Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration

Ari Prayoga Hutabarat[1], Haeruddin[2]
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam,
Sei Ladi, Jl. Gajah Mada, Baloi Permai, Kec. Sekupang, Kota Batam,
Kepulauan Riau 29442
Email : ari@uib.ac.id, haeruddin@uib.ac.id

Abstrak

Seiring makin berkembangnya teknologi informasi dan komunikasi yang mengglobal membuat setiap orang harus dapat menerima perubahan tersebut. Pada saat ini setiap orang harus berlomba-lomba dalam mempelajari perkembangan teknologi tersebut, jika tidak dapat mengikuti perkembangan teknologi tersebut maka ia tidak akan dapat selamat dari perkembangan teknologi dan ketinggalan akan teknologi. Dengan berkembangnya teknologi maka peningkatan penggunaan teknologi akan meningkat. Sehingga banyak orang yang akan mempelajari teknologi terbaru. Dengan banyaknya orang-orang yang baru mempelajari perkembangan teknologi membuat banyak kasus cybercrime yang memanfaatkan orang-orang yang tidak "melek teknologi" yang menganggap bahwa keamanan atau privasi seorang tidaklah cukup penting. Tugas akhir ini bertujuan untuk menganalisa sistem keamanan pada jaringan end user dari serangan Exploit menggunakan Metode Penetration Testing. Tugas akhir ini menghasilkan sebuah bentuk laporan penelitian beserta solusi keamanan jaringan end user dari serangan Exploit. Dalam pengujiannya, penelitian ini melakukan exploitasi menggunakan tool The Fatrat yang diinstall pada sistem operasi Parrot OS. Pada penelitian ini memanfaatkan celah dari Address Resolution Protocol (ARP), yaitu ARP Spoofing. ARP bertujuan untuk memetakan alamat IP address menjadi alamat fisik atau yang dikenal sebagai MAC Address yang sesuai dengan tujuan. Dalam ARP menggunakan system "kepercayaan", dimana seluruh mesin dipercaya memberikan ARP Reply yang benar. Hasil dari penelitian ini merupakan sebuah cara dalam menghadapi masalah keamanan jaringan end user, yaitu dengan cara dilakukannya penambahan pada konfigurasi router mikrotik sehingga membuat jaringan end user menjadi aman dari serangan Exploit yang memanfaatkan teknik ARP Spoofing.

.

Kata Kunci: *Cybercrime*, Keamanan Jaringan *End User*, *Mikrotik*, *Exploit*, *The Fatrat*, ARP, *Penetration Test.*

Abstract

As global information and communication technology develops, everyone must be able to accept these changes. At this time everyone must compete in learning the development of technology, if they cannot keep up with the development of the technology, they will not be able to survive technological developments and miss technology. With the development of technology, increasing use of technology will increase. So that many people will learn the latest technology. With so many people who are just learning about technological developments, there are many cases of cybercrime that use people who are not "technology literate" who assume that a person's security or privacy is not important enough. This final project aims to analyze the security system on the network end users of Exploit attacks using the Penetration Testing Method. This final project produces a form of research reports along with end user network security solutions from exploit attacks. In testing, this study exploited using the Fatrat tool installed on the Parrot OS operating system. In this study utilizing the gap from the Address Resolution Protocol (ARP), namely ARP Spoofing. ARP aims to map the IP address into a physical address or what is known as the MAC Address that matches the purpose. In ARP use the "trust" system, where all trusted machines provide the correct ARP Reply. The results of this study are a way of dealing with end user network security problems, namely by adding mikrotik router configuration so as to make the end user network safe from Exploit attacks that utilize the ARP Spoofing technique.

Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

***Keywords**: Cybercrime, End User Network Security, Mikrotik, Exploit, The Fatrat, ARP, Penetration Test.*

I. LATAR BELAKANG

Dewasa ini penggunaan teknologi informasi telah meningkat pesat dalam transmisi data dan informasi secara gobal. Dengan meningkatnya jumlah orang-orang yang terhubung dalam jaringan menyebabkan meningkatnya ancaman keamanan jaringan yang besar terlebih lagi dalam suatu organisasi ataupun perusahaan. Dimasa yang lalu, untuk menjadi seorang hacker haruslah mempunyai kemampuan programming dan mengerti detail dari sistem komunikasi komputer serta mengetahui cara kerja exploit vulnerabilities. Sekarang hampir semua orang dapat menjadi seorang hacker hanya dengan mengunduh tool dari internet. Tool ini banyak bertebaran di internet sebagai hasil dari meningkatnya kebutuhan akan keamanan jaringan dan dapat digunakan secara gratis (Khan & Hasan, 2014).

Dengan sifat alami dari perkembangan teknologi informasi hari demi hari maka sangatlah penting dalam metode pertahanaan juga harus berkembang. Dahulu ancaman baik bersumber dari dalam maupun luar dapat dilacak dengan mudah dan dihancurkan. Namun dengan perkembangan teknologi maka hacker selalu mencari teknologi terbaru yang dapat melewati sistem keamanan jaringan. Mempertahankan jaringan sangat penting untuk melawan dari ancaman di jaringan. Setiap perangkat hadir dalam jaringan memainkan dalam peranan penting dalam pengamanan jaringan untuk memastikan data yang bersifat privasi atau rahasia aman dari orang yang tidak bertanggung jawab (Kumar, Kamtam, & Patkar, 2016).

Penetration testing telah terbukti efektif dalam membantu dalam menangani masalah keamanan pada jaringan. Teknik penetration testing tidak hanya berpusat pada keamanan pada aplikasi tetapi juga dapat diterapkan di dalam jaringan dan sistem operasi dimana tujuan utamnya ialah untuk menemukan dan mencoba melakukan exploit vulnerabilities yang diketahui atau terdeteksi pada evaluasi sebelumnya berdasarkan teknik tertentu (Satria, Alanda, Erianda, & Prayama, 2015).

Penetration Testing merupakan proses dari simulasi penyerangan pada sistem yang membutuhkan pembuktian keamanan pada jaringan dalam menghentikan seorang hacker atau attacker dalam melakukan serangan terhadap jaringan yang menyebabkan kerugian. Orang yang melakukan penetration testing juga dikenal sebagai Pen-Test. Penetration testing membutuhkan persetujuan dari pemilik sistem jika tidak makan akan disebut tindakan illegal atau hacking. Dalam penetration testing ada yang dinamakan "Payload". Payload merupakan perangkat lunak yang memungkinkan pen-test memanipulasi sebuah sistem setelah sistem tersebut terexploitasi. Metapreter merupakan payload terbaik dan polular dalam Metasploit yang memungkinkan pen-test dalam melakukan tindakan "full control" pada target. Payload biasanya ditulis dalam sebuat script atau program yang dapat dijalankan di background oleh target setelah target telah terexploitasi (Mundalik, 2015).

The Fatrat merupakan sebuat tool yang cukup terkenal dalam melakukan exploit. The Fatrat dapat membuat sebuah backdoor untuk sistem operasi windows, linux, mac dan android (Kunwar, Sharma, & Kumar, 2009). The fatrat memiliki banyak fungsi seperti membuat backdoor menggunakan msfvenom, backdoor apk dimana menggunakan file apk original seperti file apk instalasi Instagram, line, facebook, dll. File original tersebut akan di decompile dan di inject backdoor sehingga korban tidak sadar bahwa aplikasi yang diinstal pada smartphone ternyata ada backdoor.

Berdasarkan uraian diatas, penulis melakukan penelitian dengan judul "Analisis Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration Testing".

II. METODE PENELITIAN

Untuk menghasilkan luaran yang sesuai dengan tujuan penelitian, maka dibutuhkan sebuah metode perancangan yang berguna dalam pedoman dan acuan dalam penulisan ini.

Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

Metode perancangan penelitian yang berjudul "Analisis Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration Testing" ialah metode penetration testing. Penetration testing merupakan sebuah proses dari simulasi serangan yang bertujuan untuk mengukur seberapa aman sebuah sistem dari serangan seorang hacker atupun attacker (Mundalik, 2015).

Tujuan utama dari penetration testing ini adalah untuk melakukan evaluasi suatu sistem atau jaringan komputer. Evaluasi terhadap sistem atau jaringan komputer dilakukan dengan cara evaluasi serangan (attack). Menurut Samsumar & Gunawan (2017) dalam melakukan Penetration Testing memiliki beberapa metode, diantaranya sebagai berikut:

1. Black Box
2. White Box
3. Gray Box

Menurut Satria et al., (2015), ada beberapa langkah yang harus dilakukan dalam melakukan penetration testing (lihat gambar 3.1), sebagai berikut:

Literature Review dengan membaca dan memahami suatu buku, website dan journal yang berhubungan dengan keamanan jaringan dan penetration testing.

Dalam tahap Pre Penetration Testing, akan dilakukan analisis keamanan jaringan dan kebutuhan apa saja yang akan digunakan.

Penetration Testing, dalam tahap ini akan dilakukan berbagai jenis test dalam menemukan sebuat celah keamanan dan melakukan exploit terhadap sistem yang saat ini.

Reporting, setelah semua pekerjaan keamanan jaringan telah selesai maka akan dibuat sebuah laporan berdasarkan hasil pekerjaan dan memberikan rekomendasi pada resiko keamanan jaringan yang telah ditemukan pada sistem.

III. HASIL PENELITIAN DAN PEMBAHASAN

Pada penetration test yang dilakukan oleh peneliti saat percobaan penyerangan terhadap jaringan end user, terbukti bahwa hasil dari penetration test tersebut berhasil. Dimana host client pada jaringan dapat dilacak pada aplikasi Ettercap, kemudian dapat dilakukan Exploit terhadap host tersebut. Hasil dari penetration test ini adalah dapat dilacaknya alamat client dalam jaringan yang diakses, sehingga penyerang dapat memasukkan alamat jaringan client pada target di Ettercap sehingga client dapat dieksploit dengan bantuan ARP Poisioning dan DNS Spoofing. Dimana ARP Poisioning akan berguna untuk mengelabuhi client bahwa mac address penyerang merupakan mac address router sehingga setiap request dari client akan dikirim ke penyerang dan DNS Spoofing akan memalsukan alamat ip pada domain menjadi alamat ip penyerang. Hal ini dapat dilihat ketika client melakukan ping terhadap google.com dimana mendapatkan reply bukan dari ip server google melainkan ip server penyerang. Dengan penggabungan ARP Poisioning, DNS Spoofing dan Backdoor yang dibuat dengan The fatrat serta Metasploit yang berguna untuk listening host dan port penyerang maka penyerang dapat melakukan exploit serta memiliki akses penuh terhadap device client.

Dalam hal ini dalam penyebaran file exploit yang telah dibuat dilakukan dengan bantuan Ettercap. Yang dapat melakukan DNS Spoofing dan ARP Spoofing yang berguna untuk memaksa client untuk mengarah ke halaman web palsu yang telah dibuat sebelumnya.

Penyelesaian masalah dalam penelitian ini adalah perbaikan pada konfigurasi router yang digunakan. Cara yang dilakukan adalah dengan meng- aktifkan konfigurasi "Add ARP For Leases" pada setting-an DHCP Server dan lease time diubah ke 1 hari. Dimana "Add ARP For Leases" berguna untuk mencegah ARP Spoofing yang ada di router mikrotik.

Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

IV. KESIMPULAN

Berlandaskan dari hasil pengujian yang dilakukan oleh peneliti dengan judul "Analisis Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration Testing" maka peneliti dapat menyimpulkan sebagai berikut:

1. Hasil dari penelitian yang dilakukan oleh peneliti ini ialah sebuah solusi keamanan jaringan end user terhadap sistem keamanan jaringan end user dari serangan Exploit menggunakan perangkat Router Mikrotik. Dimana serangan memanfaatkan ARP Spoofing dalam mengganti alamat mac pada arp tujuan menjadi alamat mac penyerang.
2. Seorang client dapat mendeteksi adanya serangan ARP menggunakan software Xarp jika tidak adanya konfigurasi tambahan dilakukan pada router.
3. Dari hasil penelitian ini, penulis membuktikan bahwa keamanan jaringan end user tidak dapat dibobol oleh Man In The Middle Attack dengan cara menambah konfigurasi pada router mikrotik.

Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

Daftar Pustaka

Bhatt, P. (2017). Importance of Penetration Testing for Legacy Operating System. *International Journal of Scientific & Technology Research*, *6*(12), 42–46.

Ferdiansyah, D. (2014). *Vulnerability Assessment Terhadap Jaringan Untuk Keamanan Informasi* (pp. 516–521). pp. 516–521.

Hardik J Prajapati, & Noorani, Z. (2017). A Survey on ARP Cache Poisoning and Techniques for Detection and Mitigation. *2017 4th International Conference on Signal Processing, Communication and Networking, ICSCN 2017*, (6), 594–601.

Jain, K. M., Jain, M. V, & Borade, J. L. (2016). *A Survey on Man in the Middle Attack*. *2*(09), 277–280.

Kaur, G., & Kaur, G. (2016). *Penetration Testing : Attacking Oneself to Enhance Security*. *5*(4), 574–577.

Khan, R., & Hasan, M. (2014). *Network Threats, Attacks and Security Measure: A Review*. *5*(7), 72–75.

Kumar, A., Kamtam, A., & Patkar, U. C. (2016). Self-Defending Approach of a Network. *International Research Journal of Engineering and Technology*, 2395–56.

Kunwar, R. singh, Sharma, P., & Kumar, K. V. R. (2009). Malware Analysis of Backdoor Creator : Fatrat. *Queue*, *7*(1).

Lukman, N. (2016). Studi Implementasi Aplikasi Manajemen Ruang Kelas "Netop School" Berbasikan Local Area Network (LAN). *Jurnal Sains Dan Teknologi Utama*, *XI*(152).

Muhammad, M., & Hasan, I. (2016). Analisa dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router OS V . 5.20 di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*, *2*(1), 10–19.

Mundalik, S. S. (2015). *Penetration Testing : An Art of Securing the System (Using Kali Linux)*. *5*(10), 235–242.

Najari, S., & Lotfi, I. (2014). Malware Detection Using Data Mining Techniques. *International Journal of Intelligent Information Systems*, *3*(6), 33.

Saidah, K., & Damariswara, R. (2017). *Analisa Bentuk Bentuk Penilaian Sikap Siswa Sekolah Dasar di Kota Kediri*. *4*(1), 84–96.

Samsumar, L. D., & Gunawan, K. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus di Kampus STMIK Mataram. *Ilmiah Teknologi Informasi Terapan*, *IV*(1), 73–82.

Satria, D., Alanda, A., Erianda, A., &

Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.31-36
ISSN: -

Prayama, D. (2015). *Network Security Assessment Using Internal Network Penetration Testing Methodology*. *2*, 360–365.

Setiady, T., & Rahmad, M. B. (2014). Perancangan Sistem Informasi Inventory Sparepart Elektronik berbasis WEB PHP. *Jurnal Sarjana Teknik Informatika*, *2*(2).

Syaifuddin, M., Andika, B., & Ginting, R. I. (2016). Analisis Celah Keamanan Protocol Tcp / Ip. *Jurnal Ilmiah Saintikom*, *16*(2), 130–135.