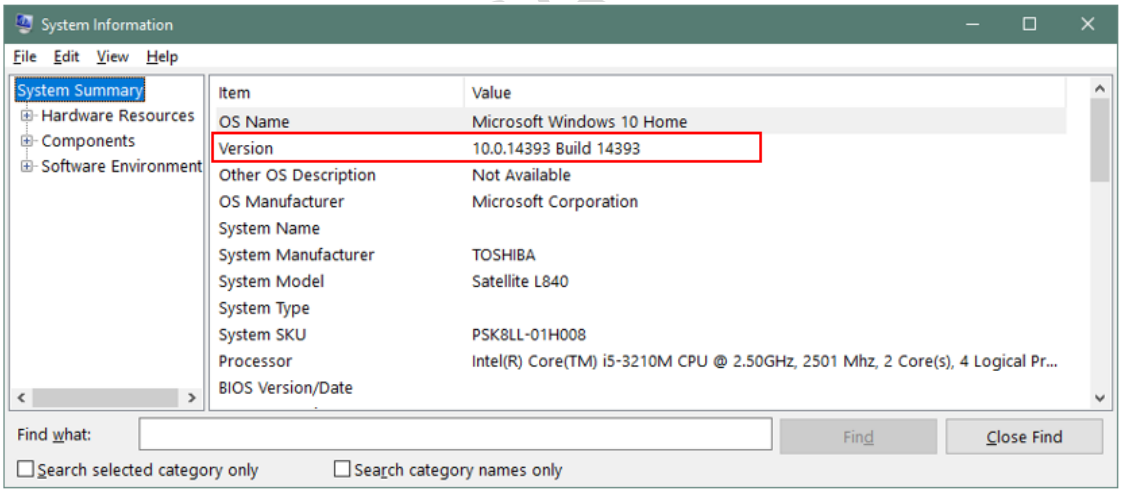
Seiring dengan maraknya serangan ***Ransomware*** bernama ***WannaCry*** atau ***WannaCrypt*** di seluruh dunia, yaitu sebuah *malware* varian baru yang diyakini dikembangkan menggunakan *exploit tools* milik NSA dengan menyerang komputer dengan sistem operasi *Microsoft Windows,* ISACA ID mencoba membantu memberikan panduan pencegahan agar terhindar dari serangan *malware* tersebut. Berikut ini adalah langkah-langkah yang dapat dilakukan untuk mencegah penularan *malware* ***WannaCry*** tersebut pada komputer *end client* yang menggunakan sistem operasi Windows 10:

Along with the rise of Ransomware attacks around the world named WannaCry or WannaCrypt, a new variant malware that is believed to be developed using NSA's exploit tools to attack computers with Microsoft Windows operating system, ISACA ID tries to help provide preventive guidance to avoid those malware attacks. Here are the steps that can be done to prevent the infection of malware WannaCry on your end client computers that use Windows operating system 10:

1. Cabut koneksi internet dari kabel LAN maupun koneksi nirkabel.
   Disconnect your machine from the internet both wired or wireless network.
2. Lakukan *backup* terhadap seluruh data yang ada di *local hard drive*.
   Backup all of your files from local drive to external storage.
3. Lakukan *update* terhadap *Antivirus* yang digunakan.
   Update Antivirus definition.
4. Instal **Security Patches MS17-010** – sesuai dengan versi OS yang digunakan. Untuk melihat versi Win10 dapat dilakukan dengan cara tekan tombol **Start** lalu ketik **msinfo**, akan tampil ***System information*** seperti berikut (Detail history dapat dilihat disini https://en.wikipedia.org/wiki/Windows_10_version_history):



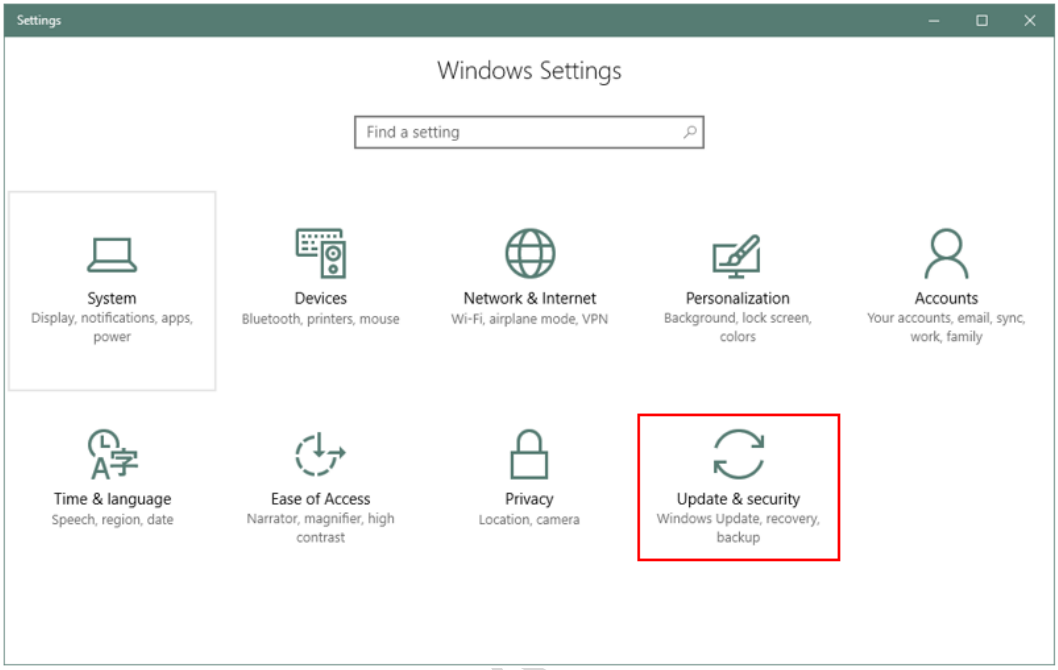
   Selanjutnya informasi detail mengenai MS17-010 dapat dilihat pada tautan berikut:
   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-tnOrm_G5.ZxMOBw54NWE1A&tduid=(858f5cbd78bd4f0d3f0ec3352b841862)(256380)(2459594)(TnL5HPStwNw-tnOrm_G5.ZxMOBw54NWE1A)()#Revisions
   *Install **MS17-010 Windows Security Patches** based on your Win10 version – You can find your Win10 version from System information. Press start button then type **msinfo** (Detail history can be seen from this link: https://en.wikipedia.org/wiki/Windows_10_version_history)*
5. Nonaktifkan layanan **SMBv1/CIFS File Sharing Support**.
   *Disabling the **SMBv1/CIFS File Sharing Support**.*

6. Tutup koneksi internet pada port **139**, **445** dan **3389**.
   Close ports that related to SMB services: 139, 445, 3389.

