DETEKSI SERANGAN *BRUTE FORCE* MENGGUNAKAN *SURICATA* PADA SERVER AMS UNIVERSITAS BINA INSAN

SKRIPSI

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan
Program Sarjana (S-1)
Pada Program Studi Rekayasa Sistem Komputer

Oleh :
ADE WAHYUDA PRATAMA
NIM : 19.02.01.0014

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU TEKNIK
UNIVERSITAS BINA INSAN
2025

HALAMAN PERSETUJUAN TIM PENGUJI

Pada hari Jumat tanggal 24 bulan Januari tahun 2025 telah dilaksanakan Sidang Skripsi oleh Program Studi Rekayasa Sistem Komputer Universitas Bina Insan.

Nama : Ade Wahyuda Pratama
Nim : 19.02.01.0014
Judul : Deteksi Serangan *Brute Force* Menggunakan *Suricata* Pada Server AMS Universitas Bina Insan

Komisi Penguji

1. Ketua : Dr. M. Agus Syamsul .A, ST., M.Kom ( )

2. Sekretaris : M. Nur Alamsyah, M.Kom ( )

3. Anggota : Dr. Rudi Kurniawan, ST., M.Kom ( )

Mengetahui,
Kepala Program Studi Rekayasa Sistem Komputer
Univetsitas Bina Insan

Armanto, M.kom

HALAMAN PENGESAHAN

DETEKSI SERANGAN *BRUTE FORCE* MENGGUNAKAN *SURICATA* PADA SERVER AMS UNIVERSITAS BINA INSAN

Oleh :
ADE WAHYUDA PRATAMA
NIM : 19.02.01.0014

Lubuklinggau, Februari 2025

Pembimbing 1	**Pembimbing II**
Dr. M. Agus Syamsul Arifin, ST., M.Kom	**M. Nur Alamsyah, M.Kom**

Mengetahui,
Dekan Fakultas Ilmu Teknik
Universitas Bina Insan

Dr. Rudi Kurniawan, ST., M.Kom

HALAMAN MOTTO DAN PERSEMBAHAN

MOTTO:

"Apa yang Melewatkanku tidak akan pernah menjadi Takdirku, dan apa yang Ditakdirkan untukku tidak akan pernah melewatkanku."

Persembahan Kepada

- Allah SWT, terima kasih atas segala rahmat dan hidayah mu sehingga skripsi ini dapat terselesaikan dengan baik.
- Kedua orang tua. Terimakasih untuk segala dukungan dan doa restu yang selalu kalian berikan untukku. Terimakasih atas perjuangannya sehingga aku bisa berpendidikan sampai aku bisa duduk dibangku perkuliahan. Terimakasih sudah memotivasiku sehingga aku bisa bertahan sampai dititik ini.
- Terimakasih kepada yang selalu memotivasi, memberi semangat dan yang selalu menasehatiku. Terimakasih sudah menjadi tempat mencurahkan segala keluh kesahku selama skripsi ini. Dan juga terimakasih kepada teman-teman seperjuangan yang selalu memberi semangat dan motivasi.
- Almamaterku.

HALAMAN PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama Mahasiswi : Ade Wahyuda Pratama

NIM : 1902010014

Program Studi : Rekayasa Sistem Komputer

Menyatakan dengan sesungguhnya bahwa penelitian dan penulisan Skripsi yang saya susun sebagai persyaratan untuk memperoleh gelar Sarjana (S-1) Universitas Bina Insan, merupakan hasil kerja saya sendiri dan tidak menyuruh orang lain yang mengerjakannya. Ada bagian tertentu dalam penulisan Skripsi ini yang saya kutip dari hasil karya orang lain dan telah saya tuliskan sumbernya secara jelas dan sesuai dengan norma, kaidah dan etika penulisan ilmiah.

Jika dikemudian hari ternyata terbukti bahwa penelitian dan tugas akhir ini bukan hasil kerja saya sendiri atau plagiat dalam bagian-bagian tertentu, maka saya bersedia dikenakan sanksi sesuai dengan peraturan perundangan yang berlaku.

Lubuklinggau, Februari 2025

Penulis,

Ade Wahyuda Pratama
NIM 1902010014

RACT

The problem in this research was Bina Insan University has experienced a brute force attack, Bina Insan University has never detected a brute force attack using suricata, and regular server detection is required by Bina Insan University to maintain security from hacker attacks. The data collection techniques used were observation, interviews, documentation and literature study. The system development method used is a prototype. Hacking and detection simulations were carried out using the Kali Linux, IPcalc, Hydra, Nmap and Suricata tools. Obtained the results of predicting the username and password used by students to log in to the SISFO page. The researcher successfully logged in to the sisfo page using username 1902010014 with password 1601010101. So it can be concluded that the hacking simulation using the brute force method with hydra was successful. Obtaining one of the messages indicating detect-parse: Duplicate signature, which means that there has been a duplicate identity on the sisfo.univbinainsan.ac.id login page. So the detection simulation is considered successful.

Keywords: Brute Force, Kali Linux, Hydra, Nmap, Ipcalc, Suricata

TRAK

Masalah dalam penelitian ini iversitas Bina Insan pernah mengalami serangan *brute force*, Universitas Bina Insan belum pernah melakukan deteksi serangan *brute force* menggunakan *suricata*, dan pendeteksian server secara berkala diperlukan oleh Universitas Bina Insan untuk menjaga keamanan dari serangan para *hacker*. Teknik pengumpulan data yang digunakan adalah observasi, wawancara, dokumentasi, dan studi pustaka. Metode pengembangan sistem yang digunakan adalah *prototype*. Simulasi *hacking* dan *detection* dilakukan menggunakan *tool kali linux, ipcalc, hydra, nmap,* dan *suricata*. Diperoleh hasil prediksi *username* dan *password* yang digunakan oleh mahasiswa untuk *login* ke halaman sisfo. Peneliti berhasil login ke halaman sisfo menggunakan *username* 1902010014 dengan *password* 1601010101. Sehingga dapat disimpulkan bahwa simulasi *hacking* menggunakan metode *brute force* dengan *hydra* berhasil dilakukan. Perolehan salah satu pesan yang menunjukkan *detect-parse: Duplicate signature*, yang berarti bahwa telah terjadi duplikasi identitas pada halaman *login* sisfo.univbinainsan.ac.id. Sehingga simulasi *detection* dianggap berhasil.

Kata Kunci : *Brute Force*, *Kali Linux*, *Hydra*, *Nmap*, *Ipcalc*, *Suricata*

KA NGANTAR

Puji syukur alhamdulillah penulis ucapkan kepada Allah SWT atas segala rahmat dan hidayah- Nya sehingga penulis masih diberikan semua kenikmatan dan kekuatan, sehingga penulis dapat menyelesaikan Skripsi ini dengan semaksimal mungkin dan tepat waktu, untuk diajukan sebagai syarat menyelesaikan pendidikan program Sarjana (S-1) Pada Program Studi Sistem Informasi Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau. Kemudian sholawat beserta salam semoga tercurahkan kepada baginda Nabi Muhammad SAW, keluarga, sahabat, serta umatnya hingga akhir zaman.

Dalam penulisan Skripsi ini penulis menyadari bahwa masih ada kekurangan akan tetapi penulis berusaha sebaik mungkin untuk menyajikan Proposal Skripsi ini. Hal ini dikarenakan keterbatasan pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan Skripsi ini diharapkan adanya kritik dan saran yang diberikan bersifat membangun agar kedepannya menjadi lebih baik dari sebelumnya. Penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam menyelesaikan Skripsi ini, yaitu:

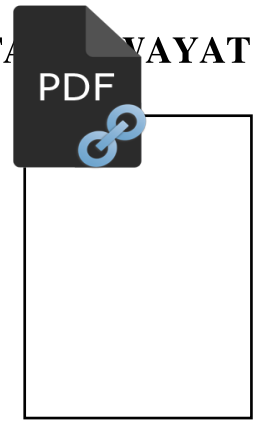
1. Kepada kedua orang tua ku yang tercinta yaitu Bapak Hermanto dan Ibu Pariem yang telah memberikan banyak sekali dukungan dan bantuannya dalam penulisan Skripsi ini.

2. Bapak Dr.H.Sardiyo, MM selaku Rektor Universitas Bina Insan.
3. Bapak Muhammad Akbar, [illegible]T selaku Wakil Rektor I Universitas Bina Insan.
4. Bapak Wakhid Nurmuklis, M.Kom selaku Wakil Rektor II Universitas Bina Insan.
5. Ibu Elmayati, M.Kom selaku Dekan Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau.
6. Ibu Nelly Khairani Daulay, M.Kom selaku Kepala Program Studi Rekayasa Sistem Komputer Universitas Bina Insan.
7. Bapak M. Agus Syamsul Arifin, ST., M.Kom selaku Pembimbing I yang telah membimbing dalam penyusunan Skripsi ini sampai dengan selesai.
8. Bapak M. Nur Alamsyah, M.Kom selaku Pembimbing II yang telah membimbing dalam penyusunan Skripsi ini sampai dengan selesai.
9. Seluruh Staf Dosen dan Karyawan Universitas Bina Insan Lubuklinggau yang telah baik dengan penulis semoga Allah SWT membalaskan kebaikannya.

