AN INTRODUCTION TO SYSTEM HARDENING - WINDOWS EDITION

2017-2018

DANIEL PLAZA
DANIEL.ROE.PLAZA@HOTMAIL.COM

Hello there! My name is Daniel Plaza. I am the writer of this manual. This manual was originally created as training material for the school I attended during CyberPatriot season VIII and IX, however, I felt that it would serve a better purpose in the hands of the community, where circulating information can educate all and give better tools for the future.

My experience comes from consistent research, study nights, teaching, and hours of preparation and experience. Those who would like to recommend and add on to this manual can contact me at daniel.roe.plaza@hotmail.com

Any additional comments and requests can be sent there. I hope you enjoy the content in this manual. – Daniel Plaza

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Notes

SECTION 1 – PREPARATIONS

Welcome to the World of Cyber Security!

I suppose that the first thing you may as well hear from me is an introduction to what cyber security is in the first place. Cyber security is the creation of systems, technology, processes, and techniques used to protect data, networks, and technology from attackers and unauthorized access.

There are many examples as to why cyber security is important. The lack of people filling jobs, hundreds of data breaches each year, ransomware attacks crippling things such as the healthcare industry. It hurts to see these things happen. Simply looking up cyber security will give you a headline of the next biggest disaster.

What can we do about it? First off, let's look into the CyberPatriot program. It is a National Youth Cyber Defense Competition. This was what got me into cyber security in the beginning.

When I was younger, I used computers all the time. It's a shame whenever something happened to any computer, I couldn't understand what was going on while trying to fix it, eventually giving up. Introducing high school, apparently there was a club about cyber security, it was called CyberPatriot. I wondered, What is there in CyberPatriot that could interest me? Just from hearing cyber security, I thought to myself that it was some shady hacker thing, but in reality, it was the exact opposite! It was hands-on, real world education that got me hooked.

While our CyberPatriot team had done poorly the first round, we improved. I had taken the initiative to create notes, documentation, and researching out of school. I had done my best, we had done better, but not good enough.
Fast forward to my junior year, I had taught, written material and trained almost every individual, and we had gotten so close to our goals, we had actually received the recognition we had gone for.

Today, I am writing a book, a book that I hope will help you in your journey in CyberPatriot. Whether you're a mentor, student, or someone who is curious about system hardening, I've worked hard for days on end to bring a fantastic guide on the basics on Windows Hardening, which is the barebones education of CyberPatriot and its core skills.

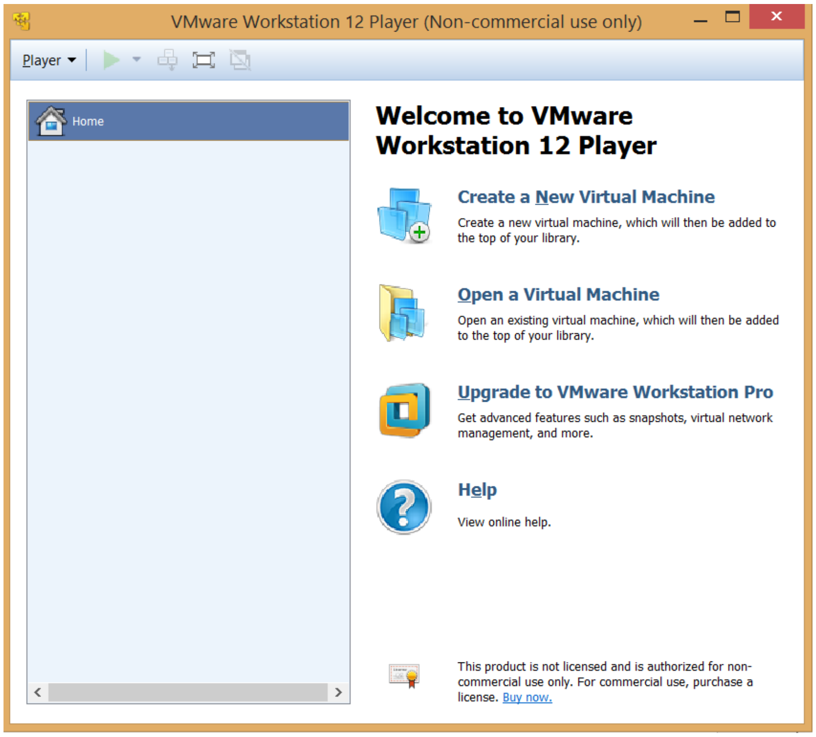
On the next page, we're going to talk about the program used at the core of the program, VMware.

What is VMware player? VMware is the program used during practice to emulate an actual computer, it will also be used during every competition for CyberPatriot. So, simulating a virtual environment.

VMware creates everything in a sandboxed environment, meaning nothing can get in, nothing can get out. So if there were any viruses in this VMware image (the simulation), we won't be in any trouble as we cannot affect any computer outside of VMware Player.

The next question would be, how do I open the images? Images can be opened by simply starting up VMware Player and loading them. Once the program has been started, this is the menu VMware greets you with. Let's start by clicking Open a Virtual Machine!

From your point of view, you won't have an image to open yet. To start, it'll be best if you place the image on your Desktop or your Documents folder. You will receive the image in a compressed folder from whoever is assisting you with setting up your computer.



Welcome to VMware Workstation 12 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

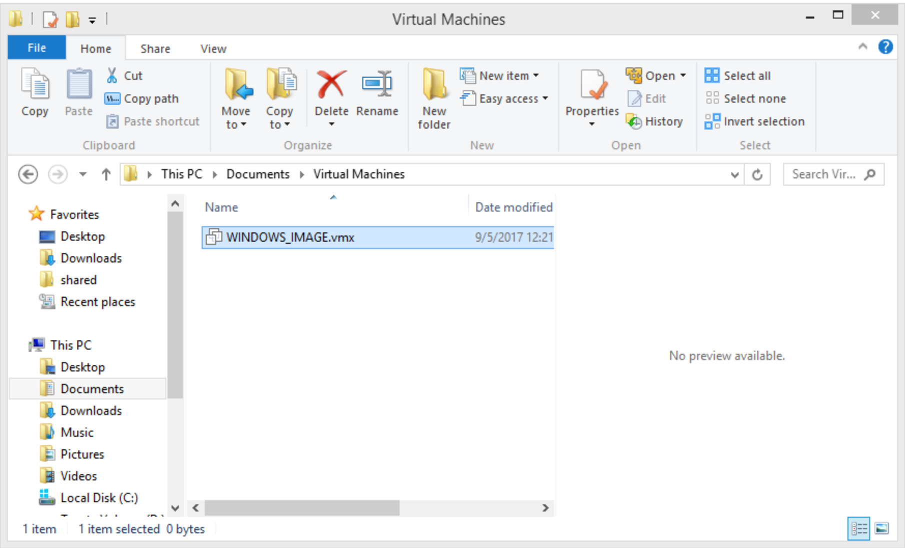
Help

View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

It is more than likely that the image will be in a compressed folder. A compressed folder is a way to save space and makes things easier to transfer. Let's assume the folder is WINDOWS_IMAGE.zip. When you right click it, there will be an option to extract all, that's what you'll want to do. Extract it wherever you want to extract it, and then get to the folder through Open a Virtual Machine on VMware as shown in the picture to the left.

When you're given an image, the file you'll want to open will be a VMware virtual machine configuration.
The configuration file will normally be placed in the folder and end up being the only file that you can select. The type will read "VMware virtual machine configuration file". It might also have the extension ".vmx"



Name	Date modified
WINDOWS_IMAGE.vmx	9/5/2017 12:21

1 item 1 item selected 0 bytes

The image will start up like any normal computer. When you first open this image, there will be a variety of accounts to choose from.

If you have anything you want to add into this book, take a second to write it in the next two pages!

In the next section, we're going to talk about passwords.

Notes

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Notes

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

SECTION 2 – PASSWORDS

No one ever thinks twice about changing their 4 year old password. If it ain't broke, don't fix it, right? This is true to most people, at least until someone accesses your account when they clearly shouldn't have been able to, then you think, "Oh boy, what was wrong with my password?"

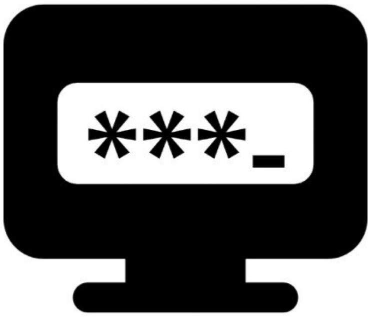
Every day, attackers guess, brute force or socially engineer their way into other user accounts, it's a cycle that repeats itself every day. This isn't anything new either, as many people tend to pick bad passwords or fall into traps that make them victims to all sorts of attacks.

Now, what is a good password? I think plenty of people have been bothered multiple times by various websites that their password needs one capital letter, a number, a symbol, or perhaps it just barks at them because their password 'password1' is way too similar to 'password'.

Good password habits are a thing you need to develop when being a system's administrator. The first thing you need to understand is that these guidelines are very important for the sake of your AND your system's security, second, you need to educate your users on the threats of attackers and what they need to practice with their password habits. We'll talk about the password habits and what they could potentially protect you against in just a second.

Now, a good password would **follow these particular guidelines**:

- The password has no relation to you
- The password has not been used in the past
- The password has one capital letter
- The password has one lowercase letter
- The password has one number
- The password has one symbol
- The password contains a length of 9 characters or more (for standard users)
- The password contains a length of 14 characters or more (for administrators)



Now, it might seem like a lot to remember, but believe me, it sticks, especially when you're reminded of it practically every day. But what do these password guidelines protect you against?

These passwords guidelines can protect you and your users from various types of attacks, I'd like to classify these types of attacks as "automated" meaning, nobody will be there constantly, they will wait for the process to finish and output results. Either way, it's better to have some protection than none at all.

- Password Guessing – Password Guessing is just simply guessing passwords, while this is not an automated process; it's still done the same way as other methods, just more simply. This can be used by attackers who have researched their subject in a way to get a better idea of what their password might be. For instance, someone might use something related to them as their password as it helps them remember it, but this should be avoided.
- Brute Forcing – Brute Forcing is the use of an automated program to guess every possible password. Now, this can be hard to do when we apply all of the guidelines above. And I mean that. It might take years, hundreds or thousands to break into your account. But this is only as long as your password is strong.
- Dictionary Attack – This is similar to a brute force, however, it incorporates large amounts of words and adds them to the process. If your password is a mix of numbers, letters, symbols, this can make this type of attack as effective as Brute Forcing a good password.

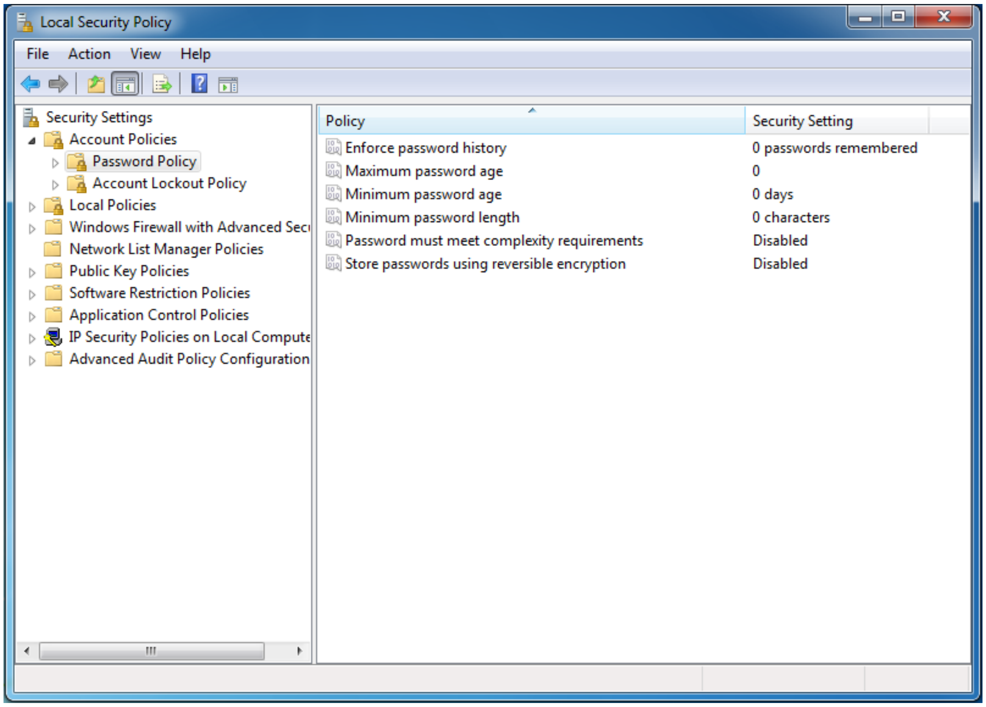
- Rainbow Tables – A rainbow table is basically a precompiled table for reversing password encryptions, which means simply it cracks the way the password was encoded. This password attacking method tends to be a very lengthy process, while it may work a lot better with older ways of storing passwords, to this day you might need terabytes of Rainbow Tables to crack into modern encryption. (Encryption is basically encoding something if you didn't know!)

These are only some of the few basic methods of breaking into passwords; fortunately, it can be avoided with a password policy and good password habits. So what do we know now? From this point, our main concern is not how can we change our password, but how can we change everyone's password?

When a system is compromised, everyone's password must be changed. Passwords would normally be changed then and once again right after the system has been fully secured, however, we won't be doing that. What we'll be doing first is enforcing a password policy. A password policy is a set of rules that must be followed for passwords.

How we'll do this is by modifying the Local Security Policy. While this part of my curriculum has been saved until the very end, you'll learn how to do just one part of it for the moment. Now, to begin modifying the Local Security Policy, you should start by hitting the home button and proceeding to type "local security policy".

Once you've done so, you'll be presented with the following.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

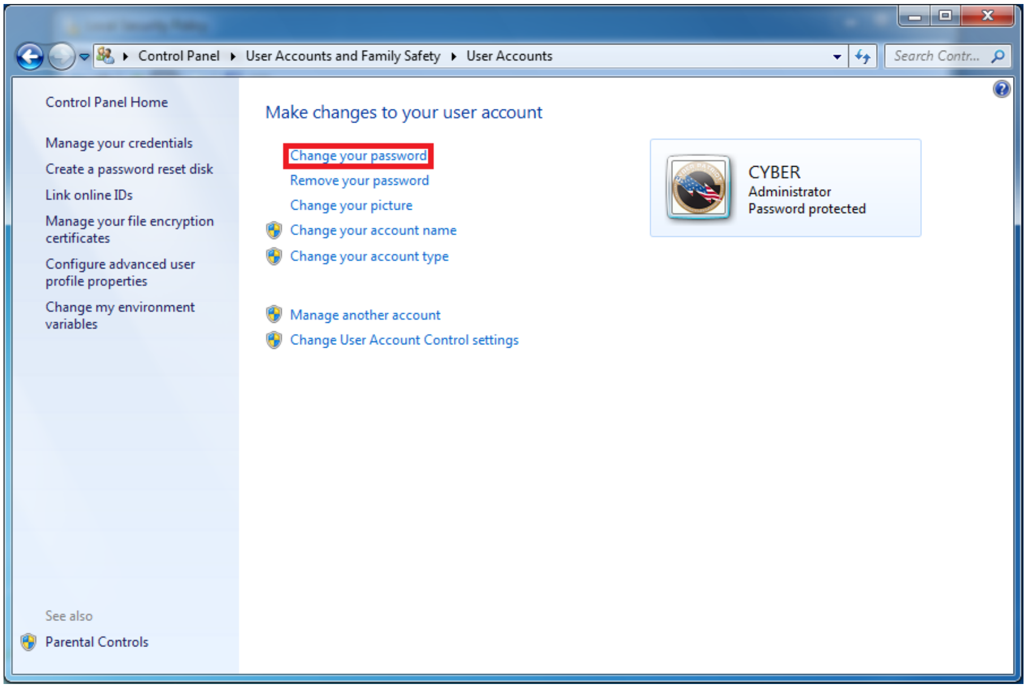
This is the Local Security Policies. Essentially, it's an area where a lot of computer settings are defined. Here, you might score a lot of points during the competition, we'll go over this a couple sections later, however, for now, we'll just be talking about passwords and password related things. Here are the recommended settings for the Password Policy:

Enforce password history	24 passwords remembered
Maximum password age	30-90 days
Minimum password age	15 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Here is my explanation for each setting:

- Enforce password history – This is to make it so that passwords cannot be reused. Windows only allows a maximum of 24 passwords kept on record, that's plenty.
- Maximum password age – This varies from account types. We'll mention it very quickly, User password ages should be 90 and Administrator password ages should be 30. What a password age is the maximum days that password can be active.
- Minimum password age – The minimum password is used to prevent people from reusing passwords. For instance, while the password history is 24, someone might want to change their password 23 times so they can reuse their password. This prevents such a thing.
- Minimum password length – The minimum password length is the minimum amount of characters the password will require to be acceptable. *This has been updated in this book, it's 8 characters.*
- Password must meet complexity requirements – This means that the password must meet at least 3 complexities
- Store passwords using reversible encryption – This means the passwords of the system are stored somewhere and are able to be decrypted, this is a very big no!

Changing passwords can be done in various ways actually, for example, one of the simplest methods to changing passwords is by using the Control Panel. To do so, go to the Control Panel, then go to the User Accounts and proceed to click the accounts. You'll receive a list of User Accounts existing on the system, click the account you'd like to modify and change the password from there.



Control Panel ▸ User Accounts and Family Safety ▸ User Accounts

Search Contr...

Control Panel Home

Manage your credentials

Create a password reset disk

Link online IDs

Manage your file encryption certificates

Configure advanced user profile properties

Change my environment variables

See also

Parental Controls

Make changes to your user account

Change your password

Remove your password

Change your picture

Change your account name

Change your account type

Manage another account

Change User Account Control settings

CYBER

Administrator

Password protected

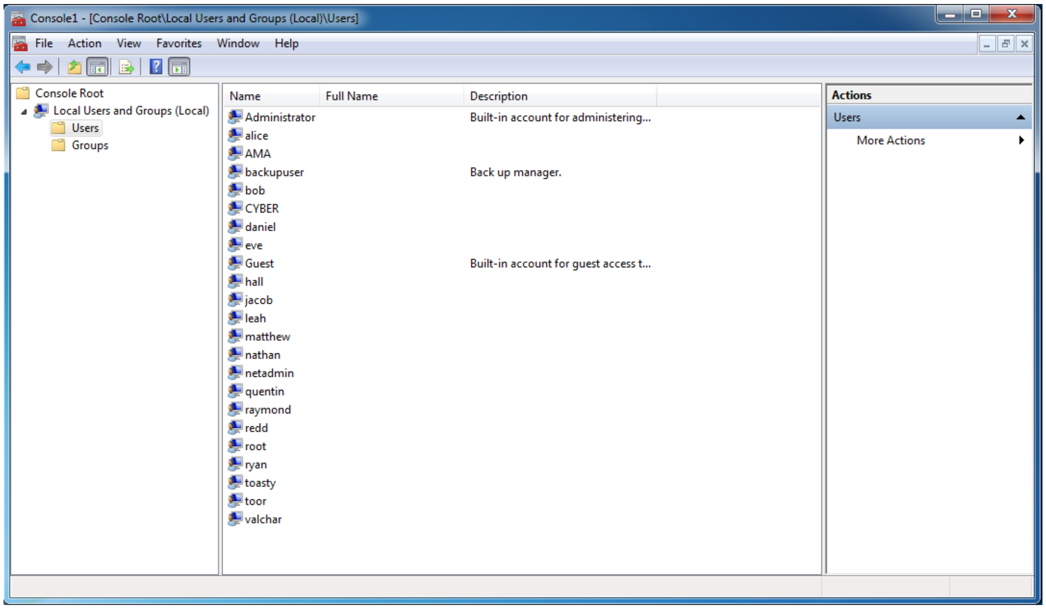
While this method is very practical and simple, it's unfortunately very tedious and inefficient when it comes to speed. The next method, however, is much more of a standard, as it allows efficient and quick password modification.

We'll be introducing our first tool, Microsoft Management Console.

The Microsoft Management Console (MMC) is used to modify a variety of settings in a very quick matter, for an Administrator. How we'll be able to modify passwords is by using the snap-in Local Users and Groups in Microsoft Management Console. From this point, you'll have a list of user accounts in Microsoft Management Console, you can right-click the user and set a password from there. This allows you to track the passwords you change with ease.

To open Microsoft Management Console, press the 'Windows Button + R' and then type "mmc" into the run prompt.

Once you've done so, the Microsoft Management Console should appear, and when it does, click File → Add/Remove Snap-In and then from within the list labeled "Available Snap-In's" click the Snap-In Local Users and Groups. Click the Add button and then press OK at the bottom. When finished, you should receive the following.


Console1 - [Console Root\Local Users and Groups (Local)\Users]
File
Action
View
Favorites
Window
Help
Console Root
Local Users and Groups (Local)
Users
Groups
Actions
Users
More Actions

Name	Full Name	Description
Administrator		Built-in account for administering...
alice		
AMA		
backupuser		Back up manager.
bob		
CYBER		
daniel		
eve		
Guest		Built-in account for guest access t...
hall		
jacob		
leah		
matthew		
nathan		
netadmin		
quentin		
raymond		
redd		
root		
ryan		
toasty		
toor		
valchar		

Now, what this is a list of all of the users currently on your system. This is a screenshot from the MVHS_WIN_7 image.

What we were talking about was modifying passwords. For instance, if you right-click a user and click Set Password, this will allow you to change their password.

Now, once you've changed a password like so, you may as well do it for ALL users.

That's all I can really say about this section when it does come to changing passwords is that it should be done with whatever method you're comfortable with, but I'd highly recommend that you practice with all methods and get used to this information.

In the next section, we'll be discussing how to manage Users.

SECTION 3 – USERS

There isn’t much of a point securing passwords when there are potentially harmful accounts and accounts avoiding our policies dwelling on your system. In this section, we’ll talk about types of accounts, account settings, what to secure and the things you’ll encounter that shouldn’t exist.

Let’s begin with the simple types of accounts, the regular User, and the all mighty Administrator.

Regular users usually have restricted rights, meaning they cannot modify system objects or settings, install or uninstall programs, commit any system changes or modify anything relating to other users. There isn’t really that much that a user can do, *however*, being a user still means access to the system.

Administrators have the ability to modify essentially anything on that system they like, which is why there should be a very small amount of Administrators on a system. The status of being an Administrator is a very important role within a system and should be only given to those who truly need the role.

Now, let’s get to the main point of what we’ll be learning. A README or someone will tell you what *should* or *should not* exist on that system. As a result, anyone who is not on said list should be removed. Now, to remove a user, we’re going to be using Control Panel. Typically, I would suggest using Microsoft Management Console (MMC) however, it may be better to use Control Panel.

Now, **before deleting a user**, you should ensure that it’s completely okay to do so. *It should be noted that if you choose to delete a user, a special identifier used SAM (Secure Account Manager) is deleted for them to prevent intrusion*. Ensure that you have answered ALL forensics questions before deleting the user. To delete a user, start by going to Control Panel → User Accounts → Manage Account → Click the Account → Delete The User.

It’s really that simple, just remember to ensure all forensics questions have been answered correctly.
Now, **what if a user is missing**? When a user is missing, you may have to end up **adding a user**. This should also be done on Control Panel as it adds both the user and the directory. You can also add a user with Local Users and Groups via Microsoft Management Console by right clicking in the middle and adding the user.

This set of instruction is making sure that the roles are established correctly to all of the users. That means Users are Users and Administrators are Administrators. How can you do this? With Microsoft Management Console.

Let’s get this started up by launching the Microsoft Management Console. Once you have the Microsoft Management Console Launched, add in the snap-in Local Users and Groups. Proceed to go into the Groups category and there you have it. What you will see is a list of various groups.

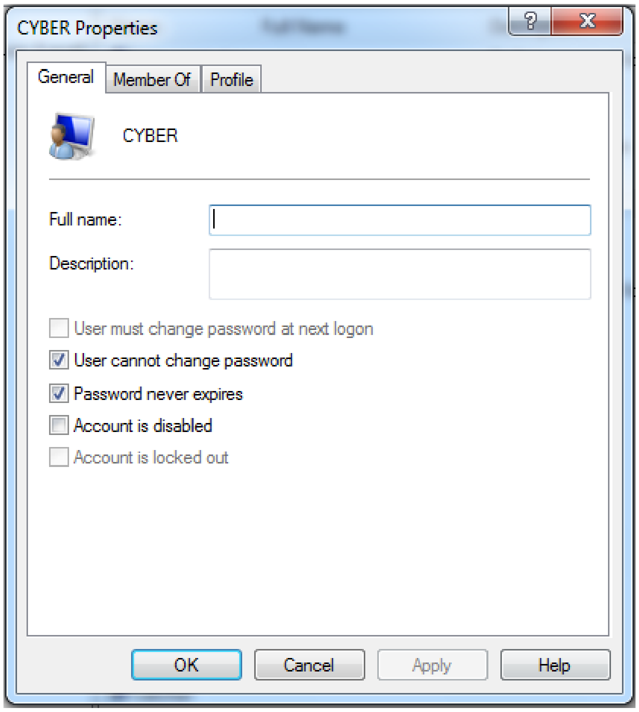
As far as I’m concerned, you’ll only have to ensure that people are either Users or Administrators unless told otherwise. Nobody will usually be in other groups, but it’s a good idea to just check at least.

The next area we’re going to look into usually passes up people. Honestly, it gets past me other times as well, but this is when I didn’t know that this feature had existed. What we’re going to look at are User properties. To start, within the Local Users and Groups snap-in, go into Users and right click on our user, CYBER.

Now let’s talk about **User Properties**.

User properties are essentially special extra settings that can be toggled for some users. I’ll explain each setting.

- ❖ User must change password at next logon – This is usually checked if that person's password has expired for instance.
- ❖ User cannot change password – Do not have this set as it violates our password policy.
- ❖ Password never expires – Self explanatory. Violates our password policy.
- ❖ Account is disabled – This is for disabling an account.
- ❖ Account is locked out – Meaning the account cannot be accessed, sometimes this setting activates if a certain thing is triggered; we’ll get to it in just a second.



CYBER

Full name:

Description:

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out

Sometimes if you try accessing an account far more than you should, you’ll get locked out, now. What can this prevent? Guessing or brute force to a certain extent. What can we set to lock out accounts? The Local Security Policies, go ahead and jump into Local Security Policies (a short cut would be press the ‘Windows Button + R’, type ‘secpol.msc’, press enter and it’ll launch. From that point, you’ll go into the Account Lockout Policy area of it within account settings.

Here are the correct settings for it, I’ll explain each setting.

Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Note: You cannot modify the 1st and 3rd setting unless you modify the 2nd setting here.

- ❖ Account lockout duration – How long this user will be locked out
- ❖ Account lockout threshold – How many times the password must be incorrect before getting triggered
- ❖ Reset account lockout counter after – This prevents the next password wrong from locking out the account for another 30 minutes instead of giving the user another 5 chances

Now, let’s talk about the built-in accounts. There are two accounts that are built into the system. The built-in Administrator and the Guest account. The built-in Administrator is usually disabled by the system, however, it might be enabled and *should* be disabled. The guest account may also be active, this account should not be allowed as well.

