BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan teknologi yang semakin canggih, situs *web* menjadi media baru untuk mengirimkan informasi. Teknologi ini sangat penting untuk menyebarkan informasi secara luas tanpa batas. Sistem penggunaan *web* sederhana yang dapat digunakan pada perangkat komputer dan *smartphone*. Institusi pendidikan juga menggunakan teknologi untuk menyediakan informasi terbaru dan mempromosikan publik. Masyarakat dapat menggunakan situs *web* institusi untuk memberikan kritik, saran, atau pertanyaan terkait (Prasetyo, dkk., 2021). Pemantauan jaringan komputer sangat penting dilakukan untuk mempermudah administrator jaringan dalam mengamati dan mengontrol sistem jaringan yang terpasang. Kebutuhan penggunaan jaringan komputer terus mengalami peningkatan yang mengakibatkan sistem jaringan yang terpasang menjadi kompleks. Resiko kerusakan dan gangguan jaringan semakin meningkat sehingga administrator jaringan harus secara terus menerus memantau seluruh sistem jaringan (Siaulhak, dkk., 2023).

Website adalah teknologi penyebaran informasi yang dapat menyampaikan informasi, seperti berita terbaru dan video dan lagu. *Website* adalah media penyampai informasi yang dapat diandalkan, yang membuatnya mudah digunakan karena dapat diakses kapan saja dan di mana saja dengan koneksi internet. Pengguna hanya perlu menggunakan *smartphone* atau perangkat komputer untuk mengunjungi *website* (Prasetyo, dkk., 2021). Tingkat keamanan yang tinggi diperlukan untuk melindungi *website* dari penipuan dan manipulasi yang dilakukan oleh pihak yang tidak bertanggung jawab. Kerentanan *web* sangat penting untuk menjaga data pengguna aman. Untuk mengidentifikasi kerentanan pada situs *web* yang dipilih oleh penulis untuk penelitian, pengujian penetrasi dapat dimulai. Hasil pengujian dapat memberikan gambaran tentang kondisi dan kerentanan pada situs *web* target (Fachri, dkk., 2021). Menurut Kamus Besar Bahasa Indonesia (KBBI) dijelaskan bahwa keamanan merupakan suatu kondisi bebas dari bahaya. Istilah bahaya disini dapat diartikan gangguan, ancaman, kecelakaan ataupun hal lainnya yang sifatnya tidak diinginkan. Keamanan sistem

informasi menjadi suatu hal yang sangat penting. Salahsatu indikator yang dapat terlihat adalah banyaknya serangan yang terjadi. Badan *Siber* dan Sandi Negara (BSSN) yang bekerja sama dengan *Indonesian Honeynet Project* (IHP) mencatat terdapat 12.895.554 jumlah total serangan *siber* dan 513.863 jumlah total serangan *malware* dengan sumber serangan tertinggi berasal dari Rusia, Tiongkok dan Amerika Serikat yang diambil rentang waktu Januari 2018 sampai dengan Desember 2018 yang dideteksi menggunakan 22 sensor aktif tersebar di 6 sampai 9 provinsi di Indonesia (Wardaya, 2019). Semua pihak harus memperhatikan keamanan sistem informasi dengan mengetahui jenis serangan yang terjadi.

Berdasarkan hasil observasi Dinas Kominfo Luwu Utara yang beralamat di Jl. Simpurusiang, Kecamatan Masamba, Kabupaten Luwu Utara. Dinas Kominfo Luwu Utara mempunyai 4 bidang. Dinas Kominfo Luwu Utara memiliki *website* resmi yang digunakan dalam menyimpan seluruh informasi. *Form login* pada *website* Dinas Kominfo Luwu Utara yaitu admin dan user. Namun *website* tersebut sering terjadi masalah teknis setiap tahunnya, seperti pada saat menggunakan *website* sering terjadi gangguan seperti gangguan saat proses *login* dan tidak dapat mengakses *website* secara tiba-tiba. Adapun jenis keamanan yang digunakan pada *website* Dinas Kominfo Luwu Utara yaitu *Intrusion Detection System* (IDS). *Intrusion Detection System* (IDS) adalah sistem yang memantau untuk mendeteksi aktivitas mencurigakan pada jaringan atau sistem komputer. Maka dari itu perlu adanya pengujian keamanan *website* Dinas Kominfo Luwu Utara untuk mengetahui celah keamanan pada *website* tersebut.

