ANALISIS DAN PERANCANGAN *INTRUSION DETECTION SYSTEM* UNTUK KEAMANAN JARINGAN: STUDI KASUS DI LINGKUNGAN BPTI UHAMKA

SKRIPSI

Disusun untuk

Memenuhi Persyaratan Kelulusan Sarjana Teknik Informatika

Oleh:

Mohamad Baskoro Aji

1903015162

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH PROF. DR. HAMKA

JAKARTA

2024

HALAMAN PERSETUJUAN

ANALISIS DAN PERANCANGAN *INTRUSION DETECTION SYSTEM* UNTUK KEAMANAN JARINGAN: STUDI KASUS DI LINGKUNGAN BPTI UHAMKA

SKRIPSI

Dibuat untuk Memenuhi Persyaratan Kelulusan Sarjana Teknik

Oleh:
Mohamad Baskoro Aji
1903015162

Telah diperiksa dan disetujui untuk diajukan ke Sidang Ujian Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri dan Informatika UHAMKA
Tanggal, 15 Januari 2024

Pembimbing

Arafat Febriandirza, S.T., M.TI., Ph.D.

Mengetahui
Ketua Program Studi Teknik Informatika

Mia Kamayani, S.T., M.T.
NIDN. 0312028704

HALAMAN PENGESAHAN

ANALISIS DAN PENGEMBANGAN *INTRUSION DETECTION SYSTEM* UNTUK KEAMANAN JARINGAN: STUDI KASUS DI LINGKUNGAN BPTI UHAMKA

SKRIPSI

Oleh:

Mohamad Baskoro Aji

1903015162

Telah diuji dan dinyatakan lulus dalam Sidang Ujian Skripsi

Program Studi Teknik Informatika Fakultas Teknologi Industri dan Informatika UHAMKA

Tanggal, 30 Januari 2024

Pembimbing

Arafat Febriandirza, S.T., M.TI., Ph.D.

NIDN. 0224028603

Penguji 1

Ade Davy Wiranata, S.Kom., M.Kom

NIDN. 0325119302

Penguji 2

Zuhri Halim, S.Kom., M.Kom.

NIDN. 0313028602

Mengesahkan,
Dekan
Fakultas Teknologi Industri dan Informatika

Dr.Dr. Dan Mugisidi, S.T., M.Si.

NIDN. 0301126901

Mengetahui
Ketua Program Studi
Teknik Informatika

Mia Kamayani, S.T., M.T.

NIDN. 0312028704

KATA PENGANTAR

Assallamu'alaikum wa rohmatullahi wa barokaatuh, Puji Syukur kehadirat Allah SWT atas limpahan rahmat dan karunianya sehingga penulis dapat menyelesaikan skripsi yang menjadi persyaratan kelulusan program studi strata satu (S1) Teknik Informatika Fakultas Teknologi Industri dan Informatika Universitas Muhammadiyah Prof. DR. HAMKA(UHAMKA).

Penulis menyadari bahwa dalam penulisan skripsi yang berjudul "Analisis dan Pengembangan *Intrusion Detection System* Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA" ini masih jauh dari kata sempurna.Penyusunan skripsi ini tidak lepas dari keterlibatan beberapa pihak.Oleh karena itu, Penulis mengucapkan terima kasih kepada:

1. Dr. Dan Mugsidi, S.T., M.Si., Selaku Dekan Fakultas Teknik Industri dan Informatika UHAMKA
2. Mia Kamayani, S.T.,M.T., Selaku Kepala Program Studi Teknik Informatika
3. Arafat Febriandirza, Ph.D, Selaku Dosen Pembimbing yang telah membantu penulis menyelesaikan skripsi ini
4. Nuroji, M.Kom., Selaku pimpinan bagian server dan jaringan BPTI UHAMKA yang telah membantu secara teknis pengerjaan rancangan ini
5. Keluarga saya, terutama ibu dan kakak saya yang telah banyak membantu dari awal perkuliahan hingga akhir perkuliahan ini
6. Teman Kuliah maupun Teman Online yang telah mendukung ketika terjadi kesulitan saat penulisan skripsi ini
7. Sandy Maulana, selaku teman saya yang telah membantu dengan basic networking dan menyelesaikan beberapa permasalahan pada penelitian ini.
8. Semua pihak yang sudah membantu dalam penyusunan skripsi ini

Jakarta,30 Januari 2024

Mohamad Baskoro Aji

PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Prof. DR. HAMKA (UHAMKA), saya yang bertandatangan di bawah ini:

Nama : Mohamad Baskoro Aji

NIM : 1903015162

Program Studi : Teknik Informatika

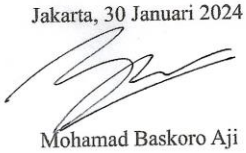
Menyetujui, memberikan Hak Bebas Royalti Noneksklusif (non-exclusive royalty free right) kepada Universitas Muhammadiyah Prof. DR. HAMKA (UHAMKA) atas karya ilmiah saya beserta perangkat yang ada (jika diperlukan) yang berjudul:

Analisis dan Perancangan *Intrusion Detection System* Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA

Hak Bebas Royalti Noneksklusif ini Universitas Muhammadiyah Prof. DR HAMKA berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Jakarta, 30 Januari 2024



Mohamad Baskoro Aji

ABSTRAK

Analisis dan Pengembangan *Intrusion Detection System* Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA

Data adalah informasi informasi yang dimiliki oleh objek,variabel, dan entitas pada lingkungan yang dimana bisa berupa informasi informasi umum atau bahkan informasi rahasia.Pada zaman sekarang, internet digunakan untuk menyimpan data perorangan atau bahkan perusahaan yang dimana disimpan pada suatu server.Mengingat bahwa banyaknya pencurian data di internet dikarenakan kurangnya keamanan pada jaringan internet penyedia layanan maka dibutuhkan keamanan tambahan selain melalui *firewall*.Tidak terkecuali BPTI UHAMKA, BPTI UHAMKA merupakan badan pengembangan teknologi dan informasi di Universitas Muhammaddiyah Prof. Dr Hamka dan juga merupakan pusat data yang dimana terdapat data data sensitif universitas disana. Berdasarkan wawancara dengan kepala jaringan BPTI UHAMKA belakangan ini banyak terjadi serangan siber seperti *Port Scanning, DoS,* dan *Deface.* Maka dari itu firewall saja tidak cukup untuk mengamankan jaringan dan server pada BPTI UHAMKA. Oleh karena itu, IDS atau *Intrusion Detection System* merupakan salah satu metode untuk keamanan tambahan yang mendeteksi aktivitas mencurigakan pada sistem.Dengan menggunakan OPNsense dan suricata yang memiliki rules untuk mendeteksi pola serangan ke sistem lalu akan dibuat alerts untuk menginformasikan ke admin jaringan yang diharapkan dapat melakukan tindakan untuk mencegah serangan.Skenario pada pengujian ini menggunakan functionality test. Hasil dari functionality test didapatkan hasil berupa *log alerts* pada *webGUI* OPNsense dapat mendeteksi serangan seperti *Port Scanning,Brute Force*,dan *Web Crawling* tetapi saat 6 kali pengujian *DoS* masih menembus keamanan jaringan tersebut.

Kata kunci: Keamanan jaringan, *Firewall*, *Intrusion Detection System*, OPNsense.

Analysis and Development of *Intrusion Detection System* for Network Security: Case Study In The Environment of BPTI UHAMKA

Data is containing information of object, variable and enitity of the environment where it can be public information or secret information.Nowadays, internet is used for storing individual data or even company data which is stored in the server.Given that a lot of data stealing in the internet because lack of network security from service providers then additional security is needed apart from firewall.no expection for BPTI UHAMKA, BPTI UHAMKA is a information and technology development agency and also the university data center where there is a lot of sensitive data.Based on interview result with head of network section, BPTI UHAMKA had a lot of cyber attack lately such as Port Scanning, DoS, and Deface.Therefore,firewall alone are not enough for securing network and server in the BPTU UHAMKA. IDS or Intrusion Detection System is one of the method for additional security that detects suspicious activity from the system.With OPNsense and suricata that have rules to detect attack pattern to the system then it create alerts for network admin that is expected to take action for mitigate attack.Scenario for the test using functionality test.The result of functionality test is alert in webGUI OPNsense can detect Port Scanning, Brute Force, and Web Crawling but after 6 times DoS testing OPNsense still penetrate network security.

Keyword: Network Security, Firewall, *Intrusion Detection System,* OPNsense.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Data adalah informasi informasi yang dimiliki oleh objek,variabel, dan entitas pada lingkungan yang dimana bisa berupa informasi informasi umum atau bahkan informasi rahasia. Server adalah sebuah komputer yang memiliki spesifikasi tinggi dan penyimpanan besar yang akan digunakan untuk melayani klien seperti menyimpan data (Marta et al., 2020).Pada zaman sekarang, orang orang menggunakan internet untuk menyimpan dan mengirim data bahkan data penting pada server, tetapi karena kemajuan teknologi ada orang orang yang menyalahgunakan internet dengan serangan siber untuk mengacaukan server,membuat server down,dan membuat server tidak bejalan dengan baik seperti Denial of Service atau DOS (Herniati, 2022).DoS ini bermula ketika penyerang mendapatkan celah port terbuka pada server atau jaringan yang membuat rentan terhadap serangan cara ini dinamakan Port Scanning yang dimana penyerang akan mencari kelemahan pada server atau jaringan dengan port terbuka lalu dari port yang terbuka itu akan bisa terjadi serangan serangan siber lainnya (NURILAHI et al., 2022).Maka dari itu, penggunaan server pada masa kini membutuhkan proteksi sebagai faktor vital dan perlu di perhatikan secara serius tujuannya untuk mencegah kerusakan fatal pada server saat terjadi serangan (Marta et al., 2020)

Dalam mengatasi kejahatan siber yang terjadi ke server dibutuhkan sistem yang memiliki *firewall* dan *Intrusion Prevention System* sebagai salah satu fitur pengamanan server yang dimana memblokir serangan dan melindungi isi dari server itu sendiri. *Intrusion Detection System* merupakan sistem pendeteksian ancaman yang ada pada tools OPNsense suricata dan OPNsense merupakan open source operating system dengan berbasis FreeBSD(Adha et al., 2021)

BPTI UHAMKA merupakan singkatan dari Badan Pengembangan Teknologi Informasi Universitas Muhammadiyah Prof. Dr. HAMKA.Badan ini setingkat dengan fakultas yang dimana memiliki fungsi sebagai pengembang informasi teknologi di Universitas Muhammadiyah Prof. Dr. HAMKA.Selain itu juga BPTI UHAMKA menjadi pusat data server dari semua Fakultas Fakultas di Universitas Muhammadiyah Prof. Dr. HAMKA.Beberapa fungsi lain dari BPTI UHAMKA pemeliharaan dan pengembangan jaringan di UHAMKA, merencanakan an

mengembangkan,serta memelihara aplikasi dan database universitas serta mengembangkan website Universitas dan Fakultas dan memutahkhirkan informasi secara berkala.

