BAB II
LANDASAN TEORI

Pada bab ini penulis akan menjabarkan teori-teori yang digunakan sebagai landasan dalam penelitian yang relevan dengan judul Tugas Akhir.

2.1 Keamanan jaringan

Pengertian Keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa ancaman fisik maupun non-fisik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.[1]

Keamanan jaringan adalah bentuk pencegahan atau deteksi pada hal yang bersifat gangguan dan akses tak seharusnya pada Sistem Jaringan Komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun non-fisik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.[2]

Kemanan jaringan sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Berikut adalah tools dan teknik yang digunakan dalam melakukan serangan kemanan pada sebuah jaringan komputer.

2.2 Jaringan Komputer

Jaringan Komputer merupakan sebuah konsep hubungan atau interkoneksi antar sekumpulan perangkat. Antar perangkat harus dibuat saling terhubung, apabila ada perangkat yang tidak terhubung, maka konsep

tersebut akan termasuk dalam definisi jaringan. Dengan terhubungnya sekumpulan komputer antara satu sama lain, dengan menggunakan satu protocol komunikasi sehingga seluruh komputer yang saling terhubung tersebut dapat berbagi informasi, program, sumber daya, dan juga dapat saling menggunakan perangkat keras lainnya secara bersamaan, seperti printer, harddisk, dan lain sebagainya.[3]

Dengan semakin majunya teknologi komputer dan semakin banyaknya masyarakat yang menggunakan teknologi ini telah menciptakan berbagai konsekuensi, antara lain meningkatkan ketergantungan terhadap teknologi. Bagi sebagian besar kalangan masyarakat, pekerjaan mereka saat ini harus diselesaikan dengan komputer dan perangkat pendukung lainnya. Salah satu bentuk penerapan teknologi komputer tersebut adalah sistem jaringan komputer.[3]

Sistem jaringan komputer merupakan sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer antara lain :

- Membagi sumber daya contohnya berbagi pemakaian hardware dan berbagi koneksi internet
- Mudah dalam berkomunikasi antar komputer contohnya penerapan e-mail surat elektronik
- Kegiatan instant messaging

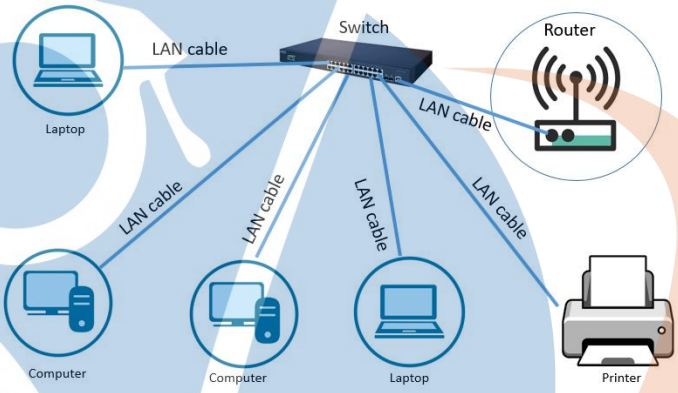
2.2.1 Jenis Jaringan Komputer

Berdasarkan luas area cakupan, jaringan komputer dibagi menjajdi :

1. LAN (Local Area Network)

   Local Area Network (LAN) adalah suatu jaringan komputer yang hanya mencakup wilayah lokal saja. Artinya, jaringan ini hanya dapat digunakan oleh pengguna di area LAN. LAN menghubungkan perangkat ke jaringan internet melalui perangkat jaringan sederhana.

