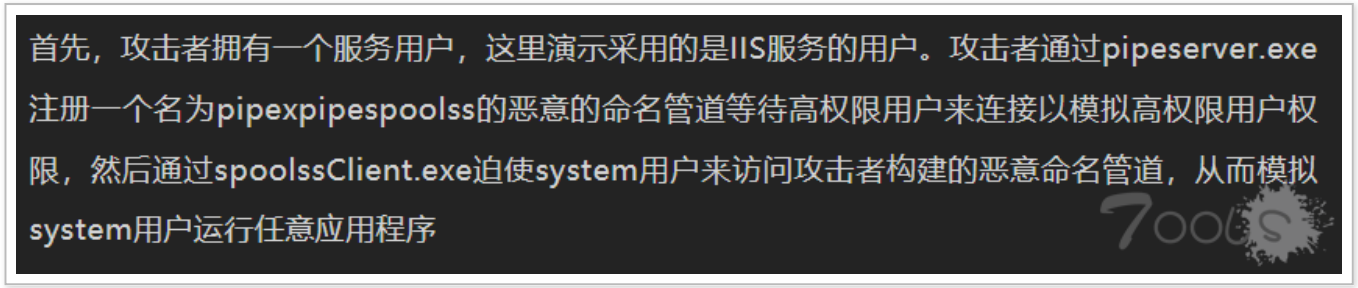
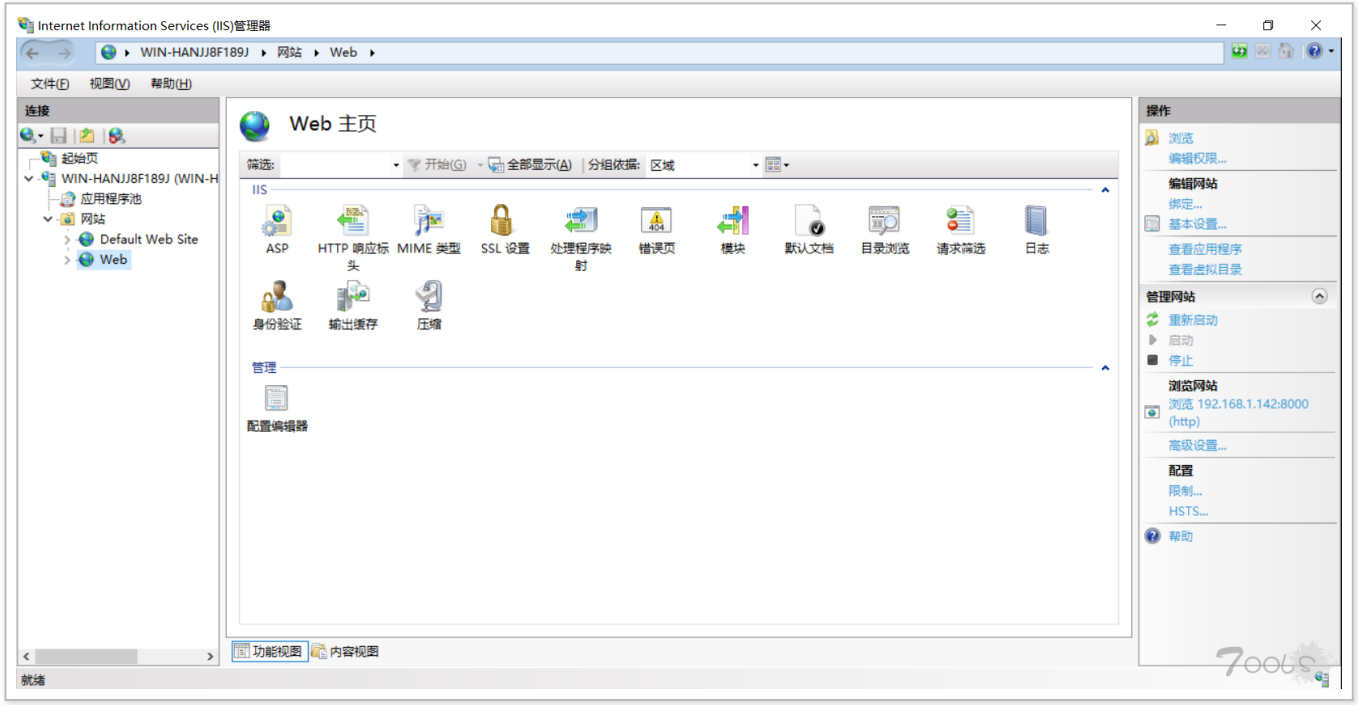
pipePotato 复现 - T00ls.Net

> 今 天 见 安 全 客 发 了 篇 "[url=https://mp.weixin.qq.com/s?__biz=MzA5ODA0NDE2MA==&mid=2649721577&idx=1&sn=634921351846.....

