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

Ari Sabela Anggraini¹, Suwanto Raharjo², Prita Haryani³

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

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.

Test of Assess				
And of Anothers	learce .	Destruituri	Pretand	Laright Diffe
MED 48-889794	107.000.0.3	131.188.222.138	HTTP-	SI2 687 /akwenel/index htsl 0770/1.1
000 18.814001	199.100.222.150	192.308.2.2	HTTP	951 HTTP/1-1 100 (N (text/itel)
888 19.268394	191.165.2.3	139.188.222.154	+1110	482 681 /favious.tco #039/1.1
691 18.175939	139, 139, 132, 156	102.160.2.3	307#	1346 HTTF/2.1 494 Hert Found. (text/Html)
752 22.019972	192.188.2.3	129.108.222.256	9119	384 007 /absensi/logie wff#/1.1
742.22.143138	134.180.222.356	192.148.2.8	4019	300 0TTF/1.1 200 0K (text/hts1)
812 27,611107	DIGHT.LA	-190.310.337.156	1173	201 H011 /whereit/lagis/lagged_in.H177/1_1 (application/s and fore atleneaded)
838.17.756407	139,100,212,190	192-388-2-8	HTTP	246 HTTP/1_1 200 (K (text/Html)
836 31.156655	192.368.2.3	120,180.222.155	HTTH	GBL GET / ANSANAL/ HTTP/1.1
949 31.475431	139.380.322.356	192,100.2.3	1077	277 HTTF/1_1 200 OK (text/intal)
Address, of the Address of			10170	And Add Takeneed Hands Planesk APPEND 0
ine rere sectored				
78 4d 26 fg fg	70 10 10 91 44 01 1	6.88.89.65.88	(11.14.)	6
78 44 25 fs 94 61 80 46 54 40 41 97 75 11	70 c0 10 90 4a 02 00 00 96 9c e0 c0	6 88 99 85 98 J 6 83 89 85 98 6 83 81 95 19 7 85 99 17	(1834) 19	6
76 44 28 ft 96 00 00 46 58 40 m 85 f7 76 11 12 10 14 47 16	70 (d) 14 90 4a (d) 00 18 96 9c 48 (d) 70 17 14 41 45 35 96 56 47 15 54 20	6. 册 99 6. 例 30 时 12 11 15 14 15 45 35 35 13 27 43 47 74 45	(28.)+) 78 1. 2.8 1. POST / W	(
711 442 28 71 90 100 90 46 99 40 100 91 75 75 11 100 91 23 42 90 46 73 93 27 6c	70 (0) 10 (0) 40 (0) 00 10 04 (c) 40 (0) 70 17 76 al ac 33 00 50 47 (3) 42 40 67 47 40 (ac 37 40)	63 朝 朝 65 前 J 44 03 前 前 14 15 43 75 13 17 41 42 73 45 17 41 42 73 45	Cull 3+ 1 1911 I di 1 Post /eir 1/logi n/logi	f P 95
78 44 28 ft 94 10 00 46 38 40 10 50 56 59 40 10 57 59 11 10 10 23 47 59 16 73 59 27 56 54 69 56 28 46	70 10 14 90 44 00 1 00 00 46 10 46 00 1 70 17 16 48 48 53 10 59 47 10 54 20 67 67 49 46 57 66 14 54 56 42 10 18	45 朝 朝 45 冊 J 編 43 目 田 田 10 七 27 45 17 11 42 79 45 17 11 42 79 45 17 11 44 94 44 57 11 44 64 44 57 11 44 64 44 57	(uli Je) 1 ali 1 POST/min 1/bg1 n/bgg aftrp /L1	6 P 95 84 86