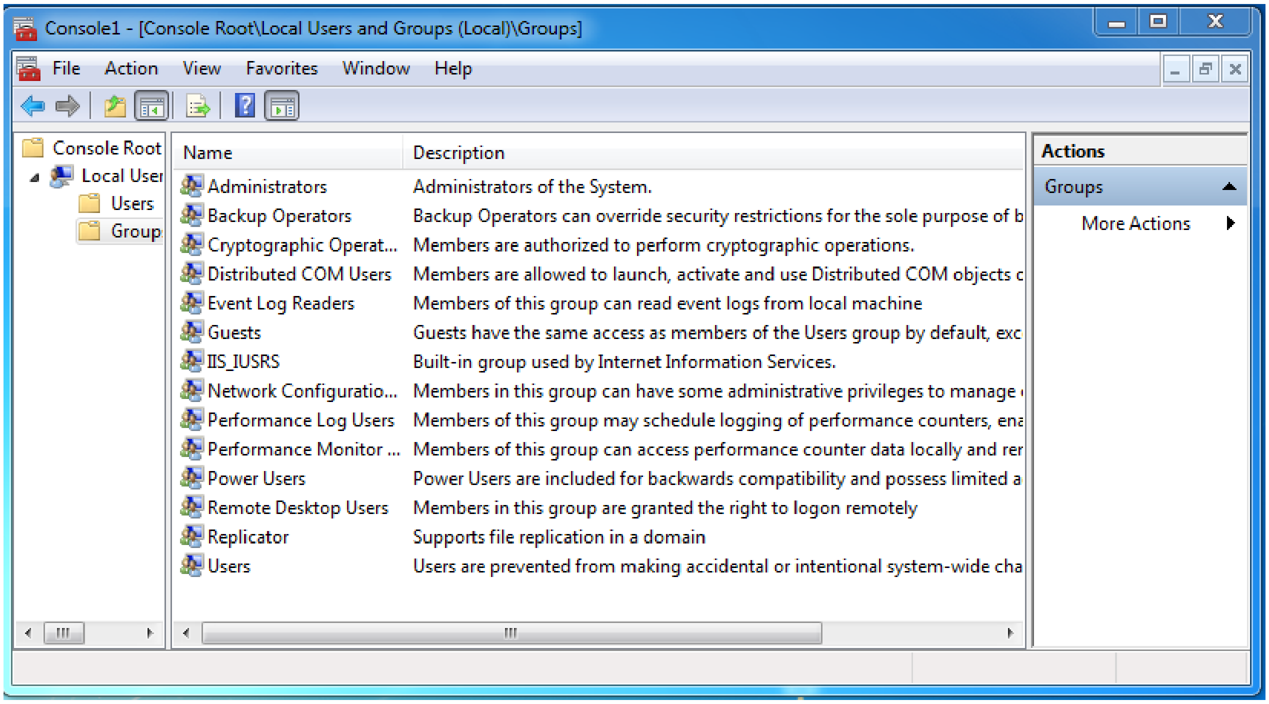
To secure the built-in accounts, give them a password and rename both of them. Simply use Local Users and Groups on Microsoft Management to go into their user properties and disable them.
In the next section, we’re going to talk about User Groups.

SECTION 4 – USER GROUPS

Since we’ve finished talking about users and rights, we’re going to dive into the subject of User Groups.

Now, we defined Users and Administrators, however, there are many more user groups, and sometimes, there might be groups that shouldn’t exist or perhaps hint at something within the system that should not exist.

For now, I’m not doing to go into detail, much rather, I’ll show you what you’ll normally see within the group's section of the Local Users and Groups Snap-In.



Name	Description
Administrators	Administrators of the System.
Backup Operators	Backup Operators can override security restrictions for the sole purpose of b
Cryptographic Operat...	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects c
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, exc
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuratio...	Members in this group can have some administrative privileges to manage
Performance Log Users	Members of this group may schedule logging of performance counters, ena
Performance Monitor ...	Members of this group can access performance counter data locally and rer
Power Users	Power Users are included for backwards compatibility and possess limited a
Remote Desktop Users	Members in this group are granted the right to logon remotely
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentional system-wide cha

This is what you’ll normally see in Local Users and Groups. Almost all of the time, you’ll only have Users in the Administrators or Users group, *be sure to check that the right users are in the right group*.

I didn’t show you how to change a users group type because that should have been saved for this section, so I’ll go ahead and elaborate on that. To do so, go to the Users section of Local Users and Groups and right-click the User and go to their properties. Next, you must go to the Member Of tab, once there, you can see who they belong to and who they don’t.

When it comes to **deleting or adding a group**, it’s the same process as adding a user on Local Users and Groups. Simply right click anywhere within the information and click New Group or right click on a group and delete it.

The default groups are something that’s perfectly fine to keep on your computer. Just ensure that people are the correct type, otherwise, you may run into problems.

This section wasn’t mean to have too much information, as it is rather simple. The next subject will be Control Panel.

SECTION 5 – CONTROL PANEL OPERATION

I'm sure plenty of ordinary people have messed with the Windows Control Panel before. From adding accounts, changing passwords, guests, etc. There are plenty of things that the Control Panel can do, but there are somethings that need to be checked to ensure that they are configured.

In this section, you'll learn about all sorts of utilities and areas in Control Panel's System and Security and learn how to configure them.

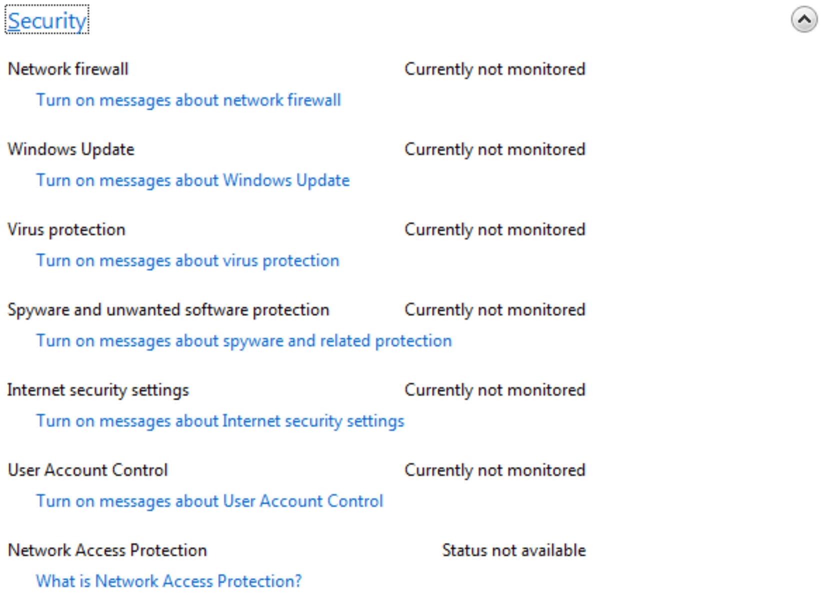
System and Security provides a wide variety of areas, we'll start with the **Windows Action Center**.

I know most Windows 7 Users have been annoyed by it, telling you that you haven't backed up in a while or that you have no Anti-Virus.

The Action Center is there to notify you about all sorts of things going on. The things that Action Center will notify you about are things such as the Firewall, Windows Update, Virus Protection, etc. One thing that attackers may attempt to do (if you didn't know this) is turn off the notification of said things. Windows Action Center is there to warn you whenever something goes wrong or things are going badly. All you can really do here is reconfigure the settings. To do so, while in Action Center, click Change Action Center settings and turn on all of the notifications.

Once that has been done, your computer will yell at you over many security issues most likely. This is good! Because now you can get an idea of what you need to do.

This is an example of the notifications in Action Center being turned off.



Security

Network firewall — Currently not monitored
Turn on messages about network firewall

Windows Update — Currently not monitored
Turn on messages about Windows Update

Virus protection — Currently not monitored
Turn on messages about virus protection

Spyware and unwanted software protection — Currently not monitored
Turn on messages about spyware and related protection

Internet security settings — Currently not monitored
Turn on messages about Internet security settings

User Account Control — Currently not monitored
Turn on messages about User Account Control

Network Access Protection — Status not available
What is Network Access Protection?

Next thing we'll be talking about is **User Account Control**, also known as UAC. UAC is a tool used to restrict the use of Run as Administrator and making any changes to the computer, unfortunately, have a couple more pop up's when we run things as an Administrator, but on the bright side, the security of the system is much increased.

For example, let's say an Administrator has made the mistake of leaving their computer open, won't be good in the end.

If User Account Controls have not been set to a higher setting, someone may be able to come by and run something with Administrator Access with Administrator Access (for example, Local Security Policies) they will be able to commit changes to your system.

How do we access User Account Control? It's in the same place as Action Center, on the left side of Action Center, you will see a setting Change User Account Control, from that point, you should increase the bar to the highest level in Action Center?

Have it raised to Always Notify; this will raise your security settings to the point where every action which requires Administrator Access will require a confirmation by an Administrator, which again is a good thing.

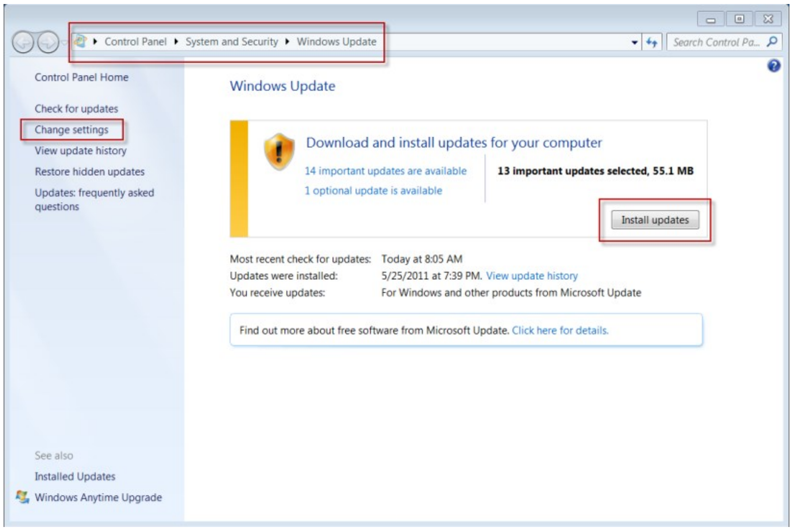
The next setting we'll be talking about is **Windows Update**.

It's bad when user's choose not to update their things. Believe me, I'm a person who does this as well, however, if a business that is vulnerable to attacks does this, it may be big trouble for them. What am I talking about? Updates. Windows Update was a program designed to allow Microsoft to send updates to their consumers and businesses so that they can prevent vulnerabilities. *To note about updates: Sometimes manual updates are better for certain environments, such as servers or places that need to have updates tested prior to implementation. If you implement it for the end user, it may be perfectly fine.*

When I say these updates are very important to a system, not only do they fix problems, but they can keep your system in shape as well. That's why I recommend keeping Windows Update always ready to do its thing.

So how do we configure Windows Update? To start, we're going into System and Security in Control Panel, from there, we'll go to the Windows Update section.

By default, we should be installing updates automatically. If the setting is not configured to that, do so as soon as possible. When it comes to updating your computer, do so as soon as you can, as this is very important for receiving points. As well, you should include recommended updates by Microsoft.



Windows Update

Download and install updates for your computer

14 important updates are available

1 optional update is available

13 important updates selected, 55.1 MB

Most recent check for updates: Today at 8:05 AM

Updates were installed: 5/25/2011 at 7:39 PM. View update history

You receive updates: For Windows and other products from Microsoft Update

Find out more about free software from Microsoft Update. Click here for details.

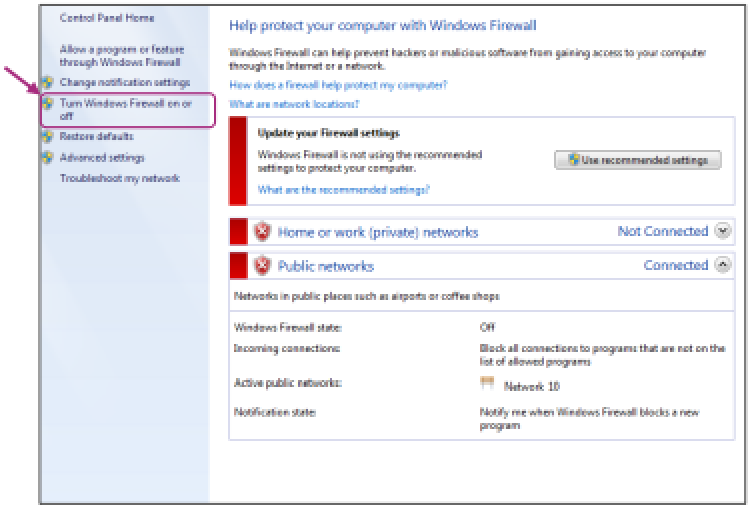
You need to understand that a patched PC is a protected PC, there are no exceptions except of course if your Administration team has to manually approve updates, however, that is not the case right now.

The next subject we're going to be talking about is the **Windows Firewall.**

Now from what I know, this is possibly one of the most loosely thrown around terms I've ever heard of. What is the firewall in the first place? Well, the Firewall is a special service added into Windows back around Windows XP, it was used to prevent unauthorized connections from getting to your computer.

We're going to call these **inbound** and **outbound** connections. Inbound is what you would consider incoming connections, noticeable, almost every type of firewall usually advise you **block inbound.** It's a different story when it comes to working with outbound. Basically, you just want **outbound connections being allowed**, if you want to make it more secure, only allow outbound with the programs you trust, but we won't worry about that right now.

To start security, simply going to Control Panel > System Security > Firewall will allow you to access its controls. Typically, the Firewall will be disabled as a whole and might have some problems starting up.


Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
How does a firewall help protect my computer?
What are network locations?
What are the recommended settings?
Use recommended settings

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

Update your Firewall settings

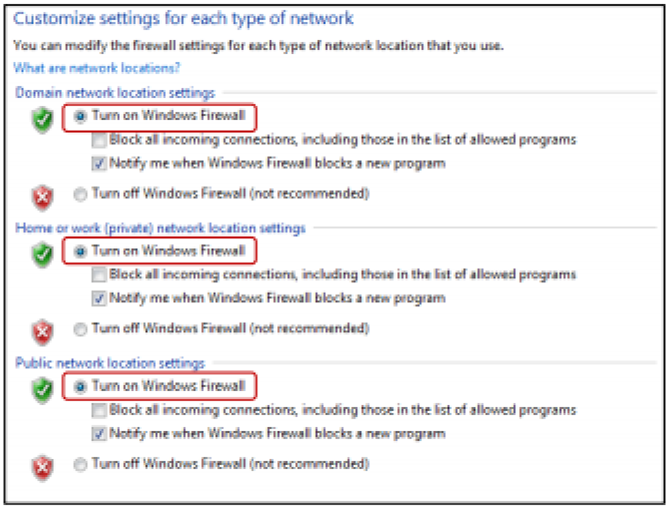
Windows Firewall is not using the recommended settings to protect your computer.

Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Network 10
Notification state:	Notify me when Windows Firewall blocks a new program



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

Domain network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

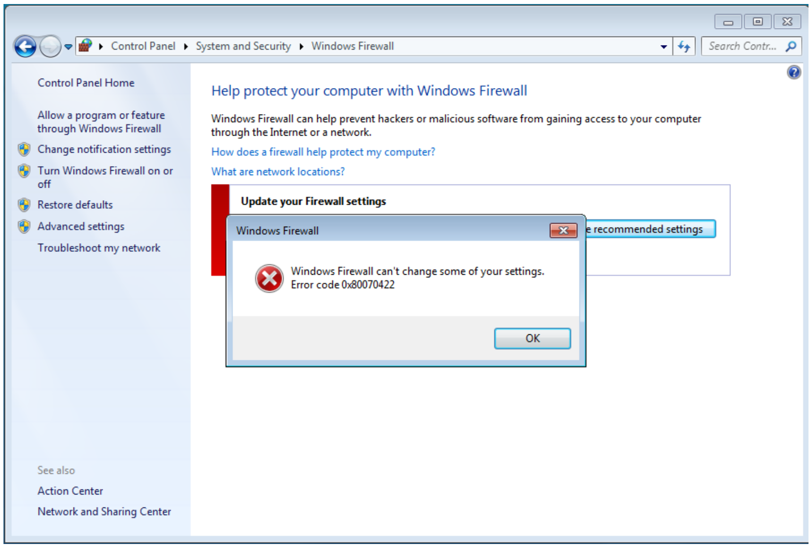
● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

From the 2 photos above, this is more than likely what you will be dealing with. In the photo on the left, you need to click the option Turn Windows Firewall on or off, then, in the photo to the right, you need to configure *your* settings to those. This will ensure that a secure and stable *basic* firewall is running and enforced. There might be the occasional error, for instance, let's look into what happens when the Firewall refuses to cooperate.


Control Panel ▸ System and Security ▸ Windows Firewall
Search Contr...
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
How does a firewall help protect my computer?
What are network locations?
e recommended settings
OK

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

Update your Firewall settings

Windows Firewall

Windows Firewall can't change some of your settings.
Error code 0x80070422

This particular error is one you may end up running into a lot more than anything else.

I've run into issues where the Firewall will not turn on because whatever infected the system has disabled its functionality, thus making the average user completely puzzled.

However, we'll be jumping into a new tool in just a second that allows you to take the first step to taking back control of your system.

Now this is just a quick visitation into this tool, it's called the Windows Services.

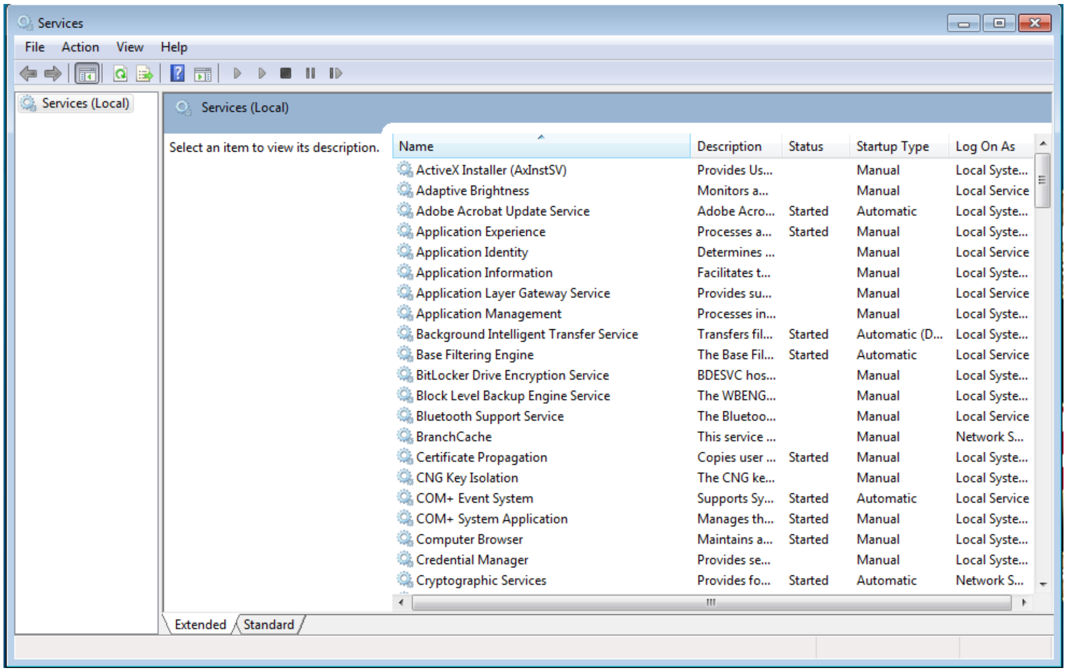
Now, I might as well say what is a service? Essentially, consider it an important process within a computer that runs in the background, something that either helps it run or is just an important utility; would a firewall be an important object? Absolutely, it's one of the most important things for a system – which is why any attacker or virus would want to disable it.

Let's jump into the Services Application.

To do so, use Windows Button + R and type 'services.msc'. This will open the Windows Services.

Once here, you'll see so many services, it's likely you won't know where to start.

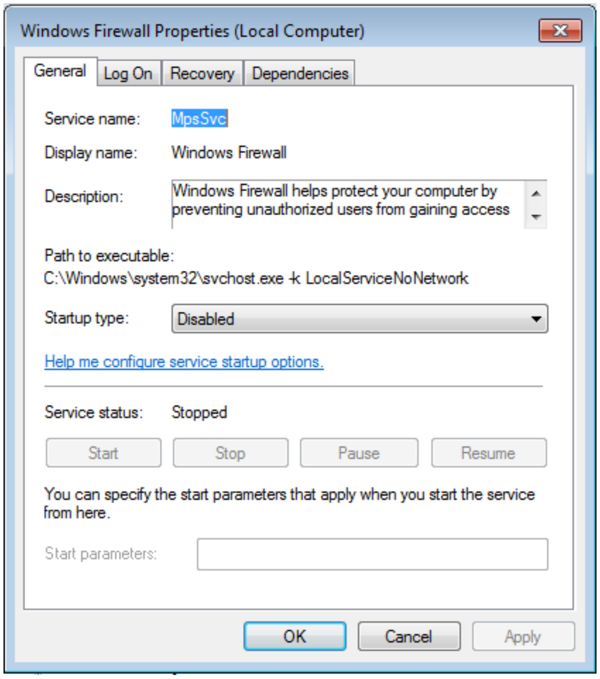
To simplify it, you should just click the Name Category, that'll rearrange everything from Z to A. This also works when you hit Startup Type (from manual to automatic, automatic to disabled, etc.) because right now we're looking for the Disabled Windows Firewall.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adaptive Brightness	Monitors a...		Manual	Local Service
Adobe Acrobat Update Service	Adobe Acro...	Started	Automatic	Local Syste...
Application Experience	Processes a...	Started	Manual	Local Syste...
Application Identity	Determines ...		Manual	Local Service
Application Information	Facilitates t...		Manual	Local Syste...
Application Layer Gateway Service	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
Background Intelligent Transfer Service	Transfers fil...	Started	Automatic (D...	Local Syste...
Base Filtering Engine	The Base Fil...	Started	Automatic	Local Service
BitLocker Drive Encryption Service	BDESVC hos...		Manual	Local Syste...
Block Level Backup Engine Service	The WBENG...		Manual	Local Syste...
Bluetooth Support Service	The Bluetoo...		Manual	Local Service
BranchCache	This service ...		Manual	Network S...
Certificate Propagation	Copies user ...	Started	Manual	Local Syste...
CNG Key Isolation	The CNG ke...		Manual	Local Syste...
COM+ Event System	Supports Sy...	Started	Automatic	Local Service
COM+ System Application	Manages th...	Started	Manual	Local Syste...
Computer Browser	Maintains a...	Started	Manual	Local Syste...
Credential Manager	Provides se...		Manual	Local Syste...
Cryptographic Services	Provides fo...	Started	Automatic	Network S...

When you find the service, you can right click it and check out its properties.


Windows Firewall Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: MpsSvc

Display name: Windows Firewall

Description: Windows Firewall helps protect your computer by preventing unauthorized users from gaining access

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

The photo that reads 'Windows Firewall Properties', and clearly it shows that it is disabled and stopped. Clearly, this should not be the state of our firewall, from this point, you should change the Startup Type to "Automatic" and then start the Service.

After that, you can go and ensure that the Windows Basic Firewall is in good condition (running, inbound blocked, outbound allowed).

There are two other categories in the Control Panel that I will talk about briefly. The first category is the Users and Accounts, as far as I'm concerned, we know quite a bit about it already so I won't touch on that one too much.

The second category is the Network and Internet Section. This section hosts the Internet Options. The Internet Options itself will have a chapter dedicated to it in a couple sections, for now, we won't touch upon that subject.

So let's get to the point of this, we know that the Control Panel hosts Windows Update, Firewall, Action Center and User Account Control.

In the next chapter, we'll learn all about the world of Malware and how it can affect your computer.

SECTION 6 – VIRUS INTRODUCTION

Computer viruses is another term that I hear very much from various people. They pretty much lump all of them into the same category. Most of them are not in the same category, and for a security professional, they need to be able to point the problems in the right direction when it comes to identifying a virus.

So let's get to the biggest question we have, what is a "virus"? A computer Virus is known as a malicious program that, when executed, replicates by copying itself into a variety of things on your computer. From other programs, your pictures or your boot sector, any part of your computer can become infected!

Computer Viruses can cause many problems from your computer; from spying on you to completely controlling your computer, it's clear they're not wanted. In this segment, we'll be learning about Viruses and little hints that can tell you that they're there.

Now, when it comes to viruses, there is more than one type of virus.

There are things such as malware, Potentially Unwanted Programs (PUPs) and worms. Have you heard of the other two? I'll address that, a Potentially Unwanted Program (PUP) doesn't have any extremely troublesome things, as far as I'm concerned, the things such as spying, hijacking your browser, making your computer slower, etc. is what you'll normally get from PUPs.

We also have worms. Worms are viruses that are standalone viruses that replicate from one computer to another, relying on exploitation and security failures to access the computer and continue from that point. Worms CAN be defeated, however, they are an absolute nightmare to deal with. Now, normally, on a local network, such as your home network, a worm may not be such a threat, however, a modern office with all the computers running the same thing can possibly be a wreck waiting to happen.

Of course, there's regular viruses, malware. Malware can intercept and steal data, launch attacks, damage computer software or hardware and cause a denial of service.

PUP - Browser Hijacker

Let's talk about this one first, it's the most common I've seen. A browser hijacker will hijack your browser, installing add-ons onto your computer, having toolbars randomly added and change your homepage. It's one of the most troublesome PUPs. Of course, it doesn't pose as too much of a threat unless you consider not being able to immediately google like you normally do a threat. But it can come at worst costs, in fact, sometimes these programs can't be detected as viruses due to not having enough malicious code, resulting in them being undetectable as a virus, but much rather as a PUP.

Typically a browser hijacker will come bundled with free programs, and it will not easily uninstall every once in a while, for instance, Search Protect by Conduit is one of the biggest offenders here, as it tends to be downloaded by those who aren't watching what they're downloading.

Symptoms of Browser Hijacker: Your homepage being changed, your search provider being changed, new add-ons, inability to be removed by normal methods, the overall takeover of your browser.

PUP - Spyware

Another Potentially Unwanted Program, and yes, it's exactly what It sounds like. Spyware is technology that will collect data about a person or organization without their knowledge. The information they get is sometimes sold, sometimes used to develop more malware and so many other things. Spyware will collect anything, and it is best that you remove it immediately as it is a direct violation of security, just like browser hijackers, they also tend to be bundled with other programs, so downloaded in the same fashion as a browser hijacker.

You can typically find Spyware as the program itself on the computer by simply checking along with seeing if the symptoms are correct. If the symptoms are there and the program you suspect has quite the reputation line, it's probably spyware.

Symptoms of Spyware: Unknown processes in Task Manager, strange programs found in the program list, computer and network slowdowns.

PUP - Adware

Very common, and possibly the most aggressive type of the Potentially Unwanted Programs. These programs will make it loud and clear that they exist. If you start seeing pop-ups, ads, messages and all other sorts of flashy ads without knowing what's going on, it's likely you have Adware on that computer. Adware, or advertising support, is Potentially Unwanted Software that creates an advertisement to make an author money or to help you get more viruses because nothing says a great time than "Download these cool viruses!" or "Free toolbar!"

If the ads get so bad to the point where they begin injecting "unmentionable" ads or more malware, it's clear that this is very bad for you and your computers.

Symptoms of Adware: Ads, unwanted ads, completely random ads & offensive ads.

Malware - Trojan horse

Let's begin with this one, ah yes. Trojan Horses are well known. Do you know of the tale of it?