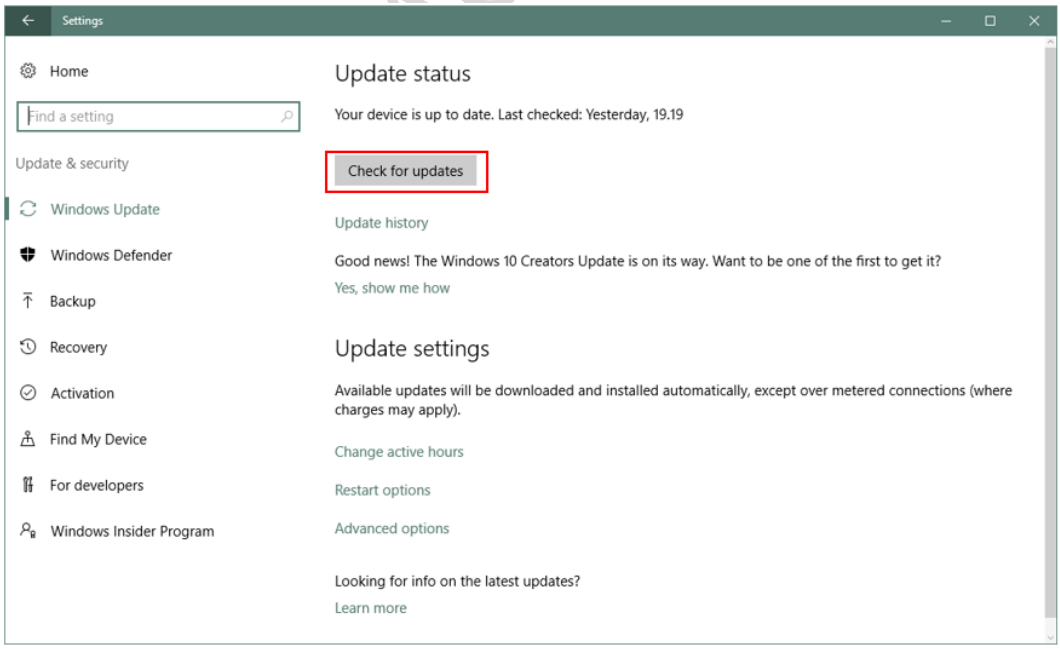
Unduh seluruh *update file* yang dibutuhkan dan simpan pada satu komputer di jaringan LAN anda, lalu perintahkan seluruh komputer lain yang dimiliki untuk mengambil *update* dari komputer tadi sehingga mencegah terjadinya infeksi dari internet serta menghemat penggunaan *bandwidth*.
Download all update that needed and save it on a network computer, then ask the people to get the updates from the computer (acting as central repository) in order to prevent external exposure and to save bandwidth.

Panduan untuk menjalankan Windows Update pada Win10
Guide to run Windows Update on Win 10

1. Jalankan fitur Auto Update melalui **Windows Settings** lalu tekan **Update & security** menu.
   *Run auto update from **windows settings** then press **Update & security** menu*



2. Tekan tombol **Check for Updates**, Windows akan menjalankan secara otomatis.
   *Press **Check for updates** button, windows update will run automatically.*



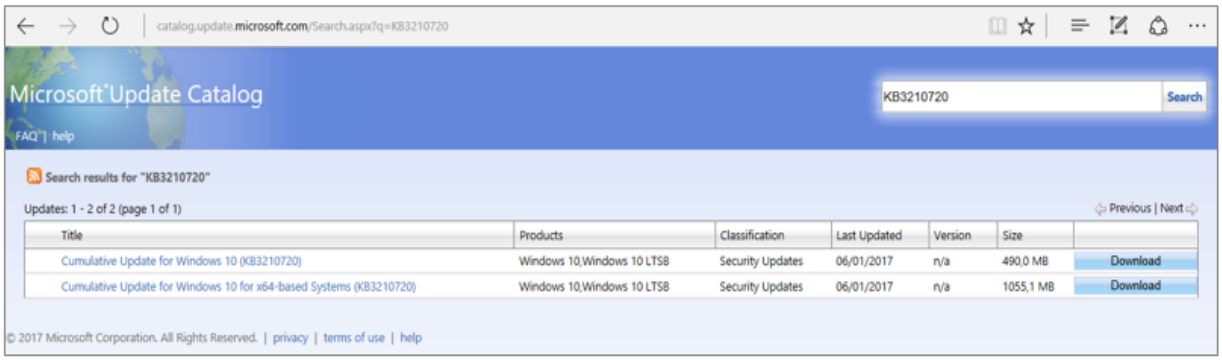
Windows update dapat juga dilakukan secara manual seperti terlihat pada panduan berikut ini:
***Windows update** can be run manually as seen on the following guide:*

Panduan untuk menjalankan Windows Update pada Win10 secara manual
Guide to run Windows Update on Win 10 manually

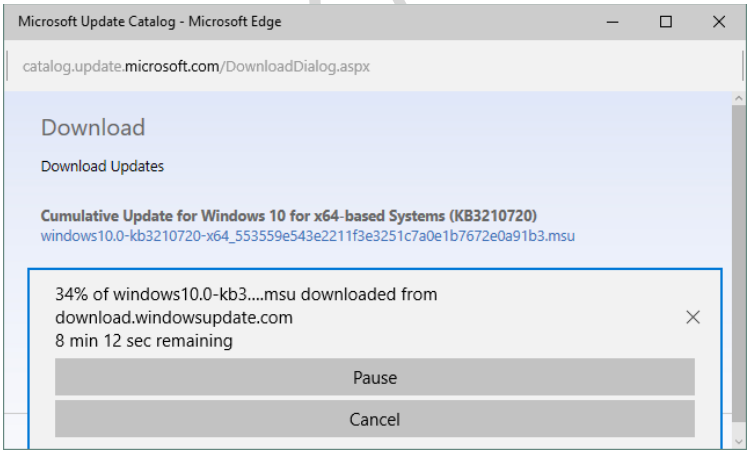
1. Unduh **Security Patch MS17-010 Patch KB3210720** dari tautan berikut ini:
   *Download **MS17-010 Windows Security Patch KB3210720** from the following link (only for Win10 final release):*

   http://www.catalog.update.microsoft.com/Search.aspx?q=KB3210720 :

