BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi semakin memudahkan penggunanya dalam menerima dan memberikan informasi. Keamanan jaringan merupakan hal yang sangat penting saat ini dan patut mendapatkan perhatian, jaringan yang terhubung ke internet pada dasarnya tidak aman dan dapat dieksploitasi oleh peretas kapan saja, baik itu jaringan *Local Area Network* (LAN) atau jaringan *wireless*. Saat ini data yang dikirim melewati beberapa perangkat sebelum mencapai tujuannya, sehingga memberikan peluang bagi pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan yang dirancang dan dipahami dengan baik agar dapat secara efektif melindungi sumber daya dalam jaringan dan meminimalkan serangan dari peretas (Siregar, 2019).

Sugiyono (2016) menegaskan bahwa keamanan jaringan komputer harus menjadi pertimbangan utama dalam mengembangkan arsitektur jaringan. Mayoritas topologi jaringan menggunakan dukungan perangkat lunak jaringan yang memudahkan kontrol akses, pemantauan paket data, dan penggunaan protokol yang diatur secara ketat, serta *router* dengan sistem keamanan internal.

Mengingat peretas akan selalu berusaha menyusupi jaringan yang sudah ada maka keamanan jaringan harus diterapkan. Kejahatan dunia maya adalah istilah untuk kejahatan teknologi yang mencakup tindakan seperti penghapusan informasi, peretasan jaringan, pencurian data dari pengguna jaringan, dan penyembunyian informasi dalam jaringan komputer. ARP *spoofing* adalah salah satu dari banyak kejahatan yang mungkin dilakukan di dalam jaringan, jika ini terjadi hal ini dapat menyebabkan serangan yang lebih berbahaya berikutnya, sehingga serangan ARP *spoofing* merupakan kunci utama dalam terjadinya serangan yang sangat berbahaya yang mengakibatkan perangkat yang digunakan untuk komunikasi dapat mengalami kerugian akibat kejahatan ini dan konektivitas jaringan terganggu dan bahkan bisa terputus. Penyerang dapat mengakses informasi pribadi, termasuk nama pengguna, kata sandi, alamat *email*, informasi

perbankan dan data sensitif lainnya, sehingga sangat berbahaya bagi pengguna jaringan (Hafizh, dkk., 2020).

Address Resolution Protocol (ARP) *spoofing* adalah teknik serangan pada jaringan komputer lokal dengan menggunakan media kabel atau *wireless* yang memungkinkan penyerang memodifikasi data dijaringan lokal dan mengubah atau menghentikan lalu lintas data. ARP *spoofing* yang digunakan untuk mengubah alamat IP menjadi MAC *address*. Protokol ARP menemukan alamat MAC dari *host* target dengan mengirimkan permintaan ARP, tingkat kerentanan memungkinkan penyerang memalsukan alamat MAC dari *host* target dengan menemukan informasi bukti serangan *spoofing Address Resolution Protocol* (ARP) berupa alamat MAC penyerang (Ginting, dkk., 2019).

Sekolah Menengah Kejuruan Negeri (SMKN) 1 Palopo merupakan salah satu sekolah yang berada di Kabupaten Luwu yang memiliki jaringan *internet*, dimana jaringan *internet* tersebut rentan terhadap serangan *address resolution protocol spoofing* karena jaringan sekolah yang belum menerapkan sebuah sistem keamanan yang kuat pada jaringan. Maka dari itu jaringan di SMK Negeri 1 Palopo mengalami beberapa masalah, seperti ganguan pada koneksi jaringan, dan terputus koneksi jaringan pada SMK Negeri 1 Palopo. Sejauh ini belum terdapat sistem keamanan yang dapat melakukan analisis dan mengimplementasi sebuah kemanan jaringan pada sekolah, sehingga bisa berdampak fatal pada koneksi jaringan di sekolah.

Berdasarkan pemaparan di atas penulis tertarik untuk melakukan penelitian dengan judul "Implementasi Keamanan Jaringan Terhadap Serangan *Address Resolution Protocol* (ARP) *Spoofing* pada Sekolah Menengah Kejuruan Negeri (SMKN) 1 Palopo". Hal tersebut dilakukan agar semua *host* yang terhubung pada jaringan bisa merasa aman dalam menggunakan jaringan di SMK Negeri 1 Palopo, sehingga penulis mengimplementasikan keamanan jaringan komputer untuk meningkatkan keamanan jaringan pada SMK Negeri 1 Palopo.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebut di atas maka rumusan masalah dalam penelitian ini yaitu "Bagaimana hasil implementasi keamanan jaringan terhadap serangan *address resolution protocol spoofing* pada SMKN 1 Palopo?".

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan di atas maka tujuan penelitian ini adalah "Bagaimana mengetahui hasil implementasi keamanan jaringan terhadap serangan *address resolution protocol spoofing* pada SMKN 1 Palopo?".

1.4 Manfaatan Penelitian

Dari hasil penelitian diharapkan dapat memberikan manfaat masing-masing kepada:

1. Manfaat bagi Dunia Akademik

   Diharapkan dari hasil penelitian ini akan memberikan suatu referensi yang berguna dalam perkembangan dunia akademik khususnya dalam penelitian-penelitain yang akan datang. Dapat pula memberikan sumbangan pemikiran bagi perkembangan teknologi informasi dalam dunia ilmu pengetahuan.

2. Manfaaat bagi Mahasiswa

   Merupakan studi kasus yang baru dalam implementasi keamanan jaringan selama duduk dibangku kuliah dan sebagai pembekalan dalam menghadapi teknologi informasi dalam dunia teknologi informasi.

3. Manfaat bagi SMKN 1 Palopo

   Agar dapat mengetahui tingkat keamanan jaringan sekolah dengan implementasian ARP statis dan aplikasi *XArp* dalam mengamankan jaringan dan mengidentifikasi serangan ARP *spoofing* pada jaringan SMK Negeri 1 Palopo.

