LAPORAN KEAMANAN JARINGAN KOMPUTER

"Penetration Testing Metodology"

Oleh:

NAMA	: Yoga Faturahman
NIM	: 09040581721006
Kelas	: TKJ4
Mata Kuliah	: Keamanan Jaringan Komputer

LABORATORIUM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

Penetration Test

Penetration Test *(pentest*) merupakan kegiatan yang dilakukan untuk melakukan pengujian terhadap keamanan sebuah sistem. Pengujian ini dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut. Hasil pengujian ini digunakan untuk memperbaiki sisi keamanan dari sistem. Yang dicari dari Pentest ini adalah apakah terdapat celah keamanan yang dapat disalahgunakan (*exploitable vulnerability*).

Langkah pertama yang dilakukan pada Pentest adalah **perencanaan**. Pada tahapan ini harus dibicarakan ruang lingkup pentest, range waktu, dokumen legal (kontrak), jumlah tim yang dibutuhkan serta apakah staff dan karyawan diberitahukan terlebih dahulu atau tidak tentang adanya pentest.

Langkah kedua adalah **information gathering dan analysis**. Pada tahapan ini dikumpulkan semua informasi tentang sistem target. Ada banyak alat bantu yang bisa digunakan, diantaranya adalah www.netcraft.com. Kemudian dilakukan network survey untuk mengumpulkan informasi domain, server, layanan yang ada, ip adress, host, adanya firewall, dll. Tools yang dapat digunakan misalnya Nmap http://nmap.org/.

Langkah ketiga adalah **vulnerability detection** (pencarian celah keamanan). Setelah mengetahui informasi tentang sistem, pencarian celah keamanan bisa dilakukan manual atau secara automatis misalnya dengan Nessus. http://www.tenable.com/products/nessus

Setelah menemukan celah keamanan, maka langkah terakhir adalah **percobaan penyerangan** (*penetration attempt*). Pada proses ini dilakukan penentuan target, pemilihan tools dan exploit yang tepat. Umumnya diperlukan juga kemampuan password cracking. Cara lain yang dapat dilakukan adalah dengan melakukan *social engineering* dan pengujian *physical security* dari sistemTahap berikutnya adalah **analisis dan pembuatan laporan**. Disini biasanya dilaporkan tentang langkah kerja yang dilakukan, celah keamanan yang ditemukan serta usulan perbaikan. Tahapan selanjutnya biasanya **tindak lanjut**, yang biasanya harus dilakukan bersama-sama dengan admin untuk memperbaiki sistem.