SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Implementasi *Backdoor Metasploit Framework* Untuk *Android* Menggunakan *Windows*

Royana [1], Supriyono [2], Munawaroh [3]
[1]Universitas Pamulang, royana.royana250@gmail.com, Tangerang Selatan, Banten, Indonesia
[2]Universitas Pamulang, supriyono200498@gmail.com, Tangerang Selatan, Banten, Indonesia
[3]Universitas Pamulang, dosen00831@unpam.ac.id, Tangerang Selatan, Banten, Indonesia

Informasi Makalah

Submit : Maret 17, 2023
Revisi : May 3, 2023
Diterima : Juni 5, 2023

Kata Kunci :

Sistem Keamanan Android
Backdoor
Metasploit Framework

Abstrak

Seiring dengan maraknya penggunaan smartphone terutama yang berbasis OS Android sudah menjadi kebutuhan yang tidak terpisahkan dalam kehidupan sehari-hari. Hal ini dikarenakan smartphone memiliki berbagai fitur yang dapat memenuhi kebutuhan penggunanya, sehingga dibutuhkan keamanan jaringan yang baik. Dalam keamanan jaringan memiliki beberapa metode yang digunakan untuk mengamankan jaringan tersebut. Salah satunya menggunakan metode Metasploit Framework yang merupakan sebuah metode keamanan yang menggabungkan antara identifikasi dan penindakan.Dalam penerapan sistem keamanan untuk mengetahui celah-celah pada sistem OS Android, peneliti menggunakan backdoor. Dalam pembuatan backdoor salah satunya dapat dilakukan dengan menggunakan metasploit framework. Metode ini dioperasikan melalui Command Prompt pada Windows yang akan membuat sebuah apk Backdoor yang akan dikirim dan diinstal didalam sistem operasi OS Android Penelitian ini dilakukan dengan tujuan untuk uji coba sistem keamanan OS Android dan mengetahui celah-celah yang terdapat pada sistem OS Android seperti data pesan sms, log panggilan telepon, data aplikasi yang terinstal, lokasi android pada sistem OS Android menggunakan framework metasploit backdoor . Pada penelitian ini menggunakan metode studi pustaka dan dokumentasi untuk mengetahui sistem keamanan OS Android. Hasil akhir dari penelitian ini adalah data pesan SMS, log panggilan telepon, data aplikasi terinstal, dan lokasi OS Android target berhasil diakses dan dapat ditampilkan melalui terminal Command Prompt.

Abstract

Along with the widespread use of smartphones, especially those based on the Android OS, it has become an integral part of everyday life. This is because smartphones have various features that can meet the needs of their users, so good network security is needed. In network security, there are several methods used to secure the network. One of them uses the Metasploit Framework

Royana, Supriyono
Email: royana.royana250@gmail.com,
supriyono200498@gmail.com

method which is a security method that combines identification and prosecution. In implementing a security system to find out the loopholes in the Android OS system, researchers use a backdoor. In making a backdoor one of which can be done by using the metasploit framework. This method is operated via Command Prompt on Windows which will create a Backdoor apk that will be sent and installed in the Android OS operating system. sms, phone call logs, installed application data, android location on Android OS system using backdoor metasploit framework. In this study using literature and documentation methods to determine the Android OS security system. The final results of this research are SMS message data, phone call logs, installed application data, and the location of the target Android OS successfully accessed and can be displayed via the Command Prompt terminal.

1. Pendahuluan

Penggunaan smartphone berbasis OS Android berkembang pesat dan melekat dalam kehidupan sehari-hari. Maka diperlukan sistem keamanan jaringan yang baik untuk mengamankan data dan hal-hal penting lainnya. Keamanan jaringan ialah seperangkat aturan dan konfigurasi yang dirancang untuk melindungi integritas, kerahasiaan, dan aksesibilitas pada jaringan komputer dan data menggunakan teknologi perangkat lunak dan perangkat keras.Keamanan jaringan pada intinya adalah mengendalikan akses terhadap sumber daya jaringan. Akses jaringan dikontrol agar bisa diakses oleh siapa saja yang berhak dan menghalangi orang atau subjek yang tidak terdaftar untuk mengaksesnya.

