BAB II
LANDASAN TEORI

2.1 Penelitian Terkait

Penelitian terdahulu sangatlah digunakan untuk memperkuat referensi bagi penelitian yang sedang berlangsung, sehingga dapat mengetahui dan menambah pemahaman dalam memaknai fenomena penelitian dan perkembangnya. Penelitian ini memiliki beberapa referensi terkait judul yang dapat dilihat pada Tabel 2.1

Tabel 2.1. 1 Penelitian Terkait

Topik	**Metode**	**Hasil**	**Referensi**
Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar	Metode Port Knocking	Hasil dari penelitian tersebut bahwa Penerapan metode Port Knocking untuk keamanan jaringan SMKN 1 Sumbawa dapat membantu dalam meningkatkan keamanan jaringan dan membantu administrator dalam mengamankan Mikrotik Routerboard pada system jaringan komputer SMKN 1 Sumbawa Besar. Dengan demikian penelitian ini dapat memberikan kontribusi untuk keamanan jaringan komputer SMKN 1 Sumbawa Besar.	[1]

IMPLEMENTASI METODE PORT KNOCKING PADA SISTEM KEAMANAN SERVER UBUNTU VIRTUAL BERBASIS WEB MONITORING	Metode Port knocking, firewall	Hasil dari penelitian tersebut bahwa 1. Metode port knocking berhasil mengamankan server dengan layanan jaringan celah port terbuka, dengan cara memblok port 22 dan melakukan knock pada server untuk membuka port SSH (22) sewaktu-waktu diperlukan layanan. Pada saat dilakukan serangan port scanning, port SSH (22) terlihat dalam keadaan tertutup dengan diimplementasikan port knocking pada sistem. 2. Berdasarkan hasil penelitian port knocking berhasil mengatasi permasalahan pemblokkan port yang di lakukan oleh firewall. 3. Dari hasil pengujian yang telah di lakukan pada sistem dengan menggunakan port scanning, DDOS attack dan brute force	[2]

PENGAMANAN MIKROTIK ROUTERBOARD DARI SERANGAN KEAMANAN DENGAN NOTIFIKASI BOT TELEGRAM	Metode IDS,port knocking ,bot telegram	Hasil dari penelitian tersebut bahwa 1. Optimalisasi keamanan mikrotik routerboardberhasil dilakukan dengan metode IDS dan fokus pada firewalldan script. 2. Adanya IDS tersebut memberi dampak antara lain, mampu mendeteksi serangan DDOS dan memberikan notifikasikepada administrator berupa bot telegram.	[3]

Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking	Metode Port Knocking, scanning, sniffing	Hasil dari penelitian tersebut bahwa konfigurasi Port Knocking dapat berfungsi dengan baik. Berdasarkan pengujian, pada saat sistem jaringan berada pada mode normal dapat di-scaning, di-sniffing dan berhasil login. Pada saat mode disable access, tidak dapat di-scan, di-sniffing maupun login juga tidak berhasil. Dan pada saat sistem jaringan berada pada mode enable access dapat di-scan, dapat di-sniffing dan berhasil login sebagaimana pada mode normal.	[4]

Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking	Metode Port Knocking	Hasil dari penelitian tersebut bahwa Pemanfaatan metode Port Knocking pada keamanan jaringana sangat cocok diterapkan untuk menjaga Router dari akses orang lain yang tidak berhak mengaksesnya. walaupun pengguna PC1 mengetahui user dan password untuk login ke Router, akan tetapi jika pengguna PC1 tersebut tidak mengetahui role (route) ping request ke Router maka ia tidak bisa login ke Router. Dengan demikian untuk mengakses admin Router harus melewati dua gerbang security. Gerbang pertama yaitu user dan password admin Router. Sedangkan gerbang kedua yaitu role (route) ping request yang dipakai untuk mengakses admin Router. Perlu adanya penelitian lebih lanjut untuk mengembangkan role (route) yang dibangun pada Router. Misalnya membangun role yang lebih kompleks agar role tersebut lebih sulit untuk ditebak oleh hacker.	[5]

