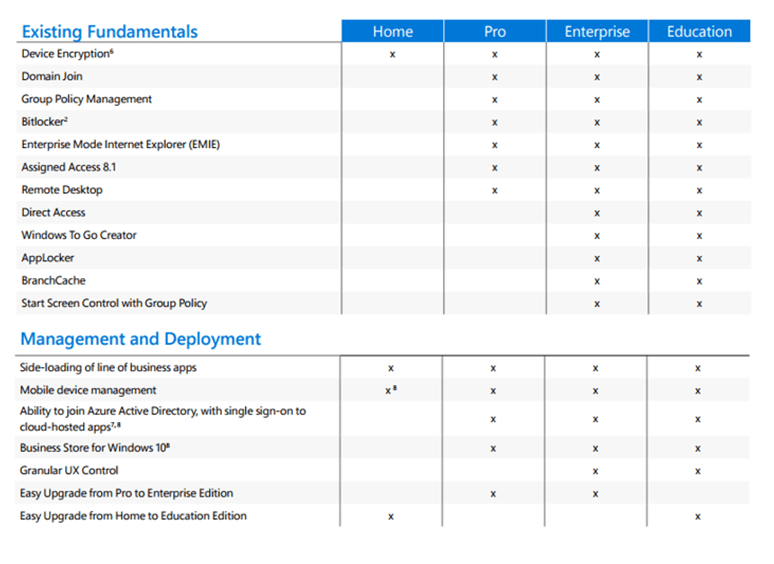
Section1: Operating System

# Microsoft Windows:



# Windows Commands:

* The Windows command prompt allows you access to the operating system through what we call **a CLI– a Command Line Interface**. **This brings up a window**. And you can type commands in in that window to interact with the operating system.
* **run by anybody with standard privileges**. These are the privileges associated with any user who might be logged into your network. This works for almost all commands that the users might use, **but if you need additional rights and permissions, you can use an elevated prompt, or an administrative prompt**.
* This means that you’ll need to be part of the administrators group. And when you start the command prompt, you’ll need to choose the option to run as administrator. You can also type **the command cmd**, which stands for the command prompt, and type **in Control+Shift+Enter to automatically launch the command prompt in administrative mode.**

## Commands:

1. Help:

* The help command can be used to give you more details about any of the other commands you might use at the command prompt.
* **Help copy,help dir,help chkdsk**.
* You can also use the command with a /? at the end, which provides you with the same help text that you see when you use the help command.
* Copy /?

1. If we were to clear this screen– I’m going to type **cls** to clear the screen.
2. Dir:

* If you’d like to see all of the files available in a particular folder, **you can use dir, which stands for directory list**, to be able to list all of the files and directories in the current folder.

1. **cd command**, **or chdir, to be able to change or move** to a different directory on that system. You would use **the backslash to be able to delineate** between different folders in that hierarchy on your drive.
2. **Cd ..** use **two dots**, or two periods to specify the folder that’s just above the folder where you happen to be working.
3. **create or remove folders** from the command line using **the mkdir, or rmdir** commands. We very often abbreviate these when we’re typing **to md for the mkdir**, and the **rd command for the rmdir.**
4. **hostname** that will put the name of the computer at the command prompt.
5. **Format:** The process of installing that file system or configuring a file system in that partition can be done in Windows using **the format command**.
6. **Copy (/v,/y):** you can copy files at the command prompt using the **copy command**. **/v. It will verify that the file that you’ve copied is identical to the original source. /y, you can tell Windows to skip over any prompts where it might be asking you whether you would really like to copy this file or not. Example copy /v.** The syntax of the copy command **uses copy**, the **name of the source fil**e, and **then the destination** where you would like to copy that file
7. **Robocopy:** This stands for robust copy. And it’s designed to be a better version of xcopy.
8. **Shotdown:** he name implies, will shut down the system.**shutdown /s /t nn**, **shutdown /r /t nn**,**shutdown /a**.
9. **Diskpart.**
10. **Winver:**
11. **gpresult** to see what the current configuration is for Group Policy on that particular device.
12. **gpresult/r**. This will compile all of the information about the current Active Directory configuration and show you all the group policy settings.
13. **gpupdat**e, or forcing a group policy update. When an administrator creates a group policy that changes the configuration of one or many remote devices, you usually require that user to log out of Windows and log back in for that change to take place. But gpupdate command can allow the user to perform that update without having to cycle through the login process.

