AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN COBIT 5 PADA UNIVERSITAS SULTAN AGENG TIRTAYASA

SKRIPSI

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

Disusun oleh:

NURFITRIANI ROMADHONA

NPM. 3332180052

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS SULTAN AGENG TIRTAYASA

2024

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya sebagai penulis Skripsi berikut:

Judul	: Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa.
Nama Mahasiswa	: Nurfitriani Romadhona
NPM	: 3332180052
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 di kemudian 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, 1 Desember 2023

Nurfitriani Romadhona

NPM. 3332180052

LEMBAR PENGESAHAN

Dengan ini ditetapkan bahwa Skripsi berikut:

Judul	: Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa.
Nama Mahasiswa	: Nurfitriani Romadhona
NPM	: 3332180052
Fakultas/Jurusan	: Teknik/Teknik Elektro

Telah diuji dan dipertahankan pada tanggal 1 Desember 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 S.Sos., M.Si	.....
Penguji I : Masjudin, S.T., M.Eng.	.....
Penguji II : Fadil Muhammad, S.T., M.T.	.....

Mengetahui,
Ketua Jurusan

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

PRAKATA

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan laporan Skripsi dengan judul "Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa". Penulisan laporan Skripsi ini merupakan salah satu syarat untuk dapat menyelesaikan program studi S1 dan untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro, Universitas Sultan Ageng Tirtayasa. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak sangatlah sulit bagi saya untuk menyelesaikan laporan Skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Orang tua dan keluarga saya yang selalu memberikan dukungan dan doa.
2. Bapak Dr. Romi Wiryadinata, S.T., M.Eng., sebagai Dosen Pembimbing Akademik dan Ketua Program Studi Teknik Elektro, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
3. Bapak Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM., sebagai Dosen Pembimbing I Skripsi yang telah memberikan arahan dan bimbingannya kepada penulis untuk menyelesaikan Skripsi.
4. Bapak Anis Fuad, S.Sos., M.Si., sebagai Dosen Pembimbing II Skripsi sekaligus kepala UPT. Pusat Data dan Informasi yang telah memberikan arahan dan bimbingannya kepada penulis untuk menyelesaikan Skripsi.

Penulis menyadari bahwa laporan Skripsi ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk meningkatkan wawasan kepada penulis agar menjadi lebih baik. Akhir kata, penulis mohon maaf apabila terdapat kekeliruan di dalam penulisan laporan ini. Semoga laporan Skripsi ini bermanfaat bagi penulis khusus-Nya dan pembaca pada umumnya.

Cilegon, 1 Desember 2023

Penulis

ABSTRAK

Nurfitriani Romadhona
Teknik Elektro

Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa

Teknologi informasi banyak digunakan oleh organisasi seperti industri, pemerintahan, dan pendidikan. Ancaman keamanan teknologi informasi merupakan salah satu permasalahan paling serius akhir-akhir ini. Sistem informasi akademik merupakan suatu sistem pengelolaan data dan kegiatan akademik, karena penggunaan *website* ini penting dan juga memiliki kerentanan yang dapat merugikan, seperti: serangan SQL injection, XSS, *Man-in-the-Middle* dan lain-lain. Oleh karena itu, perlu mengetahui kerentanan melalui metode pengujian penetrasi menggunakan *framework* ISSAF dan dengan audit berdasarkan COBIT 5. Hasil pengujian kerentanan pada Vega dan Owasp Zap memperoleh beberapa kerentanan yaitu *Sesion Cookie without HTTPOnly Flag, Session Cookie without Secure Flag, Session Cookie without Samesite Attribute, Client Cipher-suite Preference, Directory Listing, Missing Anti Click-jacking, SQL Injection, Absence of Anti CSRF tokens, X-Powered-By and Server HTTP Response Header Field, Strict-Transport-Security, Timestamp Disclosure-UNIX and X-Content-Type-Options*. Hasil pengujian COBIT 5 untuk domain APO13 dan DSS05 saat ini berada di level 3 *established process,* sedangkan yang diharapkan berada di level 5 *optimising process*. Dengan masing-masing gap sebesar 2 dan 1,57. Hasil simulasi menggunakan *tools* Sqlmap dengan menambahkan injeksi SQL ke *website* tidak berhasil karena keamanannya telah ditingkatkan.

Kata Kunci: Keamanan, Manajemen, ISSAF, COBIT 5.

ABSTRACT

Nurfitriani Romadhona
Electrical Engineering

Academic Information System Security Audit Using COBIT 5 at Sultan Ageng Tirtayasa University

Information technology is widely used by organizations such as industry, government, and education. Information technology security threats are one of the most serious problems these days. Academic information system is a system for managing data and academic activities, because the use of this website is important and also has vulnerabilities that can be detrimental, such as: SQL injection attacks, XSS, Man-in-the-Middle and others. Therefore, it is necessary to find out vulnerabilities through penetration testing methods using the ISSAF framework and with audits based on COBIT 5. The results of vulnerability testing on Vega and OwasP Zap revealed several vulnerabilities, namely Sesion Cookie without HTTPOnly Flag, Session Cookie without Secure Flag, Session Cookie without Samesite Attribute, Client Cipher-suite Preference, Directory Listing, Missing Anti Click-jacking, SQL Injection, Absence of Anti CSRF tokens, X-Powered-By and Server HTTP Response Header Field, Strict-Transport-Security, Timestamp Disclosure-UNIX and X-Content-Type-Options. The COBIT 5 test results for domains APO13 and DSS05 are currently at level 3 established process, while the expected is at level 5 optimizing process. With gaps of 2 and 1,57 respectively. The simulation results using the Sqlmap tool by adding SQL injection to the website were unsuccessful because the security has been improved.

Keyword: Security, Management, ISSAF, COBIT 5.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi merupakan bagian penting dari industri 4.0 yang dikenal dengan konsep otomatisasi melalui teknologi untuk mengurangi risiko kegagalan dan meningkatkan akurasi dan efensiensi kerja. Konsep ini diterapkan pada sektor industri, pendidikan, kesehatan dan pemerintahan [1]. Ancaman keamanan teknologi informasi merupakan salah satu permasalahan yang paling serius akhir – akhir ini. Keamanan TI adalah hal yang harus diawasi oleh semua organisasi untuk menghindari kerentanan [2]. Berdasarkan Badan Siber dan Sandi Negara (BSSN), 190 juta insiden ancaman dilakukan terhadap server web Indonesia dari Januari sampai Agustus 2020 [3].

Manajemen TI merupakan serangkaian prosedur yang memastikan implementasi TI yang tepat untuk mendukung pencapaian tujuan. Salah satu cara untuk mengetahui seberapa baik pengelolaan TI diterapkan adalah dengan mengauditnya [4]. Audit sistem informasi adalah proses terkoordinasi yang membantu, memantau, mengevaluasi cara kerja, dan memberikan perlindungan terhadap organisasi [5]. TI jelas membutuhkan suatu kerangka untuk pengolahannya. Penilaian kinerja TI dapat memanfaatkan kerangka *Control Objectives for Information and Related Technology* (COBIT) [6]. COBIT adalah pedooman manajemen TI yang mendukung administrasi, dan pengguna menggabungkan kesenjangan antara risiko dan masalah teknis [7].

