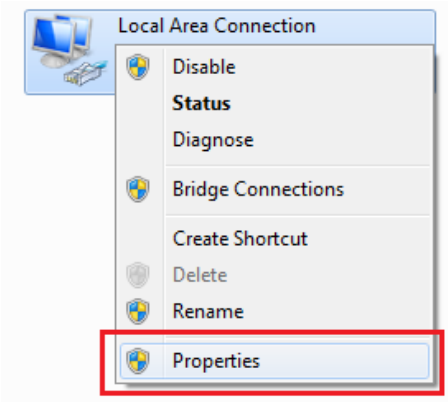
Biến thể Ransomware có tên là WanaCrypt0r 2.0 đang lan rộng thông qua một khai thác được NSA tích cực sử dụng để thâm nhập vào các máy Windows để khai thác. Các khai thác được gọi là EternalBlue cho phép kẻ tấn công truy cập vào máy tính của bạn với các đặc quyền gốc đầy đủ thông qua các giao thức SMB không an toàn, một giao thức để chia sẻ truy cập vào các tập tin, máy in và các thiết bị khác qua các cổng dịch vụ TCP 137, 445 và UDP 138, 139.

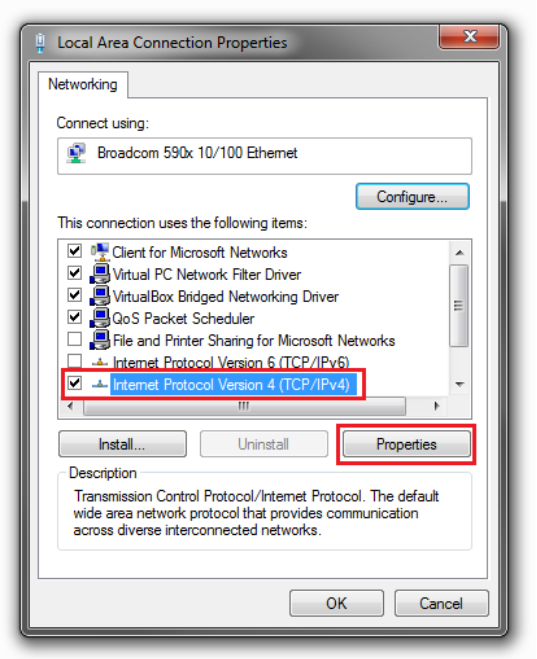
Để tự bảo vệ khỏi ransomware WanaCrypt0r 2.0 khả năng lây nhiễm trên các máy tính nội bộ, ngang hàng, ta cần vô hiệu hóa dịch vụ SMB trên máy tính Windows hoặc đóng các cổng dịch vụ TCP 139, 445 và UDP 137, 138.

I. Vô hiệu hóa tính năng NetBIOS qua TCP/IP:

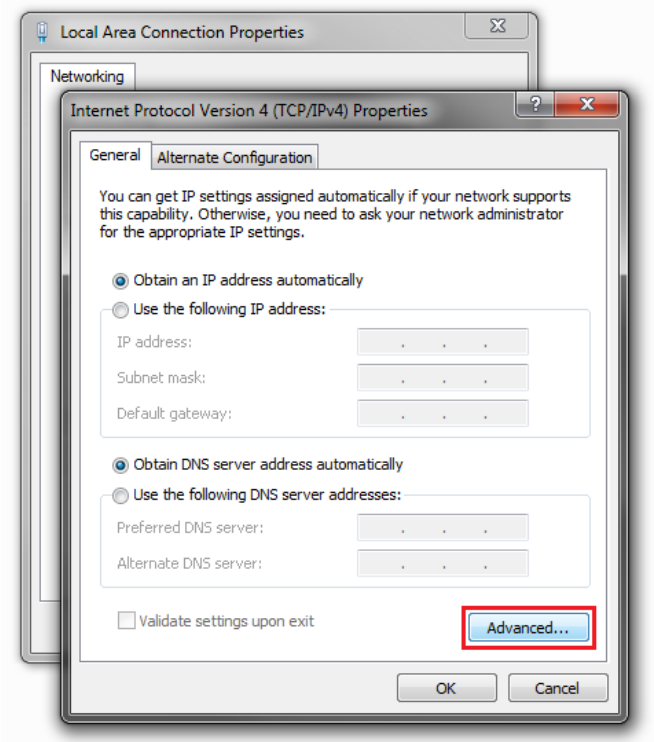
1. Click chuột phải trên card mạng và chọn "Properties"