Karena pentingnya BPTI UHAMKA yang dimana terdapat data data penting seperti data mahasiswa, data keuangan, data dosen, data rektor,dan juga data penting lainnya maka dibutuhkan perlindungan secara fisik maupun secara digital.Perlindungan secara fisik seperti perlindungan pada fisik servernya mulai dari lingkungan, ruangan, dan perawatan fisik secara berkala.Lalu perlindungan digital seperti perlindungan dari serangan siber dimana serangan siber bisa mempengaruhi fisik dari *servernya* juga.

Banyaknya kejahatan siber yang terjadi terutama yang di BPTI UHAMKA dibutuhkan sebuah keamanan jaringan berupa pendeteksi penyusup walaupun adanya tindakan preventif berupa *firewall* yang cara kerjanya seperti *behaviour-based* tetapi tetap memungkinkan adanya serangan karena cara kerja *behaviour-based* merupakan mendekteksi anomali. Dari Hasil wawancara dengan narasumber yaitu kepala jaringan BPTI UHAMKA didapatkan permasalahan yaitu banyaknya serangan atau ancaman siber pada BPTI UHAMKA seperti *Port Scanning, DDoS* dan *Deface* yang masih ditanggulangi oleh sistem *behavior-based* karena *behavior-based* sangat bergantung pada admin jaringan yang harus selalu memantau maka dibutuhkan sistem baru yang dimana menggunakan sistem otomatis yaitu *knowledge-based* agar memudahkan admin dalam menanggulangi ancaman ancaman jaringan yang ada. Maka dari itu, penulis melakukan penelitian yang dimana menggunakan cara kerja *Knowledge Based* yang berupa pencocokan dengan yang ada di *database* IDS. Maka dari itu penulis ingin melakukan penelitian dengan judul "**ANALISIS DAN PERANCANGAN *INTRUSION DETECTION SYSTEM* UNTUK KEAMANAN JARINGAN: STUDI KASUS DI LINGKUNGAN BPTI UHAMKA**" dan berdasarkan penelitian terdahulu, penulis mengambil referensi yang ada sebagai landasan teori yang cocok dalam mendukung penilitian skripsi ini.

1.2 Perumusan Masalah

Berdasarkan Latar Belakang maka didapatkan rumusan masalah:

1. Bagaiman cara merancang keamanan jaringan pada lingkungan BPTI UHAMKA dengan *Intrusion Detection System* pada OPNsense?

2. Bagaimana hasil Analisa dan rancangan keamanan jaringan dengan *Intrusion Detection System* pada OPNsense?

1.3 Batasan Masalah

Untuk menghindari luasnya pembahasan atau pembahasan yang diluar lingkup penelitian maka ada beberapa batasan penelitian:

1. Aplikasi yang digunakan adalah Oracle VirtualBox
2. OS yang digunakan pada VirtualBox hanya FreeBSD(OPNsense) dan Kali Linux
3. Uji coba menggunakan penetration test berupa port scanning, web crawl, dan brute force
4. Hanya menggunakan fitur *Intrusion Detection System* pada OPNsense

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini sebagai berikut:

1. Mendapatkan hasil berupa bentuk rancangan jaringan untuk *Instrusion Detection System* pada ancaman serangan siber di *server* BPTI UHAMKA.
2. Memberikan penjelasan dan menganalisa hasil simulasi berupa *alerts* pada *Intrusion Detection System*.

1.5 Manfaat Penelitian

Adapun manfaat penelitian yang berguna untuk instansi BPTI UHAMKA sebagai berikut.Adanya rancangan keamanan jaringan terbaru untuk mendeteksi dini serangan ke jaringan BPTI UHAMKA yang mungkin suatu saat akan dilakukan implementasi ke jaringan tersebut. Sehingga admin atau petugas yang bekerja di bagian jaringan akan bergerak cepat untuk menanggulangi serangan siber ke jaringan.

1.6 Sistematika Penulisan

Untuk memudahkan pemahaman dan pengenalan terhadap isu-isu yang dibahas dalam skripsi ini secara menyeluruh, perlu diuraikan kerangka dan panduan penulisan skripsi. Struktur penulisan yang digunakan dalam penyajian laporan skripsi ini dapat dijelaskan sebagai berikut:

1. **BAB 1. PENDAHULUAN**

   Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan skripsi.

2. **BAB 2. TINJAUAN PUSTAKA**

   Bab Tinjauan Pustaka ini meliputi kerangka teori, landasan teori yang berisi pembahasan yang relevan dengan penelitian ini, dan penelitian terdahulu yang relevan berserta kelebihan dan kekurangan.

3. **BAB 3. METODOLOGI**

   Dalam bab ini penulis mengemukakan tentang metode penelitian yang dilakukan oleh penulis dalam pengembangan sistem informasi. Agar sistematis, bab metode penelitian meliputi :

   A. Identifikasi masalah
   B. Analisa kebutuhan
   C. Alur penelitian (disertai FlowChart)
   D. Pemilihan lokasi dan waktu penelitian

4. **BAB 4. PEMBAHASAN**

   Dalam bab ini terdapat hasil hasil dari awal perancangan hingga akhir dan analisa singkat dari penulis.

5. **BAB 5. SIMPULAN**

   Dalam bab ini terdapat kesimpulan dan saran yang akan diberikan oleh penulis

BAB 2. STUDI PUSTAKA

2.1 Landasan Teori

Sebelum penulis melakukan penelitian ada baiknya penulis memberikan landasan landasan teori yang relevan pada penelitian maka dari itu berikut adalah landasan teori penelitian ini:

2.1.1 Keamanan Jaringan

Pada keamanan jaringan terdapat 3 prinsip yaitu CIA triad yaitu *Confidentiality, Integrity*, dan *Availability*(Zarkasyi, 2018) .

1. *Confidentiality*

   Adalah salah satu konsep untuk menjaga otorisasi dan kerahasiaan informasi agar tidak bocor ke pihak yang tidak mempunyai hak akses kepada informasi tersebut.

2. *Integrity*

   Adalah konsep untuk menjaga informasi dari perubahan informasi yang tidak memiliki izin akses dan menjamin keaslian informasi yang tidak dapat diganggu gugat.

3. *Availability*

   Availability merupakan konsep ketiga dari keamanan jaringan dimana akses infomasi dapat dipercaya dan diandalkan.

2.1.2 OPNsense

OPNsense adalah salah satu *software open source,firewall* dan *platform* yang memiliki *operating system* FreeBSD dimana digunakan dengan CLI (*Command Line Interface*) yang mudah digunakan dan mudah di konfigurasi. (Adha et al., 2021).OPNsense juga terdapat fitur fitur seperti *rules* komersil dan berbayar dan OPNsense juga merupakan GPL GNU yaitu *General Public License* yang merupakan lisensi dari perangkat lunak yang bebas atau gratis, sedangkan GNU merupakan sistem dari perangkat lunak bebas atau *Freeware*.Salah satu fitur fitur OPN sense merupakan WebGUI dimana banyak terdapat fitur seperti *Firewall*, *Routing*, *Web Filtering*,VPN, dan bahkan nginx server (Fauzan & Purwanto, 2021).

2.1.3 Firewall

Firewall adalah suatu aturan atau rules yang bisa diterapkan di software,hardware, dan bahkan di sistem dengan tujuan untuk melindungi, baik melakukan seleksi dan membatasi dan melindungi jaringan itu sendiri (Adha et al., 2021). Umumnya *firewall* dibuat untuk melindungi *Local Area*

Network(LAN) terhadap gangguan dari luar karena mengingat potensi serangan dari luar sangat luar biasa besar.Dengan begitu *firewall* dapat digunakan untuk melindungi data di dalam jaringan *Firewall* merupakan pendekatan keamanan yang mengimplementasikan kebijakan keamanan yang lebih luas seperti mendefinisikan akses dan servis yang diizinkan.*Firewall* menerapkan kebijakan ini dalam suatu bentuk konfigurasi pada jaringan seperti melakukan autentikasi yang kompleks.(Fauzan & Purwanto, 2021).

2.1.4 Intrusion Detection System

Intrusion Detection System merupakan sistem otomatis yang mengawasi lalu lintas jaringan dalam sebuah sistem, memberikan peringatan kepada admin jaringan jika pola tersebut sesuai dengan yang tercatat dalam database aktivitas mencurigakan. IDS memiliki dua kategori, yaitu:(Zarkasyi, 2018)

1. *Network-based intrusion detection system*(NIDS)

   Network-based intrusion detection system adalah metode di mana seluruh lalu lintas dalam suatu jaringan dianalisis untuk mendeteksi upaya serangan terhadap jaringan tersebut. Kekurangan dari NIDS adalah kesulitan implementasinya dalam suatu jaringan.

2. *Host-based intrusion detection system* (HIDS)

   Host-based intrusion detection system adalah melibatkan pemantauan aktivitas host dalam jaringan untuk mendeteksi potensi serangan. Jenis sistem ini lebih fokus pada perlindungan host dengan menetapkan aturan yang lebih sesuai dengan kondisi khusus host.

Cara kerja dari IDS ada 2 yaitu *knowledge-based* dan *behavior-based* yang akan di paparkan sebagai berikut(Zarkasyi, 2018):

1. *Knoweldge-Based*

   Knowledge-based pada IDS memiliki cara kerja dengan mengenali adanya penyusup dengan cara menyadap paket data,kemudian akan dibandingkan dengan database rule pada IDS.*Database rule* berisi tanda tanda paket serangan,jika polanya sama maka akan dianggap sebagai sebuah serangan.

2. *Behavior-based*

Behavior-based adalah cara kerja IDS dengan mendeteksi anomali atau keanehan yang terjadi pada system yang seharusnya berjalan normal.Contohnya: pelonjakan memori atau CPU usage yang melebihi batas normal secara terus menerus.

2.1.5 Suricata

Suricata adalah sebuah *firmware intrusion detection and prevention system* atau IDPS yang dimana didalamnya terdapat fitur IDS dan IPS yang berbasis open ssource yang mana dikembangkan oleh komunitas non-profit yaitu Open Information Security Foundation(OISF) (Efrando et al., 2019). Suricata dibuat sebagai sistem multithread yang bisa memanfaatkan beberapa core.IDS pada suricata ketika ada serangan akan menghasilkan alert saja dan adapun fitur fitur dari suricata yaitu, Multi Threading, Performance Statistics, Automatic Protocol Detection, Gzip Decompression, Independent HTP Library, Standart Input Methods, Unified2 Output, Flow Variables, Fast IP matching, HTTP Log Module, GPU Acceleration, IP Reputation, dan Flowint (Alamsyah et al., 2020).

2.1.6 Web Server

Web Server merupakan perangkat lunak yang menjadi pondasi dari world wide web (www). Cara kerja web server yaitu dengan menunggu permintaan client dari browser jika ada permintaan dari web browser akan langsung di proses permintaan tersebut yang memiliki hasil berupa data yang diinginkan oleh client. Salah satu web server yang bersifat open source adalah apache yang biasa digunakan untuk melayani dan mengatur fasilitas web(Raharjo, 2020). Apache merupakan perangkat lunak dari web server untuk mengatur websites yang di jalankan pada server.Web server menjadi perantara antara server fisik dan client yang dimana web server menarik kontek dari server setiap user memberikan request dan menampilkannya pada web(Putro & Supono, 2022).

