Journal of Informatics and Computer Science Vol. 8 No. 1 April 2022
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS V6.48.3 MENGGUNAKAN METODE PORT KNOCKING

NETWORK SECURITY ANALYSIS USING THE METHOD SNIFFING AND IMPLEMENTATION OF NETWORK SECURITY ON MICROTIK ROUTER OS V6.48.3 USING PORT KNOCKING METHOD

Rizka Albar [1], Rian Okta Putra [2]
[1-2] Universitas Ubudiyah Indonesia
Jl. Alue Naga, Tibang. Kec. Syiah Kuala, Banda Aceh, Indonesia
Email Corespondensi: albar@uui.ac.id, rianokta2017@gmail.com

Abstak - Perkembangan teknologi dibidang jaringan komputer pada revolusi industri 4.0 saat ini semakin berkembang pesat, pada akhirnya jaringan komputer salah satu teknologi yang sangat penting bagi semua kalangan seperti Universitas. Perkembangan tersebut juga berdampak pada keamanan dalam sebuah jaringan yang ada di lingkungan. *Software* yang terhubung pada sebuah jaringan juga perlu diwaspadai terhadap penyadapan yang dilakukan oleh pihak tidak bertanggung jawab *(Attecker)*. Dalam hal ini tidak sedikit pula Universitas yang menggunakan jaringan telah banyak menjadi korban penyadapan. permasalahan ini tentunya tidak bisa terlepas dari pengelola jaringan seperti (Administrator Jaringan). Untuk melakukan peningkatkan keamanan jaringan dari penyadapan yang dilakukan oleh *Attecker*, maka sangan perlu adanya sebuah penelitian yang dapat memberikan solusi terhadap permasalahan didalam sebuah jaringan. Sebagai salah satu solusi dari permasalahan yang ada didalam sebuah jaringan, maka dalam penelitian ini penulis membangun sebuah metode keamanan pada *firewall* yang penulis sebut dengan metode keamanan *Port Knocking* di *Mikrotik Router Os V6.48.3*. Dimana fungsi dari *metode Port Knocking* ini adalah untuk menjaga hak akses perangkat *Router Mikrotik Router Os V6.48.3* dari pengguna yang tidak bertanggung jawab untuk mengaksesnya *(Attecker)*. Adapun *Rules Port Knocking* yang penulis terapkan pada *firewall* dalam penelitian ini memanfaatkan *Port 23 (telnet), Port 80 (Webfig). Port 8291 (Winbox)* dan *Port 21 (FTP)* serta waktu akses yang penulis terapkan yaitu dalam masing-masing *port* selama 5 detik. Berdasarkan hasil analisis keamanan jaringan dan pengujian implementasi *port knocking* yang sudah dilakukan, didapatkan hasil bahwa Metode keamanan *port Knocking* dapat berjalan dengan *Optimal* dan dapat meningkatkan keamanan jaringan yang diimplementasikan pada *Mikrotik Router Os V6.48.3* dibandingkan pada jaringan yang tidak menerapkan keamanan *Port Knocking*. Hal ini penulis buktikan dengan melakukan *Authentication* yang tepat saat mengakses *Router Mikrotik Router Os V6.48.3*.

Kata Kunci : Jaringan, *Mikrotik Router Os V6.48.3, Port Knocking, Atteckker, Firewal*

Abstrack - The development of technology in the field of computer networks in the industrial revolution 4.0 is currently growing rapidly, in the end computer networks are one of the most important technologies for all circles, such as universities. These developments also have an impact on security in a network that exists in the environment. Software that is connected to a network also needs to be wary of eavesdropping by irresponsible parties (Attecker). In this case, not a few universities that use the network have become victims of eavesdropping. This problem certainly cannot be separated from network managers such as (Network Administrator). To improve network security from wiretapping carried out by Attecker, it is very necessary to have a research that can provide solutions to problems in a network. As a solution to the problems that exist in a network, in this study the author builds a security method on the firewall which the author calls the Port Knocking security method on the Mikrotik Router Os V6.48.3. Where the function of the Port Knocking method is to maintain the access rights of the Mikrotik Router Os V6.48.3 Router from users who are not responsible for accessing it (Attecker). The Port Knocking Rules that the author applies to the firewall in this study utilize Port 23 (telnet), Port 80 (Webfig). Port 8291 (Winbox) and Port 21 (FTP) and the access time that the author applies is in each port for 5 seconds. Based on the results of network security analysis and port knocking implementation tests that have been carried out, the results show that the port Knocking security method can run optimally and can improve network security which is implemented on Mikrotik Router Os V6.48.3 compared to networks that do not implement Port Knocking security. This author proves by doing the right Authentication when accessing the Mikrotik Router Os V6.48.3 Router.
Keywords: Network, Mikrotik Router Os V6.48.3, Port Knocking, Atteckker, Firewall

I. PENDAHULUAN

Perkembangan teknologi dibidang jaringan komputer pada revolusi industri 4.0 saat ini semakin berkembang pesat, pada akhirnya jaringan komputer salah satu teknologi yang sangat penting bagi semua kalangan seperti Universitas.

Jaringan komputer juga dapat memudahkan pengguna/*user* dalam segala bidang seperti halnya didunia pendidikan. Namun salah satu teknologi jaringan komputer yang paling banyak digunakan di Unit Kerja di Universitas adalah *Local Area Network* (LAN).

Keamanan jaringan menjadi sangat penting dan harus diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat disadap oleh para *Attecker*, baik di jaringan *Local Area Network (LAN)* maupun *Wireless.* Seperti pada saat data dikirim melewati beberapa terminal untuk sampai ke tujuan berarti akan memberikan kesempatan kepada *user* lain yang tidak bertanggung jawab untuk menyadap atau mengubah data *(Attecker)*, bahkan sampai merusak atau mencuri data tersebut.

Universitas Ubudiyah Indonesia sejak dulu sudah memiliki jaringan *Internet* dan menggunakan LAN yang memamfaatkan *router* dan beberapa *switch*. Permasalahan yang penulis dapati saat ini belum adanya pengujian tingkat keamanan jaringan yang ada di Universitas Ubudiyah Indonesia dalam hal ini bagian ICT juga belum mengetahui tingkat keamanan Jaringan yang ada di lingkungan Universitas Ubudiyah Indonesia dari sebuah ancaman penyerangan.

Berdasarkan permasalahan yang penulis paparkan diatas, dalam penelitian ini penulis mengusulkan sebuah judul *"Analisis Keaman an Jaringan Menggunakan Metode Sniffing Dan Impl ementasi Keamanan Jarigan Pada Mikrotik Router O s V6.48.3 Menggunakan Metode Port Knocking",* dalam penelitian ini penulis tertarik melakukan pengujian keamanan jaringan dengan melakukan penyadapan dengan Metode *Sniffing* menggunakan *Wireshark* serta menerapkan metode *Port Knocking* untuk keamanan jaringan pada *Mikrotik Router OS V6.48.3*, pengujian yang penulis lakukan berdasarkan permasalahan yang penulis temukan dalam sebuah jaringan yang telah penulis paparkan diatas.

