ANALISIS DAN SIMULASI PENGUJIAN SERANGAN KEAMANAN *ANDROID* MENGGUNAKAN *PENETRATION TESTING* DENGAN *PHONESPLOIT*

ANALYSIS AND SIMULATION OF SECURITY ATTACK TESTING ON ANDROID USING PENETRATION TESTING WITH PHONESPLOIT

Nurhamzah Juniansyah[1], Dayan Singasatia[2] & Yusuf Muhyidin[3]
[1,2,3]Sekolah Tinggi Teknologi Wastukancana
njuniansyah23@gmail.com[1], daysinga@yahoo.com[2], yusufkaito15@gmail.com[3]
Corresponding author: njuniansyah23@gmail.com

Abstrak. Di era kemajuan teknologi yang semakin pesat, kebutuhan akan layanan internet terus meningkat setiap harinya, baik untuk keperluan pribadi maupun pekerjaan yang mendesak. Hal ini mendorong pemilik fasilitas umum untuk menyediakan layanan internet berupa *Wi-Fi* yang dapat di akses oleh publik. Seiring berjalannya waktu dan perkembangan teknologi, hal ini memicu permasalahan baru yaitu serangan *hacker* yang dapat menyusup pada jaringan internet di fasilitas tersebut. Melihat permasalahan tersebut, penulis mencoba melakukan analisis dan pengujian tentang bagaimana melakukan simulasi penetrasi terhadap perangkat *smartphone android* dengan menggunakan *tools Phonesploit*. Tujuan dari penelitian ini yaitu untuk melakukan simulasi serangan berdasarkan kasus nyata yang dipraktikkan oleh *hacker* dalam mengeksploitasi perangkat *Smartphone Android*. guna mengetahui dampak yang terjadi pada perangkat *Android* pasca serangan serta menuangkan hasilnya dalam bentuk data hasil pengujian. Penelitian ini menggunakan perangkat *virtual* yang digunakan sebagai media uji coba yaitu berupa *Emulator Android*, untuk menciptakan lingkungan yang terisolasi dan mencegah potensi kerusakan perangkat fisik yang disebabkan oleh aktivitas serangan yang dilakukan. Di akhir penelitian, hasil dari penelitian ini berupa data analisis perilaku perangkat *emulator android* setelah dilakukan uji coba simulasi serangan. Data hasil analisis tersebut mencakup identifikasi perilaku perangkat *emulator android* dan dokumentasi kerentanan perangkat yang ditemukan selama periode serangan.

Kata kunci : *Smartphone Android*, *Penetration Testing*, *Phonesploit*.

Abstract, In the era of rapidly advancing technology, the demand for internet services continues to increase daily, both for personal needs and urgent work requirements. This drives the owners of public facilities to provide internet services in the form of Wi-Fi accessible to the public. Over time, and with technological developments, this has led to a new problem: hacker attacks that can infiltrate the internet networks in these facilities. In response to this issue, the author conducted an analysis and testing to simulate penetration attacks on Android smartphones using the PhoneSploit tool. The aim of this research is to simulate attacks based on real cases practiced by hackers to exploit Android smartphones, to observe the impact on the devices after the attacks, and to document the results in the form of test data. This study utilizes a virtual device, specifically an Android emulator, as the testing medium to create an isolated environment and prevent potential damage to physical devices caused by the attacks. At the conclusion of the research, the results include an analysis of the emulator's behavior after the attack simulation. The data from the analysis covers the identification of the emulator's behavior and documentation of the device's vulnerabilities discovered during the attack period.

Keywords: Android Smartphone, Penetration Testing, Phonesploit

1 Pendahuluan

Penggunaan layanan internet telah menjadi semakin umum dalam kehidupan sehari-hari. Seiring dengan berjalannya waktu, saat ini perkembangan teknologi semakin pesat, dan salah satunya adalah *smartphone*. Telepon genggam yang telah dilengkapi dengan sistem operasi yang dapat melakukan beberapa fungsi layaknya personal komputer, salah satu kegunaannya adalah akses internet. Orang-orang dapat mengakses internet kapanpun dan dimanapun dengan adanya

internet (Anggraini et al., 2020) Pada sisi lain, penggunaan internet yang nyaris tanpa kendali menyebabkan berbagai tindak kejahatan di dunia maya, angka kejahatan *online* alias *cybercrime* telah menjadi tren baru di banyak Negara saat ini, termasuk di Indonesia.(Fitriani & Pakpahan, n.d.). Indonesia menempati peringat ketiga dalam hal serangan *cybercrime* dimana 41,14 % pengguna *mobile* terkena serangan *cybercrime*. Peringkat pertama diduduki Iran, dimana separuh lebih pengguna seluler di negara tersebut (57,25%) terkena serangan *cybercrime*. Di bawahnya muncul negara Bangladesh dimana (42, 76%) pengguna seluler terkena serangan(Setiawan, 2019) Dilansir dari situs *web* : https://cyberthreat.id/ "Menurut *VashTheStampede*, juga seorang peneliti keamanan siber independen, dirinya membagikan informasi di *Twitter* agar pengguna *Android* bisa lebih berhati-hati. Jangan asal menghubungkan ponsel ke jaringan *wi-fi* publik gratis. Mengapa? Menurut dia, tidak semua *router* yang dipasang di publik di-*setting* secara aman. "Jika *router wi-fi* dinyalakan, kemudian *WPS* (*Wi-Fi Protected Setup*) diatur asal-asalan, kadang malah tidak dikasih *password*, itu sangat rentan disusupi penyerang,"(Nugroho, 2019).

