Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Analisis Serangan DHCP Starvation Attack Pada Router OS Mikrotik

Tamsir Ariyadi[1], Aidil Nur Riyansyah[2], M. Agung[3], M. Alzi Ikrar[4]

[1,2,3,4]Universitas Binadarma, Jl. Jend A. Yani No 3, Kota Palembang, Sumatra Selatan, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 14 Februari 2023
Revisi Akhir: 23 Februari 2023
Diterbitkan *Online*: 10 Maret 2023

KATA KUNCI

DHCP, Starvation attack, Teknologi informasi, Mikrotik

KORESPONDENSI

E-mail: tamsirariyadi@binadarma.ac.id

A B S T R A C T

Information technology is currently growing rapidly, characterized by the existence of various types of computer servers that are connected to each other so as to provide convenience for users. *Dynamic Host Configuration Protocol* (DHCP) is a client-server protocol that funcionts to provide IP Addresses to client computers/ network devices automatically. In using the OS proxy perform further analysis regarding attacks on DHCP starvation attacks. Where the attacker will become a host on one of the computers and request an IP to the proxy OS to obtain the client personal information which will then be recorded and analyzed for the *Man in the Middle attack.* Of course this can be prevented by the *filtering* techniques that exist on the OS proxy. The key can be seen on the *hostname* computer that is registered on the proxy, so that on DHCP *Discover*, which asks for an IP on the Mikrotik DHCP Server, if the *hostname* is not registered, it will be listed for blocking.

1. PENDAHULUAN

Teknologi informasi saat ini berkembang pesat ditandai dengan adanya berbagai jenis *server* komputer yang saling terhubung satu dengan yang lain sehingga memberikan kemudahan bagi pengguna. Namun, dengan perkembangan teknologi saat ini perlu adanya tingkat keamanan yang lebih maksimal, hal ini dapat dilakukan dengan cara komputer memperkuat sistem jaringan kemaman dengan menggunakan server DHCP *(Dynamic Host Configuration Protocol)*, DHCP merupakan server yang memberikan kemudahan dengan sistem penyebaran IP secara otomatis ke perangkat satu dengan yang lainnya. Sehingga pengalokasikan *Address* IP menjadi lebih mudah tanpa harus dilakukan secara manual, dalam hal ini DHCP *(Dynamic Host Configuration Protocol)* juga mampu memperbaruhi alamt IP secara otomatis.[1][2]

Keamanan jaringan saat ini perlu diperhatikan lebih mengingat pertumbuhan dan perluasan Internet semakin pesat. Sehingga membutuhkan beberapa tahapan untuk menciptakan *Security* melalui *layer application*, *transport*, atau *network layers*, *data link layer* (Layer 2). Saat ini, keamanan tidak mampu untuk diterapkan dengan maksimal. Oleh karena itu, perlu adanya, data link layer yang diperlukan dalam suatu LAN yang tidak dibuat dengan keamanan khas. DHCP yaitu salah satu jaringan yang banyak dipakai untuk melakukan konfigurasi pada *host* yang bekerja didalam menghubungkan lapisan data DHCP. DHCP sering terkena serangan, seperti serangan DHCP *Stravation*,serangan DHCP *Snooping* dan Serangan DHCP *rouge server*.[3][4]

Pada dasarnya dhcp memberikan host IP Address dengan subnetting yang sama, yang menjadikan kelemahan pada teknik ini karena adanya serangan yang menciptakan DHCP *server* yang palsu untuk menggantikan router yang asli.[5] Dalam hal ini, diperlukan teknik DHCP *relay Agent* yang mampu mencegah serangan DHCP starvation dengan cara meneruskan IP DHCP dari *router* kemudian meroutingnya sehingga membuat *subnet* yang berbeda ke setiap user computer. Skenario jaringan pada *Local Area Network* (LAN) yang menggunakan router mikrotik untuk mencegah adanya serangan pada *server* DHCP mikrotik perlu adanya penmbahakn switch sisco yang mampu mengangkal serangan DHCP *Starvation* pada mikrotik oleh *attacker*.[6][7]

Pembagian IP Address secara manual sangatlah merepotkan karena setiap computer harus disetting ip addressnya satu persatu. Oleh karena itu dibutuhkan settingan secara otomatis. Pada dasarnya fungsi dari DHCP memberikan setiap *host ip address* dengan sayarat menggunakan *subnetting* yang sama. Teknik ini pun ada kelemahan dikarenakan adanya serangan yang bisa saja si client menjadi DHCP *Server* palsu menggantikan *router* yang asli.[8] Teknik DHCP *Relay Agent* dapat juga mencegah serangan DHCP *Starvation* dengan skenario meneruskan ip DHCP dari router dan meroutingnya secara DHCP *Server* dengan subnet yang berbeda ke setiap *user computer* yang *merequest* DHCP *Discover*. Penelitian sebelumnya melakukan percobaan menggunakan aplikasi GNS3, skenario jaringan yang dibuat dengan menyerang router cisco dengan system operasi Ubuntu dan memanfaatkan tools yersenia untuk melakukan serangan DHCP Starvation, hasil penelitian tersebut, teknik tersebut berhasil memanfaatkan jalur DHCP Server untuk mengirimkan IP DHCP ke *server attacker*,

sampai limit ip *brief* show pada *router* habis, dalam penelitian tersebut peneliti tidak membahas firewall sebagai pencegahan serangan DHCP *Starvation*. Penelitian yang lainnya melakukan skenario jaringan pada jaringan *Local Area Network* (LAN) menggunakan router mikrotik untuk pengaturan DCHP-*Server* kemudian untuk mencegah terjadinya serangan pada jalur DHCP *Server mikrotik*, peneliti tersebut menambahkan *switch Cisco* untuk mencegah adanya serangan DHCP *Starvation* pada mikrotik. Penelitian tersebut menambahkan settingan vlan pada *switch cisco* kemudian mensetting DHCP *snooping* pada switch manage tersebut dengan limit rate user yang dapat akses ke switch /router tersebut, sehingga ip fake / ip yang tidak terlist pada switch akan di blokir. Skenario memungkinkan terhindar dari serangan DHCP Starvation oleh attacker. Penelitian sekarang menggunakan skenario serangan pada router mikrotik dengan teknik serangan DHCP Starvation. Router ini disetting sebagai DHCP Server, tanpa adanya pembahasan firewall untuk mencegah serangan. Tools Yersena juga dimanfaatkan untuk mensimulasikan serangan DHCP Starvation. Hasil yang diharapkan router asli memberikan IP DHCP yang di minta oleh client sehingga IP Address Lease terlimit.[9]