Tujuan dari penelitian ini adalah untuk mengetahui tingkat keamanan jaringan beserta meningkatkan keamanan jaringan untuk menghindari dari pihak yang tidak bertanggung jawab untuk melakukan pencurian data *(Attecker).*

II. TINJAUAN PUSTAKA

A. Jaringan Komputer

Jaringan komputer (*computer network)* dapat diartikan sebagai dua atau lebih komputer yang dihubungkan dengan sebuah sistem komunikasi. Jaringan komputer menggunakan teknik komunikasi data namun lebih mementingkan arti dari tiap bit dalam proses pengiriman hingga diterima oleh tujuannya.

Dua unit komputer dikatakan terhubung atau terkoneksi apabila keduanya bisa saling bertukar informasi dan berbagi data, berbagi *resource* yang dimiliki, seperti file, printer, media penyimpanan *(Hardisk, floppy disk, cd-room, flash disk, dll).* Data yg berupa teks, audio, maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna perangkat komputer dapat saling bertukar data/*file*, mencetak data dengan printer yang sama dan menggunakan *hardware* dan *software* yang terkoneksi dalam jaringan yang sama, (M. R. Adriansyah, 2017).

B. *IP Address*

IP *address* adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP. IP *address* terdiri dari 32 bit angka *binary*, yang ditulis dalam empat kelompok terdari dari 8 bit (oktat) yang dipisah oleh tanda titik. (R.Fitria, 2020)

Contohnya:

11000000.00010000.00001010.00000001

Atau dapat ditulis dalam bentuk empat kelompok format desimal (0-255) misalnya :

192.16.10.1

Baik bilangan *binary* dan desimal merepresentasikan nilai yang sama. Namun IP *address* lebih mudah dimengerti dalam notasi bilangan desimal. Salah satu masalah dengan penggunaan bilangan *binary* adalah pengulangan bilangan 0 dan 1 yang panjang akan membuat kesempatan terjadi kesalahan semakin besar. (R.Fitria, 2020)

IP *address* yang terdiri atas 32 bit angka dikenal sebagai IP versi 4 (IPv4). IP *address* terdiri atas dua bagian yaitu *network ID* dan *host* ID, dimana *network* ID menentukan alamat jaringan sedangkan *host* ID menentukan alamat *host* atau komputer. Oleh sebab itu, IP *address* memberikan alamat lengkap suatu komputer berupa gabungan alamat jaringan dan alamat *host.* Berapa jumlah kelompok angka yang termasuk *network* ID dan berapa yang termasuk *host* ID adalah bergantung pada kelas IP *address* yang dipakai. (R.Fitria, 2020)

C. Ancaman Keamanan Jaringan Komputer

Menurut Kasim dkk (2017:8). *Port Forwarding* merupakan suatu teknik penerusan/pengalihan paket

data dari suatu *IP* ke *IP* lain dengan *port* tertentu menggunakan fungsi *Network Address Translation* (NAT).

Dengan adanya *Port forwarding*, suatu komputer bahkan kamera *IP* dapat diakses melalui jaringan *internet* meskipun perangkat tersebut berada dalam jaringan lokal (Lex Saint Dry, 2017:38).

D. Macam Macam Tindak Kejahatan Pada Dunia Maya

Menerut Amarudin, 2018, tindak kejahatan pada dunia maya dapat di bagi beberapa macam (Sebutan) yang dijelaskan pada poin dibawah ini.

1. 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 bolakbalik, maka dengan proses *sniffing* ini dapat menangkap paket yang dikirimkan dan terkadang menguraikan isi dari RFC (*Request for Comments*).

2. ***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 .

3. 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.

4. Carding

Sama halnya dengan *cracking*. *Carder* mencari dan mencuri data *account* yang ada di *system* untuk dipakai sendiri atau bersama tim sesame *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*.

5. ***Defacing***

Defacing adalah kegiatan merubah halaman *website* orang lain. Deface terkadang hanya sekedar untuk iseng, uji kemampuan, bahkan memamerkan kemampuan. Tapi terkadang *defacer* banyak yang ikut mencuri data-data *website* sebelum melakukan perubahan tampilan pada *website* tersebut.

6. Port Scanning

Port scanning adalah teknik mendeteksi *portport* yang terbuka pada sebuah komputer. Kita dapat melakukan *port scanning* pada computer lain melalui jaringan. Tujuannya hanyalah untuk melihat *port-port* berapa saja yang terbuka pada kompoter tersebut.

E. *Mikrotik Router OS*

Mikrotik Router OS adalah sistem operasi *Linux base* yang memberikan kemudahan bagi penggunanya untuk menjadikan komputer menjadi *router network* yang handal. *Mikrotik Router OS* marupakan *router software* yang dapat menggunakan peralatan *embedded* (minimum sistem) maupun menggunakan PC (personal komputer) serta kompatibel dengan IBM PC X86. (H.I. Pohan, 2019)

Mikrotik memiliki kemampuan pengamanan jaringan menggunakan *firewall* yang dapat digunakan secara "*statefull*" maupun "*stateless*". Kemampuan paket *tracking Mikrotik* memungkinkan administrator untuk melakukan monitoring jaringan dan melakukan analisa *troubleshooting*. Kemampuan monitor ini mampu menghasilkan informasi dengan format *software* pihak ketiga sehingga memudahkan Administrator jaringan bekerja dengan *software* monitoring seperti *Cisco Netflow* maupun NTOP. (H.I. Pohan, 2019)

Mikrotik mampu difungsikan sebagai *proxy server* dengan dukungan *Squid*. *Proxy server* ini dapat digunakan secara normal maupun secara transparan. Fungsi keamanan *proxy* ini dapat dengan mudah diatur berdasarkan tujuan, sumber maupun cara akses ke tujuan. (H.I. Pohan, 2019).

F. *Applikasi Wireshark*

Wireshark adalah alat penganalisis paket jaringan *open source* yang menangkap paket data yang melewati jaringan dan menyajikannya dalam bentuk yang dapat dimengerti. Wireshark dapat dianggap sebagai pisau tentara Swiss karena dapat digunakan dalam situasi yang berbeda seperti masalah jaringan, operasi keamanan, dan protokol pembelajaran internal. *Wireshark* mendukung berbagai protokol mulai dari TCP, UDP, dan HTTP ke protokol canggih seperti *AppleTalk* (H. Jamaluddin dan N.F. Sueb, 2018).

G. *Nmap*

Nmap ("*Network Mapper*") adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. *Nmap* menggunakan paket *IP raw* untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall/filter* paket yang digunakan, dan sejumlah

karakteristik lainnya. *Output Nmap* adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. (D.B. Rendro, Dkk, 2020).

H. *Port Knocking*

Port knocking adalah sebuah metode membuka *port* secara *eksternal* melalui *firewall* dengan cara melakukan usaha koneksi pada suatu *port* yang tertutup dengan urutan upaya koneksi yang telah ditentukan. Dengan kata lain *port knocking* adalah sebuah metode untuk membangun sebuah komunikasi *host-to-host* dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas, (E.Haryanto, 2013).

