DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING

Amarudin[1)], Faruk Ulum[2)]

[1)]Teknik Elektro, Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
[2)]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
[1,2,)]Jl. H.ZA Pagaralam, No 9-11, Labuhanratu,Bandarlampung
Email : amarudin@teknokrat.ac.id[1)], faruk.ulum@teknokrat.ac.id[2)]

Abstrak

Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer.Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut sehingga dapat membuka peluang bagi para hacker untuk meretas dan merusak jaringan yang dibangun tersebut.Untuk meminimalisir terjadinya penyalahgunaan jaringan oleh para hecker, maka perlu adanya peningkatan keamanan jaringan yang akan dibangun. Dalam penelitian ini telah dilakukan penelitian untuk mengembangkan keamanan jaringan komputer dengan cara penggunakan metode Port Knocking. Adapun untuk mempermudah dalam mendesain dan menguji jaringan yang akan dibangun perlu adanya simulator yang digunakan. Dalam penelitian ini menggunakan simulator GNS3 untuk mendesain dan mensimulasikan topologi keamanan jaringan. Berdasarkan peneltian yang telah dilakukan bahwasanya simulator GNS3 dapat dengan mudah deterapkan dalam mendesain topologi jaringnan maupun dalam mensimulasikan pengujian keamanan jaringan khususnya pada metode keamanan Port Knocking. Berdasarkan hasil penelitian yang telah dilakukan juga didapatkan hasil bahwasanya Metode Port Knocking dapat diterapkan untuk mengamankan Router dari akses orang lain yang tidak berhak mengaksesnya.

Kata kunci: *Mikrotik Router OS, Topology, Simulator GNS3, Network Security, Port Knocking, Hacking.*

1. Pendahuluan

Pesatnya perkembangan teknologi internet tidak dapat dipungkiri akan berdampak pada meningkatnya *ciber cryme*. Dengan demikian yang harus diwaspadai oleh para pengelola jaringan komputer adalah terhadap banyaknya serangan yang bisa dilakukan di internet oleh para hacker. Salah satu jenis serangan yang sering terjadi pada jaringan komputer adalah *Denial of Service (DoS) attacks*. *DoS attack* adalah tindakan yang dilakukan dengan cara mencegah atau merusak pihak yang berwenang untuk menggunakan jaringan, sistem, atau aplikasi dengan menghabiskan sumber daya seperti CPU, memori, bandwidth, dan ruang disk [1]. Seiring dengan adanya beberapa jenis serangan tersebut, maka ada hal lain yang juga menarik untuk dibahas yaitu perlu adanya penerapan teknologi informasi yang aman. Untuk menerapkan teknoplogi yang aman perlu adanya perancangan sebuah sistem keamanan jaringan yang bagus. Adapun untuk mendesain sebuah jaringan komputer, ada beberapa jenis simulator yang bisa digunakan. Pada saat penelitian ini berlangsung, menurut informasi yang dipublis pada website kopas.id ada 8 (delapan) jenis *software* simulator jaringan keren dan menarik untuk belajar jaringan, yaitu: Cisco Packet Tracer, GNS3, Cisco Aspire CCNA Edition, IPSims, iNetwork, Netnotep Simulator, Boson Netsim, dan Virtualbox & Mikrotik [2]. Dari beberapa *software* (8 simulator) tersebut pada penelitian ini khusus membahas/menggunakan simulator GNS3 untuk mendesain keamanan jaringan pada Router OS menggunakan metode Port Knocking.

2. Penelitian Terkait

Beberapa penelitian sebelumnya terkait keamanan jaringan antara lain penelitian yang telah dilakukan oleh Basim Mahbooba, *et al.* [3], yang membahas penguncian port berbasis sertifikat digital untuk menghubungkan sistem yang *embedded* pada IoT. Pada penelitian tersebut bertujuan untuk memperkuat metode port knocking yang ada dengan sertifikat digital untuk otentikasi alternatif di antara perangkat IoT. Konsep-konsep tersebut akan menjadi pelengkap konsep-konsep kriptografi lainnya (yaitu kunci enkripsi bersama sebagaimana yang diadopsi dalam ZigBee).

Sedangkan penelitian yang telah dilakukan oleh Daniel Sel, *et al.* [4], menyampaikan bahwasanya penerapan Port Knocking yang dibangun menggunakan *Public Key* masih kurang aman sehingga pada penelitian tersebut memperkenalkan implementasi port-knocking berdasarkan sertifikat x509 yang ditujukan untuk menjadi sangat skalabel.

