Implementasi Serangan Man In The Middle (Mitm) Pada Software Defined Network (Sdn) Menggunakan Ettercap Dengan Metodologi Ppdioo

1st Malik Alrasyid Basori
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
malikalrasyidbasori@student.telkomuniversity.ac.id

2nd Mochamad Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

3rd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

***Abstrak*— SDN merupakan salah satu inovasi dari hasil perkembangan teknologi. Teknologi pada SDN menyediakan control plane yang terpusat dan terpisah dari data plane. Pemisahan ini juga membuat SDN memisahkan fungsi penerusan paket data dan proses routing pada jaringan ini. Pemisahan ini menjadi salah satu celah yang menjadi kelemahan pada SDN. Salah satu kelemahan yang terdapat pada SDN adalah kerentanan terhadap security attack. Peneliti menggunakan kerentanan ini untuk melihat mekanisme serangan MITM pada SDN.**

Pada penelitian ini, akan dilakukan simulasi serangan MITM menggunakan Ettercap dengan teknik serangan ARP Poisoning dan Port Stealing terhadap topologi SDN yang sudah dibuat dengan metode PPDIOO. Skenario ini memiliki dampak yang sama yaitu dapat mengubah credentials alamat IP dan alamat MAC korban pada tabel ARP. Selain itu, Port Stealing memungkinkan untuk menghasilkan dampak maksimal untuk merubah komunikasi switch korban pada switch lain dan hal ini mengakibatkan host tidak dapat berkomunikasi selain dengan penyerang.

Kata Kunci* — SDN, *MITM, ARP Poisoning, Port Stealing, PPDIOO.

I. PENDAHULUAN

Salah satu inovasi yang terjadi pada jaringan dikarenakan jaringan semakin berkembang dalam ukuran dan kebutuhan, menavigasi jaringan telah menjadi tantangan karena menyiapkan jaringan individu secara manual sangat rumit dan memakan waktu untuk jaringan dalam skala besar [1].

Meskipun SDN merupakan inovasi teknologi baru dalam sektor jaringan, hal ini tidak menutup kemungkinan masih terdapat kelemahan salah satunya adalah kerentanan dalam jaringan. Menurut [2] terdapat berbagai kerentanan seperti Weak Authentication, Incomplete Encryption, dan Information Disclosure. Dengan adanya kerentanan tersebut, SDN memiliki berbagai potensi kerentanan lainnya salah satunya kerentanan terhadap security attack. Security attack yang masih popular salah satu nya adalah Man in The Middle (MITM).

Dalam penelitian ini, Serangan MITM bertujuan untuk memanipulasi tabel ARP yang pada host korban, sehingga membuat penyerang bisa melihat data melalui lalu lintas host korban.

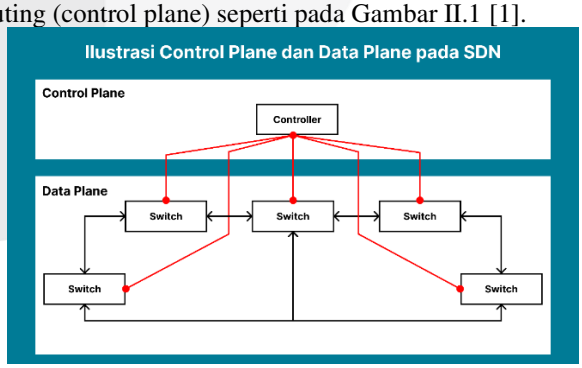
Penelitian ini akan membahas bagaimana mekanisme serangan MITM terhadap SDN menggunakan Ettercap dengan metodologi PPDIOO (Prepare, Plan, design, Implement, Operate, Optimize). Peneliti akan melakukan simulasi penyerangan dengan beberapa scenario pengujian untuk mendapatkan hasil yang maksimal. Penelitian ini dilakukan dengan mengamati 5 parameter pada simulasi yang dilakukan yaitu dampak keamanan, efisiensi serangan, efektivitas serangan latensi jaringan dan waktu serangan. Parameter ini digunakan sebagai perbandingan hasil serangan yang dihasilkan oleh serangan MITM yang dilakukan. Tujuan dari penelitian ini kedepannya adalah untuk mengetahui sistem deteksi dan mitigasi terhadap serangan MITM pada SDN yang dilakukan pada penelitian ini.

II. KAJIAN TEORI

A. SDN

SDN merupakan jaringan yang dapat diprogram dan membuat aplikasi dapat menggantikan jaringan tradisional. Perangkat yang biasa dipakai pada jaringan tradisional dapat dikontrol melalui aplikasi yang terpisah dari perangkat jaringan seperti router dan switch [3].

SDN mengusulkan untuk memusatkan kecerdasan jaringan pada satu komponen jaringan dengan membedakan mekanisme penerusan paket data (data plane) dari proses routing (control plane) seperti pada Gambar II.1 [1].



GAMBAR II.1
Ilustrasi *Control plane* dan *Data plane* [1].

