KEAMANAN SISTEM DAN JARINGAN
SCANNING & PROBING

RINANZA ZULMY ALHAMRI, S.Kom., M.Kom
PSDKU POLINEMA DI KOTA KEDIRI

Kode	: KIF195004
Kredit	: 3 SKS
Semester	: 5

MENU

- Konsep Scanning & Probing
- NMap
- NMap Basic
- Nmap Intermediate
- Nmap – Deteksi Firewall
- Tugas

Konsep Scanning dan Probing

- Metode selanjutnya setelah melakukan footprinting adalah scanning dan probing.
- Istilah scanning dan probing memiliki arti yang hampir mirip, mereka sama-sama memeriksa, mencari, dan membuat percobaan secara aktif dan lebih detail untuk tujuan tertentu pada target. Perbedaanya apabila scanning dilakukan secara otomatis, banyak, dan instan sedangkan probing manual, sedikit, tapi berkualitas.
- Apabila footprinting mengumpulkan informasi publik secara random, scanning dan probing sudah mulai teknis dan detail, misal memeriksa port yang terbuka, memeriksa sub-domain yang aktif, memeriksa alamat IP privat yang digunakan, dsb

NMAP

- Nmap (Network Mapper) adalah sebuah program open source yang berguna untuk mengeksplorasi jaringan.
- Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal.
- Nmap menggunakan paket IP untuk menentukan host- host yang aktif dalam suatu jaringan,port-port yang terbuka, sistem operasi yang dipunyai, tipe firewall yang dipakai, dll.

NMAP : Fitur

- Mengumpulkan informasi setiap host atau komputer yang hidup (life) pada jaringan lokal
- Mengumpulkan informasi setiap ipaddress pada jaringan lokal
- Mengumpulkan informasi setiap sistem operasi pada host maupun seluruh host pada target jaringan
- Menemukan setiap port yang terbuka dari host target
- Menemukan adanya infeksi dari virus maupun malware
- Mengumpulkan informasi mengenai layanan-layanan (service) pada host target dan server pada jaringan target.

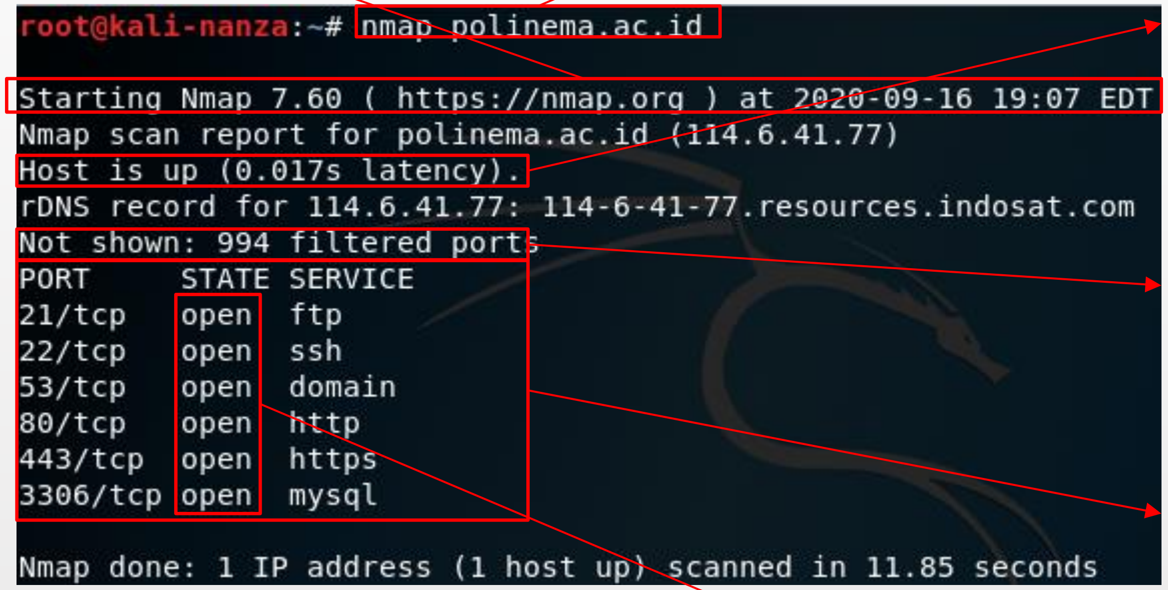
TARGET SCANNING & PROBING
Sistem informasi polinema.ac.id

Selain melakukan scanning probing pada target, scanning probing juga bisa dilakukan untuk memeriksa kondisi jaringan lokal

NMAP - Dasar

Informasi administrasi umum

Secara default nmap melakukan TCP connect berupa sinyal SYN - ACK



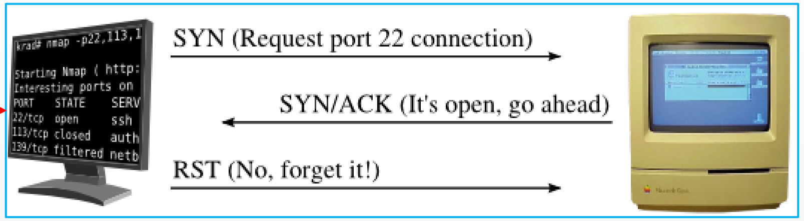
```
root@kali-nanza:~# nmap polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 19:07 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.017s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 11.85 seconds
```

Host up artinya host aktif publish di internet

Secara default >1000 port di-scan, filtered artinya gagal koneksi tanpa sebab, sehingga status close pun tidak diketahui

Daftar port yang berhasil melakukan handshaking dengan keterangan service

STATE OPEN 'koneksi lancar'

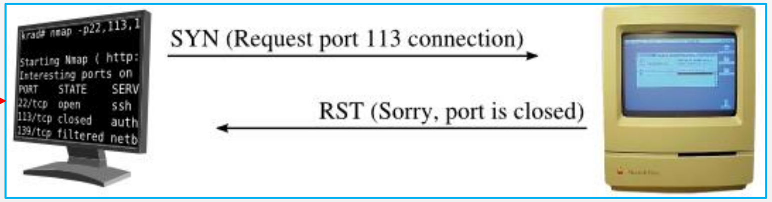


SYN (Request port 22 connection)

SYN/ACK (It's open, go ahead)

RST (No, forget it!)

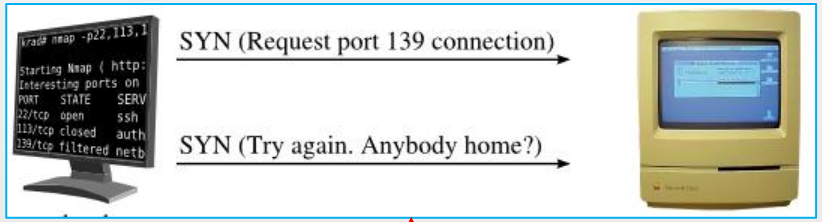
STATE CLOSED 'koneksi di-reset oleh target'



SYN (Request port 113 connection)

RST (Sorry, port is closed)

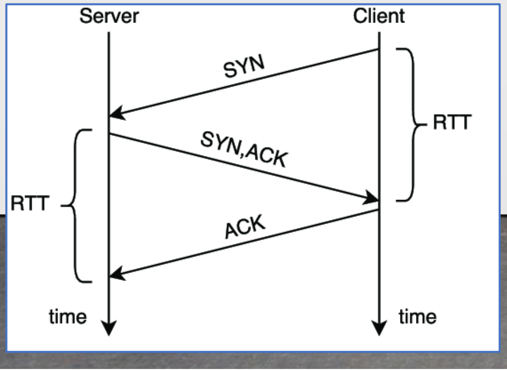
STATE FILTERED 'tidak ada jawaban – gangguan jaringan



SYN (Request port 139 connection)

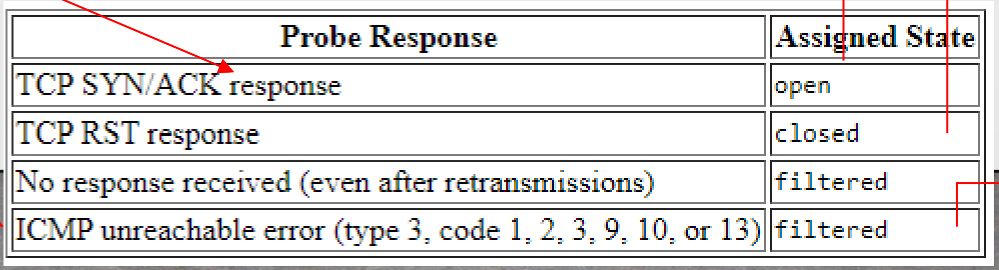
SYN (Try again. Anybody home?)

