OPEN ACCESS
JOURNAL OF TELECOMMUNICATION, ELECTRONICS, AND CONTROL ENGINEERING (JTECE) ISSN: 2654-8275 (ONLINE)
JTECE. VOL. 07, NO. 01, PP. 32-41, JAN 2025 DOI: 10.20895/JTECE.V7I1.1632

Virtual Privat Network: Koneksi Keamanan pada Aplikasi Berbasis Android

Virtual Private Network: Security Connection in Android Based Applications

Jafaruddin Gusti Amri Ginting[1], Bongga Arifwidodo*[,2], Eka Wahyudi[3]

[1,2]*Department of Telecommunication Engineering, Telkom University*
Jl.D.I Panjaitan No.128, Purwokerto, Jawa Tengah, Indonesia

[3]*Department of Telecommunication Engineering, Diploma Program, Telkom University*
Jl.D.I Panjaitan No.128, Purwokerto, Jawa Tengah, Indonesia

*,[2]Bongga Arifwidodo: bonggaa@telkomuniversity.ac.id
[2]jafargustiamri@telkomuniversity.ac.id

Received on 28-10-2024, accepted on 29-12-2024, published on 27-01-2025

Abstrak

Kasus pencurian data informasi, seperti data pribadi, PIN, dan OTP, semakin meningkat akibat serangan dari penyerang. Serangan ini dilakukan dengan mengirimkan payload berupa skrip berbahaya yang di-*inject* ke dalam aplikasi Android melalui berbagai perantara, seperti email dan media sosial. Untuk mengatasi permasalahan ini, diperlukan analisis mendalam untuk memahami kemampuan *malware* dan memberikan langkah mitigasi yang tepat sehingga data informasi tidak dicuri oleh penyerang. Penelitian ini bertujuan menganalisis pengaruh penggunaan *Virtual Private Network* (VPN) terhadap aplikasi Android yang terinfeksi malware dengan teknik serangan *Command and Control* (C&C) *attack*. Skenario pengujian dilakukan dengan membandingkan dua kondisi: perangkat Android tanpa VPN dan perangkat Android dengan VPN. Pengujian mencakup pengukuran kemampuan serangan C&C dalam mengakses data sensitif serta evaluasi kinerja sistem, seperti kecepatan koneksi internet. Hasil penelitian menunjukkan bahwa penggunaan VPN dapat membatasi akses penyerang dengan memblokir komunikasi C&C, sehingga meningkatkan perlindungan keamanan data. Namun, hasil pengujian juga menunjukkan adanya penurunan performa koneksi internet sebesar 10,7% saat menggunakan VPN.

Kata kunci: C&C, Malware, QoS, VPN

Abstract

Cases of theft of information data, such as personal data, PINs and OTPs, are increasing due to attacks from attackers. This attack is carried out by sending a payload in the form of a malicious script that is injected into an Android application through various intermediaries, such as email and social media. To overcome this problem, in-depth analysis is needed to understand the capabilities of the malware and provide appropriate mitigation steps so that attackers do not steal information data. This research aims to analyze the effect of using a Virtual Private Network (VPN) on Android applications infected with malware using the Command and Control (C&C) attack technique. The test scenario was carried out by comparing two conditions: Android devices without VPN and Android devices with VPN. Testing includes measuring the C&C attack's ability to access sensitive data as well as evaluating system performance, such as internet connection speed. The research results show that the use of VPN can limit attackers' access by blocking C&C communications, thereby increasing data security protection. However, test results also show a decrease in internet connection performance by 10.7% when using a VPN.

Keywords: C&C, Malware, QoS, VPN

I. PENDAHULUAN

Data StatCounter dari 2018 hingga 2022 mencatat bahwa sebanyak 74,95% pengguna smartphone menggunakan sistem operasi Android [1]. Dominasi Android dalam pasar smartphone memudahkan aktivitas manusia, namun di sisi lain meningkatkan risiko keamanan. Aplikasi pada perangkat Android menjadi target potensial bagi penyerang untuk melakukan berbagai serangan. Penyerang memanfaatkan berbagai media untuk mengirimkan malware kepada korban [2]. Malware adalah perangkat lunak berbahaya yang dirancang untuk menyusup atau merusak sistem, sehingga memungkinkan pencurian data dan informasi pengguna [3]. Oleh karena itu, pengujian keamanan aplikasi yang baik sesuai dengan standar ISO/IEC 27001 menjadi sangat penting untuk meminimalisir risiko tersebut [4].