Dalam jaringan LAN biasanya ditemukan kabel UTP, Hub, Switch, maupun Router. Contoh dari jaringan ini adalah komputer-komputer di sekolah, perusahaan, atau warung internet. Jaringan pada area yang terbatas tersebut biasanya merupakan jaringan LAN.[4]



Gambar 1 Local Area Network (LAN)

2. MAN (Metropolitan Area Network)

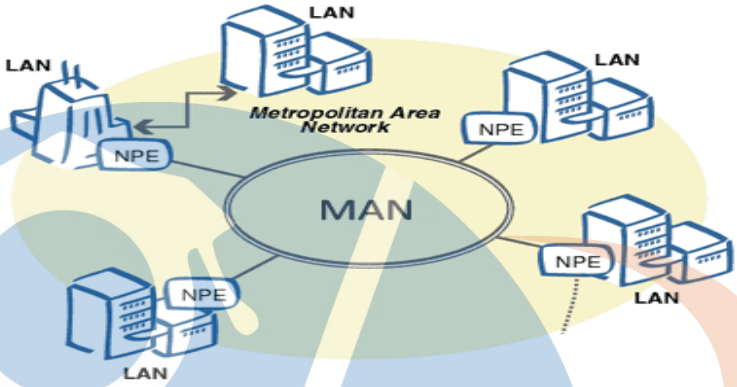
Metropolitan Area Network (MAN) adalah suatu jaringan komputer yang dapat mencakup area yang lebih luas dan menggunakan teknologi yang lebih canggih dari LAN. Jaringan MAN merupakan gabungan beberapa jaringan LAN yang mana menjangkau hingga 10 s.d. 50 km.

Jaringan MAN cocok dipakai untuk membangun jaringan antar perkantoran atau instansi yang masih dalam satu kota. Biasanya MAN dipakai untuk menghubungkan beberapa lokasi seperti perkantoran, kampus, pemerintahan, dan sebagainya.

MAN digunakan karena kecepatan transfer data yang dinilai tinggi dan proses instalasi yang tidak terlalu rumit. Di

dalam MAN, dibutuhkan operator telekomunikasi yang akan menjadi penghubung antar jaringan komputer.[4]

.



Gambar 2 Metropolitan Area Network (MAN)

3. WAN (Wide Area Network)

Wide Area Network (WAN) adalah jaringan komputer yang luas cakupannya dapat mencapai satu negara bahkan benua. Jaringan ini merupakan gabungan dari LAN dan MAN yang wilayahnya dipisahkan secara geografis.

Membangun jaringan WAN membutuhkan kabel serat optik (*fiber optic*), kabel telepon, atau bisa juga menggunakan satelit. Oleh karena jangkauannya yang luas, membuat WAN memerlukan biaya yang sangat besar.

WAN mempunyai transmisi kecepatan mulai dari 2 Mbps, 34 Mbps, 45 Mbps, 155 Mbps, 625 Mbps atau bahkan lebih. Faktor yang menjadi pengaruh design dan performa jaringan ini ada pada siklus komunikasi semacam jaringan telepon atau satelit.[4]

Gambar 3 Wide Area Network (WAN)

2.3 Cyber Attack

Serangan cyber tidak akan pernah berakhir selagi ada perangkat komputasi yang terhubung ke Internet. Serangan siber terus meningkat terutama selama pandemi corona, menyusul banyak pengguna yang bekerja dan belajar dari rumah dengan memanfaatkan jaringan Internet.

Cisco Umbrella mencatat setidaknya terjadi peningkatan sebesar 40% serangan cyber di tahun lalu.

Karena itu pengguna harus mengetahui berbagai jenis serangan cyber yang umumnya menyerang dan meningkatkan keamanan cyber-nya.

Keamanan cyber adalah praktik untuk melindungi sistem, jaringan, dan program dari ancaman atau serangan digital.