3 Ways Handshake TCP Connection



3 ways handshake harus berhasil saat pertama kali protokol TCP melakukan koneksi antar host, termasuk ICMP pada PING

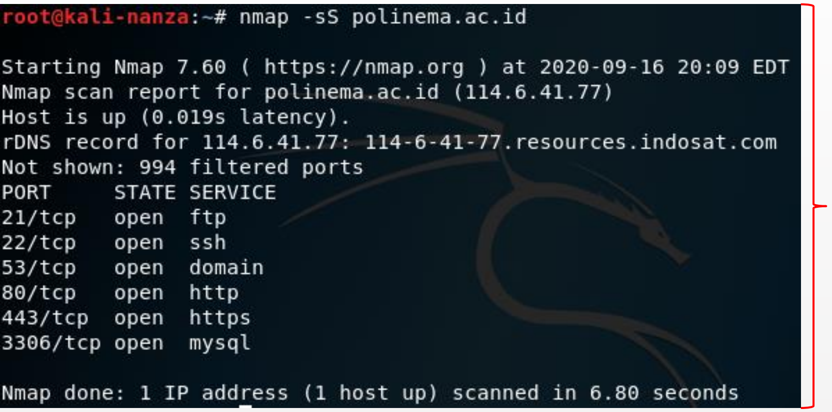
Macam-macam STATE



Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

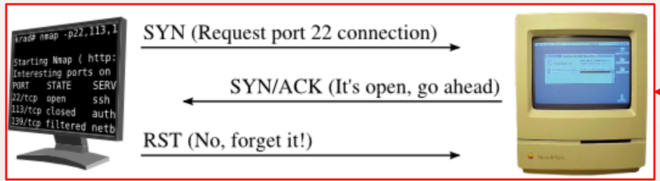
NMAP - Dasar

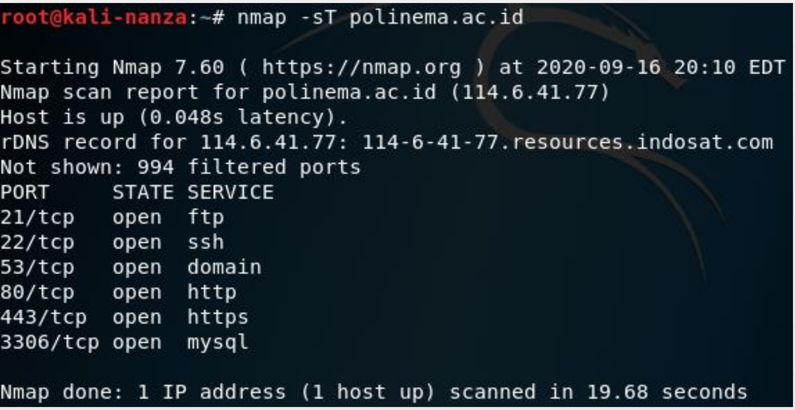
Perintah NMAP memungkinkan memilih beberapa jenis koneksi



```
root@kali-nanza:~# nmap -sS polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 20:09 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.019s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
```

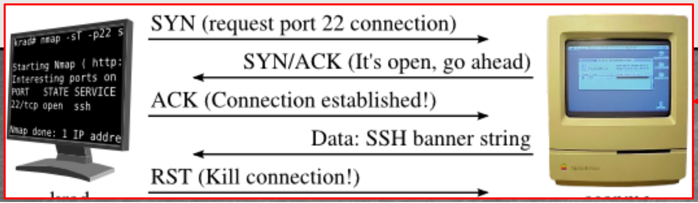
-sS (Stealth Connection) merupakan koneksi default perintah NMAP. Mengirim SYN namun setengah terbuka (*half open*) sehingga tidak terekam log jaringan pada target

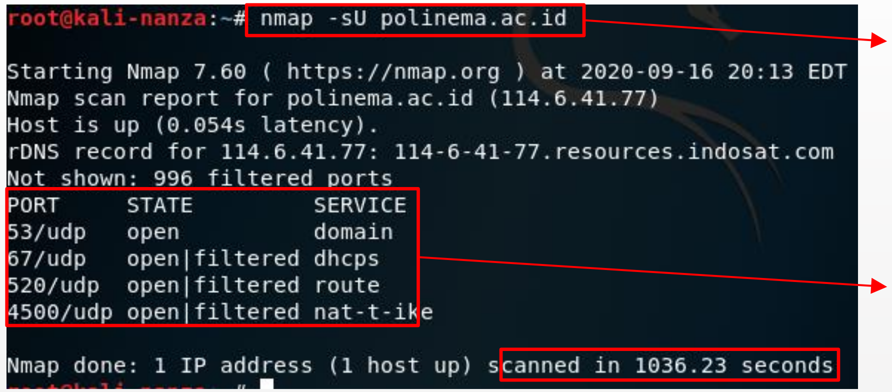




```
root@kali-nanza:~# nmap -sT polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 20:10 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.048s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 19.68 seconds
```

-sT (TCP Connection) merupakan koneksi TCP dimana hasilnya sama seperti -sS namun terekam log jaringan pada target karena *full open* → 3 ways handshake → sampai kirim ACK





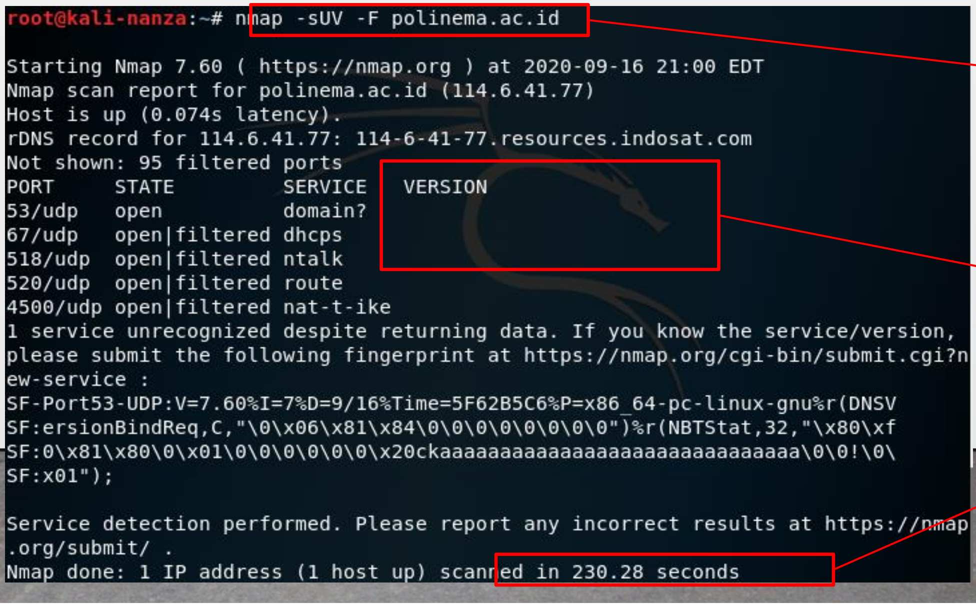
```
root@kali-nanza:~# nmap -sU polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 20:13 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.054s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 996 filtered ports
PORT     STATE         SERVICE
53/udp   open          domain
67/udp   open|filtered dhcps
520/udp  open|filtered route
4500/udp open|filtered nat-t-ike

Nmap done: 1 IP address (1 host up) scanned in 1036.23 seconds
```

-sU (UDP Connection) merupakan koneksi UDP untuk melihat port UDP yang terbuka.

State open benar-benar terbuka. Sedangkan yang open-filtered, port terbuka tetapi sistem belum bekerja dengan baik karena sinyal Nmap tidak direspon

Koneksi lemot + menggunakan koneksi UDP

Koneksi UDP lebih lama dibandingkan TCP karena UDP connectionless-oriented, sedangkan TCP connection-oriented sehingga apabila terlalu lama, TCP akan melapor sedangkan UDP tidak. Untuk itu bisa digunakan optional –F agar lebih cepat pada koneksi UDP



```
root@kali-nanza:~# nmap -sUV -F polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 21:00 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.074s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 95 filtered ports
PORT     STATE         SERVICE  VERSION
53/udp   open          domain?
67/udp   open|filtered dhcps
518/udp  open|filtered ntalk
520/udp  open|filtered route
4500/udp open|filtered nat-t-ike
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-UDP:V=7.60%I=7%D=9/16%Time=5F62B5C6%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReq,C,"\0\x06\x81\x84\0\0\0\0\0\0\0\0")%r(NBTStat,32,"\x80\xf
SF:0\x81\x80\0\x01\0\0\0\0\0\0\x20ckaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\0\0!\0\
SF:x01");

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 230.28 seconds
```

Menambahkan –V akan menampilkan versi dari layanan

Tidak ada versi yang dikenali sehingga membuat sinyal UDP Nmap tidak direspon meskiputn port terbuka

Waktu scanning jauh lebih cepat menggunakan optional -F

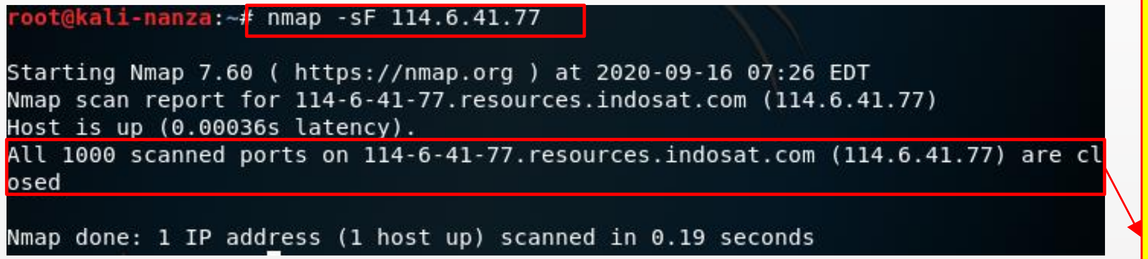
NMAP - Dasar

```
IF( TCP 3Ways Handshake == TRUE ) THEN {
        Connect can add PSH || URG; //PSH-Push data for buffering, URG-Urgent data have to prioritize
        Finish with FIN // finish connection naturally
} ELSE { Reset with RST}
```

Selain menggunakan alamat domain, target juga bisa menggunakan alamat IP, bahkan target bisa lebih dari satu

TCP FIN, Xmas, Null digunakan untuk melihat detail port yang memiliki status open, apakah benar-benar open

