ANALISIS KEAMANAN JARINGAN ROUTER MIKROTIK MENGGUNAKAN METODE PENETRATION TESTING MAN IN THE MIDDLE (MITM)

Ari Sabela Anggraini[1], Suwanto Raharjo[2], Prita Haryani[3]

[1,2] Jurusan Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
[3] Jurusan Rekayasa Sistem Komputer, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email:[1]sabellanggraini@gmail.com, [2]wa2n@akprind.ac.id, [3]pritahayani@akprind.ac.id

Abstract

The use of wireless networks that can be found in various public places makes it easy for users to access the internet network so that facility users pay less attention to communication security and data security on the network. This public or public wireless network that is easily accessible has weaknesses that allow crime and this attack can be from fellow network users themselves, therefore efforts are needed to improve the security system on the network.

From several penetration testing methods, the attack that is widely used for crimes that attack public networks is Man in the Middle Attack (MITM). This attack intercepts the network connection without the knowledge of the network user. This type of attack is very difficult to track by users even though the network has been supported by a good authentication system. This type of attack is usually carried out by the same actors connected to the network and this attack has a variety of methods and ways of implementing it and has its own characteristics for the device being attacked.Tests that have been carried out on hotspot network security systems using the MITM method with wireshark, sniffing ping flood and netcut attacks can be used to find security gaps in the boarding hotspot network successfully using two clients with test results conducted using wireshark which results in network monitoring and can be used to commit crimes with the results of getting the username and password of the victim. The second test carried out using ping flood which is run for approximately 1 - 3 minutes by opening a large number of ping flood scripts at the same time causes traffic to be heavy so that the bandwidth obtained by users is not maximized. Other tests carried out using netcut are run by limiting Speed or cutting the network to other users by controlling the IP as if the perpetrator is the MAC Address. So that the attacked IP cannot be connected to the network unless the netcut user opens the IP again or blocks the use of netcut.

Keywords: *Wireless*, Man in the Middle , Network Security, Penetration testing .

Intisari

Penggunaan jaringan nirkabel *(wireless)* yang dapat dijumpai di berbagai tempat umum ini memudahkan pengguna untuk mengakses jaringan internet sehingga pengguna fasilitas kurang memperhatikan keamanan komunikasi dan keamanan data pada jaringan tersebut. Jaringan nirkabel yang bersifat public atau umum yang mudah diakses ini memiliki kelemahan yang memungkinakan tindak kejahatan dan serangan ini bisa dari sesama pengguna jaringan itu sendiri oleh karena itu diperlukan upaya untuk meningkatkan sistem keamanan pada jaringan.Dari berberapa metode *penetration testing* serangan yang banyak digunakan untuk aksi kejahatan yang menyerang jaringan public adalah *Man in The Middle Attack (MITM)*. Serangan ini melakukan penyadapan pada koneksi jaringan tanpa sepengetahuan pengguna jaringan tersebut. Jenis serangan ini sangat sulit dilacak oleh pengguna walaupun jaringan telah didukung oleh sistem *autentifikasi* yang baik. Jenis

serangan ini biasanya dilakukan oleh pelaku yang sama sama terhubung pada jaringan tersebut dan serangan ini memiliki berbagai macam metode dan cara dalam mengimplementasikannya dan memiliki karakteristik tersendiri terhadap perangkat yang diserang.Pengujian yang telah dilakukan pada sistem keamanan jarigan *hotspot* menggunakan metode MITM dengan jenis serangan *wireshark, snifing ping flood* dan *netcut* dapat gunakan untuk mencari celah keamanan pada pada jaringan hotspot kosan berhasil dilakukan dengan menggunakan dua *client* dengan hasil pengujian yang dilakukan dengan menggunakan *wireshark* yang menghasilkan monitoring jaringan serta dapat digunakan untuk melakukan kejahatan dengan hasil mendapatkan *username* dan *password* dari korban. Pengujian kedua yang dilakukan dengan menggunakan *ping flood* yang dijalankan kurang lebih 1 – 3 menit dengan cara membuka *script ping flood* dalam jumlah banyak dalam waktu yang bersamaan menyebabkan *traffic* menjadi padat sehingga membuat *bandwith* yang didapatkan pengguna menjadi tidak maksimal. Pengujian lain yang dilakukan dengan menggunakan *netcut* yang dijalankan dengan membatasi Speed ataupun memotong jaringan pada pengguna lain dengan mengkontrol IP seolah – olah pelaku sebagai *MAC Address*. Sehingga IP yang di serang tidak dapat terkoneksi dengan jaringan kecuali pengguna netcut membuka IP kembali atau memblokir penggunaan *netcut.*
Kata kunci: *Wireless , Man in the Middle* , Keamanan Jaringan , *Penetration Testing*.