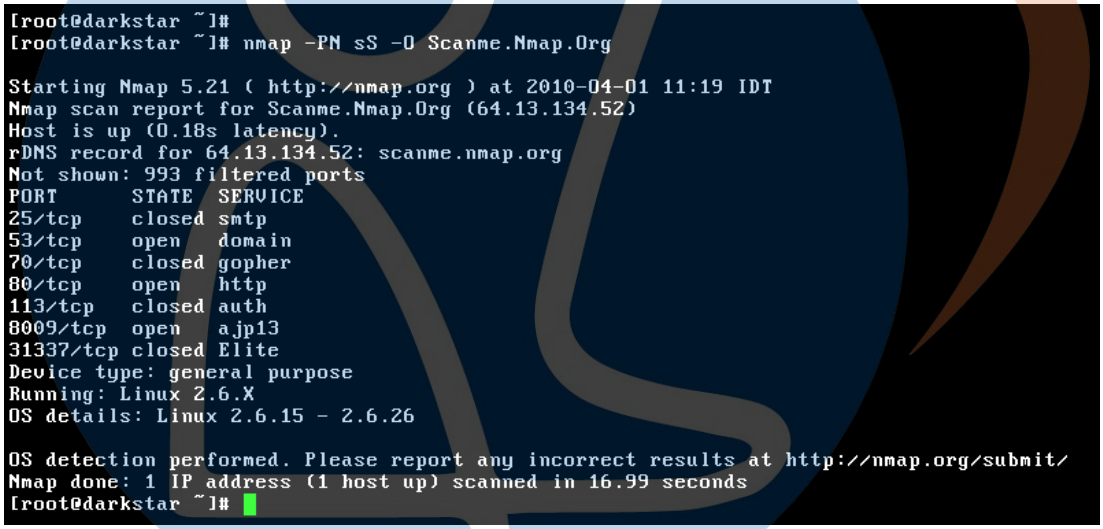
Serangan-serangan ini biasanya ditujukan untuk m

engakses, mengubah, atau menghancurkan informasi sensitif; memeras uang dari korban; atau mengganggu proses bisnis.[5]

2.3.1 Nmap

Nmap (“Nerwork Mapper”) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host

tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall atau fulter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.[6]



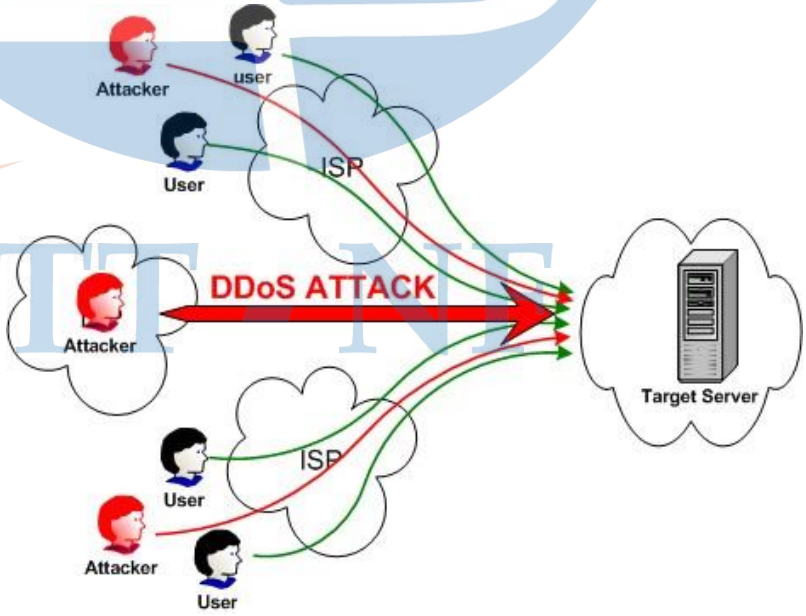
Gambar 4 Nmap

2.3.2 DDOS

Apa itu DDoS? DDoS merupakan kependekan dari Distributed Denial of Service atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi. DDoS adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa komputer host penyerang sampai dengan komputer target tidak bisa diakses.[7]

DDoS adalah serangan yang sangat populer digunakan oleh hacker. Selain mempunyai banyak jenis, DDoS memiliki konsep yang sangat sederhana, yaitu membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari user lain (overload). Salah satu cara dengan mengirimkan request ke server secara terus menerus dengan transaksi data yang besar.[7]

Berhasil atau tidaknya teknik DDoS dipengaruhi oleh kemampuan server menampung seluruh request yang diterima dan juga kinerja firewall saat ada request yang mencurigakan.[7]



Gambar 5 DDoS Attack

2.3.3 Brute Force

Serangan brute force adalah upaya mendapatkan akses sebuah akun dengan menebak username dan password yang digunakan.[8]

Brute force attack sebenarnya merupakan teknik lama dalam aksi cyber crime. Namun, masih banyak digunakan karena dianggap masih efektif.[8]

Apakah brute force attack hanya terkait mendapatkan username saja?