2. TINJAUAN PUSTAKA

2.1. DHCP

Dynamic Host Configuration Protocol adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan Server DHCP berfungsi pada saat komputer client yang sudah terhubung kejaringan meminta alamat IP dari komputer server DHCP yang mana server DHCP ini menyediakan IP address komputer didatabase yang disebut dengan DHCP *DISCOVER*. Dalam hal ini server DHCP akan memeriksa database untuk memastikan bahwa alamat IP tersebut masih tersedia, sehingga server DHCP akan memberikan alamat tersebut sebagai alamat IP komputer yang akan digunakan oleh client disebut *DHCPREQUEST*. Kemudian server DHCP akan memindahkan IP address dari *database* komputer *server* DHCP ke komputer client yang disebut dengan DHCPACK.

Bila Serangan DHCP *Starvation* terjadi,*Attacker* dapat masuk dengan DHCP server mereka sendiri kedalam jaringan kompiter yang diserang.*Attacker* kemudian dapat mulai membagikan alamat IP yang sudah disiapkan sebelumnya. Ketika alamat IP versi Attacker sudah tersebar dan digunakan oleh para klien, semua lalu lintas data yang terjadi pun bisa diakses oleh attacker, Dimana jika yang diserang adalah jaringan komputer perusahaan anda artinya dapat dipastikan data penting yang ada didalam perusahaan tersebut yang menyangkut rahasia perusahaan akan bocor di tangan attacker.

2.2 DHCP PROSES

- Ini adalah peran server Protokol Konfigurasi Host Dinamis untuk menetapkan alamat IP ke perangkat jaringan. Untuk melakukan ini, setiap klien DHCP dan server DHCP bertukar paket.
- Empat jenis paket yang membentuk operasi penetapan alamat IP DHCP adalah *DISCOVER*, OFFER, REQUEST, dan ACKNOWLEDGMENT. Jika PC adalah klien DHCP, ia akan mengirimkan paket DHCP DISCOVER saat pertama kali terhubung ke jaringan. Ini pada dasarnya bermuara pada PC yang mengatakan, "Saya baru saja sampai, hai! Server Protokol Konfigurasi Host Dinamis yang dapat menetapkan alamat IP adalah yang saya cari."
- Jika Anda membayangkan klien di jaringan Anda terhubung ke server terdekat, Anda dapat membayangkan server merespons dengan PENAWARAN. Selain itu, sebagai bagian dari penawaran ini, Anda akan diberikan alamat IP yang disetujui klien. Nyatanya, server itu menjawab, "Selamat datang, saya bisa memberi Anda sedikit tempat di 10.123.0.1. Apakah kamu tertarik?"
- jumlah maksimum alamat IP yang dapat digabungkan pada jaringan /24-bit adalah 254. Beberapa alamat ini dapat disimpan sebagai alamat router statis atau untuk tujuan lain. Oleh karena itu, kumpulan alamat server DHCP yang tersedia hanya dapat berisi sekitar 252 alamat IP.
- Server DHCP memilih salah satu alamat IP yang tersedia dari kumpulan dan mencadangkannya untuk klien baru saat menerima paket DISCOVER.
- Klien harus mengembalikan PERMINTAAN setelah menerima paket PENAWARAN. Pada dasarnya, klien berkata, "Itu sangat ideal. Bisakah Anda memberi saya akses eksklusif ke 10.123.0.1 saat saya di sini?"
- Transaksi selesai ketika server mengirimkan paket ACKNOWLEDGMENT ke klien dan semua pendengar lainnya. Ini pada dasarnya mengatakan "Anda saat ini menggunakan 10.123.0.1. Itu akan diadakan pada 10.123.0.1 jika seseorang perlu menghubungi klien ini."
- Penyiapan DHCP adalah teknik produktif yang memungkinkan pelanggan untuk bergabung dan meninggalkan jaringan dalam konfigurasi yang tidak bermusuhan.

2.3. CARA KERJA

Serangan kelaparan DHCP menggunakan sistem ini.

- Dalam serangan kelaparan DHCP, aktor jahat mengirimkan banjir paket DISCOVER fiktif, menghabiskan seluruh kumpulan paket yang tersedia, yang ia tentukan ke server DHCP.
- Pelanggan mencari alamat IP dan menemukan tidak ada yang tersedia dan ditolak. Anda bahkan dapat mencari server DHCP alternatif yang mungkin disediakan oleh pelaku yang bermusuhan. Aktor bermusuhan ini sekarang dapat melihat semua lalu lintas yang dikirim atau diterima klien menggunakan alamat IP sebagai bermusuhan atau palsu.
- Komputer yang menyiarkan paket DHCP DISCOVER bisa berada di lingkungan yang tidak bersahabat jika komputer jahat menggunakan alat seperti Yersinia.
- Klien jahat ini mengirimkan ratusan, bukan segelintir, paket DISCOVER jahat, menggunakan alamat MAC palsu dan tipuan sebagai alamat MAC sumber untuk setiap permintaan.
- Ketika server DHCP merespons masing-masing paket DHCP DISCOVER palsu ini, seluruh kumpulan alamat

IP habis dan server DHCP-nya kehabisan alamat IP untuk melayani permintaan DHCP yang valid.

- Setelah server DHCP kehabisan alamat IP, penyerang biasanya akan mengaktifkan server DHCP mereka sendiri. Server DHCP jahat ini kemudian mulai membagikan alamat IP.
- Keuntungan bagi penyerang adalah jika server DHCP palsu menggunakan alamat IP bersama dengan DNS keluaran default dan informasi gateway, setiap klien yang menggunakan alamat IP ini dan mulai menggunakan gateway default ini tidak akan dapat mengakses komputer penyerang.

