KEAMANAN KOMPUTER DAN JARINGAN

Faldi, M.Ti
Muhammad Taufiq Sumadi, M.Tr.Kom

LAPORAN PRAKTIKUM 1 : Scanning dan Probing

Oleh :

Nama.....

Nim...

Teknik Informatika
Fakultas Sains & Teknologi
Universitas Muhammadiyah Kalimantan Timur

Samarinda, 2023

Laporan Praktikum 1:
Scanning dan Probing

Pokok Bahasan:

- ❖ Konsep Scanning dan Probing
- ❖ Penggunaan Tools SS dan Nmap

Tujuan Pembelajaran:

- ✔ Mengenalkan pada mahasiswa tentang konsep Scanning dan Probing.
- ✔ Mahasiswa memahami konsep layanan jaringan dan port numbering.
- ✔ Mahasiswa mampu menganalisis kelemahan jaringan menggunakan software scanning yang ada.

Dasar Teori:

1. Konsep Scanning dan Probing

Probing adalah suatu teknik atau metode pengujian pada sistem jaringan untuk memperoleh informasi atau data yang berkaitan dengan sistem jaringan tersebut. Tujuan dari probing adalah untuk mengetahui sistem jaringan yang akan diuji dan menemukan celah keamanan yang mungkin ada di dalamnya.

Probing dilakukan dengan cara mengirimkan paket data ke sistem jaringan dan menganalisis respon yang diterima. Paket data yang dikirimkan biasanya berisi permintaan informasi yang spesifik, seperti sistem operasi yang digunakan, layanan yang tersedia, dan konfigurasi jaringan. Probing dapat dilakukan dengan cara yang berbeda, baik itu secara pasif maupun aktif.

Probing pasif tidak mengirimkan data ke sistem jaringan, sehingga tidak akan terdeteksi oleh sistem. Teknik ini dapat dilakukan dengan mengumpulkan data dari lalu lintas jaringan yang ada, seperti data paket yang sedang diproses oleh router atau switch. Dengan teknik ini, pelaku probing dapat memperoleh informasi tanpa menyebabkan gangguan pada sistem jaringan.

Probing aktif mengirimkan data ke sistem jaringan, sehingga dapat terdeteksi oleh sistem. Teknik ini dapat dilakukan dengan menggunakan berbagai tools, seperti Nmap, Nessus, dan OpenVAS. Dalam hal ini, pelaku probing akan mengirimkan paket data ke sistem jaringan dan menganalisis respon yang diterima untuk memperoleh informasi tentang sistem jaringan tersebut.

Probing sangat penting dalam keamanan jaringan karena dapat membantu mengidentifikasi celah keamanan pada sistem jaringan. Dengan teknik ini, administrator jaringan dapat memeriksa keamanan sistem jaringan mereka dan memastikan bahwa sistem jaringan terlindungi dari serangan hacker atau malware.

Scanning adalah suatu teknik atau metode pengujian pada sistem jaringan yang bertujuan untuk memeriksa port yang terbuka dan layanan yang tersedia di dalam sistem jaringan tersebut. Teknik ini biasanya dilakukan untuk mengidentifikasi celah keamanan pada sistem jaringan dan memperoleh informasi yang berguna tentang jaringan tersebut.

Scanning dilakukan dengan cara mengirimkan paket data ke sistem jaringan dan menganalisis respon yang diterima. Paket data yang dikirimkan biasanya berisi permintaan informasi tentang port dan layanan yang tersedia di dalam sistem jaringan. Scanning dapat dilakukan dengan cara yang berbeda, seperti scanning TCP, UDP, dan SYN.

Scanning TCP adalah teknik scanning yang paling umum dilakukan. Dalam teknik ini, pelaku scanning mengirimkan paket TCP ke sistem jaringan dan menganalisis respon yang diterima untuk memeriksa port yang terbuka dan layanan yang tersedia di dalam sistem jaringan. Pelaku scanning dapat menggunakan tools seperti Nmap, Netcat, dan hping untuk melakukan scanning TCP.

