BAB I

PENDAHULUAN

1.1 Latar belakang

Perkembangan ilmu pengetahuan yang semakin maju, tentu sangat berpengaruh pada perkembangan Teknologi itu sendiri apalagi ilmu komputer, dimana setiap individu bersaing dalam kemajuan zaman itu sendiri, setiap hari atau bahkan setiap menit sangatlah banyak bermunculan software software baru. Diantara banyak software tentunya tidak asing ditelinga kita sebagai orang yang mengikuti perkembangan zaman apabila mendengar kata "Android" Android sendiri sebuah sisitem operasi yang berbasis mobile.

Android adalah salah satu sistem operasi yang paling banyak digunakan saat ini terutama pada perangkat mobile. Menurut data Marketing *Land* tahun 2015 yang berada dipasaran lebih dari 50% smartphone menggunakan android sebagai sistem operasinya. Semakin banyak pengguna sebuah platfrom maka seharusnya akan sebanding juga dengan ancaman yang ada dalam keamanan *platfrom* tersebut. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam vendor terutama yang bergerak di bidang mobile.

Hal utama yang perlu diperhatikan oleh pengguna SmartPhone, meski Google meningkatkan upaya kebijakan ekosistem Android masih ada sedikit masalah keamanan penting dalam sistem operasi mobile. Mengingat semua transaksi yang ada saat ini menggunakan SmartPhone, ketika SmartPhone yang digunakan terancam keamanannya maka bisa dipastikan transaksi yang dilakukan

juga akan ikut terancam. Menurut perusahaan keamanan Bluebox, lemahnya keamanan pada Android memungkinkan para peretas mengakses aplikasi apapun dan mengubahnya menjadi program Trojan untuk memperoleh data Pribadi atau mengendalikan sistem. masalah tersebut sudah ada sejak Android 1.6.

Dengan banyaknya acaman banyak lembaga membuat standarisasi untuk proses pengujian mobile diantaranya adalah standar Top Risk yang dibuat oleh OWASP.

Berdasarkan permasalahan tersebut penulis tertarik untuk mengajukan penelitian dengan judul "Pengujian Keamanan Android Dengan Menggunakan Standar Mobille Pentesting".

1.2 Rumusan Masalah

Berdasarkan penjelasan yang telah diuraikan diatas, maka pokok permasalahan yang akan dirumuskan dalam penelitian ini sebagai berikut :

1. Bagaimana memanfaatkan standar mobile risk dari OWASP sebagai pengujian keamanan android.
2. Bagaimana cara menguji keamanan mobile terutama android untuk memberikan laporan tentang kemanan mobile terutama bagi android device.

1.3 Batasan Masalah

Agar penelitian ini terfokus pada pokok permasalahannya, maka penulis berinisiaif untuk membatasi permasalahan hanya pada Pengujian mobile diantaranya adalah standar top risk yang dibuat oleh OWASP dimana dengan metode tersebut dapat diputuskan apa saja yang harus dilakukan terhadap resiko

-resiko tersebut. Dengan mengetahui resiko yang akan terjadi maka banyak manfaat yang akan diperoleh diantaranya, menghemat waktu dan mengurangi terjadinya resiko yang lebih serius.

Berikut ini spesifikasi-spesifikasi ruang lingkup yang akan penulis gunakan sebagai acuan penelitian.

1. Versi android yang digunakan dalam penelitian ini adalah android versi 4.3 jellyben yang saat ini masih banyak digunakan di pasaran.
2. Aspek keamanan yang akan diuji yaitu CIA (*Confidentiality integrity Availibality*)
3. Pentester berhadapan langsung dengan satu jaringan dengan target.
4. Aplikasi yang akan digunakan dalam penelitian ini yaitu menggunakan aplikasi *Burpsuit, Zap-Proxy, Dnsnif, Ettercap.*
5. Dalam penelitian ini penguji terfokus pada keamanan sistem operasinya yaitu android versi 4.3 serta aplikasi-aplikasi umum yang digunakan (netif).

1.4 Tujuan Penelitian

Penelitian ini mempunyai tujuan untuk menguji seberapa amankah sistem android terhadap ancaman dari penyerang.

1.5 Metode Penelitian

Metodologi pelaksanaan selama pembuatan skrisi ini, meliputi :

1. Reconnaissance

   Metode ini mengacu pada tahap persiapan dimana seorang penyerang berusaha untuk mengumpulkan informasi sebanyak mungkin tentang

target evaluasi sebelum meluncurkan serangan ini melibatkan pemindaian jaringan baik eksternal maupun internal tanpa otorisasi.

2. Scanning

   Metode ini mengacu fase praserangan ketika hacker scan jaringan dengan informasi spesifik yang dikumpulkan selama pengintaian.

3. Gaining Access

   Metode ini mengacu pada fase serangan yang benar hacker mengeksploitasi sistem.

4. Maintaining Access

   Metode ini mengacu fase ketika hacker mencoba untuk mempertahankan "kepemilikan"nya dari sistem.

5. Covering Tracks

   Metode ini mengacu pada kegiatan yang dilakukan oleh hacker untuk memperpanjang penyalahgunaan tentang sistem tanpa terdeteksi.

1.6 Sistematika Penulisan

Agar penyajian laporan penelitian terstruktur dan mudah dimengerti, maka dibuat sistematika penulisan berdasarkan pokok-pokok permasalahan untuk mempermudah penyusunan dalam penulisan Skripsi yaitu sebagai berikut :

BAB I : PENDAHULUAN

Bab pendahuluan materinya sebagian besar berupa latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan laporan penelitian.

BAB II : LANDASAN TEORI

Bab Landasan Teori merupakan tinjauan pustaka, menguraikan teori-teori yang mendukung penelitian, dan mendasari pembahasan secara detail. Landasan teori dapat berupa definisi-definisi atau model yang langsung berkaitan dengan ilmu atau masalah yang diteliti.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan bagaimana metode-metode yang digunakan dalam penelitian dan tahapan-tahapan yang diuraikan secara terperinci

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini merupakan paparan implementasi dan analisis hasil uji coba program. Bab IV ini akan memaparkan hasil-hasil dari tahapan penelitian, dari tahap analisis, hasil testing dan implementasinya.

BAB V : PENUTUP

Berisi kesimpulan dan saran. Kesimpulan dapat mengemukakan kembali masalah penelitian (mampu menjawab pertanyaan dalam rumusan masalah), menyimpulkan bukti-bukti yang diperoleh dan akhirnya menarik kesimpulan apakah hasil yang didapat(dikerjakan), layak untuk digunakan.