# Networking Commands:

1. **ipconfig:**
2. **ping ip address**
3. **netstat: -a,-b,-n**: Netstat stands for network statistics, and it’s a utility that’s available in Windows, Linux, Mac OS, and other operating systems.
4. **Nslookup:**
5. **Net:**
6. **Net view /<servername>,net user username:** can tell you information about what shares might be available on a remote server by **using net view, backslash, backslash, and the name of the server**. If you wanted to map a drive to that share, you would use **net use**, you would specify a drive letter, and then specify the server name, and the name of the share. And if you’d like to be able to view the users that are configured on a particular device and make changes to the user account, you can use the user command.
7. **Tracert:** **Traceroute** uses the ICMP protocol to compile this information, and it takes advantage of a **Time To Live Exceeded message** that is able to provide us with more information about what routers might be along the way. This uses a mechanism with an IP **called TTL, or Time To Live**, and although time is in the name, this is really referring to the number of hops, or routers, that we use to get to that device. It’s not referring to the time of day, such as seconds or minutes.
8. **Pathping.**

# The Windows OS:

## Task Manager

* The Windows Task Manager allows you to view real time information about the performance of your operating system. You can view CPU utilization, memory usage, disk utilization, and many other statistics. There are a number of different ways to start Task Manager. You could hit **Control-Alt-Delete**, and choose the option for Task Manager. **You could right mouse click in the taskbar of Windows and select Task Manager.** Or you could use my favorite shortcut, which is **Control-Shift-escape** which immediately launches Task Manager.

## The Microsoft Management Console:

* you can of course **search** through Windows for the **Microsoft Management Console** or simply start **mmc.exe.** This will bring up this empty window where no utilities will be listed. It’s up to you to **then add the different screens** that you would like to see within this console, and if you populate the console, you can have all of these different utilities all running in the same user interface.
* So instead of **launching a lot of different tools**, you can create a customized version of the Management Console that contains just the tools that you need to use for your job.  Let’s go to **our search and type in mmc,** and this will bring up an mmc run command.

## Event Viewer:

* This is centralized logging for the Windows operating system, and it contains extensive information about your system, applications, and the overall running of your OS. This provides information across categories for applications, security, set up, and system.
* And within those different categories, you have different levels for each event**. The event might be information, warning, error, critical, successful audit, or failure audit**. This allows you to begin searching through the logs to find specific information about the operation of the operating system itself or a specific application. If you’d like to run this on its own outside of the Management Console, you can simply run **eventvwr.msc.**

Disk management utility:

* you can run this separately by **running diskmgmt.msc**. One thing to keep in mind when using this utility, is you can make dramatic changes to the configurations of your storage systems, and it is very easy to delete information. Make sure you know exactly what you’re doing when you’re making changes inside of disk management, and be sure to have a good backup on hand in case something does go wrong.

## Device Manager:

* If you’ve ever had to install a new piece of hardware or install an updated driver to an existing piece of hardware, then you’ve probably used device manager. Device manager is the front end that allows you to add hardware and device managers into the operating system. The device drivers themselves have been specifically written for the operating system that you’re using.
* You can run device manager as a snap-in inside of the Microsoft Management Console, or you can run it separately **as devmgmt.msc**.

## Local User and Groups:

* If you’re managing a number of Windows systems, then you’re also probably managing a number of users and groups on those Windows systems. **The users, of course, are the people that are logging into Windows and using the operating system**. This might be individual accounts that have been created for someone’s name, or it could be accounts that are already available in Windows, **such as the administrator account or the guest account**.
* **The administrator account is the Windows super user.** If you are the administrator, or you are part of the administrator group, then you have full access to the operating system. If you’re logging in as a guest to the operating system, then you have very limited access to the OS. And in most modern versions of Windows, this guest account is automatically disabled. And of course, if you’re logging in with your first name, or last name, or some combination of those two, then you’re probably running as a regular user, which is not an administrator or a guest, but has rights and permissions that are assigned by the administrator on that system.
* If you’d like to run the local users and groups utility outside of the Management Console, then you can **run lusrmgr.msc**.

## Performance Monitor:

* you might want to use the Windows performance monitor or **run perfmon.msc**. Performance monitor can provide you information about how the operating system is running, so you can view disk access, memory usage, CPU utilization, and much more

## Group Policy Editor:

* you’re probably using active directory as a central database to store information about users and devices on your network. **You can manage those users and devices through the use of the group policy editor,** which can be used as a snap-in inside of the Management Console or run separately on its own. **This allows you to set security policies, software restrictions, application control, and almost any other aspect of the Windows operating system.**
* If you’re not running active directory, and you’d like to configure these policies for your local device, you can run the local group policy editor, or **gpedit.msc**. But if you’re in a company where you’ll be managing and setting policies for everyone on the network, you can use the group policy management console or **gpmc.msc.**

## System information:

* Windows includes a utility that can provide you with some of these details in System Information. If you want to run this at the command line, it would be **msinfo32.exe.**

## Resources Monitor:

* This can provide details of CPU, disk, network, and memory, and detailed statistics about each one of those different categories. You can also run this at the command line by running **resmon.exe.**