Lubuklinggau, Februari 2025

Ade Wahyuda Pratama

DAFTAR RIWAYAT HIDUP



Biodata

Nama	: Ade wahyuda pratama
Tempat / Tanggal Lahir	: E. Wonokerto, 16 januari 2001
Jenis Kelamin	: Laki-laki
Agama	: Islam
Alamat	: E. Wonokerto

Pendidikan

- SD : SD Negeri E. Wonokerto
- SMP : SMP Negeri H. Wukirsari
- SMA : SMA Negeri Tugumulyo

TAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Internet merupakan jaringan komputer yang dibentuk oleh Departemen Pertahanan Amerika Serikat di tahun 1969, melalui proyek ARPA yang disebut ARPANET (*Advanced Research Project Agency Network*), di mana mereka mendemonstrasikan bagaimana dengan *hardware* dan *software* komputer yang berbasis UNIX, kita bisa melakukan komunikasi dalam jarak yang tidak terhingga melalui saluran telepon [1]. Internet sudah banyak digunakan oleh seluruh orang di dunia. Namun perlu kita ketahui bahwa terdapat macam-macam pengguna internet, salah satunya para oknum tidak bertanggung jawab seperti *hacker*.

Hacker adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivas oleh tantangan [1]. *Hacker* dalam dunia internet sangat meresahkan para pengguna lain. Banyak cara yang digunakan para *hacker* untuk membobol keamanan sistem, salah satunya adalah teknik *brute force*.

Algoritma *brute force* adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Penyelesaian permasalahan *password cracking* dengan menggunakan algoritma *brute force* akan menempatkan dan mencari semua kemungkinan *password* dengan masukan karakter dan panjang *password* tertentu tentunya

dengan banyak sekali kombinasi *password* [2]. Umumnya banyak para *hacker* yang menggunakan ini untuk meretas keamanan sistem/server. Namun dalam bidang kean gan kita dapat mengetahui aktivitas para *hacker* yang ingin meretas sistem/server, salah satunya adalah dengan menggunakan salah satu program seperti *suricata*.

Suricata engine merupakan *open source next generation intrusion detection* and *prevention engine*. *Suricata* merupakan *engine* yang memiliki kemampuan *Multi threaded*. Hal ini dapat diartikan kita dapat menjalankannya secara instan dan mengaturnya secara seimbang dalam setiap pemrosesan sensor *Suricata* yang telah terkonfigurasi [3].

AMS Universitas Bina Insan merupakan sistem informasi *website* yang digunakan untuk pengguna agar dapat mengakses sistem informasi akademik, portal akademik, sistem informasi registrasi, sistem informasi pembayaran, dan sistem informasi admisi. Universitas Bina Insan sendiri merupakan sebuah kampus yang beralamat di Jl. HM Soeharto No.Kel, Lubuk Kupang, Kec. Lubuk Linggau Sel. I, Kota Lubuklinggau, Sumatera Selatan 31626. Pada setiap kegiatan perkuliahan AMS sangat berperan penting dalam penyediaan informasi. Tentunya tidak menutup kemungkinan ada pengguna yang tidak bertanggung jawab juga ingin mengakses AMS Universitas Bina Insan. Oleh karena itu, perlu dilakukan deteksi keamanan server AMS secara berkala untuk mengetahui apakah terdapat serangan dari para *hacker* atau tidak, seperti serangan *brute force*.

Untuk membantu mengatasi permasalahan *brute force*, maka penulis tertarik untuk melakukan p dengan tema deteksi keamanan jaringan. Penelitian ini bertujuan u bantu para pengguna dalam mengetahui apakah terdapat serangan pada sistem/server mereka melalui *log suricata*.

Berdasarkan uraian di atas, penulis mengangkat judul penelitian yaitu "**Deteksi Serangan *Brute Force* Menggunakan *Suricata* Pada Server AMS Universitas Bina Insan**".

1.2 Identifikasi Masalah

Berdasarkan uraian dari latar belakang di atas, maka identifikasi masalah yang diperoleh penulis adalah:

a. Universitas Bina Insan pernah mengalami serangan *brute force*.
b. Universitas Bina Insan belum pernah melakukan deteksi serangan *brute force* menggunakan *suricata*.
c. Pendeteksian server secara berkala diperlukan oleh Universitas Bina Insan untuk menjaga keamanan dari serangan para *hacker*.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah diperoleh, maka penulis dapat merumuskan beberapa permasalahan sebagai berikut:

a. Bagaimana cara mengamankan server Universitas Bina Insan dari serangan *brute force*?

b. Bagaimana cara pendeteksian serangan *brute force* menggunakan *suricata* pada Universi Insan?

c. Bagaimana cara pende rver secara berkala yang harus dilakukan oleh Universitas Bina Insan?

1.4 Batasan Masalah

Mengingat betapa luasnya topik permasalahan yang di kaji oleh penulis, maka dalam penelitian ini diberikan beberapa batasan permasalahan yaitu:

a. Sistem operasi yang digunakan adalah *windows 10*.

b. Studi kasus penelitian adalah Universitas Bina Insan Lubuklinggau.

c. Simulasi *hacking brute force* digunakan pada server AMS Universitas Bina Insan.

d. *Software* yang digunakan dalam simulasi *hacking and detection* pada penelitian ini adalah *Suricata, Ubuntu,* dan *KaliLinux*.

e. Simulasi *hacking and detection* dilakukan pada SSH Login Server AMS Universitas Bina Insan menggunakan *hydra* dan *log suricata*.

1.5 Tujuan dan Manfaat Penelitian

Dalam penelitian ini penulis memiliki beberapa tujuan dan manfaat yang diperoleh, yaitu:

a. Tujuan Penelitian

1) Memperlihatkan t[illegible]enyerangan *brute force* pada SSH server Universitas Bina I[illegible]gunakan *hydra* dengan via *kalilinux*.

2) Memperlihatkan cara pendeteksian serangan *brute force* menggunakan *suricata* via *ubuntu*.

b. Manfaat Penelitian

1) Manfaat Bagi Tempat Penelitian

Universitas Bina Insan dapat menjaga kontrol keamanan server melalui program *suricata*.

2) Manfaat Bagi Penulis

Penulis dapat melakukan simulasi *hacking and detection brute force* menggunakan *hydra dan suricata*.

3) Manfaat Bagi Ilmu Pengetahuan

Penelitian ini dapat digunakan sarana referensi bagi penelitian dengan tema yang sama dan juga menambah ilmu pengetahuan dalam ilmu *hacking and detection*.

1.6 Sistematika Penulisan

Sistematika penulisan Skripsi ini terdiri dari 5 bab, bab-bab tersebut teridiri dari:

BAB I PENDAHULUAN

Pada bab ini berisi latar [illegible] penelitian, identifikasi masalah, rumusan masalah, batasan masalah, [illegible]an manfaat penelitian, serta sistematika penulisan.

BAB II KAJIAN PUSTAKA

Pada bab ini berisi literatur, penelitian relevan, dan kerangka berpikir.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi metode penelitian, metode pengumpulan data, metode pengembangan sistem, tempat dan waktu penelitian, alat dan bahan, analisis kebutuhan dan analisis sistem, metode pengujian sistem, dan rancangan sistem.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini berisi keseluruhan Gambaran umum, hasil penelitian, pembahasan, dan pengujian sistem yang dilakukan untuk mengkaji hasil penelitian yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan yang merupakan hasil akhir dari penelitian yang dilakukan dan saran-saran yang berguna untuk tempat penelitian, peneliti, dan penelitian selanjutnya.

BAB II
K N PUSTAKA

2.1 Literatur

a. *Brute Force*

Algoritma *brute force* adalah algoritma yang sangat rumit, alasannya dengan metode ini untuk menyelesaikan masalah dengan menggunakan teknik *straight forwad*, dibutuhkan beberapa masukan dan juga pertimbangan secara *valid*, sehingga sering mendapatkan keputusan pemecahan masalah yang langsung mengacu pada algoritma *brute force* atau mengarah pada hasil yang diinginkan [4]. Algoritma *brute force* adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode *cracking* dengan menggunakan algoritma *brute force* akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode [5]. *Brute force* adalah suatu pendekatan untuk memecahkan permasalahan, biasanya didasarkan pernyataan masalah dan definisi konsep yang dilibatkan [6].

Berdasarkan beberapa definisi *brute force* di atas, maka dapat penulis simpulkan bahwa *brute force* merupakan algoritma yang sangat rumit namun dapat memecahkan masalah dengan sangat sederhana dengan didasari pernyataan masalah dan definisi konsep yang dilibatkan.

b. SSH

SSH adalah progra[illegible]emungkinkan anda untuk login ke sistem *remote* dan memiliki [illegible]ng terenkripsi [7]. SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan [8]. SSH adalah protokol jaringan yang berada di lapisan aplikasi pada protokol TCP/IP [9].

Berdasarkan beberapa definisi SSH di atas, maka penulis dapat simpulkan bahwa SSH merupakan program/protokol jaringan yang memungkinkan pertukaran data yang berada pada lapisan aplikasi pada protokol TCP/IP.

c. *Ubuntu*

Ubuntu merupakan salah satu varian atau distro *linux* yang beredar saat ini [10]. *Ubuntu* merupakan salah satu distribusi *linux* yang paling populer digunakan. Selain karena bersifat *open source* juga dikarenakan *ubuntu* dilengkapi oleh beberapa aplikasi standar yang dibutuhkan oleh pengguna. Namun, baik *ubuntu* ataupun distro turunannya belum ada yang khusus dikembangkan untuk keperluan pemprograman, desain grafis, dan jaringan [11].

Dari beberapa definisi *ubuntu* di atas, maka dapat penulis simpulkan bahwa *ubuntu* merupakan salah satu varian distro *linux* yang dilengkapi oleh beberapa aplikasi standar yang dibutuhkan pengguna.

d. *Kali Linux*

Kali Linux meru[illegible]distro *linux* yang dikhususkan untuk melakukan penetrasi k[illegible]sistem komputer [12]. *Kali Linux* adalah distribusi berlandasan distribusi *Debian GNU/Linux* untuk tujuan forensik digital dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security* [13].

