

# SKRIPSI

*by Rafi Naufal*

---

**Submission date:** 25-Sep-2023 09:15AM (UTC+0530)

**Submission ID:** 2175955564

**File name:** BAB\_1\_-\_5\_1.pdf (769.05K)

**Word count:** 12432

**Character count:** 76456

## PENDAHULUAN

**1.1 Latar Belakang**

Keberadaan teknologi informasi saat ini merupakan sebuah hal yang sangat krusial dalam berbagai hal. Beberapa sektor yang membutuhkan penggunaan teknologi informasi ini diantaranya adalah perbankan, kesehatan, bisnis, pendidikan, dan dunia usaha [1]. Teknologi informasi juga digunakan dalam bidang pendidikan, terutama pada perguruan tinggi. Tata kelola teknologi informasi di perguruan tinggi diatur dalam Peraturan Menteri Riset Teknologi dan Pendidikan Tinggi Nomor 62 Tahun 2017 tentang Tata Kelola Teknologi Informasi. Tujuan penerapan tata kelola ini adalah untuk menyelaraskan perencanaan dan pengembangan serta implementasi teknologi informasi pada strategi bisnis atau capaian universitas [2].

Ketergantungan pada teknologi informasi semakin meningkat, begitu juga kompleksitasnya, sehingga memaksa organisasi untuk memiliki manajemen yang semakin efektif [3]. Maka dari itu diperlukan pengelolaan layanan teknologi informasi atau sering disebut *Information Technology Service Management (ITSM)*. ITSM merupakan pendekatan berorientasi proses yang bertujuan untuk mendefinisikan, mengelola, serta memberikan layanan teknologi informasi dengan benar. Pendekatan tersebut dilakukan untuk mencapai tujuan bisnis, serta memastikan kualitas layanan teknologi informasi untuk memenuhi tingkat layanan yang disepakati dengan pelanggan [4].

*Information Technology Infrastructure Library (ITIL)* adalah salah satu *framework* ITSM yang dapat membantu organisasi dalam mengelola layanan teknologi informasi secara efektif. Pada *framework* ITIL, khususnya pada ITIL v3 dibagi menjadi lima proses. Proses tersebut yaitu, *service strategy*, *service design*, *service transition*, *service operation*, dan *continual service improvement* [5].

Selain itu, keamanan sangat diperlukan dalam layanan teknologi informasi. Pelanggaran keamanan telah menyebabkan masalah besar bagi pelanggan, bisnis, dan perusahaan selama beberapa tahun terakhir [6]. Berdasarkan data lalu lintas internet yang didapatkan dari *Indonesian Security Incident Response Team on*

*Internet Infrastructure (Id-SIRTII)* pada tahun 2021, terdapat 10 serangan internet teratas. Serangan tersebut diantaranya adalah *MyIoBot*, serangan *trojan*, dan *Denial of Service (DoS) Vulnerability* [7]. Hal tersebut dikarenakan pada dasarnya jaringan komputer bersifat publik dan global sehingga tidak sepenuhnya aman [8]. Ketika data dikirim dari terminal asal menuju terminal tujuan, data tersebut akan melewati beberapa terminal lain sehingga ada peluang untuk pengguna internet lain dapat mengambil data tersebut [9]. Kebocoran data dapat merusak reputasi organisasi, menghabiskan uang dan sumber daya, serta dapat menyebabkan informasi sensitif, seperti nomor kartu kredit, tanggal lahir, atau kata sandi dapat dicuri [10].

Universitas Sultan Ageng Tirtayasa (Untirta) sebagai perguruan tinggi menerapkan tata kelola teknologi informasi. Hal tersebut diwujudkan dengan adanya Unit Pelaksana Teknis (UPT) Data dan Informasi Untirta. UPT Data dan Informasi Untirta memiliki beberapa layanan teknologi informasi. Layanan tersebut kebanyakan merupakan layanan berbasis web diantaranya adalah aplikasi web Untirta, Sistem Informasi Akademik (Siakad), e-Administrasi, dan Sistem Pembelajaran Daring (Spada). Layanan-layanan tersebut digunakan untuk membantu kebutuhan akademik serta memberikan informasi terkini yang ada di Untirta [11].

Pada kegiatan operasional UPT Data dan Informasi sempat ditemukan kendala pada layanan teknologi informasi. Beberapa waktu lalu, layanan teknologi informasi Untirta sempat mendapatkan sebuah insiden yang menyerang keamanan layanan teknologi informasi. Insiden tersebut yaitu serangan *Distributed Denial of Service (DDoS)* yang berdampak pada matinya layanan teknologi informasi Untirta untuk beberapa saat. Kemudian ditemukan permasalahan pada layanan Siakad Untirta yang mengalami *bug*. Selain itu, beberapa layanan teknologi informasi tidak berjalan dengan baik. Berdasarkan hal tersebut, maka diperlukan adanya keamanan teknologi informasi yang ketat disertai dengan manajemen yang benar dan tepat dalam layanan teknologi informasi Untirta.

Pada penanganan sebuah insiden, kerangka kerja ITIL v3 menjelaskan bagaimana cara memulihkan dan mencegah layanan teknologi informasi dari sebuah insiden. Salah satunya terdapat pada domain *service operation*. Pada domain tersebut terdapat proses *incident management* yang membahas tentang

bagaimana memulihkan layanan secepat mungkin dari suatu insiden salah satunya dari serangan keamanan. Selain itu, terdapat proses *problem management* yang membahas bagaimana mencegah masalah yang menyebabkan suatu insiden terjadi [12].

Selain itu, kerentanan yang terdapat pada layanan web dapat beragam, tergantung dari *module, library, Content Management System (CMS)*, serta *database* yang digunakan. Sehingga layanan teknologi informasi berbasis web memiliki banyak sisi yang dapat diserang. Berdasarkan hal tersebut, perlu dilakukan *vulnerability assessment* yang digunakan untuk mengevaluasi celah keamanan agar penggunaan layanan menjadi lebih efisien dan tidak terganggu oleh aktivitas serangan [13]. Setelah celah keamanan diketahui, maka akan diberikan rekomendasi yang sesuai dengan celah yang ditemukan untuk menghindari serangan terhadap layanan teknologi informasi di masa mendatang.

Terdapat penelitian terkait yang telah membahas evaluasi manajemen layanan teknologi informasi dengan menggunakan *framework ITIL v3*. Pada penelitian ini membahas evaluasi *maturity level* pada manajemen layanan teknologi informasi di perusahaan 24Slides. Penelitian tersebut menggunakan *framework ITIL v3* domain *service operation* untuk mengukur *maturity level*, analisis kesenjangan, serta membuat rekomendasi untuk perbaikan. Hasil penelitian menampilkan skor *maturity level* memiliki nilai rata-rata 2,6 dan termasuk ke dalam kategori *repeatable* dengan nilai kesenjangan 0,8 [14].

Terdapat juga penelitian terkait yang telah membahas evaluasi keamanan pada layanan berbasis web. Pada penelitian ini dijelaskan *vulnerability assessment* dan analisis model kematangan pada web di pendidikan tinggi di Indonesia. Penilaian kerentanan dilakukan dengan menggunakan *tools* Nessus dan Skipfish pada beberapa universitas di Jakarta. Hasil penilaian didapatkan 60% dari 33 situs memiliki kematangan di bawah angka 3 yang berarti tingkat kerentanan pada situs web tersebut masih tinggi [15].

Berdasarkan latar belakang tersebut, pada penelitian ini akan dilakukan evaluasi kematangan layanan teknologi informasi pada UPT Data dan Informasi Untirta dengan melakukan uji keamanan pada layanan teknologi informasi menggunakan *vulnerability assessment* serta pengukuran kematangan manajemen

79 layanan teknologi informasi dengan melakukan penyebaran kuesioner menggunakan kerangka kerja ITIL V3. 84 Hal tersebut dilakukan untuk mengetahui sejauh mana tingkat keamanan dan manajemen layanan teknologi informasi pada UPT Data dan Informasi Untirta. Dari hasil yang telah didapatkan kemudian diberikan rekomendasi yang diperlukan agar penerapan keamanan dan manajemen layanan teknologi informasi di Untirta dapat lebih baik dari sebelumnya.

## 2 1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, didapatkan rumusan masalah sebagai berikut.

1. Bagaimana evaluasi keamanan layanan teknologi informasi di UPT Data dan Informasi Untirta menggunakan *vulnerability assessment* dan forensik jaringan?
2. Bagaimana evaluasi manajemen layanan teknologi informasi di UPT Data dan Informasi Untirta menggunakan kerangka kinerja ITIL v3 menggunakan domain *service operation*?
3. Berdasarkan evaluasi yang telah dilakukan, bagaimana rekomendasi yang diberikan untuk UPT Data dan Informasi Untirta untuk meningkatkan kualitas manajemen dan keamanan layanan teknologi informasi yang ada di Untirta?

## 10 1.3 Tujuan Penelitian

Penelitian ini dilakukan untuk mencapai beberapa tujuan diantaranya adalah sebagai berikut.

1. Mengetahui sejauh mana tingkat kerentanan layanan teknologi informasi pada UPT Data dan Informasi dengan *vulnerability assessment* dan forensik jaringan.
2. Mengetahui sejauh mana tingkat kematangan layanan teknologi informasi di UPT Data dan Informasi Untirta dengan menggunakan kerangka kinerja ITIL V3 domain *service operation*.

3. Memberikan rekomendasi yang dapat digunakan oleh UPT Data dan Informasi untuk meningkatkan kualitas keamanan dan manajemen layanan teknologi informasi di Untirta.

#### **1.4 Manfaat Penelitian**

Manfaat yang dapat diambil dari hasil penelitian ini diantaranya adalah sebagai berikut.

1. Bagi peneliti, hasil penelitian ini dapat menjadi pengetahuan tentang bagaimana mengukur kematangan layanan teknologi informasi menggunakan kerangka kerja ITIL V3 dan bagaimana mengukur kerentanan layanan teknologi informasi menggunakan *vulnerability assessment* dan forensik jaringan.
2. Bagi akademisi, hasil penelitian ini dapat menjadi referensi bagi para akademisi yang sedang melakukan penelitian terkait evaluasi manajemen dan keamanan layanan teknologi informasi menggunakan kerangka kerja ITIL V3 dan *vulnerability assessment*.
3. Bagi universitas, hasil penelitian ini dapat menjadi acuan dan evaluasi keamanan dan manajemen pada layanan teknologi informasi Untirta agar kedepannya menjadi lebih baik dari sebelumnya.

#### **1.5 Batasan Masalah**

Batasan masalah penelitian ini, diantaranya adalah:

1. Penelitian dilakukan pada layanan teknologi informasi pada UPT Data dan Informasi Untirta.
2. Metode pengumpulan data menggunakan studi pustaka, kuesioner, dan observasi.
3. Layanan teknologi informasi yang akan menjadi sampel penelitian adalah SIAKAD, SPADA, Web Untirta, Web FT Untirta, dan e-Administrasi Untirta.
4. Evaluasi dibagi menjadi dua yaitu keamanan dan manajemen
5. Evaluasi keamanan dilakukan dengan melakukan *vulnerability assessment* dan forensik jaringan. Pada *vulnerability assessment*, sistem operasi yang

digunakan adalah Kali Linux, dan *tool* yang akan digunakan adalah Nmap dan Nessus.

6. Evaluasi manajemen dilakukan dengan menggunakan kerangka kinerja ITIL v3 domain *service operation*. *Template* kuesioner yang digunakan adalah UCISA *service operation readiness* sub-domain *service operation process* dan *common service operation activities*.
7. Hasil akhir penelitian ini berupa rekomendasi terhadap evaluasi keamanan dan manajemen yang bersifat deskriptif.

## 1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini akan menjelaskan secara singkat isi dari penelitian ini dari awal sampai akhir. Laporan penelitian ini terdiri dari 5 bab dan isi dari setiap bab dapat diuraikan sebagai berikut.

BAB I Pendahuluan, berisi uraian latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, serta sistematika penulisan. BAB II Tinjauan Pustaka, berisi uraian teori-teori serta penelitian serupa yang berkaitan dengan keamanan informasi, *vulnerability assessment*, ITSM, serta ITIL v3.

BAB III Metodologi Penelitian, berisi uraian tentang alur, metode, dan alat-alat yang digunakan untuk evaluasi layanan teknologi informasi menggunakan ITIL v3 dan *vulnerability assessment*. BAB IV Hasil dan pembahasan, berisi uraian dan analisis dari hasil *vulnerability assessment* dan kuesioner ITIL v3, serta uraian rekomendasi yang diberikan berdasarkan hasil yang telah didapatkan. BAB V Penutup, berisi kesimpulan dari penelitian yang telah dilakukan serta saran untuk penelitian-penelitian terkait selanjutnya.

## BAB II

### TINJAUAN PUSTAKA

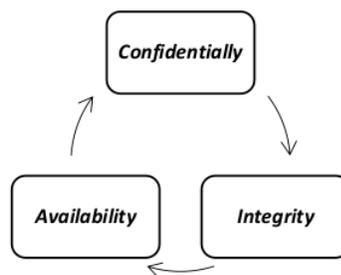
#### 2.1 Layanan Teknologi Informasi

Layanan teknologi informasi adalah sarana yang disediakan oleh industri maupun organisasi kepada penggunanya untuk menyampaikan nilai atau manfaat tanpa adanya risiko tertentu [16]. Layanan teknologi informasi merupakan campuran dari teknologi informasi, orang, dan proses.

Layanan teknologi informasi yang menghadap pelanggan secara langsung menunjang proses bisnis satu atau lebih pelanggan dan target tingkat layanannya wajib ditetapkan dalam *Service Level Agreement* (SLA). Layanan teknologi informasi yang lain disebut sebagai layanan pendukung (*supporting services*). Layanan tersebut tidak digunakan secara langsung oleh bisnis, tetapi diperlukan oleh penyedia layanan untuk menyediakan layanan yang berhadapan langsung dengan pelanggan [17].

#### 2.2 Keamanan Informasi

Keamanan informasi merupakan sebuah proses pengamanan aset informasi terhadap ancaman dan kerentanan [18]. Tujuan utama keamanan informasi ialah melindungi kerahasiaan, integritas, serta ketersediaan informasi. Keamanan jaringan bertujuan untuk menjaga kerahasiaan, integritas, dan aksesibilitas jaringan komputer dan data yang dikirimkan dalam media komunikasi. Pada keamanan informasi, terdapat prinsip utama yang dijelaskan pada Gambar 2.1.



Gambar 2.1 Prinsip Utama dalam Keamanan Informasi

Pada Gambar 2.1, dijelaskan bahwa <sup>54</sup> terdapat tiga prinsip utama pada keamanan informasi, yaitu kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) atau sering disebut CIA *triad*.

