4.2 RPC服务远程溢出漏洞攻击

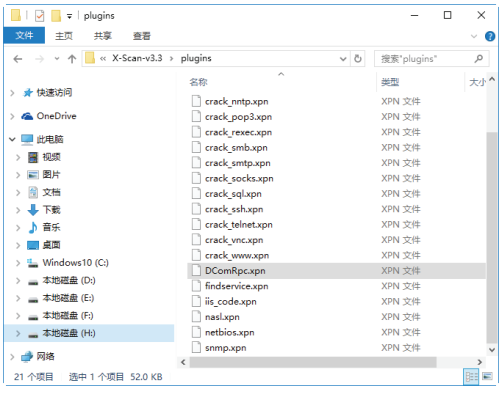
RPC 协议是 Windows 操作系统使用的一种协议，提供了系统中进程之间的交互通信，允许在远程主机上运行任意程序。在 Windows 操作系统中使用的 RPC 协议，包括 Microsoft 其他一些特定的扩展，系统大多数的功能和服务都依赖于它，它是操作系统中极为重要的一个服务。

绝招1：RPC服务远程溢出漏洞入侵演示

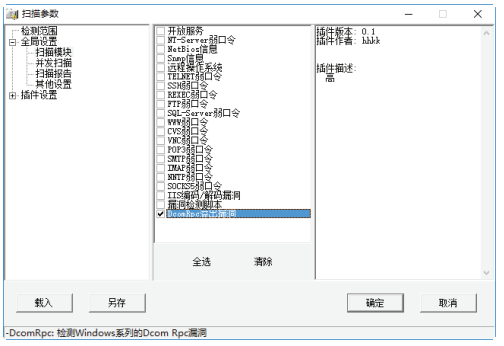
RPC 全称是 Remote Procedure Call，在操作系统中，它默认是开启的，为各种网络通信和管理提供了极大的方便，但也是危害极大的漏洞攻击点，曾经的冲击波、震荡波等大规模攻击和蠕虫病毒都是 Windows 系统的 RPC 服务漏洞造成的。可以说，每一次的 RPC 服务漏洞的出现且被攻击，都会给网络系统带来一场灾难。

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。

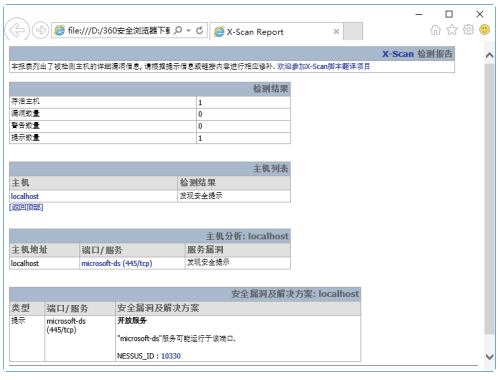
Step 01 将下载的 DComRpc.xpn 插件复制到 X-Scan 的 plugins 文件夹中，作为 X-Scan 插件，如下图所示。



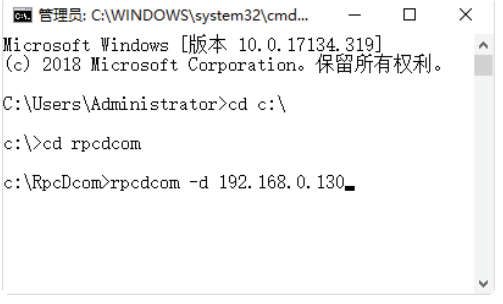
Step 02 运行 X-Scan 扫描工具，选择“设置”→“扫描参数”选项，打开“扫描参数”对话框，再选择“全局设置”→“扫描模块”选项，即可看到添加的“DComRpc 溢出漏洞”模块，如下图所示。

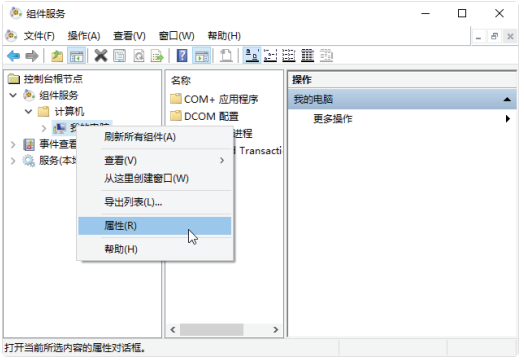


Step 03 在使用 X-Scan 扫描到具有 DComRpc 接口漏洞的主机时，可以看到在 X-Scan 中有明显的提示信息，并给出相应的 HTML 格式的扫描报告。



