7.1 Configuring Windows

A Proper configuration of Windows (Windows 7, 8, 10 and Server Editions) consists of many facets. You must disable unnecessary services, configure the registry in a proper way, enable the firewall, configure the browser properly , and so on.

Previously we have discussed the firewall concepts and the processes of both stateful packet inspection and stateless packet inspection. A subsequent section of this chapter discusses browser security. For now, let’s go over the other important factors in Windows security configuration.

7.1.1 Accounts, Users, Groups and Passwords

Any Windows system comes with certain default user accounts and groups. These can frequently be a starting point for intruders who want to crack passwords for those accounts and gain entrance onto a server or network. Simply renaming or disabling some of these default accounts can improve your security.

Note: Windows have an affinity to move things in the control panel with each version. Your version (7, 8, 8.1, 10, etc.) might be placing things in a different location. If you have not already done so, take some time to familiarize yourself with the location of utilities in your version of Windows.

In Windows 7 or Windows 8, you can find user accounts by going to Start, Settings, Control Panel, Users and Groups. In Windows 10 go to Start, Settings, and Accounts.

7.1.1.1 Administrator Accounts

The default administrator account has administrative privileges, and hackers frequently seek to obtain logon information for an administrator account. Guessing a logon is a two-step process of first identifying the username, and then the password. Default accounts allow the hacker to bypass the first half of this process. Administrators should disable this account.

Having an account with administrative privileges is necessary for maintaining your server. Following that, you must add a new account. It is best if the account has an innocuous name. It is also crucial to give that account administrative privileges. By doing so, a hacker’s

task becomes much more difficult, as he must first discover which account has administrative privileges before he can even attempt to compromise that account.

Some experts suggest simply renaming the administrator account, or using an administrator account that has a username that indicates its purpose. That is not a recommendation for the following reasons:

- The whole point is that a hacker should not be able to identify which username has administrative privileges.

- It is not enough to simply rename the administrator account to a different name, since its administrative rights will still be apparent.

7.1.1.2 Other Accounts

The administrator account is the one most often targeted by hackers, but Windows also includes other default user accounts. Applying an equally demanding behaviour to all default accounts is considered to be a good idea. Any default account can be a gateway for a hacker to compromise a system. A few accounts that you should pay particular attention are:

- **IUSR_Machine name:** When you run IIS, a default user account is created for IIS. Its name is IUSR_ together with the name of your machine. This is a common account for a hacker to attempt to compromise. It is advisable to alter it in the manner suggested for the administrator account.

- **ASP.NET:** If your machine runs running ASP.NET, a default account is created for web applications. A hacker that is familiar with .NET could target this account.

- **Database accounts:** Many relational database management systems, such as SQL Server, create default user accounts. An intruder, particularly one who wants to get at your data, could target these accounts.

When adding any new account, it is always recommended to give the new account’s user or group the least number (a small set of numbers) as well as type of privileges that are needed to perform their

job, even if it involves IT staff members accounts. Below are some examples:

- A PC technician does not need administrative rights on the database server. Even though it belongs to the IT department, it does not need access to everything in that department.

- Managers may use applications that reside on a web server, but they certainly should not have rights on that server.

- A programmer (who develops applications that may run on a server) should not necessarily have full access on the server.

These are just a few examples of things to consider when setting up user rights.

Remember: Always give the least access necessary for that person to do her job. This concept is often called least privileges, and is a cornerstone of security.

7.1.2 Setting Security Policies

Setting appropriate security policies is the next step in hardening a Windows server. This does not refer to written policies an organisation might have regarding security standards and procedures. In this case, the term security policies refers to the individual machines' policies.

The first matter of concern is setting secure password policies. The default settings for Windows passwords are not secure. The table below shows the default password policies. Maximum password age refers to how long a password is effective before the user is forced to change that password.

Enforce password history refers to how many previous passwords the system remembers, thus preventing the user from reusing passwords. Minimum password length defines the minimum number of characters allowed in a password.

Password complexity means that the user must use a password that combines numbers, letters, and other characters. These are the default security settings for all Windows versions from Windows NT 4.0 forward. If your system is protected within a business environment, the settings at Local Security will be greyed out, indicating you do not have permissions to make changes.

