

[网络安全自学篇] 六十七.WannaCry勒索病毒复现及分析

(一) Python利用永恒之蓝及Win7勒索加密

原创

Eastmount 于 2020-04-14 01:54:12 发布 9585 收藏 27

分类专栏: [网络安全自学篇](#) 文章标签: [网络安全](#) [WannaCry](#) [永恒之蓝](#) [漏洞复现](#) [安全防御](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Eastmount/article/details/105407843>

版权

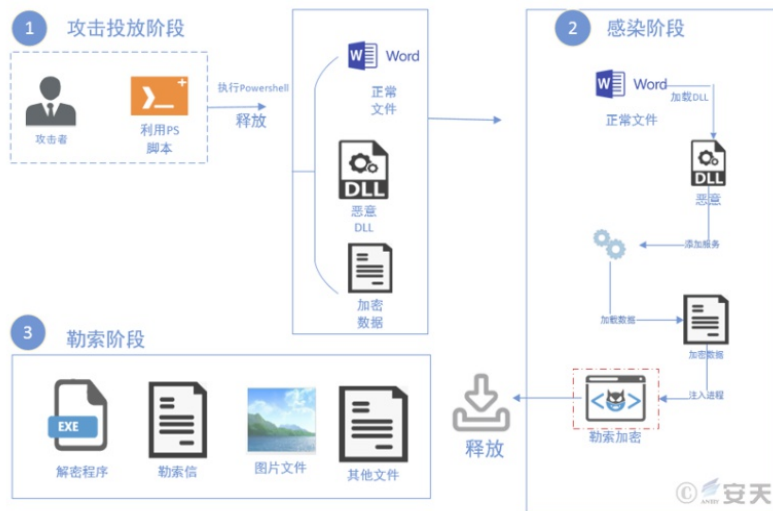


[网络安全自学篇](#) 专栏收录该内容

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏

这是作者的网络安全自学教程系列, 主要是关于安全工具和实践操作的在线笔记, 特分享出来与博友们学习, 希望您们喜欢, 一起进步。前文分享了Vulnhub靶机渗透的DC-1题目, 通过信息收集、CMS漏洞搜索、Drupal漏洞利用、Metasploit反弹shell、提权及数据库爆破获取flag。这篇文章将分享新知识, 最近WannaRen勒索软件爆发(下图是安天的分析攻击流程), 其名称和功能与WannaCry相似, 所以接下来作者将连续分享WannaCry勒索病毒的复现及分析, 第一篇文章将采用Github资源实现永恒之蓝漏洞利用及Windows7系统文件加密。希望这篇基础性文章对您有所帮助。



作者作为网络安全的小白, 分享一些自学基础教程给大家, 主要是关于安全工具和实践操作的在线笔记, 希望您们喜欢。同时, 更希望您能与我一起操作和进步, 后续将深入学习网络安全和系统安全知识并分享相关实验。总之, 希望该系列文章对博友有所帮助, 写文不易, 大神们不喜勿喷, 谢谢! 如果文章对您有帮助, 将是我创作的最大动力, 点赞、评论、私聊均可, 一起加油喔

文章目录

一.WannaCry背景

二.实验环境搭建

1.安装Win7系统和Win server 2003系统