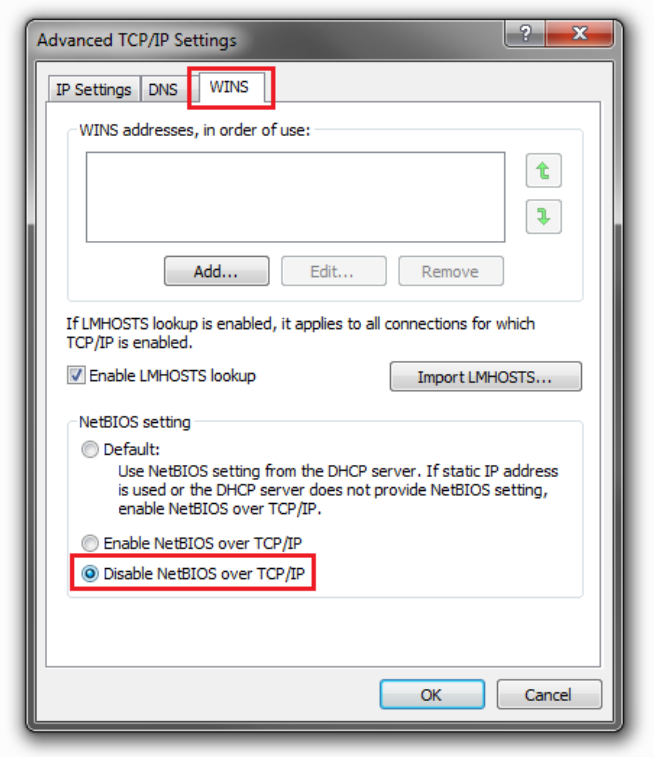
2. Chọn "Internet Protocol Version 4" và Properties. Lưu ý bỏ luôn tính năng File and Printer Sharing for Microsoft Networks để hạn chế việc chia sẻ.



6. Chọn “Advanced”



7. Chọn TAB “WINS” và tắt tính năng tại “Disable NetBIOS over TCP/IP”



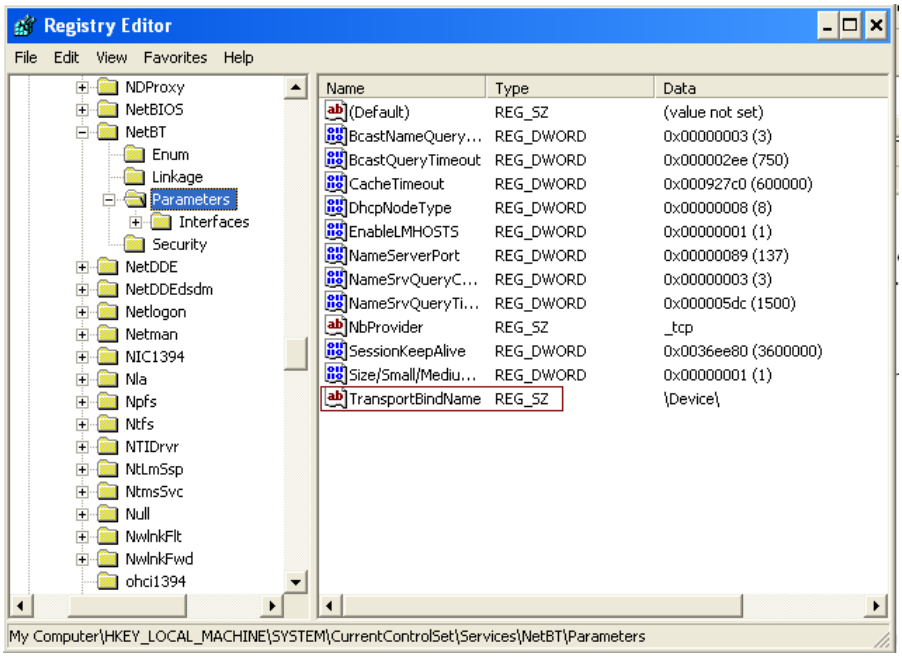
II. Vô hiệu hóa dịch vụ BindName qua cổng 445

