p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING

Amarudin
Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
Jl. Zainal Abidin Pagar Alam, No.9-11, Labuhanratu, Bandarlampung
amarudin@teknokrat.ac.id

Abstrak

Perkembangan teknologi sampai saat ini terus berkembang. Perkembangan tersebut berdampak pada keamanan sistem yang ada di dalamnya. Sehingga bagi pengguna aplikasi yang terhubung pada jaringan internet perlu lebih waspada terhadap penetrasi yang dilakukan oleh pihak lain yang tidak bertanggung jawab. Tidak sedikit pengguna jaringan (internet) yang telah menjadi korban penetrasi. Kewaspadaan ini tentunya tidak cukup hanya dilakukan oleh pengguna jaringan internet saja melainkan juga perlu dilakukan bagi pengelola jaringan (Administrator Jaringan). Untuk meningkatkan keamanan jaringan dari penetrasi yang dilakukan oleh para hacker, maka perlu adanya penelitian yang dapat memberikan solusi terhadap permasalahan tersebut. Sebagai salah satu solusi dari permasalahan tersebut, maka dalam penelitian ini dibangun sebuah protocol pada filewall yang disebut dengan Port Knocking. Dimana fungsi Port Knocking ini adalah untuk menjaga hak akses perangkat Router dari pengguna yang tidak berwenang untuk mengaksesnya. Metode Port Knocking merupakan salah satu metode keamanan jaringan yang diterapkan pada Mikrotik Router OS dengan cara kerja yaitu dapat membuka atau menutup akses Port tertentu melalui firewall pada Router sesuai dengan role yang dibangun. Adapun role Port Knocking yang dibangun pada firewall dalam penelitian ini memanfaatkan empat port yaitu Port 8291 (Winbox), Port 23 (telnet), dan Port 80 (Webfix). Dan waktu akses masing-masing port selama 10 detik. Berdasarkan hasil analisis dan pengujian implementasi sistem yang dilakukan, didapatkan hasil bahwa sistem dapat berjalan dengan baik dan dapat meningkatkan keamanan sistem jaringan yang dibangun dibandingkan pada jaringan yang tidak menerapkan keamanan Port Knocking. Hal ini dibuktikan dengan adanya autentikasi yang tepat saat mengakses Router. Yaitu autentikasi yang sesuai dengan role yang telah dibangun.

Kata kunci: Mikrotik Router OS, Penetrasi, Firewall, Port Knocking, Role.

Abstract

The technological developments to date continue to grow. These developments have an impact on the security of the system in it. So that application users connected to the internet network need to be more aware of the penetration carried out by other irresponsible parties. Not a few network users (internet) who have been victims of penetration. This caution is certainly not enough to be done only by internet network users but also needs to be done for network managers (Network Administrators). To improve network security from penetration by hackers, there is a need for research that can provide solutions to these problems. As one of the solutions to these problems, in this study a protocol was built in a filewall called Port Knocking. Where the Port Knocking function is to maintain Router device access rights from users who are not authorized to access it. Port Knocking method is one of the network security methods that are applied to the Mikrotik Router OS by working that can open or close certain access ports through the firewall on the Router in accordance with the role being built. The Port Knocking role built in the firewall in this study utilizes four ports, namely Port

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

8291(Winbox), Port 23 (Telnet), and Port 80 (Webfix). And the access time of each port for 10 seconds. Based on the results of the analysis and testing of the system implementation, the results show that the system can run well and can improve the security of the network system that is built compared to networks that do not implement Port Knocking security. This is evidenced by the right authentication when accessing the Router. That is authentication that matches the role that has been built.

Keywords : Mikrotik Router OS, Penetration, Firewall, Port Knocking, Role.