Universitas Sultan Ageng Tirtayasa (UNTIRTA) merupakan perguruan tinggi negeri yang menggunakan teknologi informasi dalam proses operasionalnya. Salah satu penerapan teknologi informasi adalah Sistem Informasi Akademik (SIAKAD). *Bug* adalah kesalahan atau error yang menyebabkan suatu program tidak berfungsi dengan baik. Siakad memiliki beberapa masalah *bug* seperti SQL *injection* serta sistem jaringan yang sering gangguan ketika digunakan oleh banyak pengguna, misalnya saat pengisian

Kartu Rencana Studi (KRS), pengisian KRS perlu dilakukan berkali-kali. Untuk mengatasi permasalahan tersebut perlu adanya peningkatan keamanan dan manajemen teknologi informasi Siakad Untirta yang baik.

Potensi kerentanan termasuk *clickjacking, sql injection, XEE, Cross-site Scripting, brute force* dan lain-lain [8]. Pengujian keamanan *website* merupakan hal yang tepat dilakukan untuk memperbaiki kerentanan dan kelemahan keamanan pada *web* terkait. Salah satu metode pengujian keamanan *website* adalah penetrasi [9]. Untuk melakukan penetrasi terdapat beberapa *framework* yang digunakan, seperti *Information Systems Security Assessment Framework* (ISSAF). ISSAF adalah kerangka terstruktur mencakup beberapa tahap pengumpulan, evaluasi, dan validasi informasi tentang sistem keamanan yang telah diuji serta dianalisis secara jelas [10].

Penelitian pertama membahas mengenai evaluasi keamanan *website.* Metode yang digunakan yaitu pentest dengan memanfaatkan kerangka ISSAF. Hasil pengujian memperoleh 18 kerentanan yang ditemukan di *website* tersebut [11]. Penelitian kedua membahas evaluasi TI. Penelitian ini memanfaatkan kerangka COBIT 2019 proses BAI11. Hasilnya tingkat kemampuan yaitu level 1 (*perfomed*) sedangkan tingkat kematangan nya level 2 (*managed projects*) [12].

Penelitian ketiga membahas menganalisa keamanan *webserver*, Metode yang digunakan yaitu *penetration testing* dengan domain *information gathering, vulnerability assessment, gaining* dan *maintaining,* serta *clearing track.* Hasil pengujian memperoleh 10 kerentanan, ditemukan beberapa *port* yang terbuka dan dalam mensimulasikan ancaman, berhasil memperoleh nama pengguna dan kata sandi [13]. Penelitian keempat membahas mengaudit Siakad, penelitian ini memanfaatkan kerangka COBIT 5 proses APO12, APO13, serta DSS05. Hasil dari penelitian tingkat kapabilitas adalah APO12 yaitu level 1, APO13 level 2, dan DSS05 level 2, artinya telah melaksanakan dan mengimplementasikan proses TI hingga memperoleh tujuan [14].

Penelitian kelima membahas pengujian penetrasi aplikasi *web* menggunakan serangan injeksi SQL. Penelitian ini menggunakan metode *black-*

box dengan *framework Open Web Application Security Project* (OWASP). Hasil pengujian terhadap 10 situs dilakukan, 80% *web* yang di uji memiliki kelemahan terhadap serangan SQL injeksi [15].

Berdasarkan latar belakang, penelitian ini melakukan audit keamanan sistem informasi akademik di Untirta dengan melakukan pengujian layanan manajemen dan keamanan Siakad menggunakan COBIT 5 serta pengujian penetrasi menggunakan *framework* ISSAF. Hasil dari penelitian akan memperoleh rekomendasi dan diperlukan untuk menerapkan manajemen serta layanan keamanan yang lebih baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang diketahui rumusan masalah dalam penelitian:

1. Bagaimana keamanan layanan siakad di Untirta berdasarkan hasil *penetration testing* menggunakan kerangka kerja ISSAF?
2. Berapa hasil kapabilitas level manajemen keamanan di Untirta dengan kerangka COBIT 5?
3. Bagaimana rekomendasi untuk Siakad agar memiliki kontrol keamanan yang baik dan benar?

1.3 Tujuan Penelitian

Berikut merupakan tujuan yang akan dicapai dalam penelitian ini:

1. Mengetahui keamanan siakad di Untirta dengan *penetration testing* menggunakan kerangka kerja ISSAF.
2. Mengetahui tingkat kapabilitas level layanan manajemen keamanan menggunakan kerangka kerja COBIT 5.
3. Memberikan rekomendasi berdasarkan hasil penelitian untuk meningkatkan keamanan dan tata kelola layanan manajemen Siakad di Untirta.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Bagi peneliti, dapat dijadikan pengetahuan mengenai keamanan Siakad dengan *penetration testing* menggunakan kerangka ISSAF dan mengetahui nilai kapabilitas manajemen keamanan TI dengan COBIT 5.
2. Bagi akademisi, dapat dijadikan referensi untuk penelitian selanjutnya terkait audit keamanan dengan kerangka ISSAF dan COBIT 5.
3. Bagi Universitas, dapat dijadikan evaluasi dan acuan untuk Universitas mengenai keamanan dan manajemen TI berdasarkan *penetration testing* dengan kerangka ISSAF dan COBIT 5.

1.5 Batasan Masalah

Agar permasalahan tetap fokus dan mudah untuk dipahami, berikut merupakan beberapa batasan masalah:

1. Pengujian audit keamanan Siakad dilaksanakan di Untirta.
2. Penilaian keamanan Siakad menggunakan *penetration testing* dan kerangka ISSAF dengan 4 langkah yaitu *Information Gathering, Network Mapping, Vulnerability Assessment,* dan *penetration testing.*
3. Melakukan *penetration testing* menggunakan sistem operasi Kali Linux. *Tools* yang digunakan untuk *information gathering* yaitu Whois, Dnsrecon, Whatweb, dan Sslscan. *Network mapping* menggunakan Nmap. *Vulnerability assessment* menggunakan Vega dan Owasp Zap, *penetration testing* berupa simulasi serangan sql *injection* menggunakan Sqlmap.
4. Penilaian manajemen keamanan dengan kerangka COBIT 5 yang fokus pada 2 domain yaitu *Align, Plan, and Organise* subdomain pengelolaan keamanan dan *Deliver, Security and Support* subdomain pengelolaan layanan keamanan.
5. Hasil penelitian ini memberikan rekomendasi terhadap pengelolaan manajemen dan keamanan TI.

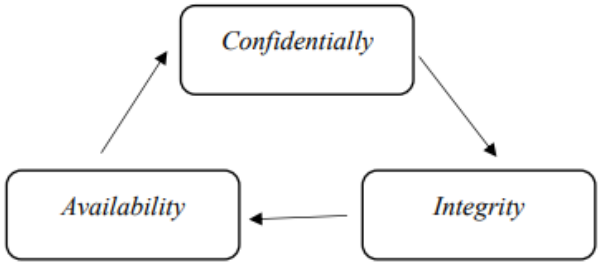
1.6 Sistematika Penulisan

Penulisan laporan skripsi, terdiri dari 5 bab. Bab I Pendahuluan memuat latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan. Bab II Landasan Teori memuat teori-teori yang relevan serta tinjauan pustaka yang memuat referensi-referensi yang digunakan. Bab III Metodologi Penelitian meliputi alur penelitian, metode dan alat yang digunakan dalam penelitian. Bab IV Hasil dan Pembahasan memuat penjelasan dan analisis yang diperoleh dari penelitian yang dilakukan. Bab V Penutup memuat kesimpulan yang dapat diambil dari penelitian dan saran untuk penelitian ini.

