**Tấn công hệ thống bằng việc giả mạo MAC address**

**I. Ý tưởng**

Mindset của những người làm hệ thống là kiểu MAC address là thứ không thể thay đổi, nó đã được dính chặt vào NIC (Network Interface Card) nên muốn chặn một thiết bị nào đó là ta sẽ chặn MAC address.

Điều trên gần như chính xác, cho đến khi tôi biết rằng MAC address vẫn có thể thay đổi được trên thiết bị. Tất nhiên là có một chút may mắn, bởi vì các thầy dạy tôi cũng chưa nhắc đến việc này (Có thầy còn xem việc giả mạo MAC address là Hacker cao siêu,...)

Vì vậy tôi nghĩ mình nên vận hành cái này, rồi sau đó tìm ra giải pháp để ngăn chặn cuộc tấn công theo dạng này.

**II. Các cách có thể thay đổi MAC address**

Thật buồn rằng, bởi vì tính chất muốn quản trị hệ thống mạng mà những người cung cấp NIC, họ thật sự cho phép thay đổi MAC address cho tiện việc quản trị.

Ví dụ: Máy tính 1 có MAC là 0200 0000 0001

Máy tính 2 có MAC là 0200 0000 0002

Máy tính 3 có MAC là 0200 0000 0003

Rất là đơn giản là vì với đám MAC address này thì người quản trị có thể dễ nhớ hơn, dễ làm việc hơn hay đặt MAC address vào “white list” (Điều này tôi đúc kết khi thầy tôi nói, mỗi Xlần nhập lô máy thì thường các máy có MAC address khá giống nhau nên các em có thể copy rồi paste cho nhanh)

Tuy nhiên do sự cho phép này, thì một điều khủng lồ có thể xảy ra, đó là hệ thống áp dụng bảo mật như “Port Security”, “White list”, “Black list”, “Timer” và Firewall chặn ở Layer 2 (ngay cả trên router của các bạn cũng có đấy- black list, white list).

Sau đây là các cách thay đổi MAC address:

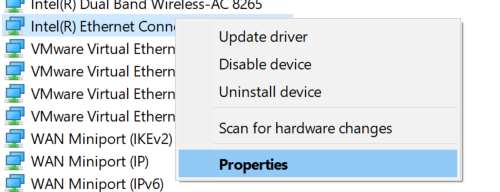
Trên Windows:

Cách 1 (Nếu không được thì qua cách 2-Tại một vài nhà sản xuất NIC không cho phép đổi trực tiếp):

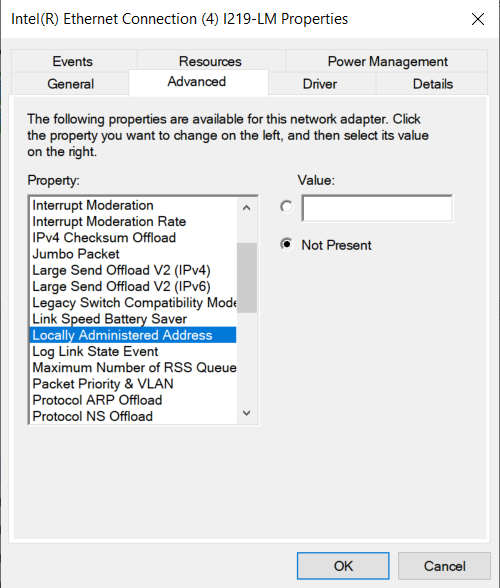
Ctrl+X (Chuột phải lên biểu tượng Windows) -> Device Manager -> Chọn vào mục Network adapters (quản lí card mạng ở đây đây) -> Tiếp theo ta phải biết chọn card mạng nào là của mình (Phân biệt: thường card mạng nó sẽ ghi kèm nhà sản xuất phía trước Intel(R),...).



Đây là 2 card mạng của tôi đây (wireless và Ethernet, không dây và dây)



Chuột phải lên card mạng -> Properties



Vào Advanced -> Chọn Locally Administered Address

(Tới giờ học lí thuyết rồi)

MAC address bao gồm 2 loại:

UAA (Universally Administered Address): Đây là địa chỉ của nhà sản xuất, nó là cái có OUI.

