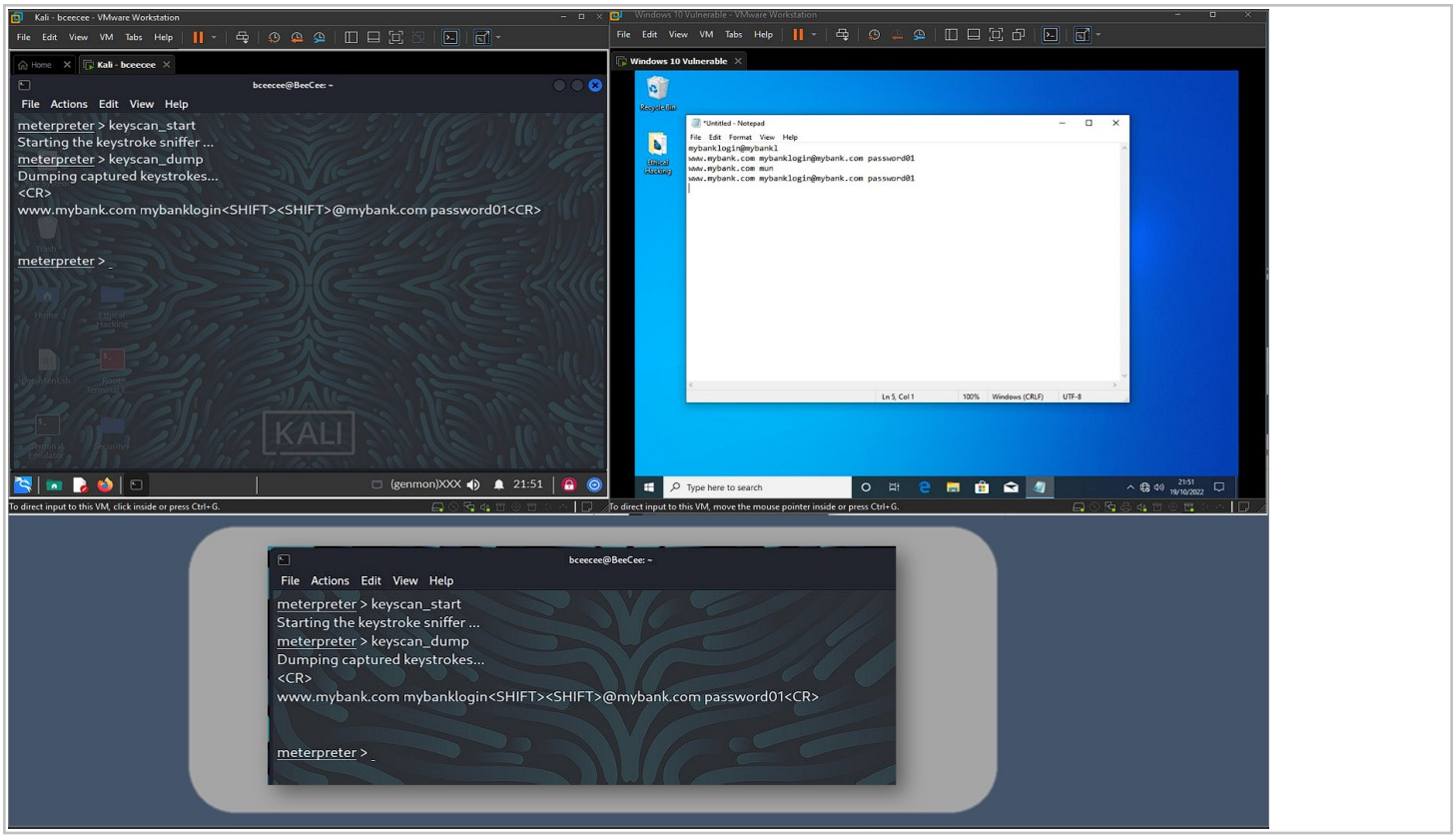
Section 11: Post Exploitation

Name:

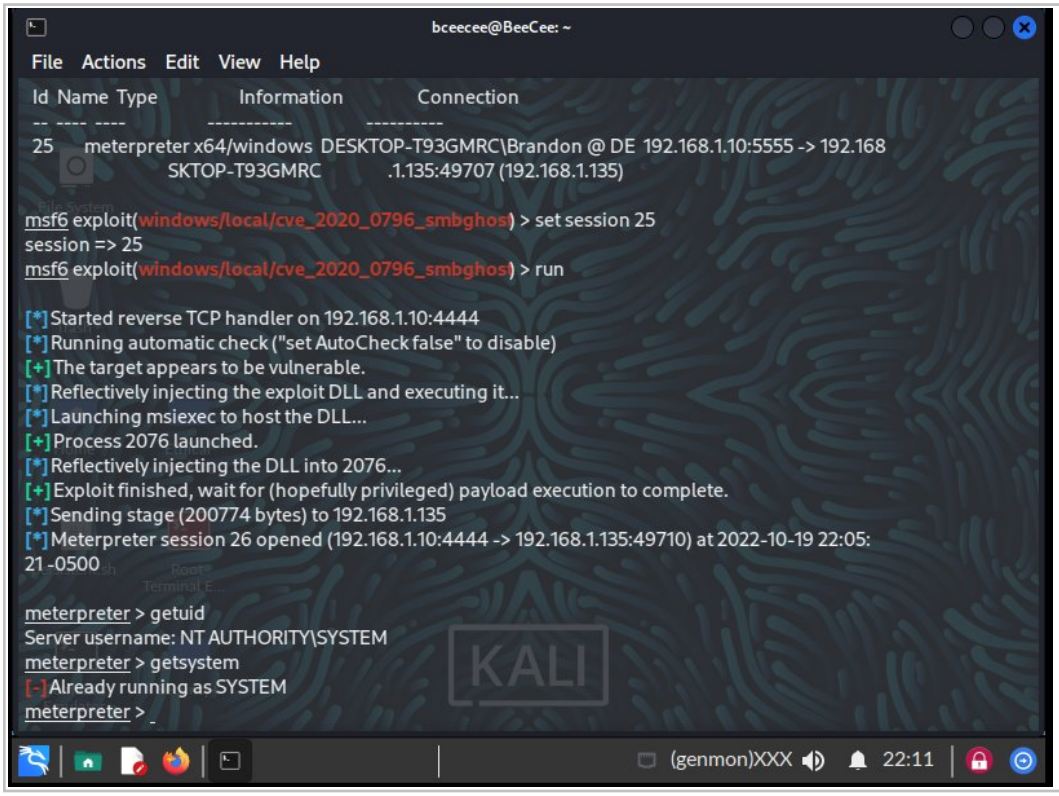
BC

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

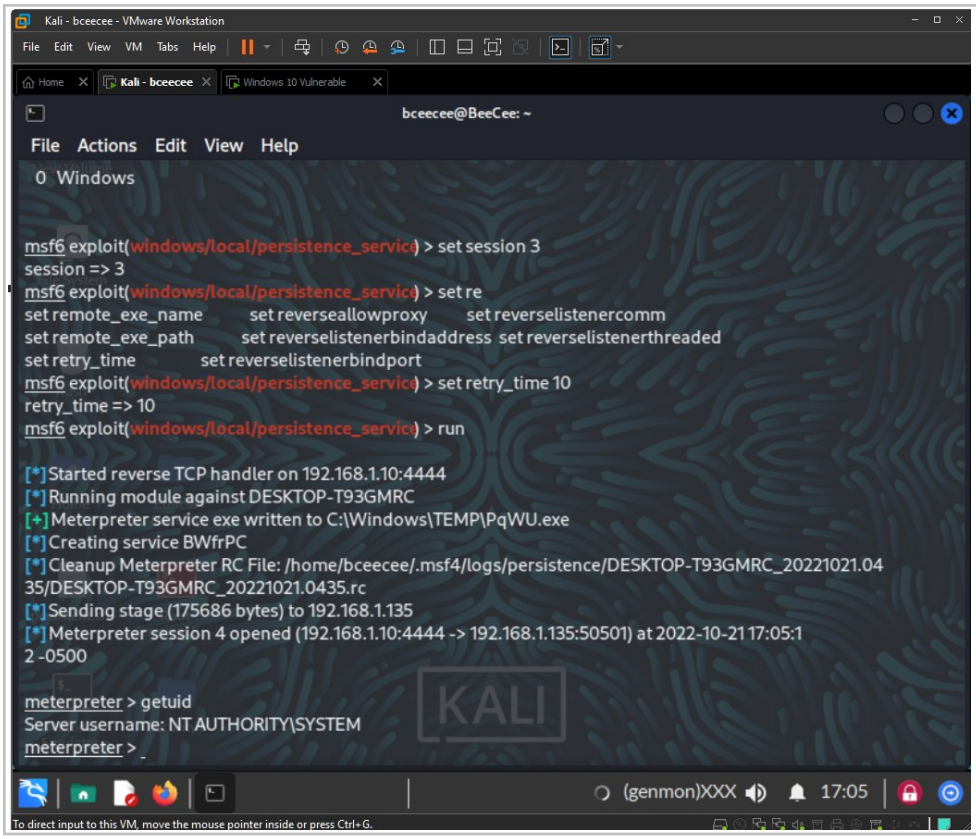