B. PPDIOO

PPDIOO atau biasa dikenal dengan Cisco Lifecycle Service merupakan metode analisis untuk pengembangan

jaringan komputer yang dikembangkan oleh Cisco [4]. PPDIOO memiliki beberapa tahapan dalam implementasinya, tahapan implementasi yang dilakukan *yaitu* prepare, plan, design, implement, operate, *dan* optimize.

C. OpenFlow

OpenFlow didasarkan pada switch ethernet, dengan tabel aliran paket internal, dan antarmuka standar untuk menambah dan menghapus aliran paket. Berbagai switch dan router dapat mengatur tabel alirannya menggunakan OpenFlow. Lalu lintas dapat dibagi menjadi aliran produksi dan penelitian oleh manajer jaringan. Dengan memilih jalur yang diambil paket mereka dan menganalisis data yang mereka dapatkan, peneliti dapat mengatur alur paketnya sendiri [5]. OpenFlow merupakan protokol yang digunakan untuk mengatur penerusan paket di Southbound API pada SDN.

D. REST API

REpresentational State Transfer (REST) adalah gaya arsitektur yang didefinisikan untuk membantu membuat dan mengatur sistem terdistribusi. Dalam implementasi arsitektur REST API terdapat beberapa constraint yang harus diikuti seperti Client-Server, Stateless, Cacheable, Uniform Interface, Layered System, dan Code-on-Demand [6]. REST API merupakan protokol yang digunakan untuk mengatur pembentukan, administrasi dan keamanan jaringan di Northbound API pada SDN.

E. Controller

Controller merupakan otak pada SDN. Dengan adanya pemisahan control plane dan data plane Controller pada SDN menjadi pusat dari logika routing pada jaringan. Controller akan secara optimal memprogram alur penerusan paket pada data plane. Controller memiliki beragam bahasa pemrograman dan set fitur. Hampir semua Controller sudah mendukung untuk penggunaan protokol OpenFlow yang digunakan untuk memprogram instruksi perutean pada data plane melalui southbound yang aman [7].

F. Mininet

Mininet adalah emulator yang mensimulasikan sekumpulan Host, switch, router jaringan, dan membuat topologi sederhana [8]. Menurut [9] mininet dapat membuat topologi jaringan yang kompleks untuk tujuan pengujian, tanpa mengkonfigurasi jaringan fisik. Mininet mendukung topologi khusus dan mendukung API Python yang sederhana serta dapat diperluas untuk pembuatan dan pengujian jaringan.

G. MITM

Menurut [10] Man in The Middle (MITM) adalah salah satu langkah paling sederhana, tetapi juga penting untuk mendapatkan kendali atas jaringan. Dasar Serangan MITM adalah dengan menyisipkan diri nya diantara dua titik dari target serangan. Dengan cara ini, semua lalu lintas dari target yang dituju akan melewati penyerang yang sedang berada ditengah target. Dengan dasar serangan seperti itu, lalu lintas paket dapat diperiksa oleh penyerang dan memungkinkan untuk mendapatkan paket dengan berisikan data yang penting atau sensitive [11].

Serangan MITM bisa terjadi pada seluruh lapisan model jaringan OSI. Sebagai contoh ARP Poisoning dapat dilakukan pada layer 2, Session Hijacking dapat dilakukan pada layer 5, dan memanfaatkan kerentanan aplikasi jaringan pada layer 7 [11].

Dalam serangan MITM, penyerang dapat mengontrol (membaca, memodifikasi, mencegat, mengubah atau mengganti) lalu lintas komunikasi antar korban. Tetapi dengan menggunakan protokol MITM penyerang yang tidak diautentikasi tidak meninggalkan petunjuk/jejak dari intersepsinya terhadap kejahatan dunia maya ini, dengan kata lain penyerang tetap tidak terlihat oleh para korban [12].

H. Ettercap

Menurut [13] Ettercap merupakan alat multi fungsi yang bisa digunakan untuk sniffer, interceptor atau logger. Ettercap merupakan tools open source dan gratis sehingga dapat digunakan oleh siapapun dengan sistem operasi windows ataupun linux. Ettercap sudah semakin berkembang sampai saat ini sudah menjadi salah satu alat manipulasi jaringan yang serbaguna.

Konsep penggunaan Ettercap sama seperti konsep metode serangan MITM, karena Ettercap harus berada ditengah target yang dituju untuk menggunakan fitur yang tersedia.

I. Tahapan MITM

Eksekusi MITM yang efektif memiliki dua tahap yang berbeda, yang melibatkan kedekatan fisik dengan target yang dituju. Berikut merupakan dua tahap dalam implementasi MITM [12], yaitu:

1. Interception

Interception merupakan langkah awal dalam penyerangan menggunakan MITM. Langkah ini mengantisipasi agar target tidak bisa mengetahui keberadaan penyerang dengan melakukan penyamaran. Hal ini akan membuat target menganggap situasi berjalan dengan normal dan berkomunikasi tanpa adanya pengganggu dari komunikasi yang dijalankan. Dengan begitu penyerang dapat mengawasi semua lalu lintas yang terjadi pada jaringan target tanpa diketahui.