Pendahuluan

Perkembangan teknologi internet yang begitu pesat dan media yang digunakan juga terus berkembang dengan cepat, seperti jaringan nirkabel *(wireless)*. Layanan jaringan nirkabel *(wireless)* dapat di jumpai di berbagai tempat umum karena memiliki keunggulan dibandingan dengan media kabel dalam hal kemudahan mengakses data dan mengakses internet yaitu lebih mudah dan fleksibel , selain perkembangan teknologi yang semakin pesat disisi lain tingkat kejahatan dunia maya juga ikut meningkat sehingga diperlukan keamanan jaringan. Ada berbagai jenis serangan yang dapat digunakan pada aksi kejahatan untuk menyerang jaringan, oleh karena itu perlu dilakukan pengujian terhadap keamanan jaringan untuk mecari celah dari kelemahan sistem jaringan tersebut. Dari berberapa metode penetration testing serangan yang banyak digunakan untuk aksi kejahatan yang menyerang jaringan *public* adalah *Man in The Middle Attack (MITM).* Serangan ini melakukan penyadapan pada koneksi jaringan pengguna dimana sebelum mencapai tujuan akan dialihkan melalui jaringan penyerang tanpa sepengetahuan pengguna jaringan tersebut .

Penelitian ini mengacu pada penelitian [1] yang membahas tentang sistem keamanan LAN dan WLAN pada segment jaringan yang sama memiliki celah keamanan yang dapat ditembus oleh serangan dengan teknik *Man in the Middle Attack*, sehingga mengakibatkan kebocoran data yang berakibat fatal. Penerapan *ARP - Replay only* dan menonaktifkan *default forward* pada *interface wireless* dapat mencegah serangan *ARP Poisioning*. Penggunaan metode *penetration testing* membantu melakukan pengujian secara terstruktur dengan hasil akhir berupa keamanan jaringan LAN dan WLAN.

Penelitian yang dilakukan oleh Bayu, Yamin, dan Aksara [2] . Memberikan kesimpulan bahwa penelitian yang telah dilakukan selama perancangan sampai Analisa Keamanan Jaringan Wireless Local Area Network dengan Metode Penetration Testing (*Cracking The Encryption, Bypassing WLAN Authentication, Attacking The Infrastructure* dan MITM) menggunakan Kali Linux pada Laboratorium Sistem Informasi dan Programming.

Penelitian yang dilakukan oleh Fajrin, Sukarno, dan Satwiko [3] dengan metode klasifikasi K-NN dan Markov Chain ini menggunakan dataset berupa hasil serangan MITM terhadap *smart lock* untuk membandingkan kedua algoritma metode tersebut dengan tujuan untuk menentukan algoritma yang memiliki pendeteksi serangan dengan akurat yang tinggi dan perbandingan disesuaikan dengan evaluasi algoritma.

Penelitian yang dilakukan oleh Iqbal, Fahru , dan Mia [4] memberikan kesimpulan bahwa injeksi BadUSB Man in The Middle Attack yang dilakukan pada Kali Nethunter berhasil dilakukan. Setelah dilakukan pengujian didapatkan hasil berupa password pada suatu web dan jenis web yang bisa untuk di bypass passwordnya hanya web dengan protocol keamanan HTTP sementara untuk web dengan *protocol* keamanan HTTPS belum bisa.

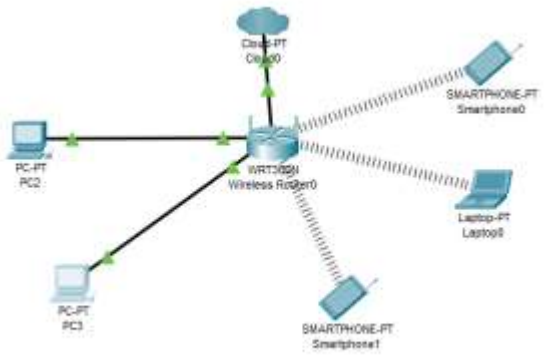
Penelitian yang dilakukan oleh Dhimas dan Indrastanti [5] menyimpulkan bahwa serangan Man in The Middle (MITM) *sniffing* menggunakan *firmware hacking* pada router Glinet 6416a di jaringan *wireless*

dapat terjadi pada server yang menggunakan protokol HTTPS, dengan catatan server HTTPS tersebut memperbolehkan client untuk melakuan request HTTP ke server, sedangkan server yang hanya menerima HTTPS only, tidak berhasil dikarenakan pertukaran informasi hanya berjalan jika terjadi koneksi HTTPS antara client dan server tersebut.

Berdasarkan uraian di atas , maka dibuatlah penelitian dengan judul " Analisis Keamanan Jaringan Router Mikrotik Menggunakan Metode Penetration Testing MITM " yang dilakukan pada jaringan lingkup kosan dengan metodelogi penelitian kualitatif.

Rancangan Alur Penelitian

Pada gambar menjelaskan alur dari penelitian analisis metode MITM ini dengan menggunakan *software* untuk melakukan penyerangan *wireshark, ping flood,* dan *netcut* dengan menggunakan dua buah pc / lapotop, router mikrotik, dua buah *smartphone*.