Awalnya memang demikian. Namun tujuan utamanya tentu untuk dapat mengakses situs, server yang menyimpan berbagai informasi dan aset penting.[8]

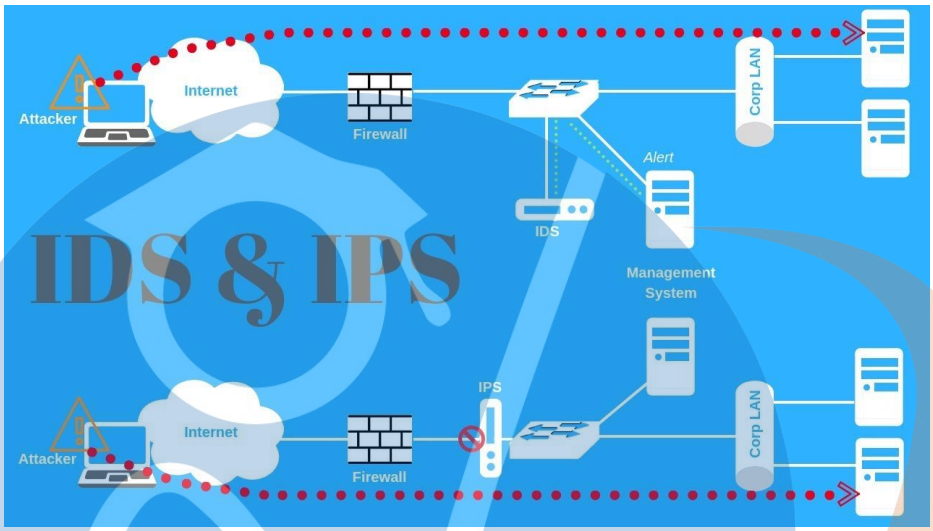
Setelah masuk ke dalam sistem, hacker dapat mengendalikan website Anda hingga mencuri data.[8]

Gambar 6 Brute Force

2.4 Intrussin Detection System (IDS)

IDS (Intrussion Detection System) merupakan sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) apakah tersebut termasuk ancaman atau tidak. Jika ternyata ancaman, maka IDS akan membangkitkan *alert* untuk memberitahu

administrator bahwa terdapat ancaman terhadap jaringan. Jika tidak, IDS menganggap sebagai packet normal/bukan ancaman.[9]



Gambar 7 Intrussin Detection System (IDS)

2.4.1 Jenis – Jenis IDS

Berdasarkan fungsinya, IDS dibagi menjadi beberapa jenis:

1. NIDS (Network Intrusion Detection System)

IDS jenis ini ditempatkan disebuah tempat/titik yang strategis atau sebuah titik didalam sebuah jaringan untuk melakukan pengawasan terhadap *traffic* yang menuju dan berasal dari semua alat-alat (*devices*) dalam jaringan. Idealnya semua *traffic* yang berasal dari luar dan dalam jaringan dilakukan di scan.[9]

2. HIDS (Host Intrusion Detection System)

IDS jenis ini berjalan pada host yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada user atau administrator sistem jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeteksi oleh HIDS.[9]

a. SignatureBased

IDS yang berbasis pada *signature* akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut demgam basis data *signature* yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hamper sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap *malware*. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan di internet dengan *signature* yang digunakan untuk melakukan deteksi yang diimplementasikan didalam basis data IDS yang digunakan. Jadi bisa saja basis data *signature* digunakan dalam sistem IDS ini tidak mampu mendeteksi adanya sebuah percobaan serangan terhadap jaringan karena informasi jenis serangan ini tidak terdapat dalam basis data *signature* sistem IDS ini. Selama waktu keterlambatan tersebut sistem IDS tidak dapat mendeteksi adanya jenis serangan baru.[9]

