Mendalami Onion Network dengan TOR

M Rizqi R
20051204034
Teknik Informatika 2020 B
Universitas Negeri Surabaya

Alfito Mulyono
20051204038
Teknik Informatika 2020 B
Universitas Negeri Surabaya

March 5, 2022

I Pendahuluan

1.1 Latar Belakang

Bocornya informasi pengguna internet memiliki dampak yang merugikan. Banyak sekali pihak yang ingin mencuri data kita untuk dimanfaatkan dalam kepentingan mereka pribadi. Mereka akan menjual data kita kepada pihak-pihak yang menginginkan data kita.

Kita dapat mengambil contoh dari sebuah perusahaan media sosial ternama seperti Facebook. Pada 19 Desember 2018, Facebook diketahui telah membocorkan 1,5 miliar data pengguna Facebook dan menjualnya kepada pihak ketiga. Mark Zuckerberd, pendiri Facebook dinyatakan bersalah dalam persidangan dan dijatuhi denda sesuai keputusan hakim.

Namun kebocoran data bisa juga terjadi karena kesalahan pengguna. Pengguna kerap mengunjungi situs-situs acak kemudian tanpa sengaja menekan iklan yang muncul dalam situs tersebut. Kemudian pengguna tanpa sadar telah mengunduh perangkat lunak yang berisi virus yang kemudian berjalan dibelakang layar. Virus ini dapat berupa berbagai jenis perangkat lunak yang dapat menginfeksi perangkat pengguna.

Ada pula virus yang bahkan bisa digunakan untuk melacak setiap jengkal aktivitas pengguna. Baik itu dari ketikan keyboard, lokasi, bahkan mampu memanipulasi berkas digital yang dimiliki oleh pengguna hingga bisa mencuri berkas tersebut.

Maka dari itu diperlukan cara agar kita terhindar dari kejahatan internet tersebut. Salah satunya ialah memilih alat penjelajah web (*web browser*) yang tepat. Web browser yang tidak melacak kita saat menjelajah internet dan mencegah situs-situs berbahaya melacak dan mencuri data kita.

1.2 Rumusan Masalah

Adapun rumusan masalah pada pemaparan ini adalah:

1. Apa yang dimaksud dengan keamanan internet?
2. Bagaimana mencegah diri dari *cyber crime*?
3. Bagaimana menggunakan TOR sebagai media penjelajah yang aman?

1.3 Tujuan

Berdasarkan latar belakang yang telah dipaparkan. Tujuan makalah ini adalah untuk memberikan wawasan tentang *web browser* yang fokus pada privasi dan keamanan pengguna. Maka dari itu, tujuan spesifik dari makalah berikut adalah sebagai berikut:

1. Membuat pembaca mengerti tentang pentingnya *cyber security.*
2. Membuat pembaca memahami cara mengamankan dirinya dari kebocoran dan pencurian data.
3. Membuat pembaca memahami konsep *Cyber Security, VPN, proxy, TOR Network.*
4. Membuat pembaca memahami cara menggunakan *TOR Network.*

II Pembahasan

2.1 Cyber Security

Adalah istilah yang digunakan untuk metode pengamanan data baik pribadi maupun publik dalam jaringan internet. Metode *cyber security* dirancang untuk melawan ancaman terhadap sistem jaringan dan aplikasi, baik itu serangan yang berasal dari dalam maupun luar sistem.

2.2 VPN

Adalah singkatan dari *Virtual Private Network* merupakan sebuah metode untuk menyembunyikan alamat IP asli dari pelacakan. Dengan VPN , alamat IP akan dipalsukan atau dialihkan dari perangkat asli pengguna ke perangkat yang ada di server penyedia VPN. Contoh kasusnya adalah jika penyedia internet kita mencegah kita untuk mengakses alamat IP tertentu, maka kita bisa memakai VPN untuk melakukan tunneling ke sever luar yang dimana alamat IP tersebut bisa di akses. Dengan ini, alamat IP pengguna yang sesungguhnya dapat di bungkus dan dialihkan ke alamat IP server luar atau pihak ketiga. Namun metode ini tidak sepenuhnya aman. Sudah banyak laporan tentang bocornya data pengguna NordVPN. NordVPN ialah salah satu penyedia layanan VPN yang sudah cukup terkenal. Namun sudah banyak laporan bahwa data pengguna bocor.

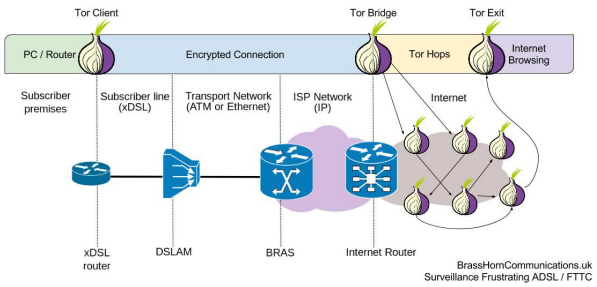
Ini disebabkan adanya tindakan penetrasi pada enkripsi saat pengguna melakukan autentifikasi ketika mencoba terhubung ke layanan penyedia VPN. Kemungkinan yang lain adalah ada yang mengakses server VPN secara langsung dan mencuri data atau kunci autentifikasi pengguna. Juga bisa terjadi ketika pengguna mengakses Wi-Fi publik yang ternyata merupakan Wi-Fi buatan peretas dan peretas tersebut mendapatkan kunci VPN melalui *Man In The Middle Attack*.