2. Decryption

Setelah *interception*, penyerang akan melakukan *decryption* yang dimana penyerang akan mengurai setiap pertukaran data dua arah dari target hingga mendapatkan informasi yang diinginkan dari paket yang korban kirimkan. Namun penguraian data ini tidak akan dicurigai dikarenakan penyerang sudah melakukan penyamaran pada tahap *interception*.

III. METODE

Penelitian ini menggunakan metode PPDIOO untuk merancang jaringan yang akan digunakan dalam pengujian serangan untuk menyelesaikan permasalahan pada penelitian ini. Metode PPDIOO pada penelitian ini hanya dilakukan sampai pada tahap desain dan dilanjutkan dengan tahap simulasi dan analisis untuk melihat mekanisme serangan MITM pada SDN.

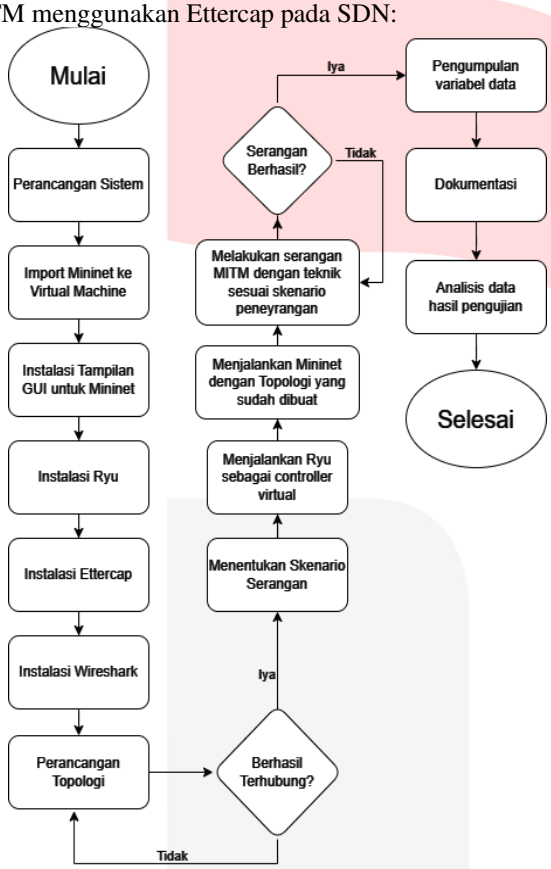
A. *Prepare*

Prepare merupakan tahap persiapan untuk melakukan penelitain, hal ini akan mencakup tujuan penelitian, *scope*

penelitian, perancangan sistem, spesifikasi perangkat keras dan perangkat lunak, topologi SDN yang akan digunakan, dan teknik serangan MITM pada Ettercap yang akan digunakan.

1. Perancangan Sistem

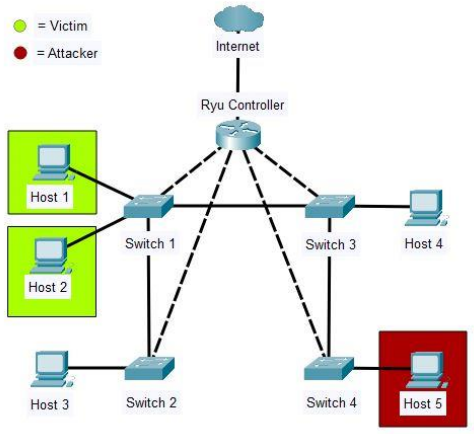
Perancangan sistem yang akan digunakan di penelitian ini akan bermulai dari tahap instalasi, tahap perancangan topologi SDN pada Mininet sampai pengujian serangan berdasarkan skenario dan berakhir dengan analisis hasil dari pengujian. Berikut ini merupakan flowchart perancangan serangan MITM menggunakan Ettercap pada SDN:



GAMBAR II.2
Perancangan Sistem

2. Topologi SDN

Pada penelitian ini, Topologi SDN yang digunakan terdiri dari 1 *Controller*, 4 *switch*, dan 5 *Host*. Dimana seluruh *switch* akan terhubung dengan *Controller* dan setiap *Host* akan terhubung dengan *switch* yang sudah ditentukan. Untuk gambaran hubungan nodes pada topologi SDN penelitian ini dapat dilihat pada GAMBAR II.3.



GAMBAR II.3
Topologi SDN

B. *Plan*

Plan merupakan tahap PPDIOO untuk perencanaan penelitian, pada tahap ini akan membahas parameter keberhasilan, scenario pengujian, dan variabel analisis.

1. Parameter Keberhasilan

Parameter keberhasilan serangan yang digunakan pada penelitian ini adalah penyerang menggunakan Ettercap berhasil memalsukan credentials dari korban. Untuk credentials disini dibatasi berupa IP address atau MAC Address.

