KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 3, Juli (2024), pp. 845-856

Analisis Keamanan Dan Eksploitasi Kernel Android 13 Menggunakan Metasploit *Reverse_Tcp*

Salman Alhidamkara[1], Somantri[2], Ivana Lucia Kharisma[3]
[1,2,3]Fakultas Teknik Komputer Dan Desain, Universitas Nusa Putra, Indonesia
E-mail: [1]salman.alhidamkara_ti20@nusaputra.ac.id, [2]somantri@nusaputra.ac.id, [3]ivana.lucia@nusaputra.ac.id

Abstract

The development of information technology, especially in the mobile field, has changed the way we interact with devices substantially. Android, as the most dominant mobile operating system used worldwide, attracts significant attention to its security aspects. Despite improvements in the security of Android devices, exploitation attempts continue to be made by security researchers and hackers using various methods, including exploitation via Reverse_TCP with tools such as Metasploit. This research aims to analyze the security of Android 13 devices using the Reverse_TCP method via Metasploit. The methods used involve exploitation by sending backdoor applications, opening Meterpreter sessions, and stealing data such as SMS and call logs. The results showed that Google Play Protect detected malicious applications, but the applications could still be installed and run, indicating a weakness in the security detection system. Reverse_TCP exploits can lead to unauthorized access to personal data and full control of the device, posing significant risks to users. Proposed preventive measures include using the Mobile Security Framework (MobSF), enabling Google Play Protect, and disabling unnecessary app permissions. This study suggests further research to overcome limitations and explore further the security aspects of Android.

Keywords: *Exploitation, Metasploit, Android 13, Reverse TCP and Security Analysis*

Abstrak

Perkembangan teknologi informasi, terutama di bidang mobile, telah mengubah cara kita berinteraksi dengan perangkat secara substansial. Android, sebagai sistem operasi mobile yang paling dominan digunakan di seluruh dunia, menarik perhatian yang signifikan terhadap aspek keamanannya. Meskipun telah ada peningkatan dalam keamanan perangkat Android, upaya eksploitasi terus dilakukan oleh para peneliti keamanan dan peretas dengan menggunakan berbagai metode, termasuk eksploitasi melalui Reverse_TCP dengan alat bantu seperti Metasploit. Penelitian ini bertujuan untuk menganalisis keamanan perangkat Android 13 menggunakan metode Reverse_TCP melalui Metasploit. Metode yang digunakan melibatkan eksploitasi dengan mengirim aplikasi backdoor, membuka sesi Meterpreter, dan mencuri data seperti SMS dan log panggilan. Hasil penelitian menunjukkan bahwa Google Play Protect mendeteksi aplikasi berbahaya, namun aplikasi tersebut masih dapat diinstal dan dijalankan, menunjukkan kelemahan dalam sistem deteksi keamanan. Eksploitasi Reverse_TCP dapat menyebabkan akses tidak sah ke data pribadi dan kontrol penuh atas perangkat, menimbulkan risiko signifikan bagi pengguna. Langkah pencegahan yang diusulkan termasuk penggunaan Mobile Security Framework (MobSF), pengaktifan Google Play Protect, dan menonaktifkan izin aplikasi yang tidak diperlukan. Penelitian ini menyarankan penelitian lebih lanjut untuk mengatasi keterbatasan dan mengeksplorasi lebih dalam aspek keamanan Android.

Kata Kunci: *Eksploitasi, Metasploit, Android 13, Reverse TCP dan Analisis keamanan*

ISSN: 2720-992X

Copyright © KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)

1. Pendahuluan

Dalam era digital yang terus berkembang, keamanan sistem operasi mobile menjadi semakin penting, khususnya dalam konteks *Android* yang merupakan sistem operasi yang paling banyak digunakan di seluruh dunia [1], [2]. *Kernel Android*, sebagai inti dari sistem operasi ini, memegang peranan krusial dalam mengelola sumber daya perangkat keras dan menyediakan antarmuka bagi aplikasi yang berjalan di atasnya [3]. Namun, dengan kemajuan teknologi juga muncul tantangan baru dalam hal keamanan [4]. Keberadaan kerentanan dalam *kernel Android* menjadi target utama bagi penyerang yang mencari celah untuk mengeksploitasi perangkat tersebut [5]. Dalam menghadapi kompleksitas dan luasnya penggunaan *Android*, diperlukan upaya yang sistematis untuk menganalisis keamanan *kernel Android versi* terbaru, dalam hal ini adalah *versi* 13 [6]. Salah satu pendekatan yang umum digunakan dalam analisis keamanan sistem adalah penggunaan alat bantu seperti *Metasploit*, yang merupakan salah satu *Framework* pengujian penetrasi yang paling populer dan kuat [7]. Modul *Reverse_TCP* dalam *Metasploit* memungkinkan peneliti keamanan untuk membangun koneksi terbalik ke perangkat target, membuka peluang untuk mengeksplorasi potensi kerentanan dan rentang serangan yang mungkin [8].

