BAB II

LANDASAN TEORI

2.1 *Internet*

Internet merupakan kepanjangan dari *interconnected networking*, yang mempunyai arti hubungan komputer dengan berbagai tipe yang membentuk sistem jaringan yang mencakup seluruh dunia (jaringan komputer global) dengan melalui jalur telekomunikasi seperti telepon, radio link, satelit dan lainnya. Istilah *INTERNET* berasal dari bahasa Latin *inter*, yang berarti "antara". *Internet* adalah sebuah dunia maya jaringan computer (interkoneksi) yang 72 terbentuk dari miliaran komputer di dunia. *Internet* merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya di mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi. Dalam mengatur integrasi dan komunikasi jaringan komputer ini digunakan protokol yaitu *TCP/IP*. *TCP (Transmission Control Protocol)* bertugas memastikan bahwa semua hubungan bekerja dengan benar, sedangkan *IP (Internet Protocol)* yang mentransmisikan data dari satu komputer ke komputer lain. *TPC/IP* secara umum berfungsi memilih rute terbaik transmisi data, memilih rute alternatif jika suatu rute tidak dapat di gunakan, mengatur dan mengirimkan paket-paket pengiriman data. Untuk dapat ikut serta menggunakan fasilitas Internet, biasanya harus berlangganan ke salah satu *ISP (Internet Service Provider)*. *ISP* ini biasanya disebut penyelenggara jasa internet ataupun. Anda dapat menggunakan fasilitas dari Telkom yakni Telkomnet Instan. Dengan memanfaatkan internet, pemakaian komputer di seluruh dunia dimungkinkan untuk saling berkomunikasi dan

pemakaian bersama informasi dengan cara saling kirim *e-mail*, menghubungkan ke komputer lain, mengirim dan menerima *file*, membahas topik tertentu pada *newsgroup* dan lain-lain. Sejarah internet dimulai dari *ARPANet*, yaitu sebuah proyek Departemen Pertahanan Amerika Serikat. Pada tahun 1969 dilakukan sebuah riset yaitu bagaimana cara menghubungkan suatu komputer dengan komputer lainnya atau membentuk suatu jaringan. Di tahun 1970 mereka berhasil menghubungkan lebih dari 10 komputer yang membentuk jaringan. Kemudian tahun 1973 jaringan *ARPANet* mulai dikembangkan di luar Amerika Serikat. (Gani, 2019)

2.2 *Wireless*

Wireless adalah sebuah jaringan nirkabel untuk memberikan akses internet secara *wireless*, pada garis besarnya bisa dikatagorikan kedalam 3 kelompok. Pertama akses internet *broadband* tradisional (*Cable* atau *ADSL*) yang bisa di *share* dengan beberapa komputer di rumah atau di kantoran kecil. Kedua berbagi internet *wireless* akses jaringan *cellular*. Terakhir akses internet *wireless* untuk *hotspots* umumnya diberikan secara cuma-cuma yang biasa di berikan di Cafe, *Airport*, Kampus, dan di hotel. (Putra, 2021).

2.3 Jenis-Jenis Keamanan Jaringan *Wireless* (WIFI)

Isu keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dieksploitasi oleh para *hacker*, baik jaringan *LAN* maupun *Wireless*. Data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan

memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut.

Pembangunan perancangan sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini dibahas mengenai ancaman, kelemahan, dan *policy* keamanan jaringan.

Keamanan jaringan *WIFI* yang secara umum terbagi menjadi 2 (dua) yaitu:

1. *NonSecure/Open*: suatu komputer yang memiliki *WIFI* dapat menangkap tranmisi pancaran dari sebuah *WIFI* dan langsung dapat masuk kedalam jaringan tersebut.
2. *Share Key*: untuk dapat masuk ke jaringan *WIFI* diperlukan *username* serta *password* (Kunang et al., 2019)

2.4 *Network Security*

Network security/Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer. Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Ancaman fisik itu adalah yang merusak bagian fisik komputer atau *hardware* komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang (dewi, 2017).