2. Skenario Pengujian

Skenario pengujian adalah serangkaian langkah atau situasi yang dirancang dan dibangun untuk menguji kinerja sebuah sistem. Tujuan dari skenario pengujian pada penelitian ini untuk menyerang SDN dengan beberapa skenario yang dijelaskan pada TABEL II-1.

TABEL II-1
Skenario Serangan

Skenario Serangan	Deskripsi	Tujuan
Skenario 1	Serangan MITM dilakukan dengan teknik serangan *ARP Poisoning* menggunakan H5 sebagai penyerang dan H1 dan H2 sebagai korban.	Pemalsuan *credentials* korban yaitu memalsukan *MAC Address* pada korban, sehingga penyerang dapat melihat lalu lintas yang dilalui antara dua korban serangan.
Skenario 2	Serangan MITM dilakukan dengan teknik serangan *Port Stealing* menggunakan H5 sebagai penyerang dan H1 dan H2 sebagai korban.	Pemalsuan *credentials* korban yaitu memalsukan *IP address* atau Port Device pada korban, sehingga korban mengirimkan data melalui penyerang terlebih dahulu.

3. Variabel Analisis

Variabel yang digunakan adalah waktu serangan, dampak keamanan efisiensi serangan dan efektivitas serangan, variabel ini akan memberikan perbandingan untuk melihat bagaimana keadaan korban setelah dilakukan.

Terdapat variabel lain yang akan digunakan untuk memastikan keadaan jaringan dengan pemantauan menggunakan wireshark yaitu latensi. Parameter ini digunakan untuk analisis apakah ada perubahan terhadap

kualitas service pada SDN. Pengukuran latensi akan menggunakan rumus:

$$\frac{Jumlah\ total\ paket}{Total\ waktu\ pengiriman}$$

Peneliti juga akan mengukur waktu yang dibutuhkan untuk melancarkan serangan. Pengukuran ini digunakan untuk mengetahui waktu yang diperlukan untuk melakukan serangan dengan teknik yang digunakan.

C. *Design*

Design merupakan tahap pembuatan topologi, pengetesan konektivitas topologi dan juga akan menjelaskan skema serangan yang akan dilakukan.

1. Pembuatan Topologi

Pembuatan topologi dilakukan pada mininet dengan membuat file python yang berisikan konfigurasi Host dan switch serta penghubungan antar nodes. Pembuatan topologi dapat dibuat dengan mengubah file topologi menjadi seperti berikut:

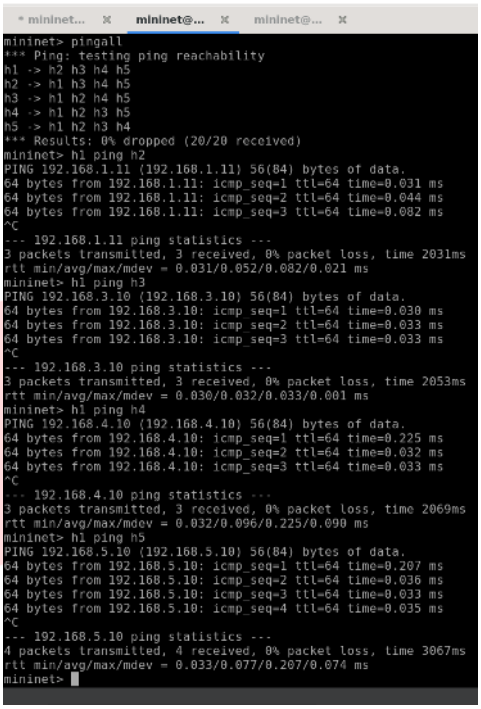
```
from mininet.topo import Topo

class MyTopo(Topo):
    def build(self):
        # Add switches
        switch1 = self.addSwitch('s1')
        switch2 = self.addSwitch('s2')
        switch3 = self.addSwitch('s3')
        switch4 = self.addSwitch('s4')

        # Add hosts
        host1 = self.addHost('h1', ip='192.168.1.10' )
        host2 = self.addHost('h2', ip='192.168.2.10' )
        host3 = self.addHost('h3', ip='192.168.3.10' )
        host4 = self.addHost('h4', ip='192.168.4.10' )

        # Add links
        self.addLink(host1, switch1)
        self.addLink(host2, switch2)
        self.addLink(host3, switch3)
        self.addLink(host4, switch4)

        self.addLink(switch1, switch2)
        self.addLink(switch1, switch3)
        self.addLink(switch3, switch4)

topos = { 'mytopo' : (lambda : MyTopo())}
```

GAMBAR II.4
Konfigurasi File Topologi

2. Tes Konektivitas Topologi

Topologi yang sudah dibuat akan dilakukan pengujian singkat untuk konektivitas dengan melakukan “ping” pada setiap Host. Hal ini dilakukan untuk melihat apakah setiap Host dapat berkomunikasi dengan baik dalam topologi yang sudah dibuat. Hal ini sangat berpengaruh terhadap kelancaran serangan, karena MITM sangat memanfaatkan topologi dengan Host yang bisa berkomunikasi dengan Host lain dan memanfaatkan hal tersebut untuk mendapatkan informasi lalu lintas data antar Host.