1.5 Batasan Penelitian

Batasan masalah pada penelitian ini adalah:

1. Penelitian ini berfokus terhadap implementasi keamanan jaringan terhadap serangan ARP *spoofing* di SMK Negeri 1 Palopo.
2. Pengujian keamanan jaringan terhadap serangan *Address Resolution Protocol* (ARP) *Spoofing* yang diuji menggunakan OS *kali linux* dengan *tools ettercap* sebagai pengujian serangan.
3. Penelitian ini hanya berfokus terhadap implementasi ARP statis dan aplikasi *XArp* pada SMK Negeri 1 Palopo.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Kajian teori yaitu penjelasan materi-materi yang dikaji dan digunakan untuk menganalisis rancangan yang akan dibangun atau kajian materi-materi yang diambil dari buku, *internet* dan media cetak lainnya.

1. Implementasi

Kamus Besar Bahasa Indonesia (2021) mengartikan implementasi sebagai kegiatan atau pelaksanaan suatu rencana yang dipikirkan dengan matang. Setelah rencana dinilai ideal, biasanya rencana tersebut dilaksanakan, yang mengarah pada berbagai aktivitas, tindakan, atau mekanisme sistem (Simorangkir & Harjani, 2021).

Implementasi adalah tindakan yang diorganisir dan dilaksanakan dengan tujuan mencapai tujuan kegiatan. Implementasi adalah suatu proses dinamis dimana suatu rencana dilaksanakan melalui serangkaian kegiatan atau tugas dengan tujuan akhir untuk menghasilkan suatu hasil yang sesuai dengan tujuan rencana atau sasaran tertentu (Andhini & Fitri) dalam (Bellmondo, 2021).

Menurut definisi yang diberikan di atas, implementasi adalah proses membawa suatu kebijakan ke perhatian publik dan memastikan bahwa kebijakan tersebut menghasilkan hasil yang diinginkan. Hal ini termasuk mengembangkan serangkaian peraturan tambahan yang mewakili interpretasi kebijakan.

2. Keamanan Jaringan

Keamanan jaringan merupakan sebuah proses pencegahan dan identifikasi dari aktifitas penggunaan yang tidak sesuai jaringan komputer tersebut. Keamanan jaringan juga bertujuan mengantisipasi ancaman dalam bentuk logika maupun fisik yang menggangu secara langsung dan tidak langsung (Ma'sum, 2017).

Strategi atau sistem yang disebut keamanan jaringan digunakan untuk melindungi jaringan dari berbagai bahaya eksternal yang dapat merusak atau mencuri datanya. Salah satu komponen kunci dari sistem informasi, seperti jaringan komputer adalah masalah keamanan, ketika sebuah komputer terhubung

ke komputer lain melalui *Local Area Network* (LAN), terdapat peningkatan risiko kelemahan keamanan yang dapat mengganggu fungsionalitas sistem.

3. *Address Resolution Protocol Spoofing*

*Address Resolution Protocol (*ARP) *spoofing* adalah mengubah alamat IP menjadi alamat MAC. ARP *spoofing* adalah kejahatan dunia maya atau serangan yang melibatkan peniruan alamat MAC di jaringan, ketika dua komputer pribadi (PC) dihubungkan ke jaringan yang sama ARP *spoofing* dapat terjadi. Setiap PC memiliki alamat MAC dan alamat IP yang unik, ketika PC1 dan PC2 mentransfer paket data satu sama lain penyerang mengubah alamat MAC sehingga ada dua alamat IP tetapi hanya satu alamat MAC dan paket data selanjutnya melewati *host* penyerang (Hafizh, dkk., 2020).

Dari pembahasan di atas dapat diartikan bahwa ARP *spoofing* merupakan serangan yang dapat terjadi pada jaringan komputer karena cela keamanan pada protokol ARP yang memungkinkan penyerang untuk memalsukan alamat MAC dan IP untuk mengirimkan data yang seharusnya ditujukan ke alamat lain.

4. Arsitektur Jaringan Komputer

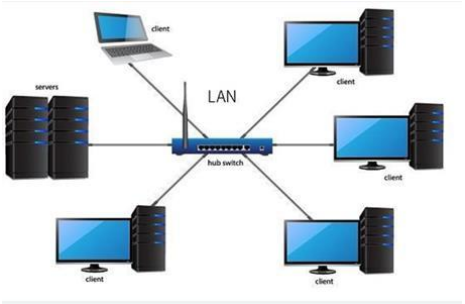
Untuk memudahkan dalam memahami jaringan komputer para ahli kemudian membagi jaringan komputer berdasarkan beberapa klasifikasi (Telaumbanu, 2022).

a. *Local Area Network* (LAN)

Local Area Network (LAN) terdiri dari beberapa komputer atau perangkat lain yang mudah diakses yang semuanya terhubung satu sama lain dan terletak di area yang sama, karena terbatas pada satu lokasi. Jaringan komputer LAN biasanya ditemukan di rumah pribadi, sekolah, dan laboratorium. *Local Area Network* (LAN) sering kali terdiri dari beberapa komputer yang dihubungkan melalui kabel.

LAN merupakan topologi jaringan yang dibatasi oleh area yang relatif kecil. Jenis jaringan ini biasanya menghubungkan satu komputer ke komputer lainnya atau bisa juga satu node ke node lainnya. Jangkauan LAN tidak terlalu jauh, misalnya di dalam ruangan atau suatu area dengan radius antara 100 m hingga 2.000 m, tergantung jenis kabel yang digunakan. Jenis aplikasi jaringan ini biasanya dibangun untuk perkantoran skala kecil atau usaha kecil menengah. Jika

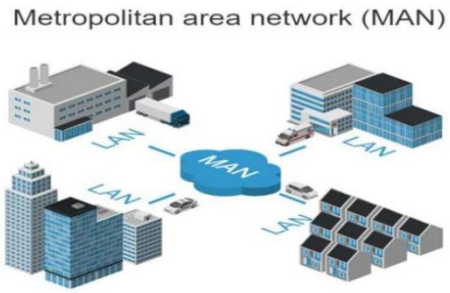
diterapkan pada perusahaan besar, penggunaannya hanya akan ditempatkan dalam ruang lingkup yang kecil, seperti per kamar atau per kantor.