2 Kajian Pustaka

2.1 Penelitian sebelumnya

Jurnal penelitian dengan judul "Implementasi *Hacking Wireless* Dengan *Kali Linux* Menggunakan *Kali Nethunter*" menjelaskan tentang bagaimana melakukan penetrasi perangkat *Smartphone Android* pada jaringan *Wireless* menggunakan *Kali Linux* dengan menggunakan *Toolkit Kali Nethunter*. Tujuan penelitian ini didasarkan pada identifikasi masalah yang dibahas, yaitu membuat sebuah *system Hacking Wireless* untuk mendapatkan sebuah *password* pada jaringan *wireless* tersebut dengan tujuan untuk melakukan pengujian kerentanan sistem keamanan pada *Smartphone Android* (Rahmadani, 2017)

2.2 Internet

Internet adalah kumpulan atau jaringan dari komputer yang ada di seluruh dunia. Internet (kependekan dari *interconnection networking*) secara harfiah ialah sistem *global* dari seluruh jaringan komputer yang saling terhubung menggun(Gani, 2020)akan standar *Internet Protocol Suite* (*TCP/IP*) untuk melayani miliaran pengguna di seluruh dunia (Saroji, 2021) Adanya teknologi informasi seperti internet telah membuka mata dunia akan sebuah dunia, interaksi dan *market place* baru serta sebuah jaringan bisnis dunia yang tanpa batas. Dunia dalam internet disebut juga dengan dunia maya (*cyberspace*) (Gani, 2020)

2.2.1 Arsitektur TCP/IP

Standar dalam komunikasi diperlukan untuk dapat dimengerti oleh dua atau lebih perangkat atau *end device* agar perangkat dapat berkomunikasi satu dengan yang lain, seperti halnya manusia menggunakan bahasa agar dapat berkomunikasi dengan baik dengan manusia lainnya. istilah tersebut dikatakan sebagai *protokol* dalam sebuah jaringan. pada jaringan terdapat kumpulan perangkat *protokol* yang terdiri dari dua protokol utama yakni *TCP/IP*.

a. *Transmission Control Protocol* (TCP)
Transmission Control Protocol atau *TCP* adalah sebagian dari *TCP/IP* yang digunakan beriringan dengan *Internet Protokol* (*IP*) dalam melakukan transfer data dalam bentuk pesan dari perangkat komputer ke internet juga sebaliknya Transfer data tersebut dapat dilakukan karena protokol ini akan meminta konfirmasi ketika selesai mengirimkan data agar memberi kepastian bahwa data yang ditransfer telah sampai pada tujuan. setelah itu *TCP* melakukan *retransmission* atau mengirimkan data urutan selanjutnya (Ardhiansyah, 2020)

b. *Internet Protocol* (*IP*)
Internet Protocol (*IP*) adalah bagian dari *TCP/IP* yang mengatur cara agar data dapat dikenal dan dapat dikirim dari satu komputer ke komputer lainnya sampai akhirnya dapat tercapai tujuan pada suatu jaringan komputer. *IP* memiliki karakteristik *connectionless protocol*, yang berarti *IP* tidak melakukan pendeteksian *recovery* dan kesalahan, atau menukar pengendalian informasi untuk membuat koneksi sebelum pengiriman data. koneksi yang baru terjadi jika dilakukan proses tadi. karena itu dalam persoalan ini,
IP memiliki ketergantungan pada lapisan lain dalam proses yang akan dilakukannya. *IP* memiliki beberapa fungsi berdasarkan *TCP/IP*, yakni:

1. Mendeskripsikan paket data sebagai dasar pada transmisi jaringan.
2. Menenetapkan skema dari pengalamatan internet.
3. Transfer data antara *transport layer* dan *layer network access* (Ardhiansyah, 2020)

2.3 Arsitektur Jaringan Internet

Jaringan komputer merupakan kumpulan beberapa komputer (dan perangkat lain seperti *printer*, *hub*, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel atau pun media tanpa kabel. Informasi berupa data yang mengalir dari suatu komputer ke komputer lain sebagai masing-masing komputer yang terhubung bisa saling bertukar data (Butsianto & Purnamasari, 2021)

1. *WAN* (*Wide Area Network*)

WAN Merupakan jaringan yang lebih luas dibandingkan dengan *MAN* dan *LAN*. Biasanya *WAN* digunakan untuk menghubungkan jaringan komputer antar negara hingga benua. Agar jaringan dapat terhubung, maka diperlukan kabel fiber optik. Kabel tersebut biasanya ditanam di tanah ataupun dibawah laut.

2. *MAN* (*Metropolitan Area Network*)

MAN menjadi jaringan yang memiliki jangkauan lebih sempit jika dibandingkan dengan *WAN* namun lebih luas jika dibandingkan dengan *LAN*. Teknologi yang digunakan pada *MAN* sudah lebih bagus jika dibandingkan dengan *LAN*. Cakupan yang lebih luas mendukung untuk menghubungkan jaringan komputer antar kota. Agar jaringan *MAN* dapat diterapkan, maka diperlukan operator telekomunikasi. Operator akan berperan menjadi penghubung antara jaringan komputer satu dengan jaringan komputer lainnya.

3. *LAN* (*Local Area Network*)

LAN merupakan jenis dari arsitektur jaringan dimana jaringannya mencakup area lokal saja. Biasanya jaringan tersebut dimanfaatkan oleh orang yang berada di area *LAN*. Penggunaan *LAN* biasanya untuk menghubungkan perangkat ke internet yang memanfaatkan perangkat jaringan sederhana. Terdapat beberapa contoh dari perangkat sederhana yang digunakan diantaranya *Router*, *Hub*, *UTP* dan *Switch*.