2.1.7 Denial Of Service

Denial-of-Service merupakan sebuah metode serangan siber yang dimana pelaku berupaya membuat sumber daya jaringan pada server tidak tersedia kepada client dengan cara mengganggu layanan host dengan internet(Adha et al., 2021).Serangan DoS ini biasanya

melakukan *flooding* ke server atau jaringan vital.Ada beberapa jenis serangan DoS yaitu (Fitri Nova et al., 2022):

1.UDP Flooding

Serangan ini akan melakukan pengiriman paket UDP secara masif kepada target agar komputer target sulit menangani request data dalam jumlah yang sangat besar.

2. SYN flooding

Serangan ini dilakukan ketika dua komputer saling berhubungan atau handshake. Serangan ini mengirimkan paket SYN/ACK dimana penyerang akan memberikan pesan "SYN/ACK" secara masif yang dimana perlu dilakukan *acknowledge* (ACK) oleh korban yang membuat *timed-out* pada koneksi.

3.ACK flood

Serangan ini membebani dengan paket TCP ACK yang dimana penyerang akan mengirimkan data sampah secara masif sehingga server tidak bisa melayani user yang sah.

4.HTTP flood

Serangan ini menggunakan *request* HTTP yang masif agar bisa membuat server down.

5. ICMP flood

Serangan ini akan membanjiri *request* ICMP dengan sangat cepat tanpa menunggu respon korban. Pada jenis ini bandwidth yang masuk dan keluar terkena dampaknya yang mengakibatkan keterlambatan.

2.1.8 DoS Testing Tools

Tools pada *DoS testing tools* menjadi salah satu alat yang membantu pada penelitian ini berikut adalah *DoS testing tools* yang digunakan pada penelitian ini:

1. Slowloris

Slowloris merupakan salah satu serangan DoS dengan cara ekploitasi HTTP *protocol* dengan cara membuat banyak permintaan yang tertunda ke target web server.Sebagai tambahan, Slowloris merupakan penopang dari perkembangan berbagai macam serangan

seperti *SlowComm, Slow Next Attack, Slow Read Attack, dan Slowreq Attack.* Semua Serangan tadi merupakan serangan rendah dan lambat atau *Low and Slow Attack* karena Slowloris terkenal karena serangan DoSnya yang lambat.Serangan Slowloris berupa request HTTP yang tidak lengkap dan mengakibatkan timeout pada server yang akan dikirim terus menerus(Sabri et al., 2021).

2. Low Orbit Ion Cannon

LOIC atau *Low Orbit Ion Cannon* merupakan sebuah *stress testing tools* yang dimana akan melakukan tes seberapa kuat server menampung *packet*.Semenjak menjadi open-source aplikasi ini sering menjadi alat untuk melakukan DoS dan salah satu penerusnya yaitu *High Orbit Ion Cannon* memiliki cara kerja yang sama dan keduanya memiliki Interface yang mudah digunakan.Kedua aplikasi ini tersedia secara legal karena aplikasi ini diklaim hanya untuk melakukan *stress testing* (Sandkühler, 2020)

2.1.9 Penetration Testing

Penetration Testing merupakan tes keamanan yang dimana seorang ahli jaringan merencanakan, membuat,dan mengevaluasi sebuah serangan siber untuk mencari letak kelemahan yang ada pada sistem komputer atau jaringan.Tujuannya agar mengetahui atau mengidentifikasi celah keamanan pada sistem yang biasanya penyerang mengambil keuntungan dari celah keamanan tersebut untuk tujuan tertentu(Aqra & Di, 2023).Ada 7 bagian ketika melakukan penetration testing sebagai berikut(Astrida et al., 2022):

1. Persiapan

Pada bagian ini bertujuan untuk memberikan dan menjelaskan *tools* dan teknik yang membantu pada tahapan persiapan *penetration testing*.Informasi didapatkan melalui berbagai sumber seperti dari pengalaman sang tester yang telah melakukan tes ini.Tahapan ini menjadi sangat penting karena penetration testing tidak selalu harus agresif, karena peneteration testing tidak selalu sedang diretas tetapi mengidentifikasi resiko bisnis yang mungkin akan di serang.

2. Pengumpulan informasi

Pada tahapan ini, mengumpulkan informasi tentang pentesting. Tujuannya agar informasi yang didapatkan berguna untuk desain serangan yang akan dilakukan sesuai dengan persetujuan dengan target

3. *Threat Modelling*

Pada tahapan ini, akan di identifikasi pendekatan model ancaman yang digunakan untuk pentesting. Focus dari standard ini tergantung pada proses bisnis perusahaan dan assetnya. Threat modelling ini sangat penting untuk tester dan perusahaan karena dari modelnya akan memberikan kejelasan pada risiko dan prioritas target.

4. Analisa Kerentanan

Pada tahapan ini, tester mencari celah kerentanan pada sistem yang mungkin akan dimanfaatkan oleh penyerang.

5. Exploitation

Pada tahapan ini diadakan uji penetrasi yang memiliki fokus pada akses ke sistem atau sumber daya dengan melewati keamanan. Fokusnya untuk mengidentifikasi titik masuk utama penyerang.

6. Post Exploitation

Pada Tahapan ini, Tujuannya adalah menentukan sebuah nilai untuk mempertahankan control dari sistem.

7. Reporting

Pada Tahapan ini, tester melaporkan yang berisi hasil pengujian dan deskripsi dari hasil pengujian beserta tata cara penyelesaiannya.

2.1.10 Penetration Testing Tools

Tools menjadi salah satu alat pembantu penelitian ini,berikut adalah *tools* yang akan digunakan dalam penelitian ini:

1. Nmap

Nmap atau *Network Mapper* merupakan alat atau *tools* untuk melakukan pengintaian dan melakukan audit terhadap network security.Nmap juga merupakan *free open source software*.Nmap menggunakan paket IP raw untuk mendeteksi host yang terkoneksi dengan jaringan biasanya terdapat informasi seperti OS dan jenis *firewall* yang digunakan.Nmap memilki output berupa table port yang berisi angka port dan *protocol*,

Skipfish merupakan *open source scanner* aplikasi web di program dengan Bahasa C yang dikembangkan oleh Google. Tujuan dari skipfish sama seperti nmap yaitu mencari kemungkinan masalah pada keamanan pada aplikasi/sistem. Skipfish juga bisa digunakan untuk mencari kerentanan pada aplikasi web yang mungkin akan di eksploit oleh penyerang dari luar(Mantra et al., 2019).

3. DirBuster

Dirbuster merupakan salah satu *tools* untuk menyerang aplikasi web yang menargetkan kepada aplikasi *file* dan *directory*.DirBuster menggunakan brute force untuk menyerang aplikasi *file* dan *directory* yang berisi informasi sensitif seperti konfigurasi aplikasi atau informasi penting seperti *user credentials*.Dirbuster akan memindai *directory file* secara terus menerus mencari apakah terdapat directory tersembunyi atau yang tidak memiliki hubungan ke aplikasi web(Daka & Banda, 2023).

2.2 Penelitian Terdahulu

Tabel 2- 1. Tabel Penelitian Terdahulu

No	Peneliti-Tahun	Judul	Metode	Kesimpulan
1	(Zarkasyi, 2018)	IMPLEMENTASI INTRUSION DETECTION SYSTEM SEBAGAI KEAMANAN JARINGAN PADA *Local Area Network*	Network Develpoment Life Cycle, Intrusion Detection System	bahwa pengujian Fucntionality Test Snort IDS berhasil mendeteksi beberapa serangan yang diujikan dan serangan tersebut dapat ditampilkan dalam bentuk grafik dalam

				tersebut dapat ditampilkan dalam bentuk grafik dalam bentuk splunk dan log peringantan yang terkirim via e-mail dan pengujian Response Time dibutuhkan waktu 4,5 detik atau <10 detik dan untuk peringatan ke e-mail memiliki rasio waktu sebanyak 29,17% untuk port scanning dan SSH brute force, 19,44% untuk FTP attack, dan 22,22% untuk DDoS attack.
2	(Alamsyah et al., 2020)	ANALISA KEAMANAN JARINGAN MENGGUNAKAN	Intrusion Detection and Prevention System	Konsep kerja IDPS dalam keamanan sebuah jaringan

		NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM		adalah mendeteksi dan mencegah adanya serangan pada jaringan komputer seperti port scanning, telnet, dan ftp
3	(Stephani et al., 2020)	Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server	Action Research, Intrusion Detection System	IDS dapat mendeteksi dan mencegah penyusup masuk ke *web server*
4	(Adha et al., 2021)	MEMBANGUN SISTEM KEAMANAN JARINGAN BERBASIS *FIREWALL* DAN IDS MENGGUNAKAN TOOLS OPNSENSE	Network Development Life Cycle, Intrusion Detection System	fitur *firewall* dan intrusion detection system (IDS) pada tools OPNsense dapat melindungi server dari serangan serangan seperti Port Scanning, DDoS, dan sniffing lalu sistem akan

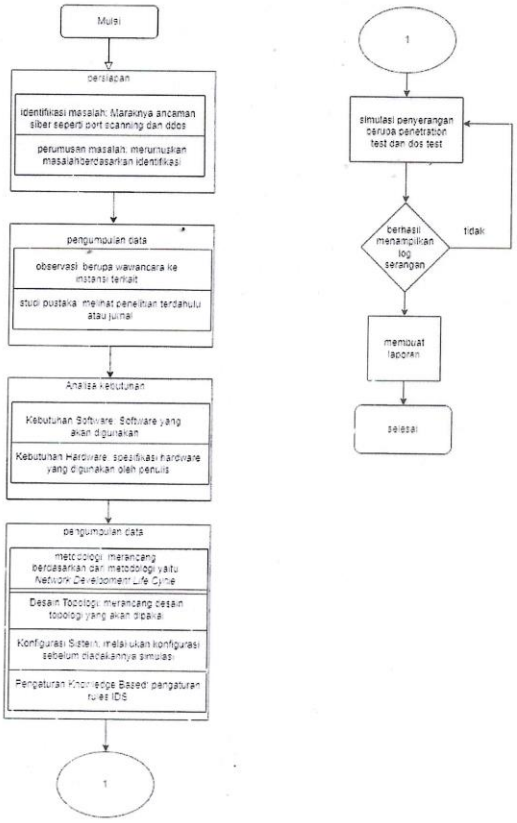
				mencatat log serangan dan mengirimkan notifikasi tentang adanya serangan.
5	(Herniati, 2022)	IMPLEMENTASI DAN ANALISA IDS (INTRUSION DETECTION SYSTEM) MENGUNAKAN SURICATA PADA WEB SERVER	Network Development Life Cycle, Intrusion Detection System	firmware suricata mampu memblokir serangan hping dimana serangan tersebut mengarah ke beberapa port tertentu dan pada serangan hping tertulis bahwa ada 100% packet loss yang dimana serangan berhasil di drop.

Dari penelitian sebelumnya yang terdapat pada tabel diatas perbedaan atau kelebihan dari penelitian ini hanya berupa pada objek penelitian yaitu pada BPTI UHAMKA.