Adapun solusi yang ditawarkan dari permasalahan mengenai *website* yang ada di Dinas Kominfo Luwu Utara yaitu perlu adanya melakukan evaluasi melalui pengujian *penetration testing* dengan *Framework ISSAF*. *Penetration testing* ini dilakukan untuk mengevaluasi bug sistem, konfigurasi yang tidak sesuai, dan kelemahan teknis sistem informasi yang diujikan. Struktur ISSAF dirancang untuk menilai kontrol aplikasi, sistem, dan jaringan. Metode *penetration testing* menggunakan *framework issaf* dilakukan secara menyeluruh untuk menemukan celah keamanan sistem dari dalam dan dari luar. Pengujian penetrasi dilakukan melalui enam tahap pengujian yang didasarkan pada pedoman *framework ISSAF* dan dilakukan pada *website* target, yang meliputi tahap *Planning and Preparation*, *Information gathering*, tahap *network mapping*, tahap *vulnerability identification*,

tahap *penetration* dan tahap *reporting*. Pemilik sistem akan menerima laporan tentang masalah keamanan yang telah ditemukan bersama dengan perkiraan dampak dan solusi teknik. *Penetration testing*, juga dikenal sebagai *black box testing* atau *ethical hacking*, akan digunakan sebagai saran untuk menentukan apa yang harus dilakukan untuk membuat aplikasi memiliki tingkat keamanan tinggi dan menjaga data pribadi yang ada di dalamnya.

Atas terjadinya permasalahan tersebut untuk memperkuat argumen, maka penulis mengambil topik penelitian tentang kemanan sistem informasi dengan judul penelitian "Evaluasi Keamanan *Website* Dinas Kominfo Luwu Utara Menggunakan Metode *Penetration testing* dengan *Framework ISSAF*" diharapkan dapat memberikan manfaat terutama bagi Dinas Kominfo Luwu Utara, dimulai dari pengujian kerentanan, pencarian celah kerentanan serta memberikan rekomendasi untuk menutupi celah yang ada sehingga ke depannya Dinas Kominfo Luwu Utara dapat terhindar dari permasalahan yang terjadi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalahnya yaitu:

1. Bagaimana identifikasi resiko celah keamanan pada *website* yang dapat ditimbulkan dengan adanya eksploitasi celah keamanan tersebut?
2. Bagaimana mengevaluasi keamanan *website* Dinas Kominfo Luwu Utara menggunakan metode *penetration testing* dengan *framework ISSAF*?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini yaitu:

1. Mengidentifikasi cara-cara potensial yang dapat digunakan untuk mengeksploitasi celah keamanan yang ada.
2. Mengevaluasi keamanan *website* Dinas Kominfo Luwu Utara menggunakan metode *penetration testing* dengan *framework ISSAF*.

1.4 Manfaat Penelitian

1. Bagi Penulis

   Manfaat yang diperoleh untuk penulis dengan adanya penelitian ini yaitu dapat mengetahui cara mengevaluasi keamanan *website* menggunakan metode *penetration testing* dengan *framework ISSAF*.

2. Bagi Dunia Akademik

   Penelitian ini diharapkan akan memberikan suatu referensi yang berguna dalam perkembangan dunia akademik khususnya dalam penelitian-penelitian terkait dengan evaluasi keamanan *website* menggunakan metode *penetration testing* dengan *framework ISSAF* Bagi Dinas Kominfo Luwu Utara.

3. Bagi Dinas Kominfo Luwu Utara

   Terhindar dari dampak buruk serangan pada *website* Dinas Kominfo Luwu Utara, sehingga informasi yang ada pada *website* tersebut menjadi aman.

1.5 Batasan Penelitian

1. Penelitian ini hanya berfokus untuk mengevaluasi keamanan *website* pada Dinas Kominfo Luwu Utara
2. Penelitian ini menggunakan metode *penetration testing* dengan *Framework ISSAF*
3. Penelitian ini menggunakan Aplikasi *Virtual Box*
4. Hasil dari penelitian ini akan memberikan rekomendasi untuk menutupi celah yang ada pada *website* Dinas Kominfo Luwu Utara.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Penelitian ini akan membahas berbagai topik melalui kajian teori.

1. Evaluasi

Evaluasi adalah suatu proses merencanakan, mendapatkan, dan menyediakan informasi yang sangat penting untuk membuat keputusan. Dengan demikian, kegiatan evaluasi adalah proses yang direncanakan untuk mendapatkan informasi atau data untuk kemudian membuat keputusan (Ridho, 2018). Evaluasi adalah tindakan yang dilakukan untuk menentukan apakah tujuan pembelajaran telah dicapai atau tidak. Karena itu, evaluasi tidak efektif jika hanya dilakukan pada waktu tertentu (Fitrianti, 2018). Berdasarkan pendapat para pakar dapat disimpulkan bahwa evaluasi adalah proses penilaian untuk mengetahui sesuatu seperti kinerja jaringan, *website*, atau proyek seseorang dengan tujuan untuk memahami kekuatan dan kelemahan yang ada pada sesuatu tersebut.

