ATT&CK框架

就我的理解而言：

从宏观的角度来看，该框架制定了红队的攻击战术，并针对每个攻击的战术规定或者是整理了需要用到的技术，并针对这些技术如何运用、用到了哪些工具等详细过程展开说明，同时针对红队的专业术语做了明确的规定，能够方便红队与蓝队等安全相关方交流时使用同一套专业术语。

从微观的角度也就是个人角度，该框架实际上是指明了红队人员的学习路线，个人可以针对某个具体的攻击环节补充、构建自己的知识体系。

该框架为每个战术、技术、子技术分配了ID

战术使用TA开头，技术使用T开头，子技术为在技术后衔接.XXX，缓解措施使用M开头，攻击组织用G开头，使用的软件用S开头。

战术-攻击路线

攻击路线分为了14个战术

分别为

侦察-->资源开发-->初始访问-->执行-->持久化-->权限提升-->防御规避-->凭据访问-->发现-->横向移动-->搜集-->命令与控制-->渗透-->影响

战术介绍

TA0043 Reconnaissance 侦察

侦察包括主动或被动的信息搜集技术，这些信息可用于支持针对特定目标的攻击，包括攻击目标的组织、基础设施或工作人员等详细信息。攻击者利用这些信息来帮助完成攻击链周期的其他阶段，例如使用收集的信息来规划和执行初始访问，确定目标沦陷后攻击的范围和优先级，或者推动和指导进一步的侦察工作。

****TA0042 Resource Development 资源开发****

资源开发包括创建、购买或窃取目标的支持资源（例如基础设施、帐户和功能）。这些资源可被攻击者用于协助整个攻击链生命周期的其他阶段，比如使用购买的域来进行命令与控制，使用电子邮件帐户作为初始访问的一部分进行网络钓鱼，或者窃取代码签名证书来进行防御规避。

TA0001 Initial Access 初始访问

初始访问指使用各种访问向量在网络中获得初始立足点的技术，如针对性鱼叉式钓鱼攻击和W公共Web站点漏洞利用。通过初始访问获得的立足点可通过有效帐户和远程服务继续访问，但也可能由于密码遭到更改而被限制。

****TA0002 Execution 执行****

执行由可以在本地或远程系统上运行从而达到控制效果的代码和技术组成。这一技术往往和其他战术结合在一起，以实现更广泛的目标，如探索网络或凭据窃取。例如，攻击者可以通过远程访问工具执行PowerShell脚本以进行远程主机发现。

****TA0003 Persistence 持久化****

持久化由用于维持访问的技术组成，这些技术可以在重启、凭据更改或其他可能导致访问中断的情况下维持对系统的访问。持久化技术包括任何访问、操作或配置更改，这些更改可以使它们在系统上保持立足点，例如替换或劫持合法代码或者添加启动代码。

****TA0004 Privilege Escalation 权限提升****

权限提升指在系统或网络中获取更高权限的攻击技术，攻击者常常通过低权限方式渗透进入网络，但往往在实现下一目标时需要更高权限。常见的提权方法包括利用系统弱点或配置错误以及系统漏洞，一种权限提升的例子为： 系统/root权限<-本地管理员权限<-拥有管理员功能的用户账户<-用户账户，访问特定系统或执行特殊功能往往与持久化技术相重叠，因为持久化技术往往需要更高的执行权限。

****TA0005 Defense Evasion 防御规避****

防御规避指在沦陷目标设备过程中用来规避防御检测的技术，用于防御规避的技术包括卸载/禁用安全软件和混淆/加密数据和脚本。攻击者也可以利用可信进程来隐藏和伪装他们的恶意程序，此战术中也交叉罗列出了一些其他战术中具有规避防御效果的技术。

****TA0006 Credential Access 凭据访问****

凭证访问指窃取帐户名和密码等凭证的技术。此类技术包括击键记录和凭据转储。攻击者使用合法凭据可以进入系统，并更难以被发现，同时也有了创建更多帐户的机会，以帮助实现进一步的目标。

****TA0007 Discovery 发现****

发现指攻击者用于获取系统及内部网络相关信息的技术，这些技术可以帮助攻击者观察环境，并决定攻击行动的具体方向。通过这一战术，攻击者可以知道哪些设备可被控制，以及哪些访问点可被用于针对当前的攻击目标。一些操作系统自带工具常被用于这一环节以获取目标信息。

****TA0008 Lateral Movement 横向移动****

横向移动指攻击者进入并控制网络上远程系统的技术。攻击者为了获取其主要的攻击目标，往往需要搜索网络以发现目标，并最终实现访问，为了达到这一目的，通常需要访问多个系统和账户。攻击者可以安装自己的远程访问工具来完成横向移动，或者使用更隐秘的网络和操作系统自带工具。

****TA0009 Collection 搜集****

搜集指攻击者用于收集攻击目标相关数据信息的技术。通常，搜集数据后的下一个目标就是进行窃取。常见的数据来源包括各种驱动类型、浏览器、音频、视频和电子邮件，常见收集方法包括屏幕捕获和击键记录。

****TA0011 Command and Control 命令与控制****

命令和控制包含攻击者与受害者网络中被控系统通信的技术。攻击者通常试图模拟正常的、预期的流量以避免被发现。根据受害者的网络结构和防御的不同，攻击者可以建立不同隐蔽级别的命令与控制信道。

****TA0010 Exfiltration 渗漏****

渗漏指各种从网络中窃取数据的技术。在攻击者完成数据搜集后，往往会将其打包移动以规避检测，这包含了压缩与加密两方面。典型的从目标网络中窃取数据的技术例如通过C&C信道或其他信道传输数据，以及在传输过程中对大小进行限制。

****TA0040 Impact 影响****

通过操纵业务和操作流程来破坏可用性完整性，包括数据损毁和干扰技术。在某些情况下，业务流程看起来很好，但可能已经遭到了更改，以有利于攻击者达成目标，这些技术可被攻击者于实现其最终目的或为破坏机密性提供掩护。

侦察-技术