2.3.1 Topologi

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. (Supriyadi et al., 2007) Jenis – jenis topologi yang digunakan pada umumnya yaitu :

1. Topologi *Star* (Topologi Bintang)

Topologi bintang adalah salah satu yang paling umum digunakan dalam jaringan komputer. Dalam topologi ini, setiap perangkat (seperti komputer, *printer*, atau perangkat jaringan lainnya) terhubung ke satu titik pusat, yang dapat berupa *switch* atau *hub*.

2. Topologi *Ring* (Topologi Lingkaran)

Topologi lingkaran adalah struktur jaringan di mana setiap perangkat terhubung langsung ke dua perangkat lainnya, membentuk struktur seperti lingkaran tertutup.

3. Topologi *Mesh* (Topologi Jaringan)

Dalam topologi *mesh*, setiap perangkat terhubung langsung ke setiap perangkat lainnya dalam jaringan. Ini menciptakan banyak jalur komunikasi yang berbeda antar perangkat, yang menghasilkan tingkat redundansi yang tinggi. Dengan banyaknya rute yang tersedia, jika satu rute mengalami kegagalan, data dapat diarahkan melalui jalur lainnya.

2.4 Cybercrime

Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan mengancam keamanan data pengguna *smartphone* yang disebut dengan "*Cyber Crime*" atau kejahatan melalui jaringan Internet. Keamanan merupakan keadaan bebas dari bahaya. Keamanan diusahakan mempunyai unsur-unsur misal adanya proteksi, integritas, keaslian suatu data, dan mempunyai hak akses (Muhyidin et al., 2022) Munculnya beberapa kasus "*Cybercrime*" di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya *email*, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam *program computer* (Ketaren, 2016)

2.4.1 Teknik serangan *Man-in-The-Middle*

Teknik serangan *Man in the Middle* (*MitM*) merupakan jenis serangan siber di mana penyerang secara diam-diam menyisipkan diri di antara dua pihak yang berkomunikasi. Penyerang dapat memantau, mencegat, dan bahkan mengubah komunikasi antara kedua pihak tanpa sepengetahuan mereka. *MitM* adalah salah satu bentuk serangan yang sangat berbahaya karena dapat digunakan untuk mencuri informasi sensitif, seperti kata sandi, data kartu kredit, dan informasi pribadi lainnya (Mallik, 2018)

Gambar 1 Teknik Serangan *Man in the Middle*

2.5 Phonesploit

Phonesploit merupakan sebuah *toolkit* yang berfungsi untuk mengendalikan perangkat *Android* dari jarak jauh menggunakan *Android Debug Bridge* (*ADB*) melalui jaringan. Secara garis besar *Phonesploit* adalah alat yang memanfaatkan perintah *ADB* untuk melakukan berbagai tindakan pada perangkat *Android* yang terhubung, seperti mengambil *screenshot*, menginstal aplikasi, menarik dokumen dari perangkat yang terhubung, dan bahkan membuka *shell command*.

2.6 Lingkungan Pengujian

Pada penelitian ini, penulis melakukan serangan pada *smartphone android* dengan melakukan simulasi pada lingkungan virtual yang di atur sesuai dengan kondisi yang ada pada dunia nyata. Pengujian tersebut dilakukan dengan menggunakan media uji coba berupa *emulator android* yang berperan sebagai target serangan dan komputer virtual dengan sistem operasi *linux* yaitu *Parrot OS* yang didalamnya telah terinstal *toolkit* untuk melakukan pengujian serangan.

2.6.1 *Parrot OS*

Parrot OS adalah distribusi *Linux* yang berfokus pada keamanan yang sebanding dengan *Kali OS*. Ini didasarkan pada *Debian Linux* seperti banyak distribusi *Linux* lainnya, bersifat *open-source* dan gratis untuk digunakan. *Parrot* dirancang untuk menawarkan privasi, pengembangan, dan keamanan serta dilengkapi dengan berbagai alat dan perpustakaan keamanan digital dan forensik.

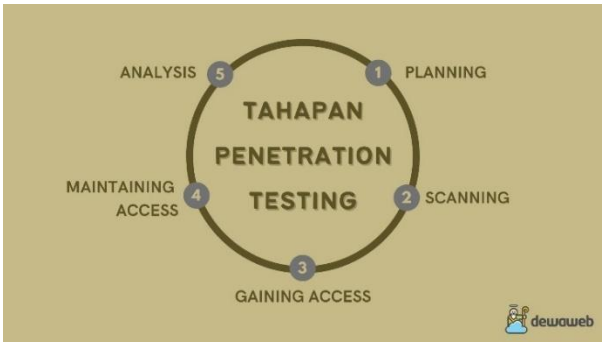
2.6.2 *Emmulator Android*

Secara singkat *emmulator* dapat diartikan sebagai suatu perangkat lunak (*software*) yang memungkinkan suatu sistem komputer (*Host*) meniru fungsi sistem dari perangkat atau komputer lain (*Guest*) (Setiawan, 2022) Sebagai bahan pengujian, penulis menyiapkan media *Emulator Android* dari *Genymotion* untuk mensimulasikan perangkat *Android* yang akan dijadikan target serangan. *Emulator* ini digunakan untuk menciptakan lingkungan pengujian yang aman dan

terkendali, di mana penulis dapat menjalankan berbagai skenario serangan tanpa risiko merusak perangkat fisik.