Berdasarkan beberapa definisi *Kali Linux* di atas, maka penulis dapat simpulkan bahwa *Kali Linux* merupakan distro *linux* yang berlandasan *debian GNU/Linux* untuk tujuan forensik digital.

e. *Suricata*

Pada tahun 2009, *US Department of Homeland Security* memberikan dana hibah yang besar kepada sebuha organisasi yang baru terbentuk bernama *Open Information Security Foundation* (OISF). Hal ini bertujuan untuk dibuatnya IDS *multithreaded* sebagai alternatif dari IDS *Snort*. IDS ini bernama *Suricata*. Pada tahun 2010, *Suricata* meluncurkan IDS mereka untuk pertama kali dengan versinya yaitu 1.2 [14]. *Suricata* merupakan *network based intrusion detection and prevention system* yaitu suatu perangkat lunak yang dapat digunakan untuk mendeteksi dan mencegah (*Detection System dan Prevention System*) terhadap lalu lintas sebuah jaringan. *Suricata* adalah IDS *open source* yang dikembangkan oleh *Open Information Security Foundation* (OISF) [15].

Berdasarkan beberapa definisi *suricata* di atas, maka penulis dapat simpulkan bahwa *suricata* adalah suatu perangkat lunak yang dapat

digunakan untuk mendeteksi dan mencegah terhadap suatu lalu lintas jaringan yang dikemba eh OISF.

2.2 Penelitian Relevan

Pada penelitian ini penulis menggunakan penelitian terdahulu sebagai pembanding dan sekaligus sebagai acuan penelitian yang sekarang dilakukan. Berikut ini merupakan beberapa penelitian relevan yang digunakan dalam penelitian ini:

a. Pada penelitian yang dilakukan oleh Mamay Syani (2020) dengan judul "Implementasi *Intrusion Detection System* (IDS) Menggunakan *Suricata* Pada *Linux Debian* 9 Berbasis *Cloud Virtual Private Server* (VPS)". Hasil penelitian ini adalah *suricata* sangat berperan penting untuk keamanan *cloud virtual private server* dari serangan - serangan yang tidak bertanggung jawab. Dengan adanya *suricata*, seorang yang bertanggung jawab terhadap *server* dapat mengatasi atau mengantisipasi serangan- serangan yang datang. Dapat dilihat pada tabel, bahwa dalam satu minggu saja banyaknya serangan yang dilancarkan kepada *server* berjumlah 86. *Port Scanning* mendominasi banyaknya jumlah serangan dari ketika metode penyerangan (*Brute Force*, DDos dan *Port Scanning*), dikarenakan untuk melakukan *Brute force* diperlukan *port scanning* terlebih dahulu. DDos Attack juga banyak dilancarkan dikarenakan DDos merupakan serangan yang dapat membuat *server* menjadi *down* dikarenakan dalam satu kali serangan DDos saja dapat dilipat gandakan

request nya sehingga menjadi *overload* dan akhirnya *server down* bahkan bisa jadi tidak bisa di[illegible]leh karena itu *suricata* adalah salah satu solusi untuk menangan[illegible]-serangan yang tidak bertanggung jawab kepada *server* [16].

b. Pada penelitian yang dilakukan oleh Fahmi Bagaskara Perdana, Dr. Ir. Rendy Munadi, M.T, dan Arif Indra Irawan, S.T., M.T (2019) dengan judul "Implementasi Sistem Keamanan Jaringan Menggunakan *Suricata* dan Ntopng". Hasil penelitian yang diperoleh adalah berdasarkan rule Suricata yang penulis buat, penulis berhasil mendeteksi semua serangan yang diujicobakan. Sedangkan pada rule default pada Ntopng, penulis hanya mampu mengidentifikasi jenis serangan DoS berupa SYN flood. Untuk serangan DoS dengan tujuan website server, pada bagian akurasinya, rule Suricata yang penulis buat lebih unggul daripada rule default pada Ntopng untuk aplikasi LOIC sebesar 52,70%, sedangkan untuk aplikasi Hping3 sebesar 48,80%, dan aplikasi GoldenEye sebesar 52,84%. Sedangkan untuk serangan DoS dengan tujuan FTP server, pada bagian akurasinya, rule Suricata yang penulis buat juga lebih unggul daripada rule default pada Ntopng untuk aplikasi LOIC sebesar 52,30%, sedangkan untuk aplikasi Hping3 sebesar 59,97%. Sehingga ada perbedaan jauh antara persentase akurasi, precision rate, dan recall rate dari Suricata dan Ntopng yaitu Suricata lebih unggul dalam ketepatan akurasi rule-nya dalam mendeteksi serangan DoS [15].

c. Pada penelitian yang dilakukan oleh Bima Putra Firdaus dan I Made Suartana (2020) dengan judul "Implementasi Keamanan Jaringan *Intrusion Detection/Prevention System* Menggunakan *PFSense*". Hasil penelitian yang diperoleh adalah fitur Suricata IDPS pada Pfsense dapat mendeteksi serangan dan dapat melakukan blokir atau drop terhadap serangan tersebut menggunakan rule yang ditambahkan secara manual atau kustom [17].

d. Pada Penelitian yang dilakukan oleh Alim Nuryanto (2015) dengan judul "Analisis dan Implementasi *Suricata, Snorby,* dan *Barnyard2* Pada VPS *Ubuntu*". Hasil penelitian ini adalah Aplikasi Suricata yang bekerja pada Server 1 mengidentifikasi serangan dengan membaca setiap datagram yang dikirim pada sesi TCP [3].

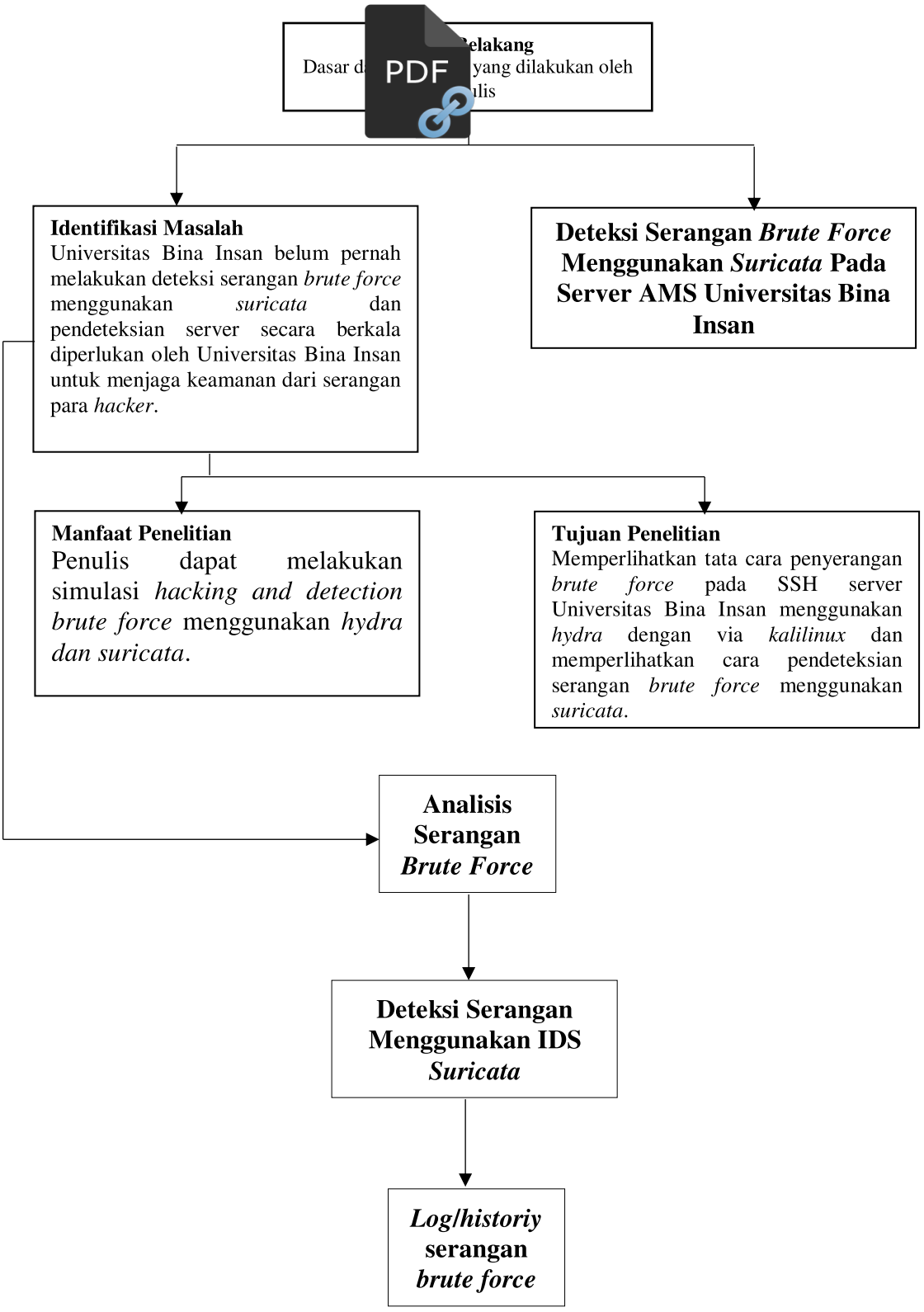
e. Pada penelitian yang dilakukan oleh Adam Dwi Ralianto dan Setiyo Cahyo (2021) dengan judul "Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan". Hasil penelitian ini adalah Dari penelitian ini didapatkan hasil bahwa Suricata versi 5.0.2 dengan pengujian menggunakan Pytbull dalam 3 skenario, memiliki akurasi lebih tinggi daripada Snort versi 2.9.15.1 karena memiliki rules yang lebih banyak. Walaupun rules lebih banyak, namun penggunaan memory Suricata lebih stabil karena menggunakan fitur multi-threading yang dimilikinya [18].