"*The Trojan horse was a huge hollow wooden horse constructed by the Greeks to gain entrance into Troy during the Trojan War. The horse was built by Epeius, a master carpenter, and pugilist. That night, Greek Warriors emerged from the horse and opened the gates of Troy to allow the Greek army to get in the city.*"

What an amazing tale, and that's what we're dealing with here- well, sort of.

Trojan Horses are a general type of malware, disguising itself as a real program or download, but once it's in, all breaks loose in your computer and the damage begins. You can consider those "Greek Warriors" as malicious code, wreaking havoc on your computer. So, symptoms would seem obvious.

Symptoms of Trojan horse: Installed a program, the program introduced viruses into my computer.

Malware - Backdoor

Another one that sounds exactly what it sounds like, a backdoor will introduce itself a new way into your computer. Sometimes, backdoors are created for no malicious intent (a software developer would do that sometimes) and then, there are backdoors that are meant for malicious intent, ones that will spy on you, install computers on your program and remotely do whatever they want. What's the worst part is? It's a human actively doing things through that backdoor. Backdoors aren't too hard to detect, for instance, most webcams have a little light that will brighten up when your webcam is active, so if you see that randomly brighten up, that's a red flag or something else. If you've got things opening when they shouldn't be, another red flag. If your computer has been very slow, files have been placed in places you don't remember, and some software has been installed randomly, maybe there's a backdoor. There can be all sorts of symptoms that a backdoor exists, and it's very clear that it's not good.

You might not truly know whether one is there, as it could be something else, but when you do, it's concise.

Symptoms of a Backdoor: Strange processes in the Task Manager, programs that were never there are installed, files changing, changes you never did being done, heavy memory usage, security errors, etc.

Severe Malware - Ransomware

Most malware itself is already pretty severe, but the only reason we don't label it "severe malware" is because it doesn't do what this one does. The word ransom stands for holding one thing in exchange for another. Ransomware can go from being a scary message to completely erasing everything you have on your computer.

Ransomware tends to be a serious threat to security, for instance, there had been a serious problem with a type of malware called CryptoLocker back in 2014. This program would encrypt all of your belongings and threaten to make them unrecoverable unless you gave them money. Of course, sometimes it can sometimes do nothing.

It's called Scareware, it does scare the user, but it does nothing other than that. It simply scares the uses and tends to be hard to remove, this would change it to PUP status.

Symptoms of Ransomware: You're being threatened to do something in exchange for the safety of your computer. This virus makes it noticeable that it exists. Scareware does the same. For regular Ransomware, that's a tough battle, for Scareware? Not as tough.

Severe Malware - Boot Sector Viruses

Sometimes this is mixed with Ransomware, but before I continue, let me give you an explanation as to what the Boot Sector is. It's also called the Master Boot Record. The Master Boot Record (or, MBR) is the beginning sector of any hard drive that identifies how and where an operating system is so that it can boot up.

When a virus infects this portion of the hard drive, not only is it extremely hard to fix for the standard user, for instances, it's already way out of the reach of anti-virus, secondly, it may prevent you from booting into your operating system. One of the only ways you can clean it is by resuscitating damages via third party tool or recovery disk.

Symptoms of Boot Sector viruses: Immediate shutdown or restart, a rewrite of the MBR or VBR, unable to boot into Windows and being told you've been infected by a Boot Sector Virus.

Severe Malware - Rootkit

This is at the end of the dangerous malware category because this one has literally no solution other than completely clear your hard drive. First, you might hear this term a lot, but what does root mean? Root is the beginning of the operating system, root is the almighty power, the iron fist that controls all changes.

The big thing about them is that when they dig deep, they're almost undetectable. They don't leave easily and they infect deep in the operating system. It's like someone is infected with a virus, it's going through their blood and it going everywhere, including the heart. It's a backdoor with no end to its potential tyranny.

There really is no method to removing rootkits. It would be time to pull the plug and start over. The good news is that you won't deal with it now.

Symptoms of Rootkits: Well, if you have one, I'm sorry. The only way you could truly know is if your anti-virus detected it, otherwise, you're on your own.

Sophisticated Malware - Polymorphic Viruses

The point of the world Polymorphic is essentially a virus that changes in real time. This can be combined with any virus category just like any other, however, it's the most commonly combined. From ports, PIDs, names, etc. A Polymorphic virus can change anything it likes to avoid detection or cause trouble.

In case you ever find a polymorphic virus, your best bet would be continuously updating statistics such as network statistics or task list statistics to find something strange, and believe me, these viruses can stand out.

Symptoms of Polymorphic Virus: The virus will change randomly from the first time you find it.

As far as I'm concerned, we talked a lot about computer viruses. I hope you defiantly learned a thing or two and may have possibly even thought to yourself "I think I might have a virus. Oh boy." Well, I hope you didn't think that.

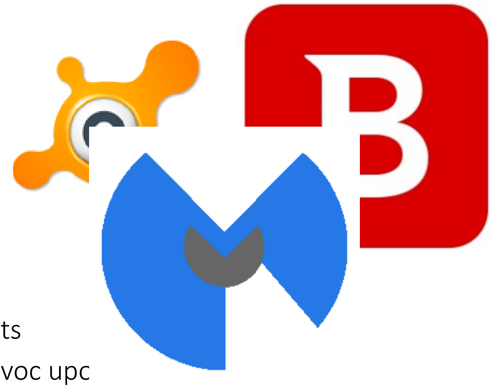
Well, *hopefully,* you can now describe a virus. Really, knowing the basics of a virus can help you find them, and when you can find them, you can eliminate them much faster!

I'll give you a list of the viruses for reference before I end this chapter. In the next chapter will talk all about anti-viruses, how to install them and how they work.

- ❖ Browser Hijackers – Changes Browser, very common
- ❖ Spyware – Collects data, fairly common
- ❖ Adware – Displays ads, fairly common
- ❖ Trojan Horse – Bundled with other software for malicious reasons, common
- ❖ Backdoor – Used to access computer without permission, uncommon
- ❖ Ransomware – Holds computer hostage for something in return, fairly uncommon
- ❖ Scareware – Attempts to scare user into committing action, uncommon
- ❖ Boot Sector Virus – Infects boot sector to prevent computer use, fairly uncommon
- ❖ Rootkit – Takes complete control of computer without knowledge, rare
- ❖ Polymorphic Virus – Can change various traits of virus, varies

SECTION 7 – ANTI-MALWARE STRATEGIES

People always allow anti-malware, anti-virus, anti-spyware, anti-literally-everything software run their computers in hopes that they can help when the time comes, unfortunately, as long as there's money to made when making malware, viruses will always exist. However, as long as there is malware, there will be companies making anti-malware software to defend their consumers. Within this chapter, we'll also mention some of the ways that users can be vulnerable.



The first subject we'll talk about is viruses. You already learned quite a bit in the last chapter, however, let's expand our knowledge of viruses again. What is a virus? It is a program that inserts itself into the computer and then proceeds to replicate and wreak havoc upc the computer. This can be done in various ways from launching from the end of the code, being inside various parts of a program or split itself into several parts that are placed in random parts. We'll label each of these methods.

- ❖ Appender Infection – The virus is at the end of the program, eventually executing when the end of the file is executed.
- ❖ Swiss cheese Infection – This is when the virus is injected into various places of the program. Anytime a specific item is executed (and it is infected), it will execute the viruses code.
- ❖ Split Infection – The virus is split into various parts and proceeds to be stored in various areas, when executed, the virus will switch to different places, executing the code.

It's not necessary to understand these things, it's more like I'm trying to give you an idea as to how these viruses evade detection or execute. People create malware for various reasons, what are these reasons?

- ❖ Malware for Hiding and Spying – This can include trojans, rootkits, and backdoors but defiantly aren't limited to those categories. This virus will prevent itself from being known by the user so it can do its work.
- ❖ Malware for Profit and Advantage – This can include botnets, adware, and spammers. They make their presence pretty well known with what they do and can take advantage of various things.
- ❖ Malware for Sending Messages or Destruction – This can include things that destroy other people's lives, destroy computers or just send a message. I'll actually talk about this one a little more in-depth. Sending a message? The world is run by politics. What better way to send a message than to infect hundreds and thousands of computers. Believe it, there have been tons of times where malware was used to spread a message since there aren't too many ways you can do so without actually getting attention.

I said two new things that I haven't actually gone into detail with. Botnets and spammers. Well, let's talk about what a botnet is. A botnet is essentially an army of computers that are being controlled by someone. Botnets can be HUGE, and by that, I mean in the hundreds of thousands. What can botnets do exactly? Well, DDoS is one thing. Distributed Denial of Service is when something happens (such as a DDoS attack) is executed upon someone. We'll talk about this more in a later method, but you always see DDoS being done in the news, it's effective but very childish.
Botnets can be used for various things; I'd recommend you look into it. I also said spammers. Spammers make up for a huge portion of malware spread through the internet. When people are targeted by spammers, you wouldn't really think people would fall for it right? I wish. A lot of people fall for scams, the human mind can be the most vulnerable thing. Getting to it is called Social Engineering.

Social Engineering is basically the psychological manipulation of humans. Quite a few big hacks have been achieved by using Social Engineering. That's not the subject right now, unfortunately, believe me, it's interesting and rather frightening as to what you can do with the art of human hacking.

Anti-Virus Details and Suggestions

Let's get back to our original subject of Anti-Attacker Strategies. The main one being anti-malware, so let's talk about anti-malware. How does an anti-virus work?

An anti-virus is a powerful piece of software that uses various different tools to prevent malware intrusion. With all of the possible ways you can get an infection, you're bound to encounter a virus. Antivirus software usually runs aside the rest of your programs, scanning all of your files and working hard. This can be called many things, let's call it *real-time scanning*. Most programs don't automatically open a lot of the time because your anti-virus is actively scanning. With the new technologies that are developed, viruses also become sophisticated. This is where things such as *heuristic scanning* or *sandboxing* come into play. Heuristic scanning is when the anti-virus checks for bad behavior and emulates the possibility of a new virus. Sandboxing is when a program is placed in a safe environment to see what happens when it works.

Any files can be scanned by your anti-virus for any potential bits of code that a virus could have, these are called *signatures*, essentially, consider the signatures your anti-virus downloads as a big library of virus samples, when one matches, it's time for a quarantine.

You have the ability to scan on demand or scan the entire disc, it's better to scan the entire disc when you have a chance. The chances of actually detecting a virus are different. Various anti-viruses have different results when scanning. Some companies have better chances, some have worse. **My personal favorite is BitDefender, Avast! Or MalwareBytes**. To me, BitDefender has proven itself to be the best anti-virus I've used. MalwareBytes has proven to be the best at getting the most stubborn viruses out of a system. Avast! Has proven to be a well-rounded anti-virus to me.

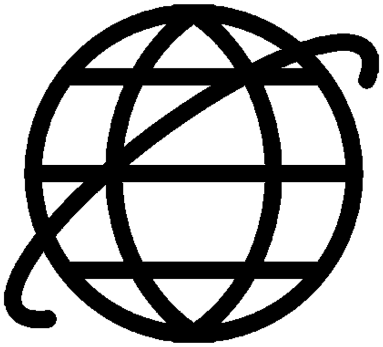
Believe me, these anti-virus programs can even pick up false positives or have trouble with a virus. It's not easy to deal with viruses sometimes, however, they work very effectively and have proven themselves to be worth the investment!

Now, how do I use anti-virus during competition or in general? Simply doing a full scan on C:\ (Or the entire computer basically) is enough to get a good overall scan!

That's it for this section; I hope you learned a lot more about viruses and anti-viruses! In our next subject, we're going to finally learn about my favorite subject, networking!

SECTION 8 – INTRODUCTION TO NETWORKING

Believe me when I say that *this* is my absolute favorite subject! The world of networking is the world that needs people to be there for it, as it is as vast and interesting as it is amazing! It's time for us to talk about the world of networking and the internet.



The internet everyone knows today started as ARPANET, a project where the US had planned to connect various computers. In the beginning, it had only been a military project for decades, eventually; it ended up being adopted by universities and large corporations, liking the idea of fast communication.

As it grew, it became more popular and eventually became a very important part of communication, with the support and growth; it was eventually relabeled the **Inter**national **Net**work, also known as the Internet.

As it improved, it became more common, as it became more common, it was soon commercialized in the late 1980s – early 1990s. So what binds us all together since ARPANET was discontinued by the 1990s? **ISP**, known as Internet Service Providers. We're talking about Time Warner, AT&T, Comcast, Version, Rock Solid and so many other service providers. This is what connects us all! The internet is literally one huge network!

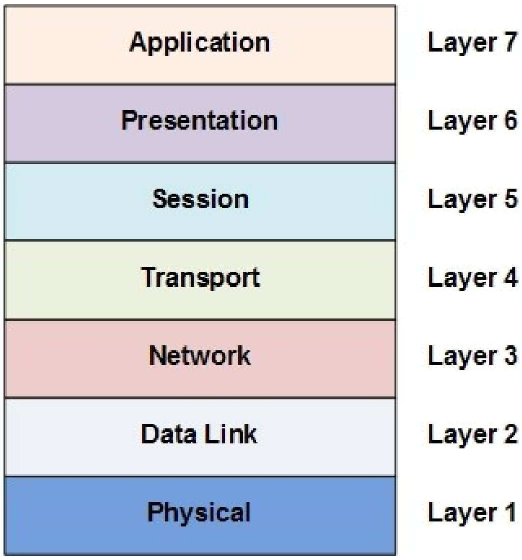
We're all connected through various backbones of the internet, from connecting with underwater cable submarines to giant cables, we all are the internet. From backbones to ISPs, we create simple or large networks together called LANs and WANs.

A **LAN**, also known as a Local Area Network are things like your home, a small office. All sorts of things that make a little Network. LANs are all local and they're all connected to one router. Next, what are WAN's?

WAN's, also known as Wide Area Networks are more like schools, college local internets, big businesses, all sorts of things. They're the same as LANs however also being very wide, giving the name Wide Area Networks. So why does this matter? The whole internet basically started as a LAN, then a WAN, and then it just continually expanded to be what we have today.

The way we connect to each other is through different layers, eventually, these layers had formed a model that many networkers would follow and use in the beginning of learning about networks, and it's called the OSI model.

By the way, OSI stands for Open Systems Interconnection. We'll explain each section of the OSI model in just a bit, for now, I'd like to teach you my favorite way acronym for remembering it from layer 1 to 7, Please Do Not Teach Students Pointless Acronyms.



Application	Layer 7
Presentation	Layer 6
Session	Layer 5
Transport	Layer 4
Network	Layer 3
Data Link	Layer 2
Physical	Layer 1

This is a quick reference chart for the OSI model

Application – Layer 7	This is where the end user is, creating or sending whatever needs to be created or sent via programs.
Presentation – Layer 6	Encryption, decryption, translation, compression, etc. This is where raw data is handled and turn into something the end user can or can't work with.
Session – Layer 5	Establishment of security, logging, synchronization and logical port usage.
Transport – Layer 4	The use of TCP or UDP, host to host communication and flow control.
Network – Layer 3	Packets, IP addresses, routing.
Data Link – Layer 2	Frames, MAC addresses, logical linking and frame checking.
Physical – Layer 1	This category goes down to the wire. Cables, electricity, you name it.

This might seem like a lot of information, however, as we learn, you'll learn more about how it all really worms with the terminology we get.

The Physical Layer – 1

The physical layer is really just all physical. From the electricity and bits to the encoding of the data, this is where a lot of the physical transferal of data works. You can expect that ISPs, landlines, broadband and hubs work in this area. (**What is a hub?** A hub is a device that repeats all network information everywhere it can, meaning anyone connected to a hub can receive packets) This is also where the modem works. **A modem** is the modulator-demodulator, usually connected via a coaxial cable. This does all the processing of data so that it can get to where it needs to go.

The Data Link Layer – 2

This is where we get into a more logical area of networks. This is where frames (containers that have **MAC addresses, known as Media Access Control addresses**. A computers MAC identifier is assigned to its **NIC, Network Interface Controller**). Anyway, so we know that within the Data Link Layer, instead of a computers packets being identified as very simple data, it's identified with its MAC address. Within the Data Link layer, this is where frames are sorted to where they need to go. This is also where switches operate. (**What is a switch?** A switch is a device that serves as a controller that allows devices to talk to each other more efficiently.)

The Network Layer – 3

This is where all the real magic happens. Let's talk packets. **What are packets exactly?** Consider packets like tiny little letters containing IP addresses and information. This is where a Router does its magic. It has the ability to route packets in the right direction. Normally, packets transfer piece by piece to allow the flexibility of networks.
This is where a lot of things such as packet filtering and traffic control come into play. **But what is a router?**
A router is exactly what it sounds like. It routes data from one network to another.

The Transport Layer – 4

The transport layer deals with traffic control and host to host communication. This two big subjects that we talk about and *must* understand called TCP and UDP. Now, these things are to ensure that messages are delivered in a sequence without loss or other errors. **TCP stands for Transmission Control Protocol**, it is a transmission process that allows data to be transferred without error or dropped packets. **Packets also work on this layer**. Now, what TCP can do to prevent such a thing is ensure that any dropped packets are recovered, any malformed packets are discarded and requested again. When you do important downloads, TCP will be what they always use.

Now let's talk about UDP. **UDP stands for User Datagram Protocol**. The main point for UDP is to allow low-latency connection types that don't really care too much about loss. This is typically for streaming data of any kind, let's say you wanted to watch a video, you will use UDP to allow the fastest downloading of data. Let's also say you play a lot of video games, it's obvious that your system will prefer a lower latency and use UDP.

This layer works mainly with these transportation protocols. That's all you need to remember essentially.

The Session Layer – 5

This is where we talk about synchronization and ports. In this layer, sessions are established and the maintenance of your connection is done. This is also where security and logging happen. **This is also where ports operate**. Ports are an extremely important part of networking. So what are ports? Ports are essentially how connections *inbound or outbound* can get in or out of the computer. To be able to access the web, you always need access to port 80 for HTTP and sometimes port 443 for HTTPS/SSL. If you wanted to download something, you would use port 21 for FTP.

We'll get more into ports and whatnot in the intermediate networking section.

The Presentation Layer – 6

I'd like to think of this as the layer that does the translation of raw data into a much more viewable format by the end user. Which is exactly what it is! **This layer deals with** raw data and converts it, encrypts or decrypts (if that is required), compresses and just translates the data into a viewable format. This can happen with pretty much any type of file, such as pictures or media, all of it is assembled here.

The Application Layer – 7

This is the user seen by the end user. Whatever is sent and received, it all ends up here. Sending mail or sending video, literally, any of those things can be considered it. Sharing resources, remotely accessing or accessing a network, this is all end user stuff!

That pretty much wraps up the OSI model for us. At least the basics, we'll be back into this subject again in couple sections when we've got a better look into the world of networking. Now, we're going to talk specifics since I've already covered the ground of how networking works with the OSI model.

So what are these specifics? We're going to talk about internal and external IP addresses.

An **Internal (Local) IP address** is one used by your LAN or WAN. This is used to identify everything inside of the network, from printers to servers, everyone has an IP address! What does an IP address look like? Well, I'm sure everyone has seen it! A typical IP address most homes give everything look like 192.168.0.1 or something of that area, it can vary. What do those numbers mean? It's surprisingly easy to understand.
An IP address is 4 numbers separated by periods; the numbers have at the most 3 digits each and at the least 1 digit. Every device needs a unique IP address, each device can choose from 0 to 255. So, 192.168.0.24 is my computer and my TV (connected to the internet) has 192.168.0.25, your router will always have the first IP address! We'll go ahead and look into some extra details on IP addresses and then begin with physical addresses after.

An **external (Remote) IP address** is used to address you to the whole internet. Because let's face it, there are so many internet-using devices on the planet to the point where it's extremely unlikely that there would be enough for everyone, plus, there are also classes for IP addresses and whatnot that were essentially abandoned because of the amount of IP addresses that currently exist.

Now, further discussion on external IP addresses. This is how the internet recognizes you, Google has its own external IP addresses, which end up hosting plenty of internal ones. Think of it as a house, a house has a unique address in it with multiple people living in it. If someone knocks and asks for a specific person, they can contact one person inside the house. People can come by to the house (external IP) and request one of the people living there (internal IP) hopefully, you understand, we'll be talking about the slightly abandoned concept of IP address classes. You can go to http://whatsmyip.org to actually check what your external IP address is!

IP address classes were a nearly abandoned concept that could've helped if there weren't so many devices using IP addresses right now. But ultimately, the concept was abandoned due to the inefficiency.
There are three classes of IP addresses, class A, B, and C.

C class networks would be considered home networks and small businesses. They can hold a maximum of 254 devices.

B class networks are network type that would suit businesses, schools, and small colleges. These types of networks can hold 65,534 addresses, so that's defiantly a huge step in the direction for how many devices, but surprisingly, some businesses can actually run out of these IP addresses.

The final type is the A class network. A class networks can hold a whopping 16,227,214 internal IP addresses. You would expect that Google, Microsoft or Apple would be using these types of networks.

If you enjoyed this chapter (I know I did enjoy writing it), talk to your Team's Leader about the MVHS Cisco Course!

Otherwise, this wraps it up for our introduction to Networking. I hope this information will provide use to you, in the next section, we'll be learning about how to use Task Manager and Resource Monitor to your advantage!

SECTION 9 – INTRODUCTION TO TASK MANAGER

Now that we've covered a whole load of things about networking, let's talk about our next fantastic tool within our arsenal, Task Manager.

This is a great tool for viewing your systems overall usage from the processes to the CPU to memory usage, it can also be good at finding the source of viruses or stopping them. This is an important tool every Windows user should know how to use, whether it's to deal with misbehaving programs or resource-hungry ones. Let's begin by learning how to access Task Manager.

There are a variety of ways to access Task Manager if you know any of the following just remember there's more than one method.

- Keyboard Shortcut: Press Ctrl+Shift+Escape anywhere in Windows.
- Mouse Shortcut: Right-click the Windows taskbar and select Start Task Manager.
- Traditional Method: Press Ctrl+Alt+Delete and select Start Task Manager.

These three methods work like any other, now, when you open Task Manager, you'll be introduced to so many tabs and data that you might not know where to begin. This is where we'll show you.

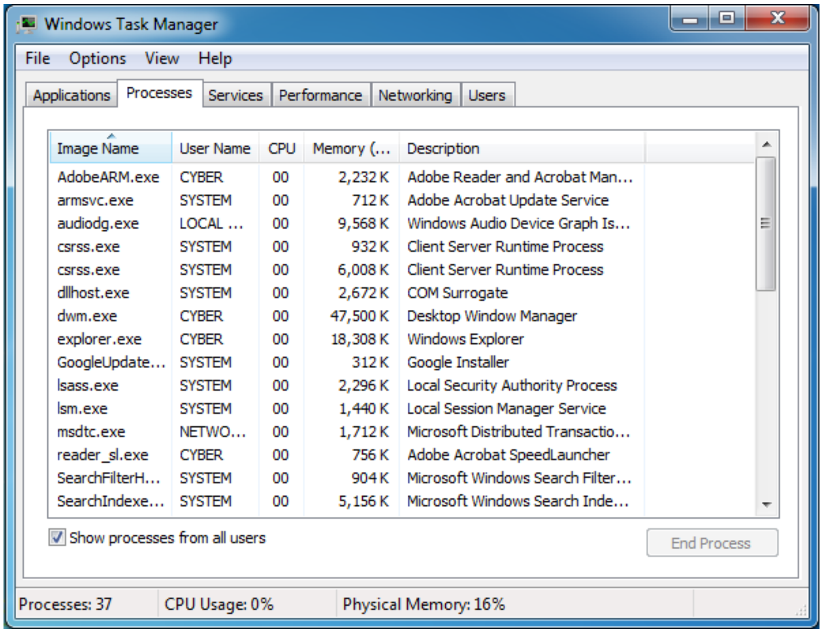


Image Name	User Name	CPU	Memory (...	Description
AdobeARM.exe	CYBER	00	2,232 K	Adobe Reader and Acrobat Man...
armsvc.exe	SYSTEM	00	712 K	Adobe Acrobat Update Service
audiodg.exe	LOCAL ...	00	9,568 K	Windows Audio Device Graph Is...
csrss.exe	SYSTEM	00	932 K	Client Server Runtime Process
csrss.exe	SYSTEM	00	6,008 K	Client Server Runtime Process
dllhost.exe	SYSTEM	00	2,672 K	COM Surrogate
dwm.exe	CYBER	00	47,500 K	Desktop Window Manager
explorer.exe	CYBER	00	18,308 K	Windows Explorer
GoogleUpdate...	SYSTEM	00	312 K	Google Installer
lsass.exe	SYSTEM	00	2,296 K	Local Security Authority Process
lsm.exe	SYSTEM	00	1,440 K	Local Session Manager Service
msdtc.exe	NETWO...	00	1,712 K	Microsoft Distributed Transactio...
reader_sl.exe	CYBER	00	756 K	Adobe Acrobat SpeedLauncher
SearchFilterH...	SYSTEM	00	904 K	Microsoft Windows Search Filter...
SearchIndexe...	SYSTEM	00	5,156 K	Microsoft Windows Search Inde...

☑ Show processes from all users

Processes: 37 CPU Usage: 0% Physical Memory: 16%

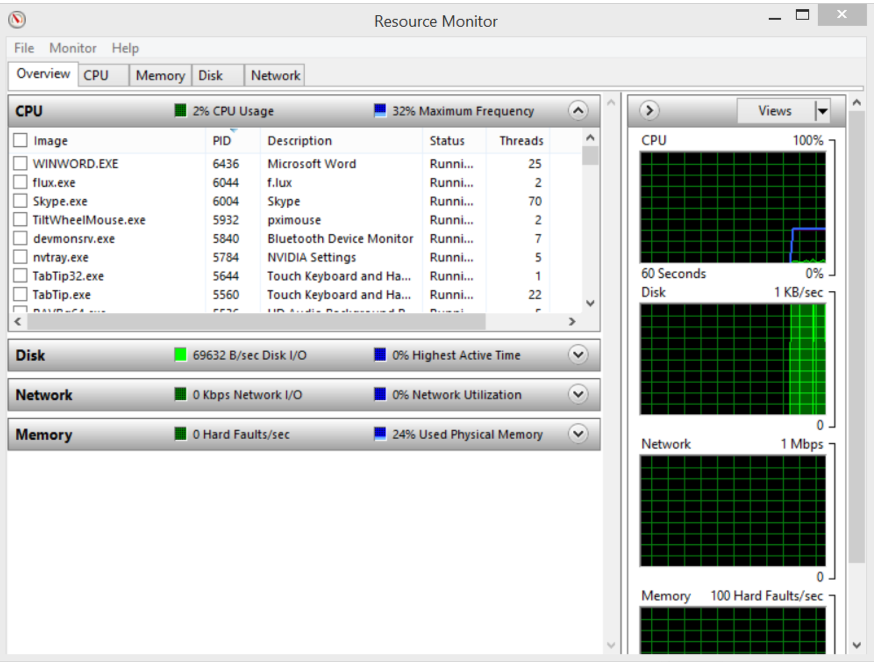
The first tab we'll be looking into here is Applications. Applications is most likely the easiest to understand as it just gives a simple look at all the programs you can mess with or actually do things with. No system processes or secret things are shown here; if you had a program that began to misbehave you'd kill it here by clicking on it and doing "End Task". In the picture to the left, are the processes. Processes show more of a technical view of your operating system, it may be a little harder to identify what is what, when you know what to look for, processes is very effective to use.