Sistem Reporting Keamanan pada Jaringan Cloud Computing Melalui bot Telegram dengan Menggunakan Teknik Intrussion Detection and Prevention System	Metode port knocking dan NIDS, bot telegram,	Hasil dari penelitian tersebut bahwa pada paper ini, sistem IDS berhasil mendeteksi serangan, yang mana dilakukan terlebih dahulu proses konfigurasi dan penambahan rulesagar snort bisa mendeteksi seranganberdasarkan pencocokan dengan signatureyang terdapat pada rulestersebut	[6]

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING	metode port knocking, scanning dan sniffing	Hasil dari penelitian tersebut bahwa konfigurasi Port Knocking dapat berfungsi dengan baik. Berdasarkan pengujian, pada saat sistem jaringan berada pada mode normal dapat di-scaning, di-sniffing dan berhasil login. Pada saat mode disable access, tidak dapat di-scan, di-sniffing maupun login juga tidak berhasil. Dan pada saat sistem jaringan berada pada mode enable access dapat di-scan, dapat di-sniffing dan berhasil login sebagaimana pada mode normal.	[7]

IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER DENGAN METODE PORT KNOCKING PADA LKP SURYA KOMPUTER	Merode Port Knocking	Hasil dari penelitian tersebut bahwa hasil untuk terhubung pada server MikroTik user/client harus melakukan autentikasi knocking 1-2-3 pada port pemicu, pada setiap autentikasi knocking memiliki waktu timeout 10 detik, dan waktu akses pada server MikroTik yaitu dengan timeout 30 menit.	[8]

ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS V6.48.3 MENGGUNAKAN METODE PORT KNOCKING	Metode port knocking dan sniffing	Hasil dari penelitian tersebut bahwa keamanan pada jaringan yang ada pada Universitas Ubudiyah Indonesia masih dapat di disadap oleh Attecker dengan melakukan scanning port dan melakukan penyerangan menggunakan Metode Sniffing pada jaringan secara mudah untuk mendapatkan informasi penting yang ada pada jaringan Universitas Ubudiyah Indonesia.	[9]

Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking	Metode port knocking	Hasil dari penelitian tersebut bahwa peneliti dapat mengetahui cara melakukan keamanan jaringan dengan menggunakan metode port knocking dan dapat disimpulkan bahwa sistem keamanan jaringan telah berhasil dibuat dan sesuai dengan yang diharapkan. Kelebihan dari port knocking yaitu mengatur knock/ketukan port yang akan di set secara manual dan dapat mengakses server dimana saja selama masih terhubung ke dalam jaringan yang sama.	[10]

PEMANFATAAN METODE PORT KNOCKING DAN BLOCKING UNTUK KEAMANAN JARINGAN BPKAD PROVINSI SUMSEL	Metode port Knocking,port scanning, service port	Hasil dari penelitian tersebut 1) Rules knocking yang dibuat menjadi tambahan pengamanan autentikasi untuk terhubung ke router. 2) Service port yang terbuka dapat diamankan dengan melakukan blocking port sehingga menjadi ter-filtered. 3) Metode port knocking dan blocking dapat meningkatkan keamanan sistem jaringan terutama dari akses yang ilegal.	[11]

PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN RANDOM PORT KNOCKING BERBASIS RASPBERRY PI YANG DIKIRM MELEWATI TELEGRAM	Metode Random port knocking,Raspberry pi, Telegram	Jaringan Menggunakan Random Port Knocking Berbasis Raspberry Pi Yang Dikirm Melewati Telegram yang telah dijelaskan dan diuraikan pada bab sebelumnya dalam skripsi ini, dapat disimpulkan bahwa: 1. Dengan metode pengacakan port yang dilakukan orang lain tidak bisa menggunakan port awal untuk masuk. 2. Metode random port knocking ini bekerja dengan baik, sebab pergantian port terjadi ketika login gagal > 3 kali.	[12]
Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode Port Knocking	Metode port knocking , email notification	Hasil dari penelitian tersebut Peneiti mengamanan port menggunakan metode port knocking dengan notifikasi email telah berhasil dilakukan. Serta notifikasi email sudah bisa diterapkan dan sudah berjalan dengan fungsinya. Sehingga administrator mudah memantau router tanpa datang ke tempat router diletakkan dengan pesan notifikasi email yang masuk.	[13]