LAA (Locally Administered Address): Còn đây là địa chỉ mà admin cấu hình.

2 loại MAC address này chỉ khác nhau đúng 1 điểm mà được quy định đó là: Bit thứ 7 của MAC address.

Với UAA là bit 0

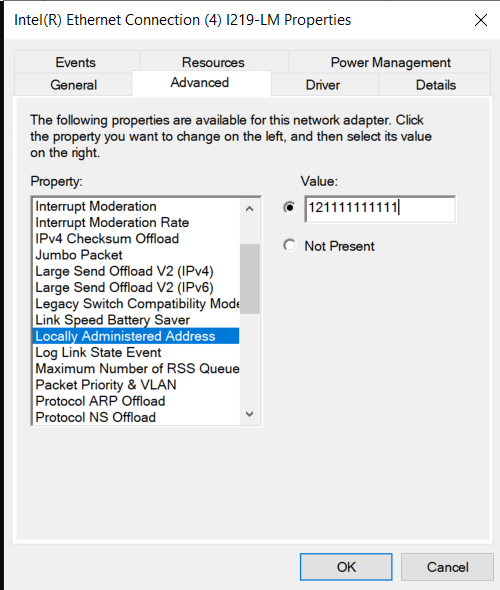
Với LAA là bit 1 (đó là lí do tại sao ta đặt MAC thì buộc nó sẽ phải rơi vào các giá trị: 2,3, 6, A và E)

MAC được viết bởi Hexadecimal (hệ 16), mỗi kí tự sẽ sinh ra từ 4 bits. Vì vậy bit thứ 7 sẽ là ở kí tự thứ 2 trừ trái qua phải.

Nó đây: XXXX.XX**2**X.

(Tốt nhất bạn nên coi về đổi qua lại Binary ra Decimal và hexadecimal cũng như ngược lại)

(Trở lại với thực hành)

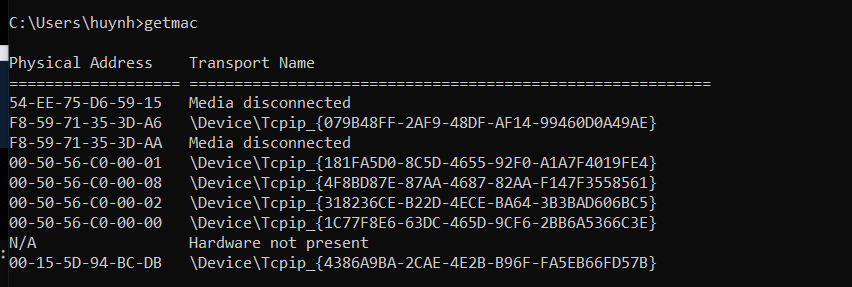


Ta chọn vào Value -> Nhập MAC Address ta muốn thay đổi -> OK (Xong)

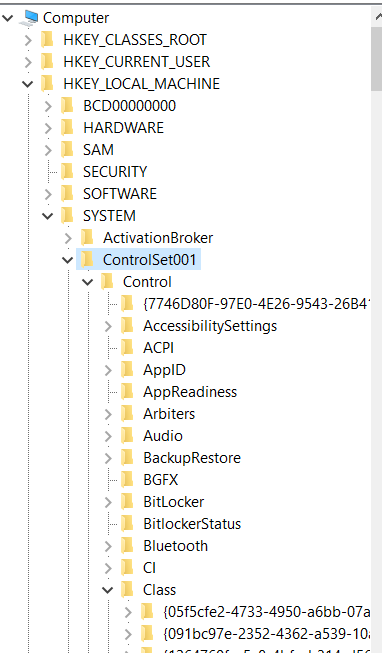
Bạn có thể check bằng: Kiểm tra card mạng ở Network Connections, hay vào CMD gõ “ipconfig /all”

Cách 2:

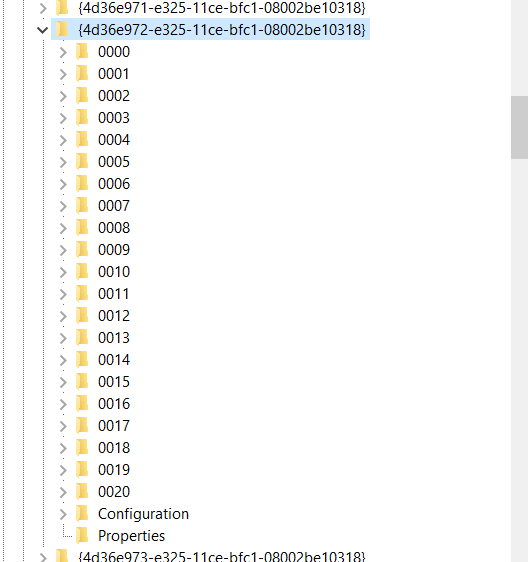
Vào CMD -> gõ “getmac” -> Ta sẽ thấy như thế này:



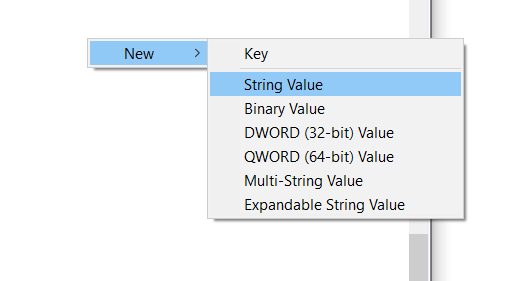
Bao gồm địa chỉ MAC address và Transport Name(Hình thức dịch vụ Tcpip là mô hình TCP/IP, còn media disconnected là do interface này chưa cắm dây) -> Nhớ dãy số đầu ở trong dấu { } tương ứng MAC adress (ở đây tôi chọn 079B48FF)



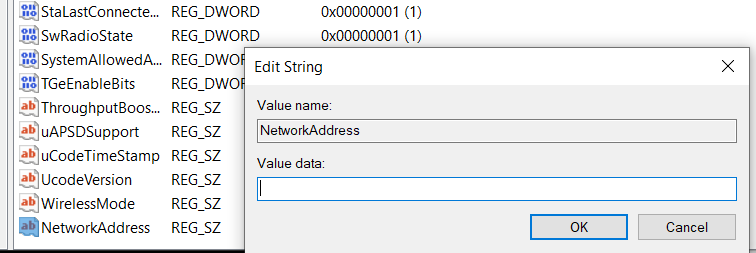
Windows + S (Gõ thanh search cũng được) -> Registry Editor -> Vào HKEY\_LOCAL\_MACHINE/SYSTEM/ControlSet001/Control/Class



Ctrl F gõ “{4D36E972-E325-11CE-BFC1-08002BE10318}” -> Ctrl F gõ “079B48FF” (chọn theo MAC address của bạn nha)

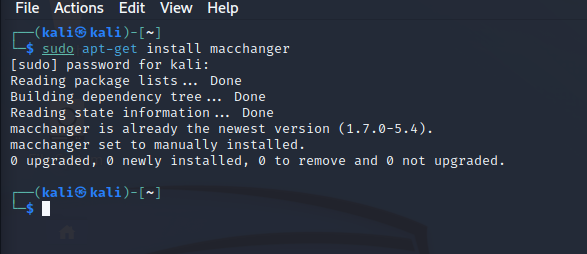


Chuột phải ở trong vùng trống-> New -> string value -> Name “NetworkAddress”

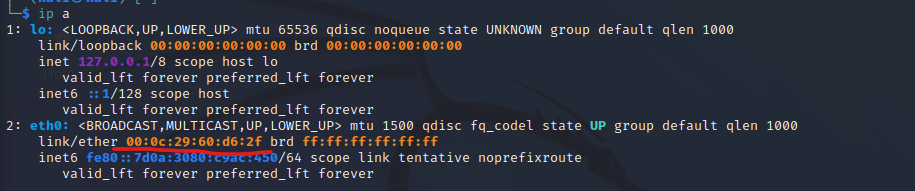


Nháy đúp vào NetworkAddress -> Nhập MAC address mong muốn -> Xong

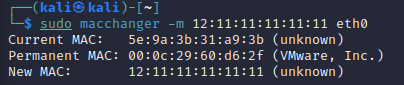
Linux (Ở đây dùng máy Kali):



sudo apt-get install macchanger



Ip a (Để coi MAC address và chọn card mạng ở đây chọn eth0)



sudo macchanger -m “Nhập MAC address muốn đổi” “Nhập tên card mạng”