Gambar 1. *Local Area Network* (LAN)
Sumber: Telaumbanu (2022)

b. *Metropolitan Area Network* (MAN)

Metropolitan Area Network (MAN) adalah hal yang memungkinkan komunikasi di seluruh wilayah metropolitan. Jaringan MAN memiliki jangkauan 50 kilometer sebagai tujuannya, banyak jaringan LAN yang terhubung satu sama lain membentuk jaringan MAN. Jaringan MAN juga ideal untuk digunakan di kampus dengan beberapa lokasi serta untuk bisnis dengan banyak kantor cabang. WMAN adalah nama lain dari jaringan MAN, yang juga dapat dibangun melalui media terarah atau nirkabel.

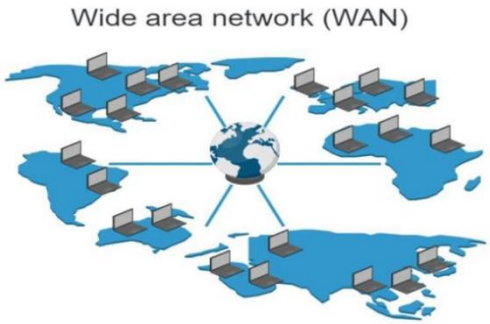


Gambar 2. *Metropolitan Area Network* (MAN)
Sumber: Telaumbanu (2022)

c. *Wide Area Network* (WAN)

Dibandingkan dengan jaringan komputer LAN dan MAN, WAN merupakan bentuk jaringan komputer yang lebih besar dan maju, karena jaringan komputer WAN menawarkan area cakupan yang luas, maka jaringan tersebut dapat terdiri dari berbagai jenis jaringan komputer LAN dan WAN. Biasanya, teknologi jaringan WAN digunakan untuk menghubungkan jaringan ke negara lain atau dari satu benua ke benua lain. Kelebihan jaringan komputer tipe WAN adalah

jaringannya lebih luas dibandingkan dengan jaringan komputer tipe LAN dan MAN. Jaringan WAN biasanya menggunakan kabel serat optik dan menempuh rute bawah tanah atau bawah air.



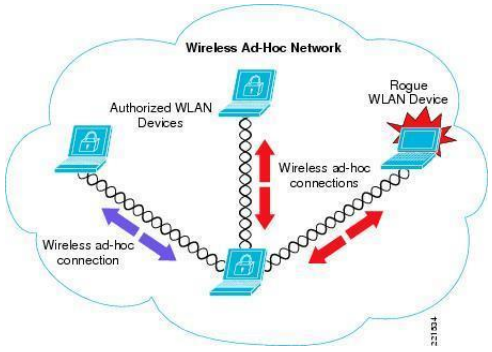
Gambar 3. *Wide Area Network* (WAN)
Sumber: Telaumbanu (2022)

d. *Wireless Local Area Network* (WLAN)

Wireless Local Area Network (WLAN) adalah sistem komunikasi fleksibel yang menggunakan teknologi frekuensi radio untuk mengirim dan menerima data melalui media nirkabel. WLAN dapat dibagi menjadi dua kategori utama:

1) *Wirelles* LAN Mode *Ad Hoc*

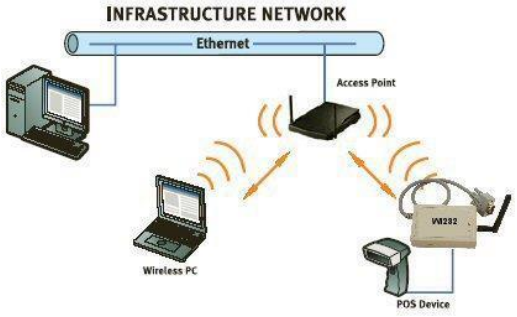
Pada arsitektur jaringan *Ad Hoc*, tidak diperlukan konfigurasi khusus karena jaringan antar perangkat dilakukan secara langsung. selama perangkat penerima, atau penerima, mampu menerima sinyal dari pemancar, atau pemancar dengan baik. Komunikasi *Ad Hoc* pada jaringan yang dirutekan antar komputer tanpa melalui sembilan titik akses dalam infrastruktur nirkabel jaringan akan dilakukan langsung oleh komputer yang berjalan melalui titik akses tersebut. Jaringan *Ad Hoc* juga disebut sebagai jaringan *peer-to-peer* atau jaringan komputer ke komputer.



Gambar 4. *Wirelles* LAN Mode *Ad-Hoc*
Sumber: Telaumbanu (2022)

2) *Wirelles* LAN Mode Infrastruktur

Arsitektur ini menawarkan komunikasi antar perangkat yang terhubung ke jaringan *wifi* dalam model jaringan mode infrastruktur. Untuk terhubung ke jaringan komputer kabel diperlukan perangkat perantara berupa *access point* sebelum mengirim ke suatu perangkat.



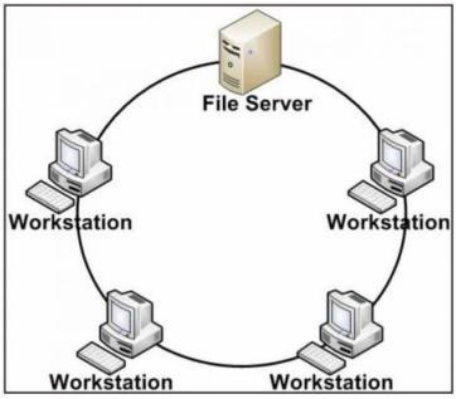
Gambar 5. *Wirelles* LAN Mode Infrastruktur
Sumber: Telaumbanu (2022)

5. Topologi Jaringan

Topologi merupakan bagian integral dari konstruksi jaringan komputer. Topologi yang menggambarkan konfigurasi perangkat yang terhubung disebut juga dengan bentuk atau struktur virtual suatu jaringan. Berikut adalah macam-macam geografi organisasi (Astuti, 2020).

a. Topologi *Ring*

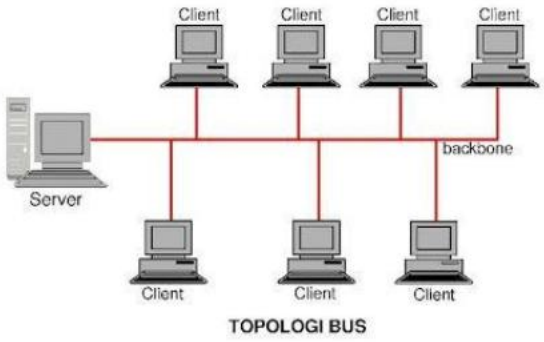
Topologi jaringan yang dikenal dengan topologi *ring* menghubungkan setiap titik di kanan dan kiri dengan komputer pertama dan terakhir. Dalam rangkaian yang berbentuk seperti cincin atau dikenal sebagai *repeater*, lokasi dalam topologi ring ini memperkuat sinyal di setiap rangkaian.