2.3 Proxy

Adalah sebuah server pihak ketiga yang menjadi perantara antara pengguna ke server yang dituju sebagai alternatif daripada langsung menghubungi server. Proxy ditujukan bila pihak penyedia internet memblokir alamat IP tertentu. Maka dengan proxy, kita bisa terlebih dahulu terhubung ke server pihak ketiga kemudian mengakses alamat IP tujuan kita melalui server tersebut. Namun metode ini tidak akan menyembunyikan alamat IP kita dan cenderung rawan untuk dipenetrasi dengan *Man In The Middle Attack*. Seseorang bisa sengaja masuk diantara jalur pengguna dan penyedia *proxy* dan melakukan *sniffing* atau melihat data yang lewat melalui jaringan.

2.4 TOR Network

TOR (The Onion Routing) adalah sebuah *Free and Open Source Software* yang merupakan sebuah protokol keamanan diinternet yang bisa digunakan secara gratis. Protokol ini akan menggabungkan teknologi *VPN* dan *Proxy*. Dimana pengguna akan masuk ke dalam jaringan TOR untuk mengakses internet. Alamat IP pengguna akan melompati beberapa server sukarelawan secara acak sebelum terhubung ke internet.

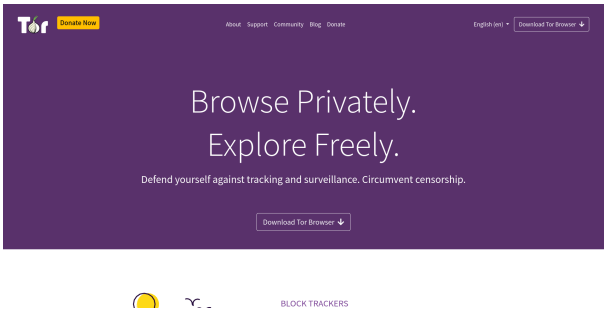


Ini dapat memberikan keamanan lebih kepada pengguna dikarenakan alamat IP pengguna akan dibungkus dengan berlapis-lapis alamat IP yang membuat penyerang kesulitan bahkan tidak mungkin

melacak alamat IP asli pengguna. Ini juga dikarenakan fitur enkripsi akan diterapkan pada setiap pembungkus alamat IP. Semua ini bisa dilakukan dengan menggunakan TOR Browser atau TOR Tunneling.

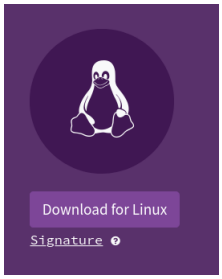
2.4.1 Instalasi TOR Browser

Kita dapat menggunakan TOR dengan menginstall TOR Browser yang bisa didapatkan melalui situs resmi yaitu `https://www.torproject.org/`.



Kemudian masuk ke laman *Download* dan pilih sistem operasi yang digunakan. Setelah selesai mendownload, jika pengguna menggunakan Sistem Operasi Windows, maka TOR Browser dapat diinstal dengan melalui file yang telah di download. Untuk Sistem Operasi Distribusi Linux, TOR Browser tersedia di *Package Manager* setiap distro atau dapat diinstall melalui Flatpack atau Snap Packages.

Jika tidak tersedia, maka kita bisa langsung masuk ke situs resmi dan mendownload *executable binnary*.



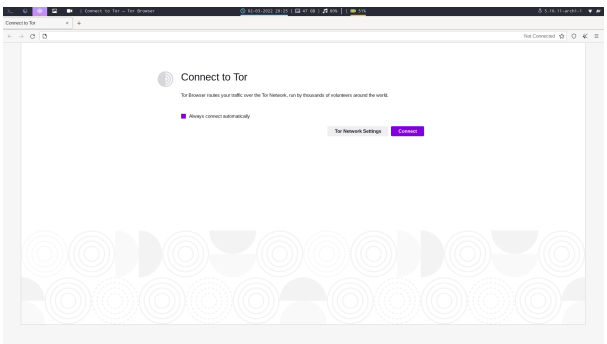
Setelah terdownload, navigasi ke folder tempat file kompresi tersebut berada dan extract menggunakan perintah :

```
tar -xvf tor-browser-linux64-11.0.6_en-US.tar.xz
```

Sesuaikan versi dengan yang telah didownload. Kemudian masuk ke directory tersebut dan eksekusi dengan :