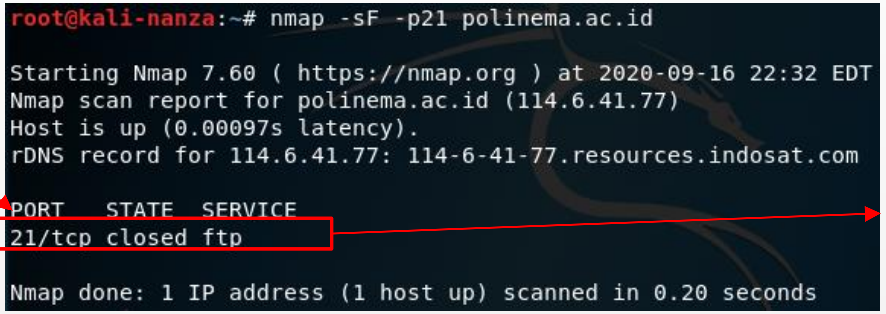
STATE RESPONSE untuk –sF, -sX, -sN	Assigned State	
No response received (even after retransmissions)	open|filtered	Open tapi tidak respon FIN, Xmas, Null, artinya dilindungi
TCP RST packet	closed	Open dan ada respon RST, berarti benar2 open
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered	Open tapi error ICMP



```
root@kali-nanza:~# nmap -sF 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 07:26 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.00036s latency).
All 1000 scanned ports on 114-6-41-77.resources.indosat.com (114.6.41.77) are cl
osed

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

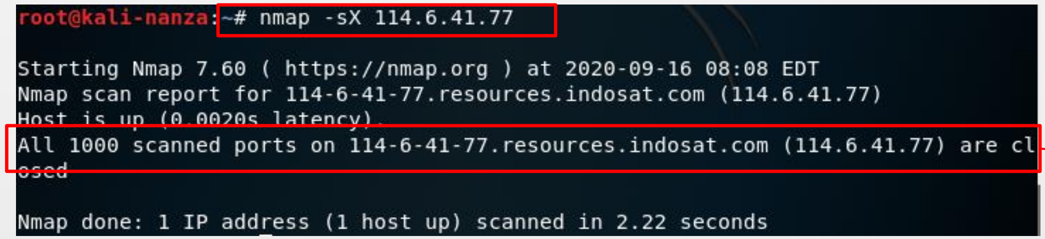
-sF (FIN scan) melakukan koneksi FIN dimana bermaksud untuk bypass koneksi TCP tanpa melalui SYN. FIN untuk finishing tetapi jika port respon pertanda port benar-benar open. Jika open dan respon RST → closed

Bukan berarti 1000 port benar2 open kerana status closed, melainkan port2 yang dilakukan TCP connect berstatus open dan dilakukan TCP FXN berstatus closed yang benar-benar open.



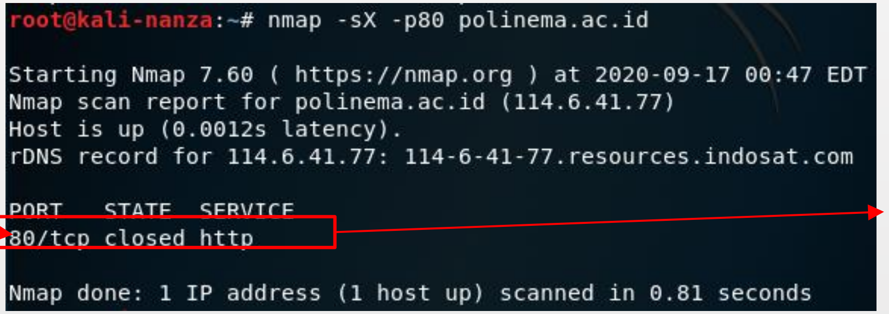
```
root@kali-nanza:~# nmap -sF -p21 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 22:32 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.00097s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Port 21 benar-benar open



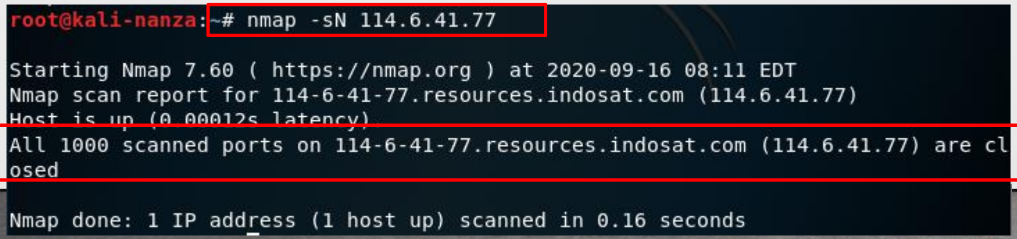
```
root@kali-nanza:~# nmap -sX 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 08:08 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0020s latency).
All 1000 scanned ports on 114-6-41-77.resources.indosat.com (114.6.41.77) are cl
osed

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
```

-sX (Xmas scan) melakukan koneksi FIN, PSH,dan URG secara serentak seperti pohon natal dimana bermaksud untuk bypass koneksi TCP tanpa melalui SYN. Jika port respon berarti benar-benar open. Jika open dan respon RST → closed



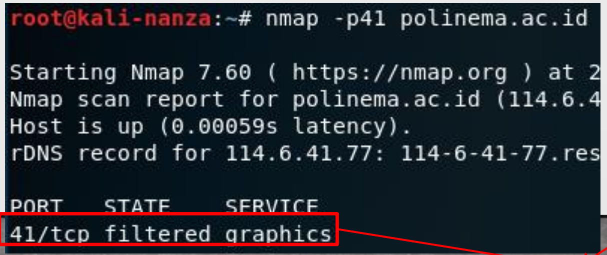
```
root@kali-nanza:~# nmap -sX -p80 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 00:47 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0012s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

Port 80 benar-benar open

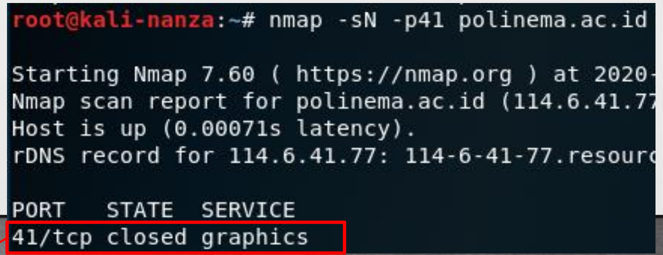


```
root@kali-nanza:~# nmap -sN 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 08:11 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.00012s latency).
All 1000 scanned ports on 114-6-41-77.resources.indosat.com (114.6.41.77) are cl
osed

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

-sN (Null scan) melakukan koneksi dengan header TCP null (tanpa jenis koneksi apapun. Jika open tetapi tidak respond maka RST → closed



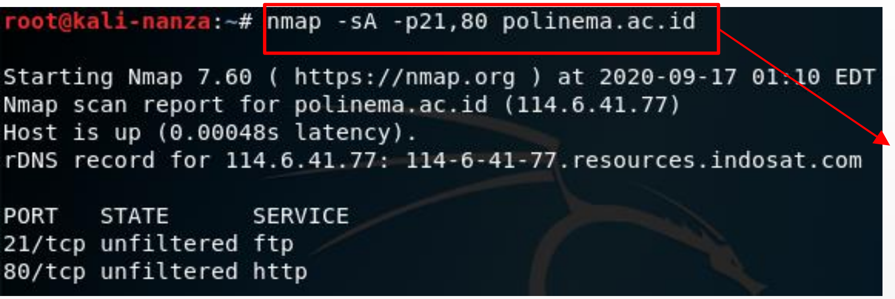
```
root@kali-nanza:~# nmap -p41 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2
Nmap scan report for polinema.ac.id (114.6.4
Host is up (0.00059s latency).
rDNS record for 114.6.41.77: 114-6-41-77.res

PORT     STATE    SERVICE
41/tcp filtered graphics
```



```
root@kali-nanza:~# nmap -sN -p41 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-
Nmap scan report for polinema.ac.id (114.6.41.77
Host is up (0.00071s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resour

PORT   STATE  SERVICE
41/tcp closed graphics
```

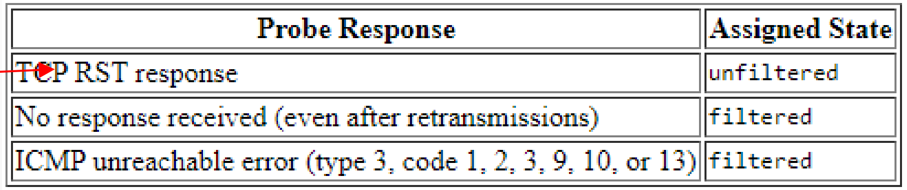
Port 41 filtered ketika nmap default kemudian closed ketika TCP FXN, artinya tidak open

NMAP – Dasar

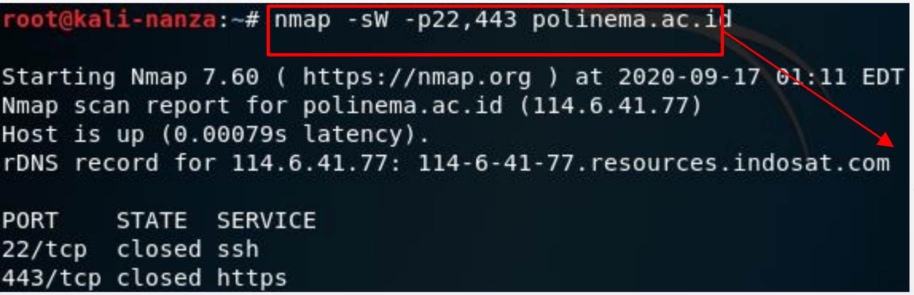


```
root@kali-nanza:~# nmap -sA -p21,80 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 01:10 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.00048s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE      SERVICE
21/tcp unfiltered ftp
80/tcp unfiltered http
```

-sA mengirim ACK langsung dengan bypass SYN. Digunakan untuk pemetaan penggunaan firewall pada sistem target. Jika terdapat respon RST berarti port open dan bisa tersambung sehingga kemungkinan tidak menggunakan firewall. Jika tidak ada respon berarti ganguan jaringan dan bisa saja firewall aktif

