Pengamatan IP Cycling Pada VPN Menggunakan GRC Fingerprints dan DNSLeakTest

R. Agastya A.R., Justinus Andjarwirawan, Agustinus Noertjahyana
Program Studi Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) - 8417658
Email: agasardhitra@gmail.com, justin@petra.ac.id, agust@petra.ac.id

ABSTRAK

Semakin berkembangnya teknologi informasi pada era modern saat ini, maka kebutuhan akan informasi semakin meningkat pula. Dimana setiap individu membutuhkan informasi dalam waktu yang cepat dan akurat oleh sebab itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi internet yang cepat .

Banyak orang paranoid pada ide pemerintahan mencuri data pribadi mereka dan menggunakannya untuk kewenangan sendiri. Tujuan dari penelitian ini adalah untuk menentukan kelayakan dan kestabilan dari layanan VPN tertentu. Data akan diambil bada basis setiap jam selama 30(tiga-puluh) hari dari www.dnsleaktest.com dan www.grc.com/fingerprints.htm.

Hasilnya akan dilanjutkan ke Website Google Sheets yang telah diprogram untuk menerima IP, Hostname, ISP dan Country dari kode HTML halaman tersebut. VPN komersial adalah jaringan pribadi yang memungkinkan pengguna tampil seolah-olah mereka berada di jaringan lain. Namun bukan tanpa risiko, karena layanan tersebut mungkin tidak aman. Dari percobaan ini, kami menyimpulkan bahwa beberapa VPN memang tidak stabil untuk digunakan pada waktu tertentu.

Kata Kunci: IP, VPN, GRC Fingerprints, DNSLeaktest, Keamanan VPN, Sertifikat

ABSTRACT

As information technology has evolved within the modern era, the needs of information rises along with it. Where every individual need information quickly and accurately, a supporting medium must support it. One of these medium is fast internet.

Many are paranoid towards the idea of the government stealing their private information and using it for what they see fit. The objective of this research is to determine whether or not the stability of said VPN is of acceptable levels. The data will be taken hour-by-hour for 30(thirty) days from www.dnsleaktest.com and www.grc.com/fingerprints.htm.

The results will then be forwarded to the Google Sheets website that has been programmed to receive the IP, Hostname, ISP and Country tags from the source code from said page. Commercial VPNs are private networks that allow its users to appear to be connecting from another network. This is however not without risk, for those services may not be safe. In this experiment, we have concluded that some VPNs are unstable when used at certain times.

Keywords: *IP, VPN, GRC Fingerprints, DNSLeaktest, Keamanan VPN, Certificate*

1. PENDAHULUAN

Semakin berkembangnya teknologi informasi pada era modern saat ini, maka kebutuhan akan informasi semakin meningkat pula. Dimana setiap individu membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh sebab itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi internet yang cepat dan stabil. Banyak orang paranoid pada ide bahwa pemerintahan mencuri data pribadi mereka dan menggunakannya untuk kewenangan sendiri. Bahkan pada hari ini sekitar 72% warga indonesia masih khawatir tentang penyalah gunaan datanya. Karena itulah beberapa institusi membuat network pribadi dimana data tersebut dienkripsi dan diamankan. Versi pertama dari ini adalah server proxi, dan tidak lama setelah itu, muncul versi yang lebih aman dan adalah topik dari penelitian ini adalah keamanan VPN.

Pada jaman sekarang, banyak orang yang tidak ingin datanya digunakan akan menggunakan VPN. Tentu, ini berarti bahwa data mereka aman, tetapi berapa aman data tersebut sebenarnya? Walaupun data yang diparse melewati VPN memang dienkripsi, data header dapat dipakai pihak ketiga untuk mengetahui arah traffic pengguna-pengguna VPN tersebut, A.K.A Sniffing

Kita sebagai individu tidak dapat mengetahui apabila serangan tersebut terjadi. Packet akan menanyakan server untuk melakukan DNS Lookup. Walaupun ini terlihat aman, pihak ketiga mungkin dapat melakukan sniffing pada server yang terkompromi dan menkorelasikan pengguna dan website yang dikunjunginya, membuat tujuan anonimitas dari sebuah VPN, tidak berguna.

Pada Penelitian yang dilakukan oleh Khan[11] telah terbuat penelitian mengenai Ekosistem VPN Komersial, yang nantinya menjadi dasar dilakukannya penelitian ini. Tidak menutup kemungkinan pada penelitian lainnya yang dilakukan oleh Senarath[16] dilakukan penelitian yang extensif, tetapi tidak mencakup kestabilan dari keamanan tersebut pada jangka waktu yang panjang. Penelitian ini bertujuan untuk memeriksa satu sisi dari pertanyaan ini, yakni DNS Leak, pada waktu yang extensif.

2. LANDASAN TEORI

2.1 Virtual Private Network (VPN)

Sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Walaupun sebenarnya menggunakan jaringan milik publik. Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaannya.

• Confidentiality (Kerahasiaan)
Memiliki sistem kerja dengan mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan Anda menjadi lebih terjaga. Biarpun ada pihak yang

dapat menyadap data Anda yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah karena memang sudah diacak.

• Data Integrity (Keutuhan Data)
VPN memiliki teknologi yang dapat menjaga keutuhan data yang Anda kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

• Origin Authentication (Autentikasi Sumber)
Memiliki keunggulan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source data tersebut.

• Non-repudiation
Proteksi dari penyangkalan oleh satu satu dari entitas yang terlibat didalam sebuah komunikasi yang turut serta secara keseluruhan atau sebagian dari komunikasi yang sedang terjadi.