78 44 24 ft 96 EI D0 46 58 40 m 85 f7 36 21 EI 73 63 27 66 54 69 42 40 73 74 28 27 66 73 74 28 27 76	18 c0 日 明 40 00 00 田谷 10 田谷 18 17 18 41 45 20 00 日4 10 18 41 45 20 00 日4 10 18 17 52 18 14 19 27 31 38 19 45 49 30 38	6. 翻動的機 2 減6. 数 数 数 数 於 64. 47 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	(9.8 3.e - 29) 1 8 4 5 90 51 /an 1/100 1 /100 8 4779 /11 - 1 toire 4008.9	6 P ## ## #4
76 44 24 54 66 00 00 46 64 66 76 74 </td <td>78 (6) 8 · 98 · 48 (0) 00 · 28 · 68 · 48 · 48 (0) 00 · 29 · 68 · 48 · 48 · 48 · 48 00 · 99 · 49 · 19 · 19 · 19 · 19 · 19 · 19</td> <td>(4.前前前前前) (4.前前前前前前前前前前) (4.11)(</td> <td>(g 8 7 * - g 9 1 8 40 1/log1 o/logp s 4079 /1.1 t bries 4008.v x 4481 Color</td> <td>6 P P P P P P P P P P P P P P P P P P P</td>	78 (6) 8 · 98 · 48 (0) 00 · 28 · 68 · 48 · 48 (0) 00 · 29 · 68 · 48 · 48 · 48 · 48 00 · 99 · 49 · 19 · 19 · 19 · 19 · 19 · 19	(4.前前前前前) (4.前前前前前前前前前前) (4.11)((g 8 7 * - g 9 1 8 40 1/log1 o/logp s 4079 /1.1 t bries 4008.v x 4481 Color	6 P P P P P P P P P P P P P P P P P P P
7% 44 28 11 96 100 00 46 96 40 100 00 46 96 40 100 00 10 7 35 11 100 100 36 420 100 100 100 100 100 100 100 100 100 100	70 (0) 目 例 40 (0) 0) 目4 (0) (1 (0) (2) 70 (7) 1 (0) (2) (2) 70 (7)) (2) (2) (2) (2) 70 (7) (2) (2) (2) (2) (2) 70 (7) (2) (2) (2) (2) (2) (2) (2)	6. 輯輯輯 6. 編 4. 4. 4. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	(y 8 3 + 1 39 3 0 57 /m 1/log r/100 2 0779 /1.1 1 toro 4008. y 4401 Com at prov 4008. y	E F F F F F F F F F F F F F F F F F F F
10 442 24 76 96 00 00 46 56 40<	76 66 86 46 60 60 86 66 </td <td></td> <td>v g. 8. 3 + 1 39 1 8 40 57 /# 17.log1 e/log2 = 4779 /1.1 1 toter 4008.4 1 toter 4008.4</td> <td>6 9 94 94 95 95 95 95 95 95 95 95 95 95 95 95 95</td>		v g. 8. 3 + 1 39 1 8 40 57 /# 17.log1 e/log2 = 4779 /1.1 1 toter 4008.4 1 toter 4008.4	6 9 94 94 95 95 95 95 95 95 95 95 95 95 95 95 95
10 44 24 fn 50 10 10 46 54 40 10 10 46 54 40 10 10 46 54 40 10 10 46 54 40 10 10 45 54 40 10 10 36 27 54 56 57 54 56 57 57 56 57 57 56 57 57 56 57 57 56 57 57 56 57	10 10	4. 截 動 約. 種 動 和 和 約. 動 動 和 和 約. 動 動 和 和 和 和 約. 助 約. 助 約. 助 約. 助 約. 助 約. 助 約. 助 約. 助	(g i 7 e 1 70 I E 40 5 PO 57 /insp 2 Thogs n//insp 2 TTP /1.1 1 1 toto 4008.4 Constant is ep-all Constant is ep-all Constant is ep-all	6 20 24 24 26 26 26 27 27 27 27 27 27 27 27 27 27 27 27 27

