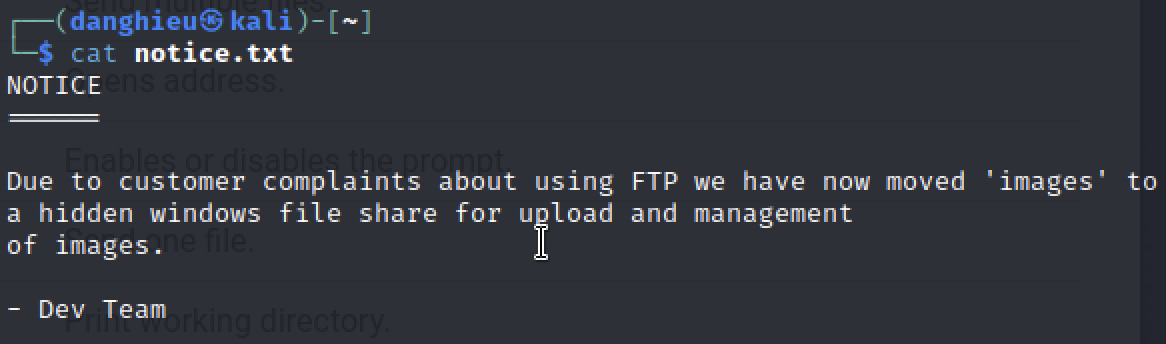
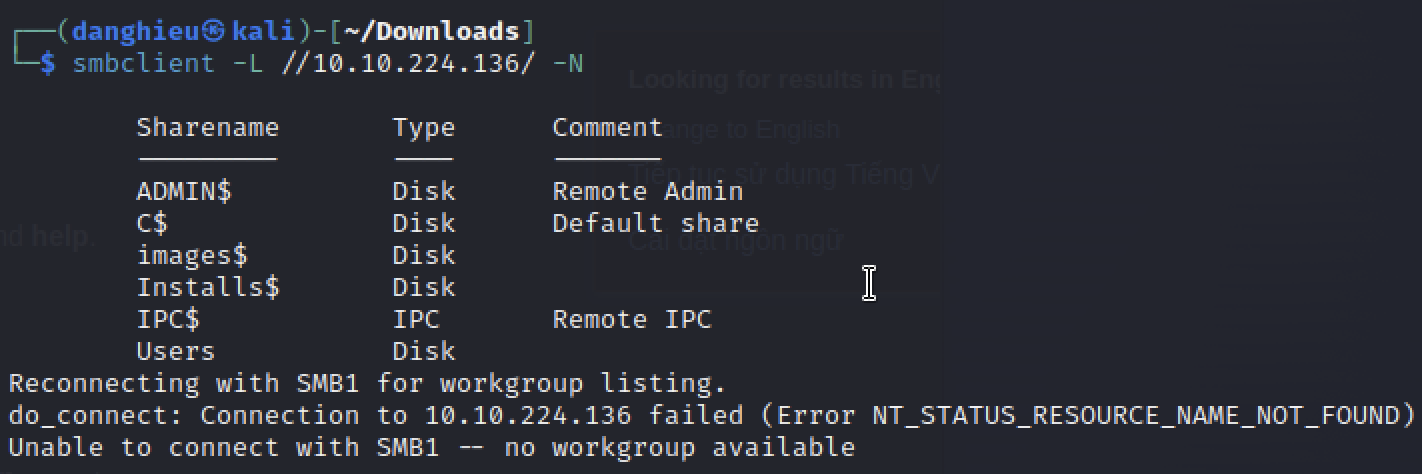
**Enumeration**

