INFOTC 3001 - Advanced Cyber Security
Laboratory # 9 - Pivoting and Meterpreter

I. Objectives

1. Understand pivoting attack.
2. Enable and use Meterpreter.
3. Use Windows commands.

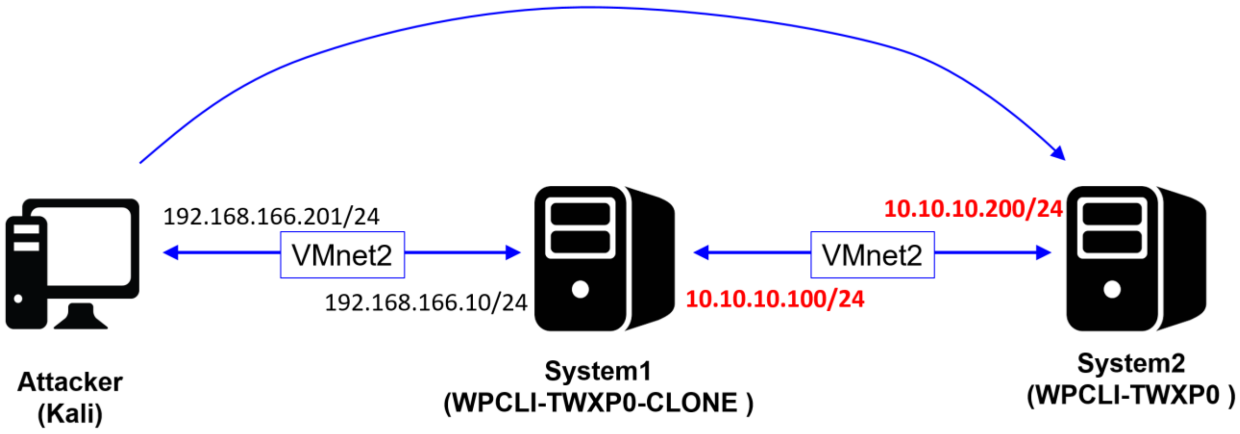
II. Material Required

Kali Linux, TWXP0 and TWXP0-CLONE VMs.

III. Activity

Before to start the laboratory make sure you covered the *Module #5 -* Meterpreter and Pivoting slides (17, 18 and 19)

Use the following network Topology for your lab. Note that the **IP addresses for system1 and system2 are 10.10.10.100/24 and 10.10.10.200/24** respectively.



Note: Use the WPCLI-TWXP0 to create a clone VM and then configure the IP addresses

IV. Review Questions

Add screenshots and description of your findings to demonstrate your work.

1. From Kali Linux, use any exploit to access to System1, and then enable a Meterpreter session on System2.
2. Once you open a Meterpreter session in System2 execute the following commands:
   a. `run checksum`
   b. `run get env`
   c. `run get_application_list`

   Add a detail description of your findings for each command.

3. Keep your session in System2 and execute `run scraper` command, Are you able to get some information? if so, what kind of information?
4. Keep your session in System2 and execute `hashdump` command to list MS Windows user accounts.
5. In Linux, user ID (located in /etc/passwd) in the range of 0 to 99 should be statically allocated by the system, while UIDs from 100 to 499 should be reserved for dynamic allocation by system administrators and post install scripts. Is there a similar logic of UID ranges for Windows users?
6. Keep your session in System2, enable the windows shell and create a `network_[YOUR_PAWPRINT].txt` file with the content of the `ipconfig /all` command execution. Can you copy the file to the Kali system, add a line to the end of the file and copy it back to System2?.
7. Keep your session in System2 with windows shell enabled and hide the `network_[YOUR_PAWPRINT].txt` file located (Use only command line in Windows).