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.

CD Drawing 12		Contraction of the local division of the loc						Add and the other
Text	Seve	Destination	Transat	Langer, Selo				1000
\$11.33 Million	WC. 888.3.3	1108.108.101.108	THE	to warms - Anna [1991] Ampel also sha	IN Level Providen London Lain	C. PERMA		10.00
ALA DI ALBORN	LTD. 149, 322, 154	CINAMATA	1.00	an want, > starts [SPh; Art] Dependent	tell, billerettell, parent Phile-Debe.	NH DK 34	ALC: FEBRUARY CO.	11-
811 IT.828248	512.188.1.8	128.108.122.158	10.0	se super - entry [-cur] ped-t word a	10-111000 10000			
R13 17 412145	The state of the second	198,188,212,198	ATTR	THE MEET PRODUCT COMPACT AND ADDRESS. IN CO.	the state of the s		. Juni I	
414 31, 254442	128.388.222.156	351.108.2.3	40.15	140 NULLANT'S THE DR CLARK VALUET	Mark Device Factor Cite	erm.		
NAL DURING	100.100.1.0	194.194.112.108	100	ne subar + quer fiers] asd-are we	Spranzföregnssa Packet Chr	60		
BILL IL CLASSES	Did. 188.3. S	100.100.001.100	NOTE:	BELLET. JARAPPEL/ PITP/L.L	Sat/Shoet Time Reference Onl	647		305
pay at sectors	529.190.111.190	101.108.1.3	100	the state is stored factor inchestor when	Time Skill Out	1.00.1	A restauration work	
AND IL ATOMAN	100.100.010.000		100	have send a month living sectors and	and a second		A CONTRACTOR AND	
949 31-4(945)	1277-1408-1402-1308.	156-108-4-3	- HULL	The sector and the constraints?	Parant Louise and			
Marriet II, Wall Marriet Protocal Tanonicities Contr Content Transfer Dis. from URL Esca	et or sire (1200 62) montairy_tains or (2 Wrains 4, Srit 201 al Wrathcol, Bro Mer Promont ded: application/re-	 a), 761 liptas captors e-monocalastroly, no 168-2-3, 2011 129 Jak to 62242, det Aurti 4 monthing-priorization 	nd (6300 837 61 / Michael 20 6 222 256 6693, 5495 1	taj os Interfece (Bellovier (2001)) 6 feiteris (Pelani, Bellovier 10) 1, Ann. 1, Lee: 201	Last Rescheel Home Apply as Piller Properties Titler Conversation Fitter Colores Conversation	:		
Hornet II, No. Internet II, Portugal Transformer Portugal Transformer Transfor HOM, Form URL Case	et an sire fuite hit mensuire dathered of worthered, Sort 100, al Wratered, Bro Aur Pretense deft application/r	 Tell lefter capture or miner dater of 1, to 168 J. S. Berr 199 Left T. Addit, dot Aurt. 4 million of Detodal 	nd (6100 AJ) 31: 70:40.27 5-222.250 6403, 5-40 1	taj es laturfaci (declarate) (antaŭ) 1919 - Senta (declarate) 1919 - Senta (declarate) 1919 - Senta (declarate)	East Reschard Hame Apply on Piller Propersion Rither Conversation Rither Colorison Conversation SCIP Fallow		KP Snam Di Ak-Seb-T	Ŷ
Henrich 23, Wei Henrich 23, Wei Informat Protocol Transferson Contr Reportant Transfer Hol, Form URL Soci	et an sire fuite hit mensuite dation de co montaire dation de co montaire dation de co di Protocol, brit foi Protocol defi applitation/r-s	1), THE lights capture action to be investigated by the 2.5 km state of the the state, but have a to state, but have a me from or becoded	of (6200 k) (1. 70,004.20 (1.222.254 (607, 566, 1	taj es laturfair (bedevaer_landar) noteren (onen-porteren) 1. aŭt 1. dec 201	List Replied Years Apply in Plan Propersis Filter Constantion Filter Calories Constraints Scatter Fallers Capy		107 Datam Dalida-Sell-T Mill Trans. Dalida-Sell-T Mill Trans. Dalida-Sell-T	ï