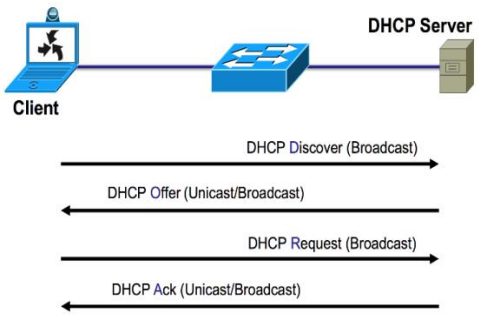
2.4 Fungsi Serangan DHCP starvation attack

- Ketika server DHCP kelebihan beban dengan permintaan alamat IP dari klien yang sah, ia menderita serangan kelaparan DHCP, yang mengakibatkan penolakan layanan (DoS). Setelah serangan knalpot DHCP, upaya serangan man-in-the-middle (MITM) sering diluncurkan.
- Setelah server DHCP membagikan semua alamat IP, apa yang terjadi ketika klien DHCP baru membutuhkan atau menginginkan alamat IP dan bergabung dengan jaringan? DoS atau Denial of Service adalah jawaban yang jelas. Tidak ada alamat IP yang tersedia.
- Untuk alasan ini, setelah serangan kelaparan DHCP, penyerang sering kembali dengan server DHCP mereka sendiri dan mulai membagikan alamat IP. Dan menyebabkan lebih banyak gangguan pada lalu lintas pengguna. Khususnya, jika penyerang melakukan serangan man-in-the-middle, dalam hal ini, lalu lintas dari perangkat yang mencoba keluar dari subnet akan melewati perangkat penyerang. Penyerang berada di jalur target yang dituju.

2.6 Serangan DHCP *Starvation Attack*

Bisa dilihat melalui gambar 1. Jika gambar tersebut merupakan hasil sumber dapat dipastikan source nya. Penjelasan gambar di letakaan pada gambar posisi bawah. DHCP Starvation Attack merupakan suatu kondisi dimana client kehabisan IP yaitu ketika client tidak dapat masuk atau terhubung pada alamat IP sehingga perlu menghubungi server DHCP agar mendapat alamat IP. Namun perlu konfigueasi jaringan DHCP supaya server segera merespon dan memberikan alamat IP yang membutuhkan jangka waktu tertentu. Sehingga pada saat ini Attacker akan mengirimkan alamat IP Palsu pada client untuk mendapatkan data. Oleh karena itu layer dua handshake biasanya akan segerakan dilakukan dengan unauthenticated.

Sesi handshake Client send DHCP to discover >> kemudian server sent over package >> Kemudia client sent request DHCP package >> terakhir sever send DHCP acknowledgment.
Ketika terjadi serangan DHCP starvation attack Attacker send DHCP discover package >> discover >> discover >> discover lagii dan terjadi secara terus menerus serta dikirim secara random pada client, menyebabkan client tidak mampu mengakses jaringanKetika terjadi serangan DHCP starvation attack Attacker send DHCP discover package >> discover >> discover >> discover lagii dan terjadi secara terus menerus serta dikirim secara random pada client, menyebabkan client tidak mampu mengakses jaringan..



Gambar 2. Serangan DHCP Stravation

2.7 Apa itu Rogue DHCP

Peretas menyiapkan server DHCP jahat dan menciptakan konflik alamat IP dengan menyiarkan alamat IP duplikat. Peretas menyusup ke jaringan dengan menyerang perute nirkabel, yang mereka lakukan dengan keracunan ARP untuk menyuntikkan paket jahat ke aliran data yang sedang diproses oleh perute. Peretasan yang cerdik ini memberi peretas akses berkelanjutan ke jaringan melalui server proxy dan surat spam, sehingga menyulitkan profesional TI untuk menghentikan atau bahkan mendeteksi terjadinya serangan dunia maya. Peretas kemudian mendengarkan koneksi masuk dan secara selektif merespons dengan pesan jahat seperti permintaan otentikasi palsu atau virus yang merusak perangkat pengguna yang tidak menaruh curiga.

Serangan server DHCP nakal semakin populer tetapi dapat dikurangi. Peretas menyiapkan server DHCP jahat dan menciptakan konflik alamat IP dengan menyiarkan alamat IP duplikat. Peretas kemudian akan mencoba membuat komputer terhubung ke perangkat jahat alih-alih router. Setelah itu selesai, peretas dapat melakukan apa saja yang diinginkannya, mulai dari mencuri informasi hingga menginstal perangkat lunak berbahaya di komputer Anda untuk mengontrolnya dari jarak jauh. Seorang pejabat pemerintah berbicara pada konferensi pers baru-baru ini mengatakan bahwa Iran telah membuat jaringan nirkabel palsu di negara-negara seperti Irak dan Afghanistan, sehingga mereka dapat memantau komunikasi dengan mudah saat orang-orang menggunakan *hotspot Wi-Fi*.

2.8 Jenis Serangan

Istilah "serangan" digunakan di sini untuk menunjukkan melakukan berbagai peretasan, termasuk kekerasan dan rekayasa sosial, yang memerlukan akses ke sistem atau jaringan komputer target. Berikut adalah beberapa istilah dan proses yang terkait dengan kamp pelatihan keterampilan ini:

a. Brute forcing

Brute force adalah upaya mendapatkan akses sebuah akun dengan menebak username dan password yang digunakan. Brute force attack sebenarnya merupakan teknik lama dalam aksi cyber crime.

b. Password Hashing

Sistem Pencirian Kata Sandi (PHS) adalah metode untuk menyimpan kata sandi dengan aman, membuatnya sulit bagi orang yang tidak berwenang untuk memecahkannya melalui serangan brute force atau kamus. PHS sering disebut sebagai fungsi hash satu arah karena kata sandi tidak direkayasa balik setelah input, tetapi hasilnya selalu sama (kata sandi yang di-hash). Saat masuk ke komputer atau jaringan target, semua PHS mengembalikan "nilai hash" yang sama yang biasanya tidak dapat diubah menggunakan metode serangan tradisional seperti serangan brute force dan dictionary attack.

c. Capture the flag (CTF)

Capture the Flag adalah salah satu jenis dari kompetisi hacking yang dimana mengharuskan seorang / tim untuk mengambil sebuah file / string yang sudah disembunyikan sistem yang dimana disebut dengan istilah “Flag”. Berbeda dari lomba lainnya seperti competitive programming yang dimana alatnya disediakan oleh panitia, Peserta CTF biasanya akan diminta untuk membawa peralatan (laptop/alat lainnya) sendiri dan diperbolehkan mempersiapkan script-script / programnya yang sudah ada dari waktu sebelum pertandingan.

d. Phising

Phising adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit, rekening),Istilah resmi phising adalah phishing, yang berasal dari kata fishing yaitu memancing.
Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan kejahatan.

e. Jenis Phising

Untuk lebih mengenal tindakan phising, mari pelajari jenis phising yang paling banyak ditemui saat ini:
1. Email Phising
Sesuai namanya, email phising menggunakan media email untuk menjangkau calon korbannya. Jumlah aksi email phising ini cukup banyak. Menurut data, terdapat 3,4 miliar email palsu yang dikirimkan setiap harinya. Anda bisa bayangkan, berapa banyak korban yang bisa terjerat aksi ini.