Scanning UDP adalah teknik scanning yang digunakan untuk memeriksa layanan yang berjalan di atas protokol UDP. Teknik ini sering digunakan untuk memeriksa celah keamanan pada protokol DNS, SNMP, dan DHCP. Pelaku scanning dapat menggunakan tools seperti Nmap dan Netcat untuk melakukan scanning UDP.

Scanning SYN adalah teknik scanning yang digunakan untuk memeriksa port yang terbuka pada sistem jaringan. Dalam teknik ini, pelaku scanning mengirimkan paket SYN ke sistem jaringan dan menganalisis respon yang diterima untuk memeriksa port yang terbuka. Pelaku scanning dapat menggunakan tools seperti Nmap dan hping untuk melakukan scanning SYN.

Scanning sangat penting dalam keamanan jaringan karena dapat membantu mengidentifikasi celah keamanan pada sistem jaringan. Dengan teknik ini, administrator jaringan dapat memeriksa keamanan sistem jaringan mereka dan memastikan bahwa sistem jaringan terlindungi dari serangan hacker atau malware.

Probing dan scanning adalah teknik yang berbeda dalam pengujian keamanan jaringan. Probing digunakan untuk mencari informasi umum tentang jaringan atau sistem jaringan, sedangkan scanning digunakan untuk memeriksa port yang terbuka dan layanan yang tersedia di dalam sistem jaringan.

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 incoming connection ke port. Koneksi bisa berupa lokal maupun 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, filtered 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 akan 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 nomor 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.

2. Beberapa Tools dan cara scanning ke sistem

   SS (Socket Statistics) adalah sebuah perintah pada sistem operasi Linux yang digunakan untuk menampilkan informasi tentang jaringan socket, termasuk port yang sedang didengarkan, koneksi aktif, dan informasi lainnya. Perintah SS biasanya digunakan untuk mengetahui kinerja jaringan, memantau koneksi, dan memperbaiki masalah jaringan.

   Berikut ini adalah beberapa contoh penggunaan SS pada Linux:

   Menampilkan daftar port yang sedang didengarkan pada sistem:

   ```
   # ss -tulw
   ```

Menampilkan daftar koneksi aktif pada sistem:

```
# ss -t -a
```

Menampilkan informasi tentang semua koneksi UDP pada sistem:

```
# ss -u -a
```

Menampilkan statistik tentang koneksi TCP pada sistem:

```
# ss -s
```

Menampilkan daftar semua koneksi yang ditolak pada sistem:

```
# ss -a -e -i '(tcp|udp)' '(sport = :ssh or dport = :ssh)'
```

Pada contoh terakhir, perintah SS digunakan untuk menampilkan daftar semua koneksi yang ditolak pada sistem dengan menggunakan filter untuk port SSH.

Penggunaan SS sangat berguna untuk memantau koneksi jaringan dan mendeteksi masalah pada jaringan. Dengan menggunakan perintah SS secara teratur, administrator jaringan dapat dengan cepat menemukan koneksi yang bermasalah dan mengambil tindakan yang diperlukan untuk memperbaiki masalah tersebut.

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

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 t o 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 ( Super micro Computer )
Nmap finished: 1 I P address ( 1 host up) scanned i n 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.

Tugas Pendahuluan:

1. Sebutkan langkah dasar yang biasa dipakai untuk melakukan proses hacking!
2. Sebutkan cara penggunaan ss dan option-option yang dipakai serta arti option tersebut?
3. Sebutkan cara pemakaian software nmap dengan menggunakan tipe scanning:
   - 3.1. TCP Connect scan
   - 3.2. TCP SYN Scan
   - 3.3. TCP FIN scan
   - 3.4. TCP Xmas Tree scan
   - 3.5. TCP null scan
   - 3.6. TCP ACK scan
   - 3.7. TCP Windows scan
   - 3.8. TCP RPC scan
   - 3.9. UDP scan
   - 3.10. OS fingerprinting
4. Bagaimana cara mematikan dan menghidupkan service pada linux, misal: service yang ingin dihidupkan dan dimatikan adalah web server apache.