PENDAHULUAN

Perkembangan teknologi sampai saat ini terus berkembang. Perkembangan tersebut berdampak pada keamanan sistem yang ada di dalamnya. Sehingga bagi pengguna aplikasi yang terhubung pada jaringan internet perlu lebih waspada terhadap penetrasi yang dilakukan oleh pihak lain yang tidak bertanggung jawab. Tidak sedikit pengguna jaringan (internet) yang telah menjadi korban penetrasi. Salah satu penetrasi yang berhasil dilakukan adalah penetrasi terhadap website resmi MUI yang berhasil diretas oleh hacker (Iqbal, 2012). Kemudian kasus yang sama juga kembali terjadi pada website MUI pada tahun 2016 bahwa website tersebut telah berhasil diretas pada hari Minggu 28 Agustus 2016 (Azis, 2016). Dengan demikian para *user*/pengguna internet harus lebih waspada terhadap kejadian-kejadian penetrsi yang bisa dialamai kapan saja dan dimana saja jika tidak memperhatikan tingkat keamanan tersebut.

Kewaspadaan ini tentunya tidak cukup hanya dilakukan oleh pengguna jaringan internet saja, melainkan juga perlu dilakukan bagi pengelola jaringan (Administrator Jaringan). Untuk meningkatkan keamanan jaringan dari penetrasi yang dilakukan oleh para hacker, maka perlu adanya penelitian yang dapat memberikan solusi terhadap permasalahan tersebut. Salah satu penelitan yang telah membahas tentang keamanan jaringan diantaranya adalah penelitian yang pernah dilakukan oleh peneliti sebelumnya dengan judul "Analisis Penerapan Mikrotik Router Sebagai *User Manager* Untuk Menciptakan Internet Sehat Menggunakan Simulasi *Virtual Machine*" (Amarudin & Atri, 2018). Selain itu juga pernah dibahas dalam penelitian sebelumnya yang membahas terkait desain sistem keamanan jaringan pada Mikrotik Router OS menggunakan metode Port Knocking (Amarudin, 2018).

Berdasarkan kondisi yang terjadi di lapangan saat ini, dirasa sangat penting untuk dibahas dan diteliti lebih lanjut terkait keamanan jaringan, dengan harapan kedepan dapat meningkatkan sistem keamanan yang lebih baik khususnya pada media komunikasi lokal maupun interlokal (internet). Dalam penelitian ini mengusulkan sebuah metode analisis terhadap implementasi Port Knocking pada Mikrotik Router OS yaitu menggunakan metode *scanning* dan *sniffing*. Adapun tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui tingkat keamanan atas implementasi kemanan jaringan pada perangkat Router yang telah dibangun di Universitas Teknoikrat Indonesia.

Port Knocking

Port-knocking adalah sebuah 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 (Sel, Totakura, & Carle, 2016).

Hacking

Hacking adalah kegiatan memasuki *system* melalui *system* operasional lain yang dijalankan oleh Hacker. Tujuanya untuk mencari *hole/bugs* pada *system* yang akan dimasuki. Dalam arti lain mencari titik keamanan *system* tersebut. Bila hacker berhasil masuk pada *system* itu, hacker dapat mengakses hal apapun sesuai keinginan hacker itu. Dari kegiatan yang mengacak *system* maupun berupa tindakan kejahatan (Dimas, 2018).

Defacing

Defacing adalah kegiatan merubah halaman website orang lain. Deface terkadang hanya sekedar untuk iseng, uji kemampuan, bahkan memamerkan kemampuan. Tapi terkadang

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

defacer banyak yang ikut mencuri data-data website sebelum melakukan perubahan tampilan pada website tersebut (Dimas, 2018).

Cracking
Cracking memiliki prinsip yang sama dengan hacking, namun tujuannya cenderung tidak baik. Pada umumnya cracker mempunyai kebiasaan merusak, mengambil data bahkan informasi penting. Cracking biasa dipanggil Blackhat Hacker. Cracker cenderung meretas berbagai *system* hanya untuk kesenangan tersendiri (Dimas, 2018).

Carding
Sama halnya dengan cracking. Carder mencari dan mencuri data *account* yang ada di *system* untuk dipakai sendiri atau bersama tim sesama carder. Dengan menggunakan alat bantu seperti *software* maupun tidak, carder dapat menjebol *system* yang sangat rentan dengan pembayaran *online*. Carder juga termasuk Blackhat Hacker. Carding biasanya dilakukan diberbagai tempat berbelanja secara *online* (Dimas, 2018).

