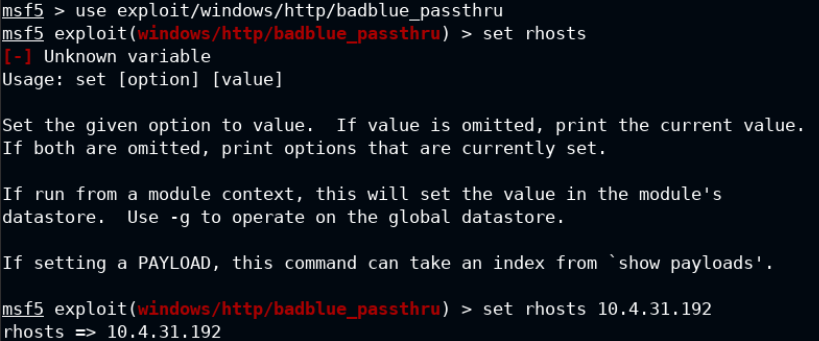
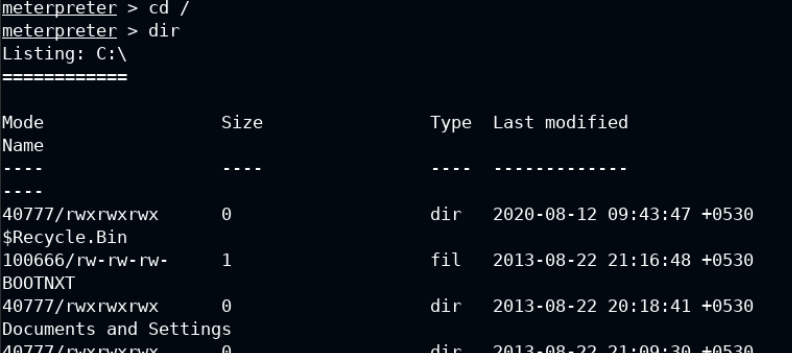
Similar to other exploits, we found badblue running over port 80 so we’re going to cut the fluff and just start with that exploit.

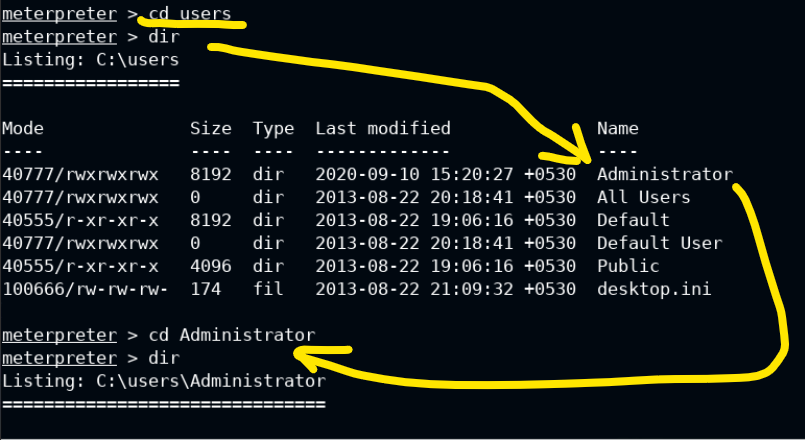
Note, if you fail to put any input after [set rhosts] you’ll get the following error. Just remember to input the actual ip address and you’ll be fine



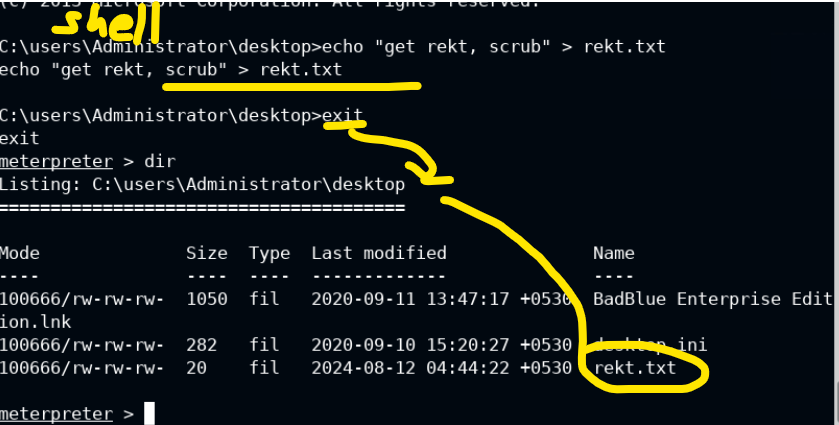
Move to the meterpreter session that opens when you run the badblue passthru.



