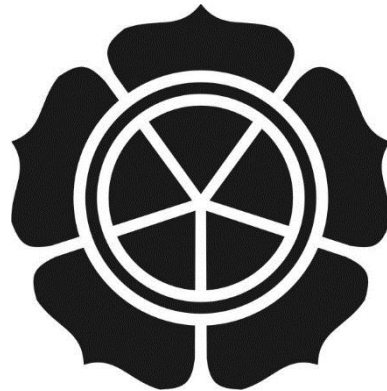


**PENGUJIAN KEAMANAN ANDROID DENGAN MENGGUNAKAN  
STANDAR MOBILE PENTESTING**

**SKRIPSI**



di susun oleh

**Rahmad Suryono**

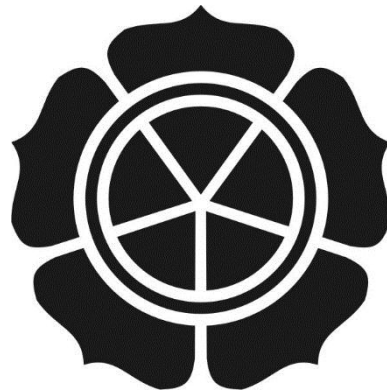
**12.11.6103**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**PENGUJIAN KEAMANAN ANDROID DENGAN MENGGUNAKAN  
STANDAR MOBILE PENTESTING**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai derajat Sarjana S1  
pada jurusan Teknik Informatika



disusun oleh

**Rahmad Suryono**

**12.11.6103**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**PERSETUJUAN**

**SKRIPSI**

**PENGUJIAN KEAMANAN ANDROID DENGAN MENGGUNAKAN  
STANDART MOBILE PENTESTING**

Yang dipersiapkan dan disusun oleh

**Rahmad Suryono**

**12.11.6103**

Telah disetujui oleh Dosen Pembimbing skripsi

Pada tanggal 22 April 2015

Dosen Pembimbing,

**Ema Utami, Dr., S.Si, M.Kom**

**NIK. 190302037**

**PENGESAHAN**

**SKRIPSI**

**PENGUJIAN KEAMANAN ANDROID DENGAN MENGGUNAKAN  
STANDAR MOBILE PENTESTING**

Yang dipersiapkan dan disusun oleh

**Rahmad Suryono**

**12.11.6103**

Telah dipertahankan di depan Dewan Penguji

Pada tanggal 24 Februari 2016

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Barka Satva, M.Kom**  
NIK. 190302126



**Hartatik, ST, M.CS**  
NIK. 190302232



**Ema Utami, Dr., S.Si, M.Kom**  
NIK. 190302037



Skripsi ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar Sarjana Komputer

Tanggal 10 Maret 2016

**KETUA STMIK AMIKOM YOGYAKARTA**



**Prof. Dr. M. Suvanto, M.M.**  
NIK. 190302001

## PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 10 Maret 2016



Rahmad Suryono  
NIM. 12.11.6103

## MOTTO

“Jadilah dirimu sebagaimana yang kau inginkan”

“Harga kebaikan manusia adalah diukur menurut apa yang telah

Dilaksanakan atau diperbuatnya”

(Ali Bin Abi Thalib)



## PERSEMBAHAN

Puji syukur kehadirat Allah SWT, karena berkat rahmat dan ridho-Nyapenulis dapat menyelesaikan Skripsi ini Skripsi ini saya persembahkan untuk:

### ***Ayah Subasri dan Ibu thokiyatun***

*Terimakasih atas dukungan, motivasi, kerja keras, kasih sayang, kepercayaan, dan do'a yang sudah diberikan. Saya merasa sangat bersyukur sudah memiliki Orang tua seperti kalian. Adik dan saudara yang telah membantu mendo'akan saya.*

### ***Ema Utami***

*Terimakasih banyak atas arahan, bimbingan, saran dan waktu yang sudah diberikan sehingga saya dapat menyelesaikan Skripsi saya dengan maksimal.*