Walaupun *kernel Android* 13 telah menerima perbaikan keamanan dari *versi* sebelumnya, namun demikian, tidak dapat dipungkiri bahwa masih terdapat risiko keamanan yang perlu dipahami dan ditangani [9]. Keberadaan celah keamanan dalam *kernel Android* 13 dapat dimanfaatkan oleh penyerang untuk mendapatkan akses yang tidak sah ke perangkat pengguna, yang pada gilirannya dapat menyebabkan kerugian data pribadi atau bahkan kerugian finansial [10]. Oleh karena itu, perlu dilakukan analisis yang mendalam terhadap keamanan *kernel Android* 13 menggunakan *Metasploit Reverse_TCP* [11]. Dengan melakukan analisis ini, diharapkan dapat diidentifikasi dan dipahami kerentanan yang mungkin ada dalam *kernel Android* 13, sehingga langkah-langkah pencegahan dan perbaikan keamanan yang tepat dapat dirancang dan diimplementasikan [12].

Pentingnya analisis keamanan *kernel Android* 13 ini tidak hanya berkaitan dengan pengembangan sistem operasi itu sendiri, tetapi juga melibatkan privasi dan keamanan pengguna [1]. Dengan meningkatnya ancaman siber yang ditujukan kepada perangkat mobile, langkah-langkah proaktif dalam meningkatkan keamanan *kernel Android* 13 akan memberikan manfaat yang signifikan bagi pengguna secara keseluruhan. Dalam konteks pengembangan keamanan *cyber*, penelitian ini juga dapat memberikan panduan yang berguna bagi pengembang dan peneliti keamanan untuk mengembangkan strategi yang lebih efektif dalam mengatasi ancaman siber terhadap sistem operasi *Android* [13]. Dengan demikian, analisis keamanan dan eksploitasi *kernel Android* 13 menggunakan *Metasploit Reverse_TCP* menjadi topik yang relevan dan perlu untuk diteliti lebih lanjut guna meningkatkan keamanan cyber secara keseluruhan [14].

Dalam memilih judul "Analisis Keamanan dan Eksploitasi *Kernel Android* 13 Menggunakan *Metasploit Reverse_TCP*", relevansi dan urgensi topik tersebut sangatlah jelas. Mengingat pentingnya keamanan sistem operasi *mobile*, khususnya *Android* yang mendominasi pasar global, fokus pada analisis keamanan *kernel Android versi* terbaru, yaitu *versi* 13, menjadi langkah yang tepat. *Metasploit Reverse_TCP* dipilih sebagai alat analisis karena popularitasnya dan kemampuannya dalam mendeteksi kerentanan serta rentang serangan yang mungkin terjadi. Dengan demikian, judul ini mencerminkan kebutuhan akan penelitian yang sistematis dan mendalam untuk menghadapi ancaman *siber* yang semakin kompleks terhadap sistem operasi *Android*, sambil memberikan kontribusi pada pengembangan strategi keamanan *cyber* yang lebih efektif secara keseluruhan.

2. Metodologi Penelitian

2.1. *Android Operating System*

Android Operating System (OS) adalah sistem operasi yang paling umum digunakan pada perangkat mobile di seluruh dunia. Dikembangkan oleh Google, *Android* OS dikenal karena fleksibilitasnya dan dominasinya di pasar perangkat *mobile*. Keamanan *Android* melibatkan mekanisme seperti *sandboxing*, izin aplikasi, enkr*ip*si data, dan deteksi *malware* untuk melindungi pengguna dari ancaman keamanan. Namun, dengan populasi pengguna yang besar dan kompleksitasnya [15].

2.2. *Linux Kernel*

Linux Kernel merupakan inti dari sistem operasi *Linux* yang mengelola sumber daya perangkat *keras* dan menyediakan antarmuka untuk aplikasi. Ini merupakan bagian terpenting dari sistem operasi karena bertanggung jawab atas manajemen memori, penjadwalan proses, manajemen sistem berkas, dan interaksi dengan perangkat keras. *Kernel* ini berfungsi sebagai penghubung antara perangkat keras komputer dan perangkat lunak yang berjalan di atasnya [16].

2.3. *Metasploit Framework*

Metasploit Framework adalah platform penetrasi *open-source* yang menyediakan alat dan modul untuk *pengujian* keamanan dan eksploitasi [17]. Sebagai salah satu alat paling kuat dalam arsenalmu, *Metasploit* memungkinkan para profesional keamanan untuk mengidentifikasi, mengeksploitasi, dan menutup celah keamanan dalam sistem target [15].

2.4. *MobSF (Mobile Security Framework)*

MobSF (Mobile Security Framework) adalah kerangka kerja keamanan seluler yang dapat digunakan untuk menganalisis aplikasi Android dan iOS. Ini mencakup fitur seperti pemindaian malware, analisis kode, dan penilaian risiko keamanan [16].

2.5. *NMAP*

Nmap adalah sebuah perangkat lunak *open-source* yang digunakan untuk pemindaian jaringan dan audit keamanan. Nmap singkatan dari "*Network Mapper*". Dengan menggunakan *Nmap*, pengguna dapat mengetahui informasi tentang host dalam jaringan, termasuk port yang terbuka, layanan yang berjalan, sistem operasi yang digunakan, dan banyak informasi lainnya yang dapat digunakan untuk menganalisis keamanan jaringan [16].