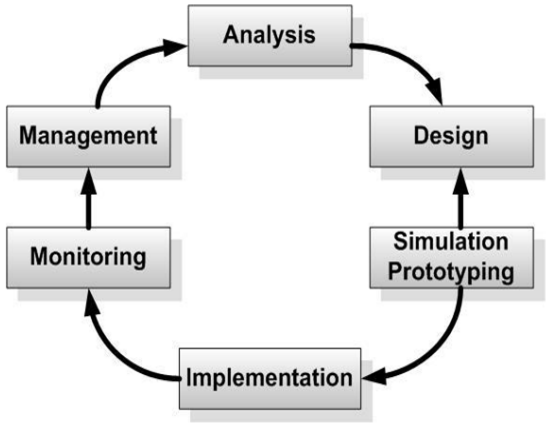
Port Scanning
Port scanning adalah teknik mendeteksi port-port yang terbuka pada sebuah komputer. Kita dapat melakukan port scanning pada komputer lain melalui jaringan. Tujuannya hanyalah untuk melihat port-port berapa saja yang terbuka pada kompoter tersebut (Iskandar, 2011).

Sniffing
Sniffing adalah tindakan penyadapan yang dilakukan dalam jaringan dengan tujuan untuk dapat mencuri data-data pribadi ataupun account lain yang bersifat pribadi. Karena data yang mengalir pada suatu jaringan bersifat bolak-balik, maka dengan proses sniffing ini dapat menangkap paket yang dikirimkan dan terkadang menguraikan isi dari RFC (*Request for Comments*).(Jong, 2013).

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 (Mikrotik, 2018).

METODE

Metode atau tahapan penelitian yang digunakan dalam penelitian ini menggunakan metode NDLC (*Network Design Life Cycle*), sehingga rangkaian proses penelitian dapat dilakukan secara terarah, teratur dan sistematis sebagaimana dijelaskan pada Gambar 1.



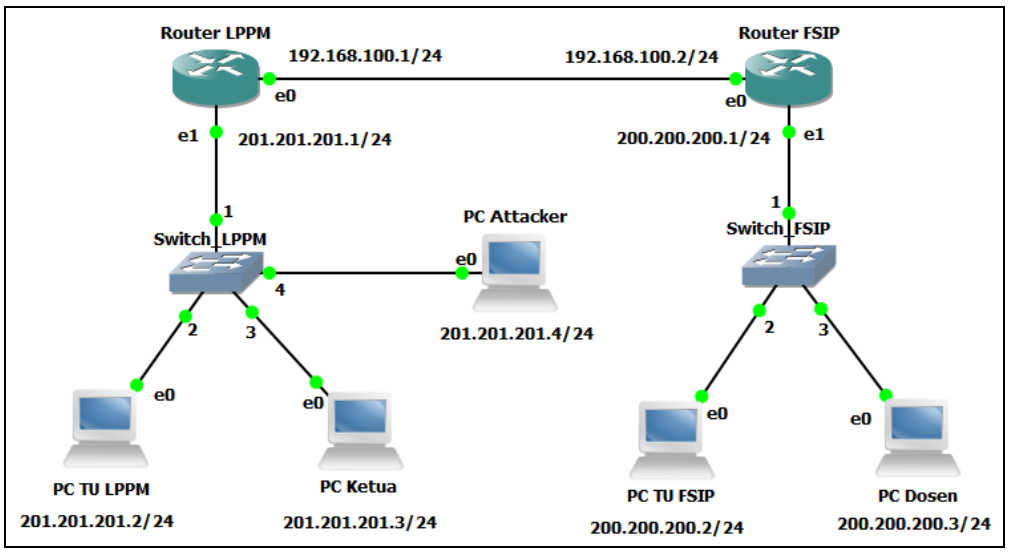
Gambar 1. Tahapan Penelitian Menggunakan NDLC (Wikosoul, 2010)

Tahap *Analysis*
Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang digunakan adalah sebagai berikut:

a) Wawancara, dilakukan dengan pihak terkait dalam hal ini adalah staf Pusat TIK tentang manajemen jaringan yang berjalan saat ini dan harapan yang diinginkan.
b) Observasi, melakukan pengamatan secara langsung pada divisi LPPM yang ada di Universitas Teknokrat Indonesia untuk mendapatkan hasil yang lebih valid dan nantinya merupakan menjadi gambaran dasar untuk masuk ke tahap desain.