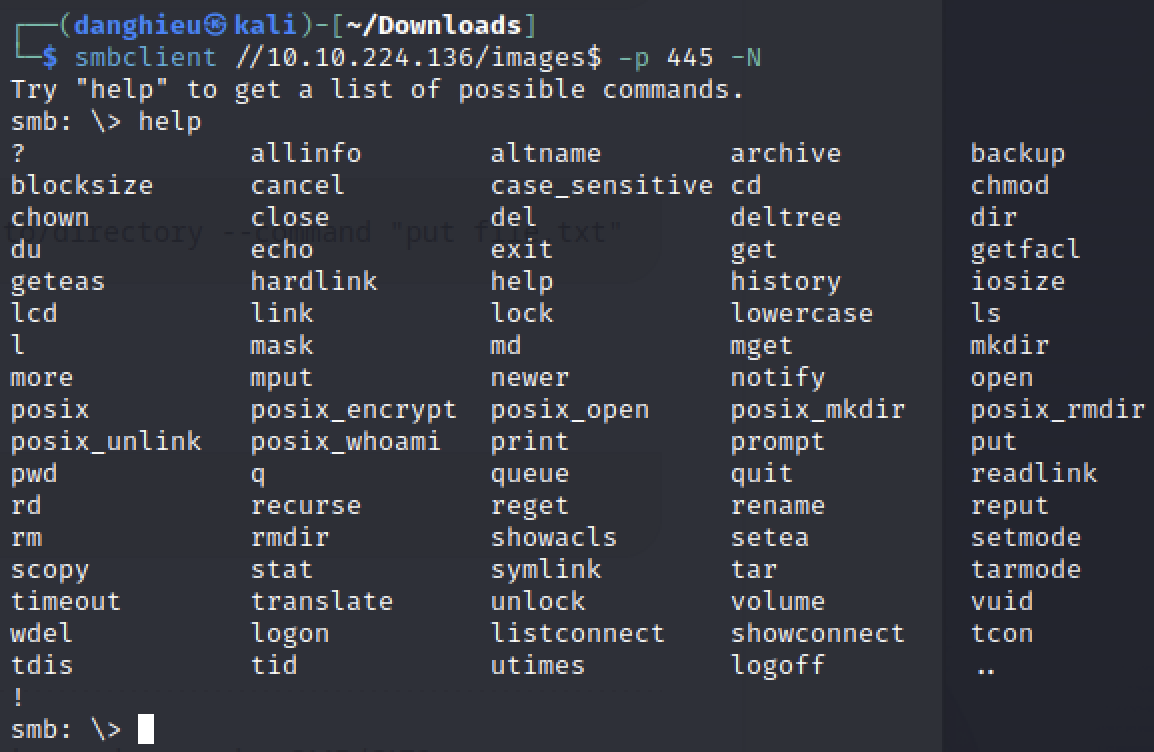




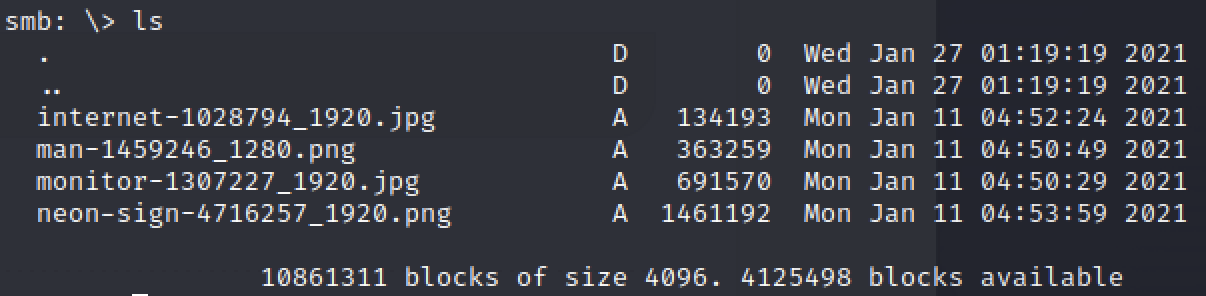
Với gợi ý như vậy, mình sẽ kiểm tra các shares trên máy chủ SMB:

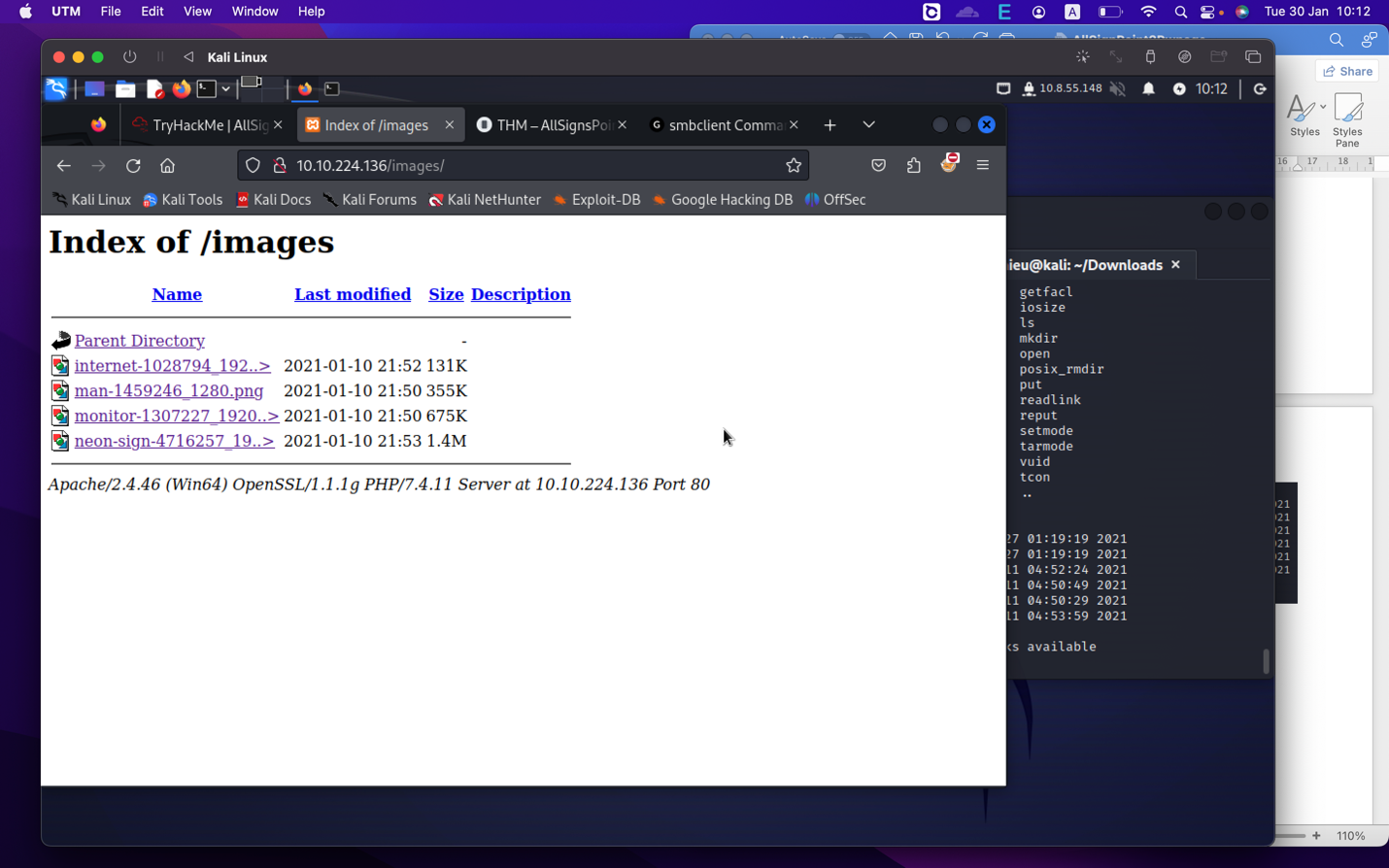


**Gaining a Foothold**

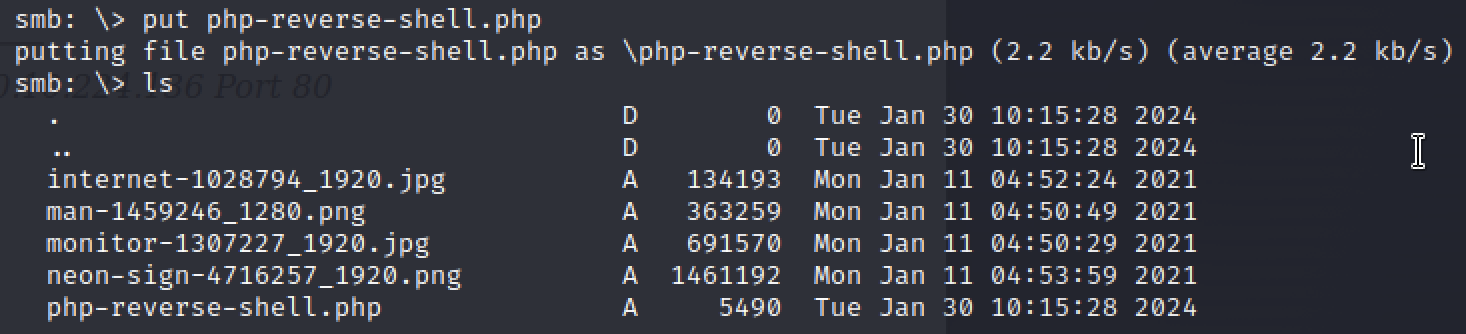


Bạn thấy thư mục images giống với share và images có thể truy cập được