Keamanan data pribadi dan privasi pengguna di berbagai platform digital kini menjadi salah satu hal krusial. Fenomena kebocoran dan penyalahgunaan data pribadi pada beberapa waktu terakhir pun memunculkan kecemasan di masyarakat. Kekhawatiran tersebut umumnya seputar integrasi data pengguna, seperti nomor telepon, layanan yang terkait dengan informasi, lokasi, dan data transaksi yang berisiko diperjualbelikan. Tak hanya itu, aksi peretasan smartphone juga semakin marak, mulai dari peretasan percakapan atau aplikasi pesan, informasi pembayaran, hingga peretasan data pribadi yang tersimpan pada perangkat smartphone. Fenomena tersebut pun mendorong masyarakat semakin waspada dan berhati-hati saat beraktivitas secara digital dengan menggunakan smartphone.

Saat ini sistem keamanan OS Android belum sepenuhnya aman dan masih memiliki celah celah yang terdapat pada sistem OS Android seperti seperti data pesan sms, log panggilan telepon, data aplikasi yang terinstal, lokasi android pada sistem OS Android Untuk mengatasi hal tersebut diperlukan suatu sistem yang salah satunya dapat menggunakan backdoor. Backdoor adalah portal tidak berdokumen. Portal ini memungkinkan administrator untuk masuk ke sistem untuk melakukan pemecahan masalah atau pemeliharaan. Saat masalah ini terjadi, backdoor adalah salah satu solusi yang berhasil. Backdoor dimasukkan ke dalam kode sistem atau program secara diam-diam sehingga pengguna tidak mengetahui bahwa ada backdoor di dalam sistem. Alhasil, backdoor bisa masuk dan mendapatkan akses ke sistem pengguna bahkan bisa mengakses keseluruhan sistem. Salah satu cara untuk membuat backdoor adalah dengan menggunakan framework metasploit, framework metasploit sendiri merupakan alat penetrasi yang cukup ampuh untuk menembus suatu sistem, metasploit merupakan framework penetrasi jaringan komputer yang bersifat free dan open source. Serangan metasploit dengan cara mengirimkan exploit yang berisi payload yang telah ditentukan oleh sistem penyusup. Payload sendiri merupakan file executable intruder yang akan berjalan di komputer dengan tujuan agar dapat mengontrol komputer dari jarak jauh atau

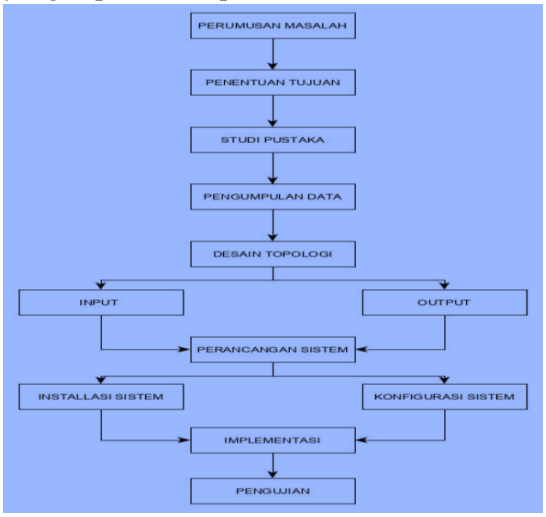
SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 1, Juni 2023, pp. 74-81
ISSN: 2527-9114, DOI: 10.33372/stn.v9i1.952

menginstall backdoor, trojan, virus, worm, dan lain-lain. Dalam mengimplementasikan sistem keamanan OS Android menggunakan backdoor framework metasploit, diawali dengan membangun framework metasploit kemudian mengumumkan dan menginstalnya ke dalam sistem OS Android kemudian menguji sistem OS Android untuk meningkatkan sistem keamanannya. Dengan menguji backdoor kerangka kerja metasploit, kita akan melihat celah di sistem OS Android seperti data pesan SMS, log panggilan telepon, data aplikasi yang diinstal, dan lokasi android dapat diakses dengan mudah.