First off is figuring what exactly is taking up the most memory, if you click things such as Memory you can rearrange the data, such as making it from the most power hungry tasks to the little tasks. To figure out whether a Task is meant to be there or not may actually be a little more difficult. Processes can also have processes, meaning you can look into them for way more details. You can right-click on a task and view things such as, where does this program exist? When did this program start up? I have so many questions! The real thing that should set off suspicion would be if the program's name is completely random, if the program took up too much or too little memory, or if the program is in a directory that you don't remember having or the directory the program exists in is a directory that's not Program Files or Windows is a red flag. When a program exhibits strange behavior such as disappearing and reappearing or better yet, changes names. (If it does change names, data or activity details, it may be considered a polymorphic Virus, a virus that can change itself to avoid anti-virus detection, which is a very sophisticated type of Malware).

It should also be noted that if you click the view menu and then select Columns, you can enable CPU Time or PID. CPU Time means how long this program has been active and PID (Process Identification) is a number the program will be referred to on the system as they're both extremely helpful and should be on. Here is something to note about PID's, they are *universal*, meaning let's say you're viewing the tasks in both Task Manager and the task list in command-prompt, you'd be shown the same PID of the same program with the results of both task programs.

You can also right click the misbehaving program in Processes and End Process manually that way, it's better doing this than in applications as it is more effective. If you look at CPU Time, you can potentially check how long ago the process started, for instance, let's say we had a backdoor, now a backdoor would typically start when the computer starts so the attacker can get instant access, many viruses start alongside the computer, so if the CPU time says it's been running as long as the CPU has been active, perhaps it flags reasonable suspicion.
The next category is the Resource Monitor, now before you tell me that there is no tab called Resource Monitor, it's actually on the Performance Tab, all the way down in the left-hand corner you'll find Resource Monitor. Since CyberPatriot won't put a virus that uses up a lot of memory and CPU usage, we won't really go over viruses that consume a lot of memory, but if we did, you know what you would look for, which is, well, a process that consumes a lot of memory.

What we might be looking for in competition is programs that take up a lot of network usage, have the longest CPU time, is constantly changing or you just know that it's a potentially hazardous program. Using PID's from processes in Task Manager and the Network feed of Resource Monitor, we can analyze and compare data as to if the computer had some sort of virus, such as spyware or a backdoor. You look in processes for a strange program, write down PID's of them, and then you jump into Resource Monitor and shirt through each category, looking at the PID and what is happening. The following photo is a picture of what Resource Monitor looks like.
In the next section, we're going to go over management of programs within your system.



CPU ■ 2% CPU Usage ■ 32% Maximum Frequency

Image	PID	Description	Status	Threads
WINWORD.EXE	6436	Microsoft Word	Runni...	25
flux.exe	6044	f.lux	Runni...	2
Skype.exe	6004	Skype	Runni...	70
TiltWheelMouse.exe	5932	pximouse	Runni...	2
devmonsrv.exe	5840	Bluetooth Device Monitor	Runni...	7
nvtray.exe	5784	NVIDIA Settings	Runni...	5
TabTip32.exe	5644	Touch Keyboard and Ha...	Runni...	1
TabTip.exe	5560	Touch Keyboard and Ha...	Runni...	22

Disk ■ 69632 B/sec Disk I/O ■ 0% Highest Active Time

Network ■ 0 Kbps Network I/O ■ 0% Network Utilization

Memory ■ 0 Hard Faults/sec ■ 24% Used Physical Memory

SECTION 10 – PROGRAM MANAGEMENT

Has anyone ever had a frustrating time with a program? One that won't uninstall as easily or provides quite the hassle just to get remove from a system? If so, then you're in luck. In this section, we're going to talk about Revo Uninstaller, one of the greatest tools we'll ever use in CyberPatriot, we'll also learn how to do general program management.

So we might as well begin on how to use the regular uninstaller. By this point, you should program know how exactly to do so, but in case you've forgotten, simply start by going to Control Panel → Programs → Uninstalling a Program.

From there, you can right-click the program and select "uninstall", from there, you can follow the instructions on how to uninstall the program. There are some problems to this though. Windows Uninstaller will begin the whole uninstallation process, however, sometimes the program won't commit through the uninstallation, leaving files and other items behind. Perhaps you attempt to uninstall spyware or adware, and it leaves behind some stuff, potentially, it can have the program reinstall itself (we're looking at you, Conduit).

One of the biggest offenders when it comes to programs that leave traces are things such as browser hijackers or PUPS in general. It leaves behind files, folders, configuration files, potentially suspicious files or the program refuses to uninstall! From this point, I'd like to introduce Revo Uninstaller! You can pick up this program at www.revouninstaller.com, this is one of the first third-party programs that will be introduced to you. This program made its debut in our sixth season of CyberPatriot, scoring us points we shouldn't have scored before. What can revo do exactly? It can:

- ❖ Hunt down traces of a program it uninstalls
- ❖ Looks for leftover registry keys (registry keys are the DNA of Windows, these can stick around)
- ❖ Forces the program to close if it refuses normally

Already, we can tell that Revo does it's well, along with the free version coming with various powerful features; it's got a relatively neat interface. As an example, let's say a computer has Nmap installed.

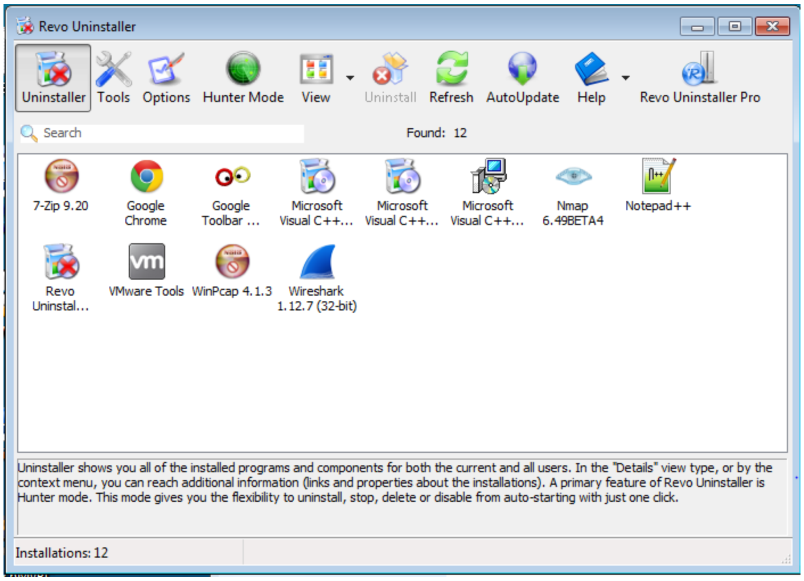
For the first part, I'll tell you what Nmap is just for the kick of it, Nmap is a security scanner used by many, if our README said we shouldn't have security tools of any sort on the computer, it's clear what we're going to uninstall first. Typically, what you shouldn't have on a computer are things that do not relate to the computer what so ever.

Security tools such as Nmap or Backtrack should not be allowed. Toolbars or any add-ons should not be installed as well. You need to research each program installed on the computer and ensure that the program should not exist.

Any program that does not exist on the README should be uninstalled. There are exceptions to this list, some of these exceptions include things such as Microsoft Visual of frameworks, VMware-based Programs, CyberPatriot items (such as the scoring engine, also, about that, **do not touch CyberPatriot items.**)

Ultimately, it's up to the user if you should keep the program or not, however, the README provides all of the details you'll need.

This is the interface of Revo Uninstaller when working with Revo, you're given a variety of options when attempting to uninstall items.



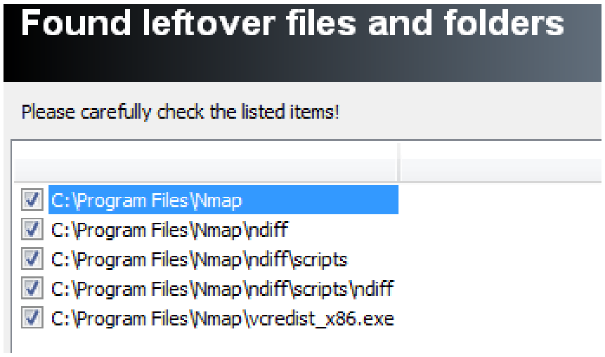
Uninstaller shows you all of the installed programs and components for both the current and all users. In the "Details" view type, or by the context menu, you can reach additional information (links and properties about the installations). A primary feature of Revo Uninstaller is Hunter mode. This mode gives you the flexibility to uninstall, stop, delete or disable from auto-starting with just one click.

Installations: 12

These options include a variety of things, such as Safe, Moderate, and Advanced.

I highly recommend moderate for programs that are just normal programs that aren't supposed to be on the computer and scanning with advanced for programs that are suspicious (programs that might be suspicious include things like Wireshark, Backtrack, and Nmap.

Now, Revo Uninstaller does *not* do all of the work for you, keep up with the program as it goes along with the process. So let's say we began the process of uninstalling Nmap, once it's finished, you should have a result that says "found leftover files and folders".



Found leftover files and folders

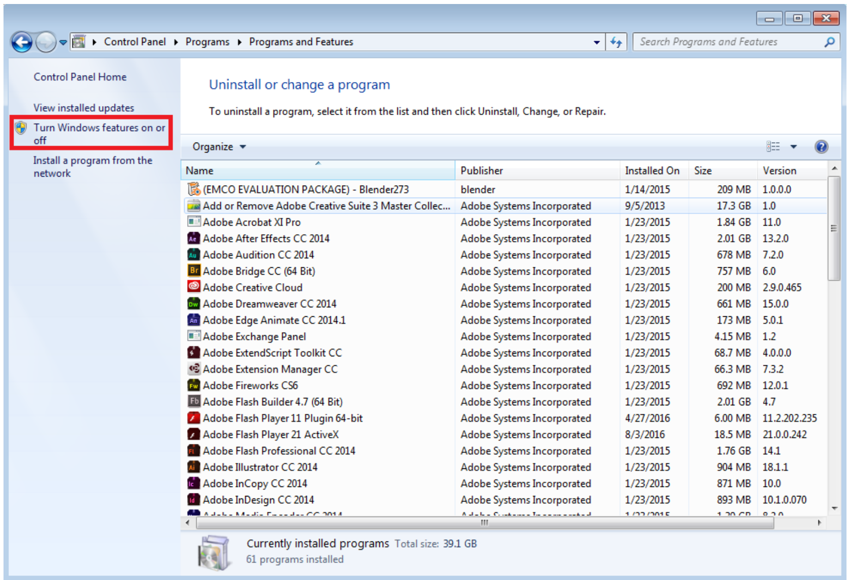
Please carefully check the listed items!

☑ C:\Program Files\Nmap
☑ C:\Program Files\Nmap\ndiff
☑ C:\Program Files\Nmap\ndiff\scripts
☑ C:\Program Files\Nmap\ndiff\scripts\ndiff
☑ C:\Program Files\Nmap\vcredist_x86.exe

Along with that, you'll also find that it informs you that you have left over registry keys and whatnot. Before I go on and tell you to delete anything about **registry keys**, you need to understand that you can consider registry keys the DNA of a Windows Operating System. If removing them, it potentially poses a risk; however, it may also pose a risk if they are kept.

Now, once you've check all of the program files you'd like to delete in the example to the right, remember to hit delete to remove them, this goes the same for any leftover registry keys.

Remember that regardless if a program can be considered good, they should be uninstalled. The next feature we're going to talk about is the Windows Features.
Windows Features.


Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
(EMCO EVALUATION PACKAGE) - Blender273	blender	1/14/2015	209 MB	1.0.0.0
Add or Remove Adobe Creative Suite 3 Master Collec...	Adobe Systems Incorporated	9/5/2013	17.3 GB	1.0
Adobe Acrobat XI Pro	Adobe Systems Incorporated	1/23/2015	1.84 GB	11.0
Adobe After Effects CC 2014	Adobe Systems Incorporated	1/23/2015	2.01 GB	13.2.0
Adobe Audition CC 2014	Adobe Systems Incorporated	1/23/2015	678 MB	7.2.0
Adobe Bridge CC (64 Bit)	Adobe Systems Incorporated	1/23/2015	757 MB	6.0
Adobe Creative Cloud	Adobe Systems Incorporated	1/23/2015	200 MB	2.9.0.465
Adobe Dreamweaver CC 2014	Adobe Systems Incorporated	1/23/2015	661 MB	15.0.0
Adobe Edge Animate CC 2014.1	Adobe Systems Incorporated	1/23/2015	173 MB	5.0.1
Adobe Exchange Panel	Adobe Systems Incorporated	1/23/2015	4.15 MB	1.2
Adobe ExtendScript Toolkit CC	Adobe Systems Incorporated	1/23/2015	68.7 MB	4.0.0.0
Adobe Extension Manager CC	Adobe Systems Incorporated	1/23/2015	66.3 MB	7.3.2
Adobe Fireworks CS6	Adobe Systems Incorporated	1/23/2015	692 MB	12.0.1
Adobe Flash Builder 4.7 (64 Bit)	Adobe Systems Incorporated	1/23/2015	2.01 GB	4.7
Adobe Flash Player 11 Plugin 64-bit	Adobe Systems Incorporated	4/27/2016	6.00 MB	11.2.202.235
Adobe Flash Player 21 ActiveX	Adobe Systems Incorporated	8/3/2016	18.5 MB	21.0.0.242
Adobe Flash Professional CC 2014	Adobe Systems Incorporated	1/23/2015	1.76 GB	14.1
Adobe Illustrator CC 2014	Adobe Systems Incorporated	1/23/2015	904 MB	18.1.1
Adobe InCopy CC 2014	Adobe Systems Incorporated	1/23/2015	871 MB	10.0
Adobe InDesign CC 2014	Adobe Systems Incorporated	1/23/2015	893 MB	10.1.0.070

Currently installed programs Total size: 39.1 GB
61 programs installed

Windows features are particular features within an operating system that can be enabled or disable, so if you've ever wanted to uninstall Microsoft Internet Explorer, we've got news for you.

You can access the Windows Features by doing to the Control Panel's Programs and Features. When you get there, if you attempt to modify it, you'll see a list of programs that Windows normally has installed.

So when you get there, you'll find a list of all sorts of Windows Applications you normally work with. Things that should be disabled are items such as Media Features. Normally, our README will tell us that they do not want media files on the computer, so disabling Media is a good idea. Another item to disable is Telnet Services.

We might as well go over Telnet. Telnet is a program used to remotely connect to a computer to do things. So this can be considered a type of "remote access", now, unless we're told in the README, we do not want Telnet on our computers. If we did want remote access on our computer, we wouldn't want telnet as it is one of the most insecure programs we could possibly use. Another program that we cannot have is Windows Gadget Platform. If you do some research, back in the day during Vista, Gadgets were a vulnerability risk as they ran in "Full Trust" mode, meaning that they had a lot more rights than a gadget should have had. You can hover over a Windows Feature to check out the details on it, but I've given you examples, remember to remove unnecessary programs.

Patching

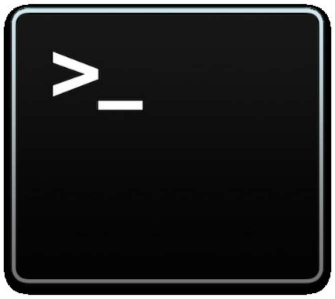
Let's talk about patching now since we learned about removing. Patching a program is a very important subject as every day; attackers find ways to get access to a system just from one program. But this is where the creators of the programs take their responsibility and patch their programs for bugs and vulnerabilities.

The first step is visiting http://ninite.com. The next step would be selecting what exactly you want to have updated, for example, a majority of the programs that we normally use are here, some of these include runtimes, web browser, document readers and etc. The faster and better a program can handle patch management, the better

Please understand that this program *does not* handle all patch management for you. To truly patch, you need to check with each of your programs. Sure, ninite can patch programs for you, but on very rare occasion will the program have something wrong with it. If it does, you will notice, but if not, then feel free to continue on with using ninite. Sometimes ninite might not support a program, in that case, it's recommended that you just manually patch a program, it's not hard, and all you have to do is look up the latest version and rerun the installer.

In the event that ninite doesn't do the job, try patchmypc, or, manually patch all programs. In the next section, we're going to be looking into and learning about how to use the Windows Command-Line.

SECTION 11 – INTRODUCTION TO CMD



We're finally getting to the box that people in the movies are normally working on, you know, the "hackers". Unfortunately, not everything you see in movies is true. But yes, a lot of work is done in a prompt.

In this section, we'll be learning how to operate the basics of command prompt and learn so many new things! I'm going to say this at both the beginning at the end, if you found this part very interesting, feel free to look into using Linux.

So let's talk command prompt. In the real world of IT professionals, you can't be taken seriously if you don't know how to master the ultimate power of the command-line. The command-line has always been a way computers were first used, in the beginning when Microsoft made its operating system (MS-DOS), a disk-based operating system, and it only used the command-line. During those days, there was no GUI (Graphic User Interface), now we have the GUI we see today, however, the power of the command-line is still available to the users today.

To begin the command line, simply press the Windows Button on your keyboard or the start menu button and then proceed to type 'cmd' into there, right-click it and then run the program as an Administrator. You can also use CTRL+R and type CMD into the run prompt for those of you who are feeling adventures and enjoy short cuts.

You'll receive a prompt and most likely you'll have no idea where you are or what anything is. **To tell if you ran it as an Administrator or not**, simply check where you are. People running as an Administrator will start in the directory C:\Windows\System32. If you are running as a regular user, you will likely start in your home directory. Now, let's identify the parts of the command prompt. You can also use the command `whoami` to check who you are.

The prompt will begin by defining where you are, for instance, the first line will start with what disk drive you're on (for instance, the C: is not a smiley, it is the C:\ drive). If you only have C:\> on your prompt, you are at the **root** of the directory. Now, you can be in a directory within a directory within a directory… One of the biggest things you need to do or learn is how to read directories. So, if you followed my instructions, you should have the following:

```
C:\Windows\System32\>
```

First off, before we learn any commands at all, let's learn some sweet tips and tricks I wish everyone would learn. To start, if you want to scroll through some commands you've executed already, you can use the up and down keys.

You can stop a command from executing by doing CTRL+C, however, it will not undo anything if the command had already executed.

You can move the cursor with the left and right keys to edit commands you may have previously used. You can use the TAB key to also finish things such as directories, so say you wanted to go to the System32 directory, you could just type a part of Windows, press TAB, then type a part of System32 and press TAB again.

Command Prompt for Windows is **NOT** case sensitive, that means you're free to type it however you'd like, just as long as you have everything typed correctly.

One more thing, if you need any help at all from any command, simply type /? Or help after the command and you'll receive some information about the command, if you still need help, ask others!

Command Prompt Shortcut Items

We already talked about how the command prompt is, what directory you're in, etc. There are some additional shortcuts you can use, for instance, if you want to open up a specific directory in command prompt and you just so HAPPEN to be within that directory, you can type "`explorer`" into the console and it'll pop up in the GUI! (By the way, a GUI is considered a Graphical User Interface) and if you just want to open up explorer, do "`explorer .`" in the console. By the way, from this point, I'll call the Command Prompt the console.

Command Arguments

Let's talk about command arguments and introduce a command or two. A command argument is essentially what the command has to work with. Let's try the command `dir` first. `dir` Is used to display the contents for a directory. Let's say you wanted to see the contents of the current directory you're in, you would input the command `dir` into the console, your output would be various folders and items in the directory.

`dir` works with your current file location to output your current directory contents. You can also make `dir` work with an argument, let's say you only wanted to output the directory contents of a specific area, like, Windows. What you would do is input the following into the console:

```
dir C:\Windows
```

What would result is the contents of C:\Windows, which is what would happen. All sorts of commands work with arguments like so. We'll go into more detail of that command later, for now, we'll go over another thing that people confuse for arguments, switches.

Command Switches

Just to make things clear, we're not talking about arguments. You usually put switches before any arguments. When it comes to the `dir` command, you have the option to implement a switch that allows you to view the hidden contents of a folder. If you didn't know this, there's an option to hide files and folders from the standard user's accesses. It's relatively easy and impossible to undo if you happen to be a standard user. The implementation of switches will give the user more flexibility and features with a command. For example, if you wanted to view the hidden contents and regular contents in the System32 folder, you would do the following:

```
dir /a C:\Windows\System32
```

The following will give you the output you requested.

Input/Output

The final feature we're going to talk about is input/output, also known as I/O. With I/O, you can get whatever commands you use to output results into something or create something to put the contents into, for instance, let's say you wanted to output the results of our command above into a text file on the desktop, Using a > will allow you to output a result, for instance, we made it so that the results of our command will go to output.txt on your desktop.

```
dir /a C:\Windows\System32 > C:\Users\TESTUSER\Desktop\output.txt
```

Piping

The whole concept of piping is to get one commands output and then proceeding to use another command on it. Most people never use the key, but it's the | key. This is right above the Enter Button, simply hold shift and press the \ key.

Now, what we could use piping for is a question that most people wonder, well, one amazing example is using the command `findstr`, which stands for find string. The term "string" is used a lot, especially in computer stuff in general, so what it means is a piece of text. I'm only giving an example of piping, I recommend you test things out with it.

We're going to issue a command called "`tasklist`", this command will essentially give us information like Task Manager, using the same info such as process name and PID, and then only find the process "explorer" (explorer.exe is the GUI of Windows) within the set of items in the tasklist.

```
    tasklist | findstr “explorer”
```

This should output the only string that has explorer in the name. Piping can be very useful if used correctly.

Now that we've talked about various ways to work with commands, we can move onto actual commands. Let's begin.

cd (Change Directory)

The command `cd` is one of the most frequently used commands for switching to the system. cd has two uses, to print your current working directory (Note! When using terminals or command prompt, if someone says print, they mean text displaying on-screen) and changing your directory.

Remember that a directory is known as a file path, **you can find your full file path by typing** cd. A cool fact about `cd` is if you want to go back a directory, you can simply do `cd ..` and you will be taken back one directory. How does this work? Consider a directory a tree. A tree starts from the roots (our root is C:\) and it continually spans out.

I was talking about directories earlier; now, with cd you can hop to any part of the system. For instance, try hopping over to the user's folder, you would have to use this command.

```
    cd C:\Users
```

After you used this command, you will have not only gone to the Users folder on your system, but you also used an absolute pathname. An **Absolute Pathname** is the full, exact directory from root to the folder. We can also use a **relative pathname**, but you would have to know the name of the folder and be one folder back from it. For example: If we're in the folder C:\, you can simply do cd users to automatically go to the Users folder. You cannot do this in any other directory because if you go to any other folder, Users will not be there. It's like, you can send mail to an exact location with the address, but you can also give the mail to the person if their house is right next to you (though I don't know what kind of person would do so) but I was just trying to give an example.

dir (Display Directory)

`dir`, short for directory, is used to list all of the contents of your directory you're currently in. If you're in C:\Windows\System32 and you decided to do the command `dir`, you'll immediately have all of the contents of system32 in your command-prompt. This command works rather simply, however, there are switches/flags you can use to add more differentiating into it. For example, if you use the /a after dir like this

```
dir /a
```

You'll be given ALL of the files in the directory, I already said that, but you never know if hidden files exist, if a file was hidden, adding the /a to dir will show it. If you do /p you'll have the data pause every time it scrolls through, so /p is a good one to use whenever the contents of a directory might be large.

Using the switches /T:A will show you the last time a file was accessedcd & /T:W will show the last time it was written to. This is good to check for tampering. To sort through your various results for specific items, you can add findstr to your command by piping as in the example a couple pages up.

So it's pretty clear that there are all sorts of handy things you can do switches, simply ask for help with the command. Don't forget that you can also get the directories contents using an absolute pathname. You should know what to do right there, so let's move on to the next command!

echo (Repeat)

`echo` is used to tell stuff back to you. Very simply, here's an example of the command.

```
echo “testing”
```

If you do this, command-prompt will you tell you back “testing”, you can also use the command pause to ask if you want to continue when writing scripts this is good to have.

You can also echo text into a file. This can be helpful in various ways!

```
echo “testing” > C:\Users\TESTUSER\Desktop\testing.txt
```

You're also able to echo variables, one example would be usernames. It would look like this.

```
Echo %username%
```

ipconfig (IP Configuration)

We've already discussed IP's and whatnot, so this is a good way to get your network information. When you type the command you'll receive a lot of data you don't know what to do with.

When you do the command.

```
ipconfig /all
```

You'll receive all sorts of information for your system, including the IP address. The IP address is displayed in IPv4 Address. Note that this is an internal IP address, if you want the external IP address, you go to a website such as http://whatsmyip.org

Another good thing to learn about ipconfig is that it can be used to flush the DNS Cache. Quick lesson here. What is DNS? DNS stands for Domain Name Service when you type www.google.com, you go to Google. You don't know its IP address, where it goes or anything like that. DNS helps this way by giving you what its IP address is. If your computers

DNS Cache is poisoned or changed, one way to fix it would be simply doing the following command, though it may not be successful if something else that's responsible for DNS is changed, so it must be investigated further.

```
ipconfig /flushdns
```

It might be a good idea to know how IP configurations work, along with strengthening your knowledge of networking in general.

ping (ICMP)

`ping` utilizes Internet Control Message Protocol's tool to test whether you can reach something or not. It's good to use whenever you cannot reach something, for example, many uses Google's Public DNS, one thing they do with it is use it to test their connection, their Public DNS' external IP address is 8.8.8.8, so doing the following command will allow you to test your connection.

```
ping 8.8.8.8
```

You can also use regular website names for ping to test connection. Along with testing the connection, you get additional information as latency and response time in MS.

nslookup (Who is?)

`nslookup` will allow you to identify your external DNS server with the IP address. It will also allow you to look at other DNS Servers, for instance, if we wanted to view what DNS server is 8.8.8.8, it would tell us it's Google's.

`nslookup` (gives us our DNS server) & `nslookup 8.8.8.8` (I use 8.8.8.8 as an example, this identifies outside DNS)

tracert (Trace Route)

`tracert` is a command that allows you to view where exactly your packets travel. This can be used to check what's wrong with your latency, why things can be going slow, etc. To start, do tracert and then use an IP address.

```
tracert 8.8.8.8
```

The next thing that would happen is that you would get results that tell you how many "hops" your packets made. What is a hop? A hop is when the packet goes from one router to the other. It's always fun to view where exactly your packets go because that's something you never really think about. This can be a different troubleshoot tool.

net user (User Modifications)

`net user` is a command used to manage all the users on your machine, I'll just explain various ways you can use this command.