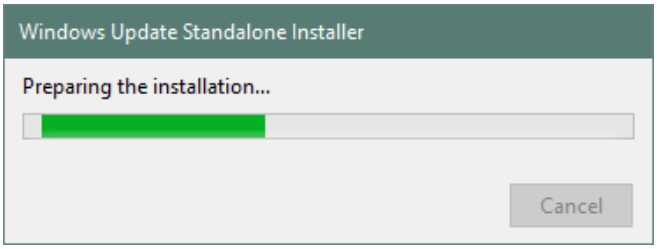
   - ❑ Unduh dan simpan file udate sesuai dengan versi komputer yang dimiliki. Pilihan pertama untuk versi x86 - 32 bit dan kedua untuk x64 - 64 bit:
     Download and save the updates that match your system version. First one for x86-32 bit and the second one for x64 – 64 bit system:



   - ❑ Halaman untuk mengunduh file yang dipilih akan muncul, lalu simpan di lokal disk:
     The download page will take sometime to show up, then save the updates onto your local drive.



2. Install *patches* sesuai versi komputer anda
   Install patches according to your computer version.

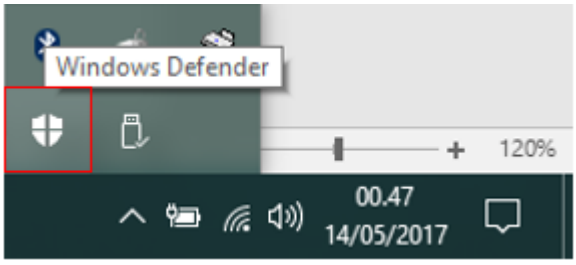


3. Setelah selesai tekan tombol **Finished.**
   Press button Finish when it's Done.

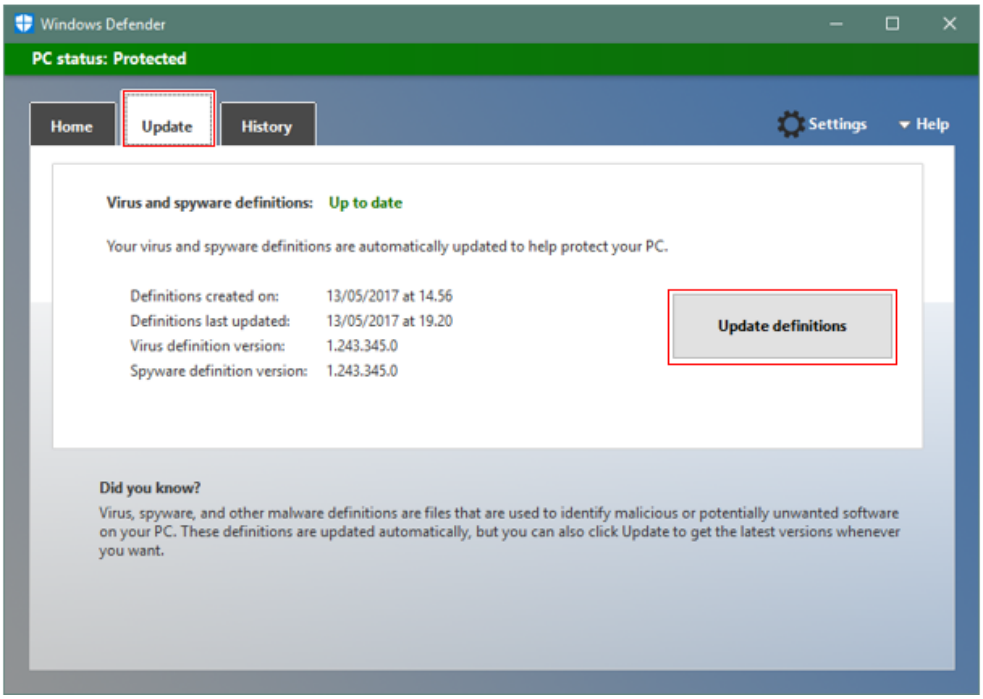
Panduan update Anti Virus Windows Defender

*Guide to update the antivirus **Windows Defender***

1. Buka antivirus **Windows Defender** pada pojok kanan bawah seperti dibawah ini:
   Run the Windows Defender antivirus form the right bottom icon.



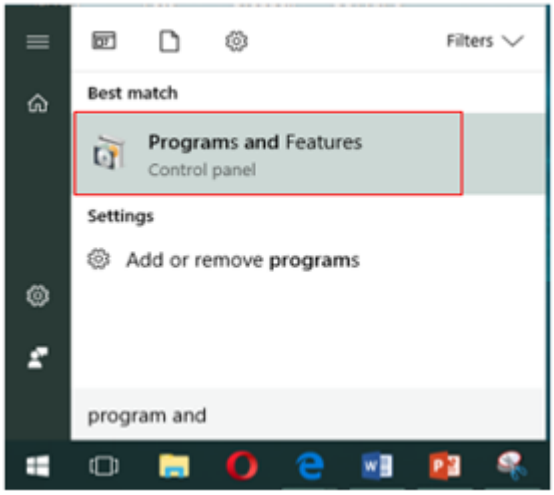
2. Pilih tab **Update** lalu tekan tombol **Update definitions**.
   *Select **Update** tab then press **Update Definitions**.*