今天见安全客发了篇＂ 首发披露！pipePotato：一种新型的通用提权漏洞 ＂的文章，找了找资料复现了一下



这里是原文对于漏洞的简介，废话不多说直接起环境开始复现。
这里用到的环境是 Windows Server 2019 Datacenter，起一个 iis，做个简单的 web



随便挂个 asp 的 shell 上去，蚁剑直接连上

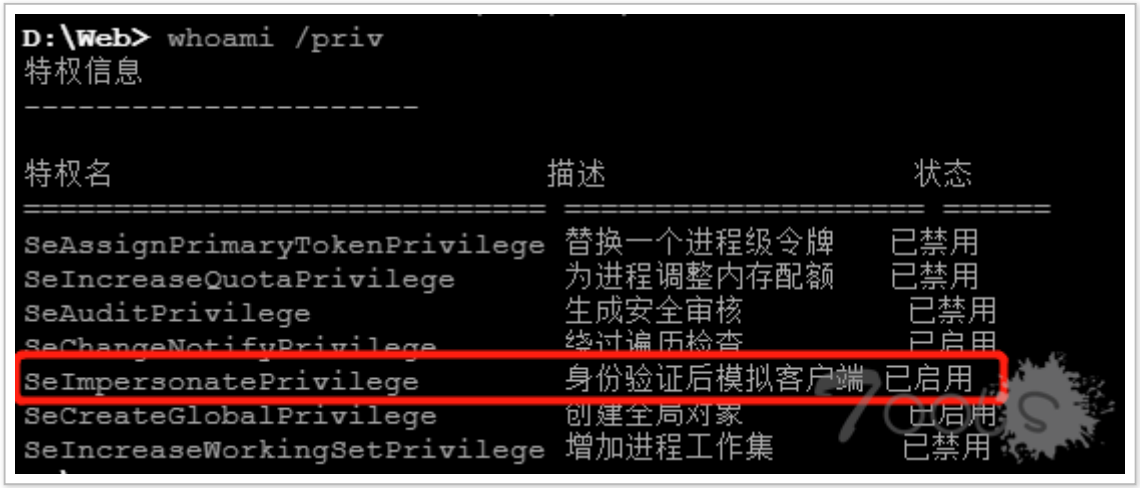
当前 webshell 权限是 iis apppool\web，也就是现在这个应用池的权限，很低。实战里面这个权限基本上什么也干不了，相信很多人在一顿操作之后把 webshell 挂上去之后一看权限只有个 iis apppool 权限心里应该难受的一批吧

重头戏：这里我引用了国外一个表哥关于利用 spoolsv.exe 进程的 RPC 服务强制 Windows 主机向其他计算机进行身份验证的一篇文章中提到的技术内容进行复现原文连接 PrintSpoofer - Abusing Impersonation Privileges on Windows 10 and Server 2019

国外的表哥也是很贴心的直接在 github 上放出了利用工具的源代码，这里给出链接 https://github.com/itm4n/PrintSpoofer ，不得不感慨下国内的安全环境..... 捂脸

