Giới thiệu

Powershell hiện nay trên Windows hiện nay là một công cụ mạnh nhất, mạnh hơn cả command line. Bởi vì nó được dùng để thực hiện các lệnh của Windows Server một cách nhanh chóng.

Ví dụ: Nếu ta có thể chạy powershell bằng scripts để thực hiện các quyền “Run as Administrator” thì sao, vậy là ta đã vượt qua được quy định của Windows về mỗi lần truy cập click Yes. Nhờ đó có thể truy xuất dữ liệu hay tấn công hệ thống một cách dễ dàng.

Việc viết scripts cho ta cơ hội về quản lí, và thực hiện các feature của Windows một cách nhanh chóng, và hiệu quả hơn về mặt tốc độ, cũng như ta hiểu mình đang làm gì trên hệ thống. Song song đó giúp ta hiểu các cách thức để lợi dụng nhằm mục đích tấn công.