Evaluasi Keamanan Serangan Exploit Pada Sistem Operasi Android

Muhammad Firdaus [1] , Wydyanto, M.M., M.Kom. [2] , Nurul Adha Oktarini Saputri, M.Kom [3]
Mahasiswa Universitas Bina Darma [1] , Dosen Universitas Bina Darma [2,3]

Jalan Jenderal Ahmad Yani No.12 Plaju Palembang 30264

E–Mail : firdaus.12142062@gmail.com [1] , widiwidyanto1969@gmail.com [2] , nuruladhaos@binadarma.ac.id [3]

Abstrak. Seiringnya perkembangan zaman teknologi kita dapat mengetahui bahwa perangkat sistem operasi *handphone* semakin berkembang, sistem operasi pada perangkat *handphone* yang memiliki kehandalan bagi pengguna sehingga dapat memodifikasi *platfrom* sesuai dengan selera keinginannya adalah sistem operasi android, akan tetapi sistem operasi android pada handphone ini seorang *hacker* dapat memanfaatkan suatu tindakan dengan cara masuk ke sebuah sistem yang dituju kapan pun dan dimana pun, terutama dari celah-celah kecil sekalipun. Banyak cara seorang *hacker* untuk melakukan tindakan menyerang kemanan sistem secara spesifik salah satunya exploit. Akan tetapi *hacker* juga memerlukan sebuah *tool* yang berfungsi dalam sebuah exploitasi perangkat *handphone* di suatu sistem operasi android yaitu *metasploit, metasploit* merupakan *software security* yang sering digunakan untuk menguji coba ketahanan suatu sistem. Agar hal tersebut tidak terjadi sebagai pengguna *handphone* android harus waspada terhadap exploitasi yang dilakukan oleh seorang *hacker* untuk bisa melihat seluruh informasi dan mengambil semua isi data yang ada di *handphone* android secara jarak jauh.

1. Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat terutama perkembangan yang signifikan di sektor keamanan sistem semakin memudahkan para penggunanya mulai dari perorangan hingga korporasi, seperti pendidikan di sekolah hingga bisnis pada perusahaan kebanyakan sudah memanfaatkan teknologi informasi, namun perkembangan teknologi ternyata tidak hanya memberi dampak positif saja pada penggunanya, namun juga memberi dampak negatif seperti keamanan dari data informasi tersebut, beberapa contoh masalah yang sudah umum sebelumnya mengenai keamanan sistem adalah *hacker* dan kegiatannya disebut *hacking*. Disisi lain dengan seiringnya perkembangan zaman teknologi kita dapat mengetahui bahwa perangkat sistem operasi *handphone* semakin berkembang, sistem operasi pada perangkat *handphone* yang memiliki kehandalan bagi pengguna sehingga dapat memodifikasi *platfrom* sesuai dengan selera keinginannya adalah sistem operasi

android, akan tetapi sistem operasi android pada handphone ini seorang *hacker* dapat memanfaatkan suatu tindakkan dengan cara masuk ke sebuah sistem yang dituju kapan pun dan dimana pun, terutama dari celah-celah kecil sekalipun.

Banyak cara seorang *hacker* untuk melakukan tindakkan menyerang kemanan sistem secara spesifik salah satunya exploit. Akan tetapi *hacker* juga memerlukan sebuah *tool* yang berfungsi dalam sebuah exploitasi perangkat *handphone* di suatu sistem operasi android yaitu *metasploit, metasploit* merupakan *software security* yang sering digunakan untuk menguji coba ketahanan suatu sistem, sistem kerja *metasploit* ini sendiri yaitu menyerang *application layer* yang merupakan metode penyerangan pada aplikasi yang belum di *encode*. Apabila melakukan exploitasi informasi seorang pengguna *handphone* dapat diketahui oleh *attacker*. Jika informasi itu sangat berharga yang bersifat privasi bisa didapatkan oleh pihak-pihak tidak bertanggung jawab, maka informasi tersebut dapat disalah gunakan. Kegiatan *hacking* ini bisa dikaitkan dengan istilah *remote exploitation*, artinya menyusup ke sistem berada pada jangkauan jarak jauh yang akan dapat mengendalikan perangkat korban. adapun batasan permasalahan dalam penelitian ini sebagai berikut :

1. Bagaimana cara agar seorang *hacker* untuk bisa melihat informasi dan mengambil data yang ada di *handphone* android ?
2. Bagaimana cara mengantisipasi *handphone* android dari serangan exploit ?

