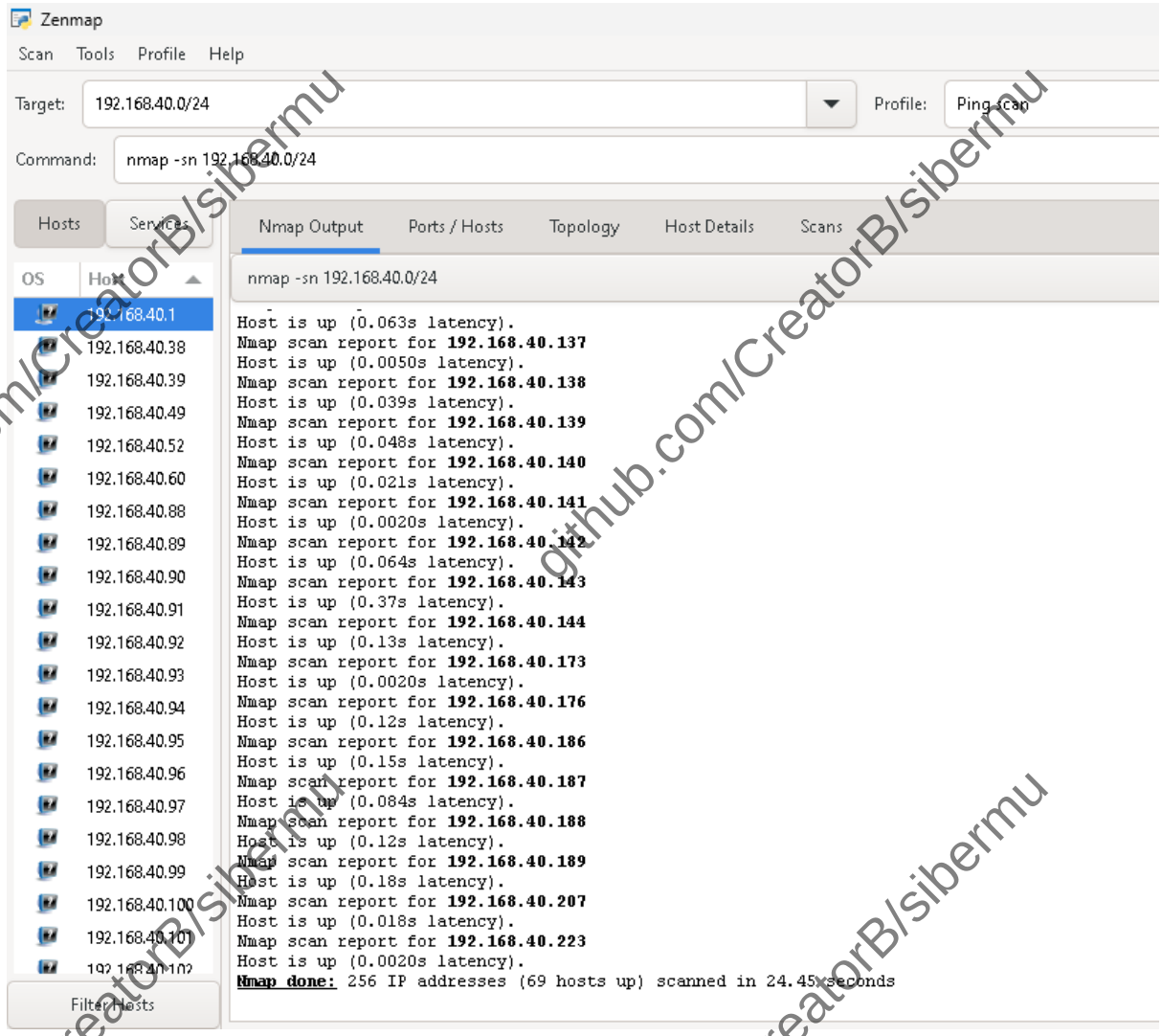
Nama: HASAN BASRI
NIM: 20230104144
Mata Kuliah: Keamanan Informasi
Angkatan: 05
Nama Tugas: Tugas 03 ZENMAP CPMK 01
Tugas Ke: 03

1. **Networking MAP**, pemetaan jaringan dengan mengirimkan paket probe (paket yang digunakan untuk mengumpulkan informasi dari segment target yang nantinya mengembalikan respon pada nmap) dengan perintah nmap -sn <target addresses> dibawah ini saya menggunakan salah satu segment IP Wi-Fi yakni 192.168.40.1 – 192.168.40.254 dan terlihat yang online Wi-Fi di segment ini hanya 69 devices. Jika tidak mau mengetikkan command diatas, bisa pilih opsi profile Ping scan.