2.2 Virtual Machine (VM)

Sebuah mesin yang mempunyai dasar logika yang menggunakan pendekatan lapisan-lapisan (layers) dari sistem komputer. Sehingga sistem komputer dengan tersendiri dibangun atas lapisan-lapisan tersebut, mulai dari lapisan terendah sampai lapisan teratas. Yaitu perangkat keras (semua bagian fisik komputer), kernel (program untuk mengontrol disk dan sistem file, multi-tasking. loadbalancing, nenvorking dan security), dan sistem program (program yang membantu general user).

Kernel yang berada pada lapisan kedua ini, menggunakan instruksi perangkat keras untuk menciptakan seperangkat system call yang dapat digunakan oleh komponen-komponen pada level sistem program. Sistem program kemudian dapat menggunakan system call dan perangkat keras lainnya seolah-olah pada level yang sama Meskipun sistem program berada di level tertinggi namun program aplikasi bisa melihat segala sesuatu pada tingkatan dibawahnya seakan-akan mereka adalah bagian dari mesin

2.2.1 Aplikasi Oracle Virtualbox

Aplikasi Oracle Virtualbox Perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows. Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

2.3 Operating System (OS)

Software pada lapisan pertama yang ditempatkan pada memori komputer pada saat komputer dinyalakan. Sedangkan software-software lainnya dijalankan diatas Sistem Operasi, dan Sistem Operasi akan melakukan layanan inti umum untuk software-software itu. Layanan inti umum tersebut seperti akses ke disk, manajemen memori, skeduling task, dan antar-muka user. Sehingga masing-masing software tidak perlu lagi melakukan tugas-tugas inti umum tersebut, karena dapat dilayani dan dilakukan oleh Sistem Operasi. Bagian kode yang melakukan tugas-tugas inti dan umum tersebut dinamakan kernel[12].

Sistem yang terdiri atas berbagai komponen kerja dan metode kerja yang digunakan untuk memerintah serta menjalankan perangkat yang dimilikinya, agar sesuai dengan yang diinginkan. Fungsi utama dari sistem operasi ialah mengelola sumber daya yang ada pada komputer. Selain itu, sistem operasi juga berfungsi untuk menyediakan layanan ke pengguna, sehingga bisa lebih mudah saat memanfaatkan berbagai sumber daya computer[13].

2.4 OS Linux Ubuntu 20.04.1

Software sistem operasi open source gratis untuk disebarluaskan di bawah lisensi GNU. Sehingga anda diijinkan untuk menginstal pada komputer anda ataupun mengkopi dan menyebarluaskannya tanpa harus membayar. linux merupakan turunan dari unix dan dapat bekerja pada berbagai macam perangkat keras koputer mulai dari inter x86 sampai dengan RISC. Dengan lisensi GNU (Gnu Not Unix) Anda dapat memperoleh program, lengkap dengan kode sumbernya (source code). Tidak hanya itu, Anda diberikan hak untuk mengkopi sebanyak Anda mau, atau bahkan mengubah kode sumbernya. Dan itu semua legal dibawah lisensi. Meskipun gratis, lisensi GNU memperbolehkan pihak yang ingin menarik biaya untuk penggandaan maupun pengiriman program. Nama Ubuntu berasal dari filosofi dari Afrika Selatan yang berarti “kemanusiaan kepada sesama”.

Proyek Ubuntu resmi disponsori oleh Canonical Ltd. yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan Mark Shuttleworth[10]. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam filosofi Ubuntu ke dalam dunia perangkat lunak.

2.5 Aplikasi Browser Google Chrome

Sebuah aplikasi peramban yang digunakan untuk menjelajah dunia maya seperti halnya Firefox, Opera ataupun Microsoft Edge. Jika Firefox dikembangkan oleh Mozilla, Google Chrome dibuat dan dirancang oleh Google, perusahaan internet terbesar di dunia. Menurut Jubliee[6] Google Chrome “ Sebagai browser baru mempunyai fasilitas yang lumayan bagus sehingga mampu menarik perhatian pecinta dunia maya dari seluruh penjuru dunia “. Google Chrome merupakan mesin pencarian mampu melakukan penelusuran dalam waktu kurang dari beberapa detik dengan perangkat lunak yang telah diinstal ke dalam Sistem Operasi windows untuk memberikan pengguna aksesoris pendukung seperti mediator layanan browser, file manager, downloader dan lain-lain. Sebagai salah satu layanan software yang memungkinkan pengguna website menelusuri informasi, media video dan audio, serta data teknis Google Chrome tersedia dan sangat mendukung untuk semua Operasi Sistem Dektop hingga pengguna smartphone seperti Android dan Apple agar broswer menjadi terkendali untuk diterima, ditelususri, disimpan hingga digunakan sebaikbaiknya dalam dunia maya.

2.5.1 Google Chrome Extension

Merupakan salah satu fitur yang disediakan oleh Google Chrome untuk memudahkan para penggunanya untuk meningkatkan produktivitas. Browser extension yang memodifikasi Google Chrome browser. Browser extension ini ditulis dengan menggunakan teknologi web seperti HTML, JavaScript dan juga CSS. Google Chrome extension menyimpan informasinya di dalam sebuah file manifest yang disebut dengan manifest.json[1]. Informasi tersebut berupa source file apa saja yang akan difungsikan pada saat extension dijalankan. Arsitektur Google Chrome extension pada umumnya mempunyai sebuah background pages yang berfungsi untuk menyimpan logika utama, sebuah UI (User Interface) sebagai jembatan agar pengguna dapat berinteraksi dengan extension dan juga sebuah content script agar extension dapat berinteraksi dengan web pages. sebuah browser dengan dua extension yang terpasang. Icon dengan warna kuning adalah browser action sedangkan icon dengan warna biru

merupakan page action. Kedua action tersebut mempunyai satu background pages yang didefinisikan dalam background. html serta memiliki kode JavaScript yang mengatur perilaku kedua window. Persistent background pages akan selalu dijalankan pada saat extension aktif sedangan even pages hanya akan dijalankan pada saat dibutuhkan saja. Informasi untuk membedakan kedua tipe tersebut dituliskan pada file manifest dari extension yang bersangkutan.