Gambar 6. Topologi *Ring*
Sumber: Astuti (2020)

b. Topologi *Bus*

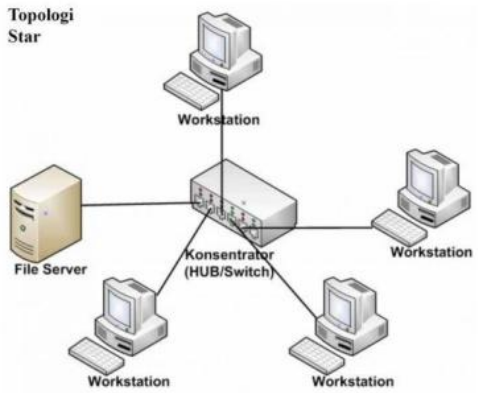
Dengan topologi *bus* ini, satu kabel berfungsi sebagai *hub* untuk semua *server* yang terhubung dengan kabel dan digunakan sebagai media komunikasi atau transmisi. Konektor BNC digunakan untuk menghubungkan setiap komputer ke kabel utama, dan terminator digunakan untuk menyelesaikan sambungan..



Gambar 7. Topologi *Bus*
Sumber: Astuti (2020)

c. Topologi *Star*

Setiap komputer yang terhubung ke *hub* atau *switch* menggunakan kabel UTP dengan menggunakan topologi *star*. Data yang dikirim dari komputer 1 ke komputer 4 disalurkan melalui *hub* atau *switch* jaringan pusat yang bertugas mengatur lalu lintas data, artinya data tidak melewati komputer lain dalam perjalanan ke komputer tujuan..

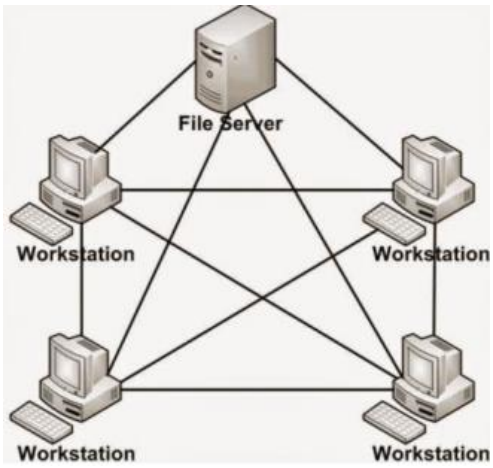


Gambar 8. Topologi *Star*
Sumber: Astuti (2020)

d. Topologi *Mesh*

Karena komputer terhubung langsung ke komputer target, tidak memerlukan komputer tambahan dan data mengalir dengan cepat, topologi *mesh*

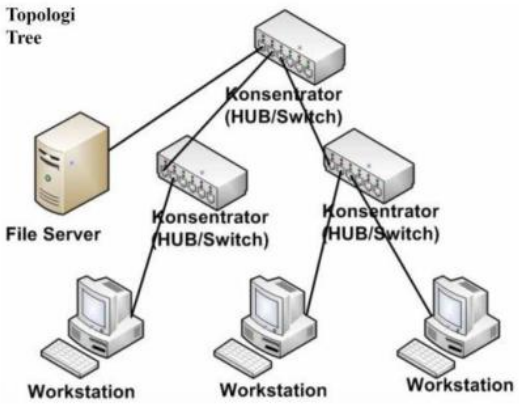
memungkinkan jaringan terhubung secara acak atau tidak menentu. Minimal ada dua jenis koneksi yang ada di setiap komputer, kabel yang menghubungkan ke komputer lain dan kabel lain yang menghubungkan ke *server* file. Disarankan untuk menggunakan topologi ini untuk ruang yang lebih kecil dari pada ruang yang lebih besar karena manajemen koneksinya yang canggih dan sangat sulit dalam pengendalian.



Gambar 9. Topologi *Mesh*
Sumber: Astuti (2020)

e. Topologi *Tree*

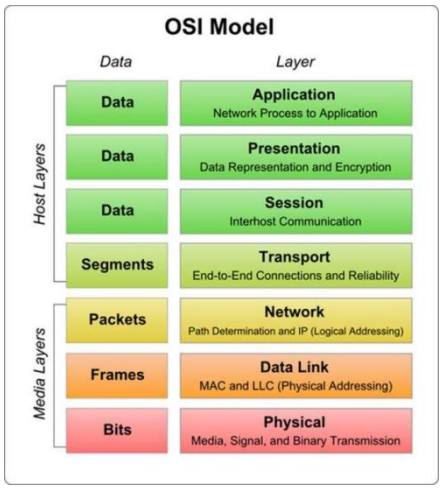
Hub atau *switch* digunakan sebagai media transmisi antar koneksi dalam topologi *tree,* yaitu struktur hierarki bertingkat di mana setiap *hub* atau *switch* terhubung ke file *server*. Pada kenyataannya, topologi *tree* adalah gabungan dari topologi *bus* dan *star,* perbedaan utamanya adalah topologi *tree* memiliki struktur hierarki dan sejumlah besar *hub* atau *switch* dalam jaringan.



Gambar 10. Topologi *Tree*
Sumber: Astuti (2020)

6. OSI *Layer*

Model OSI terdiri dari lapisan-lapisan, yang terdiri dari tujuh tingkat lapisan-lapisan *layer*. Menurut (Army, 2022) ada beberapa level yang membentuk OSI *layer* sebagai berikut.