BAB II
TINJAUAN PUSTAKA

2.1 Keamanan Komputer

Keamanan komputer adalah proses pencegahan dan pendeteksian penipuan dalam sistem informasi, dimana informasi itu sendiri tidak memiliki arti fisik [16]. Tiga prinsip dari sumber daya komputer yaitu *Confidentiality, Integrity*, dan *Availablity* (CIA), dapat digambarkan dalam segitiga CIA seperti Gambar 2.1 [17]:



Gambar 2.1 Segitiga CIA

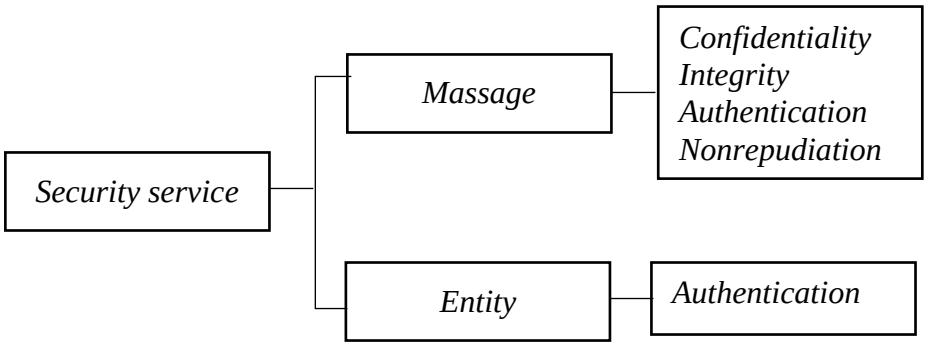
Gambar 2.1 merupakan penjelasan mengenai segitiga CIA, antara lain:

1. *Confidentiality* (Kerahasiaan), memiliki 2 pengertian yaitu kerahasiaan data dan *privacy*.
   a. Kerahasian data adalah jaminan data rahasia, seseorang tidak dapat mengubah data tersebut.
   b. Privasi menjamin bahwa individu hanya memiliki kendali atas informasi tentang diri sendiri. Informasi tersebut dapat dikumpulkan atau disimpan dengan dan kepada siapa informasi tersebut dapat dibagikan.
2. *Integrity* (Integritas), memiliki 2 konsep yaitu integritas data dan integritas sistem.
   a. Integritas data menjamin data dan program dapat berubah dengan cara yang spesifik dan resmi.

b. Integritas sistem menjamin sistem untuk melakukan fungsi yang diinginkan dalam keadaan tidak terganggu dan bebas dari pihak yang tidak berkepentingan.

3. *Availability* (Ketersediaan) adalah jaminan sistem yang berkerja dengan benar serta layanan pengguna tidak akan terganggu.

Berikut 5 layanan pada keamanan jaringan, dapat dilihat pada Gambar 2.2:



Gambar 2.2 Layanan Keamanan jaringan

Berikut Gambar 2.2 di atas merupakan penjelasan dari layanan jaringan.

1. Kerahasiaan pesan merupakan pengirim dan penerima mengharapkan kerahasiaan. Pesan yang dikirim hanya dapat diterima oleh penerima yang dituju.
2. Integritas pesan merupakan informasi harus sampai pada penerima samam dengan yang dikirim, karena semakin banyak informasi yang dipertukarkan melalui internet, maka integritas sangat penting.
3. Otentikasi pesan adalah layanan yang bukan dari bagian intgritas pesan. Dalam otentikasi pesan, penerima harus memverifikasi identitas pengirim dan penipu untuk tidak mengirimkan pesan tersebut.
4. *Nonrepudiation* pesan berarti pengirim tidak dapat menolak pengiriman pesan sebenarnya yang sudah dikirim.
5. Otentikasi Entitas berarti pengguna diautentikasi sebelum mendapat akses sumber daya sistem.

a. Keamanan Aplikasi

Keamanan aplikasi melindungi dan meningkatkan dari pencurian dan pembajakan data atau kode pada aplikasi. Berikut jenis keamanan aplikasi, yaitu:

1. Autentikasi, prosedur otentikasi menentukan pengguna yang berhak mempunyai akses.
2. Otorisasi, hanya dapat dilakukan setelah proses otentikasi berhasil. Sistem memvalidasi ruang lingkup otoritas pengguna saat menggunakan aplikasi.
3. Enkripsi, sebuah proses yang mencegah pengguna tidak bertanggung jawab membaca data sensitif pengguna aplikasi.
4. *Logging*, merekam informasi akses aplikasi.
5. Pengujian keamanan aplikasi, proses untuk memastikan bahwa semua proses keamanan berkerja dengan baik.

b. Sistem Keamanan Data

Keamanan data adalah proses melindungi informasi digital dari kerusakan, pencurian, atau akses yang tidak sah. Ini mencakupkan semua hal seperti *software*, *hardware*, alat penyimpanan, perangkat pengguna, manajemen akses, dan prosedural Universitas. Beberapa jenis keamanan data antara lain [18]:

1. Enkripsi, sebuah proses yang mencegah data pengguna aplikasi sensitif dibaca oleh pengguna yang tidak bertanggung jawab.
2. Pembersihan data, tata kelola keamanan data yang efesien untuk menghapus tanggung jawab dan potensi kesalahan data.
3. Kamuflase data, suatu gambaran enkripsi menjadikan data tidak dapat digunakan apabila disadap oleh peretas. Keaslian pesan hanya terlihat oleh orang yang mengetahui kodenya.

2.2 Serangan

Serangan keamanan dapat menyebabkan kerusakan yang signifikan, termasuk kerugian finansial, kerusakan reputasi, dan hilangnya data penting. Cara untuk megatasi serangan keamanan, Universitas harus menerapkan sistem keamanan yang ketat, melakukan peninjauan berulang, serta memberi pembelajaran

mengenai keamanan untuk memangkas dampak akibat serangan. Berikut beberapa jenis serangan *cyber*, antara lain [19]:

a. *Malware*

Malware atau *malicious software* adalah serangan komputer dengan program bawaan yang dirancang untuk mendapatkan informasi atau bahkan mendapatkan akses ke informasi korban. Berikut adalah jenis-jenis *malware,* yaitu:

1. *Ransomware* adalah serangan di mana korban dipaksa membayar sejumlah uang untuk mendapatkan akses ke informasi penting korban.
2. *Spyware* adalah perangkat lunak yang mengirimkan semua data dari komputer ke peretas yang menginstal perangkat lunak tersebut.
3. *Keylogger* memiliki prinsip yang sama dengan *spyware* tetapi hanya mengirimkan data yang dimasukkan melalui perangkat *input.*
4. *Trojan* adalah salah satu *malware* yang paling umum, karena dapat menambahkan aplikasi berbahaya ke aplikasi yang tanpa disadari telah terinfeksi oleh pengguna. Komputer yang terinfeksi kemudian dapat mengakses sebagian besar data, tergantung pada seberapa banyak akses yang diperoleh oleh *Trojan.*
5. Virus menginfeksi aplikasi atau *file* dan hanya tumbuh atau menyebar ketika aplikasi atau *file* tersebut dibuka.