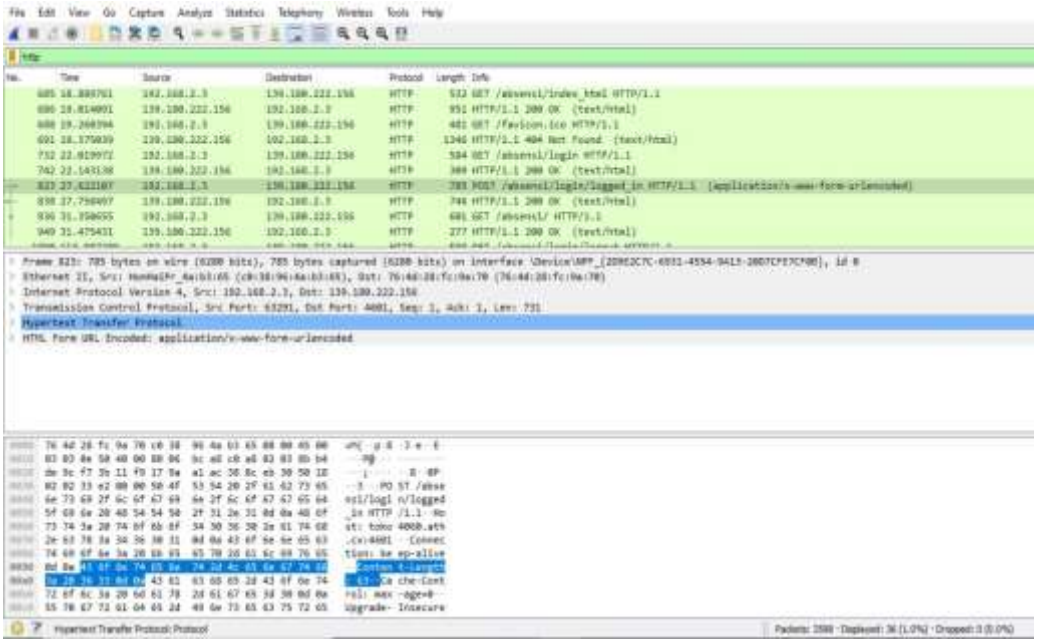
GAMBAR 1 TOPOLOGI JARINGAN

Hasil Dan Pembahasan

1 Pengujian Dengan Menggunakan WireShark

Penggunaan wireshark ini biasanya digunakan untuk memonitoring dan menangkap paket – paket jaringan yang lewat di jaringan tersebut. Dalam melakukan serangan *sniffing* ini biasanya untuk mendapatkan *user* dan *password.* Langkah – langkah untuk melakukan pengujiannya sebagai berikut:

a. Membuka program Wireshark terlebih dahulu
   Kemudian klik pada pilihan *wi-fi* kemudian klik gambar berwarna biru untuk menjalankan wireshark.
b. Setelah program dijalankan akan keluar deretan paket – paket yang sedang diakses. Disini dapat melihat *IP Address, protocol*, dan info akses paket. Kemudian jika sudah mendapat target yang diserang klik gambar kotak merah untuk menghentikan proses *sniffing,* disini mencari target yang masih menggunakan browser HTTP dengan cara memfilter paket yang menggunakan browser HTTP seperti gambar 2.

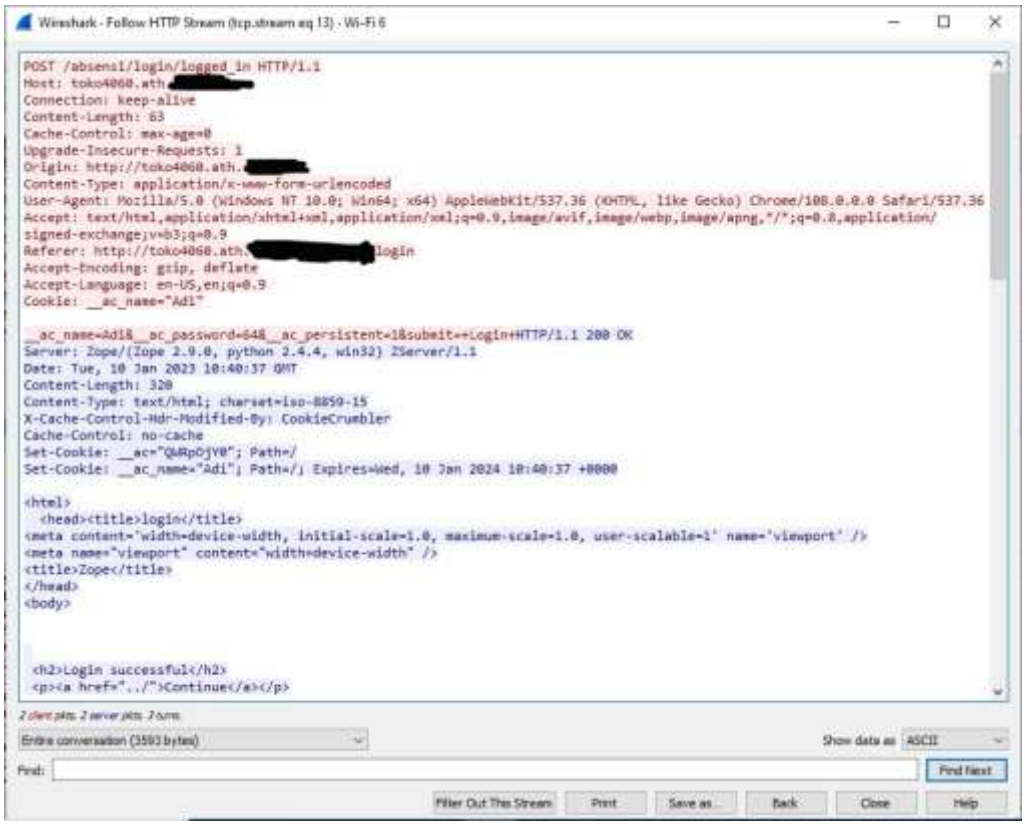


GAMBAR 2 PEMFILTERAN PAKET

c. Klik paket melakukan *sniffing* kemudian klik kanan pilih *follow* pilih HTTP Stream atau ctrl+alt+shift+H untuk melihat detail paket yang dibuka seperti gambar 3.

