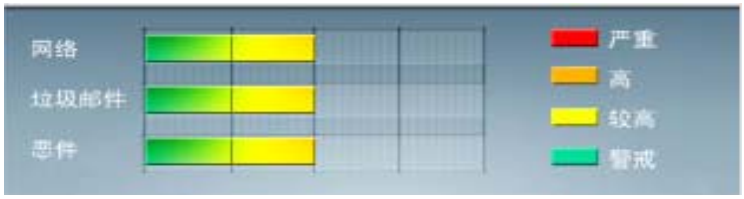
安全威胁每周警讯

2010/11/14～2010/11/20

本周威胁指数



TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	TROJ_LAMEWAR.VTG	木马	★★★	↑	木马病毒
3	WORM_DOWNAD.AD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
5	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。 当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
6	Cryp_Xed-12	木马	★★★	↓	疑似病毒
7	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	破解程序	★★	→	非法破解程序
9	Gray_Gen	加壳程序	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
10	HTML_IFRAME.AZ	网页病毒	★★	↓	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。 当这些文件被执行时，会重定向到这些 URL，并下载恶意程序

系统漏洞信息

MS10-086:Windows 共享群集磁盘中的漏洞可能允许篡改 (2294255)

受影响的软件:

Windows Server 2008

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-086.mspx

系统安全技巧

摘要: Win7 系统的网络功能比 XP 有了进一步的增强，但是默认安装系统后不但同组内的 Win7 系统互相不能共享访问，而且最头疼的问题是组内的 XP 系统计算机更难互访。通过以下步骤基本能够解决 XP 与 Win7 局域网共享设置的问题。

Win7 系统的网络功能比 XP 有了进一步的增强，使用起来也相对清晰。但是由于做了很多表面优化 的工作，使得底层的网络设置对于习惯了 XP 系统的人来说变得很不适应，其中局域网组建就是一个很大的问题。默认安装系统后不但同组内的 Win7 系统互相不 能共享访问，而且最头疼的问题是组内的 XP 系统计算机更难互访。针对这个问题，从网络上收集了一些这方面的资料，结合自己在调试过程中的情况，通过以下步 骤基本能够解决 XP 与 Win7 局域网共享设置的问题。

一、必要点

1、需要是管理员权限的帐户

2、所有入网的计算机都要在相同的 IP 段，比如都为 192.168.1.X(2≤X≤255)

3、所有入网的计算机都要在相同的工作组，比如都在 WORKGROUP 组

4、所有入网的计算机都要开启来宾账户，默认账户名为：guest。

5、关闭任何第三方的防火墙软件，或者进行一些相关设置(很重要)。Windows 自带的防火 墙。如果没有把它关闭的话，也需要进行一些设置才可以。打开 Windows 防火墙---例外---勾选 文件和打印机共享---确定---保存。 XP 系统，在 常规 选项卡中，要去掉不允许例外 前面的勾。

6、所有入网的计算机的操作系统必须有正确的权限设置(这是重点)

7、XP，是指 Windows XP Professional 版本。其中所述的部分方法，并不适用于 Windows XP Home Edition。

8、Win7，是指 Windows 7。不同版本的 Win7 可能存在一定的差异。如果你用的是 Home Basic 版本，就不要再往下看了，因为 Home Basic 不提供文件共享功能。

二、必须开启的服务

右键点击我的电脑 或计算机—管理----服务和应用程序，打开服务或者用 WIN+R 打开 运行---输入 services.msc 回车，打开服务设置

将以下服务的[启动类型]选为[自动]，并确保[服务状态]为[已启动]