Lab 1: Capture Windows 10 keystrokes using Kali Meterpreter shell (90-91)



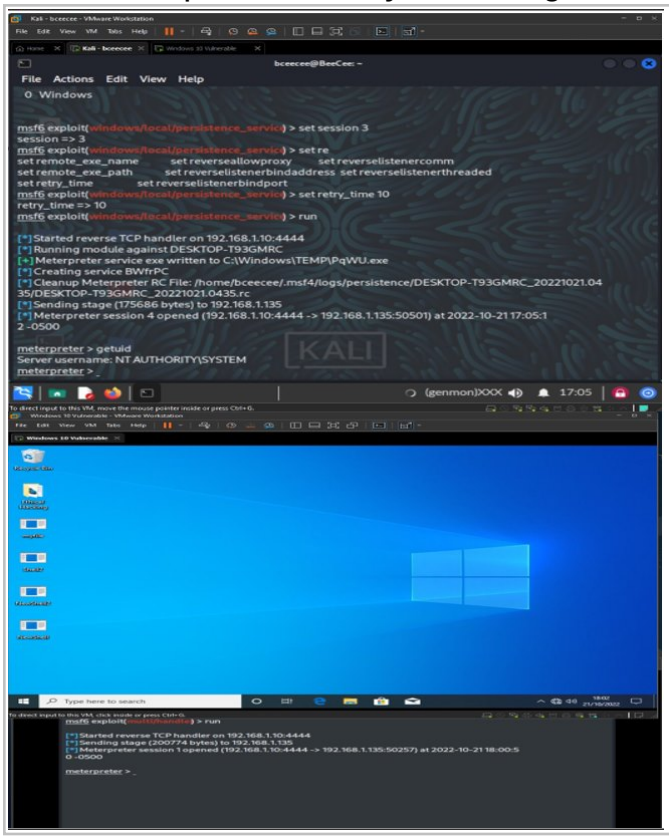
Lab 2: Elevate privileges (92)