Adapun penelitian yang dilakukan oleh Amarudin, *et al.*[5], telah membahas analisis penerapan mikrotik router sebagai *user manager* untuk menciptakan internet sehat menggunakan simulasi virtual *machine*. Dalam penelitian tersebut memperkenalkan pemanfaatan *user manager* sebagai manajemen *user* untuk meningkatkan keamanan jaringan yang disimulasikan dengan virtual *machine*. Hasil dari penelitian tersebut telah menghasilkan sistem *user manager* dengan cara dibuatkan *account* untuk setiap *user* agar terhubung ke jaringan internet hotspot. *User manager* tersebut dapat membuat jaringan internet

hotspot yang sehat dan menciptakan kenyaman bagi setiap *user* pengguna jaringan internet hotspot.

Penelitian lainnya yang membahas terkait keamanan jaringan adalah penelitian yang telah dilakukan oleh Fakariah, *et al.* [6]. Dimana dalam penelitian tersebut telah membahas metode sederhana pada Port Knocking menggunakan model random. Dalam penelitian tersebut dijelaskan bahwasanya meskipun Port Knocking merupakan alat yang mudah untuk digunakan, namun masih ada kerentanan ketika deserang menggunakan TCP Replay maupun Port Scaning. Dalam penelitian tersebut mengusulkan pendekatan baru atas Port Knocking yang ada dengan menggunakan urutan Port Sumber yang akan digunakan untuk menyederhanakan teknik untuk port sistem Knocking. Port sumber secara otomatis dihasilkan oleh sistem operasi dan telah ditetapkan sebelumnya untuk menghasilkan urutan. Suatu teknik untuk mengontrol ketika layanan tertentu mulai dan berhenti diperkenalkan untuk mengurangi masalah dengan serangan ulangan TCP dan pemindaian port. Kinerja metode yang diusulkan dievaluasi dengan mengukur waktu otentikasi untuk mengetuk (Knocking) server. Akibatnya, metode yang diusulkan bekerja lebih cepat daripada metode lain seperti mengetuk port dasar dan Fwknop+SPA. Dengan demikian dalam penelitian tersebut telah menunjukkan bahwa metode yang diusulkan lebih sederhana dan pada saat yang sama dapat menjaga dari serangan TCP Replay maupun pemindaian oleh Port Scanning.

3. Landasan Teori

3.1. Mikrotik

Mikrotik adalah perangkat jaringan komputer yang berupa *Hardware* dan *Software* yang dapat difungsikan sebagai Router, sebagai alat Filtering, Switching maupun yang lainnya. Adapun *hardware* Mikrotik bisa berupa Router PC (yang diinstall pada PC) maupun berupa Router Board (sudah dibangun langsung dari perusahaan Mikrotik). Sedangkan *software* Mikrotik atau yang dikenal dengan nama RouterOS ada beberapa versinya. Salah satu versi RouterOS yang terkenal saat ini adalah RB1100 [7]. Salah satu contoh *hardware* Router Board bisa dilihat pada Gambar 1.

Gambar 1. *Mikrotik RB450G* [8]

3.2. Router

Router adalah perangkat jaringan komputer yang dapat berfungsi untuk meneruskan paket data dari satu network ke network lain yang berbeda dalam sebuah jaringan komputer [7]. Router ini bisa dibangun menggunakan Mikrotik.

3.3. GNS3

GNS3 adalah sebuah program graphical network simulator yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan di berbagai sistem operasi, seperti Windows, Linux, atau Mac OS X [9].

3.4. Port Knocking.

Port-knocking adalah konsep menyembunyikan layanan jarak jauh di dalam sebuah firewall yang memungkinkan akses ke port tersebut hanya untuk mengetahui *service* setelah klien berhasil diautentikasi ke firewall. Hal ini dapat membantu untuk mencegah pemindai untuk mengetahui *service* apa saja yang saat ini tersedia di host dan juga berfungsi sebagai pertahanan terhadap serangan zero-day [4].