Ancaman dan Serangan terhadap Keamanan jaringan:

1. Ancaman Fisik dapat berupa:
   a. Gangguan pada kabel
   b. Konsleting
   c. Data tak tersalur dengan baik
   d. Kerusakan harddisk
2. Ancaman Logik berupa:
   a. *Deface* (merubah tampilan)
   b. *Malicious Code* (ancaman menggunakan kode berbahaya)
   c. *Request flooding* (ancaman dengan membanjiri banyak *request* pada sistem)
   d. *Socialengineering* (ancaman pada sisi sosial memanfaatkan kepercayaan pengguna)

2.5 Mikrotik

Mikrotik merupakan perusahaan produsen perangkat jaringan komputer. Saat ini produk mikrotik sudah banyak digunakan oleh pelaku bisnis di bidang komputer, seperti warnet, ISP (*Internet Service Provider*), perusahaan kecil hingga besar, bisnis rumahan dan lain sebagainya. Adapun beberapa fitur yang dapat digunakan di Mikrotik (Santoso, 2020).

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router *network* yang handal, mencakup berbagai fitur yang dibuat untuk *IP Network* dan jaringan *wireless*, cocok digunakan oleh *ISP*, provider *hotspot* dan warnet. Mikrotik didesain untuk mudah digunakan untuk keperluan administrasi jaringan komputer, seperti merancang dan membangun sebuah sistem jaringan komputer sekala kecil hingga yang kompleks. Salah satu fungsi dari mikrotik yaitu bisa mengontrol akses internet setiap pengguna dengan menggunakan *bandwidth* manajemen (Sabara & Prayogi, 2020).

2.6 *Firewall*

Firewall yaitu kombinasi antara perangkat lunak (*software*) dan perangkat keras (*hardware*) yang menjadi garis pertahanan pertama keamanan jaringan antara jaringan internet yang aman dengan jaringan internet yang tidak aman. *Firewall* memantau lalu lintas berdasarkan seperangkat aturan keamanan yang ditentukan, ia menerima, menolak, atau menjatuhkan (*drop*) lalu lintas tertentu. *Firewall* mengalisis data yang masuk dan keluar sesuai dengan kebijakan *default* (Utami,

2021). Adapun fungsi *firewall*, yaitu:

1. Mengatur lalu lintas jaringan
2. Mencatat lalu lintas jaringan
3. Mengatur autentifikasi akses data
4. Memblokir lalu lintas yang tidak aman
5. Memblokir program jahat yang bisa menginfeksi komputer

6. Menghindari peretasan dan pembobolan data
7. Melindungi informasi pribadi dari pengguna tidak sah
8. Menjaga kemanan jaringan internet

2.7 *Filltering MAC Address*

Jaringan komputer, *MAC Filtering* (atau GUI penyaringan, atau lapisan 2 alamat penyaringan) mengacu pada metode kontrol akses keamanan dimana alamat 48-bit ditugaskan untuk setiap kartu jaringan yang digunakan untuk menentukan akses ke jaringan. Alamat *MAC* yang unik ditugaskan untuk setiap kartu, sehingga dengan *MAC filtering* pada izin jaringan dan menolak akses jaringan ke perangkat tertentu melalui penggunaan *blacklist* dan *Whitelist*. Pembatasan akses jaringan melalui penggunaan daftar sangat mudah, seorang individu tidak diidentifikasi oleh alamat *MAC*, bukan perangkat saja, jadi orang yang berwenang perlu memiliki *entri* daftar putih untuk setiap perangkat yang menggunakan dan mengakses jaringan.

Sementara memberikan jaringan nirkabel beberapa perlindungan tambahan, *MAC filtering* dapat dielakkan dengan memindai *MAC* yang *valid* (melalui airodump-ng) dan kemudian *spoofing MAC* sendiri menjadi salah satu divalidasi. Dilakukan dalam Windows Registry atau dengan menggunakan alat baris perintah pada platform Linux. *MAC Address filtering* sering disebut sebagai Keamanan melalui ketidakjelasan.