2. Keamanan Jaringan

Metode pengendalian sumber daya jaringan dikenal sebagai keamanan jaringan. Tujuan pengendalian akses jaringan adalah untuk memastikan bahwa jaringan hanya dapat diakses oleh pihak tertentu yang memiliki hak untuk melakukannya (Andriyani, dkk., 2023). Seiring dengan peningkatan jumlah data yang dipertukarkan di internet, keamanan jaringan menjadi sangat penting. Setiap organisasi dan perusahaan harus selalu mematuhi standar keamanan internasional untuk menjaga kerahasiaan, integritas, dan otentikasi data di sebuah *web server*. Hal ini salah satunya disebabkan oleh meningkatnya ketergantungan masyarakat pada sistem informasi jaringan, yang menuntut pengukuran terus-menerus dan peningkatan keamanan sistem secara keseluruhan. Selain itu, kurangnya keamanan sistem meningkatkan kemungkinan *hacker* memasuki sistem, menyebabkan kerusakan atau penghentian fungsi yang telah dibuat (Fachri, dkk., 2021). Berdasarkan pendapat yang ada diatas dapat disimpulkan bahwa keamanan jaringan adalah teknologi yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data yang dikirimkan melalui jaringan komputer.

3. *Website*

Website adalah halaman informasi yang dapat diakses oleh orang-orang di seluruh dunia melalui internet tanpa batasan waktu atau ruang. Jenis konten ini dapat termasuk teks, gambar, atau video, antara lain. Karena popularitasnya saat ini, *web* telah berkembang menjadi interface aplikasi untuk melakukan transaksi dan menyediakan informasi yang lengkap dari seluruh dunia. Akibatnya, *web* identik dengan internet (Tania, dkk., 2018). *Website* adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas (Alwi, dkk., 2020). Sekelompok halaman *web* (*webpage*), yang biasanya merupakan bagian dari nama *domain* atau *subdomain* di internet, disebut "*website*". Baik *website* statis maupun dinamis terdiri dari rangkaian bangunan yang saling terkait yang dihubungkan melalui *hyperlink*. Jika konten *website* tetap dan jarang berubah, itu disebut statis. Jika itu dinamis, kontennya selalu berubah. Dalam kebanyakan kasus, situs *web* yang berfungsi sebagai situs informasi lebih menekankan pada kualitas konten karena tujuan situs tersebut adalah menyampaikan isi (Redy Susanto, 2021).

Berdasarkan pendapat diatas dapat disimpulkan bahwa *website* adalah kumpulan halaman *web* yang saling terkait dan dapat diakses melalui internet atau jaringan komputer.

4. Keamanan *Website*

Menurut Kamus Besar Bahasa Indonesia (KBBI) dijelaskan bahwa keamanan merupakan suatu kondisi bebas dari bahaya. Istilah bahaya disini dapat diartikan gangguan, ancaman, kecelakaan ataupun hal lainnya yang sifatnya tidak diinginkan. Keamanan *website* merujuk pada tindakan dan teknologi yang diimplementasikan untuk melindungi sebuah situs *web* dari ancaman keamanan seperti serangan, pencurian data, dan kerusakan yang dapat merugikan pemilik atau pengguna situs. Beberapa aspek keamanan *website* melibatkan perlindungan terhadap serangan *malware*, enkripsi data sensitif, manajemen hak akses pemantauan keamanan, dan pembaruan perangkat lunak secara teratur. Menurut pendapat diatas dapat disimpulkan bahwa Keamanan *website* adalah kegiatan melindungi situs *web* dan jaringannya, baik pribadi maupun perusahaan, dari berbagai ancaman *siber*. Ini mencakup tindakan untuk mengamankan data,

mencegah perusakan perangkat lunak dan perangkat keras, serta menghadapi potensi serangan.

5. Manfaat *Website*

Dengan adanya *website*, pemerintah dan masyarakat dapat berkomunikasi satu sama lain melalui internet. Ada banyak manfaat dari penggunaan *website* pemerintahan, termasuk sebagai media untuk informasi resmi, memudahkan aspirasi masyarakat untuk disampaikan, mempermudah akses masyarakat ke layanan publik, membantu proses administrasi, mendorong transparansi informasi, dan memungkinkan promosi (Ashar, 2022). Selain berfungsi sebagai media penyampaian informasi, adanya *website* memiliki banyak manfaat, seperti membangun branding bisnis, menjadi media promosi, membantu pelanggan, memberikan kritik dan saran, dan banyak lagi (Huda, 2020). *Website* harus memiliki keamanan yang memastikan bahwa data yang dikirim tetap aman untuk orang yang menerimanya. Jika pemilik *website* mengabaikan keamanan ini, seorang *cracker* dapat membuat program yang merusak data untuk kepentingan dirinya sendiri (Mulyanto, dkk., 2022).

6. Jenis-Jenis *Website*

Website dapat dikategorikan menurut fungsi, karakteristik, dan bahasa pemrograman yang digunakan (Mastan, 2019).

a. Jenis-jenis *website* berdasarkan sifatnya:

1. *Website dinamis* - sebuah situs web yang memiliki konten yang dapat diubah setiap saat.
2. *Website statis* - web yang halaman atau kontennya akan berubah jika filenya diubah.

b. Jenis-jenis *website* berdasarkan tujuannya:

1. *Personal website – situs web* yang dimiliki oleh seorang atau personal
2. *Corporate website* - *website* yang dikelola dan dimiliki oleh perusahaan.
3. *Portal website* - *website* yang menyediakan berbagai layanan, seperti layanan *email*, berita, dan layanan lainnya.
4. *Forum website – web* yang di gunakan sebagai tempat diskusi.

c. Jenis situs web dievaluasi berdasarkan bahasa pemrograman yang digunakan:

1. *Server Side Website* - web yang menggunakan bahas pemrograman yang tergantung pada penyedia *server*, seperti ASP.

