EVALUASI SERANGAN EXPLOIT TERHADAP SISTEM OPERASI ANDROID PADA JARINGAN INTERNET

Fauzul Akbar[1], Hanafi[2], Anita Fauziah[3]

[1,2,3] *Prodi Teknologi Rekayasa Jaringan Telekomunikasi*
Jurusan Teknik Elektro Politeknik Negeri Lhokseumawe
Email: fauzulakbar937@gmail.com, hnfbatubara@yahoo.com, anita_fy@yahoo.com

Abstrak—Populasi pengguna seluler didunia saat ini meningkat setiap hari dan bagian terbesar diantaranya adalah pengguna internet. Di indonesia sendiri saat ini pengguna internet didominasi oleh pengguna smartphone. Serangan *exploit* merupakan salah satu serangan *remote exploit* dimana serangan ini bekerja untuk mencuri data-data penting pada sebuah perangkat android dengan memanfaatkan celah yang terdapat pada sebuah system operasi android. Penelitian ini bertujuan untuk mengetahui cara kerja serangan *exploit* terhadap smartphone android yang berada dalam jaringan internet dan membandingkan keamanan yang terdapat pada system android versi sebelumnya dan versi terbaru. Penelitian ini menggunakan metode *apk msf* dan metode *apk original* sebagai metode pengujian dalam melakukan serangan *exploit.* Hasil penelitian menunjukkan bahwa serangan *exploit* masih dapat dilakukan pada smartphone android versi 8 dan versi 11 dengan durasi waktu *exploitasi* paling lama sekitar 5 menit 23 detik yang terjadi pada android versi 8 sedangkan durasi waktu exploitasi paling singkat sekitar 44 detik yang terjadi pada android versi 11. Pengujian *exploitasi* serangan *exploit* pada android versi 8 berhasil diimplementasi pada semua aspek sedangkan pengujian *exploitasi* pada android 11 dengan menggunakan metode *apk msf* tidak berhasil melakukan *webcam snap, webcam stream* dan *dump contacts*, namun ketika menggunakan metode *apk original* berhasil melakukan *exploitasi* di semua aspek impementasi kecuali *dump contacts*.

Kata-kata kunci: Exploit, Android, Evil Droid Framework, Backdoor, Smartphone.

I. PENDAHULUAN

Populasi pengguna seluler didunia saat ini meningkat setiap hari dan bagian terbesar diantaranya adalah pengguna internet. Di Indonesia sendiri saat ini pengguna internet didominasi oleh pengguna smartphone. Dikutip dari HootSuite, jumlah pengguna internet pada januari 2020 mencapai 94% [1]. Dengan jumlah pengguna yang sangat besar, tidak menutup kemungkinan jumlah ancaman dan serangan terhadap pengguna smartphone juga sangat besar.

Berdasarkan data resmi dari Badan Siber dan Sandi Negara Republik Indonesia, serangan *Exploit Kit* merupakan salah satu serangan yang masuk dalam top 5 sebagai serangan yang sering digunakan mulai periode Januari – April. Serangan *Exploit Kit* pada bulan Maret terjadi sekitar 1% dari rekapitulasi serangan cyber yang terjadi di Indonesia, kemudian pada bulan April serangan exploit mengalami peningkatan sebesar 4%. Ini membuktikan bahwa hingga kini serangan exploit masih digunakan untuk melakukan penyerangan terhadap sebuah system.

Umumnya serangan exploit bekerja dengan cara menanamkan sebuah virus ke dalam sebuah system target dengan cara mengirimkan aplikasi palsu, menanamkan virus ke aplikasi asli dan lain-lain.

Motivasi dari penelitian ini adalah untuk mengetahui cara serangan *exploit* terhadap smartphone android yang berada dalam jaringan Internet. Kemudian peneliti ingin membandingkan keamanan yang terdapat pada system android versi sebelumnya dan versi terbaru dengan cara melakukan percobaan serangan *exploit* dan melakukan eksploitasi terhadap system smartphone target.

II. TINJAUAN PUSTAKA

A. Sistem Operasi Linux

Linux adalah system operasi yang bersifat *open source*, yang berarti kode-kode sumber pada linux dapat digunakan, dimodifikasi dan didistribusikan secara bebas oleh siapapun.

B. Sistem Operasi Android

Pada dasarnya sistem operasi android menggunakan sistem yang berbasis linux. Sistem operasi android menyediakan platform yang bebas dan terbuka bagi para pengembang untuk menciptakan dan mengembangkan aplikasi mereka sendiri sehingga dapat digunakan pada perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet.

a. Fitur Keamanan Sistem Operasi Android

Android memiliki fitur keamanan bawaan yang di desain secara signifikan untuk melindungi sebuah perangkat dari software berbahaya yang dapat mengakses system pada android dengan tujuan untuk mengendalikan maupun mencuri data sensitive dari

sebuah perangkat. Beberapa fitur keamanan yang disediakan pada system operasi android adalah sebagai berikut:

- *Google Play Protect* adalah fitur keamanan yang disediakan oleh google pada sebuah perangkat android yang mampu untuk mendeteksi dan menghapus aplikasi yang berbahaya pada sebuah system android.