2.6 Commercial VPN

Jaringan yang memungkinkan pengguna untuk mengirim dan menerima data di jaringan bersama atau publik seolah-olah perangkat komputasi mereka terhubung langsung ke jaringan pribadi yang dijual dan digunakan oleh public[7]. Layanan VPN komersial telah menjadi cara populer untuk mengamankan lalu lintas internet melalui port internet terenkripsi dan tidak terenkripsi. Penggunaan VPN sedang meningkat untuk industri dan konsumen[14]. Penting untuk memahami cara kerja teknologi VPN untuk mengoptimalkan keamanan dan fungsionalitas.

2.6.1 CyberGhost VPN

VPN dengan tingkat kemanan terbaik di antara VPN lainnya. Perbaikan yang terus menerus terbayarkan ketika CyberGhost ini mendapatkan penghargaan dari bestvpn.com sebagai penyedia VPN dengan nilai terbaik. VPN terbaik untuk Android untuk menyembunyikan alamat IP Anda, mengenkripsi koneksi internet Anda dengan server proxy yang aman, dan membuat Anda aman secara online[3]. Terbukti tanpa menyimpan log, dan lebih dari 36 juta orang di seluruh dunia mempercayai kami untuk melindungi privasi digital mereka.

Saat menggunakan VPN ini, dalam satu ketukan membuat semua yang Anda butuhkan untuk mendapatkan perlindungan internet instan dengan layanan VPN aman CyberGhost![4] Dan segala sesuatu tentang aplikasi VPN Android intuitif dan ramah pengguna. Dapatkan akses aman dari seluruh dunia. Jaringan pribadi virtual kami yang luas memiliki lebih dari 7.000 server VPN tercepat yang berlokasi di 90 negara. VPN CyberGhost mengarahkan lalu lintas Anda melalui terowongan VPN terenkripsi yang membuat akses Wi-Fi menjadi Wifi Aman.

2.6.2 Windscribe VPN

Seperangkat alat yang bekerja sama untuk memblok iklan dan web beacon, mengembalikan akses ke konten terblokir dan membantumu mengamankan privasi online. Windscribe VPN adalah alat yang mengamankan Wifi dan membantu Anda menjaga privasi saat online. Bagian terbaik? Ini benar-benar gratis untuk digunakan dan menawarkan bandwidth hingga 10GB per bulan, jika Anda memberikan alamat email yang dikonfirmasi. Itu adalah sesuatu yang benar-benar dapat anda gunakan.

Dengan Windscribe VPN, Anda tidak akan pernah dipusingkan dengan pengaturan dan menu opsi yang membingungkan lagi, hanya menyalakannya sekali dan melupakannya. Mendapatkan data hingga 10GB per bulan secara GRATIS, yang dapat Anda gunakan di iPhone, iPad, Mac, atau PC Windows, atau sebagai add-on browser untuk Chrome, Firefox, dan Opera.

2.7 Man-In-The-Middle Attack

Salah satu serangan pada jaringan dengan akses terbuka. Man-in-the-middle attacks merupakan serangan yang pada dasarnya penyerang memasukkan dirinya di antara dua pihak atau perangkat dalam mode sembunyi-sembunyi sehingga semua paket yang berlintas antara kedua pihak yang sah itu dialihkan melalui penyerang tersebut[2]. Serangan ini cukup berbahaya karena penyerang kemudian dapat mengubah informasi dari paket yang dikirimkan, dan berpotensi mengirim data yang dipalsukan ke salah satu pihak[8]. Ada dua bentuk jenis a man in the middle attack. Pertama yang melibatkan kedekatan fisik dengan sasaran yang dituju dan yang kedua hanya melibatkan malware yang dikenal sebagai serangan man in the browser (MITB).

Dengan serangan MITM tradisional, penyerang perlu memiliki akses ke router WiFi yang tidak aman atau yang kurang aman. Jenis koneksi ini umumnya ditemukan di tempat umum dengan WiFi hotspot dan bahkan di rumah. Penyerang akan memindai router dengan menggunakan kode untuk mencari kelemahan tertentu seperti setting standar atau menggunakan password yang buruk atau lubang keamanan karena adanya konfigurasi router yang lemah. Setelah penyerang menemukan kerentanan, mereka kemudian akan memasukkan alat-alat mereka di antara komputer pengguna dan situs yang dikunjungi pengguna.

Versi kedua dari serangan MITM adalah MITB yang telah meraih popularitas dari para kriminal dunia maya karena kemudahan eksekusi[5]. Dengan serangan man in the-browser penyerang hanya perlu untuk menyuntikkan malware ke dalam komputer yang kemudian akan menginstal sendiri ke dalam browser tanpa sepengetahuan pengguna dan kemudian akan mencatat data yang sedang dikirim antara korban dan situs yang khusus ditargetkan, seperti lembaga keuangan yang telah dikodekan ke dalam malware.

2.8 DNS Leak

DNS Leak (kebocoran DNS) adalah bahwa komunikasi antara user dan penyedia DNS, untuk menentukan IP Adress dari nama host yang diinginkan (query DNS), sedang menuju ke arah server DNS lain, yang tidak dikenal[9]. Sebagian besar DNS Leak adalah kebocoran query sebagian, artinya sebagian dari queri DNS user menuju ke penyedia DNS yang dinginkan dan sisanya menuju ke tempat yang tidak diinginkan.

