Nguyễn Phước Thành

B1610669

THỰC HÀNH AN TOÀN HỆ THỐNG – BUỔI 3

--- o0o ---

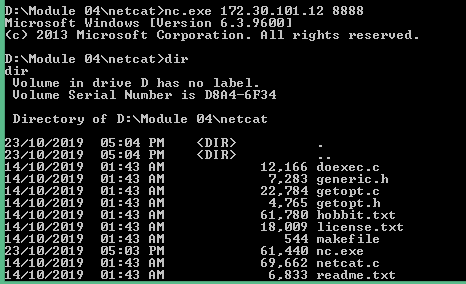
***SỬ DỤNG NETCAT:***

**1. Tiến hành chạy netcat trên máy nạn nhân**:



Mở cổng 8888 và lắng nghe, sau khi có kết nối thì chạy chương trình CMD.

**2. Sử dụng netcat để connect vào máy nạn nhận:**

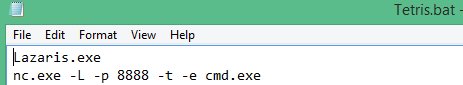


**3. Kiểm tra taskmanager trên máy nạn nhân:**

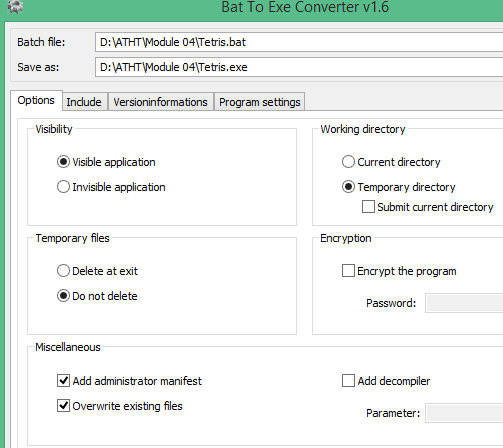


**3. Tiến hành hành kết hợp netcat với 1 chương trình xịn xò:**

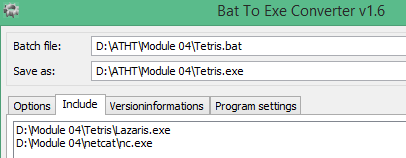
**+** Chuẩn bị file kịch bản:



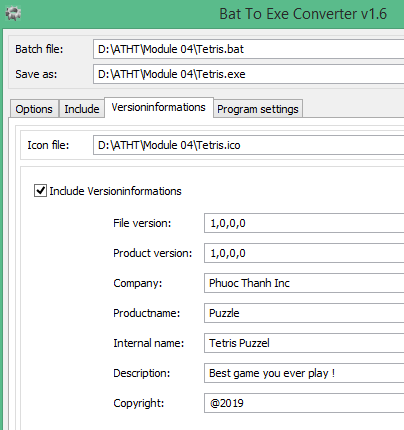
+ Lựa chọn option:



+ Thêm các đường dẫn chứa các file cần thiết: Chương trình xịn xò và chương trình trojan.

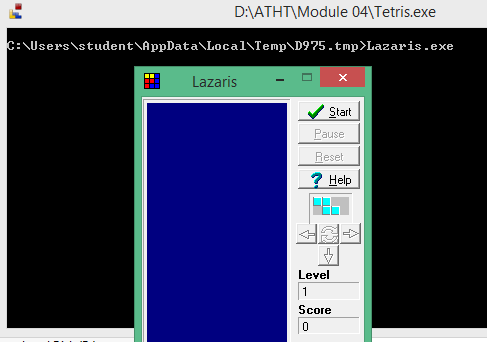


+ Tạo các chứng chỉ, tên giả:

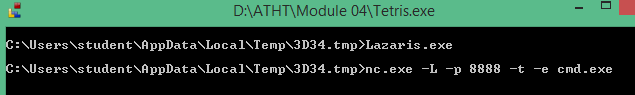


+ Tiến hành dịch chường trình. (chương trình khi thực thi sẽ show CMD để quan sát).

+ Đưa vào máy nạn nhân và kiểm tra kết quả như bước 1 và 2 sau khi nạn nhân khởi động chương trình xịn xò.

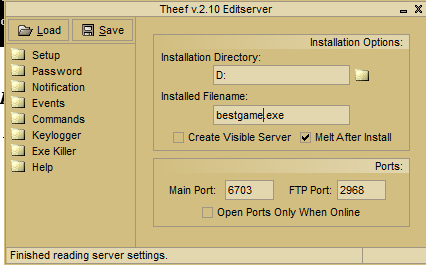


+ Sau khi nạn nhân click thoát chương trình thì chường trình TROJAN sẽ được kích hoạt

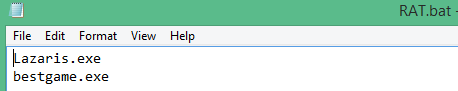


***SỬ DỤNG REMOTE ACCESS TROJANS(RAT):***

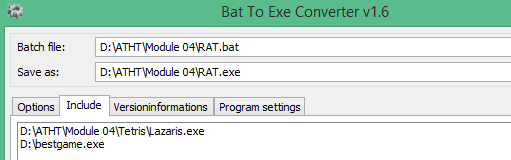
**1. Edit server với cửa sổ chọn:** bằng cách tạo ra file thực thi Trojan



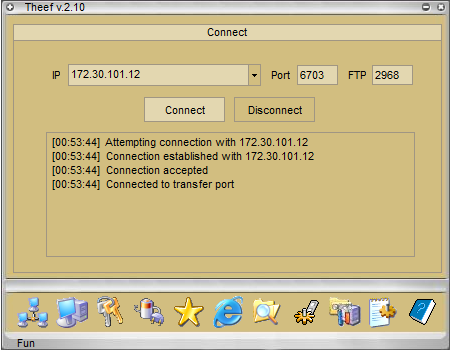
**2. Tạo file .bat với mục đích đóng gói chương trình trojan và game xịn xò:**



**3. Tiếp tục với chương trình đóng gói (**thêm vào các đường dẫn cần thiết**):**



**4. Sau khi người dùng thực thi file RAT.exe, và kết thúc chương trình, ta có thể tiến hành truy cập vào máy nạn nhân thông qua giao diện client102:**



**6. Sau khi connect ta có thể thao tác với hệ thống theo nhu cầu**