GAMBAR 3 PAKET YANG BERISI DATA

d. Tampilan dari HTTP disini hasil dari sniffing username dan password telah berhasil .



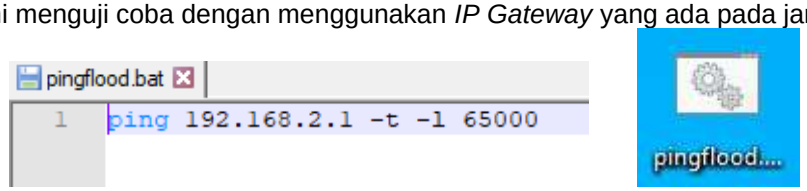
GAMBAR 4 TAMPILAN HTTP

2. *Pengujian Dengan Menggunakan Ping Flood*

Serangan *ping flood* merupakan serangan dengan membanjiri korban dengan paket *"echo reuest"* (ping) ICMP dengan cepat yang mengakibatkan peningkatan *traffic* jaringan computer menjadi penuh .
Langkah – langkah serangan *ping flood* sebelum dan sesudah diaktifkan *firewall* sebagai berikut :

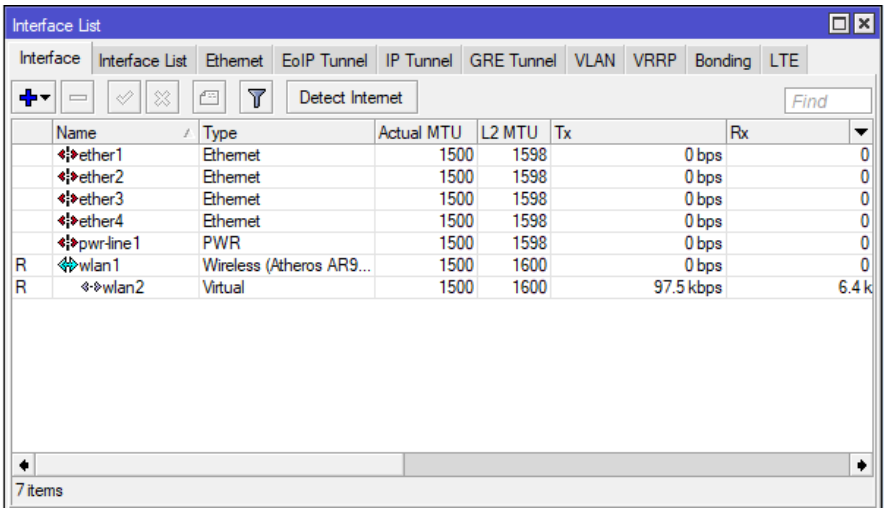
a. Langkap awal untuk melakukan uji coba penyerangan dengan membuat *script* pada notepad++ dengan isian *ping IP address* yang diserang dan disimpan dengan ekstensi .bat.

Disini menguji coba dengan menggunakan *IP Gateway* yang ada pada jaringan Internet.



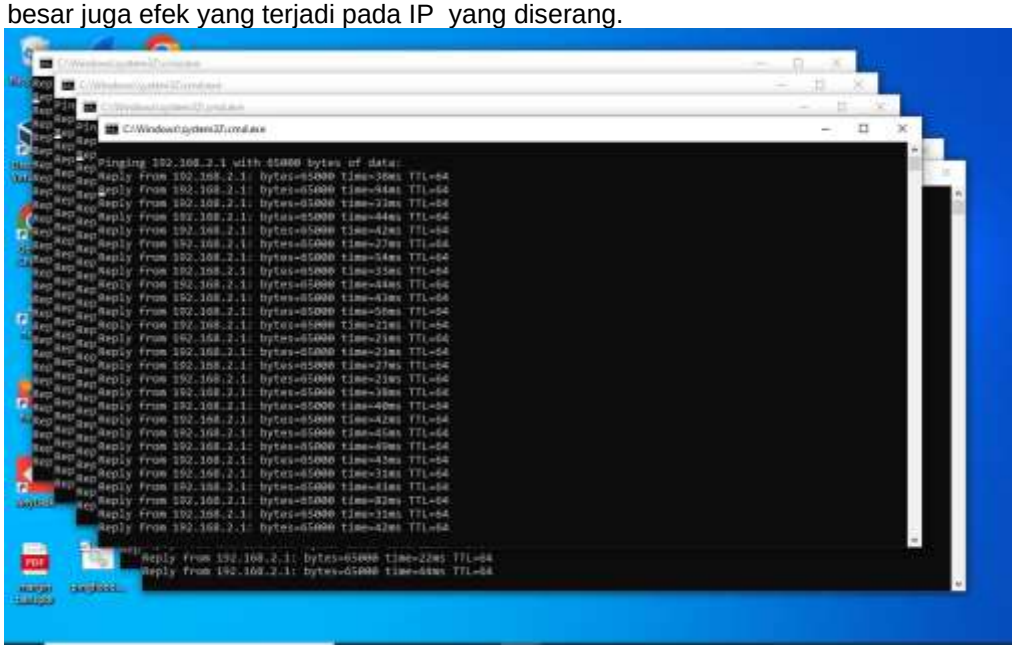
GAMBAR 5 TAMPILAN PINGFLOOD.BAT

b. Sebelum menjalankan *Ping flood* buka pada mikrotik kemudian klik di *Interface.* Terlihat pada *wlan2* atau *IP Gateway* masih dalam keadaan normal dengan Tx 97,5 Kbps dan Rx 6,4 Kbps.