2. *Client Side Website* - *web* yang dapat diakses hanya melalui browser dan tidak membutuhkan server untuk menjalankannya.

7. Macam-Macam Keamanan *Website*

Berikut ini adalah macam-macam kamanan *website*:

a. Autentikasi

Autentikasi merupakan suatu proses login kedalam sistem untuk sistem untuk memverifikasi layanan yang membutuhkan *username* dan *password*.

b. Enkripsi

Enkripsi adalah teknik mengamankan data dengan mengubah data tersebut tampak seperti data yang diacak untuk menjaga data dari peretasan.

c. DMZ (*Demiliterized Zone*)

DMZ adalah sistem untuk *server* yang dimaksudkan untuk melindungi sistem internal dari serangan *hacker*. DMZ dapat berfungsi pada seluruh dasar pelayanan jaringan yang membutuhkan akses ke jaringan itu sendiri.

d. IDS (*Intrusion Detection System*).

Intrusion Detection System (IDS) adalah sistem yang memantau untuk mendeteksi aktivitas mencurigakan pada jaringan atau sistem komputer.

8. Jenis-Jenis Serangan

Menurut (Andriyani dkk., 2023), Adapun jenis-jenis serangan yang biasanya terjadi di dalam sebuah *website* adalah sebagai berikut:

a. Serangan DDos (*Denial of Service*)

DDoS adalah serangan yang dilakukan dengan cara membanjiri sumber daya *server* dengan permintaan pengguna, membuat *server* tidak mampu menangani banyaknya permintaan tersebut, menyebabkan *server* tidak dapat berfungsi dengan baik.

b. *Serangan Brute Force*

Serangan *brute force* adalah cara untuk menyerang sistem keamanan komputer dengan melakukan percobaan pada semua kunci yang memiliki kemungkinan benar. Ini adalah kekuatan *brute* yang digunakan untuk melakukan pembobolan akses ke *host*, seperti *server*, ruangan, atau *server net*, serta data yang terenkripsi. Penyerang sering menggunakan kekuatan *brute* untuk mendapatkan akun ilegal. Apabila pengguna menggunakan kombinasi *password* yang sulit ditebak, serangan *brute force* ini akan memakan waktu lama. Tingkat kerumitan

password yang dibuat oleh pengguna menentukan lama tidaknya serangan ini. Penyerang akan menghabiskan lebih banyak waktu jika passwordnya lebih rumit

c. *Cross-Site Scripting* (XXS)

Serangan *Cross-Site Scripting* (XXS) berbeda dari serangan *web* lainnya, seperti *injeksi SQL*, karena tidak secara langsung menargetkan aplikasi *web* sebaliknya, penyerang menyisipkan kode jahat ke dalam situs *web* yang kemudian dijalankan oleh pengguna lain. Ini terjadi karena situs *web* tidak cukup memvalidasi atau membersihkan input pengguna, sehingga kode berbahaya dapat dimasukkan ke dalam konten halaman *web*.

d. Serangan *SQL Injection*

SQL injection adalah kepanjangan dari *Structured Query Language* dan merupakan teknik *hacking* yang digunakan untuk memasuki sistem dengan tujuan mengetahui isi *database* sebuah *website*, menampilkan hasil, atau melakukan sesuatu terhadap data yang tidak diinginkan..

9. Dinas Kominfo Luwu Utara

Dinas Kominfo Luwu Utara yang beralamat di jalan. Simpurusiang, Kecamatan Masamba, Kabupaten Luwu Utara. Dinas Kominfo Luwu Utara mempunyai 4 bidang didalamnya.

10. *Penetration testing*

Penetration testing (*pen test*) juga dikenal sebagai *pen test*, adalah serangan simulasi yang dilakukan pada sistem komputer untuk menilai keamanannya. Pelaku *pen test* menggunakan alat, metode, dan prosedur yang sama dengan *hacker* untuk menemukan dan menunjukkan bagaimana kelemahan sistem dapat berdampak pada bisnis. *Pen test* biasanya meniru berbagai serangan yang dapat membahayakan perusahaan. Mereka dapat menilai berbagai peran sistem dan apakah sistem cukup kuat untuk menahan serangan dari posisi yang diautentikasi dan tidak diautentikasi. Dengan cakupan yang tepat, *pen test* dapat menyelami aspek sistem apapun (Fierza, dkk., 2021). Tahap pengujian penetrasi terdiri dari serangan berulang. Untuk memulai pengujian penetrasi pada penelitian, kami melakukan wawancara dan wacana dengan pengelola *website* dan membaca literatur tentang pengujian yang telah dilakukan sebelumnya. Selanjutnya, pengujian penetrasi dilakukan menggunakan tahapan evaluasi dari *Framework ISSAF*. Setelah pengujian selesai, tahap terakhir, berdasarkan hasil pengujian

penetrasi, adalah membuat rekomendasi untuk meningkatkan keamanan *website* di lokasi tertentu (Sanjaya, dkk., 2020).