Port knocking diimplementasikan dengan mengkonfigurasi Sebuah program kecil yang disebut daemon guna memonitor log firewall untuk permintaan koneksi dan menentukan apakah klien terdaftar pada alamat IP yang disetujui dan telah melakukan urutan ketukan yang benar. Jika jawabannya adalah ya, firewall akan membuka port yang terkait secara dinamis, (E.Haryanto, 2013).

Tujuan utama dari port knocking adalah mencegah penyerang dari pemindai sistem seperti SSH dengan melakukan port scanning. Jika penyerang mengirimkan urutan ketukan yang salah, port yang dilindungi tidak akan muncul atau terbuka**.**

III. METODE PENELITIAN

A. Jenis Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode Komparatif dengan pendekatan kuantitatif, yaitu penelitian yang hasilnya diolah dan dianalisis untuk diambil kesimpulannya. Penelitian komparatif adalah sejenis penelitian deskriptif yang ingin mencari jawaban secara mendasar tentang sebab-akibat, dengan menganalisis faktor-faktor penyebab terjadinya ataupun munculnya suatu fenomena tertentu. bertujuan untuk menghasilkan tingkat keamanan jaringan yang lebih baik lagi.

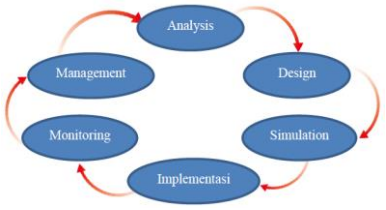
B. Tahapan Yang Akan dilakukan

Melakukan perencanaan dalam penelitian tentang data yang akan diambil pada saat melakukan penelitian seperti.

1. *Pasword* dan *Username*
2. *IP Address*
3. *Domain*.
4. Pengujian *Port Scanning* Mode Normal
5. Pengujian *Sniffing* Mode Normal
6. Pengujian *Authentication* Mode Normal
7. Pengujian *Port Scanning* Mode *Port Snoking* (Aktif)
8. Pengujian *Sniffing* Mode *Port Snoking* (Aktif)
9. Pengujian *Authentication* Mode (Aktif)
10. Pengambilan data dalam kondisi keamanan jaringan Normal (kondisi saat ini) dan disaat kondisi keamanan jaringan menggunakan metode *Port Knocking.*
11. Pengumpulan data selesai

I. Metode Pengembangan Jaringan

Metode yang penulis gunakan dalam pengembangan jaringannya menggunakan metode *Network Development Life Cycle* (NDLC) yaitu metode yang digunakan sebagai acuan (secara keseluruhan atau secara garis besar) pada proses pengembangan dan perancangan sistem jaringan yang merupakan suatu pendekatan proses dalam jaringan yang menggambarkan siklus awal dan akhirnya dalam membangun sebuah jaringan komputer. Tahapan dalam metode ini, yaitu :

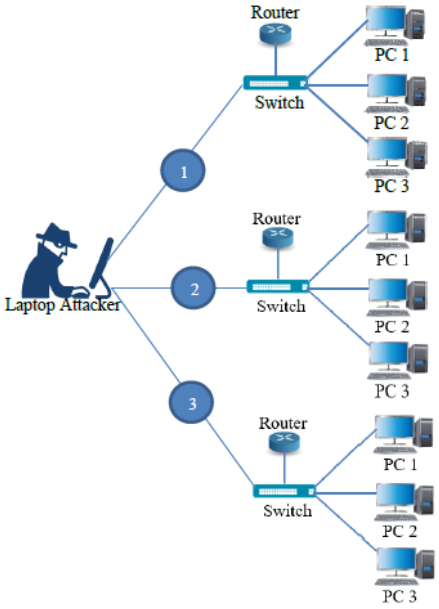


Gambar 1. Metode *Network Development Life Cycle* (NDLC)

C. TahapanPengujian Serangan

Pada tahapan ini dilakukan pengujian terhadap jaringan yang sudah ada sebelumnya menggunakan *Zenmap* dan *Wireshark* untuk melakukan proses *sniffing*, sebagai langkah untuk mencari kelemahan keamanan jaringan, serta mengkonfigurasi *Port Knocking* sebagai langkah untuk keamanan jaringan, pada tahapan ini juga akan dilakukan pengujian tingkat keamanan jaringan.

Tahapan pengujian dilakukan tiga tahapan. Pengujian pertama dilakukan dalam kondisi jaringan kurang baik (keadaan seperti yang sudah ada) tanpa adanya penerapan *Port Knocking*. Pengujian Kedua dilakukan dalam keadaan jaringan sudah menerapkan *Port Knocking* (Aktif) dan pada tahapan akhir, yaitu pengujian dalam tahapan ini sudah menerapkan *Port Knocking*, namun keadaan *Port Knocking* dalam keadaan *(Non Aktif).* Adapun Tahapan dalam pengujian diperlihatkan pada gambar dibawah ini.



Gambar 2. Tahapan pengujian dilakukan tiga tahapan Keadaan Normal, Metode Port Snoking (Aktif) dan Port Knocking.

Adapun keterangan dari Gambar Tahapan diatas adalah sebagai Berikut :

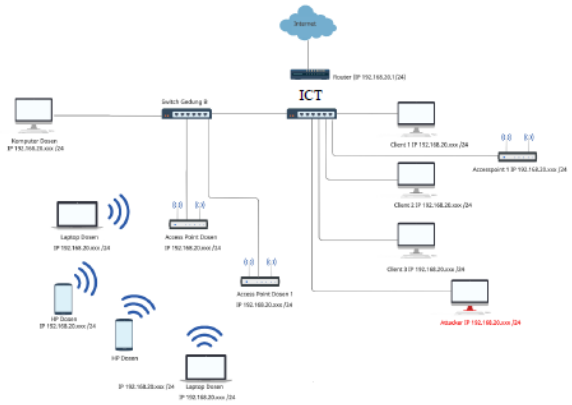
1. Pengujian di saat jaringan Normal (keadaan seperti yang sudah ada) tanpa adanya penerapan *Port Knocking*.
2. Pengujian dilakukan dalam keadaan jaringan sudah menerapkan *Port Knocking* (Aktif)
3. Pengujian *Port Knocking* dalam keadaan (Non Aktif).

Fungsi dalam pengujian ke tiga tahapan di atas adalah untuk mengetahui tingkat keamanan jarigan yang sudah ada masih bisa di serang/penyadapan oleh *Attecker*, dan fungsi selanjutnya untuk mengetahui apakah konfigurasi implementasi *Port Knocking* yang sudah di bangun berhasil dan sesuai dengan yang diharpakan atau tidak.

D. Skenario Pengujian *Port Scanning* dan Penyerangan *Sniffing*

Pada tahapan ini melakukan pengujian tingkat keamanan jaringan dengan melakukan pengujian *Scanning Port* dan melakukan pengujian penyerangan *Sniffing* dan dengan meliputi beberapa komponen yang sudah tersedia sebelumnya seperti *Router*, *Switch*, PC *Client/User* dan *Software Mikrotik Router OS V6.48.3* dan satu unit PC *Attacker*.