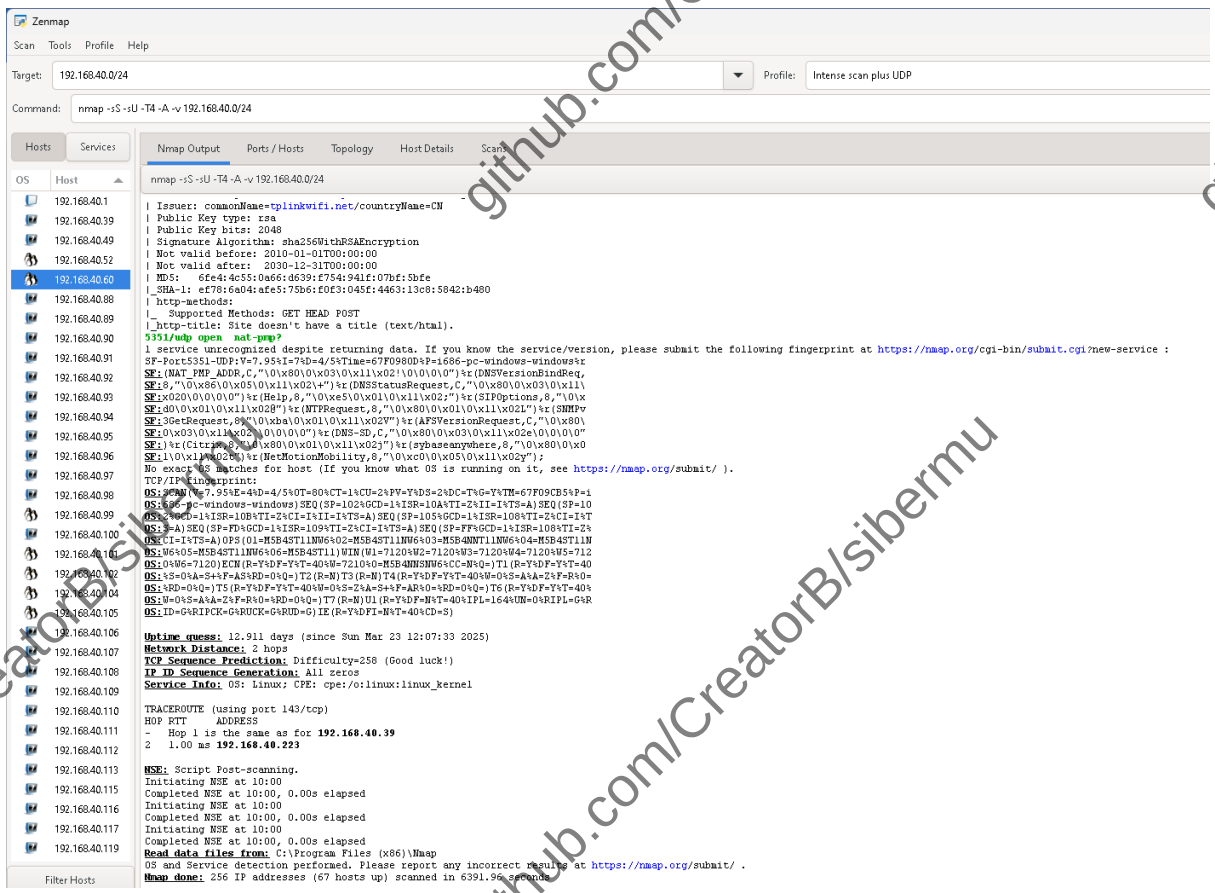
2. **Port Scanning** untuk mengetahui port mana saja yang terbuka pada jaringan, di nmap kita bisa menggunakan perintah nmap -sS <target addresses> atau dengan pilih opsi profile Intense scan plus UDP hanya saja untuk profile

Nama: HASAN BASRI
NIM: 20230140144
Mata Kuliah: Keamanan Informasi
Angkatan: 05
Nama Tugas: Tugas 03 ZENMAP CPMK 01
Tugas Ke: 03

tersebut menggunakan opsi nmap -sS -sU -T4 -A -v <target addresses> pemindaian ini lebih lengkap dan agresif dengan beberapa parameter sebagai berikut :

-sS : SYN scan (pemindaian cepat & stealthy untuk TCP).
-sU : UDP scan (memindai port UDP juga, lebih lambat dari TCP scan).
-T4 : Agresif & cepat (menggunakan waktu pemindaian lebih tinggi).
-A : Advanced scan, termasuk:
Deteksi OS (-O)
Deteksi versi layanan (-sV)
Traceroute (--traceroute)
Script scanning (--script)
-v : Verbose mode, menampilkan informasi detail selama pemindaian.

