NONTRADITIONAL NETWORK SEBAGAI WIRELESS NETWORK ATTACKS

Disusun oleh:

VALENTINA SAMAYA S. D. (21060117130076)

DEPARTEMEN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS DIPONEGORO

Abstrak

Perkembangan teknologi serta industri, khususnya pada era internet of things sekarang ini memperkenalkan jaringan wireless sebagai jaringan yang memiliki banyak keunggulan. Di mana dengan menggunakna jaringan wireless akan didapatkan produktivitas yang lebih tinggi dikarenakan kemudahan akses yang diberikan oleh jaringan wireless. Walaupun penggunaannya yang menawarkan banyak keuntungan, jaringan wireless sendiri memiliki banyak kekurangan. Dengan memancarkan sinyal ke udara bebas sebagai jaringan, maka keamanan dari jaringan wireless akan kurang lebih aman dibandingkan dengan jaringan yang menggunakan kabel sehingga akses dari jaringan dibatasi hanya dari kabel yang menguhubungkan pada provider jaringan tersebut. Salah satu ancaman yang dapat didapatkan oleh jaringan wireless sendiri adalah jaringan nontraditional.

Kata Pengantar

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan berkat dan bimbingan-Nya sehingga saya dapat menyelesaikan tugas makalah yang berjudul Nontraditional Network Sebagai Wireless Network Attacks ini tepat pada waktunya.

Adapun tujuan dari penulisan dari makalah ini adalah untuk memenuhi tugas M. Arfan ,S.Kom., M.Eng. pada mata kuliah Kriptografi. Selain itu, makalah ini juga bertujuan untuk menambah wawasan tentang Nontraditional Network Sebagai Wireless Network Attacks bagi para pembaca dan juga bagi penulis.

Saya mengucapkan terima kasih kepada bapak M. Arfan ,S.Kom., M.Eng., selaku dosen mata kuliah Kriptografi yang telah memberikan tugas ini sehingga dapat menambah pengetahuan dan wawasan sesuai dengan bidang studi yang saya tekuni.

Saya juga mengucapkan terima kasih kepada semua pihak yang telah membagi sebagian pengetahuannya sehingga saya dapat menyelesaikan makalah ini.

Saya menyadari, makalah yang saya tulis ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun akan saya nantikan demi kesempurnaan makalah ini.

Semarang, 2 Juni 2020

Penulis

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi serta industri, khususnya pada era internet of things sekarang ini memperkenalkan jaringan wireless sebagai jaringan yang memiliki banyak keunggulan. Di mana dengan menggunakna jaringan wireless akan didapatkan produktivitas yang lebih tinggi dikarenakan kemudahan akses yang diberikan oleh jaringan wireless. Selain itu, jaringan wireless juga memberikan kemudahan konfigurasi yang dapat dilakukan dengan lebih mudah, lebih cepat, serta jauh lebih murah dibandingkan dengan konfigurasi jaringan menggunakan kabel.

Walaupun penggunaannya yang menawarkan banyak keuntungan, jaringan wireless sendiri memiliki banyak kekurangan. Melihat fakta bahwa jaringan wireless menggunakan access point yang akan memancarkan sinyal dengan frekuensi radio yang merupakan jaringan. Dengan memancarkan sinyal ke udara bebas sebagai jaringan, maka keamanan dari jaringan wireless akan kurang lebih aman dibandingkan dengan jaringan yang menggunakan kabel sehingga akses dari jaringan dibatasi hanya dari kabel yang menguhubungkan pada provider jaringan tersebut.

Salah satu ancaman yang dapat didapatkan oleh jaringan wireless sendiri adalah jaringan nontraditional. Jaringan nontraditional merupakan jaringan yang melibatkan penggunaan perangkat Bluetooth, pembaca barcode, dan juga asisten digital pribadi.

B. Rumusan Masalah

1) Apakah jaringan nontraditional?
2) Bagaimana cara untuk mengamankan transmisi dari jaringan wireless?
3) Bagaimana cara untuk mengamankan access point jaringan wireless?
4) Bagaimana cara untuk mengamankan jaringan wireless?

C. Tujuan Masalah

1) Mengetahui apa yang dimaksud dengan jaringan nontraditional.
2) Mengetahui cara untuk mengamankan transmisi jaringan wireless.
3) Mengetahui cara untuk mengamankan access point jaringan wireless.
4) Mengetahui cara untuk mengamankan jaringan wireless.

BAB II
PEMBAHASAN

A. Nontraditional Network

Jaringan nontraditional di sini merupakan salah satu ancaman yang dimiliki oleh jaringan wireless, di mana pada umumnya jaringan nontraditional ini sering dianggap remeh dan sepele. Sehingga banyak orang yang berasumsi bahwa penggunaan dari jaringan nontraditional yang singkat tidak akan membahayakan keamanan dari transaksi atau bisnis yang dilakukan.