2. Metode Penelitian

2.2 Tahapan Penelitian

Penelitian ini memiliki beberapa tahapan yang dapat dilihat pada Gambar 1 berikut ini :



Gambar 1. Diagram Tahapan Penelitian

Dari diagram di atas, dapat disimpulkan bahwa alurnya adalah sebagai berikut:

a. Perumusan masalah adalah merumuskan masalah untuk mencari solusi yang tepat dari masalah tersebut.
b. Menetapkan tujuan yaitu menentukan tujuan sistem apa yang akan dibangun berdasarkan permasalahan yang ada.
c. Studi pustaka yaitu mencari sumber referensi yang sesuai dengan sistem yang akan dibangun.
d. Pengumpulan data adalah pengumpulan data yang akan digunakan sebagai sistem pendukung.
e. Perancangan topologi adalah perancangan topologi jaringan yang akan digunakan dalam implementasi sistem.
f. Input dan Output yaitu mencari masukan dari luar atau dalam untuk membuat sistem yang akan dibangun.
g. Perancangan sistem adalah merancang sistem sesuai dengan kebutuhan yang dibutuhkan, yang bersumber dari masalah yang telah dirumuskan.
h. Instalasi dan konfigurasi sistem adalah menginstal dan mengkonfigurasi sistem sesuai dengan kinerja yang diinginkan.
i. Implementasi adalah menerapkan sistem yang telah dibangun.
j. Testing adalah menguji dan menjalankan sistem secara lengkap dan detail untuk melihat hasil secara keseluruhan.

2.3 Perangkat yang Digunakan untuk Mengimplementasikan Metasploit framework pada sistem operasi android.

1. Perangkat Keras (Hardware)
   a. Laptop Lenovo Dengan Processor intel core i5 (sebagai Metasploit framework)
   b. Kabel Data Type C
   c. Smartphone Samsung Galaxy A51 (sebagai target).

2. Perangkat Lunak (Software)
   a. Command Prompt yang digunakan sebagai operating system dalam menjalankan Metasploit framework.
   b. Hotspot Seluler.
   c. Android.
   d. Windows 10.

2.4 Konsep Implementasi Backdoor Metasploit Framework Pada Sistem Operasi Android

Konsep yang digunakan untuk uji coba penyerangan terhadap sistem operasi android

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 1, Juni 2023, pp. 74-81
ISSN: 2527-9114, DOI: 10.33372/stn.v9i1.952

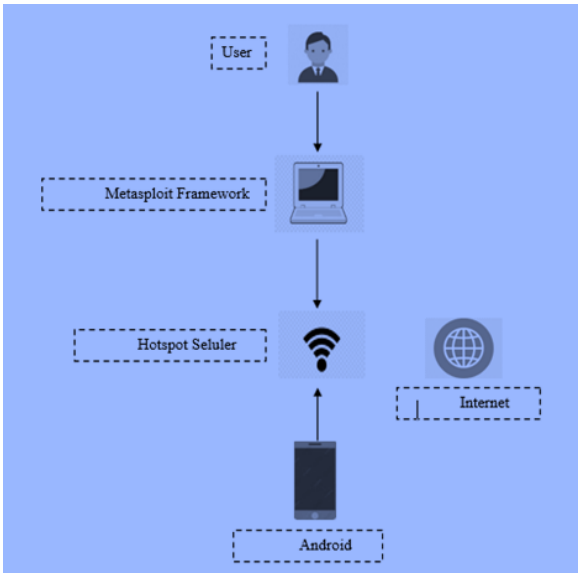
ini menggunakan metode Metasploit framework adalah, dengan cara menghubungkan antara Metasploit framework dan smartphone yang menggunakan OS Android melalui jaringan yang sama. Untuk menghubungkan keduanya maka di gunakan hotspot seluler yang kemudian akan saling terhubung antara satu dan lainnya. Implementasi ini akan berhasil apabila disaat Metasploit framework melakukan penetrasi kedalam smartphone dan kemudian HP tersebut dapat di control melalui PC Metasploit framework. Maka dari itu berarti implementasi Metasploit framework atas sistem operasi android dengan menggunakan hotspot seluler yang sama telah berhasil.