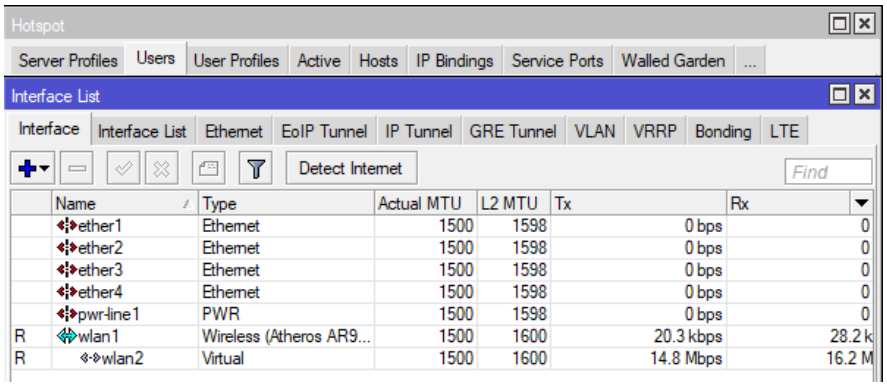
GAMBAR 6 TAMPILAN INTERFACE MIKROTIK

c. Setelah itu jalankan dengan membuka sebanyak mungkin dan jalankan selama beberapa menit. Serangan ini dijalankan dengan menggunakan dua laptop dengan membuka makin banyak *script* semakin besar juga efek yang terjadi pada IP yang diserang.



GAMBAR 7 MENJALANKAN PING FLOOD

d. Hasil dari penyerangan membuat *traffic* menjadi naik dengan pesat pada *wlan2* Tx 14,8 Mbps dan Rx 16,2 Mbps.

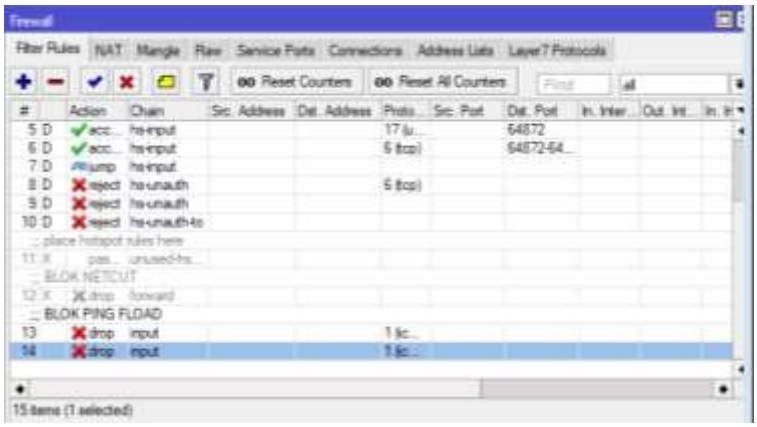


GAMBAR 8 SETELAH TERJADI SERANGAN

e. Untuk mencegah terjadinya serangan ini bisa menggunakan settingan pada *rule firewall* pilih tanda tambah lalu setting seperti pada gambar 9. Kemudian apply lalu OK.

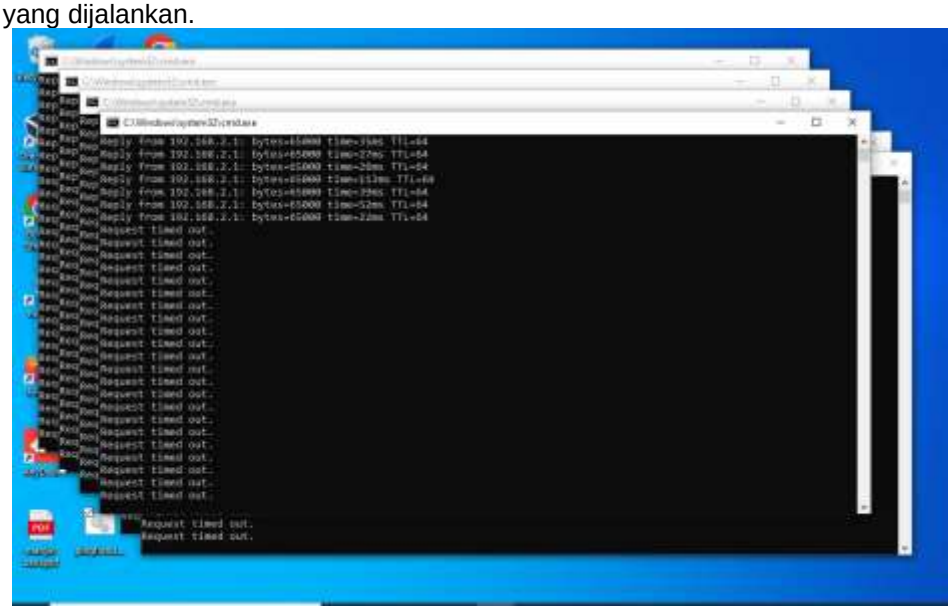
GAMBAR 9 SETTINGAN FIREWALL

f. Kemudian setelah membuat *rule firewall* untuk mengeblok ping flood pilih centang agar dapat diaktifkan.



