4.2 RPC服务远程溢出漏洞

攻击

RPC 协议是 Windows 操作系统使用的 一种协议,提供了系统中进程之间的交互 通信,允许在远程主机上运行任意程序。 在 Windows 操作系统中使用的 RPC 协议, 包括 Microsoft 其他一些特定的扩展,系统 大多数的功能和服务都依赖于它,它是操 作系统中极为重要的一个服务。

。绝招1: RPC服务远程溢出漏洞入侵演示

RPC 全称是 Remote Procedure Call,在操作系统中,它默认是开启的,为各种网络通信和管理提供了极大的方便,但也是危害极大的漏洞攻击点,曾经的冲击波、震荡波等大规模攻击和蠕虫病毒都是 Windows 系统的 RPC 服务漏洞造成的。可以说,每一次的 RPC 服务漏洞的出现且被攻击,都会给网络系统带来一场灾难。

DComRpc 接口漏洞对 Windows 操作系 统乃至整个网络安全的影响,可以说超过 了以往任何一个系统漏洞。其主要原因是 DCOM 是目前几乎各种版本的 Windows 系 统的基础组件,应用比较广泛。下面就以 DComRpc 接口漏洞的溢出为例,详细讲述 溢出的方法。

Step 01 将下载的 DComRpc.xpn 插件复制到 X-Scan 的 plugins 文件夹中, 作为 X-Scan 插件, 如下图所示。

📙 🛛 🚽 📮 🖛 plugins			-	o ×
文件 主页 共享 查看	3			~ 0
← → × ↑ 📙 « X-Scan-v	/3.3 → plugins	~ Ö	搜索'plugins'	Ą
	名称		类型	大小 ^
/ 承 快速的円	crack_nntp.xpn		XPN 文件	
> 🗥 OneDrive	crack_pop3.xpn		XPN 文件	
	crack_rexec.xpn		XPN 文件	
·	crack_smb.xpn		XPN 文件	
> 📑 60.30	crack_smtp.xpn		XPN 文件	
> 📰 图片	crack_socks.xpn		XPN 文件	
> 💼 文档	crack_sql.xpn		XPN 文件	
> 👆 下载	crack_ssh.xpn		XPN 文件	
> 🎝 音乐	crack_telnet.xpn		XPN 文件	
> 🛄 桌面	crack_vnc.xpn		XPN 文件	
Windows10 (C)	crack_www.xpn		XPN 文件	
> ******************************	DComRpc.xpn		XPN 文件	
> 🚔 本地磁畫 (D:)	findservice.xpn		XPN 文件	
> 🚔 本地磁盘 (E:)	iis_code.xpn		XPN 文件	
> 🚘 本地磁盘 (F:)	nasl.xpn		XPN 文件	
> 👝 本地磁盘 (H:)	netbios.xpn		XPN 文件	
. <u> </u>	snmp.xpn		XPN 文件	•
/ 🛃 Mae	۲			>
21 个项目 选中 1 个项目 52.0	KB			800 📼

Step 02 运行 X-Scan 扫描 工具,选择"设置"→"扫描参数"选项,打开"扫描参数" 对话框,再选择"全局设置"→"扫描模块" 选项,即可看到添加的"DComRpc 溢出漏 洞"模块,如下图所示。



Step 03 在使用 X-Scan 扫描到具有 DComRpc 接口漏洞的主机时,可以看到在 X-Scan 中有明显的提示信息,并给出相应的 HTML 格式的扫描报告。



Step 14 如果使用 RpcDcom.exe 专用 DComRPC 溢出漏洞扫描工具,则可先打开"命令提 示符"窗口,进入 RpcDcom.exe 所在文件夹, 执行"rpcdcom -d IP 地址"命令,开始扫 描并会给出最终的扫描结果,如下图所示。





Step 02 打开"我的电脑 属性"对话框,选择 "默认属性"选项卡,进入"默认属性" 设置界面,取消选中的"在此计算机上启 用分布式 COM (E)"复选框,单击"确定" 按钮即可,如下图所示。