Berbagai penelitian telah menemukan celah keamanan yang signifikan pada aplikasi Android. Penelitian terhadap aplikasi Simple Desa menggunakan *Mobile Security Framework Static Analysis* menunjukkan *risk score* sebesar 6.2 dengan temuan kerentanan seperti *Weak Crypto, Dangerous Permission, Network Security, Hardcoded Secret*, dan SSL *Pinning* [5]. Penelitian serupa pada aplikasi *game* menemukan kerentanan seperti *Dangerous Permission, Weak Crypto, Root Detectio*n, SSL *Bypass*, dan *Domain Malware Check* [6]. Analisis lebih lanjut terhadap berbagai aplikasi *.apk* juga menemukan kerentanan serupa, termasuk *Root Detection* dan SSL *Bypass* [7]. Sementara itu, penelitian menggunakan panduan OWASP Mobile Security Testing Guide menemukan kerentanan seperti penyimpanan data sensitif secara lokal, validasi input yang lemah, dan kelemahan pada mekanisme *cache keyboard* [8]. Kerentanan lainnya meliputi validasi sertifikat yang tidak tepat, referensi objek langsung yang tidak aman (IDOR), dan *weak encoding* untuk kata sandi [9]. Semua temuan ini menunjukkan bahwa ancaman keamanan pada aplikasi Android cukup serius dan memerlukan perhatian khusus.

Cara untuk mengatasi permasalahan ini memerlukan analisis mendalam terhadap kelemahan dan ancaman keamanan aplikasi Android dengan mempertimbangkan penggunaan *Virtual Private Network* (VPN) dan tanpa VPN. Hasil dari penelitian ini diharapkan dapat memberikan analisis yang komprehensif mengenai celah keamanan aplikasi Android serta menyusun rekomendasi mitigasi yang efektif. Rekomendasi ini bertujuan untuk membantu melindungi pengguna dari infeksi malware, menjaga keamanan data pribadi, serta meningkatkan kesadaran akan pentingnya praktik keamanan dalam penggunaan aplikasi Android. Dengan mitigasi yang tepat, risiko serangan terhadap perangkat Android dapat diminimalisir, sehingga pengalaman pengguna menjadi lebih aman.

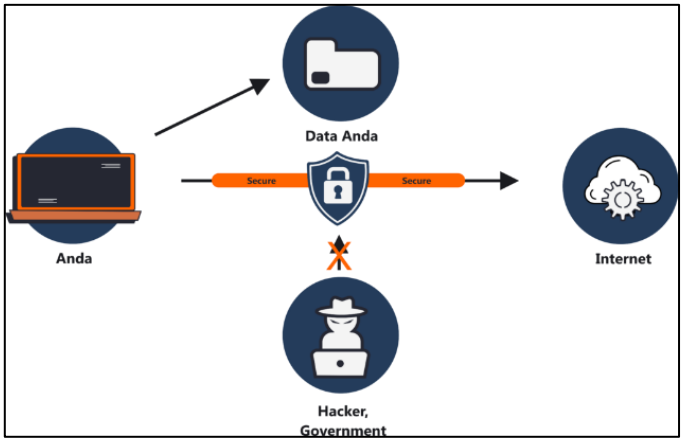
II. LITERATURE REVIEW

Keamanan informasi adalah upaya melindungi informasi, baik data maupun infrastruktur, dari tindakan yang berbahaya atau tidak sah [10]. Penelitian sebelumnya menunjukkan bahwa serangan terhadap infrastruktur organisasi, seperti serangan Distributed Denial of Service (DDoS) dan ransomware, dapat menyebabkan kerugian finansial yang signifikan serta kerusakan reputasi yang sulit dipulihkan. Studi oleh Smith et al. menemukan bahwa serangan DDoS pada layanan e-commerce dapat mengakibatkan downtime selama beberapa jam, yang berdampak pada hilangnya pendapatan dan kepercayaan pelanggan [11]. Sementara itu, penelitian oleh Chen dan Lee menunjukkan bahwa serangan ransomware yang menargetkan data sensitif organisasi dapat memaksa perusahaan membayar tebusan yang tinggi untuk memulihkan akses data, meskipun tidak ada jaminan bahwa data akan sepenuhnya dipulihkan [12]. Demikian pula, penelitian oleh Nguyen et al. menunjukkan bahwa serangan terhadap perangkat Android melalui payload injection dapat mencuri informasi pribadi seperti Credential, PIN, dan OTP [13]. Studi ini juga menekankan pentingnya perlindungan data pribadi melalui penggunaan mekanisme keamanan tambahan seperti Virtual Private Network (VPN).