- *Kontrol Privasi* adalah fitur keamanan dalam mengelola privasi pengguna diantaranya adalah manajemen location, manajemen call logs, manajemen contacts, kontrol aktivitas fisik dan kontrol app permission.

C. Jaringan Komputer

Menurut (Tanaenbaum, 2002) jaringan komputer ialah suatu kumpulan dari perangkat keras dan lunak di dalam sebuah sistem yang mempunyai aturan tertentu untuk mengatur semua anggotanya dalam melakukan suatu aktivitas komunikasi [2].

Setelah mengetahui apa itu jaringan komputer, sebaiknya pahami jenis-jenis jaringan komputer yang ada. Di luar sana ada banyak jenis jaringan komputer. Berikut ini adalah beberapa jenis-jenis jaringan computer sebagai berikut [3]:

- *Local Area Network* adalah jaringan komputer yang menghubungkan perangkat jaringan yang bersifat lokal dalam jarak yang relatif pendek.

- *Metropolitan Area Network* adalah jaringan komputer yang menghubungkan dua atau lebih jaringan LAN di dalam kota yang sama.

- *Wide Area Network* adalah jaringan komputer dari gabungan jaringan LAN dan WAN yang tersebar secara geografis.

- *Interconnection Networking* adalah sekumpulan jaringan komputer dalam skala global yang saling terhubung satu sama lain sebagai sebuah media komunikasi.

D. Exploit

Exploit adalah sebuah program yang berisi seperangkat perintah berupa kode yang dibuat untuk melakukan penyerangan terhadap sebuah sistem yang memanfaatkan kerentanan pada sistem dengan tujuan untuk mengambil keuntungan dari kerentanan sehingga penyerang dapat memasuki sistem dan memberikan intruksi kepada sistem tujuan untuk menjalankan intruksi sesuai keinginan penyerang.

E. Evil Droid Framework

Evil Droid adalah sebuah *framework tool* yang dibuat untuk mengefisiensikan pembuatan dan penanaman sebuah *payload* sebagai media untuk melakukan pengujian serangan exploit terhadap platform system operasi android.

F. Payload

Payload adalah sebuah program yang berisi kode khusus yang dibuat oleh penyerang terhadap sebuah sistem dengan tujuan agar sistem dapat mengeksekusi program yang dipilih dan dikirim oleh *framework*.

G. Ngrok

Ngrok adalah adalah program yang dapat menciptakan sebuah koneksi jaringan private melalui jaringan internet publik ke port komputer lokal yang bekerja dengan cara mengekspos *server web* yang berjalan pada mesin lokal ke internet. Sehingga akan menampilkan link acak dari *ngrok* untuk mengakses lokal *webserver*.

III. METODOLOGI

A. Teknik Pengumpulan Data

Untuk penelitian studi kasus dalam pengumpulan data penulis melakukan pengumpulkan data dengan teknik:

1. Studi Kepustakaan (*Literature*)

Data diperoleh melalui studi kepustakaan (literature) yaitu dengan mencari bahan dari internet, jurnal yang sesuai dengan objek yang akan diteliti.

2. Pengamatan (*Observasi*)

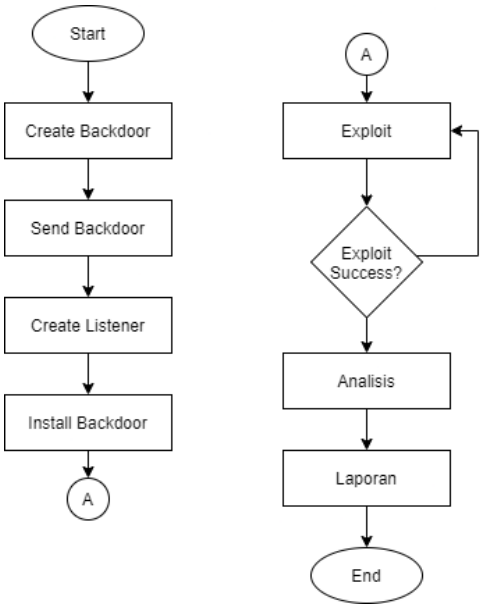
Pada penelitian ini penulis melakukan pengamatan tentang pengujian proses *exploitasi* terhadap beberapa smartphone dengan versi android yang berbeda dalam jaringan interne, dimana parameter yang diamati berupa status dan waktu serangan exploit

3. Pengujian (*Testing*)

Pada penelitian ini penulis akan melakukan pengujian serangan *exploit* terhadap beberapa versi android berdasarkan beberapa perintah *exploitasi* yang terdapat pada *modul exploit*.

