint Shared Content	Scripting	Video Capture		Remote File Copy
Logon Scripts	Service File Permissions Weakness	File System Logical Offsets		Security Software Discovery	Third-party Software	Service Execution			Standard Application Layer Protocol
Modify Existing Service	Service Registry Permissions Weakness	Indicator Blocking		System Information Discovery	Windows Admin Shares	Third-party Software			Standard Cryptographic Protocol
New Service	Web Shell	Indicator Removal from Tools		System Owner/User Discovery	Windows Remote Management	Trusted Developer Utilities			Standard Non-Application Layer Protocol
Path Interception		Indicator Removal on Host		System Service Discovery		Windows Management Instrumentation			Uncommonly Used Port
Redundant Access		InstallUtil		System Time Discovery		Windows Remote Management			Web Service

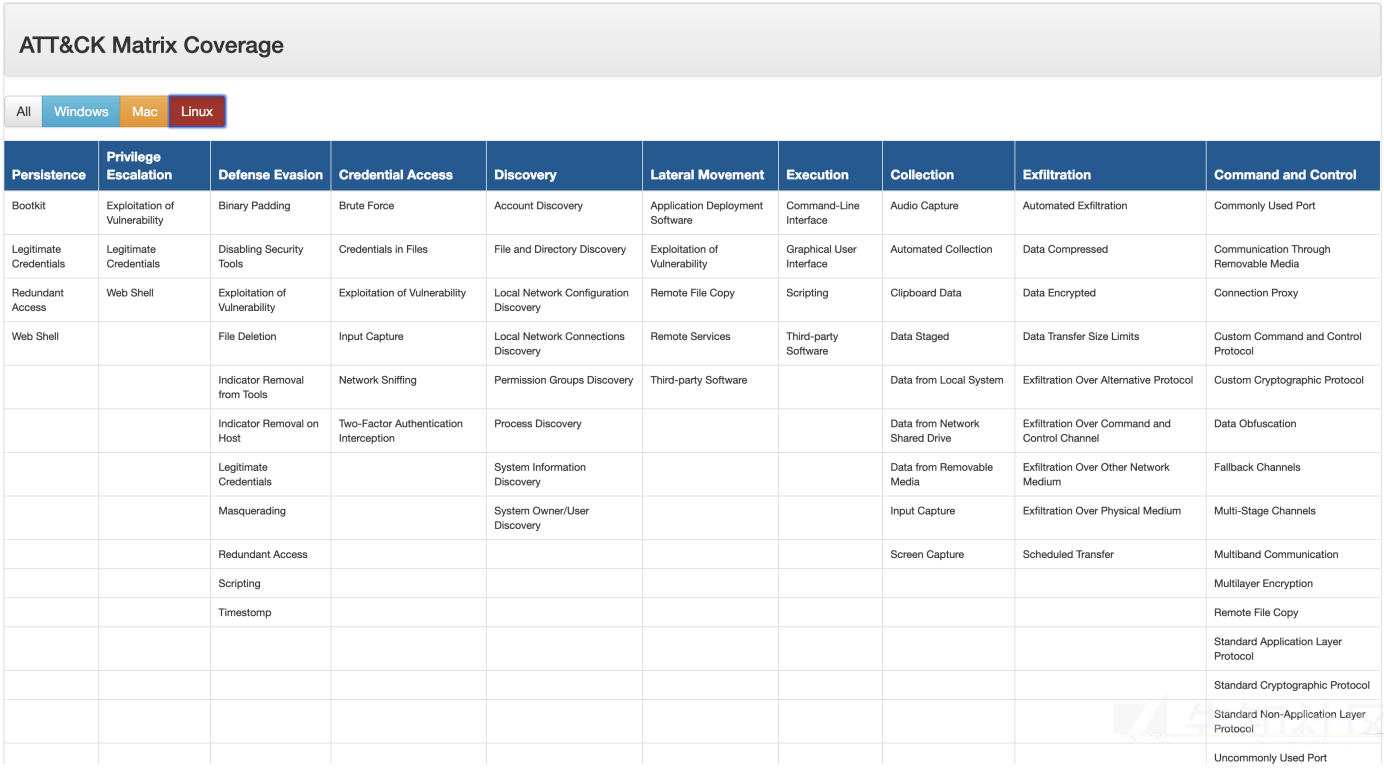
https://localhost:3344/#steps?techniques=5c9a04747fd5a200105a4e83