Seperti yang diperlihatkan pada Gambar topologi dibawah ini, konfigurasi *firewall* sebagai *otentikasi port Knocking* yang akan dibangun dalam jaringan di penelitian ini akan di lakukan penyerangan pada IP target 192.168.20.1/24. Nantinya pada sebuah *router* akan dibangun sebuah *role firewall* sebagai *role* yang harus digunakan oleh *User/admin*. Pada gambar topologi tersebut juga di perlihatkan sebuah PC *Attacker* sebagai media pengujian tingkat keamanan pada sebuah *router*.

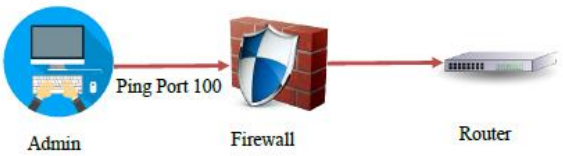


Gambar 4. Pengujian *Scanning port* dan penyerangan *Sniffing* ke *router*

E. Perancangan *Metode Port Knocking*

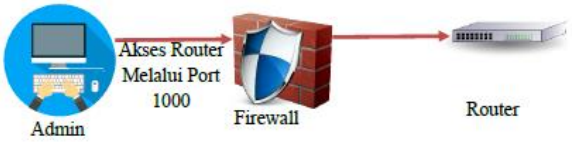
Adapun dalam tahapan ini, gambaran dalam penggunaan metode *Port Knocking* pada *Mikrotik Router OS V6.48.3* sebagai berikut:

1. Admin akan melakukan Ping ke yang sudah ditentukan pada *Firewall* yaitu *port* 1000 Dan *Mikrotik RB1100AH* akan menyimpan Admin yang ingin mengakses *Mikrotik Router OS V6.48.3*



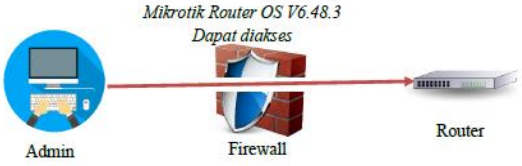
Gambar 5. Admin Melalukan Ping Ke Port 1000

2. Admin akan mencoba akses *Mikrotik Router OS V6.48.3* dengan cara ping *port* 1000, maka *Mikrotik Router OS V6.48.3* akan mengecek apakah Admin tersebut aman atau tidak.



Gambar 6. *Admin Mengakses* Port 1000

6. Namun Jika Admin masuk dalam monitoring pada *Mikrotik Router OS V6.48.3* maka Admin tersebut dapat mengakses sebuah jaringan pada *Mikrotik Router OS V6.48.3*.

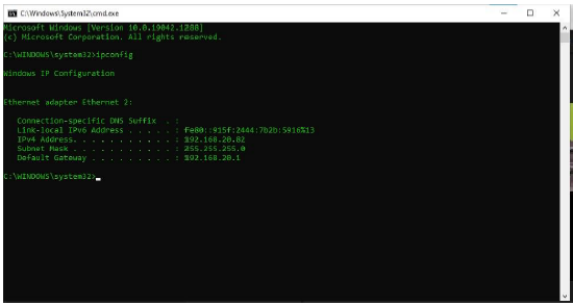


Gambar 7. Admin Berhasil Membuka Akses ke Router

IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Mengidentifikasi IP Target yang ada di Universitas Ubudiyah Indonesia.

Tahapan ini *Attecker* menggunakan komputer yang telah terhubung pada jaringan LAN Universitas Ubudiyah Indonesia pada Ruangan Direktorat Administrasi Akademik. Setelah terhubung pada jaringan LAN *Attecker* harus mengidentifikasi *host* target untuk dilakukan *Sniffing* jaringan menggunakan *software Wireshark*. Berikut ini adalah gambaran hasil dalam mencari host target dengan menggunakan *terminal-command prompt* dengan Perintah *ipconfig.*



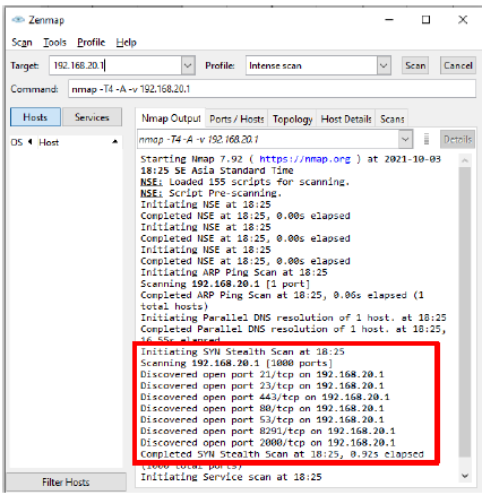
Gambar 8. Mengidentifikasi host/Clien target Menggunakan terminal-command prompt dengan Perintah ipconfig pada komputer *Attecker*

.

1. Ipv4: IP Address 192.168.20.82
   Menunjukkan alamat IP Address yang digunakan Laptop *attacker* dengan protocol IP versi 4.
2. Default Gateway: IP Address 192.168.20.1
   Menunjukkan jalur keluar masuknya packet data dalam sebuah jaringan pada perangkat Komputer user/attacker yang terhubung dengan jaringan LAN ke Internet.
3. Subnet Mask: IP Address 255.255.255.0
   Menunjukkan nilai perfic dalam alamat IP, IP yang digunakan IP kelas C dengan Nilai /24 yaitu 24 bit. Default Gateway IP 192.168.20.1 akan menjadi host/client target yang akan dilakukan proses *scanning* jaringan menggunakan software *Zenmap*.

B. Pengujian *Port Scanning* Menggunakan Software *Zenmap* dalam Mode Normal

Pada tahapan ini penulis melakukan pengujian *port Scanning*, dari hasil pengujian *scanning* yang dilakukan penulis, telah mendapatkan hasil bahwa *port* yang ada pada jaringan Universitas Ubudiyah dalam kondisi Normal yaitu mode normal masih bisa di *scan*. Adapun dari hasil scaning bisa dilihat pada Gambar 9.



Gambar 9. Hasil Ports canning dengan IP 192.168.20.1

Hasil *output* dalam melakukan *Port Scanning* ini adalah *file xml*. Hasil yang diperlihatkan dalam bentuk table merupakan hasil dari pencarian target menggunakan metode *port scanning*. Dari hasil yang sudah didapat *Attecker* masih mudah untuk menemukan target, *port* yang terbuka dan bisa mendapatkan informasi yang dibutuhkan. Terdapat info *Scan Summary* | 192.168.20.1, yang menggunakan perintah nmap *–T4 –A –v 92.168.20.1*.

