

Modul Praktikum V

Perintah Netstat dan Nmap

Kompetensi:

1. Mahasiswa mengetahui dan memahami penggunaan perintah netstat pada OS Windows dan OS Linux
2. Mahasiswa mengetahui dan memahami penggunaan perintah nmap pada OS Linux.

Alat dan bahan:

1. Komputer dengan OS Windows dan OS Linux
2. Kabel UTP
3. Koneksi internet

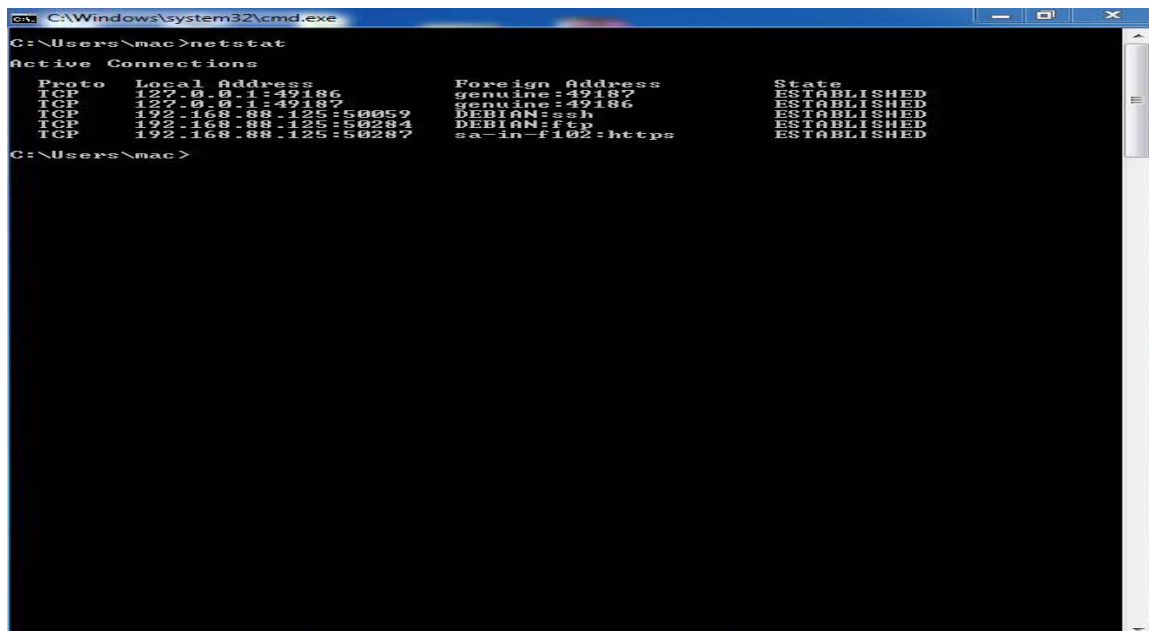
Ulasan Teori

1. Netstat

Netstat (**Network Statistics**) adalah program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal (LAN) maupun jaringan internet. Netstat dapat digunakan jika pada suatu ketika sedang internetan kemudian tiba tiba koneksi menjadi sangat lambat dan dicurigai ada program di komputer yang menjadi penyebabnya. Jika hal tersebut dialami maka perlu memanggil program netstat untuk melakukan pengecekan.

Berikut adalah tampilan dari perintah netstat di os windows dan os linux:

- a. Tampilan perintah netstat di windows dijalankan pada command prompt



```
C:\Windows\system32\cmd.exe
C:\Users\nmac>netstat
Active Connections
Proto Local Address           Foreign address         State
TCP    127.0.0.1:49186          genuine:49186           ESTABLISHED
TCP    127.0.0.1:49186          genuine:49186           ESTABLISHED
TCP    192.168.88.125:50059     DEBIAN:ssh             ESTABLISHED
TCP    192.168.88.125:50284     DEBIAN:ftp              ESTABLISHED
TCP    192.168.88.125:50287     sa-in-f102:https        ESTABLISHED
C:\Users\nmac>
```

Beberapa parameter lain yang bisa anda gunakan untuk perintah netstat.