1. Kerahasiaan berkaitan dengan perlindungan informasi dari pengguna dan program yang tidak sah di dunia digital. Kerahasiaan dibagi kedalam dua pengertian yaitu kerahasiaan data dan *privacy*. Kerahasiaan data merupakan adanya jaminan bahwa informasi rahasia atau informasi privat tidak dapat diubah atau diganti oleh seseorang yang tidak memiliki otoritas. Sementara itu, *privacy* merupakan adanya jaminan bahwa seseorang hanya mengendalikan informasi yang terkait dengan dirinya, dapat dikumpulkan atau disimpan dan oleh siapa serta untuk siapa informasi tersebut dapat dibuka.
2. Integritas berkaitan dengan akurasi, kualitas, konsistensi, dan kelengkapan data selama seluruh siklus hidupnya. Integritas dibagi kedalam dua konsep yaitu integritas data dan sistem. Integritas data merupakan jaminan sebuah informasi dan program dapat berubah dengan cara yang spesifik dan terotorisasi. Sementara itu, integritas sistem merupakan jaminan sebuah sistem melakukan fungsi yang diinginkan dalam suatu keadaan yang terhindar dari campur tangan pihak yang tidak terotorisasi.
3. Ketersediaan berkaitan dengan aksesibilitas data. Ketersediaan berarti data selalu tersedia saat pengguna resmi meminta atau menggunakannya [19]. Ketersediaan merupakan adanya jaminan bahwa sistem bekerja dengan benar dan layanan kepada pihak pengguna yang memiliki otoritas tidak terganggu [20].

Terdapat beberapa pembagian jenis keamanan informasi, yaitu <sup>67</sup> *physical security*, *personal security*, *operational security*, *communications security*, dan *network security* [21].

### 2.3 Website

*Website* pada dasarnya merupakan kumpulan dokumen yang berisi data serta informasi yang dapat diakses melalui internet. Selain itu, *website* bisa berjalan di berbagai macam *platform* serta termasuk aplikasi yang ringan untuk digunakan

[13]. *Website* saat ini menjadi sumber informasi utama dan digunakan untuk berbagai kegiatan [15]. Setiap tahun, semakin banyak aplikasi berbasis web. Seiring dengan waktu dan semakin kompleksnya layanan dan aplikasi web dalam berbagai bidang, permintaan layanan web dari pengguna terus bertambah. Pada kuartal pertama tahun 2020, ada sekitar 367 juta nama domain. Masing-masing *website* ini dapat dianggap sebagai aplikasi web statis atau dinamis [6].

Pertumbuhan *website* di Indonesia sendiri terus bertambah secara signifikan. Fenomena ini terus bertambah sebanding dengan jumlah pengguna layanan internet di Indonesia yang meningkat dari tahun ke tahun. Berbagai macam *website* yang kerap diakses oleh pengguna di Indonesia antara lain: mesin pencari, *e-commerce*, forum sosial, dan portal berita [22].

#### 2.4 Kerentanan dan Serangan Keamanan Informasi

Pelanggaran terhadap keamanan layanan teknologi informasi telah menyebabkan masalah besar bagi pelanggan, bisnis, dan perusahaan selama beberapa tahun terakhir [6]. Hal tersebut dikarenakan jaringan komputer bersifat publik dan global yang pada dasarnya tidak aman [8]. Pada sebuah layanan teknologi informasi tidak jarang menyimpan data-data pengguna terlebih lagi data yang bersifat pribadi seperti tanggal lahir, nomor telepon, serta data penting lainnya [23]. Ketika sebuah data terkirim dari satu terminal asal menuju ke terminal tujuan, data tersebut akan melewati beberapa terminal lain yang berarti akan memberi peluang untuk pengguna internet lain untuk mengambil data tersebut [9].

Kerentanan atau *vulnerability* adalah kelemahan dalam produk atau sistem yang berpotensi memungkinkan penyerang merusak kerahasiaan, integritas, atau ketersediaan produk atau sistem tersebut. Penyerang dapat mengeksploitasi kerentanan yang ada di perangkat lunak, *firewall*, protokol jaringan, jaringan nirkabel, sistem operasi, dan web *server*. Dari kerentanan tersebut, penyerang dapat melakukan serangannya.

Pada saat ini, serangan terhadap keamanan informasi semakin bervariasi. Berdasarkan data lalu lintas internet yang dihimpun dari *Indonesian Security Incident Response Team on Internet Infrastructure* (Id-SIRTII) pada tahun 2021, terdapat 10 serangan teratas beberapa diantaranya adalah *MyIoBot*, serangan *trojan*,

dan *Denial of Service* (DoS) [7]. Serangan tersebut dapat dibagi menjadi tiga jenis: serangan berbasis kelemahan perangkat keras, serangan *bug* berbasis perangkat lunak, dan serangan berbasis kerentanan dalam jaringan komputer.

Serangan berbasis kelemahan perangkat keras lebih sulit dicegah dikarenakan alat berbasis perangkat lunak saja tidak cukup untuk mendeteksi dan mencegah serangan terkait perangkat keras. Virus *Trojan* sering kali menjadi akar penyebab serangan perangkat keras. Varian perangkat lunak berbahaya ini menyebabkan penggunaan sumber daya komputer yang berlebihan, mengurangi kinerja, dan menyebabkan sistem mati dengan mengonsumsi daya yang berlebihan. Contoh serangan berbasis kelemahan perangkat keras adalah *Trojan*, *Rowhammer*, *logic bomb* dan *Malware*.

Serangan *bug* berbasis perangkat lunak disebabkan oleh kesalahan yang ada dalam perangkat lunak. Beberapa penyebab diantaranya adalah kesalahan yang terdapat pada *input* validasi, akses kendali, otentikasi, dan direktori. Selain itu, penyebab kesalahan perangkat lunak juga dapat disebabkan oleh masalah <sup>21</sup>*Structured Query Language* (SQL), *Cross-site scripting* (XSS), komponen yang memiliki kerentanan, layanan web dan *Application Programming Interface* (API) yang bermasalah, dan pengujian keamanan perangkat lunak yang tidak tepat. Contoh serangan *bug* berbasis perangkat lunak adalah *SQL Injection*, XSS, dan *Buffer overflow*.

Serangan berbasis kerentanan dalam jaringan komputer disebabkan kerentanan dalam protokol jaringan, seperti <sup>21</sup>*Transmission Control Protocol* (TCP), *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Dynamic Host Configuration Protocol* (DHCP), dan *Domain Name System* (DNS). Misalnya, karena tidak ada struktur untuk mengontrol keakuratan dan kerahasiaan paket saat membawanya melalui jaringan menggunakan IP, informasi dalam paket dapat diekspos dan diubah selama pengiriman. Demikian pula, karena respons DNS tidak diverifikasi, penyerang dapat membuat *server* palsu, dan pengguna mungkin terhubung ke *server* palsu ini, bukan ke *server* yang sebenarnya.

Penyerang juga dapat mengirim permintaan berlebihan ke *server* DNS, membuatnya tidak tersedia untuk pengguna yang sah. Selain itu, penyerang dapat menangkap informasi selama transportasi data karena konfigurasi perangkat

jaringan yang tidak lengkap atau salah, termasuk sakelar, *router*, dan titik akses nirkabel. Contoh serangan berbasis kerentanan dalam jaringan komputer adalah DoS (*Denial of Services*), MiTM (*Man in The Middle*), dan *Spoofing* [19]. Berikut beberapa penjelasan terkait kerentanan dan serangan keamanan informasi.

a. *Distributed Denial of Service* (DDoS)

*Distributed Denial of Service* (DDoS) merupakan salah satu serangan jaringan dimana penyerang berusaha membuat sumber daya jaringan tidak tersedia untuk pengguna sementara waktu. Serangan ini biasa dilakukan dengan membanting perangkat target. Serangan dilakukan dari beberapa komputer sekaligus menuju target yang disebut sebagai *zombie* atau *botnet*. DDoS memiliki tipe serangan, diantaranya adalah *UDP Flood*, *ICMP Flood*, dan *SYN Flood* [24].

Perubahan ukuran data menuju target serangan dapat meningkatkan level serangan serta menyebabkan peningkatan konsumsi daya listrik begitu juga dengan beban CPU pada *router* yang dilewati data tersebut. Teknik mitigasi yang biasa dilakukan untuk mengurangi dampak dari serangan DDoS adalah dengan *blackholing* untuk penyediaan *upstreams* atau pemberitahuan perubahan jalur [25].

b. *SQL injection*

*SQL injection* adalah salah satu metode untuk mengeksploitasi aplikasi *website* dengan menggunakan data yang disediakan atau diselipkan ke dalam kueri SQL. Serangan *SQL injection* dapat menyebabkan *server* mengembalikan data yang seharusnya dibatasi, menjalankan perintah *Data Definition Language* (DDL) yang menghapus atau mengubah objek *database*, atau sekadar menghapus data dari tabel.

*SQL injection* berkerja dengan cara memasukkan kueri SQL atau perintah (*command*) sebagai *input* yang dimungkinkan melalui halaman web atau *command prompt*. Halaman web akan mengambil parameter dari pengguna kemudian membuat kueri SQL tembus ke dalam *database*. Cara ini membuat *SQL injection* dapat dikatakan pula sebagai aktivitas yang mengelabui kueri pada *database*, sehingga pengguna yang tidak diautentikasi dapat mengetahui serta mengambil data dan informasi yang berada dalam *database* [26].

<sup>76</sup>  
c. **Cross Site Scripting (XSS)**

**Cross Site Scripting (XSS)** merupakan serangan injeksi kode dengan memasukkan skrip berbahaya. Perbedaan utama antara *SQL Injection* dan XSS adalah teknologi dasar yang menjadi sasaran serangan. *SQL Injection* menyuntikkan kode SQL berbahaya, sedangkan serangan XSS menyuntikkan JavaScript [27]. Skrip yang sudah diinjeksi ini bisa dijalankan dengan hampir seluruh *client-side script*. Serangan ini dapat menimbulkan berbagai ancaman keamanan. Hal tersebut termasuk pencurian identitas, akses ke informasi yang bersifat sensitif dan terbatas, perubahan fungsionalitas web, serta ancaman dari serangan DoS [28].

d. **DNS spoofing**

**DNS spoofing** merupakan salah satu teknik serangan *Man in The Middle Attack* (MiTM). **DNS spoofing** merupakan proses memalsukan paket DNS pada jaringan DNS dengan mengubah alamat domain menjadi alamat palsu. Metode ini mengeksploitasi *server* yang memiliki kerentanan untuk memodifikasi data yang disimpan yang kemudian akan digunakan oleh sistem yang menjadi target [29]. **DNS Spoofing** dapat mengalihkan web yang memiliki konten positif dengan web yang memiliki konten negatif.

<sup>24</sup>  
2.5 **Vulnerability Assessment**

**Vulnerability Assessment** merupakan proses mendefinisikan, mengidentifikasi, dan mengklasifikasikan celah keamanan (kerentanan) pada komputer, jaringan, atau infrastruktur komunikasi. Selain itu, *vulnerability assessment* dapat memperkirakan keefektifan tindakan pencegahan yang diusulkan dan mengevaluasi keefektifan aktualnya setelah diterapkan. Hasil kegiatan *vulnerability assessment* dapat digunakan untuk menentukan tingkat kematangan keamanan suatu *website*.

Tingkat kematangan ini dapat digunakan untuk mengukur sejauh mana penerapan kendali keamanan telah diterapkan pada suatu *website*, sehingga dapat diambil tindakan korektif untuk menghadapi ancaman yang dapat ditimbulkan oleh kerentanan keamanan pada *website* [15]. Berikut adalah beberapa *tool* yang dapat digunakan untuk melakukan *vulnerability assessment*.

a. Nmap

*Network Mapper* atau biasa disebut dengan Nmap merupakan salah satu <sup>24</sup> *tool* yang digunakan dalam melakukan audit keamanan jaringan serta melakukan eksplorasi jaringan. Nmap bersifat *open source* dan bekerja lebih optimal di sistem operasi Linux daripada Windows. Nmap dapat melakukan pemindaian jaringan dengan teknik *port scanning*, *ping scanning*, <sup>46</sup> *ping scan TCP SYN*, *ping scan TCP ACK*, *ping scan UDP*, *ping scan ICMP*, dan *ping scan IP* [30].

b. Nessus

<sup>22</sup> Nessus merupakan salah satu *tool vulnerability scanner* untuk keamanan jaringan yang wajib digunakan oleh administrator sistem. Nessus adalah *software scanning*, yang dapat digunakan untuk mengaudit keamanan suatu sistem, seperti kerentanan, kesalahan konfigurasi, *patch* keamanan yang belum diterapkan, *password default*, dan DoS. Nessus berfungsi untuk memantau lalu lintas jaringan. Karena Nessus berfungsi juga untuk mendeteksi kerentanan atau cacat pada suatu sistem, Hal tersebut menjadikan Nessus sebagai salah satu alat yang andal dalam melakukan audit keamanan suatu sistem [15].

<sup>25</sup> *Tool Nessus* memiliki sistem penilaian yang disebut *Common Vulnerability Scoring System (CVSS)*. CVSS adalah metode penilaian untuk menilai kerentanan pada pengujian sistem. CVSS diklasifikasikan berdasarkan *score* pada tingkat penilaian yaitu *None*, *Low*, *Medium*, *High*, dan *Critical* [31]

## 2.6 Forensik Jaringan

<sup>8</sup> Forensik jaringan adalah salah satu bagian dari forensik digital, dimana bukti dari jaringan ditangkap kemudian diinterpretasikan berdasarkan pengetahuan dari serangan jaringan. Bukti yang digunakan untuk melakukan forensik jaringan salah satunya adalah *log* jaringan saat serangan terjadi. Forensik jaringan dapat memberikan beberapa informasi, diantaranya adalah IP *address* penyerang, lokasi penyerang, jenis paket yang terkirim, dan beban CPU.

Tujuan dari forensik jaringan adalah untuk menemukan penyerang serta merekonstruksi kejadian pada saat serangan melalui analisis bukti penyusupan [25]. Forensik jaringan adalah tentang mencari tahu bagaimana keamanan dilanggar dan mengambil tindakan yang tepat untuk masa depan [32]. Forensik jaringan menjadi

perangkat yang sangat penting dalam melindungi keamanan serta mencari tahu pelanggaran keamanan yang dapat berdampak kepada suatu individu, perusahaan, maupun lembaga pemerintahan.

## 2.7 <sup>1</sup> Manajemen Layanan Teknologi Informasi

Manajemen layanan teknologi informasi atau *Information Technology Service Management* (ITSM) merupakan sebuah <sup>13</sup> implementasi dan pengelolaan layanan teknologi informasi berkualitas yang memenuhi kebutuhan bisnis. Manajemen layanan teknologi informasi dilakukan oleh penyedia layanan teknologi informasi melalui perpaduan yang tepat antara orang, proses, dan teknologi informasi. <sup>2</sup> Manajemen layanan teknologi informasi harus dilakukan secara efektif dan efisien. Mengelola teknologi informasi dari perspektif bisnis memungkinkan kinerja tinggi organisasi dan penciptaan nilai [17].