## System configuration utility:

* You can boot your system into a Safe Mode. You could have a log created during the boot process that may be useful for troubleshooting later, and you might change these settings to be permanent so that it always boots with these particular parameters. If you’d like to try some of these settings, they’re available in system configuration or from the command line at **msconfig.exe.**

# Windows Networking

## Proxy setting:

* Some organizations use a proxy as a security tool to separate users from the internet. This proxy configuration can sometimes be transparent, where the users don’t need to configure anything on their system. But if the proxy is not a transparent proxy, you’ll have to make changes to the operating system so that it can properly communicate to the internet.
* You’ll find these proxy settings under the settings app, under network and internet. You can also find it in the control panel under internet options, connections, and LAN settings. Under these proxy settings you can enable or disable the automatic detection of the proxy. And if you’d like to manually configure the proxy, you can also make those changes as well.

# File System:

* if you’re using Windows, you may have a file system that’s been formatted with NTFS or FAT32. Or if you’re installing Linux or Mac OS, there may be file systems that are optimized for that particular operating system.

## FAT file system:

* One of the very first file systems that we **used in the PC world is the FAT file system**. This is the File Allocation table. The most recent version of **the File Allocation Table system is FAT32**. This version **of FAT supports 2 terabyte** volume sizes and a **maximum file size of 4 gigabytes**. If **you’re using a flash drive with Windows, then you’re probably using the exFAT or extended File Allocation Table file system**. ExFAT can support larger files.
* So if you’re using FAT32 and you’re running into some of those file size limitations, you can instead format with exFAT and save files that are larger than 4 gigabytes. ExFAT is also supported across multiple operating systems, so you can store information from a Windows computer onto an exFAT formatted flash drive and use that flash drive on other operating systems, such as Mac OS or Linux.

## NTFS

* If you’re configuring a partition for Windows, then you’re probably **formatting it with NTFS, or what’s called the NT file system.** This file system supports many capabilities that you don’t find in FAT32 such as quotas, file compression built into the file system, encryption, large file support, and much more. **NTFS is considered to be a Windows-centric file syste**m. But you might find other operating systems that are at least able to read or in some ways have a limited write function to an NTFS partition. You have to check with the documentation of your operating system to see what options might be available if you’re trying to access data on an NTFS partition.

## ext3

* If you’re running Linux, you may find that your partition has been formatted with ext3. This is the third extended file system, and this is almost exclusive to a Unix or Linux operating system. There’s a newer version of ext3 called ex4. This is the fourth extended file system, and this is one that we commonly see today in Linux and Android operating systems.

## APFS

* if you’re running Mac OS, iOS, or iPadOS, you may be using the Apple File System, or APFS. This file system has been optimized for solid state drives and includes features such as encryption, snapshots, data integrity, and of course works across all of the different Apple hardware.

# Installing OS

## PXE

* Of course, in an enterprise where you have hundreds or thousands of computers that need to have operating systems installed, you would probably have a remote method of performing this installation. One common way to do this is through PXE.
* This PXE stands for pre-boot execution environment, where you can install this operating system across the network. With PXE, you would configure a centralized server on your network that has all of the operating system installation files. You would then boot your computer into this PXE, or PXE, mode, and it would search across the network to find that server and begin the installation process.

## GPT is short for GUID partition table

* If you’re installing an operating system these days, you’re installing a partition called a GPT partition style. GPT is short for GUID partition table. That **GUID is also an abbreviation that stands for globally unique identifier.**
* When you create this partition, it assigns it with a unique identifier that no other partition has in the world, which is why we call it a globally unique identifier.
* If you have a UEFI BIOS, then you can install this GPT partition style.
* On a single physical drive, you can have up to 128 GPT partitions. the GPT partition style, all partitions are equal, and you can have up to 128 of those GPT partitions. he **maximum size is over 9 billion terabytes**, and in Windows, the maximum partition size is currently set to 256 terabytes.
* You can see why having a GPT partition style gives you so much more flexibility because with GPT, you can create 128 partitions and then boot from any of those GPT partitions.

## MBR partition stands for master boot record

* This is a partition style that you’ll find a much older operating systems. For example, an MBR partition has a limitation of only **two terabytes as a maximum partition size**. And given the large size of drives that we have today, a **two-terabyte partition is very limiting**.
* MBR partition drives **have two different kinds of partitions that you might configure. One is a primary partition.** Only primary partitions on an MBR drive are bootable. So if you’re installing an operating system that you need to boot from, it needs to be located in a primary partition. You can only have a maximum of four primary partitions on an MBR partition style drive.
* Remember that **an MBR drive can only support four partitions**, but if you’re using **a GPT-formatted drive, you can have up to 128 partitions**. The process of creating or removing a partition will delete data from your system. So if there’s any data on this computer now, make sure you have a backup before making any changes to the partitions. The partition process occurs during the Window set up during this dialog box that asks where do you want to install Windows.