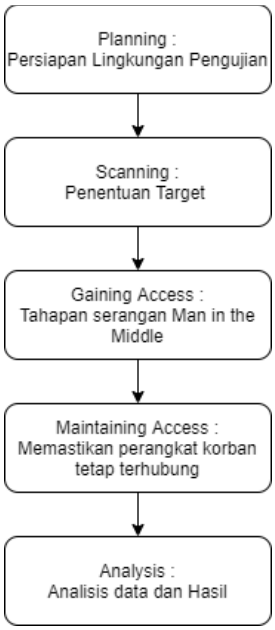
3 Metode *Penetration Testing*

Penetration testing juga dikenal sebagai *ethical hacking*, adalah operasi pada sistem komputer, jaringan, atau aplikasi web untuk menemukan celah yang dapat dieksploitasi oleh penyerang. *Penetration testing* dapat dilakukan dengan menggunakan *file*/aplikasi atau oleh individu. Sebelum melakukan pengujian, peneliti mengidentifikasi titik masuk potensial, mencoba masuk baik secara virtual maupun nyata, dan melaporkan hasilnya. Ini adalah prosedur untuk menilai keamanan suatu organisasi dengan mengeksploitasi kerentanan sedemikian rupa sehingga penyerang dapat mengeksploitasi mereka, sehingga mencegah dan mendokumentasikan proses serangan.(Arote & Mandawkar, 2021)



Gambar 2 Tahapan Metode *Penetration Testing*

Pada kasus penetrasi perangkat di dunia nyata tepatnya di dalam lingkungan jaringan *Wi-Fi* Publik, pelaku *hacker* menggunakan *toolkit* atau program khusus yang dirancang untuk melakukan serangan terhadap calon korban, salah satunya yaitu *Phonesploit.* Penulis turut menggunakan *toolkit* tersebut untuk melakukan simulasi penetrasi perangkat untuk masuk ke dalam sistem operasi *Emulator Smartphone Android.*
Tahapan – tahapan yang dilakukan untuk melakukan simulasi penetrasi perangkat dengan menggunakan metode *Penetration Testing* yaitu sebagai berikut :



Gambar 3 Diagram Alir Kerangka Penelitian

1. Persiapan Lingkungan Pengujian (*Planning)*

a. Instalasi dan konfigurasi *Emulator Android*

Tahap ini melibatkan sejumlah langkah penting untuk memastikan bahwa lingkungan pengujian siap dan sesuai untuk melakukan penelitian. Dalam penelitian ini, peneliti menggunakan lingkungan virtual berupa *Emulator Smartphone Android* dari *Genymotion.* serta melakukan konfigurasi yang sesuai agar dapat terhubung dengan sistem operasi linux. Dalam studi kasus ini peneliti menggunakan *Parrot OS* sebagai sistem operasi di dalam *virtual box.* Kebutuhan spesifikasi perangkat yang digunakan yaitu sebagai berikut :

Tabel 1 *Device Requirement Perangkat Emulator*

Prossecors	4 Core
Memory size	2048 mb
VM Heap size	256 mb

b. Persiapan *tools* penetrasi (instalasi *Phonesploit*)

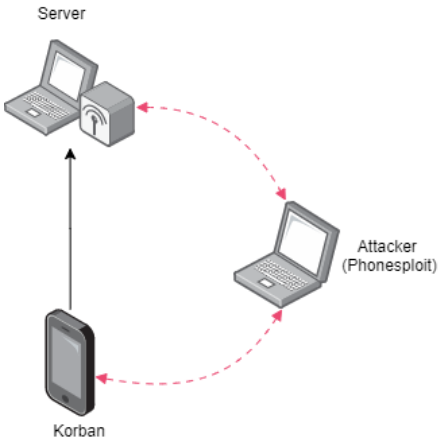
Sebagai alat uji coba serangan penetrasi, penulis melakukan instalasi *toolkit* yaitu *Phonesploit* yang di inistal ke dalam sistem operasi *Parrot OS* dan melakukan konfigurasi sesuai dengan kebutuhan dari dokumentasi *Phonesploit.* Persiapan lingkungan pengujian termasuk instalasi aplikasi dan *toolkit* untuk kebutuhan penelitian penulis lampirkan pada bagian halaman Lampiran pada akhir laporan.

2. Penentuan Target dan Pengumpulan Informasi (*Scanning)*

Setelah melakukan Langkah – Langkah instalasi serta konfigurasi *toolkit* dan konfigurasi perangkat *Emulator.* Pada tahapan pemindaian, penulis melakukan perintah *ADB Devices* dan *ADB Connect* pada *terminal* komputer utama yang berperan sebagai *Attacker*. Tujuan nya yaitu untuk melakukan pemindaian terhadap perangkat yang terhubung pada komputer utama dan menginisiasi perangkat yang akan diserang.

3. Tahap Serangan *Man in the Middle* (*Gaining Access*)

Peneliti mengatur jaringan virtual dalam *Emulator* menggunakan Parrot OS, untuk memastikan bahwa perangkat *Emulator Android* terhubung ke jaringan yang sama dengan sistem operasi yang digunakan oleh peneliti. sesuai skenario dalam kasus nyata, peneliti menempatkan diri di antara perangkat *Emulator Android* dan Sistem operasi *Parrot OS* yang terhubung pada jaringan virtual yang sama.



Gambar 4 Skenario Serangan MITM

4. Memastikan perangkat korban tetap terhubung *(Maintaining Access)*

Pada penggunaan sistem operasi *Parrot OS,* Terdapat satu perintah pada *terminal* yang dapat di eksekusi yaitu *ADB Devices* yang difungsikan untuk mengidentifikasi perangkat yang terhubung pada jaringan. Perintah ini menampilkan keterangan berupa daftar *IP Address* yang berperan sebagai indikator untuk mengetahui perangkat mana saja yang telah terhubung pada jaringan yang sama dengan yang digunakan oleh *Attacker*. Hal ini memudahkan *Attacker* untuk mengetahui koneksi terhadap perangkat korban yang akan, atau sedang diserang.