BAB 3. METODOLOGI

3.1 FlowChart Penelitian

Agar penelitian dapat berjalan lancar dan terstruktur maka dibuat flowchart penelitian untuk memudahkan penulis.Berikut adalah *flowchart* dan metodologi *Network Development Life Cycle* yang digunakan untuk merancang keamanan jaringan dari penelitian ini beserta penjelasan dibawahnya:



Gambar 3. 1 Flowchart Penelitian

3.2 Penjelasan FlowChart

Dari *Flowchart* yang disajikan diatas penulis akan menjelaskan satu persatu alur penelitian yang akan dilaksanakan. Berikut adalah penjelasan dari *flowchart* sebagai berikut:

3.2.1 Persiapan

Pada bagian ini penulis akan menjelaskan persiapan apa saja yang dilakukan sebelum memulai penelitian

1. Identifikasi Masalah

   Identifikasi masalah pada penelitian ini yaitu dengan maraknya serangan siber belakangan Ini seperti port scanning dan DDoS yang biasanya digunakan untuk mengacaukan server yang dimana untuk saat ini pendeteksi keamanan masih menggunakan cara manual.

2. Perumusan Masalah

   Berdasarkan latar belakang penelitian ini, penulis dapat merumuskan permasalahan yaitu bagaimana membuat sistem keamanan jaringan yang dapat mendeteksi ancaman serangan secara otomatis.

3.2.2 Metodologi Pengumpulan Data

Metode pengumpulan data pada penelitian ini antara lain sebagai berikut:

1. Wawancara dengan kepala bagian jaringan pada BPTI UHAMKA.Metode melakukan wawancara kepada kepala bagian server BPTI UHAMKA ditujukan untuk meminta izin melakukan penelitian dan mengetahui apa saja permasalahan serangan siber yang ada pada bagian jaringan BPTI UHAMKA.

2. Studi Pustaka dimana dilakukan observasi pada buku, jurnal-jurnal, artikel, dan skripsi mahasiswa Fakultas Teknik UHAMKA terdahulu yang masih memiliki relevansi terhadap topik penelitian ini yang memiliki jarak maksimal 5 tahun.

3.2.3 Analisa Kebutuhan

Analisa kebutuhan yang akan digunakan saat penelitian, dikarenakan penelitian ini dilakukan di rumah dan menggunakan *virtual server* maka berikut adalah kebutuhan *Software* dan *Hardware* yang digunakan penulis:

1. Kebutuhan *Software*

Tabel 3- 1. Tabel Analisa Kebutuhan

No	Software	Jumlah	Keterangan
1	OPNsense	1	Software OPNsense dan suricata untuk monitoring dan Instrusion Detection System
2	VirtualBox	1	VirtualBox untuk konfigurasi server, kali linux dan OPNsense
3	Kali Linux	1	Kali Linux sebagai OS penyerang
4	Suricata	1	Firmware dari OPNsense
5	Ubuntu	1	Sebagai HTTP web server

2. Kebutuhan Hardware

Spesifikasi Komputer

Processor: AMD Dual-Core A9-9420 APU (3 GHz base frequency, up to 3.6 GHz burst frequency, 1 MB cache)

Memory: 8GB DDR4 – 2666Mhz(1x8 GB)

Video graphic: AMD Radeon™ R5 Graphics

Storage: 256GB SSD SATA III

Operating system: Windows 10 pro

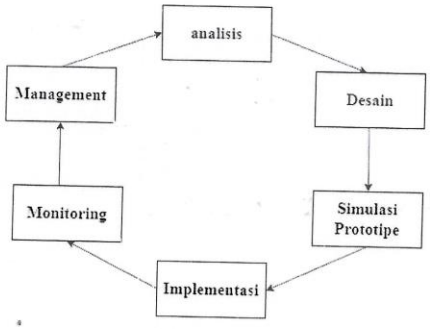
3.2.3 Perancangan Sistem

1. Metodologi

3.2.3 Perancangan Sistem

1. Metodologi

Metode yang digunakan untuk penelitian ini yaitu menggunakan *Network Development Life Cycle*(NDLC). NDLC adalah salah satu metode yang digunakan untuk jaringan yang dimana memiliki beberapa tahapan.



Gambar 3. 2 Diagram *Network Development Life Cycle*

(Referensi: (Putra et al., 2018))

A. Analisis

Melakukan analisa kebutuhan software dan hardware untuk mengembangkan IDS menggunakan OPNSense suricata.

B. Desain

Melakukan desain topologi pengembangan IDS menggunakan OPNsense suricata.

C. Implementasi

Melakukan konfigurasi pada *Rules Firewall* dan Rules IDS.

D.Monitoring

Melakukan pengawasan saat uji coba.

E. Management

2. Desain Topologi

Pada tahap ini penulis membuat perancangan topologi jaringan yang akan digunakan pada penelitian yang dibuat berdasarkan pengumpulan data yaitu observasi/wawancara dan dari landasan landasan ilmiah.

3.Konfigurasi

Pada tahap ini penulis melakukan konfigurasi pada *software* seperti OPNsense, suricata, LOIC, dan *software* lain yang menjadi pendukung dalam penelitian ini.

4. Pengaturan *Knowledge-Based*

Pada tahapan ini penulis akan membuat rules yang akan digunakan suricata IDS pada penelitian ini. Rules IDS ini berfungsi untuk mendeteksi secara otomatis ip penyerang.

3.2.5 Simulasi

Pada tahap ini adalah simulasi dari *intrusion detection system* yang sudah dirancang serta melakukan penarikan kesimpulan dari pengujian hasil serangan kepada IDS. Pengujian memiliki tahapan sebagai berikut:

1. Pada tahapan ini akan digunakan *Functionality Test* dimana penyerang akan melakukan beberapa serangan ke server yaitu *Penetration testing* dan *DoS testing* yang berada di Ubuntu menggunakan kali linux lalu melihat apakah IDS akan berhasil mendeteksi serangan yang terjadi dan akan menampilkan hasil berupa *log alerts* pada *WebGUI* OPNsense yang akan dilihat oleh admin *server* atau jaringan.

Dari parameter ini pengujian sistem dilakukan untuk mengukur keandalan dari sistem pendeteksi pada jaringan *Local Area Network* (LAN) yang dibuat.

3.3 Laporan

Pada tahapan ini penulis akan membuat laporan berdasarkan hasil Implementasi dan simulasi *intrusion detection system* yang telah dibuat.

3.4 Tempat dan Waktu Penelitian

Dalam meneliti sesuatu tentu memerlukan tempat dan waktu penelitian yang jelas maka dari itu berikut adalah penjelasan terkait tempat dan waktu penelitian sebagai berikut:

3.4.1 Tempat Penelitian

Tempat penelitian yaitu ada di kantor BPTI UHAMKA, jalan Tanah Merdeka, Jakarta Timur dan di rumah penulis sendiri.

3.4.2 Waktu Penelitian

Rencana kegiatan ini memerlukan waktu yang digunakan untuk menyelesaikan peneltian, sekitar 5 (lima) bulan dari mulai pengambilan data pada tanggal 1 Desember 2022 sampai 30 November 2023 yang diperlukan dan sampai proposal ini ditulis oleh penulis.

Tabel 3- 2. Tabel Waktu Penelitian

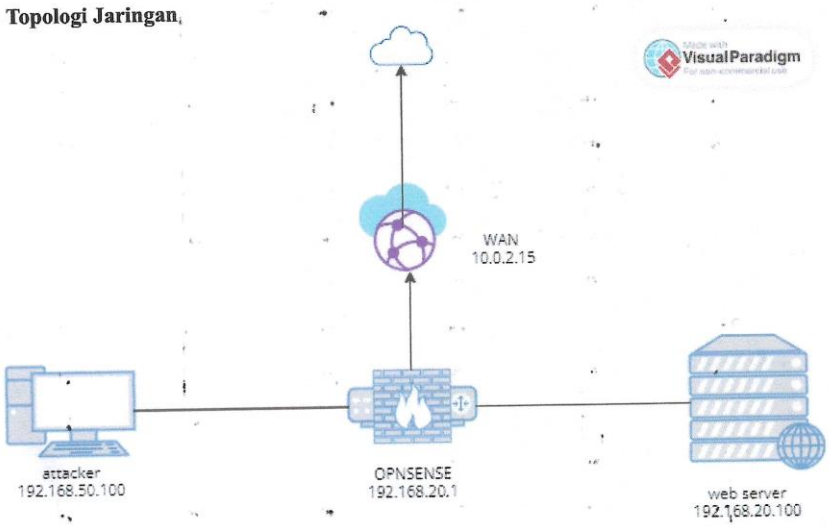
Kegiatan	Desember				Januari				Juni				Oktober				November			
	Minggu																			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Identifikasi Masalah																				
Pengumpulan Data																				
Studi Literatur																				
Perancangan Sistem																				
Pengujian Sistem																				
Pembuatan Laporan Akhir																				

BAB 4. HASIL DAN PEMBAHASAN

4.1 Perancangan

Sebelum melakukan pengujian dilakukan pengaturan awal yaitu perancangan. Perancangan pada penelitian ini terdapat perancangan topologi jaringan dan pengaturan awal pada OPNsense agar mendapatkan hasil yang diinginkan. Berikut adalah perancangan pada penelitian ini:

4.1.1 Topologi Jaringan



Gambar 4. 1 Topologi Jaringan

Pada topologi diatas terdapat beberapa komponen seperti PC *attacker* yang menggunakan OS kali linux, *Router* dan OPNsense sebagai *firewall*, dan yang terakhir *server* yang dilindungi.Disini penyerang akan melakukan *port scanning* lalu dilanjutkan dengan beberapa serangan seperti *DoS attack* dan *Penetration testing* yang ditujukan pada *web server* apache pada Ubuntu.