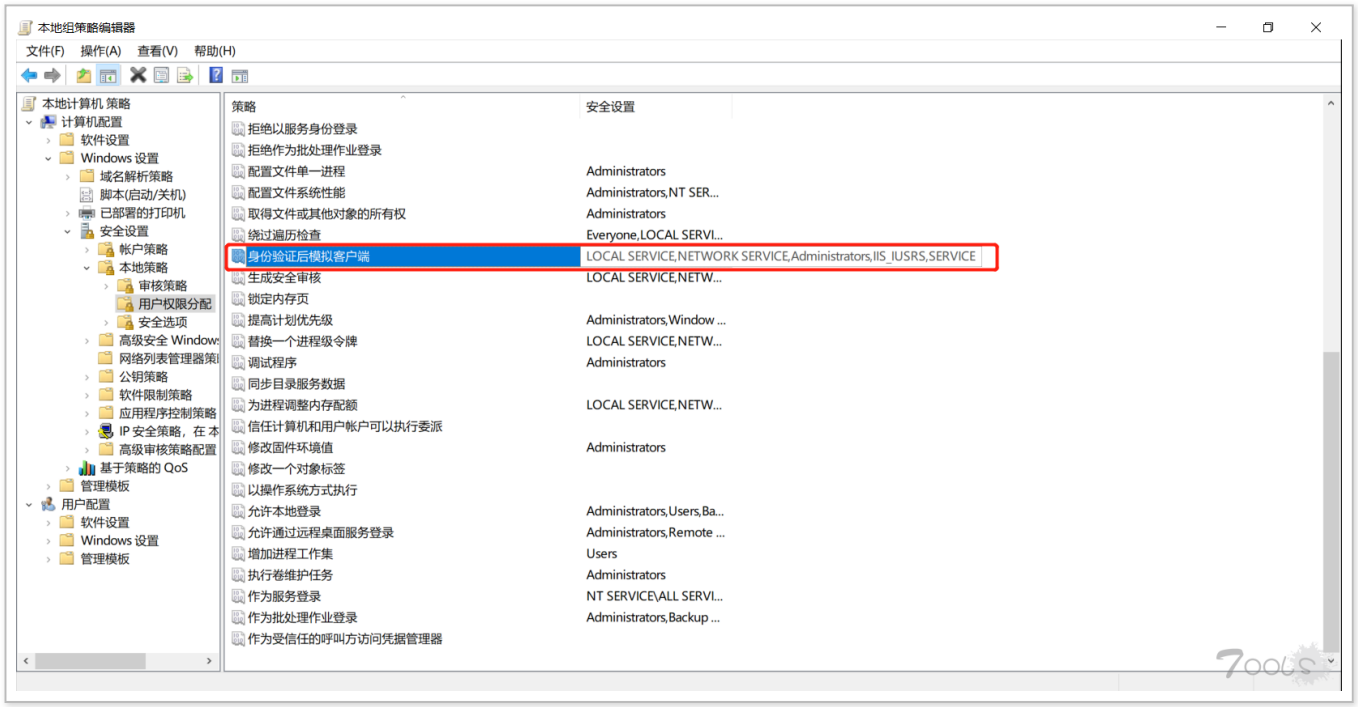
工具下载下来之后直接编译出来放进目标环境

这里有一个关键条件，在表哥的文章中提到，我们需要有 SeImpersonatePrivileg 这个权限

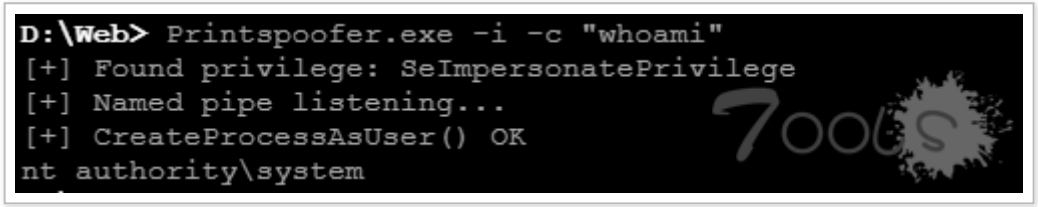


查阅微软官方给出的 相关资料 后发现，默认情况下，除普通用户外，基本上管理员，服务用户都有这个权限

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 本地服务 网络服务 服务
独立服务器默认设置	管理员 本地服务 网络服务 服务
域控制器有效默认设置	管理员 本地服务 网络服务 服务
成员服务器有效的默认设置	管理员 本地服务 网络服务 服务
客户端计算机有效的默认设置	管理员 本地服务 网络服务 服务



运行 exp



defender 暂时是不杀的

实战常见利用场景：iis 权限下本地提权

另外再给大家推荐一篇关于 Windows Token 权限利用的文章，配合食用，效果更佳， 连接