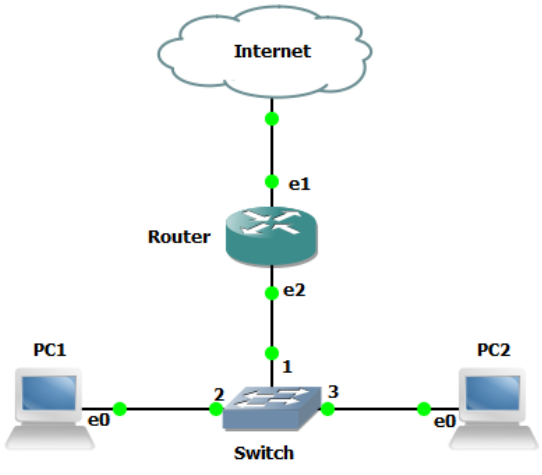
3.5. Hacking

Hacking merupakan aktivitas penyusupan ke dalam sebuah sistem komputer ataupun jaringan dengan tujuan untuk menyalahgunakan ataupun merusak sistem yang ada. Definisi dari kata “menyalahgunakan” memiliki arti yang sangat luas, dan dapat diartikan sebagai pencurian data rahasia, serta penggunaan e-mail yang tidak semestinya seperti spamming ataupun mencari celah jaringan yang memungkinkan untuk dimasuki [10].

4. Pembahasan

4.1. Desain Topologi

Desain topologi keamanan jaringan dibangun menggunakan simulator GNS3. Adapun komponen yang diperlukan antara lain: satu buah Router, satu buah Switch, dan dua buah PC sebagai client. Serta modem sebagai koneksi ke Internet. Desain topologi keamanan jaringan yang dibangun tersebut bisa dilihat pada Gambar 2.

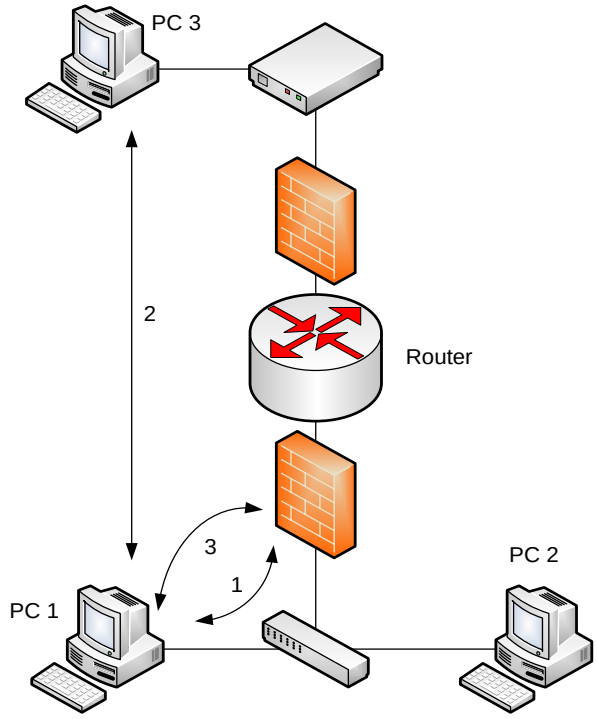


Gambar 2. *Topologi Keamanan Jaringan*

4.2. Sekenario Alur Data (Route)

Sekenario alur data mendeskripsikan urutan data yang terkirim dalam proses Port Knocking. Urutan sekenario sebagaimana pada Gambar 3 dapat dijelaskan sebagai berikut:

1. Pada PC1 ketika mengakses admin Router maka PC1 dihadang oleh Firewall sehingga PC1 tidak dapat langsung masuk ke Router melainkan harus mengakses (*Ping Request*) pada PC3 terlebih dahulu.
2. Setalah mengakses (*Ping Request*) PC3 maka PC1 baru bisa masuk ke admin Router.
3. Setelah PC1 masuk admin Router maka PC1 bisa melakukan konfigurasi pada Router. Hal ini juga berlaku pada PC2.



Gambar 3. *Sekenario Role (Route) Request Port Knocking*

4.3. Konfigurasi Routing

Router dalam hal ini dikonfigurasi dengan tujuan untuk mengaktifkan Firewall sebagai Filtering Ping Request yang berasal dari PC1, PC2 maupun PC3. Dimana pada konfigurasi ini Filtering pada Port yang terhubung pada Router difungsikan sebagai pemfilter setiap ada Request yang memasukinya. Adapun request yang diterima oleh Filtering ini ialah Ping Request yang memiliki alur Ping ke Router dan Ping Request ke Port 80 yang ada pada PC3.