1. netstat -a <host/ip target>, menampilkan semua koneksi baik yang listening maupun yang tidak
2. netstat -e <host/ip target>, menampilkan statistik paket yang dikirim dan yang diterima
3. netstat -n <host/ip target>, menampilkan alamat dan port dalam bentuk numerik
4. netstat -o <host/ip target>, menampilkan PID (Process ID) untuk setiap koneksi
5. netstat -s <host/ip target>, menampilkan statistik per protokol
6. netstat -r <host/ip target>, menampilkan routing table
7. netstat -p <host/ip target>, menampilkan statistik berdasarkan port tertentu

Berikut ini keterangan dari output netstat diatas :

1. **Proto.** Kolom proto menunjukan jenis protokol yang dipakai bisa TCP atau UDP.
2. **Local Address.** Kolom ini menjelaskan alamat dan nomor port yang ada di komputer yang mana saat itu sedang aktif melakukan koneksi. Contoh diatas 192.168.88.125 adalah nama host dari komputer saya dan 50059 adalah nomor port di komputer saya yang sedang melakukan koneksi.
3. **Foreign Address.** Kolom ini menunjukan koneksi yang dituju oleh local address beserta nomor portnya. Contoh diatas komputer sedang koneksi ke server DEBIAN melalui ssh (port 22) yang artinya sedang koneksi ke server ssh.
4. **State.** Kolom ini menunjukan status dari koneksi yang sedang terjadi. ESTABLISHED artinya sudah terhubung dengan komputer lain dan siap mengirimkan data.

State yang mungkin terjadi :

1. LISTENING -> siap untuk melakukan koneksi
2. SYN_SENT -> mengirimkan paket SYN
3. SYN_RECEIVED -> menerima paket SYN
4. ESTABLISHED -> koneksi terjadi dan siap mengirimkan data
5. TIME_WAIT -> sedang menunggu koneksi

b. Tampilan perintah netstat di linux dijalankan pada terminal

```
root@debian:/home/yuri# netstat | more
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 debian-4.local:ssh      mac-PC.local:50059      ESTABLISHED
tcp        0      0 debian-4.local:ssh      mac-PC.local:49823      ESTABLISHED
tcp        0      0 debian-4.local:telnet    mac-PC.local:49824      ESTABLISHED
udp6       0      0 localhost:59829          localhost:59829          ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node  Path
unix    29      [ ]         DGRAM      -           5404      /dev/log
unix    3        [ ]         STREAM     CONNECTED   40046     -
unix    3        [ ]         STREAM     CONNECTED   40045     -
unix    3        [ ]         STREAM     CONNECTED   40042     @/tmp/dbus-P37asQ7xX0
unix    3        [ ]         STREAM     CONNECTED   40041     -
unix    3        [ ]         STREAM     CONNECTED   40020     @/tmp/dbus-P37asQ7xX0
unix    3        [ ]         STREAM     CONNECTED   40019     -
unix    3        [ ]         STREAM     CONNECTED   39995     @/tmp/.X11-unix/X0
unix    3        [ ]         STREAM     CONNECTED   39994     -
unix    3        [ ]         STREAM     CONNECTED   39987     @/tmp/dbus-dyCpFTezkr
unix    3        [ ]         STREAM     CONNECTED   39986     -
unix    3        [ ]         STREAM     CONNECTED   39907     /var/run/dbus/system_
bus_socket
unix    3        [ ]         STREAM     CONNECTED   39906     -
unix    2        [ ]         DGRAM      -           39903     -
--More--
```

Berikut ini beberapa parameter untuk perintah netstat di linux

1. netstat -a <host/ip target>, menampilkan semua koneksi baik yang listening maupun yang tidak
2. netstat -l <host/ip target>, menampilkan semua koneksi yang listening saja
3. netstat -s <host/ip target>, menampilkan statistik per protokol
4. netstat -n <host/ip target>, menampilkan dalam bentuk numerik
5. netstat -o <host/ip target>, menampilkan timer
6. netstat -g <host/ip target>, menampilkan berdasarkan group membership
7. netstat -i <host/ip target>, menampilkan tabel network interface
8. netstat -p <host/ip target>, menampilkan spesifik port pada mesin target
9. netstat -O <host/ip target>, mengidentifikasi sistem operasi mesin
10. netstat -sV <host/ip target>, mengidentifikasi service yang berjalan pada port

Untuk lebih jelasnya untuk melihat manual dari program netstat ini dengan cara mengetikkan perintah :

man netstat

Perlu diingat linux bersifat case-sensitive artinya huruf besar dan huruf kecil dianggap berbeda. Jadi perintah netstat -n dengan netstat -N itu berbeda.

