MODUL 1
NETWORK SCANNING
DAN PROBING

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep Scanner dan Probing
2. Mahasiswa memahami konsep layanan jaringan dan port numbering
3. Mahasiswa mampu menganalisa kelemahan jaringan menggunakan software scanning yang ada

DASAR TEORI

Server tugasnya adalah melayani client dengan menyediakan service yang dibutuhkan. Server menyediakan service dengan bermacam-macam kemampuan, baik untuk lokal maupun remote. Server listening pada suatu port dan menunggu incomming connection ke port. Koneksi bisa berupa lokal maupuan remote.

Port sebenarnya suatu alamat pada stack jaringan kernel, sebagai cara dimana transport layer mengelola koneksi dan melakukan pertukaran data antar komputer. Port yang terbuka mempunyai resiko terkait dengan exploit. Perlu dikelola port mana yang perlu dibuka dan yang ditutup untuk mengurangi resiko terhadap exploit.

Ada beberapa utility yang bisa dipakai untuk melakukan diagnosa terhadap sistem service dan port kita. Utility ini melakukan scanning terhadap sistem untuk mencari port mana saja yang terbuka, ada juga sekaligus memberikan laporan kelemahan sistem jika port ini terbuka.

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host, cracker harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila cracker sudah mengetahui bahwa host menjalankan proses ftp server, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses. Dari bagian ini kita dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

Type Scanning

connect scan (-sT)

Jenis scan ini konek ke port sasaran dan menyelesaikan three-way handshake (SYN, SYN/ACK, dan ACK). Scan jenis ini mudah terdeteksi oleh sistem sasaran.

-sS (TCP SYN scan)

Paling populer dan merupakan scan default nmap. SYN scan juga sukar terdeteksi, karena tidak menggunakan 3 way handshake secara lengkap, yang disebut sebagai teknik half open scanning. SYN scan juga efektif karena dapat membedakan 3 state port, yaitu open, filterd ataupun close. Teknik ini dikenal sebagai half-opening scanning karena

suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING. Suatu RST/ACT akan dikirim oleh mesin yang melakukan scanning sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat siluman dibandingkan TCP connect penuh, dan tidak aka tercatat pada log sistem sasaran.

TCP FIN scan (-sF)
Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX.

TCP Xmas Tree scan (-sX)
Teknik ini mengirimkan suatu paket FIN, URG, dan PUSH ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.

TCP Null scan (-sN)
Teknik ini membuat off semua flag. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk semua port yang tertutup.

TCP ACK scan (-sA)
Teknik ini digunakan untuk memetakan set aturan firewall. Dapat membantu menentukan apakah firewall itu merupakan suatu simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.

TCP Windows scan
Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem-sistem tertentu (sebagai contoh, AIX dan FreeBSD) sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan.

TCP RPC scan
Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta normor versi yang berhubungan dengannya.

UDP scan (-sU)
Teknik ini mengirimkan suatu paket UDP ke port sasaran. Bila port sasaran memberikan respon berupa pesan (ICMP port unreachable) artinya port ini tertutup. Sebaliknya bila tidak menerima pesan di atas, kita dapat menyimpulkan bahwa port itu terbuka. Karena UDP dikenal sebagai connectionless protocol, akurasi teknik ini sangat bergantung pada banyak hal sehubungan dengan penggunaan jaringan dan system resource. Sebagai tambahan, UDP scanning merupakan proses yang amat lambat apabila anda mencoba men-scan suatu perangkat yang menjalankan packet filtering berbeban tinggi.

Beberapa Tools dan cara scanning ke sistem

Netstat

Netstat merupakan utility yang powerfull untuk menngamati current state pada server, service apa yang listening untuk incomming connection, interface mana yang listening, siapa saja yang terhubung.

Nmap

Merupakan software scanner yang paling tua yang masih dipakai sampai sekarang.

Nessus

Nessus merupakan suatu tools yang powerfull untuk melihat kelemahan port yang ada pada komputer kita dan komputer lain. Nessus akan memberikan report secara lengkap apa kelemahan komputer kita dan bagaimana cara mengatasinya.