Transmitti (Mill Syd Thermet J. Kur Internet Protocol Transmitticscon Control Reportant Transmitti (Chi, Apres Mill Coco	et on alle (1000 til) maniper anterier (wreins 4, Srit 100, di warined, arc Me Persona det applicatione -	(1), The lights capture as more dankers), op 1813 J. Berr 135 Me T. Added, Oct Parts 4 me from printedal en from printedal en from printedal	of (6000 10) 1. 79:364.00 1. 222.254 6607, 560, 1	taj en laturfare (deslovater janilar) 1947 de 1947 (desla de ferencia) 1. auto 4. des. 201	Tati function frame Apply in Film Apply in Film Convention Film Convention Film Colorer Fallere Fallere Copy Fallere F		127 Stram Obliviti-Sell-7 Mill Stram Obliviti-Sell-7 Mill Stram Obliviti-Sell-7 Mill Stram Obliviti-Sell-7	Ĺ
Transati Mil 201 Element J. Sol Transati Protocol Transaticular Cost Romer Sale Transati (754, Apres SEL Cost (754, Apres SEL Cost (754, Apres SEL Cost) (754, Apres SEL Cost)	et on afte (1000 60) mention action for (Mersion 4, Srit 100, al Available, Srit 100, al Available, Srit 100, Available, Signification doi: Spillable, Signification 70 of 10 50 10 50 40 41 50	(1), Tell Teltar Captors (2007) State (1991), Ob (2007) State (1991), Ob (2	9 7 7 1	taj es laturfair (belovier) jantan 1919 - Sent (belovier) 19 et de la constanti (belovier) 2. etta 1. dec 201	Tan Rechar Hanne Apply or Film Apply or Film Program of Print Convention The Convention State State State Copy Produce Rednesses Description		TCP Straam SPI St	
Transmitter, Wei Light Ethermett J. Frankreit Transmitterson Control Transmitterson Control ROM, Form ML Doci 29 44 28 fr 96 61 87 96 184 98 88 86 77 26 11	et on offin (1000 60) mention and officient of (Westion A, Sert 1001 of westion A, Sert 1001 of westion A, Sert 1001 of westion A, Sert 1001 def application/c-o	(1), TRI lights captors (0), TRI lights captors (0), TRI lights, Entry 129, 100 (10), 13, Entry 129, 100 (1), 14, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	9 9 7 1	taj en laturfare (berlevaer_jantan) Britele (berlevaer) 1. Add. 1. Janu 201	Tat function frame Apply in Film Apply in Film Apply and Film Convention Film Convention Sc27 Film Convention Convention Convention Convention Convention Convention Denote for		Y22 Staam Ori A5- Seb-T all Stream Ori A5- Seb-T all Stream Ori A5- Seb-T Sel Stream Ori A5- Seb-T Ni Stream Ori A5- Seb-T MTP Stram Ori A6- Seb-T	L
The set of	et de silve (DERM BUD mendion 4. Serit USL de Pertanol, de la con- lection 4. Serit USL de Pertanol det application de la formation de la contraction de la formation de la contraction de la formation de la contraction de la cont	 Tell Types Captors Tell Types Captor	et (6286 62) 1. 791-86.22 5. 222,256 1602, 5eq. 1 9. 7 7 8 9. 7 7 8 9. 7 7 8	taj en laturfare (belovier jantar) n ferens (on en officierne) 1, etc. 1, ene 701	Eat fraction Flame Apple of Flam Apple of Flam Program in Flam Convention The Convention Scale Factors Convention Convent		T2P Stram SP St	
Thermost 11, 10 and 10	et de selve (2008 tol) mendaris de senor en o version 4. Sett 100 de vestions, ne de Person Perso	(1), Tell lights captors (1), Tell lights captors (1), 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	9-8 (7 +)44 	toj w lotarfare (belovier) janitari 1917 - Jacob (belovier) 1, Aldi 1, Jacob 201 1 1	Ear fraction France Apply in Filter August in Filter Convention Filter Convention Filter Convention Filter Schweiter Schweiter Australi Antenessie Beerste Ke. Beerste Ke.		XP Stam Dil-M-Sell-F Off Street SET Street Dil-Model Dil-Sell-F Dil-Sell-F Dil-Model Dil-Sell-F Dil-Model Dil-Sell-F Off Street Off Street Sell-Sell-F Dil-Model Dil-Sell-F Sell-Sell-F Dil-Model Dil-Sell-F Sell-Sell-F Dil-Model Dil-Sell-F Sell-Sell-F Dil-Model Dil-Sell-F Dil-Model Dil-Sell-F	