2.4.1 Sistem Kinerja Metasploit Framework

Metasploit framework merupakan sebuah metode penyerangan yang melakukan penetrasi kedalam sistem keamanan pengguna dalam 1satu jaringan yg sama. Dalam implentasi ini akan di uji coba pada sistem android, dimana nanti Metasploit framework akan melakukan penyerangan terhadap sistem keamanan android. Kemudian akan mencoba mengakses data-data pribadi pada smartphone Samsung Galaxy A51. Untuk melakukan implementasi ini penulis menggunakan sistem operasi command prompt pada windows yang dijalankan pada laptop Lenovo intel i5.

2.5 Topologi Jaringan

Membangun Topologi Jaringan



Gambar 2. Topologi Jaringan

Dari gambar di atas dapat disimpulkan bahwa alurnya adalah sebagai berikut :

a. Pengguna Pengguna yang dapat mengoperasikan framework metasploit di android
b. Kerangka Metasploit Kerangka kerja metasploit akan terhubung ke hotspot seluler dan kemudian menembus Android
c. Hotspot Seluler Mobile hotspot menjadi jembatan antara framework metasploit dan android
d. Android Android akan terhubung ke hotspot seluler dan menjadi target kerangka kerja metasploit

3. Hasil dan Pembahasan

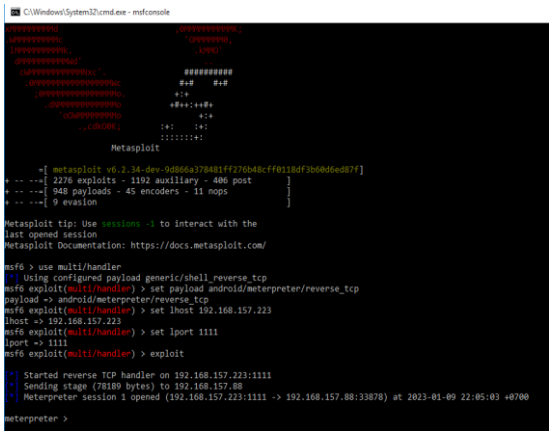
3.1 Melakukan Metasploit Framework Attack.

Serangan Metasploit Framework bekerja dengan cara meretas sistem Android secara sistematis, sehingga jika serangan ini berhasil maka smartphone dapat dikendalikan dari laptop pengguna metasploit framework. Jika smartphone dapat ditembus oleh framework metasploit, maka penyerang atau hacker akan dengan mudah masuk dan menguasai smartphone serta dapat mencuri konten dan data pribadi pada smartphone target. Serangan

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 1, Juni 2023, pp. 74-81
ISSN: 2527-9114, DOI: 10.33372/stn.v9i1.952

ini bisa dilakukan dengan beberapa cara, dan disini saya akan menggunakan script perintah di terminal. dari Command Prompt untuk menyerang android.