1. Mở chương trình biên tập Registry -Registry Editor

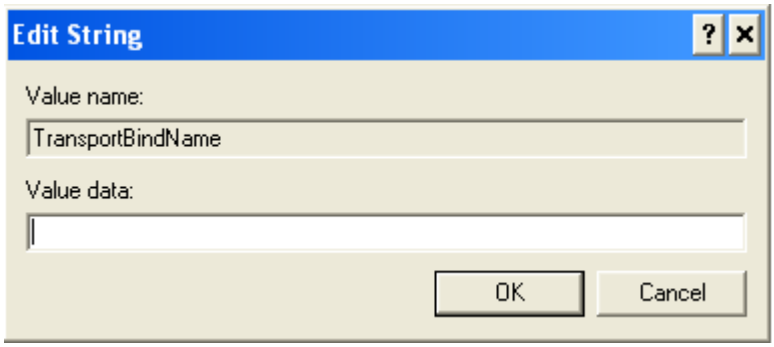
2. Tại Run dùng lệnh Regedit.exe.

3. Tìm đến khóa sau trong Registry:

HKLM/SystemCurrentControlSet/Services/NetBT/Parameters



3.1. Tại cửa sổ Window bên phải chọn một tùy chọn có tên là **TransportBindName**. Double click vào tùy chọn, sau đó xóa giá trị mặc định -default value, và do vậy khung chứa giá trị được để trống -blank value.



3.2. Tại cửa sổ Window bên phải ta tạo thêm một tùy chọn tên là:

SMBDeviceEnabled

với loại DWORD (REG_DWORD) và giá trị bằng 0

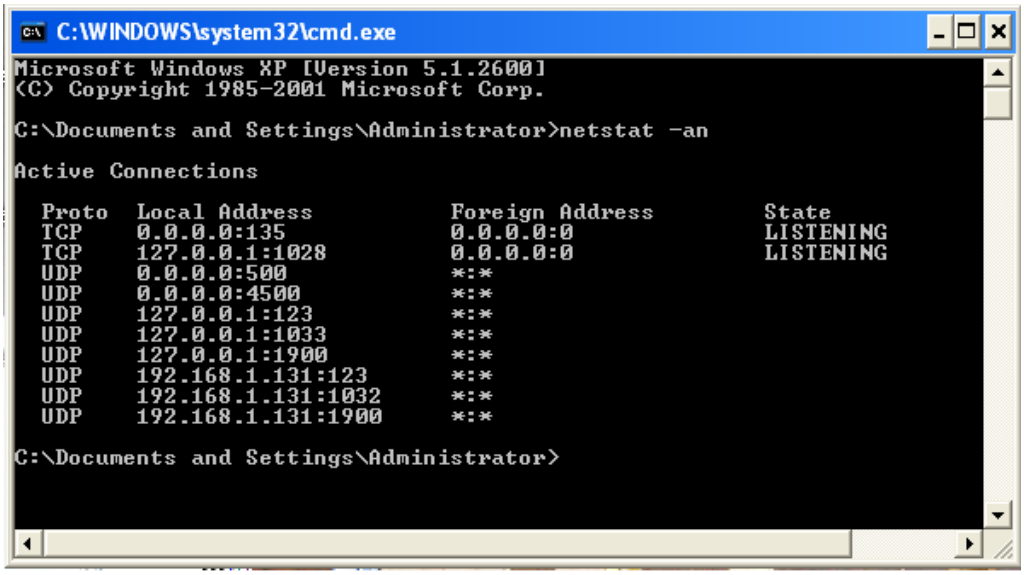
4. Đóng Registry editor.