Policy	Recommendation
Enforce password history	**1 password remembered**
Maximum password age	**42 days**
Minimum password age	**0 days**
Minimum password length	**0 characters**
Passwords must meet complexity requirements	**Disabled**
Store password using reversible encryption for all users in the domain	**Disabled**

The default password policies are not secure enough, so the question is what policies should you use instead? Different experts give different answers. The table below shows the recommendations by Microsoft and the National Security Agency.

Policy	Microsoft	NSA
Enforce password history	**3 passwords**	**5 passwords**
Maximum password age	**42 days**	**42 days**
Minimum password age	**2 days**	**2 days**
Minimum password length	**8 characters**	**12 characters**
Passwords must meet complexity requirements	**No recommendation**	**Yes**
Store password using reversible encryption for all users in the domain	**No recommendation**	**No recommendation**

Developing appropriate password policies depends largely on the requirements of your network environment. If your network stores and processes highly sensitive data and is an attractive target to hackers, you must always skew your policies and settings towards maximum

security. However, bear in mind that if security measures are too complex, your users will find it difficult to comply. For example, very long, complex passwords (such as $%Tbx38T@_FgR$$) make your network quite secure, but such passwords are virtually impossible for users to remember.

7.1.3 Account Lockout Policies

When you open the Local Security Settings dialog, your options are not limited to setting password policies. You can also set account lockout policies. These policies determine how many times a user can attempt to log in before being locked out, plus how long to lock them out for. The default Windows settings are shown in the table below.

Policy	Default Settings
Account lockout duration	**Not defined**
Account lockout threshold	**0 invalid logon attempts**
Reset account lockout counter after	**Not defined**

These default policies are not secure. Essentially, they allow an infinite number of log-in attempts to take place. This makes the use of password crackers very easy and virtually guaranteeing that someone will eventually crack one or more passwords and gain access to your system. The table below provides the recommendations by Microsoft and National Security Agency.

Policy	Microsoft	NSA
Account lockout duration	**0, indefinite**	**15 hours**
Account lockout threshold	**5 attempts**	**3 attempts**
Reset account after	**15 minutes**	**30 minutes**

7.1.4 Registry Settings

The Windows Registry is a database used to store settings and options for Microsoft Windows operating systems. This database contains critical information and settings for all the hardware, software, users, and preferences on a particular computer. Whenever users are added or software is installed or even any other change is made to the system (including security policies), that information is stored in the registry.

Secure registry settings are critical to securing a network. Unfortunately, that area is often overlooked. Keep in mind that unless you know how the registry works, serious problems will be caused. So, if you are not well acquainted with the registry, do not touch it. Even if you are confident with making registry changes, you should always back up the registry before any change is made.