Tahap *Design*
Pada tahap ini dilakukan desain topologi keamanan jaringan menggunakan simulator GNS3. Adapun komponen yang diperlukan antara lain: dua buah Router, dua buah Switch, empat PC Client dan satu buah PC sebagai Attacker. Desain topologi keamanan jaringan yang dibangun bisa dilihat pada Gambar 2.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 2. Desain Topologi Keamanan Jaringan

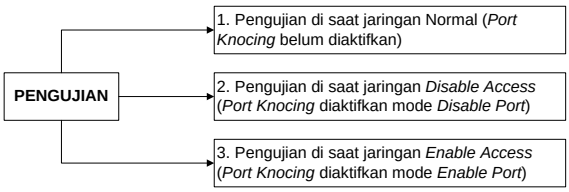
Berdasarkan topologi (Gambar 2), konfigurasi *firewall* sebagai otentikasi Port Knocking yang dibangun dalam penelitian ini berada pada Router LPPM. Pada kedua Router tersebut dibangun sebuah *role firewall* sebagai *role* yang harus digunakan oleh *user*/admin ketika akan mengakses Router sebagai Administrator.

Sedangkan fungsi PC Attacker adalah sebagai media tester (penguji) fungsionalitas Port Knocking pada kedua Router tersebut yang telah dibangun apakah dapat berhasil dijalankan atau tidak.

Tahap *Simulation Prototyping*

Pada tahap ini dilakukan simulasi atas desain jaringan yang telah dibangun menggunakan simulator GNS3 dan mengkonfigurasi pada Router LPPM berupa konfigurasi Port Knocking sebagai langkah untuk pengamanan jaringan. Pada tahap ini juga dilakukan simulasi pengujian sistem. Adapun skenario pengujian sistem sebagai berikut:

Skenario pengujian dilakukan dalam tiga tahap. Pengujian pertama dilakukan pada saat jaringan normal tanpa ada penerapan Port Knocking. Pengujian kedua dilakaukan pada saat jaringan sudah menerapkan Port Knocking dengan mode *Disable Port.* Pengujian ketiga dilakukan pada saat jaringan sudah menerapkan Port Knocking namun mode yang digunakan adalah mode *Enable Port*. Adapun diagram skenario pada pengujian ini bisa dilihat pada Gambar 3.



Gambar 3. Skenario Pengujian Sistem

Tahap *Implementation*

Pada tahap ini dilakukan implementasi sistem keamanan jaringan yang telah didesain pada tahap sebelumnya. Adapun lokasi implementasi ini berada di Gedung LPPM. Pada tahap implementasi ini dilakukan pengujian hacking pada Router yang telah dikonfigurasi pada tahap sebelumnya.

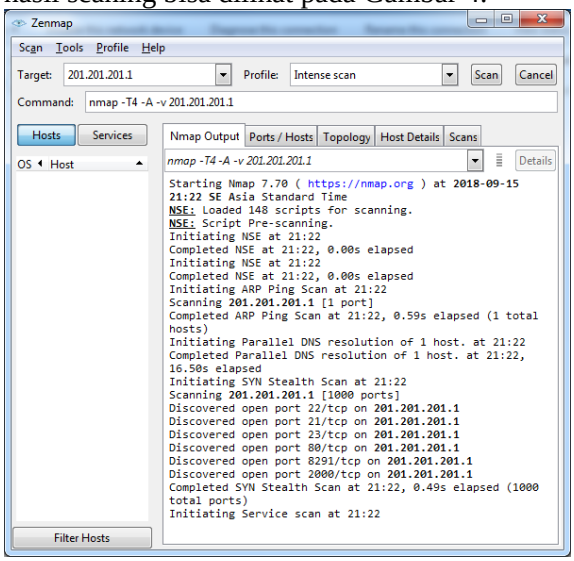
Fungsi pengujian ini adalah untuk mengetahui apakah konfigurasi dan implementasi Port Knocking yang dibangun sudah berhasil dengan baik dan sesuai dengan yang diharapkan atau tidak. Adapun jenis-jenis pengujian yang dilakukan ada tiga jenis, yaitu pengujian *Scanning*, *Sniffing* dan *Authentication*, dimana ketiga pengujian ini dilakukan pada kondisi sistem jaringan berada dalam tiga Mode yaitu (Mode Normal, Mode *Disable Access*, dan Mode *Enable Access*).