DNS Leak dapat menyebabkan masalah terhadap privacy, karena query tersebut akan meninggalkan riwayat penjelajahan user pada penyedia DNS. Semua Penyedia DNS mengetahui situs mana yang akan user kunjungi, bahkan sebelum user dapat mengunjunginya. Resolver juga mengetahui IP Adress user berdasarkan lokasi IP Address. Wilayah, waktu, tanggal adalah bagian dari queri. Fakta ini mengarah pada implikasi privasi utama bagi user. Penyedia DNS dapat melakukannya jika mereka ingin mencatat tanggal, waktu, zona waktu, IP, GeoIP, situs web dan menyimpannya untuk dijual, dianalisis atau digunakan untuk melakukan penipuan.

2.9 GRC Fingerprint

Merupakan akronim dari Governance, Risk, dan Compliance (Tata kelola, Risiko, dan Kepatuhan). Penggunaan akronim tersebut memang terkesan sangat sederhana, namun sebenarnya GRC dan implementasinya memiliki cakupan yang sangat luas.

3. ANALISA DAN DESAIN SISTEM

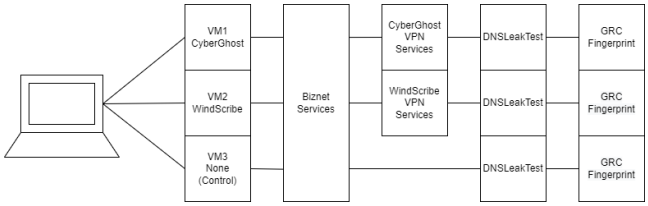
3.1 Analisa Sistem

Serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat, serta mengelolah bahan penelitian. Menurut Danial & Warsiah[15] studi literatur merupakan penelitian yang dilakukan oleh peneliti dengan mengumpulkan sejumlah buku buku, majalah yang berkaitan dengan masalah dan tujuan penelitian. Teknik ini dilakukan dengan tujuan untuk mengungkapkan berbagai teori-teori yang relevan dengan permasalahan yang sedang dihadapi

ataupun diteliti sebagai bahan rujukan dalam pembahasan hasil penelitian. Penelitian yang dilakukan oleh peneliti dengan mengumpulkan sejumlah buku buku, majalah yang berkaitan dengan masalah dan tujuan penelitian. Referensi ini dapat dicari dari buku, jurnal, artikel laporan penelitian, dan situs-situs di internet. Output dari studi literatur ini adalah terkoleksinya referensi yang relefan dengan perumusan masalah.

3.2 Desain Sistem

Pada sub bab ini akan menjelaskan mengenai flowchart dari Alur pengambilan data untuk menguji keaman vpn melalui aplikasi vm yang digunakan serta flowchart cara kerja menguji pengambilan data dari metodologi yang digunakan untuk menjalankan pengamatan ini.

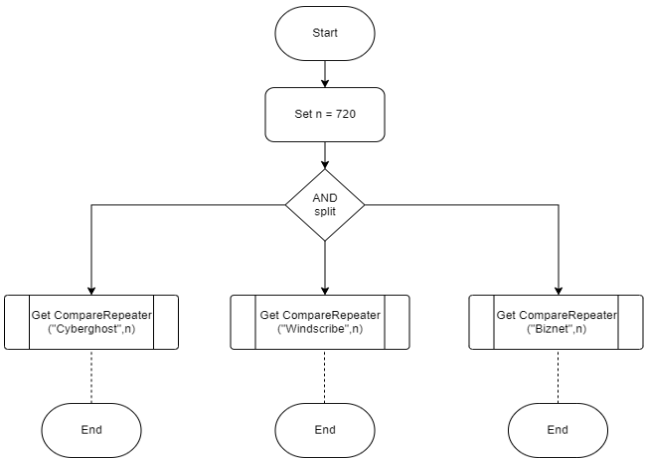


Gambar 1. Cara Kerja Pengambilan Data

Gambar 1 menjelaskan cara kerja pengambilan data. Pengambilan data dimulai dari computer yang telah diinstall VMware dan menjalankan 3 Virtual Machine (VM). Masing-masing VM kemudian menjalankan google chrome masing-masing. Pada Google Chrome tersebut diinstall kemudian dinyalakan Chrome Extension VPN. VM1 menggunakan CyberGhost VPN, VM2 menggunakan Windscribe VPN, VM3 tidak menggunakan VPN dan bertindak sebagai Control. Masing-masing VM tersebut kemudian menyambung ke provider internet, Biznet di kasus ini. Kemudian masing-masing mengakses DNSLeakTest untuk mengabil data IP. Kemudian mengakses GRC Fingerprint untuk mengambil data Sertifikat.