划的电影	商 層性						?	~
常规	选项	默认居性	默认协议	COM 安全	MSDTC			
□æ	此计算机	上启用分布;	t COM(E)					
Ē	此计算机	上启用 CON	1 Internet	服务(N)				
默	人分布式(COM 通信履	性					
身	份验证级解	則指定数据包	级别上的新	全。				
默认身份验证级别(U):								
	连接				\sim			
模标	识进行操作	<u>еле</u> лышлыц 1°с.	LH PJ KANKA	Encode Direct in			17 and	
模标	19,30(3)(和) 识进行操作 既认模拟的 标识	と近いらまかる 乍。 反形(I):			~		17 344	
模标 	机成制量和 识进行操作 跃认模拟组标识 果使用身件	2017日2738 年。 5日(1): 分验证且默认	機拟級則之	5是匿名,则可	✓	用限跨去	注.	
模标 11 如	机成到通过 识进行操作 默认模拟组 标识 果使用身作 	2007642734 F. SBU(1): SH21EER(J SH21EER(J D005517E188	.構拟级别/	、是還名,则1	マリン提供引用	用跟踪安	注.	
模标	AL AC DIFFE A TO A CONTRACT (A CONTRACT) (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)	2013日外3 年。 及則((): の給证且默认 加約31用限約 文藝運行的消	(構拟取別) (安全(P) 細信息。		可以提供引斥	用跟踪安	全,	

Step 03 对于远程计算机,则需要右击"计算机"选项,在弹出的快捷菜单中选择"新 建"→"计算机"菜单命令,如下图所示。



Step 04 打开"添加计算机"对话框,直接输入计算机名或单击右侧的"浏览"按钮来搜索计算机,如下图所示。

添加计	算机	×
	输入计算机名,或单击"浏览"按钮搜索计算机。	确定
		取消
		浏览(B)

4.3 WebDAV缓冲区溢出攻击

WebDAV漏洞也是系统中常见的漏洞 之一,黑客利用该漏洞进行攻击,可以获 取系统管理员的最高权限。

绝招3:WebDAV缓冲区溢出漏洞入侵緊發調 演示

WebDAV 缓冲区溢出漏洞出现的主要 原因是 IIS 服务默认提供了对 WebDAV 的 支持,WebDAV 可以通过 HTTP 向用户 提供远程文件存储的服务,但是该组件不 能充分检查传递给部分系统组件的数据。 这样,远程攻击者利用这个漏洞就可以对 WebDAV 进行攻击,从而获得 LocalSystem 权限,进而完全控制目标主机。

下面简单介绍一下 WebDAV 缓冲区溢 出攻击的过程。入侵之前攻击者需要准备 两个程序,即 WebDAV 漏洞扫描器一Web-DAVScan.exe 和溢出工具 webdavx3.exe,具 体的操作步骤如下。

Step 01 下载并解压缩 WebDAV 漏洞扫描器, 在解压后的文件夹中双击 WebDAVScan.exe 可执行文件,即可打开其操作主界面,在"起 始 IP"和"结束 IP"文本框中分别输入要 扫描的 IP 地址范围,如下图所示。

WebDAVScan V1.0 特	剖版(免瑞星)	>
IF地址 昆抬IF: 192.168.0.1		设置
扫描 停止		
IP Address	HTTP Banner	WebDAV

Step 02 输入完毕后,单击"扫描"按钮,即 可开始扫描目标主机,该程序运行速度非 常快,可以准确地检测出远程 IIS 服务器 是否存在 WebDAV 漏洞,在扫描列表中的 WebDAV 列中凡是标明 Enable 的,说明该 主机存在漏洞,如下图所示。