Dari beberapa penelitian relevan di atas, terdapat kesamaan dengan penelitian yang penulis lakukan yaitu dalam bidang keamanan jaringan

tentang mendeteksi serangan. Namun pada penelitian yang penulis lakukan saat ini IDS *suricata* akan [illegible] pada server AMS Universitas Bina Insan dengan fokus pada scenario *brute force*.

2.3 Kerangka Berpikir

Kerangka berpikir dalam penelitian ini dibuat agar proses penelitian yang dilakukan memiliki alur yang jelas dan sesuai dengan urutannya. Berikut ini merupakan gambar kerangka berpikir penelitian ini:



Gambar 2.1. Kerangka Berpikir

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif. Metode kualitatif digunakan karena sebagaian besar data penelitian yang digunakan adalah gambar, literature, dan dokumen-dokumen yang mengarah pada judul penulis.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan oleh penulis adalah observasi, wawancara, dan dokumentasi.

a. Observasi

Penulis melakukan observasi ke Universitas Bina Insan Lubuklinggau dengan proses mengambil sampel di tempat penelitian dan menganalisis permasalahan yang berkaitan dengan penelitian penulis.

b. Wawancara

Penulis melakukan wawancara *face to face* atau secara langsung dengan salah satu pegawai Universitas Bina Insan yang memegang kendali AMS Universitas Bina Insan Lubuklinggau.

c. Dokumentasi

Penulis mengumpulkan dokumen-dokumen penting yang dapat membantu data penelitian penulis demi tercapainya hasil penelitian yang diinginkan.

3.3 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan pada penelitian ini adalah *prototype*. *Prototyping* merupakan metode pengembangan perangat lunak, yang berupa model fisik kerja sistem dan berfungsi sebagai versi awal dari sistem. Dengan metode *prototyping* ini akan dihasilkan *prototype* sistem sebagai perantara pengembang dan pengguna agar dapat berinteraksi dalam proses kegiatan pengembangan sistem informasi. Agar proses pembuatan *prototype* ini berhasil dengan baik adalah dengan mendefinisikan aturan-aturan pada tahap awal, yaitu pengembang dan penguna harus satu pemahaman bahwa *prototype* dibangun untuk mendefinisikan kebutuhan awal. *Prototype* akan dihilangkan atau ditambahkan pada bagiannya sehingga sesuai dengan perencanaan dan analisis yang dilakukan oleh pengembang sampai dengan uji coba dilakukan secara simultan seiring dengan proses pengembangan [19].

Dibuatnya sebuah *prototyping* bagi pengembang sistem bertujuan untuk mengumpulkan informasi dari pengguna sehingga pengguna dapat berinteraksi dengan model *prototype* yang dikembangkan, sebab *prototype* menggambarkan versi awal dari sistem untuk kelanjutan sistem sesungguhnya yang lebih besar [19]. Berikut merupakan langkah-langkah dalam metode *prototype*:

a. Pengumpulan Kebutuhan

Mengumpulkan kebutuhan melibatkan pertemuan antara pengembang dan pelanggan untuk menentukan keseluruhan tujuan dibuatnya

perangkat lunak. Mengidentifikasi kebutuhan berupa garis besar kebutuhan dasar dari s g akan dibuat.

Pengumpulan keb yang dilakukan oleh Penulis yaitu, mengunduh *software suricata*, *hydra, ipcalc, nmap*, mengaktifkan *windows subsystem linux*, menyiapkan kebutuhan pada portal *website* sisfo.univbinainsan.ac.id untuk melakukan uji coba serangan dan deteksi.

b. Proses Desain yang Cepat

Desain berfokus pada representasi dari aspek perangkat lunak dari sudut pengguna. Ini mencakup *input*, proses, dan format *output*. Desain cepat mengarah ke pembangunan *prototype*. *Prototype* dievaluasi oleh pengguna dan bagian analis desain dan digunakan untuk menyesuaikan kebutuhan perangkat lunak yang akan dikembangkan.

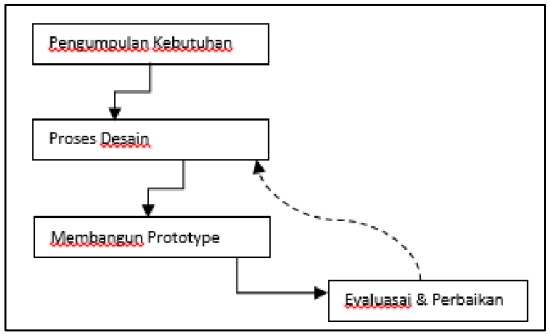
Desain yang dibuat oleh Penulis berupa *flowchart* deteksi dan serangan *brute force* pada sebuah server. Untuk uji coba simulasi ini, Penulis menggunakan portal *website* sisfo.univbinainsan.ac.id.

c. Membangun *Prototype*

Prototype yang dibangun akan mengikuti alur proses desain yang cepat pada langkah sebelumnya. Dengan membangun *prototype* ini, akan memperlihatkan desain yang telah dibuat sesuai dengan yang diharapkan atau terdapat kesalahan. Hasil *prototype* akan dievaluasi dan akan dilakukan perbaikan jika terdapat kesalahan proses atau pun kesalahan fungsi.

d. Evaluasi dan Perbaikan

Prototype dievalua pengguna dan bagian analis desain dan digunakan untuk men kebutuhan perangkat lunak yang akan dikembangkan.



Gambar 3.1. Metode *Prototype*

3.4 Tempat dan Waktu Penelitian

a. Tempat

Penelitian ini dilakukan pada Universitas Bina Insan Lubuklinggau yang beralamat di Jl. HM Soeharto No.Kel, Lubuk Kupang, Kec. Lubuk Linggau Sel. I, Kota Lubuklinggau, Sumatera Selatan 31626.

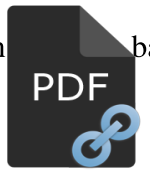
b. Waktu

Waktu penelitian diestimasikan berjalan selama 6 bulan, yaitu dimulai pada bulan Juli 2023 dan berakhir pada Desember 2023. Berikut ini merupakan tabel penelitian yang dibuat oleh penulis:

Tabel 3.1. Waktu Penelitian

Kegiatan Penelitian	Waktu Penelitian 2024																							
	Maret				A			Mei				Jun				Jul				Agu				
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pengajuan Judul																								
Penyusunan Proposal																								
Bimbingan Proposal																								
Seminar Proposal																								
Revisi Seminar Proposal																								
Penyusunan Laporan Proposal																								
Pembuatan Skripsi																								
Pembuatan Skenario Deteksi Serangan																								
Pengujian Program																								
Bimbingan Skripsi																								
Sidang Skripsi Revisi																								
Sidang Skripsi Pembuatan Laporan Skripsi																								

3.5 Alat dan Bahan

Berikut ini merupakan 

bahan yang digunakan selama penelitian dilakukan.

a. Alat

1) *Software*

(a) *Windows 10*

(b) *Kali Linux*

(c) *Ipcalc*

(d) *Command Promt*

(e) *Power Shell*

(f) *Suricata*

(g) *Nmap*

(h) *Windows PowerShell*

(i) *Microsoft Word 2016*

(j) *Microsoft Excel 2016*

(k) *Visual Paradigma*

(l) *Google Chrome*

(m) *Mendley Desktop*

2) *Hardware*

(a) Printer

(b) Laptop

b. Bahan

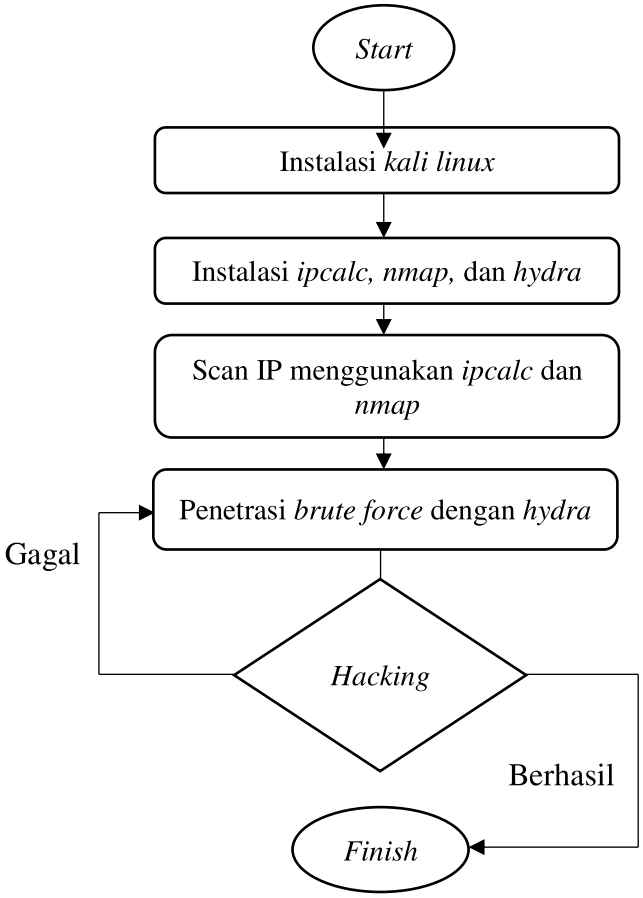
1) Kertas

2) Tinta Cair

3.6 Analisis Kebutuhan dan Sistem

a. Analisis Kebutuhan

Pada penelitian ini analisis kebutuhan dilakukan oleh penulis dengan mempersiapkan keperluan perangkat yang digunakan untuk skenario *hacking and detection*. Perangkat keperluan *hacking* dengan *brute force* adalah *kali linux*, *ipcalc*, dan *hydra*. Perangkat keperluan *detection* adalah *suricata, power shell*, dan pengaktifan *windows subsystem for linux*. Berikut merupakan gambaran *flowchart* untuk simulasi *hacking*.