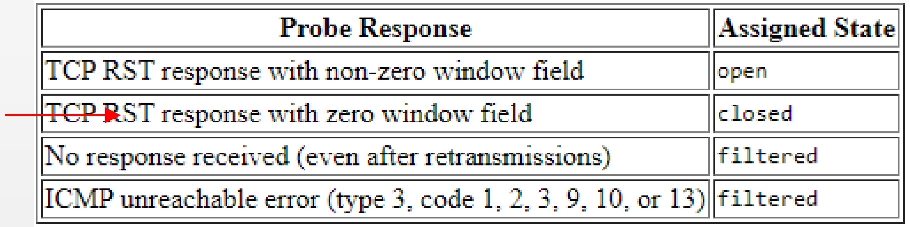


Probe Response	Assigned State
TCP RST response	unfiltered
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

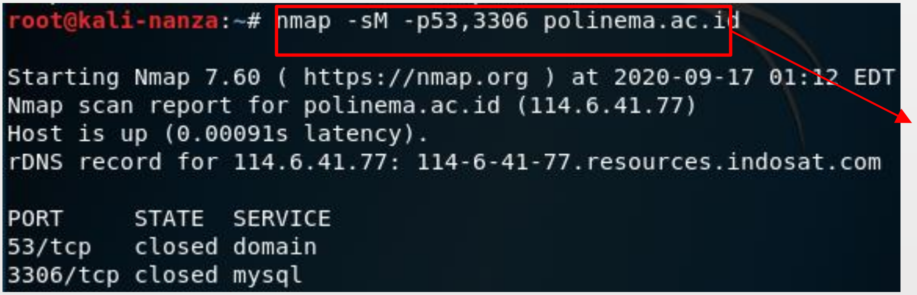


```
root@kali-nanza:~# nmap -sW -p22,443 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 01:11 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.00079s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT    STATE  SERVICE
22/tcp  closed ssh
443/tcp closed https
```

-sW melakukan TCP window scan dimana mengirim ACK untuk kemudian memeriksa respon RST secara lebih detail apakah header RST berisi window atau kosong. Jika RST berisi berarti meski closed namun sebenarnya open. Tetapi jika RST isinya kosong memang respon closed. RST berwindow ditemukan pada beberapa sistem khusus

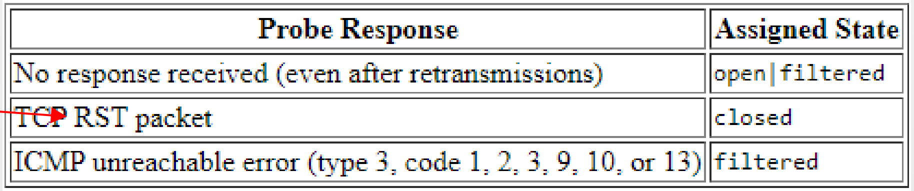


Probe Response	Assigned State
TCP RST response with non-zero window field	open
TCP RST response with zero window field	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

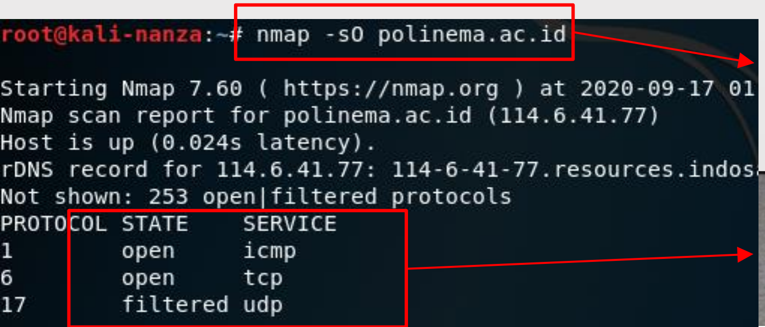


```
root@kali-nanza:~# nmap -sM -p53,3306 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 01:12 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.00091s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT     STATE  SERVICE
53/tcp   closed domain
3306/tcp closed mysql
```

-sM melakukan scan Maimon dimana sama seperti TCP FXN namun menggunakan FIN/ACK, terutama untuk sistem BSD



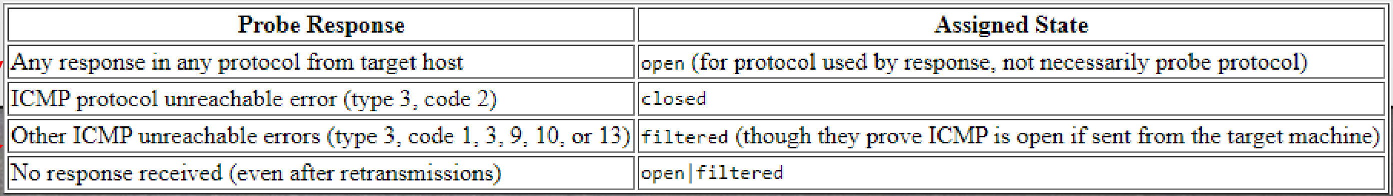
Probe Response	Assigned State
No response received (even after retransmissions)	open|filtered
TCP RST packet	closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered



```
root@kali-nanza:~# nmap -sO polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 01
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.024s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indos
Not shown: 253 open|filtered protocols
PROTOCOL STATE    SERVICE
1        open     icmp
6        open     tcp
17       filtered udp
```

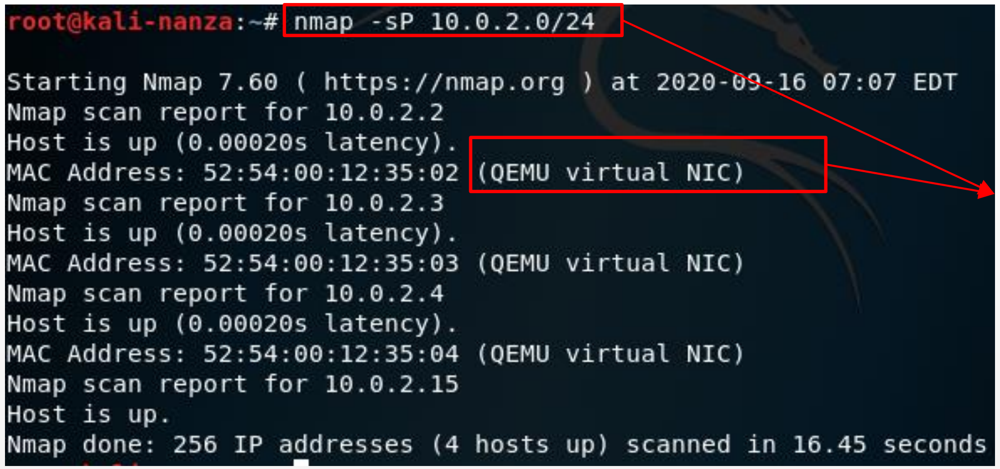
-sO memeriksa layanan protokol IP yang aktif

Open berarti ada respon, filtered berarti kesalahan koneksi ICMP



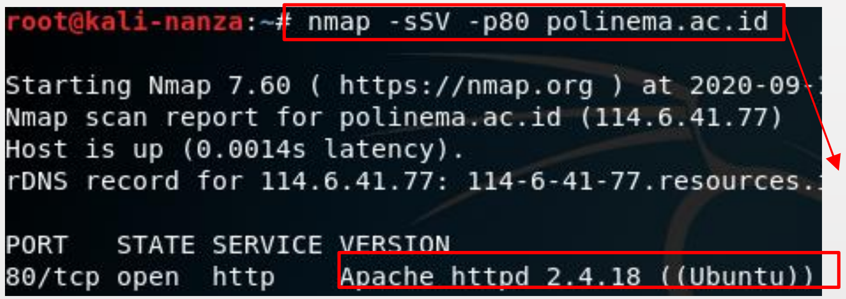
Probe Response	Assigned State
Any response in any protocol from target host	open (for protocol used by response, not necessarily probe protocol)
ICMP protocol unreachable error (type 3, code 2)	closed
Other ICMP unreachable errors (type 3, code 1, 3, 9, 10, or 13)	filtered (though they prove ICMP is open if sent from the target machine)
No response received (even after retransmissions)	open|filtered

NMAP - Intermediate



```
root@kali-nanza:~# nmap -sP 10.0.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-16 07:07 EDT
Nmap scan report for 10.0.2.2
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 16.45 seconds
```