4.1.2 Instalasi dan Pengaturan Awal

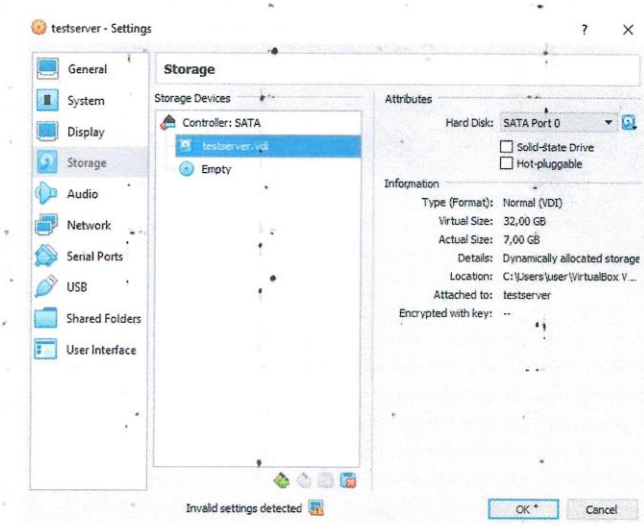
Pada Bagian ini terdapat penjelasan untuk instalasi dan perancangan *Intrusion Detection System*

1. Sebelum menginstall OPNsense berdasarkan topologi yang sudah dibuat, kita harus assign interface dari OPNsense tersebut pada virtualbox yang pertama adalah NAT, NAT disini

berfungsi sebagai WAN agar OPNsense dapat terhubung ke internet lalu ada internal network dengan 2 interface yang diasumsikan internal network pertama sebagai LAN dan internal network kedua sebagai attacker karena disini OPNsense bekerja sebagai router juga maka dari itu agar percobaan serangan berhasil attacker harus masuk melewati router dahulu jadi terdapat 3 interface yang terhubung ke router yaitu LAN yang nanti sebagai web server, attacker, dan WAN pada router OPNsense

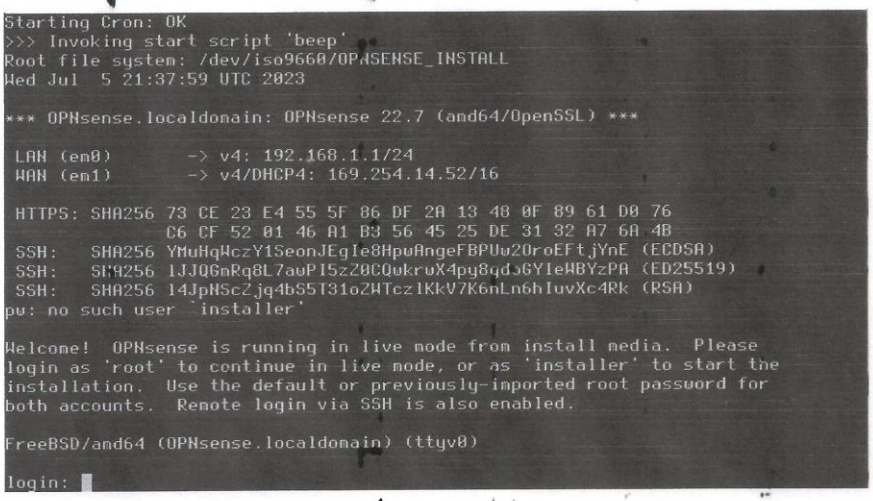
2. Untuk Instalasi OPNsense harus melakukan pengaturan pada network adapter pada Virtual Machinenya sebagai berikut:

A. Input CD yang berbentuk ISO untuk di install



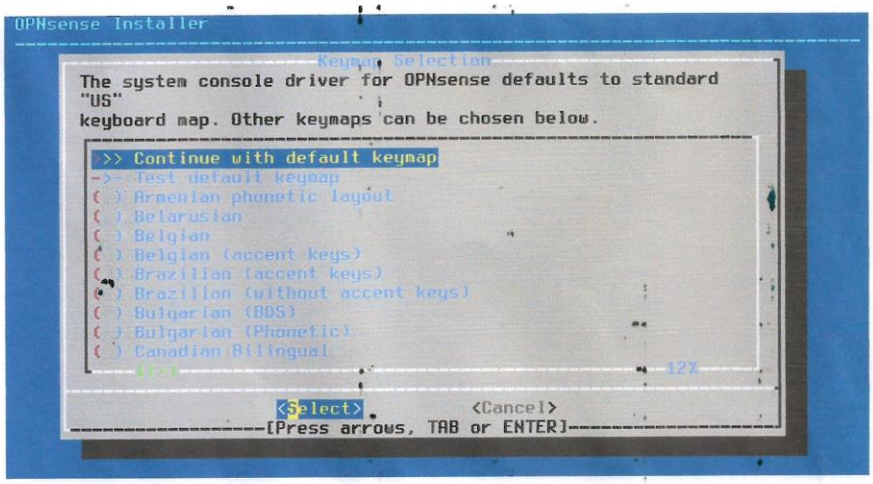
Gambar 4. 2 Input ISO OPNsense ke VirtualBox

C. Lalu jalankan Virtual Machine ketika sudah pada menu ini login dengan username "installer" dan password "opnsense"



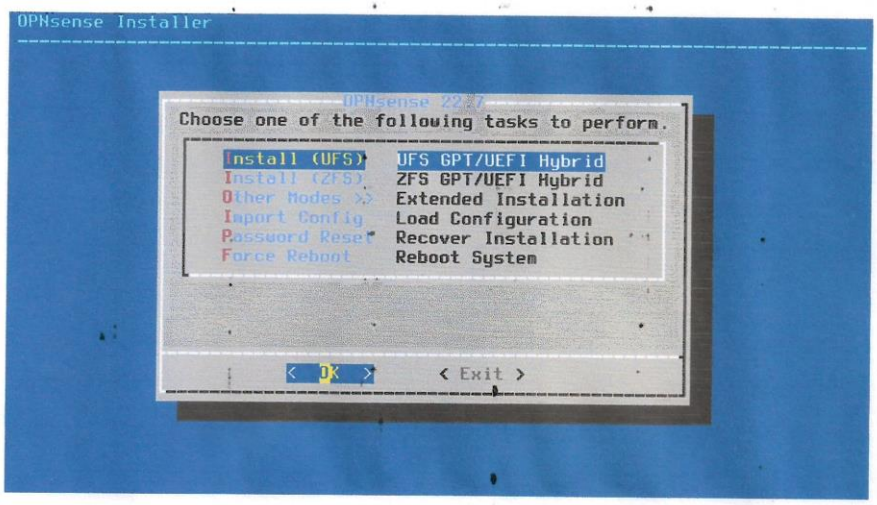
Gambar 4. 3 Tampilan Awal CLI OPNsense

D. Setelah itu masuk ke menu seperti ini pilih "Continue with default keymap"



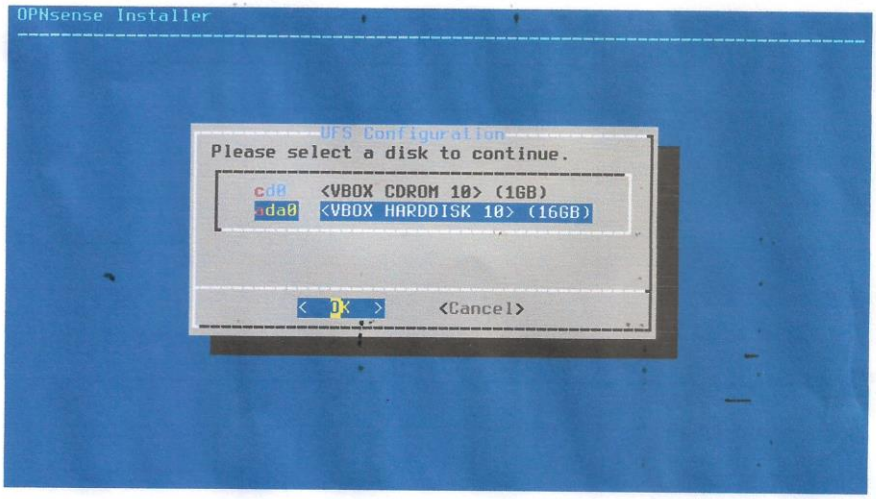
Gambar 4. 4 Instalasi OPNsense

E. Lalu install dengan UFS



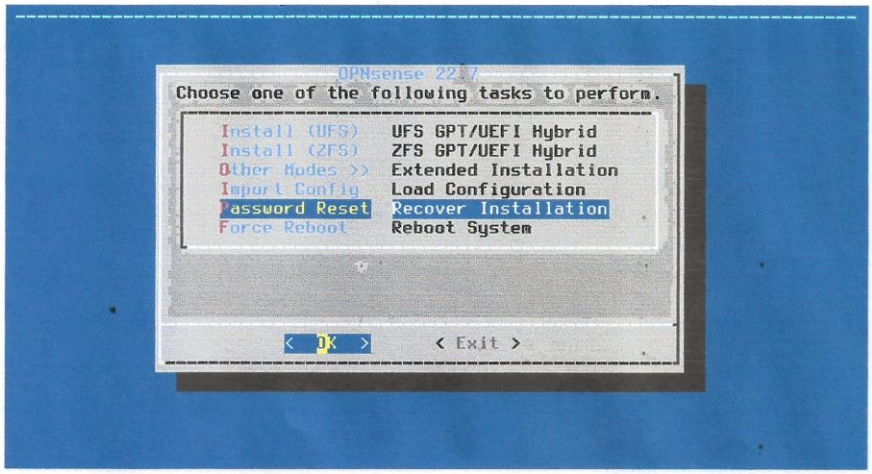
Gambar 4. 5 Install OPNsense dengan UFS

F. Pilih ada0 dengan vbox harddisk dan tunggu instalasi selesai.



Gambar 4. 6 Menggunakan ada0

G. Setelah instalasi selesai reset password dengan membuat user "root" dan password apa saja bisa 1234, tetapi disarankan password yang memiliki karakter unik.