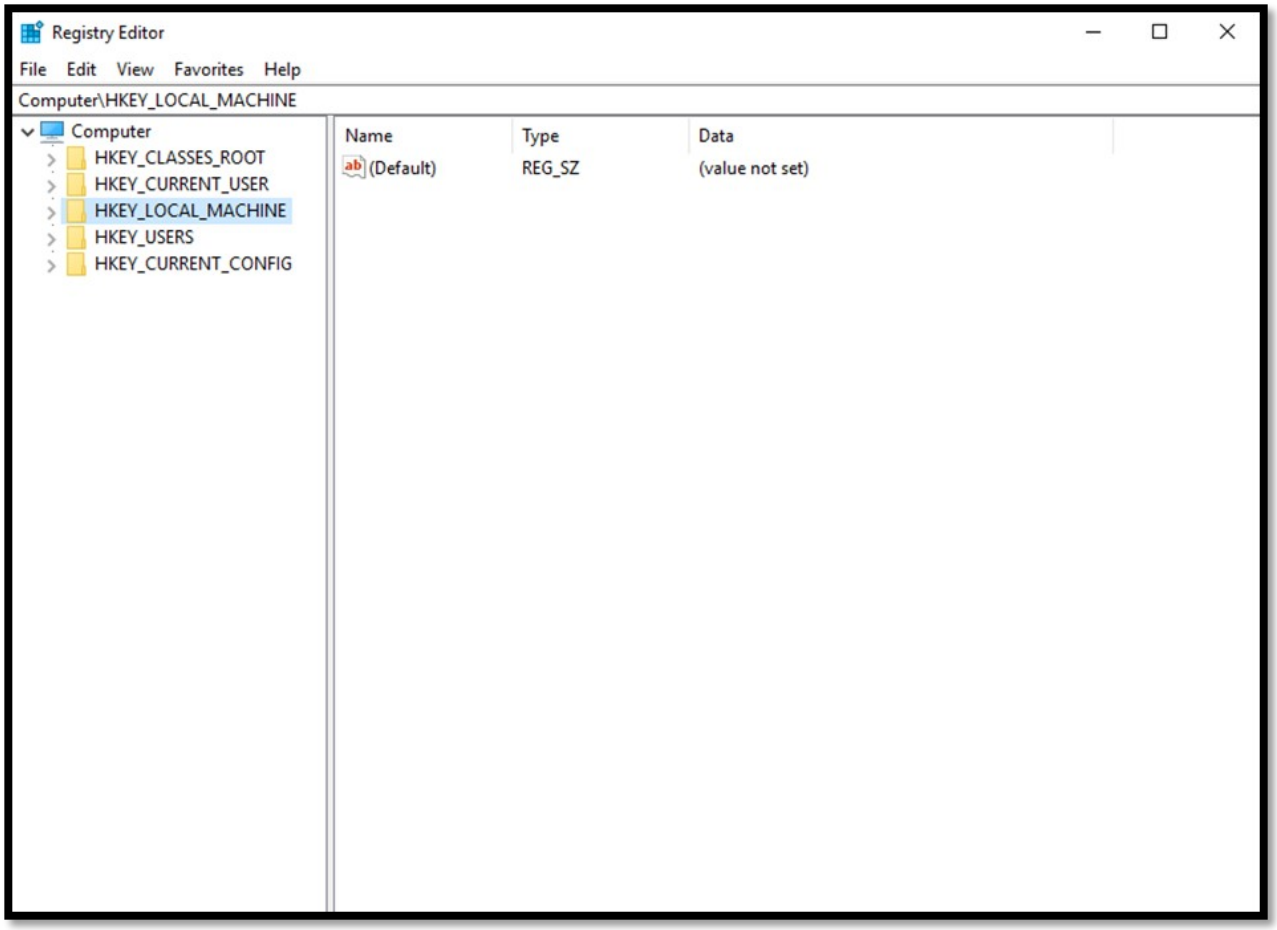
7.1.5 Registry Basics

The physical files that make up the registry are stored differently depending on which version of Windows you are using. Older versions of Windows (that is, Windows 95 and 98) kept the registry in two hidden files in your Windows directory, called USER.DAT and SYSTEM.DAT. In every version of Windows, since XP, the physical files that made up the registry had been stored in %SystemRoot%\ System32\Config. Since Windows 8, the file has been named ntuser.dat.

Regardless of the version of Windows you might be using, you cannot edit the registry by directly opening and editing these files. Instead you must use a tool, regedit.exe, to make any changes. There are newer tools such as regedit32. However, many users find the older regedit has a more user friendly “find” option for searching the registry. Both options work.

Although the registry is referred to as a “database,” it does not actually have a relational database structure (like a table in MS SQL Server or Oracle). The registry has a hierarchical structure similar to the directory structure on the hard disk. In fact, when you use regedit, you will note it is organized like Windows Explorer. To view the registry, go to Start, Run, and type regedit. You should see the Registry Editor

dialog box as shown below. Some of the folders in your dialog box might be expanded.



Your Registry Editor dialog box will likely have the same five main folders as the one shown above in the screenshot. Each of these main branches of the registry is briefly described in the following list. These five main folders are the core registry folders. A system might have additions. Nevertheless, these are the primary folders containing information necessary for your system to run.

- **HKEY_CLASSES_ROOT:** This branch contains all of your file association types, OLE information, and shortcut data.
- **HKEY_CURRENT_USER:** This branch links to the section of HKEY_USERS appropriate for the user who might be currently logged on to the PC.
- **HKEY_LOCAL_MACHINE:** This branch contains computer-specific information about the type of hardware, software, and other preferences on a given PC.
- **HKEY_USERS:** This branch contains individual preferences for each user of the computer.

- **HKEY_CURRENT_CONFIG:** This branch links to the section of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.

If you expand a branch, you will see its subfolders. Many of these have, in turn, more subfolders, possibly as many as four or more before you get to a specific entry. A specific entry in the Windows Registry is referred to as a key. A key is an entry that contains settings for some particular aspects in your system. If you alter the registry, you actually change the settings of particular keys.