Uji penetrasi, juga dikenal sebagai uji penetrasi, adalah suatu simulasi serangan terkontrol yang digunakan untuk membantu mengidentifikasi kerawanan terhadap aplikasi, jaringan, dan cabang sistem operasi. Uji penetrasi melibatkan analisis aktif seluruh kerentanan yang mungkin terjadi pada sistem, termasuk konfigurasi sistem yang tidak sesuai, celah perangkat lunak atau perangkat keras, dan masalah operasi proses atau penanganan teknis (Utoro, dkk., 2020). Berdasarkan beberapa pendapat pakar dapat disimpulkan bahwa *penetration testing* adalah proses evaluasi keamanan untuk mengidentifikasi dan mengeksploitasi kelemahan dalam sistem atau jaringan komputer.

11. Framework ISSAF

Framework ISSAF dikembangkan oleh OISSG (*Open Information System Security Group*). OISSG (*Open Information System Security Group*) mengembangkan *Framework ISSAF*, yang menawarkan metodologi uji penetrasi yang paling efektif untuk mengevaluasi jaringan, sistem, dan kontrol aplikasi. Tujuan dari *Framework ISSAF* adalah untuk menawarkan arahan kepada auditor untuk melakukan pengujian penetrasi secara menyeluruh dan benar, sehingga auditor dapat menghindari kesalahan acak dalam melakukan pengujian serangan (Sanjaya, dkk., 2020). Metode evaluasi keamanan sistem komputer atau jaringan ISSAF melibatkan simulasi serangan dari sumber berbahaya (Zein, 2022). *ISSAF* merupakan salahsatu *framework* yang dikembangkan oleh *Open Information System Security Group* yang khusus dirancang untuk mengevaluasi jaringan, sistem, dan kontrol aplikasi (Mahendra, 2021).

Berdasarkan beberapa pendapat maka disimpulkan bahwa *framework ISSAF* adalah suatu kerangka kerja yang dirancang untuk membimbing profesional keamanan informasi dalam melakukan penilaian keamanan sistem informasi.

12. *VirtualBox*

Perangkat lunak *virtualisasi Oracle VM VirtualBox* dimaksudkan untuk *virtualisasi* sistem operasi dan dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. Penggunaan *VirtualBox* ditargetkan untuk server, desktop, dan penggunaan *embedded* (Anam, dkk., 2020). *VirtualBox* adalah perangkat lunak *virtualisasi* yang memungkinkan pengguna

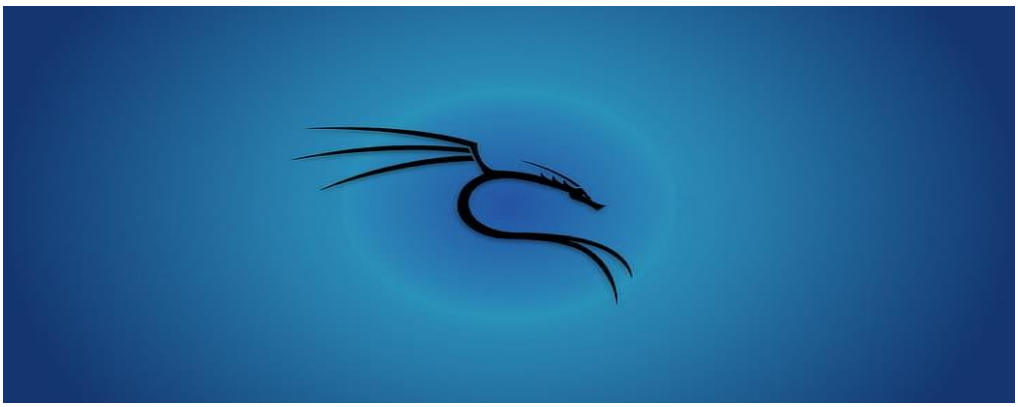
menjalankan sistem operasi lain di dalam sistem operasi utama (*host*).



Gambar 1. Virtual Box
Sumber. Putra (2021)

13. *Kali Linux*

Kali linux adalah pengembangan kembali *BackTrack Linux* yang sempurna, mengikuti standar pengembangan *Debian*, dan merupakan salah satu distribusi Linux tingkat lanjut untuk *penetration testing* dan *audit* keamanan (Rusdi, dkk., 2019).