# Wireless Encryption:

* Our wireless network communication commonly includes a message integrity check, or MIC, to ensure that all of the data is sent across the network without any changes.
* The root challenge, of course, is that anything we send over this wireless network is going into the air and anyone nearby is able to listen in on the signal and potentially grab information that we’re sending between stations. The obvious solution then is to encrypt all of this data that’s being sent over the wireless network so that if someone does grab these packets they wouldn’t recognize any of the data that’s inside.
* On today’s wireless networks, we tend to use one of two different types of wireless encryption either WPA2 or WPA3.

## WPA2:

* We introduced **Wi-Fi Protected Access version 2 in 2004**. We often abbreviate this as WPA2. WPA2 uses what’s known as a block cipher mode, which means it takes a block of data and encrypts all of that data and it sends the entire block across the network to the other side. **WPA2 uses a block cipher mode called CCMP.**
* **The full name of this is actually counter mode with Cipher Block Chaining message authentication code protocol or counter CBC Mac protocol.** All you really need to remember is that this is the CCMP block cipher mode it provides data confidentiality using APIs for encryption and it adds a message integrity check that uses CBC-MAC to provide that verification.

## WPA3:

* This was introduced in 2018 and it introduced a new type of block cipher mode called **GCMP**. **This is called Galois/Counter Mode Protocol and it’s a stronger and more powerful encryption than WPA2**.
* Similar to WPA2, we **are still using AES** for the encryption and the message **integrity check is now using the Galois message authentication code or GMAC**. If you’re using wireless networks at work, you’re probably not all sharing the **same pre-shared key or PSK. I**nstead, you’re using a separate username and password to log in with 802.1X authentication. But at home, we often use shared pass phrases and there may be times in your office where shared pass phrases makes more sense than having 802.1X.
* We knew that we would need to change this process to remove any possibility of an attacker gaining access to the hash and performing a brute force attack. **To provide this additional security, WPA3 uses a completely different method for authenticating with pre-shared keys**. This uses a mutual authentication method. So not only does the access point know that you’re the proper user for this network with a pre-shared key, but you know that you’re talking to the correct access point.
* We’re now able to create session keys for our wireless networks without actually sending any of the key information across the network. This means we don’t have any four way handshakes, there’s no hash going across the network. Therefore, nobody can capture the hash and there’s no brute force attacks. **This new method of authenticating with pre-shared keys is called SAE or the Simultaneous Authentication of Equals.**

## RADIUS

* One of these protocols that’s used to communicate to an authentication server is called RADIUS.
* RADIUS is an abbreviation for remote authentication dial in user service. And although it references dial in the name of the protocol, this is used on almost any type of network connection. You’ll sometimes hear the authentication server referred to as a AAA server that stands for authentication, authorization, and accounting. So whenever we refer to a protocol that communicates to the authentication server, we are referring to a AAA protocol.
* Without having some type of centralized authentication on the network, you would have to manage authentication on all of these separate devices. So you would have to manage authentication on your VPN server, a file server, a web server, and so on. Instead, you can have one central authentication source, such as a RADIUS server, and send all of your authentication requests to that server for approval.
* If, it’s not obvious by having the word dial in the name RADIUS has been around for a very long time. And because of that, it has a great deal of support in the industry. There are many devices and many operating systems that can support RADIUS communication. And you’ll find that many of the VPN servers and other devices that you’re connecting on your network do have an option to provide authentication via RADIUS.

## TACACS:

* RADIUS is not the only way to provide authentication to a AAA server. One very common protocol is TACACS that stands for terminal access controller access control system. Although TACACS and TACACS+ are commonly associated with Cisco devices. This was released as an open standard in 1993. Even so, whenever you hear TACACS or TACACS+, it’s very common for that to be associated with a Cisco device.

## Kerberos

* if you log into a Windows domain, then you’re using an authentication method called Kerberos. This is an authentication method that supports single sign on. So you would log in the morning with your username and password, and throughout the day as you’re accessing other resources, you’re now forced to log in with your credentials every time you connect to a new device. This is also a standard that’s been around for a long time. It was developed in the 1980s at MIT.
* But where it really became popular in the enterprise is with the introduction of Kerberos in Windows 2000. Now when you log into a Windows domain, the authentication method that’s occurring behind the scenes is using Kerberos. The single sign on functionality of Kerberos is enabled through the use of cryptographic tickets. When a user is initially logging in to the domain, they’re provided with a ticket that they can then show to all of the devices that they would like to use.