b. *Phishing*

Serangan ini menggunakan pesan-pesan yang menipu kepada korban, sehingga korban tidak merasa terancam dengan bocornya informasi yang diberikan. Biasanya, serangan *phishing* dikirim melalui email atau media sosial atau bahkan pesan teks yang dikenal dengan istilah smishing dan melalui telepon yang dikenal dengan istilah *phishing*. Serangan ini dapat dikerjakan oleh pihak tidak bertanggung jawab, akibatnya korban masuk ke dalam *website,* pengguna dialihkan ke berbagai serangan kejahatan dunia maya lainnya. Kedua situs tersebut meminta informasi pribadi, otorisasi pembayaran, halaman palsu, dan lainnya. Beberapa serangan *phishing* yang terkenal adalah *spear phishing, whaling,* dan *angler phishing.*

c. *Man-in-the-Middle*

Serangan ini dilakukan pada jaringan yang tidak aman dan tidak terenkripsi. Peretas mencoba mengarahkan semua lalu lintas jaringan ke komputer atau perangkat bekas. Besarnya kerugian korban tergantung pada informasi apa yang diterima korban. Jika korban menggunakan rekening bank, ada kemungkinan nama pengguna, kata sandi dan informasi dibagikan kepada pelaku.

d. *Distributed Denial of Service* atau *Denial of Service*

Denial of Service (DOS) adalah serangan *server* yang dimaksudkan untuk menghancurkan atau menonaktifkan sistem target, sehingga komputer tidak dapat dijalankan fungsinya. Sedangkan *Distributed Denial of Service* **(**DDOS**)** merupakan serangan *denial of service* yang memanfaatkan beberapa server atau komputer untuk mengeksplotasi server target di jaringan.

Perbedaan antara DoS dan DDoS adalah jumlah perangkat yang digunakan untuk serangan pada waktu yang bersamaan. Tujuan serangan ini bukan untuk mencuri data, melainkan untuk melemahkan *server*, yang menciptakan celah untuk kemungkinan serangan *cyber* lainnya di *server*.

e. *Domain name system spoofing*

Domain name system (DNS) *spoofing* adalah serangan peretas yang mengalihkan lalu lintas *web* ke situs *web* palsu. Halaman ini terlihat identik dengan halaman yang dimaksud korban. Tetapi setiap informasi yang dimasukkan korban di situs web palsu dikirim langsung ke peretas, memberikan akses ke akun anda kepada penjahat dunia maya. Peretas juga dapat menggunakan DNS *spoffing* untuk menyabotase sistem dengan mengarahkan pengunjung ke situs *web*.

f. *Cross-site scripting*

Cross-site scripting (XSS) adalah kejahatan ancaman situs *web* untuk mengeksploitasi kerentanan dalam formulir entri situs *web*. Saat penyerang menemukan kerentanan XSS di sebuah situs *web*, penyerang mengeksploitasinya dengan memasukkan *script* yang salah satunya dirancang untuk menjebak korban

[20]. Jika korban tertangkap, situs bisa diambil alih. Serangan XSS terbagi dalam dua macam, yaitu:

1. Permanen

Serangan ini biasanya disebut *stored* XSS, yang biasanya ditemukan di halaman web tempat pelanggan dapat misalnya, mengetikkan *script* ke dalam kotak pencarian halaman.

2. Tidak secara permanen

Serangan XSS ini sering disebut sebagai XSS tercermin, dimana penyerang dapat memasukkan *script* yang dapat disimpan dalam *database website*. *Script* yang dimasukkan dikembalikan ke *server* aplikasi *web* korban, misalnya dengan menampilkan pesan kesalahan yang dapat terlihat di program klien lain.

g. *Padding oracle on downgraded legacy encryption*

Padding oracle on downgraded legacy encryption (POODLE) adalah serangan yang mengeksploitasi kerentanan dalam protokol SSL 3.0 (CVE-2014-3566). Kerentanan ini memungkinkan penyerang mendengarkan komunikasi terenkripsi SSLv3. Kerentanan tidak lagi ada di protokol *Transport Layer Security* (TLS) penerus *Secure Socket Layer* (SSL). Penyerang dapat mencuri data rahasia yang dikirimkan, misalnya kata sandi atau cookie sesi, lalu menyamar sebagai pengguna.

Kerentanan POODLE mepengaruhi *cipher suite* yang berisi *cipher blok* serta *cipher simetris*, seperti algoritma AES atau DES. *Cipher blok* mengenkripsi data dalam blok dengan panjang tetap, seperti 8 Byte atau 16 Byte [21]. Solusi yang disarankan untuk mencegah serangan POODLE adalah menonaktifkan SSL versi 3.0 pada HTTPS, atau SSL versi 3.0 masih diperlukan dapat menggunakan mekanisme `TLS_FALLBACK_SCSV`.

h. SQL *injection*

SQL *injection* merupakan teknik serangan yang mengekspoilitasi kode dengan memodifikasi *backend* SQL dengan menambahkan pernyataan, dengan mencoba memanipulasi parameter pada URL target dengan memasukan tanda petik (‘) [22]. SQL *injection* memungkinkan peretas untuk mendapatkan akses ke sistem *database*

tanpa otentikasi dan dapat menghapus atau mengubah semua data yang disimpan dalam *database*. Ketika kerentanan itu terjadi dan tidak ada cadangan *database*-nya itu sangat berbahaya. Keamanan data tersebut harus dicadangkan di penyimpanan eksternal atau *cloud*. Efek yang ditimbulkan dari SQL *injection*, yaitu:

1. SQL *injection* memungkinkan akses ke sistem tanpa memiliki akun. Hal ini berlaku baik pengguna biasa maupun administrator.
2. SQL *injection* memungkinkan seseorang dapat membobol *database*, mengubah, menghapus, atau bahkan menambahkan data ke dalamnya.
3. *Hacker* tidak hanya mengubah data tetapi juga menanamkan akun yang tidak dikenal. Oleh karena itu, jika system sudah diperbaiki dan peretas masih memiliki akun cadangan, dapat *login* tanpa harus injeksi SQL lagi.
4. Basis data itu sendiri mungkin dimatikan sehigga server web yang tidak dapat melayani pengguna dengan baik.

i. *Penetration Testing*

Pengujian penetrasi berbasis modul CEH adalah prosedur penilaian keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber risiko dan bagian pengujian keamanan informasi. Pengujian simulasi serangan dilakukan dalam bentuk skenario yang dilakukan oleh *hacker, cracker,* dan lain-lain. Tujuan untuk mengidentifikasi dan memahami serangan terhadap sistem dan kemungkinan konsekuensi dari kelemahan sistem. Metode pengujian penetrasi terbagi dalam tiga kategori:

1. *Black-box* adalah jenis pengujian penetrasi yang mirip dengan peretas sungguhan, dimana penguji mendapatkan nama dan informasi dari jaringan serta penguji harus mendapatkan sendiri informasi lainnya.
2. *White-box* merupakan jenis pengujian yang merupakan kebalikan dari pengujian *black-box*, karena informasi sudah diketahui terlebih dahulu dan infrastruktur seperti apa yang akan diuji.
3. *Grey-box* merupakan kombinasi dari data terbatas dan pengujian internal, selain itu semua program diperiksa kesalahannya. Simulasi yang digunakan pada

grey-box didasarkan pada pengujian *black-box* dan pengetahuan yang ada, sehingga dapat dianalisis secara menyeluruh.