Simply just using `net user` will display all the users on your system, the command goes as shown.

```
net user
```

If you want to add a user, you start with net user, you then add as arguments a username and a password and then finally a switch to add at the end. This is how it should look.

```
net user username password /add
```

If you want to delete a user, simply do the same except without the password there and /add is changed to /del. Now that you've added the user, is it active? No. The user must be activated before it can be logged into, to activate our newly added user, simply do the following command.

```
net user username /active:yes
```

When you've done this command, you will now have that user ready to log into. If you wanted to deactivate it, simply change /active:yes to /active:no, next, to change a password, simply do the following command.

```
net user username *
```

That's it. It's extremely simple within the command line.

net localgroup (Group Modification)

`net localgroup` is used to view all the groups in your system. From Users to Guests to Administrators, all their respective groups are here and viewable, if we wanted to view who's an Administrator, you can simply do.

```
net localgroup administrators
```

When you do that, you'll view all the Administrators on your system, if you just wanted to view the groups on the system all you would have to do is type net localgroup and it'll display. If you wanted to add a user to a localgroup, you'd have to type the command as shown.

```
net localgroup Administrators username /add
```

If you wanted to delete someone from that group, all you'd have to do is change /add to /delete, this can work with any localgroup. So that's localgroups for you.

net share (Network Shares)

`net shares` are where all your share folders exist. Typically on a standalone system you don't want any shared things, folders such as C$, ADMIN$ and IPC$ will usually be there, if you see any different shares, it's a good idea to delete them.

```
net share sharename /del
```

net sessions (Current Remote Sessions Connected)

`net session` is used to view local computer connections, it's a big no-no if you see anyone connected, and if you do, simply do the following to disconnect them. You can also view if there are any current connections with just the command net session, but if you do see anything, you should delete them.

```
net session \\computername /del
```

net accounts (Brief Password Policy)

`net accounts` are used to enforce certain password policies as soon as possible. If you ever plan on immediately changing passwords, it's wise to use this to enforce some basic password policies. This is the best way the command could look.

```
net accounts /minpwlen:8 /maxpwage:90 /minpwage:15 /uniquepw:24
```

We'll look into the details of this command.

net accounts are the beginning of the command, if you just put net accounts without all of the switches then it'll only print out what the current account settings are. Here are the switches.
`/minpwlen:` is used to determine the minimum password length.
`/maxpwage:` is used to determine the maximum password age.
`/minpwage:` is used to determine the minimum password age.
`/uniquepw:` is used to determine how many passwords are kept to prevent reuse.

If you use this command, you'll only have these settings enforced, any others will have to be reinforced in the Local Security Policies, but this is a good command to do prior to changing passwords through command prompt.

net use (Access Network Share)

If you were wondering how shares were connected to, this command is the one to use. Rather simply, you can connect to any share if you know the IP, the name of the share and have a username and password of the system you're trying to access, a good example of using this command I will list here.

```
net use C: \\192.168.0.1\C$
```

Typically it's not as easy as it says here, and that IP address was only used an example. There's more to the command if you look into it. But it starts with net use, the drive you're trying to access, an IP address or computer name and then the share you're attempting to access, such as C$ for instance.

netsh advfirewall (Firewall settings)

I know I said I wouldn't talk about the advanced firewall until later, but this is very important.
You want to make sure that the Firewall is very cleaned up because if it's not then you may potentially have some problems in the future, such as an attacker's backdoor still having access to your computer or a port is still vulnerable.

The best way to clean things up first is resetting the firewall, to do so, simply launch this command to reset the firewall.

```
netsh advfirewall reset
```

After executing that command, the firewall will be completely back to stock settings, but you might as well go through the advanced Firewall again. If you want to start the firewall and check if the Firewall service is on or not, you can try this command.

```
netsh advfirewall set currentprofile state on
```

There are many more commands for netsh advfirewall, however, those are more helpful when it comes to administration with scripting or setting certain specific details, so look into the other commands when you have a chance!

The next command is probably one of the most important, please pay attention closely.

netstat (Network Statistics)

`netstat` is used to view network statistics, active TCP connects and ports currently open on the computer. This is very helpful to see if anything is connected to you. Now, we'll be looking into the flags you can use with this command first because if you just only do netstat then you'll only get little details and information. Note this about flags; you can combine them all together. Remember, flags use dashes instead of slashes. - instead of /

-a displays all of the active TCP connections along with the TCP and UDP ports that the computer has open.
-n displayers the active TCP connections but the port numbers and addresses are expressed with numbers.
-o displays the active TCP connection while also displaying the Process Identification (PID)

So, we can see that netstat gives us network statistics, -a will give us ports and types of connections open, -n will give us addresses and port numbers we can understand more clearly. –o will give us process ID's for each network connection if applicable. And I said that you can combine them, for example, if I wanted all three features for netstat, I would do this.

```
netstat –ano
```

From there, I'd get what I wanted. There is another flag you can use with netstat, it's –p and it's used to specify the protocol. If you wanted TCP connects, you'd do.

```
netstat –p tcp
```

This can also apply to tcp, udp, ip, icmp and many others that you don't have to learn. If you want a netstat connection that constantly updates, simply put a number at the end of netstat, that number will represent how many seconds it will take to update.

```
netstat 5
```

Now, if we wanted a constantly updating every 5 seconds netstat with with active connections, ports & PID's only focusing on TCP, you'd put the command like this.

```
netstat –ano –p tcp 5
```

And that's it! Now let's talk about the options that netstat will allow you to identify. There are a couple categories you'll get when using a netstat.

Proto
Proto is the name of the protocol, such as TCP or UDP.
Local Address (Internal IPs)
This is used to identify any connections to local computers.
Foreign Address (External IPs)
This IP address and port number are for the computer you're currently connected to for that statistic.
State
This indicates the state of a connection. There are 3 you'll find typically, LISTEN, ESTABLISHED, and CLOSED. Listening means it's waiting for a connection, Established means a connection is already made, closed is closed. And I should note that an ESTABLISHED connection is the most worrying as it means that data is being exchanged at that very moment.

sfc (System File Checker)

This last command will be rather brief as it just tells you about a certain command used to check on certain files and whatnot. If any of your important Windows Files are bad then this tool will pick it up. Here's the command.

```
sfc /scannow
```

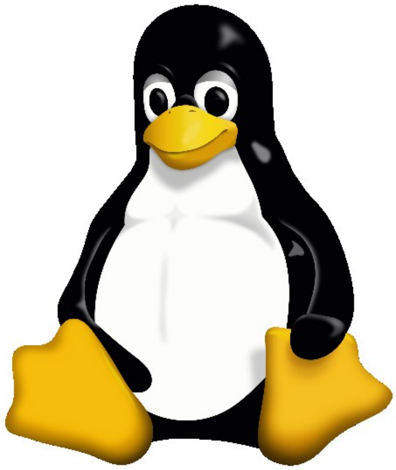
So now we've gotten a full look into command-prompt, a brief but power collection of commands are now in your hands! Remember some of these commands when the time is right, don't forget to check out more, google is your friend!

Let's talk about Linux

It's time for me to talk about Linux. Within the competition, we're also going to be working with an operating system called Linux. Linux is a free operating system that is being developed by hundreds of people, constantly providing fixes and working with it. When working with Linux, you'll mostly be working with a command line. There are no bells and whistles, slow interfaces or GUI's unless you'd like there to be, there's the ability to take complete advantage of the command line.

Skills you learn in Linux are skills that stick for a very long time and are extremely useful. They are looked for by industry professionals because finding young talent with Linux is hard. Hardly anyone knows what Linux is, and yet, it runs hundreds of thousands of web servers, services and so much more you've never thought of.

Now that we've talked about command-line and Linux, we're going to talk about configuring the essentials of internet security.



SECTION 12 – GENERAL INTERNET SECURITY

There are a lot of things that people never think or talk about when it comes to securing even the most basic things that have to do with your internet connections. For instance, some people might not know that their connections are going through a proxy, or they have some settings that aren't correctly configured.

Perhaps every time they go to one website, they ultimately go somewhere completely different. By the time a person would realize these things, it's too late. We're going to talk about configuring some general internet settings.

The first thing we're going to talk about is the host's file. The host's file is where you manually input DNS entries. We looked into DNS a bit when we learned about the command `nslookup`. Let's use a more thorough description here, DNS, known as Domain Name Server/Service, is a database that contains a directory of domain names and translates them from the IP addresses (Internet Protocol). The main reason for such a thing to exist is because obviously, nobody can easily remember an IP address.

Hosts File

So let's talk about accessing the host's file, normally, your host's file will be particularly blank, this a good thing because you don't want any entries in there *at all.* To access your host's file, place the following in the Run Prompt. (Quick note, you can execute commands from the run prompt!)

```
notepad C:\Windows\System32\drivers\etc\hosts
```

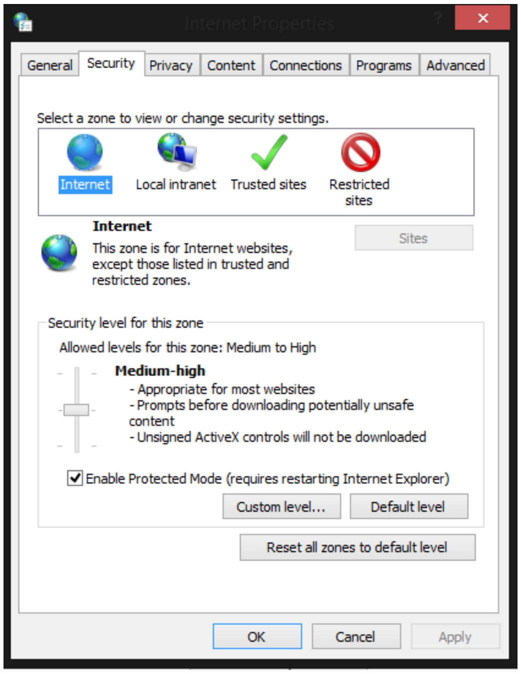
From that point, you'll be able to view everything in there and be able to edit it as well. This is simple tip and something that applies to many different configuration things, but the act of "commenting out" is when you make something ignored on purpose, in this case, there are # symbols in front of lines, these are used to comment out lines that the computer should ignore. Anything that does not start with # will be read by the computer when DNS is taken into effect.

Internet Options

This particular area has to do with browsers. Browsers meaning your internet browsers. Your internet browser has some things that can make them particularly vulnerable, from not updating to having bad settings, but we can fix these things and make them better.

Let's start with viewing our internet options, to do so, press the Windows Key and type "Internet Options".

The tabs we'll be concerning ourselves with will be the general, security, privacy, content, connections and advanced. We'll discuss each way we should handle this.



Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone
Allowed levels for this zone: Medium to High

Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

The beginning step would be going into advanced tab and selecting the button at the bottom to reset Internet Explorer. This part is vital as it will hopefully undo any possible things that may be wrong with Internet Explorer.

From that point, go to the security tab and ensure the security level for all of the settings are at the highest level available. From that point, you should also enable protected mode. This will ensure the automatic enforcing of various security settings. To the privacy tab, you should set it to the highest setting, never allowing websites to request your location, turning on the pop-up blocker and disabling toolbars and extensions when In-Private browsing starts.

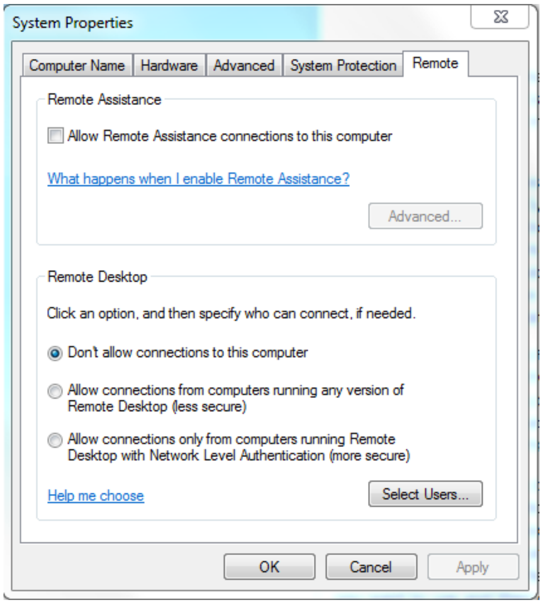
Within the LAN settings in the connections tab, you should ensure that there is **no** use of a proxy and that there are **no** automatic configuration scripts being used. Automatically detecting settings is what you should go with. And finally, In the content tab, clear the SSL state to allow a fresh start with your connections. From this point, a basic standpoint of security has been established. The next step from this point would be ensuring that there are no third party tools, extensions or toolbars in your third-party browsers such as Chrome, Opera, and Firefox.

Along with that, try tweaking the settings for each of those browsers (if they are on the system and required).

Remote Access

This is one of the most important topics when it comes to the security of computers. First, let's establish that most of the time, you'll either be working on a standalone system or a remote system. Standalone systems work by themselves and must be accessed locally, remote systems can be accessed both locally and remotely via the remote desktop application. First, let's learn how to **disable remote access** for a standalone system. Start by going to Control Panel. Once you're there, click System and Security and then System.

When you're on the system page, click Remote Settings to the left. This opens up the System Properties where you can edit the settings for Remote Access. Simply start by **unchecking the Allow Remote Assistance to this computer THEN ensuring that *Don't allow connections to this computer* is checked**.



Remote Assistance

☐ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

After that, Remote Desktop is disabled! But what if we wanted remote access on?

Well, go to System Properties and then check the Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure). This will allow secure remote access to your system, now, if the README asks that you allow specific user's access to Remote Desktop, you must add them via Select Users in the same place you enable/disable remote desktop).

For reference, this is what it looks like. **Otherwise, you may want to consider disabling any Services in Windows Services** relating to anything Remote and Remote Desktop (such as Remote Registry) and deleting any remote access firewall rules. (*Remember to check the README if the system is standalone or not!)* That just about does it for this section. In the next section, we're finally going to cover the full functionality of Microsoft Management Console!

SECTION 13 – MICROSOFT MANGEMENT CONSOLE

Before we learn about anything else, we're going to learn how to use a system administrator's favorite interface for configuring and monitoring your systems. This is the Microsoft Management Console, also known as MMC. Microsoft Management Console is basically an Administrators toolbox. It's a fun way to think of it that way because the beauty of it is that we're able to access an arsenal of tools that will make system's administration snappy and efficient. I'm not going to mention adding snap-in's, but I will say go to page # to quickly review how to add them into the console.

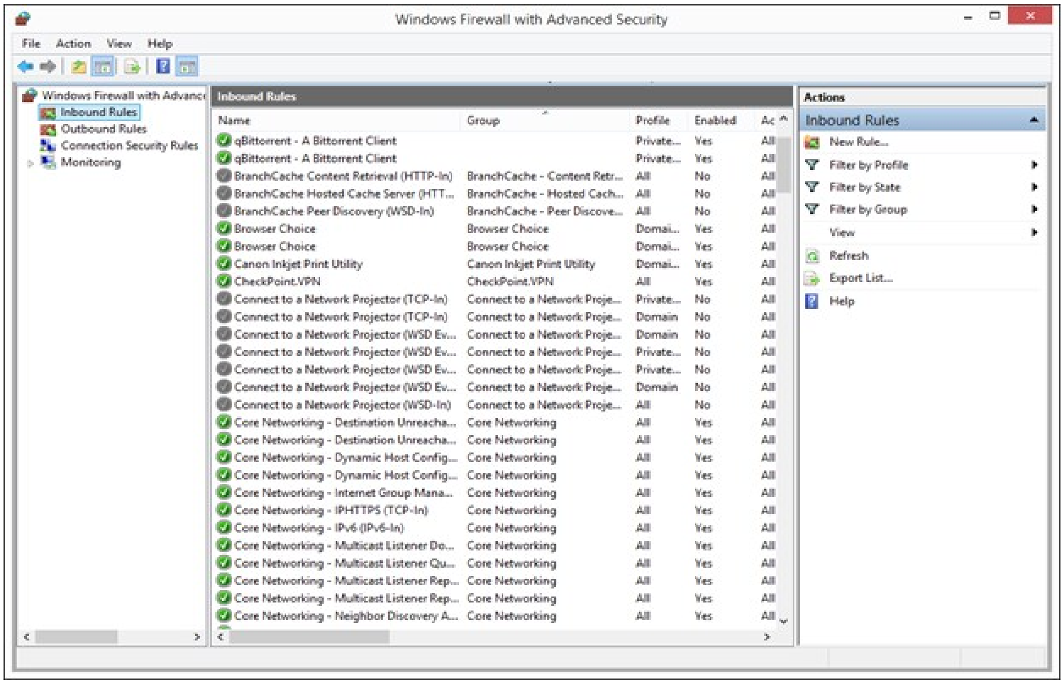
Here is the list of each tool we'll be going over within Microsoft Management Console:

- Windows Firewall with Advanced Settings
- Event Viewer
- Task Scheduler
- Services
- Shared Folders
- Local Users and Groups (not explained in this section, read section's 1, 2 and 3.)
- Local Computer Policy/Group Policy Object
- Computer Management (All of the previous snap-ins except for Local Computer Policy and Firewall)

We'll be going over each tool in detail to ensure you understand the use, details, and interface. The better you know these tools, the faster you can get work done in a snap-in! (*Pun intended for those of you who caught it*)

Windows Firewall with Advanced Settings

We already worked with the basics of Windows Firewall, you know, the one in Control Panel, but now that you have a basic understanding of networking, we can get better with it, and by better, it means we can view the advanced version of Windows Firewall, the one that provides a much better look at your first and best line of defense.



Name	Group	Profile	Enabled	Ac
qBittorrent - A Bittorrent Client		Private...	Yes	All
qBittorrent - A Bittorrent Client		Private...	Yes	All
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	All
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	All
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	All
Browser Choice	Browser Choice	Domai...	Yes	All
Browser Choice	Browser Choice	Domai...	Yes	All
Canon Inkjet Print Utility	Canon Inkjet Print Utility	Domai...	Yes	All
CheckPoint.VPN	CheckPoint.VPN	All	Yes	All
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	All
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	All
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	All
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	All
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	All
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	All
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	All
Core Networking - Destination Unreacha...	Core Networking	All	Yes	All
Core Networking - Destination Unreacha...	Core Networking	All	Yes	All
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	All
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	All
Core Networking - Internet Group Mana...	Core Networking	All	Yes	All
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	All
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	All
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	All
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	All
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	All
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	All
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	All

Within the interface, there will be a drop down menu with inbound rules, outbound rules, connection security rules and monitoring.

Our main focuses will be inbound and outbound rules, the other two categories should be empty. We might as well explain what a firewall is.

Firewalls can block and allow certain inbound and outbound connections; it should be noted that normally, all inbound connections should not be enabled and most outbound connections should be both allowed and limited. The main reason for me to say such a thing is because if inbound connections were constantly allowed, it would mean constant harassment would be essentially allowed by the attacker, resulting in a huge security risk.

A majority of connections going outbound from the network would be okay, but in some instances, it may not, as a result, most companies and schools design a proxy to allow only certain connections to go out. This means blocking ports and preventing certain categories of things to not go outbound, most unknown connections would be blocked. One particular reason for this would be the fact that malicious programs such as *backdoors* or *rootkits* might attempt to call home, meaning it would attempt to communicate with its creators. If it cannot initiate a connection, it cannot connect, resulting in a much more secure environment.

The first step to securing your firewall would be doing a complete factory reset of the settings. This can be accomplished by issuing the following command into command prompt.

```
netsh advfirewall reset
```

This would result in a fresh, brand new set of Firewall rules. Now, within the advanced Firewall, there are individual sets of rules for a variety of programs, most of them being for regular programs or remote stuff. Now here's where we need to do some corrections, if your system is **not** a remote system, then you need to ensure that all remote connection rules are either disabled or deleted. To do either of those things, you must right-click the rule and either disable or delete it.

There is a particular column called profiles within both inbound and outbound with these settings:

- Domain profile: Used when your computer is connected to a domain, a domain being a set of computers
- Private: Used when connected to private networks like homes and work
- Public: Used when connected to Wi-Fi or direct internet connections

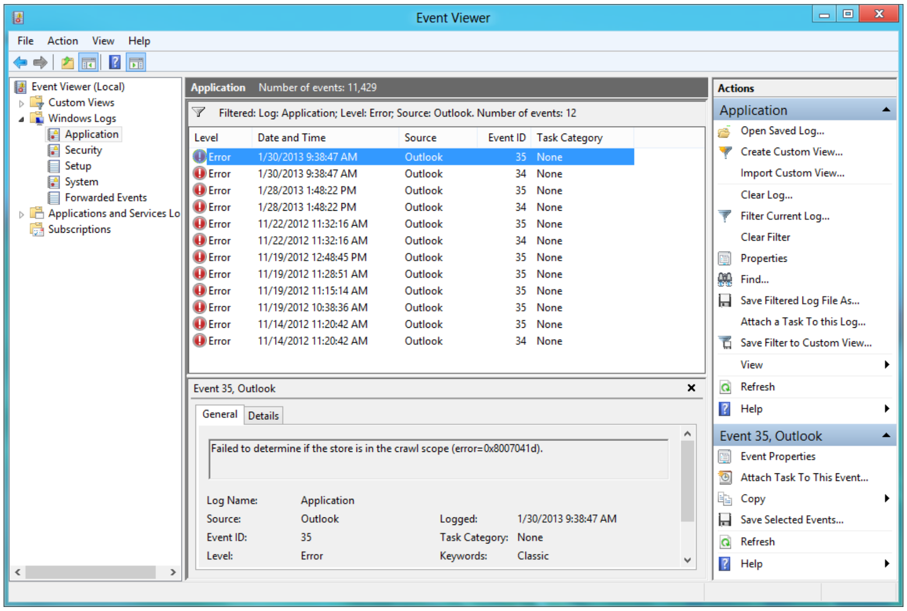
Windows are usually going to bug you about some programs, and sometimes a computer may use both, but ultimately, we're going to enforce the same settings for all Firewalls. Where inbound is not allowed, and outbound is allowed. And before you ask the same question I've heard from everyone, outbound is exclusively outbound, *nobody from outside can initiate a connection with our network,* is what I mean.

That said, particular rules to look into are the ones that are empty, have protocols that we do not approve, have programs that we do not approve, have remote protocols (unless the computer is remote) or are just suspicious.

Event Viewer

This particular area helps the most when it comes to computer forensics. Computer forensics being *forensics questions*. We're going to talk about these quickly before we go into any other subjects. Now, during CyberPatriot competition, you're going to encounter forensics questions, these questions will have things that you need to do and I **highly** recommend that you look into them, like, before you do anything, do the forensics questions first.

Now Event Viewer is a tool that allows you to look into the auditing settings that have happened. Computers that are not auditing events are not capturing proof that something is happening. Sometimes, a forensics question may require that you look into the event log. When it comes to this, you need to ask yourself, "do I really need to?"



Application Number of events: 11,429

Filtered: Log: Application; Level: Error; Source: Outlook. Number of events: 12

Level	Date and Time	Source	Event ID	Task Category
Error	1/30/2013 9:38:47 AM	Outlook	35	None
Error	1/30/2013 9:38:47 AM	Outlook	34	None
Error	1/28/2013 1:48:22 PM	Outlook	35	None
Error	1/28/2013 1:48:22 PM	Outlook	34	None
Error	11/22/2012 11:32:16 AM	Outlook	35	None
Error	11/22/2012 11:32:16 AM	Outlook	34	None
Error	11/19/2012 12:48:45 PM	Outlook	35	None
Error	11/19/2012 11:28:51 AM	Outlook	35	None
Error	11/19/2012 11:15:14 AM	Outlook	35	None
Error	11/19/2012 10:38:36 AM	Outlook	35	None
Error	11/14/2012 11:20:42 AM	Outlook	35	None
Error	11/14/2012 11:20:42 AM	Outlook	34	None

Event 35, Outlook

Failed to determine if the store is in the crawl scope (error=0x8007041d).

Log Name:	Application		
Source:	Outlook	Logged:	1/30/2013 9:38:47 AM
Event ID:	35	Task Category:	None
Level:	Error	Keywords:	Classic

At times, you might not even need to consider the idea of using Microsoft Event Viewer, but when you do, you'll know because the Forensics Question might very well hint such a thing.

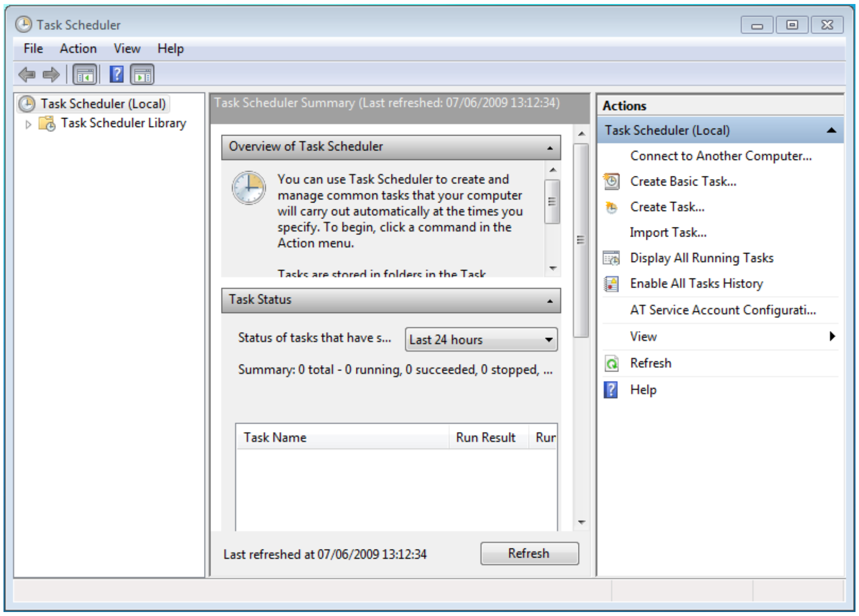
The main area you might be looking into is the security section of the event viewer. What the Event Viewer looks into would be the level of severity, date and time, the source, event ID and task category. With all of those details, you can get a good idea as to what exactly is happening on your computer.

If you can't find anything wrong within the Event Viewer, then maybe the answer you're looking for is not there. Ultimately, exploring Event Viewer will be your best bet to learning to use it.

Task Scheduler

Task Scheduler is a tool that allows people to set things to execute when they're set to. There can be a whole variety of things being executed; one of those things, for instance, would be a script that would execute with Administrative privilege. I'm just trying to give an example.

Task Scheduler can have good things or bad things, how you determine either of those things is by investigating what exactly they are. For instance, when looking into tasks, there will be a name, status, and trigger within the Task Scheduler Library. Triggers and Actions are the most important parts of these scheduled tasks, for instance, if a task simply launches a google application for launching, then it should be fine.



Task Scheduler Summary (Last refreshed: 07/06/2009 13:12:34)

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task

Status of tasks that have s...

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, ...

Last refreshed at 07/06/2009 13:12:34

One of the most notable things I recommend you check is the location of what is executed, how it is executed (privileged or no), where is it being executed and the description.

If no description exists for the items you find within the Task Scheduler Library, then you must investigate further, and by investigating further, we mean potentially delete them.

Services

We briefly covered the Windows Services back in another chapter, so I'll only go into detail or talk about things that you did not know. Windows Services is a place where we can manually turn on and off important services and functions of the Windows Operating System. For instance, you can manually disable or enable Windows Firewall here.

It is highly recommended that you research services, and create a list of services for each version of Windows. You can find many guides and lists on the internet, but I advise you thoroughly research what you need for secure systems and what you don't need.

If the System is standalone (which means you cannot access it through remote access), should the system have services such as Remote Registry be enabled? Absolutely not.

If you don't know how to access services yet, simply do the following.

- Hit the Windows button on your keyboard or hit the start Button
- Type Services into it, Services will appear
- Right-click Services and run it as an Administrator

After that, you will hop into Services, so what makes a Service bad or harmful to the system?

Like I said, if the service is for remote systems and it's enabled on a standalone system, it should **not** be enabled.
If a Service has a blank description, is not in a recognized directory or is extremely suspicious, then it should most likely be looked into. If the service is useless and not required on the system, then you should disable it. Last but not least, services that pose a security risk or as potentially unviable to your system, it should be disabled.