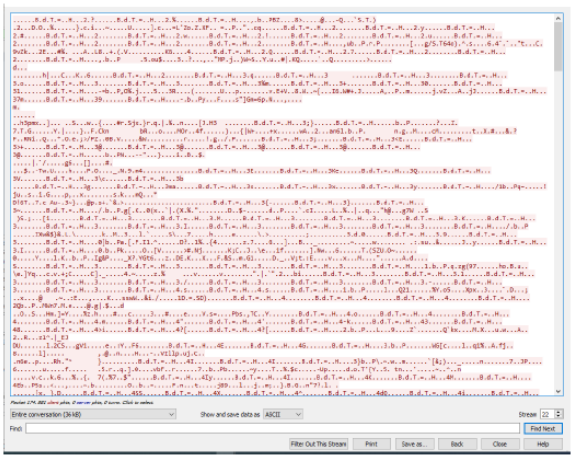
- **Address**
- **192.168.20.1 –(ipv4)**
- **64:D1:54:81:3D:9F**
- **Routerboard.com (mac)**

Tabel 1. Laporan Dalam Bentuk *xml* *192.168.105.254* Menggunakan *Zenmap*

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	MikroTik router ftpd	6.48.3	
23	tcp	open	telnet	syn-ack	Linux telnetd		
53	tcp	open	domain	syn-ack			generic dns response: NOTIMP
80	tcp	open	http	syn-ack	MikroTik router config httpd		
443	tcp	open	https	syn-ack			
2000	tcp	open	bandwidth-test	syn-ack	MikroTik bandwidth-test server		
8291	tcp	open	unknown	syn-ack			

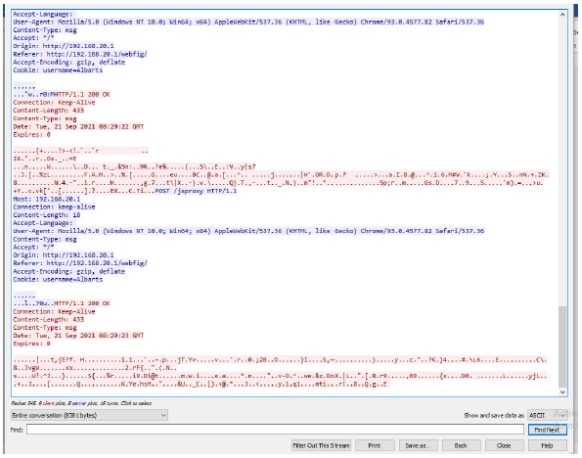
C. Hasil Pengujian Penyerangan metode *Sniffing* dalam *Mode* Normal

Pada tahapan pengujian penyerangan dengan menggunakan metode *sniffing* ini mendapatkan hasil bahwa ketika *Router* diakses menggunakan via *winbox* (8291) oleh target maka penulis *(Attecker)* tidak mendapatkan informasi dari packet data yang di dapatkan seperti *username* dan *password* dikarenkan *packet* data yang di kirimkan dari sumber ke tujun sudah terenkripsi. Hasil dapat diperlihatkan pada gambar 10 dibawah ini.



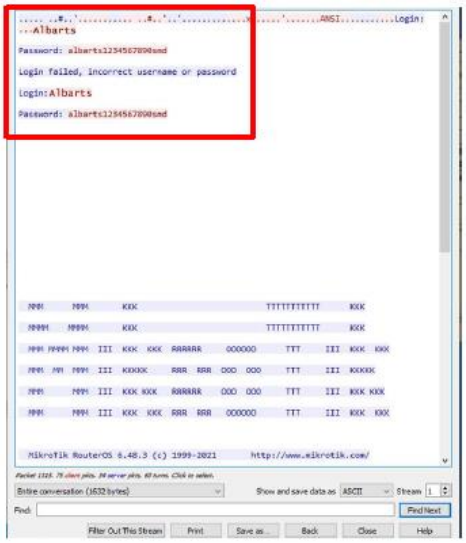
Gambar 10. Hasil Sniffing Router Via Winbox port (8291)

Pada pengujian selanjutnya penulis melakukan *sniffing* berfokus pada protocol HTTP ketika target melakukan login via *webfig (80)* maka penulis *(Attecker)* mendapatkan informasi dari packet data yang di dapatkan seperti *username* nya saja namun *password* yang digunakan telah di*enkripsi*. Sehingga tidak mudah untuk dibaca. Hasil *sniffing* tersebut bisa dilihat Gambar 11.

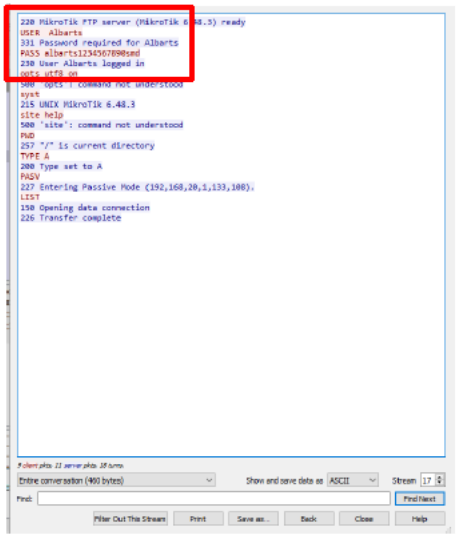


Gambar 11 Hasil Sniffing Router Via Webfig port (80)

Pada pengujian selanjutnya penulis melakukan *sniffing* berfokus pada protocol TELNET (23) dan FTP (21), ketika target melakukan *login via Telnet (23)* dan *via FTP (21)*, ternyata penulis *(Attecker)* mendapatkan informasi dari packet data yang di dapatkan seperti *username* dan *password* yang digunakan untuk login ke *Mikrotik Router OS V6.48.3* tersebut. Dan dalam pengujian penyerangan menggunakan metode *sniffing* ini penulis *(Attecker)* masih bisa mendapatkan informasi packet data yang di *sniffing* dalam hal ini *packet* data berupa informasi *username dan pasword* tidak terenkripsi, sehingga sangat mudah untuk di *sniffing*. Hasil *sniffing* tersebut bisa dilihat pada gambar 12 dan 13 dibawah ini.



Gambar 12. Hasil *Sniffing Router Via TELNET (23)*



Gambar 13. Hasil Sniffing Router Via FTP (21)

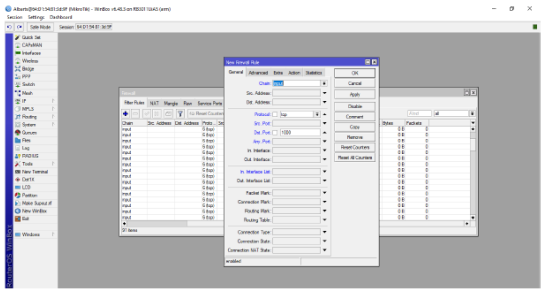
A. Implementasi Metode *Port Knocking*

Pada tahapan implementasi *Metode Port Knocking*, penulis memilih *Sofftware winbox V6.48.3*, Penulis memilih *software Winbox* tersebut karena terdapat banyak fitur-fitur yang memudahkan penulis dalam merancang dan mengkonfigurasi keamanan jaringan dengan menggunkan metode *port knoking.* Tampilan *Login* menggunakan *Winbox*.