Pengujian ping dilakukan dengan menggunakan command “pingall” pada terminal Mininet. Hasil dari pengujian ping dapat dilihat pada gambar … dibawah ini.

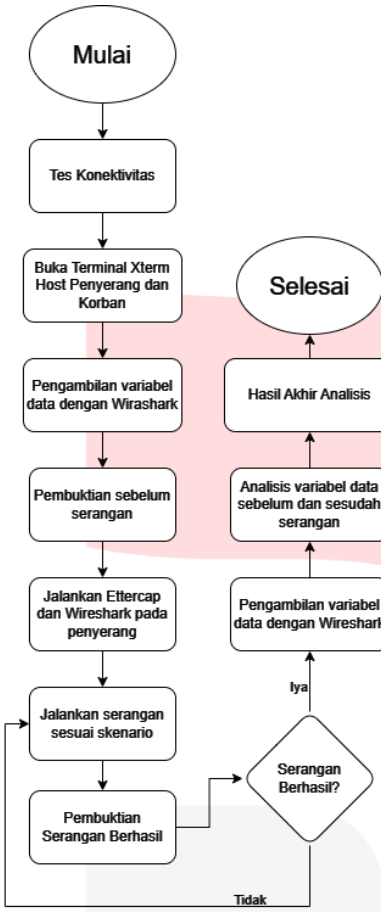


GAMBAR II.5
Tes Konektivitas

Seperti pada GAMBAR II.5 dapat dilihat bahwa setiap Host dapat berkomunikasi satu dengan lainnya melalui pengiriman protokol ICMP dengan command “h1 ping hx” dan “pingall”.

3. Skema Pengujian

Skema pengujian pada penelitian ini digunakan untuk menentukan tahapan pengujian yang dilakukan pada setiap teknik serangan yang dilakukan. Skema pengujian penelitian ini dapat dilihat pada GAMBAR II.6 dibawah ini.



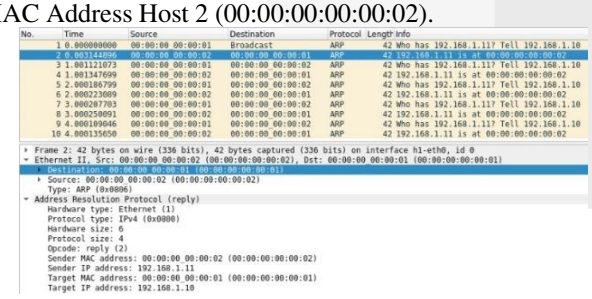
GAMBAR II.6
Skema Pengujian

D. Simulasi

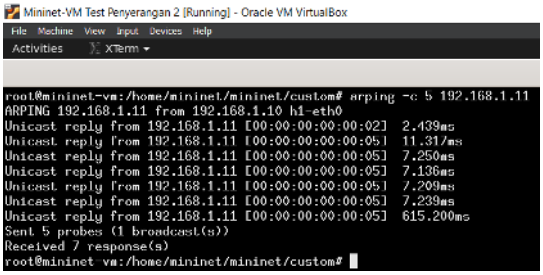
Pada tahap simulasi akan dilakukan sesuai dengan skema pengujian yang telah ditentukan sebelumnya pada GAMBAR II.6. Simulasi pada penelitian ini akan dibagi menjadi 2 karena terdapat dua skenario yang akan dijalankan, yaitu skenario 1 teknik serangan *ARP Poisoning* dan skenario 2 teknik serangan *Port Stealing*.

1. Skenario 1 *ARP Poisoning*

Pada GAMBAR II.7, peneliti melakukan pengiriman paket ARP menggunakan arping untuk melihat tabel ARP target yang diinginkan. Disini peneliti menggunakan perintah "arping -c 5 192.168.1.11" seperti GAMBAR II.8 untuk memastikan tabel ARP pada Host 2. Dan disini IP Host 2 masih terletak pada MAC Address yang seharusnya yaitu MAC Address Host 2 (00:00:00:00:00:02).



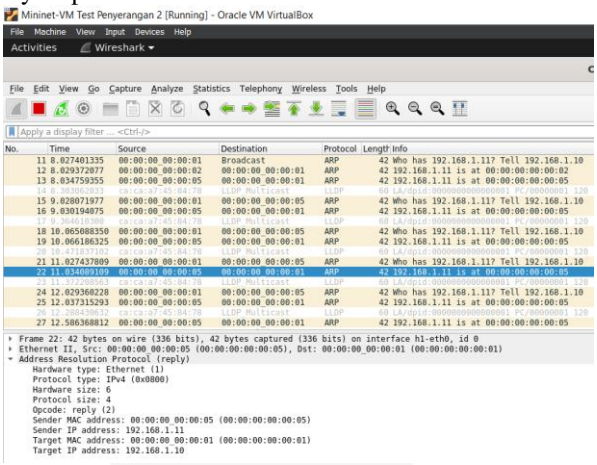
GAMBAR II.7
Bukti Sebelum Serangan



GAMBAR II.8
Command Arping

Pada GAMBAR II.9, setelah dijalankan nya ARP Poisoning pada Ettercap terlihat ada peneliti sekali lagi menguji dengan "arping -c 5 192.168.1.11" untuk melihat tabel ARP Host 2. Dan pada gambar sudah terlihat kalau IP Host 2 sudah dipalsukan posisi nya menjadi terletak pada MAC Address Host 5 (00:00:00:00:00:05) yang bertindak sebagai penyerang.