### ***Teman - teman***

*Terimakasih untuk teman – teman 12-SITI-06 dan para sahabat yang tidak bisa saya sebutkan namanya satu persatu, terimakasih telah memberikan dukungan sampai selesainya Skripsi ini.*

### ***STMIK AMIKOM Yogyakarta***

*Terimakasih untuk semua ilmu pengetahuan yang sudah diberikan selama masa kuliah, semoga lebih bermanfaat, dan Amikom menjadi lebih baik serta sukses.*

## KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan penulis. Tidak lupa sholawat serta salam penulis haturkan pada junjungan umat yaitu Nabi Muhammad SAW, yang telah menyebarkan agama Islam sehingga penulis dan seluruh umat islam dapat merasakan indahnya Islam.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M.suyanto, MM. Selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan MT, selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ayahanda Subasri & Ibunda Thokiyatun, kakak saya tercinta Eka Ruli safitri, yang selalu memberikan do'a dan dukungan kepada saya.
4. Terimakasih untuk Lia Choria Santi yang sudah memberikan semangat dan dukungan agar saya segera menyelesaikan skripsi.



5. Dan juga tidak lupa teman – teman seperjuangan dan para sahabat yang membantu kelancaran penulisan laporan Skripsi ini
6. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama penulis kuliah.

Penulis menyadari sepenuhnya bahwa laporan ini masih jauh dari kata sempurna, itu semua karena keterbatasan penulis dalam hal pengetahuan. Kritik dan saran yang bersifat membangun guna mencapai kesempurnaan akan selalu penulis harapkan sehingga dapat menjadi lebih bermanfaat bagi penulis serta pihak – pihak yang membutuhkan.

Akhirnya dengan do'a kepada Allah SWT, semoga laporan skripsi ini bermanfaat bagi semua pihak yang membutuhkan.