Gambar 11. Bagian Layer pada OSI Layer
Sumber: Army (2022)

a. *Physical Layer*

Desain jaringan seperti *ethernet*, sinkronisasi *bit*, topologi jaringan, pengkabelan jaringan, dan media transmisi jaringan semuanya ditentukan oleh *physical layer*. Lapisan ini menetapkan protokol yang dapat digunakan oleh kartu antarmuka jaringan (NIC) untuk berkomunikasi dengan media kabel atau nirkabel. Data *biner* diformat dan dikodekan oleh *physical layer* sehingga dapat dikirim melalui media jaringan seperti kabel, transceiver, dan *port*. Perangkat termasuk *hub,* kartu jaringan, dan *repeater* adalah bagian dari lapisan ini..

b. *Data Link Layer*

Susunan potongan data dalam format bingkai ditentukan oleh *data link layer*. Level ini juga ditentukan oleh lapisan data link, yang juga mengontrol aliran, koreksi kesalahan, pengalamatan perangkat keras (MAC, kontrol akses media, dan alamat lainnya), dan fungsionalitas perangkat jaringan (*hub, repeater,* dan *switch*).

c. *Network Layer*

Pada lapisan jaringan, pengamatan dan perutean adalah dua tugas yang paling penting. Pada tingkat ini, pengamatan ditangani oleh lapisan jaringan. alamat *host* yang dalam situasi tertentu sama dengan alamat perangkat keras, ditentukan oleh

lapisan jaringan bersama dengan alamat lingkungan tempat *host* tersebut ditempatkan.

d. *Transport Layer*

Pemanfaatan sumber daya jaringan secara efisien dan transfer data ujung ke ujung (stasiun ke stasiun) dikelola oleh *transport layer*. Itu dapat memilih protokol mana yang akan didukung pada tingkat ini dan apakah akan didebug atau tidak. Lapisan *transport* ini juga mereplikasi dan mengurutkan data jika data yang diterima tidak berurutan.

e. *Session Layer*

Hubungan komunikasi antara dua stasiun disebut sebagai *session layer. Session layer* melakukan transfer file di setiap stasiun, dan prosesor pusat dapat melakukan beberapa sesi bersamaan dengan terminal jarak jauh sekaligus. Selain itu, lapisan ini mengontrol awal, tengah, dan akhir diskusi.

f. *Presentation Layer*

Memberikan informasi kepada entitas aplikasi yang berpartisipasi dalam komunikasi tentang cara terbaik untuk mengatasi perbedaan sintaksis adalah tanggung jawab *presentation layer*. Pada *presentation layer* memformat data, memilih sintaks yang tepat, dan melakukan transformasi data seperti enkripsi dan kompresi untuk mencapai hal ini, format data yang dapat dipahami oleh berbagai jenis media juga termasuk dalam lapisan ini. Lapisan berikut dapat memahami format komunikasi dengan mengubah format data.

g. *Application Layer*

Dengan menawarkan layanan aplikasi pengguna, lapisan ini bertugas menetapkan parameter komunikasi antara aplikasi jaringan dan layanan jaringan. Komunikasi data antara program komputer, seperti program *email,* dan layanan jaringan lainnya, *server* cetak atau aplikasi komputer lainnya, menjadi lebih mudah pada lapisan ini.

7. Kabel Jaringan

Salah satu bagian terpenting yang memudahkan transfer data dan berfungsi sebagai penghubung antara dua perangkat atau lebih agar dapat saling bertukar data atau berkomunikasi satu sama lain adalah kabel. Jaringan komputer menggunakan berbagai jenis kabel diantaranya sebagai berikut.

a. UTP (*Unshielded Twisted Pair*)

Kabel UTP disebut kabel tanpa lapisan pelindung luar. Kabel jaringan jenis ini yang paling sering digunakan untuk membuat jaringan komputer lokal, biasanya digunakan untuk instalasi interior dan aliran data non-rahasia *Local Area Network* (LAN). Media ini digunakan karena dapat diandalkan, harga terjangkau, dan mudah dipasang. Pasangan inti kabel yang terjalin membentuk kabel UTP memiliki 16 kode warna yang berbeda untuk setiap pasangannya, meskipun kabel UTP tidak menawarkan perlindungan interferensi elektromagnetik, penggunaannya secara luas disebabkan oleh harganya yang terjangkau dan serangkaian fitur yang memenuhi standar industri.



Gambar 12. Kabel UPT
Sumber: Telaumbanua (2022)

b. FTP (*Foiled Twisted Pair*) atau S/UTP

Aluminium foil digunakan pada kabel FTP, biasa disebut kabel S/UTP, untuk melindungi lapisan luar (di belakang karet luar) dan mengurangi interferensi elektromagnetik dari luar. Salah satu kelemahan kabel STP adalah kabel ini menjadi lebih dilemahkan pada frekuensi yang lebih tinggi. Frekuensi tinggi menyebabkan keseimbangan menurun, sehingga tidak mampu mengikuti pertumbuhan dan menjadi mahal. Namun, ia memiliki lapisan pelindung kabel interior yang melindungi data yang dikirim dari gangguan dan manfaat kabel STP. Selain itu, STP (*Shielded Twisted Pair*) melindungi kabel dari gangguan sinyal dan induksi eksternal dengan menempatkan lapisan aluminium foil di depan lapisan kertas terluar.

Kabel STP berfungsi sebagai media transmisi, menghubungkan pemancar dan penerima untuk memudahkan pertukaran data antar berbagai peralatan elektronik. Media transmisi diperlukan untuk penerimaan data oleh beberapa perangkat elektronik, termasuk radio, komputer, televisi, dan telepon. Kabel digunakan

sebagai media komunikasi, seperti halnya telepon, untuk menghubungkan dua buah telepon (Telaumbanua, 2022).



Gambar 13. Kabel FTP
Sumber: Telaumbanua (2022)

8. Perangkat Keras Jaringan

Dalam sebuah jaringan juga terdapat beberapa perangkat keras jaringan, berikut beberapa perangkat keras jaringan:

a. *Router*

Router adalah sejenis peralatan jaringan yang menghubungkan dua jaringan lokal dengan protokol lapisan fisik dan lapisan tautan yang berbeda tetapi protokol lapisan jaringan OSI yang sama. Perangkat keras yang mampu menghubungkan beberapa jaringan dengan *subnet* berbeda adalah *router*, ketika terdapat variasi pada banyak komponen protokol, *router* tetap dapat mengirimkan data (Hanifia & Asmunin, 2019).