Fokus ITSM adalah mengelola siklus hidup penuh layanan teknologi informasi. Ruang lingkupnya biasanya tidak mencakup manajemen proyek atau program, dan juga tidak mencakup pengembangan aplikasi atau perangkat lunak. Namun, proses ITSM harus dirancang dan diimplementasikan dengan cara yang selaras dan terintegrasi dengan manajemen proyek dan program serta proses pengembangan aplikasi dan perangkat lunak.

Pada ITSM terdapat beberapa kerangka kerja. Kerangka kerja tersebut menjelaskan praktik terbaik yang dapat digunakan organisasi teknologi informasi untuk mengimplementasikan dan terus meningkatkan kemampuan ITSM mereka. Banyak organisasi mengadopsi dan mengadaptasi praktik terbaik dari berbagai kerangka kerja dalam upaya mengembangkan serangkaian proses yang memenuhi kebutuhan mereka. Kerangka ITSM yang paling umum digunakan adalah: <sup>42</sup> *Information Technology Infrastructure Library* (ITIL), *Control Objectives for Information and Related Technology* (COBIT), dan *Microsoft Operations Framework* (MOF). Kerangka kerja khusus vendor meliputi *IBM Tivoli Unified Process* dan *HP Service Management Framework* [33].

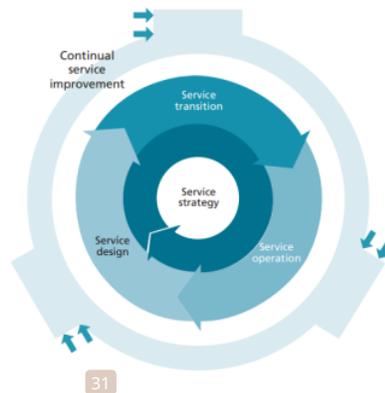
## 2.8 ITIL V3 Service Operation

*Information Technology Infrastructure Library (ITIL)* adalah salah satu aplikasi terbaik untuk manajemen layanan teknologi informasi. ITIL menawarkan pendekatan sistematis guna memberikan layanan teknologi informasi yang bermutu. ITIL membantu penyedia layanan dalam memberikan panduan tentang penyediaan layanan teknologi informasi yang bermutu, serta proses, fungsi, dan kemampuan lain yang dibutuhkan untuk mendukungnya. Digunakan oleh ratusan organisasi di seluruh dunia, ITIL membagikan panduan aplikasi terbaik yang berlaku untuk seluruh jenis organisasi yang menyediakan layanan teknologi informasi [17].

ITIL dikembangkan pada tahun 1980-an dan 1990-an oleh *Central Computer and Telecommunications Agency (CCTA)*, yang saat ini bernama *Office of Government Commerce (OGC)*, di bawah kontrak dengan Pemerintah Inggris. Semenjak saat itu, ITIL tidak hanya menawarkan kerangka kerja berbasis praktik terbaik untuk manajemen TI, namun juga pendekatan serta filosofi yang dibagikan oleh orang-orang yang bekerja dengannya dalam aplikasi. ITIL sudah mengalami dua kali perubahan. Perubahan pertama dilakukan pada tahun 2000-2002 (ITIL V2), dan yang kedua dilakukan pada tahun 2007 (ITIL V3). ITIL didukung oleh *IT Service Management Forum (itSMF)*, sebuah organisasi nirlaba yang diakui secara internasional yang didedikasikan untuk menunjang pengembangan ITSM [34].

Perubahan kedua ITIL pada tahun 2007 diterbitkan sebagai tanggapan atas kemajuan signifikan dalam teknologi dan tantangan yang muncul bagi penyedia layanan teknologi informasi. Model serta arsitektur baru seperti *outsourcing*, layanan bersama, komputasi utilitas, komputasi awan, virtualisasi, layanan web, serta perdagangan seluler telah tersebar luas di dalam teknologi informasi. Pendekatan berbasis proses ITIL ditambah dengan siklus hidup layanan untuk mengatasi tantangan manajemen layanan tambahan ini.

Kerangka kerja ITIL didasarkan pada lima tahap siklus hidup yang dijelaskan pada Gambar 2.2.



Gambar 2.2 Siklus Hidup Layanan ITIL [17]

Gambar 2.2 merupakan siklus hidup layanan ITIL. Siklus hidup pada kerangka kerja ITIL v3 menggunakan desain *hub-and-spoke*, dengan *service strategy* di *hub*, kemudian *service design*, *transition*, dan *operation* di siklus hidup bergulir atau jari-jari. *Continual service improvement* meliputi serta menunjang seluruh tahapan siklus hidup layanan.

Setiap tahap siklus hidup memengaruhi yang lain serta bergantung pada masukan dan umpan balik mereka. Menggunakan metode ini, serangkaian pemeriksaan dan keseimbangan yang konstan sepanjang siklus hidup layanan memastikan layanan dapat beradaptasi dan merespons secara efektif saat permintaan bisnis berubah seiring dengan kebutuhan bisnis. Siklus hidup layanan, memiliki publikasi utama membagikan panduan tentang aplikasi terbaik di tiap tahap. Panduan ini mencakup prinsip-prinsip utama, proses serta aktivitas yang dibutuhkan, organisasi dan peran, teknologi, tantangan terkait, aspek penentu keberhasilan, serta risiko.

Pada panduan inti ITIL, terdapat 26 proses dan empat fungsi yang dijelaskan. Definisi proses adalah sekumpulan aktivitas terstruktur yang ditujukan untuk mencapai tujuan tertentu. Suatu proses mengambil satu atau lebih *input* spesifik dan mengubahnya menjadi *output* tertentu. Sedangkan definisi fungsi adalah tim atau sekelompok orang dan alat atau sumber daya lain yang digunakan untuk melakukan satu atau lebih proses atau aktivitas. Proses dan fungsi berjalan sepanjang siklus hidup layanan tetapi sebagian besar dimiliki oleh satu tahap siklus hidup [35].

Perbedaan kerangka kerja ITIL dengan yang lain seperti COBIT 5, ITIL memiliki 5 domain sedangkan COBIT hanya memiliki 4 domain. Perbedaan

lainnya, pada ITIL proses dijelaskan dan dikelola pada setiap aktivitas dan *flowchart*. Penggunaan ITIL diharapkan dapat memberikan arahan untuk organisasi dalam penggunaan teknologi informasi yang efektif dan efisien. Selain itu, ITIL menjelaskan bagaimana merencanakan, merancang, dan mengimplementasikan fungsi manajemen layanan secara efektif. Sementara itu, COBIT berfokus pada apa yang perlu dilakukan untuk memastikan tata kelola yang baik dari semua proses teknologi informasi terkait, termasuk proses manajemen layanan informasi. COBIT memberikan panduan, kerangka kerja, dan alat untuk mencapai tingkat kepatuhan dan kinerja yang diinginkan untuk proses teknologi informasi yang diperlukan untuk memenuhi kebutuhan bisnis [36].

*Service operation* merupakan salah satu domain yang termasuk dalam kerangka kerja ITIL v3. Domain ini menjelaskan praktik terbaik untuk mengelola layanan di lingkungan yang didukung. *Service operation* mencakup panduan untuk mencapai efektivitas dan efisiensi dalam penyampaian dan dukungan layanan untuk memastikan nilai bagi pelanggan, pengguna, dan penyedia layanan. Tujuan strategis pada akhirnya diwujudkan melalui layanan operasi, menjadikan *service operation* sebagai kemampuan yang kritis.

*Service operation* memberikan panduan untuk menjaga stabilitas dalam operasi layanan dan memungkinkan perubahan dalam desain, skala, cakupan, dan tingkat layanan. Organisasi diberikan panduan terperinci tentang proses, metode, dan alat yang dapat digunakan untuk dua perspektif *main control*, yaitu reaktif dan proaktif. Manajer dan praktisi diberikan pengetahuan yang memungkinkan mereka untuk membuat keputusan yang lebih baik di berbagai bidang seperti manajemen ketersediaan layanan, kendali permintaan, optimalisasi pemanfaatan kapasitas, penjadwalan operasional, pencegahan atau penyelesaian insiden layanan, dan manajemen masalah.

a. Proses dalam *service operation*

Pada *service operation*, terdapat sejumlah proses utama yang harus terhubung bersama untuk menyediakan struktur dukungan teknologi informasi yang efektif secara keseluruhan. *Service operation* memiliki lima proses utama:

### 2 1. *Event management*

*Event management* mengelola *event* sepanjang siklus hidupnya. Siklus hidup ini melibatkan koordinasi aktivitas untuk mendeteksi peristiwa, memahaminya, dan menentukan tindakan kendali yang sesuai.

### 2. *Incident management*

*Incident management* berfokus pada pemulihan layanan yang secara tidak terduga terdegradasi atau terganggu kepada pengguna secepat mungkin untuk meminimalkan dampak bisnis.

### 3. *Problem management*

*Problem management* mencakup analisis akar penyebab untuk mengidentifikasi dan menyelesaikan akar penyebab insiden, dan aktivitas proaktif untuk mengidentifikasi dan mencegah masalah atau insiden di masa depan. Hal ini termasuk juga pembuatan catatan atau *database* kesalahan yang diketahui, yang mendokumentasikan akar penyebab dan solusi untuk memungkinkan diagnosis dan resolusi yang lebih cepat jika insiden lebih lanjut terjadi.

### 4. *Request fulfilment*

*Request fulfilment* adalah proses untuk mengelola siklus hidup semua permintaan layanan. Permintaan layanan dikelola sepanjang siklus hidupnya, dari permintaan awal hingga pemenuhan, menggunakan catatan atau tabel pemenuhan permintaan terpisah untuk mencatat dan melacak statusnya.

### 5. *Access management*

*Access management* merupakan proses pemberian hak kepada pengguna yang berwenang untuk menggunakan layanan sambil membatasi akses ke pengguna yang tidak berwenang. Hal ini bergantung pada kemampuan untuk secara akurat mengidentifikasi pengguna yang berwenang kemudian mengelola kemampuan mereka untuk mengakses layanan sesuai kebutuhan untuk peran organisasi atau fungsi kerja spesifik mereka.

#### b. Fungsi dalam *service operation*

Proses saja tidak mengarah pada operasi layanan yang efektif. Infrastruktur yang stabil dan staf yang terampil juga diperlukan. *Service operation* bergantung

pada berbagai fungsi untuk melakukan tugas operasional supaya hal tersebut dapat tercapai. Fungsi mencakup kelompok individu terampil yang melakukan satu atau lebih proses dan aktivitas siklus hidup layanan. Ada empat fungsi utama dalam operasi layanan:

### 1. *Service desk*

*Service desk* adalah titik kontak tunggal bagi pengguna jika terjadi gangguan layanan, untuk permintaan layanan, atau bahkan untuk beberapa kategori *Request for Change* (RFC). *Service desk* adalah titik komunikasi bagi pengguna dan titik koordinasi untuk berbagai kelompok dan proses teknologi informasi.

### 2. *Technical management*

*Technical management* menyediakan keterampilan teknis terperinci dan sumber daya yang diperlukan untuk mendukung operasi berkelanjutan dari layanan teknologi informasi dan pengelolaan infrastruktur teknologi informasi. *Technical management* juga memainkan peran penting dalam merancang, menguji, merilis, dan meningkatkan layanan teknologi informasi. Pada organisasi kecil dimungkinkan untuk mengelola keahlian ini dalam satu departemen, tetapi organisasi yang lebih besar biasanya dibagi menjadi beberapa departemen teknis khusus.

### 3. *IT operations management*

*IT operations management* menjalankan kegiatan operasional sehari-hari yang diperlukan untuk mengelola layanan teknologi informasi dan infrastruktur teknologi informasi pendukung. Hal ini dilakukan sesuai dengan standar kinerja yang ditetapkan selama *service design*. Di beberapa organisasi ini merupakan satu departemen terpusat, sementara di organisasi lain terdapat beberapa kegiatan serta staf terpusat dan beberapa disediakan oleh departemen terdistribusi atau khusus. *IT operations management* memiliki dua sub-fungsi yang unik dan umumnya berbeda secara organisasi. Kedua sub-fungsi tersebut, adalah:

- a. *IT operations control*. Ini biasanya dikelola oleh *shift operator* yang memastikan bahwa tugas operasional rutin dilakukan. Kendali operasi teknologi informasi juga menyediakan aktivitas pemantauan

dan pengendalian terpusat, biasanya melalui jembatan operasi atau pusat operasi jaringan.

- b. *Facilities management*. Ini mengacu pada pengelolaan lingkungan fisik teknologi informasi, biasanya pusat data atau ruang komputer. Di banyak organisasi, manajemen teknis dan aplikasi ditempatkan bersama dengan operasi teknologi di pusat data besar.

#### 4. *Application management*

*Application management* bertanggung jawab untuk mengelola aplikasi sepanjang siklus hidupnya. Fungsi manajemen aplikasi mendukung dan memelihara aplikasi operasional dan juga memainkan peran penting dalam merancang, menguji, dan meningkatkan aplikasi yang merupakan bagian dari layanan TI.

ITIL memandang manajemen aplikasi secara berbeda dari pengembangan aplikasi. Di dalam TI, pengembangan aplikasi biasanya difokuskan pada aktivitas internal untuk merancang, membangun, menguji, dan menyebarkan solusi teknologi informasi yang sedang dibangun di dalam organisasi TI. *Application management* mengambil pandangan yang jauh lebih luas yang mengakui kemampuan di pasar saat ini untuk mendapatkan aplikasi dari banyak sumber selain organisasi teknologi informasi internal. Selain itu, ini juga berfokus pada pengelolaan dan pemeliharaan aplikasi yang berkelanjutan yang terjadi setelah aplikasi diterapkan.

## 2.9 Layanan Teknologi Informasi di Untirta

UPT Data dan Informasi Untirta memiliki layanan teknologi informasi yang dapat membantu pelayanan akademik serta administrasi di Untirta. Terdapat sekitar 33 layanan teknologi informasi yang dimiliki UPT Data dan Informasi Untirta [11]. Layanan ini digunakan untuk mempermudah dalam akses serta efisiensi dalam kebutuhan akademik maupun administrasi universitas dimana saja dan kapan saja.

Beberapa layanan teknologi informasi tersebut diantaranya adalah Sistem Informasi Akademik (SIKAD), Sistem Informasi Kinerja (SIKITA) Untirta, Sistem Pembelajaran Daring (SPADA), Sistem Informasi Tugas Akhir (SISTA), e-Administrasi, dan Solusi Laporan Terkini Antar Sivitas (SULTANS). Layanan

Untirta yang sering digunakan untuk kebutuhan akademik adalah SIAKAD dan SPADA, sedangkan layanan yang sering digunakan untuk kebutuhan administrasi adalah e-Administrasi.