Yogyakarta, 11 Maret 2016

Rahmad Suryono

12.11.6103

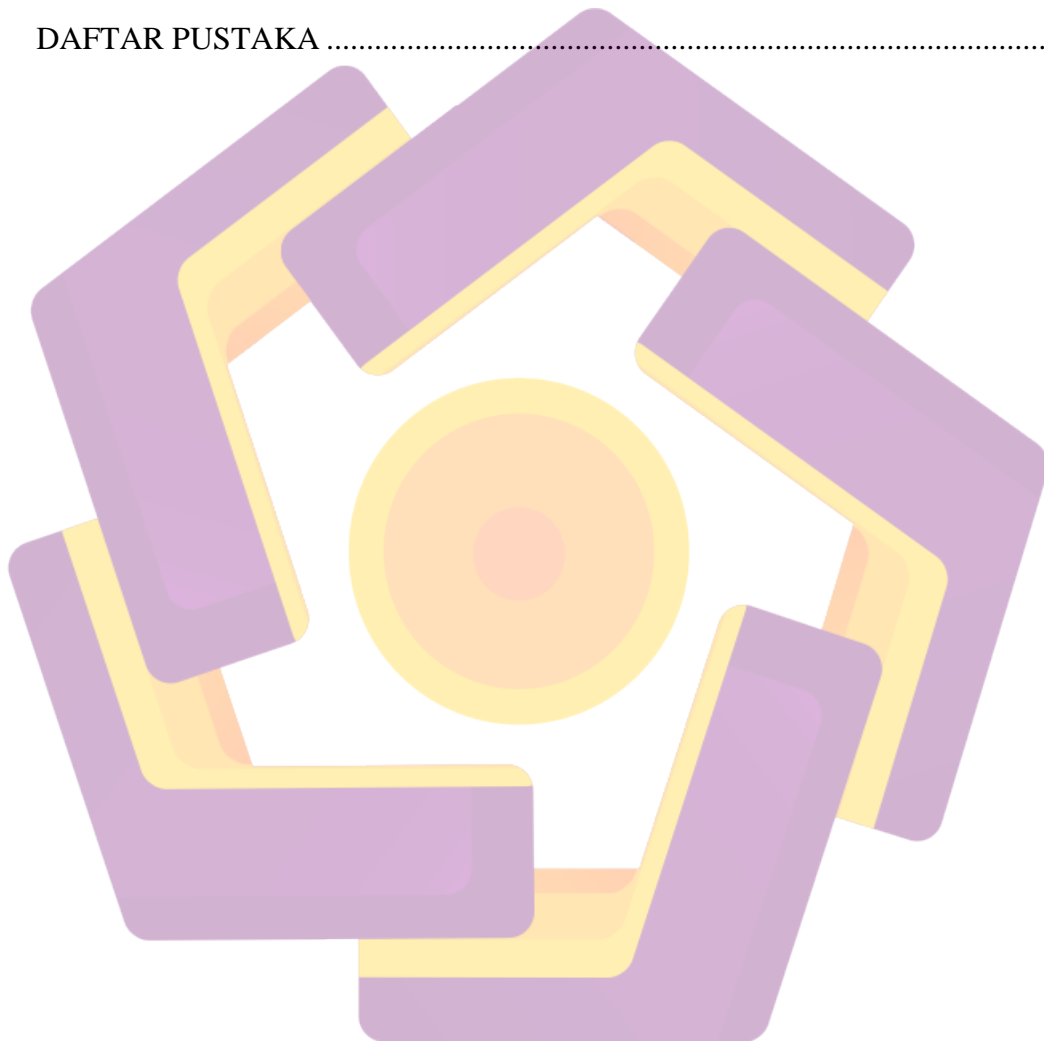
## DAFTAR ISI

HALAMAN JUDUL.....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN.....	iv
MOTTO .....	v
PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR .....	xiv
INTISARI.....	xvi
<i>ABSTRACT</i> .....	xvii
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
BAB II.....	6
LANDASAN TEORI.....	6

2.1	Tinjauan Pustaka .....	6
2.2	Sejarah Android.....	7
2.2.1	Versi Android.....	8
2.2.2	APK.....	8
2.3	OWASP.....	9
2.3.1	Tahapan Pentest .....	9
2.4	Jenis Jenis penyerangan.....	11
2.4.1	ARP Spoofing .....	13
2.4.2	DNS Spoofing.....	14
2.4.3	MITM Attack .....	15
2.4.4	Intercept Packet.....	16
2.4.5	Eksplorasi.....	18
2.4.6	Browser attack.....	19
2.4.7	Social Engineering .....	19
2.5	Metasploit Framework .....	20
2.5.1	Meterpreter.....	21
2.6	Backdoor .....	22
BAB III .....		24
METODE PENELITIAN.....		24
3.1	Gambaran umum Mobile Pentesting.....	24

3.2	Alat dan Bahan .....	24
3.2.1	Kebutuhan Software.....	24
3.2.2	Kebutuhan Hardware .....	25
3.2.3	Kebutuhan Fungsional .....	25
3.2.4	Kebutuhan non Fungsional .....	26
3.3	Kerangka Berpikir .....	26
3.4	Reconnaissance .....	27
3.4.1	Scanning.....	29
3.4.2	Gaining Access.....	34
3.4.3	Maintaining Access.....	35
3.4.4	Covering Track.....	35
BAB IV	.....	36
HASIL DAN PEMBAHASAN.....		36
4.1	Proses Pengujian Keamanan Android .....	36
4.2	Proses Identifikasi .....	36
4.3	Proses Eksploitasi .....	36
4.4	Covering Track.....	49
4.4.1	Proses Pembersihan via smartphone .....	49
4.4.2	Pembersihan melalui adb shell.....	50
4.5	Mitigasi.....	51

BAB V.....	53
PENUTUP.....	53
5.1 Kesimpulan.....	53
5.2 Saran.....	53
DAFTAR PUSTAKA .....	54