201 40 20 20 20 20 20 20 20 20 20 20 20 20 20	at at<	11.7. 701 bytes captors 01.7. 701 bytes captors 109.2.3.5. Text 129.100 109.2.5.5. Text 129.100 109.2.5.5.5. Text 129.100 109.2.5.5. Text 129	9-8-37 - 70-0012 - 522-254 - 522-254 - 522-554 - 522-554 - 522-554 - 522-554 - 522-54 - 522-55 - 525-55 - 555-55 - 555-555-55 - 555-55 - 555-5	taj en laturfare (belovier) jantari 19 (r. 1947) 19 (r. 1	Ear fraction Flame Apple of Ver Propers on Prev Convention The Convention The Convention State Convention Conv		T2P Stram ST2 Stam St2	
201 40 20 40 20 40 201 40 201 4 201	es on serve public de mension autores o mension a serve o mension a serve o mension a serve o mension a communication and a mension a mens	11.), 701, 1ghas capture 101, 714, 1ghas capture 101, 21, 5, 1brt 129, 100 101, 21, 100 101, 100 1	p.3 () + () p.3 () + () p.3 () + () () p.3 () + () () p.3 () + () () p.3 () + () () () p.3 () + () () () () () () () () () ()	toj es laturfare (belovier) jonizan Riferie de (delene de ference) 1, Alto 1, Amer 201 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Ear fraction France Apply in Filter Program in Filter Concessation Filter Concessation Filter Concessation Filter Concessation Filter Concessation Filter Concessation Filter Fil		KP Snam Sill Snam Sn	
The second	 a) and set a public field of the public field of the	11), 201, 201, 201, 201, 201, 201, 201, 201	9-8 (2) 9-8	tzj wolaturfare Geoloview Lantzen Riferarte (telescon telescon 1, alte 1, alte 201 2, alte 1, alte 201 3 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Ear fraction Figure Apple or War Program on Fine Concentration (The Content Concentration 5527) Fathere Conp Produce Technology Research Ro. Descrift Ro.		T27 Staam CH-146-Stdi-T Will Stream CH-146-Stdi-T Will Stream CH-146-Stdi-T Will Stream CH-146-Stdi-T Will Stream CH-146-Stdi-Stdi- Stfill Stream Of Staam Of Staam Stream CH-146-Stdi-Stdi-Stdi-Stdi- Stfill Stream Of Staam	
200 44 20 57 40 201 44 20 57 50 201 44 20 57 50 201 44 20 57 50 201 40 20 57 50 201 40 20 57 50 201 40 20 50 201 40 20 201 40 201 40 2	et also starts plant mail mentaria starts of a mentaria starts of a deventorial, nor fee Performant Ref. application/or- donated starts of a fee also starts of a deventorial starts of a plant starts of a deventorial starts	11), 78, 1914 - Capton Capton Capton Capton 161, 24, 597 - 193, 104 161, 24, 597 - 193, 104 161, 24, 597 - 193, 104 161, 24, 597 - 194, 104 161, 24, 597 - 194, 104 161, 24, 24, 24, 24, 24, 24, 24, 24, 24, 24	p - 4 (-)	tzj w latarfar (belovar) janiza 1917 - Part (belovar) 1917 - Part (belovar) 1, Alai 1, Amer 201 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Lan Inschort fanne Apply en Filter Progene en Filter Consentation Filte Colorer Concensation 5/CP Felfere Felfere Pensite A Descrite Factorerse Descrite Factorerse Descrite Factorerse Descrite Factorerse		T2P Stram SIT Stress SIT Str	
Total Total Total Total Total To	at or start plant with mention automotion (s) (s) mention (s) (s) (s) (s) (s) mention (s)	11), 201, 201, 201, 201, 201, 201, 201, 201	p. 8 (2) +	tzj so istarfar (Geslevier jantar) 19 (r. 1967) 19 (r. 1967) 1, anii 1, anii 721 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Ear fraction Figure Apple or War Program on Fine Concentration (The Concentration (The Concentration (The Concentration) State Conp Figure (Concentration) Conp Figure (Concentration) Figure (Concentration)		T27 Stram Divide Statist Mill Strame Divide Statist Statistics of the Statistics Statist Statistics of the Statistics Statistics Statistics Statistics Stat	