2. NMAP

Nmap (“Network Mapper”) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Informasi itu adalah “tabel port”. Tabel tersebut berisi daftar angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi probe Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika ia tidak dapat menentukan status manakah yang menggambarkan sebuah port.

Cara Menggunakan Nmap

Berikut beberapa contoh teknik yang dapat digunakan menggunakan nmap.

- Memeriksa port yang terbuka
`nmap<host/IP target>`
- Memeriksa spesifik port pada mesin target
`nmap -p <host/IP target>`
- Memeriksa service yang berjalan pada port
`nmap -sV <host/IP target>`

- Memeriksa port mesin target dalam 1 segmen jaringan
nmap <host/IP target>
- Mengidentifikasi sistem operasi mesin
nmap -O <host/IP target>

Langkah-Langkah Praktikum

1. Netstat di OS Windows

- Pastikan komputer anda terkoneksi dengan jaringan lokal maupun interne
- Buka browser anda akseslah suatu alamat website
- Buka netstat pada windows dengan cara Start> All Programs> Accessories> Command Prompt atau Start> Run> ketik cmd lalu Ok. Ketikkan perintah netstat
- Screenshot hasil dari perintah netstat, kemudian analisislah apa yang terjadi
- Coba beberapa parameter netstat berikut ini:
 - netstat -a
 - netstat -e
 - netstat -n
 - netstat -o
 - netstat -s
 - netstat -r
 - netstat -p
- Jelaskan screenshot hasil percobaan anda, catat dan laporkan hasil analisa anda.

2. Netstat di OS Linux

- Pastikan komputer anda terkoneksi dengan jaringan lokal maupun interne
- Buka browser anda akseslah suatu alamat website
- Buka netstat pada linux caranya klik Start> Applications> Accessories> Root Terminal> tekan enter.
- Pada terminal linux ketikkan **netstat |more** (tekan enter), tambahan option **|more** digunakan supaya tampil perlayar, sehingga memudahkan melihat data yang tampil
- Screenshot hasil dari perintah netstat, kemudian analisislah apa yang terjadi
- Coba beberapa

- netstat -a
- netstat -l
- netstat -s
- netstat -n
- netstat -o
- netstat -g
- netstat -i menampilkan network interface tertentu misal netstat -i eth0
- netstat -p
- netstat -O
- netstat -sV
- netstat -p 1-65535 -sV -O <host/ip target>

g. Jelaskan screenshot hasil percobaan anda, catat dan laporkan hasil analisa anda.

3. Nmap Di OS Linux

- Pastikan komputer anda terkoneksi dengan jaringan lokal maupun internet
- Buka terminal pada linux anda
- Ketikkan perintah pada terminal `#dpkg --get-architecture`, seperti dibawah ini untuk mengetahui apakah paket nmap sudah terinstall di komputer linux anda



The screenshot shows a terminal window titled "Terminal (as superuser)". The command `dpkg --get-architecture` has been executed, resulting in the following output:

```

root@debian:/home/yuri# dpkg --get-architecture
ii nmap                     6.00-0.3+deb7u1          i386
    The Network Mapper
root@debian:/home/yuri#