7.1.6 Restrict Null Session Access

Null sessions are a significant weakness that can be exploited through the various shares that are on the computer. A null session is Windows' way of designating anonymous connections. Any time you allow anonymous connections to any server, you are inviting significant security risks. Modify null session access to shares on the computer by adding **RestrictNullSessAccess**, a registry value that toggles null session shares on or off to determine whether the Server service restricts access to clients logged on to the system account without username and password authentication. Setting the value to "**1"** restricts null session access for unauthenticated users to all server pipes and shares except those listed in the **NullSessionPipes** and **NullSessionShares** entries.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer

Action: Ensure that it is set to: Value = 1

7.1.7 Restrict Null Session Access Over Named Pipes

The null session access over named pipes registry setting should be changed for much the same reason as the preceding null session registry setting. Restricting such access helps to prevent unauthorised access over the network. To restrict null session access over named pipes and shared directories, edit the registry and delete the values, as shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer

Action: Delete all values

7.1.8 Restrict Anonymous Access

The anonymous access registry setting allows anonymous users to list domain user names and enumerate share names. It should be shut off. The possible settings for this key are:

- 0—Allow anonymous users
- 1—Restrict anonymous users
- 2—Allow users with explicit anonymous permissions

Key Path: HKLM\SYSTEM\CurrentControlSet\Control\Lsa

Action: Set Value = 2

7.1.9 Remote Access to the Registry

Remote access to the registry is another potential opening for hackers. The Windows XP registry editing tools support remote access by default, but only administrators should have remote access to the registry. Fortunately, later versions of Windows turned this off by default. In fact, some experts advise that there should be no remote access to the registry for any person. This point is certainly debatable. If your administrators frequently need to remotely alter registry settings, then completely blocking remote access to them will cause a reduction in productivity for those administrators. However, completely blocking remote access to the registry is certainly more secure. To restrict network access to the registry:

1. Add the following key to the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg.

2. Select winreg, click the Security menu, and then click Permissions.

3. Set the Administrator’s permission to Full Control, make sure no other users or groups are listed, and then click OK.

Recommended Value = 0

7.1.10 Services

A service is a program that runs without direct intervention by the computer user. In Unix/Linux environments, these are referred to as daemons. Many items on your computer run as services. Internet Information Services, FTP Service, and many system services are some good examples. Any running service is a potential starting point for a hacker. Obviously, you must have some services running for your

computer to perform its required functions. However, there are services your machine does not use. If a service is not being used at that moment, it should be shut down.

7.1.11 Encrypting File System

Beginning with Windows 2000, the Windows operating system has offered the Encrypting File System (EFS), which is based on public key encryption and takes advantage of the CryptoAPI architecture in Windows 2000.

This still exists in Windows 7, 8, and 10; however, if you take the later versions of Windows, EFS is only available in the upper-end editions of Windows such as Windows Professional. With EFS, each file is encrypted using a randomly generated file encryption key, which is independent from a user's public/private key pair; this method makes the encryption resistant to many forms of cryptoanalysis-based attacks. For our purposes the exact details of how EFS encryption work are not as important as the practical aspects of using it.

7.1.12 Security Templates

We have been discussing a number of ways on how to make a Windows system more secure. Nevertheless, exploring services, password settings, registry keys, and other tools can be quite a daunting task for the administrator who is new to security. Applying such settings to a host of machines can be a tedious task for even the most experienced administrator.

The best way to simplify this aspect of operating system hardening is to use security templates. A security template contains hundreds of possible settings that can control a single or multiple computers. Security templates can control areas such as user rights, permissions, and password policies, and they enable administrators to deploy these settings centrally by means of Group Policy Objects (GPOs).

Security templates can be customized to include almost any security setting on a target computer. A number of security templates are built into Windows. These templates are categorized for domain controllers, servers, and workstations. These security templates have default settings designed by Microsoft. All of these templates are located in the C:\Windows\Security\Templates folder. The following is a partial list of the security templates that you will find in this folder:

- **Hisecdc.inf:** This template is designed to increase the security and communications with domain controllers.

- **Hisecws.inf:** This template is designed to increase security and communications for client computers and member servers.

- **Securedc.inf:** This template is designed to increase the security and communications with domain controllers, but not to the level of the High Security DC security template.

- **Securews.inf:** This template is designed to increase security and communications for any of the client’s computers or member’s servers.

- **Setup security.inf:** This template is designed to reapply the default security settings of a freshly installed computer. It can also be used to return a system that has been misconfigured to the default configuration.