Contoh Scanning menggunakan nmap tipe tcp syn scan

```
# nmap -sT -v 192.168.0.10

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-04-11
12:30 EDT
Initiating Connect() Scan against 192.168.0.10 [1663 ports] at 12:30
Discovered open port 3389/tcp on 192.168.0.10
Discovered open port 80/tcp on 192.168.0.10
Discovered open port 3306/tcp on 192.168.0.10
Discovered open port 445/tcp on 192.168.0.10
Discovered open port 139/tcp on 192.168.0.10
Discovered open port 520/tcp on 192.168.0.10
Discovered open port 135/tcp on 192.168.0.10
The Connect() Scan took 1.45s to scan 1663 total ports.
Host 192.168.0.10 appears to be up ... good.
Interesting ports on 192.168.0.10:
(The 1656 ports scanned but not shown below are in state: closed)
PORT   STATE   SERVICE
80/tcp  open       http
135/tcp  filtered    msrpc
139/tcp  filtered    netbios-ssn
445/tcp  open       microsoft-ds
520/tcp  open       efs
3306/tcp open       mysql
3389/tcp open       ms-term-serv
MAC Address: 00:30:48:11:AB:5A (Supermicro Computer)

Nmap finished: 1 IP address (1 host up) scanned in 2.242 seconds
```

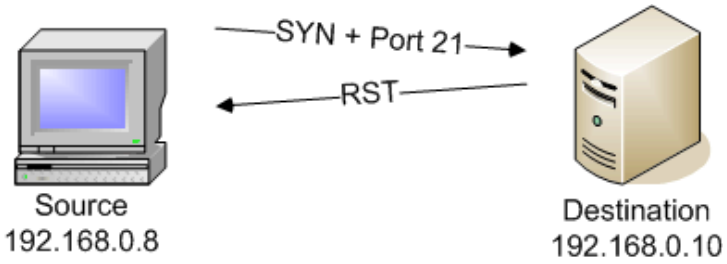
```
# nmap -sP 192.168.4.0/24
```

Option –sP merupakan salah satu type scanning dari Nmap berbasis ICMP, dimana umumnya dipergunakan untuk melakukan ping terhadap sejumlah IP sekaligus.

Mendeteksi OS dengan Nmap

```
# nmap -O no_ip_target
```

Pada dasarnya tcp SYN melakukan half koneksi ke target dan secara berulang-ulang mencari port yang terbuka



TUGAS PENDAHULUAN

1. Sebutkan langkah dasar yang biasa dipakai untuk melakukan proses hacking !
2. Sebutkan cara penggunaan netstat dan option-option yang dipakai serta arti option tersebut ?
3. Sebutkan cara pemakaian software nmap dengan menggunakan tipe scanning:
   - TCP Connect scan
   - TCP SYN Scan
   - TCP FIN scan
   - TCP Xmas Tree scan
   - TCP null scan
   - TCP ACK scan
   - TCP Windows scan
   - TCP RPC scan
   - UDP scan
   - OS fingerprinting
4. Bagaimana cara mematikan dan menghidupkan service yang ada
5. Sebutkan cara pemakaian software nessus untuk melihat kelemahan sistem jaringan kita !

PERCOBAAN

1. Melihat status service yang aktif di local komputer
   Gunakan command netstat –tpane dan netstat –tupane bandingkan hasilnya .
   Lakukan beberapa option netstat untuk mengetahui hanya tcp atau udp saja yang terlihat
   Lakukan pula options – options yang lain
2. Pastikan nmap dan wireshark terinstal pada komputer anda,jika belum lakukan installasi
   - Jalankan wireshark pada komputer target lalu lakukan command nmap pada komputer sumber, analisa hasil dan perilaku data yang dikirim ke jaringan oleh masing- masing nmap.
   - Pastikan koneksi terhubung dengan baik antara komputer sumber dan target, gunakan perintah ping.
     Misal beberapa perintah nmap berikut
     nmap –sT –v Nama_IP_Target
     nmap –sS –v Nama_IP_Target

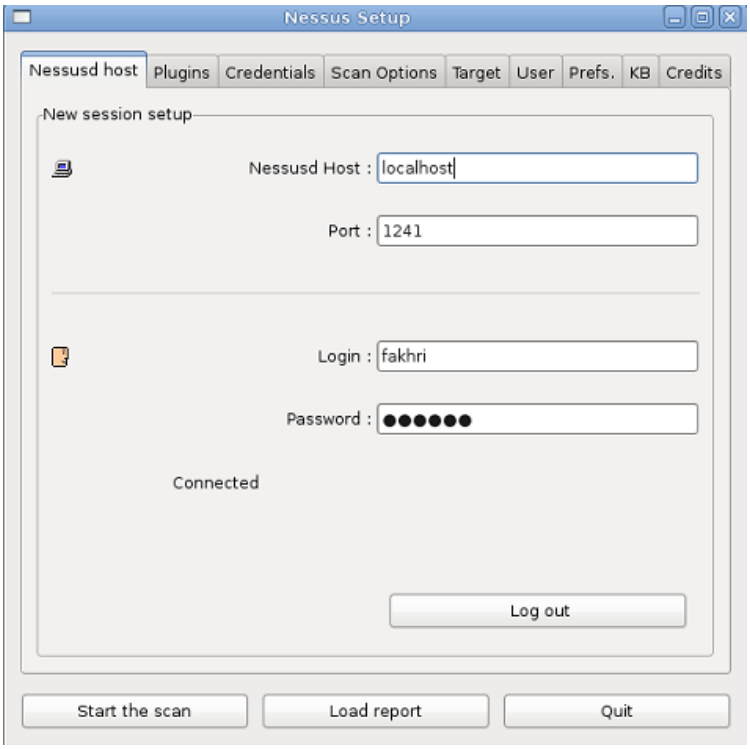
nmap –O –v Nama_IP_Target
nmap –sF –v Nama_IP_Target