## DAFTAR TABEL

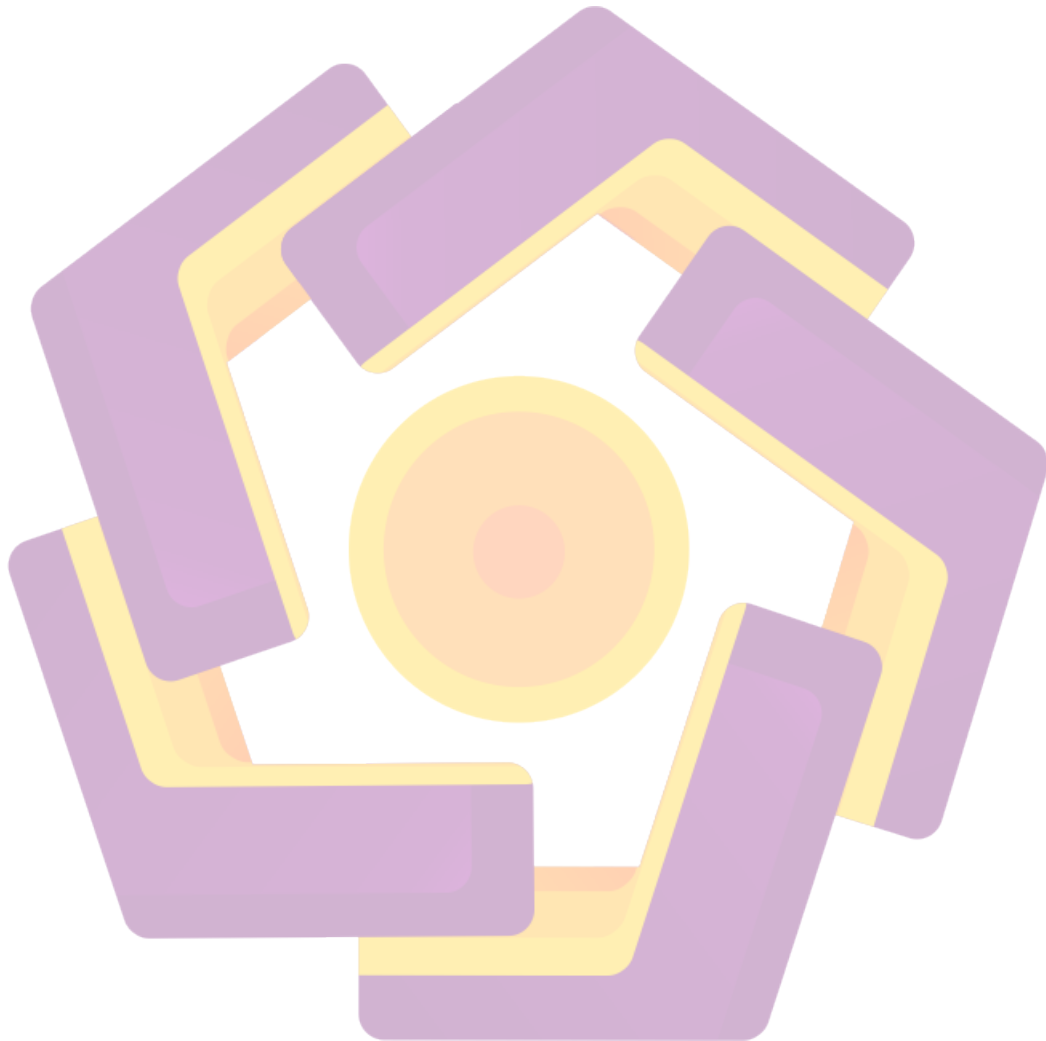
Tabel 4.1 *Paramater Generate File Malware* .....39