3.2 Script Untuk Melakukan Metasploit Framework Attacks Berikut ini adalah salah satu cara yang digunakan untuk menguji serangan terhadap Android menggunakan framework Metasploit, dalam hal ini akan diuji apakah sistem operasi Android pada Samsung Galaxy A51 dapat ditembus atau tidak oleh serangan Metasploit Framework dengan langkah-langkah sebagai berikut: Melakukan exploit pada OS android Untuk mengeksekusi framework metasploit ini kita hanya perlu mengetikkan 1 perintah lagi di terminal CMD yaitu exploit setelah perintah diketik akan menghubungkan antara CMD PC dengan smartphone target. Eksploitasi berikut sedang berjalan:



Gambar 3. Serangan metasploit framework

Setelah eksploitasi dilakukan, PC dan smartphone akan terhubung satu sama lain. Dan untuk membuktikannya, ketikkan perintah sysinfo di CMD seperti berikut :

```
meterpreter > sysinfo
Computer        : localhost
OS              : Android 12 - Linux 4.14.113-24700230 (aarch64)
Architecture    : aarch64
System Language : in_ID
Meterpreter     : dalvik/android
meterpreter >
```

Gambar 4. Info perangkat Android terhubung

Pada gambar diatas sudah jelas kita bisa masuk ke performance system di Android. Untuk membuktikannya, kami akan melakukan serangan dan dapat mengakses data pribadi di OS Android target. Berikut adalah perintah serangan yang dapat mengakses data pribadi target yaitu:

1. Perintah dump_sms untuk mendapatkan data pesan sms pemilik os android target.

```
meterpreter > dump_sms
[*] Fetching 4741 sms messages
[*] SMS messages saved to: sms_dump_20230109222048.txt
meterpreter >
```

Gambar 5. Perintah dump_sms

Dari gambar diatas terlihat perintah-perintah yang dapat dijalankan melalui CMD untuk mengakses data pada smartphone target, untuk mengambil data pesan SMS pada smartphone melalui CMD digunakan perintah berikut : dump_sms digunakan untuk pesan sms pada os android .

Gambar 6 Menampilkan pesan sms pada android

Pada dump SMS Message di atas terlihat bahwa semua pesan yang disimpan di Android pengguna telah berhasil diambil, semua pesan, waktu dan tanggal SMS diterima terlihat.

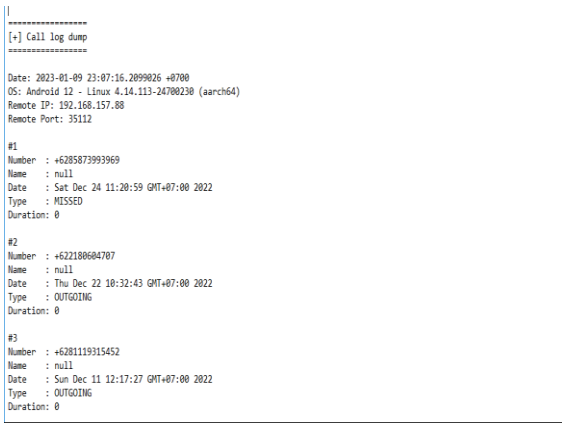
2. Perintah dump_calllog untuk mendapatkan data panggilan untuk pemilik os android.

```
meterpreter > dump_calllog
[*] Fetching 934 entries
[*] Call log saved to calllog_dump_20230109230715.txt
meterpreter >
```

Gambar 7. Perintah dump_calllog

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 1, Juni 2023, pp. 74-81
ISSN: 2527-9114, DOI: 10.33372/stn.v9i1.952

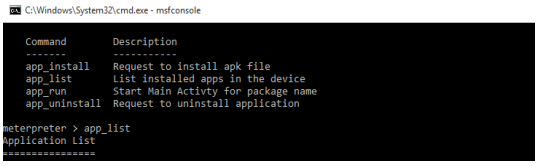
Dari gambar diatas terlihat bahwa perintah dapat dijalankan melalui CMD untuk mengakses data pada smartphone target, untuk mengambil data panggilan pada smartphone melalui CMD digunakan perintah berikut: dump_calllog digunakan untuk data panggilan pemilik os android.