## 2.10 Maturity Model

*Maturity model* merupakan alat yang digunakan untuk mengukur seberapa baik kinerja atau proyek sesuatu organisasi atau perusahaan dan seberapa jauh organisasi tersebut melakukan perbaikan berkelanjutan. Tidak seperti alat pengukur yang digerakkan oleh tujuan lainnya, *maturity model* dapat mengevaluasi data kualitatif untuk menentukan lintasan dan kinerja jangka panjang perusahaan. Model bertujuan untuk melihat apakah perusahaan semakin matang, yang berarti mereka terus-menerus menguji, tumbuh, dan berkembang. Model dapat menentukan tingkat efektivitas yang berbeda dan dapat menunjukkan posisi seseorang, tim, proyek, atau perusahaan saat ini dalam model.

*Maturity model* merupakan hal yang penting, karena memberikan pemantauan kinerja yang fleksibel yang dapat mengungkapkan informasi berharga tentang kesehatan dan potensi perusahaan. Sementara model tidak memperbaiki inefisiensi itu sendiri, model tersebut dapat mengidentifikasi area di mana organisasi tidak beroperasi pada standar dan memungkinkan mereka untuk menentukan strategi yang dapat meningkatkan operasi dan proses mereka [37].

Pada ITIL sendiri terdapat *maturity model* yang didasarkan pada lima tingkat *maturity*. Definisi tingkat kematangan ini selaras dengan definisi COBIT dan CMMI [38].

### a. Level 1 (Initial)

Pada level ini, proses atau fungsi bersifat *ad hoc*, tidak terorganisir atau kacau. Terdapat bukti bahwa organisasi sudah menyadari bahwa masalah tersebut ada serta perlu ditangani. Akan tetapi, tidak terdapat prosedur standar ataupun kegiatan manajemen proses atau fungsi. Pada level ini, proses atau fungsi dianggap tidak terlalu berarti, dengan sedikit sumber daya yang dialokasikan untuk itu di dalam organisasi. Selain itu, terdapat pendekatan *ad hoc* yang cenderung diterapkan secara individual ataupun bersumber pada tiap kasus. Seluruh pendekatan untuk manajemen tidak terorganisir dengan baik.

b. *Level 2 (Repeatable)*

Pada level ini, proses atau fungsi mengikuti pola yang teratur. Mereka sudah berkembang ke tahap di mana prosedur serupa diiringi oleh orang yang berbeda melaksanakan tugas yang sama. Pelatihan bersifat informal, tidak terdapat komunikasi terkait prosedur standar dan tanggung jawab diserahkan kepada individu. Terdapat tingkat ketergantungan yang tinggi pada pengetahuan individu dan oleh sebab itu kesalahan mungkin terjadi. Secara umum, aktivitas yang berkaitan dengan proses atau fungsi tidak terkoordinasi, tidak teratur, dan mengarah pada efisiensi proses atau fungsi.

c. *Level 3 (Defined)*

Pada level ini, proses atau fungsi sudah diakui dan prosedur sudah distandarisasi, didokumentasikan, serta dikomunikasikan lewat pelatihan. Prosedur tersebut tidak mutakhir, namun merupakan formalisasi dari aplikasi yang sudah ada. Akan tetapi, hal tersebut diserahkan kembali kepada individu untuk mengikuti ataupun tidak sehingga dari hal tersebut penyimpangan dapat terjadi. Proses memiliki pemilik proses, tujuan serta target formal dengan sumber daya yang dialokasikan dan fokus pada efisiensi dan efektivitas.

d. *Level 4 (Managed)*

Pada level ini, proses atau fungsi saat ini sudah sepenuhnya diakui dan diterima di segala teknologi informasi. Level ini berpusat pada layanan dan memiliki target yang didasarkan pada tujuan serta sasaran bisnis. Hal tersebut sepenuhnya ditentukan, dikelola, serta menjadi *pre-emptive*, dengan antarmuka dan dependensi yang terdokumentasi dan mapan ke proses teknologi informasi lainnya. Proses atau fungsi dipantau dan diukur. Kepatuhan terhadap prosedur serta tindakan yang diambil dipantau dan diukur. Proses atau fungsi terus ditingkatkan dan menunjukkan aplikasi terbaik. Otomatisasi dan peralatan semakin banyak digunakan guna menciptakan operasi yang efisien.

e. *Level 5 (Optimized)*

Pada level ini, praktik kerja unggulan diikuti serta diotomatisasi. Sebuah proses perbaikan terus-menerus mandiri didirikan, yang saat ini sudah menciptakan pendekatan *pre-emptive*. Teknologi informasi digunakan secara terintegrasi guna mengotomatisasi alur kerja, menyediakan peralatan untuk meningkatkan mutu dan

daya guna, serta memungkinkan organisasi bisa menyesuaikan diri dengan cepat. Proses atau fungsi mempunyai tujuan serta sasaran strategis yang sejalan dengan bisnis strategis dan tujuan teknologi informasi secara keseluruhan.

Perhitungan nilai *maturity* menggunakan perhitungan yang dirumuskan pada Persamaan (2.1).

$$Maturity\ Level = \frac{Total\ Bobot}{Total\ Responden} \quad (2.1)$$

Pada Persamaan (2.1), nilai *maturity* diperoleh dari hasil total bobot dibagi dengan total responden. Total bobot merupakan jumlah  $n$  dikali dengan parameter ( $n \times$  parameter), dimana  $n$  adalah jumlah tanggapan untuk setiap parameter. Sedangkan total responden adalah jumlah orang yang menjadi responden [39].

### 2.11 Analisis Kesenjangan

Analisis kesenjangan atau *gap analysis* merupakan teknik umum untuk penemuan dan pengelolaan kesenjangan yang dihasilkan selama perencanaan transisi antara keadaan awal dan keadaan target. Analisis kesenjangan adalah sebuah alat atau teknik yang sering digunakan dalam konteks perencanaan strategis. Hal tersebut berkaitan dengan penilaian keadaan atau target yang diinginkan terhadap keadaan saat ini, dengan tujuan untuk memahami kesenjangan antara keduanya [40].

Tingkat kesenjangan menggunakan perhitungan yang dirumuskan pada Persamaan (2.2).

$$Tingkat\ Kesenjangan = Tingkat\ harapan - Tingkat\ maturity \quad (2.2)$$

Berdasarkan Persamaan (2.2), tingkat kesenjangan diperoleh dari tingkat harapan dikurangi dengan tingkat *maturity*. Analisis kesenjangan dapat membantu untuk mengetahui bagian-bagian yang memiliki kesenjangan yang besar serta penyebab dari kesenjangan tersebut.

### 2.12 Kajian Pustaka

Penelitian tentang evaluasi keamanan menggunakan *vulnerability assessment* serta evaluasi manajemen menggunakan ITIL v3 telah dilakukan oleh berbagai pihak. Penelitian tersebut telah dibuktikan melalui karya tulis jurnal yang

telah dipublikasikan. Penelitian-penelitian tersebut dijadikan referensi oleh penulis pada penelitian ini.

Penelitian sebelumnya membahas analisis celah keamanan aplikasi *web learning* pada universitas ABC dengan *vulnerability assessment*. Metode yang digunakan pada penelitian ini adalah *Vulnerability Assesment and Penetration Testing (VAPT) Life Cycle*. Hasil analisis didapatkan bahwa *Overall Risk Level Web* Aplikasi berada pada level *High* sehingga diharuskan untuk melakukan perbaikan serta evaluasi sistem [13].

Penelitian selanjutnya membahas *vulnerability assessment* dan analisis model kematangan pada web di pendidikan tinggi di Indonesia. *Vulnerability assessment* dilakukan dengan menggunakan *tools* Nessus dan Skipfish pada beberapa universitas di Jakarta. Hasil penilaian didapatkan 60% dari 33 situs memiliki kematangan dibawah angka 3 yang berarti tingkat kerentanan pada situs web tersebut masih tinggi [15].

Penelitian selanjutnya membahas penggunaan Wireshark dan Nessus untuk analisis SSL/TLS pada keamanan data pengguna *website* Badan Meteorologi Klimatologi dan Geofisika (BMKG). Pengujian dilakukan dengan menggunakan metode penelusuran paket data dengan aplikasi Wireshark dan metode pemindaian *website* berupa *vulnerability assessment* dengan aplikasi Nessus. Hasil menggunakan metode penelusuran paket data didapatkan bahwa web *server* sudah diverifikasi sertifikat SSL/TLS dan *server public key* dengan protokol TLS 1.2 sehingga dapat melindungi data pengguna menggunakan enkripsi client dan *server* menggunakan algoritma hash SHA256. Sementara hasil analisis pemindaian berupa *vulnerability assessment* menunjukkan level risiko keseluruhan adalah medium [22].

Penelitian selanjutnya membahas evaluasi *maturity level* pada manajemen layanan teknologi informasi di perusahaan *24Slides*. Penelitian tersebut menggunakan *framework* ITIL v3 domain *service operation* untuk mengukur *maturity level*, analisis kesenjangan, serta merumuskan rekomendasi perbaikan. Kuesioner dilakukan pada tiga responden dan kuesioner yang digunakan adalah kuesioner berbasis *Universities and Colleges Information Systems Association*

(UCISA). Hasil penelitian didapatkan skor rata-rata *maturity level* yang bernilai 2,6 dan masuk dalam kategori *repeatable* dengan kesenjangan sebesar 0,8 [14].

Penelitian selanjutnya membahas pengukuran tingkat kematangan ITSM menggunakan *framework* ITIL pada layanan teknologi informasi STMIK Mikroskil. Penelitian tersebut menggunakan *framework* ITIL v3 domain *service operation* untuk mengukur *maturity level*. Kuesioner yang digunakan juga merupakan kuesioner berbasis UCISA. Selain itu terdapat dokumentasi ISO 9001:2008 yang telah dibuat oleh departemen IT. Hasil penelitian didapatkan *maturity level* dengan nilai rata-rata 2,01 dan masuk dalam kategori *repeatable*. Walaupun sudah ada dokumentasi ISO 9001:2008 terkait tahapan *service operation*, namun belum mengikuti detail proses *framework* ITIL [41].

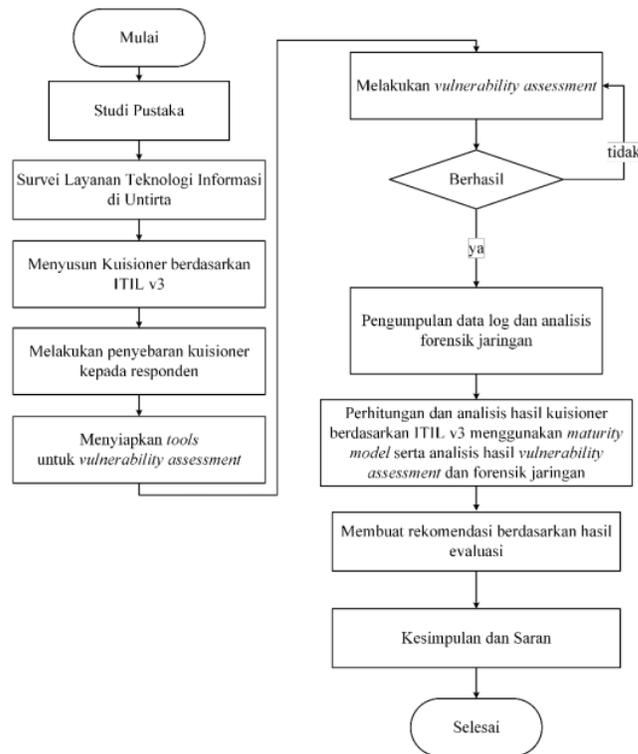
Penelitian selanjutnya membahas audit tata kelola layanan teknologi informasi di Institusi X. Pada penelitian tersebut, untuk mengukur *maturity level* digunakan *framework* COBIT, sedangkan untuk rekomendasi digunakan *framework* ITIL v3 domain *service operation*. Hasil penelitian didapatkan nilai yang diperoleh dari audit manajemen tata kelola teknologi informasi pada Instansi X adalah 3,19 dan terletak pada level 3 (*Established Process*) [42].

Berdasarkan penelitian tersebut, dapat diketahui bahwa analisis celah keamanan dengan *vulnerability assessment* khususnya menggunakan tool *nessus* dapat mengetahui celah keamanan yang terdapat pada sebuah layanan teknologi informasi khususnya layanan *website*. *Vulnerability assessment* juga dapat mengevaluasi celah keamanan dalam suatu layanan sehingga dapat dilakukan perbaikan pada layanan tersebut. Selain itu juga, dapat diketahui bahwa analisis manajemen dengan *framework* ITIL v3 dapat mengetahui celah keamanan yang terdapat pada sebuah layanan teknologi informasi khususnya layanan *website*.

## BAB III METODOLOGI PENELITIAN

### 3.1 Alur Penelitian

Alur penelitian berisikan diagram alir yang menjelaskan setiap langkah atau metode penelitian dari awal dimulai penelitian hingga akhir. Adapun alur penelitian dalam evaluasi menggunakan *framework* ITIL v3 *service operation* seperti pada Gambar 3.1:



Gambar 3.1 Alur Penelitian

Alur dalam menyelesaikan penelitian ini adalah sebagai berikut:

1. Studi literatur dengan mencari referensi dari jurnal maupun buku yang berkaitan dengan permasalahan pada penelitian. Referensi tersebut berkaitan dengan keamanan IT, *vulnerability assessment*, ITSM, dan kerangka kerja ITIL v3 domain *service operation*.

2. Melakukan survei ke lokasi untuk mengetahui proses layanan teknologi informasi yang terdapat pada UPT Data dan Informasi Untirta.
3. Menyusun kuesioner ITIL v3 menggunakan *template UCISA Service Operation*.
4. Menyebar kuesioner ITIL v3 kepada responden UPT Data dan Informasi yang ahli dibidangnya.
5. Menyiapkan *tools* yang akan digunakan untuk *vulnerability assessment*.
6. Melakukan *vulnerability assessment* pada layanan yang telah ditentukan.
7. Mengumpulkan data *log* jaringan dari UPT Data dan Informasi Untirta.
8. Menganalisis hasil dari kuesioner berdasarkan ITIL v3 menggunakan *maturity model*, serta hasil dari *vulnerability assessment* dan forensik jaringan.
9. Membuat rekomendasi berdasarkan hasil dari kuesioner ITIL v3 serta hasil dari *vulnerability assessment* dan forensik jaringan.
10. Membuat kesimpulan, saran, serta rekomendasi dari hasil evaluasi yang telah didapatkan.

### **3.2 Analisis Forensik Jaringan**

Pada analisis forensik jaringan, dilakukan analisis terhadap *log* yang didapatkan saat keadaan normal dan saat serangan terjadi. Analisis *log* juga dilakukan sebagai informasi awal sebelum melakukan *vulnerability assessment* yang akan dilakukan. Analisis *log* dapat memberikan beberapa informasi diantaranya adalah IP *address* penyerang, lokasi penyerang, jenis paket yang terkirim, dan beban CPU.