2.6. *Payload*

Payload adalah bagian dari kode yang dieksekusi setelah eksploitasi berhasil. Jenis-jenis *Payload* yang tersedia, seperti *reverse shell*, memungkinkan penyerang untuk mendapatkan akses jarak jauh ke sistem target. Dalam konteks analisis dan eksploitasi *Android*, pemahaman tentang *Payload* penting untuk mengukur sejauh mana sistem rentan terhadap serangan dan untuk merancang pertahanan yang efektif [18].

2.7. *Meterpreter*

Meterpreter adalah muatan lanjutan yang *dapat* diperluas yang menggunakan injeksi *DLL* dalam memori. Ini secara signifikan meningkatkan kemampuan pasca-eksploitasi dari *Metasploit Framework*. Dengan berkomunikasi melalui soket stager, itu menyediakan *API Ruby* sisi klien yang luas[15].

2.8. *MSF Venom*

MSF Venom adalah alat yang digunakan untuk menghasilkan *Payload* berbagai *platform*. Dengan parameter yang dapat disesuaikan, *MSF Venom* memungkinkan

pengguna untuk membuat *Payload* sesuai kebutuhan. *MSF Venom* memainkan peran kunci dalam pengembangan dan uji coba *exploit*, *memungkinkan* para profesional keamanan untuk membuat dan menyesuaikan *Payload* sesuai dengan kebutuhan spesifik mereka [19].

2.9. *Reverse_TCP Connection*

Teknik *Reverse_TCP Connection* adalah salah satu metode serangan yang digunakan dalam bidang keamanan informasi, khususnya dalam konteks analisis perangkat Android dengan menggunakan Metasploit *Framework.* Dalam teknik ini, perangkat yang terinfeksi akan membuka koneksi ke server yang dikendalikan oleh penyerang, sehingga memungkinkan penyerang untuk *mengakses* dan mengontrol perangkat tersebut dari jarak jauh [14].

2.10. *Backdoor*

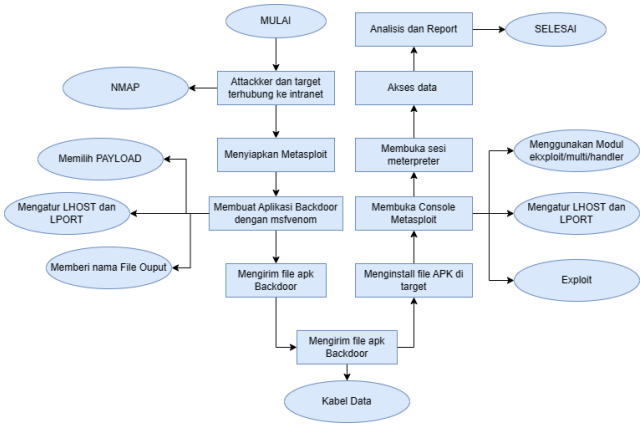
Sebuah *"backdoor"* (atau pintu belakang) adalah sebuah metode yang digunakan oleh pembuat perangkat lunak atau penyerang komputer untuk memasukkan akses tidak sah ke dalam suatu sistem atau perangkat. *Backdoor* bisa berupa sebuah fitur tersembunyi yang sengaja dibuat oleh pembuat perangkat lunak untuk tujuan pemeliharaan atau pemecahan masalah, tetapi bisa juga merupakan perangkat lunak yang sengaja dimasukkan oleh penyerang untuk mendapatkan akses ilegal ke system [20].

2.11. Metode Penelitian

Penelitian ini mengadopsi suatu kerangka kerja penelitian yang canggih dan efektif dengan menerapkan metode *eksperimental* yang dirancang secara khusus untuk mengamati dan menganalisis keamanan perangkat *Android* 13. Metode eksperimental ini difokuskan pada penerapan metode *Reverse_TCP*, sebuah pendekatan yang telah terbukti relevan dalam konteks pengujian keamanan pada perangkat *Android* [1].

2.12. Metode Serangan / Eksploitasi

Metode serangan ini menggunakan metode reverse_tcp menggunakan Metasploit *Framework*. Berikut adalah alur dari eksploitasi:



Gambar 1. *Flowchart* Metode *Reverse TCP*

Flowchart menggambarkan serangkaian langkah-langkah yang dilakukan oleh seorang penyerang *(Attacker)* untuk mengeksploitasi sebuah target menggunakan *Backdoor.*

Berikut adalah penjelasan dari *Flowchart* pada gambar 1.

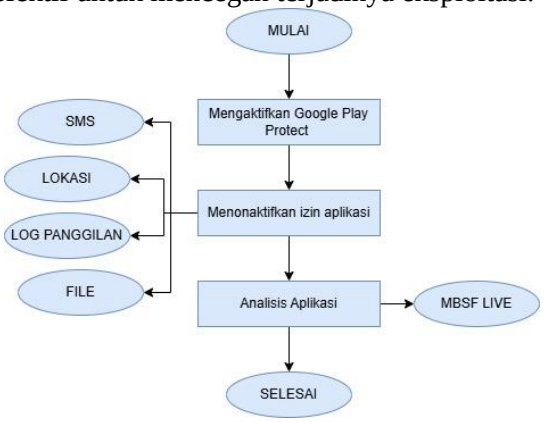
1) *Attacker* dan target terhubung ke intranet
   Penyerang dan target terhubung ke jaringan intranet yang sama. Menggunakan *nmap* untuk memastikan bahwa target sudah terhubung ke intranet.

