

Re: Win 2000 security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-09/0298.html>

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/09/04

Date: Thu, 09 Sep 2004 04:46:05 GMT

You could restrict access to your computer by either computers or users. To restrict by computers you would have to use either an ipsec filtering policy or a software firewall to restrict access by allowing only certain IP addresses which may not be effective unless the other computers have static IP addresses. Ipsec can also be used to allow only certain other W2K or XP Pro computers to access your computer if your computer has an ipsec require policy and the other computers have a compatible ipsec policy using either kerberos [domain computers], computer certificate or preshared key for authentication. Ipsec is an advanced topic but if interested see the link below.

<http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp>

Otherwise you can restrict what "users" can access your computer by configuring share permissions to only contain those users/groups you want to allow access and what kind of access. Share and ntfs permissions both restrict a user's access to a share with the most restrictive setting of the two being the effective permission. The link below explains share permissions in more detail.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:301281>

<http://support.microsoft.com/default.aspx?kbid=300691>

You can also modify the Local Security Policy of your computer for the user rights for logon locally and deny logon locally to control who can access your computer. Try not to use the deny logon locally and never add users or everyone to that user right. User rights are found in Local Security Policy [secpol.msc] under security settings/local policies/user rights. The "effective" setting is the setting that is applied and should only be of a concern to domain computers.

If a user is not prompted for credentials when they access shares on your computer that means they are logging onto their computer with a logon/password that exists in the local users on your computer [or domain controller for domain computers], or have a mapped drive with persistent credentials that matches a local user on your computer. The exception would be if you have the guest account enabled which it would not be by default but be sure to check in Local Users and Group/users on your computer or use the command " net user guest " and see if it is listed as no for act