MAC filtering bukan merupakan kontrol yang efektif di jaringan nirkabel sebagai penyerang dapat menguping transmisi nirkabel. Namun *MAC filtering*

lebih efektif dalam jaringan kabel, karena lebih sulit bagi penyerang untuk mengidentifikasi *MAC* yang berwenang. *MAC filtering* juga digunakan pada jaringan nirkabel perusahaan dengan beberapa jalur akses untuk mencegah klien dari berkomunikasi satu sama lain. Jalur akses dapat dikonfigurasi untuk hanya memungkinkan klien untuk berbicara dengan *default gateway*, tapi tidak klien nirkabel lainnya. Hal ini meningkatkan efisiensi akses ke jaringan (Kusuma, 2016).

2.8 *MAC Address Cloning*

MAC (*Mac Access Control*) *address* adalah alamat sebuah *hardware* atau alamat fisik yang secara unik mengidentifikasi setiap komputer atau alat yang terhubung dalam jaringan, *MAC address* juga sering disebut *physical/hardware address*. Berikut adalah beberapa fungsi dari *MAC address*:

1. Memberikan kontrol terhadap alat yang bisa terkoneksi dengan router.
2. Membatasi akses berdasarkan *MAC access lists (*ACLs) yang tersimpan dan didistribusikan dalam hampir setiap jenis router.
3. Memiliki kmampuan penyaringan akses ke dalam sebuah komputer menggunakan daftar perijinan (*permissions list*) yang dibuatkan berdasarkan *MAC address*.

MAC cloning merupakan suatu tindakan pembobolan, duplikasi (*cloning*) pada alamat sebuah *hardware* atau alamat fisik pada komputer agar memiliki *MAC address* yang sama tujuannya agar dapat dengan mudah masuk ke dalam

jaringan tanpa melakukan perijinan dari administrator terlebih dahulu (Dwi Ratnasari & Safiroh Utsalina, 2017).

2.9 *ARP*

ARP memiliki kepanjangan *Address Resolution Protocol* yang merupakan sebuah protokol jaringan yang digunakan untuk mengetahui alamat *hardware*. Protokol ini digunakan untuk mengetahui *MAC Address* dari suatu perangkat. *ARP* digunakan jika ingin melakukan komunikasi dengan beberapa perangkat lainnya pada jaringan lokal. Misalnya, jaringan ethernet yang memang memerlukan alamat sebelum melakukan komunikasi atau melakukan pengiriman paket jaringan. Sebuah perangkat yang bertugas sebagai pengirim yang menggunakan *ARP* akan menerjemahkan *IP address* ke *MAC address*.

Peran ARP (*Address Resolution Protocol*) yaitu:

1. *ARP* mempunyai peran yang sangat penting di dalam jaringan. Terutama jika berkaitan dengan komunikasi data yang ada di dalam jaringan tersebut. Setiap *host* yang terhubung ke dalam jaringan *LAN* bisa saling berkomunikasi dengan menggunakan alamat fisik atau *MAC address* dan tidak menggunakan alamat logis atau *IP address*.
2. Seperti yang sudah dijelaskan di *point* pertama bahwa setiap *host* dapat berkomunikasi menggunakan *MAC address*. Setiap *host* yang ingin

berkomunikasi dengan *host* lainnya harus memiliki alamat fisik atau *MAC address* dari *host* tujuannya tersebut.

3. Transfer data, data tersebut sebelumnya harus diberi *IP address*. *IP address* yang ditambahkan tersebut merupakan alamat *IP* yang dimiliki oleh *host* pengirim dan penerima.
4. Menentukan *MAC address* dari *host* tujuan. Di sinilah peran penting *ARP*. Memanfaatkan alamat *IP host* tujuan, *host* pengirim dapat melakukan pencarian dengan menggunakan protokol *ARP* (Efendi, 2020).

2.10 Penelitian Terkait

Tabel 2.1 Penelitian terkait mengumpulkan jurnal penelitian mengenai *filtering MAC address*, *MAC address cloning* dan perancangan jaringan *wiereless* sebagai rujukan pembuatan penelitian ini.