Gambar 2. *Kali Linux*
Sumber. Lawrence (2023)

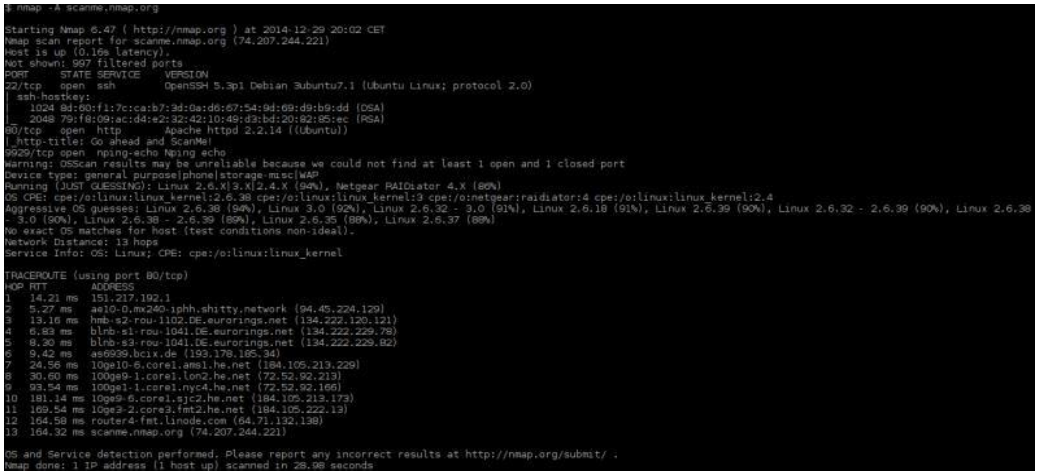
Adapun Fitur-fitur *Kali linux* adalah sebagai berikut:

a. Lebih dari 300 tools *penetration testing*
b. Gratis dan akan selalu gratis
c. Mengikuti FHS *compliant*
d. Dukungan perangkat *wireless* yang luas
e. Lingkungan pengembangan yang aman

f. Dukungan banyak bahasa

14. *Nmap*

Nmap adalah alat yang digunakan melalui *scanning port* untuk mengetahui *service* yang diberikan oleh suatu komputer. Penyerang sering menggunakan *Nmap* untuk mengetahui *port* komputer korban yang aktif, lalu menggunakan *port* tersebut untuk masuk ke sistem komputer korban (Anis, dkk., 2022). *Nmap*, atau *Network Mapper*, adalah alat *open source* yang digunakan untuk mengeksplorasi dan menganalisis keamanan jaringan. Paket *IP raw* digunakan oleh *Nmap* untuk mengidentifikasi host yang terhubung ke jaringan. Paket ini memiliki informasi seperti nama aplikasi dan versinya, versi sistem operasi, jenis *firewall*/filter paket yang digunakan, dan banyak atribut lainnya (Dwiyatno, 2020). *Nmap* adalah perangkat lunak *open-source* yang digunakan untuk menemukan perangkat yang terhubung ke jaringan, menemukan layanan yang berjalan pada perangkat, dan menemukan *port* yang terbuka.



Gambar 3. Tampilan *Nmap*
Sumber. Wikipedia

15. Owasp-Zap

Tools Owasp-Zap memungkinkan *penetration testing* pada situs *web*. Fitur ini mendeteksi kerentanan pada situs *web* (Hasibun, dkk., 2023). Salahsatu dari banyak standar keamanan yang tersedia adalah *Open Web Application Security Project*, atau OWASP, yang awalnya adalah organisasi yang berfokus pada keamanan *website*. Namun, seiring berjalannya waktu, OWASP menjadi standar keamanan *website* yang populer (Febriana, 2022). OWASP adalah organisasi *nirlaba global* yang berkonsentrasi pada meningkatkan keamanan perangkat lunak. OWASP unik karena dapat memberi orang, perusahaan, dan lembaga

pemerintah informasi praktis tentang keamanan perangkat lunak. Selain itu, OWASP adalah komunitas online yang secara bebas menyediakan artikel, metode, instruksi, dan program tentang keamanan aplikasi *website*. Dikenal sebagai proyek unggulan OWASP, ZAP adalah program pengujian penetrasi terintegrasi pada OWSAP yang gratis, mudah digunakan, dan *open source* yang mendeteksi celah keamanan dalam aplikasi *website*. ZAP juga menyediakan seperangkat program yang memungkinkan untuk mendeteksi celah keamanan secara manual selain pendeteksian otomatis (Ula, 2019).

16. *Gray Box Testing*

Metode pengujian *Gray Box* adalah kombinasi dari kedua metode pengujian hitam dan putih. Metode ini melakukan pengujian dengan menggunakan bahasa spesifikasi sesuai kebutuhan, seperti metode pengujian kotak hitam, dan kemudian memverifikasi kebenarannya berdasarkan kode *struktural*, seperti metode pengujian *white box* (Setiawan, dkk., 2019). Berdasarkan pendapat diatas, dapat disimpulkan bahwa *gray box testing* adalah metode pengujian perangkat lunak di mana penguji memiliki pengetahuan sebagian tentang desain internal, struktur, dan implementasi kode program yang diuji. Penguji biasanya memiliki akses terbatas ke kode sumber atau dokumentasi sistem.