WebDAVScan V1.0 特别	板(免璃星)	>
IF地址 起始IF: 192.168.0.1		超时: 10000 端口: 80
扫描 傳止	HTTP Banner	WebDAV
192. 168. 0. 10	Hicrosoft-IIS/5.1	Enable
192.168.0.7 登着1	数站点 United State	Disable
192.168.0.1	Wavenlug HTTPD	Disable

Step [03 选择"开始"→"运行"选项,打开 "运行"对话框,在"打开"文本框中输 入 cmd,单击"确定"按钮,打开"命令 提示符"窗口,输入 cd c:\命令,进入 C 盘 目录中,如下图所示。



 Step 04
 在 C 盘目录中输入 "webdavx3.exe

 192.168.0.10"命令,按Enter键,即可开始

溢出攻击,如下图所示。

om 管理员: C:\WINDOWS\system32\cmd.exe	-	×
Microsoft Windows [版本 10.0.17134.319] (c) 2018 Microsoft Corporation。保留所有权利。		^
C:\Users\Administrator>cd c:\		
c:\>webdavx3.exe 192.168.0.10		
IIS WebDAV overflow remote exploit by isno@xfocus.org start to try offset		
if STOP a long time, you can press ^C and telnet 192.168.0.10 try offset: 0	7788	
try offset: 1 try offset: 2		
try offset: 3		
waiting for its restart		

其运行结果如下:

IIS WebDAV overflow remote exploit b	sу
isno@xfocus.org	
start to try offset if STOP a long time, you can pres	5 S
^C and telnet 192.168.0.10 7788	
try offset: 0	
try offset: 1	
try offset: 2	
try offset: 3	
waiting for ii	S
restart	

Step 05 如果出现上面的结果则表明溢出成 功,稍等 2~3 分钟后,按 Ctrl+C 组合键结 束溢出,再在"命令提示符"窗口中输入 telnet 192.168.0.10 7788 命令,如下图所示, 当连接成功后,则就可以拥有目标主机的 系统管理员权限,即可对目标主机进行任 意操作。



Step 06 在"命令提示符"窗口中输入 cd c:\命 令,即可进入目标主机的 C 盘目录。





如果不能立刻安装补丁或者升级,用 户可以采取以下措施来降低威胁。

(1)使用微软提供的 IIS Lockdown 工 具防止该漏洞被利用。

(2)可以在注册表中完全关闭 Web-DAV 包括的 PUT 和 DELETE 请求,具体 的操作步骤如下。

Step 01 启动注册表编辑器。打开"运行"对 话框,在"打开"文本框中输入 regedit, 然后按 Enter 键,打开"注册表编辑器"窗 口,如下图所示。



Step 02 在注册表中依次找到如下键: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\W3SVC\ Parameters。



Step 03 选中该键值后单击右键,在弹出的快捷菜单中选择"新建"选项,即可新建一个项目,并将该项目命名为 DisableWebDAV,如下图所示。



Step 04 选中新建的项目 Disable WebDAV,在 窗口右侧的"数值"下侧右击,在弹出的 快捷菜单中选择"DWORD(32位)值(D)" 选项,如下图所示。

論 注册表编编器			- D >
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助	(H)		
> - wscsvc	^	名称 美型	and and a state of the state of
WSearch		est(默认) REG_SZ	(数值未设置)
>		+78 an	
> wuauserv		初雄(N) シー 現(K)	
		字符串值(S)	
WUDFRd		二进制值(B)	
> wudfsvc		DWORD (32	位)值(D) 、
> WUDFWpdFs		OWORD (6	(前債(0)) 🗟
> - WUDFWpdMtp		安 安竹里//	()
> - WwanSvc		S* 5* 5* 4* (B()	
> - XblAuthManager		可扩充子行机	值(E)
> - XblGameSave			
> xboxgip			
> 🔜 XboxNetApiSvc			
> - kmlprov			
V - W3SVC			
V Parameters			
> Software	~		
<	>	<	
计算机\HKEY LOCAL MACHINE\SYSTEM\Cu	rrentCo	olSet\Services\W3SVC\Parameters\DisableWebD	AV