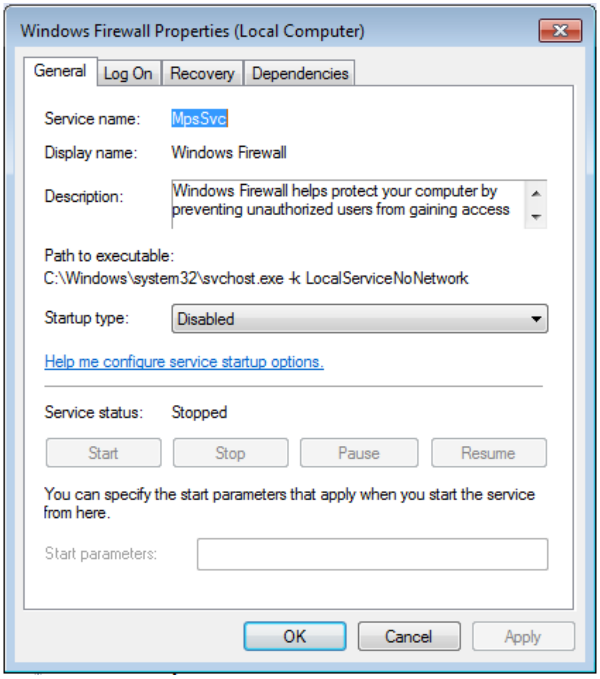
To edit services, simply right-click the Service and go into its properties. From there, you can choose the following settings for it on the General Tab in Startup type.

- ❖ Automatic - Automatic is used for a service to be automatically started as soon as the computer is turned on with Windows. This can be good for things like Windows Firewall.
- ❖ Manual **-** Manual is used so that when a service is started, it'll work, if not, the service will remain dormant.
- ❖ Disabled **-** Disabled is rather simple because it just simply means that the Service will not be started at all unless reactivated via Services.

Also, if you decide to edit any services, it's wise to stop the service after you have modified it.

To identify bad services, a blank description, strange executable in a strange directory or just knowing it is bad is a sign. It wouldn't hurt to disable it and see what happens.

Just for reference, this is the window you get if you are editing any Services.



Service name: MpsSvc

Display name: Windows Firewall

Description: Windows Firewall helps protect your computer by preventing unauthorized users from gaining access

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork

Startup type: Disabled

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Shared Folders

In an earlier chapter, I discussed the net share command, this command allowed you to review what shares existed on a system. Using Microsoft Management Console, you can view the shares from this snap-in. Remember that default shares ADMIN$, C$ and IPC$ are normally hidden, if you delete them, they will come back. If you happen to see any other shares other than those, it is a security risk that should be dealt with.

There is also a session and open files folder, if there should not be sessions open or open files, then having those items in either is bad. To truly learn how to use the Shared Folders Snap-In, you need to explore and learn how to use it. If you saw important files, things from the Windows Folder, etc. In the shares, it's no good clearly.

Local Computer Policy

The Snap-In Local Computer Policy gives you full access to computer configurations. These configurations go from Local Security Policies to Local Group Policies. Both of these items are extremely important and feature their own section as a guide on how to configure everything.

Computer Management

The Snap-In Computer Management actually gives you a majority of the tools listed above (Event Viewer, Shared Folders, Services, Local Users and Groups) only lacking Local Computer Policy, Windows Firewall with Advanced Security, and Task Scheduler.

Using the Microsoft Management Console to Your Advantage

The main point of introducing this tool is to familiarize you with how exactly you're going to get further into CyberPatriot. This tool is probably one of the most important tools you could possibly use.

To take advantage of it, you can save the console onto your desktop so that if you close it, all of the snap-ins you chose are located there.

From this point, I hope that you take full advantage of the Microsoft Management Console. In the next section, we're going to talk about file permissions and finding files that should *not* exist on your systems.

SECTION 14 – FILE MANAGEMENT AND SEARCHING

Files are an important item when it comes to computers. Why? Almost everything is a file; you need to have access to your things while no one else can have access to your things. How can this be accomplished? Let's get to enforcing file security.

The first thing we want to do is understand the exact basics of file security. That is reading, writing and executing. What are those exactly? They're right you can have to a file. To have all of those, you either own the file or are an Administrator.

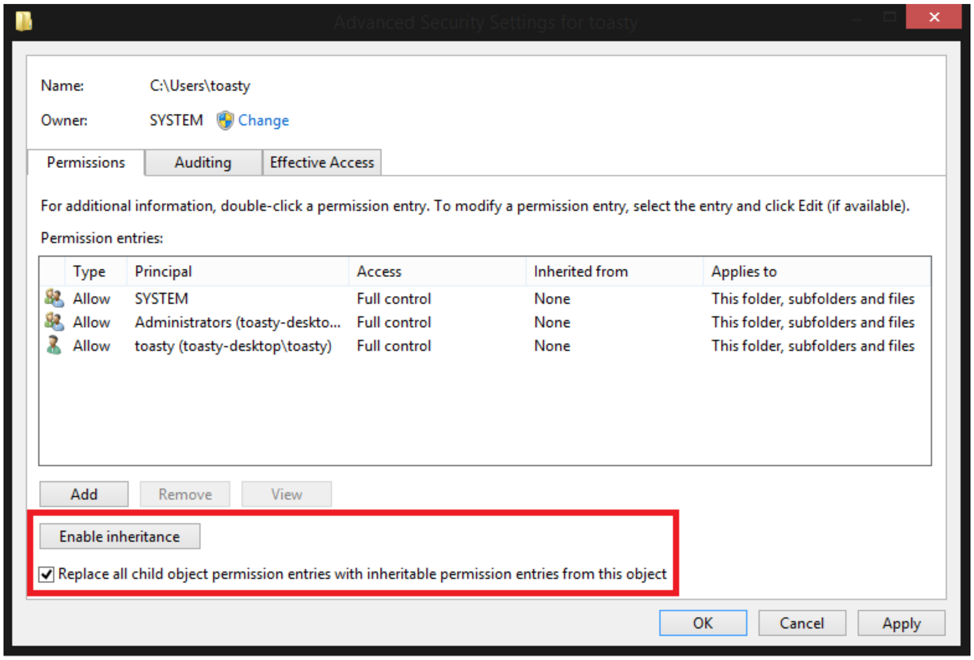
- **Read** – The ability to read the file
- **Write** – The ability to edit the file
- **Execute** – The ability to execute the file

In the Windows Operating System, our main concern here is ensuring that the people who own the files are the only ones (with the exception of Administrators) that can manage their own files. Anyone else managing files like that will pose a security risk. Imagine if someone had access to read, write and execute in the Windows folder? Clearly, it would be bad. The next thing I would like to explain is Explicit vs. Inherited.

Explicit is when the permissions set is exclusively for that folder. If you want specific permissions for that folder, you can absolutely set it to be like that.

Inherited is when you make it so that a parent folder enforces all children objects below it to inherit the permissions it received. You can do this with many folders to quickly secure them. Simply by going into the Properties, down below in the security tab you can select certain permissions and set the child objects from that point onward to receive the exact same permissions.

Places you need to check in the case whether permissions are actively guarding the files or not are places such as user folders, important items, and other items.



Advanced Security Settings for toasty

Name: C:\Users\toasty

Owner: SYSTEM Change

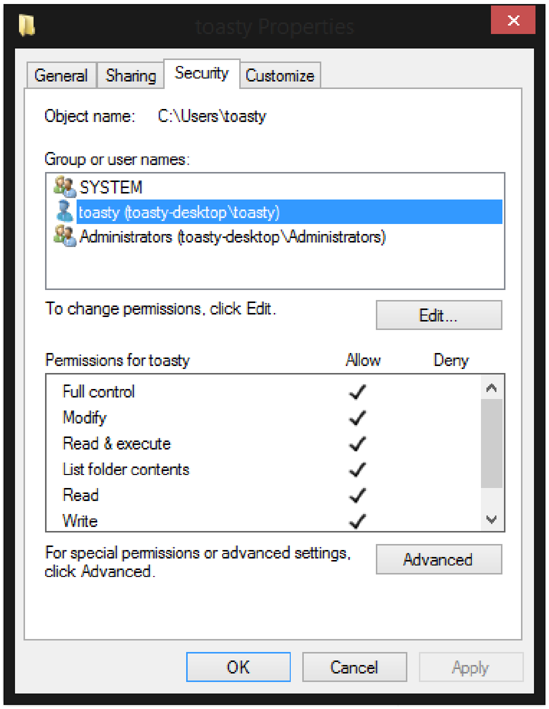
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (toasty-deskto...	Full control	None	This folder, subfolders and files
Allow	toasty (toasty-desktop\toasty)	Full control	None	This folder, subfolders and files

☑ Replace all child object permission entries with inheritable permission entries from this object

Let's talk about NTFS. Originally, you would use the file system, FAT32, would be used on USBs and whatnot much more. Because of how old and standard it's become, you see many different things with it. There are some limitations on FAT32, such as a 4GB max on file sizes and a max of 8TBs. The good part is how it's compatible with practically everything due to being the standard file format.



toasty Properties

Object name: C:\Users\toasty

Group or user names:

- SYSTEM
- toasty (toasty-desktop\toasty)
- Administrators (toasty-desktop\Administrators)

To change permissions, click Edit.

Permissions for toasty	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

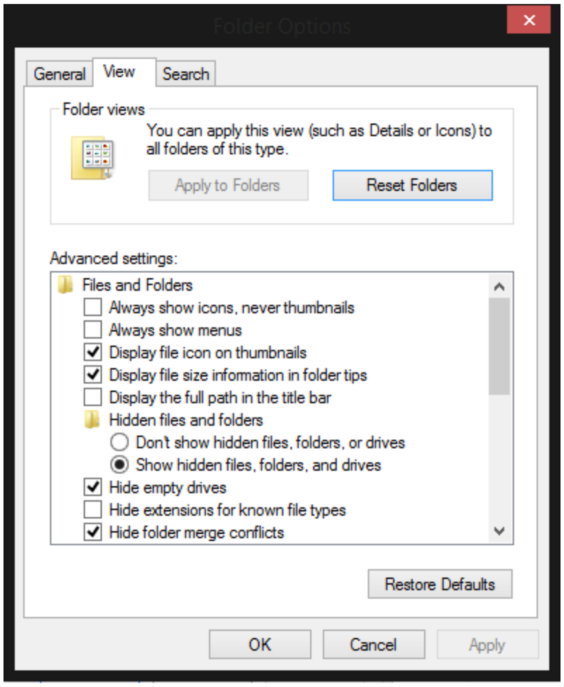
For special permissions or advanced settings, click Advanced.

But NTFS is Window's new file system. NTSF has many different file permission types unlike FAT32 and comes with some advantages, such as the increased security, error recovery and ability to store larger files. A big problem, however, is it's only truly compatible with Windows Systems.

So now we know the file system we use on Windows, NTSF, is unique to Windows only. Unfortunately, we don't get simple file permissions like Linux. We get many, complex features. This can easily be worked with, though. We'll start with regular user directories. The truth is, if you're the owner, these are the permissions you should have (exclude Special Permissions). Administrators and SYSTEM should have the same settings. No one else should have access. Notice how it says C:\Users\toasty, it's *my* directory, meaning no one else should be allowed to have access, any other people attempting to access it will be denied from this point.

Now, we're going to talk about permissions for let's say the Windows Folder, the security permissions should be so that only TrustedInstaller, System, Administrators should have full control of this area. No one, not even you, should have full control of the Windows Directory, especially the subfolders and whatnot. I think you understand what I mean by this. Mess around with the security settings of folders for better examples.

Next thing we're going to talk about is finding files. This part you may actually find useful, so let's get start with the first step. I believe a long time ago, I had told you that files *can* be hidden from the regular user. Did you also know that you can change the extension of a file, ultimately fooling the user? This is taking advantage of the fact that Microsoft Windows *does not* hide common file extensions, these extensions include .exe or .com.



Folder Options

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

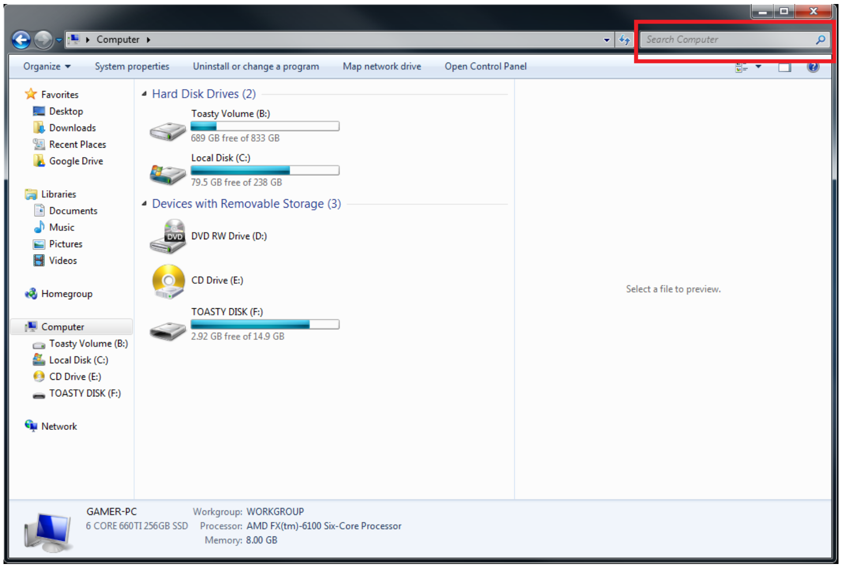
Files and Folders
- ☐ Always show icons, never thumbnails
- ☐ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- ☐ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives
- ☐ Hide extensions for known file types
- ☑ Hide folder merge conflicts

Anything. If it is common, will be hidden from the user. How can we fix this problem? We have Windows fix it for us. Start by looking up "folder options", from there, you can go to view the current settings for folder options within the View tab.

These are the correct settings for Folder Options, and by "correct settings" I mean that **Show hidden files, folders, and drives should be *checked*** and **Hide extensions for known file types should be *unchecked.***

This can allow you to look for files without any problems at all.

Some directory I would recommend you check is C:\Users\, C:\ProgramFiles\, or just do a broad search of the entire C: drive, regardless, you'll be having to find files within an entire disk.



From that point, you're now ready to search for files, but what kind of files are we searching for? All sorts of things, in the README, CyberPatriot will tell you what is not allowed on a system, things such as media, pictures, or "hacking tools".

So when we search for files, we use *extensions.* When we use extensions, we're asking for specifics from Windows. Extensions are specific, things such as .mp3, .exe, .png, .pdf, etc. An extension is used to address what type of file a file is, the media player only supports .mp3 and .wav, so it looks for and uses those. A photo editor will only edit .png, .jpg, etc. How can we look for specific files?

The first thing we're going to do is go into our main volume, C: from that point, you can go into a specific directory and search from there. Try typing *.mp3 into the search box. If you do this, you will have only MP3 results in Windows Explorer. There are so many different types of file extensions you can search for.

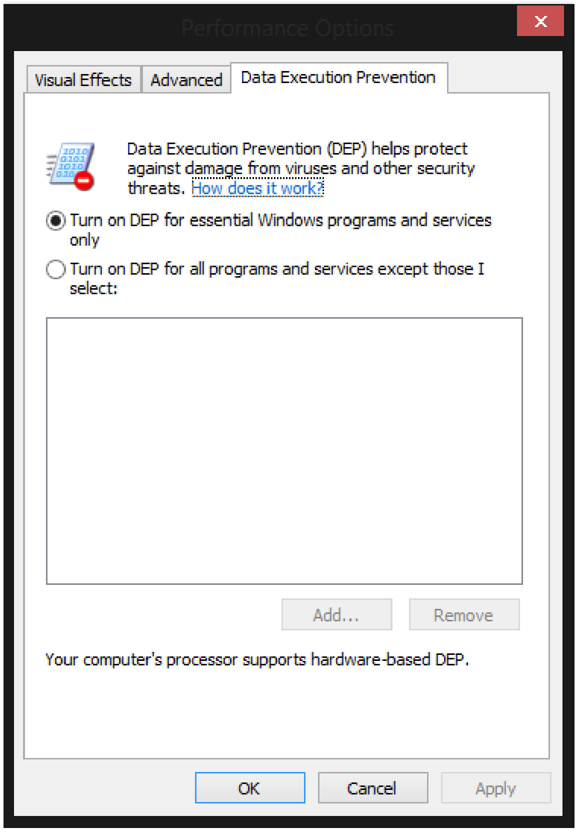
- Music - .mp3, .wav, .m4a, .ogg
- Video - .avi, .mp4, .flv, .wmv, .mov, .webm, .mpg
- Documents - .pdf, .docx, .txt

Now, when you search in a specific directory, you'll get very specific results. If you are in the root of the drive, or, C:, , every file would be checked and resulted if it matched the criteria or not. *If you want a much broader search, try using the advanced query syntaxes in the Window's Search. An example would be putting 'kind:' into the search bar followed by things such as music, videos, programs, docs, etc.*

The final topic we're going to talk about is DEP, also known as Data Execution Prevention. It's a small but very important feature. To access DEP, go to Control Panel → System and Security → System → Advanced System Settings → Advanced Tab → Performance → Settings → Data Execution Prevention.

This feature performs additional checks on your computer's memory to prevent malicious code from running. The only thing you should make sure of is that DEP is turned on for All Programs and Services and no exceptions are made.

In the next section, we're going to talk about everyone's favorite set of tools, the Sys Internals.



Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

● Turn on DEP for essential Windows programs and services only

○ Turn on DEP for all programs and services except those I select:

Your computer's processor supports hardware-based DEP.

SECTION 15 – INTRODUCTION TO THE SYS INTERNALS

The SysInternal tools were created in 1996 by Mark Russionovich to help IT professionals make their tasks a little easier. With this platform of tools, you've got a much stronger set of items to work with.

Here's a list of all the tools we may be using during competition. Each tool serves a role which is described below.

- ❖ Process Explorer – Used to find out what files, registry keys, and other objects processes have open.
- ❖ TCP View – Active connection viewer.
- ❖ Autoruns – Used to view all processes that start with the system.
- ❖ Sigcheck – Sigcheck is used to show a file's signature details. It works well for malware hunting and authenticity of files.
- ❖ Sdelete – Sdelete is used to delete files completely, to the point where it **cannot** be recovered.
- ❖ AccessEnums – Allows easy file permission management.

Each of these tools have a vibrant and important role in basic administrative tasks, mastering each tool by messing around with them and practicing is key to becoming an IT professional, we'll start with everyone's favorite tool.

Process Explorer (procexp.exe)

Processor Explorer is said to be the absolute best and most powerful utility of the SysInternal toolkit. It's a task manager and system monitor and has been used in the beginning when regular old' Task Manager just wasn't enough. With accurate, real-time data, many useful features & amazing flexibility, this tool is used for powerful task management.

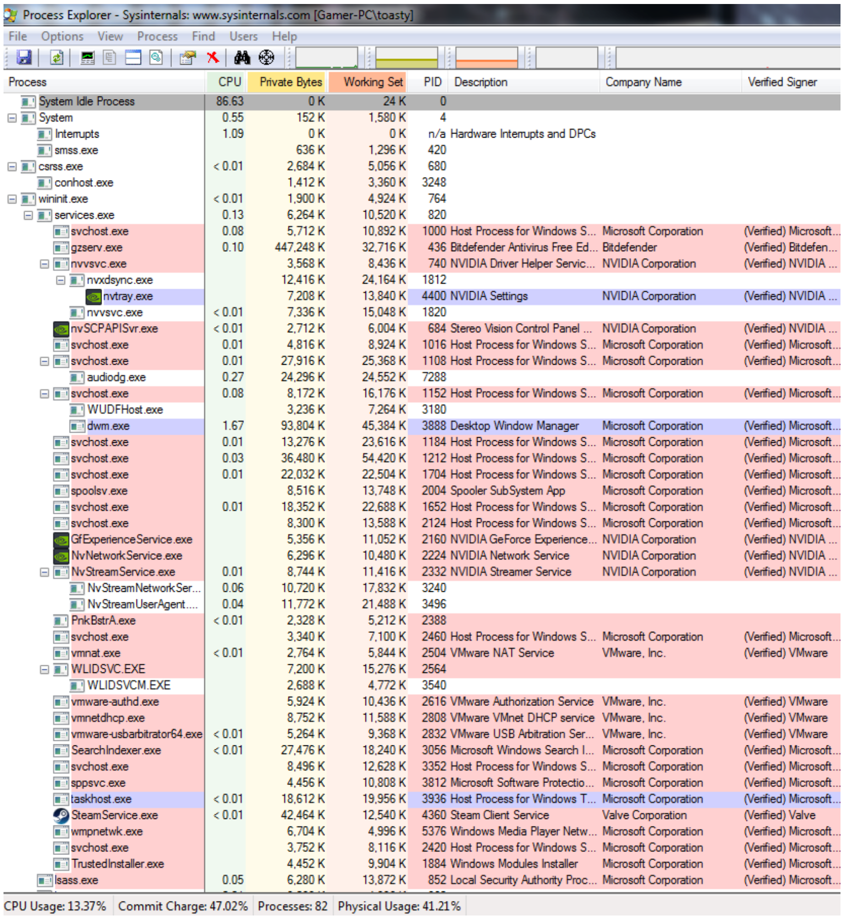
Before I begin, let's look into some terminology and explain some things that would be considered confusing.
A good place to start would be talking about processes column. Processes listed there are programs running and current doing tasks, whatever it may be, it's going to have a CPU usage and whole other load of information.
A process can have more processes branch off of it, this is called a process tree. The beginning process would be considered the parent and any processes that started off of it are called children.

The next column is CPU, which is how much of the CPU the program is using. System Idle has the most CPU usage, however, it is idle so it's waiting to be used.

The working set is how much memory is being used. PID is the Process Identification, the way the process is recognized by the system from Command-Prompt to Task Manager to Process Explorer.

The description is the description, the company name is the company that created the program and the verified signer is who signed it. As far as we're concerned, what we need to know is whether all of those programs are the real deal and we know what should and shouldn't be running on the system.

Here’s a screenshot of Process Explorer.



Process Explorer - Sysinternals: www.sysinternals.com [Gamer-PC\toasty]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
System Idle Process	86.63	0 K	24 K	0			
System	0.55	152 K	1,580 K	4			
Interrupts	1.09	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		636 K	1,296 K	420			
csrss.exe	< 0.01	2,684 K	5,056 K	680			
conhost.exe		1,412 K	3,360 K	3248			
wininit.exe	< 0.01	1,900 K	4,924 K	764			
services.exe	0.13	6,264 K	10,520 K	820			
svchost.exe	0.08	5,712 K	10,892 K	1000	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
gzserv.exe	0.10	447,248 K	32,716 K	436	Bitdefender Antivirus Free Ed...	Bitdefender	(Verified) Bitdefen...
nvvsvc.exe		3,568 K	8,436 K	740	NVIDIA Driver Helper Servic...	NVIDIA Corporation	(Verified) NVIDIA ...
nvxdsync.exe		12,416 K	24,164 K	1812			
nvtray.exe		7,208 K	13,840 K	4400	NVIDIA Settings	NVIDIA Corporation	(Verified) NVIDIA ...
nvvsvc.exe	< 0.01	7,336 K	15,048 K	1820			
nvSCPAPISvr.exe	< 0.01	2,712 K	6,004 K	684	Stereo Vision Control Panel ...	NVIDIA Corporation	(Verified) NVIDIA ...
svchost.exe	0.01	4,816 K	8,924 K	1016	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.01	27,916 K	25,368 K	1108	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
audiodg.exe	0.27	24,296 K	24,552 K	7288			
svchost.exe	0.08	8,172 K	16,176 K	1152	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe		3,236 K	7,264 K	3180			
dwm.exe	1.67	93,804 K	45,384 K	3888	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.01	13,276 K	23,616 K	1184	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.03	36,480 K	54,420 K	1212	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.01	22,032 K	22,504 K	1704	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
spoolsv.exe		8,516 K	13,748 K	2004	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.01	18,352 K	22,688 K	1652	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		8,300 K	13,588 K	2124	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
GfExperienceService.exe		5,356 K	11,052 K	2160	NVIDIA GeForce Experience...	NVIDIA Corporation	(Verified) NVIDIA ...
NvNetworkService.exe		6,296 K	10,480 K	2224	NVIDIA Network Service	NVIDIA Corporation	(Verified) NVIDIA ...
NvStreamService.exe	0.01	8,744 K	11,416 K	2332	NVIDIA Streamer Service	NVIDIA Corporation	(Verified) NVIDIA ...
NvStreamNetworkSer...	0.06	10,720 K	17,832 K	3240			
NvStreamUserAgent....	0.04	11,772 K	21,488 K	3496			
PnkBstrA.exe	< 0.01	2,328 K	5,212 K	2388			
svchost.exe		3,340 K	7,100 K	2460	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
vmnat.exe	< 0.01	2,764 K	5,844 K	2504	VMware NAT Service	VMware, Inc.	(Verified) VMware
WLIDSVC.EXE		7,200 K	15,276 K	2564			
WLIDSVCM.EXE		2,688 K	4,772 K	3540			
vmware-authd.exe		5,924 K	10,436 K	2616	VMware Authorization Service	VMware, Inc.	(Verified) VMware
vmnetdhcp.exe		8,752 K	11,588 K	2808	VMware VMnet DHCP service	VMware, Inc.	(Verified) VMware
vmware-usbarbitrator64.exe	< 0.01	5,264 K	9,368 K	2832	VMware USB Arbitration Ser...	VMware, Inc.	(Verified) VMware
SearchIndexer.exe	< 0.01	27,476 K	18,240 K	3056	Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		8,496 K	12,628 K	3352	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
sppsvc.exe		4,456 K	10,808 K	3812	Microsoft Software Protectio...	Microsoft Corporation	(Verified) Microsoft...
taskhost.exe	< 0.01	18,612 K	19,956 K	3936	Host Process for Windows T...	Microsoft Corporation	(Verified) Microsoft...
SteamService.exe	< 0.01	42,464 K	12,540 K	4360	Steam Client Service	Valve Corporation	(Verified) Valve
wmpnetwk.exe		6,704 K	4,996 K	5376	Windows Media Player Netw...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		3,752 K	8,116 K	2420	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
TrustedInstaller.exe		4,452 K	9,904 K	1884	Windows Modules Installer	Microsoft Corporation	(Verified) Microsoft...
lsass.exe	0.05	6,280 K	13,872 K	852	Local Security Authority Proc...	Microsoft Corporation	(Verified) Microsoft...

CPU Usage: 13.37% | Commit Charge: 47.02% | Processes: 82 | Physical Usage: 41.21%

At first, the window might seem filled with clutter, but as far as I’m concerned all of those programs are not clutter, in fact, a majority of them are child processes.

Now that I’ve explained the interface, I’m going to need to show a particularly handy feature. If you press Options, you’ll be able to use a variety of things. The first one is Verify Image Signature.

This is used to review the file to see if it matches with the original publishers, if it is not, you may have a faulty program on your hands. Another thing in Options is virustotal, virustotal.com is used by Process Explorer to check if whatever you’re running on your system has anything wrong with it.

Also, if you’re wondering, svchost.exe (Service Host) is a system process that hosts multiple Windows Services of the Operating System. It’s an essential program that has reduced resource consumption and allows more efficient work with processes.