2. Spear Phising
Spear phising adalah jenis dari email phising. Bedanya, alih-alih menggunakan pengiriman email secara masif dengan calon korban yang acak, spear phising menarget calon korban tertentu. Biasanya, teknik ini dilakukan setelah beberapa informasi dasar calon korban dimiliki, seperti nama dan alamat.

3. Whaling
Whaling adalah langkah phising yang tidak hanya menarget individu secara spesifik, tapi juga individu yang memiliki kewenangan tinggi di suatu organisasi, misalnya pemilik bisnis, direktur perusahaan, manajer personalia, dan lainnya.
Dengan demikian, jika tindakan whaling ini berhasil, akan banyak keuntungan yang bisa dimanfaatkan dari akses yang didapatkan.

4. Web Phising

Web phising adalah upaya memanfaatkan website palsu untuk mengelabui calon korban. Website untuk phising akan terlihat mirip dengan website resmi dan menggunakan nama domain yang mirip. Hal ini disebut domain spoofing.

a. Key point

- Serangan brute force adalah metode serangan yang paling umum digunakan untuk meretas.
- Sistem Pencirian Kata Sandi banyak digunakan di semua platform.
- Capture the flag dapat dilakukan oleh banyak pengguna secara bersamaan, yang memotivasi peretas untuk lebih meningkatkan keterampilan mereka.

b. Sniffing Attack in System Hacking

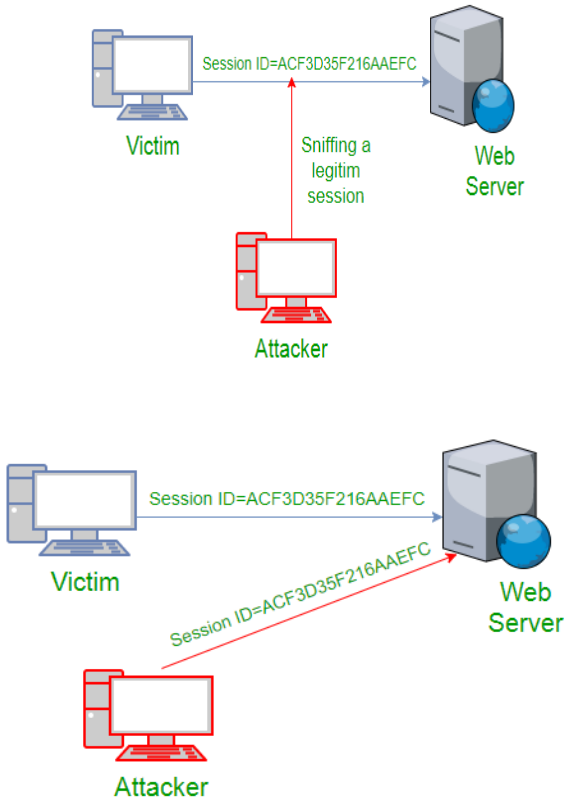
Serangan mengendus dalam peretasan sistem adalah bentuk serangan denial-of-service yang dilakukan dengan mengendus atau menangkap paket di jaringan, dan kemudian mengirimkannya berulang kali ke mesin korban atau memutarnya kembali ke pengirim dengan modifikasi. Sniffer sering digunakan dalam peretasan sistem sebagai alat untuk menganalisis pola lalu lintas dalam skenario di mana melakukan serangan yang lebih mengganggu dan merusak tidak diinginkan.

c. Sniffing Attack

Serangan mengendus juga dapat digunakan dalam upaya memulihkan kata sandi, seperti ketika kunci privat SSH telah disusupi. Sniffer menangkap paket SSH yang berisi versi terenkripsi dari kata sandi yang diketik oleh pengguna di terminalnya, yang kemudian dapat diretas secara offline menggunakan metode brute force.

- Istilah "mengendus" didefinisikan dalam RFC 2301 sebagai: "Setiap tindakan menangkap lalu lintas jaringan dan memutarnya kembali, biasanya untuk tujuan spionase atau sabotase."
- Definisi ini tidak akurat untuk sistem berbasis UNIX, karena lalu lintas apa pun dapat diendus selama penyerang memiliki akses ke antarmuka jaringan (NIC) atau memodifikasi paket yang tidak dapat diubah saat transit. Sniffing dapat dilakukan dengan menggunakan program khusus seperti tcpdump, tcpflow, atau LanMon yang terhubung ke port dimana paket dapat diperiksa dari jarak jauh.
- Serangan sniffing lain yang disebut ARP spoofing melibatkan pengiriman pesan Address Resolution Protocol (ARP) yang dipalsukan ke lapisan tautan data Ethernet. Pesan-pesan ini digunakan untuk mengaitkan alamat IP mesin korban dengan alamat MAC yang berbeda, mengarahkan mesin target untuk mengirimkan semua lalu lintasnya yang ditujukan untuk korban melalui host yang dikendalikan penyerang.

- ❖ Ini digunakan untuk membajak sesi dan juga menyebabkan banjir jaringan melalui serangan denial-of-service (lihat serangan Smurf). Setiap paket IP berisi, selain muatannya, dua bidang: header IP, dan header Ethernet yang merangkumnya.
- ❖ Kombinasi dari dua header ini sering disebut sebagai "paket" oleh mereka yang bekerja dengan komunikasi internet. Oleh karena itu, penyerang dapat melihat dan memodifikasi header IP paket IP tanpa harus melihat muatannya.
- ❖ Header Ethernet berisi informasi tentang alamat MAC tujuan (alamat perangkat keras dari mesin penerima) dan bidang Jenis Ether berisi nilai yang menunjukkan jenis layanan apa yang diminta (misalnya, prioritas atau kontrol aliran).
- ❖ Tipe Ether bisa jadi "0xFFFF", menunjukkan bahwa tidak ada bidang layanan yang disertakan untuk bingkai Ethernet. Ini digunakan dalam implementasi Cisco sebelum versi 8.0.