PENGAMANAN MIKROTIK ROUTERBOARD DARI SERANGAN KEAMANAN DENGAN NOTIFIKASI BOT TELEGRAM	Metode Port knocking, bot telegram	Hasil dari penelitian tersebut Port knocking digunakan sebagai pencegah dan mengirimkan notifikasi serangan DDoS pada router Mikrotik melalui bot Telegram. Proses pengujian serangan DDoS berupa ping flood, SYN Flood dan UDP Flood, notifikasi bot telegram berhasil diimplementasikan dengan cukup baik, dimana Port knocking mengirimkan notifikasi melalui bot telegram admin jaringan	[14]

IMPLEMENTASI PORT KNOCKING UNTUK KEAMANAN LAYANAN JARINGAN PADA ROUTER MIKROTIK	Metode port knocking,Mikrotik, Winbox	Hasil dari penelitian tersebut Peneliti dapat mengetahui cara melakukan keamanan jaringan dengan menggunakan metode port knocking dan dapat disimpulkan bahwa sistem keamanan jaringan telah berhasil dibuat dan sesuai dengan yang diharapkan. Kelebihan dari port knocking yaitu mengatur knock/ketukan port yang akan di set secara manual dan dapat mengakses server dimana saja selama masih terhubung ke dalam jaringan yang sama. Kekurangannya yaitu penyetingan yang cukup rumit dan adanya celah pembobolan server mikrotik dari serangan bruteforce.	[15]

2.2 Teori Pendukung

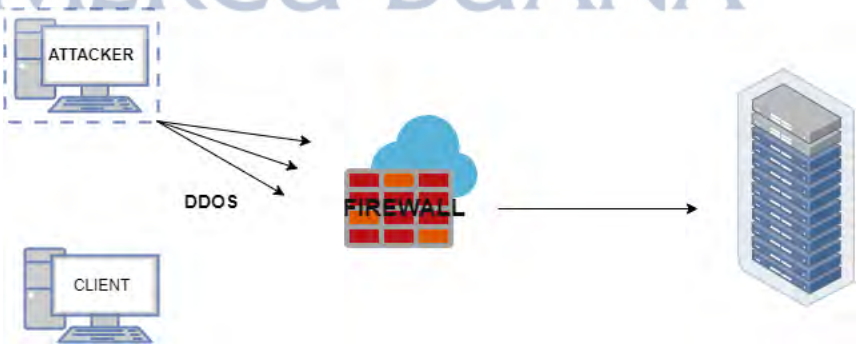
2.2.1 Port Knocking

Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupun ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewal akan memberikan akses ke port yang sudah diblock[15].

Gambar 2.2.1 1 Port Knocking

2.2.2 DDoS (*Distributed Denial of Service)*

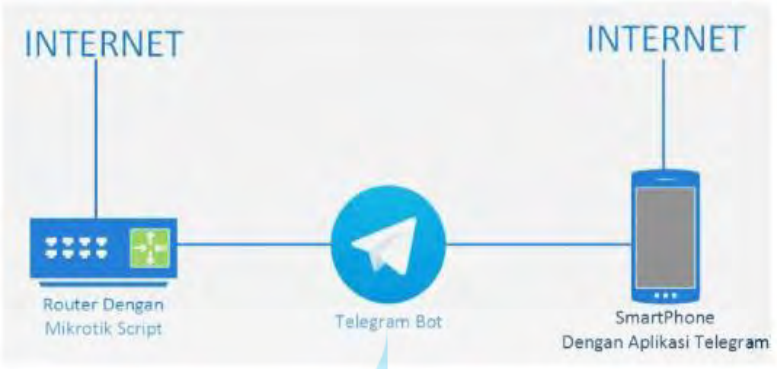
Distributed Denial of Service atau DDoS Merupakan sebuah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut [3].