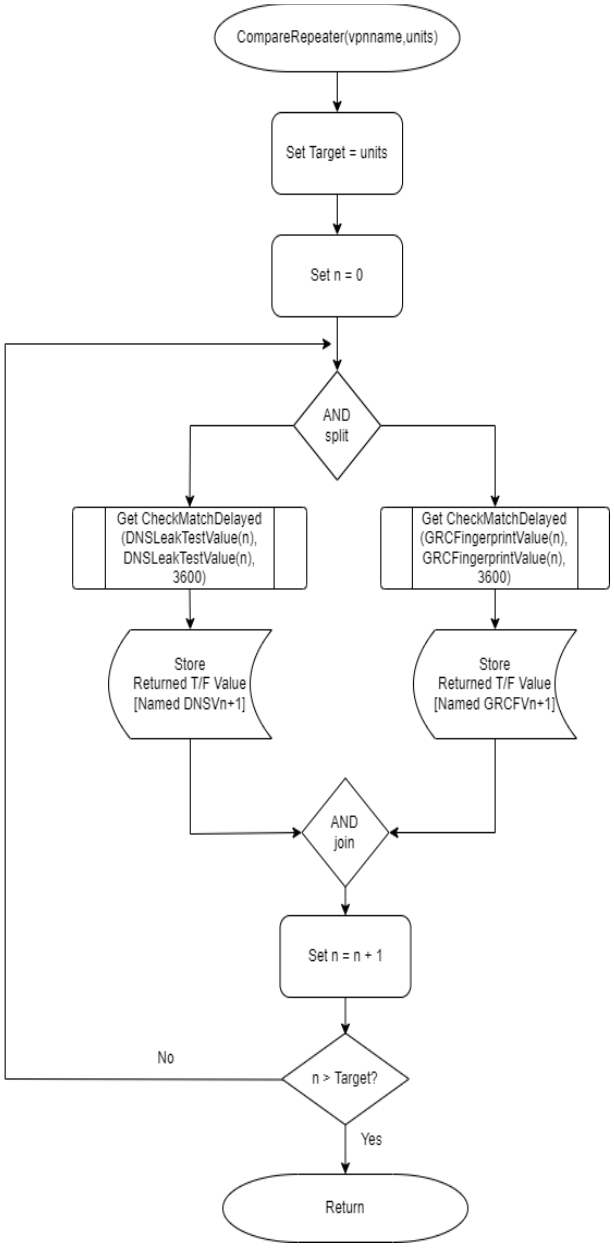
4. IMPLEMENTASI SISTEM

Bab ini akan membahas mengenai implementasi sistem sesuai dengan analisa dan desain pada bab sebelumnya. Implementasi yang dibahas mencakup perangkaian lingkungan untuk Virutal Machine (VM) dan langkah-langkah pengambilan data.



Gambar 2. Flowchart Metodologi Bagian 1

Pada Gambar 2 ditunjukkan secara umum bagaimana data akan diproses. Pada Start adalah dimana program dimulai. Dibawahnya berada Set n = 720 (tujuh-ratus dua-puluh) yang menyatakan bahwa program akan berjalan sepanjang 720 (tujuh-ratus dua-puluh) jam. 720 (tujuh-ratus dua-puluh) jam terangkai dari 24 (dua-puluh empat) jam x 30 (tiga-puluh) hari. Dibawanya berada decision gate AND, yang berarti program akan dibelah tiga dan proses selanjutnya akan dilakukan secara bersamaan. Kemudian beradanya SubRoutine Get CompareRepeater yang akan memroses data lebih lanjut pada Gambar 3. SubRoutine ini menerima dua input. Input pertama akan menunjukkan nama network VPN yang akan diperiksa, Sedangkan input kedua, yang menerima bilangan bulat positif (positive integer), menentukan berapa kali putaran sebelum program berhenti memproses.



Gambar 3. Flowchart Metodologi Bagian 2

Pada Gambar 3 ditunjukkan cara kerja Routine CompareRepeater. CompareRepeater ini menerima dua input. Input pertama menunjukkan nama network VPN yang akan diperiksa, yang memiliki nilai "vpnname" sebagai nilai sementara. Input kedua, yang menerima bilangan bulat positif (positive integer), akan menentukan untuk berapa kali putaran sebelum program akan berhenti memproses. Nilai sementara untuk variable ini adalah units.

Pada tahap selanjutnya berada nilai Target, akan diisi oleh nilai yang diisi pada Gambar 2 menurut jalurnya. Selanjutnya nilai n, yang akan diisi oleh nilai 0(nol) sebagai titik mulai program. Kemudian program akan dilalui decision gate AND yang memparalelkan program menjadi 2(dua) proses.

Pada proses kiri berada SubRoutine Get CheckMatch yang bertugas untuk membandingkan 3(tiga) input. Input pertama tersebut adalah "DNSLeakTestValue" yang menunjukkan array alamat IP sesuai pada Tabel 1. Pada Input kedua beradanya array alamat IP yang juga bernama "DNSLeakTestValue" juga menunjukkan array alamat IP sesuai pada Tabel 1. Pada input ketiga berada nilai dimana program akan menunggu selama waktu yang tertera pada Gambar 3. Dalam konteks ini, nilai yang dimasukkan adalah 3600. Nilai tesebut adalah hitungan waktu detik dalam waktu 1(satu) jam.

Setelah proses tersebut data tersebut akan disimpan pada dokumen Google Sheets. Data yang disimpan akan memiliki hasil True, Yaitu benar dan False, Yaitu salah. Pernyataan tersebut akan digunakan untuk menentukan pertanyaan "Apakah IP telah berubah setelah 1(satu) jam telah terlampau?"

