HARDENING WINDOWS COMPUTERS

OVERVIEW

A. Automatic Updates

B. Encrypted File System

C. Configure Logging using Event Viewer

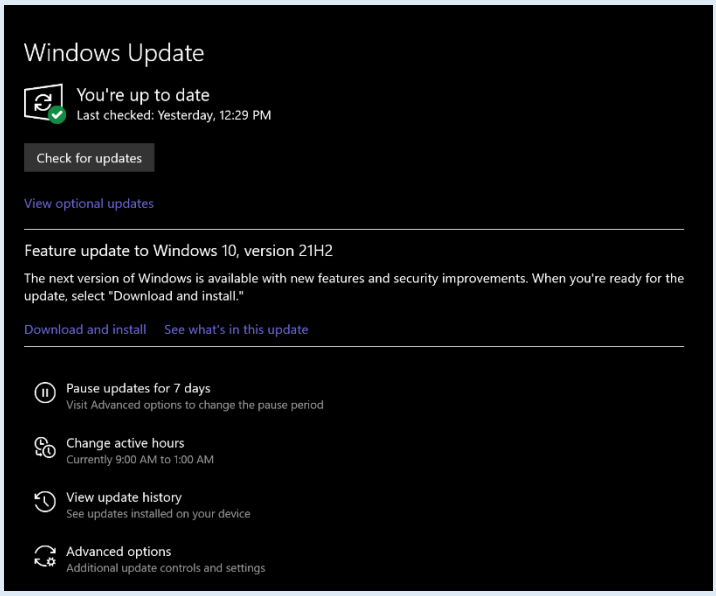
D. Disable Unused Services and Filter Ports

Image by rawpixel.com

A. AUTOMATIC UPDATES

1.1 Windows Update

The **Windows Update** feature can be utilized to install and manage updates for individual systems.



- **Quality updates** include regular security patches and software updates
- **Feature upgrades** consist of new features and Windows functionality

Both types contain all previous updates, which helps reduce the chance that a hacker or malware attack might succeed in exploiting a mising update.

- Security updates are distributed on the second Tuesday of every month by Windows Update
- Configure **Active Hours** to set when updates should NOT be installed

1.2 System Center Configuration Manager

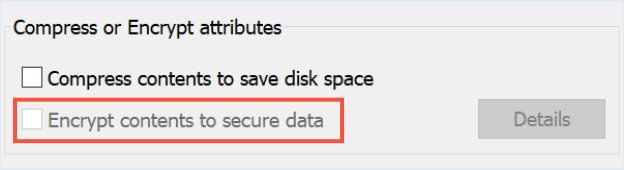
- SCCM, a Microsoft software product, is a common standard for device patch-management. It includes a suite of tools that administrators can use to manage servers and devices on a domain.
- In a corporate setting, the use of a software like SCCM is much more practical when it comes to managing and configuring a significant number of systems.
- More recently, SCCM has undergone a name change and is currently referred to by Microsoft as “Microsoft Endpoint Manager”. The functionality of Configuration Manager remains the same.

Third-party vendors such as **BigFix, BladeLogic,** and **Tanium** also offer patch-management solutions.

B. ENCRYPTED FILE SYSTEM

Windows EFS utilizes encryption to enhance the security of files and directories. It is available for Windows 10 Pro / Enterprise / Education on NTFS volumes.

Any other Windows edition will display **Encrypt contents to secure data** greyed out on a selected item as follows:



The following items cannot be encrypted by EFS:

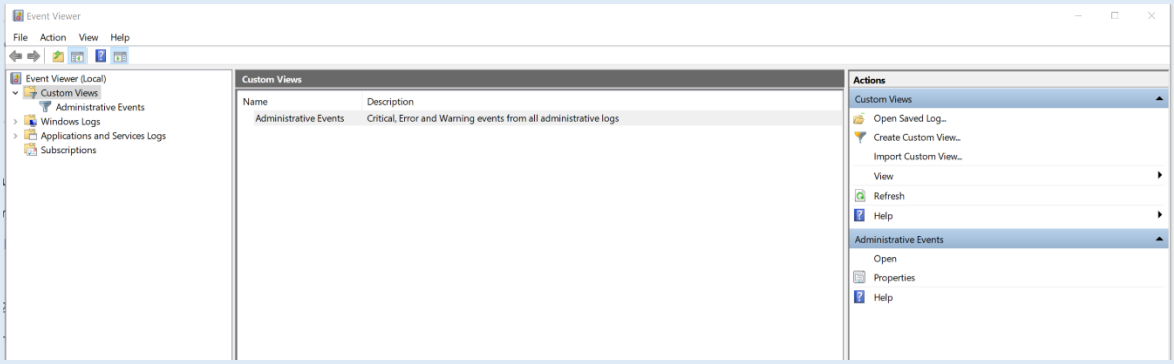
- Transactions
- Compressed Files
- System Files/Directories
- Root Directories

See here for more information.