Pengujian *Scanning* Mode Normal

Pada tahap ini dilakukan *scanning* pada jaringan kondisi normal (belum diterapkan metode Port Knocking). *Scanning* ini dilakukan pada Router LPPM (201.201.201.1/24). Berdasarkan hasil *scanning* yang dilakukan, didapatkan hasil bahwa port yang ada pada jaringan pada mode

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

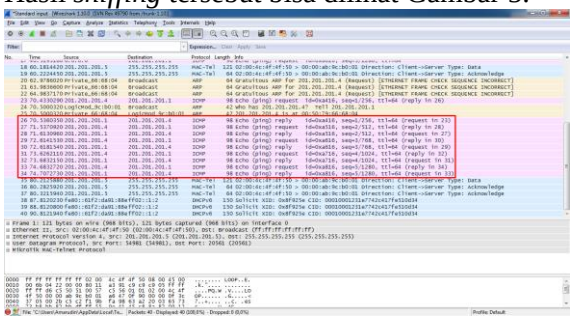
normal masih bisa di-*scan* dan terbaca. Adapun hasil scaning bisa dilihat pada Gambar 4.



Gambar 4. *Port Scanning* pada Mode Normal

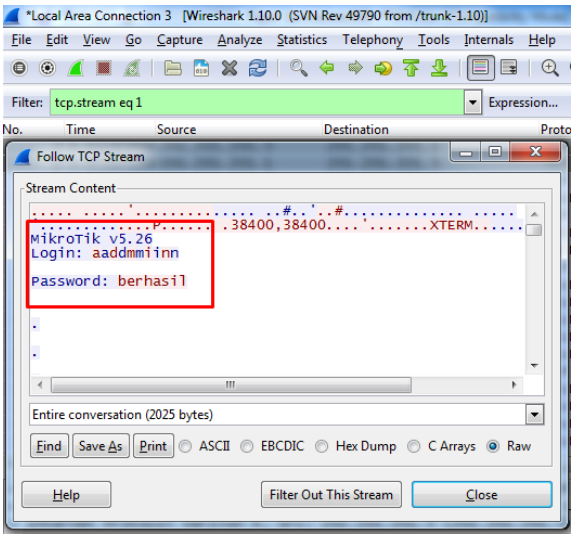
Pengujian *Sniffing* Mode Normal

Pada pengujian *sniffing* mode normal ini didapatkan hasil bahwa ketika Ruter LPPM diakses via winbox (8291) maupun webfix (80) maka dapat disadap untuk *user name*-nya saja. Namun *password* yang digunakan telah dienkripsi, sehingga tidak mudah untuk dibaca. Hasil *sniffing* tersebut bisa dilihat Gambar 5.



Gambar 5. *Sniffing* Router LPPM via winbox (8291) dan webfix (80)

Akan tetapi ketika Router LPPM diakses via Telnet (23), ternyata *username* dan *password* yang digunakan untuk login ke Router LPPM tersebut masih bisa disadap dan tidak terenkripsi, sehingga sangat mudah untuk disadap. Hasil sniffing tersebut bisa dilihat pada Gambar 6.