Gambar 14. *Router*
Sumber: Hanifia & Asmunin (2019)

b. *Switch*

Dengan menggabungkan dua LAN, *switch* digunakan sama seperti *bridge*. karena kapasitasnya. Sebuah *switch* disebut memiliki jangkauan multiport karena memiliki beberapa *port*, bahkan ketika satu *port* terisi maka *port* lainnya tetap

berfungsi. Namun, *switch* dan *bridge* tidak dapat meneruskan paket IP ke komputer lain yang terhubung ke jaringan berbeda.

Switch adalah bagian dari jaringan komputer yang menggabungkan beberapa komputer ke dalam satu jaringan komunikasi atau ke segmen jaringan yang berbeda sehingga data dapat diterima, diproses, dan dikirim ke penerima yang dituju.



Gambar 15. *Switch*
Sumber: Hanifia & Asmunin (2019)

c. *Acces Point*

Pada jaringan nirkabel local *acces point* adalah perangkat jaringan yang digunakan untuk transmisi dan penerimaan data. Perangkat ini berfungsi mirip dengan saklar, dengan konsentrator yang menggunakan komunikasi frekuensi radio untuk menghubungkan berbagai perangkat satu sama lain secara *mobile*. *Acces point* memerlukan media propagasi yang bebas interferensi, artinya tidak dapat diintervensi oleh perangkat di dekatnya melalui benda seperti dinding, partisi, bangunan, atau pohon.

Antena pada titik akses *acces point* dapat digunakan sebagai pemancar dan penerima. Dengan menggunakan *port ethernet* pada kabel, titik akses dapat dihubungkan ke perangkat tambahan seperti *switch* distribusi dan *router.* Anda dapat memanfaatkan titik akses baik di dalam maupun di luar,



Gambar 16. *Acces Point*
Sumber: Hanifia & Asmunin (2019)

d. Komputer *Server*

Mesin yang digunakan untuk mengawasi semua aktivitas jaringan disebut *server*. Dalam suatu jaringan, termasuk jaringan lokal dan *internet,* komputer berperan sebagai pusat komando. Tanggung jawab utama komputer *server* adalah mengawasi dan mengendalikan semua aktivitas jaringan dan aliran data.



Gambar 17. Komputer *Server*
Sumber: Hanifia & Asmunin (2019)

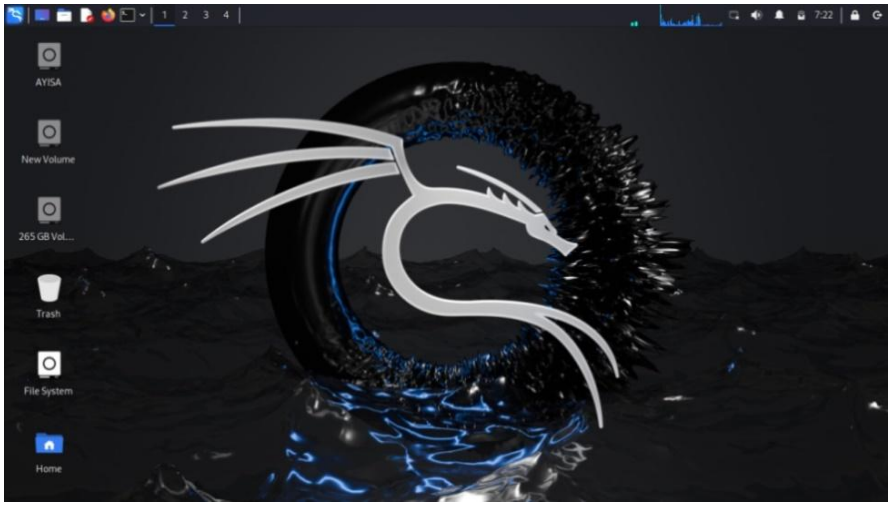
9. Perangkat Lunak Jaringan

Dalam penelitian yang akan dilakukan terdapat perangkat lunak jaringan yang digunakan adalah:

a. *Kali Linux*

Sistem *Linux open source* yang dibangun pada platform *debian*, *kali linux* dirancang untuk melakukan berbagai aktivitas keamanan informasi termasuk forensik komputer, pengujian penetrasi, investigasi keamanan, dan rekayasa balik. Pakar keamanan dan peretas etis dapat mengungkap kelemahan jaringan dan sistem komputer dengan melakukan pengujian penetrasi dengan *kali linux*. Alat untuk pemindaian jaringan, peretasan kata sandi, dan penilaian kerentanan sistem adalah beberapa di antara banyak alat pengujian penetrasi yang tersedia untuk kali linux (Rudiarto, 2023).

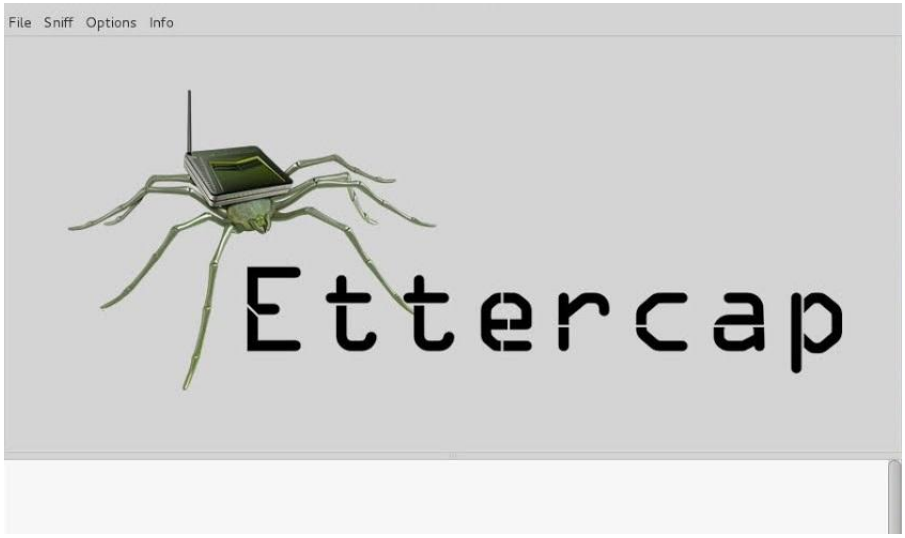
Distribusi *linux* yang dibuat khusus untuk pengujian keamanan dan penetrasi disebut *kali linux*. Sistem operasi *kali linux* tidak bermaksud melakukan aktivitas yang merugikan orang lain. Sebaliknya, *kali linux* berupaya untuk meningkatkan keamanan jaringan dan sistem komputer, sehingga mengurangi kemungkinan intrusi dan potensi penyimpangan keamanan..