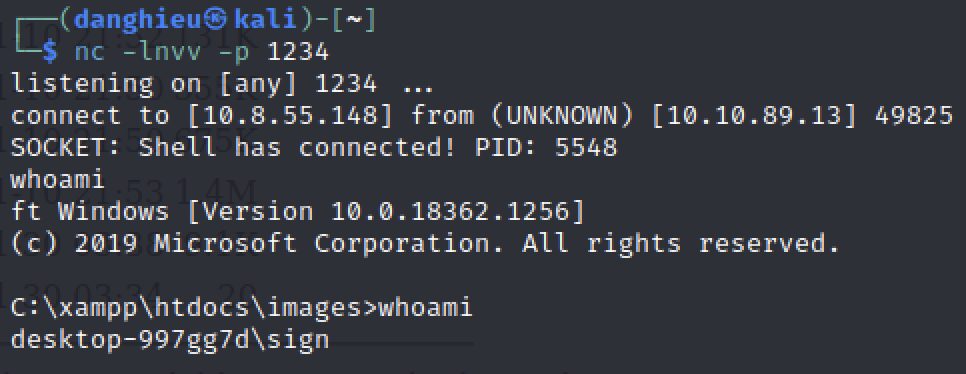


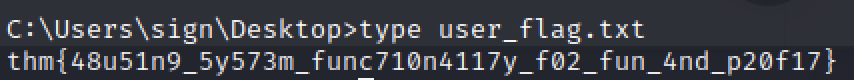


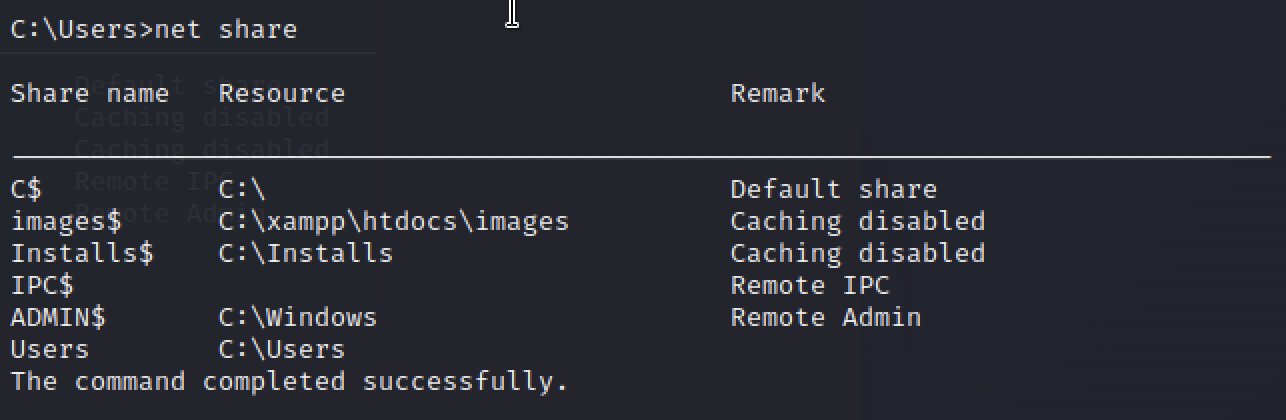
Nên mình sẽ upload 1 reverse-shell lên share images$



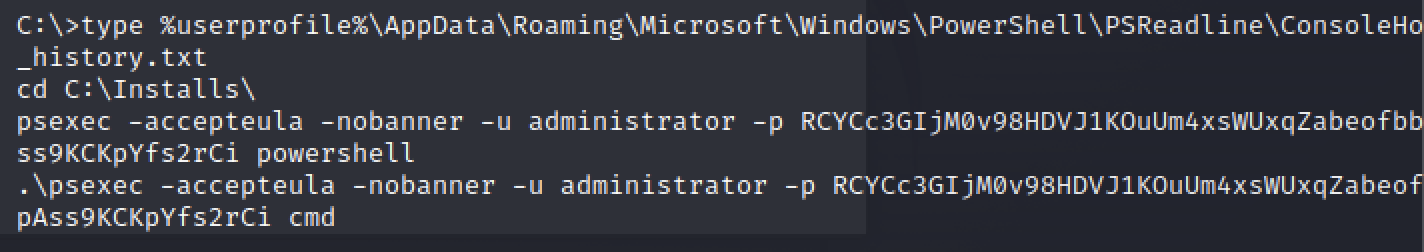
Mình upload rất nhiều reverse shell nhưng không spawn thành công cho đến khi chọn payload của Ivan Sincek.