B. Flowchart

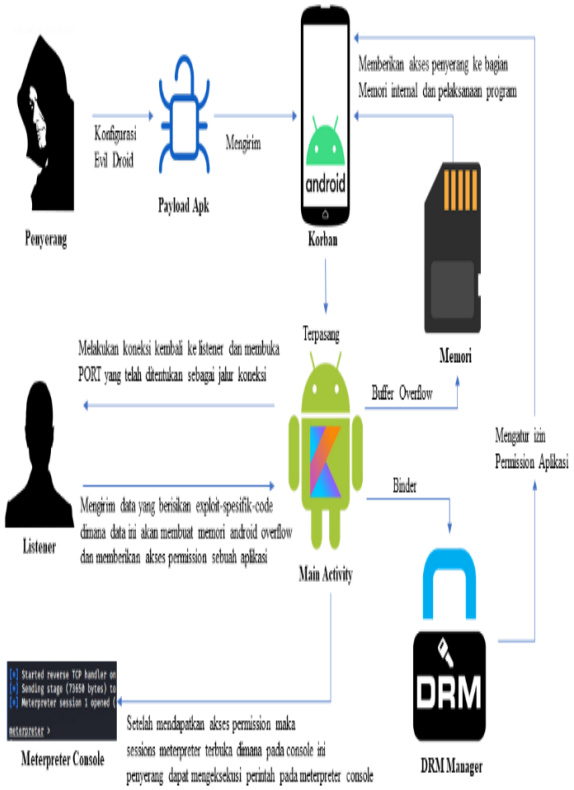
Berikut ini adalah langkah-langkah yang akan digunakan dalam penelitian ini dijelaskan pada gambar 1 berikut.



Gambar 1 Diagram Alir Penelitian

C. Skema Serangan Exploit

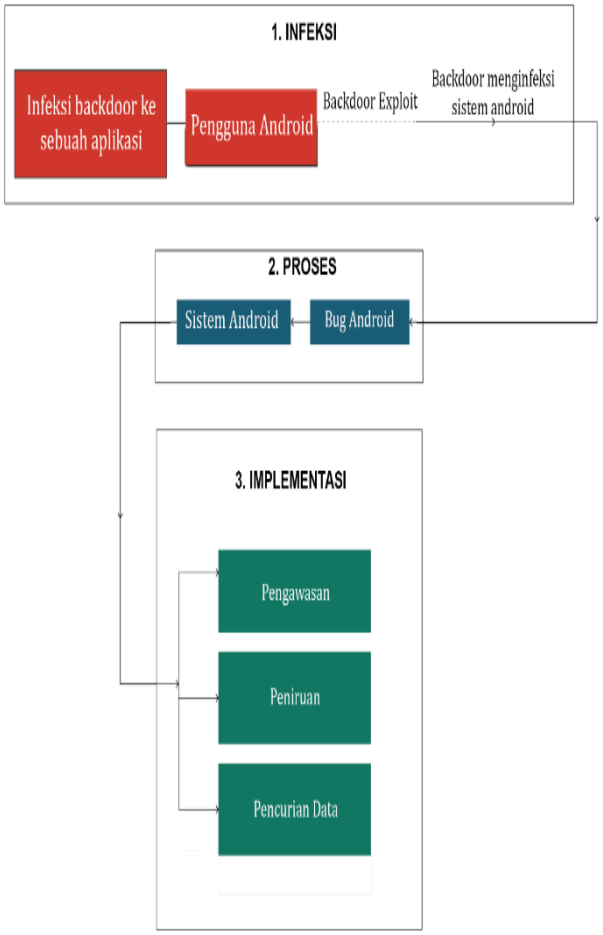
Berikut ini adalah skema serangan exploit terhadap smartphone android menggunakan tool *Evil Droid Framework.*



Gambar 2 Skema Serangan Exploit

D. Skenario Exploit

Pada penelitian ini skenario pengumpulan data terhadap hasil serangan *exploit* pada beberapa perangkat dengan system android yang berbeda dan kemudian menjadi data yang akan di analysis pada tahap berikutnya. Berikut ini adalah skenario hasil serangan *exploit* terhadap beberapa jenis system operasi android sebagaimana ditunjukkan pada gambar 3.



Gambar 3 Skenario Serangan Exploit

E. Metode Analisis

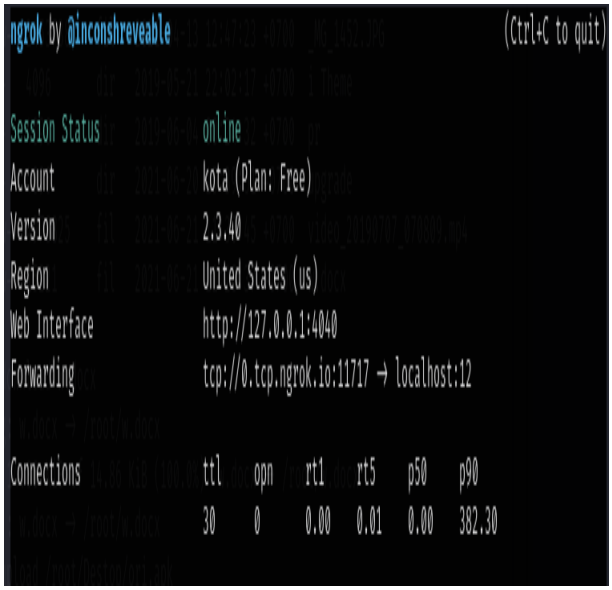
Pada penelitian ini peneliti menggunakan pendekatan metode penelitian *kualitatif*. Penelitian *kualitatif* pada umumnya dirancang untuk memberikan pengalaman senyatanya dan menangkap makna sebagaimana yang tercipta di lapangan penelitian melalui interaksi langsung antara peneliti dan yang diteliti [4].