3. Selesai.
   Done

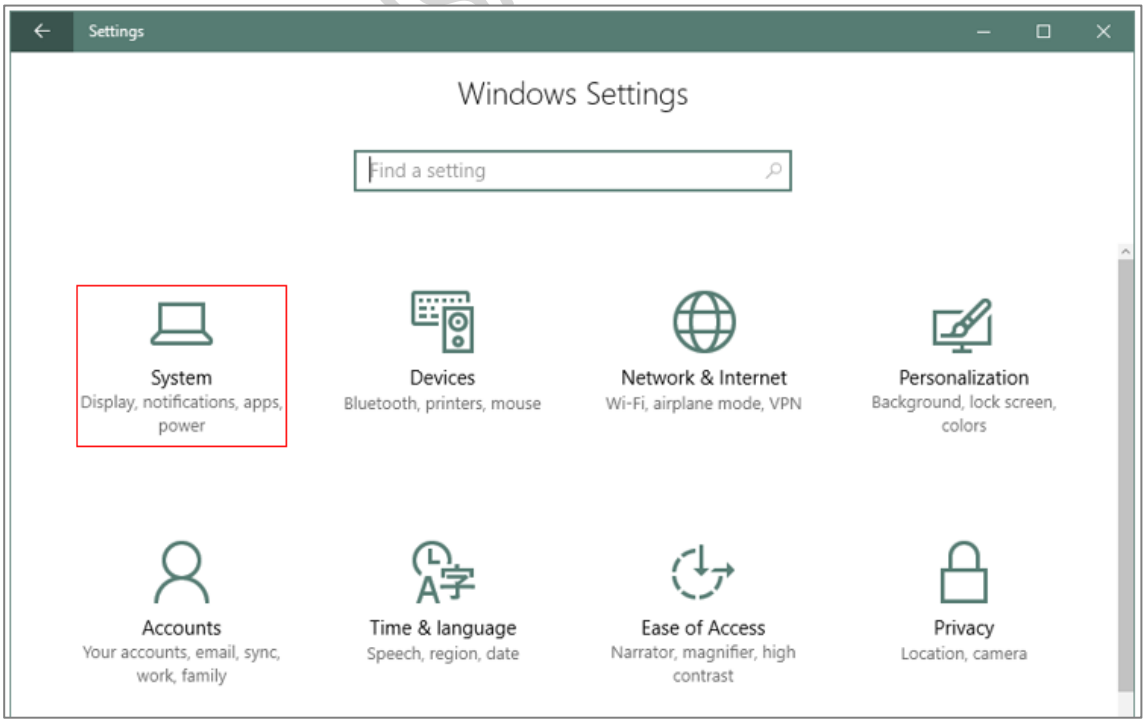
Panduan untuk menonaktifkan fitur *SMBv1/CIFS File Sharing Support*:
Guide to disable SMBv1/CIFS on Windows 10:

1. Tekan tombol start windows dan ketik "**Programs and Features**", menu tersebut akan muncul seperti terlihat pada gambar berikut:
   *Click on the windows start button and type "**Programs and Features**", the menu will show up as seen by the picture below:*

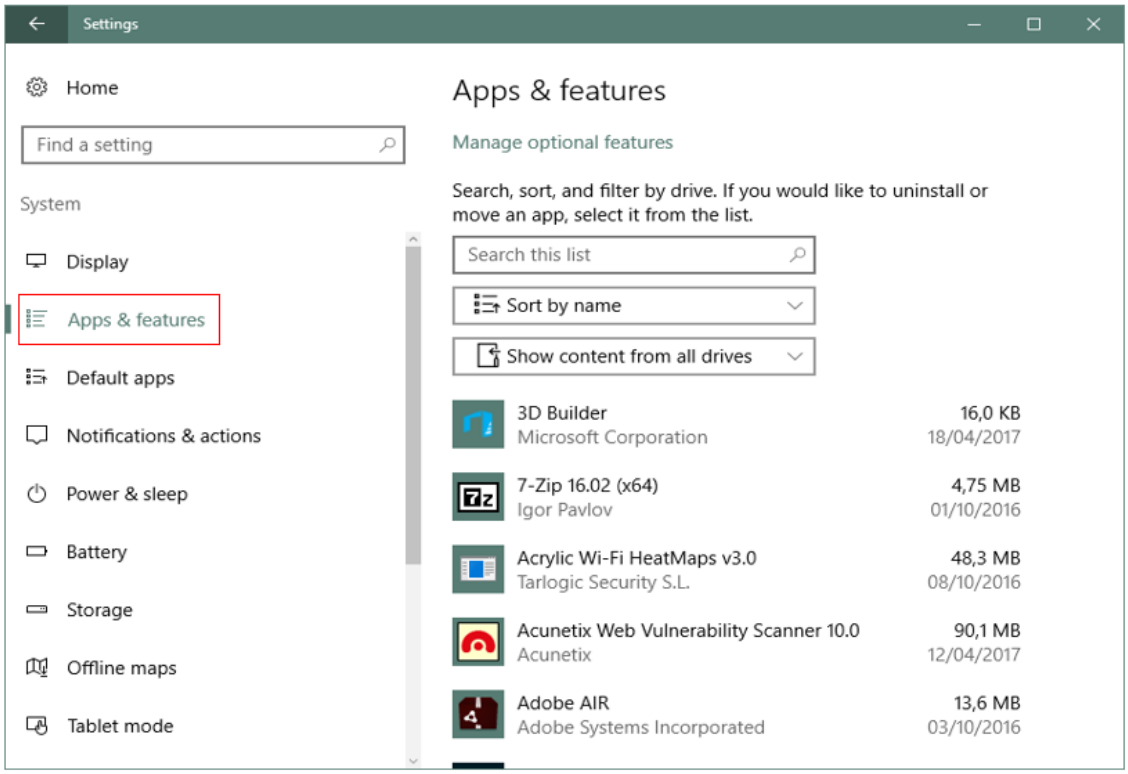


Atau anda dapat menelusur dari pengaturan Windows sesuai langkah-langkah berikut:
Or you can also browse from the windows settings as the following steps:

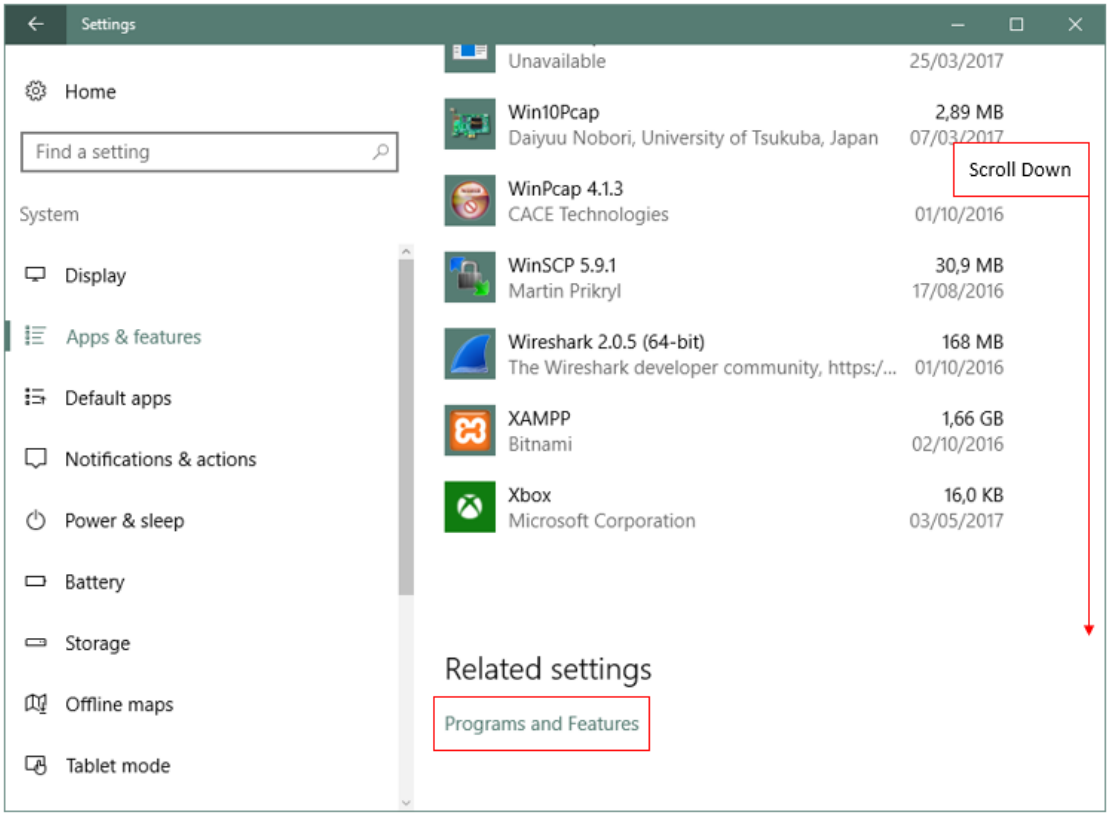
- ❑ Tekan ikon windows pada sudut kiri bawah lalu tekan ikon pengaturan
  Press windows icon on your left bottom then press settings
- ❑ Pilih menu **System**
  *Select **System** menu*



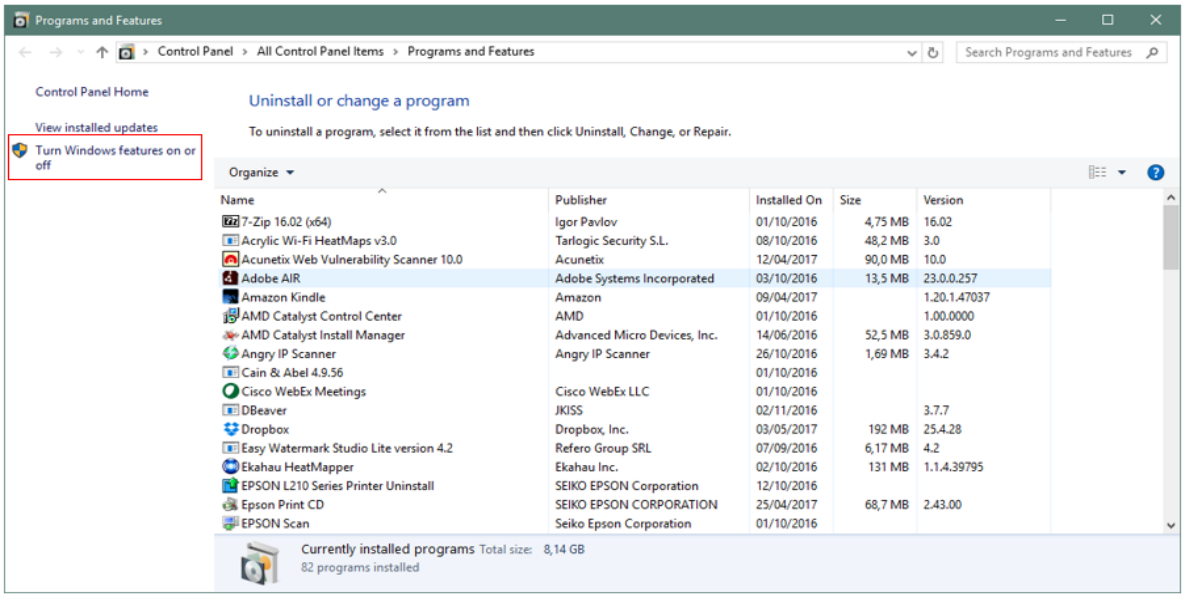
- Pilih menu **Apps & Features** pada bagian sebelah kiri.
  *On the left side bar select "**Apps & features**".*



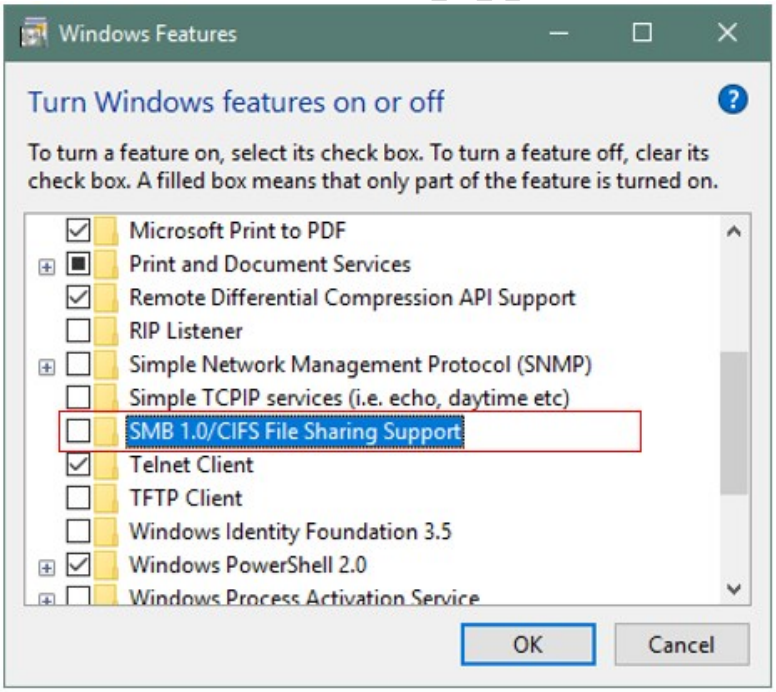
- Gulirkan laman ke bawah dan tekan menu **Programs and Features**
  *Scroll down the center windows and click on the **Programs and Features** menu*