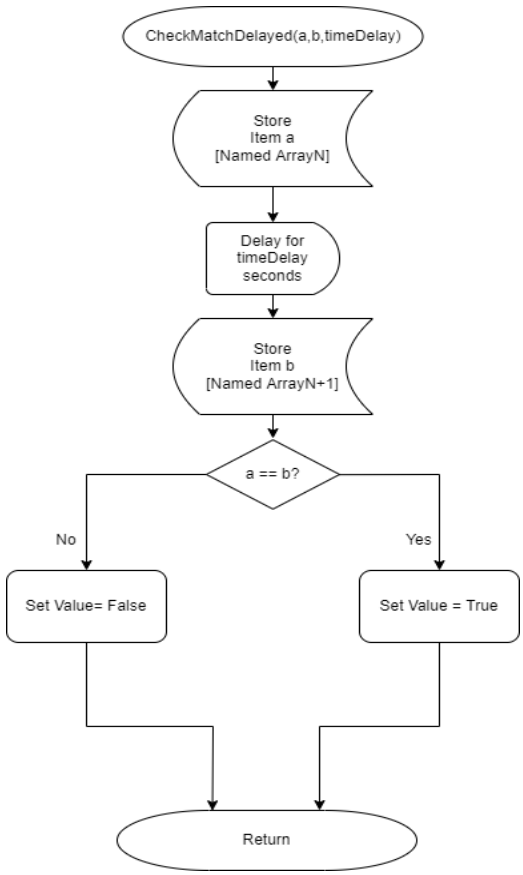
Pada proses kanan berada SubRoutine Get CheckMatchDelayed yang bertugas untuk membandingkan 3(tiga) input. Input pertama tersebut adalah "GRCFingprintValue" yang menunjukkan array Fingerprint website sesuai pada Tabel 2. Pada Input kedua beradanya array alamat IP yang juga bernama "DNSLeakTestValue" juga menunjukkan array Fingerprint website sesuai pada Tabel 2. Pada input ketiga berada nilai dimana program akan menunggu selama waktu yang tertera pada Tabel 3. Dalam konteks ini, nilai yang dimasukkan adalah 3600. Nilai tesebut adalah hitungan waktu detik dalam waktu 1(satu) jam.

Setelah proses tersebut data tersebut akan disimpan pada dokumen Google Sheets. Data yang disimpan akan memiliki hasil True, Yaitu benar dan False, Yaitu salah. Pernyataan tersebut akan digunakan untuk menentukan pertanyaan "Apakah Fingerprint website telah berubah setelah 1(satu) jam telah terlampau?"

Proses selanjutnya adalah decision gate AND yang bertujuan menyatukan proses DNSLeakTest dan GRC Fingerprint, menggabungkan kedua proses kembali menjadi 1(satu).

Pada proses berikutnya berada Set n = n + 1. Pertama nilai n akan diambil dan ditambahkan dengan nomer 1(satu). Nilai baru tersebut akan kemudian disimpan kembali ke n, menambahkan jumlah lalu yang n menjadi n+1. Proses ini berfungsi untuk menambahkan penghitung berapa kali program telah berulang.

Kemudian pada proses selanjutnya berada proses n > Target. Proses ini bertugas untuk memeriksa apakah nilai n telah melampaui nilai yang tertera di Target. Jika nilai tersebut belum terlampaui, maka program akan memulai lagi dari antara Set n = 0 dan AND split. Tujuan dari proses ini untuk memastikan bahwa proses berakhir setelah nilai Target terlampaui, yang menurut konteks pada Gambar 2 adalah 720(tujuh-ratus dua-puluh). Setelah proses ini selesai program akan kembali pada Gambar 2.



Gambar 4. Flowchart Metodologi Bagian 3

Pada Gambar 4 tertunjukkan cara kerja Routine CheckMatchDelayed. Routine CheckMatchDelayed menerima 3(tiga) nilai, yaitu nilai a, nilai b, dan nilai bilangan bulat (integer) yang sementara bernama "TimeDelay". Nilai a dan nilai b menerima rangkaian kata yang disebut array, sedangakan nilai "TimeDelay" menerima integer. Tujuan dari Routine ini adalah untuk mengambil suatu data dan data sama yang setelah waktu pada "TimeDelay" telah terlampau. Data kemudian dibandingkan untuk kesamaannya, yang lalu dikirim kembali ke Gambar 3.

Pada proses pertama beradanya Get Item a. Get Item a akan menerima nilai yang dikirmkan dari Gambar 3, dalam kasus Gambar 3, berbentuk rangkaian data Array dan menyimpannya pada Google Sheets sementara bernama "ArrayN".

Kemudian proses selanjutnya menghentikan program secara sementara. Program akan melanjutkan ke proses selanjutnya setelah waktu telah lewat nilai yang tertera pada "TimeDelay" pada Gambar 3. Tujuan penungguan program ini adalah untuk mengambil data yang mungkin berubah pada waktu yang mendatang. Pada skenario 3, ditunjukkan waktu ini adalah 3600(tiga-ribu enam-ratus) detik atau 1(satu) jam.

Setelah itu beradanya Get Item b. Get Item b akan menerima nilai yang dikirmkan dari Gambar 3, dalam kasus Gambar 3, berbentuk rangkaian data Array dan menyimpannya pada Google Sheets sementara bernama "ArrayN+1".

Pada proses selanjutnya berada decision gate yang berkondisi a == b. a == b adalah argument dimana ditanyakan apakah nilai a sama dengan nilai b. Jika kondisi ini benar, maka nilai true akan disimpan pada tempat “Value”. Jika nilai a dan b tidak sama, maka nilai false akan tersimpan pada tempat “Value”. Nilai “Value” kemudian dikembalikan kepada SubRoutine-nya pada Gambar 3.

4.1 Implementasi Sistem

Pada sub bab ini akan menjelaskan mengenai proses installasi dari Vm dan pengujian dari DNSlLeakTest dan GRCFingerprint serta mekanisme program dari CyberGhost VPN, dan DNSLeakTest.

5. HASIL PENGUJIAN

Pada bab ini akan membahas mengenai hasil pengambilan data dari VPN Pada Virtual Machine 1(VM1) (CyberGhost), VM2(Windscribe), dan VM3(None/Control).