Gambar 2.2.2 2 DDOS (*Distributed Denial of Service*)

2.2.3 Bot Telegram

Telegram merupakan aplikasi chat yang bersifat opensource yang dapat diaplikasikan pada perangkat lain dengan membuat bot dan memanfaatkan API dari bot tersebut maka akan lebih mudah dalam mengirim informasi jaringan secara real-time.



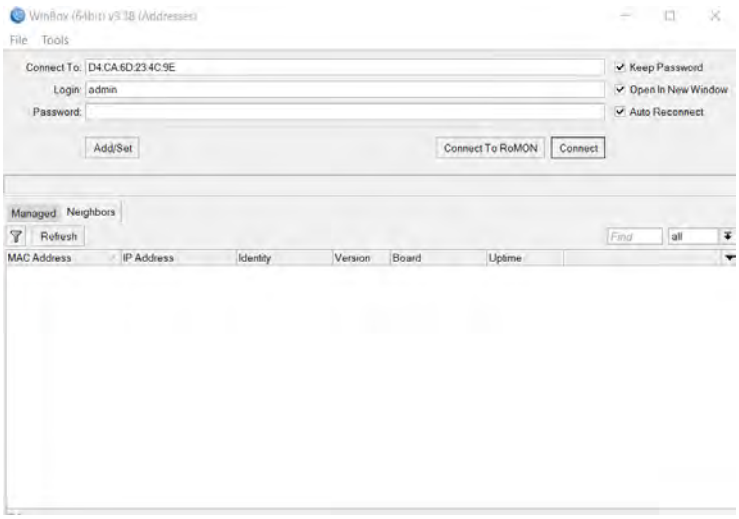
Gambar 2.2.3 3 Bot Telegram (Kusuma Hakim et al., 2019)

2.2.4 Mikrotik

Mikrotik adalah perangkat jaringan komputer yang berupa hardware dan software yang dapat difungsikan sebagai Router, sebagai alat Filtering, Switching maupun yang lainnya. Adapun hardware Mikrotik bisa berupa Router PC (yang diinstall pada PC) maupun berupa Router Board (sudah dibangun langsung dari perusahaan Mikrotik). Sedangkan software Mikrotik atau yang dikenal dengan nama RouterOS ada beberapa versinya. Salah satu versi RouterOS yang terkenal saat ini adalah RB1100 (Mikrotik, 2018)[4].

2.2.5 Winbox

Winbox adalah utility yang digunakan untuk konektivitas dan konfigurasi MikroTik menggunakan MAC Address atau protokol IP. Dengan winbox kita dapat melakukan konfigurasi MikroTik RouterOS menggunakan modus GUI dengan cepat dan sederhana. Winbox dibuat menggunakan win32 binary tapi dapat dijalankan pada Linux, Mac OSX dengan menggunakan Wine. Mengkonfigurasi mikrotik ini lebih banyak diunakan karena selain penggunaanya yang mudah anda juga tidak harus menhapal perintah-perintah console.