Docker Container adalah paket perangkat lunak yang berisi semua dependensi yang diperlukan untuk menjalankan aplikasi tertentu [14]. Penelitian Brown & Kumar mengamati efektivitas Docker dalam mempercepat proses pembelajaran CLI bagi pengembang dan administrator sistem. Mereka menemukan bahwa Docker menyediakan lingkungan yang mudah diatur dan dihapus ulang, memungkinkan eksperimen CLI dilakukan tanpa risiko merusak sistem utama [15].

Malware telah mempengaruhi banyak gadget komputasi di era digital. Perangkat lunak dibuat untuk tujuan negatif yaitu menyerang jaringan, merusak infrastruktur penting hingga mencuri data sensitif. Malware biasanya masuk ke sistem melalui lampiran email, situs web berbahaya, unduhan yang terinfeksi, atau perangkat yang terhubung ke jaringan [16] [17]. *Virtual Private Network* (VPN) adalah perangkat

lunak yang memungkinkan para pengguna untuk tersambung ke layanan internet secara pribadi. VPN memberikan akses secara aman melalui koneksi server dengan menyembunyikan jejak data pribadi pengguna.



Gambar 1. Ilustrasi Jaringan VPN

Ilustrasi jaringan VPN dapat dilihat pada Gambar 1. Layanan koneksi VPN memberikan keamanan pengguna saat akan mengakses website dengan mengubah jalur koneksi dengan server dan menyembunyikan pertukaran data [18].

A. Parameter Nilai Quality of Service (QoS)

Quality of Service merupakan mekanisme yang memberikan kemampuan seoranng admistrator jaringan untuk mengelola *bandwidth, delay, jitter, loss*, dan *congestion* dari *throughput* dalam sebuah jaringan. Sehingga dapat memberikan jaminan atas akses jaringan [19]. Penelitian ini melihat parameter *throughput* (bandwidth yang diterima) dan *packet loss* saat menentukan kualitas akses suatu jaringan. Nilai standar rekomendasi berdasar standar TIPHON TR 101 328 pada Tabel 1 dan Tabel 2 [20].

Tabel 1. Parameter *Throughput*

Kategori	Nilai	Indeks
Sangat Baik	>2,1 Mbps	4
Baik	1200 kbps – 2,1 Mps	3
Cukup	700 –1200 kbps	2
Buruk	<700 kbps	1

Tabel 2. Parameter Packet Loss

Kategori	Nilai
Sangat Baik	0%
Baik	3%
Cukup	15%
Buruk	25%

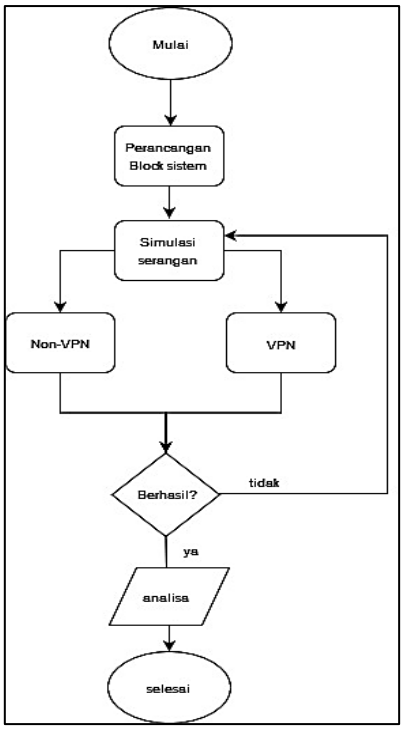
B. Metode Command and Control attack (C&C)

Serangan *command and control* (C&C), yang sering dikaitkan dengan botnet dan malware, telah banyak diteliti dalam bidang keamanan siber, terutama karena taktiknya yang terus berkembang dan sulitnya mendeteksi [21]. Studi menyoroti bahwa infrastruktur C&C digunakan oleh botmaster untuk berkomunikasi dengan perangkat yang terinfeksi (bot) guna menjalankan perintah untuk aktivitas seperti eksfiltrasi data, serangan DDoS, dan manipulasi sistem. Infrastruktur ini sering kali tersembunyi di dalam layanan atau platform *cloud* yang sah, sehingga pendeteksiannya menjadi lebih sulit [22].