2) Menyiapkan Metasploit
   Penyerang menyiapkan perangkat lunak Metasploit, yang merupakan alat penetrasi yang populer digunakan untuk mengeksploitasi kelemahan dalam sistem komputer.
3) Membuat aplikasi *backdoor* dengan *msfvenom*
   Dalam langkah ini, penyerang menggunakan alat Metasploit bernama msfvenom untuk membuat aplikasi *backdoor*. Mengirim file APK *backdoor.* Penyerang mengirimkan file APK *backdoor* ke perangkat target. Metode pengiriman menggunakan kabel data
4) Menginstall file APK di target
   Perangkat target menginstal file APK *backdoor* yang diterima dari penyerang.
5) Membuka console Metasploit
   Penyerang membuka konsol Metasploit dan menggunakan modul exploit/multi/handler untuk menyiapkan layanan penanganan yang akan menangani koneksi dari perangkat target yang terinfeksi. Dan Penyerang juga harus mengatur parameter *LPORT* (*Port Listener*) dan *LHOST* (*Host Listener*) dalam modul *exploit,* dan kemudian melakukan eksploitasi pada perangkat target.
6) Membuka sesi Meterpreter
   Jika eksploitasi berhasil, penyerang dapat membuka sesi Meterpreter, yang merupakan shell interaktif yang memberikan akses ke sistem target.
7) Mengakses data
   Dengan sesi Meterpreter yang terbuka, penyerang dapat mengakses dan memanipulasi data yang ada di dalam sistem target. Ini bisa mencakup akses ke file, informasi pengguna, dan layanan sistem lainnya.
8) Analisis dan *report*
   Setelah mengeksploitasi target dan mengakses data yang diinginkan, penyerang dapat melakukan analisis lebih lanjut terhadap informasi yang diperoleh dan menyusun laporan tentang serangan yang dilakukan.

Flowchart ini memberikan gambaran tentang serangkaian langkah yang dilakukan oleh penyerang untuk mengeksploitasi perangkat menggunakan Metasploit Framework.

2.13. Tahapan Pencegahan Eksploitasi

Untuk mencegah terjadinya eksploitasi pada perangkat android saya memberikan sebuah tahapan yang efektif untuk mencegah terjadinya eksploitasi.



Gambar 2. Tahapan Pencegahan Eksploitasi

Berikut adalah tahapan yang dilakukan ;

1) Mengaktifkan *Google Play Protect*
2) Menonaktifkan izin Aplikasi
   Izin aplikasi yang dinonaktifkan seperti izin sms, pesan dan log paggilan beserta lokasi

3) Menganalisis Aplikasi yang akan digunakan
Aplikasi yang akan diinstall dianalisis menggunakan mbsf live untuk memastikan bahwa aplikasi itu memiliki izin yang berbahaya

Dengan mengikuti tahapan ini secara teratur dan konsisten, pengguna smartphone dapat meningkatkan keamanan perangkat Android Anda dan mencegah terjadinya risiko eksploitasi.

2.14. Analisis Kebutuhan

Berikut adalah beberapa analisis kebutuhan yang perlu dipertimbangkan:

a) Spesifikasi Perangkat Target :

Tabel 1. Informasi perangkat

No	Spesifikasi Target	Deskripsi
1	Nama Perangkat : Xiaomi Redmi 12	Perangkat smartphone yang dirilis pada bulan Agustus 2023
2	Memori Perangkat : RAM 8/256 GB	Memiliki RAM sebesar 8 GB, memungkinkan untuk menjalankan aplikasi dan proses dengan lancar tanpa terlalu banyak gangguan kinerja
3	Sistem Operasi : Android 13	Menggunakan *versi Android* 13, yang merupakan *versi* terbaru dari sistem *Android* saat ini
4	Versi Kernel : Kernel 4.19.191	*Versi kernel* yang digunakan adalah 4.19.191 yang merupakan *versi kernel Android* 13 yang menyediakan kontrol inti dari sistem operasi tersebut dan mengelola sumber daya perangkat keras

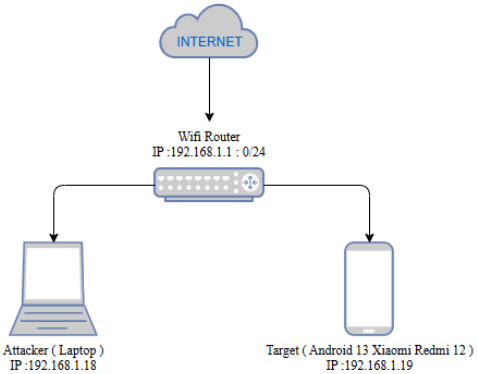
b) Spesifikasi *Tools Attacker*

Berikut adalah alat dan bahan yang digunakan dalam penelitian ini :