5. Analisis Data dan Hasil (*Analysis*)

a. Analisis *real-time* dari data yang dikumpulkan

Semua data yang dikumpulkan selama serangan *Man-in-the-Middle* (*MITM*) dan pengujian *Phonesploit* disusun dan diorganisasi untuk analisis lebih lanjut. Ini mencakup paket data yang disadap, *log* aktivitas, tangkapan layar, dan hasil dari perintah yang dijalankan selama periode serangan.

b. Analisis *source code* dari perintah serangan yang dilakukan.

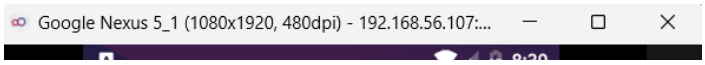
Peneliti memeriksa *source code* dari serangan yang dilakukan oleh *Phonesploit* secara detail untuk memahami fungsi-fungsi yang diimplementasikan dalam satu serangan. Tahap ini termasuk analisis terhadap skrip dan modul yang digunakan untuk eksploitasi perangkat *Android.*

4 Hasil dan Pembahasan

Bab ini bertujuan untuk memberikan gambaran menyeluruh mengenai hasil implementasi yang diperoleh dari hasil analisis pengujian penetrasi keamanan *Smartphone Android* dengan menerapkan metode *Penetration Testing* dari mulai tahapan *Scanning, Gaining Access, Maintaining Access,* dan *Analysis*. tujuan utamanya adalah yaitu untuk mempraktikan serangan pada perangkat *Emulator* dan memaparkan *source code* yang bekerja dibalik setiap serangan.

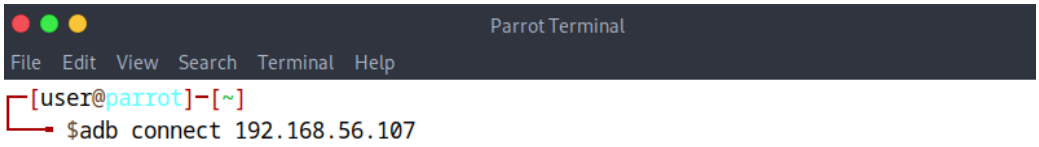
1. Penentuan Target (*Scanning*)

Pada tahapan ini, dilakukan penentuan target serangan dengan melakukan pemindaian perangkat yang terhubung pada jaringan yang sama. Langkah pertama yaitu Menghubungkan *IP Address Emulator Android* ke sistem operasi *linux* menggunakan *terminal*. *IP Address* perangkat *Genymotion* dapat dilihat pada *bar* bagian atas pada tampilan *emulator*.



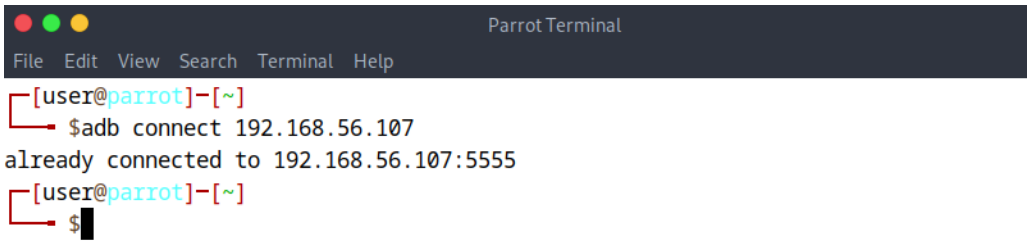
Gambar 5 *IP Address* Perangkat *Emulator*

Dengan menggunakan perintah *adb connect* [*IP_ADDRESS*] pada *terminal*, penulis menghubungkan *Phonesploit* ke *emulator* yang berjalan di *Genymotion*. Ini memungkinkan *Phonesploit* untuk berkomunikasi dengan perangkat target melalui jaringan.



Gambar 5 Menghubungkan Perangkat *Genymotion* Menggunakan *ADB*

Langkah selanjutnya yaitu Melakukan verifikasi Koneksi menggunakan perintah *adb devices* untuk memverifikasi bahwa *emulator Android* telah terhubung dan siap untuk diuji.



Gambar 6 Verifikasi *emulator Android*

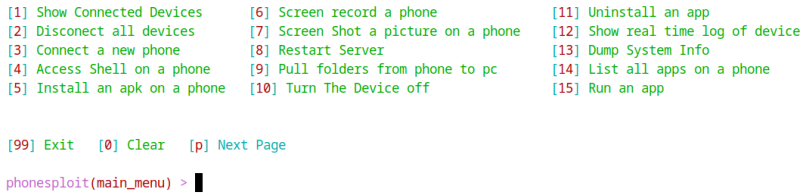
2. Tahapan Serangan *Man in the Middle* (Gaining Access)

Pada menu terminal *Parrot OS*, lakukan perintah berikut :

```
cd PhoneSploit
pip3 install colorama
python3 phonesploit.py
```

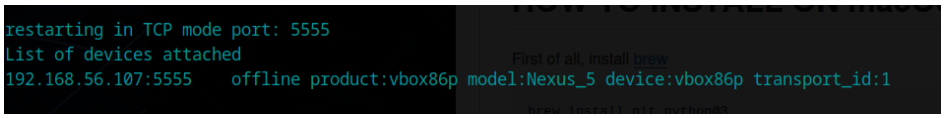
Gambar 7 perintah instalasi phonesploit pada *terminal linux*

Maka akan muncul tampilan utama dari *Phonesploit* sebagai berikut :