- Mintalah pada komputer yg discan untuk menjalankan scanning pada diri sendiri. Cocokkan dengan hasil scanning nmap.
  # nmap localhost
  Salin hasilnya dan bandingkan. Sama atau tidak ? Mengapa?
- Jalankan nmap dengan beberapa option yang berdasarkan tipe-tipe scanning yang ada (FIN scan, TCP Xmas Tree scan, TCP null scan, TCP ACK scan, TCP Windows scan, TCP RPC scan, UDP scan, OS fingerprinting) dan analisa perilaku data yang dikirim dengan wireshark.

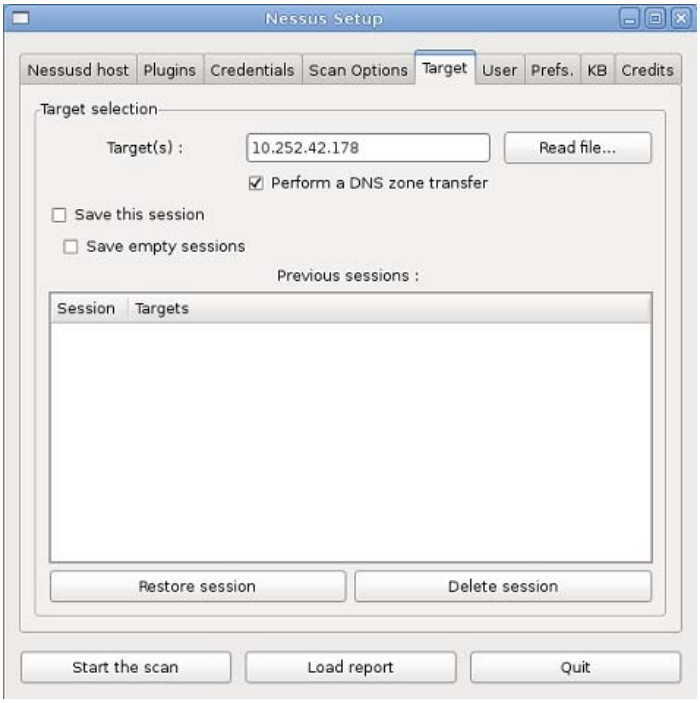
3. Pastikan nessus terinstal pada komputer anda, lakukan installasi.
   Berikut beberapa langkah installasi nessus

```
#apt-get install nessus nessusd -y

#nessus-adduser

Add a new nessusd user
----------------------


Login : faruq
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that isbat has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)



Login             : faruq
Password          : ***********
DN                :
Rules             :



Is that ok ? (y/n) [y] y
user added.

#pens1:/home/faruq# /etc/init.d/nessusd start  -> sbg nessus server
#Starting Nessus daemon: nessusd.

#pens1:/home/faruq# nessus                    -> sbg nessus client
```

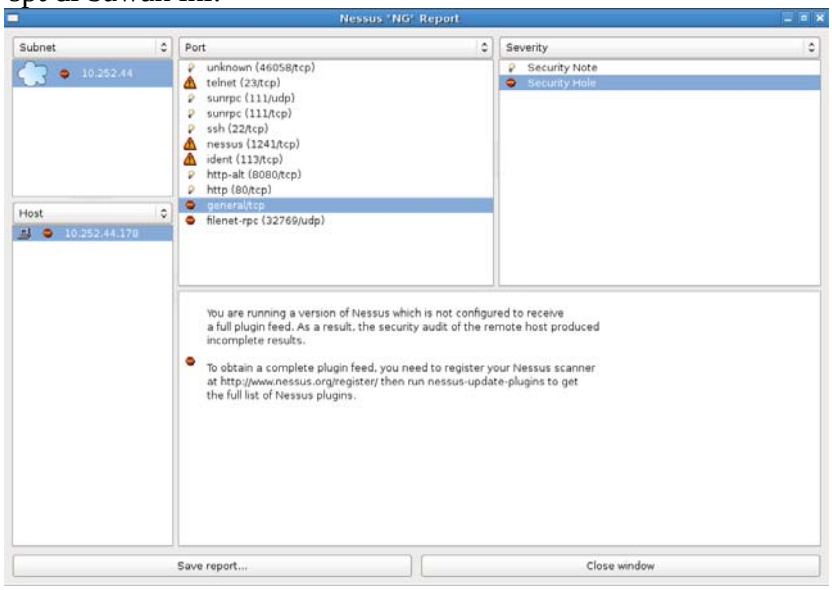
Jalankan nessus dan lakukan scanning ke beberapa komputer teman
Awalnya melakukan setup



