Hardening Windows NT/2000/XP Information Systems

Date: Jul 31, 2003
Section: Articles :: Windows OS Security
Author: Ricky M. Magalhaes
Printable Version

This article is written as a security guideline to help administrators and security professionals to be able to configure windows in a more robust way. The recommendations in this whitepaper assume that the computer is physically secure.

Firewalls and their roles.

A firewall is an integral part of any network that is connected to the internet. If no firewall is set up as a bastion host, many attacks can take place against windows without the administrator knowing. The multitude of these attacks can be so great that the machine will hang-up, this will make the task of isolating what attack took place incredibly challenging. If no firewall is available a router can be used to filter out unwanted protocols and ports that intruders may use to attack network. The most used and known protocol is TCP/IP and within its stack lies a multitude of protocols that have vulnerabilities that. At very minimum TCP ports 135, 139, and 445, and UDP ports 135, 137, and 445 should be blocked as well as all the other unused ports. A basic firewall principal is as follows: Think of a firewall as a physical wall that has been built around your network. Each time you open a port you create a hole in the wall and install a window. Some windows open outwards and some open inwards. Intruders can use the windows but only to see what is inside the network. The more windows (ports) you install the more transparent your wall becomes.

Service packs.

Service packs are applications that are released after the public discharge of a certain product. If a product hat has been released is found to have a flaw a hot fix is developed for that product and when the hot fixes are put together they form a service pack. Windows does not function as it was intended without its service packs. Security patches are also released occasionally to patch up areas that have vulnerabilities and that programmers have not secured. Millions of users make use of the windows platform daily and a multitude of these users are programmers and people with advanced technical skill. Some of these people like to stress test and find vulnerabilities within the windows platform. When a vulnerability is found it may be days or even weeks before software vendors write an effective patch that is publicly released. The chance that your machine will be scanned and the vulnerability found are higher than you imagine. Keep all machines on the network updated and check with Microsoft on a scheduled basis for service releases to software that you may be running.

Underestimating this function can cost your organization many hours of down time equating to losses if you do not want to become a statistic ensure that your machines are properly patched.

Account considerations.

Ensure that if you are using Windows NT and above that your administrative account is secure. Renaming the account to something ordinary is good practice then recreating another account named administrator and giving that account the most restrictive privileges will give any intruder a challenging time if he does manage to gain access to your "bait" administrative account.

Antivirus.

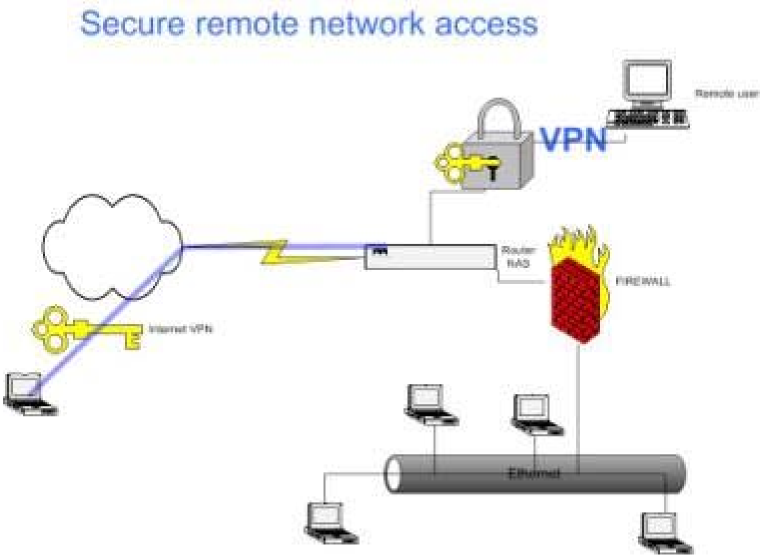
Viruses are a fast growing irritation and many new viruses are released weekly. If your machine has an internet connection or has had any sort of media interaction like foreign discs then antivirus is required. If the antivirus software is updated then the risk is greatly reduced. Using licensed original software also lessons the risk and scanning of email and foreign disks helps keep viruses at bay. For high level security web browser settings should be set to high maximum security. Web browsing should not be done from servers or critical machines. Any software that is downloaded should be downloaded and installed on test systems and the system should be patched and scanned for viruses after the software has been tested, this not only quality assures the software but also verifies the integrity of the installation. Do not download software form unknown sources. Downloading software from file sharing services is not only dangerous but can also compromise the entire network. Some viruses spread after execution onto the entire network and depending on the strain of virus if it is a malicious type can cause many hours of down time resulting in financial loss.