Tabel 2. *Tools* yang digunakan

No	Alat / *Tools*	Kegunaan
1	Laptop Windows 10 (Dell Lattitude E7250) Ram 8 GB SSD 120GB	Laptop dengan spesifikasi yang mendukung kebutuhan penelitian seperti pemrosesan RAM yang memadai, dan konektivitas yang diperlukan
2	*Metasploit Framework versi* 6.3.55	Alat uji penetrasi untuk melakukan eksploitasi dan analisis keamanan menggunakan *Reverse_TCP*.
3	*MSF Venom*	Alat yang termasuk dalam kerangka kerja keamanan *Metasploit*.
4	*Nmap*	*Nmap* adalah sebuah *tool* atau perangkat lunak yang digunakan untuk pemindaian jaringan dan audit keamanan.

c) Topologi Jaringan Serangan Eksploitasi



Gambar 3. Tampilan Topologi Jaringan

Berikut penjelasan rinci mengenai setiap komponen dan bagaimana mereka berinteraksi dalam topologi ini:

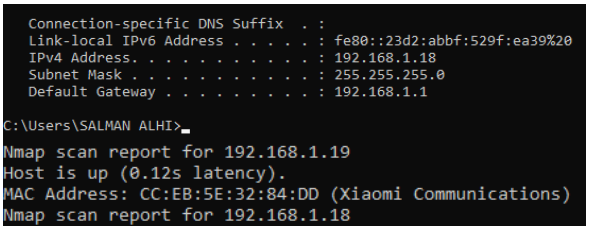
1) Internet
   Sumber koneksi eksternal yang menyediakan akses ke sumber daya global, seperti website, email, dan layanan online lainnya. Terhubung ke router Wi-Fi rumah melalui koneksi dari ISP (*Internet Service Provider*).
2) Router Wi-Fi Rumah
   Router juga berfungsi sebagai titik akses Wi-Fi, memungkinkan perangkat nirkabel untuk terhubung ke jaringan.
3) Perangkat Android (Target)
   Berfungsi sebagai target yang akan dieksploitasi dalam skenario ini.
4) Laptop/PC dengan Metasploit (*Attacker*)
   Laptop atau PC ini juga terhubung ke router Wi-Fi melalui koneksi nirkabel atau kabel.

Berfungsi sebagai perangkat yang akan menjalankan Metasploit untuk mengeksploitasi perangkat Android.

3. Hasil dan Pembahasan

3.1. Implementasi Pengujian Serangan Eskploitasi

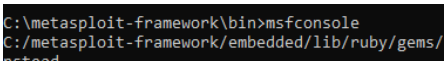
a) *Attacker* dan target terhubung ke intranet



Gambar 4. Tampilan terminal windows

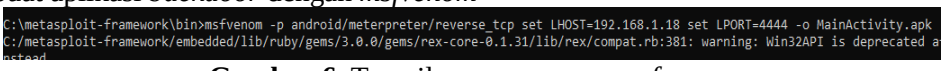
Dari Gambar 4 dapat dilihat bahwa attacker dan target sudah terhubung ke jaringan intranet. Dengan menggunakan perintah *ifconfig* dan juga nmap.

b) Menyiapkan Metasploit
   Menggunakan perintah *msfconsole* untuk membuka metasploit



Gambar 5. Tampilan Terminal *Metasploit*

c) Membuat aplikasi *backdoor* dengan *msfvenom*



Gambar 6. Tampilan penggunaan *msfvenom*

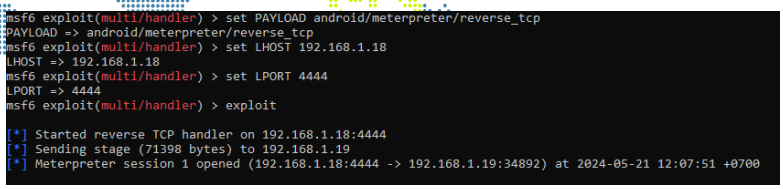
Dari Gambar 6 Attacker membuat aplikasi *backdoor* menggunakan *msfvenom***.**

d) Mengirim file APK *backdoor* ke target menggunakan kabel data
e) Menginstall file APK di target

Gambar 7. Tampilan *Backdoor* terinstall

Gambar 7 menampilkan bahwa aplikasi berhasil diinstall dan siap untuk di eksploitasi

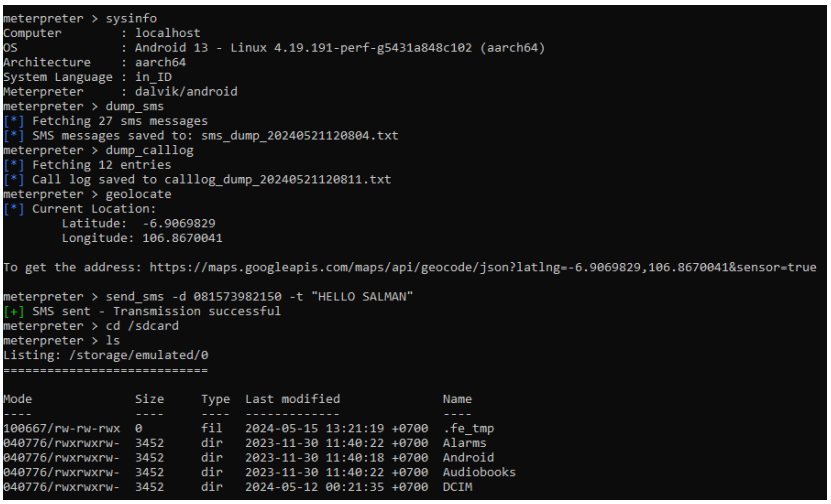
f) Membuka *console* Metasploit dan membuka sesi meterpreter



Gambar 8. Tampilan *Console Metasploit*

Menggunakan *use exploit/multi/handler* serta melakukan set PAYLOAD, LHOST dan juga LPORT untuk membuka sesi meterpreter.