## DAFTAR GAMBAR

Gambar 2. 1 Skenario <i>Spoofing</i> .....	14
Gambar 2. 2 Skenario DNS <i>Spoofing</i> .....	15
Gambar 3. 1 Proses Penelitian .....	27
Gambar 3. 2 <i>developer.android.com</i> .....	28
Gambar 3. 3 <i>cve.mitre.org</i> .....	28
Gambar 3. 4 referensi dari <i>www.exploit.db.com</i> .....	29
Gambar 3. 5 proses <i>scanning</i> nmap .....	30
Gambar 3. 6 proses <i>scanning</i> .....	31
Gambar 3. 7 Speksifikasi ponsel.....	32
Gambar 3. 8 <i>Impact Level High</i> .....	33
Gambar 3. 9 <i>Impact Level High Medium</i> .....	33
Gambar 4. 1 Menggunakan Metasploit ( <i>Msfconsole</i> ).....	37
Gambar 4. 2 menjalankan <i>service postgresql</i> .....	37
Gambar 4. 3 menjalankan <i>msfconsole</i> .....	38
Gambar 4. 4 <i>generate file malware</i> .....	39
Gambar 4. 5 proses <i>copy</i> ke root folder web server .....	40
Gambar 4. 6 Untuk menjalankan <i>web server Apache</i> .....	41
Gambar 4. 7 proses membuat server handler .....	41
Gambar 4. 8 <i>show options</i> .....	42
Gambar 4. 9 <i>payload</i> .....	43
Gambar 4. 10 Pengisian Parameter IP server Handler .....	43
Gambar 4. 11 set LPORT .....	44
Gambar 4. 12 proses <i>handler</i> .....	44
Gambar 4. 13 proses run identifikasi 1 .....	45
Gambar 4. 14 run session 2 .....	45
Gambar 4. 15 run session 11 .....	46
Gambar 4. 16 <i>dump_sms</i> .....	46
Gambar 4. 17 <i>dump_sms ke 2</i> .....	47

Gambar 4. 18 contacts korban.....	48
Gambar 4. 19 isi contacs korban setelah proses pengetesan ulang.....	48
Gambar 4. 20 pembersihan file apk .....	50
Gambar 4. 21 langkah awal pebersihan melalui adb shell.....	50
Gambar 4. 22 proses pengecekan data .....	51





## INTISARI

Android adalah salah satu sistem operasi yang paling banyak digunakan saat ini terutama pada perangkat mobile. Menurut data android yang berada dipasaran lebih dari 50 % smartphone menggunakan android sebagai sistem operasinya. Dapat dibayangkan banyaknya smartphone android yang berada dipasaran. Semakin banyak pengguna sebuah platform maka seharusnya akan sebanding juga dengan ancaman yang ada dalam keamanan platform tersebut.

Keamanan merupakan salah satu hal yang utama yang perlu diperhatikan oleh pengguna smartphone, mengingat semua transaksi yang ada saat ini menggunakan smartphone. Sehingga ketika smartphone yang digunakan terancam keamanannya maka bisa dipastikan transaksi yang dilakukan juga akan ikut terancam. Dengan banyaknya ancaman banyak lembaga membuat standarisasi untuk proses pengetesan mobile diantaranya adalah standar top risk yang dibuat oleh owasp dari sinilah penulis membuat judul pengujian Keamanan android dengan menggunakan standar mobile pentesting sebagai acuan seberapa amankah mobile yang ada dalam genggaman banyak pengguna saat ini.

Kata Kunci : Linux, Metasploit , Android, OWASP

## **ABSTRACT**

*android operating system is one of the most widely used today, especially on mobile device. According to data from android that sold more than 50% of SmartPhone that sold. The more users a platform that should be comparable also with the existing threats to the security of the platform.*

*Security is one of the main things that need to be considered by SmartPhone users, considering all existing transactions using SmartPhones. So that when the SmartPhone is used then certainly threatened the security of transactions carried out will also be threatened. With so many threats for many institutions to standardize the testing process include standard mobile top risk created by OWASP is where the author makes the title "Security Testing Using The Standard Android Pentesting" as a reference to how safe that is in the hands of mobile users today.*

**Keywords** - *linux, metasploit ,android, OWASP*