Tabel 2.1 Penelitian Terkait

No	Penelitian	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian	Kelebihan dan Kekurangan
1	Susianto, Yulianti, 2015	*Filtering MAC address*	Mengamankan *Wireless* Dengan Menggunakan *Two Factor*, *Password* Dan *Mac Address Filtering*	Mengamankan akses internet dengan dua lapis keamanan	Kelebihan penelitian ini menggunakan dua factor keamanan, kekurangannya masih bisa di retas dengan *MAC address cloning*

2	Aziz Setyawan Hidayat, Ulin Nuha , Yamin Nuryamin , Suleman, 2021	*Filtering MAC address*	*Quality Of Service Filtering* Dengan Metode *Filtering MAC Address* Jaringan *Wireless*	Membatasi hak akses berdasarkan *MAC Address* perangkat	Kelebihan penelitian ini membatasi hak akses *MAC address*, kekurangannya *firewall rule MAC Address* terdapat celah untuk di duplikat

No	**Penelitian**	**Metode dan *Tools***	**Judul Penelitian**	**Hasil Penelitian**	**Kelebihan dan Kekurangan**
3	Desi Maya Sari, Muh. Yamin, LM. Bahtiar Aksara, 2017	*Penetration testing* dan aircrack	Analisis Sistem Keamanan Jaringan *Wireless* (WEP, WPAPSK/WPA2PSK) *MAC Address*, Menggunakan Metode *Penetration Testing*	Hasil penelitian dari dua jenis serangan yang dilakukan, yaitu pada jenis serangan *cracking the encryption tipe* keamanan WEP berstatus berhasil dengan 3 pengujian dengan 3 kombinasi	Kelebihan penelitian ini menggunakan dua kemanan, kekurangan penelitian ini masih bisa di retas dengan *cracking WLAN*
4	Dwi Ratnasari, Safiroh Utsalina, 2017	*MAC Clone* dan mikrotik	Implementasi Penanganan Serangan *Mac-Clone* Pada *Hotspot* Mikrotik Di STMIK Pradnya Paramita Malang PARAMITA MALANG	Dengan terbangunnya keamanan internet menggunakan *firewall* yaitu melakukan setting pada *filter rules* dan *NAT* membantu pengguna untuk meminimalisir terjadinya *MAC Cloning*	Kelebihan penelitian ini menggunakan *Access Control List*, kekurangan penelitian ini penanganan *MAC address cloning* tidak disertai dengan pendeteksian *MAC address cloning*

5	Lukyto Rachmat Widodo, Henni Endah Wahanani, Agung Mustika Rizki	*Filtering MAC address*	Pengamanan Jaringan *WLAN* Dari Serangan *Sniffing* Menggunakan *Arpwatch* Dan *MAC Address Filtering*	*MAC address filtering* menjadi salah satu solusi untuk mencegah *user* yang mencurigakan agar tidak dapat terhubung ke dalam jaringan *WLAN*	Kelebihan penelitian ini dapat mendeteksi serangan *sniffing* yang terjadi dalam jaringan *WLAN*, kekurangannya serangan *sniffing* dapat melewati *MAC address filtering*

No	**Penelitian**	**Metode dan *Tools***	**Judul Penelitian**	**Hasil Penelitian**	**Kelebihan dan Kekurangan**
6	Michael, Ikhwan Ruslianto, 2021	*Filtering MAC address* dan Xterm	Analisis Perbandingan Sistem Keamanan Jaringan Wi-fi *Protected Access 2-PreShared Key* (WPA2-PSK) Dan *Captive Portal* Pada Jaringan Publik *Wireless*	Pengujian sistem keamanan *captive portal* dengan tipe serangan *packet capture*, *deauthentication*, *MAC Address Clone*, dan *ARP attack* pada 10 sampel pengujian terdapat 4 sampel memiliki tingkat keamanan *low* dan 6 sampel memiliki tingkat keamanan medium	Mengetahui Perbandingan sistem keamanan *WPA2-PSK* dan *captive portal* dapat dilihat dari status keberhasilan serangan, kekurangan penelitian ini Sistem keamanan *captive portal* yang rentan terhadap serangan *MAC address clone*
7	Imam Kreshna Bayu, Muh. Yamin, LM Fid Aksara, 2017	*Filtering MAC address dan ettercap*	Analisa Keamanan Jaringan *Wlan* Dengan Metode *Penetration Testing*	Pengujian *Attacking The Infrastructure* dan *Man In The Middle*, jaringan *WLAN* belum bisa memberi keamanan kepada user yang terkoneksi.	Kelebihan penelitian ini menghalau *Cracking The Encryption*, kekurangannya *user* masih bisa melakukan penyadapan