Penelitian ini adalah penelitian yang bersifat komparatif yaitu perbandingan. Makna dari kata tersebut menunjukan bahwa dalam penelitian ini peneliti bermaksud mengadakan perbandingan kondisi yang berbeda pada parameter yang akan diteliti yakni serangan *exploit* terhadap android versi 8 dan versi 11 pada jaringan internet.

IV. HASIL DAN PEMBAHASAN

A. Hasil Server Ngrok

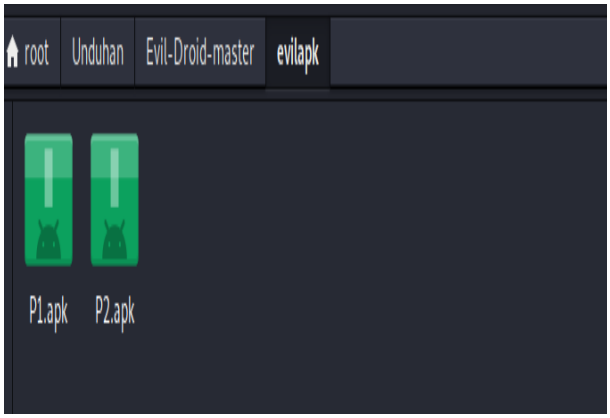
Dari hasil langkah-langkah koneksi ngrok dapat dilihat pada gambar dibawah ini dimana server ngrok dibangun dengan menggunakan *protocol tcp* pada *port* 12.



Gambar 4 Server Ngrok

B. Hasil Backdoor Android

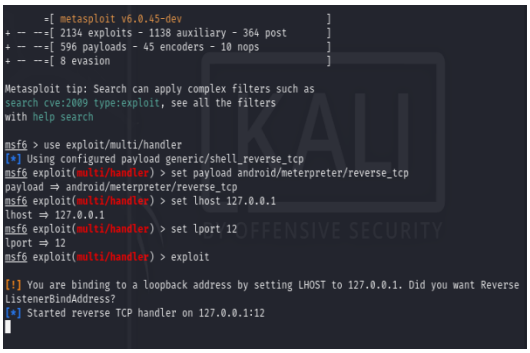
Berdasarkan Langkah-langkah pembuatan *backdoor exploit* dengan menggunakan dua metode serangan *exploit* dapat dilihat pada gambar dibawah ini.



Gambar 5 Backdoor Android

C. Hasil Listener

Berdasarkan langkah-langkah dalam pembuatan listener untuk serangan *exploit* terhadap smartphone android dengan menggunakan 2 metode dapat dilihat pada gambar 6.



Gambar 6 Listener

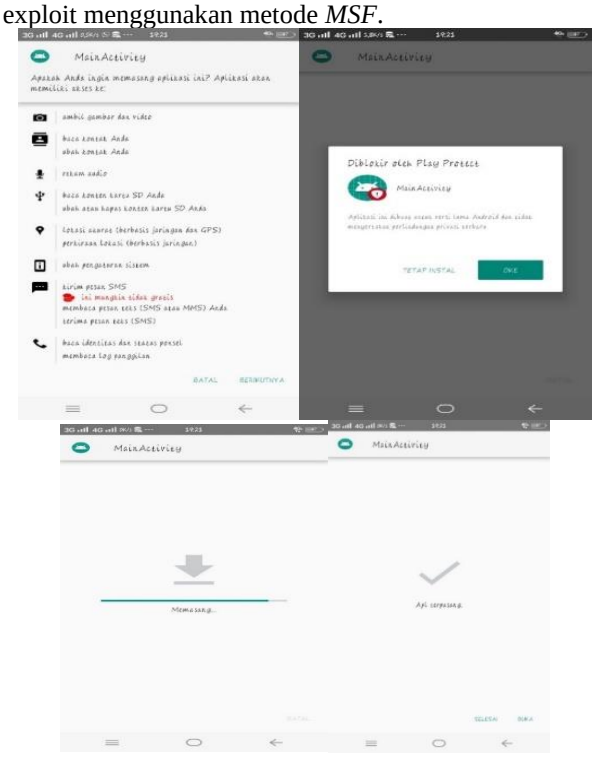
Listener untuk serangan *exploit* pada penelitian ini menggunakan modul "*exploit/multi/handler*" dengan jenis *payload* android metode "*reverse_tcp*". Kemudian digunakan localhost internet yaitu 127.0.0.1 dengan local port 12 sesuai dengan port yang dijalankan pada *server ngrok*. Listener digunakan untuk mendengarkan koneksi yang disampaikan oleh *backdoor* yang terdapat pada android yang diserang sehingga penyerang dapat mengeksekusi perintah-perintah *exploit* terhadap perangkat yang berhasil diserang..