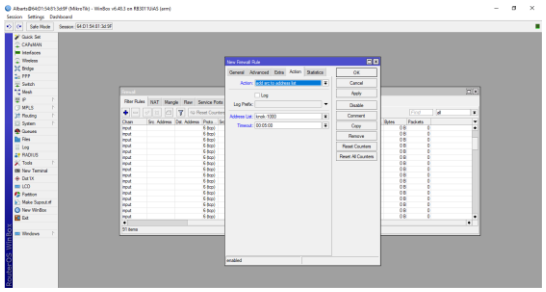
B. Konfigurasi *Port Knocking (Knock 1000)*

Port Knocking adalah sebuah metode keamanan yang dilakukan untuk membuka akses ke *port* tertentu yang telah *diblock* oleh *Firewall* pada sebuah perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Dalam hal ini koneksi bisa berupa protocol *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP) maupuan *Internet Control Message Protocol* (*ICMP*) Jika koneksi yang dikirimkan oleh *host* tersebut sudah sesuai dengan *rule knocking* yang diterapkan pada *mikrotik*, maka secara *dinamis firewall* akan

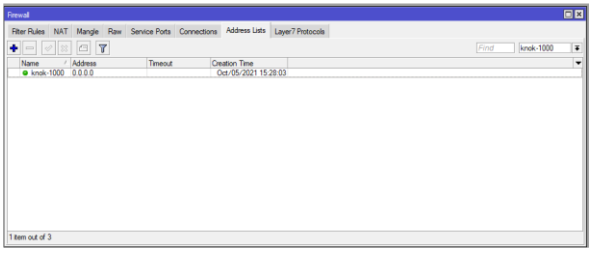
memberikan sebuah akses ke *port* yang sudah *deblock* sebelumnya. Dengan Langkah ini, perangkat jaringan seperti *Router* akan lebih aman dari sebuanya serangan *Attecker*, dikarenakan dengan menggunkan metode *Port knocking* admin jaringan bisa melakukan *blocking* terhadap *port-port* yang rentan terhadap serangan *Sniffing* dari *Attecker* seperti *TELNET* (23) FTP (21) atau *webfig* (80). Dengan metode Ini penulis berharap Jika *Attecker* melakukan serangan dengan menggunakan metode *Sniffing* dengan melakukan Langkah awal *port scanning* maka *port-port* tersebut akan terlihat tertutup.



Gambar 14. Konfigurasi Filter Rules



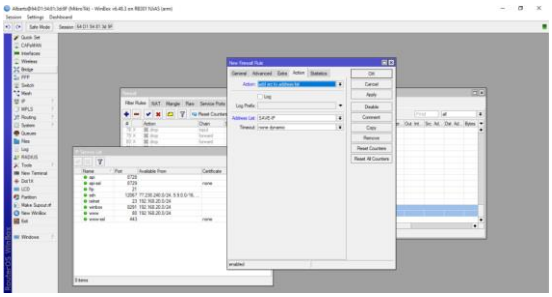
Gambar 15. Konfigurasi Filter Rules (Tab Action)



Gambar 16. *Address Lists (*Hasil konfigurasi *knock 1000)*

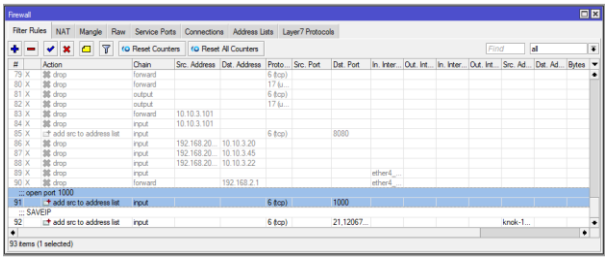
C. SAVE IP

Langkah selanjutnya penulis membuat sebuah *rule Firewall Filter* untuk melakukan *blocking* akses ke *Router* dari sumber *(src-address)* selain dari IP *Address* yang sudah masuk dalam *Address-List.* Pada gambar 4.20, sama halnya dengan melakukan konfigurasi knock 1000 hanya saja terdapat perbedaannya yang terletak pada *port* yang akan digunakan merupakan *port* dari mikrotik yaitu 8291 *(Winbox)*, kemudian akan dialihkan ke tab *Advanced*.



Gambar 17. *Konfigurasi Save IP*

Pada gambar 18 dibawah ini memperlihatkan sebuah hasil inplementasi dari Konfigurasi *SAVE IP* yang dapat dilihat pada tab *Rules Filter.*

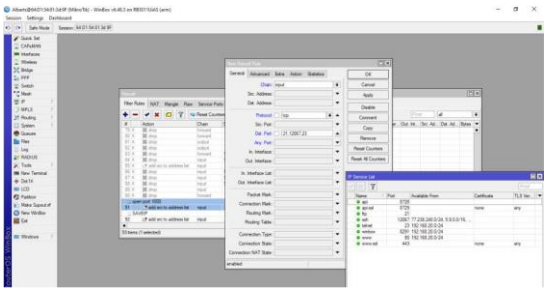


Gambar 18. *Rules Filter Save IP*

D. Konfigurasi IP Penyusup

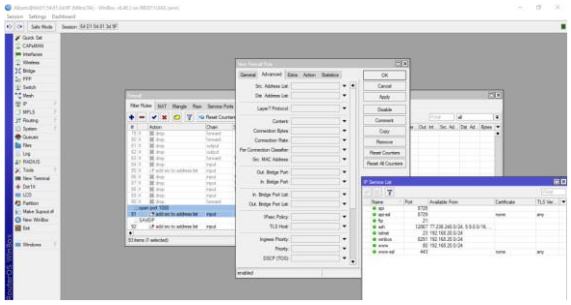
Pada tahapan ini penulis melakukan konfigurasi IP Penyusup sama halnya dengan Langkah -langkah pada saat melakukan konfigurasi *Knock-1000* dan *Save IP* hanya saja pada bagian ini tab *Advanced* di kecualikan Siapapun yang masuk ke *port* 21,12067,23,80 dan tidak ada di *list knock-1000* maka di anggap sebagai penyusup.

Pada Gambar 19 dapat dilihat *Chain – input, Protocol* - TCP, dan *Dst.port*- 21,12067,23 dan 80. Dapat di lihat pada gambar di bawah ini.



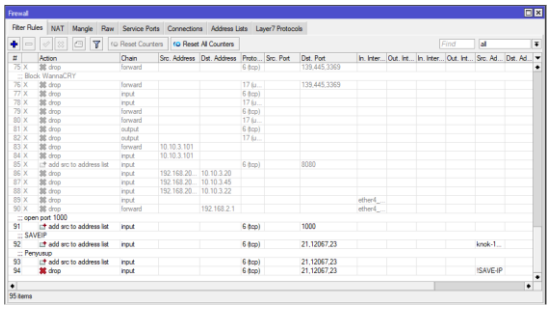
Gambar 19. *Konfigurasi IP* Penyusup

Pada gambar 20 ini merupakan sebuah tampilan tab *Advanced*, dalam hal ini dapat dilihat pada tab *Src.Address List* penulis memilih *Knock-1000* dan penulis membuat tanda seru ! (NOT) pada samping kiri yang artinya adalah siapapun yang tidak termasuk pada *list knock-1000* dinyatakan sebagai IP Penyusup *(Attecker)* terkecuali telah diberikan akses pada *port 1000* atau *knock-1000*.