### **3.3 Vulnerability Assessment**

Pada *vulnerability assessment*, dilakukan uji kerentanan terhadap layanan yang terdapat pada UPT Data dan Informasi Untirta. Layanan yang akan dilakukan uji *Vulnerability* adalah SIAKAD Untirta, SPADA Untirta, *website* Untirta, *website* FT Untirta, dan e-Administrasi Untirta. Layanan-layanan tersebut dipilih karena sering digunakan baik sebagai layanan akademik, maupun sebagai layanan penyampaian informasi terkini yang ada di Untirta. *Vulnerability assessment*

menggunakan sebuah laptop dengan sistem operasi Kali Linux. Kali Linux merupakan salah satu sistem operasi yang sering digunakan dalam *ethical hacking*. Sistem operasi ini memiliki beberapa *tool* yang berguna untuk mencari informasi dan celah kerentanan pada sebuah jaringan komputer.

*Tools* yang digunakan untuk *vulnerability assessment* yaitu Nmap dan Nessus. Nmap digunakan untuk *network mapping*, mengetahui informasi terkait IP *address server, port* yang terbuka, jenis sistem operasi yang digunakan oleh *server*, dan lain sebagainya. Sedangkan Nessus digunakan sebagai alat untuk uji *vulnerability*. Penggunaan aplikasi Nessus dapat memberikan informasi kerentanan yang ada pada layanan teknologi informasi Untirta berdasarkan tingkat kerentanannya. Tingkat kerentanan pada nessus dibagi menjadi 4 level, yaitu *low* yang paling rendah, diikuti *medium, high*, dan *critical* yang paling tinggi.

### 3.4 Kuesioner ITIL v3 Service Operation

Kuesioner dilakukan menggunakan template UCISA ITIL v3 *service operation readiness*. Tingkat maturitas didasarkan pada level yang telah dijelaskan ITIL *maturity model* pada subbab 2.6. Pada penelitian ini hanya difokuskan pada dua sub-domain yaitu *service operation processes*, dan *common service operation activities*. Pertanyaan yang diberikan berjumlah 53 pertanyaan pada sub-domain *service operation processes* dan 28 pertanyaan pada sub-domain *common service operation activities*.

Sub-domain *service operation processes* berisi pernyataan yang berkaitan dengan manajemen seluruh proses yang ada pada *service operation*, yaitu *event management, incident management, request fulfillment, problem management*, dan *access management*. Sementara itu, sub-domain *common service operation activities* berisi pernyataan yang berkaitan dengan aktivitas umum pada penerapan proses dan fungsi yang ada pada *service operation*. Rancangan tabel kuesioner yang akan digunakan dijelaskan pada Tabel 3.1.

Tabel 3.1 Rancangan Kuesioner ITIL *Service Operation*

Sub-Domain							
No.	Pernyataan	Jawaban					Keterangan
		1	2	3	4	5	
1.							
2.							
3.							

Rancangan kuesioner pada Tabel 3.1 diberikan beberapa pernyataan terkait domain *service operation*. Kemudian responden akan memberikan nilai 1-5 terhadap pernyataan yang diberikan sesuai dengan keadaan yang dialami saat ini. Setelah itu dilakukan perhitungan *maturity* model untuk menentukan nilai kematangan terhadap layanan operasional UPT Data dan Informasi.

Berdasarkan penelitian sebelumnya, jumlah responden untuk kuesioner ITIL v3 dapat dilakukan serta dinyatakan valid dengan minimal 3 responden yang ahli di bidangnya [14]. Pada penelitian ini, kuesioner dilakukan kepada 4 responden ahli di bidangnya. Responden dipilih berdasarkan keahlian mereka di bidang IT serta posisi yang mereka tempati di UPT Data dan Informasi Untirta. Responden kuesioner pada penelitian ini diantaranya adalah

1. Bapak Arry Setiyadi sebagai Kepala Subkooor Jaringan
2. Bapak Permadi sebagai Admin *Server* Untirta
3. Bapak Ramdhan J sebagai Kepala Subkooor Pengembangan Sistem
4. Bapak Firman Riyadhhi sebagai Spv. *Engineering* PT. MMD

### 3.5 Analisis *Maturity Model* dan Kesenjangan

Analisis *maturity* model dilakukan untuk menghitung nilai kematangan manajemen layanan teknologi informasi. Sementara itu, Analisis kesenjangan dilakukan untuk menghitung nilai kesenjangan terhadap nilai yang diharapkan dengan keadaan saat ini.

## HASIL DAN PEMBAHASAN

## 4.1 Evaluasi Keamanan Layanan Teknologi Informasi

Evaluasi keamanan layanan teknologi informasi dilakukan dengan menganalisis kerentanan yang terdapat pada keamanan layanan teknologi informasi Untirta. Evaluasi keamanan dilakukan dengan forensik jaringan menggunakan *log* jaringan yang didapatkan saat serangan terjadi, serta dilakukan *vulnerability assesment* pada beberapa layanan teknologi informasi Untirta.

## 4.1.1 Analisis Forensik Jaringan

Pada forensik jaringan, dilakukan analisis mendalam terhadap *log* jaringan pada saat terkena serangan. Pada *log* jaringan, terdapat beberapa informasi yang didapatkan. Salah satu informasi tersebut diantaranya adalah IP *address*. Dari IP *address* tersebut, dapat diketahui lokasi penyerang. *Server* UPT Data dan Informasi sempat mendapatkan serangan DDoS pada tanggal 12 Agustus 2022. Data *log* jaringan didapatkan dari pihak ketiga yang bekerja sama dengan UPT Data dan Informasi Untirta. *Log* jaringan saat serangan DDoS terjadi dijelaskan pada Gambar

4.1.

Eth.	Prot.	Src.	Dst.	VLAN	DSCP	Tx Ra.	Rx Ra.	Tx Pack.	Rx Pack.
800 (...)		2.112.245.3	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.117.198.155	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.109.108.193	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.97.54.96	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.42.55.110	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.79.255.217	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.86.154.192	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.85.125.201	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.63.44.148	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.59.9.187	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.81.227.176	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.41.241.228	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.77.159.112	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.45.88.160	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.111.209.106	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.96.242.239	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.69.102.115	103.142.195.252			0 bps	528 bps	0	1

700 items    Total Tx: 377.5 kbps    Total Rx: 17.5 Mbps    Total Tx Packet: 552    Total Rx Packet: 31 448

Gambar 4.1 Log Jaringan Saat Serangan DDoS

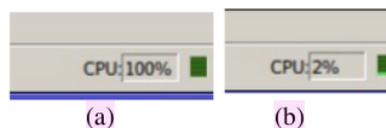
Pada Gambar 4.1, *log* jaringan didapatkan dari aplikasi Winbox Router OS pada menu Torch. Dari data *log* tersebut didapatkan informasi bahwa IP Address Server UPT Data dan Informasi Untirta adalah 103.142.195.252, sementara itu IP Address penyerang bervariasi. Berikut adalah daftar IP Address yang menyerang server UPT Data dan Informasi Untirta yang diuraikan pada Tabel 4.1.

Tabel 4.1 IP Address Penyerang

IP Address	Lokasi	IP Address	Lokasi
2.112.245.3	Italia	2.59.9.187	Rumania
2.117.198.155	Italia	2.81.227.176	Portugal
2.109.108.193	Denmark	2.41.241.228	Italia
2.97.54.96	Britania Raya	2.77.159.112	Kazakhstan
2.42.55.110	Italia	2.45.88.160	Italia
2.79.255.217	Kazakhstan	2.111.209.106	Denmark
2.86.154.192	Yunani	2.96.242.239	Britania Raya
2.85.125.201	Yunani	2.69.102.115	Swedia
2.63.44.148	Rusia		

Dari Tabel 4.1, dapat dilihat bahwa lokasi IP Address bervariasi. Informasi lokasi IP Address penyerang didapatkan melalui pencarian melalui *website* [www.whatismyip.com/ip-address-lookup/](http://www.whatismyip.com/ip-address-lookup/). Semua IP Address penyerang berlokasi di benua Eropa dan sebagian besar serangan berasal dari IP Address yang berlokasi di Italia. Hal ini merupakan salah satu karakteristik serangan DDoS dimana serangan dilakukan menggunakan *botnet* sehingga IP Address penyerang bervariasi. Semua oktet awal pada IP Address penyerang merupakan angka 2.

Selain itu, terdapat kondisi beban CPU pada saat serangan dan sesudah serangan terjadi yang terdapat pada Gambar 4.2.



Gambar 4.2 Kondisi Beban CPU, (a) Saat Serangan, (b) Sesudah

Pada Gambar 4.2 (a) didapatkan bahwa beban CPU pada saat serangan adalah 100%. Hal tersebut berdampak pada terputusnya koneksi internet ke seluruh layanan dan *server* milik UPT Data dan Informasi Untirta. UPT Data dan Informasi Untirta melalui pihak ketiga melakukan aksi sementara untuk mengurangi dampak dari serangan yang ditimbulkan. Aksi yang dilakukan adalah melakukan *blackhole IP Address server* Untirta ke arah internet internasional. Hasil dari aksi yang telah dilakukan adalah beban CPU kembali normal seperti pada Gambar 4.2 (b). Namun, dampak dari aksi sementara tersebut adalah *server* Untirta tidak dapat diakses oleh beberapa *provider* internet dikarenakan *blackhole* yang telah dilakukan.

#### 4.1.2 Analisis Vulnerability Assessment

Pada *vulnerability assessment*, dilakukan uji kerentanan pada beberapa layanan teknologi informasi Untirta. *Vulnerability assessment* dilakukan dalam dua tahapan, yaitu *network scanning*, dan *vulnerability scanning*. Layanan teknologi informasi yang akan dilakukan penetration test adalah SIAKAD Untirta, SPADA Untirta, Website Untirta, dan eAdministrasi Untirta.

##### 1. Network Scanning

Tahap awal pada *vulnerability assessment* adalah *network scanning*. Hal ini dilakukan untuk mengetahui beberapa informasi terkait dengan layanan teknologi informasi diantaranya adalah *IP address server* layanan, *port* yang terbuka, serta memperkirakan sistem operasi yang digunakan oleh *server* layanan. *Tool* yang digunakan pada *network scanning* adalah nmap. Berikut adalah salah satu contoh *network scanning* menggunakan nmap yang terdapat pada Gambar 4.3.

```
(root@DESKTOP-EP29EPG)~# nmap siakad.untirta.ac.id
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-15 12:30 +07
Nmap scan report for siakad.untirta.ac.id (103.142.195.98)
Host is up (0.013s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    filtered smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   filtered netbios-ssn
443/tcp   open  https
445/tcp   filtered microsoft-ds
3306/tcp  open  mysql
5678/tcp  filtered rrac
Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
```

Gambar 4.3 Hasil Network Scanning Menggunakan nmap

Pada Gambar 4.3 merupakan hasil *network scanning* pada layanan SIAKAD Untirta menggunakan aplikasi nmap. Pada hasil scan tersebut, didapatkan beberapa informasi terkait layanan SIAKAD Untirta. Informasi tersebut diantaranya adalah IP *Address* layanan yaitu 103.142.195.98. Selanjutnya, didapatkan informasi beberapa *port* layanan yang terbuka. Salah satu contohnya adalah layanan Mysql yang terdapat pada port 3306 dengan protokol TCP. Layanan Mysql sering digunakan untuk manajemen *database*.

Pada Lampiran B.1 sampai Lampiran B.4 merupakan hasil *network scanning* seluruh layanan yang diuji. Dari hasil-hasil tersebut, didapatkan rekap keseluruhan pada Tabel 4.2.

Tabel 4.2 Hasil *Network Scanning*

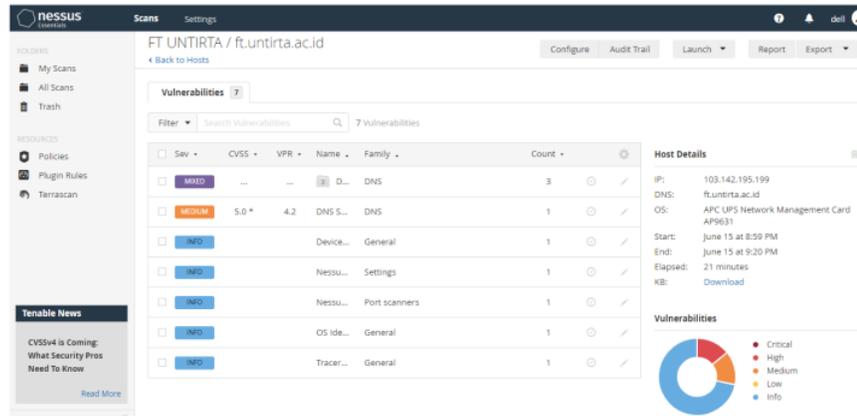
Layanan	IP Host	Sistem Operasi	Jumlah Port Terdeteksi
SIAKAD Untirta (siakad.untirta.ac.id)	103.142.195.98	OpenBSD 4.0 (86%)	8
SPADA Untirta (spada.untirta.ac.id)	103.142.195.106	OpenBSD 4.0 (86%)	12
eAdministrasi Untirta (eadministrasi.untirta.ac.id)	103.142.195.194	OpenBSD 4.0 (86%)	6
Website Untirta dan FT Untirta (untirta.ac.id dan ft.untirta.ac.id)	103.142.195.199	FreeBSD 6.2- RELEASE (87%)	14

Pada Tabel 4.2, didapatkan bahwa layanan Untirta memiliki IP *Host* yang sama dan berbeda tergantung pada layanan, serta *port* yang terdeteksi pada tiap layanan jumlahnya berbeda-beda. Pada layanan web Untirta dan FT Untirta memiliki IP *Host* yang sama serta memiliki jumlah *port* terdeteksi paling banyak di antara layanan yang lainnya.

## 2. *Vulnerability Scanning*

Pada *vulnerability scanning*, dilakukan pemindaian kerentanan yang terdapat pada layanan teknologi informasi Untirta. *Vulnerability scanning* dilakukan menggunakan *tools* Nessus. *Tools* tersebut dapat memberikan *report*

pada hasil pemindaian yang telah dilakukan. Berikut adalah contoh hasil pemindaian menggunakan Nessus yang terdapat pada Gambar 4.4.



Gambar 4.4 Hasil *Vulnerability Scanning* Menggunakan Nessus

Pada Gambar 4.4, hasil *vulnerability assessment* pada layanan web FT Untirta yang didapatkan pada aplikasi Nessus. Aplikasi Nessus memberikan *report* kerentanan yang ada pada layanan berdasarkan tingkat *risk* serta terdapat nilai kerentanan berdasarkan *Common Vulnerability Scoring System* (CVSS). Selain itu, terdapat informasi *IP Address*, DNS, sistem operasi, serta grafik kerentanan yang terdapat pada layanan. Berikut adalah contoh dari hasil *vulnerability scanning* pada Gambar 4.4 yang dijelaskan pada Tabel 4.3.