Gambar 8 Tampilan data panggilan pada android

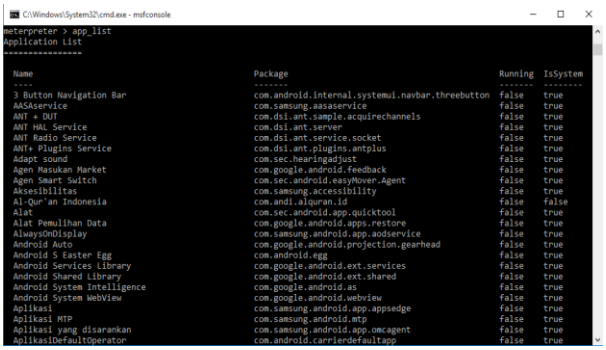
Terlihat pada gambar di atas adalah data panggilan yang merupakan panggilan masuk dan keluar pengguna pada perangkat Android, mulai dari jam panggilan, durasi panggilan, hari & tanggal serta nama pengguna yang melakukan panggilan ke ponsel pengguna.

3. Perintah app_list adalah untuk menginstal data aplikasi di OS Android



Gambar 9 Perintah app_list

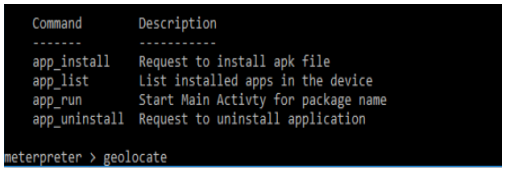
Gambar di atas menunjukkan beberapa aplikasi yang terpasang di perangkat Android pengguna, dengan memberikan nama dan Dari Gambar dibawah menunjukan beberapa aplikasi yang terpasang di android dengan memberikana nama dan informasi paket yang digunakan. Ini juga menampilkan keadaan aplikasi sedang berjalan atau tidak



Gambar 10. Data aplikasi yang terinstall

Dari gambar diatas dapat dilihat perintah-perintah yang dapat dijalankan melalui CMD untuk mengakses data pada smartphone target, untuk mengambil data aplikasi yang terinstal pada smartphone melalui CMD, gunakan perintah berikut: app_list digunakan untuk mendapatkan data aplikasi yang terinstal pada android os.

4. Perintah geolocate untuk mendapatkan lokasi target saat ini di OS Android



Gambar 11. Tampilan perintah geolokasi

Dari gambar diatas terlihat perintah yang dapat dijalankan melalui CMD untuk mengakses lokasi pemilik gunakan perintah berikut: geolocate digunakan untuk target saat ini lokasi di os android

Gambar 12. Lokasi target saat ini

Penulis mengecek lokasi pengguna Android saat ini, namun gagal untuk diakses hanya beberapa informasi yang dapat dilihat seperti letak latitude dan longitude. Untuk melihat informasi melalui google maps dengan mengklik tautan di command prompt terminal.

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 1, Juni 2023, pp. 74-81
ISSN: 2527-9114, DOI: 10.33372/stn.v9i1.952

3.3 Performa Metasploit Framework

Performa framework metasploit dapat diukur dari berhasil atau tidaknya melakukan serangan terhadap target yaitu smartphone Android. Pada uji coba ini, framework Metasploit yang dijalankan melalui command prompt berhasil mendapatkan akses data pribadi di smartphone target. Dalam rangkaian uji coba yang dilakukan, kesimpulan dari uji coba tersebut dapat diuraikan dalam tabel berikut:

Tabel 1 Hasil Uji Coba

No	Jenis Serangan	Target	Keterangan
1	Metasploit Framework	Samsung Galaxy A51	Berhasl
2	Pesan Sms Android	Samsung Galaxy A51	Berhasl
3	Data Panggilan Android	Samsung Galaxy A51	Berhasl
4	Daftar Aplikasi Android	Samsung Galaxy A51	Berhasl
5	Cek Lokasi Android	Samsung Galaxy A51	Gagal

Penjelasan dari tabel diatas adalah :

1. Menguji framework metasploit pada Samsung Galaxy A51 mendapatkan akses data yang terdapat pada smartphone target

2 Pengujian framework metasploit dengan mengeksekusi perintah dump_sms pada Samsung Galaxy A51, pada pengujian ini framework metasploit berhasil mendapatkan data pesan sms pada smartphone target.

