EVALUASI KEMATANGAN LAYANAN TEKNOLOGI INFORMASI MENGGUNAKAN *FRAMEWORK* ITIL V3 *DOMAIN SERVICE OPERATION* (Studi Kasus: UPT DATA DAN INFORMASI UNTIRTA)

SKRIPSI

Disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik (S.T)

Disusun oleh:

RAFI' MUHAMMAD NAUFAL

NPM. 3332180040

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS SULTAN AGENG TIRTAYASA

2023

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya sebagai penulis Skripsi berikut:

Judul	: Evaluasi Kematangan Layanan Teknologi Informasi Menggunakan *Framework* ITIL v3 Domain *Service Operation* (Studi Kasus: UPT Data dan Informasi Untirta)
Nama Mahasiswa	: Rafi' Muhammad Naufal
NPM	: 3332180040
Fakultas/Jurusan	: Teknik/Teknik Elektro

Menyatakan dengan sesungguhnya bahwa Skripsi tersebut di atas adalah benar-benar hasil karya asli saya dan tidak memuat hasil karya orang lain, kecuali dinyatakan melalui rujukan yang benar dan dapat dipertanggungjawabkan. Apabila dikemudian hari ditemukan hal-hal yang menunjukkan bahwa sebagian atau seluruh karya ini bukan karya saya, maka saya bersedia dituntut melalui hukum yang berlaku. Saya juga bersedia menanggung segala akibat hukum yang timbul dari pernyataan yang secara sadar dan sengaja saya nyatakan melalui lembar ini.

Cilegon, 3 Juli 2023

Rafi' Muhammad Naufal

NPM. 3332180040

LEMBAR PENGESAHAN

Dengan ini ditetapkan bahwa Skripsi berikut.

Judul	: Evaluasi Kematangan Layanan Teknologi Informasi Menggunakan *Framework* ITIL v3 Domain *Service Operation* (Studi Kasus: UPT Data dan Informasi Untirta)
Nama Mahasiswa	: Rafi' Muhammad Naufal
NPM	: 3332180040
Fakultas/Jurusan	: Teknik/Teknik Elektro

Telah diuji dan dipertahankan pada tanggal .....Juli 2023..... melalui Sidang Skripsi di Fakultas Teknik Universitas Sultan Ageng Tirtayasa Cilegon dan dinyatakan LULUS.

	Dewan Penguji	Tanda Tangan
Pembimbing I	: Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM	.....
Pembimbing II	: Anis Fuad, M.Si.	.....
Penguji I	: Masjudin, S.T., M.Eng.	.....
Penguji II	: Cakra Adipura W, S.T., M.T.	..... Digitally signed by Cakra Adipura Wicaksana Date: 2023.08.02 16:14:25 +07'00'

Mengetahui,
Ketua Jurusan

Dr. Romi Wiryadinata, S.T., M.Eng.
NIP. 198307032009121006

PRAKATA

Segala puji hanya milik Allah Subhanahu Wata'ala, tuhan semesta alam yang telah memberikan limpahan nikmat dan karunianya sehingga penulis dapat menyelesaikan skripsi dengan topik Evaluasi Layanan Teknologi Informasi dengan Studi Kasus pada UPT Data dan Informasi Universitas Sultan Ageng Tirtayasa. Skripsi ini dilakukan sebagai salah satu syarat untuk menyelesaikan studi S1 di Universitas Sultan Ageng Tirtayasa. Shalawat serta salam selalu dilimpahkan kepada uswah, suri tauladan, Sayyidina wa Maulana Nabi Muhammad Shalallahu 'alaihi wa sallam, yang telah membawa umat manusia dari zaman kegelapan menuju zaman terang benderang.

Penulisan skripsi ini tidak dapat terwujud tanpa adanya bantuan dari pihak lain. Oleh karena itu, penulis ingin mengucapkan terima kasih sebanyak-banyaknya kepada semua pihak yang telah membantu dalam pelaksanaan, penulisan laporan, dan penyelesaian penelitian Skripsi ini, yaitu:

1. Kedua orang tua tercinta, ayah dan ibu yang selalu mendidik serta mendoakan untuk keberhasilan anaknya, memberikan kasih sayang serta memberikan dukungan baik berupa usaha, material, maupun moral yang sangat besar kepada penulis selama proses dan pengerjaan laporan skripsi.
2. Bapak Dr. Romi Wiryadinata, S.T., M. Eng. selaku Ketua Program Studi Teknik Elektro, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
3. Bapak Ir. Ri Munarto, M.Eng. selaku Dosen Pembimbing Akademik yang telah membimbing serta memberikan arahan selama perkuliahan, termasuk dalam penelitian kali ini.
4. Bapak Prof. Dr. Supriyanto, S.T., M.Sc., IPM. selaku Dosen Pembimbing 1 sekaligus Wakil Dekan 1 Fakultas Teknik, Universitas Sultan Ageng Tirtayasa yang telah membimbing dalam menyelesaikan penelitian ini.
5. Bapak Anis Fuad, M.Si. selaku Dosen Pembimbing 2 sekaligus Kepala Unit Pelaksana Teknis Data dan Informasi Universitas Sultan Ageng Tirtayasa yang telah memberi izin penulis untuk melaksanakan penelitian serta membimbing dalam menyelesaikan penelitian ini.

6. Seluruh dosen dan staff akademik Jurusan Teknik Elektro, Fakultas Teknik Untirta yang tidak bisa disebutkan namanya satu-persatu karena telah memberikan serta menyampaikan ilmu-ilmu serta jasa yang bermanfaat dan tak terhingga.

Penulis menyadari bahwa hasil penelitian ini masih memiliki beberapa kekurangan, namun penulis berharap hasil penelitian ini dapat bermanfaat bagi para pembaca, khususnya bagi penulis sendiri. Oleh karena itu, penulis menerima berbagai kritik dan saran demi kemajuan hasil penelitian ini.

Cilegon, 27 Juni 2023

Rafi' Muhammad Naufal

ABSTRAK

Rafi' Muhammad Naufal
Teknik Elektro

Evaluasi Kematangan Layanan Teknologi Informasi Menggunakan *Framework* ITIL v3 Domain *Service Operation*
(Studi Kasus: UPT Data dan Informasi Untirta)

Pada saat ini, keberadaan teknologi informasi menjadi sebuah hal yang sangat penting. Pada penerapan teknologi informasi tersebut diperlukan manajemen serta keamanan. Untirta sebagai perguruan tinggi menerapkan tata kelola teknologi informasi. Hal tersebut diwujudkan dengan adanya UPT Data dan Informasi Untirta. Beberapa waktu lalu, layanan teknologi informasi Untirta sempat mendapatkan sebuah insiden yang menyerang keamanan layanan teknologi informasi. Maka dari itu perlu diadakan evaluasi pada manajemen dan keamanan pada layanan Untirta. Penelitian ini menggunakan metode kuesioner ITIL v3 untuk evaluasi manajemen serta metode forensik jaringan dan *vulnerability assessment* dengan aplikasi Nmap dan Nessus untuk evaluasi keamanan. Dari penelitian tersebut, didapatkan hasil evaluasi manajemen layanan teknologi informasi dengan ITIL v3 *service operation* pada level 3 (*Defined*). Sementara itu, hasil evaluasi keamanan layanan teknologi informasi didapatkan beberapa kerentanan dengan rata-rata level *medium*. Rekomendasi dari hasil evaluasi tersebut adalah meningkatkan pemenatauan dan pengelolaan manajemen pada proses yang ada dalam *service operation*. Selain itu, diperlukan *upgrade* pada aplikasi yang digunakan pada layanan teknologi informasi Untirta untuk meningkatkan keamanan.

Kata Kunci: Teknologi Informasi, Manajemen, Keamanan, ITIL, Nmap, Nessus

ABSTRACT

Rafi' Muhammad Naufal
Electrical Engineering

Evaluation of Information Technology Service Maturity using ITIL v3 Framework in Service Operation Domain
(Case Study: UPT Data dan Informasi Untirta)

Currently, the existence of information technology has become a very important thing. The use of information technology requires management and security. Untirta implements information technology governance. This is realized by the existence of UPT Data dan Informasi Untirta. Some time ago, there was an incident in Untirta's information technology service where the security of the information technology services was attacked. Therefore, the management and security of Untirta's information technology services should be evaluated. This study uses the ITIL v3 questionnaire method for management evaluation as well as network forensic and vulnerability assessment methods using nmap and Nessus applications for security evaluation. From this study, the results of evaluating information technology service management with ITIL v3 service operation were obtained at level 3 (Defined). Meanwhile, the results of an evaluation of the security of information technology services identified several vulnerabilities with an average level of medium. The recommendation from the evaluation results is to improve monitoring and management of existing processes in service operations. In addition, an upgrade is required for the application used in Untirta's information technology services to improve security.

