1. Single Host

Dengan penggunaan domain maupun ip address. Dengan ip address. Perintah standart scanning ke single ip address : **nmap 192.168.1.1**

2. Dengan Domain

Perintah standart scanning dengan domain. Perintah standart dengan tambahan informasi lainnya : **nmap unika.ac.id**

3. Multi ip address dan subnet

Untuk melakukan scanning lebih dari satu ip address atau mungkin bertujuan untuk melakukan scanning ke satu subnet. Salah satu contoh jika kita hendak melakukan scanning terhadap 2 ip address 192.168.2.1 dan 192.168.2.2. Jika kita hendak melihat informasi host yang sedang dalam keadaan up pada satu subnet. Jika berdasarkan ip address :

nmap 192.168.1.1 192.168.1.2

Perintah untuk melakukan scann ke seluruh jaringan berdasarkan subnet :

nmap 192.168.1.*

nmap 192.168.1.1/24

save output ke file.. ==> **nmap 192.168.1.1 > output.txt**

4. Menampilkan paket diterima dan dikirim

Anda dapat menampilkan paket-paket yang dikirim dan diterima nmap pada proses scann : **nmap --packet-trace 192.168.2.1**

5. Menampilkan semua interface dan rute

Untuk menampilkan interface dan rute yang tersedia didalam os , anda dapat menggunakan perintah iflist : **nmap –iflist**

Anda dapat tidak menyertakan host dengan domain dan ip address tertentu saat melakukan scanning terhadap sebuah jaringan. Hal ini sangatlah bermanfaat pada saat anda melakukan scanning pada tingkat jaringan yang besar.

nmap 192.168.2.0/24 --exclude 192.168.2.3

nmap 192.168.2.0/24 --exclude 192.168.2.5,192.168.2.254

Contoh di atas berarti anda tidak melakukan scanning pada ip 192.168.2.3, 192.168.2.5, 192.168.2.254 pada sebuah subnet 192.168.2.0/24

6. Mendeteksi sistem operasi dan layanan (services) target :

nmap -A 192.168.2.11

Dari hasil di atas anda dapat mengetahui beberapa service yang berjalan serta Operating system yang digunakan target. OS: Windows XP (Windows 2000 LAN Manager).

Penggunaan -v (service scan) juga akan menampilkan hasil yang akurat : **nmap -v -A 192.168.2.11**

7. Remote operating system

nmap -O 192.168.2.11

Beberapa kombinasi yang dapat digunakan

nmap -O --osscan-guess 192.168.1.1
nmap -v -O --osscan-guess 192.168.1.1

8. Mendeteksi layanan dan device yang sedang up

Untuk mendeteksi layanan (services) dan device yang sedang up pada satu jaringan/subnet tertentu : **nmap -sP 192.168.2.1/24**

9. Mendeteksi versi dari layanan (service)

Untuk mendeteksi beberapa versi layanan (service) pada target , anda dapat menggunakan opsi -sV : **nmap -sV 192.168.2.2**

10. Mendeteksi firewall

Mendeteksi adanya penggunaan firewall pada service berjalan, anda dapat menggunakan opsi -sA : **nmap -sA 192.168.2.11**

Hasil di atas memberitahu kita bahwa beberapa service tanpa dalam keadaan status unfiltered.

Contoh kasus adanya penggunaan Firewall terhadap sebuah server :

nmap -sA site.org

11. Scanning firewall

Untuk mendeteksi kelemahan firewall pada sistem target

TCP Null Scan untuk menipu firewall untuk memberikan respon ,dalam kondisi TCP flag header adalah nol (null) : **nmap -sN 192.168.2.1**

TCP Fin scan untuk mengecek firewall ,hanya TCP FIN bit.

nmap -sF 192.168.2.1

Penggunaan TCP Xmas

setting FIN, PSH, dan URG

nmap -sX 192.168.2.1

12. Firewall untuk packets fragments

opsi ini akan membuat nmap mengirimkan paket data dengan menggunakan tiny fragmented IP packets. Dengan menggunakan opsi ini , anda dapat melewati berbagai filtered, IDS/IPS : nmap -f site.org

Melakukan scanning disaat target menggunakan firewall : nmap -PN site.org