Server

Workstation

Computer Browser

DHCP Client

Remote Procedure Call

Remote Procedure Call (RPC) Locator

DNS Client

Function Discovery Resource Publication

UPnP Device Host

SSDP Discovery

TIP/IP NetBIOSHelper //这个很重要，其他的条件即使都满足了，没有这个也不行。

三、基本设置

A. XP 系统：

下载 XP 局域网一键共享，按里边的操作设置后，重启即可。

XP 系统文件共享：右键单击要共享的文件夹，选择[共享和安全]，勾选 在网络上共享这个文件夹。

B. Win7 系统：

1.网络和共享中心---点击 网络 右边的 自定义---将网络类型设置为 专用网络。

2.共享和发现---启用 网络发现、文件共享、打印机共享。密码保护的共享则可以设置为关闭。

3. 跨操作系统的打印机共享涉及到驱动的问题，为了避免麻烦，建议不要跨操作系统共享打印机。

4.访问策略设置

用 WIN+R 打开 运行---输入 secpol.msc 回车，打开本地安全设置

安全设置----本地策略----安全选项

帐户：使用空白密码的本地帐户只允许进行控制台登录，设置为 已禁用。

此选项默认为 已启用。这是很关键的一步，因为很多人的电脑都是没有加密码的的。如果你当前使用的帐号没有密码的话，只允许控制台登录，就无法通过 网上邻居(XP)或网络(Vista)来访问了。所以此处需要禁用。

网络访问：不允许 SAM 帐户和共享的匿名枚举] ，设置为 已禁用。

此选项默认为 已禁用。Windows 允许匿名用户执行某些活动，如枚举域帐户和网络共享的名称。这提供了方便，也带来潜在的风险。有的版本的系统(比如 GhostXP 电脑公司版)为了安全起见，将其设置为启用，但这样一来，局域网其它电脑就会无法查看你共享的内容了。

网络访问：本地帐户的共享和安全模型，设置为 仅来宾。

此选项对加入了域的计算机默认为[经典]，对独立的计算机默认为[仅来宾]。这是一个共享安全的 辅助选项。小规模局域网内部的计算机彼此之间都是信任的，不存在非法访问的问题，为了方便起见，建议使用 仅来宾 方式。而使用 经典 模式可以更好地划定共享资源的访问权限，对于规模稍大的局域网，为了防止共享的资源被非法访问，就可以使用这种方式。

安全设置---本地策略---用户权利指派

从网络访问此计算机： 查看有没有本机来宾帐户即 guest，如果没有就加上。

拒绝从网络访问这台计算机：查看有没有本机来宾帐户名，如果有就删除。

5. Win7 系统文件共享设置

文件夹右键---共享---选择要与其共享的用户---点击黑色的小三角箭头---在下拉菜单中选择---everyone(这个列表中的所有用户)。

注意：在进行以上设置之前共享过的文件夹，可能需要重新共享后才能被正常访问。比如说以前使用 经典 模式共享了该文件夹，改为 仅来宾 模式后再访问就会出错，提示没权限。解决的办法就是先取消共享，再重新共享。

ps：防火墙没必要关闭，毕竟开方共享不是开放黑客!安全依然重要，在享有共享的时候，不能丢弃安全。

防火墙只要设定开放端口 139 和 445 的 TCP 口，还有 137 和 138 的 UDP 口就可以了。

另外，在服务中，确保 TCP/IP NetBIOSHelper 服务是自动的没错，但是并不等于这个功能在 WINS 下启用了，必须还得到网卡的 TCP/IP 设置里，WINS 里面打开 TCP /IP 上的 NETBIOS 启用勾勾，这才能真正生效!没这玩艺，就算前面所有工作都做到家了，还是不容易通!就算偶尔通了，也是暂时通，时而通时而不通， 通通断断、断断通!

只要这个小勾勾打上，就能稳稳地通!

另外再补充

对于刚刚玩共享的人，有时会找不到该开什么窗口该按哪个钮才能看到对方，Win7 和 XP 还有蛮大的区别。

XP 下，一切设置好了，是点网上邻居进去的，或我的电脑文件夹里左边的按钮中，也有网上邻居。不过因为各种复杂的原因，并不是每个 XP 电脑都能在这里看到共享 的 Win7 电脑，概率只有 50%，原因非常复杂，若没看到，可以点网上邻居左边的查看”工作组计算机“，如果 Win7 端设定好的话，那一定会在”工作组计 算机“中列出，然后就可以进行操作了。

Win7 下，很多很多人会直接去点家庭网络的自动发现按钮，玩命地点，结果只有一个，”未找到共享计算机“，这种事情我碰到不少了，别往这方向努力了，这是给 Win7 和 Win7 之间家庭内网搞的按钮，就算两个 Win7 都未必能通，白费力!

真正顶用的，直接点开桌面的”计算机“文件夹，左边的一排按钮里就有”网络“二字，直接点这玩艺儿，一切共享的机机统统跑出来。

来源： 网络转载