C. CONFIGURE LOGGING USING EVENT VIEWER

Windows Event Viewer is used to access logs regarding system events.

Press **Windows Key + R** to open **Run** and type **eventvwr.msc**



There are two types of log files:

- **Windows Logs –** application, security, setup, system events
- **Applications & Services Logs –** other logs from applications and services to record events

Create a custom view to monitor critical system events:

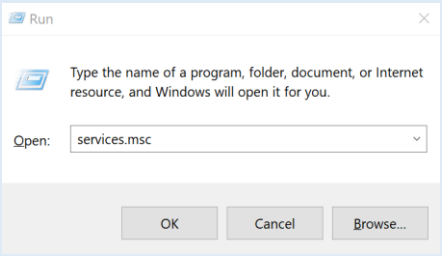
1. Under **Action**, click **Create Custom View**
2. On **Filter** tab, select **Critical** check box in **Event Level**

3. In **By Log**, expand Windows Logs with the down arrow and select only **System**
    a. Click **OK**
4. Enter a name, such as **System Critical Events** and click **OK**
    a. Your new custom view will now be located in the left pane under **Custom Views**

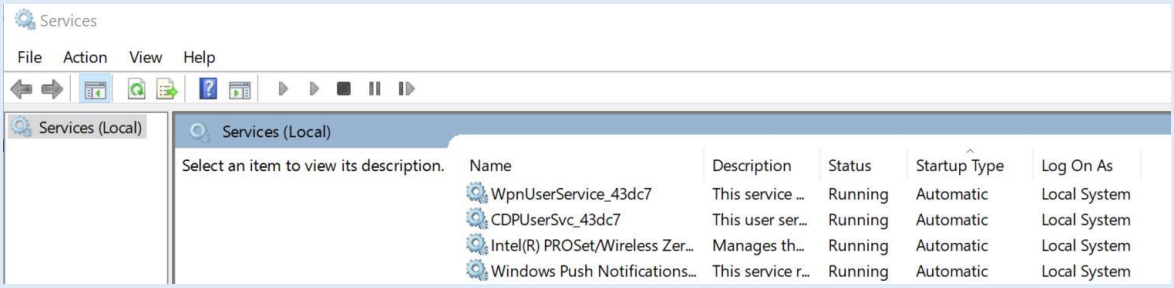
D. DISABLE UNUSED SERVICES AND FILTER PORTS

Open **Services**:

1. Press **Win Key** + **R** to open Run
2. Type **services.msc**



3. Press **Enter**

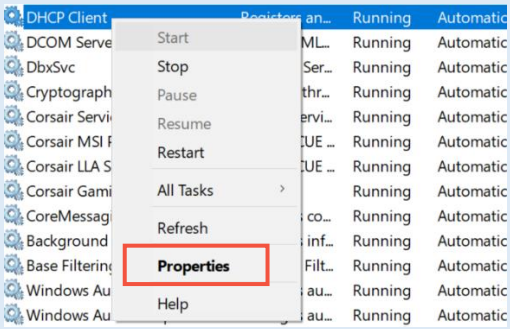


- Each service's status indicates whether it is currently **Running** or not

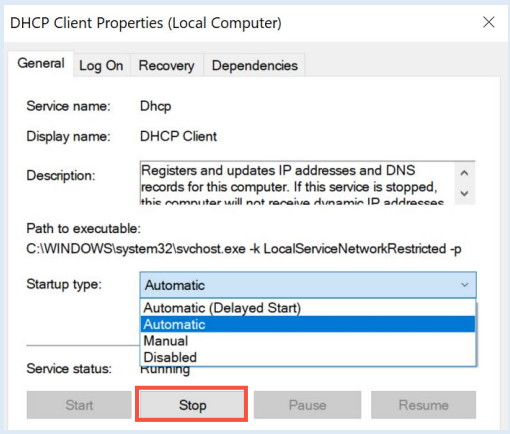
Services should be managed accordingly with the purpose of a particular device. For example, if you were setting up a workstation to use a static IP address, you might disable the **DHCP Client** service.