Gambar 3.2. Simulasi *Hacking*

b. Analisis Sistem

Penulis melakukan analisis sistem dengan persiapan pengaturan perangkat lunak yang terpasang di dalam laptop penulis. Persiapan pengaturan dilakukan dengan memperhatikan serangan oleh *attacker*, sistem keamanan jaringan yang digunakan oleh AMS Universitas Bina Insan, aplikasi *suricata* sebagai pengganti sistem keamanan yang saat ini digunakan Universitas Bina Insan, dan menampilkan hasil deteksi berbentuk *log suricata*.

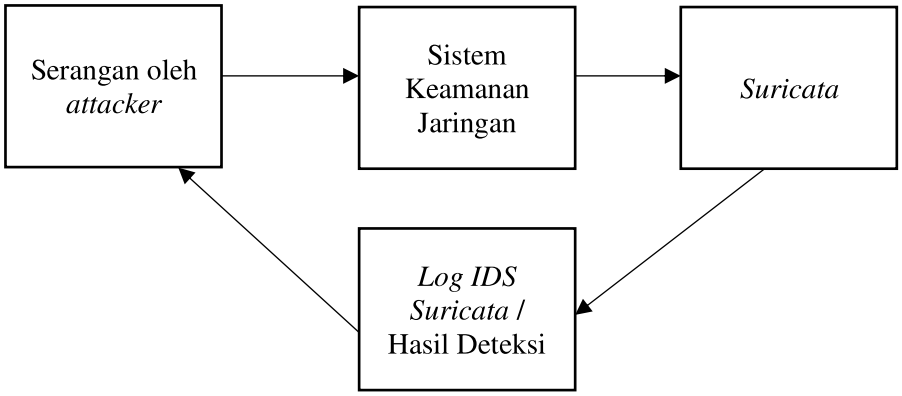
Pada simulasi yang dilakukan, penulis menjadi *attacker* dan sekaligus menjadi pengguna yang mengalami serangan. Serangan oleh *attacker* akan dilakukan pada server AMS Universitas Bina Insan dengan lebih spesifiknya ke halaman *login* sisfo.univbinainsan.ac.id. Metode serangan yang digunakan adalah *brute force* pada terminal *kali linux* berbantuan aplikasi *hydra*.

Simulasi serangan tersebut digunakan untuk mengetahui celah keamanan pada sistem keamanan jaringan yang saat ini digunakan oleh AMS Universitas Bina Insan. Sistem keamanan yang saat ini digunakan di AMS Universitas Bina Insan yaitu *port* SSH, anti *malware*, dan sebagainya yang merupakan keamanan standar pada jasa layanan *hosting*. Sehingga perlu dilakukan simulasi serangan ini untuk meningkatkan keamanan server kedepannya.

Untuk membantu kerentanan menurut penulis tersebut, maka digunakan aplikasi IPS dan IDS *suricata* yang dimana aplikasi ini

bekerja sebagai pendeteksi serangan yang dilancarkan pada sebuah server. Dengan diguna[PDF]plikasi ini, diharapkan dapat mendeteksi serangan lebih akurat dapat menjadi bahan evaluasi keamanan server AMS khususnya pada halaman *login* sisfo.univbinainsan.ac.id.

Hasil deteksi akan ditampilkan ke dalam *log IDS suricata*, hasil *log* tersebut menampilkan siapa penyerang dan metode apa yang digunakan oleh penyerang tersebut.



Gambar 3.3. Deteksi Serangan

3.7 Metode Pengujian Sistem

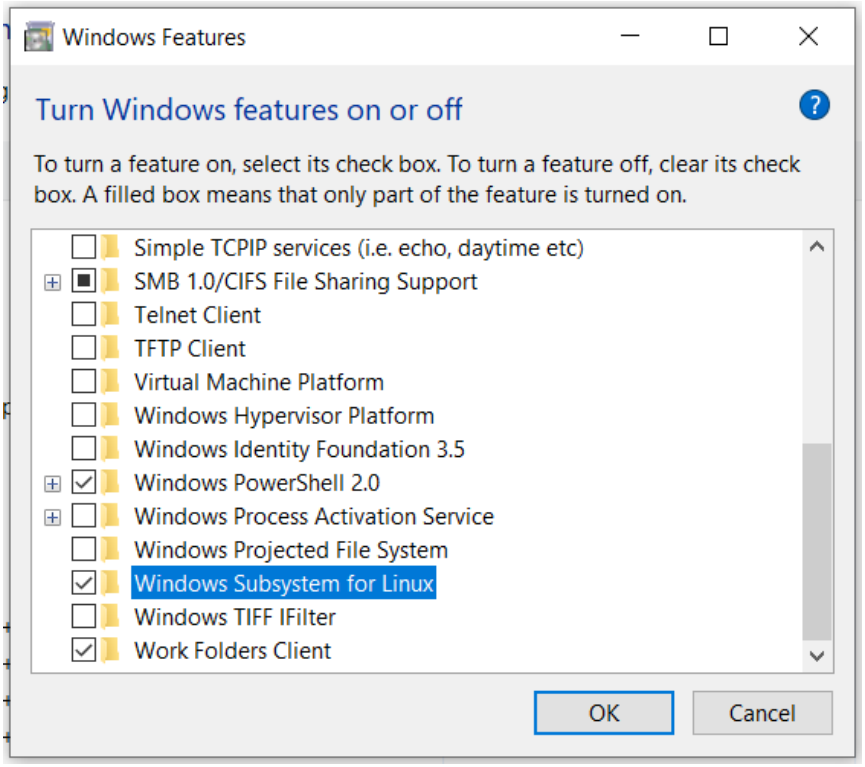
Metode pengujian sistem yang digunakan pada penelitian ini adalah metode fungsionalitas. Metode fungsionalitas yaitu pengujian yang difokuskan pada setiap fungsi dari masing-masing sistem. Pengujian yang akan dilakukan adalah teknik penyerangan yang dilakukan menggunakan *Brute Force* dan *tool Hydra, Nmap,* serta *Ipcalc*. Kemudian dari penyerangan yang telah dilakukan penulis akan mendeteksi serangan tersebut melalui *IDS* suricata, pengujian tersebut antara lain:

a. Langkah Penyerangan *Brute Force*

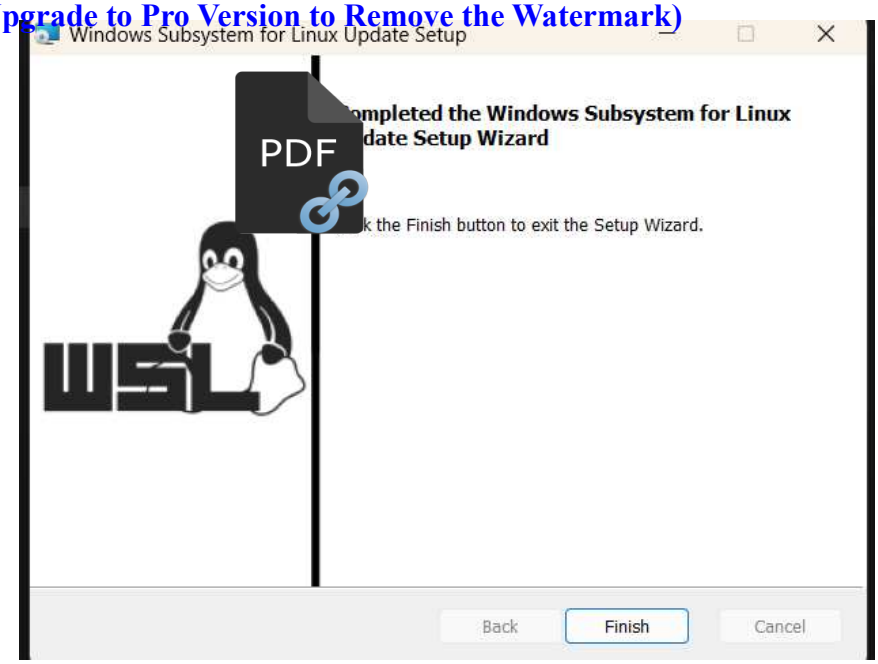
1) Instalasi WSL2

Pada sistem *windows*, untuk menginstal WSL2 harus mengaktifkan fitur *windows subsystem for linux* dan *hyper-V* di *windows features turn on or off*. Setelah fitur diaktifkan, download dan install WSL2.

WSL2 digunakan untuk menjalankan aplikasi *linux* pada sistem operasi *windows*. Setelah proses instalasi selesai penulis merestart laptop agar fitur dapat digunakan. Berikut merupakan gambar proses instalasi WSL2.