Tabel 4.3 Hasil *Vulnerability Scanning*

<b>Domain Name</b>	ft.untirta.ac.id	
<b>IP Host</b>	103.142.195.199	
<b>Sistem Operasi</b>	APC UPS Network Management Card	
<b>Tingkat Kerentanan</b>	<b>Celah Keamanan</b>	<b>Skor</b>
HIGH	DNS Server Spoofed Request Amplification DDoS	7,5
MEDIUM	DNS Server Recursive Query Cache Poisoning Weakness	5,0

Pada Tabel 4.3 merupakan hasil *vulnerability scanning* pada layanan *website* FT Untirta. Hasil tersebut didapatkan bahwa terdapat dua kerentanan pada *website* FT Untirta yaitu *DNS server spoofed request amplification DDoS* dengan tingkat

kerentanan <sup>47</sup> *High* dan *DNS server recursive query cache poisoning weakness* dengan tingkat kerentanan *Medium*.

*DNS server spoofed request amplification DDoS* merupakan kerentanan ketika *server* DNS jarak jauh menjawab permintaan apa pun, memungkinkan untuk meminta *name server* (NS) dari *root zone* ('.') dan mendapatkan jawaban yang lebih besar dari permintaan awal. *Spoofing* alamat IP sumber menyebabkan penyerang jarak jauh dapat memanfaatkan 'amplifikasi' ini untuk meluncurkan serangan *Denial of Service* (DoS) terhadap *host* pihak ketiga menggunakan *server* DNS jarak jauh. Solusi untuk kerentanan ini adalah dengan membatasi akses ke *server* DNS dari jaringan publik atau konfigurasi ulang *server* DNS untuk menolak permintaan tersebut.

Sementara itu, *DNS server recursive query cache poisoning weakness* merupakan kerentanan ini memungkinkan penyerang untuk melakukan serangan *cache poisoning* terhadap NS. Solusi untuk kerentanan ini adalah dengan membatasi *recursive queries* ke *host* yang harus menggunakan NS.

Pada Lampiran C.1 sampai Lampiran C.4 merupakan hasil *vulnerability scanning* seluruh layanan yang diuji. Dari hasil-hasil tersebut, didapatkan rekap jumlah *vulnerability* pada Tabel 4.4.

Tabel 4.4 Rekap Jumlah *Vulnerability Scanning*

Layanan	Tingkat Kerentanan				Jumlah
	<i>Critical</i>	<i>High</i>	<i>Medium</i>	<i>Low</i>	
SIKAD Untirta (siakad.untirta.ac.id)	9	16	19	6	50
SPADA Untirta (spada.untirta.ac.id)	1	1	6	1	9
eAdministrasi Untirta (eadministrasi.untirta.ac.id)	1	4	5	1	11
Website Untirta (untirta.ac.id)	0	1	2	2	5
Website FT Untirta (ft.untirta.ac.id)	0	1	1	0	2

Pada Tabel 4.4, didapatkan bahwa tiap layanan Untirta memiliki jumlah kerentanan yang berbeda-beda. Layanan yang memiliki jumlah kerentanan paling banyak adalah SIKAD Untirta. Sementara itu, layanan yang memiliki jumlah

kerentanan paling sedikit adalah *website* FT Untirta. Kerentanan tersebut memiliki dampak yang berbeda-beda terhadap layanan. Keseluruhan kerentanan beserta tingkat kerentanan dijelaskan pada Tabel 4.5

Tabel 4.5 Keseluruhan Kerentanan Layanan Teknologi Informasi Untirta

No.	Kerentanan	Tingkat Kerentanan
1.	PHP <i>Multiple Vulnerabilities</i>	<i>Critical, High, Medium, Low</i>
2.	SSL/TLS <i>Version Vulnerabilities</i>	<i>Critical, High, Medium</i>
3.	SNMP <i>Agent Default Community Name (public)</i>	<i>High, Medium</i>
4.	SNMP <i>'GETBULK' Reflection DDoS</i>	
5.	SSH <i>Weak Algorithms Supported</i>	<i>Medium, Low</i>
6.	SSH <i>Weak MAC Algorithms Enabled</i>	
7.	SSH <i>Weak Key Exchange Algorithms Enabled</i>	
8.	SSH <i>Server CBC Mode Ciphers Enabled</i>	
9.	DNS <i>Server Spoofed Request Amplification DDoS</i>	<i>High</i>
10.	ADODB <i>tmssql.php do Parameter Arbitrary PHP Function Execution</i>	<i>High</i>
11.	CGI <i>Generic SQL Injection (blind)</i>	<i>High</i>
12.	nginx <i>&lt; 1.17.7 Information Disclosure</i>	<i>Medium</i>
13.	Web Server <i>info.php / phpinfo.php Detection</i>	<i>Medium</i>
14.	DNS <i>Server Recursive Query Cache Poisoning Weakness</i>	<i>Medium</i>
15.	Web <i>Application Potentially Vulnerable to Clickjacking</i>	<i>Medium</i>
16.	JQuery <i>1.2 &lt; 3.5.0 Multiple XSS</i>	<i>Medium</i>
17.	DNS <i>Server Cache Snooping Remote Information Disclosure</i>	<i>Medium</i>
18.	<i>Browsable Web Directories</i>	<i>Medium</i>
19.	Git <i>Repository Served by Web Server</i>	<i>Medium</i>
20.	Web <i>Server Transmits Cleartext Credentials</i>	<i>Low</i>
21.	Web <i>Server Allows Password Auto-Completion</i>	<i>Low</i>

Pada Tabel 4.5, merupakan keseluruhan *vulnerability* yang ada pada layanan teknologi informasi Untirta. Terdapat sekitar 21 kerentanan yang terdeteksi pada keseluruhan layanan UPT Data dan Informasi Untirta, dengan tingkat kerentanan paling tinggi adalah PHP dan SSL/TLS. Berikut penjelasan beberapa kerentanan yang ada pada layanan UPT Data dan Informasi Untirta.

a. PHP *multiple vulnerabilities*

Kerentanan ini disebabkan oleh versi PHP yang sudah kadaluwarsa atau sudah tidak didukung. Versi yang sudah tidak didukung ini memiliki banyak kerentanan, beberapa diantaranya adalah dapat menyebabkan DoS, *buffer overflow*, dan kebocoran informasi. Kerentanan tersebut dapat dilihat pada Gambar 4.5.

(a)

PHP Version 5.4.45	
System	Linux vps-lokal1 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64
Build Date	Jan 10 2021 19:32:21
Configure Command	'./configure' '--prefix=/opt/php54' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-gd-native-ttf' '--enable-shmop' '--enable-sigchild' '--enable-syssem' '--enable-sysvshm' '--enable-wddx' '--with-jpeg-dir' '--with-png-dir' '--with-freetype-dir' '--with-zlib' '--with-zlib-dir' '--with-xsl' '--with-gd' '--with-gettext' '--with-mcrypt' '--with-mhash' '--enable-sockets' '--enable-mbstring' '--with-curl' '--enable-mbregex' '--enable-exif' '--with-bz2' '--with-libxml-dir' '--enable-pcntl' '--with-mysql' '--with-mysqli' '--with-iconv' '--with-pdo-mysql' '--with-pdo-sqlite' '--with-openssl' '--enable-zip'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/php54/lib
Loaded Configuration File	/opt/php54/lib/php.ini

(b)

PHP Version 5.3.29	
System	Linux web1730100 5.15.0-73-generic #80-Ubuntu SMP Mon May 15 15:18:26 UTC 2023 x86_64
Build Date	Dec 30 2022 18:48:47
Configure Command	'./configure' '--prefix=/www/server/php/53' '--with-config-file-path=/www/server/php/53/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-ipv6' '--enable-magic-quotes' '--enable-safe-mode' '--enable-bcmath' '--enable-shmop' '--enable-syssem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmllib' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/53/etc
Loaded Configuration File	/www/server/php/53/etc/php.ini

Gambar 4.5 Versi PHP Layanan Untirta (a) SIAKAD (b) e-Administrasi

Pada Gambar 4.5 merupakan informasi PHP yang digunakan SIAKAD Untirta dengan mengakses *file* info.php pada <https://siakad.untirta.ac.id/portal> dan <https://eadministrasi.untirta.ac.id>. Berdasarkan *file* tersebut, didapatkan pada Gambar 4.5 (a) bahwa PHP yang digunakan SIAKAD Untirta adalah PHP versi

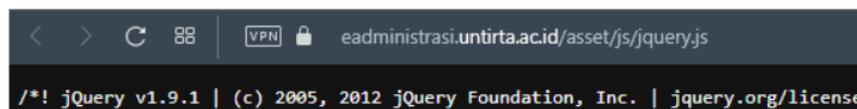
5.4.45, sedangkan pada Gambar 4.5 (b) PHP yang digunakan e-Administrasi Untirta adalah PHP versi 5.3.29 dimana dua versi tersebut merupakan versi PHP yang cukup lawas. Sementara itu, PHP terbaru yang telah dirilis saat ini adalah versi 8.2.7. Untuk menghindari kerentanan tersebut, perlu dilakukan *upgrade* PHP ke versi terbaru.

b. *SSL/TLS version vulnerabilities*

Protokol keamanan juga menjadi masalah pada layanan teknologi informasi Untirta. Hal tersebut dikarenakan beberapa layanan Untirta terdeteksi masih menggunakan protokol *Secure Socket Layer* (SSL) yang merupakan protokol keamanan yang cukup lawas. Protokol SSL sendiri memiliki beberapa kelemahan kriptografi. Disarankan menggunakan protokol *Transport Layer Security* (TLS) yang memiliki tingkat keamanan lebih tinggi dari SSL untuk menghindari kerentanan tersebut.

c. <sup>80</sup> *Jquery 1.2 < 3.5.0 multiple XSS*

Jquery merupakan pustaka <sup>65</sup> JavaScript yang digunakan untuk menyederhanakan *client-side scripting* pada HTML. Jquery yang digunakan oleh e-Administrasi Untirta dapat dilihat pada Gambar 4.6.



Gambar 4.6 Jquery e-Administrasi Untirta

Pada Gambar 4.6 didapatkan versi Jquery yang digunakan pada layanan e-Administrasi Untirta yaitu versi 1.9.1. Hal tersebut dapat diketahui dengan mengakses file jquery.js pada asset <https://eadministrasi.untirta.ac.id>. Jquery versi terbaru yang dirilis adalah versi 3.7.0. Versi dibawah 3.5.0 memiliki kerentanan *Cross-Site Scripting* (XSS). XSS sendiri merupakan kerentanan yang dapat dieksploitasi dengan menginjeksi kode berbahaya pada skrip. Diperlukan *update* Jquery minimal ke versi 3.5.0 untuk menghindari hal tersebut.

d. *Information disclosure*

Pada sebuah *website* terdapat beberapa informasi di dalamnya. Informasi terbuka pada sebuah *website* dapat menjadi sebuah bahaya jika informasi tersebut bersifat sensitif. Contohnya adalah *backup file* SQL, foto *user*, atau *file* penting lainnya. *Information disclosure* pada layanan Untirta dapat dilihat pada Gambar 4.7.



The screenshot shows a web browser window with the address bar displaying "siakad.untirta.ac.id/portal/.git/". The page title is "Index of /portal/.git". Below the title is a table with columns "Name", "Last modified", "Size", and "Description". The table lists various Git repository files and directories, including "Parent Directory", "FETCH\_HEAD", "HEAD", "ORIG\_HEAD", "branches/", "config", "description", "hooks/", "index", "info/", "logs/", "objects/", "packed-refs", and "refs/".

Name	Last modified	Size	Description
Parent Directory	-	-	-
FETCH_HEAD	2023-01-16 14:56	256	
HEAD	2021-08-24 17:44	23	
ORIG_HEAD	2023-01-16 14:56	41	
branches/	2021-08-24 17:42	-	
config	2021-08-24 17:44	298	
description	2021-08-24 17:42	73	
hooks/	2021-08-24 17:42	-	
index	2023-01-16 14:56	247K	
info/	2021-08-24 17:42	-	
logs/	2021-08-24 17:44	-	
objects/	2023-01-16 14:56	-	
packed-refs	2021-08-24 17:44	176	
refs/	2021-08-24 17:44	-	

Apache/2.4.18 (Ubuntu) Server at siakad.untirta.ac.id Port 443

(a)



The screenshot shows a web browser window with the address bar displaying "siakad.untirta.ac.id/portal/images/announcement/". The page title is "Index of /portal/images/announcement". Below the title is a table with columns "Name", "Last modified", "Size", and "Description". The table lists "Parent Directory", "Thumbs.db", and "photo-unavailable.gif".

Name	Last modified	Size	Description
Parent Directory	-	-	-
Thumbs.db	2021-08-24 17:44	8.0K	
photo-unavailable.gif	2021-08-24 17:44	2.5K	

Apache/2.4.18 (Ubuntu) Server at siakad.untirta.ac.id Port 443

(b)

Gambar 4.7 *Information Disclosure* (a) Web Directories (b) Git Repository

Pada Gambar 4.7 merupakan informasi terbuka pada SIAKAD Untirta yang dapat diakses pada laman <https://siakad.untirta.ac.id>. Gambar 4.7 (a) merupakan *git repository* web SIAKAD website SIAKAD Untirta. Sementara itu, pada Gambar 4.7 (b) merupakan direktori website SIAKAD Untirta. Dua hal tersebut berisi *file* yang digunakan, dijelajah, dan diakses pada website SIAKAD Untirta. Sebaiknya

*file* yang dapat dijelajah tersebut tidak mengandung informasi yang bersifat sensitif. Jika diperlukan, batasi akses atau menonaktifkan indeks direktori website.

e. DNS *spoofing* dan *poisoning*

DNS *spoofing* dan *poisoning* juga merupakan celah kerentanan yang terdapat pada layanan teknologi informasi Untirta. Hal ini dapat menyebabkan pengguna dialihkan ke alamat palsu. Kerentanan tersebut perlu diperbaiki oleh UPT Data dan Informasi supaya layanan teknologi informasi Untirta dapat diakses pengguna dengan aman.

## 4.2 Evaluasi Manajemen Layanan Teknologi Informasi

Evaluasi manajemen layanan teknologi informasi dilakukan untuk mengetahui sejauh mana manajemen layanan teknologi informasi Untirta. Evaluasi manajemen dilakukan dengan menyebarkan kuesioner pada beberapa staff UPT Data dan Informasi Untirta yang menangani layanan teknologi informasi Untirta.

