PERANCANGAN DAN REALISASI PROGRAM PENDETEKSI CELAH DAN PEMBERI SARAN KEAMANAN SISTEM SERVER BERBASIS PYTHON DAN SHELL SCRIPT

Ahsan Fathoni[1], Muhammad Iqbal[2], Surya Michrandi Nasution[3]

[1]Teknik Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom

Abstrak

Perkembangan teknologi informasi dan komunikasi sangatlah cepat. Penggunaan internet sebagai hasil perkembangan teknologi ini juga semakin meluas. Kebanyakan institusi pemerintahan, perusahaan, universitas, sekolah, dan institusi-institusi lain menggunakan internet untuk berbagai keperluan. Tentu saja dengan perkembangan yang seperti ini muncul juga ancaman terhadap sistem komputer itu sendiri. Dengan demikian diperlukan pengetahuan mengenai kelemahan dari sistem komputer yang dimiliki agar mempermudah untuk memperbaiki dan mengamankannya. Untuk melakukan hal tersebut, biasanya dilakukan sebuah ujian terhadap sistem yang biasa dikenal dengan penetration testing.

Dalam proyek akhir ini dirancang sebuah perangkat lunak untuk menganalisa kelemahan sistem yang dimiliki. Tahapan ini dikenal sebagai pemindaian dan menggunakan berbagai tools seperti nmap, netcat, dan sebagainya. Perangkat lunak yang ditulis dengan Python dan shell script ini menganalisa hasil pemindaian dari tools tersebut. Selain itu juga ditampilkan saran konfigurasi perbaikan berdasarkan hasil analisa untuk membantu sistem menjadi lebih aman.

Program yang dibuat dalam proyek akhir ini telah dapat digunakan untuk memindai sistem operasi Windows dan Linux. Kelemahan dan saran juga dapat ditampilkan sesuai hasil pemindaian. Pemindaian pada sistem operasi Windows rata-rata membutuhkan waktu 140,83 detik dan Linux rata-rata membutuhkan waktu 36,43 detik.0

Kata Kunci : kemanan sistem, python, shell, scanning

Abstract

Development of information and communication technology is growing rapidly. Internet usage as a result of the development of technology is also spreading widely. Most of government institutions, companies, universities, schools, and many other institutions are using the internet for many purposes. By this rapid development of technology there are also threats to the computers them selves. It causes knowledge about the weaknesses of the computer system is highly required in order to fix the weaknesses and keep the computer safe.

To do such task, there is a test that is usually known as penetration testing. In this final project, a software had been built to analyze weaknesses of a system. This stage is known as scanning and usually needs several tools such as nmap, netcat, and other tools. The software is built using Python and Shell Script. It will analyze the results of the scanner tools. Beside that, some recommendations to re-configure the system will be displayed based on the examination in order to help the system to be safer.

The program which has been made in this final project could be used to scan both Windows and Linux. Flaws and recommendations are also displayed according to the scanning results. The scanning on Windows needs 140.83 seconds in average and 36.43 seconds on Linux.

Keywords : system security, python, shell, scanning

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem dan jaringan komputer merupakan komponen penting di berbagai bidang pada era ini. Sistem dan jaringan ini biasanya menangani berbagai macam layanan pada perusahaan, universitas, instansi pemerintahan, sekolah, dan sebagainya. Layanan tersebut bisa berupa *website*, *mail server*, penyimpan data-data penting, dan sebagainya. Layanan semacam ini tentunya harus terjaga agar data-data yang terdapat di dalamnya tetap menjadi rahasia instansi yang memilikinya. Selain itu, layanan harus tetap bisa diakses kapan pun. Oleh karena itu, elemen keamanan sistem menjadi salah satu yang terpenting untuk menjaga kerahasiaan data dan ketersediaan layanan.

Seperti filosofi yang digunakan oleh *Certified Ethical Hacker* (CEH)*:* Jika Anda ingin menghentikan *hacker,* maka Anda harus bisa berlaku dan bertindak seperti *hacker* (S'to, 2009). Maka untuk mengamankan sistem komputer yang dimiliki tentu langkah pertama yang mungkin dilakukan adalah mencari kelemahan yang ada pada sistem. Tahapan mencari kelemahan sistem ini biasa disebut sebagai tahapan pemindaian. Pemindaian dapat dilakukan dengan bantuan berbagai macam *tools* yang telah dibuat oleh para profesional. Misalnya saja untuk mengetahui *port* mana saja yang memberikan layanan bisa menggunakan program *nmap*.

Tools yang telah ada hanya sebatas menampilkan hasil pemindaian tanpa analisa. Orang yang melakukannya yang harus melakukan analisa sendiri. Tentunya ini hanya bisa dilakukan oleh orang yang memiliki pengetahuan yang cukup. Oleh karena itu, dalam proyek akhir ini akan dirancang sebuah program yang akan menjalankan aktivitas pemindaian sesuai apa yang diinginkan. Pemindaian yang dilakukan sebenarnya adalah hasil pemindaian yang dilakukan oleh *tools* seperti *nmap*. Program juga akan menganalisa hasil pemindaian dan memberikan saran yang tepat

sesuai hasil analisa. Program ini akan ditulis menggunakan *Python* dan *shell script* yang sudah banyak digunakan sebagai *script* di dunia jaringan dan banyak dipilih karena kesederhanaan *syntax*-nya.

1.2 Tujuan

a) Dapat menggunakan *tools* pemindaian dan memanggilnya menggunakan program yang ditulis menggunakan Python.
b) Dapat membuat program yang bisa menganalisa kelemahan sistem yang dipindai berdasarkan versi perangkat lunak layanan.
c) Dapat memberikan saran konfigurasi yang tepat berdasarkan analisa hasil pemindaian.