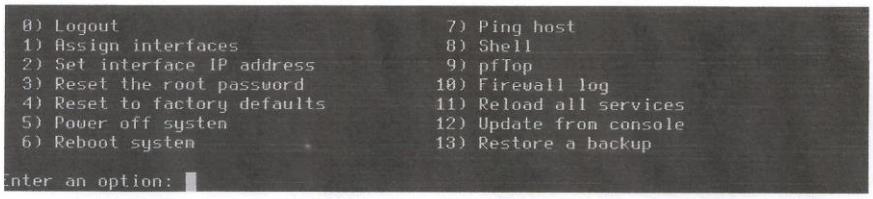
Gambar 4. 7 Reset Password OPNsense

H. Lalu masuk menu ini dengan menggunakan username dan password yang dibuat tadi

```
>>> Invoking start script 'newwanip'
Reconfiguring IPv4 on em1
Reconfiguring IPv4 on em0
>>> Invoking start script 'freebsd'
Starting suricata.
5/7/2023 -- 22:32:01 - <Info> - Including configuration file installed_rules.yam
l.
5/7/2023 -- 22:32:01 - <Info> - Configuration node 'rule-files' redefined.
5/7/2023 -- 22:32:01 - <Info> - Including configuration file custom.yaml.
>>> Invoking start script 'syslog'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Wed Jul  5 22:32:05 UTC 2023

*** OPNsense.localdomain: OPNsense 22.7 (amd64/OpenSSL) ***

 LAN (em1)       -> v4/DHCP4: 169.254.14.51/16
 WAN (em0)       -> v4/DHCP4: 10.0.100.4/24

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

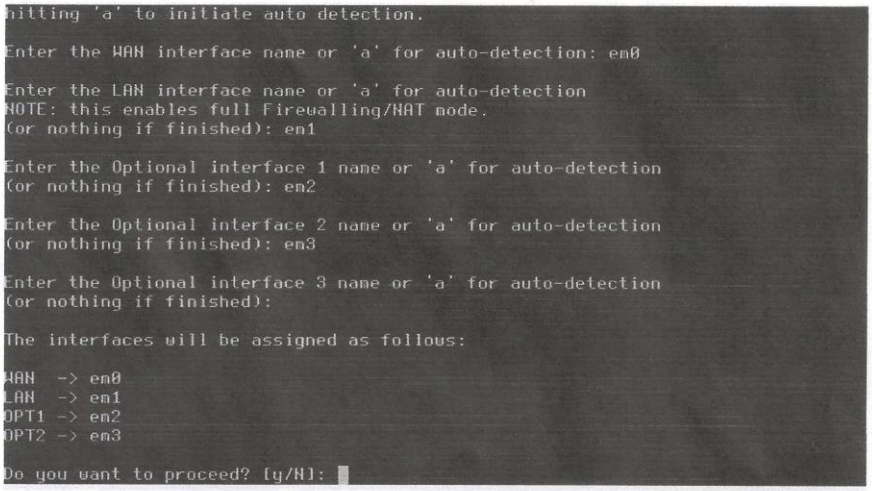
Gambar 4. 8 Tampilan Login setelah install

I.Karena interface masih berbentuk default bawaan maka dari itu butuh di setting ulang, jadi setelah melakukan login maka pilih pilihan pertama pada menu dibawah ini



Gambar 4. 9 Pilihan Saat Setelah Login

J. Lalu masukan seperti settingan dibawah ini dan press "y" disini tidak diperlukan LAGGs atau VLAN maka dari itu interface yang disetting akan seperti ini.



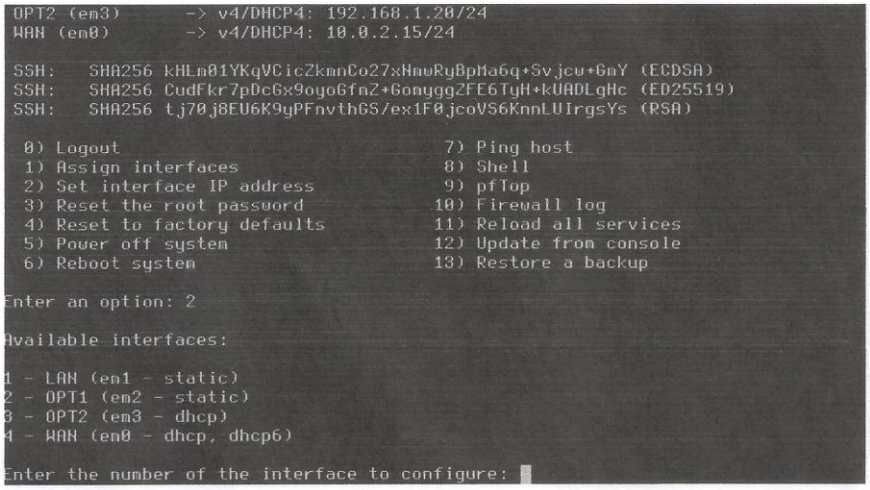
Gambar 4. 10 Setting Interface

K. Lalu setelah mengganti interface maka selanjutnya adalah mengganti IP interface seperti pada settingan dibawah ini dengan keterangan sebagai berikut

1) pada LAN em1 menggunakan static IP dengan gateway 192.168.20.1 lalu dengan start address 192.168.20.100 dan end address 192.168.20.200.

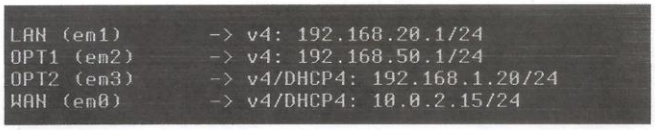
2) Pada OPT1 yang dimana ini di asumsikan sebagai IP *attacker* yang ada pada *router* menggunakan 192.168.50.1 sebagai *gateway* lalu dengan *start address* 192.168.50.100 dan *end address* 192.168.50.200.

3) Pada WAN menggunakan DHCP agar IP nya otomatis dapat dari NAT virtualbox.



Gambar 4. 11 Setting *IP address*

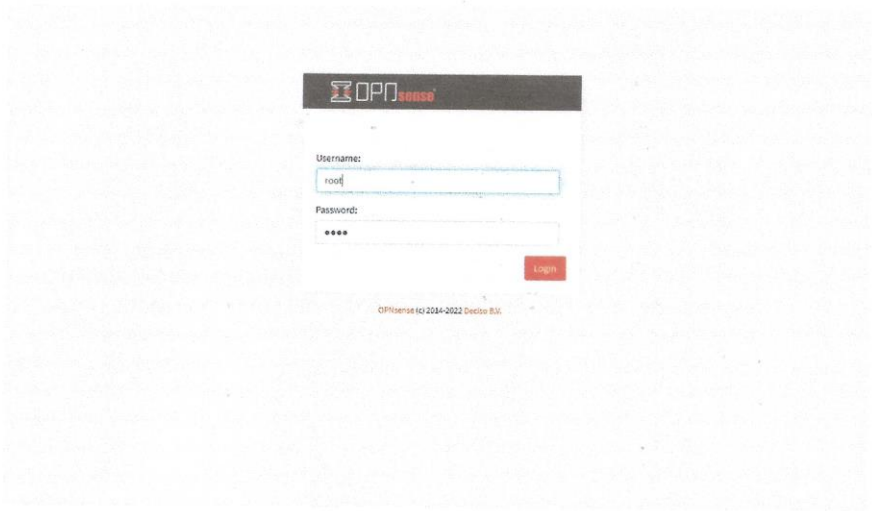
L. Setelah itu kita mendapatkan IP untuk LAN, *Attacker*,dan WAN



Gambar 4. 12 Hasil dari Setting *IP Address*

4.1.3 Pengaturan Web Gui OPNsense

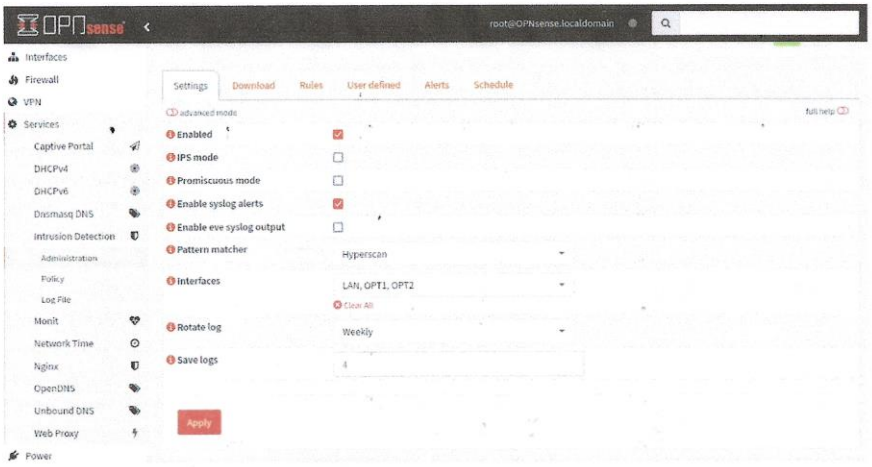
Pada pengaturan Web Gui OPNsense ini login dengan username dan password root yang sudah dibuat di awal



Gambar 4. 13 Halaman Login WebGUI

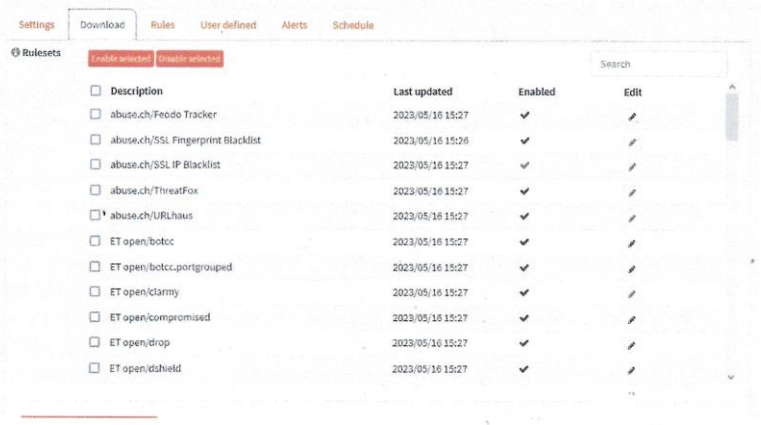
Lalu masuk services => *Intrusion Detection System* => Administration

Aktifkan *intrusion detection*, IPS mode dan Promiscuous mode.



Gambar 4. 14 Halaman IDS OPNsense

Lalu menuju download dan ceklis semua rules dan download lalu enable rules tersebut, agar opnsense dapat mendowload *rules* maka harus mengecek apakah opnsense *route* sudah terhubung ke WAN, saran dari penulis adalah jangan mencoba *download* dan *enable* semua rule sekaligus jika *resource* yang ada kurang mumpuni dalam hal ini adalah komputer dari penulis karena akan mengakibatkan *timeout* dan memerlukan waktu yang lama ketika akan *apply setting* pada *intrusion detection system* maka dari itu penulis hanya menggunakan 2 *rulesets* yaitu ET open/emerging-scan dan ET open/emerging-dos.



Gambar 4. 15 Rules yang di download

4.2 Hasil Pengujian

1. Sebelum pengujian menggunakan *penetration testing tools* dan *stress testing tools* harus dilakukan *port scanning* agar mengetahui apakah ada *port* yang terbuka atau tidak, disini *port web server* berjalan di port 80 pada *web server* ubuntu

2. Setelah itu jalakan kali linux pada virtualbox lalu install nmap dengan command jika pada kali linux belum terdapat aplikasinya "sudo apt install nmap" .Nmap seharusnya sudah menjadi aplikasi bawaan kali linux saat menginstall OS tersebut setelah itu gunakan "sudo nmap –v –A –sV IP target, disini IP sesuai dengan IP *webserver* yaitu 192.168.20.100 dan terdapat *open port* yaitu *port* 80

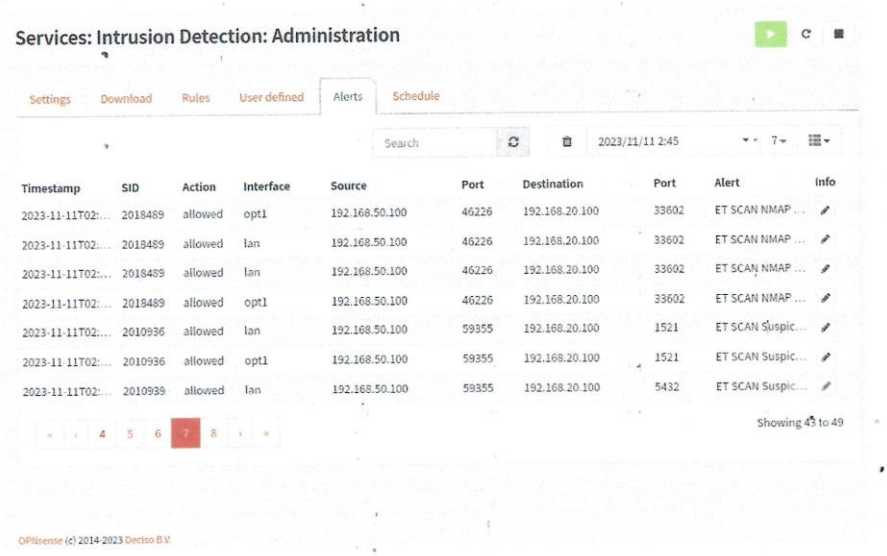
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -A -sV 192.168.20.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 14:45 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:45
Completed NSE at 14:45, 0.00s elapsed
Initiating NSE at 14:45
Completed NSE at 14:45, 0.00s elapsed
Initiating NSE at 14:45
Completed NSE at 14:45, 0.00s elapsed
Initiating Ping Scan at 14:45
Scanning 192.168.20.100 [4 ports]
Completed Ping Scan at 14:45, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:45
```