Kuesioner yang digunakan adalah kuesioner UCISA ITIL v3 Service Operation Readiness berjumlah 81 pertanyaan yang dibagi menjadi dua sub-domain. Pertanyaan untuk sub-domain *service operation process* berjumlah 53 pertanyaan, sedangkan untuk sub-domain *common service operation activities* berjumlah 28 pertanyaan.

Perhitungan kuesioner menggunakan perhitungan *maturity* model serta *gap analysis*. Dari hasil perhitungan tersebut, didapatkan analisis *maturity* model serta *gap analysis* pada tiap sub-domain pada *service operation* UPT Data dan Informasi Untirta.

### 4.2.1 Analisis Service Operation Process

Pada sub-domain *service operation process* dilakukan evaluasi manajemen layanan teknologi informasi pada tiap proses yang ada dalam domain *service operation*. *Service operation* memiliki 5 proses utama, yaitu *event management*, *incident management*, *request fulfillment*, *problem management*, dan *access management*. Hasil kuesioner *service operation process* dapat dilihat pada Tabel 4.6.

Tabel 4.6 Hasil Kuesioner *Service Operation Process*

<i>Service Operation Process</i>									
No	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-1	3	4	4	5	16	4	4	1
2	SOP-2	3	4	5	5	17	4	4,25	0,75
3	SOP-3	3	4	3	5	15	4	3,75	1,25
4	SOP-4	3	4	4	5	16	4	4	1
5	SOP-5	3	4	5	4	16	4	4	1
6	SOP-6	3	3	3	4	13	4	3,25	1,75
7	SOP-7	3	4	2	5	14	4	3,5	1,5
8	SOP-8	3	4	5	4	16	4	4	1
Skor		24	31	31	37	123	32	3,84	1,16

<sup>1</sup> Tabel 4.6 merupakan hasil kuesioner bagian awal pada *service operation process*. Bagian awal berisi pernyataan yang diajukan untuk setiap proses secara keseluruhan. Dari hasil kuesioner didapatkan nilai maturity pada bagian awal *service operation process* adalah 3,84 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-6 dikarenakan memiliki nilai *maturity* paling kecil. SOP-6 menyatakan bahwa UPT Data dan Informasi telah menetapkan Indikator Kinerja Utama (IKU) serta metrik dari setiap proses pada *service operation*. Saran untuk UPT Data dan Informasi Untirta dalam *service operation process* adalah meningkatkan peran, fungsi, kebijakan, serta faktor keberhasilan terutama indikator kinerja utama pada *service operation process* yang dimiliki oleh UPT Data dan Informasi Untirta.

#### <sup>2</sup> 1. *Event management*

Proses *event management* merupakan proses dalam mengelola *event* atau peristiwa sepanjang siklus hidup layanan. Pengelolaan ini mencakup kegiatan untuk mendeteksi dan memahami peristiwa yang terjadi serta menentukan tindakan pengendalian yang tepat. Hasil kuesioner pada proses *event management* dapat dilihat pada Tabel 4.7.

Tabel 4.7 Hasil Kuesioner *Event Management*

<i>Service Operation Process (Event Management)</i>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-9	3	3	4	4	14	4	3,5	1,5
2	SOP-10	3	4	4	3	14	4	3,5	1,5
3	SOP-11	3	3	4	4	14	4	3,5	1,5
4	SOP-12	3	3	5	4	15	4	3,75	1,25
5	SOP-13	3	3	3	4	13	4	3,25	1,75
6	SOP-14	3	3	4	4	14	4	3,5	1,5
7	SOP-15	3	3	5	4	15	4	3,75	1,25
8	SOP-16	3	3	3	4	13	4	3,25	1,75
9	SOP-17	3	4	4	4	15	4	3,75	1,25
Skor		27	29	36	35	127	36	3,53	1,47

Tabel 4.7 merupakan hasil kuesioner bagian *event management* pada *service operation process*. Pada proses *event management* berisi pernyataan terkait penanganan terhadap suatu peristiwa. Dari hasil kuesioner didapatkan nilai *maturity* pada *event management* adalah 3,53 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-16 dikarenakan memiliki nilai *maturity* paling kecil. SOP-16 menyatakan bahwa UPT Data dan Informasi melakukan tinjauan dari hasil tanggapan yang diberikan pada peristiwa yang terjadi dari layanan teknologi informasinya. Saran untuk UPT Data dan Informasi Untirta dalam *event management* adalah meningkatkan pengelolaan peristiwa terutama dalam peninjauan setiap peristiwa yang ada pada layanan teknologi informasi Untirta.

## 2. Incident management

Proses *incident management* merupakan proses dalam pemulihan layanan dari insiden yang secara tidak terduga terdegradasi atau terganggu. Proses ini mencakup kegiatan identifikasi, dokumentasi, diagnosa, dan pemulihan terhadap suatu insiden yang terjadi pada layanan teknologi informasi. Hasil kuesioner pada proses *incident management* dapat dilihat pada Tabel 4.8.

Tabel 4.8 Hasil Kuesioner *Incident Management*

<i>Service Operation Process (Incident Management)</i>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-18	3	4	4	3	14	4	3,5	1,5
2	SOP-19	3	3	4	5	15	4	3,75	1,25
3	SOP-20	3	4	5	4	16	4	4	1
4	SOP-21	3	3	3	4	13	4	3,25	1,75
5	SOP-22	3	3	3	4	13	4	3,25	1,75
6	SOP-23	3	3	4	4	14	4	3,5	1,5
7	SOP-24	3	4	4	4	15	4	3,75	1,25
8	SOP-25	3	4	3	4	14	4	3,5	1,5
9	SOP-26	3	4	5	4	16	4	4	1
10	SOP-27	3	4	3	4	14	4	3,5	1,5
11	SOP-28	3	4	4	5	16	4	4	1
12	SOP-29	3	4	4	4	15	4	3,75	1,25
Skor		36	44	46	49	175	48	3,65	1,35

Tabel 4.8 merupakan hasil kuesioner bagian *incident management* pada *service operation process*. Pada proses *incident management* berisi pernyataan terkait penanganan serta pemulihan terhadap suatu insiden yang terjadi. Dari hasil kuesioner didapatkan nilai *maturity* pada *incident management* adalah 3,65 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-21 dan SOP-22. SOP-21 menyatakan bahwa UPT Data dan Informasi memiliki aktivitas pengidentifikasian insiden yang terjadi pada layanan teknologi informasi. Sementara itu, SOP-22 menyatakan bahwa UPT Data dan Informasi melakukan *logging* pada setiap insiden yang terjadi pada layanan teknologi informasi. Saran untuk UPT Data dan Informasi Untirta dalam *incident management* adalah meningkatkan penanganan insiden terutama dalam pengidentifikasian insiden serta mendokumentasikan insiden yang terjadi pada layanan teknologi informasi Untirta.

### 3. *Request fullfilment*

Proses *request fullfilment* merupakan proses dalam pemenuhan permintaan pada layanan. Proses ini mencakup pemenuhan kebutuhan yang diperlukan pada layanan teknologi informasi. Hasil kuesioner pada proses *request fullfilment* dapat dilihat pada Tabel 4.9.

Tabel 4.9 Hasil Kuesioner *Request Fullfilment*

<b>Service Operation Process (Request Fullfilment)</b>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-30	3	3	3	4	13	4	3,25	1,75
2	SOP-31	3	4	3	3	13	4	3,25	1,75
3	SOP-32	3	4	3	3	13	4	3,25	1,75
4	SOP-33	3	4	3	3	13	4	3,25	1,75
5	SOP-34	3	4	4	4	15	4	3,75	1,25
Skor		15	19	16	17	67	20	3,35	1,65

Tabel 4.9 merupakan hasil kuesioner bagian *request fullfilment* pada *service operation process*. Pada proses *request fullfilment* berisi pernyataan terkait permintaan pemenuhan kebutuhan yang diperlukan untuk layanan teknologi informasi. Dari hasil kuesioner didapatkan nilai *maturity* pada *request fullfilment* adalah 3,35 atau *defined*. UPT Data dan Informasi Untirta perlu meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.

#### 4. *Problem management*

Proses *problem management* merupakan proses dalam mencegah masalah yang ada dalam layanan. Proses ini mencakup penyelesaian akar masalah dari suatu insiden serta melakukan pendeteksian dan pencegahan masalah atau insiden di masa depan. Hasil kuesioner pada proses *problem management* dapat dilihat pada Tabel 4.10.

Tabel 4.10 Hasil Kuesioner *Problem Management*

<b>Service Operation Process (Problem Management)</b>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-35	3	3	4	5	15	4	3,75	1,25
2	SOP-36	3	3	3	5	14	4	3,5	1,5
3	SOP-37	3	3	4	4	14	4	3,5	1,5
4	SOP-38	3	4	3	4	14	4	3,5	1,5
5	SOP-39	3	4	4	4	15	4	3,75	1,25
6	SOP-40	3	4	5	3	15	4	3,75	1,25
7	SOP-41	3	3	5	3	14	4	3,5	1,5
8	SOP-42	3	4	4	4	15	4	3,75	1,25
9	SOP-43	3	4	3	4	14	4	3,5	1,5

No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
10	SOP-44	3	4	4	4	15	4	3,75	1,25
11	SOP-45	3	3	3	4	13	4	3,25	1,75
12	SOP-46	3	3	5	3	14	4	3,5	1,5
13	SOP-47	3	3	3	4	13	4	3,25	1,75
Skor		39	45	50	51	185	52	3,56	1,44

Tabel 4.10 merupakan hasil kuesioner bagian *problem management* pada *service operation process*. Pada proses *problem management* berisi pernyataan terkait pendeteksian serta pencegahan masalah yang terdapat pada suatu layanan. Dari hasil kuesioner didapatkan nilai maturity pada *problem management* adalah 3,65 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-45 dan SOP-47. SOP-45 menyatakan bahwa UPT Data dan Informasi melakukan pendeteksian kesalahan dalam lingkungan pengembangan. Sementara itu, SOP-47 menyatakan bahwa UPT Data dan Informasi memiliki database kesalahan yang diketahui (*known error database*) untuk memungkinkan diagnosis dan resolusi yang lebih cepat. Saran untuk UPT Data dan Informasi Untirta dalam *problem management* adalah meningkatkan pencegahan masalah yang ada pada layanan terutama pada pendeteksian kesalahan serta membuat *known error database* untuk memudahkan diagnosis serta resolusi pada suatu masalah.

17

##### 5. Access management

Proses *Access Management* merupakan proses dalam pemberian akses terhadap pengguna yang berwenang untuk menggunakan layanan. Proses ini mencakup permintaan, verifikasi, pemantauan, serta penelusuran terhadap akses layanan. Hasil kuesioner pada proses *access management* dapat dilihat pada Tabel 4.11.

Tabel 4.11 Hasil Kuesioner *Access Management*

<i>Service Operation Process (Access Management)</i>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	SOP-48	3	4	3	3	13	4	3,25	1,75
2	SOP-49	3	4	3	4	14	4	3,5	1,5
3	SOP-50	3	4	4	3	14	4	3,5	1,5
4	SOP-51	3	4	4	4	15	4	3,75	1,25
5	SOP-52	3	4	4	5	16	4	4	1
6	SOP-53	3	4	4	3	14	4	3,5	1,5
Skor		18	24	22	22	86	24	3,58	1,42

Tabel 4.11 merupakan hasil kuesioner bagian *access management* pada *service operation process*. Pada proses *access management* berisi pernyataan terkait permintaan, verifikasi, pemantauan, serta penelusuran terhadap akses layanan. Dari hasil kuesioner didapatkan nilai *maturity* pada *problem management* adalah 3,58 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-48. SOP-48 menyatakan bahwa UPT Data dan Informasi memiliki aktivitas permintaan untuk mengakses layanan. Saran untuk UPT Data dan Informasi Untirta dalam *access management* adalah meningkatkan manajemen dalam pemberian akses terhadap layanan teknologi informasi Untirta. Hasil keseluruhan kuesioner *service operation process* dapat dilihat pada Tabel 4.12.

Tabel 4.12 Rekap Hasil Kuesioner *Service Operation Process*

No.	Proses	Maturity Level	Gap
1	<i>Service Operation Process in General</i>	3,84	1,16
2	<i>Event Management</i>	3,53	1,47
3	<i>Incident Management</i>	3,65	1,35
4	<i>Request Fullfilment</i>	3,35	1,65
5	<i>Problem Management</i>	3,56	1,44
6	<i>Access Management</i>	3,58	1,42
Skor		3,60	1,40

Tabel 4.12 merupakan hasil keseluruhan kuesioner *service operation process*. Dari hasil kuesioner didapatkan nilai *maturity* keseluruhan *service operation process* adalah 3,60 atau *defined* dengan gap 1,40. Nilai *maturity* tersebut menunjukkan bahwa manajemen layanan teknologi informasi UPT Data dan

Informasi Untirta pada domain *service operation* telah terdefinisi serta memiliki prosedur yang jelas. Tahap selanjutnya adalah bagaimana UPT Data dan Informasi meningkatkan nilai *maturity* manajemen layanan teknologi informasi ke level 4 (*Managed*). Bagian yang menjadi perhatian pada *service operation process* adalah proses *request fulfillment*. UPT Data dan Informasi harus meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.

#### 4.2.2 Analisis *Common Service Operation Activities*

Pada *common service operation activities* dilakukan evaluasi aktivitas umum yang terdapat dalam proses atau fungsi pada domain *service operation*. Aktivitas umum tersebut berdasarkan pada proses dan fungsi yang ada dalam *service operation*. Hasil kuesioner *common service operation activities* dapat dilihat pada Tabel 4.13.