GAMBAR 10 MENGAKTIFKAN FIREWALL BLOK PING FLOOD

g. Setelah mengaktifkan *rule firewall blok ping flood* dan menunggu beberapa menit maka bekerja, cara kerjanya adalah memblokir aktifitas ping yang sedang terjadi sehingga mengalami *time out* pada *script ping flood* yang dijalankan.

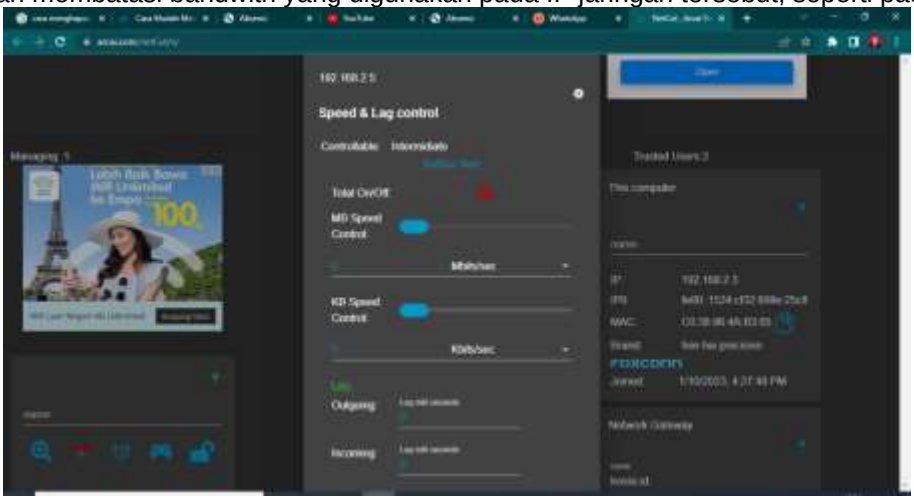


GAMBAR 11 SETELAH DILAKUKAN BLOK PING FLOOD

3. Pengujian Dengan Menggunakan NetCut

Serangan menggunakan Netcut ini biasanya digunakan untuk membatasi *bandwith* yang digunakan ataupun memutus jaringan tanpa diketahui korban. Serangan ini membutuhkan laptop / pc sebagai pengguna untuk membuka *software* kemudian *scan* pada jaringan yang digunakan untuk menampilkan *IP address* yang terdapat pada jaringan tersebut. Langkah – langkah sebagi berikut:

1. Menginstall software Netcut kemudian buka dan ditujukan pada web setelah itu *scan* untuk memilih *IP address* yang menjadi korban. Setelah mendapatkan kemudian klik IP address yang ditargetkan dan disini dengan membatasi bandwith yang digunakan pada IP jaringan tersebut, seperti pada gambar 12.



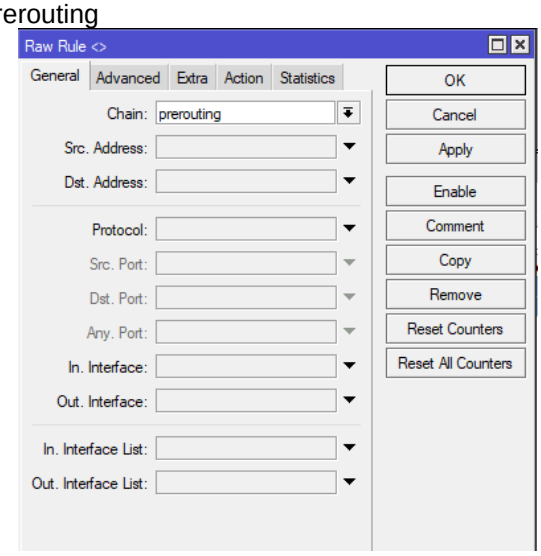
GAMBAR 12 PENYERANGAN NETCUT

2. Dengan dilakukan serangan maka jaringan yang mendapatkan IP yang diserang kemudian mengalami *trouble* pada jaringan.

GAMBAR 13 TAMPILAN PENGGUNA IP YANG DISERANG

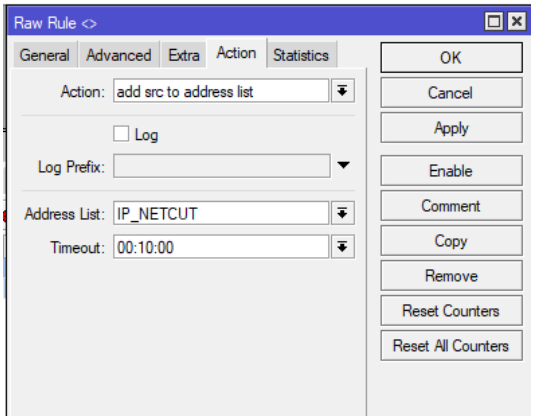
3. Cara mengatasi serangan ini dengan cara membuat *rule firewall* tambahan untuk mengeblok serangan Netcut dengan langkah – langkah sebagai berikut :

a. Membuka *firewall* kemudian pilih Raw lalu klik tambah lalu setting seperti pada gambar 14. General pilih Chain kemudian isi Prerouting