3 Pengujian framework metasploit dengan mengeksekusi perintah dump_calllog pada Samsung Galaxy A51, pada pengujian ini framework metasploit berhasil mendapatkan data panggilan pada smartphone target.

4 Pengujian framework metasploit dengan mengeksekusi perintah app_list pada Samsung Galaxy A51, pada pengujian ini framework metasploit berhasil menginstal data aplikasi pada smartphone target.

5 Pengujian metasploit framework dengan melakukan perintah geolocate pada Samsung Galaxy A51, pengujian ini gagal dilakukan lokasi dapat di buka apabila android sudah di root. Jika android belum di root maka yang terlihat hanya di terminal , tidak bisa memperlihakan di google maps pada web browser pc/laptop

3. Kesimpulan

1. Berdasarkan hasil penelitian dan pengujian dapat disimpulkan :
   Pada pengujian ini metasploit framework mampu masuk kedalam sistem kerja smartphone Samsung Galaxy A51 sebagai target, sehingga dapat mengakses data data yang pada OS Android target dan Implementasi metasploit framework ini dapat dilakukan apa bila antara penyerang dan target berada dalam 1 jaringan yang sama..Pengujian Sistem Keamanan OS Android menggunakan Metasploit Framework berhasil melakukan uji coba serangan untuk mendapatkan data pesan sms, data panggilan telepon, data aplikasi yang diinstal berhasil diakses dan ditampilkan pada terminal command prompt , hanya cek lokasi Android yang gagal diakses lokasi dapat di buka apabila android sudah di root. Jika android belum di root maka yang terlihat hanya di terminal , tidak bisa memperlihakan di google maps pada web browser pc/laptop.

4. Referensi

Daeng, I.T.M,. Mewengkang, N.N,. Kalesaran, E.R,(2015). “Penggunaan Smartphone Dalam Menunjang Aktivitas

Perkuliahan Oleh Mahasiswa Fispol Unsrat Manado".E-jurnal, Vol.6 No.1

Darmawan, D, Marlinda, L,(2017). " Impelementasi Jaringan Wireless Outdoor Menggunakan NaniBridge". Jurnal teknik informatika, Vol.1 No.12. ISSN : 2442-2436.

Fachri, B, (2018). "Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif". Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.

Halawa, S, (2016) " Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (Smk) Teknik Komputer Dan Jaringan (Tkj) Dengan Metode Computer Based Instruction". Jurnal Riset Komputer (JURIKOM), Volume : 3, Nomor: 1. ISSN : 2407-389X.

Harjono, E.B, (2016) "Analisa Dan Implentasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER". Jurnal teknik informatika, Vol.1 No.1. ISSN : 2541-2019.

Juansyah, A, (2015) "Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-Gps) Dengan Platform Android". jurnal komputa, Vol.1. ISSN : 2089-9033

Maiyana, E, (2018) "Pemanfaatan Android Dalam Perancangan Aplikasi Kumpulan Doa".Jurnal sains dan informatika. Vol.4 No.11. ISSN: 2459-9549.

Nurmiati, E, (2012) " Analisis Dan Perancangan Web Server Pada Handphone". Jurnal Sistem Informasi, 5 (2), 1-17, ISSN: 1979-0767.

Putra, R.A. Fadli, A. Riadi, I, (2017) "Forensik Mobile pada Smartwatch Berbasis Android". Jurnal TI. Vol.1 No.1. ISSN: 2579-8790

Rahmadani, M.A. Rizal, M.F, (2017) "Implementasi Hacking Wireless Dengan KaliLinux Menggunakan Kali Nethunter". E-jurnal, Vol.3 No.3. ISSN: 2442-5826.