b. AnomalyBased

IDS jenis ini mengawasi *traffic* dalam jaringan dan melakukan perbandingan *traffic* yang terjadi dengan rata-rata *traffic* yang ada (stabil). Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan "normal" dalam jaringan tersebut, berapa banyak *bandwidth* yang biasanya digunakan dijaringan tersebut, *protocol* apa yang digunakan, *port-port* dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal, atau secara signifikas berbeda dari kebiasaan yang ada.[9]

c. PassiveIDS

IDS jenis ini hanya berfungsi sebagai pendeteksi dan pemberi peringatan. Ketika *traffic* yang mencurigakan atau membahayakan terdeteksi oleh IDS maka IDS akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirmkan ke administrator atau *user*

dan selanjutnya terserah administrator apa tindakan yang dilakukan terhadap hasil laporan IDS.[9]

d. ReactiveIDS

IDS jenis ini tidak hanya melakukan deteksi terhadap traffic yang mencurigakan dan membahayakan kemudian memberi peringatan kepada administrator tetapi juga mengambil tindakan proaktif untuk merespon terhadap serangan yang ada. Biasanya dengan melakukan pemblokiran terhadap traffic jaringan selanjutnya dari alamat IP sumber atau user jika alamat IP sumber atau user tersebut mencoba melakukan serangan lagi terhadap sistem jaringan diwaktu selanjutnya.[9]

2.4.2 Cara Kerja IDS

1. Signature (*Misuse*) Based

IDS yang berbasis pada *signature* akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data *signature* yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hamper sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap *malware*. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan di internet dengan *signature* yang digunakan untuk melakukan deteksi yang diimplementasikan didalam basis data IDS yang digunakan.[9]

2. Anomaly Based

IDS jenis ini mengawasi *traffic* dalam jaringan dan melakukan perbandingan *traffic* yang terjadi dengan rata-rata *traffic* yang ada (stabil). Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan "normal" dalam jaringan tersebut, berapa banyak *bandwidth* yang biasanya digunakan dijaringan tersebut, *protocol* apa yang digunakan, *port-port* dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika

dideteksi ada yang tidak normal, atau secara signifikas berbeda dari kebiasaan yang ada.[9]

Langkah dan Teknik yang digunakan dalam mendeteksi anomaly terdiri atas:

- *Threshoold Detection*, dimana beberapa atribut dari user dan perilaku sistem dinyatakan dalam jumlah atau angka, dengan beberapa tingkatan toleransi yang diperbolehkan.
- *Statitical measures*, baik parameterik dimana distribusi atribut profil di asumsikan cocok dengan pola tertentu, dan non-parameterik, dimana distribusi profil atribut di pelajari dari kumpulan ukuran *historis* yang diamati sepanjang waktu.
- *Rule-Based*, Measures pola tersebut dispesifikasikan dalam aturan dan bukan dalam angka.

2.5 Snort

Snort adalah sebuah software ringkas yang sangat berguna untuk mengamati aktivitasdalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu Network IntrusionDetection System (NIDS) yang berskala ringan (lightweight), dan software inimenggunakan sistem peraturan-peraturan (rules system) yang relatif mudah dipelajariuntuk melakukan deteksi dan pencatatan (logging) terhadap berbagai macam seranganterhadap jaringan komputer.[10]

Dengan membuat berbagai rules untuk mendeteksi ciri-cirikhas (signature) dari berbagai macam serangan, maka Snort dapat mendeteksi danmelakukan logging terhadap serangan-serangan tersebut. Software ini bersifatopensource berdasarkan GNU General Public License [GNU89], sehingga boleh digunakan dengan bebas secara gratis, dan kode sumber (source code) untuk Snort jugabisa didapatkan dan dimodifikasi sendiri bila perlu. Snort pada awalnya dibuat untuk sistem operasi (operating system)

berdasarkan Unix, tetapi versi Windows juga sudah dibuat sehingga sekarang ini Snort bersifat cross-platform.[10]

Snort sendiri merupakan software yang masih berbasis command-line, sehingga cukupmerepotkan bagi pengguna yang sudah terbiasa dalam lingkungan Graphical UserInterface (GUI). Oleh karena itu, ada beberapa software pihak ketiga yang memberikanGUI untuk Snort, misalnya IDScenter untuk Microsoft Windows, dan Acid yangberbasis PHP sehingga bisa diakses melalui web browser.[10]