Atau juga bisa menggunakan opsi profile yang disediakan nmap yakni Intense scan plus UDP.



Nama: HASAN BASRI	
NIM: 2023010144	
Mata Kuliah: Keamanan Informasi	
Angkatan: 05	
Nama Tugas: Tugas 03 ZENMAP CPMK 01	
Tugas Ke: 03	

3. **SERVICE RUNNING**, memetakan layanan yang sedang berjalan pada port tertentu. Perintah yang digunakan dalam materi yaitu nmap -sV <target addresses> atau jika hendak menggunakan opsi profile nmap bisa menggunakan profile Quick scan plus.

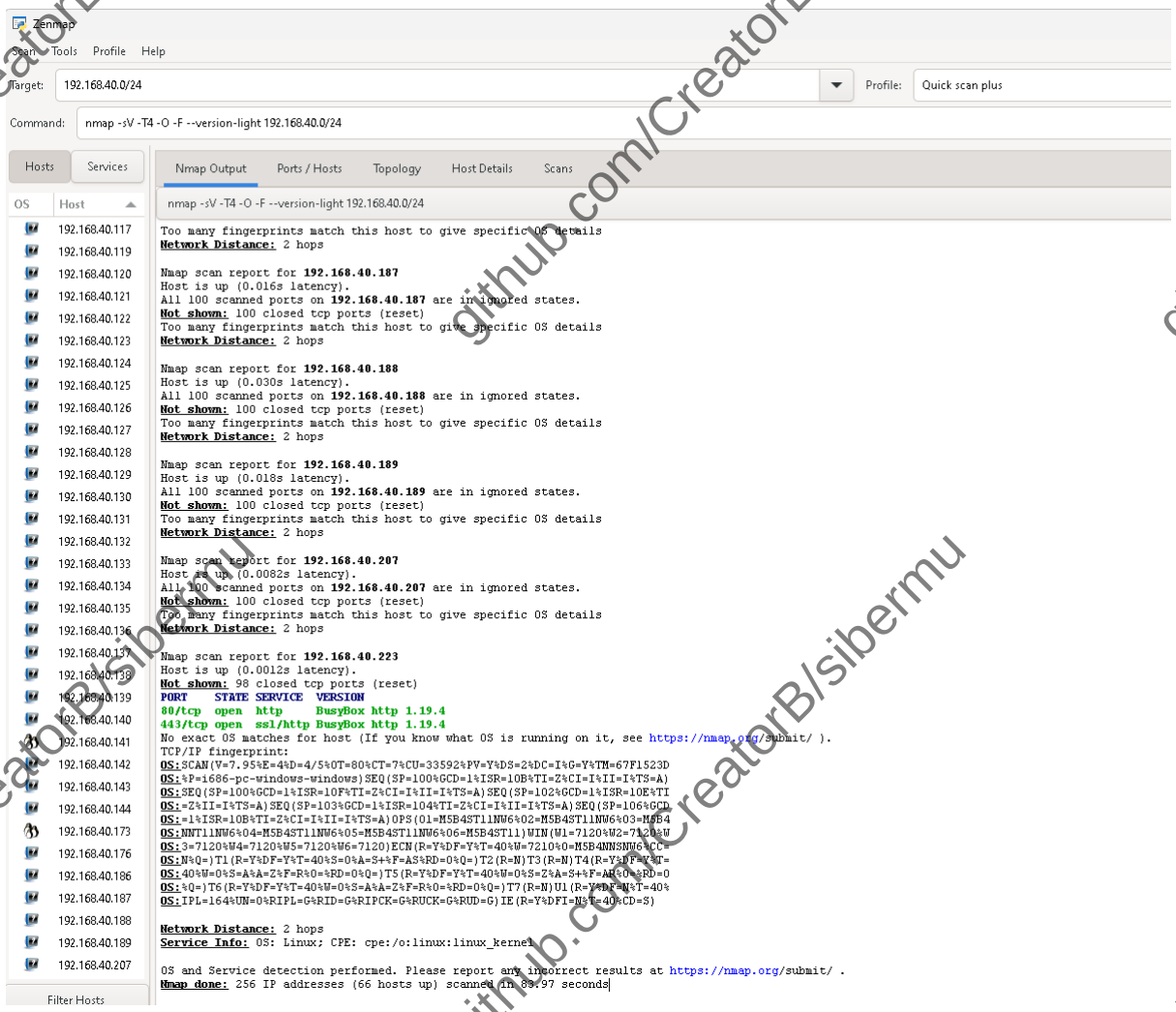
   -sV Deteksi versi layanan

   -T4 Atur kecepatan pemindaian (T4 = agresif tapi masih stabil)