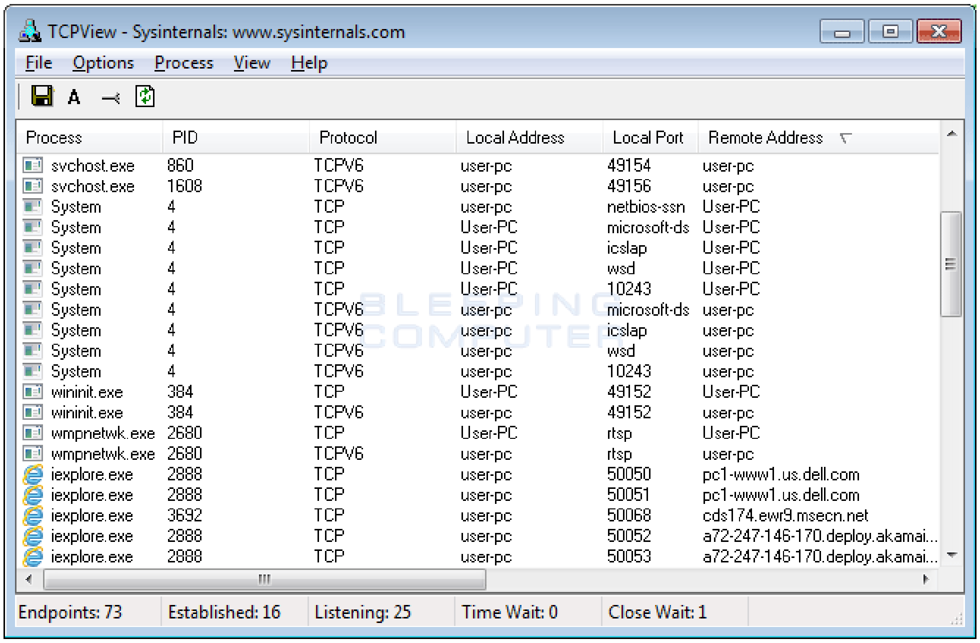
This is a good way to find malware or any programs that can be flagged PUPs or Malware. If you right-click a process, you’ll be able to end it, find the properties or all those other things. Process Explorer is a very good tool so keep in mind this is one tool to rely on when you really need the upper hand.

TCPView (tcpview.exe)

TCPView is a program that shows you what is connecting to the internet. Pretty simple, and it can really help you pinpoint an IP address or port a program is using.

Let’s say you’ve got a Forensics Question asking “What IP address is the backdoor attempting to communicate with?”

You can easily find the answer to your question in TCPView. Let’s look at a screenshot by bleepingcomputer.com



Process	PID	Protocol	Local Address	Local Port	Remote Address
svchost.exe	860	TCPV6	user-pc	49154	user-pc
svchost.exe	1608	TCPV6	user-pc	49156	user-pc
System	4	TCP	user-pc	netbios-ssn	User-PC
System	4	TCP	User-PC	microsoft-ds	User-PC
System	4	TCP	User-PC	icslap	User-PC
System	4	TCP	User-PC	wsd	User-PC
System	4	TCP	User-PC	10243	User-PC
System	4	TCPV6	user-pc	microsoft-ds	user-pc
System	4	TCPV6	user-pc	icslap	user-pc
System	4	TCPV6	user-pc	wsd	user-pc
System	4	TCPV6	user-pc	10243	user-pc
wininit.exe	384	TCP	User-PC	49152	User-PC
wininit.exe	384	TCPV6	user-pc	49152	user-pc
wmpnetwk.exe	2680	TCP	User-PC	rtsp	User-PC
wmpnetwk.exe	2680	TCPV6	user-pc	rtsp	user-pc
iexplore.exe	2888	TCP	user-pc	50050	pc1-www1.us.dell.com
iexplore.exe	2888	TCP	user-pc	50051	pc1-www1.us.dell.com
iexplore.exe	3692	TCP	user-pc	50068	cds174.ewr9.msecn.net
iexplore.exe	2888	TCP	user-pc	50052	a72-247-146-170.deploy.akamai...
iexplore.exe	2888	TCP	user-pc	50053	a72-247-146-170.deploy.akamai...

Endpoints: 73 | Established: 16 | Listening: 25 | Time Wait: 0 | Close Wait: 1

Now, from the screenshot, we’ll identify each thing about TCPView.
Process – The process on your system using the connection
PID – The Process Identification Number of the process
Protocol – The protocol being used to communicate
Local Address – Typically your Local Address (i.e. your computer's name)
Local Port – The port being used to communicate
Remote Address – The address your computer is connected to

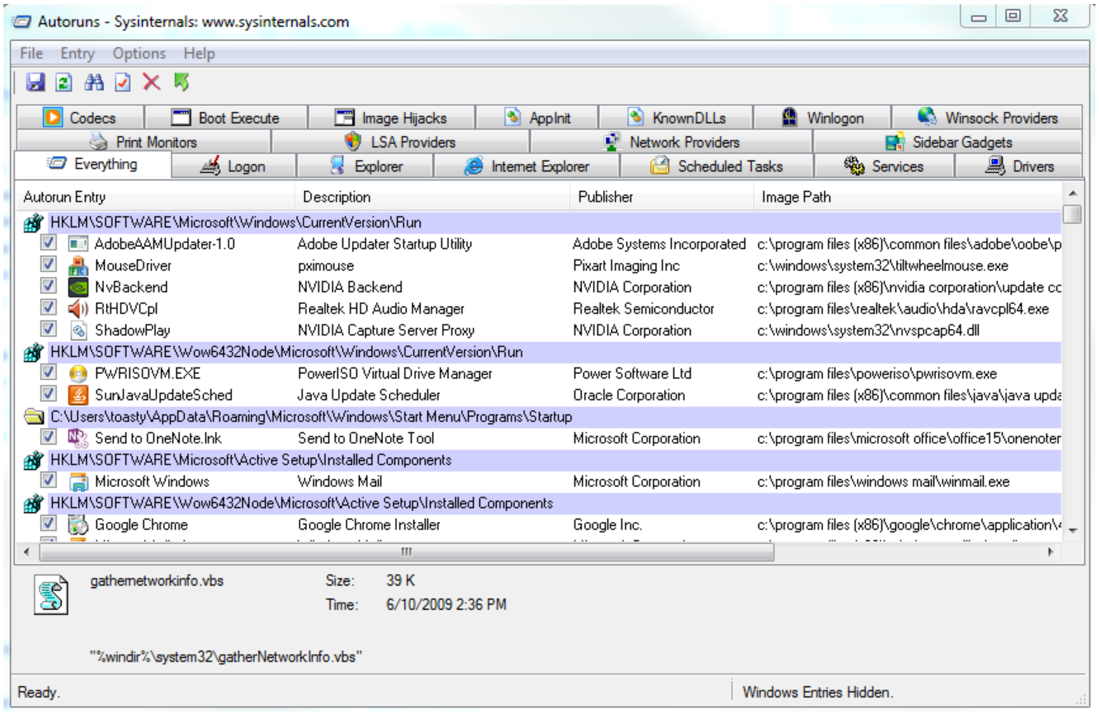
You’d find your answer to the question by using the PID or Process name and then looking at what Remote Address the program is connecting to.

So TCPView is great for looking at connections, but so is netstat and a program I’ll mention in the future called CurrPorts, so just use whatever you’re good with!

Autoruns (autoruns.exe)

The real reason why some computers might be so slow to start up or have so many things starting up is because you might not have cleaned up your programs that run automatically. I'll explain two ways to view what starts up automatically but I'll explain the SysInternal tool Autoruns, why? Because some programs might not be able to be easily edited when starting up, like some viruses.

This is the interface for Autoruns.



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\oobe\p
☑ MouseDriver	pximouse	Pixart Imaging Inc	c:\windows\system32\tiltwheelmouse.exe
☑ NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporation\update cc
☑ RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\ravcpl64.exe
☑ ShadowPlay	NVIDIA Capture Server Proxy	NVIDIA Corporation	c:\windows\system32\nvspcap64.dll
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
☑ PWRISOVM.EXE	PowerISO Virtual Drive Manager	Power Software Ltd	c:\program files\poweriso\pwrisovm.exe
☑ SunJavaUpdateSched	Java Update Scheduler	Oracle Corporation	c:\program files (x86)\common files\java\java upda
C:\Users\toasty\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ Send to OneNote.lnk	Send to OneNote Tool	Microsoft Corporation	c:\program files\microsoft office\office15\onenoter
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components			
☑ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\application\

gathernetworkinfo.vbs Size: 39 K
Time: 6/10/2009 2:36 PM

"%windir%\system32\gatherNetworkInfo.vbs"

Ready. Windows Entries Hidden.

Autoruns is used to edit all of the items that automatically run the program. I'll explain what everything means, however, you may as well stay on the Everything tab because you'll end up covering everything Autoruns has.
It also allows you to look at everything or only specifics; it comes with the entry for automatically running, or, the name. The description is a simple description, the publisher is who created the program and the image path is where the file exists.

Now, if you feel suspicious about a program, right-click it and click Search Online. Another good idea is right-clicking and opening it in Process Explorer and then verifying it or scanning it in VirusTotal through there. Another way to view your automatically running programs is msconfig.exe

You can run msconfig.exe by pressing the Windows Button and R at the same time; this will open the run prompt. Once you've done so, type msconfig.exe, when you do this, it'll show up.

We're going to have a section dedicated to start up, and note this: **Unless you are absolutely sure, do not delete anything. If it's flagged by anti-virus, sure, if it's literally causing havoc, sure, if it's showing suspicious activity, maybe but ultimately, do not delete things at random.**

Sigcheck (sigcheck.exe)

Sigcheck is a command-line based tool. So this will be rather easy to explain. First off. Sigcheck does **not** have a GUI, you will have to have a command prompt with administrative rights open. Now, when you have that, go ahead and run Sigcheck through there (whether with a relative or absolute pathname) when it opens, it'll give you all the things you can do with Sigcheck. This is a good idea to check a lot of files. Now, there are a variety of flags you can use with Sigcheck. Here they are.

- -e will allow you to check only executables for their signature
- -u will only report any problems with the files' signatures
- -v and –vt you should use both of these, it will allow you to check the files with VirusTotal

Some examples, if I wanted to scan all of System32's executables for their digital signatures, I would do this.

```
Sigcheck –e –u C:\Windows\System32
```

If I wanted to scan a file with VirusTotal, I would do this.

```
Sigcheck –v –vt <filename>
```

You can combine as many flags as you want I believe. Just remember you have to meet the criteria for using Sigcheck;

- You are in the directory with sigcheck.exe or know the absolute pathname
- The file you scan you either use the relative name or use the absolute pathname

Other than that, you can verify things with ease now.

Sdelete (sdelete.exe)

When you delete a file, normally, it's not actually deleted. It's only marked as deleted, but anything that Is still intact can still be recovered, this can be changed.

Note, that this program is also command line based! So, you must follow this criteria.

- You are in the directory with sdelete.exe or know the absolute pathname
- The file you delete you either use the relative name or use the absolute pathname

So, if you wanted to delete a file, simply do.

```
Sdelete <filename>
```

Just remember, an attacker that has direct access to the original disk can still recover the files contents, so if there is something that you need to go through great lengths just to delete, sdelete is your best bet.

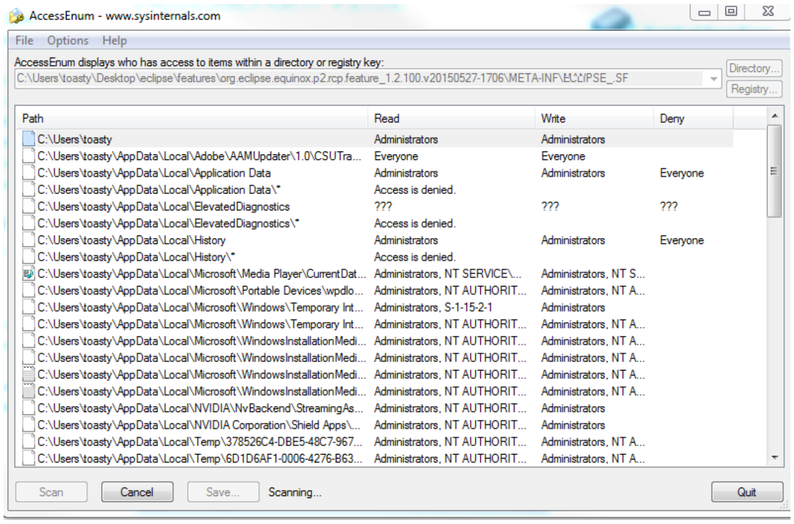
AccessEnums (accessenums.exe) and Learning File Permissions

Before we talk about AccessEnums, I'd like to clarify what File Permissions are again if you did not understand a simple explanation on it before. There are three permissions, Read, Write, and Execute, also known as RWX.

- Read, is used to read files and look into the contents. You cannot Read unless you can execute.
- Write is used to edit and make changes to the file, you cannot write without read.
- Execute, is the ability to execute and operate the program, you cannot execute unless you can read.

Notice how you can't do some of these without the other? Remember, **the only people who should be able to access a file is you and the Administrator.** AccessEnums shows you the permissions of files and folders if someone else has access to another person's folder, that **cannot** be allowed.

Now then, let's look at AccessEnums' interface.



AccessEnum displays who has access to items within a directory or registry key:

C:\Users\toasty\Desktop\eclipse\features\org.eclipse.equinox.p2.rcp.feature_1.2.100.v20150527-1706\META-INF\ECLIPSE_.SF

Path	Read	Write	Deny
C:\Users\toasty	Administrators	Administrators	
C:\Users\toasty\AppData\Local\Adobe\AAMUpdater\1.0\CSUTra...	Everyone	Everyone	
C:\Users\toasty\AppData\Local\Application Data	Administrators	Administrators	Everyone
C:\Users\toasty\AppData\Local\Application Data*	Access is denied.		
C:\Users\toasty\AppData\Local\ElevatedDiagnostics	???	???	???
C:\Users\toasty\AppData\Local\ElevatedDiagnostics\*	Access is denied.		
C:\Users\toasty\AppData\Local\History	Administrators	Administrators	Everyone
C:\Users\toasty\AppData\Local\History\*	Access is denied.		
C:\Users\toasty\AppData\Local\Microsoft\Media Player\CurrentDat...	Administrators, NT SERVICE\...	Administrators, NT S...	
C:\Users\toasty\AppData\Local\Microsoft\Portable Devices\wpdlo...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Microsoft\Windows\Temporary Int...	Administrators, S-1-15-2-1	Administrators	
C:\Users\toasty\AppData\Local\Microsoft\Windows\Temporary Int...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Microsoft\WindowsInstallationMedi...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Microsoft\WindowsInstallationMedi...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Microsoft\WindowsInstallationMedi...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Microsoft\WindowsInstallationMedi...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\NVIDIA\NvBackend\StreamingAs...	Administrators, NT AUTHORIT...	Administrators	
C:\Users\toasty\AppData\Local\NVIDIA Corporation\Shield Apps\...	Administrators, NT AUTHORIT...	Administrators	
C:\Users\toasty\AppData\Local\Temp\378526C4-DBE5-48C7-967...	Administrators, NT AUTHORIT...	Administrators, NT A...	
C:\Users\toasty\AppData\Local\Temp\6D1D6AF1-0006-4276-B63...	Administrators, NT AUTHORIT...	Administrators, NT A...	

Scanning...

I decided to scan my own directory, it appears only Administrators may access it, anyone else who attempts to access it will fail. I might as well talk about trees again.

With files and folders, things typically branch out. If you use the command tree in your command prompt, you'll get a tree. Now, there are parent directories and subdirectories.

The subdirectories are contained in the parent directory, consider C:\Users\Toasty as a Parent directory and everything in it considered a subdirectory.

That's how it goes. However, a parent directory can still be considered a subdirectory, since the folder C:\Users\Toasty is in the directory C:\Users.

Some individual folders may have different permissions, however, so scanning the whole directory and reviewing for any bad permissions may be your best bet. So, how do we change these permissions?

If you happen to find bad permissions here in AccessEnums, you can right click the entry and click properties; from there, you can edit the permissions in the Security tab.

Now, what you do is click edit and then edit these settings to your content... But what if you can't? What if you're completely locked out of editing the file? Well, you can defiantly help that.

There are owners for files, if the file was yours, you can do anything you want, but sometimes the owner's permissions may have been reassigned. We recently covered files, so use what you learned in Section 14 here.

In the next section, we're going to cover Startup Management.

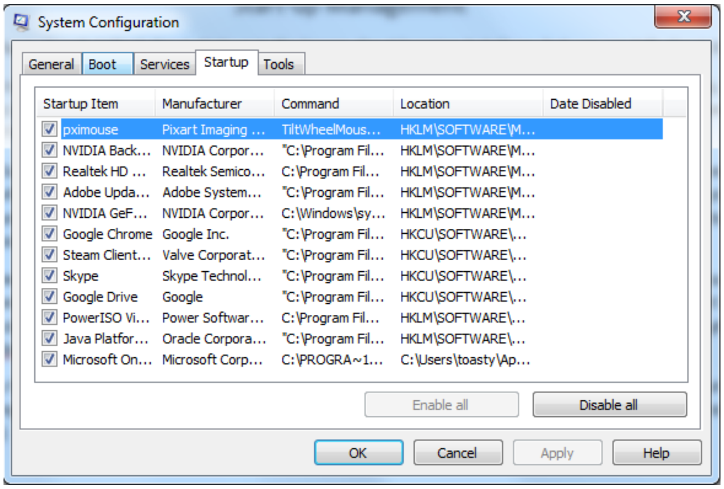
SECTION 16 – STARTUP MANAGEMENT

Sometimes some of the biggest problems you find on a computer might just be in the startup area. From having scripts to things that should not be there, this is how some people do their IT stuff, and how some attackers can have their stuff hide. We're going to talk about startup locations.

The start-up is can defined as many things, for one, it may have all of the programs that normally start when you get your computer booted up, otherwise, you might have programs in the start-up so that you can work on them as soon as possible. It's better to have just what you need on your computer. To do this, we have four different methods of viewing what start's up. The first one is by using AutoRuns from the SysInternals suite.

SysInternals Suite (www.sysinternals.com) contains a tool called AutoRuns. We already reviewed over what exactly you can do with AutoRuns, but I'll remind you again. AutoRuns has the ability to view everything that begins with the computer so that nothing is hidden. How does it do this? It checks the DNA of Windows, the registry.
It's probably the most accurate tool you can use for startup and allows you to really take control of everything.

So how do I know if a program is suspicious? Well for one, if the program already observes suspicious behavior (such as being unsigned, flagged by anti-virus, doing strange things or you have no idea what it's even for) it should not belong among your startup programs.



Startup Item	Manufacturer	Command	Location	Date Disabled
☑ pximouse	Pixart Imaging ...	TiltWheelMous...	HKLM\SOFTWARE\M...	
☑ NVIDIA Back...	NVIDIA Corpor...	"C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Realtek HD ...	Realtek Semico...	C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Adobe Upda...	Adobe System...	"C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ NVIDIA GeF...	NVIDIA Corpor...	C:\Windows\sy...	HKLM\SOFTWARE\M...	
☑ Google Chrome	Google Inc.	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ Steam Client...	Valve Corporat...	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ Skype	Skype Technol...	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ Google Drive	Google	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ PowerISO Vi...	Power Softwar...	C:\Program Fil...	HKLM\SOFTWARE\...	
☑ Java Platfor...	Oracle Corpora...	"C:\Program Fil...	HKLM\SOFTWARE\...	
☑ Microsoft On...	Microsoft Corp...	C:\PROGRA~1...	C:\Users\toasty\Ap...	

Only a few programs should, two I should mention are any VMWare related items and anything related to CyberPatriot. You should discuss with your team whether a program is considered bad or good.

The next way to view your start-up is by using msconfig.exe. It's one of the programs you can use off of the Run Prompt or by searching through the start menu. Anyway, once you've done so, you'll likely encounter a box like this (not the same results).

Now, from what I have here, I've already ensured that I'm running everything I normally run. You can read the Command and Location columns and what they show to view whether a program is truly harmful or not. Depending on the location of some things, it might provide insight as to whether the program is harmful or not, especially if it does not have a manufacturer or looks generally suspicious.

The use of msconfg is a good suggestion, but ultimately, Autoruns is the most efficient way for viewing your items within the startup. I highly recommend you practice and learn how to use AutoRuns.

The other way you can find them is through the start-up folders. Windows typically has two auto-run folders, one for a specific user and another for all users. This is the typical directory for your start-up folder.

C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Where I put **USERNAME** is where the username SHOULD go, for instance, on my computer my username is toasty, so it would look like this for me.

C:\Users\CYBER\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Anyway, ensure you have to view hidden files and extensions unhidden before you check there. To quickly check a directory, either paste the absolute pathname of it into Windows Explorer or use command-prompt.

To open a directory immediately in command prompt, use the command like this.

```
explorer <directory>
```

Here’s the absolute pathname for the Global Directory. (The directory that affects everyone’s start-up)

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

You can ultimately view your items within the registry to get a full understanding of how to take control of startup. Speaking of the registry, you can control startup from there the best.

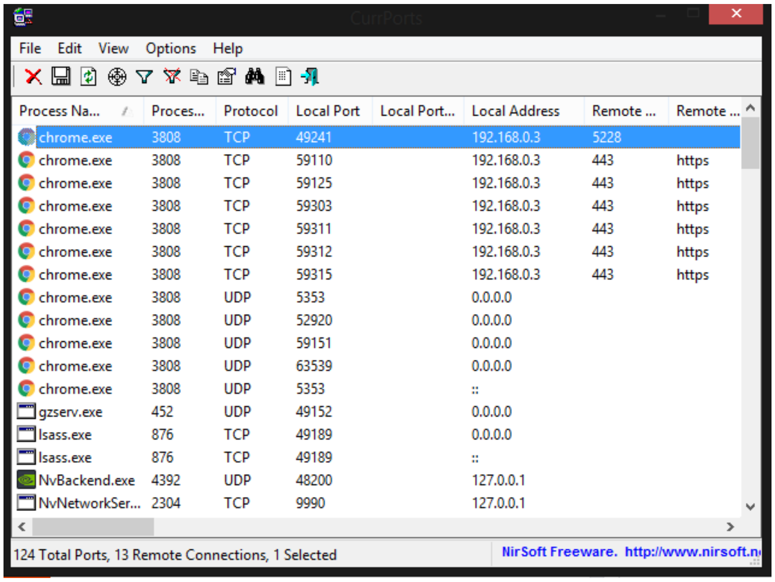
This is the end of this section, in the next section, we’re going to talk about Networking and Protocols.

SECTION 17 – NETWORKING PROTOCOLS

In the previous section, we had gone over networking but we had missed some things that we should have specified or talk about more. I'm talking about my favorite networking tool, Currports and the various internet protocols that exist.

Currports (cports.exe)

CurrPorts is a network monitoring tool that displays connections just like TCPView, however, it has much more functionality and I highly recommend that you use it for most networking things. The reason why I highly recommend it so much is because it gives you so much data to work with along with a very large amount of tools you can use.



Process Na...	Proces...	Protocol	Local Port	Local Port...	Local Address	Remote ...	Remote ...
chrome.exe	3808	TCP	49241		192.168.0.3	5228	
chrome.exe	3808	TCP	59110		192.168.0.3	443	https
chrome.exe	3808	TCP	59125		192.168.0.3	443	https
chrome.exe	3808	TCP	59303		192.168.0.3	443	https
chrome.exe	3808	TCP	59311		192.168.0.3	443	https
chrome.exe	3808	TCP	59312		192.168.0.3	443	https
chrome.exe	3808	TCP	59315		192.168.0.3	443	https
chrome.exe	3808	UDP	5353		0.0.0.0		
chrome.exe	3808	UDP	52920		0.0.0.0		
chrome.exe	3808	UDP	59151		0.0.0.0		
chrome.exe	3808	UDP	63539		0.0.0.0		
chrome.exe	3808	UDP	5353		::		
gzserv.exe	452	UDP	49152		0.0.0.0		
lsass.exe	876	TCP	49189		0.0.0.0		
lsass.exe	876	TCP	49189		::		
NvBackend.exe	4392	UDP	48200		127.0.0.1		
NvNetworkSer...	2304	TCP	9990		127.0.0.1		

124 Total Ports, 13 Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.n

Here is the interface of Currports, if you've noticed, it has a similar interface of other programs we've used, such as TCPview.

We've already talked about most of those features (PID, Local Address, Remote, etc.) but, here are some fantastic things CurrPorts offers in the category of features.

- CurrPorts allows you to close unwanted TCP/UDP connections
- You can kill the process that opened those ports
- CurrPorts automatically highlights suspicious applications with a pink color
- CurrPorts gives you the Remote Address and Remote Host Name
- CurrPorts shows you the state of the connection (established, listening, closed, etc.)
- CurrPorts tells you the process' path
- CurrPorts allows you to create a report in HTML by right-clicking

Common Internet Protocols

Within this section, we're going to talk about all sorts of internet protocol's people use every day, and then some protocols that are not used every day. As a normal person, you never really think about what you're doing when you're on the internet, at least not the technologies that handle everything. Let's cover the specifics on some common protocols, including what they are, how they work, and an example of how they can be attacked if applicable.

DNS (Domain Name Service)

The protocol DNS runs on both TCP and UDP Ports 53. What I'd like to think DNS is is a huge directory full of where websites are, as they're a naming system for resources on the internet. It links up a domain name (let's say, http://google.com) to an IP address, meaning you won't have to remember every IP address, just the names of things.

You'd think that things such as DNS would be safe, but they're not, in fact, some stuff concerning DNS can actually be very harmful.

For example, there's an attack method called Cache Poisoning, which is the corruption of DNS cache data. Now what this means is that data within DNS is changed into something it's not supposed to be, ultimately leading users to a website controlled by an attack, that attacker can then put up a clone (let's say the website was a bank website a user uses) and the person attempts to log in, sending their data. This results in usernames, passwords, emails and credit cards being captured for those who fell for it.

DHCP (Dynamic Host Configuration Protocol)

The protocol DHCP runs on UDP ports 67 and 68. DHCP is a client/server-based protocol that hands out dynamic IP addresses to those who need it along with other important network information. A lot of companies might have their own DHCP server, in fact, many things have DHCP services. When a computer joins a network, the first thing that greets them is DHCP, DHCP will give them an IP address from a pool of currently unused IPs. Now, sometimes, we don't want this to happen. Printers and Servers need an IP address that sticks to this; these are called *static IP addresses*. Dynamic IP addresses are ones that are assigned when someone joins a network, when that person is no longer using the network, they will no longer need their IP address.

A big attack against DHCP is DHCP consumption/starvation attacks. What this type of attack does is it broadcasts many DHCP requests with spoofed MAC addresses to take as many of the available IPs as possible. This can result in something known as a *denial of service* against anyone wanting to access the network. One of the hardest parts is finding who is doing such a thing. This can be prevented with some safeguards provided by some companies such as Cisco, but ultimately, it's a denial of service.

SMTP (Simple Mail Transfer Protocol)

The protocol SMTP uses TCP port 25, sometimes using SMTP + SSL (creating SMTPS, Simple Mail Transfer Protocol Secure) for port 587. SMTP is a protocol used for sending mail from the user to the server along with being Vice Versa until the near end.

One attack that SMTP would fall against would be attempting to verify whether an email address exists or not. This can be done by attempting to communicate with servers. Whether a spammer or attacker, this can be done effectively.

POP/POP3 (Post Office Protocol)

The protocol POP/POP3 runs on port 110. Encrypted communication is requested after communication has been initialized, which changes the protocol to a version of with using Secure Socket Layer (SSL) on port 995. What POP/POP3 is an internet protocol that receives emails from email servers. So SMTP is used to send mail and get mail sent to the mail server while POP/POP3 is used to communicate with the mail server once again, to receive the mail.

Other than spoofing or attempting to intercepts, there aren't any specific attacks.

IMAP (Internet Message Access Protocol)

The protocol IMAP uses port 143 and encrypts it with SSL on port 993. IMAP is a much more advanced method when it comes to accessing your email.