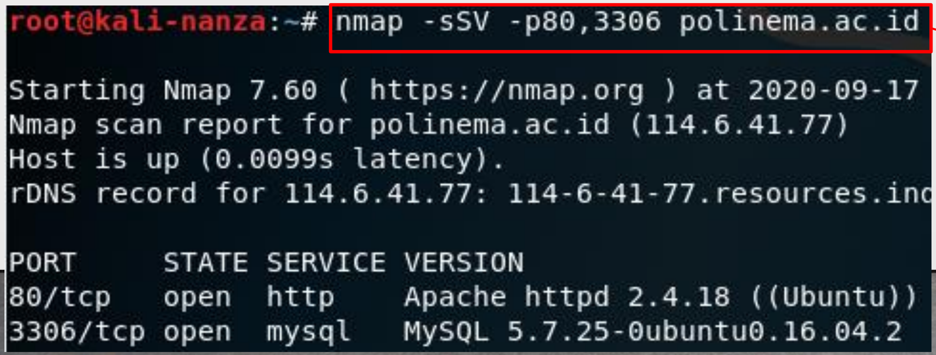
-sP Mengetahui IP n MAC address pada jaringan lokal. Karena menggunakan NAT Virtual maka yang terlihat host virtual



```
root@kali-nanza:~# nmap -sSV -p80 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0014s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

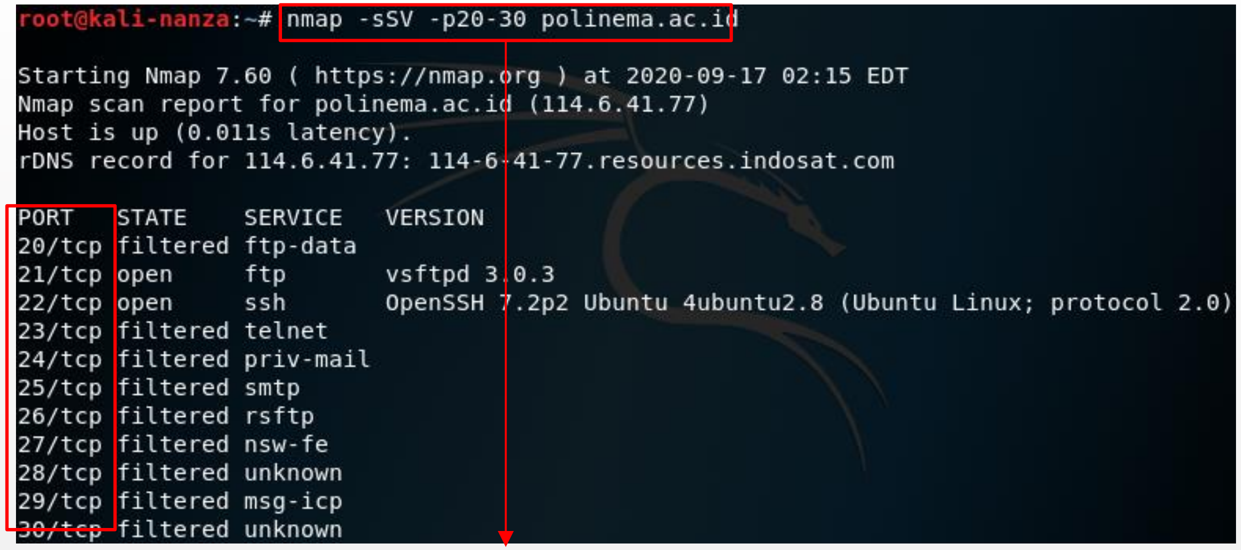
-p optional untuk port spesifik

V memeriksa versi



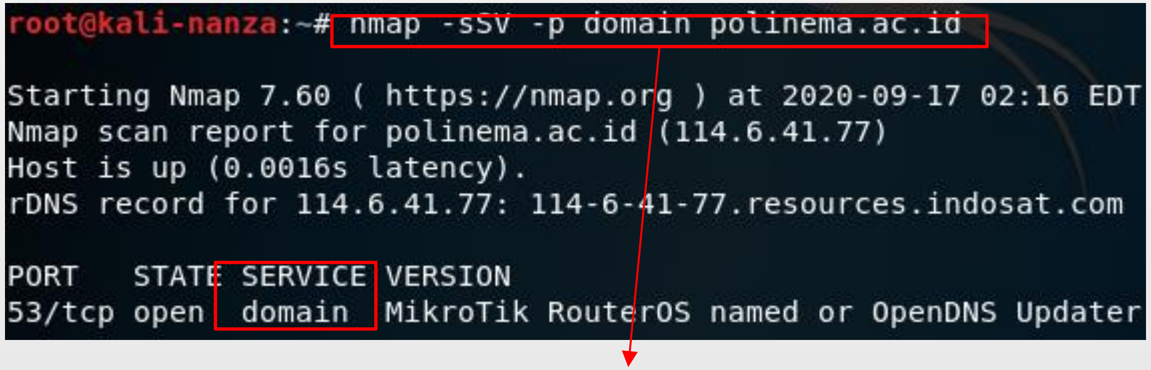
```
root@kali-nanza:~# nmap -sSV -p80,3306 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0099s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.ind

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.7.25-0ubuntu0.16.04.2
```

Optional –p boleh multipel



```
root@kali-nanza:~# nmap -sSV -p20-30 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:15 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.011s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE    SERVICE   VERSION
20/tcp filtered ftp-data
21/tcp open     ftp       vsftpd 3.0.3
22/tcp open     ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
23/tcp filtered telnet
24/tcp filtered priv-mail
25/tcp filtered smtp
26/tcp filtered rsftp
27/tcp filtered nsw-fe
28/tcp filtered unknown
29/tcp filtered msg-icp
30/tcp filtered unknown
```

Optional –p bisa inisiasi range

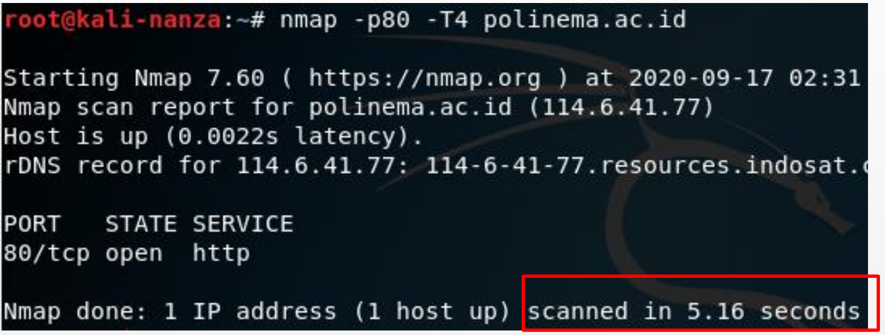


```
root@kali-nanza:~# nmap -sSV -p domain polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:16 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0016s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT    STATE SERVICE VERSION
53/tcp open  domain  MikroTik RouterOS named or OpenDNS Updater
```

Optional –p boleh bernilai String

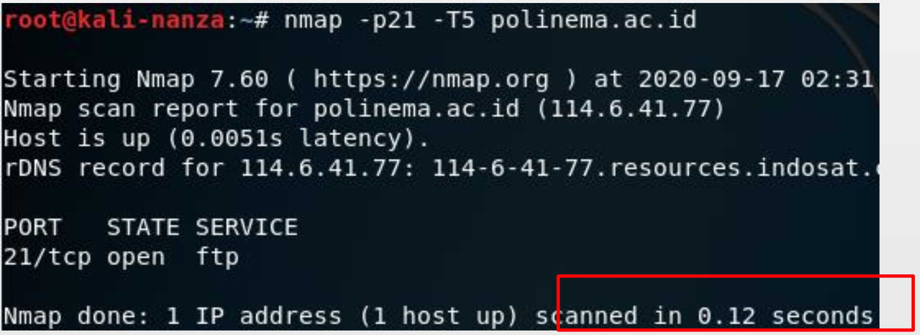
NMAP-Intermediate

Terdapat optional yang menyediakan template waktu scanning dari –T0(sangat lambat) sampai –T5(sangat agresif)



```
root@kali-nanza:~# nmap -p80 -T4 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:31
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0022s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