Virus software settings need to be set to the most restrictive. This ensures that any form of malicious virus activity I not tolerated. Setting the system to repair the virus infected file is acceptable but if the file is un-repairable try not to keep the file on the system if it is not needed. Hardening your system means zero tolerance. A Trojan horse type virus can easily compromise your network even if your firewall has all of its ports closed. A user can be dialed up to a service provider on a machine infected with a Trojan and the backdoor to your network is wide open. On your mail server block all potentially malicious file types. VBS, EXE, COM etc are examples of file types that can be blocked these file are rarely used for business purposes and can be executed by unsuspecting users and potentially can compromise your network. If a user needs to send you an .exe get them to rename the file and send it with a different extension. Set your antivirus to scan the selected extension for virus patterns that may exist to ensure that a virus does not slip past in that way.

Dial in access or Remote network access.

Restrict dial in access to trusted users and limit the functionality of the users from remote locations. Policies can be designed in such away that user activity will be traced. When accessing a network remotely a VPN is secure method that can be used and trusted. Data that travels over a VPN connection is much less susceptible to interception than normal PPP connections over the PSTN networks. In high security environments put systems in place that require credential validation for any resource that is accessed remotely. Client side certificates can be used and strong password authentication methods should be applied. Remote access remains one of the weakest links in network security if incorrectly implemented and in many cases is just the break intruder are looking for.

In saying this the BBS days have passed us by and intruder would much rather use the convenience of the internet than use elaborate war dialing techniques. Dialing in to a separate network segment is a good way of segmenting the dialing users from the corporate network. This solution can have many functional features. If your network users require dial back setting the dial back to predetermined numbers is a good way of ensuring that the connection is in-fact connecting to the user’s home. The other consideration is that a user must not store the credentials locally on the machine that he/she accesses the network with passwords should not be saved and should be typed each time a dial up connection is made.



The above diagram represents remote network access through a secure VPN route from both the internet and a dial up location. Note that the firewall treats these users as external network users and created virtual network access depending on permissions set on the firewall.

Intrusion detection.

Intrusion detection is a vital part of hardening the windows network and various intrusion detection products exist that can aid an organization in detection of unwanted intruders for a comparative analysis on IDS look in www.windowsecurity.com

Strong password practices - What constitutes a good password?

- Longer than 8 characters
- Contains elements from at least three of the following four character sets
  - Uppercase characters
  - Lowercase characters
  - Numbers
  - Non-alpha numeric characters
- Does not contain any part of the users name, username, or any common word
- Use ALT characters. ALT characters are those that you type by holding down the ALT key (the FN+ALT keys on a laptop) and typing a three or four digit number on the numeric keypad (the numeric overlay keypad on a laptop). Most password crackers are not capable of testing the vast majority of ALT characters.
- Do not allow storage of the LMHash.

This complexity is enforced via a password filter, and can be optionally required using group policy.

Services installed

Services run on most windows machines as registered processes. Theses services are what intruders attempt to find vulnerabilities within. Disabling any unused services is good practice and leaves less for the intruders to find exploits within. It also puts less strain on the hardware and requires less monitoring.

File system

File systems should be installed on secure machine with the highest form of file security. NTFS is a strong secure file system that let the administrator and user control access to files that have respective assigned permissions. This added level of control not only protects the user against potential intruder but also provides as a shield against viruses when they attempt to install them selves as a user that does not have rights to the hardware. It is a good idea to format all mobile machines with NTFS as this provides added security if the machine is stolen or misplaced. The data on the drive is not as vulnerable as it would be if it were on a Fat partition, in the same breath a few companies have developed software that will be able to read file on NTFS partitions if permissions are assigned or not.

Bios

Do not leave your bios open. By this I mean assign a password to the Bios. If a user wants to change the boot order of drive within the computer he will first log into the bios and change the order to boot off of the CD-ROM. The utilities that let a user gain access to the machine are typically on a CD-ROM. By assigning a password to the Bios it adds a small added level of security. If the user can not gain access to the inside of the computer because it is physically restrained the bios can also not be reset and the bios then remains locked. Please note that some bios manufactures have master passwords that override any previous entered passwords it is a good idea that when choosing the hardware that a vendor is chosen that has not mater password capability.

Booting drives.

When assigning the drive to boot ensure that only the C: drive has the booting capability as other drive like CD and floppy disk drive provide an avenue for attack. Intruders may need to install or load third party applications and by booting around the operating system this may be possible. Many administrators secure the operating systems and overlook the underlying booting and removable disk options.