Contoh dari jaringan nontraditional yang memiliki potensi menjadi ancaman bagi jaringan wireless adalah pada perangkat Bluetooth, pembaca barcode, asisten digital pribadi, dan bahkan wireless printers dan mesin copy. Namun, semua perangkat tersebut dapat dikatakan tidak aman apabila tidak dilakukan pengamanan pada jaringannya.

Jaringan traditional yang ada dapat sangat mudah untuk dapat diintip oleh orang IT yang berfokus untuk mengakses access point atau pada end point seperti laptop atau perangkat lainnya yang berada pada jaringan.

B. Pengamanan Transmisi Jaringan Wireless

Pada dasarnya, dengan adanya jaringan wireless, maka sudah tercipta 3 ancaman terhadap jaringan wireless itu sendiri yaitu, interception, alteration, dan juga disruption. Ketiga ancaman tersebut berada pada fase transmisi yang dilakukan pada jaringan wireless. Sehingga untuk dapat mengatasi ketiga masalah tersebut, dapat dilakukan beberapa hal di bawah:

1. Menjaga kerahasiaan dari transmisi wireless

   Terdapat dua cara yang dapat dilakukan untuk menjaga kerahasiaan dari transmisi wireless. Cara yang pertama adalah dengan teknik signal-hiding. Teknik signal-hiding ini merupakan salah satu cara yang digunakan oleh suatu organisasi agar access point dari jaringan wireless lebih susah untuk ditemukan dan dideteksi. Hal tersebut dapat dilakukan dengan mematikan SSID broadcasting, memberikan nama SSID yang telah terenkripsi, atau bahkan mengurangi sinyal menjadi lebih

rendah namun masih dapat digunakan, sehingga sinyal yang dipancarkan tidak akan menembus dinding. Cara kedua yang dapat dilakukan adalah dengan melakukan enkripsi.

2. Mencegah perubahan dari informasi pada proses komunikasi

   Perubahan yang dilakukan pada informasi pada proses transmisi dilakukan pada saat file berada di tengah-tengah proses transmisi. Sehingga hal ini sering disebut sebagai serangan "man-in-the-middle". Untuk mencegah hal ini terjadi, dapat dilakukan 2 cara yaitu menggunakan enkripsi yang kuat dan autentikasi yang kuat pada setiap perangkat user dari jaringan.

C. Pengamanan Access Point Jaringan Wireless

Access point dari jaringan wireless yang tidak dikonfigurasi secara aman akan dapat menoleransi kerahasiaan dari access point tersebut dengan memberikan akses pada pihak yang tidak terotorisasi masuk ke dalam jaringan. Agar kerahasiaan access point dapat terjaga, serta access point dapat terkonfigurasi secara aman, maka dilakukan 3 langkah berikut ini:

1. Menghilangkan access point yang mencurigakan atau tidak terotorisasi.
2. Menkonfigurasi access point satu persatu secara benar
3. Menggunakan 802.1x untuk autentikasi semua perangkat.

D. Pengamanan Jaringan Wireless

Berikut beberapa cara yang dapat digunakan untuk dapat menjaga agak jaringan wireless tetap aman.

1. Menggunakan enkripsi
2. Menggunakan software antivirus, anti-spyware, dan juga firewall
3. Mematikan identifier broadcasting
4. Mengubah identifier router dari default
5. Mengubah router pre-set password untuk administrasi
6. Hanya beberapa computer yang memiliki akses pada jaringan wireless
7. Mematikan jaringan wireless saat tidak sedang digunakan
8. Jangan berasumsi bahwa public hotspot merupakan jaringan yang aman
9.

BAB III
PENUTUP

A. Kesimpulan

Jaringan wireless memiliki banyak kesempatan untuk dapat meningkatkan produktivitas dengan aksesnya yang mudah dan biaya yang tidak mahal. Namun dengan segala kelebihannya tersebut, jaringan wireless juga memiliki beberapa kekurangan yang tidak dapat dihindari, beberapa permasalahannya merupakan keamanan yang diberikan dari jaringan wireless itu sendiri. Walaupun akan tidak mungkin untuk dapat mengeliminasi setiap resiko atau ancaman dari jaringan wireless, namun akan sangat memungkinkan untuk dapat mencapai suatu level keamanan yang cukup untuk jaringan wireless dapat digunakan secara aman.

DAFTAR PUSTAKA

1. Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.
2. Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.
3. Graham, E., Steinbart, P.J. (2006) Wireless Security.
4. Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems. NIST Special Publication 800-30.
5. Choi, Min-kyu, et al. (2008). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering Vol. 3.