解疑Windows服务器是如何受到攻击的Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_A7_A3_E7_96_91Wind_c100_644364.htm 当我们听到黑客这个词时，我们通常会想到复杂的神秘的技术，并且世界上只有少数人能够执行。然而这是一个误导，并且是当今黑客流行的一大因素。 实际上，服务器入侵没有那么复杂。黑客可能炫耀他们“ 疯狂的技能 ”，但这些人不是我们真正需要担心的。相反，通常是那些技术欠佳又作出错误判断的人会导致最多问题。事实上，这些人现在就存在于许多网络里，寻找可挖掘的漏洞。 当谈到保护Windows服务器阻止入侵时，我非常赞同首先聚焦在容易实现的目标。记住，这是每次难倒你的最基本的安全弱点。在以前的文章里，我介绍了出现Windows安全漏洞的一些原因。现在，我们看看在Windows服务器里两个常见的弱点，并描述它们是如何执行的。 缺失的补丁导致远程命令提示符 打补丁非常麻烦，你想多数Windows服务器能在补丁上作出更新。不过通常不是这么回事。不一致的补丁管理是造成Windows服务器弱点的最大因素。 下面是“ 黑客 ”如何利用未打补丁的Windows服务器作出攻击的步骤 ：攻击者从外面或者（更常见地）在网络里运行免费的漏洞扫描工具，发现缺失的补丁。攻击者确认可以使用免费的Metasploit工具挖掘这个弱点。攻击者启动Metasploit并获得远程命令提示符。 攻击者设置一个后门用户账户并将他们自己添加到本地管理员组。攻击者对系统拥有完全访问权，如本地登录、远程桌面、VPN等。其他人都不会注意到他们的存在。不安全的网络共享导致未授权的文件访问在网络上共

享文件是Windows服务器的基本功能之一。 不过，这也是个致命弱点，使得所谓“ 受信任 ”的用户能够不经授权访问。有时候员工出于无聊、好奇或报复在WindowsExplorer里点击，并会偶然发现他们应该不能访问的敏感信息。 下面是“ 黑客 ”利用不安全的Windows共享作出攻击的步骤： 攻击者在网络里运行免费的共享扫描工具（如GFILANguard），发现Windows服务器上的众多共享信息，多数信息恰好对每个人都拥有完全控制授权。攻击者通过点击这些共享找到他们所需的信息。 攻击者可能偶然发现一些敏感信息或者能下载和安装免费的本文搜索工具，如FileLocatorPro。攻击者在本文搜索工具里插入一些关键字，如能表示敏感信息的“ 密码 ”、“ SSN ”或者“ confidential ”。攻击者找到微软Excel电子表格、Word文档、PDF文件和数据库，里面都是敏感员工的资料和客户信息，能用于非法目的。再次重申，可能没有人会发现这些行为。 有了足够多的“ sticktuitiveness ”，攻击者能在Windows服务器、薄弱的SQLServer配置和基于IIS配置的服务器上发现缺失或简单的密码，通过匿名FTP共享整个驱动等。如果可以访问物理服务器，攻击者能使用包含Ophcrack或 ElcomsoftSystemRecovery的CD重新启动Windows服务器。然后他们能获得对所有用户账户和密码的完整访问，包括 ActiveDirectoryfilentdis.dit。 整个Windows环境都被暴露了，并且无人会发现。 对于外部的黑客或恶意的内部人员，在Windows服务器上有许多弱点能挖掘。只要有足够的时间，他们就能成为黑客。你的任务就是找到这些弱点，在别人进行攻击之前做好防护措施。 