2.2 Hasil Penelitian yang Relevan

Penelitian yang relevan adalah penelitian sebelumnya yang telah dilakukan oleh seseorang dan menghasilkan hasil yang valid sesuai dengan judul dan tujuan peneliti. Penelitian ini merujuk pada beberapa penelitian sebelumnya sebagai referensi untuk diukur, penelitian tersebut antara lain:

1. Prasetyo & Hassanah (2021) dengan judul penelitian "Analisis Keamanan *Website* Universitas Internasional Batam Menggunakan Metode ISSAF" dalam penelitian ini digunakan *framework ISSAF* sebagai metode penelitian dan menggunakan metode *blackbox testing* dalam pengujian pentest. Dalam penulisan penelitian ini agar sesuai dengan tahapan yang diperlukan maka menggunakan alur penelitian. Studi menunjukkan bahwa situs *web* utama Institusi Universitas Internasional Batam, *www.uib.ac.id*, cukup aman dari serangan *hacker*. Dari empat tahap pengujian menggunakan metode ISSAF, ditemukan bahwa serangan DDOS dapat menembus *website*

utama, menyebabkan *server down* sementara. Namun, backup keamanan *firewall* yang aktif cukup membantu *server* melindunginya dari serangan *hacker*. Secara keseluruhan, sistem *web* utama masih dianggap cukup aman dari serangan *hacker*.

2. Fachri, Fadlil & Riadi (2021) dengan judul penelitian "Analisis Keamanan *Webserver* Menggunakan *Penetration* Test" *Penetration testing* pada penelitian diawali dengan studi literatur mengenai pengujian yang dilakukan dan melakukan diskusi dan wawancara terhadap pihak pengelola *website*. Berdasarkan penelitian yang dilakukan mengenai keamanan *web server* maka kesimpulan yang didapat adalah terdapat kelemahan pada Sistem Informasi Akademik. Jenis kelemahan pada Sistem Informasi Akademik didapatkan tiga kategori adalah *level high, level medium dan level low*. Simulasi serangan menggunakan *Parrot OS* menghasilkan keberhasilan masuk kedalam *system*, dengan ditemukannya *username* dan *password* maka dapat *Login* ke target. Saran dan masukan terhadap Perguruan tinggi agar segera mengambil tindakan penutupan *port TCP* yang terbuka, serta perbaikan bug pada sistem yang dapat dimanfaatkan penyerang sebagai celah keamanan mengenai Sistem Informasi Akademik.
3. Andriyani, Sidiq & Zen (2023) dengan judul penelitian "Analisis Celah Keamanan Pada *Website* dengan Menggunakan Metode *Penetration testing* dan *Framework Issaf* pada *Website* SMK Al-Kautsar" pada tahapan information gathering berguna untuk mencari informasi yang berkaitan dengan website target. Seperti informasi mengenai alamat ip yang dapat diketahui dengan menggunakan terminal pada kali linux.penelitian ini menguji celah keamanan pada situs *web* SMK Al-Kautsar Purwokerto dengan menggunakan metode *penetration testing* berbasis *framework ISSAF*. Hasilnya menunjukkan bahwa situs web tersebut tidak memiliki celah keamanan yang dapat menyebabkan serangan *SQL Injection*, seperti yang ditunjukkan oleh peneliti dengan melakukan pengujian menggunakan alat *SQL Injection*, dan sebuah database tidak dapat menemukan hasilnya. Setelah melakukan pengujian dengan *tools* LOIC, peneliti menemukan bahwa *website* tersebut rentan terhadap serangan ddos. Hasilnya menunjukkan bahwa selama serangan, *website* tersebut tidak dapat diakses. Serangan yang memanfaatkan