Untuk melakukan scanning buka tab **Target** dan masukkan no_IP target , setelah itu klik **Start the Scan** , dan akan butuh beberapa waktu.

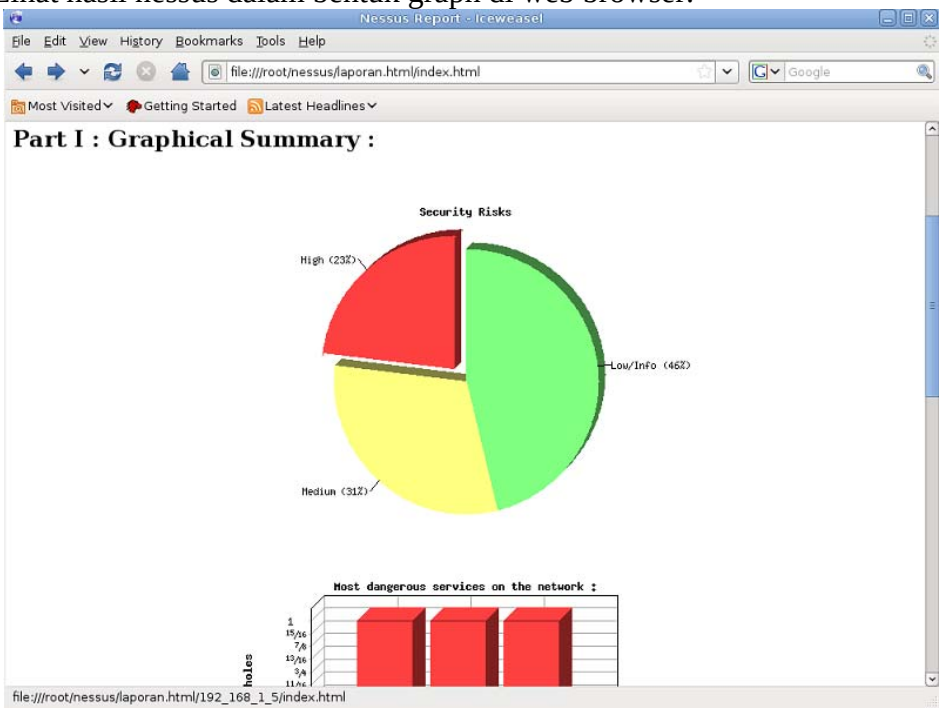


Lihat hasil vulnerabilitas pada sistem dan tulis kelemahan-kelemahan target yang ada Misal hole spt di bawah ini:



4. Simpan report-nya dalam bentuk HTML agar lebih mudah dianalisa.

5. Lihat hasil nessus dalam bentuk graph di web browser.



6. Lakukan analisa paket nessus dan bandingkan dengan yang dilakukan nmap.

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Sebutkan option atau bentuk-bentuk scanning yang bisa dilakukan nmap
3. Cari di internet beberap tools scanning yang ada dan bagaimana cara pemakaian dan hasilnya?

LEMBAR ANALISA

Praktikum Network Security (Network Scanning dan Probing)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Percobaan mengunakan perintah ”netstat” (poin 1)

B. Percobaan mengunakan perintah ”nmap” (poin 2), bandingkan hasilnya dari masing-masing perintah nmap

- `nmap –sT –v no_ip_target`
- `nmap –sS –v no_ip_target`
- `nmap –sF –v no_ip_target`
- `nmap –sX –v no_ip_target`
- `nmap –sA –v no_ip_target`
- `nmap –sN –v no_ip_target`
- `nmap –sU –v no_ip_target`
- `nmap –O no_ip_target`

Note : Jika nmap –sU terlalu lama, dapat dicancel dgn Ctrl + C

C. Percobaan mengunakan nessus, catat hasil scan yang didapat oleh nessus