Setup Target Part 1

[1] Pemasangan dan Konfigurasi metasploitable2	
1	Muat turun **metasploitable2** dari url: https://information.rapid7.com/download-metasploitable-2017.html atau https://sourceforge.net/projects/metasploitable/files/
2	Install Virtual Box ke dalam Windows OS anda.
3	Extract (unzip file metasploitable-linux-2.0.0) dan loadkan ke dalam Virtual Box atau VMWare

4	Login ke dalam metasploitable2 vm menggunakan credentials dibawah:
	`username : msfadmin`
	`password : msfadmin`

5	Dapatkan ip metasploitable dengan menngunakan command dibawah: `$ ifconfig`

6	Buka windows terminal dan taipkan command berikut untuk menguji connectivity terhadap metasploitable2 vm
	`ping ip_metasploitable2`
	
	`curl http://ip_metasploitable2`

7	Start kali-linux wsl dan taipkan command berikut untuk membuat simple nmap port scanning terhadap metasploitable2 vm `$ sudo nmap ip_metasploitable2`

[2] Asas Port Scanning	
1	Pastikan anda memasang / install Wireshark ke dalam Windows Host anda, kemudian runkan wireshark dan mulakan capture pada wsl interface
2	Buka Windows Terminal dan akses ke kali-linux wsl

3	Runkan command nmap portscan berikut terhadap ip metasploitable2
	`$ sudo nmap -sT -p80 ip_metasploitable2`
	`$ sudo nmap -sT -p88 ip_metasploitable2`

4	Analisa trafik berkenaan menggunakan wireshark. Anda boleh merujuk pada demo video.

5	Runkan command nmap portscan berikut terhadap ip metasploitable2
	`$ sudo nmap -sS -p80 ip_metasploitable2`
	`$ sudo nmap -sS -p88 ip_metasploitable2`

6	Analisa trafik berkenaan menggunakan wireshark. Anda boleh merujuk pada demo video.
7	Setup profile baru di dalam wireshark untuk enable features Packet Diagram, anda boleh melihat demo video untuk langkah-langkah selanjutnya.