2.3 *Information System Security Assessment Framework*

Kerangka penilaian keamanan sistem informasi (ISSAF) merupakan kerangka acuan dan tujuan penggunaannya meliputi tahapan menginformasikan, evaluasi dan melaporkan hasil pengujian sistem keamanan pada domain yang di tes dan analisis hasilnya [23]. ISSAF memiliki 3 pendekatan, yaitu:

1. *Planning and preparation* merupakan tahap awal yang terdiri dari penyiapan jaringan target dan pengumpulan informasi untuk uji penetrasi.
2. *Assessment* merupakan tahap pengujian suatu sistem informasi yang terdiri dari tahapan sebagai berikut:
    a. Pengumpulan informasi mengacu terkait sistem informasi target, seperti IP *address*, nama domain, dan lain sebagainya.
    b. Pemetaan jaringan adalah melakukan langkah untuk mencari informasi contohnya *port* yang terbuka, bentuk ancaman, dan lain-lain.
    c. Identifikasi kerentanan adalah identifikasi kelemahan sistem informasi.
    d. *Penetration testing* adalah menguji sistem keamanan target.
3. *Reporting* merupakan tahap dimana suatu laporan dibuat berdasarkan hasil yang diperoleh pada tahap sebelumnya.

Berikut merupakan *tools* yang digunakan pada metode ISSAF, yaitu:

1. Whois adalah layanan untuk mengetahui informasi seperti, domain, tanggal registrasi, tanggal expired, nama server dan lain sebagainya.
2. Dnsrecon adalah *tools* yang ditulis dengan bahasa pemrograman Python. *Tool* ini digunakan untuk recon DNS saat melakukan *information gathering.*
3. Nmap adalah aplikasi *open source* untuk mengeksplorasi keamanan jaringan. Nmap dikembangkan pada tanggal 1 September 1997 oleh Fyodor Vaskovich. Nmap melakukan deteksi jaringan menggunakan teknik seperti, *port scanning, ping scanning, ping TCP ACK, ICMP, IP, UDP*, dan *TCP SYK.*

4. Vega adalah *tools open source* untuk mendeteksi celah kerentanan keamanan *website* atau informasi sensitif yang diungkapkan secara tidak sengaja. Vega dikembangkan oleh subgraph di Montreal.
5. Owasp Zap adalah *tools vulnerability* untuk mendeteksi celah kerentanan *website*. Owasp Zap diciptakan oleh organisasi Owasp, *tools* ini dikembangkan terus sehingga siapa saja dapat mengembangkan *tools* tersebut.

2.4 Sistem Informasi Akademik

Sistem Informasi Akademik (Siakad) merupakan suatu sistem pengelolaan dan pengolahan data yang berkaitan dengan aktifitas akademik mahasiswa, dosen dan pegawai. Siakad digunakan untuk mengelola proses seperti mengatur proses kemahasiswaan, proses belajar mengajar antara dosen dan mahasiswa, keutuhan dokumen, dan kegiatan registrasi akademik pada saat melakukan kegiatan pengelolaan akademik. Siakad dirancang khusus untuk memenuhi kebutuhan layanan pendidikan yang terkomputerisasi, sehingga menaikkan kemampuan dan mutu.

Unit Pelaksanaan Teknis yang ditugaskan untuk mengelola Siakad di Untirta adalah Pusat Data dan Informasi (Pusdainfo). Pusdainfo Untirta memiliki sekitar 33 layanan teknologi informasi yang dapat mendukung layanan akademik dan administrasi. Berikut layanan TI tersebut:

a. Sistem Informasi Akademik (Siakad).
b. Sistem Pembelajaran Daring (Spada).
c. Sistem Informasi Tugas Akhir (Sista)
d. Sistem informasi Kinerja Untirta (Sikita).
e. e-administrasi.

2.5 Audit Sistem Informasi

Audit sistem informasi merupakan metode pengumpulan serta penilaian untuk menentukan apakah sistem yang berisi *asset* dapat dilindungi. Kredibilitas data dianggap konsisten dengan tujuan Universitas apabila mendapat penerapan

sumber dayanya yang baik. Berikut merupakan tujuan untuk audit sistem informasi [24]:

a. Keamanan aset, seperti *software*, *hardware* dan sumber daya dijamin dengan sistem penanganan intern untuk menghindari penyimpangan.
b. Melindungi kredibilitas data, seperti data-data yang lengkap.
c. Pengaruh teknologi, Universitas memiliki kewajiban dalam proses mengambil kesimpulan. TI dinyatakan efesien apabila dapat melengkapi kebutuhan jumlah pengguna dan sumber daya yang minimum.
d. Ekonomi adalah aspek keuangan. Dalam ilmu ekonomi, kerugian dihitung dalam satuan moneter.

2.6 *IT Governance*

Tata kelola TI adalah proses pengelolaan organisasi secara keseluruhan, seperti proses struktur organisasi digunakan sebagai perpanjangan TI dalam organisasi untuk mengembangkan tujuan dan strategi organisasi [25]. Tata kelola TI terdiri dari lima bagian, yaitu:

1. Penyelarasan strategis adalah penyelarasan perencanaan bisnis dan TI. Penyelarasan strategi ditunjukkan untuk mendefinisikan, mempertahankan dan memvalidasi posisi nilai TI dalam operasional perusahaan.
2. Penciptaan nilai merupakan proses yang dirancang agar informasi yang dikomunikasikan menghasilkan keuntungan dengan biaya yang lebih optimal.
3. Manajemen sumber daya untuk meningkatkan dan mengatur pengelolaan TI yang tepat seperti aplikasi, informasi, dan infrastruktur.
4. Manajemen risiko adalah proses manajemen tingkat risiko yang meningkatkan transparansi risiko yang terjadi dalam suatu perusahaan.
5. Pengukuran kinerja mengacu pada evaluasi dan pengukuran perilaku sistem secara berkala.

2.7 *Control Objective for Information and Related Technology*

COBIT adalah kerangka TI untuk melakukan penilaian guna mengoptimalkan dan menyeimbangkan manfaat, tingkat risiko, dan penggunaan

sumber daya. COBIT merupakan kumpulan praktik tata kelola TI dirancang untuk mendukung pelaksanaan manajemen dalam menghubungkan kesenjangan antara risiko TI.

Tahun 1996 pertama kali COBIT diluncurkan dengan versi 1 hanya focus di area pengujian. COBIT berkembang tahun 1998 menjadi versi 2 fokus di domain proses. Versi 3 berevolusi tahun 2000, yang menambahkan pedoman operasional yang fokus terhadap manajemen. Manajemen TI merupakan tambahan penting terhadap berubahnya kerangka versi COBIT 4.0/4.1 yang dirilis tahun 2005-2007. Tahun 2012, ISACA merilis versi 5 ini mencakup cakupan yang lebih luas dibandingkan versi sebelumnya dan membahas mengenai tata kelola TI, khususnya tata kelola TI di Universitas [26].

2.7.1 Prinsip COBIT 5

Prinsip dan dasar COBIT 5 dapat berguna bagi Universitas, baik komersial, nirlaba, atau publik. ISACA dan ITGI memiliki kerangka COBIT 5 yang berisi lima prinsip dalam mengimplementasikan bagian pengelolaan pada suatu Universitas. Dibawah ini merupakan lima prinsipnya:

1. Pemenuhan kebutuhan *stakeholder*
2. Meliputi bisnis dari awal sampai akhir
3. Penggunaan kerangka terpadu
4. Mengaktifkan pendekatan holostik
5. Pemisahan administrasi dan manajemen

Menurut COBIT 5, berikut merupakaan perbedaan antara tata kelola dan manajemen:

a. Tata kelola

Tata kelola menentukan bahwa kualitas, ketentuan, dan prioritas pemangku kepentingan dinilai dan diidentifikasi untuk mencapai tujuan yang diakui. Khususnya dalam organisasi yang besar dan kompleks, tugas administratif tertentu dapat ditugaskan ke tingkat yang sesuai dalam struktur organisasi.

b. Manajemen

Manajemen mendefinisikan, melaksanakan, dan mengendalikan kegiatan sebagaimana diarahkan oleh otoritas untuk mencapai tujuan. Universitas dapat menciptakan manajemen efektif yang memaksimalkan pemodalan pemangku kepentingan dan pengguna TI.

