[网络安全自学篇] 六十五.Vulnhub靶机渗透之环境搭建及JIS-CTF入门和蚁剑提权示例（一）

原创

Eastmount 于 2020-04-10 19:31:23 发布 6834 收藏 38

分类专栏： 网络安全自学篇 文章标签： Web渗透 Vulnhub靶场 JIS-CTF 提权 网络安全

本文链接：https://blog.csdn.net/Eastmount/article/details/105423490

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SMBv3服务远程代码执行漏洞（CVE-2020-0796），攻击者可能利用此漏洞远程无需用户验证，执行恶意代码并获取机器的完全控制。本文将详细讲解Vulnhub靶机渗透的环境搭建和JIS-CTF题目，采用Nmap、Dirb、中国蚁剑、敏感文件分析、SSH远程连接、Shell提权等获取5个flag。由于hack the box速度堪忧，作者选择了Vulnhub靶场，希望深入分析来帮助初学者。本文是一篇Web渗透的基础性文章，希望对您有所帮助。

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