D. Hasil Instalasi Backdoor Exploit

Instalasi aplikasi yang mengandung backdoor exploit pada umumnya sama seperti aplikasi lain. Tahapan-tahapan instalasi aplikasi yang mengandung *backdoor exploit* ditunjukkan seperti berikut.

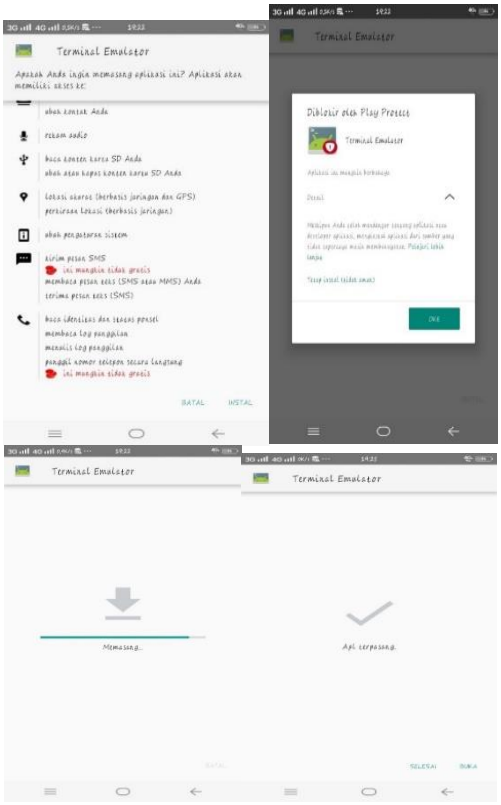
- **Smartphone Android 8**

Gambar dibawah ini merupakan hasil tahapan-tahapan instalasi aplikasi yang mengandung backdoor exploit menggunakan metode *MSF*.



Gambar 7 Instalasi APK Metode MSF

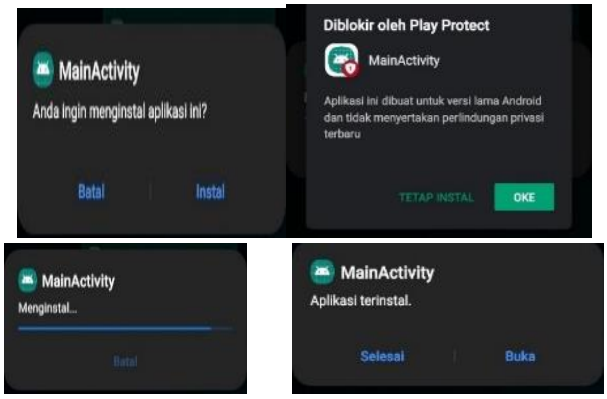
Sedangkan tahapan-tahapan instalasi aplikasi yang mengandung *backdoor exploit* menggunakan metode *Original* ditunjukan seperti gambar 8.



Gambar 8 Instalasi APK Metode Original

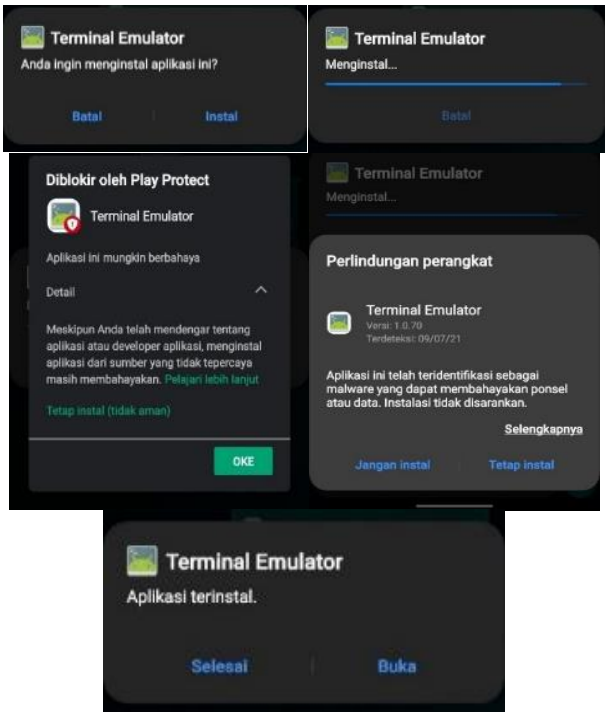
- **Smartphone Android 11**

Gambar dibawah ini merupakan hasil tahapan-tahapan instalasi aplikasi yang mengandung *backdoor exploit* menggunakan metode *MSF*.



Gambar 9 Instalasi APK Metode MSF

Sedangkan tahapan-tahapan instalasi aplikasi yang mengandung *backdoor exploit* menggnakan metode *Original* ditunjukan seperti gambar 10..