Gambar 20. Konfigurasi IP Penyusup (Advenced)

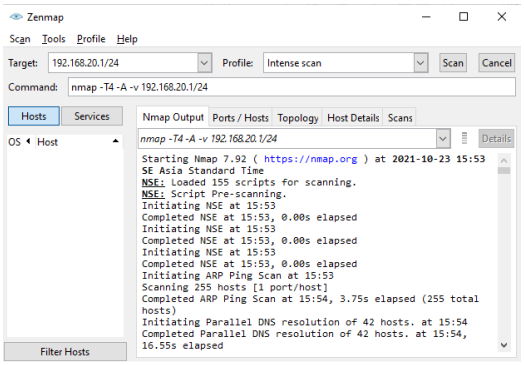
Dibawah ini memperlihatkan sebuah hasil inplementasi dari Konfigurasi *Block IP* yang dapat dilihat pada tab *Rules Filter* dan Jika dilihat secara keseluruhan *Rules Firewall Filter* yang penulisbuat menjadi seperti pada gambar dibawah ini.



Gambar 21. *Rules Firewall Filter* Secara keseluruhan.

E. *Scanning Port* dalam Keadaan *Mode Port Knocking* Aktif

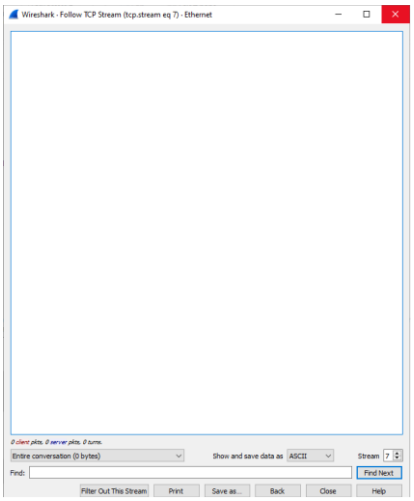
Diperlihatkan pada gambar diatas hasil *scanning* yang penulis lakukan denga IP Target *192.168.20.1/24* dan *Command: nmap-T4-A-v 192.168.20.1/24* didapatkan hasil saat *Port Knocking* dalam keadaan aktif bahwa *port* yang ada pada jaringan UUI tidak bisa di*scan* dalam artian (tidak terbaca) semua *port* tidak terbaca.



Gambar 22. Hasil *Scanning Port* Dalam Keadaan *Port Knocking* Aktif.

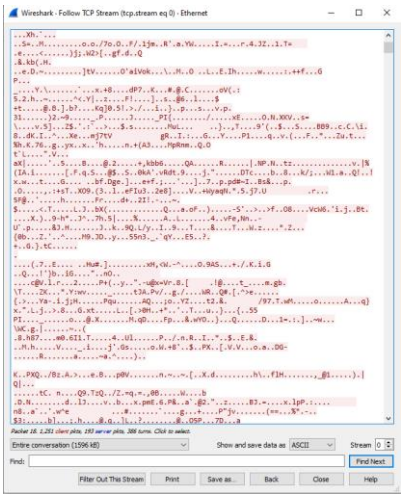
F. Hasil Pengujian *Authentication* berdasarkan IP Target menggunakan TELNET (23).

Pada tahapan berikutnya penulis/ Attecker mencoba untuk Memanggil data (Follow) namun hasil yang didapatkan tidak terdapatnya informasi dari packet data yang di dapatkan dari hasil *Sniffing* seperti *username* dan *password* dikarenkan *packet* data yang di kirimkan dari sumber ke tujun sudah ditutup. Hasil dari pengujian dapat dilihatkan pada gambar 23 dibawah ini.



Gambar 23. Hasil *Sniffing Router Via Telnet port (23)* dalam kondisi *Port Knocking* diaktifkan

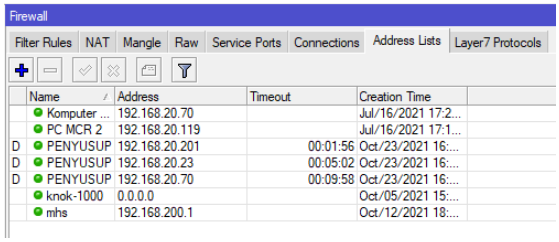
Terlihat pada gambar 23 dibawah ini penulis mencoba untuk melakukan *sniffing* dengan menargetkan FTP yaitu *Port* 21 diketahui pada saat sebelum metode *Port Knocking* diaktifkan hasil dari penyerangan *Attecker* Menggunakan metode *Sniffing Attecker*/penulis mendapatkan Informasi penting berupa *Pasword* dan *Username*. Namun pada saat dilakukan pengujian dengan menggunakan metode *Sniffing* dalam keadaan *port Knocking* Aktif, Penulis/Attecker tidak mendapatkan Informasi Penting Apapun. Seperti *username* dan *password* dikarenkan *packet* data yang di kirimkan dari sumber ke tujun sudah di enkripsi. Hasil dari pengujian dapat dilihatkan pada gambar 24 dibawah ini.



Gambar 24. Hasil *Sniffing Router Via FTP port (21)* dalam kondisi *Port Knocking* diaktifkan.

G. Monitoring

Pada tahap ini penulis melakukan monitoring terhadap metode *port Knocking* pada *Mikrotik Router Os V6.48.3* yang sudah penulis Implementasikan untuk melihat dan juga memastikan bahwa konfigurasi *Port Knocking* dapat berjalan sesuai dengan harapan dan memenuhi kebutuhan. Dilihat dari hasil monitoring di Firewall bahwa kesalahan dari *port Knocking* yang di rancang serta diimplementasikan tidak terjadinya kesalahan dalam jaringan UUI.



Gambar 25. Pengujian beserta *Monitoring Port Knocking* pada *Mikrotik Router Os V6.48.3*

H. Hasil Pengujian Perbandingan Jaringan tanpa *Port Knocking* dan *Port Knocking Aktif*

Berdasarkan hasil analisis dan pengujian metode *Port Knocking* pada *Mikrotik Router Os V6.48*, mendapatkan hasil bahwa dalam pengujian dan implementasi keamanan jaringan menggunakan tanpa menggunakan metode *Port Knocking* dan menggunkan metode *Port Knocking* dapat berfungsi dengan optimal. Hasil pengujian perbandingan dapat dilihat pada table 4.1 dibawah ini.