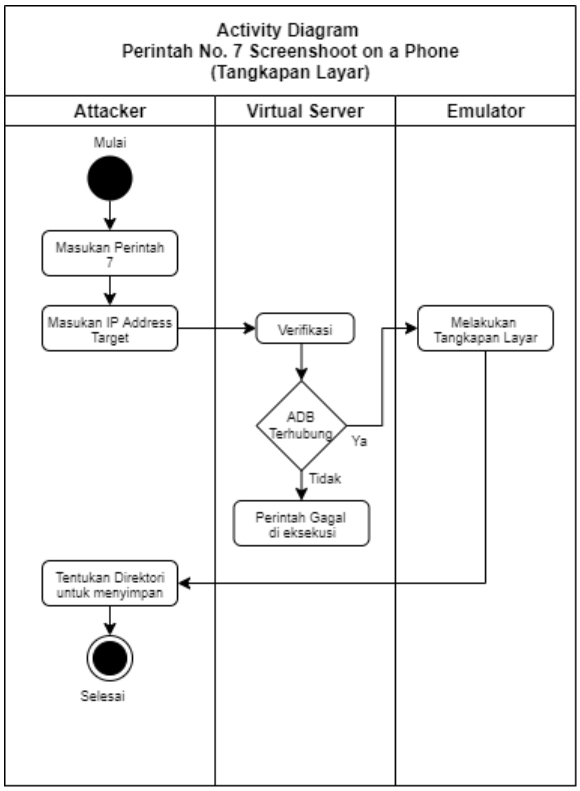
Gambar 8 Halaman Menu Utama *Phonesploit*

Untuk mendapatkan akses pada perangkat yang korban, lakukan perintah hubungkan perangkat dengan mengetik menu 3 (*Connect a new devices*), jika perangkat korban berhasil terhubung maka akan muncul keterangan sebagai berikut.



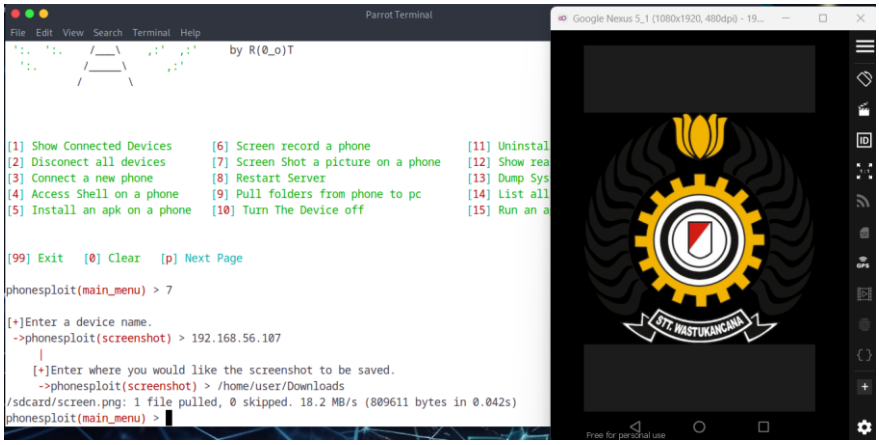
Gambar 9 Perangkat *Emulator* sudah terhubung dengan *Phonesploit*

Setelah peragkat korban berhasil terkoneksi dengan *Phonesploit*, maka pada tahapan ini penulis dapat melakukan simulasi pengujian serangan berdasarkan perintah – perintah krusial yang biasa dilakukan oleh *hacker* dalam mengeksploitasi perangkat korban. Dengan melakukan salah satu perintah pada menu *phonesploit* yaitu tangkapan layar yang diinisiasikan sebagai perintah nomor 7. *Screen shot a picture on a Phone.* Pada perintah ini, *Attacker* melakukan serangan terhadap perangkat *Emulator* dengan melakukan perintah tersebut. Berikut Langkah-langkah yang diterapkan :



Gambar 10 *Activity Diagram* Perintah *Screenshot*

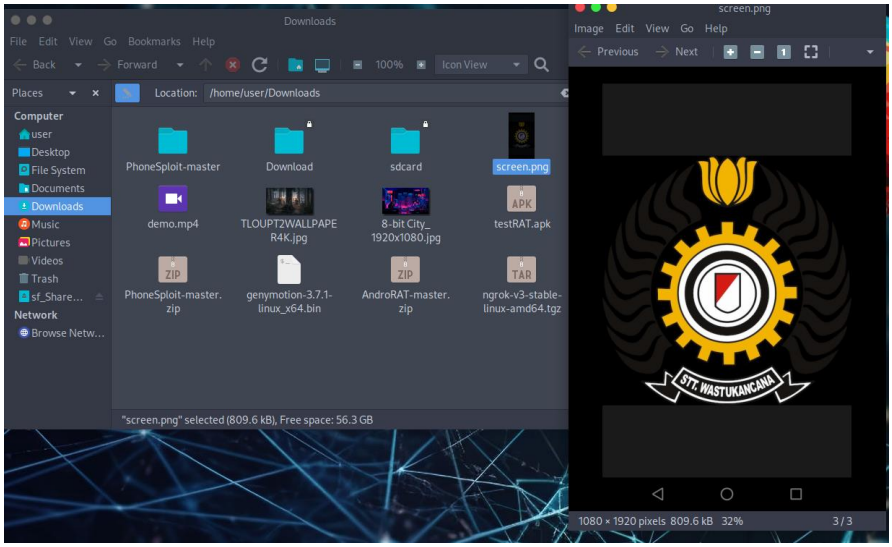
Pada diagram di atas menceritakan tentang skenario bagaimana perintah serangan ini bekerja, yaitu pada Langkah pertama *Attacker* memasukan perintah nomor 7 untuk meninisiasi perintah serangan. Dilanjutkan dengan memasukan *IP Address* perangkat korban, setelah itu *server* virtual melakukan verifikasi terhadap permintaan yang datang dari arah *Attacker*. Jika perangkat korban tidak terhubung dengan *server virtual* melalui *ADB*. Maka perintah akan gagal di eksekusi. Jika perangkat korban terhubung, maka secara otomatis perangkat korban akan melakukan tangkapan layar secara *Backdoor*, lalu proses serangan diakhiri dengan menentukan direktori untuk menyimpan hasil tangkapan layar pada perangkat komputer *Attacker*.