III. RESEARCH METHOD

A. Alur Penelitian

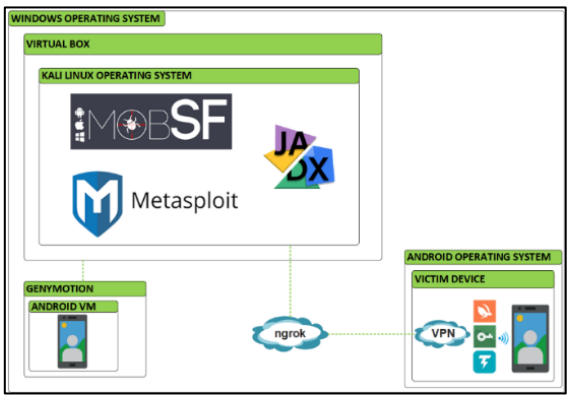
Diagram alir pada bagian ini merupakan penjelasan langkah-langkah dalam proses perancangan dan pengujian keamanan aplikasi Android dengan mempertimbangkan penggunaan VPN dan non-VPN. Proses ini bertujuan untuk menganalisis kelemahan serta risiko keamanan yang mungkin terjadi saat pengujian.



Gambar 2. Alir Penelitian

B. Merancang Sistem

Penelitian ini bertujuan untuk melakukan simulasi menggunakan *Mobile Security Framework* untuk menemukan kerentanan pada aplikasi. Gambar 2 menunjukkan proses kerja sistem pada penelitian ini yaitu *Genymotion* yang berfungsi untuk menginstal sistem operasi Android yang akan diintegrasikan dengan *VirtualBox*. Setelah sistem operasi diintegrasikan ke dalam *VirtualBox*, peneliti dapat menjalankan sistem operasi sebagai perangkat korban untuk mengetahui aktivitas akibat *Malware* pada aplikasi yang ingin dianalisis.



Gambar 3. Blok Sistem

VirtualBox juga memasang sistem operasi Kali Linux sebagai lingkungan lab untuk pengujian penetrasi. Semua *tools* pendukung terinstal di Kali Linux termasuk *framework* yang akan digunakan yaitu MobSF. *Mobile Security Framework* (MobSF) adalah alat *open-source* yang digunakan untuk menganalisis keamanan aplikasi *mobile*, baik untuk *platform* Android maupun iOS Jika sudah terinstall barulah analisa aplikasi dapat dilakukan. *Ngrok* berfungsi sebagai layanan yang akan melakukan tunneling agar perangkat korban dapat dikontrol meskipun tidak berada dalam satu jaringan dengan perangkat penyerang.

C. Konfigurasi Aplikasi

Penelitian ini menggunakan beberapa konfigurasi diantaranya:

a. Konfigurasi MobSF

Instalasi dan konfigurasi MobSF bertujuan untuk menjalankan service MobSF pada Kali Linux. Sehingga dapat melakukan analisis pada .APK file.

b. Konfigurasi ADB

Instalasi dan konfigurasi ADB bertujuan sebagai command line yang digunakan untuk komunikasi dengan perangkat. Perintah ADB memfasilitasi berbagai tindakan perangkat seperti: menginstal dan men-debug aplikasi, serta memberikan akses ke *shell unix* yang dapat digunakan untuk menjalankan berbagai perintah di perangkat.

c. Konfigurasi *Ngrok*

Instalasi dan konfigurasi *ngrok* bertujuan untuk membangun koneksi antara *local network* dengan internet.

d. Konfigurasi JADX

Instalasi dan konfigurasi JADX bertujuan untuk melakukan *reverse engineering* dengan membuka isi *directory* pada aplikasi dengan tujuan mendapatkan lokasi *command and control*.

D. Skenario

Berikut merupakan skenario pengujian aplikasi yang telah diklasifikasikan ke dalam beberapa indikator pengujian pada aplikasi yang terinfeksi malware untuk dapat dilakukan analisis. Berdasar Gambar 1, blok Sistem yang telah dibuat, digunakan metode C&C *Attack Analysis* melalui perangkat lunak Metasploit pada kondisi perangkat (*device*) target dengan kondisi tanpa VPN dan dengan VPN. Kemudian hasil performansi dari kualitas layanan aksesnya berdasarkan parameter throughput dan packet loss. VPN berfungsi untuk mengenkripsi koneksi internet sehingga data lebih sulit diakses oleh pihak ketiga. Pada perangkat tanpa VPN, data dapat lebih mudah disadap atau dicuri, sedangkan pada perangkat yang menggunakan VPN, serangan ini lebih sulit dilakukan, tetapi tetap memungkinkan jika ada celah lain.