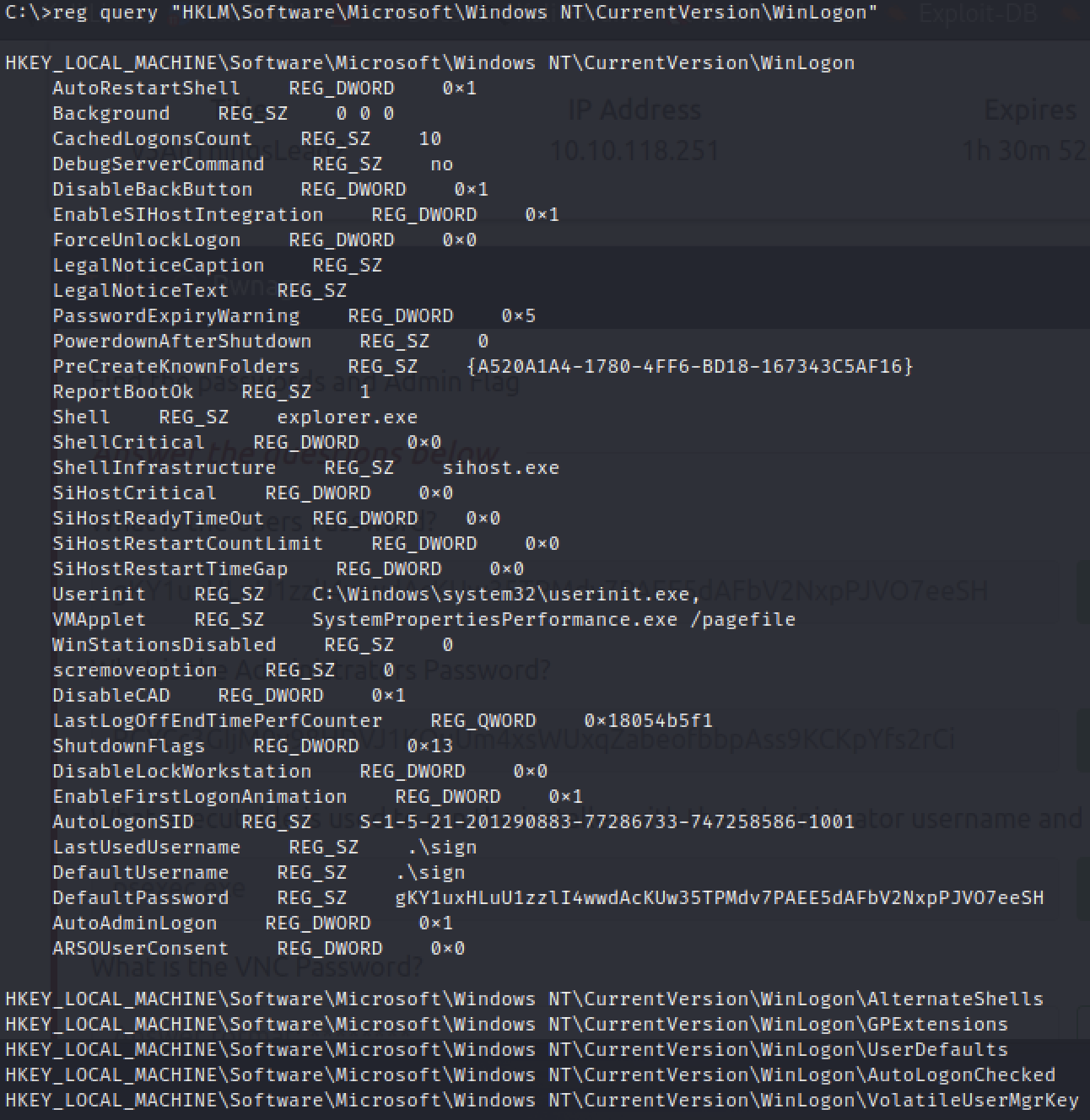




**Pwnage**

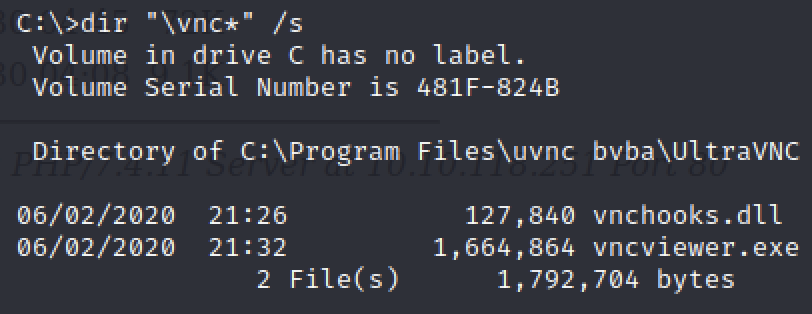


Mật khẩu của Administrator: RCYCc3GIjM0v98HDVJ1KOuUm4xsWUxqZabeofbbpAss9KCKpYfs2rCi

