第2章作业

姓名：袁昊男 学号：2018091618008

1、请描述远程主动攻击模式和远程被动攻击模式之间的区别，并列出目前典型的漏洞CVE编号和攻击实例。

**答：**远程主动攻击模式：若目标主机上的某个网络程序存在漏洞，则攻击者可能通过利用该漏洞获得目标主机的访问或控制权。远程被动攻击模式：当一个用户访问网络上的一台恶意主机，就可能遭到目标主机发动的针对性恶意攻击。它们之间的区别是，远程主动攻击模式对攻击者来说是主动的，其利用已存在的网络程序漏洞来攻击目标主机，而远程被动攻击模式对被攻击者来说是主动的，其主动访问一台恶意主机，从而导致可能被其攻击。

|  |  |
| --- | --- |
| **漏洞CVE编号** | **攻击实例** |
| CVE-2009-2496 | 堆损耗远程代码执行漏洞，又称作“Office Web 组件堆损耗漏洞” |
| CVE-2016-7279 | Microsoft Internet Explorer/Edge远程内存破坏漏洞 |
| CVE-2016-7855 | Adobe Flash Player 释放后重利用远程代码执行漏洞 |
| CVE-2018-8174 | 利用浏览器0day漏洞的新型Office文档攻击 |

2、请查阅并列举微软公布的其对Windows安全漏洞的分类和处理方式。

**答：**微软首次向安全研究界公开发布了两份文件，详细介绍了其对Windows安全漏洞的分类和处理方式。

第一个文件是名为“微软的Windows安全服务标准”的网页。该页面涵盖的主要信息包括：哪些类型的Windows功能通常通过紧急的“周二补丁日”（Patch Tuesday）提供安全更新服务，以及哪些漏洞留给Windows主开发团队修复并在一年两次（bi-annual）的Windows操作系统更新中推出。该文件将所有内容分为3大类：安全边界、安全功能以及深度防御安全功能。

1. 安全边界（9个）：网络、内核、进程、AppContainer沙箱、用户、会话、Web浏览器、虚拟机以及虚拟安全模式边界。
2. 安全功能：BitLocker、Windows Defender、Secure Boot等。
3. 深度防御安全功能：用户帐户控制（UAC）功能、AppLocker、地址空间布局随机化（ASLR）、控制流保护（CFG）等。

第二份文件是一个PDF文档，该文档描述了微软如何将错误报告按严重性分级排名。该文档详细说明了哪些错误被评为严重、哪些被评为重要、哪些被评为中等以及哪些被评为低风险。例如，允许未经授权访问文件系统并在磁盘上写入数据的错误被列为严重漏洞，而仅仅重启应用程序的拒绝服务错误就始终被视为低风险漏洞。

3、请从分配方式、使用情况以及释放方式等方面来对比分析堆和栈的区别。

答：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据结构 | 分配方式 | 使用情况 | 释放方式 |
| 栈 | 编译器自动分配，存放函数的参数值，局部变量的值等，其操作方式类似于数据结构的栈。 | 在 Windows 下，栈是向低地址扩展的数据结构，是一块连续的内存区域，栈顶的地址和栈的最大容量是系统预先规定好的，能从栈获得的空间较小。 | 编译器自动释放。 |
| 堆 | 一般是由程序员分配释放，若程序员不释放的话，程序结束时可能由OS回收，值得注意的是他与数据结构的堆是两回事，分配方式倒是类似于数据结构的链表。 | 堆是向高地址扩展的数据结构，是不连续的内存区域，这是由于系统是由链表在存储空闲内存地址，自然堆就是不连续的内存区域，且链表的遍历也是从低地址向高地址遍历的，堆得大小受限于计算机系统的有效虚拟内存空间，由此空间，堆获得的空间比较灵活，也比较大。 | 由程序员自己负责使用内存释放函数（如 free 函数）来释放。 |

4、什么是SQL注入，其本质原因是什么，如何防范？

答：SQL注入是指攻击者可以在Web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。本质原因是web应用程序对用户输入数据的合法性没有判断或过滤不严。防范方式有分级管理、参数传值、基础过滤与二次过滤、使用安全参数、漏洞扫描、多层验证以及数据库信息加密。

5、反射型XSS和基于DOM的XSS的区别是什么？比较XSS和CSRF的异同点。

**答：**反射型XSS是指链接包含错误参数，触发错误显示页面；服务器使用动态页面向用户显示错误消息。基于DOM的XSS是指受害者端的网页脚本在修改本地页面DOM环境时未进行合理的处置，而使得攻击脚本被执行。它们的区别是基于DOM的XSS漏洞由服务器响应到客户端的页面中并没有直接包含攻击的恶意代码，而是由客户端在运行时动态生成了最终执行的恶意脚本代码。

XSS是指跨站脚本攻击，黑客将恶意脚本代码植入到页面中从而实现盗取用户信息等操作。CSRF是指跨站请求伪造，黑客伪装成用户身份来执行一些非用户自愿的恶意以及非法操作。它们都是利用Web应用程序漏洞进行攻击的漏洞，区别和联系如下：

1. CSRF相对于XSS漏洞的危害程度更高一些。
2. XSS有局限性，而CSRF则不。
3. CSRF相当于是XSS的基础版，CSRF能做到的XSS都可以做到。
4. XSS主要指向客户端，而CSRF针对服务端。
5. XSS是利用合法用户获取其信息，而CSRF是伪造成合法用户发起请求。

6、下面代码中存在漏洞，请分析漏洞类型成因和利用方式

int main(int argc, char \*\* argv)  
{  
 printf(argv[1]);  
 return 0;  
}

答：漏洞类型为格式化字符串溢出漏洞。攻击者通过打印出argv中的值来查看程序所在路径、用户等敏感信息。