   -O Deteksi sistem operasi target (OS detection)

   -F "Fast mode", hanya scan port yang umum (default: ~100)

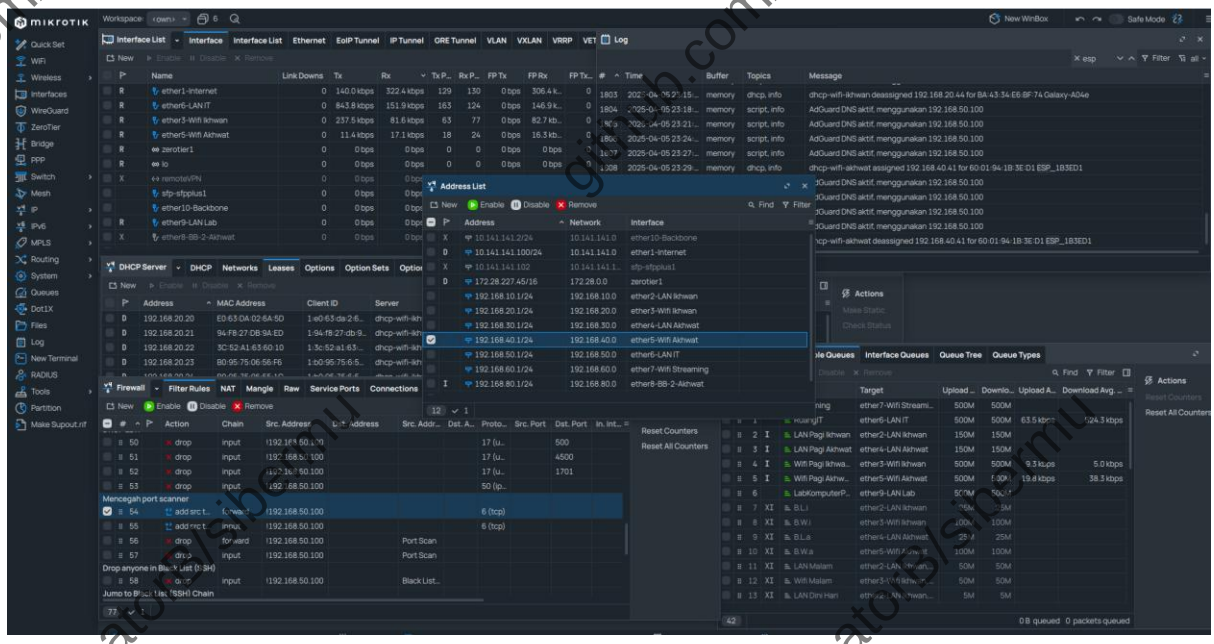
   --version-light Melakukan pemeriksaan versi layanan lebih ringan & cepat (kurangi akurasi sedikit demi efisiensi)



Nama: HASAN BASRI	
NIM: 2023010144	
Mata Kuliah: Keamanan Informasi	
Angkatan: 05	
Nama Tugas: Tugas 03 ZENMAP CPMK 01	
Tugas Ke: 03	

4. **OPERATING SYSTEMS**, tool nmap juga sering dipakai untuk mendeteksi system operasi dari sebuah mesin, bemanfaat untuk inventaris, exploitasi kerentanan untuk di patch, dll karena tool ini dikenal memiliki basis data fingerprint OS yang paling lengkap. Perintah dasarnya : nmap -O <target addresses sedangkan untuk menggunakan profile sudah dilampirkan di poin 3.

Walhamdulillah, demikian hasil pengerjaan tugas kali ini semoga bermanfaat, Zenmap yang saya pakai diatas versi 7.95, adapun jaringan yang saya scan adalah jaringan kantor saya, Mahad Al-Imam Asy-Syathiby, Cileungsi, Bogor, 04-04-2025 – 05-04-2025. Ada banyak cara dalam mencegah network mapping seperti yang saya lakukan diatas, salahsatunya menggunakan MikroTik seperti yang saya lakukan, baik itu dengan cara membuat firewall supaya jika ada yang scan port dalam hitungan detik maka masukkan dalam list banned dan jangan lupa IP anda sebagai network administrator di exclude supaya tidak ikut kebanned ketika melakukukan operasi diatas.



github.com/CreatorBysibermu