# Malwares:

## Remote access backdoor:

* This might lead to a bot being installed onto your system and it effectively gives the malware author complete access to your system. This is one of the reasons we often tell you to make sure your system is always updated with the latest set of security patches to ensure that none of these vulnerabilities can be exploited by a third party.
* If your system is patched, that means that you are going to be the weakest link in this scenario. It’s very easy to have malware installed if you click a link in your email or click a pop up that might be on a web page. Or you might be browsing a website that downloads a file to your system, and from that point on you might want to click that file to see exactly what it does. In some cases, you have no control over this and it’s a worm that’s able to hop between systems without having any type of human intervention.
* To best protect against all of these types of malware, you want to be sure to keep your operating system up to date with the latest security patches, continue to maintain and run your antivirus and anti-malware software, and make sure that all of your applications are up to date. You may have to visit the publisher of the applications to make sure that you’re running the latest version.

# Type of malware:

## Trojan:

* This was named after the Trojan Horse that Greeks used to capture the city of Troy from the Trojans themselves. They used a large physical horse to be able to get into the gates of Troy. On your system, the Trojan Horse is software that appears to be one thing, but in reality behind the scenes is actually malware. This might be a link in an email that says click here for a funny video I found of yourself, or you might be on a website that says download the software to run this utility for your operating system.
* But in reality it’s not a utility, it’s a piece of malware and it is disguised itself as a Trojan Horse. If you double click this Trojan Horse software and execute this program, it now has effectively circumvented all of the security that you had in place. Hopefully, the last thing that can protect you is your antivirus or anti-malware software which hopefully will be up to date to be able to recognize this Trojan Horse and prevent it from executing on your system.

## Rootkit:

* This was originally a technique used in Unix, and that’s where we get the name root in rootkit. Because in Linux and Unix, the root is the Super User on the system.
* One of the key characteristics of rootkits is that they embed themselves deep in the operating system. In some cases, so deep that it’s very difficult to identify that the rootkit is even installed in the system. It’s not unusual for rootkits to embed themselves within the kernel of the operating system itself, turning it into a core piece of the OS. And because it is part of the kernel, it’s able to hide from other applications that may be running on top of this operating system.
* So even if you’re running anti-malware software, that software would have no idea that a rootkit is installed on your system. This means if you perform a scan of your system, your antivirus or anti-malware software will tell you your system is perfectly clean, and there’s nothing to worry about. Although it may be difficult to find a rootkit using your antivirus software, you may still notice things happening in the operating system that seem unusual or out of place.
* In those cases, it might give you a clue that there’s software running on your system that might be malicious. If you have identified the type of rootkit that might be installed on your computer, then you might be able to use a third party removal utility that is specifically built for this type of rootkit. These are usually built after a rootkit is discovered, and it’s something that everyone can use to either check or remove a rootkit that’s on their system.
* Many of the reasons you don’t see rootkits on systems today is that we’ve created a series of security controls built into the BIOS of our computers. If you’re running a UEFI BIOS, you have a functionality called secure boot. Secure boot checks the operating system files and the core kernel of your OS to ensure that nothing has changed, and that there’s no malware or rootkit that’s been installed without your knowledge.

## Virus:

* A virus is probably one of the most popular forms of malware that can be installed in our system. A virus is effectively malware **that can replicate itself from computer to computer. It needs human intervention to be able to make this happen.** But unfortunately, **humans are all too good at clicking or double clicking to launch applications** that perhaps they should not be running.
* Once you double click this virus and it’s executing on your computer, it can then jump to other systems, either through the network or through other removable drives that you might have connected to your computer. Although there are some viruses that don’t tend to do anything on your system, the vast majority of viruses create problems with displays, performance, and other issues in your operating system.
* This is why we often say to have antivirus or anti-malware software running on your system, and to keep the signatures for that software always up to date.

## Boot sector virus

* The virus itself is part of the boot sector. So every time you start your system, that virus is automatically loaded from the boot sector on your drive. This means the malicious software is already running when your operating system begins, and your antivirus software doesn’t have a way to prevent that software from executing. Even if you were able to clean this virus or malware out of memory, the next time you rebooted your system, the malware would simply load itself again from the boot sector.

## Spyware:

* Spyware may sit on your system and provide advertising, it may wait for you to type in information about your bank accounts, or it may cause you to click on links that normally you would never click on. It’s not uncommon for this spyware to become installed on your system as a Trojan Horse.
* It poses as peer to peer software, a streaming media server, maybe it appears to be some fake security software, and encourages you to install it. And once you install that software, you’re now running spyware on your computer. This can monitor your browsing habits it can see what websites you happen to visit and What you’re typing in at those websites by using a keylogger. So you might visit your bank’s website and type in a username and password to log in.
* Everything that you’ve just done, including what’s on the screen and the information, you’ve typed in has now been sent to the attacker who’s managing this spyware. Keyloggers are an especially nasty form of spyware because they’re constantly storing everything that you type in at your keyboard, they take screenshots of the information that’s on your screen, and they check to see where you’re clicking on the screen. And they store all of that information and then send it to the attacker.