2.7.2 Model Referensi Proses

Model referensi proses merupakan penghubung antar model proses sebelumnya, pada COBIT 5 dibagi 5 domain dengan 37 proses manajemen, 5 domain tersebut adalah [27]:

1. *Evaluate, direct and monitor*

Proses EDM terkait tujuan manajemen penanggung jawab seperti pembentukan nilai, mengoptimalkan risiko dan sumber daya, memberikan hasil konsultasi serta pemantauan TI. Evaluasi, pengarahan, dan pemantauan (EDM) mencakup 5 subdomain dan metode pengelolaan utamanya:

a. Menentukan penyusunan dan perlindungan tata kelola manajemen (EDM01).
b. Menentukan manfaat keluaran (EDM02).
c. Pengelolaan risiko (EDM03).
d. Mengoptimalkan sumber daya (EDM04).
e. Menjelaskan penanggung jawab kepentingan (EDM05).

2. *Align, plan and organise*

Proses APO menyelaraskan, merencanakan, mengatur strategi dan taktik untuk identifikasi tentang bagaimana TI akan mencapai tujuan bisnisnya dengan sebaik-baiknya. Berikut ini adalah subdomain prosesnya.

a. Pengelolaan manajemen IT (APO01).
b. Pengelolaan strategi (APO02).
c. Pengelolaan arsitektur Universitas (APO03).
d. Pengelolaan inovasi (APO04).
e. Pengelolaan dokumen (APO05).
f. Pengelolaan anggaran dan manajemen biaya (APO06).

g. Pengelolaan sumber daya manusia (APO07).
h. Pengelolaan hubungan (APO08).
i. Pengelolaan perjanjian layanan (APO09).
j. Pengelolaan pemasok (APO10).
k. Manajemen mutu (APO11).
l. Pengelolaan risiko (APO12).
m. Pengelolaan keamanan (APO13).

3. *Build, acquire and implement*

Proses BAI membangun tata kelola untuk menghasilkan solusi layanan. Strategi TI dijalankan untuk mengidentifikasi, mengembangkan serta mengintegrasikan solusi TI ke dalam proses memperoleh tujuan bisnisnya. Berikut adalah subdomain dari prosesnya:

a. Pengelolaan program dan project (BAI01).
b. Pengelolaan persyaratan (BAI02).
c. Pengelolaan manajemen dan pengembangan solusi identitas (BAI03).
d. Pengelolaan ketersediaan dan kapabilitas (BAI04).
e. Pengelolaan aktivasi perubahan (BAI05).
f. Pengelolaan perubahan (BAI06).
g. Pengelolaan penerimaan dan transformasi perubahan (BAI07).
h. Pengelolaan pengetahuan (BAI08).
i. Pengelolaan asset (BAI09).
j. Pengelolaan konfigurasi (BAI10).

4. *Deliver, service and support*

Proses DSS mencakup strategi yang digunakan untuk memastikan bagaimana TI dapat memberi peran terbaik terhadap tujuan Universitas. Penerapan strategi harus diatur, dihubungkan, dan dikelola dari berbagai sudut pandang. Berikut ini adalah subdomain prosesnya:

a. Pengelolaan operasi (DSS01).
b. Pengelolaan layanan insiden dan manajemen (DSS02).
c. Pengelolaan masalah (DSS03).
d. Pengelolaan keberlanjutan (DSS04).

e. Pengelolaan layanan keamanan (DSS05).
f. Pengelolaan pengendalian proses (DSS06).

5. *Monitor, evaluate and assets*

Proses MEA memastikan kualitas seluruh proses TI dan kepatuhan terhadap persyaratan manajemen, seperti pemantauan pengendalian internal dan eksternal, peraturan manajemen, dan tata kelola. Berikut ini adalah subdomain prosesnya:

a. Memonitoring, mengevaluasi kinerja, melakukan penyesuaian (MEA01).
b. Memonitoring dan mengevaluasi sistem pengendalian internal (MEA02).
c. Memonitoring dan mengevaluasi persyaratan eksternal (MEA03).

2.7.3 *Capability Level*

Kapabilitas level adalah proses kemampuan untuk mencapai tingkat kemampuan yang ditentukan oleh atribut proses. Untuk menginterprestasikan tingkat kemampuan, dapat diasumsikan bahwa setiap subproses memiliki nilai bobot untuk tingkat kemampuan, seperti terlihat di Tabel 2.1.

Tabel 2.1 Jawaban Nilai dan Tingkat Kapabilitas

Nilai	Jawaban	Nilai Kapabilitas	Tingkat Kapabilitas
0,00-0,50	A	0,00	0 (*incomplate process*)
0,51-1,50	B	1,00	1 (*perfomed process*)
1,51-2,50	C	2,00	2 (*managed process*)
2,51-3,50	D	3,00	3 (*established process*)
3,51-4,50	E	4,00	4 (*predectable process*)
4,51-5,00	F	5,00	5 (*optimising process*)

Berdasarkan Tabel 2.1, aspek fungsional model peniliaan formatif mencakup enam tingkatan fungsional. Keenam level ini berisi indikator atribut proses, untuk mengasumsikan bobot tingkat kapabilitas.

2.7.4 Perhitungan *Capability Level*

Perhitungan untuk rekapitulasi jawaban kuesioner menggunakan perhitungan yang dirumuskan pada Persamaan (2.1).

$$C = \frac{H}{JR}\ x\ 100\% \qquad (2.1)$$

Berdasarkan Persamaan (2.1), nilai untuk rekapitulasi kuesioner dari hasil total jawaban responden dibagi dengan jumlah responden. Perhitungan nilai *capability level* menggunakan perhitungan yang dirumuskan pada Persamaan (2.2).

$$NK = \frac{(LPxNka)+(LPxNkb)+(LPxNkc)+(LPxNkd)+(LPxNke)+(LPxNkf)}{100} \quad (2.2)$$

Berdasarkan persamaan (2.2), nilai *capability* diperoleh dari hasil level presentase dikali dengan nilai kematangan proses. Analisis kesenjangan adalah teknik umum untuk mengidentifikasi dan mengelola kesenjangan yang terjadi selama perencanaan transisi antara keadaan awal dan keadaan target. Analisis kesenjangan adalah sebuah alat atau teknik yang sering digunakan dalam konteks perencanaan strategis. Hal ini melibatkan evaluasi keadaan atau tujuan yang diinginkan dibandingkan dengan keadaan saat ini dan memahami kesenjangan antara keduanya [28]. Tingkat kesenjangan menggunakan perhitungan yang dirumuskan pada Persamaan (2.3)

$$Tingkat\ kesenjangan = Kondisi\ yang\ diharapkan - Kondisi\ saat\ ini \quad (2.3)$$

Berdasarkan Persamaan (2.3), tingkat kesenjangan ditentukan dari kondisi yang diharapkan dengan kondisi saat ini. Analisis kesenjangan membantu mengidentifikasi kesenjangan yang besar dan penyebabnya.