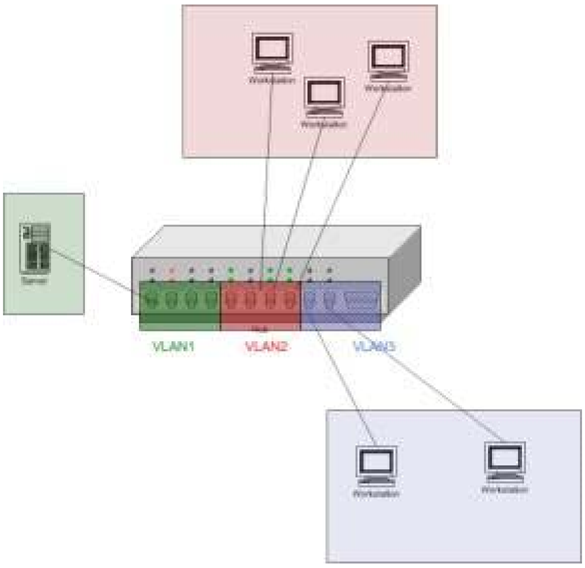
Install IIS on separate network segments

Many exploits are found for IIS because it is a very generic and widely used. Note that due to the prevalence of worms exploiting unsecured systems on most networks, it is highly recommended that system running IIS are installed on an isolated network segment, or with no network cable attached, until the latest service packs are installed. Microsoft has published an IIS lock down tool and it is recommended that this tool is used to lock down any known issues and vulnerabilities that may be present on the IIS box search the Microsoft website for this tool. Typically IIS servers need to be accessed by users on the internet and this makes the server particularly susceptible. Publishing an IIS server through an ISA server may help to alleviate any known vulnerabilities and will help in adding an extra layer of security to your IIS windows server. SQL servers that also need to be accessed from the internet should also be published through ISA for more information visit www.ISAsever.org .

Segment the network

Physical segmentation of the network is always a healthy scenario and if your hardware facilitates this act then it is advised that you implement this form of security. As with can be used to VLAN a network and an access list can be set up that only specific machines can talk to a preconfigured segment. If you VLAN your firewall form your network and only allow your firewall to access your network you eliminate the possibility that intruders use another form of entry other than your firewall form the internet. It is a good idea to segment your network if you are testing software that is from an un-trusted source as this software may contain vulnerabilities and or viruses that may want to spread to other networked machines. Opaserv virus is a good example of this.

VPN for remote access. Segmentation of a network can also add an element of security form an internal perspective as you can segment a network in such a way that all users can see the servers but no user can see each other. This reduces the possibility of hacking of user data stored on user machines and greatly improves security from the perspective that if a machine were to be infected with a LAN scanning virus the virus could not spread because it would find itself isolated from the other computers.



Segmented switch diagram

Branch offices

Branch office that a permanently connected by form of physical data lines can also pose a certain amount of risk as these smaller offices are often remote and detailed attention is often not paid to the security vulnerabilities that may lurk from the branch office side. A branch office should be treated as a segment of the LAN and should not be overlooked when designing the entire security policy it is important that the branch office also be segmented in a way that it can not access any other machines on the LAN except for pertinent machines like mal server and directory server if this a need business service. Routing packets from branch offices should be limited to validated business traffic and having only legitimate network use will ensure that discrepancies be picked up quickly. If you see fit it may be a good idea to put branch offices behind a firewall and regulation of traffic could be done through the firewall. This will add an extra level of security and it will also keep both sides safe from opposing breach access attempts.

Backups

In any organization business continuity should be part of the disaster recovery strategy and backups will be part of this strategy. All data should be backed up and should be restored frequently. Backups are important and it is vital that the media is stored offsite. Storing backup media onsite will not help in a situation where a physical disaster destroys the site. Offsite storage is needed in situations that require an extra level of data security.

Summary

There is a myriad of tools that help access the status of the security of your network. Tools that help with event monitoring prove to be useful and help to maintain the network in a functional stat as they help detect irregularities even if the machine has been patched against attacks. In this article I have covered many overlooked parts of a network and windows platform. It is important that all the recommendations be adhered to ascertain completeness.

If you would like us to email you when Ricky Magalhaes releases another article on WindowSecurity.com, subscribe to our 'Real-Time Article Update' by clicking here. Please note that we do NOT sell or rent the email addresses belonging to our subscribers; we respect your privacy!