Berikut adalah tampilan dari data yang berhasil diakses oleh penyerang terhadap target sebagai berikut:



Gambar 9. Tampilan Console Metasploit

Dari Gambar 9 penyerang berhasil melihat system target dan juga berhasil mengambil data sensitif seperti log panggilan, data sms, mengirim sms, dan juga lokasi target.

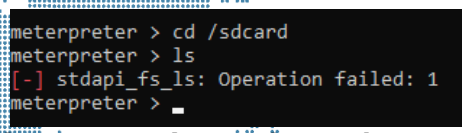
3.2. Pencegahan Serangan Metasploit

a) Mengaktifkan *GooglePlay Protect*

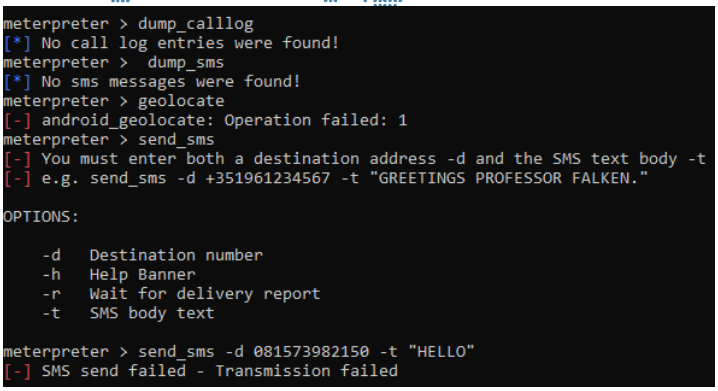
Gambar 10. Tampilan *Google protect* Aktif

Dengan mengaktifkan fitur google play protect maka aplikasi backdoor akan terdeteksi sebagai aplikasi yang berbahaya

b) Menonaktifkan semua izin Aplikasi *Backdoor*



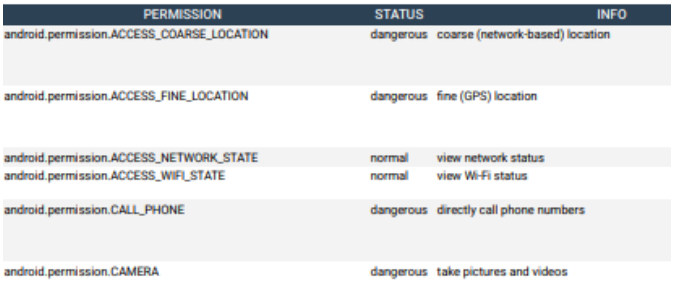
Gambar 11. Tampilan gagal mengakses Direktori



Gambar 12. Tampilan Console Metasploit

Dengan menonaktifkan beberapa izin pada aplikasi backdoor maka penggunaan meterpreter dengan perintah dump_sms, dump_calllog, geolocate dan send_sms.

c) Analisis Aplikasi



PERMISSION	STATUS	INFO
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location
android.permission.ACCESS_NETWORK_STATE	normal	view network status
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status
android.permission.CALL_PHONE	dangerous	directly call phone numbers
android.permission.CAMERA	dangerous	take pictures and videos

Gambar 13. Tampilan *Static Analysis Mbsf*

Izin ini digunakan untuk mengakses berbagai fungsi perangkat dan penting untuk dipertimbangkan saat menginstal dan menggunakan aplikasi *backdoor*.

3.3. Pengujian Serangan Metasploit

Sebuah laporan penelitian disusun secara rinci, mencakup hasil eksploitasi dan temuan keamanan perangkat *Android* 13. Berikut adalah Laporan dari hasil temuan dan Eksploitasi pada *Android* 13 Xiaomi Redmi 12.

Tabel 3. Laporan hasil penyerangan

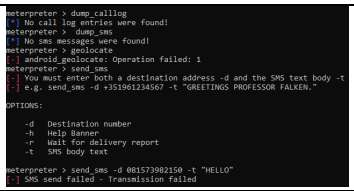
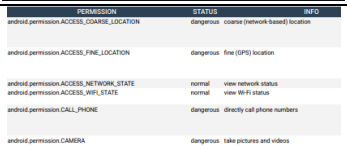
Pengujian	Analisis Informasi	Hasil	
		Success	***Failed***
Mendapatkan informasi sistem	Informasi sistem perangkat Android 13 berhasil diperoleh, mencakup model perangkat, versi sistem operasi, dan informasi relevan lainnya.	√	
Aplikasi terinstall diperangkat target	Aplikasi berhasil diinstal pada perangkat target, meskipun terdeteksi oleh Google Play Protect. Ini menunjukkan bahwa langkah-langkah keamanan perangkat dapat dilewati, dan aplikasi yang tidak sah dapat diinstal.	√	
Membuka sesi	Sesi meterpreter berhasil dibuat pada perangkat	√	