GAMBAR 3 PAKET YANG BERISI DATA

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

📕 Winshark - Follow HTTP Stream (tcp.stream eq 13) - Wi-Fi 6					5		×
POST /absensi/login/logged_in HTTP/1.1 Nost: toko4000.sth Connection: keep-alive Content-Langth: 63 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://toko4060.sth. Content-Type: application/x-waw-form-unlencoded User-Agent: Mozilla/5.0 (Window: NT 10.0; Win54) Accept: tast/html.application/xittel+sml.applicati signed-exchange; vw05;q=0.9 Referer: http://toko4066.sth. Accept-Language: en-US,en;q=0.9 Cookie: us. name="Adi"	x54) ApplewebKit/537 on/wel;q=0.0,lmage/a n	.36 (XMTML, wif,image/w	like Gecka) hbp.image/ap	Chrome/108.0 ng,*/*;q=0.0,	.0.0 Safa applicati	ri/537. m/	36
<pre>_ac_name=Ad18ac_password=448ac_persistent=18 Saruar: Zope/(Zope 2.9.8, python 2.4.4, win32) 25 Date: Tue, 10 Jan 2023 10:40:37 0MT Content=Uength: 320 Content=Type: text/html; charset=iso=859=15 X-Cache-Control=Hdm-Podified=By: CookieCruebler Cache-Control=Ndm-Podified=By: CookieCruebler Cache-Control: no-cache Set-Cookie: _ac_name="Ad1", Path=/; Explres=Wed,</pre>	subelt=+login+HTTP/1 erver/1.1 10 Jan 2024 10:60:3	.1 200 OK 7 +0000					
<pre>chtel> chead>ctitle>loginc/title> chead>ctitle>loginc/title> cmata content="width-device-width, initial-scale- meta name="viewport" content="width-device-width ctitle>Zopec/title> c/hwads cbody> </pre>	1.8, maximum-scale-1 * />	.0, user-sci	alable-1' na	ee-'viewport'	D		
<pre>ch2>LogIn successful cp>ca href=""".,/">Continue</pre>							
2 client plats: 2 nerver jats: 3 cums				1.12	- CONTRACTOR	200	
Entre conversation (3593 bytes)				Sho	e datu as 🖓	SCIL	
finds						Find	inst.

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.

E	🚽 pingflo	od.bat 🔀	
Γ	1	ping 192.168.2.1 -t -1 65000	- 63a
			pingilood

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.

Interfa	Interface List	Ethemet EoIP Tunnel	IP Tunnel (GRE Tunne	el VLAN	VRRP Bond	ding LT	E
┝▼		Detect Inte	emet					Find
1	Name 🛛 🗡	Туре	Actual MTU	L2 MTU	Tx		Rx	
•	ether1	Ethemet	1500	1598		0 bps		
•	♦ ether2	Ethernet	1500	1598		0 bps		
•	ether3	Ethernet	1500	1598		0 bps		
•	ether4	Ethernet	1500	1598		0 bps		
•	pwr-line1	PWR	1500	1598		0 bps		
4	₩wlan1	Wireless (Atheros AR9	1500	1600		0 bps		
	«-»wlan2	Virtual	1500	1600		97.5 kbps		6

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.