Gambar 3. *Web Server*

Ada sejumlah metode berbeda yang dapat digunakan penyerang untuk melakukan spoofing ARP. Mereka termasuk:

- ❖ Penyerang memiliki akses ke "cache ARP" pada mesin mereka yang terinfeksi, yang juga berisi alamat MAC mesin lain, tetapi tidak memiliki atau tidak menggunakan alamat IP yang sama dengan mesin lain dengan alamat MAC yang sama di cache ARP mereka.
- ❖ Penyerang tidak tahu metode apa yang digunakan mesin lain untuk menyimpan tabel alamat MAC, dan dengan demikian mengatur jaringan dengan banyak entri duplikat.
- ❖ Penyerang mengirimkan pesan ARP palsu, mencoba menghubungkan mesin mereka yang terinfeksi dengan alamat MAC mesin lain.

d. Cara Pencegahan

- Selalu gunakan hotspot WLAN tepercaya.
- Aktifkan MAC filtering/SSID broadcast pada jaringan nirkabel Anda sebanyak mungkin. Ini akan membantu mencegah jaringan Anda diakses oleh pengguna yang tidak diinginkan.
- Perbarui firmware dan aplikasi setiap kali pembaruan keamanan tersedia untuk mereka (terutama firmware). Ini akan menutup celah dan menambal kerentanan di jaringan nirkabel Anda yang dapat dieksploitasi oleh peretas untuk mendapatkan akses ke perangkat Anda atau jaringan perusahaan di belakangnya.
- Nonaktifkan berbagi file (CIFS/SMB) di jembatan nirkabel, router, dll.
- Catat dan pantau semua lalu lintas masuk/keluar.
- Catat semua peristiwa penyewaan DHCP di jaringan nirkabel Anda.
- Jika server DHCP nakal diakses dari dalam jaringan, maka batasi alamat IP yang memiliki akses ke server DHCP Anda dan/atau setel ulang alamat MAC pada router/firewall Anda, sehingga hanya menerima paket dari alamat MAC spesifik tersebut sebagai yang berwenang perangkat yang diizinkan untuk terhubung ke jaringan Anda (inspeksi paket stateful).
- Ubah kata sandi default (selalu pilih kata sandi yang rumit) untuk peralatan nirkabel Anda seperti router, titik akses, dll.

3. METODOLOGI

3.1 Research Method

[10]*Research method* adalah hal yang sangat penting dalam Research adalah metode penilitian Action Research penelitian tersebut adalah bagian bentuk rancangan penelitian dalam penelitian tindakan,peneliti menggambarkan,menafsirkan dan menjelaskan situasi sambil membuat perubahan dan intervensi untuk mengningkatkan atau berpartisipasi. Menurut pandangan tradisional, penelitian tindakan adalah kerangka kerja penelitian dalam pemecahan masalah dimana kolaborasi antara peneliti dank lien diatur untuk mencapai tujuan, dan bahwa penelitian tersebut sebagai metode penelitian didasarkan pada asumsi bahwa teori dan praktir dapat terkait erat dengan sedang belajar.

Hasil penelitian yang direncanakan setelah di diagnosis rinci dari konteks bermasalah. Tahapan – tahapan proses penyelesaian penelitian ini membutuhkan metodologi yang mana tahapan proses dimulai dari instalasi dan konfigurasi mikrotik OS, dan akhir tahapan yaitu melakukan skenario serangan menggunakan DHCP Starvation Attack dan DCHP spoofing Attack, sehingga tujuan penelitian tercapai dengan adanya attacker melakukan percobaan phising terhadap computer client yang telah menerima IP Palsu yang diberikan oleh Server Palsu. Adapun aliran proses konfigurasi dan skenario serangan yang dilakukan dalam penelitian ini dapat dilihat pada Gambar.

Gambar 4. *Action Research*

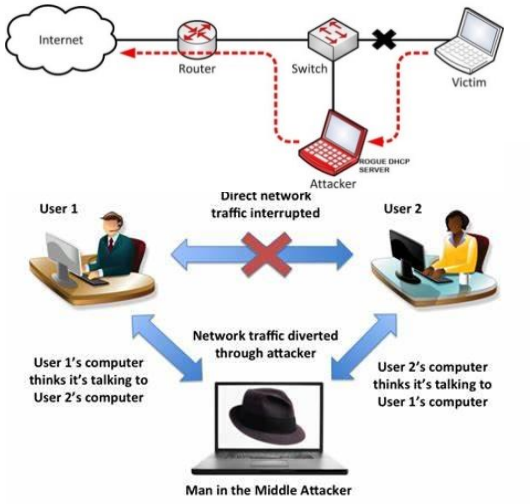
1. *Planning* (Perencanaan)
   Pada Fase ini melakukan identifikasi masalah, mencari informasi terkait penelitian yang dilakukan, menentukan lokasi penelitian, membuat rencana penlitian.
2. *Acting* (Bertindak)
   Pada tahap ini melakukan uji coba,mengumpulkan sumber informasi yang didapat dari berbagai macam referensi.
3. *Observing* (Mengamati)
   Pada tahap ini adalah tahahp pertemuan, saat client terhubung dengan jaringan, client akan mencari DHCP server yang bekerja pada jaringan tersebut.
4. *Reflecting* (Memikirkan dan Mempertimbagkan)
   Pada fase ini setelah semua nya dilakukan hasil dari analisis data akan dilaporkan dalam bentuk laporan.

4. HASIL DAN PEMBAHASAN

4.1 Serangan DHCP *Rogue*

Rogue DHCP adalah salah satu sistem yang memanfaatkan cela security pada konfigurasi mekanisme jaringan DHCP. *Server Rogue* DHCP memberikan alamat konfigurasi pada client yang tergabung dalam jaringan sehingga menciptakan seranganan yaitu Man in the middle berupa ancaman terhadap privasi client tergabung pada jaringan tersebut.