Pengujian	Analisis Informasi	Hasil	
		Success	*Failed*
meterpreter	Android 13, memungkinkan eksplorasi dan eksploitasi perangkat lebih lanjut.		
Dump SMS (Mengambil pesan SMS)	Data SMS berhasil diekstraksi dari perangkat Android 13, termasuk pesan yang dikirim dan diterima, yang dapat digunakan untuk mendapatkan informasi sensitif.	√	
Geolocate (Melihat lokasi perangkat target)	Lokasi perangkat target berhasil diperoleh, yang dapat digunakan untuk berbagai tujuan, seperti pelacakan atau pengawasan.	√	
Mengambil data didalam direktori target	Penyerang mencoba mengambil gambar pada direktori target	√	
Dump Call Log (Memuat Log Panggilan)	Data log panggilan berhasil diekstraksi dari perangkat Android 13, mencakup detail seperti nomor telepon, durasi panggilan, dan stempel waktu panggilan masuk dan keluar.	√	
Send_sms (Mengirim pesan kepada target)	Pesan SMS berhasil dikirim ke perangkat target dari perangkat Android 13. Ini dapat digunakan untuk berbagai tujuan, seperti rekayasa sosial atau serangan phishing.	√	
Mengakses Sistem direktori	Beberapa direktori di perangkat Android 13 berhasil diakses, dan dapat dimanfaat penyerang untuk mengakses data sensitive seperti gambar video dan juga file penting yang terdapat di perangkat target.	√	
Kesimpulan	Perangkat Android 13 ditemukan rentan terhadap berbagai serangan, termasuk pemasangan aplikasi yang tidak sah, ekstraksi data sensitif, dan pelacakan lokasi perangkat.		

3.4. Pencegahan Serangan Metasploit

Berikut adalah Laporan pencegahan dengan menerapkan Langkah – Langkah yang efektif untuk mencegah terjadinya Eksploitasi

Tabel 4. Laporan Pencegahan Eksploitasi

No	Pencegahan	Analisis Informasi	Keterangan
1	Mengaktifkan Google Play Protect pada perangkat target		Dengan mengaktifkan google play protect maka aplikasi backdoor yang akan diinstal akan terdeteksi sebagai aplikasi berbahaya
2	Menonaktifkan Beberapa izin aplikasi		Dengan menonaktifkan izin Log Panggilan, sms, dan lokasi maka meterpreter tidak dapat mengakses log panggilan, mengirimkan pesan sms, dan lokasi.
3	Menganalisis Aplikasi		Untuk memastikan ulang bahwa aplikasi backdoor ini berbahaya penulis menggunakan Mobsf live untuk melihat beberapa akses izin yang berbahaya.

4. Kesimpulan

Penelitian ini mengimplementasikan dan menganalisis keamanan perangkat Android 13 dengan menggunakan metode Reverse_TCP melalui Metasploit. Pertama, terkait proses analisis dan eksploitasi menggunakan Metasploit Reverse TCP pada perangkat Android 13, penelitian ini menunjukkan bahwa langkah-langkah eksploitasi termasuk pengiriman aplikasi backdoor, pembukaan sesi Meterpreter, dan manipulasi data seperti pencurian SMS, log panggilan, dan informasi lokasi. Meskipun Google Play Protect dapat mendeteksi aplikasi berbahaya, aplikasi tersebut masih bisa diinstal dan dijalankan, menunjukkan kelemahan dalam sistem deteksi keamanan. Kedua, mengenai dampak dan potensi risiko dari eksploitasi menggunakan metode Reverse_TCP pada perangkat Android 13, penelitian ini menemukan bahwa eksploitasi ini dapat menyebabkan berbagai risiko, seperti akses tidak sah ke data pribadi dan kontrol penuh atas perangkat. Penyerang bisa memanfaatkan kerentanan ini untuk mencuri informasi sensitif, mengendalikan fungsi perangkat, dan menyebabkan kerugian yang signifikan bagi pengguna. Ketiga, untuk langkah-langkah pencegahan yang bisa dirancang dan diterapkan untuk meningkatkan keamanan kernel Android 13, penelitian ini menekankan pentingnya langkah-langkah pencegahan untuk mengurangi risiko eksploitasi. Penggunaan Mobile Security Framework (MobSF) terbukti efektif dalam mengevaluasi dan mengidentifikasi kerentanan dalam aplikasi backdoor. Mengaktifkan Google Play Protect membantu dalam mendeteksi dan mencegah instalasi aplikasi berbahaya. Selain itu, menonaktifkan izin aplikasi yang tidak diperlukan secara signifikan mengurangi risiko eksploitasi, karena aplikasi backdoor tidak bisa mengakses data atau menjalankan perintah berbahaya tanpa izin yang memadai.