Percobaan & Latihan:

1. **Melakukan instalasi nmap pada Kali Linux yang terdapat di dalam VirtualBox:** Pastikan Kali Linux yang berada di dalam VirtualBox sudah diaktifkan dan terhubung ke internet. Uji dengan melakukan ping ke 8.8.8.8
   Jawaban (sertakan screenshot hasil).
2. Buka Terminal di Kali Linux dengan mengklik drop down menu di atas kiri sebelah icon terminal, klik Root Terminal Emulator.
   Jawaban (sertakan screenshot hasil).
3. Ketikkan perintah berikut untuk memperbarui daftar paket di Kali Linux:

   ```
   # apt update
   ```
   Jawaban (sertakan screenshot hasil).
4. Setelah selesai, ketikkan perintah berikut untuk menginstal nmap:

   ```
   # apt install nmap
   ```
   Jawaban (sertakan screenshot hasil).
5. Tunggu hingga proses instalasi selesai. Setelah selesai, nmap akan terinstal di Kali Linux yang berada di dalam VirtualBox. Untuk memeriksa apakah nmap sudah terinstal dengan benar, Anda dapat menjalankan perintah berikut:

   ```
   # nmap --version
   ```
   Jawaban (sertakan screenshot hasil).
6. Shutdown kali linux anda untuk proses selanjutnya.
   Jawaban (sertakan screenshot hasil).
7. **Install tools ssh server, apache, dan ftp pada debian 10:** Buka terminal pada Debian. Masuk dengan super user (root) dengan perintah.
   `# su`
   Jawaban (sertakan screenshot hasil).
8. Instal SSH server dengan menjalankan perintah berikut di terminal:

   ```
   # apt-get install ssh
   ```
   Jawaban (sertakan screenshot hasil).
9. Cek status SSH dan pastikan sudah aktif, dengan cara:

   ```
   # systemctl status ssh
   ```
   Jawaban (sertakan screenshot hasil).
10. Instal Apache dengan menjalankan perintah berikut di terminal:

    ```
    # apt-get install apache2
    ```
    Jawaban (sertakan screenshot hasil).
11. Cek status apache dan pastikan sudah aktif, dengan cara:

    ```
    # systemctl status apache2
    ```
    Jawaban (sertakan screenshot hasil).

12. Instal FTP dengan menjalankan perintah berikut di terminal:
    ```
    # apt-get install vsftpd
    ```
    Jawaban (sertakan screenshot hasil).

13. Cek status FTP dan pastikan sudah aktif, dengan cara:
    ```
    # systemctl status vsftpd
    ```
    Jawaban (sertakan screenshot hasil).