Tabel 3. Skenario Pengujian

Jenis Serangan	Kondisi
sysinfo	Non VPN | VPN
dump_calllog	
dump_SMS	
geolocate	

Tabel 3 menampilkan jenis serangan yang akan disimulasikan yakni *sysinfo* (Informasi Sistem), *dump_calllog* (Ekstraksi Riwayat Panggilan), *dump*_SMS (Ekstraksi SMS) dan *geolocate* (Pelacakan Lokasi). Berdasarkan hasil pengujian, perbedaan antara kondisi NonVPN dan VPN akan menunjukkan efektivitas VPN dalam mengurangi keberhasilan serangan C&C. Jika serangan berhasil dalam kondisi NonVPN tetapi gagal atau terhambat dalam kondisi VPN, maka VPN dapat dianggap efektif sebagai langkah mitigasi keamanan. Sebaliknya, jika serangan tetap berhasil meskipun VPN diaktifkan, maka diperlukan langkah mitigasi tambahan untuk melindungi data pengguna. Hasil ini dapat digunakan untuk memberikan rekomendasi keamanan bagi pengguna Android agar lebih waspada terhadap serangan C&C dan mempertimbangkan penggunaan VPN sebagai salah satu langkah mitigasi.

IV. HASIL DAN PEMBAHASAN

Simulasi serangan dengan menggunakan Metasploit pada kondisi perangkat (*device*) korban tidak terinstal VPN dan menggunakan VPN dengan hasil performansinya.

A. Tanpa VPN

1. Serangan sysinfo

Command and Control (C&C) attack dapat berjalan 100% tanpa adanya blocking sehingga data atau informasi pribadi korban dapat diakuisisi oleh penyerang. Dalam kasus ini, tanpa penggunaan VPN, komunikasi antara perangkat korban dan server C&C yang dikendalikan penyerang berjalan sepenuhnya tanpa enkripsi tambahan, yang memungkinkan penyerang memiliki kontrol penuh terhadap perangkat tanpa hambatan. C&C attack ini umumnya digunakan untuk memanipulasi atau mencuri data dari perangkat korban. Hal ini dapat kita lihat pada gambar berikut:

```
meterpreter > sysinfo
Computer        : localhost
OS              : Android 13 - Linux 4.19.113-27114284 (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
```

Gambar 4. Sysinfo Analysis

Gambar 4 merupakan serangan yang dilakukan oleh penyerang dengan mengirimkan komen "*sysinfo*" pada meterpreter dengan tujuan untuk mengetahui detail informasi pada device korban yang meliputi computer name, operating system dan lain sebagainya. Serangan C&C *attack* dengan penggunaan payload seperti *Meterpreter* yang mengeksekusi perintah "sysinfo" adalah tahap awal dari serangan yang dapat berkembang menjadi intrusi penuh jika tidak terdeteksi. Tanpa perlindungan VPN, perangkat korban lebih rentan terhadap pengintaian data dan manipulasi.

2. Serangan dump_callog

Merupakan serangan yang dilakukan oleh penyerang dengan mengirimkan *command* "*dump_calllog*" pada meterpreter dengan tujuan untuk mengumpulkan log panggilan telepon korban. Pengambilan data riwayat panggilan melanggar privasi pengguna secara signifikan. Riwayat panggilan sering kali mencerminkan pola komunikasi pengguna, mengungkapkan siapa yang sering dihubungi, kapan mereka berkomunikasi, dan berapa lama. Data ini dapat digunakan untuk membangun profil korban secara lebih rinci, yang bisa disalahgunakan dalam berbagai skenario serangan sosial (*social engineering*). Informasi yang bisa didapatkan oleh penyerang seperti nomor yang sering dihubungi oleh korban (anak, ibu, ayah dan lain sebagainya). Kasus yang terjadi memungkinkan terjadinya penipuan mengatasnamakan korban. Gambar 5 merupakan hasil dari *dump_calllog* dengan menjalankan perintah ini, penyerang berhasil mengambil data riwayat panggilan (*call log*) dari perangkat korban.

```
meterpreter > dump_calllog
[*] Fetching 2 entries
[*] Call log saved to calllog_dump_20231201022847.txt
```