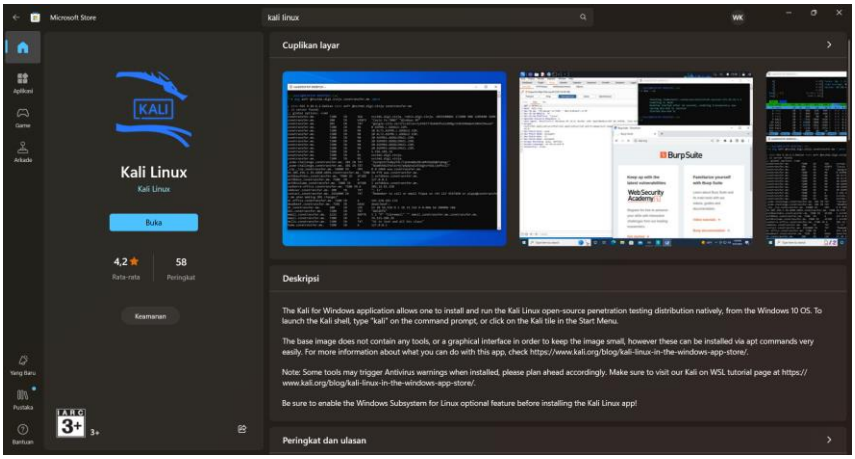
Gambar 3.4. Mengaktifkan *Windows Subsystem for Linux* dan *Hyper-V*



Gambar 3.5. Instalasi WSL2

2) Instalasi *Kali Linux*

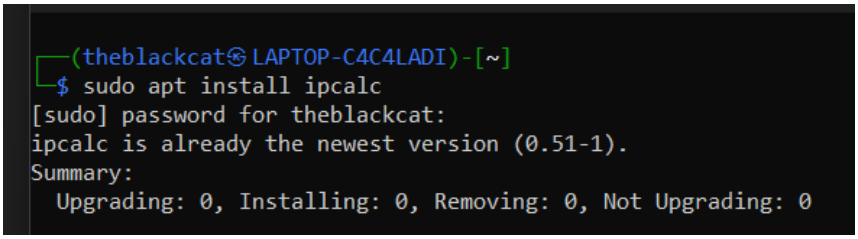
Kali linux digunakan untuk menjalankan terminal *linux* dan melakukan instalasi aplikasi berbasis *linux*. *Kali linux* memiliki fungsi sama dengan *command promt* pada *windows*, yang membedakan hanya peraturan perintah dan fitur aplikasi yang berjalan berdasarkan sistem operasi. Berikut merupakan gambaran *download* dan instalasi *kali linux*.



Gambar 3.6. *Download* dan Instalasi *Kali Linux*

3) Instalasi *Ipcalc*

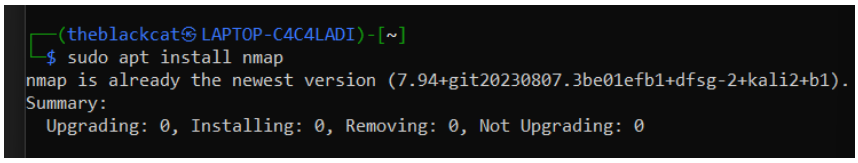
Ipcalc dapat [illegible] melalui *kali linux* dengan mengetikkan perintah pada pr[illegible]*li linux* yaitu *sudo apt install ipcalc*. Aplikasi tersebut berfungsi untuk mengetahui alamat jaringan/internet pada suatu server. Berikut gambar *download* dan instalasi *ipcalc*.



Gambar 3.7. Instalasi *Ipcalc*

4) Instalasi *Nmap*

Nmap digunakan untuk melakukan *scan* IP yang memiliki *port* terbuka pada suatu jaringan. Penulis membutuhkan aplikasi ini untuk mendapatkan alamat jaringan yang digunakan untuk simulasi *hacking*. Untuk melakukan instalasi ketikkan perintah pada terminal *kali linux* dengan *sudo apt install nmap*. Berikut gambar *download* dan instalasi *nmap*.



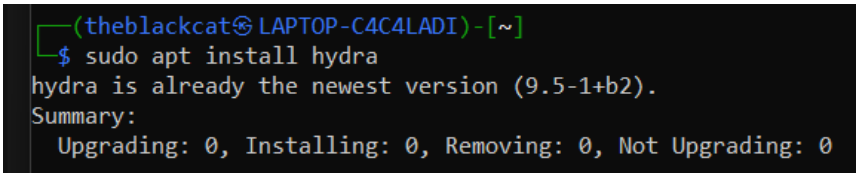
Gambar 3.8. Instalasi *Nmap*

5) Instalasi *Hydra*

Hydra digunakan untuk melakukan *ethical hacking* dengan menggunakan metode *brute force*. Simulasi *hacking* diarahkan pada

server Universitas Bina Insan Lubuklinggau yang lebih spesifiknya pada portal *login* ...vbinainsan.ac.id. Dalam melakukan *brute force* penulis me... daftar NIM mahasiswa yang digunakan sebagai *username* dan daftar *password* yang digunakan untuk *login* ke halaman tersebut.

Untuk menginstall *hydra* ketikkan *sudo apt install hydra* pada terminal *kali linux*. Kemudian untuk melakukan *brute force* menggunakan *hydra* ketikkan perintah pada terminal *kali linux* yaitu *hydra* univbinainsan.ac.id -L /home/theblackcat/Hacking/wordlist/username.txt -P /home/theblackcat/Hacking/wordlist/password.txt https-post-form "/login/proses:UserName=^USER^&passwordSha=^PASS^:F=Login Gagal". Berikut merupakan gambar download dan instalasi *hydra*.



Gambar 3.9. Instalasi *Hydra*

b. Langkah Keamanan *IDS Suricata*

1) *Download* dan instalasi *suricata*.

2) Masuk ke direktori penyimpanan dengan mengetikkan perintah pada *PowerShell* yaitu cd C:/Program File/Suricata.

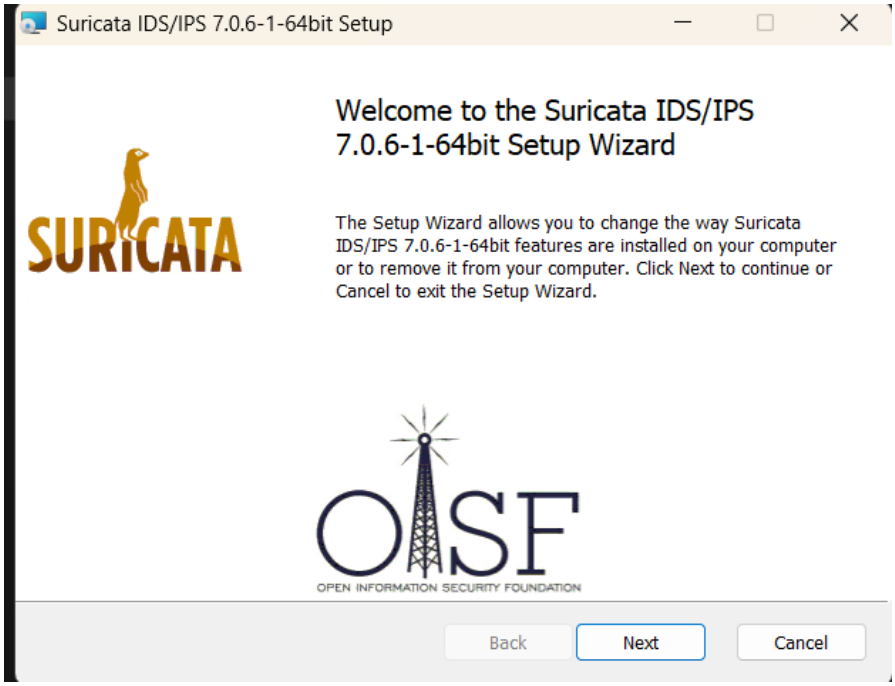
3) Pilih *file suricata.yaml* dan rubah alamat IP pada lokasi server yang ingin digunakan sebagai penerapan keamanan.

4) Aktifkan semua *rules* yang ada pada *file suricata.yaml*.

5) Aktifkan direktori *suricata* sebagai *service* dengan mengetikkan perintah pada *Po* yaitu .*suricata.exe* -c *suricata.yaml* -i alamat IP -l *log –i ice*.

6) Untuk menjalankan deteksi keamanan hanya perlu mengetikkan .*suricata.exe* -c *suricata.yaml* -i alamat IP -l *log*.

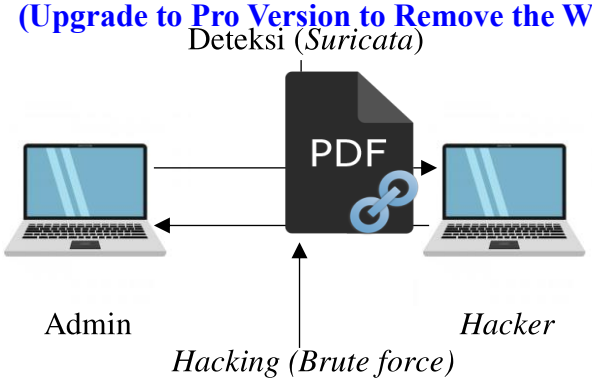
7) Maka *suricata* sudah siap untuk mendeteksi serangan yang dilancarkan pada IP yang sudah ditentukan.