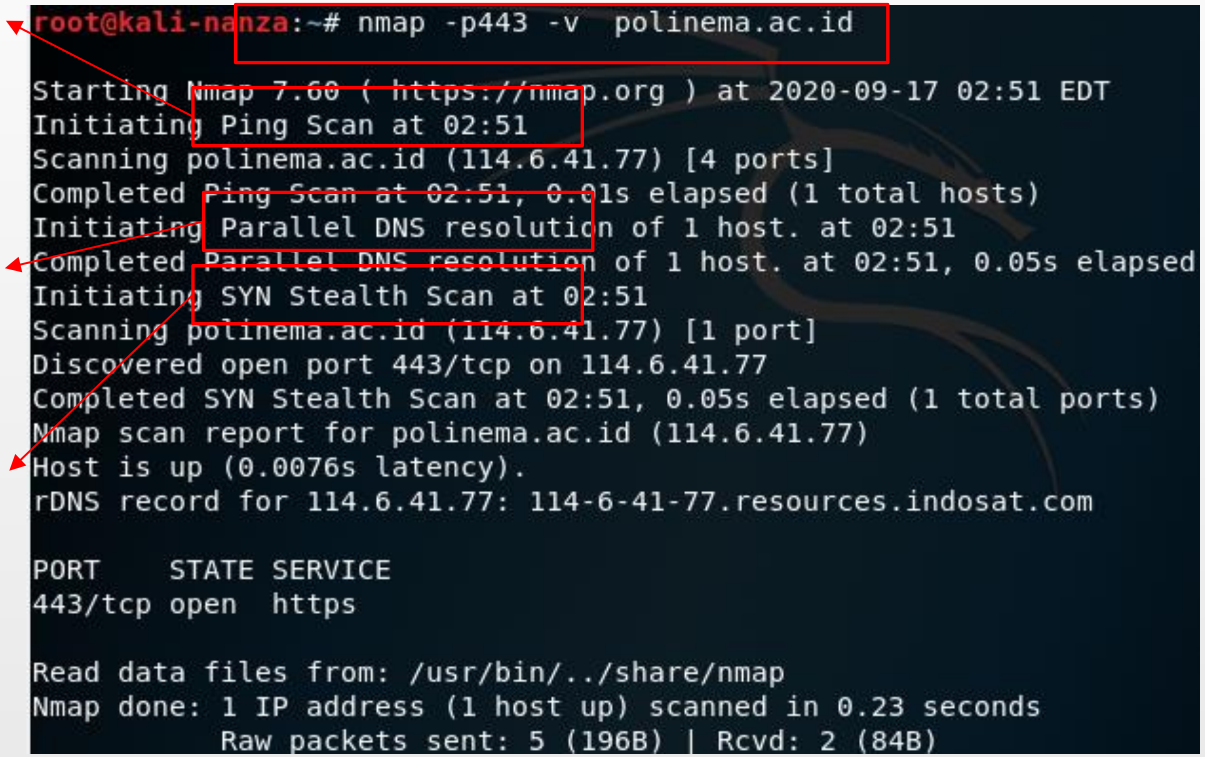
-T4 scanning menghabiskan waktu 5,16s



```
root@kali-nanza:~# nmap -p21 -T5 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:31
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0051s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

-T5 scanning menghabiskan waktu 0.12s

Dengan –v (varbose) tampilan scanning jadi lebih detail



Secara default Nmap mangawali dengan protokol ICMP Ping

Karena target diinisiasi dengan domain name maka perlu DNS

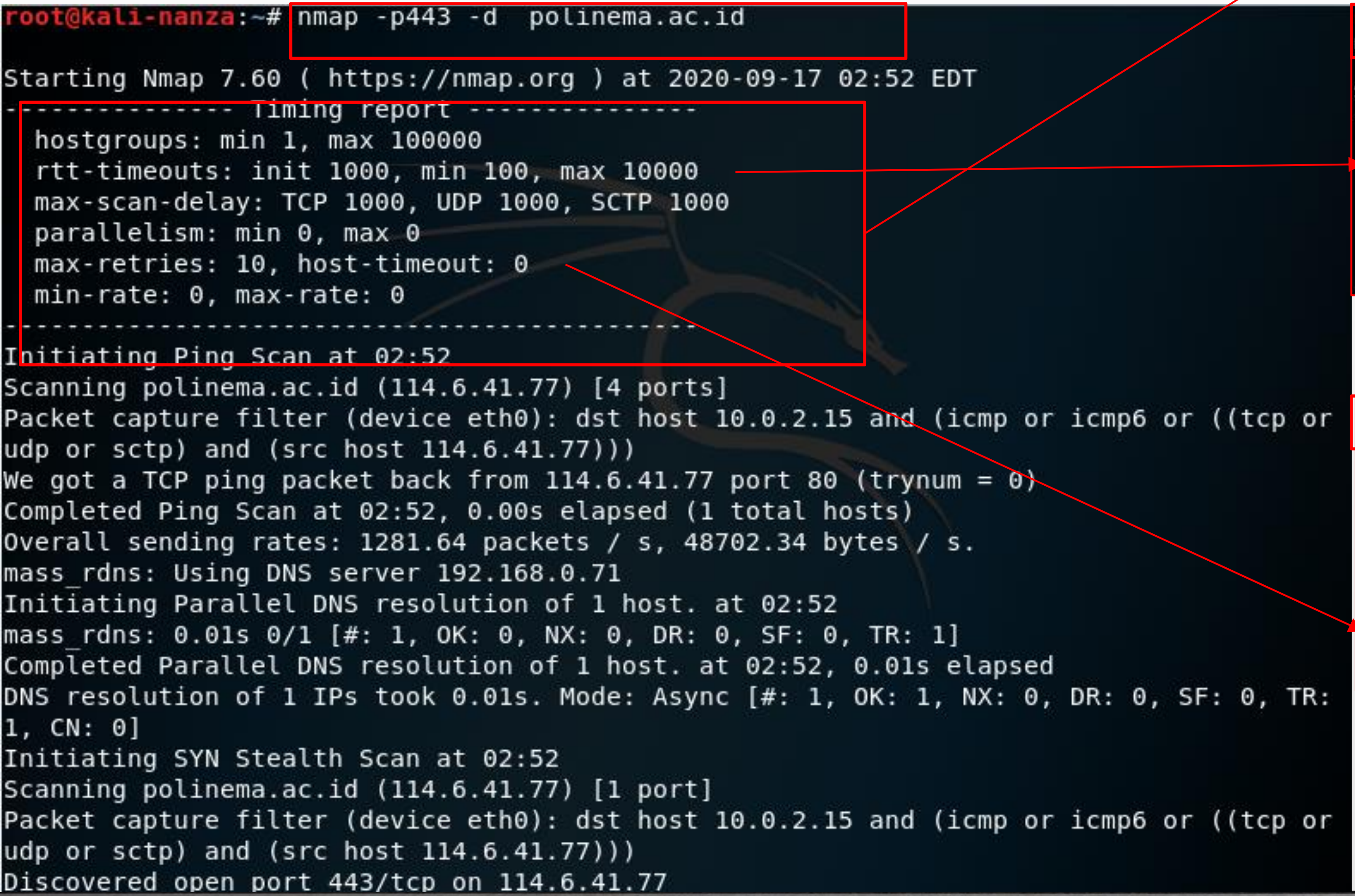
Koneksi TCP 3 Ways Handshake diawali SYN

```
root@kali-nanza:~# nmap -p443 -v  polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:51 EDT
Initiating Ping Scan at 02:51
Scanning polinema.ac.id (114.6.41.77) [4 ports]
Completed Ping Scan at 02:51, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:51
Completed Parallel DNS resolution of 1 host. at 02:51, 0.05s elapsed
Initiating SYN Stealth Scan at 02:51
Scanning polinema.ac.id (114.6.41.77) [1 port]
Discovered open port 443/tcp on 114.6.41.77
Completed SYN Stealth Scan at 02:51, 0.05s elapsed (1 total ports)
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0076s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT    STATE SERVICE
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```

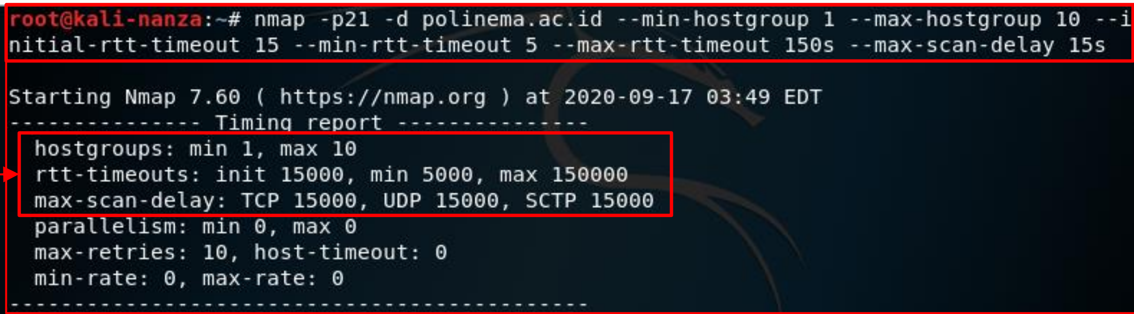
NMAP - Intermediate

Untuk tampilan scanning probing lebih detail dan lengkap dalam menamplkan informasi atribut bisa menggunakan optional –d. Satu target dengan satu port tampilan lebih dari satu halaman.

Timing bisa diubah atributnya sesuai dengan kebutuhan

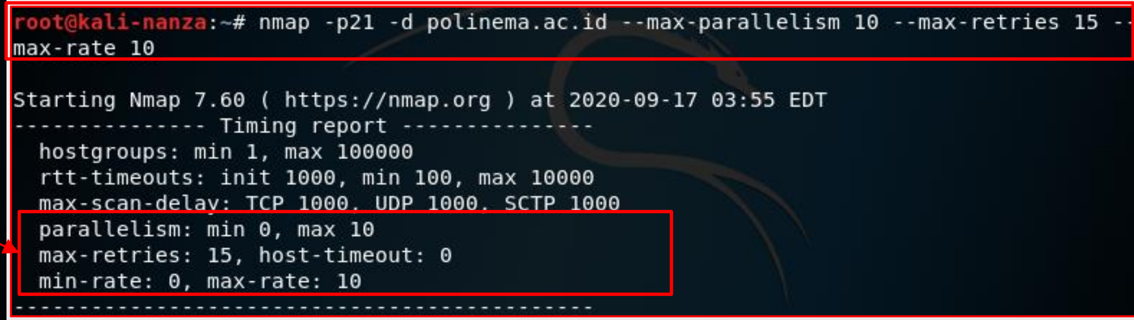


```
root@kali-nanza:~# nmap -p443 -d  polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 02:52 EDT
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Initiating Ping Scan at 02:52
Scanning polinema.ac.id (114.6.41.77) [4 ports]
Packet capture filter (device eth0): dst host 10.0.2.15 and (icmp or icmp6 or ((tcp or
udp or sctp) and (src host 114.6.41.77)))
We got a TCP ping packet back from 114.6.41.77 port 80 (trynum = 0)
Completed Ping Scan at 02:52, 0.00s elapsed (1 total hosts)
Overall sending rates: 1281.64 packets / s, 48702.34 bytes / s.
mass_rdns: Using DNS server 192.168.0.71
Initiating Parallel DNS resolution of 1 host. at 02:52
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 02:52, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR:
1, CN: 0]
Initiating SYN Stealth Scan at 02:52
Scanning polinema.ac.id (114.6.41.77) [1 port]
Packet capture filter (device eth0): dst host 10.0.2.15 and (icmp or icmp6 or ((tcp or
udp or sctp) and (src host 114.6.41.77)))
Discovered open port 443/tcp on 114.6.41.77
```



```
root@kali-nanza:~# nmap -p21 -d polinema.ac.id --min-hostgroup 1 --max-hostgroup 10 --i
nitial-rtt-timeout 15 --min-rtt-timeout 5 --max-rtt-timeout 150s --max-scan-delay 15s

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 03:49 EDT
-------------- Timing report --------------
  hostgroups: min 1, max 10
  rtt-timeouts: init 15000, min 5000, max 150000
  max-scan-delay: TCP 15000, UDP 15000, SCTP 15000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
-------------------------------------------
```