Tabel 4.13 Hasil Kuesioner *Common Service Operation Activities*

<i>Common Service Operation Activities</i>									
No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
1	CSOA-1	3	4	4	2	13	4	3,25	1,75
2	CSOA-2	3	4	3	2	12	4	3	2
3	CSOA-3	3	4	4	4	15	4	3,75	1,25
4	CSOA-4	3	4	3	4	14	4	3,5	1,5
5	CSOA-5	3	4	4	4	15	4	3,75	1,25
6	CSOA-6	3	4	4	3	14	4	3,5	1,5
7	CSOA-7	3	2	4	5	14	4	3,5	1,5
8	CSOA-8	3	4	3	4	14	4	3,5	1,5
9	CSOA-9	3	4	4	4	15	4	3,75	1,25
10	CSOA-10	3	4	4	3	14	4	3,5	1,5
11	CSOA-11	3	4	4	4	15	4	3,75	1,25
12	CSOA-12	3	4	4	3	14	4	3,5	1,5
13	CSOA-13	3	3	3	2	11	4	2,75	2,25
14	CSOA-14	3	3	5	2	13	4	3,25	1,75
15	CSOA-15	3	4	5	4	16	4	4	1
16	CSOA-16	3	4	4	2	13	4	3,25	1,75
17	CSOA-17	3	4	2	5	14	4	3,5	1,5
18	CSOA-18	3	4	4	4	15	4	3,75	1,25
19	CSOA-19	3	4	4	4	15	4	3,75	1,25

No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	Maturity Level	Gap
		1	2	3	4				
20	CSOA-20	3	4	4	4	15	4	3,75	1,25
21	CSOA-21	3	4	4	4	15	4	3,75	1,25
22	CSOA-22	3	4	4	4	15	4	3,75	1,25
23	CSOA-23	3	4	4	4	15	4	3,75	1,25
24	CSOA-24	3	4	4	4	15	4	3,75	1,25
25	CSOA-25	3	4	4	4	15	4	3,75	1,25
26	CSOA-26	3	4	4	3	14	4	3,5	1,5
27	CSOA-27	3	4	4	3	14	4	3,5	1,5
28	CSOA-28	3	4	4	4	15	4	3,75	1,25
Skor		84	108	108	99	399	112	3,56	1,44

Tabel 4.13 merupakan hasil keseluruhan kuesioner *common service operation activities*. Dari hasil kuesioner didapatkan level *maturity* keseluruhan *service operation process* berada pada nilai 3,56 atau *defined* dengan *gap* 1,44. Nilai *maturity* tersebut menunjukkan bahwa manajemen layanan teknologi informasi UPT Data dan Informasi Untirta pada aktivitas umum *service operation* telah terdefinisi serta memiliki prosedur yang jelas. Tahap selanjutnya adalah bagaimana UPT Data dan Informasi meningkatkan nilai *maturity* manajemen layanan teknologi informasi ke level 4 (*Managed*).

Bagian yang perlu menjadi perhatian adalah pernyataan CSOA-2. CSOA-2 menyatakan bahwa UPT Data dan Informasi memastikan bahwa kondisi tertentu dipenuhi atau tidak terpenuhi dan jika tidak, maka akan menaikkan peringatan ke grup yang sesuai. UPT Data dan Informasi Untirta harus meningkatkan manajemen pada aktivitas umum *service operation* dengan melakukan pemantauan dan *service control*, melakukan audit *service operation*, serta mengukur ketersediaan dari perspektif teknologi informasi dan organisasi.

### 4.3 Rekomendasi

Setelah dilakukan analisis keamanan dan manajemen terhadap layanan teknologi informasi Untirta, hasil analisis tersebut digunakan untuk membuat rekomendasi. Hal tersebut dilakukan supaya layanan teknologi informasi Untirta dapat berkembang menjadi lebih baik.

#### 4.3.1 Rekomendasi Keamanan Layanan Teknologi Informasi

Rekomendasi untuk keamanan layanan teknologi informasi UPT Data dan Informasi adalah memperbaiki layanan dari kerentanan yang ada pada layanan. Rekomendasi untuk keamanan layanan teknologi informasi Untirta dijelaskan pada Lampiran D.1.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran D.1, sebagian besar yang perlu dilakukan UPT Data dan Informasi Untirta untuk meningkatkan keamanan layanan teknologi informasi adalah mengupgrade aplikasi yang digunakan dalam layanan. Aplikasi tersebut diantaranya adalah PHP, SSL/TSL, nginx, dan JQuery. Selain itu, perlu dilakukan perubahan pada kueri dan menambahkan atribut pada aplikasi tertentu.

#### 4.3.2 Rekomendasi Manajemen Layanan Teknologi Informasi

Rekomendasi untuk manajemen layanan teknologi informasi UPT Data dan Informasi adalah meningkatkan pengelolaan manajemen pada proses dan aktivitas umum pada *service operation*. Rekomendasi untuk manajemen layanan teknologi informasi Untirta dijelaskan pada Lampiran D.2.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran D.2, sebagian besar yang perlu dilakukan UPT Data dan Informasi Untirta untuk meningkatkan manajemen layanan teknologi informasi ialah meningkatkan manajemen pada tiap proses yang ada pada *service operation*. Sementara itu, pemantauan dan pengelolaan layanan juga perlu ditingkatkan supaya layanan teknologi informasi dapat digunakan dan dimanfaatkan oleh civitas akademika Untirta dengan baik.

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Berdasarkan hasil dari penelitian yang telah dilakukan, didapatkan kesimpulan sebagai berikut:

1. Pada evaluasi manajemen layanan teknologi informasi, UPT Data dan Informasi didapatkan level kematangan dengan nilai rata-rata pada level 3 (*defined*). Rekomendasi yang diberikan untuk manajemen layanan teknologi informasi UPT Data dan Informasi adalah meningkatkan pemantauan dan pengelolaan pada proses dan aktivitas *service operation* yang ada.
2. Sedangkan pada evaluasi keamanan layanan teknologi informasi, level kerentanan layanan teknologi informasi yang ada UPT Data dan Informasi mendapatkan nilai rata-rata *medium*. Rekomendasi yang diberikan untuk keamanan layanan teknologi informasi UPT Data dan Informasi adalah memperbaiki kerentanan yang ada pada layanan serta melakukan *upgrade plug-in* atau aplikasi yang ada pada layanan secara berkala.

#### **5.2 Saran**

Adapun saran yang diberikan berdasarkan hasil penelitian yang telah dilakukan adalah sebagai berikut:

1. Pada evaluasi manajemen layanan teknologi informasi dapat menggunakan domain yang lain pada kerangka kinerja ITIL v3 atau dapat menggunakan *framework* lain seperti COBIT, ISO, atau ITIL 4 yang merupakan versi ITIL yang lebih mutakhir.
2. Pada evaluasi keamanan layanan teknologi informasi, tahap *Vulnerability assessment* dapat ditingkatkan menjadi *penetration test* dengan menambah tahap *exploitation*.
3. Pada tahap *vulnerability assessment* dapat menambah aplikasi yang lain selain *nmap* dan *nessus* untuk mencari data *vulnerability* seperti WPScan, OWASP ZAP, OpenVas, dan lain sebagainya.

# SKRIPSI

---

## ORIGINALITY REPORT

---

24%

SIMILARITY INDEX

23%

INTERNET SOURCES

4%

PUBLICATIONS

12%

STUDENT PAPERS

---

## PRIMARY SOURCES

---

1	<a href="http://repository.ub.ac.id">repository.ub.ac.id</a> Internet Source	5%
2	<a href="http://repository.its.ac.id">repository.its.ac.id</a> Internet Source	2%
3	Submitted to Universitas Brawijaya Student Paper	2%
4	<a href="http://journal.umpr.ac.id">journal.umpr.ac.id</a> Internet Source	2%
5	<a href="http://jurnal.umt.ac.id">jurnal.umt.ac.id</a> Internet Source	1%
6	<a href="http://j-ptiik.ub.ac.id">j-ptiik.ub.ac.id</a> Internet Source	1%
7	123dok.com Internet Source	1%
8	<a href="http://journal.uad.ac.id">journal.uad.ac.id</a> Internet Source	<1%
9	<a href="http://vdokumen.com">vdokumen.com</a> Internet Source	<1%

---

10	<a href="http://docplayer.info">docplayer.info</a> Internet Source	<1 %
11	<a href="http://jurnalunibi.unibi.ac.id">jurnalunibi.unibi.ac.id</a> Internet Source	<1 %
12	<a href="http://jurnal.pancabudi.ac.id">jurnal.pancabudi.ac.id</a> Internet Source	<1 %
13	<a href="http://gita-kartika.blogspot.com">gita-kartika.blogspot.com</a> Internet Source	<1 %
14	<a href="http://anggiyolandaf.blogspot.com">anggiyolandaf.blogspot.com</a> Internet Source	<1 %
15	Submitted to Universitas Pelita Harapan Student Paper	<1 %
16	<a href="http://aryjambi.blogspot.com">aryjambi.blogspot.com</a> Internet Source	<1 %
17	<a href="http://digilib.uinsby.ac.id">digilib.uinsby.ac.id</a> Internet Source	<1 %
18	Submitted to Sriwijaya University Student Paper	<1 %
19	<a href="http://jurnal.umj.ac.id">jurnal.umj.ac.id</a> Internet Source	<1 %
20	<a href="http://repository.upi.edu">repository.upi.edu</a> Internet Source	<1 %
21	<a href="http://www.mdpi.com">www.mdpi.com</a> Internet Source	<1 %

22	Submitted to Academic Library Consortium Student Paper	<1 %
23	Submitted to LL DIKTI IX Turnitin Consortium Part II Student Paper	<1 %
24	<a href="http://eprints.itn.ac.id">eprints.itn.ac.id</a> Internet Source	<1 %
25	<a href="http://journal.universitaspahlawan.ac.id">journal.universitaspahlawan.ac.id</a> Internet Source	<1 %
26	Submitted to SDM Universitas Gadjah Mada Student Paper	<1 %
27	Submitted to Noroff University College Student Paper	<1 %
28	<a href="http://id.scribd.com">id.scribd.com</a> Internet Source	<1 %
29	<a href="http://journal.uniku.ac.id">journal.uniku.ac.id</a> Internet Source	<1 %
30	<a href="http://library.binus.ac.id">library.binus.ac.id</a> Internet Source	<1 %
31	<a href="http://repository.uin-suska.ac.id">repository.uin-suska.ac.id</a> Internet Source	<1 %
32	<a href="http://www.yasteq.com">www.yasteq.com</a> Internet Source	<1 %
33	<a href="http://dspace.uii.ac.id">dspace.uii.ac.id</a> Internet Source	<1 %

<1 %

34

[repository.unhas.ac.id](http://repository.unhas.ac.id)

Internet Source

<1 %

35

[text-id.123dok.com](http://text-id.123dok.com)

Internet Source

<1 %

36

[eprints.undip.ac.id](http://eprints.undip.ac.id)

Internet Source

<1 %

37

[lontar.ui.ac.id](http://lontar.ui.ac.id)

Internet Source

<1 %

38

[repositori.unud.ac.id](http://repositori.unud.ac.id)

Internet Source

<1 %

39

Submitted to Queen's College

Student Paper

<1 %

40

[ejournal.unsrat.ac.id](http://ejournal.unsrat.ac.id)

Internet Source

<1 %

41

[essafadly.blogspot.com](http://essafadly.blogspot.com)

Internet Source

<1 %

42

[www.miratech.kiev.ua](http://www.miratech.kiev.ua)

Internet Source

<1 %

43

[eprints.uns.ac.id](http://eprints.uns.ac.id)

Internet Source

<1 %

44

[peraturan.bpk.go.id](http://peraturan.bpk.go.id)

Internet Source

<1 %

45	<a href="http://repository.iainbengkulu.ac.id">repository.iainbengkulu.ac.id</a> Internet Source	<1 %
46	Submitted to London Metropolitan University Student Paper	<1 %
47	Submitted to Staffordshire University Student Paper	<1 %
48	<a href="http://afnoriestia.blogspot.com">afnoriestia.blogspot.com</a> Internet Source	<1 %
49	<a href="http://jist.publikasiindonesia.id">jist.publikasiindonesia.id</a> Internet Source	<1 %
50	<a href="http://repository.ar-raniry.ac.id">repository.ar-raniry.ac.id</a> Internet Source	<1 %
51	<a href="http://www.neliti.com">www.neliti.com</a> Internet Source	<1 %
52	<a href="http://eprints.polbeng.ac.id">eprints.polbeng.ac.id</a> Internet Source	<1 %
53	Submitted to Syiah Kuala University Student Paper	<1 %
54	Submitted to UIN Sultan Syarif Kasim Riau Student Paper	<1 %
55	<a href="http://repository.dinamika.ac.id">repository.dinamika.ac.id</a> Internet Source	<1 %
56	<a href="http://digilib.unila.ac.id">digilib.unila.ac.id</a> Internet Source	<1 %

57	<a href="http://dokumen.tips">dokumen.tips</a> Internet Source	<1 %
58	<a href="http://eprints.ubhara.ac.id">eprints.ubhara.ac.id</a> Internet Source	<1 %
59	<a href="http://journal.unla.ac.id">journal.unla.ac.id</a> Internet Source	<1 %
60	<a href="http://moam.info">moam.info</a> Internet Source	<1 %
61	<a href="http://repositori.usu.ac.id">repositori.usu.ac.id</a> Internet Source	<1 %
62	<a href="http://repositorio.uam.es">repositorio.uam.es</a> Internet Source	<1 %
63	<a href="http://repository.radenfatah.ac.id">repository.radenfatah.ac.id</a> Internet Source	<1 %
64	<a href="http://academic-accelerator.com">academic-accelerator.com</a> Internet Source	<1 %
65	<a href="http://desy.lecturer.pens.ac.id">desy.lecturer.pens.ac.id</a> Internet Source	<1 %
66	<a href="http://eprintslib.ummgl.ac.id">eprintslib.ummgl.ac.id</a> Internet Source	<1 %
67	<a href="http://media.neliti.com">media.neliti.com</a> Internet Source	<1 %
68	<a href="http://mikroskil.ac.id">mikroskil.ac.id</a> Internet Source	<1 %

69	<a href="http://www.tenable.com">www.tenable.com</a> Internet Source	<1 %
70	<a href="http://core.ac.uk">core.ac.uk</a> Internet Source	<1 %
71	<a href="http://docobook.com">docobook.com</a> Internet Source	<1 %
72	<a href="http://doku.pub">doku.pub</a> Internet Source	<1 %
73	<a href="http://download.garuda.kemdikbud.go.id">download.garuda.kemdikbud.go.id</a> Internet Source	<1 %
74	<a href="http://himagro.faperta.untirta.ac.id">himagro.faperta.untirta.ac.id</a> Internet Source	<1 %
75	<a href="http://justdodos.blogspot.com">justdodos.blogspot.com</a> Internet Source	<1 %
76	<a href="http://quizlet.com">quizlet.com</a> Internet Source	<1 %
77	<a href="http://e-repository.perpus.iainsalatiga.ac.id">e-repository.perpus.iainsalatiga.ac.id</a> Internet Source	<1 %
78	<a href="http://ejournal.upnvj.ac.id">ejournal.upnvj.ac.id</a> Internet Source	<1 %
79	<a href="http://kc.umn.ac.id">kc.umn.ac.id</a> Internet Source	<1 %
80	<a href="http://openlibrarypublications.telkomuniversity.ac.id">openlibrarypublications.telkomuniversity.ac.id</a> Internet Source	<1 %

81	<a href="http://repository.uir.ac.id">repository.uir.ac.id</a> Internet Source	<1 %
82	<a href="http://vdoc.pub">vdoc.pub</a> Internet Source	<1 %
83	<a href="http://vdocuments.site">vdocuments.site</a> Internet Source	<1 %
84	<a href="http://www.kesad.mil.id">www.kesad.mil.id</a> Internet Source	<1 %
85	<b>Heri Wijayanto. "Budaya Organisasi dalam Implementasi Enterprise Resources Planning Perguruan Tinggi di Jawa Timur", Jurnal Perilaku dan Strategi Bisnis, 2020</b> Publication	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off