Namun, keterbatasan dalam penelitian ini dan menekankan perlunya penelitian lebih lanjut untuk mengatasi kekurangan yang ada serta untuk mengeksplorasi lebih jauh aspek-aspek keamanan pada perangkat Android.Namun, penulis menyadari bahwa penelitian ini masih memiliki banyak kekurangan dan keterbatasan. Penelitian lebih lanjut diperlukan untuk mengatasi kekurangan ini dan untuk mengeksplorasi lebih banyak aspek keamanan pada perangkat Android**.**

Daftar Pustaka

[1] P. Sharma, C. Lepcha, S. T. Bhutia, And A. Sharma, “Case Study Exploit Of Android Devices Using Payload Injected Apk,” 2023, [Online]. Available: Www.Irjmets.Com

[2] Deshinta. Arrovadewi Dan Jelita. Asian Somantri, “Implementasi Computer Based Test Pada Smp Pgri Se-Gugus V Kecamatan Cileungsi Kabupaten Bogor,” 2023, Accessed: May 08, 2024. [Online]. Available: Https://Restikom.Nusaputra.Ac.Id/Issue/View/18

[3] D. Özdemir And H. Ç. Zaim, “Investigation Of Attack Types In Android Operating System,” 2021.

[4] S. Raj And N. K. Walia, “A Study On Metasploit Framework: A Pen-Testing Tool,” In *2020 International Conference On Computational Performance Evaluation, Compe 2020*, Institute Of Electrical And Electronics Engineers Inc., Jul. 2020, Pp. 296–302. Doi: 10.1109/Compe49325.2020.9200028.

[5] A. Dwivedi, “Launching An Attack And Exploiting The Android Using Metasploit Framework,” 2022. [Online]. Available: Www.Ijsrmst.Com

[6] Mr. Gokul Reghu, Ms. Anjaly Prasad, Ms. Athira Prasad, And Ms. Grace Joseph, “Novel Approach For Android Hacking Using Bluesnarfer,” 2023.

[7] T. Yerlikaya And S. Sen, “Hacking Android Mobile Phone With Phishing,” 2021. [Online]. Available: Http://10.40.48.145/Police.Apk

[8] I. Riadi, D. Aprilliansyah, And S. Sunardi, “Mobile Device Security Evaluation Using Reverse Tcp Method,” *Kinetik: Game Technology, Information System,*

Computer Network, Computing, Electronics, And Control, Sep. 2022, Doi: 10.22219/Kinetik.V7i3.1433.

[9] S. Thomas, P. G. Scholar, And T. Bijimol, "Vulnerability Testing On Rooted Android Phones Using Msf Venom Payloads," Vol. 3, No. 1, P. 27, 2021, Doi: 10.5281/Zenodo.5112704.

[10] R. Dwiananda, L. Putra, And I. Mardianto, "Jepin (Jurnal Edukasi Dan Penelitian Informatika) Exploitation With Reverse_Tcp Method On Android Device Using Metasploit," *Universitas Trisakti Jl. Letjen S. Parman*, No. 1, P. 11440, 2019.

[11] R. Satrio Hadikusuma And E. M. Rizaludin, "Methods Of Stealing Personal Data On Android Using A Remote Administration Tool With Social Engineering Techniques," *Ultimatics : Jurnal Teknik Informatika*, Vol. 15, No. 1, 2023.

[12] K. Barapatre And P. Parkhi, "Android Spy Agent-Remote Access Trojan," *International Research Journal Of Engineering And Technology*, 2020, [Online]. Available: Www.Irjet.Net

[13] N. Kar Zuin And V. Selvarajah, "A Case Study: Syn Flood Attack Launched Through Metasploit," 2021.

[14] N. Jaswal, *Mastering Metasploit : Exploit Systems, Cover Your Tracks, And Bypass Security Controls With The Metasploit 5.0 Framework*. 2020.

[15] S. Rahalkar, *Metasploit 5.0 For Beginners : Perform Penetration Testing To Secure Your It Environment Against Threats And Vulnerabilities*. 2020.

[16] K. N. Isnaini And D. Suhartono, "Security Analysis Of Simpel Desa Using Mobile Security Framework And Iso 27002:2013," *Intensif: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, Vol. 7, No. 1, Pp. 84–105, Feb. 2023, Doi: 10.29407/Intensif.V7i1.18742.

[17] A. Arote And U. Mandawkar, "Android Hacking In Kali Linux Using Metasploit Framework," *International Journal Of Scientific Research In Computer Science, Engineering And Information Technology*, Pp. 497–504, Jun. 2021, Doi: 10.32628/Cseit2173111.

[18] V. K. Velu And R. Beggs, *Mastering Kali Linux For Advanced Penetration Testing Secure Your Network With Kali Linux 2019.1 - The Ultimate White Hat Hackers' Toolkit, 3rd Edition*. 2019.

[19] A. Sabbah, M. Kharma, And M. Jarrar, "Creating Android Malware Knowledge Graph Based On A Malware Ontology," Aug. 2023, [Online]. Available: Http://Arxiv.Org/Abs/2308.02640

[20] H. Singh And H. Sharma, *Hands-On Web Penetration Testing With Metasploit : The Subtle Art Of Using Metasploit 5.0 For Web Application Exploitation*. 2020.