8	Husna & Rosyani, 2021	Zabbix, Grafana, Telegram	Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram	Integrasi Zabbix dan telegram berhasil mendeteksi serangan *MAC address cloning*	Kelebihan tools zabbix mampu membantu *network administrator* dalam memantau gangguan pada jaringan, kelemahannya pemantauan dilakukan secara manual

No	Penelitian	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian	Kelebihan dan Kekurangan
9	Hariadi, Wire Bagye, Mohammad Taufan Asri Zaen, 2019	Winbox	Membangun Server *Hotspot* Berbasis Mikrotik Di Sman 1 Praya Tengah	Memanfaatkan *firewall* pada mikrotik untuk mengatur hak akses internet	Perancangan *hotspot* mikrotik dengan *filtering MAC address*, kekurangannya hanya menggunakan satu jenis keamanan
10	Firmansyah a, Rachmat Adi Purnama, Rachmawati Darma Astuti, 2021	*Filtering MAC address* dan winbox	Optimalisasi Keamanan *Wireless* Menggunakan *Filtering MAC Address*	Dengan pengimplementasian keamanan jaringan wireless menggunakan filtering MAC address mampu melakukan block terhadap user yang melakukan percobaan akses kedalam jaringan	Menggunakan dua jenis keamanan ,kekurangannya serangan *MAC address cloning* tidak dapat di deteksi
11	Kholiq, Khoirunnisa, 2019	*Mac clone dan t-mac*	Analisis Keamanan *Wireless Local Area Network (WLAN)* Dengan Metode *Penetration Testing Execution Standard (PTES)* (Studi Kasus : PT. Win Prima Logistik)	Menemukan celah keamanan yang bisa diserang menggunakan teknik *MAC address cloning*	Kelebihan penelitian ini menerapkan sistem keamanan setingkat *WPA/WPA2-PSK*, kekurangannya masih bisa diserang menggunakan teknik serangan *bypassing MAC Address* dan *ARP Spoofing*

No	Penelitian	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian	Kelebihan dan Kekurangan
12	Syaiful, Novia, 2018	*Filtering MAC address*	Perancangan Jaringan Internet Dengan *Hotspot* Mikrotik Dan *Mac Address Filtering*	Mencegah *wireless client* terkoneksi ke *access point* dengan *mac-address* tertentu	Kelebihan penelitian ini, menggunakan *Access List* untuk mencegah *MAC address* acak, kekurangannya masih bisa di retas dengan *MAC address cloning*
13	Sihotang, Sumarno, Effendi Damanik., 2020	*Filtering MAC address, Access Control List*, dan winbox	Implementasi *Access Control List* Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara	*MAC Address* yang terdaftar saja yang dapat mengakses *hotspot* sehingga jaringan *hotspot* lebih *private*.	Sistem *ACL* pada mikrotik hotspot dapat lebih mempermudah melakukan monitoring, kekurangannya dapat diretas dengan *MAC address cloning*
14	Ismail Maafin, 2020	*Filtering MAC address*, winbox	Analisis Dan Pembuatan Keamanan Jaringan *Wireless Fidelity* Berbasis Mikrotik Di Sekolah Menengah Pertama Negeri 4 Palopo	Dengan *filtering MAC address* menutup celah bagi peretas yang ingin mengakses jaringan *wifi*	Menggunakan *fitering MAC address* dan *password* voucher, kekurangannya tidak dapat memonitoring aktifitas *user*
15	Bima Pramudya, 2021	*Filtering MAC address, winbox*	Implementasi *MAC Address Register* Untuk Mengatasi Pengguna Anonim Dalam Jaringan	Kemanan jaringan berbasis *MAC Address Register* untuk mencegah Pengguna Anonim	*MAC Address Register* mencegah Pengguna Anonim, kekurangannya tidak dapat menemukan identitas peretas