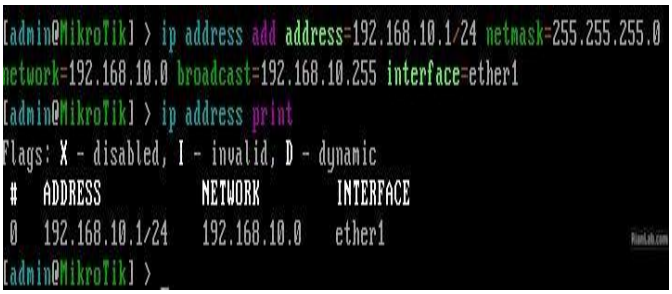
Serangan MITM sendiri merupakan serangan digunakan untuk mencuri informasi client dengan cara memutus jaringan antar client yang tergabung, serangan ini dapat menjadi ancaman, Setelah Attacker dapat mengatur multiple DHCP atau DHCP Rouge, kemudian attacker dapat mendistribusikan IP address ke klien, bukan IP Address saja yang didistribusikan oleh attacker, attacker dapat juga mengganti IP gateway dan IP DNS asli dengan IP DNS dan IP gateway yang dibuat sendiri, kemudian didistribusikan kembali ke klien yang meminta/ request IP ke DHCP Server. Pada proses ini client pasti nya mengirimkan paket-paket data yang diperlukan. Attacker dengan mudah mengakses paket-paket data tersebut dikarenakan client mengakses data melalui DHCP Server palsu. Attacker dapat juga melakukan phising dengan mengirimkan web palsu, sehingga user/computer host mengisi data sebenarnya yang sebenarnya adalah website palsu yang dibuat oleh attacker dan didistribusikan ke computer host yang meminta akses page tertentu. Ataupun mengarahkan computer host untuk mengakses jaringan eksternal yang dimana server jahat telah menunggu untuk merekam data yang diinputkan oleh computer host / korban.



Gambar 5. User Client

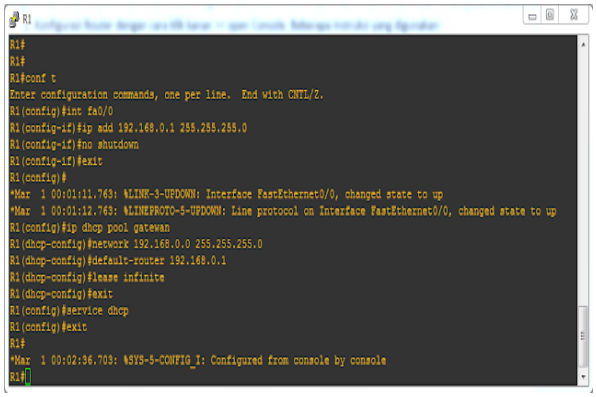
Apabila Attacker selesai mengatur multiple DHCP Rouge maka dapat didistibusikan alamat IP pada client berupa alamat IP palsu yang dibuat sendiri. Pada saat inilah client akan mengisi data pada alamat tersebut yang membuat server jahat mengunggu dan merekap data yang client input pada komputer.

Dalam konfigurasi Router OS pada Mikrotik. Pertama perlu adanya instalasi Mikrotik pada Virtual box, sampai muncul konfigurasi *Addres IP Print*`



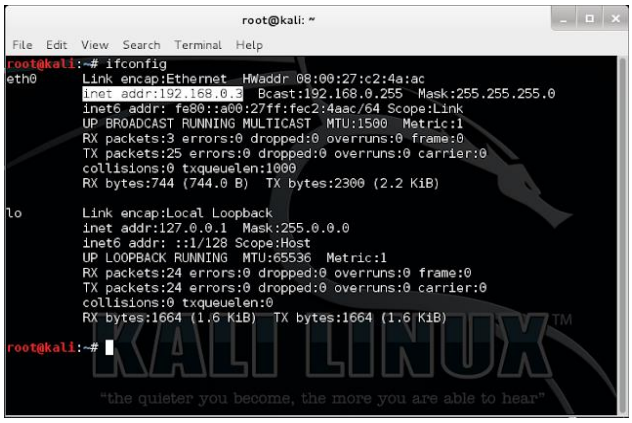
Gambar 6. IP Address Pada Mikrotik OS

Pada saat konfigurasi Addres IP muncil pada mirotik yang sudah terinstral, maka DHCP Lease juga terinstral pada mikrotik tersebut. Dalam hal ini DHCP Lease merupakan data yang sangat dibutuhkan attacker dalam melakukan penyerangan starvation attack. Sebelum melakukan penyerangan attacker memerlukan konfigurasi Router dimana running topologi sudah di buat di GNS3 yang kemudian konfigurasi router tersebut dilakukan dengan cara klik kanan >> open Console untuk mengaktifkan layanan DHCP pada router.



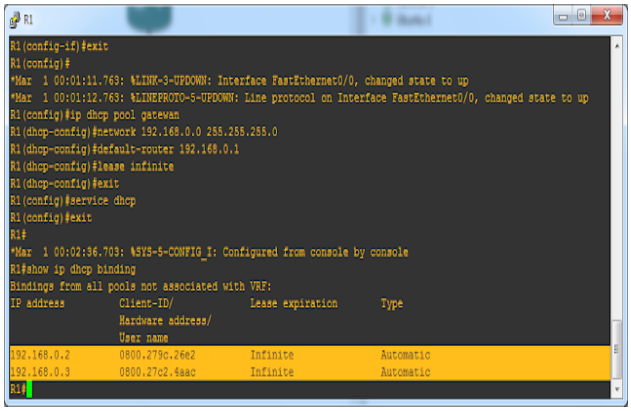
Gambar 7. Mengaktifkan Layananan DHCP

Dalam melakukan serangan dengan teknik Starvation *Attack* dapat menggunakan sistem operasi Ubuntu dan Kalilinux . Tools yang digunakan pada serangan ini yaitu yersenia. Pada Topology GNS3, klik bagian kanan PC Ubuntu> start, saat jendela ubuntu muncul,klik open terminal dan ketik iconfig.