GAMBAR 14 TAMPILAN RAW GENERAL

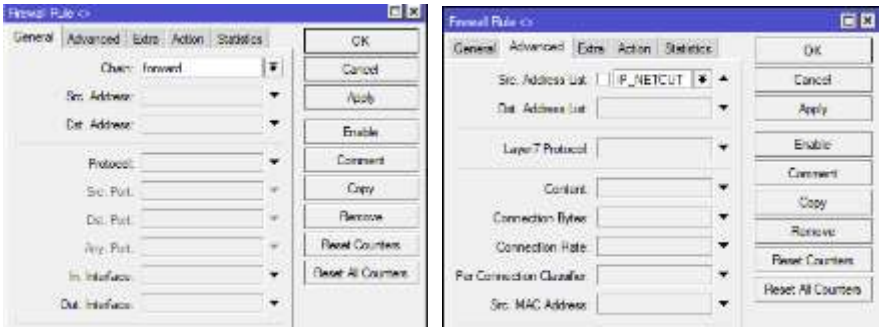
b. Pilih Action Pilih Address List IP_NETCUT



GAMBAR 15 TAMPILAN RAW ACTION

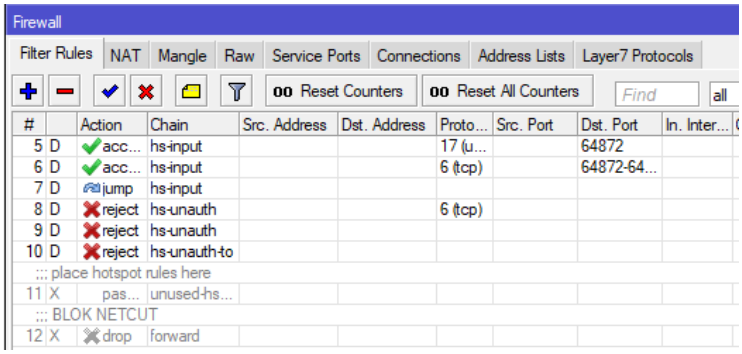
Kemudian klik Apply lalu OK.

c. Membuka pada *firewall* kemudian tambah masuk pada *rule firewall* pilih General kemudian pada *Chain* diisi *Forward* . Kemudian pilih Advanced pilih Src. Address list isi dengan IP_NETCUT. Lalu pilih Applay klik OK.



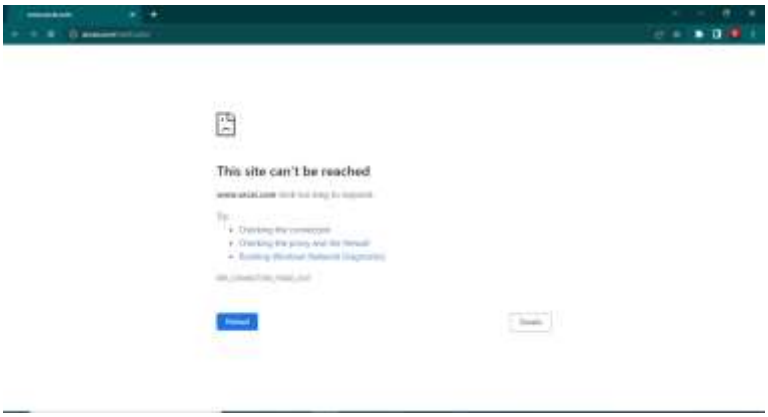
GAMBAR 16 TAMPILAN FIREWALL BLOK NETCUT

d. Kemudian aktifkan *rule firewall* blok Netcut dengan mengklik *rule firewall* lalu klik centang biru agar aktif



GAMBAR 17 HASIL RULE FIREWALL NETCUT

e. Sesudah diaktifkan *rule firewall* yang telah dibuat maka bagi pengguna jaringan hotspot yang membuka *software* Netcut kemuidian terblokir dari web Netcut . seperti Gambar I8.



GAMBAR 18 TAMPILAN SAAT BROWSER NETCUT TERBLOKIR

4. Hasil Analisis Pengujian Penetration Testing Man in The Middle

Dari pengujian yang telah dilakukan dengan menggunakan tiga *software wireshark, ping flood,* dan *netcut* dengan keterangan dan cara menangatsinya. Berikut table hasil dari pengujian penetration testing MITM dapat dilihat pada Tabel 1 :

TABEL 1 HASIL PENGUJIAN PENETRATION TESTING MITM

Pengujian Penetration Testing MITM				
No	*Software* yang digunakan	Hasil Pengujian	Keterangan	Cara mengatasi
1	*Wireshark*	berhasil	Dikatakan berhasil dalam pengujian ini karena dalam pengujian yang sudah dilakukan menggunakan aplikasi *wireshark* ini dapat menangkap paket – paket data yang terkoneksi dalam jaringan internet. Dalam melakukan pengujian ini tertangkap membuka browser dengan *protocol* HTTP dengan memasukkan *username* dan *password* yang bisa dilihat dalam aplikasi *wireshark.*	Cara mengatasi atau menangguanginya dengan cara tidak sembarangan memasukkan *username* dan *password* terutama jika browser masih menggunakan *protocol* HTTP.
2	*Ping flood*	berhasil	Dikatakan berhasil dipengujian ini karena saat melakukan pengujian dengan menggunakan serangan ini yaitu dengan melakukan serangan membanjiri *request ping* dalam jumlah pada IP yang menjadi target membuat lalu lintas pada jaringan IP mengalami penurunan fungsi maupun layanan.	Cara menanggulanginya dengan mengkonfigurasi *firewall* atau alat keamanan lainnya untuk memblokir paket *ping* dalam jumlah besar atau memperkuat jaringan untuk menangani serangan *Ddos.*