4.4. Pengujian Port Knocking

Pengujian Port Knocking dilakukan dengn cara mengakses admin Router dari PC1. Adapun hasil pengujian dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pengujian Port Knocking

No	Komponen Uji	Keterangan
	Pengujian Pertama	
1	Login ke Router	Gagal
2	Ping ke Router	Ping Replay
3	Ping ke PC2	Ping Replay
4	Login ke Router	Gagal
	Pengujian Kedua	
1	Ping ke PC3	Ping Replay
2	Login ke Router	Berhasil

Berdasarkan hasil pengujian didapatkan hasil bahwasanya admin Router tidak bisa diakses dari PC1 karena PC1 hanya Ping Request ke PC2, maka Admin Router tetap tidak bisa diakses. Adapun pengujian kedua dilakukan dengan cara mengakses admin Router dari PC1 dengan cara Ping Request ke PC3 terlebih dahulu baru kemudian bisa login ke admin Router. Dengan demikian admin Router hanya bisa diakses dari PC1 jika PC1 telah melakukan Ping Request ke PC3 terlebih dahulu.

5. Kesimpulan

Pemanfaatan metode Port Knocking pada keamanan jaringana sangat cocok diterapkan untuk menjaga Router dari akses orang lain yang tidak berhak mengaksesnya. Walaupun pengguna PC1 mengetahui *user* dan *password* untuk login ke Router, akan tetapi jika pengguna PC1 tersebut tidak mengetahui *role* (*route*) ping *request* ke Router maka ia tidak bisa login ke Router. Dengan demikian untuk mengakses admin Router harus melewati dua gerbang *security*. Gerbang pertama yaitu *user* dan *password* admin Router. Sedangkan gerbang kedua yaitu *role* (*route*) ping *request* yang dipakai untuk mengakses admin Router.

6. Saran

Perlu adanya penelitian lebih lanjut untuk mengembangkan *role* (*route*) yang dibangun pada Router. Misalnya membangun role yang lebih kompleks agar role tersebut lebih sulit untuk ditebak oleh hacker.

Daftar Pustaka

[1] W. Stallings and L. Brown, *Computer Security Principles and Practice*, Second. 2012.

[2] E. Hendratno, “8 Software Simulator jaringan

keren dan menarik untuk belajar jaringan." [Online]. Available: https://kopas.id/8-software-simulator-jaringan-keren-dan-menarik-untuk-belajar-jaringan/. [Accessed: 01-Jul-2018].

[3] B. Mahbooba and M. Schukat, "Digital certificate-based port knocking for connected embedded systems," in *2017 28th Irish Signals and Systems Conference (ISSC)*, 2017, pp. 1–5.

[4] D. Sel, S. H. Totakura, and G. Carle, "SKnock: Port-Knocking for Masses," *Proc. IEEE Symp. Reliab. Distrib. Syst.*, vol. 2016–Octob, pp. 1–6, 2016.

[5] A. Amarudin and Y. Atri, "Analisis Penerapan Mikrotik Router Sebagai User Manager Untuk Menciptakan Internet Sehat Menggunakan Simulasi Virtual Machine," *J. TAM (Technology Accept. Model.*, vol. 9, no. 1, pp. 62–66, 2018.

[6] F. H. Mohd Ali, R. Yunos, and M. A. Mohamad Alias, "Simple port knocking method: Against TCP replay attack and port scanning," *Proc. 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic, CyberSec 2012*, pp. 247–252, 2012.

[7] Mikrotik, "Mikrotik News," 2018. [Online]. Available: https://mikrotik.com/software. [Accessed: 30-Apr-2018].

[8] Bhinneka.Com, "No Title." .

[9] L. Herlina, "Pengertian GNS3 dan Konfigure," 2017. [Online]. Available: https://gualinaherlinablog.wordpress.com/2017/01/13/pengertian-gns3-dan-konfigure/. [Accessed: 12-Feb-2018].

[10] No name, "Definisi Hacking," 2014. [Online]. Available: https://penjelasanhacking.wordpress.com/2014/06/27/definisi-umum-hacking/.

Ucapan Terimakasih

Terima kasih kepada Direktorat Riset dan Pengabdian kepada Masyarakat (DRPM) Dikti yang telah mendanai kegiatan penelitian ini pada skema Penelitian Dosen Pemula (PDP) sesuai dengan kontrak penugasan pelaksanaan penelitian nomor SK:0045/E3/LL/2018 dan Nomor Kontrak PenelitianLPPM Universitas Teknokrat Indonesia nomor: 011/LPPMUTI/PDP/VI/2018.

Terima kasih juga peneliti sampaikan kepada LPPM Universitas Teknokrat Indonesia yang telah memfasilitasi kegiatan penelitia ini khususnya tim Pusat TIK atas fasilitas perangkat dan laboratorium yang telah digunakan