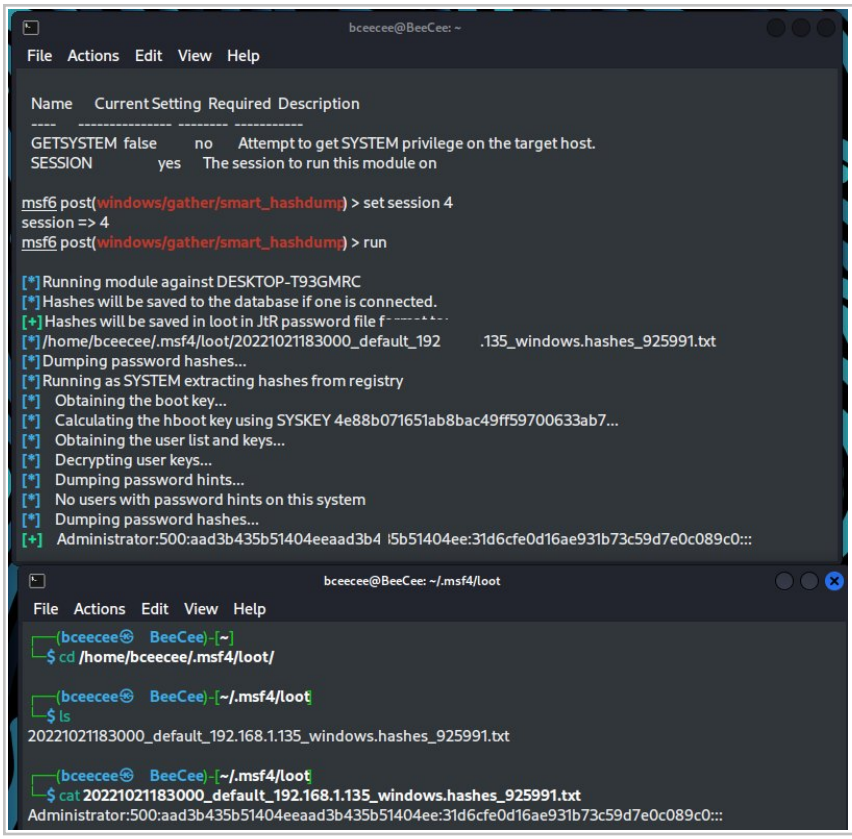
Lab 3: Create persistence with the exploit above (93)



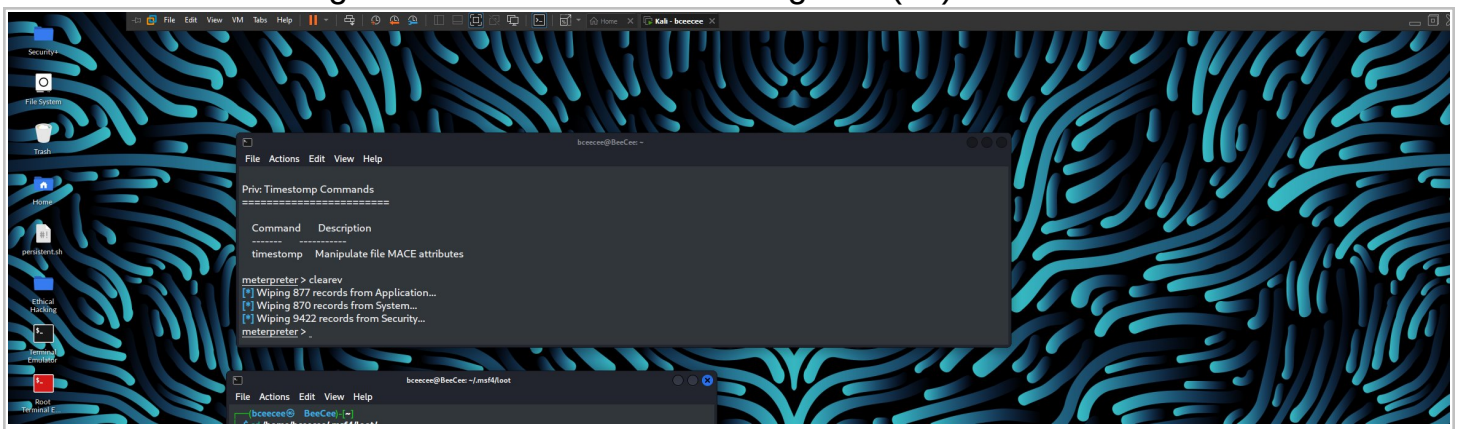
Lab 4: Test persistence by rebooting the target machine (93)



Lab 5: Find password hashes on the Windows 10 machine using post exploitation (94)



Lab 6: Clear event log events on Windows 10 using Kali (94)



Lab 7: From within a meterpreter prompt, display applications on Win10 (94)