			Disini dapat terlihat dari yang semula Tx 97,5 Kbps dan Rx 6,4 Kbps menjadi Tx 14,8 Mbps dan Rx 16,2 Mbps dalam waktu pengujian selama 1-3 menit .	
3	*Netcut*	berhasil	Dikatakan berhasil dipengujian ini karena dalam pengujian dengan menggunakan aplikasi *netcut* dengan cara masuk disatu jaringan yang sama kemudian membuka aplikasi dan melakukan *scan* jaringan untuk mengetahui di jaringan internet yang terhubung ada berapa IP yang terkoneksi dengan jaringan tersebut dan memilih target yang akan diputuskan pada koneksi yang terhubung.	Cara menanggulanginya dengan cara mengkonfigurasi *firewall* untuk memblokir *IP address netcut.*

Kesimpulan

Dari hasil uraian pada bab sebelumnya maka disimpulkan bahwa Pengujian yang telah dilakukan pada sistem keamanan jarigan *hotspot* menggunakan metode mitm dengan jenis serangan *wireshark, snifing ping flood* dan *netcut* dapat gunakan untuk mencari celah keamanan pada pada jaringan *hotspot* kosan berhasil dilakukan dengan menggunakan dua client dengan hasil pengujian yang dilakukan dengan menggunakan *wireshark* yang menghasilkan monitoring jaringan serta dapat digunakan untuk melakukan kejahatan dengan hasil mendapatkan *username* dan *password* dari korban. Pada penelitian ini menunjukan bahwa jika melakukan upaya *login* dengan menggunakan browser dengan *protocol* HTTP mudah untuk dilakukan penyerangan dibandingan dengan HTTPS. Pengujian kedua yang dilakukan dengan menggunakan *ping flood* yang dijalankan kurang lebih 1 – 3 menit dengan cara membuka *script ping flood* dalam jumlah banyak dalam waktu yang bersamaan menyebabkan *traffic* menjadi padat sehingga membuat *bandwith* yang didapatkan pengguna menjadi tidak maksimal. Dapat dilihat saat melakukan uji coba saat belum dilakukan serangan *transmisi* dan *received* yang terdapat pada *IP gateway* pada mikrotik stabil Tx 97,5 Kbps dan Rx 6,4 Kbps tetapi setelah dilakukan serangan *ping flood* pada *IP gateway* menjadi lebih padat Tx 14,8 Mbps dan Rx 16,2 Mbps. Pengujian lain yang dilakukan dengan menggunakan *netcut* yang dijalankan dengan membatasi *Speed* ataupun memotong jaringan pada pengguna lain dengan mengkontrol *IP* seolah – olah pelaku sebagai *MAC Address*. Sehingga *IP* yang di serang tidak dapat terkoneksi dengan jaringan kecuali pengguna *netcut* membuka *IP* kembali atau memblokir penggunaan *netcut*. Berdasarkan hasil pengujian menggunakan *wireshark* yang mendapatkan *user* dan *password* pada *protocol* HTTP, pengujian *ping flood* yang membuat *traffic bandwith* pada mikrotik menjadi padat serta penggunan *netcut* yang membatasi dan memutus koneksi internet pada pengguna lain jaringan maka harus ditingkatkan keamanan jaringannya dengan menambahkan fitur *rule firewall* untuk memblokir serangan yang terjadi seperti pada pengujian diatas serta lebih berhati – hati atau menghindari *login* yang meyertakan *user* dan *password* kedalam suatu situs browser yang masih menggunakan *protocol* HTTP.

Daftar Pustaka

[1] Haeruddin, "Security Design And Testing of LAN and WLAN Network in Mikrotik Router Using Penetration Testing Method FROM Mitm Attack," JITE (Journal of Informsties and Telecommunication Engineering), vol. 4(1), pp. 119-127, juli 20202.

[2] Aksara, Bayu and Yamin, "Analisa Keamanan Jaringan WLAN Dengan Metode Penetration Testing (STUDI KASUS : LABORATORIUM SISTEM INFORMASI DAN PROGRAMMING TEKNIK INFORMATIKA UHO)," vol. 3, pp. 69-78, juli - Desember 2017.

[3] M. Fajrin, P. Sukarno and A. G. P. Satwiko, "Perbandingan Metode K-NN dan Markov Chain Untuk Deteksi Anomali Serangan Man in The Middle Pada Smart LOck Berbasis Wifi," 2020.

[4] I. Z. Muhammad, M. F. Rizal, S.T.,M.T and M. Rosmiati,S.Si.,M.T, "IMPLEMENTASI BADUSB MITM ATTACK MENGGUNAKAN REMOTE PENETRATION TEST PADA KALI NETHUNTER," vol. 3(3), p. 1909, Desember 2017.

[5] D. Wiharjo and I. R. Widiasari, "Analisis Serangan Man in The Middle (MitM) Menggunakan Firmware Hacking Glinet Router 6416a di Jaringan Wirelles," Agustus 2019.

[6] H. J. Prajapati and Noorani, "Rancang Bangun Sistem Hostpot Menggunakan Captive Portal," Jurnal Sarjana Teknik Informatika, vol. 1 (1), 2017.