5. Khởi động lại Computer.

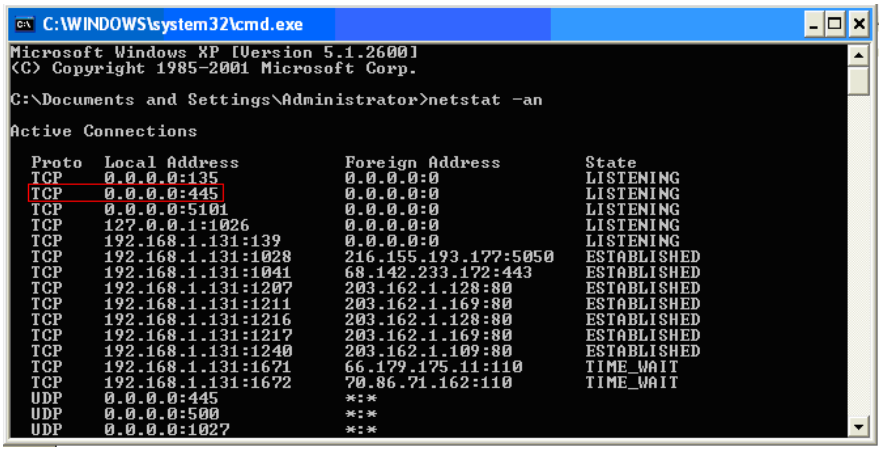
Kiểm tra lại các port đang lắng nghe:

Sau khi khởi động và log-on vào Computer, tại Run, điền lệnh cmd và đưa vào lệnh sau:
netstat –an

Nhận thấy rằng Computer không còn lắng nghe ở port 445.

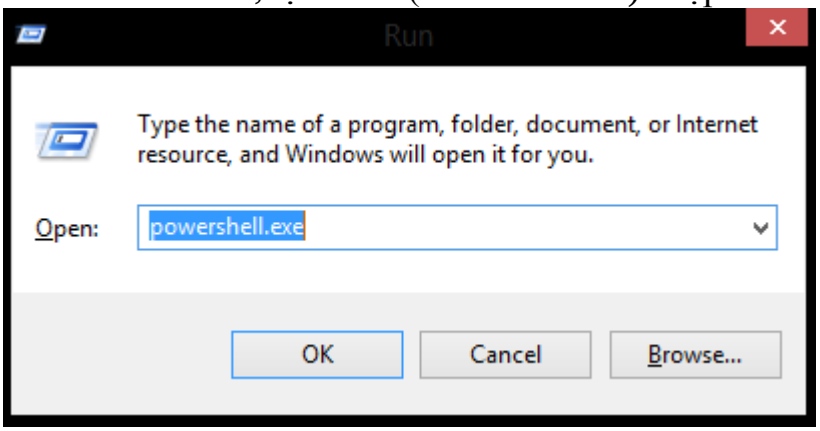


So với trước khi tiến hành Disable port 445, hình bên dưới



III. Vô hiệu hóa dịch vụ SMB

1. Mở chương trình Powershell, tại RUN (Windows + R) nhập PowerShell.exe:



2. Trong cửa sổ PowerShell vô hiệu hóa SMB tùy theo phiên bản Windows:

Trong Hệ điều hành Windows 8 và Windows Server 2012:

- Để vô hiệu hóa SMBv1 ta chạy dòng lệnh sau:

  Set-SmbServerConfiguration -EnableSMB1Protocol $false

- Để vô hiệu hóa SMBv2, v3 ta chạy dòng lệnh sau:

  Set-SmbServerConfiguration -EnableSMB2Protocol $false

Trong Hệ điều hành Windows 7, Windows Server 2008 R2, Windows Vista, và Windows Server 2008:

- Để vô hiệu hóa SMBv1 ta chạy dòng lệnh sau:

  Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force

- Để vô hiệu hóa SMBv2 và SMBv3 ta chạy dòng lệnh sau:

  Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force