BAB I
PENDAHULUAN

1.1. Latar Belakang

Saat ini perkembangan teknologi yang semakin pesat mempengaruhi gaya hidup. Mulai dari mempengaruhi model berkomunikasi massa dan juga membantu apa yang dibutuhkan dan dicari dengan cepat dan mudah untuk melakukan pencarian informasi dengan penggunaan teknologi yaitu s*martphone.* Menurut (Ferdiana, 2008) *smartphone* adalah perangkan telepon seluler yang dilengkapi dengan berbagai fitur. Dengan begitu, selain menjadi alat telekomunikasi, *smartphone* juga dapat digunakan buat keperluan bisnis oleh pengusaha dan juga masyarakat generik. Menurut (*Williams* & *Sawyer*, 2011) *smartphone* adalah telepon selular dengan mikroprosesor, *modem* bawaan, layer dan memori. *smartphone* merupakan ponsel multimedia yang menggabungkan fungsionalitas *PC* dan *handset* sehingga menghasilkan *gadget* yang mewah, di mana terdapat pesan teks, kamera, pemutar musik, *search engine*, *email*, *tv games* dan *videogame*, pengelola informasi pribadi, fitur *GPS*, jasa telepon internet dan bahkan terdapat telepon yang juga berfungsi sebagai kartu kredit.

Android salah satu dari sekian banyak nya *Operation System* (OS) *smartphone*. Menurut (Satyaputra & Aritonang, 2014) *Android* adalah sebuah sistem operasi untuk *smartphone* dan tablet. Dimana sistem operasi ini dapat di ilustrasikan sebagai jembatan antara piranti dan penggunanya, sehingga pengguna

bisa berinteraksi dengan *device*-nya dan menjalankan aplikasi - aplikasi yang tersedia pada *device*. Dengan perkembangan sistem operasi *android* yang semakin pesat mulai dari versi *android 1.0* (Astro) Pertama kali dirilis pada tanggal 23 September 2008 dan sampai pembaruannya dengan versi *android* 9.0 (Pie) pada tanggal 6 Agustus 2018.

Dilansir dari halaman *website android*. *Google* merilisi data jumlah distribusi sistem operasi android. Pada data periode 2017 bahwa pengguna *Android* 5.0 (*Lollipop*) merupakan yang paling tinggi yakni mencapai angka 33.4%. Data periode 2018 *android* version 7.0 memiliki distribusi terbesar mendapat angka 30,8% (“Dasbor,” n.d.).

Pada umum nya keamanan *Operation System (OS) Android* memiliki fitur keamanan bawaan yang secara signifikan mengurangi frekuensi dan dampak masalah keamanan aplikasi. Sistem ini dirancang agar secara khusus dapat membuat aplikasi dengan izin file dan sistem *default* yaitu, izin yang ditetapkan aplikasi untuk mengontrol data aplikasi pada basis per-aplikasi dan juga izin yang diberikan pengguna untuk membatasi akses ke fitur sistem dan data pengguna (“Arsitektur Platform,” n.d.).

Operation System android memiliki batasan penggunanya agar tidak mengubah system yang telah dibuat oleh produsen resmin nya. *Root android* merupakan suatu *system account* yang memiliki kekuasaan mutlak, tertinggi atau absolut untuk mengakses dan mengeksekusi semua *file*, *command*, *system*, dalam sistem operasi berbasis *linux*, salah satunya adalah *android* (“Root (Android),” 2019) . Dengan melakukan *root android* dapat mengubah settingan *system default smartphone* agar pengguna bisa melakukan hal menguntungkan. Fungsinya yang di

gemari oleh pengguna *android* adalah memudahkan pengguna melakukan kustomisasi *ROM*, meningkatkan kinerja *processor smartphone* (*Overclock*) dan modifikasi ponsel agar terlihat lebih menarik dan berkualitas. Tetapi di balik kelebihan *Root android* ada juga sisi kekurangan nya yaitu, rawan terkena *malware* dan pencurian data, di karenakan *system default* dapat di ubah oleh pengguna sehingga tingkat keamanan menjadi renda karena perizinan keamanan menjadi manual. Seperti contoh kasus yang sering di temukan ketika mengakses *website* hiburan di *browser smartphone* yaitu *malware Screen Locker* yang berjenis iklan memaksa membuat akses *website* terhalangi atau layar terkunci dan juga memaksakan kita mengungunduh file pake yang tidak jelas.

Salah satu nya kerentanan yang ada di android yaitu, yang di identifikasi sebagai *CVE*-2018-9581 (*Common Vulnerabilities and Exposures*) ditemukan bahwa sistem operasi android menyiarkan informasi tentang koneksi *WiFi* secara teratur ("Sensitive Data Exposure via RSSI Broadcasts in Android OS [CVE-2018-9581] | Nightwatch Cybersecurity," n.d.), diakses tanggal 13 Juli 2019). Dengan asumsi bahwa ponsel yang lebih dekat ke *router Wi-Fi* akan menerima sinyal yang lebih kuat, maka mungkinkan untuk menyimpulkan lokasi pengguna di rumah atau kantor.