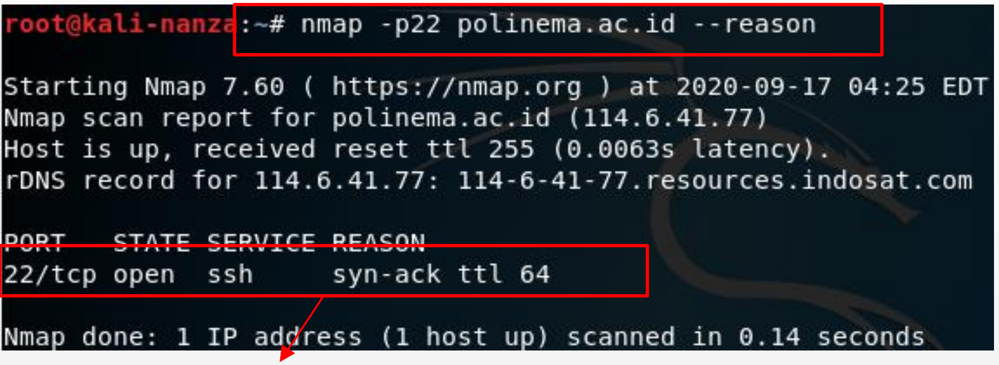
Hostgroup (jumlah host target) maks 10; rtt (rount trip time) maks 150s, min 5s, init 15s konversi jadi ms; maks scan delay 15s konversi jadi ms



```
root@kali-nanza:~# nmap -p21 -d polinema.ac.id --max-parallelism 10 --max-retries 15 --
max-rate 10

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 03:55 EDT
-------------- Timing report --------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 10
  max-retries: 15, host-timeout: 0
  min-rate: 0, max-rate: 10
-------------------------------------------
```

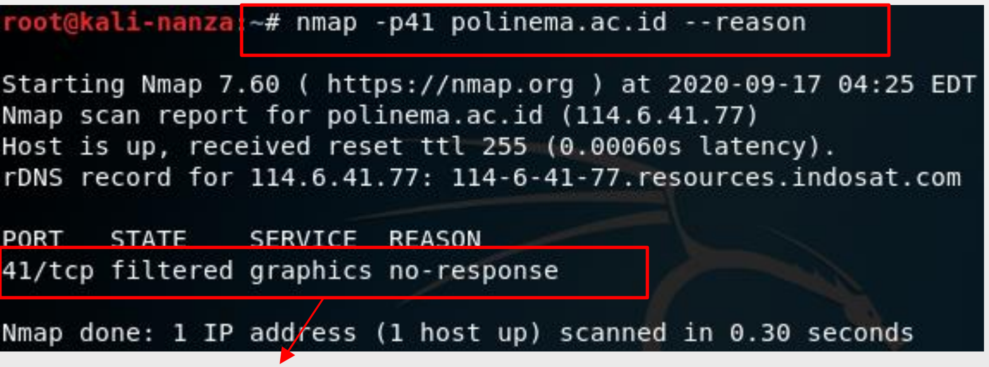
Ketika scan selesai nmap kembali ke atribut default. Diubah parallelism (jumlah port yang discan) maks 10; retries (jumlah percobaan scan) maks 15; dan rate (jumlah paket) maks 10

NMAP - Intermediate



```
root@kali-nanza:~# nmap -p22 polinema.ac.id --reason

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 04:25 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up, received reset ttl 255 (0.0063s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

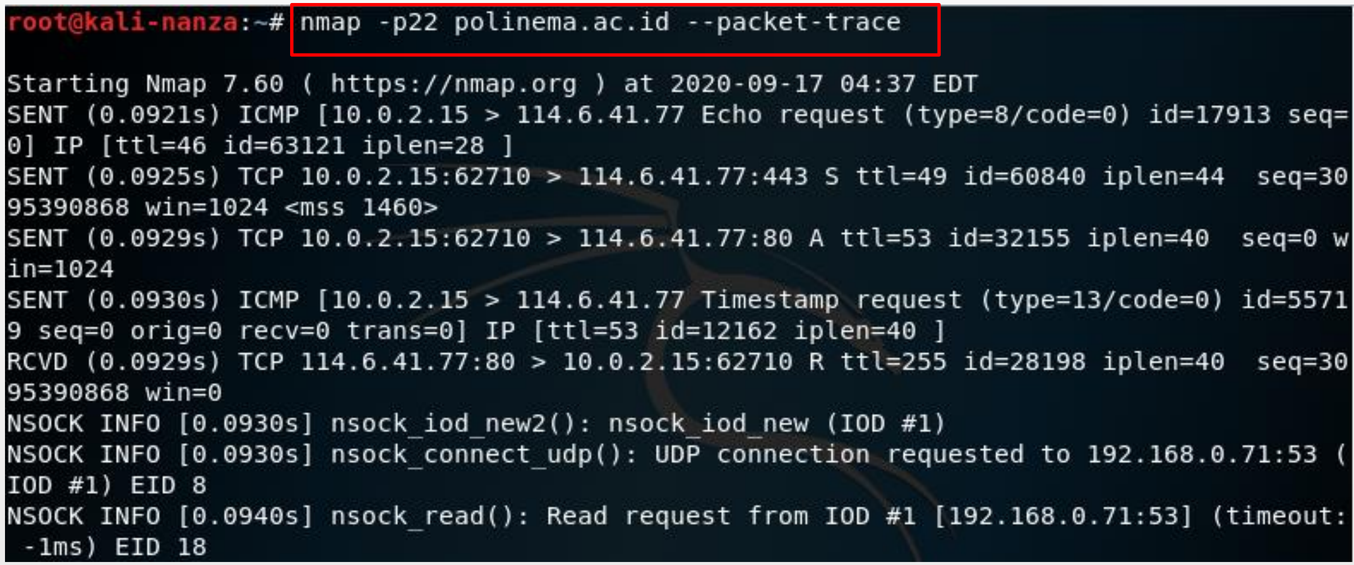
Dengan –reason akan diketahui penyebab dari state. State open karena berhasil SYN-ACK



```
root@kali-nanza:~# nmap -p41 polinema.ac.id --reason

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 04:25 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up, received reset ttl 255 (0.00060s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE    SERVICE  REASON
41/tcp filtered graphics no-response

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Dengan –reason akan diketahui penyebab dari state. State filtered karena tidak ada respon

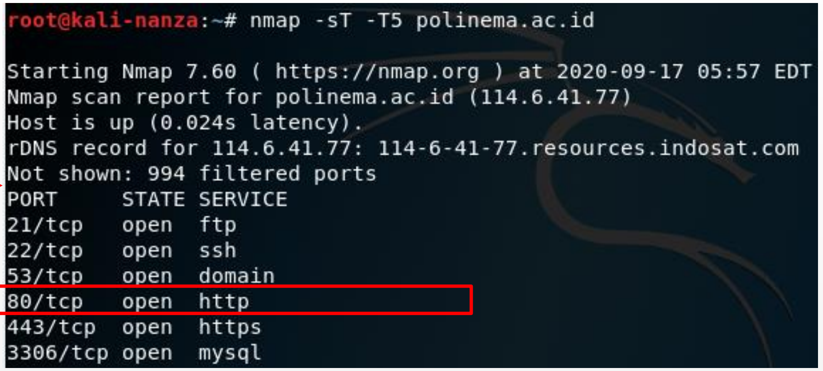
Dengan packet tracer bisa ditampilkan proses pengiriman packet Nmap untuk melakukan scanning dimulai dari Ping ICMP kemudian paket koneksi TCP



```
root@kali-nanza:~# nmap -p22 polinema.ac.id --packet-trace

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 04:37 EDT
SENT (0.0921s) ICMP [10.0.2.15 > 114.6.41.77 Echo request (type=8/code=0) id=17913 seq=
0] IP [ttl=46 id=63121 iplen=28 ]
SENT (0.0925s) TCP 10.0.2.15:62710 > 114.6.41.77:443 S ttl=49 id=60840 iplen=44  seq=30
95390868 win=1024 <mss 1460>
SENT (0.0929s) TCP 10.0.2.15:62710 > 114.6.41.77:80 A ttl=53 id=32155 iplen=40  seq=0 w
in=1024
SENT (0.0930s) ICMP [10.0.2.15 > 114.6.41.77 Timestamp request (type=13/code=0) id=5571
9 seq=0 orig=0 recv=0 trans=0] IP [ttl=53 id=12162 iplen=40 ]
RCVD (0.0929s) TCP 114.6.41.77:80 > 10.0.2.15:62710 R ttl=255 id=28198 iplen=40  seq=30
95390868 win=0
NSOCK INFO [0.0930s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0930s] nsock_connect_udp(): UDP connection requested to 192.168.0.71:53 (
IOD #1) EID 8
NSOCK INFO [0.0940s] nsock_read(): Read request from IOD #1 [192.168.0.71:53] (timeout:
 -1ms) EID 18
```

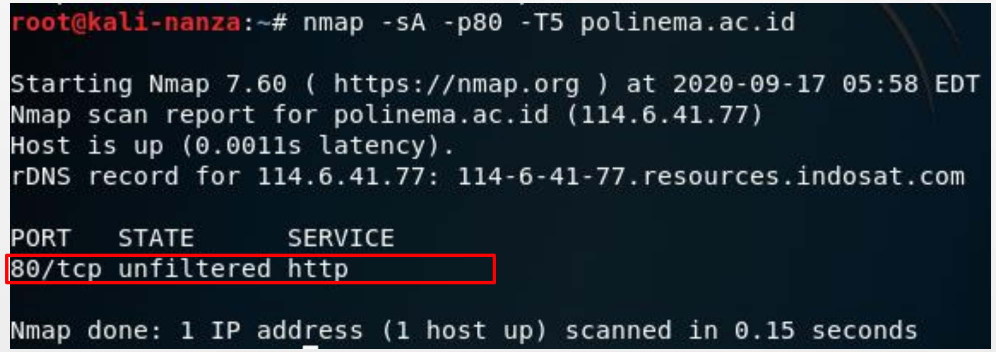
NMAP – Deteksi Firewall

1. **Cari port terbuka**
2. **Scan salah satu port sebagai sample menggunakan ACK**
3. **Jika hasil filtered berarti menggunakan Firewall**