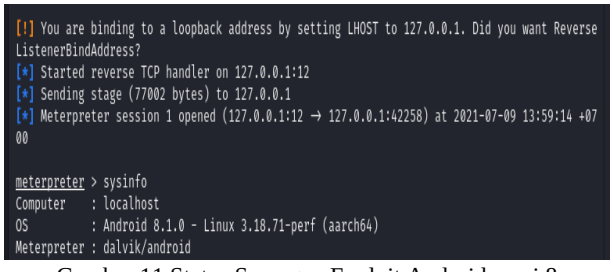
Gambar 10 Instalasi APK Metode Original

E. Hasil Data Pengamatan

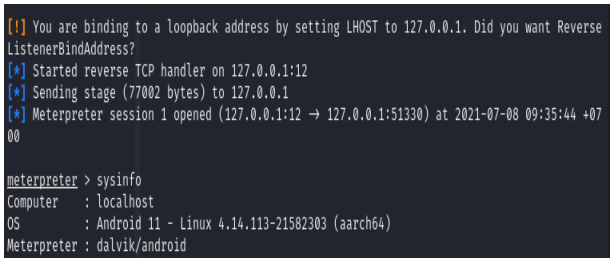
Berdasarkan pembahasan pada sebelumnya data yang diamati berupa status dan waktu serangan *exploit* dilakukan. Berikut ini merupakan hasil data pengamatan serangan *exploit*.

- **Status Serangan Exploit**

Berdasarkan tahapan-tahapan dalam melakukan serangan *exploit* berhasil dilakukan, maka untuk membuktikan serangan tersebut berhasil untuk mengakses smartphone android target ditunjukkan seperti gambar dibawah ini.



Gambar 11 Status Serangan Exploit Android versi 8



Gambar 12 Status Serangan Exploit Android versi 11

- **Waktu Serangan Exploit Smartphone Android 8**

Hasil serangan exploit pada smartphone android versi 8 dengan menggunakan metode *APK MSF* dapat dilihat pada table dibawah ini.

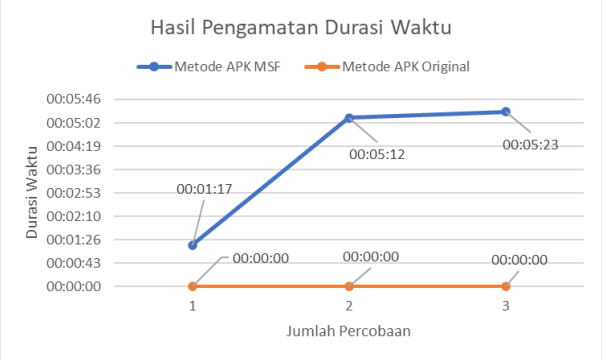
Tabel 1 Serangan Exploit APK MSF

Test	Attacker		Victim		Waktu	
	IP	Port	IP	Port	Terkoneksi	Terputus
1	127.0.0.1	12	127.0.0.1	42258	13:59:14	14:00:31
2	127.0.0.1	12	127.0.0.1	42266	14:00:53	14:06:05
3	127.0.0.1	12	127.0.0.1	42280	14:06:09	14:11:32

Sedangkan hasil serangan exploit pada smartphone android versi 8 dengan menggunakan metode *APK Original* dapat dilihat pada tabel dibawah ini.

Tabel 2 Serangan Exploit APK Original

Test	Attacker		Victim		Waktu	
	IP	Port	IP	Port	Terkoneksi	Terputus
1	127.0.0.1	12	127.0.0.1	35244	22:20:20	∞
2	127.0.0.1	12	127.0.0.1	35260	22:21:25	∞
3	127.0.0.1	12	127.0.0.1	35268	22:21:56	∞



Gambar 13 Durasi Waktu Serangan Exploit Android 8

Smartphone Android 11

Hasil serangan exploit pada smartphone android versi 11 dengan menggunakan metode *APK MSF* dapat dilihat pada table dibawah ini.

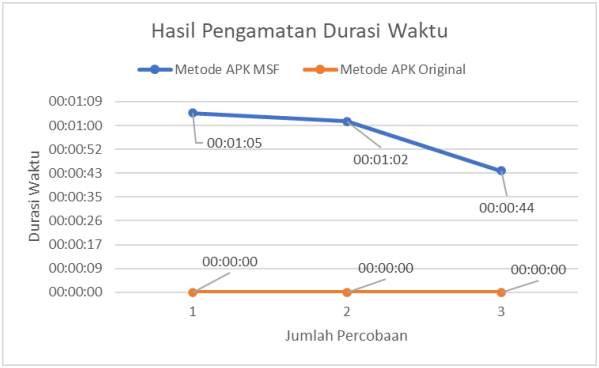
Tabel 3 Serangan Exploit APK MSF

Test	Attacker		Victim		Waktu	
	IP	Port	IP	Port	Terkoneksi	Terputus
1	127.0.0.1	12	127.0.0.1	51330	09:35:44	09:36:49
2	127.0.0.1	12	127.0.0.1	51334	09:37:39	09:38:41
3	127.0.0.1	12	127.0.0.1	51338	09:39:32	09:40:16

Sedangkan hasil serangan exploit pada smartphone android versi 8 dengan menggunakan metode *APK Original* dapat dilihat pada table 4.