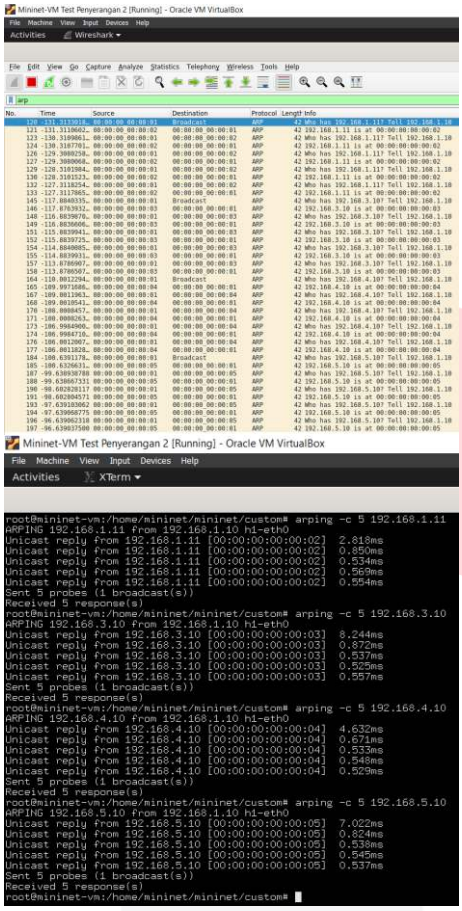
Dengan ini, semua informasi yang melalui Host 1 dan Host 2 akan melewati Host 5 juga sebagai pihak ketiga yang berhasil memalsukan tabel ARP kedua Host korban dan menyusupi lalu lintas data korban.



GAMBAR II.9
Bukti Setelah Serangan

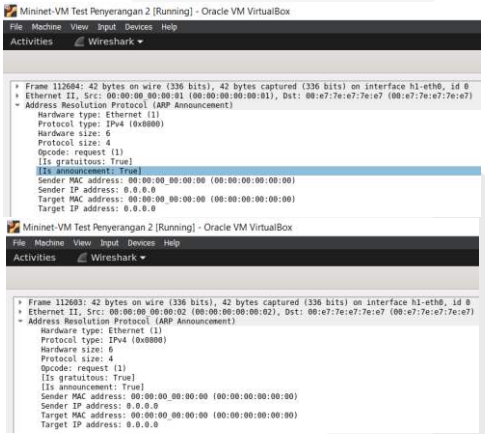
2. Skenario 2 *Port Stealing*

Pada GAMBAR II.10, peneliti mengirimkan paket ARP kepada *Host* yang terhubung dengan *Host* 1 menggunakan arping seperti pada scenario sebelumnya, dan disini masih terdapat jawaban dari seluruh *Host* dan tabel ARP setiap *Host* masih terletak pada posisi yang seharusnya.



GAMBAR II.10
Bukti Sebelum Serangan

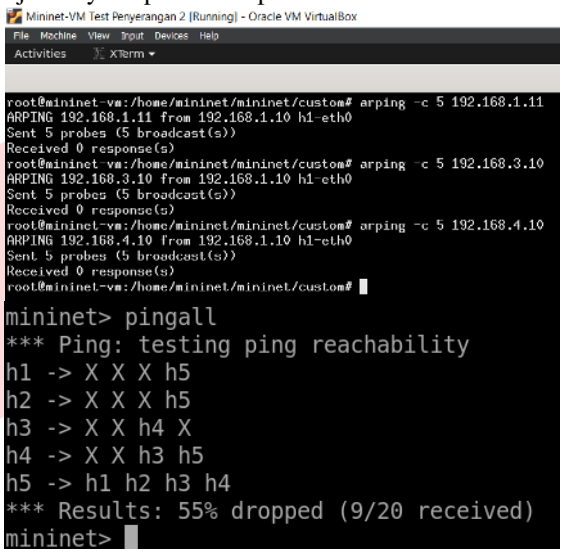
Setelah melakukan serangan, akan melihat tabel ARP korban menggunakan command “arping” dan melihat pada wireshark apakah tabel ARP korban sudah berhasil dimanipulasikan.



GAMBAR II.11
Bukti Setelah Serangan

Pada GAMBAR II.11, terlihat bahwa credentials Host yang terhubung dengan switch korban sudah terpalsukan dimana Host 1 dengan MAC Address 00:00:00:00:00:01 dan Host 2 dengan MAC Address 00:00:00:00:00:02 dan membuat tabel ARP kedua nya menjadi memiliki alamat IP 0.0.0.0 dan Alamat MAC 00:00:00:00:00:00 untuk sender maupun target.