Gambar 4. 20 Pengetasan Port Scanning

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
```

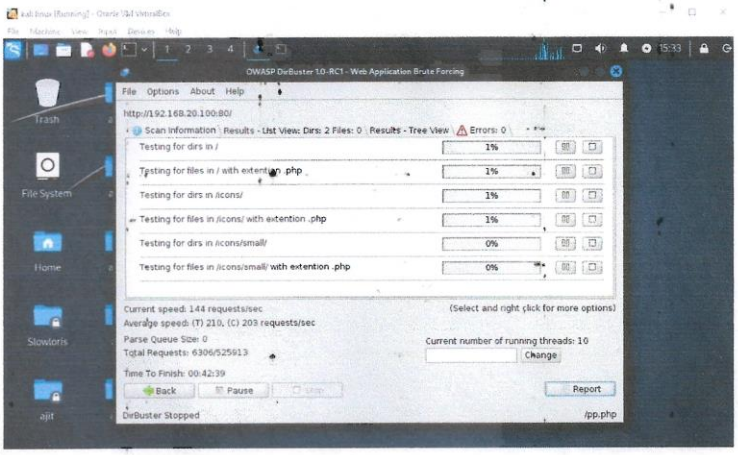
Gambar 4. 21 Terdapat port terbuka di jaringan

Dan akan tampil alerts pada *intrusion detection system* bahwa ada yang melakukan *port scanning* yaitu hasil *log* bertulisakan ET SCAN NMAP.



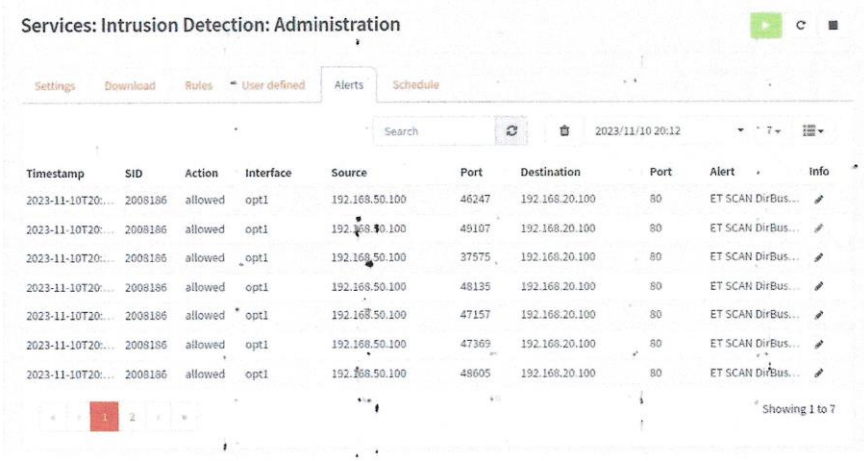
Gambar 4. 22 Hasil Testing *Port Scanning*

4. selanjutnya gunakan dirbuster untuk melakukan *brute force* pada web server



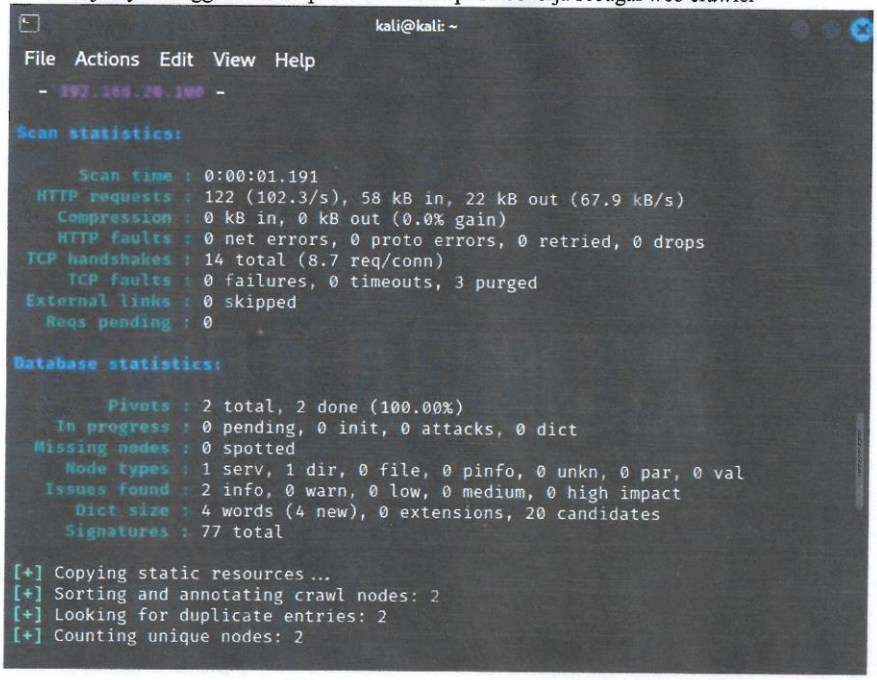
Gambar 4. 23 Pengujian *Brute Force*

Dan akan tampil hasil dari dirbuster tersebut pada *alert instrusion detection system* berupa log yang bertuliskan ET SCAN DirBuster.



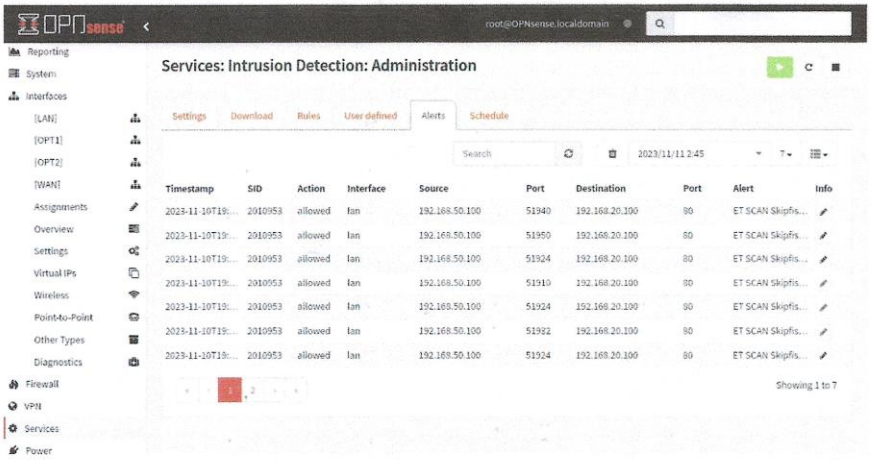
Gambar 4. 24 Hasil Pengujian *Brute Force*

5. Selanjutnya menggunakan skipfish dimana skipfish bekerja sebagai web crawler



Gambar 4. 25 Pengujian *Web Crawling*

Dan hasil dari test dengan skipfish pada *intrusion detection system* yaitu berupa log yang bertuliskan ET SCAN Skipfish.



Gambar 4. 26 Hasil dari Pengujian *Web Crawling*

4.3 Pembahasan

Pada perancangan dan pengujian diatas dapat dilihat bahwa OPNsense dapat bekerja sebagai router yang dimana disini diasumsikan attacker sudah memasuki dan mendapatkan IP router dan pada pengujian diatas dapat diketahui bahwa open port seperti port 80 sangat sekali rentan terhadap serangan,karena awal mula dari serangan ke webserver atau ke jaringan berasal dari open port yang ada pada jaringan atau pada server. OPNsense bekerja dengan baik sebagai *firewall* ketika ada serngan masuk dimana semua serangan serangan dari penetration testing dapat terdeteksi yaitu berupa *log* pada *alerts* yaitu ET SCAN NMAP, ET SCAN DirBuster, dan ET SCAN Skipfish oleh OPNsense *Intrusion Detection System*. Tetapi saat ini setelah dilakukan 6 kali DoS testing masih bisa menembus keamanan jaringan tersebut.

BAB 5. SIMPULAN

5.1 Simpulan

Bisa disimpulkan bahwa pada penelitian kali ini sebagai berikut:

1. OPNsense pada penelitian ini menjadi sebuah router yang dimana diasumsikan attacker sudah memasuki router dan web server berjalan pada port 80 yang dimana posisi OPNsense sebagai router penghubung dari web server ke internet begitu pula ke attacker. Setelah itu dilakukan pengujian seperti penetration testing menggunakan dirbuster, skipfish dan DoS testing untuk mengetahui apakah OPNsense bisa untuk mengamankan jaringan.

2.Setelah dilakukan beberapa testing pada OPNsense terdapat beberapa hasil yang didapatkan yaitu hasil berupa *alerts* pada *Intusion Detection System* dari penetration testing .Pada penetration testing OPNsense melakukan pendeteksian dengan baik dimana dirbuster dan skipfish dapat terdeteksi yaitu hasil *log* bertuliskan *alerts* ET SCAN NMAP, ET SCAN Dirbuster,dan ET SCAN Skipfish. Sedangkan pada *DoS testing* setelah 6 kali percobaan masih bisa menembus keamanan jaringan tersebut.

5.2 Saran

Saran dari penulis untuk penelitian ini kedepannya sebagai berikut:

1. Memperbanyak penelitian tentang keamanan jaringan menggunakan OPNsense karena banyak fitur OPNsense yang bisa dibahas seperti pada *firewall* dan *web filtering*.

2. Mendetailkan bahasan terutama pada rules rules yang ada pada *Instrusion Detection System*

DAFTAR PUSTAKA

Adha, R. R., Rizal, M. F., & Isma, S. J. I. (2021). Membangun Sistem Keamanan Jaringan Berbasis Firewall Dan Ids Menggunakan Tools Opnsense. *EProceedings ...*, *7*(6), 2846–2856. https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034/16747

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Aqra, M. Y. A., & Di, X. (2023). Intelligent Automated Penetration Testing Using Reinforcement Learning to Improve the Efficiency and Effectiveness of Penetration Testing. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *507 LNICST*, 30–42. https://doi.org/10.1007/978-3-031-34497-8_3/COVER

Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2022). Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sinkron*, *7*(1), 147–154. https://doi.org/10.33395/sinkron.v7i1.11249

Daka, M., & Banda, D. E. (2023). *STRENGTHENING WEB APPLICATION SECURITY THROUGH TECHNICAL MEASURES*. *05*, 154–168.

Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://doi.org/10.30656/prosisko.v7i2.2522

Efrando, A., Herwin, & Haryono, D. (2019). *SATIN – Sains dan Teknologi Informasi Monitoring pada Server STMIK Amik Riau dengan Menggunakan Suricata Melalui Notifikasi Bot Telegram*. *5*(1).

Fauzan, M. A. Al, & Purwanto, T. D. (2021). Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih. *Prosiding Semhavok*, 137–146.

http://conference.binadarma.ac.id/index.php/semhavok/article/view/2222

Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. https://doi.org/10.30630/jitsi.3.1.59

Herniati, W. O. (2022). *IMPLEMENTASI DAN ANALISA IDS (INTRUSION DETECTION SYSTEM) MENGUNAKAN SURICATA PADA WEB SERVER*. https://repository.ittelkom-jkt.ac.id/

Mantra, I. G. N., Hartawan, M. S., Saragih, H., & Rahman, A. A. (2019). Web vulnerability assessment and maturity model analysis on Indonesia higher education. *Procedia Computer Science*, *161*, 1165–1172. https://doi.org/10.1016/j.procs.2019.11.229

Marta, I. K. K. A., Hartawan, I. N. B., & Satwika, I. K. S. (2020). Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort. *INSERT : Information System and Emerging Technology Journal*, *1*(1), 25. https://doi.org/10.23887/insert.v1i1.25874

NURILAHI, D. K., MUNADI, R., SYAHRIAL, S., & BAHRI, A. (2022). Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, *10*(2), 309. https://doi.org/10.26760/elkomika.v10i2.309

Putra, G. M., Sembiring, M. A., Akmal, A., Sapta, A., Dristyan, F., Rizaldi, R., Firmansyah, A. U., Irianto, I., Abdullah, D., & Simarmata, J. (2018). Retracted: Concept of Analysis and Implementation of Burst on Mikrotik Router. *Journal of Physics: Conference Series*, *1114*(1). https://doi.org/10.1088/1742-6596/1114/1/012071

Putro, Z. P., & Supono, R. A. (2022). Comparison Analysis of Apache and Nginx Webserver Load Balancing on Proxmox VE in Supporting Server Performance. *International Research Journal of Advanced Engineering and Science*, *7*(3), 144–151.

Raharjo, M. F. (2020). *Evaluasi Kinerja Web Server Apache menggunakan Protokol HTTP2*. *2*(1), 19–31. https://doi.org/10.36079/lamintang.jetas-0201.92

Sabri, S., Ismail, N., & Hazzim, A. (2021). *Slowloris DoS Attack Based Simulation*. https://doi.org/10.1088/1757-899X/1062/1/012029

Sandkühler, D. (2020). *Exploring the methods and goals of students who DDoS educational facilities CC-BY-NC.*

Stephani, E., Fitri Nova, & Ervan Asri. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(2), 67–74. https://doi.org/10.30630/jitsi.1.2.10