1.3 Rumusan Masalah

a) Bagaimana membuat program dengan *Python* dan *shell script*?
b) Bagaimana mengintegrasikan (menjalankan) *tools* yang sudah ada dengan program yang kita buat?
c) Bagaimana mengolah informasi hasil pemindaian?
d) Dari mana mendapat informasi tentang kelemahan dan saran yang sesuai?

1.4 Batasan Masalah

a) Analisa dan pemberian saran dilakukan berdasarkan informasi hasil pemindaian saja, tidak dilakukan tahapan yang lebih lanjut seperti eksploitasi dan *gaining access*.
b) Program berjalan optimal di Sistem Operasi GNU/Linux berbasis Debian.
c) Sistem Operasi target difokuskan untuk Windows dan Linux.
d) Parameter kelemahan yang dianalisa adalah perangkat lunak yang digunakan sebagai layanan pada server dan versinya

1.5 Metodologi Penelitian

Metode yang digunakan pada Proyek Akhir antara lain:

a) Studi Literatur

Studi Literatur dimaksudkan untuk mencari konsep, dasar, teori, dan tutorial yang berhubungan dengan proyek. Banyak hal yang dipelajari seperti: keamanan komputer, bahasa pemrograman Python, *tools* pemindai, dan dokumentasi-dokumentasi Python untuk pengolahan data. Ini didapat dari buku, buku elektronik, jurnal, artikel di internet, dan sebagainya.

b) Konsultasi

Konsultasi dilakukan dengan pembimbing untuk mendapat bimbingan dan arahan Proyek Akhir.

c) Perancangan dan Pembuatan Program

Merancang program seperti membuat diagram alir. Kemudian mengkodekan dengan Python dan *shell script* dan memanfaatkan beberapa *tools* yang ada.

d) Tahap Pengujian

Program diujikan untuk melakukan pemindaian pada beberapa komputer.

1.6 Sistematika Penulisan

Adapun sistematika penyusunan laporan Proyek Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi tentang penjelasan mengenai latar belakang masalah, tujuan, batasan masalah, perumusan masalah, metodologi, serta sistematika penulisan Proyek Akhir ini.

BAB II LANDASAN TEORI

Bab ini berisi tentang penjelasan teori dasar mengenai Keamanan Jaringan, Bahasa Pemrograman Python, nmap, serta beberapa komponen lain yang digunakan pada Proyek Akhir ini.

BAB III PERANCANGAN DAN REALISASI

Pada bab ini dibahas mengenai perancangan program dengan menggunakan bahasa pemrograman Python.

BAB IV PENGUJIAN DAN ANALISA

Bab ini membahas mengenai pengujian Program Pendeteksi Celah dan Pemberi Saran Keamanan dan menganalisa hasil pengujian tersebut.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang didapat dari proyek akhir ini serta saran pengembangan proyek akhir ini ke depannya.

BAB IV
PENUTUP

5.1 Kesimpulan

Dari hasil pengujian dapat ditarik kesimpulan sebagai berikut:

1. Program sudah dapat menjalankan fungsinya untuk melakukan pemindaian, mencari sistem operasi target, *port* yang terbuka, perangkat lunak yang berjalan beserta versinya, dan kelemahan dan saran yang diambil dari database program.
2. Untuk memindai sistem operasi Windows dibutuhkan waktu rata-rata 140,83 detik dan pada Linux dibutuhkan 36,43 detik. Mentarget Windows lebih lama karena jumlah *port* yang terbuka pada target Windows lebih banyak.
3. Dibandingkan dengan program Nessus, program yang dibuat memindai dengan waktu yang jauh lebih singkat tetapi dengan parameter yang dipindai hanya perangkat lunak yang berjalan. Nessus memiliki kelebihan memindai dengan lebih banyak parameter tetapi juga memerlukan waktu yang jauh lebih lama.

5.2 Saran

Pengembangan yang dapat dilakukan dalam proyek akhir ini antara lain:

1. Database program sebaiknya dilengkapi agar terdapat data mengenai layanan, kelemahan, dan saran yang lebih banyak pada *port-port* yang lain. Database juga sebaiknya selalu diperbarui karena selalu ditemukan kelemahan-kelemahan baru.

2. Program dapat diintegrasikan dengan *tools* yang lain agar lebih kaya fitur.

3. Dokumentasi yang lebih baik sebaiknya dibuat agar memudahkan pengembangan program di kemudian hari.

DAFTAR PUSTAKA

[1] Agung, Wahyu. 2010. *Membuat Distro Linux Sendiri (Remastering Linux Ubuntu 10.04 Lucid Lynx)*. Jakarta. Buku elektronik.

[2] Fajar, Moch. 2001. *Pengantar Pemrograman Bash Shell di Linux.* (Daring), (http://pemula.linux.or.id/programming/bash-shell.html, diakses 5 November 2012).

[3] Kak, Avi. 2012. *Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing.* (Daring), (https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf, diakses 28 November 2012).

[4] metasploit.com. *Metasploit Auxiliary Module & Exploit Database (DB)* (Daring), http://www.metasploit.com/modules/.

[5] Moody, Robert. 2001. *Port and Port Scanning: An Introduction.* (Daring), (http://www.isaca.org/Journal/Past-Issues/2001/Volume-5/Pages/Ports-and-Port-Scanning-An-Introduction.aspx diakses 5 November 2012).

[6] nmap.org. *Chapter 15: Nmap Reference Guide* (Daring), http://nmap.org/book/man.html.

[7] S'to. 2009. *C|EH 100% Illegal*. Jakarta: Penerbit Jasakom.

[8] Sugiana, Owo. 2003. *Membuat Aplikasi Bisnis Menggunakan Bahasa Python dan Database Berbasis SQL.* Jakarta. Buku elektronik.