Selain memalsukan credentials korban yang berpengaruh pada tabel switch, dampak maksimal yang dapat dihasilkan oleh teknik serangan Port Stealing ini adalah dapat membuat Host korban dan Host penyerang terisolasi. Hal ini membuat Host korban hanya dapat berkomunikasi dengan Host penyerang. Begitu pula Host lainnya, Host lain diluar tidak akan bisa berkomunikasi dengan Host yang terisolasi. Untuk lebih jelas nya dapat dilihat pada GAMBAR II.12.



GAMBAR II.12
Bukti Komunikasi Setelah Serangan

IV. HASIL DAN PEMBAHASAN

A. Dampak Keamanan

Data variabel dampak keamanan ketika dilakukannya teknik serangan, kedua teknik serangan akan memalsukan credentials korban yaitu IP address atau MAC Address sehingga data yang mengalir pada lalu lintas topolgi akan dapat dipantau oleh penyerang dan hal ini menyebabkan akan kerentanan terhadap integritas data.

B. Efisiensi Serangan

Terdapat sedikit perbedaan pada efisiensi serangan pada masing masing teknik, dimana jika dilakukan teknik serangan ARP Poisoning, lalu lintas yang dipantau secara berkala memiliki jangkauan fleksibel yang dapat diatur dengan menetapkan dua target Host. Sedangkan Port Stealing akan membuat korban mengirimkan data atau paket ke penyerang terlebih dahulu secara intens.

C. Efektivitas Serangan

Dampak serangan yang dihasilkan oleh kedua teknik serangan adalah pemalsuan tabel ARP dan tabel switch yang membuat perubahan pada IP address maupun MAC address. Seperti yang terlihat pada TABEL II-2, ARP Poisoning memalsukan lokasi IP Host 2 menjadi terletak pada MAC penyerang dan hal ini membuat Host 1 sebagai korban harus mengirimkan paket yang dikirimkan ke penyerang juga sehingga penyerang dapat melihat data dari paket yang dikirimkan.

Sedangkan Port Stealing memalsukan tabel switch sehingga kedua korban memiliki IP dan MAC seperti pada tabel, hal ini membuat penyerang melihat data yang mengalir pada korban karena sudah mendapatkan akses pada switch sehingga paket apapun yang melintas dapat dilihat oleh penyerang.

Tabel ARP *Host* 1 Sebelum Serangan		
Host	IP Address	MAC Address
H1	192.168.1.10/24	00:00:00:00:00:01
H2	192.168.1.11/24	00:00:00:00:00:02
H5	192.168.5.10/24	00:00:00:00:00:05
Tabel ARP *Host* 1 Setelah Serangan *ARP Poisoning*		
Host	IP Address	MAC Address
H1	192.168.1.10/24	00:00:00:00:00:01
H2	192.168.1.11/24	00:00:00:00:00:05
H5	192.168.5.10/24	00:00:00:00:00:05
Tabel ARP *Host* 1 Setelah Serangan *Port Stealing*		
Host	IP Address	MAC Address
H1	0.0.0.0	00:00:00:00:00:00
H2	0.0.0.0	00:00:00:00:00:00
H5	192.168.5.10/24	00:00:00:00:00:05

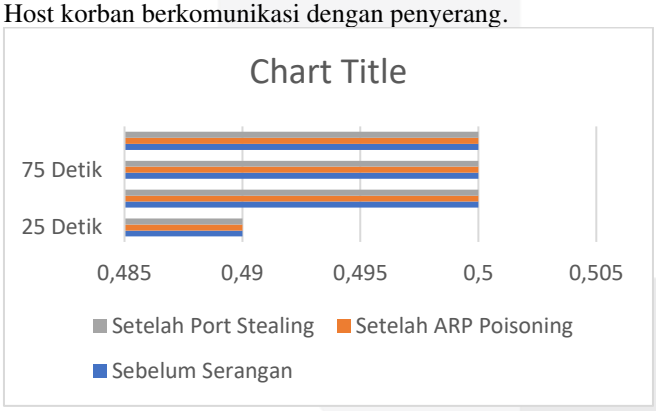
TABEL II-2
Tabel ARP Host

Pada efektivitas serangan yang dapat dihasilkan juga ada perbedaan hasil, dengan teknik serangan Port Stealing selain dapat melihat data yang mengalir pada lalu lintas, dampak maksimal yang dapat dibuat oleh Port Stealing adalah mengisolasi Host korban sehingga korban hanya dapat berkomunikasi dengan penyerang seperti yang terlihat pada GAMBAR II.12.

Namun, dampak maksimal serangan Port Stealing tidak dapat dilakukan secara konsisten. Hal ini dikarenakan pada topologi SDN yang dimana terdapat Controller sebagai pengatur lalu lintas arus data jaringan dan ketika mininet diulang kembali maka serangan Port Stealing hanya dapat memalsukan credentials dan melihat data pada lalu lintas korban sama seperti teknik serangan ARP Poisoning.