To disable a service and prevent it from starting up:

1. **Right-click** on the desired service to bring up a context menu



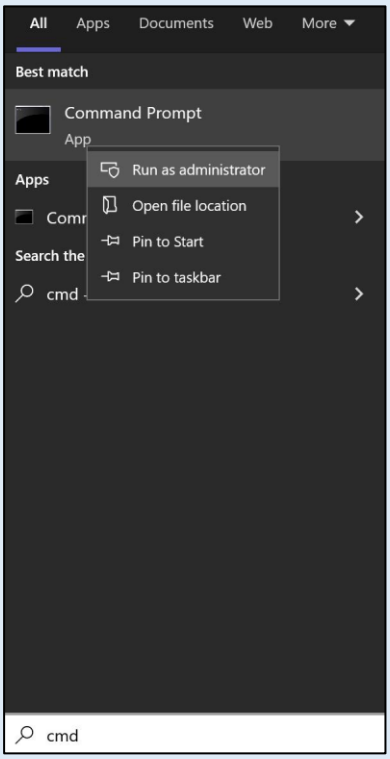
2. Select **Properties**
3. Change **Startup type** to **Disabled**



4. Click **Stop** at the bottom to shutdown the service (if running)
5. Click **Apply** to save changes and then click **OK**

Find all open ports and connections in command prompt:

1. Go to Windows search and type **cmd**
2. Right-click to **run as administrator**



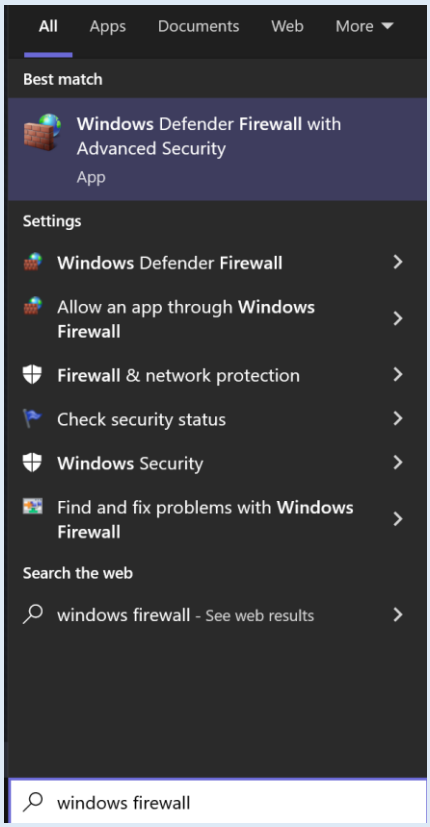
3. Type **netstat -ab**

```
C:\WINDOWS\system32> netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-DJU8GO0:0      LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            DESKTOP-DJU8GO0:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:902            DESKTOP-DJU8GO0:0      LISTENING
 [vmware-authd.exe]
```

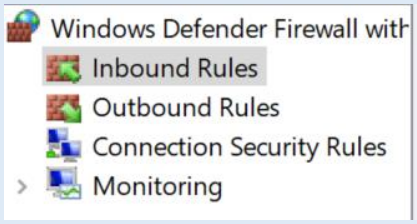
Note: Output includes open network ports and related applications/services using them

Close open ports using Windows Firewall:

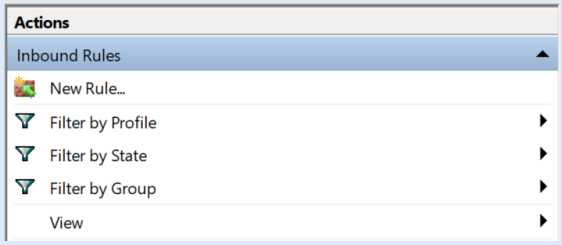
1. Go to **Start >** type **Windows Firewall >** Open **Windows Defender Firewall with Advanced Security**