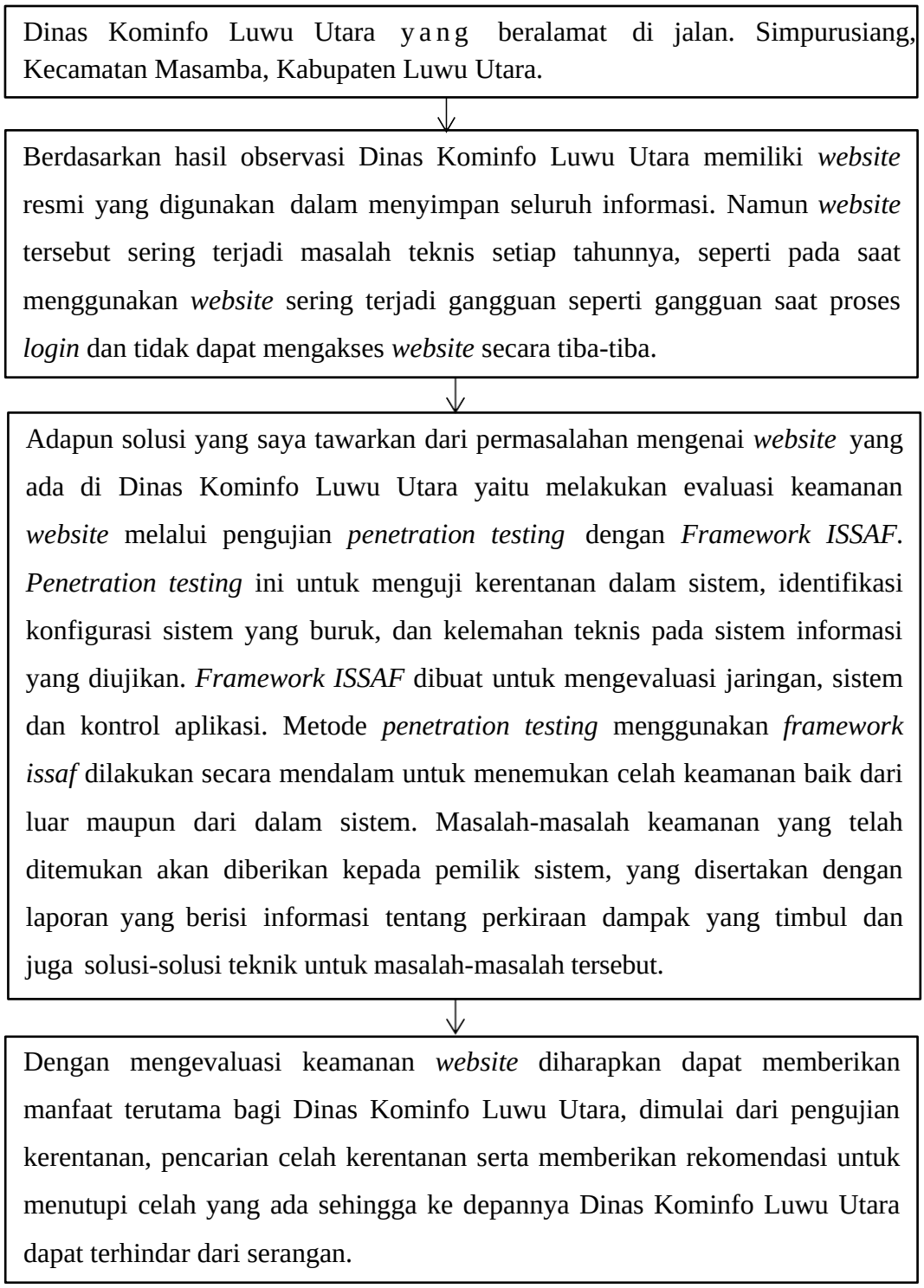
port 21—*port* ftp—tidak dapat mengancam situs *web* ini. Dengan menggunakan serangan *brute force*, peneliti berhasil mendapatkan akses ke akun *cpanel* dan *web hosting*.

4. Sanjaya, Sasmita & Asra (2020) dengan judul penelitian "Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration testing* Menggunakan *Framework ISSAF*" dengan menggunakan Framework ISSAF, pengujian penetrasi pada situs *web* Lembaga X dilakukan dalam sembilan tahap. Tahap-tahap ini meliputi pengumpulan informasi, pemetaan jaringan, pengenalan kelemahan, penetrasi, memperoleh akses dan peningkatan hak, enumerasi lebih lanjut, pelanggaran oleh pengguna atau situs *web* yang jauh, pengamanan akses, dan penutup jalur. Sembilan langkah tersebut menunjukkan bahwa celah keamanan yang berbahaya seperti *SQL Injection* dan XSS pada *website* Lembaga X. *Port* TCP yang terbuka juga merupakan masalah keamanan karena memungkinkan serangan dari pihak luar dan bug sistem yang dapat digunakan sebagai celah keamanan. Salahsatu solusi yang dapat diberikan adalah validasi pada level php untuk mencegah serangan *SQL Injection* dan XSS, yang merupakan sumber setelah perbaikan dilakukan berdasarkan rekomendasi yang diberikan, penelitian penetrasi pengujian dapat dilakukan pada Lembaga X di masa depan. Selain itu, *framework* pengujian penetrasi lainnya dapat digunakan sebagai perbandingan hasil pengujian.
5. Zein (2022) Dengan judul penelitian "Evaluasi Keamanan *Wireless Lan* Menggunakan ISSAF (*Information System Security Assessment Framework*)" dari penelitian yang telah dilakukan, dapat ditarik kesimpulan bahwa: Menghasilkan model/teknik evaluasi jaringan *nirkabel* melalui pengujian penetrasi mode (topologi) jaringan nirkabel. menggunakan ISSAF (*Information System Security Framework Planning*) untuk membuat evaluasi model proses LAN nirkabel. Evaluasi termasuk evaluasi dan laporan. untuk menghitung tingkat mempertahankan akses tahapan untuk mempertahankan hak yang sudah dimiliki. Karena sangat berbahaya bagi *network*, tidak digunakan dalam penelitian ini. Tahapan *Covering Track* untuk melakukan penghapusan aktivitas log pada mesin yang dimaksud. Jika mesin tujuan dikuasai secara penuh, ia akan dapat melakukan tugas ini. Dalam proses ini, *Metasploit* digunakan. Setelah penilaian selesai, akan ada prosedur untuk

meningkatkan keamanan jaringan nirkabel yang telah digunakan.

2.3 Kerangka Pikir

Diagram menunjukkan kerangka pikir penelitian untuk menyelesaikan masalah.



Gambar 4: Kerangka Pikir