Keywords: Information Technology, Management, Security, ITIL, Nmap, Nessus

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
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 24*Slides*. 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. Penilian 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

layanan teknologi informasi dengan melakukan penyebaran kuesioner menggunakan kerangka kerja ITIL V3. 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.

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?

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 samapai 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

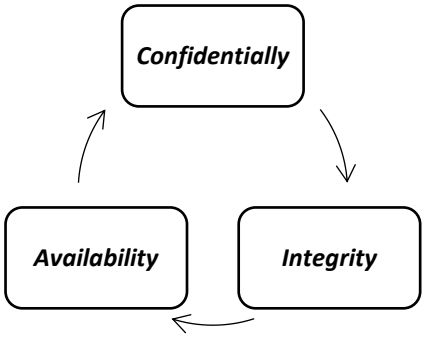
2.1 Layanan Teknologi Informasi

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 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 *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 *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 *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)

Distrributed 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 membanjiri 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].

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.

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 *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 scannning*, *ping scan* TCP SYN, *ping scan* TCP ACK, *ping scan* UDP, *ping scan* ICMP, dan *ping scan* IP [30].

b. Nessus

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].

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

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 Manajemen Layanan Teknologi Informasi

Manajemen layanan teknologi informasi atau *Information Technology Service Management* (ITSM) merupakan sebuah 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. 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: *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].

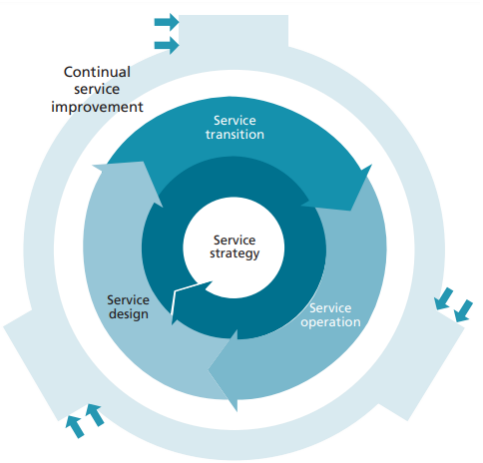
2.8 ITIL V3 *Service Operation*

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, transisition*, 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 pengunaan 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 infomasi 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. S*ervice operation* memiliki lima proses utama:

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 meningkatan 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 efesiensi dalam kebutuhan akademik maupun administrasi universitas dimana saja dan kapan saja.

Beberapa layanan teknologi informasi tersebut diantaranya adalah Sistem Informasi Akademik (SIAKAD)**,** 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 × 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].

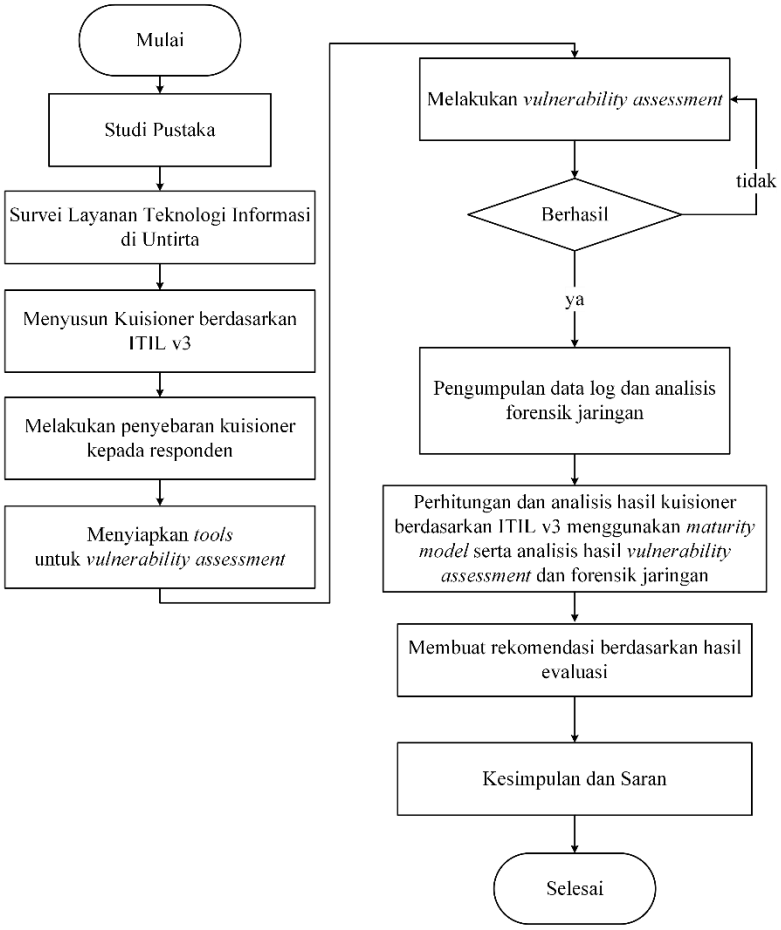
Penelitian selanjtnya membahas audit tata kelola layanan teknologi informasi di Institusi X. Pada penelitian tersebut, untuk mengukur *maturity level* digunakan *framework* COBIT, sedangkan untuk rekomendasi digunakan *framework* ITIL v3 domain *service operation*. Hasil penelitian didapatkan nilai yang 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 berikaitan 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 a*ddress* 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 fullfilment, 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 bidangya [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 Subkoor Jaringan
2. Bapak Permadi sebagai Admin *Server* Untirta
3. Bapak Ramdhan J sebagai Kepala Subkoor Pengembangan Sistem
4. Bapak Firman Riyadhi 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.

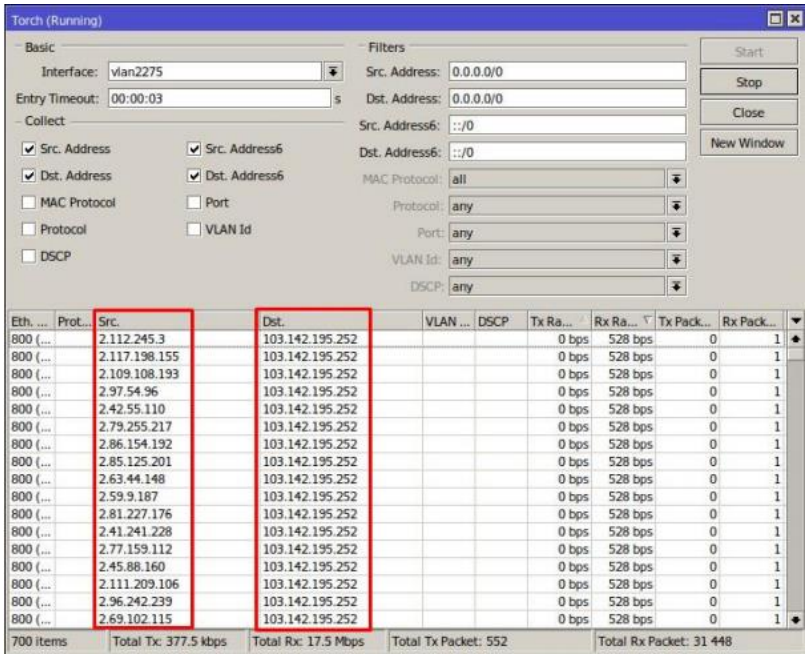
BAB IV
HASIL DAN PEMBAHASAN

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 assessment* 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.



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.

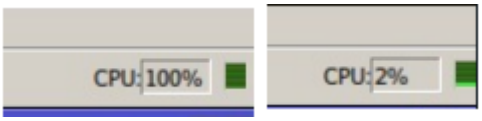
Tabel 4.1 IP *Address* Penyerang

IP Address	**Lokasi**
2.112.245.3	Italia
2.117.198.155	Italia
2.109.108.193	Denmark
2.97.54.96	Britania Raya
2.42.55.110	Italia
2.79.255.217	Kazakhstan
2.86.154.192	Yunani
2.85.125.201	Yunani
2.63.44.148	Rusia

IP Address	**Lokasi**
2.59.9.187	Rumania
2.81.227.176	Portugal
2.41.241.228	Italia
2.77.159.112	Kazakhstan
2.45.88.160	Italia
2.111.209.106	Denmark
2.96.242.239	Britania Raya
2.69.102.115	Swedia

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/. 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.