Gambar 8 Snort

2.6 Suricata

Surciata adalah IDS, IPS dan monitoring engine untuk jaringan yang berkinerja tinggi. Suricata merupakan Opern Source dan dimiliki oleh masyarakat yang dikelola yayasan non-profit, Open Information Security Foundation (OISF). Suricata dikembangkan oleh OISF dan vendor pendukungnya.[11]

Tiga (3) alasan utama mengapa kita perlu mencoba suricata:

- Highly Scalable - Suricata adalah multi threaded. Ini berarti anda dapat menjalankan satu instance dan akan menyeimbangkan beban pengolahan di setiap prosesor pada sensor Suricata yang dikonfigurasi untuk menggunakan. Hal ini memungkinkan perangkat keras komoditas untuk mencapai kecepatan 10 gigabit pada lalu lintas real tanpa mengorbankan cakupan ruleset.

- Identifikasi Protocol - Protokol yang paling umum secara otomatis dikenali oleh Suricata saat stream komunikasi dimulai, sehingga memungkinkan penulis rules untuk menulis aturan untuk protokol, tidak ke port yang diharapkan. Hal ini membuat Suricata Malware Command dan Control Channel tidak seperti yang lain. Saluran off HTTP CnC, yang biasanya meluncur tepat oleh sebagian besar sistem IDS, di Suricata ini merupakan hal yang mudah! Selain itu, berkat kata kunci khusus anda dapat mencocokan field protokol yang berkisar dari http URI sampai SSL certificate identifier.
- Identifikasi File, MD5 Checksum, dan File Extraction - Suricata dapat mengidentifikasi ribuan jenis file yang melintasi jaringan anda! Tidak hanya dapat anda mengidentifikasi, tetapi jika anda memutuskan anda ingin melihat lebih jauh anda dapat menandai untuk diekstraksi dan file akan ditulis ke disk dengan file data meta yang menggambarkan situasi penangkapan dan aliran. MD5 checksum file dihitung dengan cepat, jadi jika anda memiliki daftar md5 hash yang anda ingin menyimpan dalam jaringan anda, atau ingin mencegah, Suricata dapat menemukannya.

Gambar 9 Suricata

2.7 Fail2ban

Fail2ban adalah sebuah aplikasi yang mencegah alamat IP dari login ke SmartVPS Linux anda setelah terlalu banyak upaya login gagal. Karena login yang sah biasanya tidak lebih dari 3 kali mengulang (dan dengan kunci SSH, tidak lebih dari 1 kali), server yang spammed dengan login gagal menunjukan upaya jahat untuk mengakses Linode Anda.

Fail2ban dapat memonitor berbagai protocol termasuk SSH, HTTP, dan SMTP. Secara default, Fail2ban memonitor SSH saja, dan merupakan penghalang kemanan yang membantu untuk setiap server karena daemon SSH biasanya dikonfigurasi untuk berjalan terus-menerus dan mendengarkan koneksi dari remote IP addres.