5.1 Pengujian Sistem

Pada sub bab ini akan menjelaskan mengenai hasil analisa dari pengujian dari vpn cyberghost, windscribe serta No VPN pada tahapan ini ada beberapa tahapan pengujian seperti dari pengecekan IP ,ISP dan Negara yang mengakses vpn tersebut. Dan table setelahnya untuk memeriksa kesamaan Fingerprintnya.

5.1.1 Pengujian Cyberghost

Pada sub bab ini akan membahas mengenai hasil pengujian dari vpn cyberghost ini dan pada pengujian ini dilaksanakan dan dibuat berdasarkan tanggal dan waktu. Waktu dimana tidak ada perubahan tidak tercatat.

Tabel 1. Tabel Pengujian DNSLeakTest CyberGhost

DNSLeakTest						
IP	Hostname	ISP	Country	Date	Time	Value
193.176.84.15	None	M247 Ltd	Burcharest,Romani	01/03/2022	00:10:56	TRUE
193.176.84.15	None	M247 Ltd	Burcharest,Romani	31/03/2022	23:10:56	TRUE

Tabel 2. Tabel Pengujian GRC Fingerprints CyberGhost

GRC Fingerprint			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	01/03/2022	00:11:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
08:D3:BB:A5:FA:E0:4D:95:84:B1:BD:D7:DF:28:99:22:B9:B8:CB:86	04/03/2022	11:11:56	FALSE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
No			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	04/03/2022	12:11:56	FALSE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	04/03/2022	13:11:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	31/03/2022	23:11:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			

Pada Tabel 1, DNS Leak test menunjukkan bahwa Fingerprint tidak melakukan IP Cycling, yang menunjukkan bahwa Cyberghost melakukan perubahan network sebanyak 2(dua) kali pada jangka waktu 30(tiga-puluh) hari.

Pada Tabel 2, GRC Fingerprint menunjukkan bahwa fingerprint berubah 2 kali, yang menunjukkan bahwa Cyberghost melakukan perubahan sertifikat sebanyak 2(dua) kali pada jangka waktu 30(tiga-puluh) hari.

5.1.2 Pengujian Windscribe

Pada sub bab ini membahas mengenai Chrome yang menggunakan Windscribe sebagai VPNnya. Waktu dimana tidak ada perubahan tidak tercatat.

Tabel 3. Tabel Pengujian DNSLeakTest WindScribe

DNSLeakTest						
IP	Hostname	ISP	Country	Date	Time	Value
146.70.97.226	None	M247 Ltd	Burcharest,Romani	01/03/2022	00:16:56	TRUE
89.46.103.226	mx-pool226.jvlists.com	M247 Ltd	Russian Federation	04/03/2022	14:16:56	FALSE
146.70.97.226	None	M247 Ltd	Burcharest,Romani	04/03/2022	15:16:56	FALSE
146.70.97.227	None	M247 Ltd	Burcharest,Romani	04/03/2022	16:16:56	TRUE
185.217.68.13(	None	M247 Ltd	Burcharest,Romani	26/03/2022	14:16:56	FALSE
185.217.68.13(	None	M247 Ltd	Burcharest,Romani	26/03/2022	15:16:56	TRUE
185.217.68.13(	None	M247 Ltd	Burcharest,Romani	31/03/2022	23:16:56	TRUE

Tabel 4. Tabel Pengujian GRC Fingerprints WindScribe

GRC Fingerprint			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	01/03/2022	00:17:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
08:D3:BB:A5:FA:E0:4D:95:84:B1:BD:D7:DF:28:99:22:B9:B8:CB:86	24/03/2022	18:17:56	FALSE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
No			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	24/03/2022	19:17:56	FALSE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	24/03/2022	19:17:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	31/03/2022	23:17:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			

Pada Tabel 3, DnsLeakTest menunjukkan Windscribe memiliki 2(dua) perubahan IP, yang menunjukkan bahwa Cyberghost melakukan perubahan network sebanyak 2(dua) kali pada jangka waktu 30(tiga-puluh) hari

Pada Tabel 4, GRC Fingerprint menunjukkan Windscribe memiliki 2 perubahan Fingerprint, yang menunjukkan bahwa Cyberghost melakukan perubahan sertifikat sebanyak 2(dua) kali pada jangka waktu 30(tiga-puluh) hari.

5.1.3 Pengujian Control

Pada sub bab ini membahas mengenai hasil dari Virtual Machine yang tidak meneggunakan VPN. Waktu dimana tidak ada perubahan tidak tercatat.

Tabel 5. Tabel Pengujian DNSLeakTest Control

DNSLeakTest						
IP	Hostname	ISP	Country	Date	Time	Value
117.102.76.134	None	Biznet Network	Surabaya, Indones	01/03/2022	00:22:56	TRUE
117.102.76.134	None	Biznet Network	Surabaya, Indones	05/03/2022	21:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	01/03/2022	22:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	01/03/2022	23:22:56	TRUE
117.102.76.162	None	Biznet Network	Surabaya, Indones	22/03/2022	15:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	22/03/2022	16:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	22/03/2022	16:22:56	TRUE
117.102.76.134	None	Biznet Network	Surabaya, Indones	23/03/2022	18:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	23/03/2022	19:22:56	TRUE
117.102.76.162	None	Biznet Network	Surabaya, Indones	24/03/2022	22:22:56	FALSE
117.102.76.162	None	Biznet Network	Surabaya, Indones	24/03/2022	23:22:56	TRUE
117.102.76.134	None	Biznet Network	Surabaya, Indones	31/03/2022	21:22:56	FALSE
117.102.76.134	None	Biznet Network	Surabaya, Indones	31/03/2022	22:22:56	TRUE
117.102.76.134	None	Biznet Network	Surabaya, Indones	31/03/2022	23:22:56	TRUE