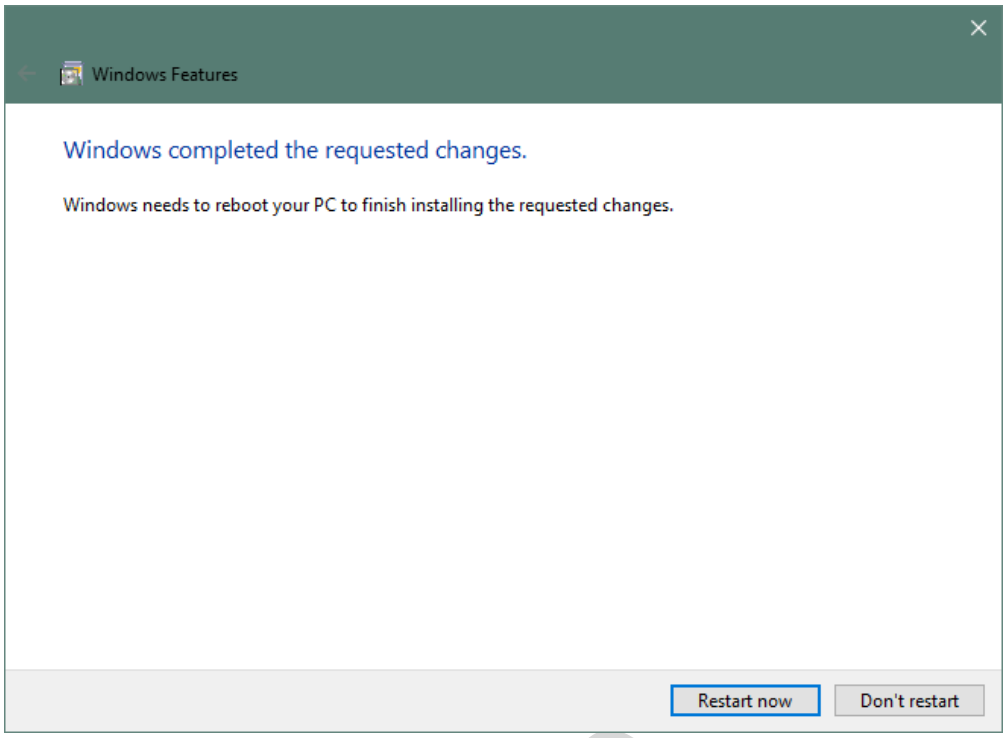
2. Setelah jendela *Programs and Features* terbuka, pilih menu "***Turn Windows features on or off***" pada sisi sebelah kiri.
   *On the left bar menu of **Program and Features** window, Select "**Turn Windows features on or off**".*



3. Hapus centang pada pilihan **SMB 1.0/CIFS File Sharing Support** lalu tekan tombol **OK**.
   *Uncheck option for **SMB 1.0/CIFS File Sharing Support**, then press **OK** button.*



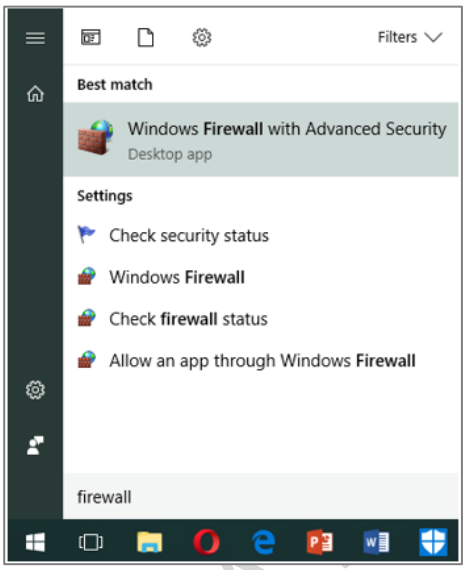
4. Setelah selesai tekan tombol **Restart now**.
   *When it's done restart your system by pressing **Restart now** button.*



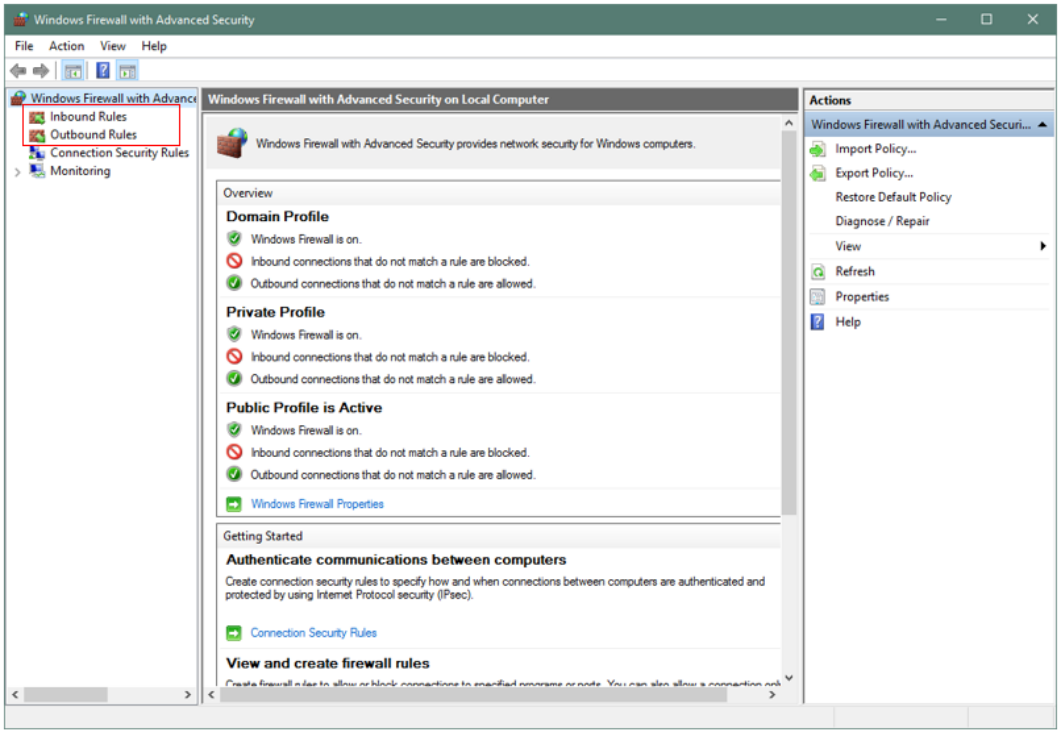
5. Layanan **SMBv1** anda telah dinonaktifkan.
   *Your **SMBv1** services has been disabled.*

Panduan untuk menutup port 139, 445 & 3389 menggunakan Windows Firewall pada Windows 10
Guide to block specific ports 139, 445 & 3389 using win Firewall on Windows 10