No	Penelitian	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian	Kelebihan dan kekurangan
16	Wibowo, Triyono, Sutanta, 2017	*Bypassing MAC*	Keamanan Jaringan *Wlan* Terhadap Serangan Wireless *Hacking* Pada Dinas Komunikasi & Informatika DIY	Keamanan *filtering mac address* dapat mencegah *bypassing mac address*	Menerapkan sistem keamanan setingkat *WPA/WPA2-PSK*, kekurangannya h pengguna yang sedang menggunakan jaringan *WLAN* masih bisa diserang oleh pengguna lain pada jaringan *wireless* yang sama

Tabel 2.2 Penelitian yang dibuat

No	Penelitian	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian	Kelebihan dan Kekurangan
1	Anggi pranata	*Filtering MAC address, MAC address cloning*	Integrasi *Firewall* Dan *ARP List* Untuk Mengamankan *MAC Address Cloning* Pada *Wireless LAN*	Menemukan celah keamanan filtering *MAC address* Melakukan pengujian serangan *MAC address cloning* dengan sistem operasi android, mengantisipasi serangan *MAC address cloning*	Mengintegrasikan *ARP list* dan *Firewall* untuk menangani serangan *MAC address cloning*, kekurangannya proses monitoring dilakukan secara manual

Tabe 2.2 Hasil penelitian terkait dengan penelitian yang akan dibuat, memiliki kesamaan dalam pengujian sistem keamanan *filtering MAC address* yang membedakan ada pada penggunaan *ARP list* dan *firewall* sebagai penaganan *MAC address cloning* dan peretasan *MAC address cloning* menggunakan sistem operasi android karena pada penelitian sebelumnya masih terdapat celah.

2.3 Tabel Matriks Penelitian

No	Peneliti	Ruang lingkup										
		Metode Keamanan			System Operasi			Tools				
		Filtering MAC	WPA/WPA2	WPA2-PSK	Windows	Liinux	Android	Winbox	Aircrack-ng	Xterm	Change My MAC	Busy Box
1	Didi Susianto, Iis Yulianti 2017	✓		✓								
2	Aziz Setyawan Hidayat, Ulin Nuha, Yamin Nuryamin, Suleman 2021	✓		✓				✓				
3	Desi Maya Sari, Muh. Yamin, LM. Bahtiar Aksara 2017		✓		✓					✓		
4	Santi Dwi Ratnasari, Dwi Safiroh Utsalina 2017	✓			✓				✓			
5	Lukyto Rachmat Widodo, Henni Endah Wahanani, Agung Mustika Rizki 2021	✓			✓	✓						
6	Michael, Ikhwan Ruslianto, Rahmi Hidayati 2021		✓			✓						
7	Imam Kreshna Bayu, Muh. Yamin, LM Fid Aksara 2017	✓	✓	✓		✓						
8	Muhamad Hariadi, Wire Bagye, Mohammad Taufan Asri Zaen 2019	✓			✓				✓			
9	Firmansyah a, Rachmat Adi Purnama, Rachmawati Darma Astuti 2021	✓		✓				✓				
10	Abdul Kholiq, Diyah Khoirunnisa 2019	✓		✓	✓							
11	Syaiful, Cahyuni Novia 2018	✓		✓				✓				
12	Bil Klinton Sihotang, Sumarno, Bahrudi Effendi Damanik 2020	✓		✓				✓				
13	Ismail Maafin 2020	✓		✓				✓				
14	Pahala Bima Pramudya, Djuniadi 2021		✓	✓	✓				✓			
15	Mochamad Gilang Hari Wibowo, Joko Triyono, Edhy Sutanta 2017		✓	✓		✓			✓			
16	Husna & Rosyani 2021		✓		✓				✓			
17	Anggi Pranata 2021	✓	✓	✓	✓	✓	✓				✓	✓

Penelitian yang akan dilakukan, yaitu Integrasi *Firewall* Dan *ARP List* Untuk Mengamankan *Mac Address Cloning* Pada *Wireless LAN*. Penelitian ini menggunakan Metode Keamanan *Filltering MAC Address*, WPA/WPA2, WPA2/PSK, Sistem Operasi yang digunakan windows, android dan *tools* yang digunakan yaitu winbox, Change My MAC dan Busy Box.