Zarkasyi, K. M. I. (2018). *IMPLEMENTASI INTRUSION DETECTION SYSTEM SEBAGAI SISTEM KEAMANAN JARINGAN PADA LOCAL AREA NETWORK.*

LAMPIRAN

LAMPIRAN

Lampiran A

Tempat : Kantor BPTI UHAMKA

Narasumber : Nuroji, M.Kom.

Tanggal : 6 Februari 2023

Keterangan :

Q= Penanya A= Jawaban

Q	apakah belakang ini bpti uhamka pernah terjadi serangan serangan siber?
A	Ya, pernah dan sering contohnya seperti port scanning,DDoS,dan deface
Q	apakah jika ada serangan siber apa tindakan yang biasa dilakukan?
A	Biasanya dilakukan tindakan preventif yaitu mitigasi dengan firewall untuk mengantisipasi serangan serangan tersebut
Q	apakah ada tindakan preventif dalam menangani ini seperti pendeteksi otomatis?
A	Ya, Otomatis
Q	Adakah persamaan/perbedaan antara firewall ini dengan intrusion detection system yang dimana IDS ini terdapat 2 cara kerja yaitu knowledge-based dan behaviour-based dimana knowledge-based itu mencocokan dengan database IDS sedangkan behaviour-based mendeteksi dengan anomaly?
A	Persamaan ada pada cara kerja yang behaviour-based

Q	Apakah BPTI UHAMKA bersedia jika dilakukan penelitian tentang intrusion detection system dengan knowledge-based?
A	Ya,saya sangat menerima adanya penelitian tentang keamanan jaringan disini

Kepala Bagian Jaringan

BPTI UHAMKA

Nuroji, S.T., M.Kom.

NIDN. 0304048505

UNIVERSITAS MUHAMMADIYAH PROF. DR. HAMKA
FAKULTAS TEKNOLOGI INDUSTRI DAN INFORMATIKA
Jl. Tanah Merdeka No. 6, Kp. Rambutan, Ps. Rebo, Jakarta Timur. Telp. (021) 8400941; Fax. (021) 87782739
Website : www.ftii.uhamka.ac.id; E-mail : ftii@uhamka.ac.id

Nomor : **141/B.02.01/2023**
Lampiran : -
Perihal : Permohonan Izin Riset

26 Jumadil Akhir 1444 H
19 Januari 2022 M

Yang terhormat,
Kepala BPTI UHAMKA
Jl. Tanah Merdeka No.20 RT11/RW2, Rambutan,
Ps.Rebo Jakarta Timur, 13830

Assalamu'alaikum warahmatullahi wabarakatuh,

Pimpinan Fakultas Teknologi Industri dan Informatika Universitas Muhammadiyah Prof. DR. HAMKA mengharapkan kesediaan Bapak/Ibu kiranya dapat berkenan memberikan izin kepada mahasiswa kami yang bernama:

N a m a	:	Mohamad Baskoro Aji
Tempat, Tgl. Lahir	:	Bekasi, 25 November 2001
No. Pokok/NIM	:	1903015162
Jurusan/Prog. Studi	:	Teknik Informatika
Semester/Thn Akademik	:	Gasal 2022/2023
Alamat	:	Jl. Al Amin II No. 124, Jatirahayu, Pondok Melati, Bekasi 17414
Telepon	:	08999382868

untuk mengadakan riset dalam rangka pengambilan data untuk penyelesaian tugas akhir. *dengan judul* ***"IMPLEMENTASI INTRUSION DETECTION SYSTEM MENGGUNAKAN TOOLS OPNSENSE UNTUK MENGAMANKAN JARINGAN PADA BPTI UHAMKA".*** Lamanya riset yang dibutuhkan selama 1 (satu) bulan, dimulai pada bulan Januari s.d. Februari 2023 atau menyesuaikan kondisi intansi/perusahaan yang Bapak/Ibu pimpin.

Demikian permohonan ini dibuat, atas perhatian bapak/ibu, kami ucapkan terima kasih.

Wabillahit taufiq walhidayah,
Wassalamu'alaikum warahmatullahi wabarakatuh,

a.n. Dekan
Wakil Dekan I,

Ir. Rifky, ST., MM., MT., IPP

Tembusan :
1. Dekan (sbg laporan)
2. Ketua Program Studi
   Teknik Informatika FTII. UHAMKA

Mohamad Baskoro Aji - Analisis dan Pengembangan Intrusion Detection System Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA

ORIGINALITY REPORT

15%	15%	1%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docplayer.info Internet Source	2%
2	123dok.com Internet Source	1%
3	conference.binadarma.ac.id Internet Source	1%
4	publishing-widyagama.ac.id Internet Source	1%
5	adoc.pub Internet Source	1%
6	openlibrary.telkomuniversity.ac.id Internet Source	1%
7	id.123dok.com Internet Source	1%
8	repository.uin-suska.ac.id Internet Source	1%
	repository.wiraraja.ac.id	

LEMBAR REVISI SIDANG SKRIPSI ONLINE
TEKNIK INFORMATIKA UHAMKA

Report Status Kelulusan Mahasiswa Sidang

Nama Mahasiswa	:	MUHAMAD BASKORO AJI
NIM	:	1903015162
Tanggal Sidang	:	2024-01-26 14:15:00
Nama Pembimbing	:	Arafat Febriandirza, S.T., M.TI., Ph.D.
Judul Skripsi	:	Analisis dan Pengembangan Intrusion Detection System Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA

No	Catatan
1	Judul Skripsi disesuaikan dengan objek penelitian Format penulisan disesuaikan panduan skripsi FTII UHAMKA
2	Abstrak disesuaikan dengan skripsi Jadwal kegiatan, tempat dan hasil penelitian disesuaikan dengan objek penelitian
3	- Kutipan Jurnal disesuaikan dengan penelitian dan panduan skripsi FTII UHAMKA - Bukti penelitian di lampirkan

Validasi Revisi	Nama Dosen	Tanggal Revisi	Paraf
Ketua Sidang	Ade Davy Wiranata, S.Kom., M.Kom.	02-02-2024	
Pembimbing-1	Arafat Febriandirza, S.T., M.TI., Ph.D.	31-1-2024	
Pembimbing-2	-		
Penguji-1	Ade Davy Wiranata, S.Kom., M.Kom.	02-02-2024	
Penguji-2	Zuhri Halim, S.Kom., M.Kom.	1-2-2024	

Selanjutnya, yang bersangkutan harus segera menyelesaikan permasalahan sehubungan dengan skripsi ini, selambat-lambatnya 7 (tujuh) hari setelah tanggal pelaksanaan sidang.

Apabila revisi telah selesai dan mendapatkan approval (penguji, pembimbing, Kaprodi dan Dekan), maka tulisan (Skripsi, Jurnal) dan Program dikumpulkan dalam bentuk CD diberi label sebanyak 3 buah (lengkap) dan hardcover (Fakultas/Perpustakaan, Pembimbing dan Program Studi)

Berkas disusun sesuai petunjuk dan tanda tangan setiap berkas Asli, untuk softtcopy dilampirkan hasil pemindaian / scaning.

Batas Akhir Revisi ..... (hh/bb/tttt)

Batas Akhir Pengumpulan Berkas dan CD (Skripsi, Jurnal) ..... (hh/bb/tttt)

Wassalamu'alaikum wa Rohmatullahi wa Barokaatuh,

LEMBAR REVISI SIDANG SKRIPSI ONLINE
TEKNIK INFORMATIKA UHAMKA

Report Status Kelulusan Mahasiswa Sidang

Nama Mahasiswa	:	MUHAMAD BASKORO AJI
NIM	:	1903015162
Tanggal Sidang	:	2024-01-26 14:15:00
Nama Pembimbing	:	Arafat Febriandirza, S.T., M.TI., Ph.D.
Judul Skripsi	:	Analisis dan Pengembangan Intrusion Detection System Untuk Keamanan Jaringan: Studi Kasus di Lingkungan BPTI UHAMKA

No	Catatan

Validasi Revisi	Nama Dosen	Tanggal Revisi	Paraf
Ketua Sidang	Ade Davy Wiranata, S.Kom., M.Kom.	1/02/2024	
Pembimbing-1	Arafat Febriandirza, S.T., M.TI., Ph.D.	31/01/2024	
Pembimbing-2	-		
Penguji-1	Ade Davy Wiranata, S.Kom., M.Kom.	02-02-2024	
Penguji-2	Zuhri Halim, S.Kom., M.Kom.	1-2-2024	

Selanjutnya, yang bersangkutan harus segera menyelesaikan permasalahan sehubungan dengan skripsi ini, selambat-lambatnya 7 (tujuh) hari setelah tanggal pelaksanaan sidang.

Apabila revisi telah selesai dan mendapatkan approval (penguji, pembimbing, Kaprodi dan Dekan), maka tulisan (Skripsi, Jurnal) dan Program dikumpulkan dalam bentuk CD diberi label sebanyak 3 buah (lengkap) dan hardcover (Fakultas/Perpustakaan, Pembimbing dan Program Studi)

Berkas disusun sesuai petunjuk dan tanda tangan setiap berkas Asli, untuk softtcopy dilampirkan hasil pemindaian / scaning.

Batas Akhir Revisi . . . . . (hh/bb/tttt)

Batas Akhir Pengumpulan Berkas dan CD (Skripsi, Jurnal) . . . . . (hh/bb/tttt)

Wassalamu'alaikum wa Rohmatullahi wa Barokaatuh,