Gambar 3.10. Instalasi *Suricata*

3.8 Rancangan Sistem

Berikut merupakan *use case* diagram dalam simulasi *hacking and detection* pada penelitian ini:



Gambar 3.11. Rancangan Sistem

Dari gambar 3.11, diketahui proses *hacking* dan deteksi menggunakan dua laptop. Laptop pertama dengan keterangan admin digunakan sebagai pendeteksi dengan melakukan pemasangan aplikasi *suricata*. Setelah itu menjalankan fitur IDS *suricata* untuk menampilkan hasil *log history* yang berjalan baik dari dalam laptop maupun interaksi dari luar laptop. Kemudian laptop kedua sebagai *hacker* menjalankan proses *hacking* menggunakan metode *bruteforce*. *Hacking* ditujukan pada sisfo Universitas Bina Insan dengan melakukan *scanning* terlebih dahulu menggunakan *Nmap* untuk mengetahui perangkat yang terhubung di jaringan tersebut. Ketika proses *hacking* dilakukan, laptop admin sebagai pengontrol server akan mendeteksi adanya ancaman serangan *brute force* dan menampilkannya di *log suricata*.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum

AMS Universitas Bina Insan merupakan sistem informasi *website* yang digunakan untuk pengguna agar dapat mengakses sistem informasi akademik, portal akademik, sistem informasi registrasi, sistem informasi pembayaran, dan sistem informasi admisi. Universitas Bina Insan sendiri merupakan sebuah kampus yang beralamat di Jl. HM Soeharto No.Kel, Lubuk Kupang, Kec. Lubuk Linggau Sel. I, Kota Lubuklinggau, Sumatera Selatan 31626. Pada setiap kegiatan perkuliahan AMS sangat berperan penting dalam penyediaan informasi. Tentunya tidak menutup kemungkinan ada pengguna yang tidak bertanggung jawab juga ingin mengakses AMS Universitas Bina Insan.

Pada server AMS terdapat salah satu fitur yang dapat digunakan oleh para mahasiswa, yaitu portal sisfo yang dapat diakses melalui *link* sisfo.univbinainsan.ac.id. Portal tersebut digunakan oleh mahasiswa untuk dan mengakses fitur di dalam sisfo. Fitur tersebut melayani seputar perkuliahan dari pengisian KRS dan sebagainya.

4.2 Hasil Penelitian

Hasil dari penelitian ini adalah simulasi *hacking* dan *detection* pada server AMS Universitas Bina Insan yang berfokus pada halaman *login* sisfo.univbinainsan.ac.id. Terdapat beberapa aplikasi yang digunakan untuk

melakukan *hacking*, diantaranya *kali linux, ipcalc, hydra,* dan *nmap*. Kemudian untuk simulasi *detection* menggunakan *tool* IDS dan IPS *suricata*.

4.3 Pembahasan

Berikut merupakan pembahasan mengenai simulasi *hacking* dan *detection* pada penelitian ini:

a. Simulasi *Hacking*

1. Konfigurasi *Kali Linux*

Pada pengaturan *kali linux*, peneliti mengunduh aplikasi *kali linux* agar dapat menggunakan fitur *linux* di dalam sistem operasi *windows*. Sebelum mengunduh aplikasi tersebut, peneliti mengaktifkan fitur *windows subsystem for linux* pada *windows features on or off* untuk dapat menggunakan aplikasi *kali linux*.

Setelah pengunduhan selesai, peneliti melakukan pemasangan aplikasi *kali linux* di dalam *windows*. Setelah pemasangan aplikasi selesai, peneliti membuka aplikasi *kali linux* dan kemudian melakukan pengaturan *username* dan *password* untuk *kali linux*. Berikut merupakan tampilan awal terminal *kali linux*.

Gambar 4.1. Tampilan Awal *Kali Linux*

2. Konfigurasi *Ipcalc*

Setelah selesai pada konfigurasi *kali linux*, selanjutnya peneliti melakukan pengunduhan *ipcalc* pada terminal *kali linux*. Perintah untuk melakukan di *kali linux* yaitu dengan mengetikkan perintah *sudo apt install ipcalc*. *Kali linux* akan otomatis melakukan pemasangan setelah pengunduhan selesai.

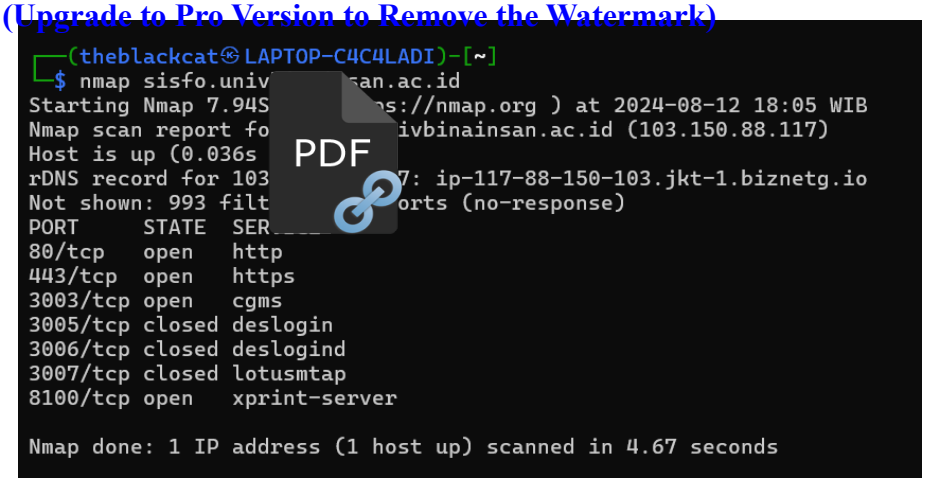
Ipcalc digunakan untuk mendeteksi perangkat yang terhubung pada sebuah jaringan. Pada simulasi ini, peneliti menggunakan jaringan yang digunakan oleh sisfo.univbinainsan.ac.id. Perintah *ipcalc* dapat dilakukan dengan mengetikkan *ipcalc* 103.150.88.117 (IP server sisfo). Berikut merupakan tampilan menggunakan *ipcalc*.

Gambar 4.2. Tampilan Penggunaan *Ipcalc*

3. Konfigurasi *Nmap*

Konfigurasi *nmap* dapat dilakukan dengan mengunduh *tool nmap* pada terminal *kali linux* dengan mengetikkan perintah *sudo apt install nmap*. Setelah proses pengunduhan selesai, *kali linux* akan otomatis melakukan pemasangan aplikasi *nmap*.

Selanjutnya mengarahkan *nmap* untuk mencari *port* yang terbuka pada server AMS melalui halaman *login* sisfo dengan mengetikkan *nmap* sisfo.univbinainsan.ac.id. Seperti yang diketahui bahwa *port* untuk mengakses server secara normal adalah 22, disini peneliti tidak menemukan *port* 22 yang terbuka saat *scanning* menggunakan *nmap.* Maka pilihan selanjutnya adalah menggunakan *hydra* untuk melakukan *brute force*. Berikut merupakan tampilan hasil penggunaan *nmap*.



Gambar 4.3. Tampilan Penggunaan *Nmap*

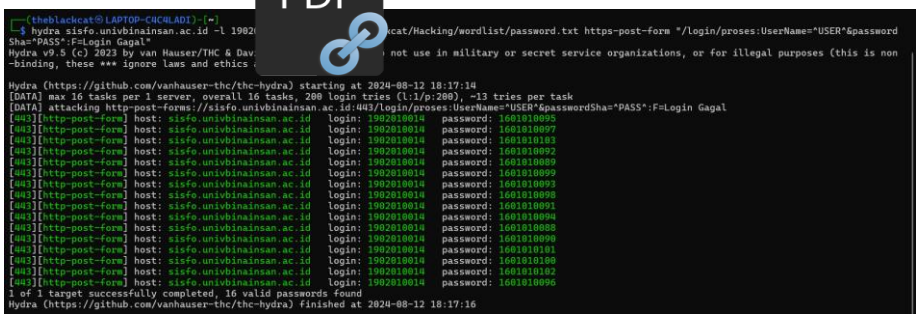
4. Metode *Brute Force* Menggunakan *Hydra*

Dari hasil *scanning nmap*, tidak ditemukan *port* 22 yang terbuka, maka peneliti melakukan pengunduhan *hydra* untuk *brute force* pada halaman *login* sisfo.univbinainsan.ac.id. Pengunduhan dilakukan melalui terminal *kali linux* dengan mengetikkan perintah *sudo apt install hydra*. *Kali linux* akan otomatis melakukan pemasangan aplikasi saat proses pengunduhan selesai.

Brute force sendiri termasuk salah satu metode yang memakan waktu cukup lama, karena peneliti harus menebak-nebak *username* dan *password* yang digunakan untuk *login*. Sehingga penulis menyiapkan NIM dan *password* yang kemungkinan besar digunakan untuk *login* ke halaman sisfo.

Perintah *brute force* menggunakan *hydra* dapat dilakukan dengan mengetikkan perintah hydra sisfo.univbinainsan.ac.id -l 1902010014 -P /home/theblackcat/Hacking/wordlist/password.txt https-post-form "/login/proses:UserName=^USER^&passwordSha=^PASS^:F=Login

Gagal". Berikut Gambaran proses penerapan metode *brute force* menggunakan *hydr*



Gambar 4.4. Proses *Brute Force* Menggunakan *Hydra*

b. Simulasi *Detection*

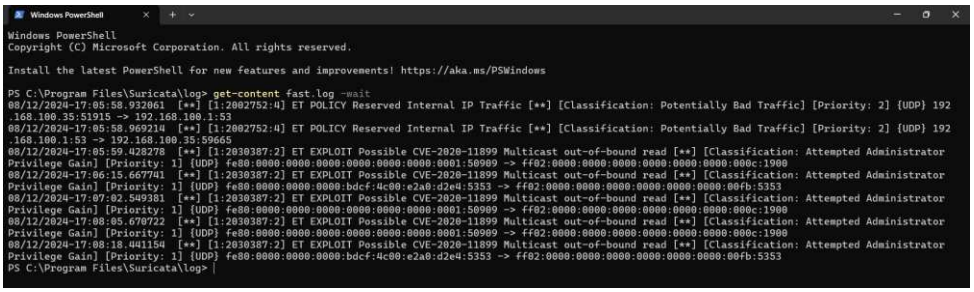
Simulasi *detection* dilakukan dengan aplikasi IDS dan IPS *suricata*. Konfigurasi *suricata* dilakukan dengan mengunduh *suricata* melalui portal resminya. Selanjutnya, peneliti mengaktifkan seluruh *rules* yang terdapat pada *file suricata.yaml*. Selain itu, peneliti juga mengatur penerapan IP pada *suricata.yaml* dengan IP laptop peneliti.