Constant and Constant and Constant	
🚾 🖬 C. Statesburg and the D.Correct and	· · · · · · · · · · · · · · · · · · ·
👬 📅 🖬 Collegender (1) and an	- E &
📰 🖓 🗰 C/Window@aydem3D.org4.exe	- 🗆 X
APPEN Pinging 102,108.2.1 with 45800 bytes of data:	
Rep Rep Reply from 102 168 2 1 hytes=15000 Time=30et TTL=54	
mental Reply From 182,168,2.11 Dyte:=55800 Time-Stat TIL-54	
Real Reply from 192 108 2 1; bytes-05000 time-21ms TTL-04	
and any fight from 100, 100, 2 1, bridge 5000 time-64mb TTL-64	
And Series - Series 102, 208, 2, 1 Drts: 05800 Time-4281 Til-54	
Red Redly from 152, 108, 2, 1) hyter-55000 time-27mg TTL-54	
Rep. Reply from 102.108.2.1 hytos-45000 time-14ms TTL-04	
sen Septem Reply From 102 108 2.1 Dylus-05000 Line-51es TTL-04	
Reply From 192 168,2.1 Uvtes-15800 Time-1885 TTL-56	
Repart Apply from 152.108.2.1 http://5000 time-films TTL-00	
and apply from 152, 108, 2, 1; bytus=05000 time=50ms 771-94	
Rep. 4001y from 192 108.2.1. byte:=05800 time=2101 TTL=54	
Reply Reply From 162.152.2.1 https://5000 time-21mt TTL-04	
and Reply from 192.168.2.1: bytes-dime-lime-lime TIL-64	
and Her and Apply from 192, 158,2.1: bytes-05000 time-27es TTL-54	
men men ments from 192.168.2.1. bytes=05000 time=21ws TTL=04	
Replace Reply from 192.108.2.1: hyter-d5040 time-30mm TTL-60	
Rep Rep April Reply from 192,108.2.1. hytes-55000 time-40ms TTL-54	
Reg men maply From 192.168.2.11 bytes-65898 time-42mi Tit-64	
apt 40 mar Apply from 192.168-2.11 bytes-15000 time-45ms TTL-64	
ter deply from 192.108.2.1: bytes-65000 time-69es TTL-56	
and Apply Fruit 102.108.2.1: bytes-05000 time-43ms TTL-64	
Beply From 192.160.2.11 bytes=65000 time=3100 TTL=64	
Apply From 192.108.2.1: hytes-65000 time-dime TTL-50	
Ter Reply from 102,100.2.1: bytes=01000 time=02ms TTL+04	
"Reply From 102.168.2.1 Dytes=05000 time=31ms T7L=64	
Reply From SP2.108.2.1. Dyte:=65000 time=4200 TTL=64	
	*
Theply From 192 100.2.11 bytes=65600 time=22ms TFL=64	564U
Reply from 192.105.2.1: bytes-d5000 time-dtms TTL-68	
The Instantial Contract	
122	

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.

Hotsp	ot												
Serv	er Profiles	Users	User Profiles	Active H	Hosts IP Bir	dings 3	Servic	e Ports	Walled G	iarden			
Interface List													
Inter	face Inter	face List	Ethernet I	EoIP Tunne	I IP Tunnel	GRE 1	Funne	VLAN	VRRP	Bond	ding	LTE	
⊹ •		2 🐹	▼	Detect In	temet							Fin	d
	Name	1	Туре		Actual MT	J L2 M	TU	Tx			Rx		•
	ether1		Ethernet		15	00	1598			0 bps			0
	+ether2		Ethernet		15	00	1598			0 bps			0
	ether3		Ethernet	Ethernet		00	1598	0 bps		0 bps	3		0
	ether4		Ethernet		15	1500 159		0 bps		0 bps	(0
	pwr-line	e1	PWR		15	00	1598			0 bps			0
R	⇔ wlan1		Wireless (At	heros AR9.	15	00	1600		20.3	kbps			28.2 k
R	≪->wla	n2	Virtual		15	00	1600		14.8	Mbps			16.2 M

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.

inered Table Co		20	Frend Puls co	. 10
Grout Absent Lits Alle	(Bemin)	04	Gerent Athenuel Edge Attan Subdice	-DH
Chan yest		Geol	Aption des	Canad
Se: Address	•	Anti-	Cites	Auto
Dat Address	•	Over	Log Fails	Dable
Petand C 1 horse		Date and		Connert
Sec. Park		Cree		Day
the first	1	Famous		Periore
Jug Part [Rever Courters		Pearl Durber
in starface		Read /# Courtery		Proset Al Courses
Gat Interface	•			
in Intelesciat				
Out. Hereface Lat.	•			
Partiel Heli:			1	
Comedian Ball				
Autry Hat:	•			
Romy Talle				
Connection Type:	•			
Cerventer Sale	•			