Gambar 18. OS *Kali Linux*
Sumber: Penulis (2024)

b. *Ettercap*

Ettercap memiliki banyak alat untuk analisis jaringan dan *host* serta memungkinkan diskriminasi aktif dan pasif terhadap berbagai protokol, termasuk protokol terenkripsi. Injeksi data ke dalam koneksi yang sudah ada memungkinkan penggantian atau penghapusan paket dengan cepat, menjaga sinkronisasi koneksi. Rangkaian penciuman yang kuat dan komprehensif dicapai dengan menerapkan berbagai mode *sniffing*. Tersedia empat jenis *sniffing*, yaitu IP *address*, MAC *address*, ARP *full-duplex*, dan ARP berbasis publik (*half-duplex*). Selain itu, *Ettercap* dapat mengidentifikasi koneksi nirkabel dan LAN, serta geometri LAN menggunakan sidik jari OS aktif atau pasif.



Gambar 19. *Ettercap*
Sumber: Penulis (2024)

c. *XArp*

Serangan ARP *spoofing* pada jaringan komputer diidentifikasi oleh perangkat lunak yang disebut *XArp*, melalui penggunaan sinyal ARP fiktif, penyerang dapat mencoba mengirimkan paket data ke jaringan dengan merutekan lalu lintas ke alamat MAC yang salah. Teknik ini dikenal sebagai ARP *spoofing*. Ketika ada kelainan pada lalu lintas ARP, *XArp* dapat mendeteksi setiap *port* yang terhubung ke jaringan LAN, memungkinkannya beroperasi sebagai alat informasi dengan mencari indikasi serangan *spoofing*. Untuk memungkinkan pengguna segera mengambil tindakan forensik jaringan, *XArp* akan mengirimkan pesan, atau peringatan, secara *realtime* (Choiruman, Ginting & Iryani, 2022).



Gambar 20. *XArp*
Sumber: Penulis (2024)

d. *WinBox*

Dengan *winbox, mikrotik routerOS* dapat dikonfigurasi melalui antarmuka pengguna grafis. Konfigurasi akan dibuat lebih sederhana dengan menggunakan antarmuka pengguna grafis (GUI). *Winbox* adalah program portabel yang berjalan pada sistem operasi *windows*. Oleh karena itu, *winbox* seringkali memiliki ukuran yang lebih kecil dan menggunakan memori yang lebih sedikit. *Linux* dan *MacOS* juga dapat menjalankan *winbox*. Hampir setiap fungsi *winbox* identik dengan fungsi konsol (baris perintah). Di sisi lain, *winbox* tidak mengizinkan konfigurasi fitur tertentu, seperti kemampuan untuk mengubah alamat MAC suatu antarmuka.

Tergantung pada IP dan alamat MAC *router* yang akan digunakan, *winbox* dapat terhubung dengannya dengan mudah. *winbox* juga memudahkan konfigurasi *mikrotik*, di antara fitur-fitur lainnya ia memiliki fitur sesi yang memungkinkan mempertahankan sesi konfigurasi.

Gambar 21. *WinBox*
Sumber: Penulis (2024)

10. Profil SMK Negeri 1 Palopo

SMK Negeri 1 Palopo merupakan salah satu sekolah negeri yang berada di Jl. Khm Kasim No. 10, Desa/Kelurahan. Pattene, Kecematan. Wara Utara, Kota. Palopo, Provinsi. Sulawesi Selatan. Dimana penulis memilih SMK Negeri 1 Palopo sebagai tempat penelitian dalam hal melakukan pengimplementasian keamanan jaringan, sebagai dasar masalah yang ditemukan dalam observasi terhadap kondisi jaringan di SMK Negeri 1 Palopo.



Gambar 22. SMK Negeri 1 Palopo
Sumber: Penulis (2024)

2.2 Hasil Penelitian yang Relevan

Hasil penelitian relevan di bawah ini dengan penelitian yang akan penulisan lakukan baik segi rancangan maupun penerapannya, tempat dan sistem yang berbeda.

1. Penelitian yang dilakukan oleh Simorangkir & Harjanti (2021) dengan judul "Implementasi keamanan jaringan menggunakan perangkat lunak *SOPHOS XG Firewall*". Metode penelitian yang digunakan adalah menggunakan *Network Development Life Cycle* (NDLC) yang merupakan metode dalam mengembangkan jaringan infrastruktur dalam pemantauan jaringan untuk mengetahui secara fisik dan kinerja jaringan. Hasil penelitian menunjukan bahwa setelah diimplementasikan kemanan jaringan dengan perangkat lunak *Sophos XP Firewall* adalah membantu petugas *Network Engineer* dalam melakukan pengamanan seperti pembatasan user untuk mengakses website-website yang tidak boleh diakses, pengaturan penggunaan *internet* dan mengamankan jaringan dari serangan *hacker*, juga melakukan *blocking access* terhadap *user* yang dianggap tidak berkepentingan.
2. Penelitian yang dilakukan oleh Suhada, Tukiyat dan Makhsun (2023) dengan judul "Analisis keamanan jaringan lokal pada media *Acces Control Address Spoofing* Dengan Metode *Address Resolution Protocol*". Metode penelitian yang digunakan adalah metode *Address Resolution Protocol*. Hasil penelitian menunjukan bahwa dari tampilan *dashboard winbox* bahwasanya dapat menjadi acuan atau bahan memonitoring perangkat yang terhubung dan bisa mencegah terjadinya *spoofing* MAC *address*.
3. Penelitian yang dilakukan oleh Amien (2020) dengan judul "Implementasi keamanan jaringan dengan IP *Tables* sebagai *firewall* menggunakan metode *Port Knocking*". Metode penelitian yang digunakan adalah *Confidentiality, Integrity,* dan *Availability.* Hasil penelitian menunjukan bahwa dengan penerapan metode yang digunakan bahwa telah berhasil dilakukan pengujian dan dapat sudah diterapkan pada *server* dengan menggunkan sistem operasi *debian server Wheezy* 7.3 *linux*, Dengan *port* yang di buka *port22* SSH *(Secure Shell).*
4. Penelitian yang dilakukan oleh Ginting, Data dan Kartikasari (2019) dengan judul "Deteksi serangan ARP *Spoofing* berdasarkan analisis lalu lintas paket