Gambar 2.2.5 4 Winbox

2.2.6 IPtables

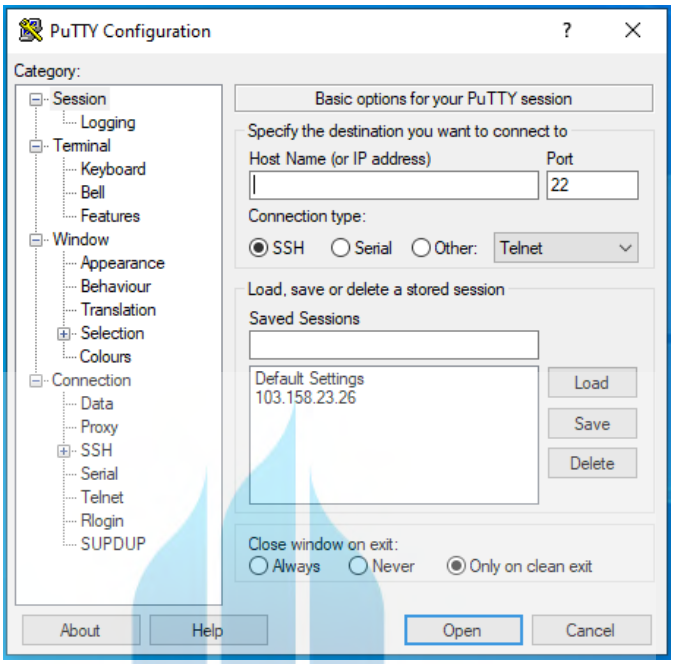
IPtables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalulintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Sebuah policy pada iptables dibuat berdasarkan sekumpulan peraturan yang diberikan pada kernel untuk mengatur setiap paket yang datang. Pada iptables ada istilah yang disebut dengan ipchain yang merupakan daftar aturan bawaan dalam iptables[20].

2.2.7 Firewall

Firewall adalah komponen jaringan yang penting dalam hal mengontrol aliran akses di lingkungan jaringan dan bertujuan untuk memungkinkan konektivitas terkontrol antara client dan server, mencegah komunikasi yang tidak sah atau tidak berada pada area jaringan komputer. Firewall berupa perangkat keras digunakan untuk membatasi hak akses dari jaringan satu ke jaringan yang lain. Mekanisme akses kontrol yang ditawarkan firewall bergantung pada perangkat aturan yang ditentukan administrator, kemudian diterapkan ke setiap paket yang mengalir melalui firewall [20].

2.2.8 Putty

Putty adalah alat SSH dan Telnet, yang dimaksudkan untuk menjalankan protokol jaringan SSH, Telnet, dan Rlogin. Protokol dapat digunakan untuk menjalankan sesi jarak jauh pada komputer melalui jaringan jarak jauh.



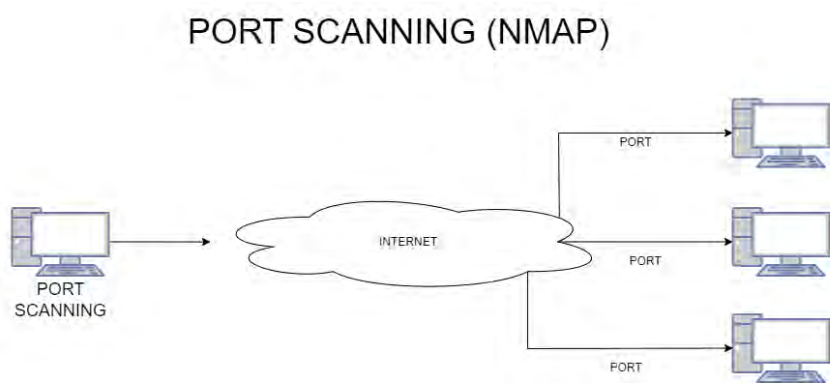
Gambar 2.2.8 5 Putty

2.2.9 Tarpit

Suatu jaringan yang merespon, mengecek paket penyerang dengan reaksi sangat lambat merupakan tarpit(sebutan yang dipinjam dari pakar geologi serta dinosaurus yang kesimpulannya meninggal di kolam renang tar(aspal) diselatan Los Angeles). Dengan sebagian besar penyerang modern serta menyebar dengan cepat adalah worm, paket penyelidikan buat mengintai tujuan mendahului paket serangan.

2.2.10 Port scanning

Port Scanning ialah metode yang digunakan untuk menerapkan scanning terhadap port port yang terbuka pada fitur. Dengan terdapatnya port scanning ini sehingga orang lain mampu mengenali port port yang terbuka, sehingga mempermudah orang lain untuk menerapkan serangan ke perangkat kita.