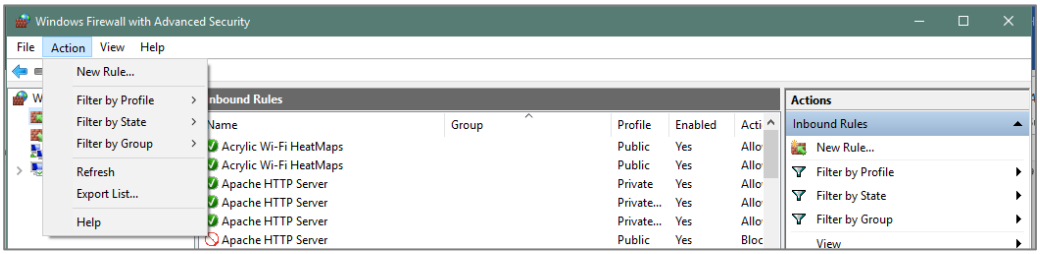
1. Tekan tombol start windows dan ketik "**Firewalls**", tersebut akan muncul seperti terlihat pada gambar berikut
   *Click on the windows start button and type "**Firewalls**", the menu will show up as seen by the picture below:*



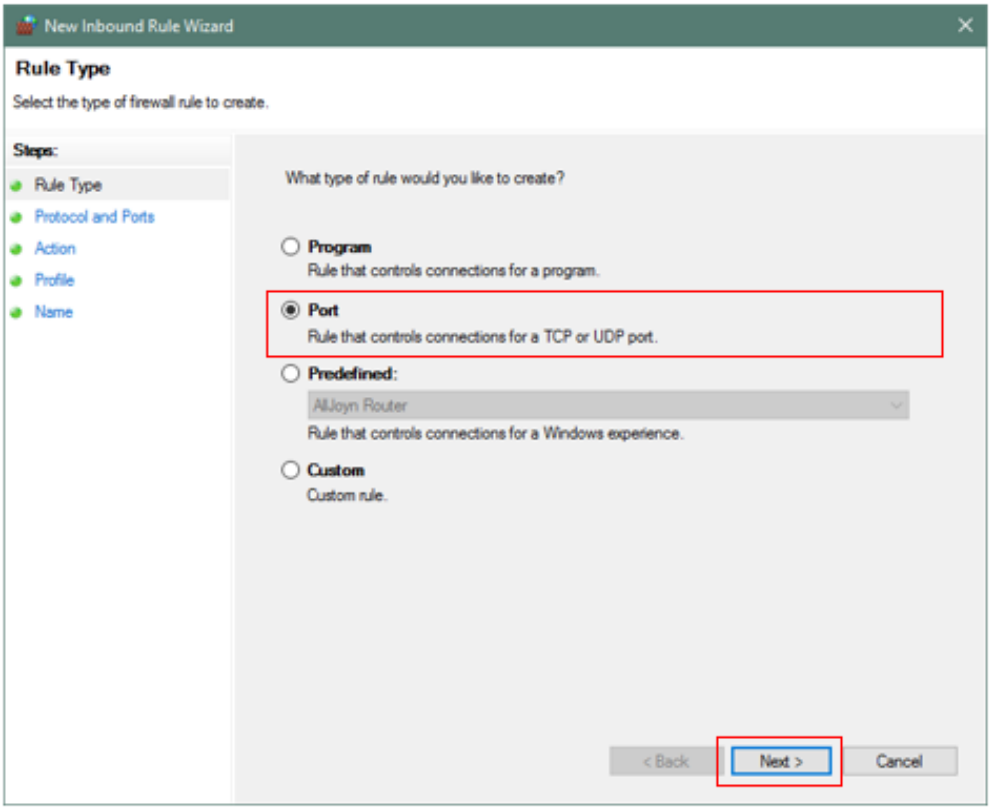
2. Akan muncul program ***Windows Firewall*** seperti terlihat dibawah ini. Pilih menu ***Inbound rules*** pada sisi sebelah kiri:
   *The **firewall** application will show up, select **Inbound Rules** menu on the left side bar.*



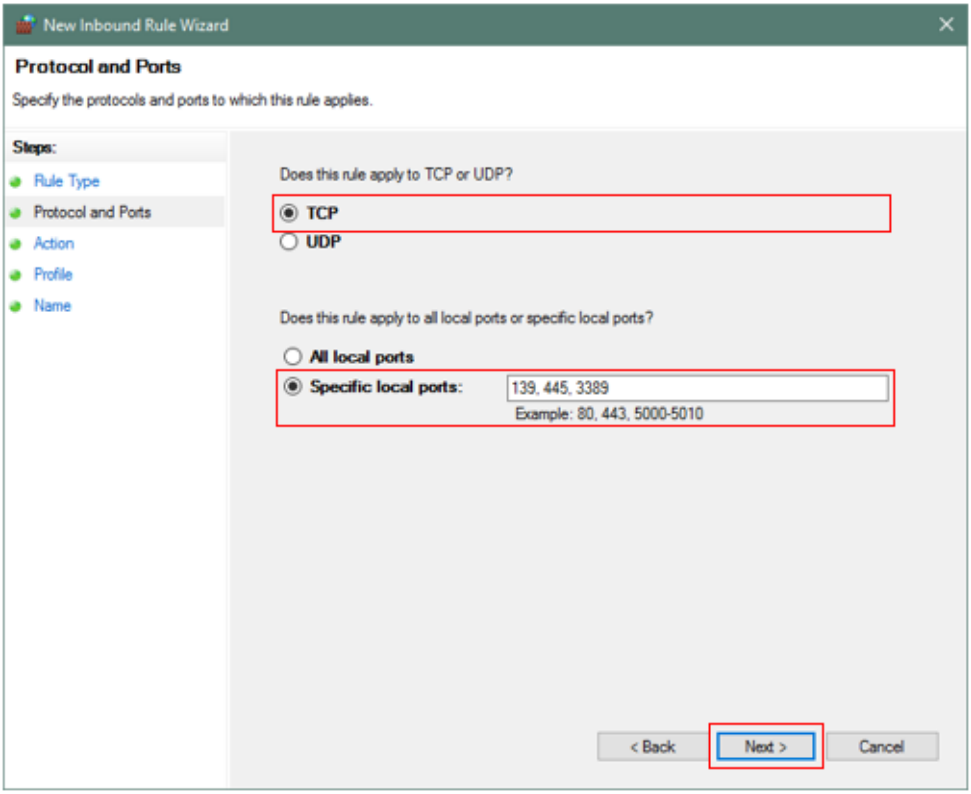
3. Pada deretan menu di atas, tekan menu **Action** lalu tekan menu **New Rule.**
   *On the top menus, select **Action** then press **New Rules** menu.*