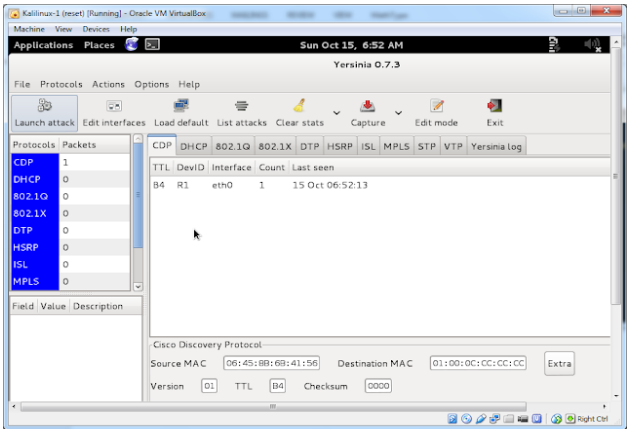
Gambar 8. Konfigurasi IP PC Pada KaliLinux

Sebelum melakukan serangan attacker akan terlebih dahulu mendampilkan daftar IP pool yang sudah ada dengan cara show IP DHCP binding via Console Router,Dalam data ini mennjukan 192.168.0.2 digunakan pada Ubuntu,sedangkan IP 192.168.0.3 digunakan pada kali linux



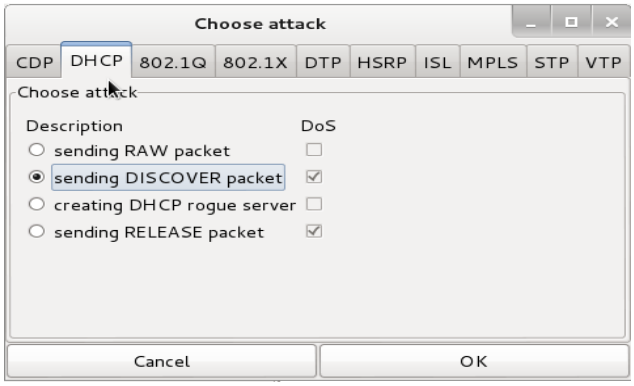
Gambar 9. Check Daftar IP Pada Router

Dalam hal ini kita menggunakan tool yersinia yang telah tersedia di kali linux,ketik application > kali linux > Explotiation Tools > Cisco attack > yersinia, makan akan muncul terminal baru dalam menggukan mode grafic, klik yersinia – G terlebih dahulu berikut gambar tampilannya

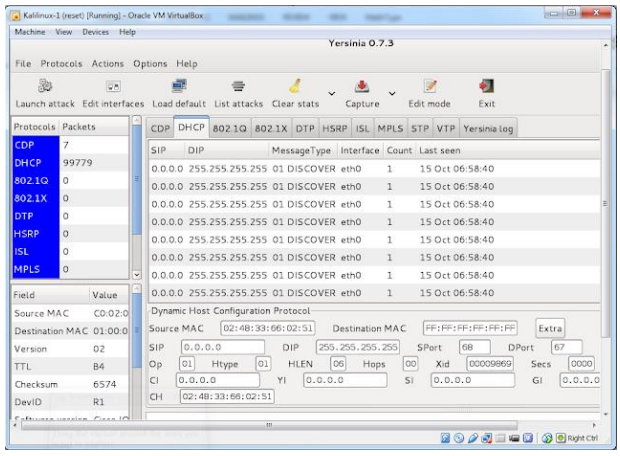


Gambar 9. Melakukan Serangan Attacking

Selanjutnya anda cari tahapan tabulasi DHCP lalu klik > Launch attack > pilih send Discover packet > Ok

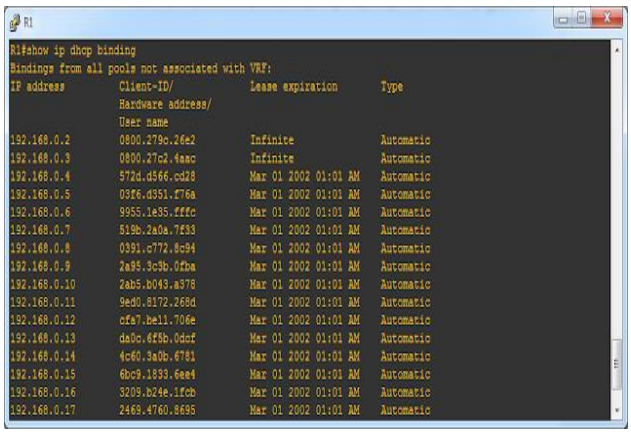


Gambar 10. Tabulasi DHCP



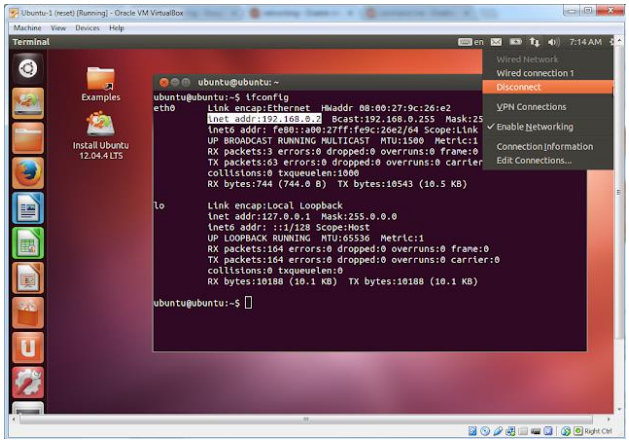
Gambar 11. Hasil Dari Sending Discover

Dampak yang ditimbulkan pada Router, menggambarkan semua IP sudah digunakan.

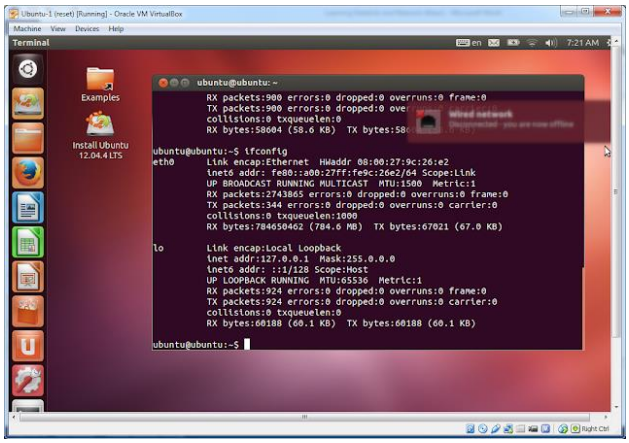


Gambar 12. IP Address Menggunakan DHCP Snooping

Dampak yang ditimbulkan pada PC ubuntu,dapat diartikan sekarang IP 192.168.0.2 yang kita gunakan bisa lepas dengan cara recconecting Disconnect > Connect Wired connection via try menu.