**Vậy là ta đã biết cách đổi MAC address, vậy giờ việc làm sao dùng cái này để tấn công đây ?**

**III. Ngữ cảnh tấn công**

Hiện giờ thì mình chưa có ngữ cảnh cụ thể, nhưng có thể sơ lược một vài ý để khai thác.

**Ngữ cảnh 1: Áp dụng khi firewall chặn MAC người dùng thực theo chính sách.**

Chẳng hạn, ta vào được hệ thống wireless của một công ty nào đó rồi, ta thực hiện scan port, và con firewall phát hiện ra là ta đang scan port và block MAC ta luôn.

Có thể đổi MAC address để thực hiện scan port, viết script để chạy scan port và đổi mac address liên tục. Có thể áp dụng ngữ cảnh tương tự như: Firewall hay router giới hạn thời gian sử dụng dịch vụ,...

**Ngữ cảnh 2: Tấn công bằng MAC snoofing**

Nên nhớ nó chỉ chạy được trên mấy máy dùng Linux thôi (Như đã nói ở trên về UAA, và LAA). Giờ ta có thể fake MAC address của các thiết bị trong mạng nội bộ. Làm thay đổi ARP của router, và MAC Table của switch (nếu ta được kết nối dây với switch). Nhờ vậy có thể vượt qua được hàng rào bảo mật, đặc biệt về Port security (switch), hay filter MAC address(firewall và router), cũng như do ARP table và MAC address table bị thay đổi, các gói tin giờ sẽ được chuyển về thẳng máy của ta.

Hoặc là ta có thể làm giả là một con wireless router khác, bằng việc giả mạo MAC address của con wireless router của công ty. Ta có thể cung cấp một con malware nếu cần.

**Ngữ cảnh 3: Ta có thể dùng nhiều MAC Address trên một card mạng để buộc DHCP phải cấp liên tục các IP address**

(Chưa thử)

**IV. Giải pháp**

Do vấn đề về MAC này cũng thường khó xảy ra, vì buộc kẻ tấn công phải tới tận công ty chúng ta. Tuy nhiên nó nhắc ta nhớ rằng nếu chỉ bảo vệ theo phương pháp filter MAC address thì chưa bao giờ là đủ, vì vậy tốt hơn hết ta nên hạn chế dùng DHCP ở một số khu vực. Nghĩa là Static IP address và MAC address phối hợp dùng trong quản trị.

Tiếp theo, đừng lấy MAC address để quản lí nữa, tốt nhất đừng chỉnh sửa nó. Bởi vì nếu MAC address đã thành LAA, nghĩa là bất cứ ai cũng có thể sao chép nó. Tuy nhiên nếu nó là UAA, thì gần như rất khó và có thể là không sao chép được (đó là lí do có sự khác nhau ở vị trí bit thứ 7), và các nhà sản xuất NIC, người ta cũng không cho phép việc chỉnh sửa MAC address ở bit thứ 7 đâu.

Đề tài này có thể mở rộng ở một vài điểm, như tấn lấy MAC address (rất dễ ta hoàn toàn có thể biết được thông qua ARP table, tuy nhiên cái này sẽ không được đề cập, ít nhất là bây giờ), và thêm rằng chúng ta có thể nghĩ ra một vài ngữ cảnh như ở phần ngữ cảnh 3, sẽ thế nào nếu ta làm cho toàn bộ IP address của hệ thống bị dùng hết (thường các công ty dùng DHCP, và họ rất ít cấu hình tay cho đám Ip address này).

DONE, nội dung sẽ được cập nhật tiếp ở tương lai.