(a) (b)

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)-[/home/dell]
└─# 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*

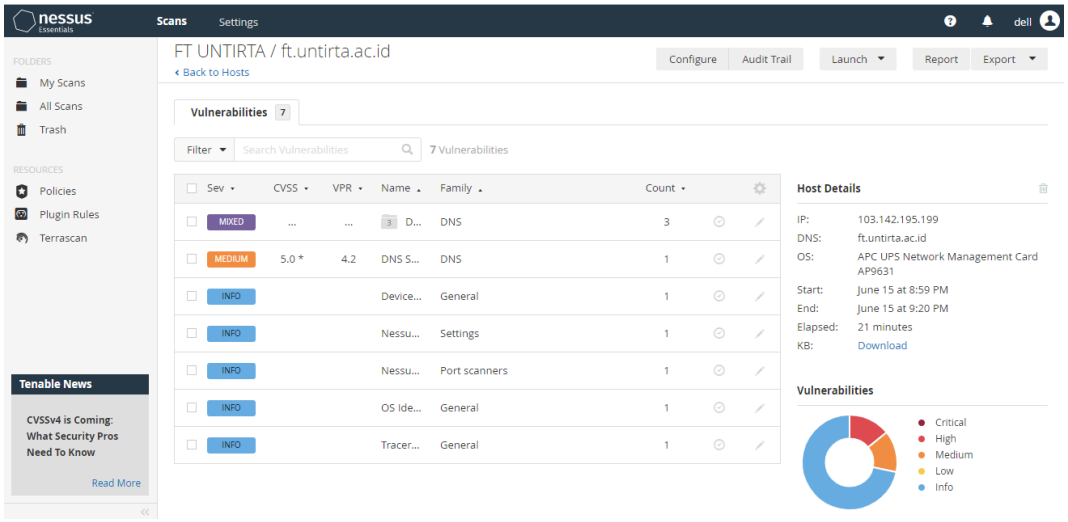
Layanan	**IP *Host***	**Sistem Operasi**	**Jumlah *Port* Terdeteksi**
SIAKAD Untirta (siakad.untirta.ac.id)	103.142.195.98	OpenBSD 4.0 (86%)	8
SPADA Untirta (spada.untirta.ac.id)	103.142.195.106	OpenBSD 4.0 (86%)	12
eAdministrasi Untirta (eadministrasi.untirta.ac.id)	103.142.195.194	OpenBSD 4.0 (86%)	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*

Domain Name	ft.untirta.ac.id	
IP *Host*	103.142.195.199	
Sistem Operasi	APC UPS *Network Management Card*	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
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 *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**
	Critical	***High***	***Medium***	***Low***	
SIAKAD 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 SIAKAD 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

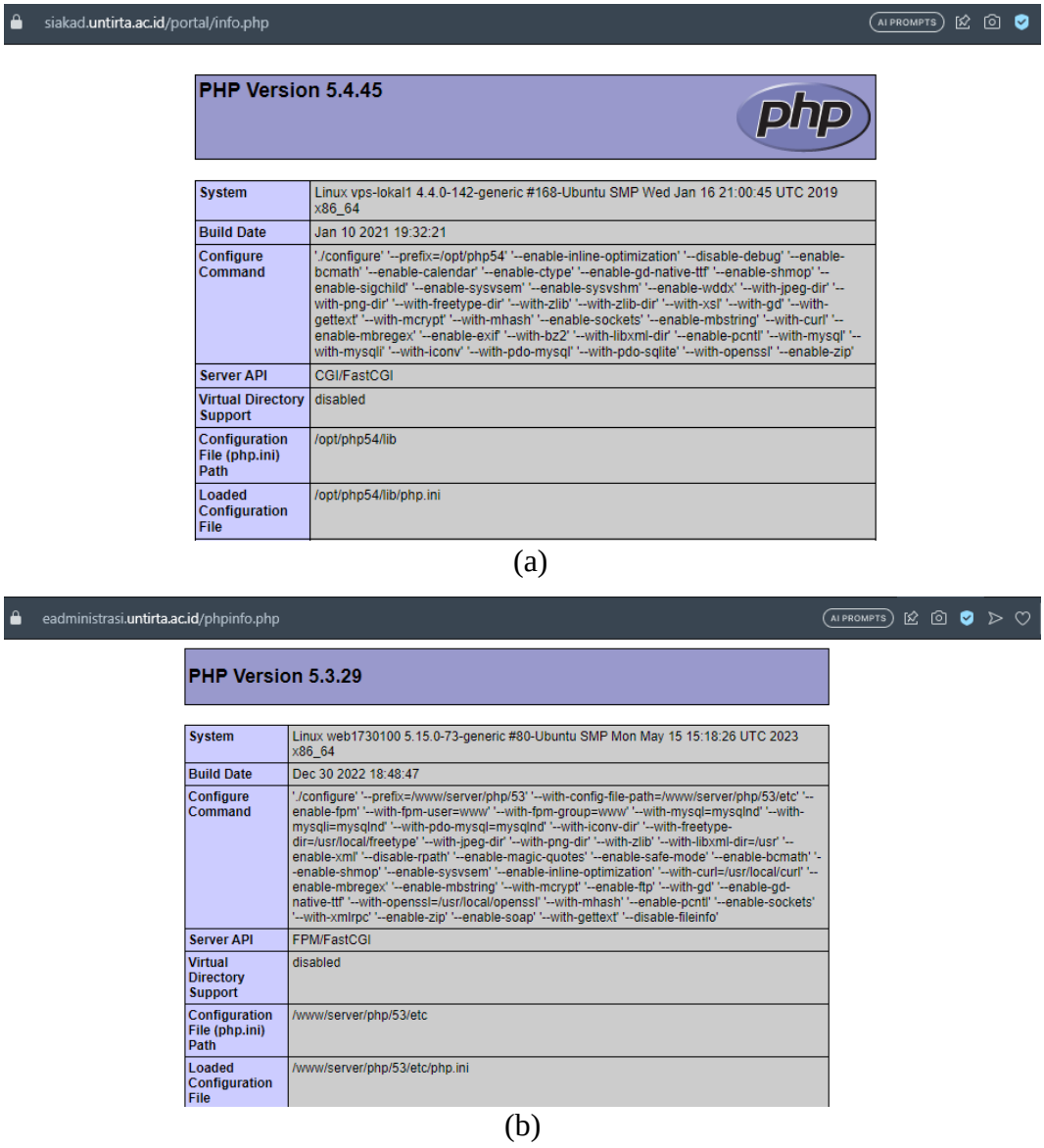
Tabel 4.5 Keseluruhan Kerentanan Layanan Teknologi Informasi Untirta

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

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.



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

Pada Gambar 4.5 merupakan infomasi 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

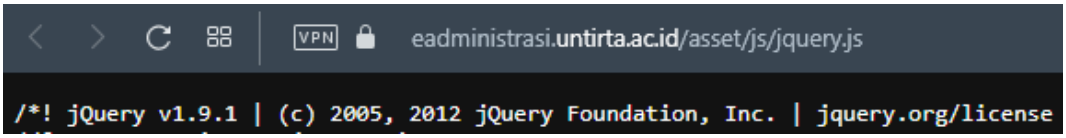
5.4.45, sedangkan pada Gambar 4.5 (b) PHP yang digunakan e-Administrasi Untirta adalah PHP versi 5.3.29 dimana dua versi tersebut merupakan versi PHP yang cukup lawas. Sementara itu, PHP terbaru yang telah dirilis saat ini adalah versi 8.2.7. Untuk menghindari kerentanan tersebut, perlu dilakukan *upgrade* 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. Jquery 1.2 < 3.5.0 *multiple* XSS

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

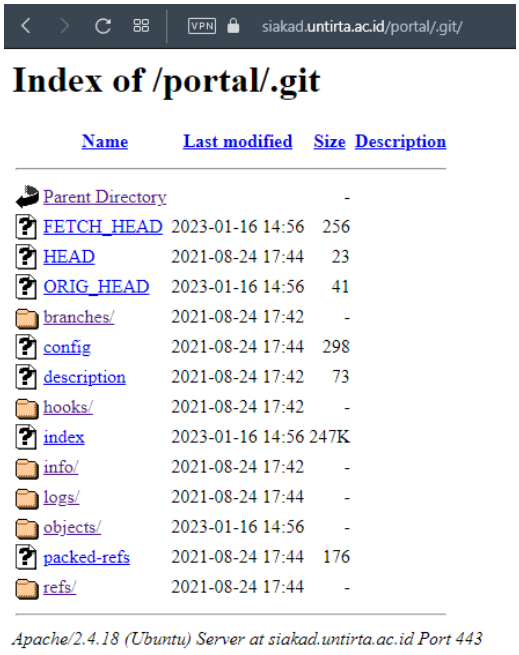


Gambar 4.6 Jquery e-Administrasi Untirta

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.