D. Latensi Jaringan

Peneliti sudah mendapatkan data variabel latensi ketika Host korban berkomunikasi dengan penyerang.



GAMBAR II.13
Grafik Perbandingan Latensi

Seperti yang terlihat pada GAMBAR II.13 Host korban memiliki lama latensi yang sama dari sebelum serangan dan setelah serangan dilakukan, tidak terdapat perubahan pada latensi dalam komunikasi atau pengiriman paket yang dilakukan antar Host setelah teknik serangan telah dilakukan. Ini membuktikan kalau kinerja jaringan tidak terpengaruh dengan adanya serangan MITM yang telah dilakukan walaupun teknik serangan ini memalsukan tabel ARP pada Host korban.

E. Waktu Serangan

Waktu serangan diukur secara manual menggunakan stopwatch dari awal melakukan tes konektivitas hingga akhir melakukan pengambilan data variabel. Pengukuran ini menghasilkan teknik serangan ARP Poisoning membutuhkan waktu 34 menit 33 detik untuk melancarkan serangan dan teknik serangan Port Stealing membutuhkan waktu 34 menit 28 detik untuk melancarkan serangan. Berikut merupakan rincian waktu yang dibutuhkan oleh kedua teknik serangan.

V. KESIMPULAN

Berdasarkan impelentasi dan analisis serangan dengan menggunakan metode PPDIOO untuk pengembangan jaringan, maka dapat disimpulkan sebagai berikut:

1. Dampak serangan MITM pada SDN yaitu dapat memantau lalu lintas data pada korban dengan memalsukan credentials korban seperti IP address dan MAC Address. Pemalsuan ini membuat korban harus memperlihatkan data yang ingin dikirim kepada penyerang terlebih dahulu. Hal ini sangan berdampak pada integrasi data karena penyerang bisa saja mendapatkan data sensitif atau data penting yang dapat dimanfaatkan untuk kepuasa diri penyerang.
2. Teknik serangan Port Stealing memiliki dampak maksimal yang dapat mengisolasi korban sehingga tidak dapat berkomunikasi dengan Host lain selain Host penyerang walaupun dampak maksimal ini tidak konsisten dikarenakan ada nya controller yang dapat memulihkan kembali lalu lintas data dalam jaringan.
3. Serangan MITM dengan teknik ARP Poisoning merupakan serangan yang lebih konsisten dalam pemantauan data untuk jangkauan yang luas karena pemalsuan tabel ARP tidak terpengaruh oleh controller.
4. Pengukuran latensi pada jaringan korban menghasilkan dengan tidak adanya perubahan pada latensi pada saat sebelum serangan maupun setelah serangan dilakukan.

REFERENSI

[1] S. H. Haji *et al.*, “Comparison of Software Defined Networking with Traditional Networking,” *Asian Journal of Research in Computer Science*, 2021, doi: 10.9734/ajrcos/2021/v9i230216.

[2] A. Pradhan and R. Mathew, “Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN),” in *Procedia Computer Science*, 2020. doi: 10.1016/j.procs.2020.04.280.

[3] T. A. Assegie and P. S. Nair, “A review on software defined network security risks and challenges,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13119.

[4] C. P. Cisco, C. R. Customer, and A. / Cisco Services, “The Cisco Lifecycle Services ‘Valorisez votre solution avec les Services Cisco,’” 2006.

[5] N. McKeown *et al.*, “OpenFlow: enabling innovation in campus networks,” *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, 2008.

[6] F. Doglio, *REST API Development with Node.js*. 2018. doi: 10.1007/978-1-4842-3715-1.

[7] L. Mamushiane, A. Lysko, and S. Dlamini, "A comparative evaluation of the performance of popular SDN controllers," in *IFIP Wireless Days*, 2018. doi: 10.1109/WD.2018.8361694.

[8] A. Sebbar, M. Boulmalf, M. Dafir Ech-Cherif El Kettani, and Y. Badd, "Detection MITM Attack in Multi-SDN Controller," in *Colloquium in Information Science and Technology, CIST*, 2018. doi: 10.1109/CIST.2018.8596479.

[9] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in *Proceedings of the 9th ACM Workshop on Hot Topics in Networks, Hotnets-9*, 2010. doi: 10.1145/1868447.1868466.

[10] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," in *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*, 2016. doi: 10.1109/LISAT.2016.7494156.

[11] M. Brooks and B. Yang, "A man-in-the-middle attack against OpenDayLight SDN controller," in *RIIT 2015 - Proceedings of the 4th Annual ACM Conference on Research in Information Technology*, 2015. doi: 10.1145/2808062.2808073.

[12] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-middle-attack: Understanding in simple words," *International Journal of Data and Network Science*, vol. 3, no. 2, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[13] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," in *IEEE International Conference on Electro Information Technology*, 2018. doi: 10.1109/EIT.2018.8500082.