2.7.5 Diagram *Responsible, Accountable, Consulted, and Informed*

Diagram *responsible, accountable, consulted, and informed* (RACI) merupakan matriks dari seluruh aktivitas mengambil keputusan yang dilaksanakan Universitas untuk setiap peran dalam proses [29].

1. Bertanggung jawab mendeskripsikan siapa yang akan mengerjakan pekerjaan. Artinya seseorang bertanggung jawab dalam menjalankan kegiatan operasional untuk melengkapi kebutuhan serta mencapai hasil yang diharapkan.
2. Akuntabel mendeskripsikan siapa yang berkewajiban atas keberhasilan pekerjaan. Berarti mengambil tanggung jawab penuh atas pekerjaan yang diselesaikan.
3. Konsultasi mendeskripsikan pihak yang akan memberi pendapat. Berarti yang berkewajiban atas pengumpulan data.

4. Informasi mendeskripsikan pihak yang akan memperoleh data. Mengacu pihak yang berkewajiban mendapatkan data yang sesuai, untuk memverifikasi pekerjaan yang diselesaikan.

2.8 Kajian Pustaka

Penelitian mengenai audit keamanan menggunakan *penetration testing* serta layanan manajemen menggunakan COBIT 5 telah banyak dilakukan oleh berbagai pihak. Penelitian tersebut dibuktikan oleh karya tulis yang dipublikasikan di jurnal. Berikut penelitian yang penulis gunakan sebagai referensi.

Penelitian pertama membahas mengenai evaluasi keamanan *website*. Metode yang digunakan yaitu pentest dengan memanfaatkan kerangka ISSAF. Hasil pengujian memperoleh 18 kerentanan yang ditemukan di *website* tersebut [11]. Penelitian kedua membahas evaluasi TI. Penelitian ini memanfaatkan kerangka COBIT 2019 proses BAI11. Hasilnya tingkat kemampuan yaitu level 1 (*perfomed*) sedangkan tingkat kematangan nya level 2 (*managed projects*) [12].

Penelitian ketiga membahas menganalisa keamanan *webserver*, Metode yang digunakan yaitu *penetration testing* dengan domain *information gathering, vulnerability assessment, gaining* dan *maintaining*, serta *clearing track.* Hasil pengujian memperoleh 10 kerentanan, ditemukan beberapa *port* yang terbuka dan dalam mensimulasikan ancaman, berhasil memperoleh nama pengguna dan kata sandi [13]. Penelitian keempat membahas mengaudit Siakad, penelitian ini memanfaatkan kerangka COBIT 5 proses APO12, APO13, serta DSS05. Hasil dari penelitian tingkat kapabilitas adalah APO12 yaitu level 1, APO13 level 2, dan DSS05 level 2, artinya telah melaksanakan dan mengimplementasikan proses TI hingga memperoleh tujuan [14].

Penelitian kelima membahas pengujian penetrasi aplikasi *web* menggunakan serangan injeksi SQL. Penelitian ini menggunakan metode *black-box* dengan *framework Open Web Application Security Project* (OWASP). Hasil pengujian terhadap 10 situs dilakukan, 80% *web* yang di uji memiliki kelemahan terhadap serangan SQL injeksi [15].

Penelitian selanjutnya membahas evaluasi tata kelola keamanan TI. Penelitian ini menerapkan kerangka COBIT 5 dan ISO 27002 dengan subdomain APO12, APO13, dan DSS05. Hasil dari penelitian ini menunjukkan bahwa nilai kapabilitas dari subdomain yang di uji *as is* pada level 2 (*managed process*) dengan tingkat kemampuan *to be* berada pada level 3 (*established process*) dengan hasil nilai kesenjangan yaitu 1.13, 1.10, dan 0.97 [30].

Berdasarkan penelitian tersebut, terlihat bahwa menganalisis dan mensimulasikan dengan *penetration testing* menggunakan *framework* ISSAF, dapat mengidentifikasi kerentanan dan memeriksa layanan *website* dapat disusupi atau tidak. Selain itu terlihat bahwa analisis manajemen menggunakan kerangka COBIT 5 dapat melihat tingkat kapabilitas manajeman keamanan dan kesenjangan yang diakibatkannya.

BAB III
METODOLOGI PENELITIAN

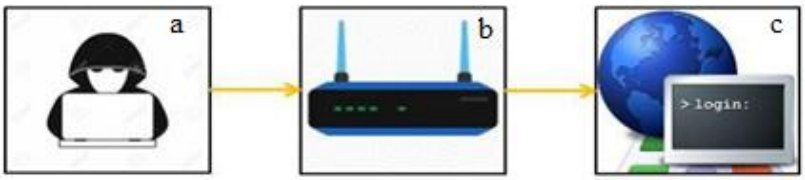
3.1 Metodologi Penelitian

Berdasarkan bab sebelumnya, tujuan penelitian ini untuk mengaudit sistem informasi akademik Universitas Sultan Ageng Tirtayasa menggunakan metode COBIT 5, agar dapat melakukan analisis penelitian perlu adanya pengambilan data secara langsung. Sebelum pengambilan data ada beberapa tahap yang harus diselesaikan sampai dengan penelitian ini selesai, berikut merupakan penjelasan alur penelitian antara lain:

1. Studi literatur yang dilakukan yaitu dengan mencari referensi-referensi seperti jurnal, buku-buku mengenai penelitian terkait dengan pokok permasalahan yang akan diteliti. Referensi-referensi yang dipergunakan kemudian dipelajari serta diimplementasikan.
2. Observasi ke lokasi penelitian untuk mengetahui proses layanan teknologi informasi.
3. Menyusun kuesioner berdasarkan COBIT 5.
4. Menyebar kuesioner COBIT 5 pada responden.
5. Menyiapkan *tools* untuk *penetration testing.*
6. Melakukan *penetration testing.*
7. Menghitung dan analisa hasil dari kuesioner berdasarkan COBIT 5 menggunakan *capability level* serta menganalisa hasil *penetration testing.*
8. Membuat rekomendasi berdasarkan hasil dari kuesioner dan hasil *penetration testing.*
9. Membuat kesimpulan dan saran untuk hasil pengujian yang di peroleh.

3.2 *Penetration Testing*

Tahap *penetration testing* dilakukan untuk menguji kerentanan keamanan layanan Siakad. Layanan tersebut dipilih karena umum digunakan untuk layanan akademik dan layanan informasi. Berikut merupakan alur *penetration testing,* ditunjukan di Gambar 3.2.



(a) Penyerang (b) Koneksi internet (c) *Web server*

Gambar 3.1 Alur *Penetration Testing*

Berdasarkan Gambar 3.1 merupakan penjelasan *penetration testing* menggunakan sistem operasi Kali linuk, koneksi internet dan beberapa *tools* serta menggunakan 4 tahapan ISSAF, antara lain:

1. *Information gathering*, pengujian ini menggunakan *tools Whois* untuk mengetahui registrasi dan sistem administrator, *DNSrecon* untuk mengetahui DNS target, *whatweb* untuk mendapatkan informasi tentang teknologi web, sslscan untuk mendapatkan informasi tentang SSL/TSL target.
2. *Network mapping* dalam pengujian ini menggunakan *tools* Nmap digunakan untuk mencari *port* yang terbuka.
3. *Vulnerability identification* dalam melakukan pengujian menggunakan *tools* Vega *vulnerability* dan owasp ZAP sebagai proses mencari celah kerentanan.
4. *Penetration testing* mensimulasikan serangan terhadap *website* yang ditargetkan. Pengujian ini akan melakukan serangan SQL *injection* atau menambahkan injeksi pada *website* target menggunakan *tools* Sqlmap.