Tabel 4 Serangan Exploit APK Original

Test	Attacker		Victim		Waktu	
	IP	Port	IP	Port	Terkoneksi	Terputus
1	127.0.0.1	12	127.0.0.1	51420	10:40:49	∞
2	127.0.0.1	12	127.0.0.1	51474	10:50:15	∞
3	127.0.0.1	12	127.0.0.1	51506	10:59:18	∞



Gambar 14 Durasi Waktu Serangan Exploit Android 11

F. Hasil Data Pengujian

- **Perintah Exploitasi pada Android versi 8**

Berikut ini merupakan data hasil pengujian *exploitasi* pada smartphone android versi 8 dengan menggunakan metode *APK MSF*.

Tabel 5 Pengujian Exploitasi APK MSF

No	Pengujian Exploitasi	Hasil Pengujian
1	Sysinfo	✓
2	Download (Doc)	✓
3	Download (Pdf)	✓
4	Download (Images)	✓
5	Download (Mp4)	✓
6	Upload (apk)	✓
7	Upload (sh)	✓
8	Record mic	✓
9	Webcam snap (1)	✓
10	Webcam snap (2)	✓
11	Webcam stream (1)	✓
12	Webcam stream (2)	✓
13	Dump call log	✓
14	Dump contacts	✓
15	Dump sms	✓
16	Send sms	✓
17	Geolocate	✓

Gambar 15 Pengujian Exploitasi Metode APK MSF

Sedangkan data hasil pengujian *exploitasi* pada smartphone android versi 8 dengan menggunakan metode *APK Original* ditunjukkan seperti tabel dibawah ini.

Tabel 6 Pengujian Exploitasi APK Original

No	Pengujian Exploitasi	Hasil Pengujian
1	Sysinfo	✓
2	Download (Doc)	✓
3	Download (Pdf)	✓
4	Download (Images)	✓
5	Download (Mp4)	✓
6	Upload (apk)	✓
7	Upload (sh)	✓
8	Record mic	✓
9	Webcam snap (1)	✓
10	Webcam snap (2)	✓
11	Webcam stream (1)	✓
12	Webcam stream (2)	✓
13	Dump call log	✓
14	Dump contacts	✓
15	Dump sms	✓
16	Send sms	✓
17	Geolocate	✓

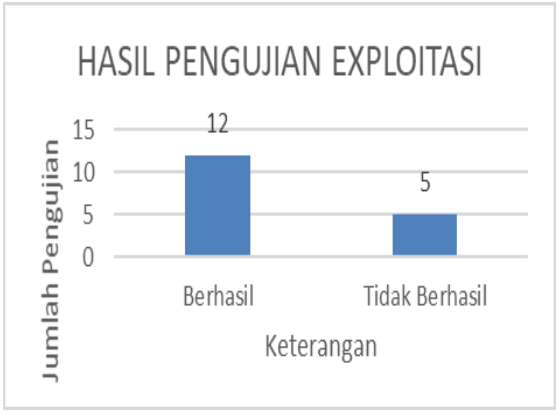
Gambar 16 Pengujian Exploitasi Metode APK Original

- **Perintah Exploitasi pada Android versi 11**

Berikut ini merupakan data hasil pengujian *exploitasi* pada smartphone android versi 11 dengan menggunakan metode *APK MSF*.

Tabel 7 Pengujian Exploitasi APK MSF

No	Pengujian Exploitasi	Hasil Pengujian
1	Sysinfo	✓
2	Download (Doc)	✓
3	Download (Pdf)	✓
4	Download (Images)	✓
5	Download (Mp4)	✓
6	Upload (apk)	✓
7	Upload (sh)	✓
8	Record mic	✓
9	Webcam snap (1)	×
10	Webcam snap (2)	×
11	Webcam stream (1)	×
12	Webcam stream (2)	×
13	Dump call log	✓
14	Dump contacts	×
15	Dump sms	✓
16	Send sms	✓
17	Geolocate	✓

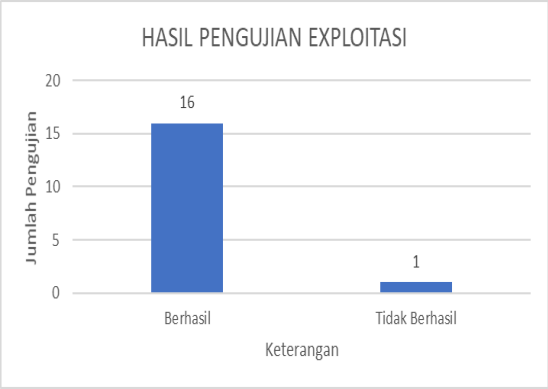


Gambar 17 Pengujian Exploitasi Metode APK MSF

Sedangkan data hasil pengujian exploitasi pada smartphone android versi 11 dengan menggunakan metode *APK Original* ditunjukkan seperti table 8

Tabel 8 Pengujian Exploitasi APK Original

No	Pengujian Exploitasi	Hasil Pengujian
1	Sysinfo	✓
2	Download (Doc)	✓
3	Download (Pdf)	✓
4	Download (Images)	✓
5	Download (Mp4)	✓
6	Upload (apk)	✓
7	Upload (sh)	✓
8	Record mic	✓
9	Webcam snap (1)	✓
10	Webcam snap (2)	✓
11	Webcam stream (1)	✓
12	Webcam stream (2)	✓
13	Dump call log	✓
14	Dump contacts	✗
15	Dump sms	✓
16	Send sms	✓
17	Geolocate	✓