Mac



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Legitimate Credentials	Exploitation of Vulnerability	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Logon Scripts	Legitimate Credentials	Code Signing	Credentials in Files	Application Window Discovery	Exploitation of Vulnerability	Graphical User Interface	Clipboard Data	Data Compressed	Communication Through Removable Media
Redundant Access	Web Shell	Disabling Security Tools	Exploitation of Vulnerability	File and Directory Discovery	Logon Scripts	Scripting	Data Staged	Data Encrypted	Connection Proxy
Web Shell		Exploitation of Vulnerability	Input Capture	Local Network Configuration Discovery	Remote File Copy	Third-party Software	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
		File Deletion	Network Sniffing	Local Network Connections Discovery	Remote Services		Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
		Indicator Removal from Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Third-party Software		Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
		Indicator Removal on Host		Process Discovery			Input Capture	Exfiltration Over Other Network Medium	Fallback Channels
		Legitimate Credentials		Remote System Discovery			Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
		Masquerading		Security Software Discovery				Scheduled Transfer	Multiband Communication
		Redundant Access		System Information Discovery					Multilayer Encryption
		Scripting		System Owner/User Discovery					Remote File Copy
									Standard Application Layer Protocol
									Standard Cryptographic Protocol
									Standard Non-Application Layer Protocol

Linux



ATT&CK Matrix Coverage

All | Windows | Mac | Linux

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Bootkit	Exploitation of Vulnerability	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials	Legitimate Credentials	Disabling Security Tools	Credentials in Files	File and Directory Discovery	Exploitation of Vulnerability	Graphical User Interface	Automated Collection	Data Compressed	Communication Through Removable Media
Redundant Access	Web Shell	Exploitation of Vulnerability	Exploitation of Vulnerability	Local Network Configuration Discovery	Remote File Copy	Scripting	Clipboard Data	Data Encrypted	Connection Proxy
Web Shell		File Deletion	Input Capture	Local Network Connections Discovery	Remote Services	Third-party Software	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
		Indicator Removal from Tools	Network Sniffing	Permission Groups Discovery	Third-party Software		Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
		Indicator Removal on Host	Two-Factor Authentication Interception	Process Discovery			Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation
		Legitimate Credentials		System Information Discovery			Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels
		Masquerading		System Owner/User Discovery			Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
		Redundant Access					Screen Capture	Scheduled Transfer	Multiband Communication
		Scripting							Multilayer Encryption
		Timestomp							Remote File Copy
									Standard Application Layer Protocol
									Standard Cryptographic Protocol
									Standard Non-Application Layer Protocol
									Uncommonly Used Port

在这里面你可以创建对手，并配置它要进行哪些操作，好处是什么？
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。
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

上次看到的红蓝技能排行

RedTeam
进入攻击者的海洋并尽可能地发挥你的创造力

- 跳跃性思维，猪猪侠跟我说的猥琐
  - 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
- Program开发能力
  - 定制测试工具
- pentesting，也是重要的一部分
- 社工

BlueTeam
你将不得着承担这大多数人不知道的后门和漏洞

- 有组织，注重细节
- 网络安全分析和威胁概况
  - 在评估公司或组织的安全性时，您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
- 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。

- SIEM
  - SIEM或安全信息和事件管理是提供安全事件实时分析的软件。它从外部源收集数据，能够根据特定的标准执行数据分析。

总结

大家可能会认为，当涉及到红队或蓝队时，你可能会偏向另一个团队，但事实是，只有两个团队一起合作，才能为任何网络攻击准备一个完整有效的安全基础设施方案。

整个网络安全行业需要更多地去了解如何让两个团队一起工作并相互学习。有些人可能称之为紫队，Whatever，红队和蓝队的完美协作是真正彻底实现网络安全的唯一途径

上一篇：TeaserCONFidence ... 下一篇：OSINT Primer：人员（第...

1. 2 条回复

systemkid 2019-04-01 10:14:16

您公众号的那篇译文Extracting NTLM Hashes from keytab files，链接有问题。
这里帮您补一下。https://mp.weixin.qq.com/s/ItAJXzpBw_cbmVIYRH0v-g

0 回复Ta

wing 2019-04-01 17:21:28

@systemkid 谢谢师傅，没注意是临时链接

0 回复Ta