Gambar 5. Hasil *dump_calllog*

3. Serangan dump_SMS

Penyerang melakukan "*dump_sms*" pada meterpreter dengan tujuan untuk mengumpulkan log SMS korban. Gambar 6. memberikan hasil dumps_sms yang telah dilakukan oleh penyerang. Meterpreter sedang mengambil sebanyak 121 pesan SMS dari perangkat target. Ini menunjukkan jumlah pesan yang ditemukan di perangkat. Pesan SMS yang diambil telah disimpan dalam file teks bernama sms_dump_2023101023018.txt. File ini berisi seluruh pesan SMS yang berhasil diekstraksi dan dapat diakses untuk dianalisis lebih lanjut. Informasi yang bisa didapatkan oleh Penyerang seperti: kode OTP,

credential banking dan memungkinkan untuk melakukan *reset* password pada akun mobile banking korban ketika dilakukan kombinasi serangan menggunakan malware yang di *attach* pada aplikasi.

```
meterpreter > dump_sms
[*] Fetching 121 sms messages
[*] SMS messages saved to: sms_dump_20231201023018.txt
```

Gambar 6. Hasil *dump_sms*

4. Serangan Geolocate

Gambar 7 merupakan serangan yang dilakukan oleh Penyerang dengan mengirimkan *command* "*geolocate*" pada meterpreter dengan tujuan untuk mengetahui lokasi spesifik korban. Informasi yang bisa didapatkan oleh Penyerang seperti: *latitude* dan *longitude* serta link google maps yang mengarahkan langsung ke posisi korban. Terdapat tautan yang dapat dibuka untuk melihat lokasi tersebut secara langsung di google maps. Tautan ini memungkinkan pengambil data untuk menemukan alamat fisik atau lokasi spesifik perangkat berdasarkan koordinat yang diberikan. Mengakses lokasi fisik perangkat target dapat membantu dalam memahami keberadaan pengguna perangkat tersebut atau mengidentifikasi lokasi tempat perangkat itu berada.

```
meterpreter > geolocate
[*] Current Location:
        Latitude:  -6.1930296
        Longitude: 106.8481283

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=-6.1930296,106.8481283&sensor=true
```

Gambar 7. Geolocate Analysis

5. Kualitas QoS

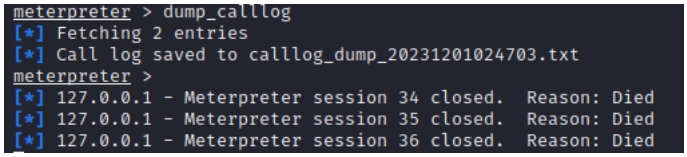
Pada saat perangkat korban terinfeksi malware, maka dilakukan uji kualitas jaringan internet. Berdasarkan hasil Gambar 8, dapat dilihat *speedtest* yang dilakukan dengan menggunakan *Internet Service Provider* (ISP) diperoleh hasil download 28 Mbps, upload 20,9 Mbps dan *packet loss* 0%. Hasil tersebut menunjukkan kualitas jaringan internet sangat baik menurut standar TIPHON.

Gambar 8. Hasil uji layanan

B. Menggunakan VPN

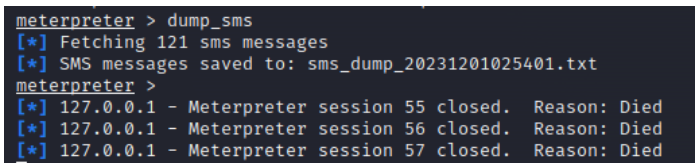
Simulasi serangan yang pada skenario kedua, yaitu: kondisi VPN on dan user menginstal *malicious application*. Simulasi serangan *command and control attack* mengalami kegagalan. Kegagalan ini

dikarenakan perbedaan segmentasi network yang terdapat pada device ketika telah terintal VPN. Konfigurasi VPN berhasil melakukan blocking terhadap serangan. Sehingga, *command and control attack* tidak dapat dilakukan. Kemudian melakukan uji kualitas layanan internet saat VPN "*on*" dan terinfeksi malicious pada perangkat.