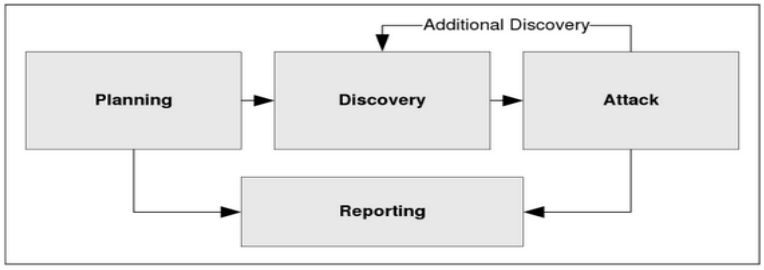
2. Metode

Metode yang digunakan dalam penelitian ini adalah *action research*. *Action Research* merupakan kegiatan penelitian yang difokuskan secara *kolaboratif* untuk menyelesaikan permasalahan yang ada, dimana permasalahan lebih kepada masyarakat secara langsung maupun tidak langsung[2].

3. Teknik Pengujian

Teknik pengujian yang digunakan untuk mengevaluasi keamanan serangan exploit di sistem operasi android pada penelitian ini menerapkan pengujian *White Box Testing* yang memperhitungkan mekanisme internal dari sebuah sistem atau komponen. *Penetration testing* yang dilakukan terhadap sistem dengan tipe *white box* ini, biasanya informasi-informasi mengenai sistem sudah diketahui, tetapi hal tersebut tidak serta-merta memberikan kemudahan dalam melakukan penetrasi. Hal tersebut tergantung dari penguji yang melakukan pengujian menilai sejauh mana kelemahan-kelemahan yang terdapat di dalam sistem[1].

Selain menggunakan metode penelitian *White Box Testing*, penelitian ini juga mengacu pada dokumen *Guideline* untuk pengujian yang dikeluarkan *United States National Institute of Standard and Technology* (NIST), pada rujukan tersebut untuk melakukan Fase *Penetration Testing* terdiri dari empat tahap[3].



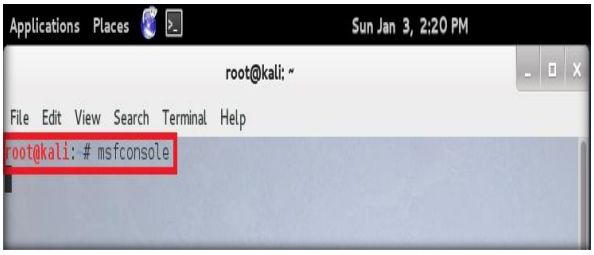
Gambar 1 Fase *Penetrasi Testing*

4. Hasil dan Pembahasan

4.1 Hasil

Pada penelitian ini akan melakukan teknik serangan exploit melalui cara kerja *shell injection* pada ketiga versi sistem operasi android yaitu versi froyo, versi kitkat dan versi lollipop dengan menggunakan *tools metasploit-framework*.

Tools metasploit-framework telah ada ataupun sudah terinstall di *Operation System Kali Linux* yang berfungsi untuk masuk ke sebuah sistem yang dituju, cara membuka *tools metasploit-framework* pada *Operation System Kali Linux* terlebih dahulu membuka terminal dan masukan peritah "*msfconsole"*.



Gambar 2 perintah msfconsole

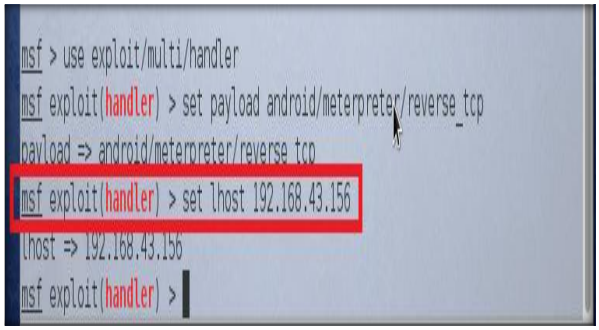
Setelah memberikan perintah "*msfconsole"* di terminal maka aplikasi *metasploit-framework* sudah terbuka dan lakukan perintah selanjutnya yaitu memberikan perintah "*use exploit/multi/handler*" pada terminal yang ada.

Gambar 3 Perintah *use exploit/multi/handler*

Sesudah memberikan perintah "*use exploit/multi/handler"* di terminal maka menu *exploit(handler)* sudah masuk dan lakukan perintah berikutnya yaitu memberikan perintah "*set payload android/meterpreter/reverse_tcp*" pada terminal yang sudah terbuka.

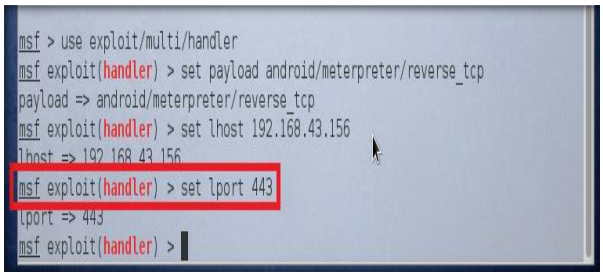
Gambar 4 Perintah *set payload android/meterpreter/reverse_tcp*

Jika sudah beri perintah "*set payload android/meterpreter/reverse_tcp"* di terminal maka *payload => android/meterpreter/reverse_tcp* sudah diatur dan lakukan perintah selanjutnya yaitu memberikan perintah "*set lhost* 192.168.43.156" pada terminal yang sudah terbuka.