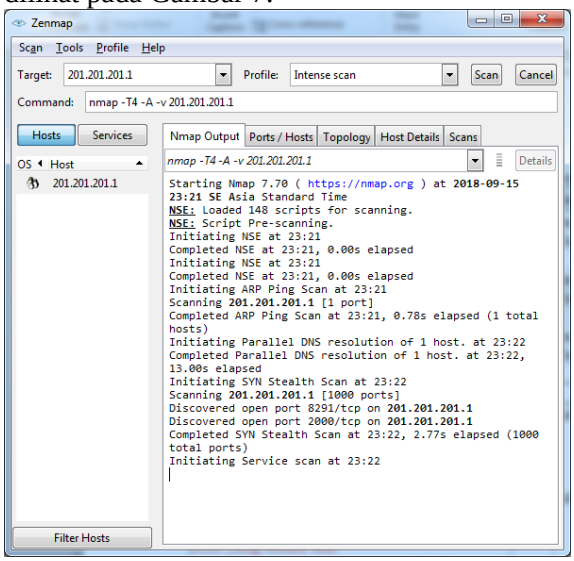
Gambar 6. *Sniffing* Router via Telnet (23)

Pengujian *Authentication* Mode Normal

Pada tahap ini dilakukan pengujian otentikasi dengan cara login ke Router LPPM menggunakan beberapa *tools*, yaitu (winbox (8291), Webfix (80) dan telnet (23). Berdasarkan pengujian ini didapatkan hasil bahwa dari ketiga pengujian ini berhasil login.

Pengujian *Scanning* Mode *Disable*

Berdasarkan hasil *scanning* yang dilakukan pada tahap ini didapatkan hasil bahwa port yang ada pada jaringan pada mode *disable* tidak bisa di-*scan* (tidak terbaca). Adapun hasil *scaning* bisa dilihat pada Gambar 7.

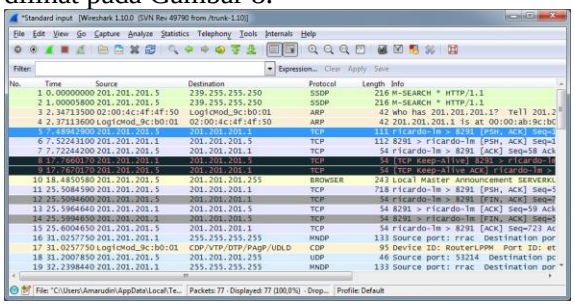


Gambar 7. *Port Scanning* pada Mode *Disable*

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Pengujian *Sniffing* Mode *Disable*

Pada pengujian *sniffing* mode disable ini didapatkan hasil bahwa ketika Ruter LPPM diakses via winbox (8291) , telnet (23) maupun webfix (80), maka tidak dapat disadap baik *user name* maupun *password*-nya, dan telah terenkripsi, sehingga tidak mudah untuk dibaca. Hasil *sniffing* via winbox, telnet dan webfix bisa dilihat pada Gambar 8.



Gambar 8. *Sniffing* Router LPPM via winbox (8291), telnet (23) dan webfix (80)

Pengujian *Authentication* Mode Disable

Pada tahap ini dilakukan pengujian otentikasi dengan cara login ke Router LPPM menggunakan beberapa *tools*, yaitu (winbox (8291), Webfix (80) dan telnet (23). Berdasarkan pengujian ini didapatkan hasil bahwa dari ketiga pengujiannya tidak berhasil login.

Pengujian *Scanning, Sniffing* dan *Authentication* Mode Enable

Berdaasrkan pengujian yang dilakukan pada mode *enable* ini didapatkan hasil bahwa port yang diaktifkan (tanpa port knocking) bisa di-*scan* serta *user name* dan *password* bisa disadap. Begitupula untuk otentikasi bisa berhasil dilakukan.

Tahap *Monitoring*

Pada tahap ini dilakukan monitoring terhadap infrastruktur yang sudah dibuat untuk melihat dan memastikan bahwa konfigurasi Port Knocking dapat berjalan sesuai dengan harapan dan memenuhi kebutuhan.

Tahap *Management*

Pada tahap terakhir perlu dibuatkan kebijakan manajemen untuk mengatur sistem yang sudah dikembangkan agar dapat berjalan dengan baik dan dapat berlangsung lama serta unsur *security* dapat terjaga dengan baik sesuai dengan yang diharapkan.

HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis dan pengujian sistem yang dilakukan, diperoleh hasil bahwa konfigurasi Port Knocking dapat berfungsi dengan baik. Berdasarkan pengujian, pada saat sistem jaringan berada pada mode normal dapat di-*scaning*, di-*sniffing* dan berhasil login. Pada saat mode *disable access*, tidak dapat di-*scan*, di-*sniffing* maupun login juga tidak berhasil. Dan pada saat sistem jaringan berada pada mode *enable access* dapat di-*scan*, dapat di-*sniffing* dan berhasil login sebagaimana pada mode normal. Adapun hasil lengkap pengujian bisa dilihat pada

Tabel 1.

Tabel 1. Hasil Pengujian

No	Mode Access	Jenis Pengujian	Alat Uji (*tools*)	Hasil Pengujian
1	Mode Normal	*Scanning*	Nmap	*Discovered open port*
2	Mode Normal	*Sniffing*	Wireshark	Terenkripsi, kecuali Telnet.
3	Mode Normal	*Authentication*	-	Berhasil *Login*
4	Mode *Disable Access*	*Scanning*	Nmap	*Port Disable*
5	Mode *Disable Access*	*Sniffing*	Wireshark	Terenkripsi, kecuali Telnet.
6	Mode *Disable Access*	*Authentication*	-	Gagal *Login*
7	Mode *Enable Access*	*Scanning*	Nmap	*Discovered open port*
8	Mode *Enable Access*	*Sniffing*	Wireshark	Terenkripsi, kecuali Telnet.
9	Mode *Enable Access*	*Authentication*	-	Berhasil *Login*

SIMPULAN DAN SARAN

Dengan adanya penerapan implementasi keamanan jaringan menggunakan metode Port Knocking, dapat meminimalisir terjadinya penyalahgunaan akses Router dari pihak yang tidak bertanggung jawab.

Adapun saran untuk penelitian lebih lanjut ialah perlu adanya pengujian yang dilakukan menggunakan *tools* hacking lainnya

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

yang lebih tinggi tingkat teknologi pengujiannya. Selain itu juga perlu dilakukan pengembangan metode port knocking yang digunakan.

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 nomor SK:0045/E3/LL/2018 dan Nomor Kontrak Penelitian: 011/LPPM-UTI/PDP/VI/2018.

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

DAFTAR PUSTAKA

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo, 12*(2), 35-38.

Amarudin, A., & Atri, Y. (2018). Analisis Penerapan Mikrotik Router Sebagai User Manager Untuk Menciptakan Internet Sehat Menggunakan Simulasi Virtual Machine. *Jurnal TAM (Technology Acceptance Model), 9*(1), 62-66.

Azis, L. (2016). Disangka Markas ISIS, Situs Resmi MUI Di-HACK Retrieved 1 Juni 2018, 2018, from https://jalantikus.com/news/11527/situs-mui-di-hack/

Dimas, N. (2018). Pengertian Hacking, Cracking, Carding, dan Defacing. Retrieved from http://theamazingjoker.blogspot.com/2014/03/pengertian-hacking-cracking-carding-dan.html

Iqbal, M. (2012). Situs Resmi MUI Disusupi \'Jember\' Hacker Retrieved 3 Juni 2017, 2017, from https://news.detik.com/berita/d-1982971/situs-resmi-mui-disusupi-jember-hacker-

Iskandar, I. (2011). Belajar Port Scanning dan Sniffing. Retrieved from https://iwaniskandar.wordpress.com/2011/03/10/belajar-port-scanning-dan-sniffing/

Jong, R. (2013). 19 Mei 2013. Retrieved from http://reckyjong.blogspot.com/2013/05/sniffing.html

Mikrotik. (2018). Mikrotik News, from https://mikrotik.com/software

Sel, D., Totakura, S. H., & Carle, G. (2016, 26-26 Sept. 2016). *sKnock: Port-Knocking for Masses.* Paper presented at the 2016 IEEE 35th Symposium on Reliable Distributed Systems Workshops (SRDSW).

Wikosoul. (2010). Tahapan pada Network Development Life Cycle (NDLC). Retrieved from https://wikusoul.wordpress.com/2010/07/26/tahapan-pada-network-development-life-cycle-ndlc/