INFOTC 3001 - Advanced Cyber Security
Laboratory # 6 - Exploitation framework

I. Objectives

1. Use Metasploit to exploit vulnerabilities in remote systems.
2. Use auxiliary module, exploits, and payloads in Metasploit.

II. Material Required

Kali Linux, TWXP0 and TW3P0 VMs.

III. Activity

Go through the *Module #5 - Exploitation Frameworks* before to start the laboratory.

IV. Review Questions

Add screenshots to demonstrate your work for questions 1, 2 and 4.

1. Use `nmap` tool with the `-Pn` flag to list the systems connected to the network 192.168.166.0/24.
2. Initialize Metasploit and use SYN scan auxiliary module to scan open ports in remote systems.
3. Describe the benefit(s) of using SYN scan vs TCP scan.
4. Using the *mc03_026_dcom* Exploit and the *windows/adduser* Payload create the ***tom*** user and a password for TWXP0 and TW3P0 VMs.