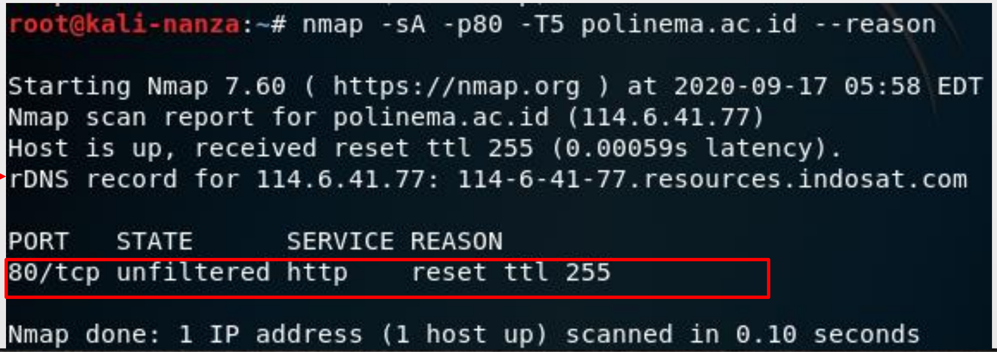
```
root@kali-nanza:~# nmap -sT -T5 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 05:57 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.024s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
```

Mencari port terbuka, tetapi penetrasi akan kesulitan jika firewall aktif. Untuk itu pilih port yang menjadi target untuk diperiksa apakah firewall aktif



```
root@kali-nanza:~# nmap -sA -p80 -T5 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 05:58 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.0011s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE      SERVICE
80/tcp unfiltered http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Menggunakan scanning ACK dimana koneksi port di-bypass dari sinyal SYN. Jika target respon RST berarti unfiltered artinya mau respon sehingga tidak ada pengahalang firewall. Jika target tanpa respon apa-apa berarti filtered, terdapat firewall

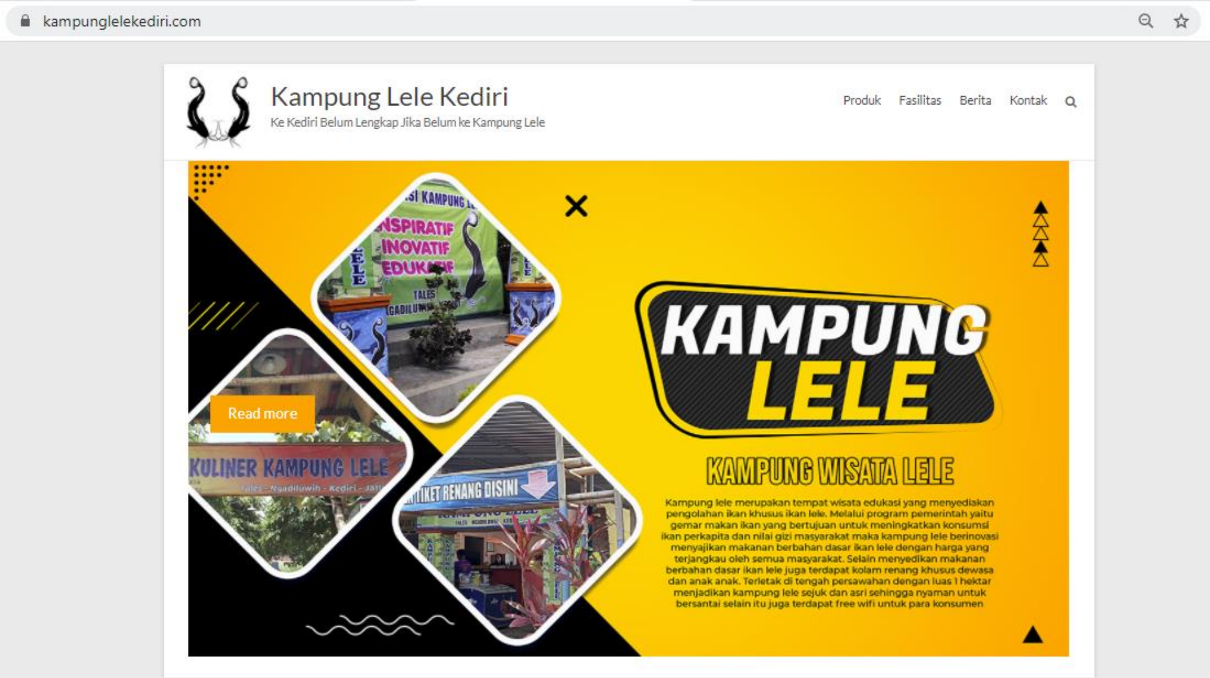


```
root@kali-nanza:~# nmap -sA -p80 -T5 polinema.ac.id --reason

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 05:58 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up, received reset ttl 255 (0.00059s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE      SERVICE REASON
80/tcp unfiltered http    reset ttl 255

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Alasan kenapa unfiltered bisa menggunakan optional –reason dimana terdapat reset yang artinya target merespon RST sehingga firewall tidak aktif

TUGAS

- Lakukan Scanning dan Probing dengan target

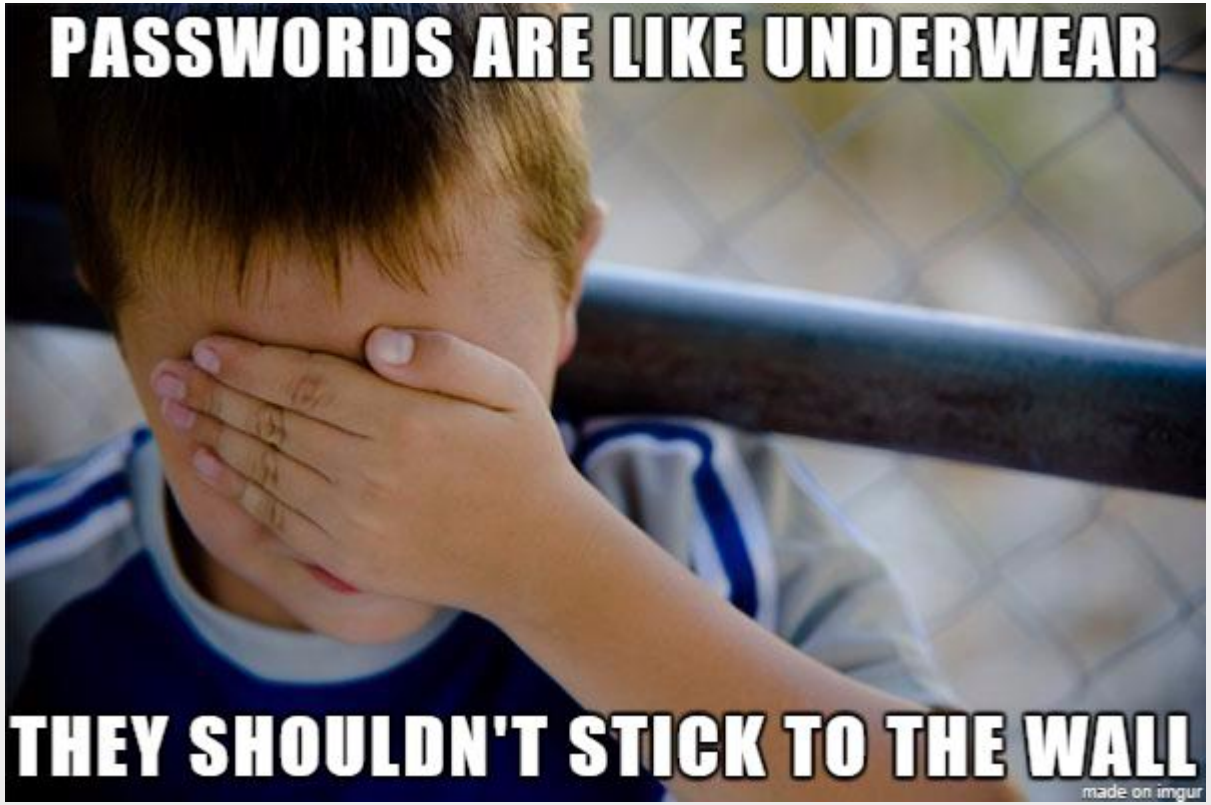


Kampung lele merupakan tempat wisata edukasi yang menyediakan pengolahan ikan khusus ikan lele. Melalui program pemerintah yaitu gemar makan ikan yang bertujuan untuk meningkatkan konsumsi ikan perkapita dan nilai gizi masyarakat maka kampung lele berinovasi menyajikan makanan berbahan dasar ikan lele dengan harga yang terjangkau oleh semua masyarakat. Selain menyedikan makanan berbahan dasar ikan lele juga terdapat kolam renang khusus dewasa dan anak anak. Terletak di tengah persawahan dengan luas 1 hektar menjadikan kampung lele sejuk dan asri sehingga nyaman untuk bersantai selain itu juga terdapat free wifi untuk para konsumen

Buat rekaman layar secara individu:

- Buka website https://kampunglelekediri.com, buka salah satu menu Kontak pada website
- Melalui Kali, cari informasi port TCP yang terbuka apa saja, termasuk versi yang digunakan
- Pilih salah satu port kemudian periksa secara lebih detail apakah memang benar-benar terbuka
- Pada port tersebut, cari informasi apakah target mengaktifkan firewall pada port tersebut

TERIMAKASIH


PASSWORDS ARE LIKE UNDERWEAR
THEY SHOULDN'T STICK TO THE WALL
made on imgur