Tabel 6. Tabel Pengujian GRC Fingerprint Control

GRC Fingerprint			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	01/03/2022	00:23:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			
Chrome Fingerprint	Date	Time	Value
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9	31/03/2022	23:23:56	TRUE
GRC Fingerprint			
3D:EC:16:F4:DC:E1:C7:36:82:10:58:9B:7D:AB:E4:DB:32:F9:6B:B9			
Match?			
Yes			

Pada Tabel 5, Dapat dilihat bahwa IP berubah sebanyak 3 kali, yang menunjukkan bahwa Cyberghost melakukan perubahan network sebanyak 3(tiga) kali pada jangka waktu 30(tiga-puluh) hari

Pada Tabel 6, Fingerprint Biznet tidak mencycle, menyatakan tidak ada perubahan sertifikat.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Dari penelitian yang telah dilakukan, maka kesimpulan yang dapat diambil adalah sebagai berikut:

6.1.1 CyberGhost

DNS Leak test menunjukkan bahwa Fingerprint tidak melakukan IP Cycling, menunjukkan bahwa kelancaran dari VPN dapat ditentukan sebagai lancar. GRC Fingerprint menunjukkan bahwa fingerprint berubah 2(dua) kali. Fakta ini menentukan bahwa mesin yang menjalankan layanan VPN ini telah berubah 2(dua) kali.

6.1.2 Windscribe

DnsLeakTest menunjukkan Windscribe memiliki 2(dua) perubahan IP. Dengan ini dinyatakan bahwa IP range pada VPN ini tidak stabil dan dapat mempengaruhi kestabilan. GRC Fingerprint menunjukkan Windscribe memiliki 2(dua) perubahan Fingerprint. Perubahan tersebut menandakan bahwa mesin yang digunakan sebagai layanan VPN berubah 2 kali.

6.1.3 Biznet(Control)

Dapat dilihat bahwa IP berubah sebanyak 5(Lima) kali. Dengan in dapat dinyatakan bahwa network VPN ini memiliki routing banyak yang berarti kestabilan saluran akan terdampak. Fingerprint selama waktu penelitian tidak berubah. Dengan ini dapat dinyatakan bawah keaslian website dinyatakan.

6.2 Saran

Seiring dengan melesatnya perkembangan Tehnologi Informasi pada saat ini, dan meningkatnya kebutuhan akan jaringan alternatif dalam mengakses data, diperlukan penelitian lebih lanjut terhadap informasi keamanan VPN lain, di masa sekarang maupun yang akan datang.

7. REFERENSI

[1] Agustinus Raharjo, Hendry, Ramos Somya. "Perancangan dan Implementasi File Sharing Extension Pada Browser Google Chrome." Artikel Ilmiah (2012).

[2] backup_8a418a1e6ea10f17. Apa dan Bagaimana A Man In The Middle Attack? 6 Maret 2015. 21 September 2021.

[3] CyberGhost SA Dionisie. VPN by CyberGhost - Fast & Secure WiFi Protection. Bucharest, Romania, 13 September 2021.

[4] CyberGhostVPN. CyberGhost. Bucharest, Romania, 2011.

[5] Dedi Irawan, Fatoni. "Penerapan IP Security pada Jaringan VPN Site to Site di PT. Pertamina Ubeb Adera Pengabuan." (n.d.).

[6] fathurhoho. Optimalkan Google Chrome dengan Extension. 4 April 2016. 21 September 2021.

[7] Galang. Fungsi, Cara Kerja dan Apakah VPN. 2021. 21 September 2021.

[8] Herru Hardiyansah, S.Kom. Keamanan Komputer dan Jaringan. 7 Desember 2017. 21 September 2021.

[9] IRAWAN AFRIANTO, EKO BUDI SETIAWAN. "Kajian virtual private network (vpn) sebagai sistem pengamanan data pada jaringan komputer (studi kasus jaringan komputer unikom)." Majalah Ilmiah UNIKOM (2015): 44-45.

[10] Kadek Jeny Femila Devi, I Ketut Resika Arthana, I Gede Mahendra Darmawiguna. "Pengembangan Distribusi Luxpati Berbasis Ubuntu Sebagai Penunjang Proses Belajar Mengajar di Jurusan Pendidikan Teknik Informatika." Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI) (2015): 2087-2658.

[11] Khan, Mohammad Taha, et al. "An empirical analysis of the commercial vpn ecosystem." Proceedings of the Internet Measurement Conference 2018. 2018.

[12] Kompas.com. Sistem Operasi Komputer: Pengertian, Fungsi, Jenis, Cara Kerja, dan Contohnya. 15 April 2021. 21 September 2021.

[13] Listyorini, Tri. "NETWORKING OPERATING SYSTEM (NOS) BERBASIS SIMULASI." Jurnal SIMETRIS, Vol. 9 (2018): 2252-4983.

[14] Maharani, Fitri Latifah. "Penerapan Teknologi Virtual Private Network." Indonesian Journal on Networking and Security - Volume 7 No 2 (2017): 2354-6654.

[15] Nurul Hidayah. "Nurul Hidayah, Sulfahmi, Iani Zairani, Marwah Yusuf, Sufiati." COMBINE ASSURANCE DALAM KONTEKS PENGENDALIAN (2019): 32-37.

[16] Senarath, A. and Arachchilage, N.A.G. Why Developers Cannot Embed Privacy into Software Systems? Conference on Evaluation and Assessment in Software Engineering - EASE, ACM (2018), 211–216.