Setup Target Part 2

[3] Port Scanning menggunakan nmap	
1	Startkan vm metasplotable2 dan buka terminal kali-linux wsl

2	Taipkan command berikut dan analisa output yang dihasilkan (tonton video demo untuk penerangan setiap command dan output berkenaan)
	`$ nmap --help`
	`$ cd Desktop`
	`$ mkdir nmap && cd nmap`
	`$ sudo nmap -v -sS -A -T4 ip_metasploitable2 -oX T4.xml`
	`$ sudo nmap -v -sS -A -T5 ip_metasploitable2 -oX T5.xml`
	`$ pip install pyndiff`
	`$ pyndiff -f1 T4.xml -f2 T5.xml`
	
	`$ sudo nmap -A -T4 -p- ip_metasploitable2 -oA full_tcp_scan`
	`$ sudo nmap -A -T4 -sU -p- ip_metasploitable2 -oA full_udp_scan`

3	Taipkan command berikut untuk nmap parsing
	`$ wget https://raw.githubusercontent.com/actuated/nmaparse/master/nmaparse.sh`
	`$ ./nmaparse.sh full_tcp_scan.gnmap`
	`$ cd nmaparse-tarikh/`
	`$ cat nmaparse-summary-tarikh.txt`

[4] vulnscan

1 Runkan command berikut untuk setup vulnscan ke dalam kali linux anda:

```
$ cd ~
$ mkdir tools && cd tools
$ git clone https://github.com/scipag/vulscan scipag_vulscan
$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

2 Taipkan command berikut dan analisa output yang dihasilkan

```
$ sudo nmap -sV --script=vulscan/vulscan.nse ip_metasploitable2 -oN vulnscan
$ cat vulnscan | more
$ cp vulnscan /mnt/c/Users/gh1mau/Desktop/
```

[5] searchsploit

1 Runkan command berikut dan analisa ouput yang berkenaan:

```
$ cd /mnt/c/Users/gh1mau/Desktop/nmap
$ searchsploit --nmap full_tcp_scan.xml
$ searchsploit --nmap full_tcp_scan.xml -www
```