Penelitian ini mengenai tentang kerentanan yang di identifikasi dalam sistem operasi *android* dan juga di fokuskan pada menganalisis keamanan *operation system (OS) android* pada *smartphone.* Menurut (Kennedy, 2011) *Penetration Testing* (disingkat *pentest*) adalah kegiatan (mensimulasikan serangan yang bisa dilakukan dikarenakan ada kerentanan lalu mensimulasi kan nya dan menganalisis kerentanan tersebut.

Berdasarkan latar belakang tersebut, maka penulis mengambil judul ANALISIS SISTEM KEAMANAN *OPERATION SYSTEM* (OS) *ANDROID* PADA *SMARTPHONE*.

1.2. Perumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalahnya adalah Bagaimana cara menganalisis sistem keamanan *operation system (OS) android* pada *smartphone.*

1.3. Batasan Masalah

Agar pembahasan lebih terarah dan tidak menyimpang dari yang direncanakan sebelumnya, Batasan masalah sebagai berikut :

1. Menganalisis sistem keamanan *Operation system* (OS) *android* version 4.3 (*Jelly Bean*) pada *smartphone Samsung Galaxy Note 2 GT-N7100*
2. Menganalisis sistem keamanan *Operation system* (OS) *android* version 5.1.1 (*Lollipop*) pada *smartphone Samsung Galaxy J1 Ace*
3. Menganalisis sistem keamanan Operation system (OS) android version 7.0 (nougat) pada *smartphone Xiaomi Mi 4c* status (Root system)
4. Lokasi pengujian di lakukan dalam lingkungan jaringan *WLAN* (*Wireless Local Area Network*).

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan

Tujuan dari penelitian yang ingin dicapai adalah sebagai berikut :

1. Mengetahui kerentanan sistem keamanan pada *Operation system* (OS) *android* version 4.3 (*Jelly Bean*) *smartphone Samsung Galaxy Note 2 GT-N7100* dan *android version 5.1 (Lollipop)* pada *smartphone Samsung Galaxy J1 Ace.*
2. Mengetahui kerentanan sistem keamanan pada *Operation system (OS)* Menganalisis sistem keamanan pada *Operation system (OS) android version 7.0 (Nougat)* pada *smartphone Xiaomi Mi 4c* status *(Root system)*

1.4.2. Manfaat Penelitin

Manfaat yang di dapat dari penelitian ini adalah :

1. Pembaca dapat mengetahui bagaimana cara menganalisis sistem keamanan *operation system android* pada *smartphone*.
2. Dapat mempelajari cara kerja aplikasi seperti perizinan hak akses aplikasi
3. Sebagai pengetahuan bagi pengguna *smartphone operation system (OS) android* agar lebih berhati – hati memasang aplikasi yang tidak dikenal store.
4. Hasil penelitian ini diharapkan dapat memberikan kesempatan bagi penulis dan pembaca untuk menambah pengetahuan dan wawasan dalam bidang *IT Securty*, khusus nya tentang *penetration test* pada sistem operasi *smartphone android*.

1.5. Metodologi Penelitian

1.5.1. Tempat Dan Waktu Penelitian

Penelitian ini dilakukan oleh penulis kurang lebih selama 8 bulan mulai dari Januari 2019 sampai dengan Agustus 2019 dengan mengumpulkan data yang tepat sesuai dengan penelitian

1.5.2. Data Penelitian

Data-data yang dibutuhkan untuk proses menganalisis sistem keamanan android ini menggunakan data sekunder. Menurut (Sugiyono 2015: 15) Data sekunder adalah data yang diperoleh dari buku atau internet yang ada hubungannya dengan penulisan skrpsi ini

1.5.3. Metode Penelitian

Penulis menggunakan metode penelitian kualitatif, yaitu dengan cara mencari informasi tentang adanya permasalahan yang ada lalu mencari solusi untuk permasalah tersebut. Menurut Sugiyono (2012: 15) metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada filsafat postpositivisme, digunakan untuk meneliti pada kondisi obyek yang alamiah.

1.5.4. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian adalah studi pustaka, penulis mengumpulkan data dan mempelajari buku artikel, jurnal, dan situs-situs internet yang berhubungan dengan analisis sistem keamanan android yang dibuat.