Gambar 11 *Command Shell no.7 Screen Shot on a phone*

Pada gambar diatas menunjukan di sisi kanan merupakan tampilan perangkat korban sedang mengakses galeri dan menampilkan sebuah *file* gambar. Sedangkan di sisi

kiri menunjukan bagaimana proses eksekusi perintah yang dilakukan untuk melakukan tangkapan layar. Perintah tangkapan layar pada *command shell phonesploit* berhasil di eksekusi dan disimpan pada direkori *linux /home*/user/*Downloads*

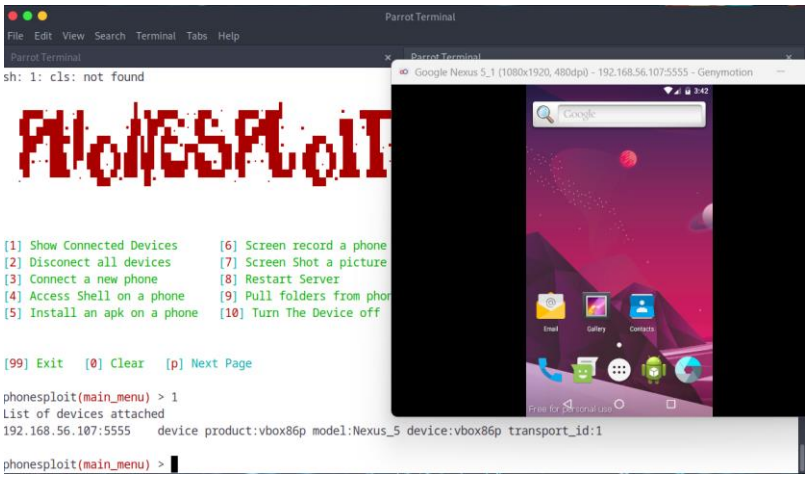


Gambar 12 Hasil perintah tangkapan layar berhasil dieksekusi

Pada gambar di atas menunjukan hasil dari perintah tangkapan layar berhasil di eksekusi dan disimpan di dalam direktori yang sudah ditentukan.

3. Memastikan Koneksi Perangkat Korban (*Maintaining Access*)

Pada tahapan ini, penulis melakukan pengecekan terhadap perangkat yang terhubung pada jaringan. Tujuan nya untuk mengetahui koneksi antara *Phonesploit* dengan perangkat *Emulator* tetap terhubung atau terputus. Tindakan ini diperlukan untuk menjaga koneksi antar jaringan. Karena jika jaringan tidak saling terhubung antara *Phonesploit* dengan perangkat *Emulator,* maka sesi penetrasi akan berakhir. Dan untuk melanjutkan sesi serangan maka harus melakukan rekoneksi terhadap kedua perangkat tersebut.



Gambar 13 Perintah no.1 *Show Connected Devices*

Pada gambar di atas, dapat dilihat perangkat *emulator* dengan keterangan nama perangkat *Nexus_5* dan Alamat *IP Address* 192.168.56.107 dengan *port* 5555 sedang terhubung dengan *Phonesploit*

4. Analisis data dan Hasil (*Analysis*)

Dalam studi kasus simulasi pengujian serangan terhadap perangkat menggunakan media *emulator* ini, terdapat beberapa hasil dari pengujian serangan yang berdampak pada perangkat *emulator* yang dapat dirasakan oleh penulis pada perangkat *emulator* selama masa pengujian yaitu sebagai berikut :

a. Penurunan Kinerja Sistem

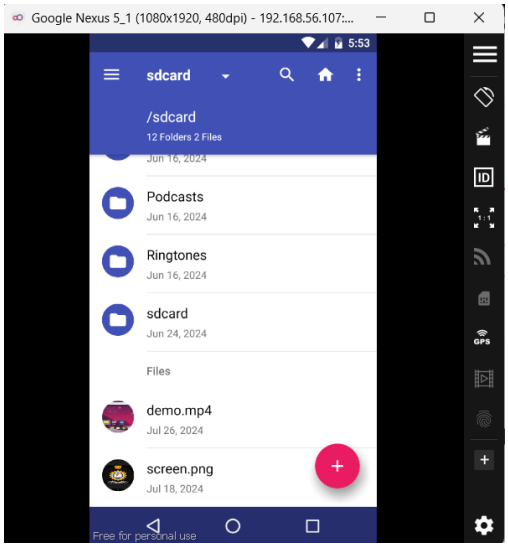
Dampak yang dapat dirasakan dengan jelas yaitu menurunnya kinerja pada sistem operasi *emulator,* yaitu perangkat *emulator* menjadi lambat dalam merespon perintah (*lagging/hanging*), butuh beberapa detik hingga menit hanya untuk sekedar berpindah halaman pada menu perangkat *emulator* dan bahkan tidak merespon perintah sama sekali (*freeze*). Hal ini disebabkan karena adanya aktivitas tidak sah yang terjadi dibalik tampilan utama perangkat *emulator* (*backdoor)* yang mengganggu kelancaran sistem operasi dalam merespon perintah atau aktivitas yang dilakukan oleh penulis.

b. Peningkatan Penggunaan Sumber Daya

Selain menurunnya kinerja, pada perangkat *emulator* tersebut juga menunjukkan peningkatan penggunaan sumber daya sistem seperti *CPU*, *RAM*, dan baterai. Hal ini disebabkan oleh proses yang berjalan di latar belakang yang dikendalikan oleh penyerang, aktivitas ini menguras sumber daya sistem secara keseluruhan disertai dengan menurunnya kinerja perangkat.

c. Anomali

Adanya Anomali atau *file* tidak dikenal pada direktori perangkat selama pengujian yang disebabkan oleh serangan yang dilakukan oleh penulis.



