[网络安全提高篇] 一一三.Powershell恶意代码检测 (1)论文总结及抽象语法树（AST）提取

原创

Eastmount 已于 2022-03-11 21:10:53 修改 8724 收藏 15

分类专栏： 网络安全自学篇 文章标签： web安全 APT Powershell 恶意代码检测 论文总结
于 2022-03-11 11:58:56 首次发布

“网络安全提高班”新的100篇文章即将开启，包括Web渗透、内网渗透、靶场搭建、CVE复现、攻击溯源、实战及CTF总结，它将更加聚焦，更加深入，也是作者的慢慢成长史。换专业确实挺难的，Web渗透也是块硬骨头，但我也试试，看看自己未来四年究竟能将它学到什么程度，漫漫长征路，偏向虎山行。享受过程，一起加油~

前文介绍作者2020年参加清华大学、Coremail、奇安信DataCon举办的比赛，主要是关于钓鱼和异常邮件识别研究。这篇文章将详细讲解PowerShell、Powershell恶意代码检测总结及抽象语法树（AST）提取。希望这篇文章对您有帮助，也推荐大家去阅读论文，且看且珍惜。

文章目录