1.5.5. Metode Pengujian

Metode yang digunakan pada penelitian ini yaitu penetration test. Menurut (Kennedy, 2011) Merupakan sebuah metode untuk mengevaluasi keamanan sistem komputer melalui simulasi penyerangan terhadap target dengan menggunakan *malicious source* (program jahat). Secara umum, proses *pentration system* banyak disamakan oleh para junior *system administrator* dengan proses *vulnerability system assessment.* Secara garis besar kegiatan Pentest adalah suatu kegiatan yang memiliki etika baik, dengan keadaan yang terbuka dan dilakukan oleh para *White Hat Hacker* untuk mencoba masuk ke sistem dengan menggunakan berbagai teknik yang mungkin dapat dilakukan oleh para *Black Hat Hacker* maupun *cracker*, Sifatnya lebih ke *defensive purpose* (mencoba menyerang, kemudiann memberitahukan letak celah untuk diperbaiki oleh pemilik sistem yang bersangkutan).

Pentration Testing memiliki standar (*PTES*) yang digunakan sebagai acuan dalam pelaksanaanya ayng di bagi ke dalam beberapa tahap :

1. Pre-engagement Interactions

   Tahap (Penjelasan sebelum melakukan pengujian. Dimana pentester menjelaskan kegiatan pada *client*.

2. Intelligence Gathering

   Tahap dimana seorang pentester berusaha mengumpulkan sebanyak mungkin informasi mengenai target yang bisa didapatkan dengan berbagai metode dan berbagai media. Hal yang perlu dijadikan dasar dalam

pengumpulan informasi adalah : karakteristik sistem jaringan, cara kerja sistem jaringan, dan metode serangan yang bisa digunakan.

3. Threat Modeling

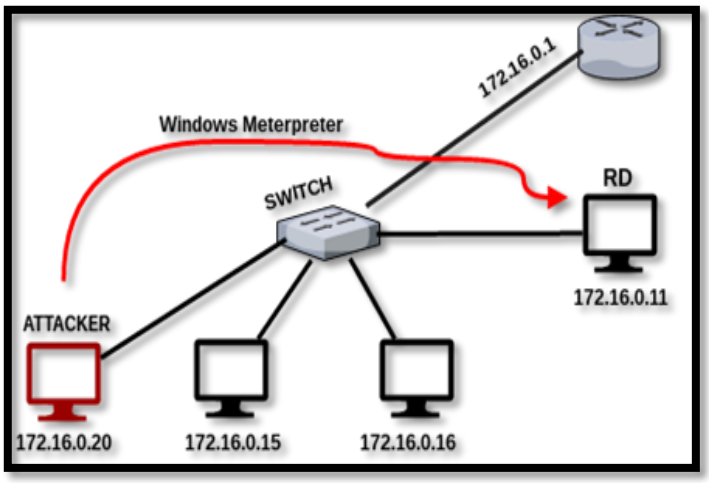
   Tahap dimana seorang pentester mencari celah keamanan (*vulnerabilities*) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya. Pada tahap ini seorang pentester tidak hanya mencari celah keamanan, tetapi juga menentukan celah yang paling efektif untuk digunakan.

4. Vulnerability Analysis

   Tahap dimana seorang pentester mengkombinasikan informasi mengenai celah keamanan yang ada dengan metode serangan yang bisa dilakukan untuk melakukan serangan yang paling efektif.

5. Exploitation

   Tahap dimana seorang pentester melakukan serangan pada target.



Gambar 1.1 Contoh simulasi penyerangan target

6. Post Exploitation

   Tahap dimana seorang pentester berhasil masuk ke dalam sistem jaringan target dan kemudian melakukan analisis infrastruktur yang ada. Pada tahap ini seorang pentester mempelajari bagian-bagian di dalam sistem dan menentukan bagian yang paling *critical* bagi target. seorang pentester bisa menghubungkan semua bagian-bagian sistem yang ada untuk menjelaskan dampak serangan / kerugian yang paling besar yang bisa terjadi pada target.

7. Reporting

   Reporting adalah bagian paling penting dalam kegiatan pentest. Seorang pentester menggunakan report (laporan) untuk menjelaskan pada target mengenai pentesting yang dilakukan seperti, apa yang dilakukan ?, bagaimana cara melakukannya ?, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya ?.

1.6. Sistematika Penulisan

Sistematika penulisan skripsi ini memberikan penjelasan penelitian secara jelas supaya terlihat tersusub dalam kerangka sub-babnya. Adapun sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang uraian latar belakang, perumusan masalah, Batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematikan penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab ini akan menjelaskan hasil – hasil penelitian sejenis terdahulu yang menginspirasi atau melandasi pelaksanakan penelitian dan juga mengulas landasan teoritik yang berhubungan dengan penelitian yang akan dilakukan, seperti landasan teori, penelitian sebelumnya dan kerangkan berpikir.

BAB III ANALISIS DAN PERANCANGAN

Pada bab menguraikan secara rinci metode pengujian dan perancangan yang di gunakan serta tahap tahap teknik analisis.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang hasil dari pengujian analisa yang dilakukan dalam penelitian

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan – kesimpulan yang di dapat dari hasil penelitian dan saran – saran untuk perbaikan atau pengembangan selanjutnya dari hasil penelitian ini