(a)

(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 menyebar 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 fullfilment*, *problem management*, dan *access management*. Hasil kuesioner *service operation process* dapat dilihat pada Tabel 4.6.

Tabel 4.6 Hasil Kuesioner *Service Operation Process*

Service Operation Process									
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

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.

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 persitiwa 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*

***Service Operation Process* (*Event Management*)**									
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*

***Service Operation Process* (*Incident Management*)**									
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 aktivititas 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 pengidentifiksian 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*

***Service Operation Process* (*Request Fullfilment*)**									
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*

***Service Operation Process* (*Problem Management*)**									
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.

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*

***Service Operation Process* (*Access Management*)**									
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	*Service Operation Process in General*	3,84	1,16
2	*Event Management*	3,53	1,47
3	*Incident Management*	3,65	1,35
4	*Request Fullfilment*	3,35	1,65
5	*Problem Management*	3,56	1,44
6	*Access Management*	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 fullfilment*. 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*

Common Service Operation Activities									
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 *updgrade 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.

DAFTAR PUSTAKA

[1] Dalle, J., A. Akrim, dan Baharuddin, "PENGANTAR TEKNOLOGI INFORMASI" Depok: Rajawali Press, 2020.

[2] Wiranti, Y. T., H. M. J. Saputra, D. B. Tandirau, T. P. Fiqar, M. G. L. Putra, E. Ramadhani, A. I. N. F. Abdullah, "Managing Service Level for Academic Information System Help Desk for XYZ University Based on ITIL V3 Framework," *Proceedings: 2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, https://doi.org/10.1109/ICIC50835.2020.9288592.

[3] Serrano, J., J. Faustino, D. Adriano, R. Pereira, dan M. M. da Silva, "An it service management literature review: Challenges, benefits, opportunities and implementation practices," *Information.*, vol. 12, no. 3, 2021, https://doi.org/10.3390/info12030111.

[4] Trinidad, M., E. Orta, and M. Ruiz, "Gamification in it service management: A systematic mapping study," *Applied Science.*, vol. 11, no. 8, 2021, https://doi.org/10.3390/app11083384.

[5] Rubio, J. L. and M. Arcilla, "How to optimize the implementation of itil through a process ordering algorithm," *Applied Science.*, vol. 10, no. 1, 2020, https://doi.org/10.3390/app10010034.

[6] Mohammed, A., J. Alkhathami, H. Alsuwat, and E. Alsuwat, "Security of Web Applications: Threats, Vulnerabilities, and Protection Methods," *IJCSNS International Journal of Computer Science and Network Security*, vol. 21, no. 8, p. 167, 2021, https://doi.org/10.22937/IJCSNS.2021.21.8.22.

[7] ID-SIRTII/CC, "Data Internet Trafik Tahun 2021 ID-SIRTII/CC," 2021. [Online]. Available: https://www.idsirtii.or.id/trafik/tahunan/2021.html [Accessed 28 November 2022].

[8] Kamilah, I., Ritzkal, dan A. H. Hendrawan, "Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika," *Prosiding Seminar Nasional Sains dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta*, vol. 16, no. 0, pp. 1–9, 2019.

[9] Juardi, D., “Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus,” *Syntax Jurnal Informatika.*, vol. 6, no. 1, pp. 11–19, 2017.

[10] Altulaihan, E. A., A. Alismail, and M. Frikha, “A Survey on Web Application Penetration Testing,” *Electronics.*, vol. 12, no. 5, 2023, https://doi.org/10.3390/electronics12051229.

[11] Pusdainfo Untirta, “Layanan Online Universitas Sultan Ageng Tirtayasa.” [Online] https://pusdainfo.untirta.ac.id/apps/ [Accessed 28 November 2022]

[12] Cartlidge, A., A. Hanna, C. Rudd, I. Macfarlane, J. Windebank, and S. Rance, "An Introductory Overview of ITIL® V3,″ London: The UK Chapter of the itSM, 2007.

[13] Budiman, A., S. Ahdan, dan M. Aziz, “Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment,” *Jurnal Komputasi*, vol. 9, no. 2, pp. 1–10, 2021.

[14] Febriant, A. B., Y. T. Mursityo, dan A. Rachmadi, “Evaluasi Maturity Level Manajemen Layanan Teknologi Informasi Menggunakan Framework ITIL v3 Domain Service Operation Pada 24Slides Corporation,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 6, pp. 5608–5615, 2019.

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

[16] Priyohutomo, A. N. dan M. N. N. Sitokdana, “Dampak Implementasi Iso/Iec 20000 Pada Perusahaan Pt. Visionet Data Internasional,” *SEBATIK*, vol. 24, no. 1, pp. 29–36, 2020.

[17] Steinberg, R., "ITIL Service Operation" Norwich: The Stationery Office, 2011.

[18] Kyytsönen, M., J. Ikonen, A. M. Aalto, dan T. Vehko, “The self-assessed information security skills of the Finnish population: A regression analysis,” *Computer & Security*, vol. 118, 2022, https://doi.org/10.1016/j.cose.2022.102732.

[19] Aslan, Ö., S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, p. 1333, 2023, https://doi.org/10.3390/electronics12061333.

[20] Supriyanto, "Keamanan Jaringan". Serang: Untirta Press, 2017.

[21] Basyarahil, F. A., H. M. Astuti, dan B. C. Hidayanto, “Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya,” *Jurnal Teknik ITS*, vol. 6, no. 1, pp. 122–128, 2017.

[22] Syahab, A. S., E. I. H. Ujianto, dan Rianto, “Penggunaan Wireshark dan Nessus untuk Analisis SSL/TLS Pada Keamanan Data Pengguna Website,” *JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang*, vol. 7, no. 2, pp. 183–192, 2023.

[23] Prakasa, J. E. W., “Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi,” *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 14, no. 2, p. 75, 2020.

[24] Firmansyah M. D., “Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive,” *TELCOMATICS*, vol. 6, no. 1, pp. 2541–5867, 2021, https://doi.org/10.37253/telcomatics.v6i1.4990.

[25] Fadlil A., I. Riadi, dan S. Aji, “Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan,”*Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 3, no. 1, p. 11, 2017.

[26] Yogi, I. Ruslianto, dan S. Bahri, “Analisa Log Web Server Untuk Mengetahui Pola Perilaku Pengunjung Website Menggunakan Teknik Regular Expressions,” *Coding: Jurnal Komputer dan Aplikasi*, vol. 07, no. 01, pp. 120–130, 2019.

[27] Spendolini, S., "Expert Oracle Application Express Security," New York: Apress, 2013.

[28] Hany, M. I., A. Bhawiyuga, dan A. Kusyanti, “Implementasi Cross Site Scripting Vulnerability Assessment Tools berdasarkan OWASP Code Review,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , vol. 5, no. 9, pp. 3745–3753, 2021.

[29] Sulaksono, D. H., G. E. Yuliastuti, C. N. Prabiantissa, dan I. K. A. Ariyasa, "Implementasi Domain Name Server (DNS) Spoofing pada Jaringan Nirkabel," *SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informasi*, pp. 429–434, 2023, https://doi.org/10.31284/p.snestik.2023.4288.

[30] Orisa, M. dan M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web," *Jurnal MNEMONIC*, vol. 4, no. 1, pp. 16–19, 2021.

[31] Raazi, I. M., I. Dwitawati, dan P. Nabila, "Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo dan Sandi Aceh," *JINTECH: Journal of Information Technology*., vol. 4, no. 1, pp. 1–15, 2023.

[32] Sivaprasad, A., "Secured Proactive Network Forensic Framework," *Proceedings: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, pp. 695–699, 2017.

[33] Knapp, D., "The ITSM Process Design Guide Developing, Reengineering, and Improving IT Service Management" Florida: J. Ross Publishing, 2010.

[34] de Jong, A., A. Kolthof, M. Pieper, R. Tjassing, A. van der Veen, and T. Verheijen, "ITIL® V3 Foundation Exam - The Study Guide," Zaltbommel: Van Haren Publishing, 2008.

[35] Rudd, C., J. Sansbury, "ITIL® Maturity Model and Self-assessment Service: user guide" Norwich:AXELOS, 2013.

[36] Nainggolan, J., "Analisis Perbandingan Framework COBIT 5.0 Dengan ITIL Dalam Mengaudit Sistem Informasi," *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, vol. 5, no. 1, pp. 76–85, 2021.

[37] Indeed Editorial Team, "What Are Maturity Models? (With Definition, Types and Benefits)," 2021.[Online] https://www.indeed.com/career-advice/career-development/what-are-maturity-models [Accessed 28 November 2022].