## Ransomware:

* Instead of monitoring your keystrokes or presenting advertising on your screen, it instead encrypts all of the personal data that you have on your system.
* So now all of the word processing documents, spreadsheets, pictures, music, and anything else that’s in your Documents folder is now encrypted and unavailable to you. The attackers are more than happy to provide you with the decryption key that will unlock all of your personal files, as long as you’re willing to send them money. Usually, this is through a cryptocurrency or some other untraceable method.
* If you do find that ransomware is encrypted all of your personal files, instead of sending the attackers money, you can simply just delete everything that’s on your computer, which effectively cleans away the ransomware, and then you can restore from a known good backup. Some types of cryptocurrency require you to perform a series of tasks to be able to mine that cryptocurrency or earn different pieces of that cryptocurrency. This is usually based around a very difficult math problem dealing with prime numbers.

# Anti-Malware Tools

## Windows Recovery Environment:

* This is a command line that you can launch on your Windows computer that is used without having to start the entire operating system. This effectively gives you access to all of the files that are in your operating system. So it is a very dangerous way of changing things that are inside of your operating system, and it should be considered a method of last resort when it comes to removing malware.
* But with that warning in place, this Windows Recovery Environment gives you a lot of access to the operating system, and you can effectively make any change you would like to any of the files in the OS. But of course, because this is simply giving you a command line prompt, you now have to be knowledgeable enough to know what to do at this prompt to be able to remove the malware.
* From here, you can copy or modify files that are part of your operating system. You can enable or disable services from starting during startup. Or you can modify the file system, run some diagnostics, or modify any part of the underlying file system. One of the ways to start this recovery environment is from inside of Windows itself. When you click on the power icon, get the options for sleep shutdown and restart, you would click restart but you would hold down the Shift key while clicking that option.

## Software firewall:

* you want to be sure that you’re running a real time version of this software so that it’s always activated. And if you happen to accidentally download some malware, it can immediately prevent it from executing on your system.
* And there’s even a new style of anti-malware software that looks for malicious activity on your system instead of relying on a set of signatures. This is an even more advanced form of anti-malware because it can look at the symptoms and results of anti-malware and prevent any of those malicious acts from occurring, regardless of the software that might be running.
* We also want to prevent anyone from outside of our system from gaining access to our operating system across the network. One way to do this is to run a software firewall on your operating system so that it sits on your local computer and monitors all of the inbound and outbound traffic from your PC. This might stop malware that’s been recently installed from communicating outbound from your system, and it would certainly prevent any type of malware from coming inbound to your computer.
* If you’ve installed Windows you’re already using software firewall in the form of Microsoft’s Defender Firewall and this is what you’d like to use at a bare minimum. This software runs by default it is constantly monitoring the network communication, and it can allow or block based on a number of different criteria. But even with all of the necessary security software in place, you still have vulnerabilities on your network in the form of the users.

# Windows Security:

## Microsoft Defender Antivirus:

* Your antivirus software should always be enabled and it should always be configured for real time analysis. This means that when you download a file or launch an application, your antivirus software will examine that code and will determine whether it’s malicious or not.
* owever, there may be times when you’re troubleshooting an application and the application developer asks you to temporarily disable the real time access to see if that’s what’s causing the issue. Microsoft Defender Antivirus allows you to enable and disable this real time protection. And you can find this in the Windows Security app under virus and threat protection settings, , manage settings and real time protection.

# Securing a SOHO Network:

* If you’re installing a router or access point into **a small office or home office**, a SoHo, then you want to be sure that you’re not using the **default username and password for that device**. When these devices ship from the manufacturer, they all have a standard set of usernames and passwords.
* You certainly don’t want to leave those default credentials because anyone who comes along and tries that combination will have complete access to your router. This is a good best practice for any device or operating system that you’re installing in your office or your home, is that all of these default credentials need to be **changed from the default**. This is a very easy step for the attacker because all of this information is documented online.
* There may be content filtering built in to your SoHo router in the form of IP address filtering or content filtering. You may be able to create an allowed list on this router that would block all traffic through the router except the traffic destined for certain IP addresses or fully qualified domain names. This is obviously a very restrictive form of security, and it requires that you as the administrator always keep that list up to date.
* A different philosophy on filtering is to create a denial list where everything is allowed through the router except for access to very specific IP addresses or sites. This might be a list of IP addresses, domain names, or URLs that is filtered in your device, and no one will be able to access that device from your **SoHo router**.