Get into the users and go to the Administrator dir

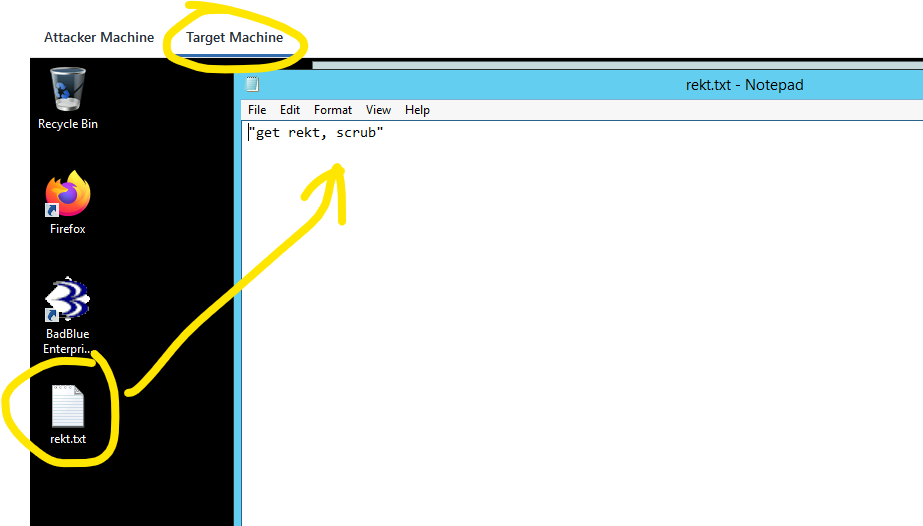


Make the defaced text file from command line



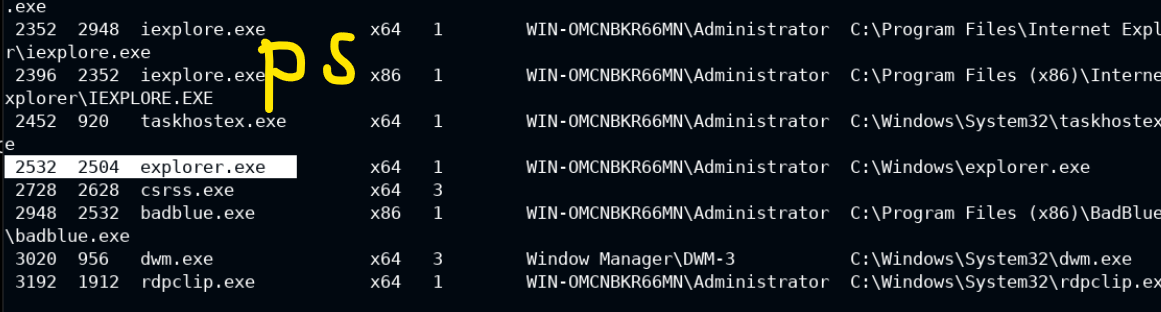
The above file is just a dumb text file we’re putting on the admin’s desktop to prove we can

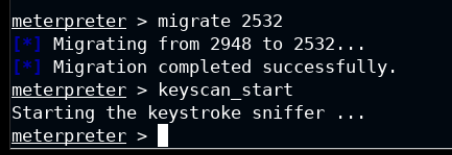
It appears on the target machine as shown below



..

Check ps to find the explorer.exe process so we can migrate our meterpreter to it

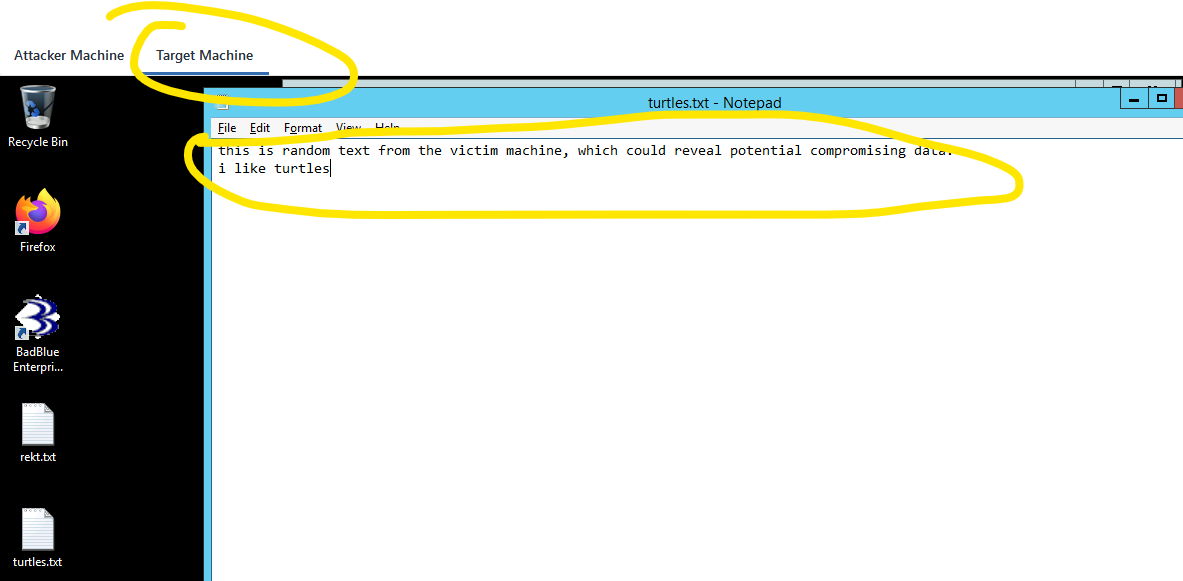




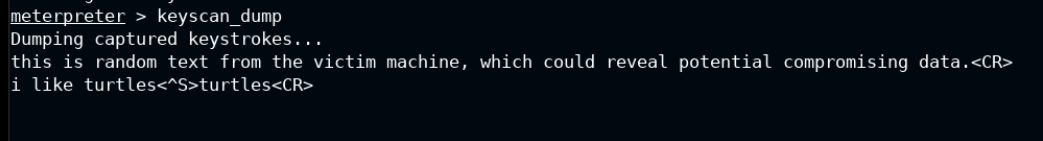
Command: keycan\_start begins the keylogger

Keylogging happens on the victim machine, for demo purposes.

Note the text input from the victim machine



We can view the keystrokes captured



Note how <^S> shows where the ctrl + s command for saving was done, and carriage returns were made when hitting enter <CR>. The last entry, “turtles” was when naming a file.

Patterns emerge around certain behaviors

<^S> text <CR> would usually encapsulate naming a file, which we could search for later.