Gambar 14 *Kondisi direktori Emulator pasca serangan*

Pada gambar tersebut, dapat dilihat dokumen hasil dari pengujian *Screenshot* dan *Screen Record* turut tersimpan pada direktori perangkat *Emulator.*

Dengan mengenali dampak-dampak tersebut, penulis dapat lebih memahami dampak yang terjadi pada perangkat *Smartphone Android* berdasarkan hasil uji coba pada perangkat *Emulator.* Pada kasus nyata, dampak yang terjadi kemungkinan tidak akan jauh berbeda dari hasil pengujian pada hasil penelitian ini, dikarenakan perangkat *Emulator* yang berperan sebagai bahan uji coba memiliki spesifikasi dan sistem operasi yang sama dengan perangkat *Smartphone Android* yang sesungguhnya.

5 Kesimpulan

Berdasarkan hasil pengujian dari simulasi serangan yang dilakukan, terdapat beberapa kesimpulan selama periode serangan yang dilakukan terhadap perangkat *Emulator Android* yaitu sebagai berikut :

1. Pada penelitian ini penulis berhasil melakukan pengujian simulasi serangan terhadap perangkat *emulator android* dengan menggunakan *toolkit Phonesploit* pada sistem operasi *Parrot OS*. Selama periode serangan penulis berhasil melakukan eksploitasi terhadap direktori maupun sistem operasi pada *Emulator*. Pada pengujian tersebut dapat disimpulkan perangkat *emulator Android* dengan spesifikasi tersebut dapat dengan mudah di eksploitasi dan cenderung memiliki keamanan perangkat yang kurang memadai. Hasil dari pengujian ini berdampak pada kinerja sistem operasi yang menurun, ditandai dengan terjadinya *Lagging* pada perangkat *Emulator* dikarenakan akses *Backdoor* selama periode serangan.

2. Penulis berhasil melakukan pengujian keamanan dengan menyusupkan dokumen berupa *malware* untuk menguji keamanan perangkat *Emulator*. Hasil yang didapat yaitu *Malware* tersebut dapat dengan mudah masuk ke dalam direktori *Emulator*.

3. Hasil dari perintah yang dilakukan selama periode serangan seperti melakukan perekaman layar, tangkapan layar. Selain tersimpan pada direktori komputer *Attacker*. Dokumen – dokumen tersebut juga tersimpan pada direktori perangkat *emulator*. Sehingga dapat memenuhi ruang direktori pada perangkat tersebut.

Referensi

Andi Nugroho. (2019, October 11). *Waspadai, Serangan Man-in-the-Middle di Wi-fi Publik Gratis*. Https://Cyberthreat.Id/Read/3329/Waspadai-Serangan-Man-in-the-Middle-Di-Wi-Fi-Publik-Gratis.

Anggraini, N., Masruroh, S. U., & Tiaraningtias, H. (2020). Analisa Forensik Whatsapp Messanger Pada Smartphone Android. *Jurnal Ilmiah FIFO*, *12*(1), 83. https://doi.org/10.22441/fifo.2020.v12i1.008

Ardhiansyah Shandi Noris Romi Andrianto Jl Surya Kencana No, M., Gd, P. A., & Pamulang Tangerang Selatan -Banten, U. (n.d.). *JARINGAN KOMPUTER*. www.unpam.ac.id

Arote, A., & Mandawkar, U. (2021). Android Hacking in Kali Linux Using Metasploit Framework. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 497–504. https://doi.org/10.32628/cseit2173111

Eliasta Ketaren. (2016). CYBERCRIME, CYBER SPACE, DANCYBER LAW. *Jurnal TIMES , Vol. V No 2 : 35-42 , 2016*, *2*, 35–42.

Fitriani, Y., & Pakpahan, R. (n.d.). *Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace*. https://doi.org/10.31294/jc.v19i2

Gani, A. G. (n.d.). *SEJARAH dan PERKEMBANGAN INTERNET DI INDONESIA*.

Muhyidin, Y., Hafid Totohendarto, M., Undamayanti, E., & Tinggi Teknologi Wastukancana, S. (n.d.). *Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods*.

Mallik, A. (2018). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. In *Jurnal Pendidikan Teknologi Informasi* (Vol. 2, Issue 2).

Rahmadani, M. A., Rizal, M. F., & Gunamawan, T. (n.d.). *IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER WIRELESS HACKING IMPLEMENTATION USING KALI LINUX KALI NETHUNTER*.

Rony Setiawan. (2022, January 19). *Apa itu Emulator? Pahami pengertian dan Fungsinya*. Https://Www.Dicoding.Com/Blog/Apa-Itu-Emulator/.

Setiawan, N. (2019). *KASUS KEJAHATAN SIBER PADA TELEPON SELULER ANDROID* (Vol. 2, Issue 1).

Sufajar Butsianto, & Anisah Purnamasari. (2021). IMPLEMENTASI JARINGAN HOTSPOT DAN BANDWIDTH MANAGEMENT DENGAN MENGGUNAKAN MIKROTIK ROUTERS PADA CAFÉ ROEMAH KEDUA. *Jurnal Teknologi Pelita Bangsa*, *Vol.12*(p-ISSN: 2407-3903 e-ISSN: 2407-3903), 2–3.

Supriyadi, A., Gartina, D., Komputer, F., & Badan Litbang, S. (2007). *MEMILIH TOPOLOGI JARINGAN DAN HARDWARE DALAM DESAIN SEBUAH JARINGAN KOMPUTER Recognizing Topology And Network Hardware, Computer Network* (Vol. 16, Issue 2).