Gambar 2.2.11 6 Port Scanning

2.2.11 Hacking

Hacking adalah kegiatan memasuki system melalui system operasional lain yang dijalankan oleh Hacker. Tujuanya untuk mencari hole/bugs pada system yang akan dimasuki. Dalam arti lain mencari titik keamanan system tersebut. Bila hacker berhasil masuk pada system itu, hacker dapat mengakses hal apapun sesuai keinginan hacker itu. Dari kegiatan yang mengacak system maupun berupa tindakan kejahatan (Dimas, 2018)[4].

2.2.12 OSI Layer

Layer OSI (Open System Inter Connection) adalah sebuah layer yang membantu terjadinya transfer data antar host yang berbeda. Layer OSI terdiri atas tujuh lapisan yaitu Layer Application, Layer Presentation, Layer Session, Layer Transport, Layer Network, Layer Data Link, Layer Physical.Tujuan diciptakannya OSI adalah untuk menjembatani proses komunikasi data melalui kerangka logika yang terstruktur. Dengan begitu para desainer jaringan dapat dengan mudah memahami metode, jenis protokol maupun tiap layer dalam proses pencarian titik awal permasalahan, sehingga meminimalkan waktu yang diperlukan untuk melacak masalah jaringan.

2.2.13 Jenis- jenis jaringan komputer

Jaringan komputer adalah sistem yang terdiri dari komputer yang dirancang untuk berbagi sumber daya (printer, CPU), berkomunikasi (email, pesan instan) dan mengakses informasi (browser). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan

komputer dapat meminta dan memberikan layanan. Pihak yang meminta/menerima layanan disebut klien dan pihak yang menyediakan/mengirim layanan disebut server. Desain ini disebut sistem client-server dan digunakan di hampir semua aplikasi jaringan komputer.

jaringan dapat bersifat pribadi atau publik. Saat menggunakan jaringan pribadi, akses pengguna biasanya diperlukan untuk memberikan kredensial berupa kata sandi, baik yang dimasukkan secara manual oleh administrator atau diperoleh langsung dari pengguna. Itu tidak membatasi akses ke jaringan publik seperti Internet.Dalam jaringan komputer, terdapat jenis-jenis jaringan yang berbeda. Diantaranya :

1. Jaringan LAN

   Jaringan LAN didefinisikan sebagai jaringan komputer yang sering digunakan untuk menghubungkan komputer dan workstation di perusahaan atau kantor bisnis untuk berbagi sumber daya (sumber daya, misalnya printer) dan bertukar informasi yang masih berdekatan. Saat ini, sebagian besar LAN berbasis teknologi IEEE 802.3 Ethernet menggunakan perangkat switching dengan kecepatan transfer data 10, 100 atau 1000 Mbit/s. Selain teknologi Ethernet, teknologi 802.11b (atau sering disebut Wi-Fi) kini banyak digunakan untuk membuat LAN.

2. Jaringan MAN

   Jaringan MAN adalah jaringan komputer yang mencakup area yang sangat luas, yang dapat berlokasi di dalam kota. Jarak antara server dan pengguna adalah dari 5 hingga 50 km. Jenis jaringan ini sering digunakan untuk menghubungkan server pusat perusahaan ke pengguna di kantor cabang.

3. Jaringan WAN

   Jaringan WAN adalah jaringan yang menjangkau area geografis yang lebih luas, sering kali mencakup negara atau bahkan lintas benua. WAN terdiri dari kumpulan mesin yang dirancang untuk menjalankan program

pengguna (aplikasi). WAN dapat dikatakan sebagai Internet seperti yang dikenal sekarang.

2.2.14 Tipe Jaringan Berdasarkan Fungsinya

Berdasarkan pola pengoprasiannya atau fungsi masing-masng komputer maka jaringan koputer dapat di bagi menjadi:

1. Peer-to-Peer

   Peer-to-Peer adalah jenis jaringan komputer di mana setiap komputer dapat menjadi server dan klien. Setiap komputer dapat mengakses dan mengakses komputer lain.

2. Client-Server

   Client-Server adalah jaringan komputer yang salah satu komputernya bertindak sebagai server. Misalnya, komputer server di kantor 7Skynet yang menyediakan akses browser ke Internet, email, file, dan aplikasi intranet yang berjalan di klien.