14. **Mengatur jaringan internal pada VirtualBox untuk menghubungkan 2 guest OS:** Buka VirtualBox Manager dan pilih salah satu mesin virtual yang ingin dihubungkan ke mesin virtual lain.
    Jawaban (sertakan screenshot hasil).
15. Klik kanan pada mesin virtual dan pilih "Settings".
    Jawaban (sertakan screenshot hasil).
16. Pilih "Network" dari menu di sebelah kiri.
    Jawaban (sertakan screenshot hasil).
17. Pilih “Adapter 2” klik enable, di bawah "Adapter 2", pilih "Internal Network" dari dropdown menu "Attached to".
    Jawaban (sertakan screenshot hasil).
18. Ulangi langkah 14-17 untuk mesin virtual kedua.
    Jawaban (sertakan screenshot hasil).
19. Nyalakan kedua mesin virtual dan masuk ke sistem operasi masing-masing.
    Jawaban (sertakan screenshot hasil).
20. **Langkah-langkah untuk mengatur IP address pada Debian melalui terminal:** Buka terminal pada Debian. Masuk dengan super user (root) dengan perintah.
    ```
    # su
    ```
    Jawaban (sertakan screenshot hasil).
21. Periksa interface jaringan yang tersedia dengan perintah:
    ```
    # ip address
    ```
    Jawaban (sertakan screenshot hasil).
22. Buat salinan file konfigurasi default interface jaringan dengan menjalankan perintah:
    ```
    # cp /etc/network/interfaces /etc/network/interfaces.orig
    ```
    Jawaban (sertakan screenshot hasil).
23. Buka file konfigurasi interface jaringan dengan perintah:
    ```
    # nano /etc/network/interfaces
    ```
    Jawaban (sertakan screenshot hasil).
24. Untuk mengkonfigurasi IP address statis, tambahkan konfigurasi berikut pada file interfaces pada baris paling bawah: catatan: sesuaikan **[nama_interface]** dengan adapter yg menggunakan tipe internal network pada langkah 17.
    ```
    auto [nama_interface]
    iface [nama_interface] inet static
    ```

```
address [alamat_IP]
netmask [netmask_address]
gateway [alamat_gateway]
```

Misalnya, jika interface jaringan yang digunakan adalah eth0, dan alamat IP yang ingin dikonfigurasi adalah 192.168.1.100, maka konfigurasinya akan terlihat seperti berikut:

```
auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1
```

Jawaban (sertakan screenshot hasil).

25. Setelah selesai mengkonfigurasi, simpan file dan keluar dari editor nano dengan menekan ctrl+x, y, enter.
    Jawaban (sertakan screenshot hasil).
26. Restart interface jaringan dengan perintah:
    # systemctl restart networking
    Jawaban (sertakan screenshot hasil).
27. Periksa apakah konfigurasi IP address sudah diterapkan dengan benar menggunakan perintah:
    `# ip address`
    Jawaban (sertakan screenshot hasil).
28. Ulangi langkah 20-27 untuk kali linux, dan pada langkah 24 bedakan ip address pada kali linux, berikan ip address pada kali linux 192.168.1.2, selain itu sama.
    Jawaban (sertakan screenshot hasil).
29. Uji koneksi pada kali linux dan debian dengan menjalankan perintah ping.
    `# ping [ip_debian]`
    Jawaban (sertakan screenshot hasil).
30. **Jalankan nmap pada kali linux untuk melakukan scanning pada debian**. Kali linux sebagai attacker dan Debian sebagai server. Menjalankan nmap pada host tunggal:
    `# nmap [alamat_IP]`
    Jawaban (sertakan screenshot hasil).

    Hasil Analisa.
31. Menjalankan nmap pada kisaran alamat IP:
    `# nmap [alamat_IP1]-[alamat_IP2]`
    Jawaban (sertakan screenshot hasil).

    Hasil Analisa.
32. Menjalankan nmap pada seluruh subnet jaringan:

```
# nmap [alamat_subnet]/24
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

33. Menampilkan informasi hostname, sistem operasi, dan versi aplikasi yang dijalankan oleh host:
```
# nmap -A [alamat_IP]
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

34. Melakukan scanning port dengan nmap:
```
# nmap -p [nomor_port] [alamat_IP]
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

35. Menjalankan nmap dalam mode verbose untuk menampilkan lebih banyak detail:
```
# nmap -v [alamat_IP]
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

36. Menjalankan nmap dengan opsi output ke file:
```
# nmap -oN [nama_file_output] [alamat_IP]
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

37. Menjalankan nmap dengan opsi untuk mengecek keberadaan host pada jaringan:
```
# nmap -sn [alamat_IP]
```
Jawaban (sertakan screenshot hasil).

Hasil Analisa.

Kesimpulan:

Kesimpulan dapat berupa paragraf atau dijelaskan per poin.