## firmware updates

* This new firmware may have bug fixes, security patches, or new features available in the operating system of the device. As a general rule, you’ll want to make sure that you always maintain the latest version of software for these devices. Each time a security patch is updated, it’s pushed down as one of these firmware updates, and you want to be sure that your system always has the latest set of security patches installed.

## Content filtering:

* This content filtering provides an additional layer of security that you don’t normally get from the firewall. This allows you to really focus on allowing or disallowing access to certain locations. In a corporate environment, this may be implemented to allow or disallow access of sensitive information. You may be restricted from visiting certain sites because those sites may be inherently insecure. Or this remote site might have content on it that’s not appropriate for work.

## IP addressing

Static IP

DHCP(Dynamic Host Configuration Protocol

## UPnP

* Many of the Soho routers we use today include a function known as UPnP. That stands for universal plug and play. This is a way to have the router automatically configure itself when certain applications are being used on the network. We sometimes refer to this as zero configuration.
* When you start an application that uses UPnP, it will communicate to the router, and tell the router to create a port forward from the outside to be able to allow access to the application service. This means that while this application is active, anyone is able to communicate through your firewall and talk directly to this application service.
* You might already be thinking that having an application make configuration changes to a router that allows access from the internet could possibly be a security issue, and you’d be correct. **The best practice would be to completely disable universal plug and play**. And **if somebody does need access to a service that’s on your network, it might be a better idea to use a screen subnet.**

## Screen subnet:

* A screen subnet is what we used to call a demilitarized zone or DMZ. It’s a section of the network that is on the firewall but is not connected to your internal network. It’s a perfect place to put resources that need to be accessed from the internet but still need to be limited from the rest of your network. If you need to build out a service and have someone access that service from anywhere in the world, you’ll probably want to install that on a screened subnet.

## service set identifier, or SSID:

* When you first turn on a SoHo router, it will have a particular wireless name associated with the access point. That wireless name is called a service set identifier, or SSID. And the defaults for many access points are SSIDs by the name of Linksys, default, Netgear, and others.
* It’s usually not a good idea to use the name or manufacturer of the device as the SSID. This would make it very easy for someone to look up what the default credentials for this device might be. And if there are any known vulnerabilities, they’d be able to easily find them, based on the manufacturer’s name.
* You may also notice an option within your Soho router called Enable or Disable the SSID broadcast. This is the message that is sent out to all of your devices that populates the list of the wireless networks that are in your area. And if you disable that SSID broadcast, it won’t show up on any of those lists.
* However, removing the name from a list doesn’t somehow make the network secure. If somebody knows the name of the wireless network, they can still connect to it. And if someone’s using Wireshark or any network analysis tool, it will be very easy to determine the SSID for this network, even if the SSID broadcast is not enabled.

## Wireless Channels and encryption:

## Disable guest network:

Disabling ports:

* If your office has a break room or conference room, you may notice on the wall that there are probably ethernet connections that could possibly be used. This is very common in a place of work, especially if you need to be able to connect to a network very quickly.
* But if any of these interfaces are not going to be used, they should be administratively disabled on the switch. This requires a bit more work to administer this and maintain that list. But it ensures that nobody can walk into an empty conference room, plug into the network, and have full access to your internal network.
* In many corporate environments, these are often configured with **network access control, or NAC. This uses a 802.1X** to require authentication before anyone is able to communicate on the network. So even if there is an open port in the conference room and someone plugs in, they would still have to authenticate to gain access to the rest of the network.

## Port Forwarding:

# Malware Removal:

* this is not a best practice because you never know if you’ve been able to 100% remove every of malware from a system. The best practice almost universally is to delete everything on a system, and either install from the original installation media, or reinstall from a known good backup.

## Verify malware symptom:

* The first step in removing malware is recognizing you have malware to begin with. You’ll probably see messages appear on the screen or some aspect of the normal use of your operating system is not working as expected. You might see a message that says an operation did not complete successfully because the file contains a virus or potentially unwanted software. Or it may be that the antivirus software that’s already running on your system has identified malware, and it’s giving you a warning that something has been installed without your knowledge.
* But it may not be something as obvious as a message on the screen. It could be that the system is booting very slowly, or when you try to start an application, you have very poor performance. If you do think that you ran a program that installed malware on your system, you may be able to research that executable and see what malware may be contained within that executable file.

## Quarantine infected

* The moment you think that this system may be infected with some type of malicious software it’s time to completely quarantine the system from the rest of the network. We don’t want that malware finding its way onto someone else’s system, which creates even more problems for removing this from your network. You should unplug from any physical wired ethernet connections and be sure that you’ve disabled any wireless networks on this computer.
* You’ll then want to isolate any removable media. So if you have an external storage drive or you’re using a USB drive, you want to unplug those from your system, set them aside, and make sure nobody uses that media. The goal here is to prevent the spread of this malware onto other systems that may be on your network. At this point, you don’t want to perform backups or transfer files off of your system because all of those files could be infected with this malware.