Gambar 13. Hasil Check akibat yang timbul pada PC



Gambar 14. PC Ubuntu

Dapat kita lihat PC Ubuntu tidak mendapatkan ip (*Reconnecting).* Dan pada saat melakukan handshake akan selalu gagal atau selalu RTO *(request time out).* Pada data router diatas menggambarkan semua Ip sudah digunakan sehingan DHCP Starvation Attack akan meminta request IP pada mikrotik OS sehingga ketika di cek pada ip dhcp-server lease pint, sehingga akan muncul ip address yang telah di berikan ke computer. Dalam hal ini, computer yang meminta adalah palsu, yaitu packet yang dikirim oleh attacker sebagai computer utama dengan memanfaatkan fitur Yesenia pada system operasi Ubuntu 14. Teknik selanjutnya yang digunakan attacker dalam melancarkan serangan DHCP *Rogue* dengan cara membuat computer attacker sebagai DHCP *Server* penganti DHCP Server asli pada mikrotik, sehingga attacker memberikan IP gateway dan DNS yang dibuatnya dan didistribuskan kepada para client computer yang terhubung pada satu switch hub yang sama dan meminta request IP Address pada DHCP Server palsu. Selanjutnya attacker sudah akan menggunakan teknik *man-in-the-middle*, dimana data-data yang sudah diinput dan melewati DHCP Server palsu akan direkam dan di analisis oleh attacker untuk mendapat informasi tertentu yang dapat salah gunakan nantinya.

5. KESIMPULAN DAN SARAN

Dari informasi sudah didapat diketahui, serangan DHCP *Starvation Attack* mendukung berbagai serangan yang digunakan oleh attacker seperti contohnya serang *Man In the Middle.* Dimana hal ini digunakan *attacker* untuk mendapatkan berbagai informasi pribadi client yang nantinya dapat disalah gunakan. Teknik serangan DHCP *starvation Attack* ini dapat dicegah dengan menggunakan teknik *filtering* yang *disetting* pada mikrotik OS, Kuncinya dapat dilihat pada komputer *hostname* yang terdaftar pada mikrotik, sehingga pada proses DHCP *Discover* yang meminta IP pada DHCP *Server* mikrotik jika tidak terdaftar *hostname* nya maka akan di list untuk di blokir.

UCAPAN TERIMA KASIH

Puji syukur kami haturkan kepada Allah SWT. Karena segala limpahan Rahmatnnya yang telah di berikannya kepada kita semua, Sehingga kami dapat menyelesaikan jurnal ini dengan mudah, dalam menyelesaikan penelitian ini dengan lancar. Terima kasih juga kepada Tim Jurnal Informatika Universitas Putra Batam.

DAFTAR PUSTAKA

[1] D. Kurnia. (2020). Analisis serangan DHCP starvation attack pada router OS Mikrotik". Jurnal Ilmiah Coret IT Vol. 8, No. 5

[2] T. Ariyadi. (2018). Mitigasi Keamanan Dynamic Host Control Protocol (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN). Jurnal Inovtek Polbeng, Vol. 3 No. 2

[3] Bundet. (2020). Pengertian DHCP Starvation Attack. Diperoleh 30 Desember 2022 pada https://bundet.com/d/923-pengertian-dhcp-starvation-attacks

[4] Maneka, A. D dan Kahewu, M. L. L. (2021). Analisis Keamanan Jaringan *Local Area Network* Perpustakaan Universitas Kristen Wira Wancana Sumba Menggunakan DHCP Server Berbasis Cisco Packet Tracer. Reputasi Jurnal Rekayasa Perangkat, Vol 2 No 1

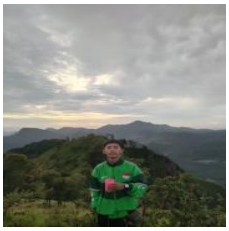
[5] Saputra, B. R dan Chandra, D. W. (2022). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN Mengggunakan CISCO. Jurnal Teknik Informatika dan Sistem Informasi. Vol 9 No 4

[6] Sarip dan A. Setyanto, "Filter Paket Berdasarkan Differentiated Services Code Point untuk Pencegahan Serangan DHCP Starvation," Jurnal Pekommas, Vol. 4, No. 2, pp. 137–146, 2019

[7] N. Abdulhafiz A., E. Faith O. dan O. Oyenike M., " Mitigating DHCP Starvation Attack Using Snooping Technique", FUDMA Journal of Sciences (FJS), Vol. 4 No. 1, pp. 560-566, 2020
[8] R. Adipranata dan I. Gunawan, "Penggunaan DHCP Relay Agent untuk Mengoptimalkan Penggunaan DHCP Serverp pada Jaringan dengan Banyak Subnet," Prosiding Seminar Nasional Aplikasi Teknologi Informasi (SNATI), pp. H99-H103, 2005
[9] Komputer, Wahana. 2003. Konsep Jaringan Komputer dan Pengembangannya, Penerbit Salemba Infotek, Jakarta
[10] Sukmaaji, Anjik dan Rianto. 2008. Jaringan Komputer, Penerbit Andi, Yogyakarta.
[11] T. Ariyadi & A.T. Maulana.(2021). Penerapan Web Proxy dan Manajemen Bandwidth Menggunakan Mikrotik Router Board pada kantor Pos Palembang 30000. Jurnal Ilmiah(JIF) F.Vol. 9. No. 02.

BIODATA PENULIS

Tamsir Ariyadi, M.Kom.
Dosen Prodi Teknik Komputer Univesitas Bina Darma Palembang



Aidil Nur Riyansyah
Mahasiswa Universitas Bina Darma Palembang.

M. Alzi Ikrar Agamuri
Mahasiswa Universitas Bina Darma Palembang.

M. Agung
Mahasiswa Universitas Bina Darma Palembang.