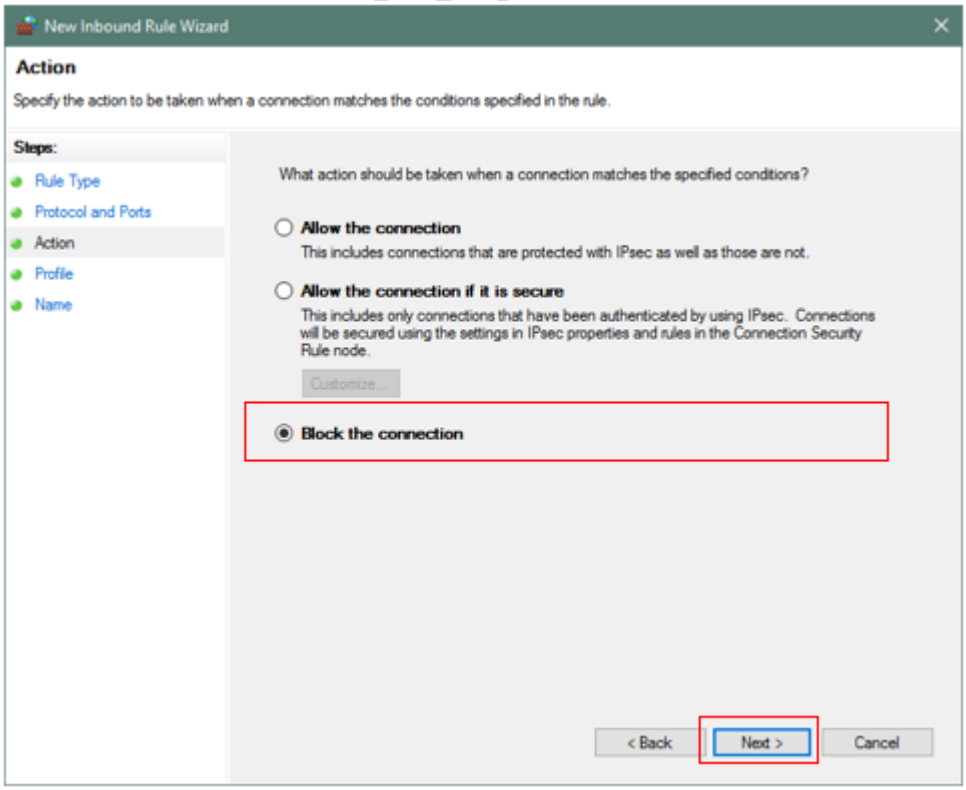
4. Pilih tombol **Port** lalu tekan tombol **Next** di bagian bawah
   *New Inbound window will show up, select **Port** button then press **Next***



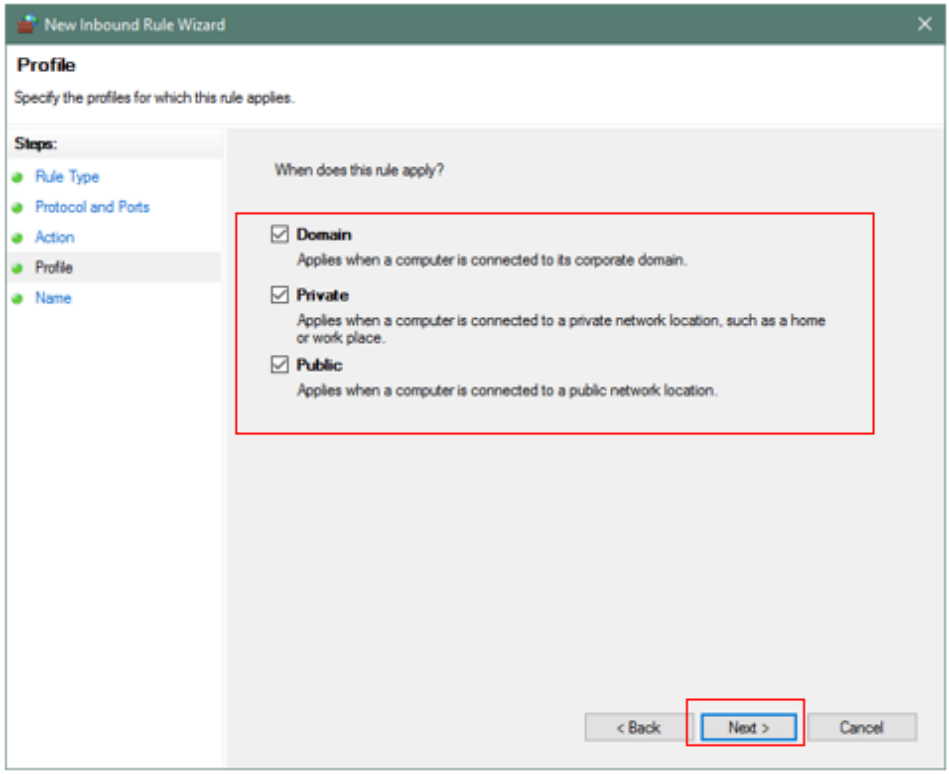
5. Pada bagian atas pilih tombol menu **TCP** lalu di bagian tengah pilih **Specific local ports** dan tuliskan nomor port 139, 445, 3389 pada kolom yang tersedia. Lakukan langkan yang sama untuk protokol **UDP**.
   *Select **TCP** menu on the top and **Specific local ports** on the bottom. Insert port number 139, 445, and 3389 on the text field then press **Next**. Do the same thing for the UDP protocol.*



6. Pada bagian **Action**, pilih tombol **Block the connection** lalu tekan tombol **Next**.
   *On the Action section, select **Block the connection** then press **Next** button.*



7. Pada bagian Profile, centang pilihan koneksi di ketiganya bila diperlukan (**Domain, Private & Public**) lalu tekan tombol **Next.**
   *On the profile section, check all the connection mode if necessary, then press **Next**.*



8. Beri nama **Rules** yang baru anda buat dengan nama apa saja lengkap dengan keterangannya, lalu tekan tombol **Finish**.
   *Give any name to identify your New Rules and fill the description, then press **Finish**. Done.*