

HƯỚNG DẪN ĐẢM BẢO AN TOÀN KHI QUẢN TRỊ TỪ XA DÙNG REMOTE DESKTOP

1. Sử dụng tên toàn khoản và mật khẩu mạnh

Thay vì đặt tên tài khoản là tên bản thân, bạn bè, gia đình thú cưng... Hoặc những tài khoản mặc định như Admin thì hãy đổi tên tài khoản khác.

Khi sử dụng mật khẩu, cần đặt mật khẩu :

- Chứa 8 ký tự trở lên;
- Chứa các ký tự từ 2 trong 3 trường ký tự như sau :
 - + Bảng chữ cái (ví dụ: a->z, A->Z)
 - + Số (0->9)
 - + Các ký tự đặc biệt (:! @ # \$% ^ & * () _ + | ~ - = \ ` { } [] : " ; ' < > ? , . /)
- Mật khẩu không nên bao gồm:
 - + Tên username
 - + Các cụm từ xuất hiện trong từ điển
 - + Đánh vắn ngược

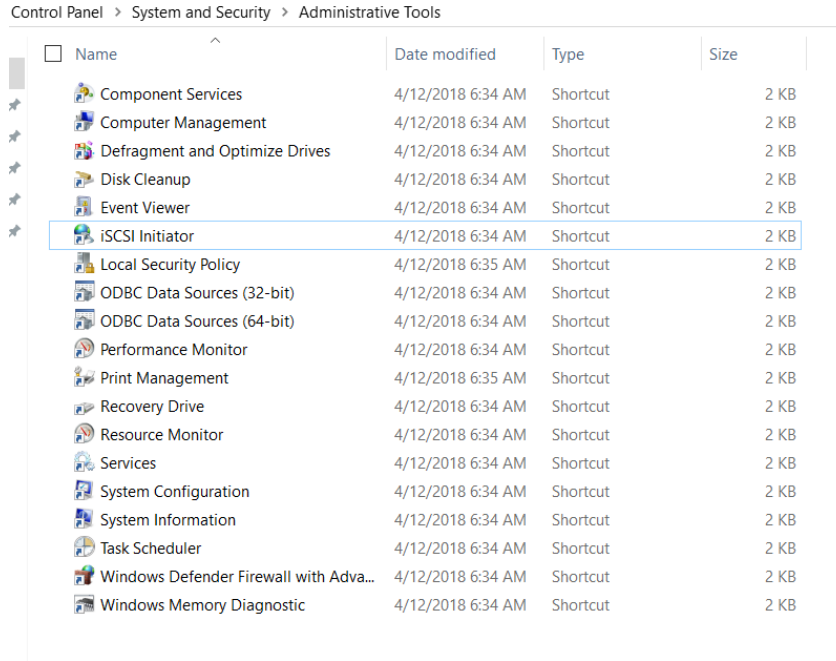
2. Giới hạn số lần đăng nhập sai

Các cuộc tấn công RDP cần phải dùng hàng ngàn, triệu lần đăng nhập liên tục. Vì vậy có thể tăng thời để thực hiện tấn công lên rất nhiều lần thì nên khóa người dùng sau một số lần đăng nhập sai nhất định trong 1 khoảng thời gian nhất định

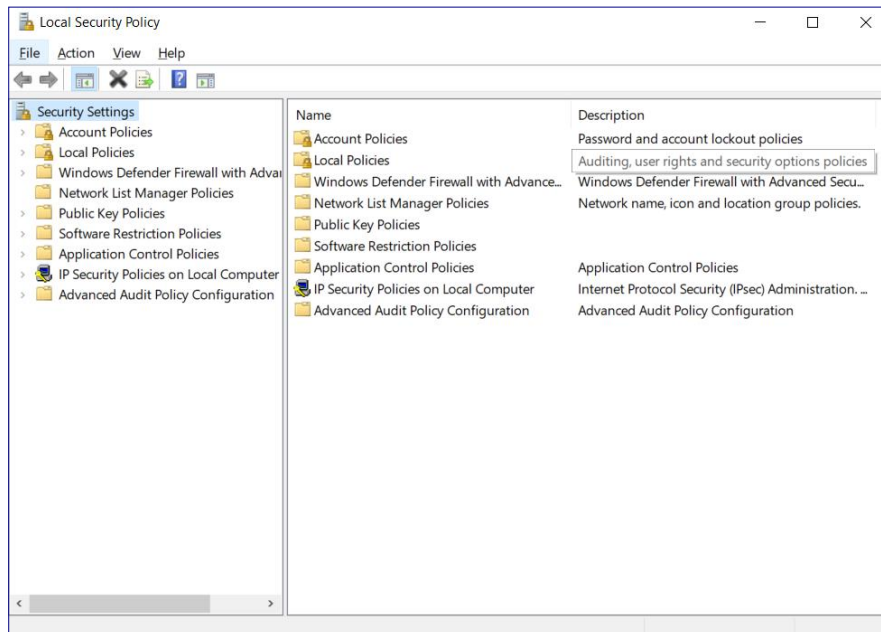
Cách thiết lập giới hạn:

Mở Administrative Tools

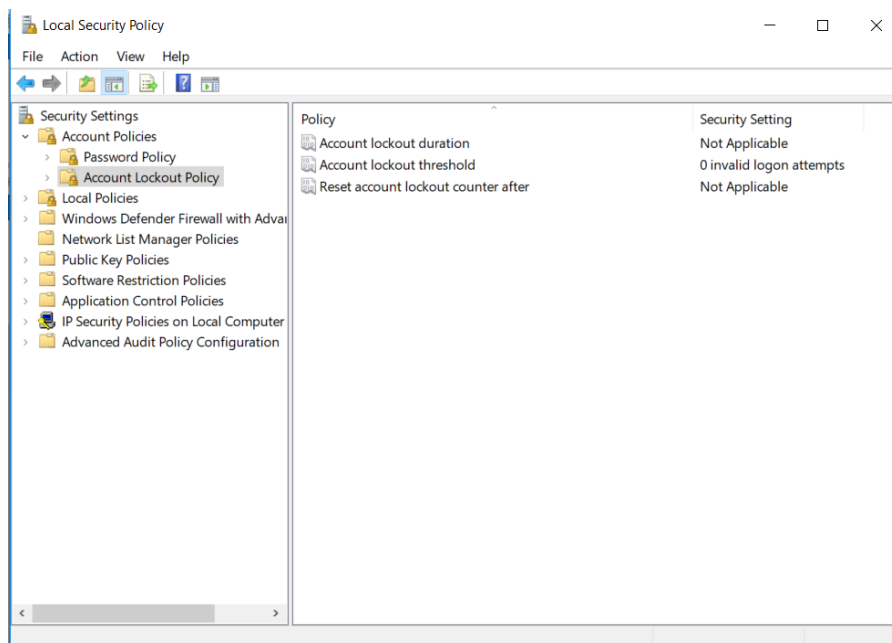
- **Control panel -> System and Security -> Administrative Tools**



- Mở Local Security Policy



- Mở tab Account Policies rồi bên trong mở tab Account Lockout Policy



- Kích hoạt giới hạn ở phần **Account Lockout Threshold**
- Chỉnh thời gian khóa tại tab **Account Lockout Duration**

3. Thay đổi cổng RDP

- Khi quét, Hacker thường tìm kiếm các kết nối sử dụng cổng RDP mặc định (TCP 3389). Chúng ta có thể ẩn các kết nối RDP của mình bằng cách thay đổi cổng sang cổng khác. Tuy nhiên cần lưu ý tránh xung đột cổng kết nối với phần mềm khác (như cổng 80 – HTTP , cổng 443 – HTTPS ...)

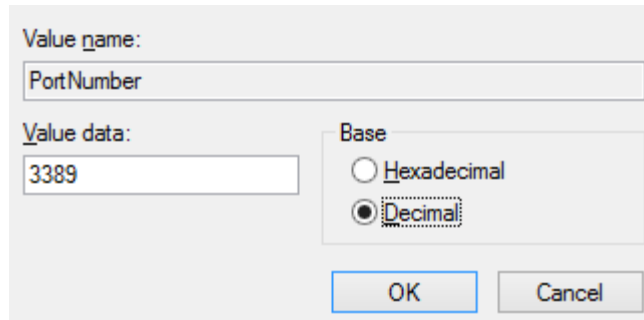
- Cách thực hiện:

+ Vào **Start**, chọn **Run** (hoặc bấm phím **Windows + R**)

+ Tìm đến đường dẫn:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

Click đúp vào PortNumber và chọn Decimal sau đó nhập vào số port cần thay đổi ở mục Value data:



4. Triển khai giải pháp bảo đảm an toàn khi truy cập từ xa

- Nếu cần truy cập quản trị server từ xa dùng Remote Desktop, ưu tiên sử dụng kênh kết nối VPN
- Kênh kết nối VPN có thể triển khai trên các hệ thống Windows Server hoặc các thiết bị Firewall chuyên dụng.