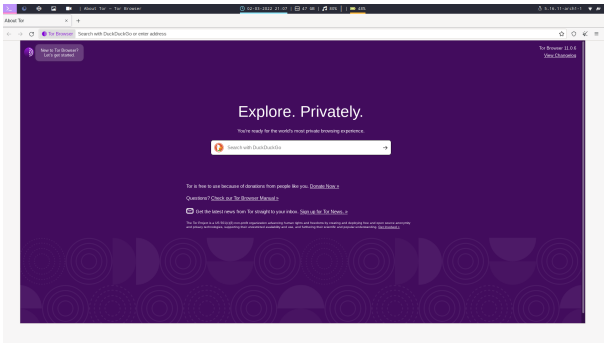
```
./start-tor-browser.desktop
```

kemudian akan muncul tampilan seperti berikut :



Kita bisa langsung memilih 'Connect' untuk menyambungkan ke jaringan TOR. Akan membutuhkan sedikit waktu untuk terhubung, terutama bila jaringan internet pengguna terbilang lambat. Maka waktu

yang diperlukan untuk menghubungi TOR Network juga akan lebih lambat. Dikarenakan alamat IP harus melompat ke banyak node agar bisa mencapai onion routing. Bila sudah terhubung, akan muncul tampilan sebagai berikut :



Setelah ini, kita dapat mengakses internet tanpa perlu khawatir dengan adanya pelacakan. Dengan TOR juga kita dapat mengakses situs-situs yang tidak biasa ada di internet dengan domain *.onion*. Biasanya situs yang menggunakan domain *.onion* merupakan situs-situs tersembunyi berisi layanan ilegal seperti cuci uang, senjata ilegal, penyewaan hacker, pembunuh bayaran, dan lain-lain.

III Penutup

Dengan ini dapat dikatakan bahwa untuk mencegah diri dari *cyber attack*. terdapat berbagai metode. Beberapa diantaranya ialah menggunakan *proxy, VPN, dan TOR*. untuk menyembunyikan identitas kita di internet dan mencegah penjahat untuk melacak aktivitas dan keberadaan kita. Namun cara diatas tidak akan berhasil jika tidak disertai dengan kesadaran berinternet yang memadai dan mawas akan teknologi. Melakukan tindakan seperti mendownload dan/atau menginstall konten bajakan seperti film, perangkat lunak, dan sebagainya juga mampu mendatangkan marabahaya dikarenakan kita tidak bisa memastikan apakah file tersebut aman dari virus atau perangkat lunak berbahaya lainnya.

Selain itu, juga lebih banyak metode yang biasa digunakan oleh para kriminal untuk mengakses data kita. Namun karena hal tersebut barada diluar konteks pembahasan tulisan ini, maka penulis tidak mencantumkan penjelasan lebih lanjut mengenai metode yang digunakan. Selama kita berhati-hati dalam menjelajah internet maka kita akan mendapatkan keamanan dan kenyamanan yang kita inginkan dan kita butuhkan.

Sekian yang dapat penulis sampaikan. Kurang dan lebihnya mohon dimaafkan dikarenakan penulis juga hanya manusia biasa yang tak luput dari kesalahan. **Terima kasih.**

References

Karthigeyan 1, Robinson Joel, M 2, Manikandan 3, Guru 4, and Raman 5. A comprehensive behavior analysis of tor versus i2p, 2018.

Saurav Dahal. Study on existing attacks to reveal bittorrent user's ip address in tor network channel characterization in millimeter wave frequencies view project tor network view project, 2017.

Roger Dingledine. Tor: The second-generation onion router, 07 2018.

Roger Dingledine and Steven Murdoch. Performance improvements on tor or, why tor is slow and what we're going to do about it, 2009.

David Dwiputra Kurniadi. The difference between using proxy server and vpn. *The Difference Between Using Proxy Server and VPN*, 2:19–22, 2015.

Ramzi Haraty and Bassam Zantout. The tor data communication system: A survey damage assessment and recovery from malicious attacks for defensive information warfare view project high-performance and accurate mathematical solvers in hardware view project the tor data communication system. *Article in Journal of Communications and Networks*, 2014. doi: 10.1109/JCN.2014.000071.

Aduragbemi Ogundijo and Atiff Abdalla. Zero-trust vs. software defined perimeter vs. vpn (networks) the opinion of intellectuals: questions and answers view project. *Zero-Trust vs. Software Defined Perimeter vs. VPN (NETWORKS)*, 10 2021. doi: 10.13140/RG.2.2.19996.62086.

Antonio Ruiz-Martínez and Diana Trujillo. Tor hidden services: a systematic literature review electronic and mobile payment view project iot security view project tor hidden services: a systematic literature review, 08 2018.

Bheemarjuna Tamma, A Madhura, Antony Franklin, and Tulika Agrawal. *Final Report Research Engagemenet On IPv6 for IoT*. NASSCOM CENTER OF EXCELLENCE FOR INTERNET OF THINGS, 01 2020.

Nicky Van Rijsbergen and Kevin Valk. Tor vs the nsa, 09 2020.