[38] AXELOS, *ITIL Maturity Model*, Norwich:AXELOS, 2013.

[39] Setyadi, R. and E. Priyatiningsih, “Maturity Level of ITSM Analysis Using ITIL V3 Framework in State Electricity Enterprise Purwokerto,” *JUITA: Jurnal Informatika*, vol. 9, no. 1, p. 77, 2021.

[40] Yandri, R., Suharjito, D. N. Utama, dan A. Zahra, “Evaluation model for the implementation of information technology service management using fuzzy ITIL,” *Procedia Computer Science*, vol. 157, pp. 290–297, 2019, https://doi.org/10.1016/j.procs.2019.08.169.

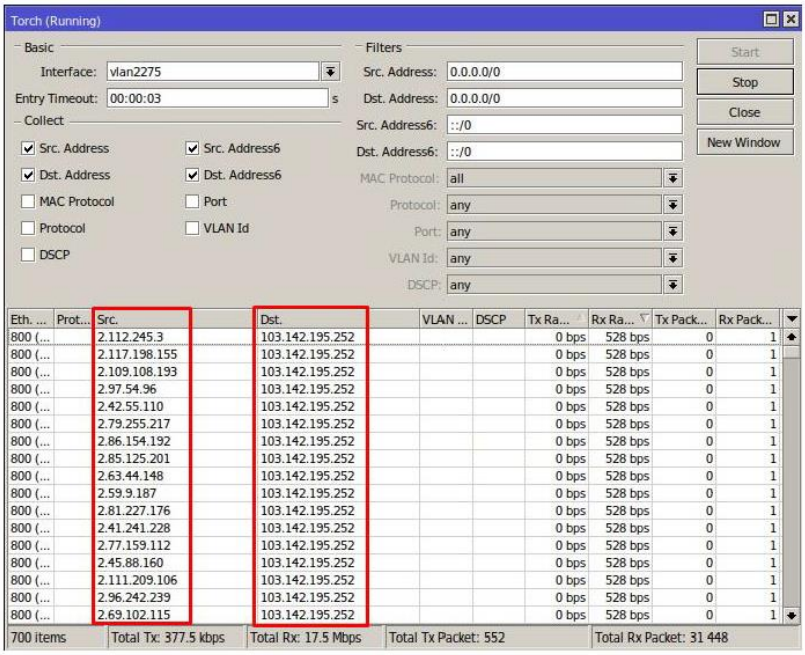
[41] Andri, Paulus, Hanes, and N. P. Wong, “Measuring the Maturity Level of ITSM Using ITIL Framework,” *Proceedings: 2019 Fourth International Conference on Informatics and Computing (ICIC)*, 2019, https://doi.org/10.1109/ICIC47613.2019.8985879.

[42] Suryani, N. P. S. M., I. M. D. Ardiada, and I. G. N. Janardana, “Audit of Governance Information Technology Services Using ITIL v3 Focuses on Service Operation Domain in Institution X,” *International Journal of Engineering and Emerging Technology*, vol. 2, no. 2, pp. 91–95, 2017.

LAMPIRAN A DATA *LOG SERVER* UNTIRTA

Pada tanggal 12 Agustus 2022 Server UNTIRTA Terkena DDOS/serangan

Berikit hasil Torch dari sisi Router UNTIRTA terdapat DDOS/serangan ke arah IP Server UNTIRTA (103.142.195.252).

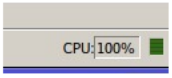


Log dari sisi Server

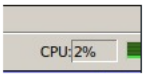
```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    132 103.142.195.252:2406    182.0.183.189:58411     ESTABLISHED
tcp        0      1 103.142.195.252:57594   74.125.24.26:25         SYN_SENT
tcp6       0      0 103.142.195.252:80      140.213.138.40:11387    FIN_WAIT2
tcp6       0      0 103.142.195.252:443     114.119.155.96:51383    TIME_WAIT
tcp6       0      0 103.142.195.252:443     114.119.152.108:27539   TIME_WAIT
tcp6       0      0 103.142.195.252:443     114.119.155.96:50921    TIME_WAIT
tcp6       0      0 103.142.195.252:443     182.3.40.223:37048      TIME_WAIT
tcp6       0      0 103.142.195.252:443     182.3.40.223:37050      TIME_WAIT
tcp6       0      0 103.142.195.252:443     182.3.40.223:37044      TIME_WAIT
tcp6       0      0 103.142.195.252:80      140.213.136.168:12594   SYN_RECV
tcp6       0      0 103.142.195.252:443     182.3.39.246:55525      TIME_WAIT
tcp6       0      0 103.142.195.252:443     182.3.38.117:59403      ESTABLISHED
tcp6       0      0 103.142.195.252:443     182.3.39.234:55529      ESTABLISHED
tcp6       0      0 103.142.195.252:443     182.3.40.223:37046      TIME_WAIT
tcp6       0      0 103.142.195.252:443     114.119.152.108:28473   TIME_WAIT
tcp6       0      0 103.142.195.252:443     114.119.141.173:52255   TIME_WAIT
tcp6       0      0 103.142.195.252:2222    182.0.183.189:45223     ESTABLISHED
tcp6       0      0 103.142.195.252:443     182.0.147.147:42056     TIME_WAIT
tcp6       0      0 103.142.195.252:443     140.213.132.195:54882   ESTABLISHED
```

Berikut salah satu IP Address yang terdeteksi melakukan DDOS/serangan kea rah IP Server UNTIRTA.

Dampaknya Load CPU Router UNTIRTA full 100%, Sehingga koneksi internet semua site UNTIRTA dan Servers Down.



Action sementara dari sisi kami dilakukan Drop/Blackhole IP Server UNTIRTA (103.142.195.252) ke atah internet internasional, Load CPU Router UNTIRTA sudah normal kembali dan Internet sudah bisa digunakan, namun Server tidak dapat dapat di akses dari beberapa Proviser seperti Indihome.



Pada tanggal 28 Agustus 2022 hasil monitoring sudah tidak ditemukan DDOS/serangan kearah Server UNTIRTA, Sehingga kami lakukan disable IP Server UNTIRTA dari list Drop/Blackhole

Internet dan Server untirta sudah normal kembali.

LAMPIRAN B HASIL *NETWORK SCANNING*

Lampiran B.1 *Network Scanning* SIAKAD Untirta

Domain Name		siakad.untirta.ac.id	
***Host* IP**		103.142.195.98	
Sistem Operasi		OpenBSD 4.0 (86%)	
No	**Port/Protokol**	**Status**	***Service***
1	25/tcp	*Filtered*	*smtp*
2	80/tcp	*Open*	*http*
3	111/tcp	*Open*	*rpcbind*
4	139/tcp	*Filtered*	*netbios-ssn*
5	443/tcp	*Open*	*https*
6	445/tcp	*Filtered*	*microsoft-ds*
7	3306/tcp	*Open*	*mysql*
8	5678/tcp	*Filtered*	*rrac*

Lampiran B.2 *Network Scanning* SPADA Untirta

Domain Name		spada.untirta.ac.id	
***Host* IP**		103.142.195.106	
Sistem Operasi		OpenBSD 4.0 (86%)	
No	**Port/Protokol**	**Status**	***Service***
1	25/tcp	filtered	smtp
2	80/tcp	open	http
3	139/tcp	filtered	netbios-ssn
4	443/tcp	open	https
5	445/tcp	filtered	microsoft-ds
6	888/tcp	open	accessbuilder
7	2000/tcp	open	cisco-sccp
8	3003/tcp	open	cgms
9	5060/tcp	open	sip
10	5678/tcp	filtered	rrac

11	8080/tcp	open	http-proxy
12	8888/tcp	open	sun-answerbook

Lampiran B.3 *Network Scanning* e-Administrasi Untirta

Domain Name		eadministrasi.untirta.ac.id	
***Host* IP**		103.142.195.194	
Sistem Operasi		OpenBSD 4.0 (86%)	
No.	**Port/Protokol**	**Status**	***Service***
1.	25/tcp	Filtered	smtp
2.	80/tcp	Open	http
3.	139/tcp	Filtered	netbios-ssn
4.	443/tcp	Open	https
5.	445/tcp	Filtered	microsoft-ds
6.	5678/tcp	filtered	rrac

Lampiran B.4 *Network Scanning Website* Untirta dan FT Untirta

Domain Name		untirta.ac.id/ft.untirta.ac.id	
***Host* IP**		103.142.195.199	
Sistem Operasi		FreeBSD 6.2-RELEASE (87%)	
No.	**Port/Protokol**	**Status**	***Service***
1.	20/tcp	closed	ftp-data
2.	21/tcp	open	ftp
3.	22/tcp	closed	ssh
4.	53/tcp	open	domain
5.	80/tcp	open	http
6.	110/tcp	open	pop3
7.	143/tcp	open	imap
8.	443/tcp	open	https
9.	465/tcp	open	smtps
10.	587/tcp	open	submission
11.	993/tcp	open	imaps