Gambar 5 Perintah *set lhost* 192.168.43.156

Sesudah masukan perintah "*set lhost* 192.168.43.156*"* di terminal maka *lhost* => 192.168.43.156 sudah diatur dan lakukan perintah selanjutnya yaitu memberikan perintah "*set lport* 443" pada terminal yang sudah terbuka.



Gambar 6 Perintah *set lport* 443

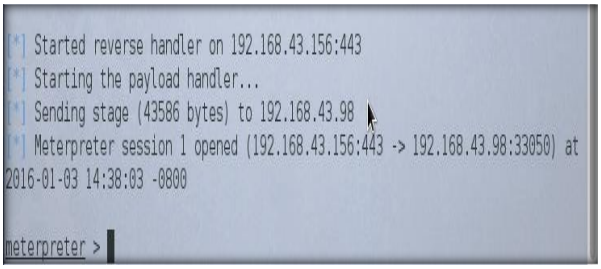
Setelah masukan perintah "*set lport* 443*"* di terminal maka *lport* => 443 sudah diatur dan lakukan perintah selanjutnya yaitu memberikan perintah "*exploit"* pada terminal yang sudah ada.

Gambar 7 Perintah *exploit*

Dengan memasukkan perintah "*exploit"* seperti gambar diatas maka terdapat keterangan bahwa serangan exploit mulai berjalan untuk masuk ke sebuah sistem operasi android.

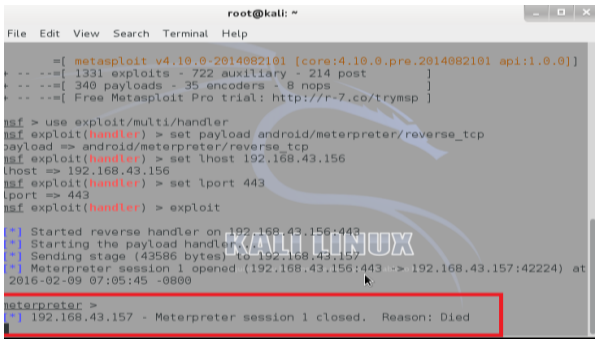
4.2 Pembahasan

Pada penelitian ini peneliti akan melakukan pengujian keamanan serangan exploit pada sistem operasi android versi 2.2 froyo, 4.4 kitkat dan 5.0 lollipop dimana pada tahap sebelumnya telah melakukan *social engineering* agar pengguna (*user*) yang akan dapat mendownload dan memasang bahkan membuka sebuah aplikasi *backdoor* di *handphone* android supaya proses serangan exploit dapat berjalan.



Gambar 8 Eksekusi Serangan Exploit Android Versi 2.2 Froyo

Gambar 9 Eksekusi Serangan Exploit Android Versi 4.4 KitKat



Gambar 10 Eksekusi Serangan Exploit Android Versi 5.0 Lollipop

5. Kesimpulan

Berdasarkan dari penelitian yang sudah dilakukan dalam evaluasi keamanan serangan exploit pada sistem operasi android, maka penulis mengambil kesimpulan sebagai berikut:

1. Hasil dari serangan exploit melalui cara kerja *shell injection* memiliki keberhasilan untuk mendapatkan sebuah informasi dan data pada android versi 2.2 froyo dan android versi 4.4 kitkat kecuali pada android versi 5.0 lollipop dikarenakan, sudah memiliki tingkat keamanan yang lebih aman sehingga proses untuk mendapatkan sebuah informasi maupun pengambilan data tidak bisa dilakukan.
2. Terdapat perbedaan saat pengambilan sebuah informasi, untuk android versi 2.2 froyo tidak memiliki sebuah izin keamanan saat pengambilan informasi maka informasi yang didapatkan sangat mudah untuk diambil sedangkan untuk android versi 4.4 kitkat memiliki sebuah izin keamanan saat pengambilan informasi sehingga proses pengambilan informasi harus melalui perizinan keamanan terlebih dahulu.

Referensi

1. Ali, Shakeel., Heriyanto, Tedi. 2011. Backtrack 4: *Assuring Security by Penetration Testing*, Packt Publishing.
2. BOPTN. 2013. Panduan *Action Research*.
3. Scarfone, Karen., Souppaya, Murugiah., Cody, Amanda., Orebaugh, Angela. 2008. *Technical Guide to Information Security Testing and Assessment*.