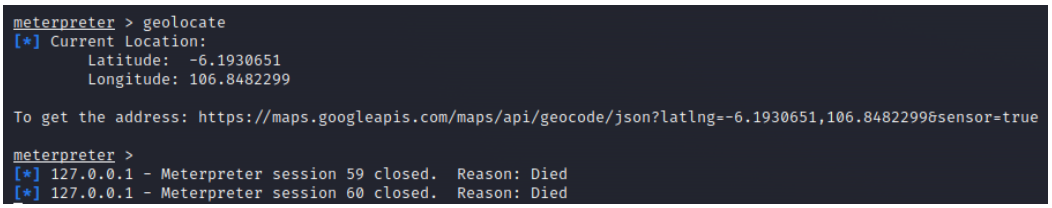
Gambar 9. Serangan *dump_calllog* saat VPN "*on*"

Dump_calllog adalah perintah yang digunakan di dalam *Meterpreter* untuk mengekstrak log panggilan dari perangkat target. Gambar 9 perintah berhasil dieksekusi, dan hasilnya menunjukkan bahwa dua entri (riwayat panggilan) telah diambil dan disimpan dalam file bernama "calllog_dump_20231201024703.txt". Data log panggilan dapat digunakan oleh penyerang untuk menganalisis kebiasaan komunikasi korban atau untuk mencari kontak penting yang dapat dimanfaatkan dalam serangan rekayasa sosial (*social engineering*). Saat reason : *died* menunjukkan VPN memiliki fitur proteksi tambahan yang memutus koneksi apabila aktivitas mencurigakan terdeteksi, meskipun fitur ini biasanya berfungsi lebih pada tingkat lalu lintas data dan bukan pada perangkat yang sudah berhasil diakses.



Gambar 10. Serangan *dump_sms* saat VPN "*on*"

Gambar 10 menjelaskan penggunaan VPN dapat mempengaruhi kestabilan koneksi dengan indikator reason *died* pada *Meterpreter*. Hal ini terjadi karena VPN mengenkripsi dan mengalihkan jalur koneksi yang menyebabkan latensi atau perubahan IP *address*, sehingga sesi eksploitasi menjadi tidak stabil atau bahkan terputus.



Gambar 11. Serangan *geolocate* saat VPN "*on*"

Selanjutnya Gambar 11 VPN berfungsi untuk menyamarkan alamat IP pengguna dan mengalihkan lalu lintas internet melalui server yang aman dan berlokasi di tempat lain, sehingga memungkinkan pengguna untuk terlihat seperti mengakses internet dari lokasi yang berbeda. Selain itu, status "*Reason: Died*" yang muncul pada sesi Meterpreter menunjukkan bahwa koneksi antara penyerang dan target tidak stabil dan terputus setelah informasi geolokasi diambil. Hal ini bisa disebabkan oleh VPN atau mekanisme keamanan lainnya yang mengakibatkan sesi Meterpreter menjadi tidak konsisten. Meskipun VPN tidak sepenuhnya menghalangi pelacakan lokasi, kehadirannya dapat membantu mengganggu stabilitas koneksi penyerang, sehingga mempersulit mereka untuk mempertahankan akses jangka panjang ke perangkat.

Gambar 12. Uji test koneksi saat VPN "*on*"

Uji hasil test dapat kita lihat pada Gambar 12. menunjukkan hasil download 26,3 Mbps, upload 17,7 Mbps dan packet loss 0%. Namun terdapat penurunan saat download dan upload saat VPN tidak aktif dan VPN aktif. Saat VPN diaktifkan, terjadi enkripsi data serta proses data harus melalui server VPN tambahan sebelum mencapai tujuan, yang dapat mempengaruhi kecepatan koneksi dan latensi. Berdasarkan hasil pengujian kualitas jaringan, kecepatan *download* mengalami penurunan sebesar 6,07% dan *upload* sebesar 15,31% saat VPN diaktifkan Jadi, penggunaan VPN pada pengujian kedua memberikan beban tambahan pada koneksi internet sehingga menyebabkan penurunan kecepatan rata-rata sekitar 10,7% dibandingkan saat VPN tidak aktif.

V. KESIMPULAN

Berdasarkan studi literatur dan simulasi untuk penelitian ini, dapat disimpulkan menggunakan VPN memang menambah perlindungan terhadap data dan privasi, seperti terlihat dari pembatasan hingga pemblokiran akses data sensitif. Namun, ini dapat berdampak negatif pada kualitas jaringan, terutama dampak penurunan kecepatan sekitar 10,7% dari uji tanpa VPN. Saat kebutuhan aplikasi yang membutuhkan performa jaringan tinggi, penggunaan VPN mungkin tidak ideal, namun untuk meningkatkan keamanan, VPN adalah solusi yang efektif.