FTP/TFTP/SFTP (File/Trivial/Secure File Transfer Protocol)

The protocol FTP will run actively or passively, on port 21. TFTP runs on port 69 on both UDP and TCP. SFTP runs the same way that SSH runs on, port 22. The thing about all of these protocols is that each of them is used for the exact same thing. Transferring files.

FTP is the very well-known one, allowing clients to receive files. The problem is that there are some problems with the security when it comes to trying to stay open, this FTP is *not* encrypted. SFTP is a much more secure version of FTP, using a higher degree of security. TFTP is a very simple version of FTP, the problem is the amount of care needed to work with TFTP makes it harder to keep secure.

HTTP/HTTPS/SSL (Hypertext Transfer Protocol/Protocol Secure)

The protocol HTTP runs on port 80 and HTTPS runs on port 443. This is a protocol that almost everyone uses every day. HTTP is the under-the-hood protocol used for the internet for how messages work, how they're formatted, the transmission and how servers and browsers will work with everything. There are many things that run off of HTTP to the point where it's become a standard.

It's not that HTTP would be attacked; it's more like people would attempt to break what works with HTTP, such as SQL, PHP, Jquery, Javascript, etc.

The protocol SSL will run on 443. SSL has become a standard to this day for establishing encrypted links between two different clients/servers.

One major attack I can think of is the POODLE attack. POODLE stands for Padding Oracle On Downgraded Legacy Encryption, this attack exploits the internet and security software clients using version SSL 3.0. SSL 3.0 ultimately became replaced TLS 1.0 and beyond to where people now use TLS 1.2 (TLS is the same thing as SSL, but better, it stands for Transport Layer Security)

SSH (Secure Shell)

The protocol SSH runs on port 22. So what is SSH? SSH offers a variety of things, from secure terminal environments to the ability to send and receive files in a secure manner. This is typically used if remote shells are required.

The great part about SSH is the fact that everything is encrypted and if you secure it correctly, the only type of attack you would have to worry about is a potential brute force.

Telnet (Telnet)

This protocol runs on port 23. Telnet is a very old and outdated protocol. It's essentially SSH but without the security. Ultimately, there is no reason to use Telnet and highly advise against it due to the fact that it is unencrypted and sends passwords and whatnot in plain text, which is one of the worst things you can do.

That's all for this section. In the next section, we're doing the unthinkable, we're diving into the Local Security Policies.

SECTION 18 – LOCAL SECURITY POLICY

There comes a time, where one security enthusiast, must take the task of enforcing security policy. I'm not talking about a few items, I'm talking about a whole security policy. Today, we're going to learn about Local Security Policy.

Now that I'm done making it sound dramatic, this lesson isn't necessarily going to be long due to the fact that you're already given a list of security policies.

The only thing about configuring your local security policy is the fact that it takes a while, and for every item you configure, you need to ask yourself if that configuration is right for the system. Many things must be taken into consideration when it comes to a policy, such as, is this a remote system? Should this privilege be given? There's a lot to consider, and the best way to learn is to configure and see what works best. **Here is the most important part, you really need to understand why each setting is set.**

Here is the list. Modify it as you choose, this list is essentially universal with Windows Vista and beyond.

Account Policies – Password Policy

Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	15 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies – Account Lockout Policy

Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Local Policies – Audit Policy (split between non-server and server with the pipe |)

Account logon events	Successes and Failures | Successes and Failures
Account management	Successes and Failures | Successes and Failures
Directory service access	No auditing | Successes and Failures
Logon events	Successes and Failures | Successes and Failures
Object access	No auditing | Successes and Failures
Policy change	Successes and Failures | Successes and Failures
Privilege use	No auditing | Successes and Failures
Process tracking	Successes and Failures | Successes and Failures
System events	Successes and Failures | Successes and Failures

Local Policies - User Rights Assignment

Access Credential Manager as a trusted caller	(blank)
Access this computer from the network	Administrators
Act as part of the operating system	(blank)

Add workstations to domain	Administrators
Adjust memory quotas for a process	Administrators
Allow log on locally	Administrators and Users
Allow log on through remote Desktop Services	(blank)
Back up files and directories	Administrators
Bypass traverse checking	Administrators
Change the system time	Local Service, Administrators
Change the time zone	Local Service, Administrators
Create a pagefile	Administrators
Create a token object	(blank)
Create global object	Local Service, Network Service, Administrators
Create permanent shared objects	(blank)
Create symbolic links	Administrators
Debug programs	(blank)
Deny access to this computer from the network	Guest and Guests
Deny log on as a batch job	Guest and Guests
Deny log on as a service	Guest and Guests
Deny log on locally	Guest and Guests
Deny log on through Remote Desktop Services	Guest, Guests, and Everybody
Enable computer and user accounts to be trusted for delegation	(blank)
Force shutdown from a remote system	(blank)
Generate security audits	LOCAL SERVICE, NETWORK SERVICE, Administrators
Impersonate a client after authentication	LOCAL SERVICE, NETWORK SERVICE, Administrators
Increase a process working set	Administrator(THE BUILD-IN ADMIN)
Increase scheduling priority	Administrators
Lock and unload device drivers	Administrators
Lock pages in memory	(blank)
Log on as a batch job	(blank)
Log on as a service	(blank)
Manage auditing and security log	Administrators
Modify an object label	(blank)
Modify firmware environmental values	Administrators
Preform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE, Administrators
Restore files and directories	Administrators
Shut down the system	Administrators, Users
Synchronize directory service data	(blank)
Take ownership of files or other objects	Administrators

Local Policies – Security Options

Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can’t add or Sign in with Microsoft Accounts

Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	You can decide the name of the Administrator Account
Accounts: Rename guest account	You can decide the name of the Guest Account
Audits: Audit the access of global system objects	Disabled
Audits: Audit the use of Backup and Restore privilege	Disabled
Audits: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Disabled
Audits: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	(blank)
DCOM: Machine Launch Restrictions in Security Descriptor Language (SDDL) syntax	(blank)
Devices: Allow undocks without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on users only	Enabled
Devices: Restrict floppy access to locally logged-on users only	Disabled
Domain controller: Allow server operator to schedule tasks	Disabled
Domain controller: LDAP server signing requirements	Require Signature
Domain controller: Refuse machine account password changes	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	90
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when session is locked	User Display Name Only
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	5
Interactive logon: Machine inactivity limit	300 seconds
Interactive logon: Message text for users attempting to log on	This computer is for authorized use only!

Interactive logon: Message title for users attempting to log on	WARNING!
Interactive logon: Number of previous logons to cache (in case domain control is not available)	2 or less
Interactive logon: Prompt user to change password before expiration	14 days or more
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	Do Nothing
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted passwords to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending	15 Minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Default
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnects clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Accept if provided by the client
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Name Pipes that can be accessed anonymously	(blank)
Network access: Remotely accessible registry paths	(blank if standalone) if not standalone, then. System\CurrentControlSet\Control\ProductionOptions
Network access: Remotely accessible registry paths and sub-paths	(blank if standalone) if not standalone, then. System\CurrentControlSet\Control\Print\Printers
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	(blank)

Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
Network security: Allow Local System to use computer identify for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Allow PKU2U authentication requests to this computer to use online identities	Disabled
Network security: Configure encryption types allowed for Kerberos	Enable RC4HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1 and Future Encryption Types
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Sent NTLMv2 response only. Refuse LM and NTLM.
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security and 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security and 128-bit encryption
Network security: Restrict NTLM: Add remote servers exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for all accounts
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Enable all
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Enabled
System cryptography: Force strong key protection for user keys stored on this computer	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Require case insensitivity for non-Windows subsystem	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	

System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Enabled
User Account Control: Admin Approval Mode for the Built-In Administrator account	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure location	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry writes failures	Enabled

Windows Firewall with Advanced Security – Firewall State (**Note, these particular settings are all the same, which means these apply to Domain Profile, Private Profile and Public Profile in Local Security Policies)**

Firewall State	On (recommended)
Inbound connections	Block (default)
Outbound connections	Allow (default)

Windows Firewall with Advanced Security – Settings

Display a notification	Yes
Allow unicast response	No
Apply local firewall rules	Yes
Apply local connections security rules	Yes

Windows Firewall with Advanced Security – Logging

Name	Specified
Size limits	16384
Log dropped packets	Yes
Log successful connections	Yes

Advanced Audit Policies – Local Group Policy Object – Account Logon (Note: All audit policies may vary)

Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	No Auditing
Audit Kerberos Service Ticket Operations	No Auditing
Audit Other Account Logon Events	No Auditing

Advanced Audit Policies – Local Group Policy Object – Account Management

Audit Application Group Management	No Auditing
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	No Auditing
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

Advanced Audit Policies – Local Group Policy Object – Detailed Tracking

Audit DPAPI Activity	No Auditing
Audit Process Creation	Success
Audit Process Termination	No Auditing
Audit RPC Events	No Auditing

Advanced Audit Policies – Local Group Policy Object – DS Access

Audit Detailed Directory Service Replication	No Auditing
Audit Directory Service Access	No Auditing
Audit Directory Service Changes	No Auditing
Audit Directory Service Replication	No Auditing

Advanced Audit Policies – Local Group Policy Object – Logon/Logoff

Audit Account Lockout	Failure
Audit IPsec Extended Mode	No Auditing
Audit IPsec Main Mode	No Auditing
Audit IPsec Quick Mode	No Auditing
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	No Auditing
Audit Other Logon/Logoff Events	No Auditing
Audit Special Logon	Success

Advanced Audit Policies – Local Group Policy Object – Object Access

Audit Application Generated	No Auditing
Audit Certification Service	No Auditing
Audit Detailed File Share	No Auditing
Audit File Share	No Auditing
Audit File System	Failure
Audit Filtering Platform Connection	No Auditing
Audit Filtering Platform Packet Drop	No Auditing
Audit Handle Manipulation	No Auditing
Audit Kernel Object	Failure
Audit Other Object Access Events	No Auditing
Audit Registry	Failure

Audit SAM	Failure

Advanced Audit Policies – Local Group Policy Object – Policy Change

Audit Audit Policy Changes	Success and Failure
Audit Authentication Policy Changes	Success
Audit Authorization Policy Changes	Success
Audit Filtering Platform Policy Change	No Auditing
Audit MPSSVC Rule-Level Policy Change	No Auditing
Audit Other Policy Change Events	Success and Failure

Advanced Audit Policies – Local Group Policy Object – Privilege Use

Audit Non Sensitive Privilege Use	Failures
Audit Other Privilege Use Events	No Auditing
Audit Sensitive Privilege Use	Success and Failure

Advanced Audit Policies – Local Group Policy Object – System

Audit IPsec Driver	Success and Failure
Audit Other System Events	No Auditing
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure

Advanced Audit Policies – Local Group Policy Object – Global Object Access Auditing

Audit File System	Success and Failure
Audit Registry	Success and Failure

I would have explained each and every part of these settings, however, due to the complexity and need for greater explanation, I would much rather you investigate these by yourself, as you will gain a better understanding.

This is the end of this section, however, in the next section; we're going to be learning about the things that make Windows 8/8.1 and 2008 Server different from Windows 2008 Server.

SECTION 19 – WINDOWS 8/8.1 AND WINDOWS 2008 SERVER FEATURES

Now, I mostly worked with Windows 7 in this book, but that doesn't mean you'll only be working with Windows 7. During the competition, you may encounter operating systems such as Windows 8, 8.1 and Windows 2008 Server. The interfaces might be different, but in no way should you be discouraged. To take things head on is the way I will prepare you. For now, we're going to talk about these particular operating systems and whatever makes them different from Windows 7.

The first topic we're going to discuss is Windows 2008 Server. First of all, what is a server? A server is a device that serves clients and processes requests for clients. This is called the client-server model. This is how things have been working for the longest time, and it will probably stick to this.

This means that a server needs to be far more secure than your average client. There are some particular things that I had not covered in the past; this will be my time to discuss them. When you first begin Windows 2008 Server, you might notice that it looks far more different than it should, and by different, I mean older.

Windows 2008 Server does not run off of a modern GUI, it runs and tries to consume the least amount of resources possible. There's a particular client that it takes advantage of to get some basic tasks finished, it's the Windows Configuration Panel, also known as Initial Configuration Tasks, and what I like to call it, **OOBE**.

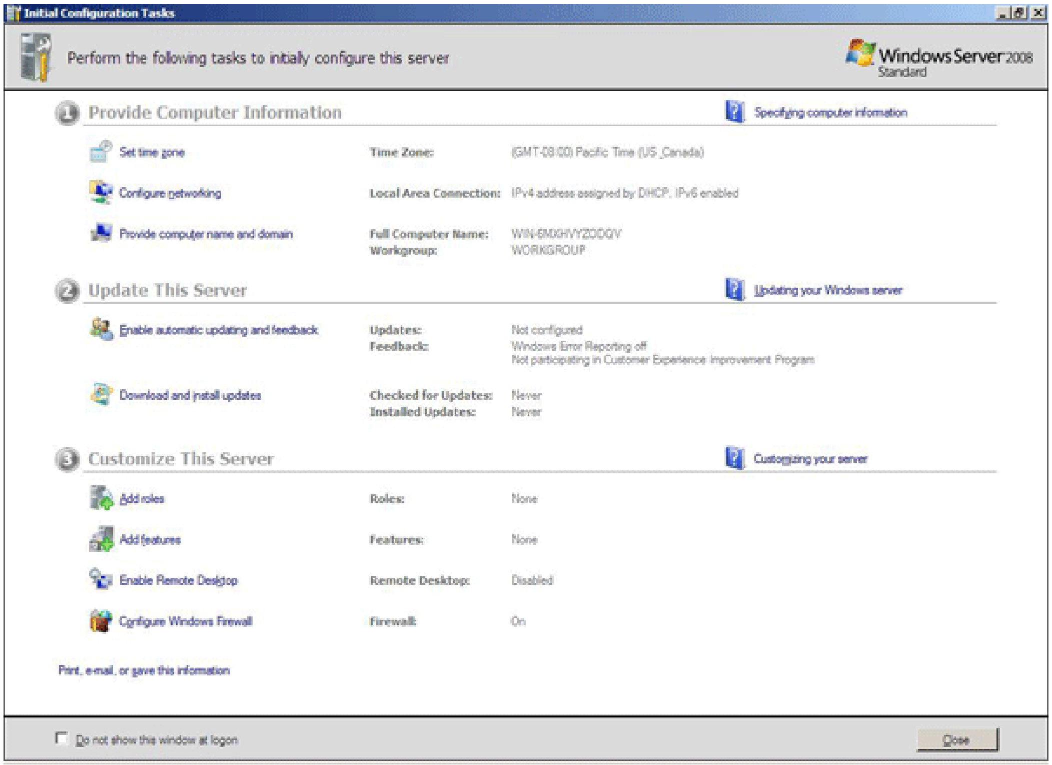
You can run OOBE by doing Windows Button + R, and type "oobe" into the run prompt. From there, this should pop up. Now, there are various tasks that you can do with OOBE, the first one being setting the time. Don't set the time.

The next thing is configuring networking, The only thing you might possibly be able to configure here is IPv6. Having IPv6 on when it's not required may pose as a security risk, so as a result, it should be turned off.

The next thing you can do is enable automatic updating on the machine. *In real world application, installing updates manually might not be the smartest idea.* Nevertheless, this is an important step as it can potentially earn you points. Downloading and installing updates is also an important topic¸ **but before you download updates**, wait until we get to the next page.

Along with those things, you should configure remote desktop and Windows Firewall to a correct configuration; refer to chapters relating to those items for more information.

I had not touched this subject until now, but there are packs that you can get for your items (such as Windows 7 or Windows 2008 Server) that can install a majority of the updates you need. They're



Initial Configuration Tasks

Perform the following tasks to initially configure this server

Windows Server 2008 Standard

1 Provide Computer Information — Specifying computer information

Set time zone — Time Zone: (GMT-08:00) Pacific Time (US Canada)

Configure networking — Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled

Provide computer name and domain — Full Computer Name: WIN-6MXHVYZODQV; Workgroup: WORKGROUP

2 Update This Server — Updating your Windows server

Enable automatic updating and feedback — Updates: Not configured; Feedback: Windows Error Reporting off, Not participating in Customer Experience Improvement Program

Download and install updates — Checked for Updates: Never; Installed Updates: Never

3 Customize This Server — Customizing your server

Add roles — Roles: None

Add features — Features: None

Enable Remote Desktop — Remote Desktop: Disabled

Configure Windows Firewall — Firewall: On

Print, e-mail, or save this information

☐ Do not show this window at logon

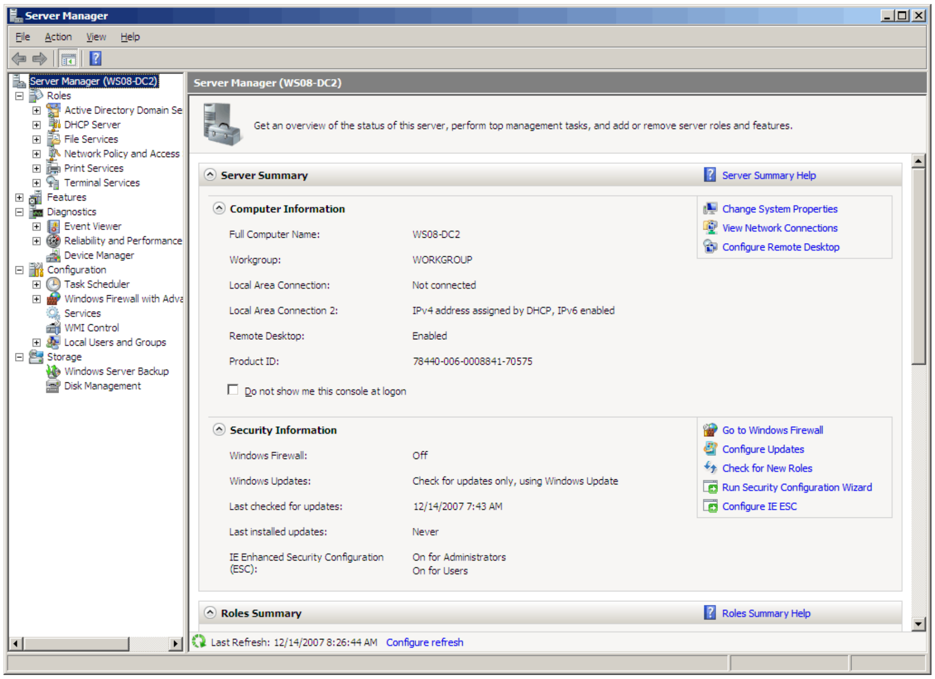
Close

called **Service Packs**. Simply google them and find them on Microsoft's Website to download and install them, OR, ask someone if he/she has them on a USB so that you can get it from there. You can once again do this for Windows *Vista, Windows 7 and Windows 2008 Server.*

There is another feature that is Windows 2008 Server exclusive, it's called **IE ESC**. It stands for **Internet Explorer Enhanced Security Configuration**. The problem with it is the fact that it's a pain for most people, but if security policy demands it, turn it on when no longer need to browse the internet when you're done configuring the server.

To be able to turn it on/off, go to Server Manager → Security Information → Configure IE ESC.

I may as well introduce Server Manager. Server Manager Is a tool you might be working on as a base.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Computer Information

Full Computer Name:	WS08-DC2
Workgroup:	WORKGROUP
Local Area Connection:	Not connected
Local Area Connection 2:	IPv4 address assigned by DHCP, IPv6 enabled
Remote Desktop:	Enabled
Product ID:	78440-006-0008841-70575

□ Do not show me this console at logon

Security Information

Windows Firewall:	Off
Windows Updates:	Check for updates only, using Windows Update
Last checked for updates:	12/14/2007 7:43 AM
Last installed updates:	Never
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users

Last Refresh: 12/14/2007 8:26:44 AM

This is what you'll be using to configure your server *sometimes*. Why I say sometimes is because there aren't too many things that you need to configure here. When you do need to do something, you'll know when to run it through here.

The next feature is available on all systems of Windows, specifically the professional versions of Windows 7, 8, 8.1 or Windows 2008 Server SP2.

BitLocker is a program used to protect data with a strong encryption to prevent the intrusion of protected data.

To access BitLocker, it's likely to be located within System and Security → BitLocker Drive Encryption. It may be required for you to encrypt your operating system, but it may also not. ***Just don't lose your master password.***

You also have the ability to back up your system, that features being on System and Security, but that's up to you.

The next feature is *partially* Windows 8/8.1 exclusive feature, it can still be configured on Windows 7 and below if the version of Internet Explorer is up-to-date. Microsoft SmartScreen is a feature in Internet Explorer that prevents malicious software, actions, etc. I never use Microsoft Internet Explorer, but other people might, so enforcing this setting is one of the things you'll need to do.

To start, go to control panel and click System and Security → Security and Maintenance → Change Windows SmartScreen and set it to the highest setting. Normally, I would not like this, but every bit of security is required.

Also, you can configure Microsoft Smart Screen by opening Microsoft Internet Explorer, going to the settings (at the right), clicking the gear Icon, going to safety, and clicking the option Turn on SmartScreen Filter…

Now, I'm going to talk more about server configuration.

What is Server Configuration?

I'd like to say that server configuration is one of the most difficult things to master, simply because it requires you to think deep about what you are "configuring" and choosing to toy with the settings until you've got a good set up going. But what is a good set up? What is considered secure?

I've taught you that secure is, good passwords, encryption, no leaked passwords, and stopping your server from getting attacked. The only problem is that you may want to clarify, what am I getting attacked by? Who is doing this? Why are they doing it? The most important thing you need to understand is that **nothing is 100% secure.**

Nothing. Not even the biggest data centers have protocol to stop everything. What needs to be done is the **mitigation of risk**. Mitigation is the process of handling a threat and stopping it in its tracks. With every valuable **asset**, such as customer data, payment information, etc. comes the thought that someone will want to steal it or damage it because it is valuable.

So we know what we're protecting, data, assets, etc. This stuff is very important. This is why people are committing crimes to take it. How do we stop this from happening? We harden servers. **Hardening** is the process of locking down every possible setting to the highest level of security while maintaining balance. What balance? The midway point between secure and usable. If you want security, you'll have to give up convenience, if you want convenience, you'll have to give up security.

Securing the Application

Everything must have some sort of setting you can configure. For example, FileZilla, the FTP server, may have some configurable settings such as **Autoban or FTP with SSL**. To understand how to configure these things, you need to keep in mind what exactly is usable by the people. From there, you need to establish a security policy that covers this:

1. What is being accessed?
2. Who is accessing what?
3. How are they accessing it?
4. How can it be abused?
5. What can I do to stop them?

These questions are relatively important. First of all, let's talk about **what is being accessed**. First and foremost, what is FileZilla? FileZilla is an FTP server. FTP is File-Transfer Protocol, it is used to transfer files from one place to another. This means that ordinary users will be accessing these files.

Next, **who is accessing what**? In the event that you want to limit who gets what, this question is very important. You may only want to limit the access to these files to certain people. FileZilla does allow you to configure who gets what. So in the event that only specific users should be accessing the files, you will need to ensure that only the right users will have access, no one more, no one less.

How are they accessing it is the next question. This one is very important. Let's assume that this FTP server is used to transfer extremely confidential files. FTP by default does not encrypt files for transmission, this means that in the event that anyone is transferring these files, and someone is listening over the wire with a **man-in-the-middle attack** (A man-in-the-middle attack is when someone intercepts a connection to take or modify files in transmission.)

The integrity of that file is void or it may have been stolen. In this case, you may need to implement encryption, likely **SSL**, or, **Secure Socket Layer**. Whenever you are using an application that requires a secure connection (encrypted), it will likely use SSL. For example, **HTTPS**, or, **Hyper Text Transfer Protocol Secure**, uses SSL to keep connections secure. Now, if we wanted to keep things secure, we would find a way to implement SSL into our system.

The question remains as to what we're protecting our assets from, or simply, **how can these applications be abused**? Imagine on our system where we allowed as many access attempts as people want. This can be very troublesome. For example, a **DDoS** attack, or, **Distributed Denial of Service**, is where many connections are coming at a system at the same time, preventing legitimate users from getting their requests fulfilled. To stop this, you can implement a system that will ban certain IP addresses after too many attempts.

This type of system is similar to any other security system, where too many attempts can result in a timed lockout of some sort. Of course, this is not the only vulnerability to look out for. When working with systems, you will need to do research and see what types of attacks your system could suffer from. This is where you find a way to mitigate the risk. For example, FireZilla's autoban is a way to mitigate the risk. SSL is a way to mitigate the risk. You may also implement auditing, or, logging, to ensure that any attacks will be recorded for future evidence and assistance in the event where digital forensics is a subject.

What it comes down to is understanding that your system can be broken into and how can you stop the attack? What measures will slow it down or ease damage? This is what you need to ask yourself if you want to know **what you can do to stop the attackers.**

In our analysis, we can answer the previous questions with little examples like so:

1. What is being accessed? Assets and data.
2. Who is accessing what? Either a certain amount of users or everyone, depends on scenario.
3. How are they accessing it? Through FTP.
4. How can it be abused or attacked? Exploiting current vulnerabilities and trying to gain data.
5. What can I do to stop them? Implementing SSL, Autoban, using logging, hardening server, encryption, etc.

The biggest thing to understand is that you need to minimize the risk of what you are protecting. You will need to minimize your attack surface and give attackers little to nothing to worth with. There is a lot to this stuff that can be done, you simply need to do your research and find the best methods.

SECTION 20 – MISCELLANEOUS SECURITY FEATURES

There are some particular items that I couldn't exactly categorize or just wanted to hold until the end as extras, I'll just talk about them and tell you can do so.

Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer is a tool released by Microsoft. This program has been around for quite a while and is used to analyze a system for missing security updates and common security misconfigurations! It's not hard to run this program either, simply search it up, download it, and we'll show you how to run it.

Now, remember to run MBSA as an Administrator. The first thing you ensure is that you've checked all the potential settings that you'll need and then review the report when you're done. Ensure that you're scanning the local computer and not anything else. Also, you can't really scan anything outside of your computer, so either use the address 127.0.0.1 or just select the Local Computer options.

Really, it isn't a hard program to use, just use it to see where you stand for a secure computer!

To find Microsoft Baseline Security Analyzer, google MBSA and install the tool or ask your

Screensaver Lock

In the modern world, a lot of people leave their computers open. It can't be helped, but, some people may take advantage of it, from changing the wallpaper to leaving a minimizing script inside of someone's start-up folder, having your computer open to people is not good.

This is where a screensaver lock comes in. When your computer is inactive for a certain amount of time, your computer will lock out and you will be unable to access it.

Now, for this, we're going to introduce a brand new item I really should have to introduce completely, the Local Group Policy Editor. How we're going to enforce our setting is by using this. To start, hit the Windows button or the start menu button and type "edit group policy". This will open the group policy for you to edit. Now! Follow the path I type out!

User Configuration > Administrative Templates > Control Panel > Personalization > Password protect the screen saver and screen saver timeout.

For Password protect the screen saver, you need to enable this setting. This will make it so that when someone resumes the computer after it timed out, they will require a password.

The second setting, Screen saver timeout, will be configured for 600 seconds, or, 10 minutes.

This means after 10 minutes of inactivity, the computer will lock out and require a password to resume. This is a good policy, even if it may be considered annoying. Never leave your computer unattended.

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

You’ve reached the end of the manual!

It’s a lot of reading you just did, but I can only hope that you truly learned something from this. It brought me a lot of joy writing this for those who have a hope to learn, and hopefully, you learned a lot and hope to continue your education.

If you are a mentor/teacher, try researching these topics more in-depth to help answer any questions your students might have! I wish you the best of luck!

This book is v1.0.