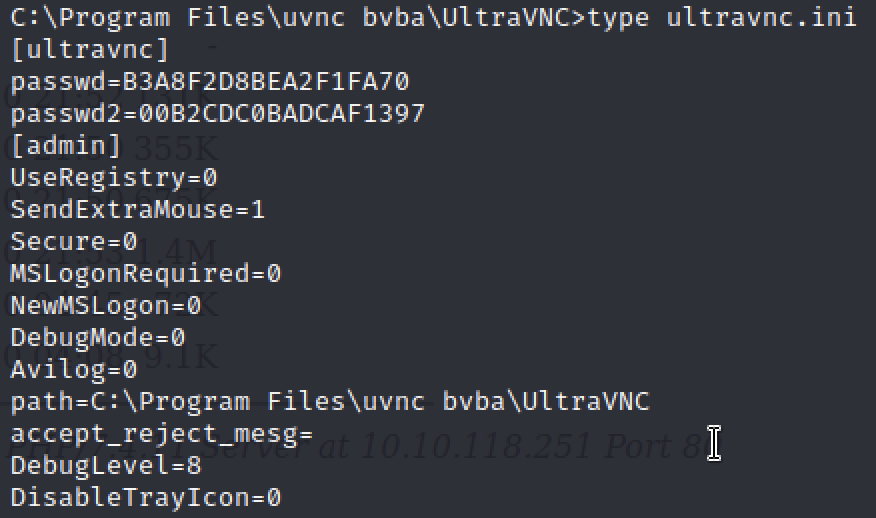


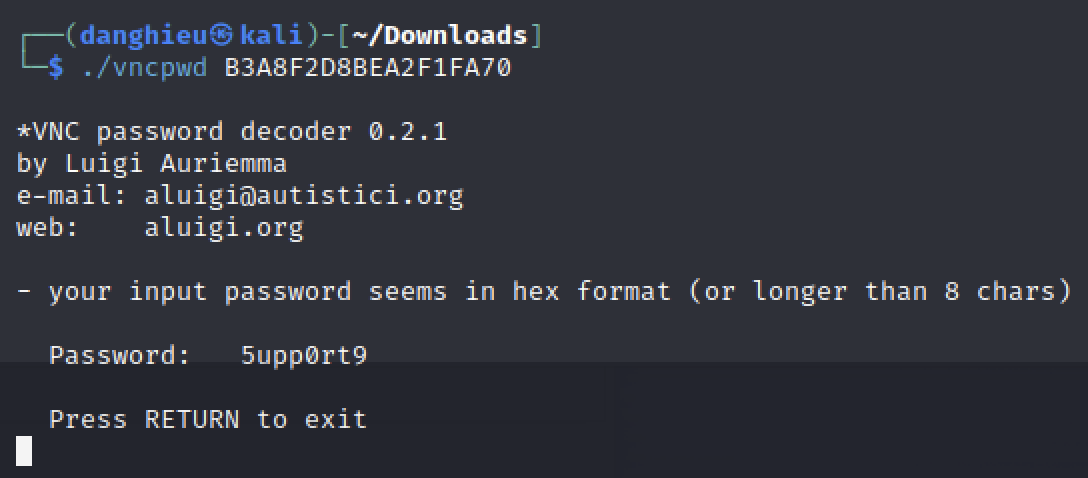
Mật khẩu của user: gKY1uxHLuU1zzlI4wwdAcKUw35TPMdv7PAEE5dAFbV2NxpPJVO7eeSH

Để tìm được mật khẩu của vnc:



Mình vào thư mục UltraVNC, đọc file cấu hình:

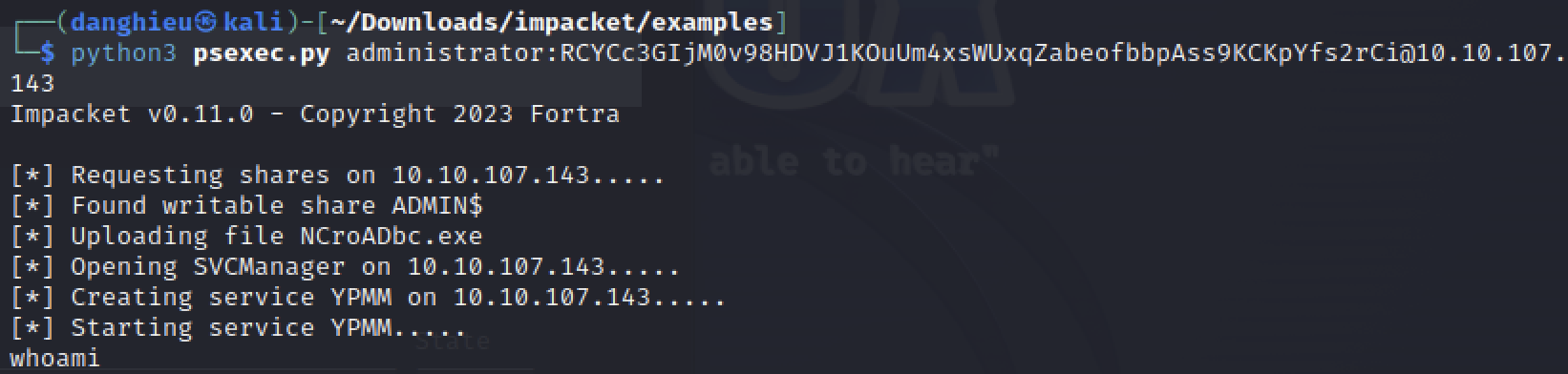




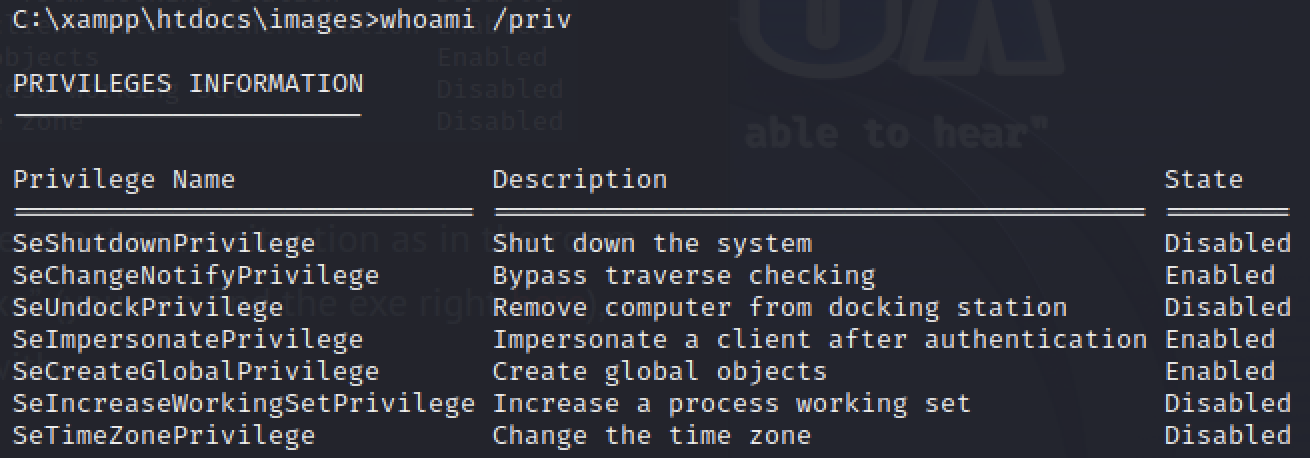
Bây giờ với mật khẩu của quản trị viên tôi nghĩ tôi có thể đăng nhập với sự giúp sức của PsExec.

PsExec là 1 công cụ quản trị hệ thống đa năng của Microsoft mà bạn có thể dùng để truy cập từ xa một máy chủ đích.

Nhưng bạn không thể đăng nhập được:



Tiếp theo, mình kiểm tra đặc quyền của người dùng hiện tại:



SeImpersonatePrivilege đã được bật. Vì vậy tôi đã upload PrintSpoofer.exe giống như reverse shell và thực thi nó.

Khai thác printspoofer có thể được dùng để leo thang đặc quyền trên Windows Server 2016, Server 2019 và Windows 10.

Để leo thang đặc quyền, người dùng hiện tại phải có đặc quyền SeImpersonate. Để thực thi:

PrintSpoofer.exe -i -c cmd