ACKNOWLEDGMENT

Penulis ingin mengucapkan terimakasih kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Telkom University Kampus Purwokerto yang sudah memberikan pendanaan untuk penelitian internal ini.

REFERENSI

[1] StatCounter, "StatCounter GlobalStats," 2022. [Online]. [Accessed 2024].

[2] I. G. Adnyana, P. G. S. C. Nugraha and B. R. A. Nugroho, "Reverse Engineering for Static Analysis of Android Malware in Instant Messaging Apps," *Journal of Computer Networks, Architecture and High Performance Computing,* vol. 6, no. 3, p. 1460, 2024.

[3] B. A. Saputro, L. I. Alfitra and R. B. Oktaviaji, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *REPOSITOR,* vol. 2, no. 10, pp. 1331-337, 2020.

[4] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management," *Bulletin of Computer Science and Electrical Engineering,* vol. 1, no. 1, pp. 1-11, 2020.

[5] 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, 2023.

[6] A. R. Tambunan, T. Yuniati and Y. A. Setyoko, "Implementasi Static Analysis Dan Background Process Untuk Mendeteksi Malware Pada Aplikasi Android Dengan Mobile Security Framework," *LEDGER*, vol. 1, no. 2, 2022.

[7] I. Himawan, K. Septianzah and I. Setiadi, "Analisis Keamanan Informasi Malware Terhadap Aplikasi Apk Dengan Metode Static Analysis Menggunakan Mobsf," *JRKT (Jurnal Rekayasa Komputasi Terapan)* , vol. 2, no. 2, 2022.

[8] A. D. Pratama and A. Amiruddin, "Uji Keamanan Aplikasi ABC Milik Instansi XYZ Menggunakan OWASP Mobile Security Testing Guide," *Jurnal Info Kripto*, vol. 15, no. 3, pp. 113-122, 2021.

[9] F. A. Alviansyah and E. Ramadhani, "Implementasi Dynamic Application Security testing pada Aplikasi Berbasis Android," *Automata* , vol. 2, no. 1, 2021.

[10] CISCO, Introduction to Cybersecurity, CISCO, 2020.

[11] S. J, B. R and P. M, "Impact of Distributed Denial of Service Attacks on E-Commerce Platforms," *Journal of Cybersecurity Research*, vol. 12, no. 3, pp. 145-160, 2021.

[12] C. H and L. S, "Ransomware Attacks: Threats and Mitigation Strategies in Organizational Networks," *International Journal of Information Security*, vol. 8, no. 4, pp. 210-225, 2020.

[13] N. T, W. Y and Z. L, "Payload Injection Attacks in Android Applications: Detection and Prevention," *Mobile Security Journal*, vol. 5, no. 1, pp. 34-50, 2020.

[14] M. D, "Docker: Lightweight Linux Containers for Consistent Development and Deployment," *Linux Journal*, vol. 2, 2014.

[15] B. K and K. P, "Enhancing CLI Learning with Docker Environments," *Journal of Computer Education Research*, vol. 18, no. 3, pp. 56-70, 2021.

[16] V. A and S. R, "A Study on Malware Propagation Methods and Detection Techniques," *International Journal of Computer Applications*, vol. 112, no. 4, pp. 23-30, 2018.

[17] E. S. Alomari, R. R. Nuiaa, Z. A. A. Alyasseri, H. JasimMohammed, N. S. Sani, M. I. Esa and B. A. Musawi, "Malware Detection Using Deep Learning and Correlation-Based Feature Selection," *Symmetry*, vol. 15, pp. 1-21, 2023.

[18] B. Arifwidodo, "Mekanisme Keamanan Jaringan Menggunakan Protokol Wireguard Pada Jaringan Privat," *Journal of ICT*, vol. 5, no. 2, pp. 1-9, 2023.

[19] I. Suryani, L. Lindawati and I. Salamah, "Analisa QOS (Quality Of Service) Jaringan Internet Di Teknik Elektro Politeknik Negeri Sriwijaya," *IT Journal Research and Development (ITJRD)*, vol. 3, no. 1, pp. 32-42, 2018.

[20] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS," 1999. [Online]. Available: http://www.etsi.org.. [Accessed 2024].

[21] C. D. Xuan, L. V. Duong and T. V. Nikolaevich, "Detecting C&C Server in the APT Attack based on Network Traffic using Machine Learning," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, pp. 22-27, 202.

[22] L. Lu, Y. Feng and K. Sakurai, "C&C Session Detection Using Random Forest," in *IMCOM*, Beppu, Japan, 2017.