```

- d. Pastikan server ssh di OS Linux anda telah terinstall untuk mengamati port 22 pada ssh , jika belum terinstall lakukan proses instalasi paket ssh dengan perintah `#apt-get install ssh`.
- e. Aktifkan server tersebut dengan perintah `#/etc/init.d/ssh restart`
- f. Ketikkan perintah `nmap` dengan memasukkan alamat ip address tujuan yang mau dianalisa, sebagai contoh `#nmap 192.168.130.169`



```
Applications  Places  Thu Sep 29, 5:32 AM

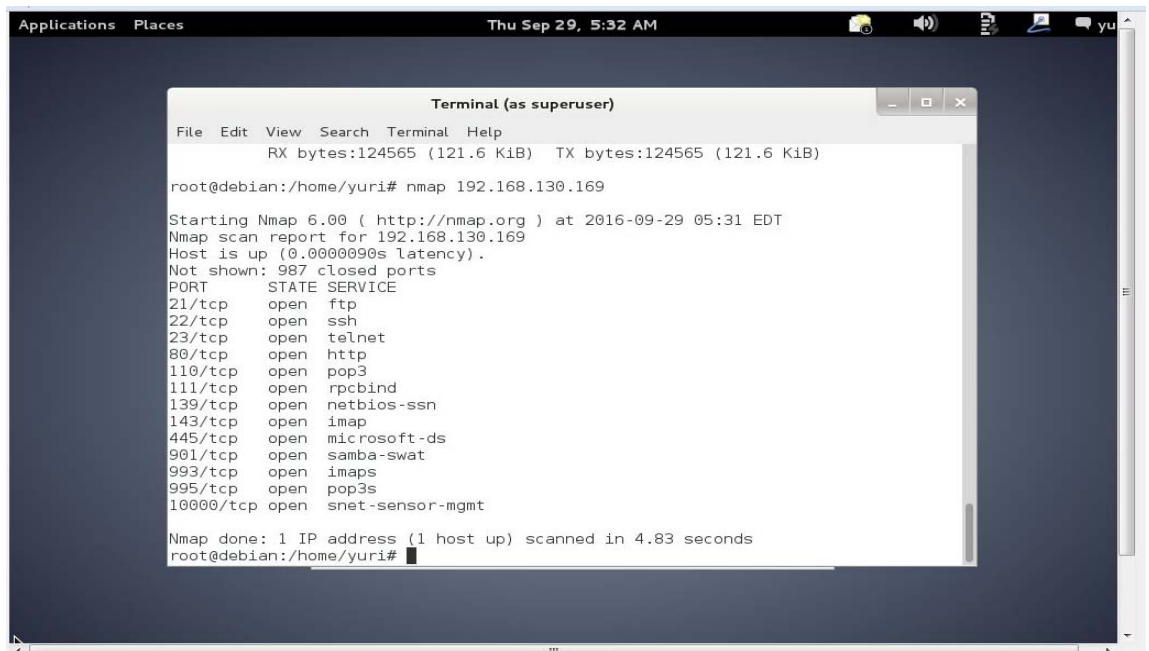
Terminal (as superuser)
File Edit View Search Terminal Help
RX bytes:124565 (121.6 KiB) TX bytes:124565 (121.6 KiB)

root@debian:/home/yuri# nmap 192.168.130.169

Starting Nmap 6.00 ( http://nmap.org ) at 2016-09-29 05:31 EDT
Nmap scan report for 192.168.130.169
Host is up (0.0000090s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
901/tcp   open  samba-swat
993/tcp   open  imaps
995/tcp   open  pop3s
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
root@debian:/home/yuri#
```

- g. Pada screenshot diatas port ssh statusnya “open”
- h. Lakukan perintah stop service ssh `#/etc/init.d/ssh stop`



```
Applications  Places  Thu Sep 29, 5:32 AM

Terminal (as superuser)
File Edit View Search Terminal Help
RX bytes:124565 (121.6 KiB) TX bytes:124565 (121.6 KiB)

root@debian:/home/yuri# nmap 192.168.130.169

Starting Nmap 6.00 ( http://nmap.org ) at 2016-09-29 05:31 EDT
Nmap scan report for 192.168.130.169
Host is up (0.0000090s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
901/tcp   open  samba-swat
993/tcp   open  imaps
995/tcp   open  pop3s
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
root@debian:/home/yuri#
```

- i. Amati perubahan percobaan yang terjadi, screenshot hasil percobaan anda
- j. Catat dan laporkan hasil analisa anda
- k. Lakukan percobaan pada target <host/ip> komputer teman Anda. Kemudian jelaskan apa hasilnya sebagai laporan.