网络攻防战术科普之 ATT&CK MITRE 篇

ATT&CK MITRE 框架即对抗战术、技术和常识，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。常见的应用场景主要有网络红蓝对抗模拟、网络安全渗透测试、网络防御差距评估、网络威胁情报收集等。

一．ATT&CK 框架可以理解为一个红队或者攻击者在攻击一个目标系统，他所用到的技术路径。

1）比如首先通过钓鱼邮件发送一个附件，客户端那边去执行，通过钓鱼来实现持久化和权限提升；

2）窃取目标系统的账号和密码，通过网络环境发现、横向移动，来对整个网络实现漫游

3）最后窃取对方的网络数据。

二．MITRE 的 ATT&CK 框架基础元素为战术、技术和程序，也就是 TTPs

1）战术： 回答了攻击者想要实现的目标；

2）技术或子技术： 展示了攻击者实际的攻击方式以及目标如何实现；

3）程序框架： 解决了威胁行为者与攻击组织为达到目标所使用技术的特定应用。

在渗透测试中，渗透测试人员可以根据 ATT&CK 中的高频技术对需求方企业进行安全测试，形成安全方案，以加固企业的安全性；在红蓝对抗中，无论是蓝方还是红方都可以使用 ATT&CK 框架，红方可以进行网络钓鱼、水坑攻击等技术，蓝方可以利用框架中的技术提前对系统网站做审计和防护工作。

三．ATT&CK 攻击矩阵框架

攻击矩阵框架如下图所示，作战行动不要求使用所有战术，战术也没有先后顺序，战术的数量和顺序可自行定义。

战术仅为作战行动提供目标纲领，具体行动由战术中的技术与子技术实现。

序号	战术	战术功能
1	侦察	攻击方收集信息，以便未来的行动。包含主动和被动地搜集侦察技术。此类信息一般包含受害者组织、基础设施或人员
2	资源开发	建立攻击者行动所需资源，包含基础设施、攻击人员创建、购买/窃取用于支持目标定位的资源技术。
3	初始访问	攻击方试图进入目标网络，获取一个入口
4	执行	运行恶意代码
5	持久化	保持攻击立足点，获得永久的控制能力
6	权限提升	获取最高权限
7	防御绕过	避免被发现
8	凭证获取	窃取账号、密码、凭证等
9	发现	弄清对方网络环境
10	横向移动	内网漫游，攻击其他网络
11	搜集	收集感兴趣的数据
12	命令控制	试图与目标网络通信，操纵目标系统和网络
13	数据渗出	窃取数据并输出
14	影响	中断和破坏对手网络和数据，给对方网络造成伤害

四．ATT&CK 攻击模拟场景实战

1.攻击模拟背景

攻击者首先是对被攻击者感兴趣的一个事件发送钓鱼邮件，payload 是一个 zip 文件，其中包含一个诱饵 PDF 文档和一个恶意可执行文件，该恶意文件在使用系统上已经安装的 PDF 阅读器来进行伪装。

运行时，可执行文件将下载第二阶段使用的远程访问工具有效负荷，让远程操作人员访问受害计算机，并可让远程操作人员在网络中获得一个初始访问点，然后攻击者会生成用于“命令控制”的新域名，并定期更改自己的网络用户名，将这些域发送到受感染的远程 RAT 上，用于“命令控制”的域和 IP 地址是临时的，并且攻击者每隔几天都会对此进行更改。

2.攻击模拟流程

确定目标-搜集数据-过程分析-构建场景-模拟威胁-调查攻击-评估表现

3.场景示例

假设在 windows 操作环境中，红队采用的工具提供了一个访问点和 C2 通道，攻击者通过交互式 shell 命令与系统进行交互，蓝队已部署 sysmon 作为探针，对过程进行持续监控并搜集数据，此场景的目标是是基于 sysmon 从网络端点中搜集数据来检测红队的入侵行为。

详细场景：

(1)模拟攻击者通过白队提供的初始访问权限后，获得”执行”权限

ATT&CK 战术	技术
命令与控制	标准应用层协议
命令与控制	常用端口
命令与控制	远程文件拷贝

(2)通过命令行界面执行“执行”战术

ATT&CK 战术	技术	工具/命令
发现	账户发现	Netlocalgroup administrator
发现	文件与目录发现	Dir /cd
发现	进程发现	Tasklist /v
发现	远程系统发现	Net view
……	……	……

(3)获得足够信息后，根据需要自由执行其他战术，获得足够权限后，使用 mimikatz 转储凭据，或尝试使用键盘记录器获取凭据，捕获的用户输入信息

ATT&CK 战术	技术
持久化	新服务
提升权限/防御绕过	绕过用户 UAC 控制权限
凭据访问	凭据转储
凭据访问	输入捕获

(4)如果获得了凭据并且通过“发现”技术对系统有了全面的了解，就可以尝试横向移动来实现该方案的主要目标

ATT&CK 战术	技术	工具/命令
横向移动	Windows amdin 共享	/user:<domain>/<account>
横向移动	远程文件拷贝	Copy<file>
执行	服务执行	psexec

(5)根据需要继续使用横向移动等技术，获取并渗透目标敏感信息

ATT&CK 战术	技术
搜集	本地系统数据
搜集	网络共享驱动中的数据
渗透	数据加密
渗透	通过命令与控制渠道渗透

五.模拟威胁

让红队模拟威胁行为并执行白队确定的战术，在攻击模拟作战中，可以让场景的开发人员来验证网络防御的有效性，红队则需要专注于红队入侵之后的攻击行为。通过给定网络环境中特定网络系统上的远程访问工具访问企业网络，此访问权限可以加快评估速度，并确保充分测试入侵后的防御措施。

ATT&CK MITRE 可用于红蓝对抗和恶意代码分析，一定程度上能够提升企业的综合防御能力，同时也能模拟真实环境下的各种黑客攻击行为，为企业风险控制提供有力支撑。