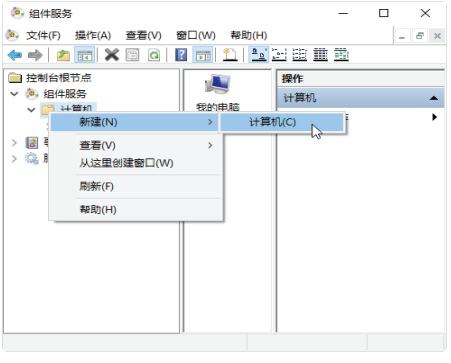
Step 04 如果使用 RpcDcom.exe 专用 DComRPC 溢出漏洞扫描工具，则可先打开“命令提示符”窗口，进入 RpcDcom.exe 所在文件夹，执行“rpcdcom -d IP 地址”命令，开始扫描并会给出最终的扫描结果，如下图所示。



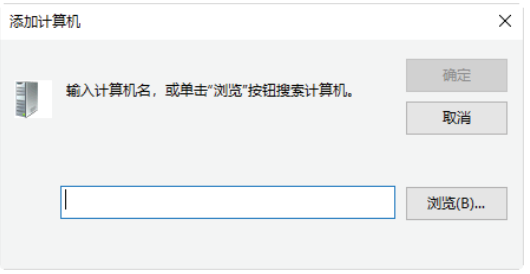


Step 02 打开“我的电脑 属性”对话框，选择“默认属性”选项卡，进入“默认属性”设置界面，取消选中的“在此计算机上启用分布式 COM（E）”复选框，单击“确定”按钮即可，如下图所示。

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。



4.3 WebDAV缓冲区溢出攻击

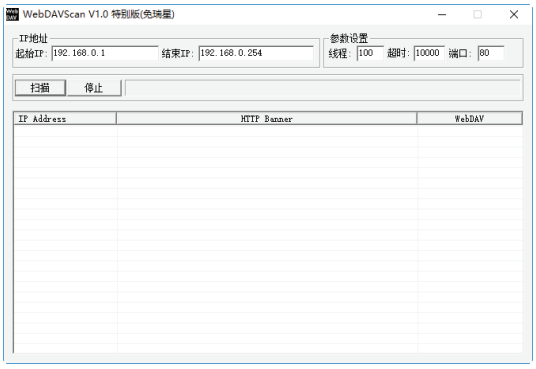
WebDAV 漏洞也是系统中常见的漏洞之一，黑客利用该漏洞进行攻击，可以获取系统管理员的最高权限。

绝招3：WebDAV缓冲区溢出漏洞入侵演示

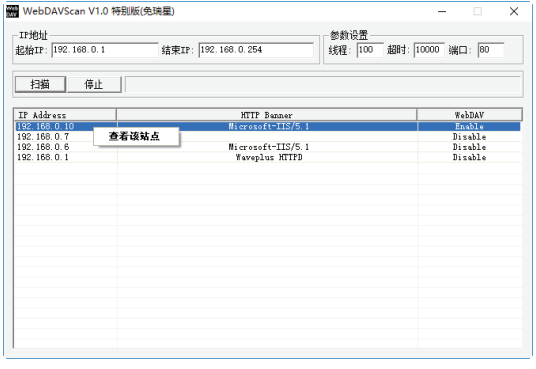
WebDAV 缓冲区溢出漏洞出现的主要原因是 IIS 服务默认提供了对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务，但是该组件不能充分检查传递给部分系统组件的数据。这样，远程攻击者利用这个漏洞就可以对 WebDAV 进行攻击，从而获得 LocalSystem 权限，进而完全控制目标主机。

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—WebDAVScan.exe 和溢出工具 webdavx3.exe，具体的操作步骤如下。

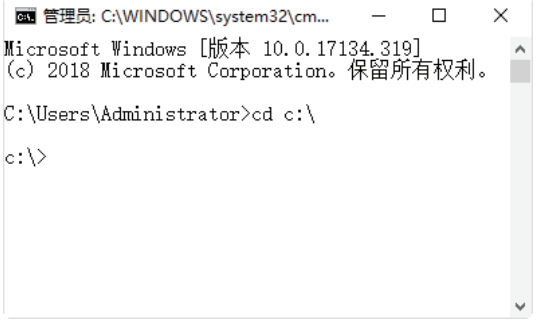
Step 01 下载并解压缩 WebDAV 漏洞扫描器，在解压后的文件夹中双击 WebDAVScan.exe 可执行文件，即可打开其操作主界面，在“起始 IP”和“结束 IP”文本框中分别输入要扫描的 IP 地址范围，如下图所示。



