PRAKTIKUM 2

Network Scanner & Network Probing

A. TUJUAN PEMBELAJARAN

- Melakukan instalasi nmap
- Mengenalkan tentang penggunaan aplikasi nmap untuk melakukan scanning dan probing pada host
- Mengenalkan tentang penggunaan aplikasi nmap untuk melakukan scanning dan probing pada sebuah jaringan
- Membaca hasil outputdari nmap

B. DASAR TEORI

Pada pemrograman berbasis socket, server adalah host yang menyediakan sebuah layanan (service) dan client adalah host yang mengakses atau menggunakan layanan tersebut. Soket sendiri adalah gabungan dari alamat IP dan nomor port, salah satu contohnya adalah layanan mail di kampus menggunakan socket 202.9.85.49:25. Alamat IP dari layanan adalah 202.9.85.49 dengan nomor port 25 (layanan berbasis protocol SMTP). Atau dengan kata lain host dengan IP 202.9.85.3 membuka port nomor 25 untuk menyediakan layanan SMTP.

Pada praktikum kali ini kita melakukan pemindaian terhadap port-port (*port-scanning*) yang terbuka pada suatu host.

Layanan jaringan dapat diserang dalam berbagai cara. Aplikasi layanan sendiri mungkin mempunyai beberapa kelemahan seperti kesalahan pemrograman, penggunaan autentikasi/password yang lemah, sensitive data tidak terenkripsi atau mengijinkan koneksi dari berbagai alamat IP dan lain sebagainya. Kelemahan-kelemahan tersebut memungkinkan host yang menyediakan layanan tersebut rentan terhadap serangan. Oleh karena itu sebaiknya host

hanya menyediakan layanan yang diperlukan saja, atau dengan kata lain meminimalkan port yang terbuka.

Pemindaian Port sebagai langkah awal untuk meretas layanan jaringan

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host, penyerang harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila penyerang sudah mengetahui bahwa host menjalankan proses SMTP server, ia dapat menggunakan kelemahan-kelemahan yang ada pada SMTP 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.

Pemindaian dengan menggunakan aplikasi Nmap

Nmap ("Network Mapper") adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP raw untuk mendeteksi host yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

Output Nmap adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. Berikut adalah beberapa informasi tambahan yang menarik untuk ditelaah :

- nomor port
- nama layanan
- status port : terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered).
- nama reverse DNS
- prakiraan sistem operasi
- jenis device, dan
- alamat MAC.

Tipe-tipe pemindaian dengan menggunakan Nmap

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.

Contoh hasil pemindain dengan perintah : # nmap –T4

```
ferry@pr1:~$ nmap -A -T4 10.252.44.47

Starting Nmap 5.00 ( http://nmap.org ) at 2012-12-13 17:17 WIT
Interesting ports on 10.252.44.47:
Not shown: 990 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              ProFTPD 1.3.4a
|_ ftp-anon: Anonymous FTP login allowed
22/tcp    open  ssh              OpenSSH 5.9p1 Debian 5ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 5a:80:5c:97:d0:c8:0e:e3:35:46:82:96:b0:1c:d8:3c (DSA)
|_ 2048 98:62:00:0c:12:02:e2:e4:a3:8b:bf:3e:f3:46:06:ad (RSA)
80/tcp    open  http             Apache httpd 2.2.22 ((Ubuntu))
|_ html-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn      Samba smbd 3.X (workgroup: AI)
445/tcp   open  netbios-ssn      Samba smbd 3.X (workgroup: AI)
873/tcp   open  rsync            (protocol version 30)
1723/tcp  open  pptp             linux (Firmware: 1)
Host script results:
| smb-os-discovery: Unix
| LAN Manager: Samba 3.6.3
| Name: AI\Unknown
|_ System time: 2012-12-13 17:18:03 UTC+7
```

C. LANGKAH PERCOBAAN

Percobaan C.1. Network scan

Langkah percobaan

1. Jalankan nmap dengan menggunakan option : -sL .
    a. Ada berapa host yang sedang dalam keadaan beroperasi ?
2. Jalankan nmap dengna menggunakan option : -sP
    a. Ada berapa host yang sedang dalam keadaan beroperasi ?
    b. Adakah perbedaan hasil dengan menggunakan option –sL ? Sebutkan perbedaannya dan jelaskan maksud dari informasi tambahan yang muncul !
3. Tambahkan option “-v” pada percobaan 2.
    a. Amati perbedaanhasil yang ada! Beri komentarmu!

Percobaan C.2. Hosts scan

Langkah percobaan

1. Lakukan pemindaian ke alamat host : scanmap.eepis-its.edu dengan memakai teknik pemindaian
    a. –F
    b. -sV
2. Catat dan bandingkan hasil dari kedua opsi diatas ! Beri komentarmu!

Percobaan C.3. Hosts scan dengan menggunakan script yang telah disediakan oleh nmap

1. Dengan menggunakan manual dari nmap :
    a. Di folder mana, scripts nmaps disimpan dalam sistem
    b. jelaskan penggunaan dari scripts (-sC) !
2. Lakukan pemindaian ke alamat host : scanmap.eepis-its.edu dengan menggunakan opsi –sC. Amati perbedaan hasil dari perintah yang dijalankan pada percobaan nomor 2. Jelaskan minimal tiga percobaan yang kamu peroleh !

D. TUGAS

1. Jalankan nmap dengan menggunakan teknik TCP half open atau dengan menggunakan opsi –sS. Amati paket anatara host anda dan hoist target dengan menggunakan wireshark.

Apakah yang dimaksud dengan half-open dengan melihat hasil dari analisa paket anda? Gambarkan diagram TCPnya

2. Dengan menggunakan referensi dari http://www.sans.org/reading_room/whitepapers/hackers/fundamentals-computer-hacking_956, apa yang harus dilakukan oleh hacker untuk mengetahui informasi dari hosts target yang akan diserang ?
3. Beri kesimpulan dari percobaan-percobaan yang telah anda lakukan diatas !

DAFTAR PUSTAKA

1. URL http://nmap.org/book/nse-usage.html
2. URL http://www.sans.org/reading_room/whitepapers/hackers/fundamentals-computer-hacking_956
3. Stuart McClare, Web Hacking Attack and Defense, Pearson Education 2003
4. Anonymous, Maximum Security, The Third Edition, Sams Publications, 2002
5. Smart McClure, Joe Scrambay, Goerge K , Hacking Exposed, The Third Edition, Network Security Secret and Solutions, Sams Publications 2002
6. James Stanger, Patrick T. Lane, Hack Proofing Linux, Syngress Publishing, 2001
7. Douglas E Comer, Computer Networks and Internet, Sams Publications, 2000.
8. Nicholas Marsh, Nmap Cookbook The Fat-free Guide to Network Scanning,2010