Gambar 18 Pengujian Exploitasi Metode APK Original

- **Waktu Serangan Exploit**

Smartphone Android 8

Berdasarkan table 4.1 Serangan Exploit *APK MSF*, percobaan serangan *exploit* dilakukan sebanyak 3 kali dimana pada percobaan pertama didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh *backdoor* pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 42258. Serangan *exploit* pada percobaan pertama berhasil dilakukan di mulai pada pukul 13:59:14 sampai 14:00:31 yang berarti pada percobaan pertama serangan exploit berlangsung selama 1 menit 17 detik.

Pada percobaan kedua didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh backdoor pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 42266. Serangan *exploit* pada percobaan pertama berhasil dilakukan di mulai pada pukul 14:00:31 sampai 14:06:05 yang berarti pada percobaan pertama serangan *exploit* berlangsung selama 5 menit 12 detik.

Pada percobaan ketiga didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh backdoor pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 42280. Serangan *exploit* pada percobaan pertama berhasil dilakukan di mulai pada pukul 14:06:09 sampai 14:11:32 yang berarti pada percobaan pertama serangan exploit berlangsung selama 5 menit 23 detik.

Kemudian berdasarkan tabel 4.2 Serangan Exploit *APK Original*, percobaan serangan exploit dilakukan sebanyak 3 kali dimana pada percobaan pertama didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh *backdoor* pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 35244. Serangan *exploit* pada percobaan pertama berhasil dilakukan di mulai pada pukul 22:20:20 dengan durasi waktu selama aplikasi tersebut tidak ditutup yang berarti ketika aplikasi yang berisi *backdoor* tersebut ditutup maka sesi serangan exploit juga akan berakhir.

Pada percobaan kedua didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh backdoor pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 35260. Serangan *exploit* pada percobaan kedua berhasil dilakukan di mulai pada pukul 22:21:25 dengan durasi waktu selama aplikasi tersebut tidak ditutup yang berarti ketika aplikasi yang berisi backdoor tersebut ditutup maka sesi serangan exploit juga akan berakhir.

Pada percobaan ketiga didapatkan bahwa IP yang digunakan oleh penyerang adalah 127.0.0.1 pada Port 12 sedangan IP yang digunakan oleh backdoor pada android untuk terhubung ke penyerang yakni menggunakan IP yang sama dengan Port 35268. Serangan *exploit* pada percobaan kedua berhasil dilakukan di mulai pada pukul 22:21:56 dengan durasi waktu selama aplikasi tersebut tidak ditutup yang berarti ketika aplikasi yang berisi backdoor tersebut ditutup maka sesi serangan *exploit* juga akan berakhir.

V. KESIMPULAN

Berdasarkan hasil penelitian dalam uji serangan exploit pada beberapa versi android menggunakan metode APK MSF dan APK Original maka dapat disimpulkan bahwa:

1. Sesi serangan exploit pada android versi 8 dengan metode APK MSF memiliki durasi waktu akses paling lama 5 menit 23 detik sedangkan durasi waktu akses paling singkat selama 1 menit 17 detik.

2. Sesi serangan exploit pada android versi 11 dengan metode APK MSF memiliki durasi waktu akses paling lama 1 menit 5 detik sedangkan durasi waktu akses paling singkat selama 44 detik.

3. Sedangkan sesi serangan exploit dengan metode APK Original pada dua versi android tergantung pada durasi waktu pemakaian dari aplikasi tersebut.

4. Pengujian exploitasi serangan exploit pada android versi 8 dengan metode APK MSF dan Metode APK Original memiliki keberhasilan dalam melakukan eksploitasi di semua aspek implementasi.

5. Pengujian exploitasi serangan exploit pada android versi 11 dengan metode APK MSF memiliki keberhasilan dalam melakukan eksploitasi kecuali pada implementasi webcam snap, webcam_stream, dan dump contacts.

6. Sedangkan pengujian exploitasi dengan metode APK Original memiliki keberhasilan dalam melakukan exploitasi kecuali pada implementasi dump contacts.

REFERENSI

[1] D. Reportal, "**DIGITAL 2020: INDONESIA,**" 18 Februari 2020. [Online]. Available: https://datareportal.com/reports/digital-2020-indonesia.

[2] Tanaenbaum, "**Pengertian Jaringan Komputer,**" 30 April 2021. [Online]. Available: https://www.gurupendidikan.co.id/pengertian-jaringan-komputer/. [Accessed 15 Maret 2021].

[3] D. Web, "**Jaringan Komputer: Pengertian, Topologi, dan Jenisnya,**" 10 Oktober 2020. [Online]. Available: https://www.dewaweb.com/blog/jaringan-komputer-pengertian-jenis/.

[4] P. L. Pendit, "**Penelitian Kualitatif,**" 2003. [Online]. Available: http://eprints.undip.ac.id/40650/3/BAB_III.pdf. [Accessed 15 Maret 2021].