## Disable System Restore:

* This third step is not completely obvious, but it does make sense once you understand the reasoning behind it. You want to go into your system protection on your computer and disable the system protection function. Turning this function off will delete any restore points that were previously saved on your computer. That’s because the malware authors are not only infecting your current system, they’re going back into all of your restore points and infecting the restore points as well.
* It might seem that you’d be able to use the system restore function to go back in time, put your system back to an earlier configuration, and therefore, remove the malware from your system. But now that this malware is on your system and has most likely infected all of the restore points, we simply need to delete those from your system.

## remediate phase: Update anti-virus, Scan and Remove

* Step 4 is the remediate phase where we identify and remove this malware from your computer.
* Before we begin the removal process we need to make sure that we’re running with the latest version of our antivirus software, and that we have the latest antivirus signatures. So there may be an update option within your antivirus that will check it to ensure you’re running the latest engine and the latest signatures. Hopefully, your computer has configured for automatic updates of these signatures. If it’s been set to manual, then that’s probably why this system was infected to begin with.
* Manual updates would require someone to go into this system multiple times a day to keep it up to date.
* certain drivers and files will not be loaded during the Safe Mode process, and this might be just enough to get your system up and running to allow you to transfer those files out of your Windows operating system.
* You can also boot your system with a PE, or a pre-installation environment. These commonly boot from a USB drive or DVD-ROM, and they can provide you with a recovery console that you can then use to transfer files off of your system.

## Schedule scans and run update:

* You simply tell the antivirus software to automatically keep itself up to date. But if you wanted to perform this task manually, you could create a task schedule for this that will go through the process of updating that particular antivirus software. If you’re running Windows, you’ll probably find in your test scheduler some options for Windows Defender cache maintenance, a Defender cleanup, a scheduled scan, and a verification.
* You not only want to be sure that your antivirus is updating itself automatically, you want the operating system to update automatically as well. So check your settings for Windows Update and make sure that it’s set to automatically update your operating system. Earlier, we disabled the system restore function so we could delete any previous restore points that may have been infected with malware. Now that we’ve cleaned the system, we can turn this feature back on.
* So you want to go back into the system protection settings, turn on the system protection, and make sure that you have plenty of drive space available to store multiple restore points. Now we can shift our focus into educating the end user on how they may be able to avoid this type of problem in the future. We could do this through one on one training, where we step through some of the best practices to prevent someone from installing malware on their computer.

## Educate the end user:

# Remote Access:

## Remote desktop connections

* We refer to this as remote desktop connections, and there’s different types of connections depending on what operating system you’re connecting to.
* For example:

if you’re connecting to a **Windows device, then you’re probably using Microsoft’s Remote Desktop Protocol or RDP.** And although RDP is primarily a Windows technology, there are clients available for many different operating systems. So you could be running Mac OS, Linux, and other operating systems and connect via RDP to a Windows device. If you’re not running Windows, then you don’t have access to RDP.

But there are technologies that are very similar **for Mac OS and Linux. One of these is VNC, or Virtual Network Computing. This uses RFB, or Remote Frame Buffer protocol to be able to communicate with this remote desktop.** There are clients available for VNC on many different operating systems, including Windows, and you can commonly find them as open source projects. If you work in a support role then you’ll be using these remote desktop technologies quite a bit. This technology is so good that even the scammers are using it as a way to provide access to your computer.

## Secure Remote access:

* One way to tell if a system is listening for an **RDP connection is to see if TCP port 3389 is currently open on that device. If an attacker finds that port is open, they’ll try connecting to that device and they’ll keep trying different passwords until they find one that works.**
* **This same security concern also applies to VNC and all of the third party remote desktop systems.** These are often just secured with a username and password, and it’s very common for people to reuse those credentials from system to system.

## Virtual Private Network:

* Another type of remote access comes in the form of a VPN, or Virtual Private Network. With so many people working at home, we’ve become very accustomed to using VPN technology on today’s networks. Everyone using this VPN is commonly connecting to a central concentrator. This is a single device that handles the encryption and decryption of these VPN tunnels. This is sometimes a standalone device, but you can often find it integrating into other devices such as a firewall.
* You can also build your own VPN concentrator by installing Linux and installing some specialized cryptographic hardware. And there are other systems that are software only for limited implementations. To use this VPN, we would install client software on everyone’s machine, and many operating systems include a VPN client that’s built into the OS. This VPN client can be configured for on demand access. So when we need to use the VPN, we would turn on the VPN software. And when we want to disconnect from the VPN, we would click a button to disconnect.