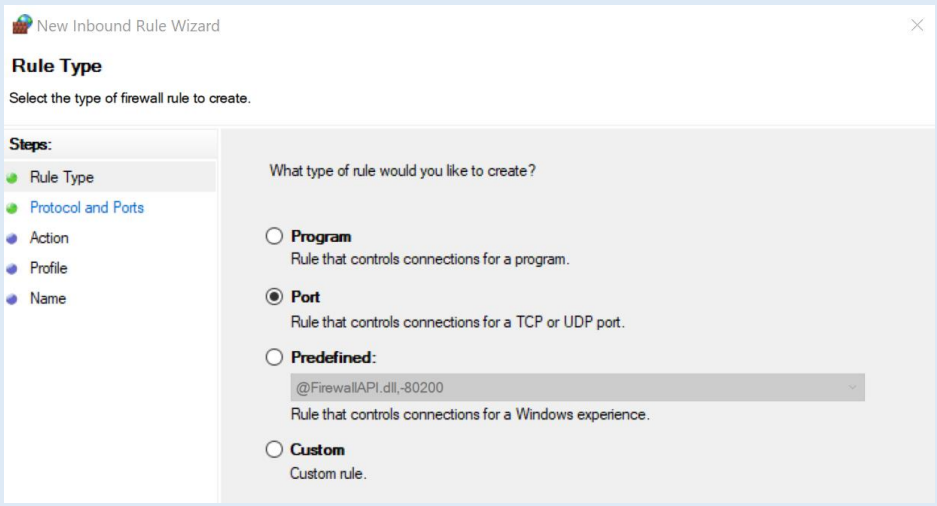
2. Once open, select **Inbound Rules**



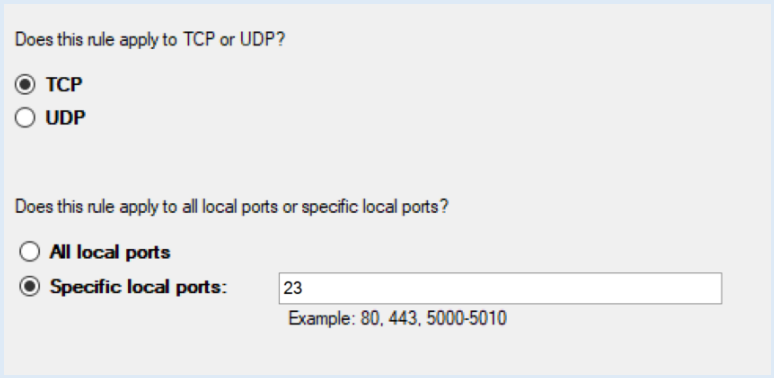
3. The panel on the right will now display the option to create a **New Rule** for incoming network traffic



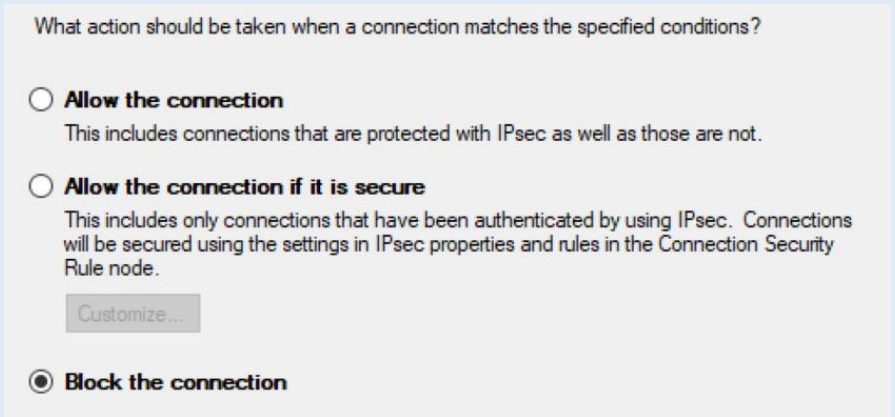
4. Click **New Rule** and then select **Port**



5. Click **Next** at the bottom
6. Select **TCP** or **UDP** depending on the service you're trying to block. For this example, we will block Telnet, an unsecure service used to remotely interface into a system. Telnet uses port 23 and TCP

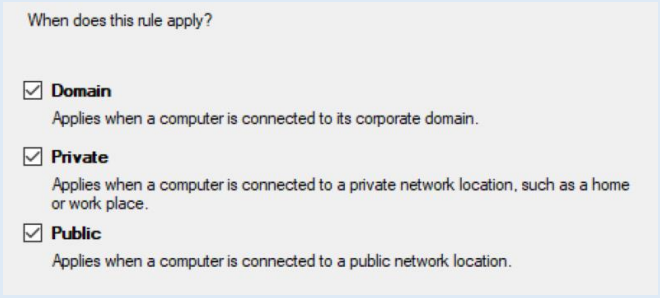


7. Click **Next**
8. Select **Block the connection**



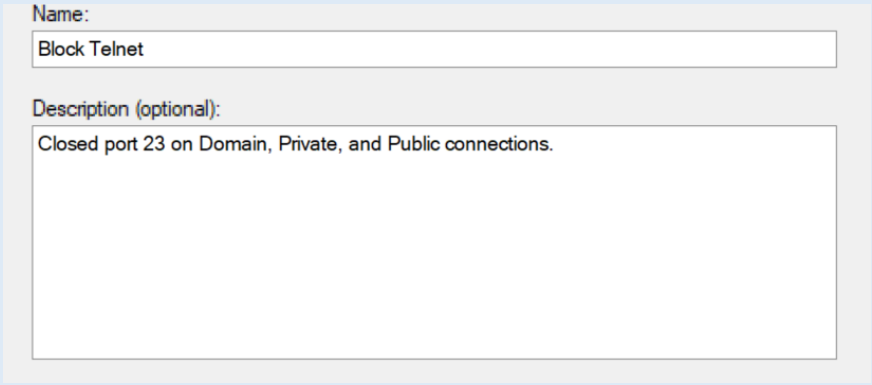
9. Click **Next**

10. A rule can be enforced over different connections as desired



Since Telnet is unsecure, leave all selected to block it no matter the connection.

11. Click **Next**
12. Enter a name to recognize the rule and note documentation



13. Click **Finish**