12.	995/tcp	open	pop3s
13.	2222/tcp	open	EtherNetIP-3
14.	35500/tcp	closed	unknown

LAMPIRAN C HASIL *VULNERABILITY SCANNING*

Lampiran C.1 *Vulnerability Scanning* SIAKAD Untirta

Domain Name	siakad.untirta.ac.id	
***Host* IP**	103.142.195.98	
Sistem Operasi	Linux Kernel 2.6.32-754.23.1.el6.x86_64	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
Critical	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)	9.8
9	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)	9.8
	SSL Version 2 and 3 Protocol Detection	9.8
	PHP Unsupported Version Detection	10
	PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow	10
High	PHP 5.4.x < 5.4.17 Buffer Overflow	9.3
16	CGI Generic SQL Injection (blind)	8.3
	PHP < 7.3.24 Multiple Vulnerabilities	7.5
	SSL Medium Strength Cipher Suites Supported (SWEET32)	7.5
	ADOdb tmssql.php do Parameter Arbitrary PHP Function Execution	7.5
	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption	7.5
	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities	7.5
	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities	7.5
	PHP 5.4.x < 5.4.36 'process_nested_data' RCE	7.5
	SNMP Agent Default Community Name (public)	7.5
	PHP 5.4.x < 5.4.13 Information Disclosure	7.3
	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation	7.2
MEDIUM	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities	6.8
19	TLS Version 1.0 Protocol Detection	6.5
	TLS Version 1.1 Protocol Deprecated	6.5

	Browsable Web Directories	5.3
	PHP 5.4.x < 5.4.12 Information Disclosure	5.3
	PHP < 7.3.28 Email Header Injection	5.3
	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	nginx < 1.17.7 Information Disclosure	5.3
	Git Repository Served by Web Server	5.0
	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS	5.0
	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.35 'donote' DoS	5.0
	SNMP 'GETBULK' Reflection DDoS	5.0
	SSH Weak Algorithms Supported	4.3
	Web Application Potentially Vulnerable to Clickjacking	4.3
LOW	Web Server Allows Password Auto-Completion	N/A
6	Weak Key Exchange Algorithms Enabled	3.7
	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS	2.6
	SSH Server CBC Mode Ciphers Enabled	2.6
	SSH Weak MAC Algorithms Enabled	2.6
	Web Server Transmits Cleartext Credentials	2.6

Lampiran C.2 *Vulnerability Scanning* SPADA Untirta

Domain Name	spada.untirta.ac.id	
***Host* IP**	103.142.195.106	
Sistem Operasi	Linux Kernel 4.15.0-211-generic	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
CRITICAL 1	PHP Unsupported Version Detection	10
HIGH 1	SNMP Agent Default Community Name (public)	5.9
MEDIUM	TLS Version 1.0 Protocol Detection	6.5
6	TLS Version 1.1 Protocol Deprecated	6.5
	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	nginx < 1.17.7 Information Disclosure	5.3
	SNMP 'GETBULK' Reflection DDoS	5.0
LOW 1	Web Server Allows Password Auto-Completion	N/A

Lampiran C.3 *Vulnerability Scanning* E Administrasi Untirta

Domain Name	eadministrasi.untirta.ac.id	
***Host* IP**	103.142.195.98	
Sistem Operasi	Linux Kernel 2.6	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
CRITICAL 1	PHP Unsupported Version Detection	10
HIGH	CGI Generic SQL Injection (blind)	8.3
4	DNS Server Spoofed Request Amplification DDoS	7.5
	PHP < 7.3.24 Multiple Vulnerabilities	7.5
	CGI Generic SQL Injection (blind, time based)	7.5
MEDIUM	JQuery 1.2 < 3.5.0 Multiple XSS	6.1
5	PHP < 7.3.28 Email Header Injection	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	DNS Server Recursive Query Cache Poisoning Weakness	5.0
	Web Application Potentially Vulnerable to Clickjacking	4.3
LOW 1	Web Server Allows Password Auto-Completion	N/A

Lampiran C.4 *Vulnerability Scanning* Web Untirta

Domain Name	untirta.ac.id	
***Host* IP**	103.142.195.199	
Sistem Operasi	Linux Kernel 2.6	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
HIGH 1	DNS Server Spoofed Request Amplification DDoS	7.5
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	5.3
2	DNS Server Recursive Query Cache Poisoning Weakness	5.0
LOW	SSH Weak Key Exchange Algorithms Enabled	3.7
2	SSH Server CBC Mode Ciphers Enabled	2.6

Lampiran C.5 Vulnerability Scanning Web FT Untirta

Domain Name	ft.untirta.ac.id	
***Host* IP**	103.142.195.199	
Sistem Operasi	APC UPS Network Management Card	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
HIGH	DNS Server Spoofed Request Amplification DDoS	7.5
MEDIUM	DNS Server Recursive Query Cache Poisoning Weakness	5.0

LAMPIRAN D REKOMENDASI

Lampiran D.1 Rekomendasi Keamanan Layanan Teknologi Informasi Untirta

Kerentanan	Rekomendasi
PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)	Upgrade PHP ke versi terbaru
PHP 5.4.x < 5.4.39 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.40 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.41 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.42 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)	
PHP Unsupported Version Detection	
PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow	
PHP Unsupported Version Detection	
PHP Unsupported Version Detection	
PHP 5.4.x < 5.4.17 Buffer Overflow	
PHP < 7.3.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption	
PHP 5.4.x < 5.4.30 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.34 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.36 'process_nested_data' RCE	
PHP 5.4.x < 5.4.13 Information Disclosure	
PHP 5.4.x < 5.4.19 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.37 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.44 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.45 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation	
PHP < 7.3.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.32 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.12 Information Disclosure	
PHP < 7.3.28 Email Header Injection	
PHP 5.4.x < 5.4.16 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.26 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS	
PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities	
PHP 5.4.x < 5.4.35 'donote' DoS	

PHP < 7.3.28 Email Header Injection	
PHP 5.4.x < 5.4.31 CLI Server 'header' DoS	
SSL Version 2 and 3 Protocol Detection	Upgrade protokol keamanan ke TLS 1.2 atau 1.3
SSL Medium Strength Cipher Suites Supported (SWEET32)	
TLS Version 1.0 Protocol Detection	
TLS Version 1.1 Protocol Deprecated	
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	
TLS Version 1.0 Protocol Detection	
TLS Version 1.1 Protocol Deprecated	
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	
SSH Weak Algorithms Supported	Hubungi vendor atau lihat dokumentasi produk untuk menghapus chipers(sandi) yang lemah
SSH Server CBC Mode Ciphers Enabled	
SSH Weak MAC Algorithms Enabled	
SSH Weak Key Exchange Algorithms Enabled	
SSH Server CBC Mode Ciphers Enabled	
SSH Weak Key Exchange Algorithms Enabled	
DNS Server Spoofed Request Amplification DDoS	Batasi akses ke server DNS dari jaringan publik atau konfigurasi ulang untuk menolak permintaan tersebut.
DNS Server Spoofed Request Amplification DDoS	
DNS Server Spoofed Request Amplification DDoS	
DNS Server Recursive Query Cache Poisoning Weakness	Batasi kueri rekursif ke host yang harus menggunakan nameserver ini
DNS Server Recursive Query Cache Poisoning Weakness	
DNS Server Recursive Query Cache Poisoning Weakness	
CGI Generic SQL Injection (blind)	Ubah skrip CGI yang terpengaruh sehingga terhindar dari argumen dengan benar
CGI Generic SQL Injection (blind, time based)	
CGI Generic SQL Injection (blind)	
SNMP Agent Default Community Name (public)	Nonaktifkan layanan SNMP pada host jarak jauh ketika tidak menggunakannya
SNMP Agent Default Community Name (public)	
SNMP 'GETBULK' Reflection DDoS	
SNMP 'GETBULK' Reflection DDoS	
nginx < 1.17.7 Information Disclosure	Upgrade nginx ke versi terbaru

nginx < 1.17.7 Information Disclosure	
Web Server info.php / phpinfo.php Detection	Hapus file yang terpengaruh (phpinfo.php)
Web Server info.php / phpinfo.php Detection	
Web Server info.php / phpinfo.php Detection	
Web Server Allows Password Auto-Completion	Tambahkan atribut 'autocomplete=off' untuk mencegah browser menyimpan kredensial dalam cache
Web Server Allows Password Auto-Completion	
Web Server Allows Password Auto-Completion	
Web Application Potentially Vulnerable to Clickjacking	Kembalikan header HTTP X-Frame-Options atau Content-Security-Policy (dengan arahan 'frame-ancestors') dengan respons halaman
Web Application Potentially Vulnerable to Clickjacking	
JQuery 1.2 < 3.5.0 Multiple XSS	Upgrade JQuery ke versi terbaru
DNS Server Cache Snooping Remote Information Disclosure	Hubungi vendor perangkat lunak DNS untuk perbaikan.
ADOdb tmssql.php do Parameter Arbitrary PHP Function Execution	Hapus skrip pengujian atau tingkatkan ke ADOdb versi 4.70 atau lebih tinggi
Browsable Web Directories	Pastikan direktori yang dapat dijelajahi tidak membocorkan informasi rahasia atau memberikan akses ke sumber daya sensitif. Selain itu, gunakan pembatasan akses atau nonaktifkan pengindeksan direktori untuk semua yang melakukannya
Git Repository Served by Web Server	Verifikasi bahwa repositori Git yang terdaftar disajikan dengan sengaja
Web Server Transmits Cleartext Credentials	Pastikan bahwa setiap formulir sensitif mengirimkan konten melalui HTTPS