GAMBAR 9 SETTINGAN FIREWALL

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

		19901	- see ge	100	Service	our correc	ages (A	ocheste ross -	Lingues i Prop	ocos :		
٠	-	-	× 🗂	7	00 Rese	Counters	00 Fest	et All Countern	Find	a	Č.	
#		Action	Dian	96	Address	Del Address	Prote	Se Pat	Diff. Port	b. Itler.	Out HE	10.81
5	Ð	Vace.	hereput	-			17.4.		64872			- 14
6	D	V 800	heirput				S tcp)		64872-64			1
7	D	Philipp	he-input.									
8	D	× reject	heunauth				5 8cp)					
3	D	Xeject	In-unauth									
10	0	Xeject	he-madh-to	6								
	plat	e hutapot	takes here									
tt.	ж.,	201	unused-ba.									
	21.0	W. NETCI	UT.									
ų,	5	Xino	doward.									
	BL0	K PING R	FLOAD									
13		X 000	input				1.60					
54		Xang	input				1.80.					
E.												

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.

The second s	
🖬 Colombul a fait Durat as	
ang Mara 🗃 Chilledowriagnewillichidaus	- B X
App 10 App 10<	

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.

C + C + everymentation		
	167 108.2 5	
	Speed & Lag control	
Henry A	Comulate Internation	Transforms2
All Installed	Teas Certor	Destangelier
	MD Speed Carded	
	Mahar	
No or Variation of Street, Str	KD Speed	
	Kinkster.	transf his he per test
		AWARE TRADUCT + 27 48 PM
	Odgeng territoria	Milwook Costronia
	lacoming for the second	

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

••••••	3					
Raw Rule	0					
General	Advanced	Extra	Action	Statistics	Ε.,	OK
	Chain: p	rerouting	9		₹	Cancel
Src.	Address:				•	Apply
Dst.	Address:				•	Enable
	Protocol:				•	Comment
	Src. Port:				-	Сору
	Dst. Port:				-	Remove
	Any. Port:				-	Reset Counters
In.	Interface:				•	Reset All Counters
Out.	Interface:				-	
In. Inter	face List:				•	
Out. Inter	face List:				-	

GAMBAR 14 TAMPILAN RAW GENERAL

b. Pilih Action Pilih Address List IP_NETCUT

Raw Rule <>	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
	Apply
Log Prefix:	Enable
Address List: IP_NETCUT	Comment
Timeout: 00:10:00	Сору
	Remove
	Reset Counters
	Reset All Counters

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.

Reval Pule of			Enough Bulle Co.		
General Advanced Edra Actio	n Statistics	CK	General Advanced Edge Action	Statutics	DK
Chain: forward	1	Canod	See Address List 1 1 P. MET	TUT	Fancel
Set. Address	•	Apple	Out Address Lat		Apply
Det Address:		Enable			- CHIE
Protocol:		Corport	Lager7 Protocol	*	ENDIE
Sc. Pot.		Crevy	Contant	-	Connect
Dr. Put		Bercove	Connection Bytes		Copy
20.00		Reset Counters	Connection Rate	<u> </u>	Reteve
reg. Fut.		0	Contraction mate.		Reset Courters
In Haface.		Caser al Courters	Per Connection Glazafier		Reset All Courters
Dut. Herface	*		Sirc: MAC Address		

GAMBAR 16 TAMPILAN FIREWALL BLOK NETCUT

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

Firewall									
Filte	r Ru	les NAT	Mangle R	aw Service P	orts Connect	ions Ad	ddress Lists	Layer7 Proto	ocols
+ - V X OO Reset Counters OO Reset All Counters Find all									
#		Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter
5	D	✓acc	hs-input			17 (u		64872	
6	D	✓acc	hs-input			6 (tcp)		64872-64	
7	D	@ jump	hs-input						
8	D	💢 reject	hs-unauth			6 (tcp)			
9	D	💢 reject	hs-unauth						
10	D	X reject	hs-unauth-to						
	;;; place hotspot rules here								
11	Х	pas	unused-hs						
	::: BLOK NETCUT								
12	Х	🗶 drop	forward						

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 :

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

TABEL 1 HASIL	PENGUJIAN PENETRATION TESTING MITM
---------------	------------------------------------

			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 <i>netcut</i> dengan cara masuk disatu jaringan yang sama kemudian membuka aplikasi dan melakukan <i>scan</i> 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 <i>firewall</i> untuk memblokir <i>IP</i> 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.