Tabel 2. Hasil Pengujian Perbandingan Jaringan tanpa *Port Knocking* dan *Port Knocking Aktif*

Pengujian	Model Pengujian	Jenis Pengujian	Software Pengujian	Hasil Pengujian
1	Tanpa Metode *Port Knocking*	*Scanning Port*	*Zenmap*	*Open Port*
2	Tanpa Metode *Port Knocking*	*Sniffing*	*Wireshark*	- Winbox (8291)Terenkripsi - Webfig (80) Hanya *Pasword* yang terenkripsi - TELNET (23) *Username* dan *Pasword* masih bisa di sadap - FTP (21) *Username* dan *Pasword* masih bisa di sadap
3	Tanpa Metode *Port Knocking*	*Authentication*	- Winbox (8291) - Webfig (80) - TELNET (23) - FTP (21)	- Winbox (8291) Gagal *Login* - Webfig (80) gagal *Login* - TELNET (23) Berhasil *Login* - FTP (21) Berhasil *Login*
4	Metode *Port Knocking Aktif*	*Scanning Port*	*Zenmap*	Tidak Menemukan Port yang terbuka
5	Metode *Port Knocking Aktif*	*Sniffing*	*Wireshark*	- Winbox (8291) Terenkripsi - Webfig (80) Terenkripsi - TELNET (23) Terenkripsi FTP (21) Terenkripsi
6	Metode *Port Knocking* Aktif	*Authentication*	- Winbox (8291) - Webfig (80) - TELNET (23) - FTP (21)	- Winbox (8291) Gagal *Login* - Webfig (80) gagal *Login* - TELNET (23) Berhasil *Login* - FTP (21) Berhasil *Login*

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil penelitian ini dengan judul yang penulis angkat "Analisis Keamanan Jaringan Menggunakan Metode *Sniffing* Dan Implementasi Keamanan Jaringan Pada *Mikrotik Router Os V6.48.3* Menggunakan *Metode Port Knocking*". Didapat bahwa keamanan pada jaringan yang ada pada Universitas Ubudiyah Indonesia masih dapat di disadap oleh *Attecker* dengan melakukan *scanning port* dan melakukan penyerangan menggunakan Metode *Sniffing* pada jaringan secara mudah untuk mendapatkan informasi penting yang ada pada jaringan Universitas Ubudiyah Indonesia.

Pada tahap pengujian yang penulis lakukan menggunakan *Zenmap* dan *Wireshark*, penulis menggunakan IP target untuk melakukan *Scanning Port* beserta melakukan penyerangan menggunakan metode *Sniffing* serta menganalisis. Adapun IP target yang penulis gunakan diantaranya adalah IP 192.168.20.1.

Kesimpulan dari hasil penelitian berdasarkan pada pengujian dan analisis keamanan jaringan dalam keadaan jaringan tanpa menggunakan metode *Port knocking* yang menggunakan *software Zenmap* dan *Wireshark* dengan melakukan beberapa tahapan uji coba dan penulis dapat menarik kesimpulan diantaranya:

1. Software *Zenmap* masih dapat digunakan dalam melakukan *scanning port* pada jaringan Universitas Ubudiyah Indonesia dengan target berupa *IP Address* 192.168.20.1. Dan mampu melakukan pemindaian *port* yang terbuka pada jaringan Universitas Ubudiyah Indonesia.
2. Dengan mendapatkan status *port* yang terbuka *(open port)*, Penulis/*Attecker* dapat

mengetahui informasi yang didapat tersebut, sehingga penulis dapat melakukan penyerangan dengan menggunakan metode *Sniffing*.

3. Dengan Melakukan penyerangan menggunakan Metode *Sniffing* penulis*/Attecker* bisa mendapatkan informasi Penting yang dikirimkan oleh target tujuan ke penerima *(Destination-Source)* berupa *Username* dan *Pasword Login* Ke *Mikrotik Router Os V6.48.3* dengan menggunakan *Telnet* (23), FTP (21) dan hasil *Authentication* Penulis/*Attecker* berhasil *login* ke *Mikrotik Router Os V6.48.3*

Dari hasil pengujian ini juga penulis dapat mengambil kesimpulan dalam mengimplementasikan *Metode Port knocking* pada *Mikrotik Router Os V6.48.3* sebagai berikut:

1. *Mikrotik Router Os V6.48.3* pada jaringan Universitas Ubudiyah Indonesia yang menggunakan keamanan dengan metode *port knocking* sudah bisa meningkatkan pengamanan *Authentication* pada *user* administrator di *Mikrotik Router Os V6.48.3*.
2. Metode *port knocking* yang telah penulis terapkan terdapat pada semua metode akses *remote* ke *router Mikrotik Router Os V6.48.3* diantarnya yang sering digunakan seperti *winbox*, *webfig*, STP dan *Telnet*.
3. Metode *port knocking* tidak hanya bisa melindungi akses *Attecker* masuk dari jaringan *local* saja namun dari jaringan *Public* juga bisa dilindungi sehingga meskipun ada *Attecker* ataupun orang lain yang memanajemen *router Mikrotik Router Os V6.48.3* pada Jaringan Universitas Ubudiyah Indonesia yang ingin menggunakan hak akses *administrator* meski mengetahui *Username* dan *pasword* namun tetap tidak mendapat hak akses pada *Router Mikrotik Router Os V6.48.3*.
4. Setelah keamanan *port knocking* diterapkan sehingga bisa membuat *Attecker* tidak dapat mengetahui *port* mana yang terbuka *(Open port*). hasil *Authentication* Penulis/*Attecker* tidak bisa lagi *login* ke *Mikrotik Router Os V6.48.3*.

REFERENSI

Edwin Mandala Putra. Dkk, 2021. Analisis Kemanan Jaringan Internet *(Wifi)* Dari Serangan Packet Data *Sniffing* Di Universitas Muhammadiyah .Jurnal, 2021

Hasbullah Jamaluddin. Dkk. 2018. Analisis Keamanan Website Terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus : Simak Unismuh). Skripsi, 208

Wanto, Anjar. dkk. 2019. Kombinasi *Port Knocking* Dan VPN Guna Pengamanan *Akses Secure Shell Pada Cloud Computing*. Vol 12, No.1, July 2019.

Fatma Suhaila. 209. Analisis Jaringan LAN Di SMK 5 Telkom Banda Aceh. Skripsi. 2019

VariantoEka. Badrul Mohammad, 2015. Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear OS Pada PT.Valdo International. Vol. 1 No. 1. Feb 2015.

R. Fitria, 2020. Rancang Bangun Dan Analisis Ip Address Menggunakan Metode Variable Length Subnet Mask (Vlsm). Skripsi. 2020.

Z. Munawar. Dkk. 2020. Keamanan Jaringan Komputer Pada Era Big Data. Vol.2 No. Juni 2020. Jurnal Sistem Informasi.

Amarudin. 2018. Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking. Jurnal 2018. E-Issn 2460-846.

H.I. Pohan, 2019. Analisis Dan Implementasi Internet Gateway Menggunakan Mikrotik Router Board Di Virtualbox. Skripsi 2019.

D.B. Rendro, Dkk, 2020. Analisis *Monitoring* Sistem Keamanan Jaringan Komputer Menggunakan *Software Nmap* (Studi Kasus Di Smk Negeri 1 Kota Serang). Jurnal 2018. Vol. 7 N0. 2 E-Issn 2597-9922. September 2020. Jurnal PROSISKO

E.Haryanto, 2013. Meningkatkan Keamanan Port Ssh Dengan Metode Port Knocking Menggunakan Shorewall Pada Sistem Operasi Linux. Skripsi. 2013