Lampiran D.2 Rekomendasi Manajemen Layanan Teknologi Informasi Untirta

No.	Proses	Rekomendasi
1	*Service Operation Process in General*	Meningkatkan peran, fungsi, kebijakan, serta faktor keberhasilan terutama indikator kinerja utama pada *service operation process* yang dimiliki oleh UPT Data dan Informasi Untirta.
2	*Event Management*	Meningkatkan pengelolaan peristiwa terutama dalam peninjauan setiap peristiwa yang ada pada layanan teknologi informasi Untirta.
3	*Incident Management*	Meningkatkan penanganan insiden terutama dalam pengidentifiksian insiden serta mendokumentasikan insiden yang terjadi pada layanan teknologi informasi Untirta.
4	*Request Fullfilment*	Meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.
5	*Problem Management*	Meningkatkan pencegahan masalah yang ada pada layanan terutama pada pendeteksian kesalahan serta membuat *known error database* untuk memudahkan diagnosis serta resolusi pada suatu masalah.
6	*Access Management*	Meningkatkan manajemen dalam pemberian akses terhadap layanan teknologi informasi Untirta
7	*Common Service Operation Activities*	Meningkatkan manajemen pada aktivitas umum service operation dengan melakukan pemantauan dan kendali layanan, melakukan audit service operation, serta mengukur ketersediaan dari perspektif teknologi informasi dan organisasi

LAMPIRAN E HASIL KUESIONER ITIL V3 *SERVICE OPERATION*

No		Proses Operasi Layanan	Responden				Total	Count	AVG	Gap
			1	2	3	4				
1		UPT Data dan Informasi memiliki dan menetapkan peran dan fungsi **dari setiap proses pada service operation** dengan jelas	3	4	4	5	16	4	4	1
2		UPT Data dan Informasi telah menentukan *Goal*, Objektif, tujuan dan ruang lingkup yang jelas **dari setiap proses service operation** pada layanan teknologi informasi	3	4	5	5	17	4	4,25	0,75
3		UPT Data dan Informasi telah menentukan nilai bisnis **dari setiap proses pada service operation**	3	4	3	5	15	4	3,75	1,25
4		UPT Data dan Informasi telah menetapkan kebijakan, prinsip, dan konsep dasar **dari setiap proses service operation** pada layanan teknologi informasi	3	4	4	5	16	4	4	1
5		UPT Data dan Informasi telah menentukan pemicu, input, output, dan antarmuka **dari setiap proses service operation** pada layanan teknologi informasi	3	4	5	4	16	4	4	1
6		UPT Data dan Informasi telah menenetapkan IKU dan metrik **dari setiap proses pada service operation**	3	3	3	4	13	4	3,25	1,75
7		UPT Data dan Informasi telah menentukan pelaporan **dari setiap proses service operation** pada layanan teknologi informasi	3	4	2	5	14	4	3,5	1,5
8		UPT Data dan Informasi telah menentukan tantangan, faktor keberhasilan dan risiko yang kritis pada **setiap proses service operation** pada layanan teknologi informasinya	3	4	5	4	16	4	4	1
SCORE			24	31	31	37	123	32	3,84	1,16
No	**EM**	**EVENT MANAGEMENT / MANAJEMEN ACARA**								
9	1	UPT Data dan Informasi memiliki cara mengetahui terjadinya suatu peristiwa dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5

10	2	UPT Data dan Informasi memiliki aktivitas pemberitahuan peristiwa dan pendektesian peristiwa pada layanan teknologi informasinya	3	4	4	3	14	4	3,5	1,5
11	3	UPT Data dan Informasi menyaring peristiwa-peristiwa yang terjadi pada layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
12	4	UPT Data dan Informasi mengkategorisasi setiap peristiwa yang terjadi dari layanan teknologi informasinya	3	3	5	4	15	4	3,75	1,25
13	5	UPT Data dan Informasi melakukan korelasi antar peristiwa yang terjadi dari layanan teknologi informasinya	3	3	3	4	13	4	3,25	1,75
14	6	UPT Data dan Informasi mengetahui pemicu/penyebab peristiwa yang terjadi dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
15	7	Setelah peristiwa terjadi, UPT Data dan Informasi memiliki aktivitas untuk memilih tanggapan yang tepat untuk peristiwa pada layanan teknologi informasi tersebut	3	3	5	4	15	4	3,75	1,25
16	8	UPT Data dan Informasi melakukan tinjauan dari hasil tanggapan yang diberikan pada peristiwa yang terjadi dari layanan teknologi informasinya	3	3	3	4	13	4	3,25	1,75
17	9	UPT Data dan Informasi mengetahui jika peristiwa tersebut telah selesai dan dapat ditutup	3	4	4	4	15	4	3,75	1,25
SCORE			30	33	40	39	142	40	3,53	1,47
No	**IM**	**INCIDENT MANAGEMENT / MANAJEMEN INSIDEN**								
18	1	UPT Data dan Informasi telah menyepakati rentang waktu untuk semua tahapan penanganan insiden pada layanan teknologi informasinya	3	4	4	3	14	4	3,5	1,5
19	2	UPT Data dan Informasi telah menentukan model insiden yang terjadi pada layanan teknologi informasi	3	3	4	5	15	4	3,75	1,25
20	3	UPT Data dan Informasi telah menentukan Insiden utama (*Major*) yag terjadi pada layanan teknologi informasi	3	4	5	4	16	4	4	1

21	4	UPT Data dan Informasi memiliki aktivititas pengidentifikasian insiden yang terjadi pada layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
22	5	UPT Data dan Informasi melakukan *logging* pada setiap insiden yang terjadi pada layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
23	6	UPT Data dan Informasi melakukan pengelompokan insiden yang terjadi pada layanan teknologi informasi	3	3	4	4	14	4	3,5	1,5
24	7	UPT Data dan Informasi mengurutkan insiden yang terjadi pada layanan teknologi informasi berdasarkan priotitas	3	4	4	4	15	4	3,75	1,25
25	8	UPT Data dan Informasi melakukan diagnosa awal dari insiden yang terjadi pada layanan teknologi informasi	3	4	3	4	14	4	3,5	1,5
26	9	UPT Data dan Informasi melakukan eskalasi insiden pada beberapa insiden yang terjadi pada layanan teknologi informasi	3	4	5	4	16	4	4	1
27	10	UPT Data dan Informasi melakukan investigasi pada insiden yang terjadi pada layanan teknologi informasi	3	4	3	4	14	4	3,5	1,5
28	11	UPT Data dan Informasi melakukan pemulihan pasca insiden yang terjadi pada layanan teknologi informasi	3	4	4	5	16	4	4	1
29	12	UPT Data dan Informasi mengetahui jika insiden tersebut telah selesai ditangani dan dapat ditutup	3	4	4	4	15	4	3,75	1,25
SCORE			39	48	50	53	190	52	3,65	1,35
No	**RF**	**REQUEST FULLFILMENT / PEMENUHAN PERMINTAAN**								
30	1	UPT Data dan Informasi memiliki pilihan untuk meminta kebutuhan apa saja yang ingin dipenuhi untuk mengembangkan layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
31	2	Dalam permintaan pemenuhan kebutuhan, UPT Data dan Informasi memerlukan persetujuan keuangan dari pihak yang berwenang	3	4	3	3	13	4	3,25	1,75
32	3	Dalam permintaan pemenuhan kebutuhan, UPT Data dan Informasi juga memerlukan persetujuan lainnya dari pihak yang berwenang	3	4	3	3	13	4	3,25	1,75