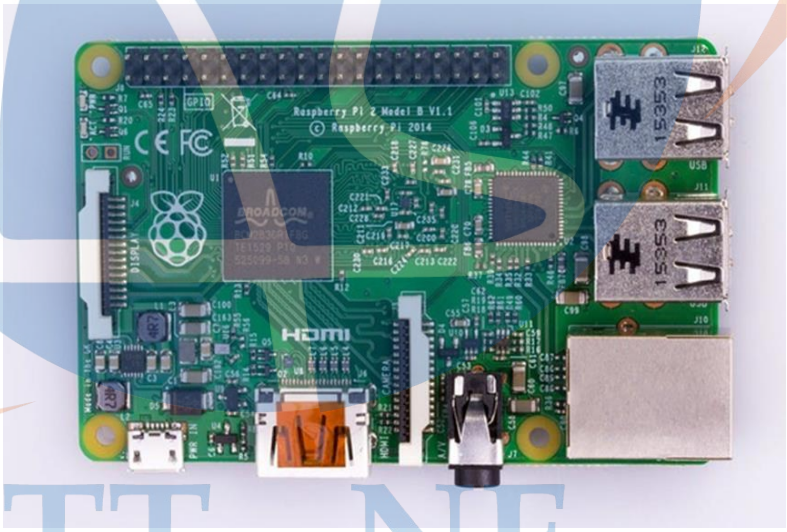
Gambar 10 Fail2ban

2.8 Raspberry Pi

Raspberry PI adalah komputer mini berukuran kartu yang dapat beroperasi dengan baik pada listrik atau daya baterai. Raspberry menyediakan berbagai Sistem Operasi (OS), ada berabagai varian ARM Linux lainnya yang dapat berjalan di Raspberry ini. Raspberry PI 2 model B (Versi terbaru dari Hardware ini) memiliki 1 gigabyte (GB) Random Acces Memory (RAM), Prosesor ARM Quad-core 900Mhz, Empat USB, Port Ethernet, USB mini untuk sumber power dan High Definition Multimedia Interface (HDMI) untuk tampilan. Perangkat yang berjalan dapat diakses secara langsung

menggunakan USB keyboard, mouse dan menampilkan atau melalui port LAN dengan menciptakan Secure shell (SSH) dengan sesi remote. Berikut ini merupakan spesifikasi pada Raspberry PI yang digunakan dan ditunjukan pada Gambar :

- A 900Mhz quad-core ARM Cortex-A7 CPU
- 1GB RAM
- 100 Base Ethernet
- 4 USB Ports
- 40 GPIO Pins
- Full HDMI port
- Combined 3,5mm audio jack and composite video
- Camera Interface (CSI)
- Display Interface (DSI)
- Mirco SD card slot
- VideoCore IV 3D graphics core



Gambar 11 Raspberry Pi

2.9 Penelitian Terkait

Dalam penelitian ini peneliti melakukan studi literature penelitian terkait, sebagai komparasi dan keterkaitan dengan masalah yang peneliti ambil. Hal ini bertujuan untuk mengetahui posisi penelitian yang dilakukan peneliti.

Daftar penelitian terkait yang peneliti temukan bisa dilihat ditabel dibawah ini.

Table 1 Penelitian Terkait

No	Judul Penelitian	Tahun	Kesimpulan
1	IMPLEMENTASI INTRUSION DETECTION SYSTEM(IDS) DI JARINGAN UNIVERSITAS BINA DARMA Oleh Maria Ulfa Dosen Universitas Bina Darma	2012	Berdasarkan hasil pengujian yang sudah dilakukan didapatkan bahwa serangan dapat terdeteksi atau tidak tergantung pada pola serangan tersebut ada didalam Rule IDS atau tidak.[12]
2	EVALUATION OF OPEN SOURCE INTRUSIN DETECTION SYSTEM (IDS) ON RASPBERRY PI Oleh Ar Kaw Kyaw Yuzhu Chen Justin Joseph Whitireia Community Polythechnic	-	Berdasarkan hasil penelitian evaluasi performa dari Snort IDS dan Bro IDS, Snort memiliki performa yang lebih baik dibanding Bro IDS pada Raspberry Pi2.[13]
3	PERANCANGAN DAN IMPLEMENTASI INTRUSION PREVENTION SYSTEM(IPS) DENGAN MIKROTIK ROUTER BERBASIS INTRUSION DETECTION SYSTEM(IDS) SURICATA Oleh Dede Setiawan	2017	1. Teknik untuk mencegah intrusion berbasis jaringan (network based) dapat dilakukan dengan menempatkan IDS dititik yang strategis didalam sebuah jaringan. 2. Metode pendeteksian intrusi dapat diakukan dengan berbasis SignatureBased yaitu bekerja dengan cara mencocokan rule dengan traffic yang ada 3. Teknik pencegahan intrusi dapat dilakukan dengan cara menggunakan firewall external (mikrotik) sebagai memblokir IP address peneyrang dengan bantuan program trigger firewall yang akan membaca log intrusi yang dihasilkan oleh sensor IDS[3]