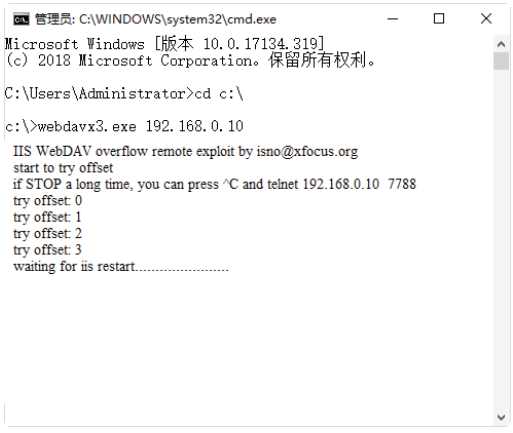
Step 02 输入完毕后，单击“扫描”按钮，即可开始扫描目标主机，该程序运行速度非常快，可以准确地检测出远程 IIS 服务器是否存在 WebDAV 漏洞，在扫描列表中的 WebDAV 列中凡是标明 Enable 的，说明该主机存在漏洞，如下图所示。



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。



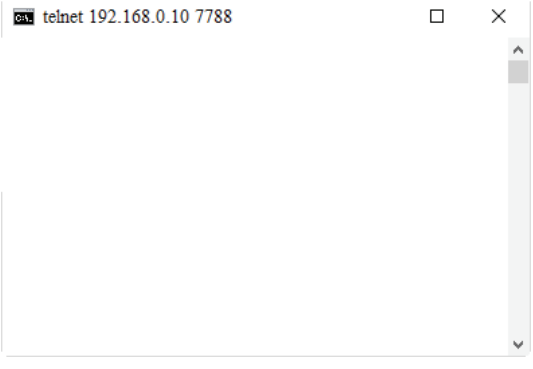
Step 04 在 C 盘目录中输入“webdavx3.exe 192.168.0.10”命令，按 Enter 键，即可开始溢出攻击，如下图所示。



其运行结果如下：

```
    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  7788
    try offset: 0
    try offset: 1
    try offset: 2
    try offset: 3
    w a i t i n g    f o r    i i 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。

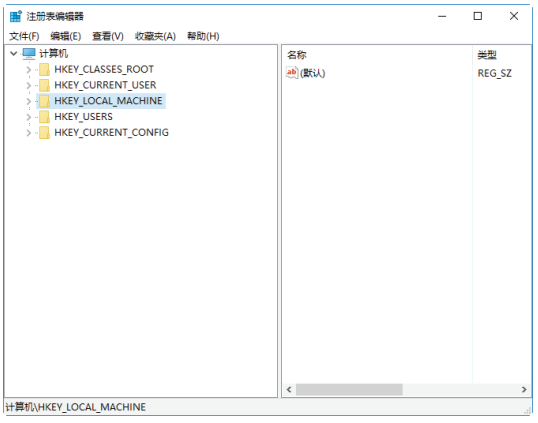
绝招4：WebDAV缓冲区溢出漏洞的防御

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。

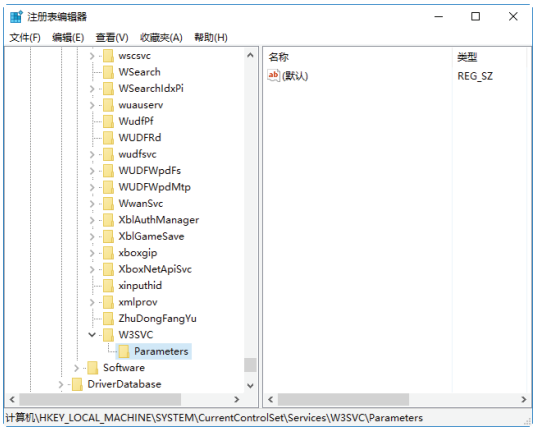
（1）使用微软提供的 IIS Lockdown 工具防止该漏洞被利用。

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

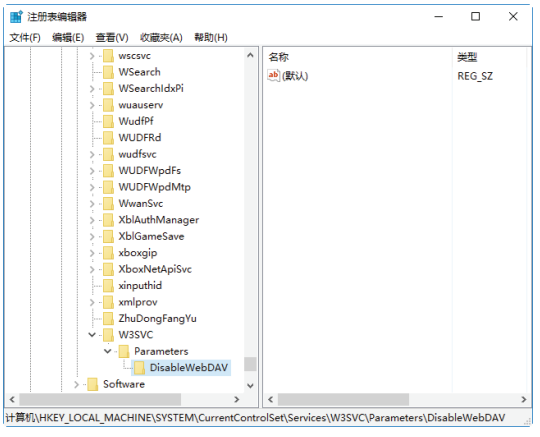
Step 01 启动注册表编辑器。打开“运行”对话框，在“打开”文本框中输入 regedit，然后按 Enter 键，打开“注册表编辑器”窗口，如下图所示。



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 DisableWebDAV，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。