BẢO MẬT CỔNG 445 TRONG WINDOWS 2000/XP/2003

Trên các hệ thống Windows 2000, XP và Windows Server 2003 có một số cổng mới được sử dụng, trong số đó, cổng (port) 445 TCP dùng cho dịch vụ SMB truyền qua TCP. SMB (Server Message Block) được sử dụng cho mục đích chia sẻ file. Trên các hệ thống Windows NT cũ nó vận hành với

Trên các hệ thống Windows 2000, XP và Windows Server 2003 có một số cổng mới được sử dụng, trong số đó, cổng (port) 445 TCP dùng cho dịch vụ SMB truyền qua TCP. SMB (Server Message Block) được sử dụng cho mục đích chia sẻ file. Trên các hệ thống Windows NT cũ nó vận hành với NetBT (NetBIOS over TCP/IP), sử dụng các port thông dụng như 137, 138 (UDP) và 139 (TCP). Trên các hệ thống Windows 2000/XP/2003, Microsoft hỗ trợ khả năng vận hành trực tiếp SMB qua TCP/IP (port 445), không cần qua NetBT. NetBIOS cho phép thực hiện đơn giản việc chia sẻ file qua mạng nội bộ (LAN), tuy nhiên đó lại là mối nguy hiểm tiềm tàng khi hệ thống kết nối WAN hay Internet. Tất cả thông tin về mạng (như tên miền) và tài khoản truy cập mạng nội bộ của bạn đều có thể bị thu thập. Cấm NetBT Trên Windows 2000/XP/2003 tiến hành cấm NetBT như sau: Nhấn phải chuột vào biểu tượng My Network Places tại Desktop sau đó chọn Properties; tiếp tục nhấn phải vào Network Card, chọn Properties; kế tiếp, nhấn vào Internet Protocol (TCP/IP) và Properties; rồi nhấn vào Advanced và chọn tab WINS. Tại đây bạn chọn Disable NetBIOS over TCP/IP, thay đổi có hiệu lực ngay, không cần phải khởi động lại hệ thống. Lưu ý, các máy tính chạy HĐH trước Windows 2000 sẽ không thể định vị, tìm kiếm hoặc thiết lập kết nối chia sẻ file và in ấn đến các máy tính Windows 2000/XP/2003 khi NetBT bị cấm. Cấm cổng 445 Theo báo cáo của SANS.Org, port này có tần suất bị tấn công cao nhất (thông tin chi tiết tại http://isc.sans.org/port_details.php?port=445). Port 445 có thể cấm theo các bước sau: 1. Mở trình Registry Editor: vào Run, gõ regedit. 2. Tìm đến khóa HKLM\System\CurrentControlSet\Services\NetBT\Parameters 3. Trong cửa sổ bên phải, chọn TransportBindName. 4. Nhấn đúp chuột (hay gõ Enter) và xóa giá trị của biến này (khung Value data được để trống). 5. Đóng Registry editor 6. Khởi động lại máy tính Sau khi khởi động và đăng nhập vào máy tính, tại Run, gõ lệnh cmd và nhập lệnh sau: netstat -an Bạn sẽ thấy máy tính không còn "lắng nghe" ở port 445. Khi nào Windows 2000/XP/2003 dùng port 445 và khi nào dùng 139? Để đơn giản, tôi dùng thuật ngữ "client" để chỉ máy tính truy xuất các nguồn tài nguyên mạng như ổ đĩa và các file được chia sẻ tại "server" - máy tính có nguồn tài nguyên. Nếu server có NetBT được bật, nó sẽ lắng nghe trên port 137, 138 (UDP) và trên port 139, 445 (TCP). Nếu NetBT bị cấm, server chỉ lắng nghe trên port 445 (TCP). Nếu client có NetBT được bật, nó sẽ luôn thử kết nối đến server đồng thời tại port 139 và 445. Nếu nhận được phản hồi từ port 445, nó sẽ gửi phản hồi đến port 139 và tiếp tục phiên giao tiếp SMB chỉ với port 445. Nếu không nhận được phản hồi từ port 445, nó sẽ tiếp tục giao tiếp SMB chỉ với port 139, khi nhận được thông tin phản hồi từ port này. Nếu không nhận được bất cứ phản hồi nào từ 2 port trên, kết nối sẽ kết thúc. Khi client có NetBT bị cấm, nó sẽ luôn kết nối đến server tại port 445. Nếu server trả lời trên port 445, kết nối sẽ được thiết lập. Nếu không nhận được trả lời, kết nối kết thúc. Ho Viet Ha Network Information Security Vietnam NetworkSecurity@Nis.com.vn