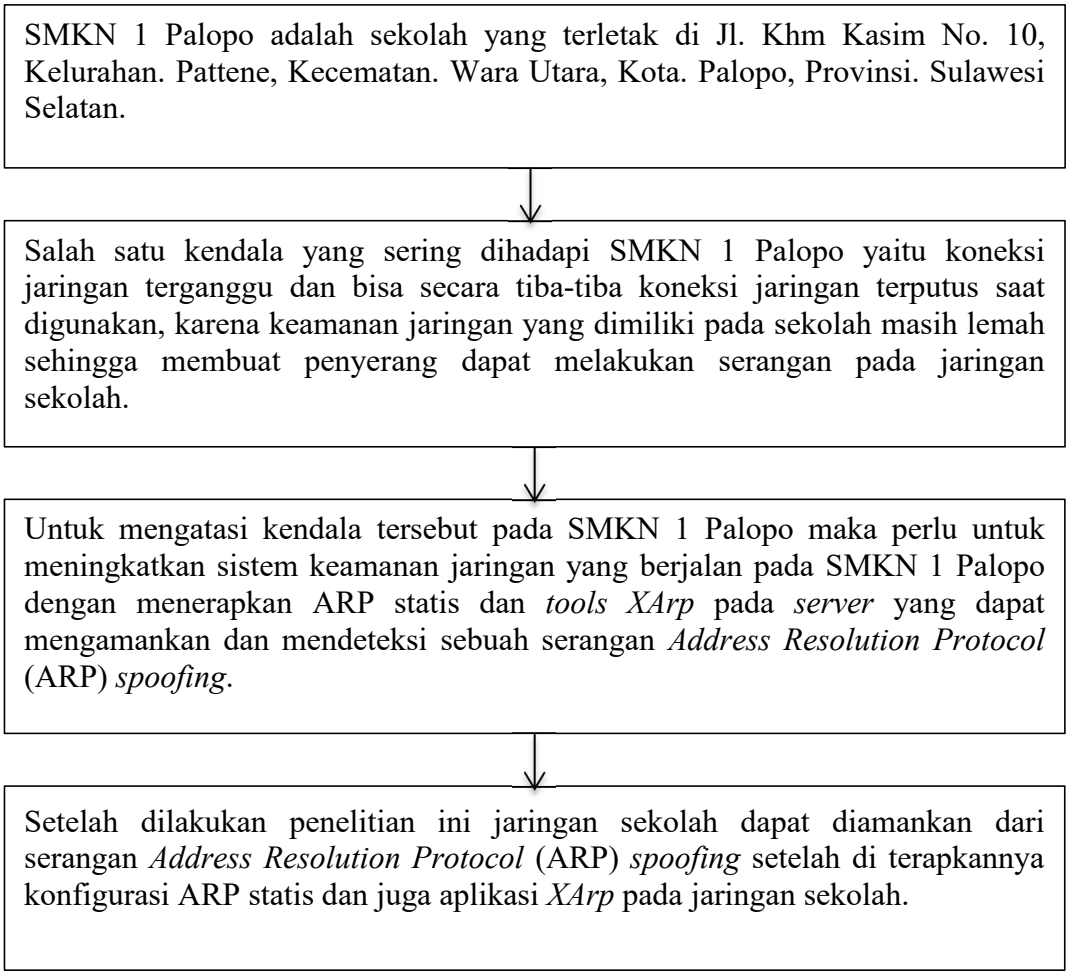
protokol ARP". Metode yang digunakan dalam penelitian adalah metode analisis lalu lintas secara aktif pada paket ARP untuk mendeteksi serangan ARP *spoofing.* Hasil penelitian menunjukkan bahwa berdasarkan hasil perancangan, implementasi dan pengujian deteksi ARP *spoofing* yang dilakukan dengan menganalisis paket ARP yang masuk dapat dilakukan. Untuk melakukan deteksi serangan ARP *spoofing* menggunakan 1 *detektor host* yang melakukan analisis lalu lintas paket ARP pada jaringan lokal tersebut. Adapun waktu yang dibutuhkan untuk mendeteksi serangan ARP *spoofing* adalah 0.4 detik. Hasil tersebut didapatkan pada saat pengujian skenario. Akurasi dari metode ini adalah 89.46%.

2.3 Kerangka Pikir

Kerangka pikir adalah model konseptual tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting. Kerangka pikir adalah sintesa atau model konseptual yang menjelaskan bagaimana teori itu berhubungan satu dengan lainnya berdasarkan teori-teori yang dikumpulkan. Kerangka pikir merupakan penjelasan sementara terhadap suatu gejala yang menjadi objek permasalahan peneliti. Kerangka pikir ini disusun dengan berdasarkan kajian teori dan hasil penelitian terdahulu.

Kerangka pikir merupakan penjelasan sementara terhadap suatu permasalahan yang dikembangkan berdasarkan kajian teori dan penelitian yang relevan. Sekolah Menengah Kejuruan Negeri 1 Palopo merupakan sekolah yang terletak di wilayah Kota Palopo yang saat ini sedang mengalami perkembangan pemanfaatan jaringan *internet* dalam proses belajar mengajar, namun belum diterapkannya keamanan jaringan yang kuat di SMK Negeri 1 Palopo sehingga dapat menimbulkan kendala dalam penggunaan jaringan. Adapun sistem yang diusulkan penulis yaitu keamanan jaringan berupa ARP statis dan *tools XArp* untuk mengamankan jaringan dari serangan pada sekolah. penulis harapkan sistem ini dapat menyelesaikan permasalahan yang dihadapi pada SMK Negeri 1 Palopo.

Skema kerangka pikir dalam penelitian ini dapat dilihat pada gambar yang akan disajikan di bawah sebegai berikut:



Gambar 23. Kerangka Pikir