33	4	UPT Data dan Informasi mendapatkan permintaan kebutuhan yang teepenuhi untuk layanan teknologi informasi	3	4	3	3	13	4	3,25	1,75
34	5	UPT Data dan Informasi mengetahui kapan permintaan kebutuhan telah selesai	3	4	4	4	15	4	3,75	1,25
SCORE			18	23	20	21	82	24	3,35	1,65
No	**PM**	**PROBLEM MANAGEMENT / MANAJEMEN MASALAH**								
35	1	UPT Data dan Informasi memiliki aktivitas untuk mendeteksi masalah pada layanan teknologi informasi	3	3	4	5	15	4	3,75	1,25
36	2	UPT Data dan Informasi melakukan *logging*/membukukan masalah yang terjadi pada layanan teknologi informasi	3	3	3	5	14	4	3,5	1,5
37	3	UPT Data dan Informasi mengkategorisasi setiap masalah yang terjadi dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
38	4	UPT Data dan Informasi mengurutkan masalah yang terjadi pada layanan teknologi informasi berdasarkan priotitas	3	4	3	4	14	4	3,5	1,5
39	5	UPT Data dan Informasi melakukan penyelidikan dan diagnosis masalah yang terjadi pada layanan teknologi informasi	3	4	4	4	15	4	3,75	1,25
40	6	UPT Data dan Informasi melakukan pencarian solusi masalah yang terjadi	3	4	5	3	15	4	3,75	1,25
41	7	UPT Data dan Informasi menambahkan masalah layanan kedalam catatan kesalahan yang telah diketahui (*known error record*)	3	3	5	3	14	4	3,5	1,5
42	8	UPT Data dan Informasi melakukan proses pemecahan masalah	3	4	4	4	15	4	3,75	1,25
43	9	UPT Data dan Informasi mengetahui jika suatu masalah telah selesai ditangani dan dapat ditutup	3	4	3	4	14	4	3,5	1,5
44	10	UPT Data dan Informasi melakukan peninjauan kembali jenis masalah pada layanan teknologi informasi	3	4	4	4	15	4	3,75	1,25
45	11	UPT Data dan Informasi melakukan pendeteksian kesalahan dalam lingkungan pengembangan	3	3	3	4	13	4	3,25	1,75

46	12	UPT Data dan Informasi memanfaatkan CMS (*Configuration Management System*) sebagai sumber yang berharga untuk manajemen masalah	3	3	5	3	14	4	3,5	1,5
47	13	UPT Data dan Informasi memiliki database kesalahan yang diketahui (*Known Error Database*) untuk memungkinkan diagnosis dan resolusi yang lebih cepat	3	3	3	4	13	4	3,25	1,75
SCORE			42	48	53	55	198	56	3,56	1,44
No	**AM**	**ACCESS MANAGEMENT / MANAJEMEN AKSES**								
48	1	UPT Data dan Informasi memiliki aktivitas permintaan untuk mengakses layanan	3	4	3	3	13	4	3,25	1,75
49	2	UPT Data dan Informasi melakukan verifikasi dari permintaan akses layanan tersebut	3	4	3	4	14	4	3,5	1,5
50	3	UPT Data dan Informasi menyediakan hak untuk mengakses layanan	3	4	4	3	14	4	3,5	1,5
51	4	UPT Data dan Informasi melakukan pemantauan status identitas	3	4	4	4	15	4	3,75	1,25
52	5	UPT Data dan Informasi melakukan pencatatan dan penelusuran kegiatan akses	3	4	4	5	16	4	4	1
53	6	UPT Data dan Informasi dapat mengahapus atau mengurangi hak akses	3	4	4	3	14	4	3,5	1,5
SCORE			21	28	26	25	100	28	3,58	1,42
OVERALL SCORE SOP			159	192	201	211	763	212	3,60	1,40
Kegiatan Umum Operasi Layanan										
1		UPT Data dan Informasi melakukan kegiatan pemantauan dan kendali pada layanan dengan teratur dan berkelanjutan	3	4	4	2	13	4	3,25	1,75
2		UPT Data dan Informasi memastikan bahwa kondisi tertentu dipenuhi (atau tidak terpenuhi) dan jika tidak,maka akan menaikkan	3	4	3	2	12	4	3	2

	peringatan ke grup yang sesuai (mis. Ketersediaan perangkat jaringan utama)								
3	UPT Data dan Informasi memastikan bahwa kinerja atau pemanfaatan komponen atau sistem berada dalam kisaran yang ditentukan (mis. Ruang disk atau pemanfaatan memori)	3	4	4	4	15	4	3,75	1,25
4	UPT Data dan Informasi mendeteksi jenis atau tingkat aktivitas yang abnormal dalam infrastruktur (mis. Ancaman keamanan potensial)	3	4	3	4	14	4	3,5	1,5
5	UPT Data dan Informasi mendeteksi perubahan yang tidak sah (mis. Pengenalan perangkat lunak baru)	3	4	4	4	15	4	3,75	1,25
6	UPT Data dan Informasi memastikan kepatuhan terhadap kebijakan organisasi (mis. Penggunaan email yang tidak tepat)	3	4	4	3	14	4	3,5	1,5
7	UPT Data dan Informasi melacak informasi apa pun yang digunakan untuk mengukur indikator kinerja utama	3	2	4	5	14	4	3,5	1,5
8	UPT Data dan Informasi menafsirkan makna sebuah informasi dengan tepat	3	4	3	4	14	4	3,5	1,5
9	UPT Data dan Informasi dapat menentukan dimana informasi akan digunakan (mis. data masalah di suatu divisi dapat diakses divisi yang bertanggung jawab)	3	4	4	4	15	4	3,75	1,25
10	UPT Data dan Informasi memastikan bahwa pembuat keputusan memiliki akses ke informasi yang akan memungkinkan mereka untuk membuat keputusan	3	4	4	3	14	4	3,5	1,5
11	UPT Data dan Informasi merutekan informasi yang dilaporkan ke orang, kelompok, atau alat yang tepat	3	4	4	4	15	4	3,75	1,25
12	UPT Data dan Informasi menggunakan alat untuk menentukan kondisi apa yang mewakili operasi normal atau abnormal	3	4	4	3	14	4	3,5	1,5
13	UPT Data dan Informasi memiliki kegiatan dalam mengatur kinerja perangkat, sistem atau layanan	3	3	3	2	11	4	2,75	2,25

14	UPT Data dan Informasi mengukur ketersediaan dari perspektif TI dan organisasi	3	3	5	2	13	4	3,25	1,75
15	UPT Data dan Informasi memulai tindakan korektif, yang dapat diotomatisasi (mis. Reboot perangkat dari jarak jauh atau jalankan skrip), atau manual	3	4	5	4	16	4	4	1
16	UPT Data dan Informasi melakukan audit operasi layanan	3	4	4	2	13	4	3,25	1,75
17	Dalam operasi TI UPT Data dan Informasi memiliki peran penjadwalan pekerjaan, peran cadangan dan pemulihan, dan peran cetak dan output yang ditentukan	3	4	2	5	14	4	3,5	1,5
18	UPT Data dan Informasi memiliki manajemen mainframe	3	4	4	4	15	4	3,75	1,25
19	UPT Data dan Informasi memiliki manajemen dan dukungan server	3	4	4	4	15	4	3,75	1,25
20	UPT Data dan Informasi memiliki manajemen Jaringan	3	4	4	4	15	4	3,75	1,25
21	UPT Data dan Informasi memiliki penyimpanan dan arsip	3	4	4	4	15	4	3,75	1,25
22	UPT Data dan Informasi memiliki Administrasi Database	3	4	4	4	15	4	3,75	1,25
23	UPT Data dan Informasi memiliki Manajemen Layanan Direktori	3	4	4	4	15	4	3,75	1,25
24	UPT Data dan Informasi memiliki Dukungan desktop	3	4	4	4	15	4	3,75	1,25
25	UPT Data dan Informasi memiliki Manajemen Middleware	3	4	4	4	15	4	3,75	1,25
26	UPT Data dan Informasi memiliki Manajemen Internet/Web	3	4	4	3	14	4	3,5	1,5
27	UPT Data dan Informasi memiliki Fasilitas dan manajemen pusat data	3	4	4	3	14	4	3,5	1,5
28	UPT Data dan Informasi memiliki Manajemen Keamanan Informasi dalam Operasi Layanan	3	4	4	4	15	4	3,75	1,25
OVERALL SCORE CSOA		84	108	108	99	399	112	3,56	1,44