基于 Kali Linux 的网络渗透技术研究

摘 要

这个时代，信息网络飞速发展，如何确保我们的网络信息安全，使信息网络得以正常工作，是我们必须要解决的问题，网络渗透技术随之出现。渗透测试是从事网络安全工作的人员在网络安全方面使用的一种新型攻防技术，Kali Linux 作为网络安全工作人员和黑客最常用的系统平台，它集成了非常多的用于渗透测试工作的软件和工具。本文的网络渗透技术研究就是基于此平台来进行的。

本文使用 VMware Workstation 12 搭建模拟网络环境，创建了 Kali Linux 虚拟机来充当攻击机，创建了 windows 7 虚拟机充当靶机。首先在 Kali Linux 系统平台上使用自带的 Nessus 扫描工具对我们的 windows 7 靶机进行漏洞扫描，通过扫描来收集漏洞信息，找到需要用来攻击的漏洞。本次攻击的是 windows 7 系统一个非常典型的漏洞——ms17-010，也叫做永恒之蓝。然后使用 Metasploit（msf）对扫描到的漏洞 ms17-010 进行渗透攻击，获取靶机的主机权限，完成渗透测试。

关键字：Kali Linux；渗透测试；Nessus；Metasploit

Abstract

In this era, with the rapid development of information network, how to ensure our network information security and make the information network work normally is a problem we must solve, and network penetration technology appears. Penetration test is a new attack and defense technology used by network security personnel. Kali Linux, as the most commonly used system platform for network security personnel and hackers, integrates a lot of software and tools for penetration test. The research of network penetration technology in this paper is based on this platform.

In this paper, VMware Workstation 12 is used to build a simulated network environment, Kali Linux virtual machine is created to act as an attack machine, and windows 7 virtual machine is created to act as a target machine. First, use Nessus scanning tool in Kali Linux platform to scan the vulnerability of Windows 7 target, collect the vulnerability information through scanning, and find the vulnerability that needs to be used for attack. This attack is a very typical vulnerability of Windows 7 system - ms17-010, also known as eternal blue. Then use Metasploit (MSF) to attack the vulnerability ms17-010, obtain the host permission of the target machine, and complete the penetration test.

Keywords: Kali Linux; penetration testing; Nessus; Metasploit

目 录