Setelah konfigurasi selesai, peneliti mengetikkan perintah pada CMD yaitu *suricata -c suricata.yaml -i* 192.168.100.35 (IP laptop peneliti) -l log --*service-install*. Perintah tersebut berguna untuk mengaktifkan direktori *suricata* sebagai *service*.

Selanjutnya, peneliti mengetikkan perintah untuk menjalankan *suricata* dengan *suricata -c suricata.yaml -i* 192.168.100.35 (IP laptop peneliti) -l log. Maka *suricata* akan menjalankan semua *rules* yang sudah diaktifkan. Berikut gambar *running suricata*.

Gambar 4.5. *Running Suricata*

Setelah *running* dilakukan, peneliti mengetikkan perintah pada *power shell* yaitu *get-content fast.log -wait* untuk menampilkan hasil deteksi *suricata*. Perlu diketahui *log* berisi perintah seluruh *rules* yang dijalankan. Berikut gambaran tampilan *log* IDS dan IPS *suricata*.



Gambar 4.6. *Log* IDS dan IPS *Suricata*

4.4 Pengujian Sistem

Berdasarkan pembahasan yang telah dilakukan, peneliti akan melakukan pengujian dan telaah terhadap hasil simulasi *hacking* dan *detection*. Pengujian dilakukan dengan menggunakan satu buah laptop sebagai alat *hacking* dan *detection*. Berikut merupakan hasil pengujian dan telaah:

1. *Hacking*

Berdasarkan ga[illegible] diperoleh hasil prediksi *username* dan *password* yang diguna[illegible]ahasiswa untuk *login* ke halaman sisfo. Berikut merupakan daftar *username* dan *password* yang diperoleh:

Tabel 4.1 Hasil *Username* dan *Password Brute Force*

No	*Username*	*Password*	Keterangan *Login*
1	1902010014	1601010095	Gagal
2	1902010014	1601010097	Gagal
3	1902010014	1601010103	Gagal
4	1902010014	1601010092	Gagal
5	1902010014	1601010089	Gagal
6	1902010014	1601010099	Gagal
7	1902010014	1601010093	Gagal
8	1902010014	1601010098	Gagal
9	1902010014	1601010091	Gagal
10	1902010014	1601010094	Gagal
11	1902010014	1601010088	Gagal
12	1902010014	1601010090	Gagal
13	1902010014	1601010101	Berhasil
14	1902010014	1601010100	Gagal
15	1902010014	1601010102	Gagal
16	1902010014	1601010096	Gagal

Sumber: Hasil Pengujian *Brute Force* 2024

Dari tabel tersebut, peneliti berhasil *login* ke halaman sisfo menggunakan *username* 1902010014 dengan *password* 1601010101. Sehingga dapat disimpulkan bahwa simulasi *hacking* menggunakan metode *brute force* dengan *hydra* berhasil dilakukan.

2. *Detection*

Berdasarkan gar diperoleh hasil deteksi yang ditampilkan melalui log IDS dan IP . Dari hasil tersebut, diperoleh salah satu pesan yang menunjukkan *detect-parse*: *Duplicate signature*, yang berarti bahwa telah terjadi duplikasi identitas pada halaman *login* sisfo.univbinainsan.ac.id. Sehingga simulasi *detection* dianggap berhasil. Berikut gambaran spesik baris yang menunjukkan peringatan tersebut.

Gambar 4.7. Hasil Spesifik Deteksi

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka Kesimpulan akhir penelitian ini adalah:

a. Diperoleh hasil prediksi *username* dan *password* yang digunakan oleh mahasiswa untuk *login* ke halaman sisfo. Peneliti berhasil *login* ke halaman sisfo menggunakan *username* 1902010014 dengan *password* 1601010101. Sehingga dapat disimpulkan bahwa simulasi *hacking* menggunakan metode *brute force* dengan *hydra* berhasil dilakukan.

b. Perolehan salah satu pesan yang menunjukkan *detect-parse*: *Duplicate signature*, yang berarti bahwa telah terjadi duplikasi identitas pada halaman *login* sisfo.univbinainsan.ac.id. Sehingga simulasi *detection* dianggap berhasil.

5.2 Saran

Berdasarkan kesimpulan yang diperoleh, maka saran yang dapat diberikan adalah:

a. Penelitian ini dapat dijadikan sebagai salah satu sumber referensi dan penambah wawasan ilmu pengetahuan khususnya tentang *hacking* dan *detection*.

b. Universitas Bina Insan dapat menjadikan aplikasi *suricata* sebagai salah satu *tool* untuk menambah keamanan server AMS Universitas Bina Insan.

c. Penelitian selanjutnya diharapkan dapat mengembangkan lebih jauh baik dari segi manfaat maup[illegible]de yang digunakan.

DAFTAR PUSTAKA

[1] A. G. Gani, "Pengenalan gi Internet Serta Dampaknya," *J. Sist. Inf. Univ. Suryadarma*, vol. 2 014, doi: 10.35968/jsi.v2i2.49.

[2] K. E. Pramudita, "Brute ttack dan Penerapannya pada Password Cracking," *Makal. IF30 g. Algoritm. – Sem. I Tahun 2010/2011*, vol. I, no. 2011, 2011.

[3] A. Nuryanto, "ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DANBARNYARD2 PADA VPS UBUNTU," *Ekp*, vol. 13, no. 3, pp. 1576–1580, 2015.

[4] R. Wahyu Nur Hidayah, A. Rubhasy, and U. Nasional, "Algoritma Brute Force Pada Aplikasi Kritik Dan Saran Mahasiswa Berbasis Digital Brute Force Algorithm in Digital-Based Student Criticism and Suggestion Applications," *J. Inf. Technol. Comput. Sci.*, vol. 4, no. 1, pp. 97–103, 2021.

[5] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 52–55, 2016, doi: 10.30743/infotekjar.v1i1.48.

[6] Y. Rahmawati, I. Adi Pribadi, and Y. Heningtyas, "Penerapan Algoritma Brute Force Pada Menu Search Website 'Calonku' Dalam Rangka Pemilu Berbasis Web," *J. Pepadun*, vol. 2, no. 1, pp. 60–70, 2021, doi: 10.23960/pepadun.v2i1.36.

[7] I. D. Cahyani, "Sistem keamanan enkripsi secure shell (ssh) untuk keamanan data," *J. Tek. Elektron. Fak Tek. Univ. Pandanaran*, pp. 1–8, 2011.

[8] B. Sakti, A. Aziz, and A. Doewes, "Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing," *J. Teknol. Inf. ITSmart*, vol. 2, no. 1, p. 44, 2016, doi: 10.20961/its.v2i1.620.

[9] jusuf Heni, "Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online," *Bina Insa. Ict J.*, vol. 2, pp. 75–84, 2015.

[10] M. A. Muslim, "Pengembangan Distro Ubuntu untuk Aplikasi Game Centre," *J. Teknol. Inf. Din.*, vol. XI, no. ISSN: 0854-9524, pp. 16–22, 2006.

[11] K. J. F. Devi, I. K. R. Arthana, and I. G. M. Darmawiguna, "Pengembangan Distribusi Luxpati Berbasis Ubuntu Sebagai Penunjang Proses Belajar Mengajar di Jurusan Pendidikan Teknik Informatika," *J. Nas. Pendidik. Tek. Inform.*, vol. 4, no. 3, p. 87, 2015, doi: 10.23887/janapati.v4i3.9783.

[12] I. P. A. Eka Pratama and A. A. B. A. Wiradarma, "Implementasi Katoolin Sebagai Penetrasi Tools Kali Linux Pada Linux Ubuntu 16.04 (Studi Kasus: Reverse Engineering File .Apk)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 86–93, 2018, doi: 10.31598/jurnalresistor.v1i2.278.

[13] M. A. Rahmadani, M. F. Rizal, T. Gunamawan, F. I. Terapan, U. Telkom, and H. Wireless, "Implementasi Hacking Wireless dengan Kali Linux

Menggunakan Kali Nethunter," *e-Proceedings Appl. Sci.*, vol. 3, no. 3, pp. 1767–1774, 2017.

[14] E. Risyad, M. Data, ar Pramukantoro, "Perbandingan Performa Intrusion Detection Syst) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flo *engemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9, pp. 2615–2

[15] Fahmi Bagaskara Perdana, M. . Dr. Ir. Rendy Munadi, and M. . Arif Indra Irawan, S.T., "Implementasi Sistem Keamanan Jaringan Menggunakan Suricata Dan Ntopng," *e-Proceeding Eng.*, vol. 6, no. 2, p. 4076, 2019.

[16] K. K. Ids, B. Force, and P. Scanning, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS) Mamay Syani Jurusan Teknik Komputer dan Informatika / Politeknik TEDC Bandung / Perkembangan Teknologi Informasi , khsu," vol. 1, no. 1, pp. 13–20, 2020.

[17] B. P. Firdaus and I. M. Suartana, "Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan Pfsense," *J. Manaj. Inf.*, vol. 4, no. 1, pp. 1–9, 2021.

[18] Adam Dwi Ralianto and S. Cahyono, "Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan," *Info Kripto*, vol. 15, no. 2, pp. 69–75, 2021, doi: 10.56706/ik.v15i2.10.

[19] D. Purnomo, "Model Prototyping Pada Pengembangan Sistem Informasi," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 2, no. 2, pp. 54–61, 2017, doi: 10.37438/jimp.v2i2.67.