3.3 Kuesioner COBIT 5

Sebelum penyebaran kuesioner, perlu dilakukan pemetaan RACI dengan tujuan untuk mendapati siapa saja responden yang akan menjawab kuesioner setara dengan tugasnya, sehingga perlu dilakukan pemetaan antara RACI *Chart* dengan struktur di Pusdainfo yang dipetakan, seperti terlihat pada Tabel 3.1 responden yang akan mengisi jawaban kuesioner pada penelitian ini.

Tabel 3.1 Responden Penelitian

No	Fungsional Struktur COBIT 5	Fungsional Struktur Pusdainfo
1	*Information security manager*	Kepala sub koordinator pengembangan sistem
2	*Bussiness process owners*	Kepala sub koordinator jaringan
3	*Head development*	Admin server
4	*Head IT operations*	Spv *engineering* PT. MMD

Berdasarkan Tabel 3.1 merupakan pemetaan RACI *chart* dan struktur Pusdainfo. Kuesioner yang akan digunakan dalam penelitian ini yaitu *key management practices* (KMP). Pada penelitian ini hanya difokuskan pada 2 sub-domain yaitu pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05). Hasil kuesioner tersebut didapatkan nilai kapabilitas level setiap proses. Pasca perhitungan hasil kapabilitas level akan dilakukan analisis *gap.* Analisis *gap* digunakan untuk mengetahui jarak dari nilai kapabilitas yang didapatkan dengan target yang diharapkan. Memberikan saran yang diperlukan agar pengelolaan serta pelayanan keamanan Siakad menjadi lebih baik dari sebelumnya.

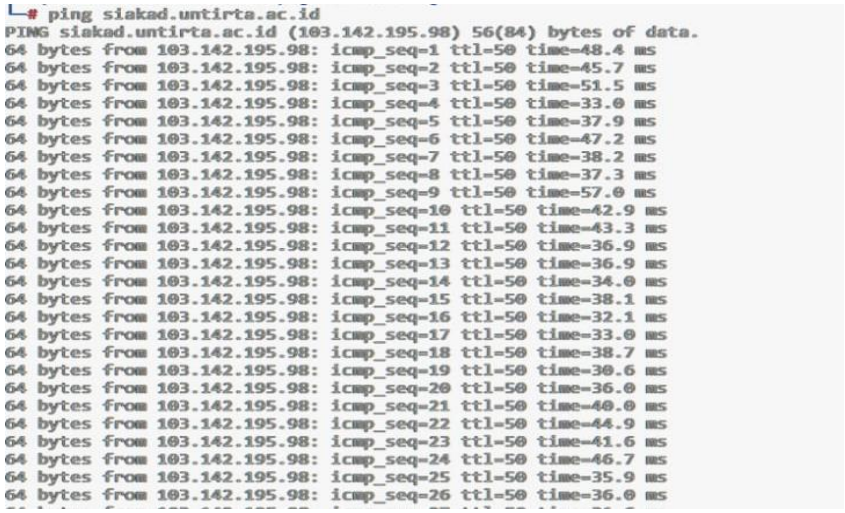
BAB IV
HASIL DAN PEMBAHASAN

4.1 Pengujian *Penetration Testing*

Pemeriksaan audit keamanan Siakad Untirta dengan cara menganalisis kerentanan yang terdapat pada *website.* Pengujian penetrasi dilakukan dengan melakukan simulasi serangan terhadap layanan Siakad menggunakan SQL *injection*. Berikut merupakan pengujian penetrasi menggunakan 4 tahap ISSAF.

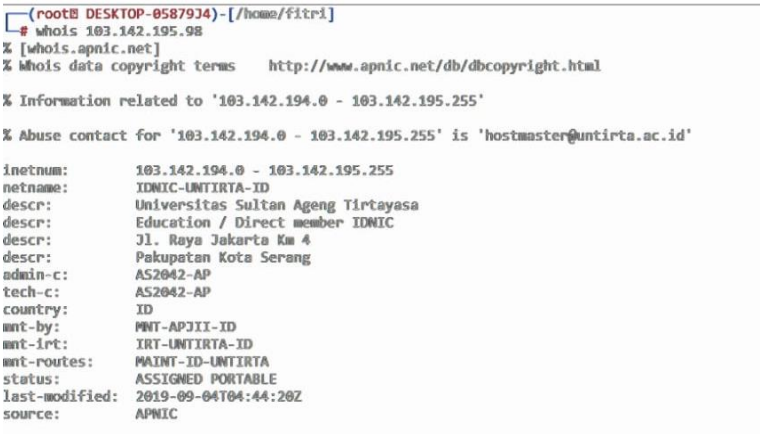
4.1.1 Analisis Pengumpulan Informasi

Langkah pengumpulan informasi digunakan untuk mencari informasi terkait *website* target, seperti alamat IP, nama domain, dan lain-lain. Pengujian untuk mendapatkan informasi tersebut menggunakan sistem operasi Kali Linux dan beberapa *tools* sepertii Whois, Dnsrecon, Sslscan dan lain-lain. Penelitian ini menggunakan target *website* yaitu https://siakad.untirta.ac.id/portal/, untuk mengetahui informasi mengenai alamat IP dari *website* tersebut dengan menggunakan perintah *ping* pada halaman Kali Linux, hasil pengujian dapat dilihat pada Gambar 4.1.



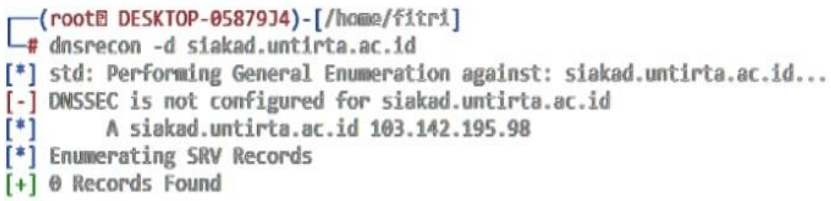
Gambar 4.1 Hasil Pengujian *IP Address* Menggunakan Kali Linux

Gambar 4.1 merupakan hasil pengujian IP *address* pada *website* https://siakad.untirta.ac.id menggunakan Kali Linux, dari pengujian didapatkan informasi bahwa *website* tersebut memiliki IP *address* `103.142.195.98`. Untuk mendapatkan informasi lebih lengkap mengenai *website* tersebut menggunakan *tools* Whois sehingga didapatkan informasi, hasil pengujian dapat dilihat di Gambar 4.2 berikut.



Gambar 4.2 Hasil Pengujian Menggunakan *Tools Whois*

Gambar 4.2 merupakan hasil pengujian menggunakan *tools* Whois, dari pengujian tersebut diperoleh informasi pribadi yang lebih lengkap dari *website* tersebut seperti nama pegawai, alamat *email*, dan nomor telepon pegawai. Dimana informasi tersebut dapat digunakan untuk melakukan serangan lain, yaitu manipulasi. Penyerang menggunakan informasi yang diperoleh untuk menyerang korban *phishing* atau teknik manipulasi lainnya. Hasil pengujian menggunakan *tools* Dnsrecon dapat dilihat pada Gambar 4.3.



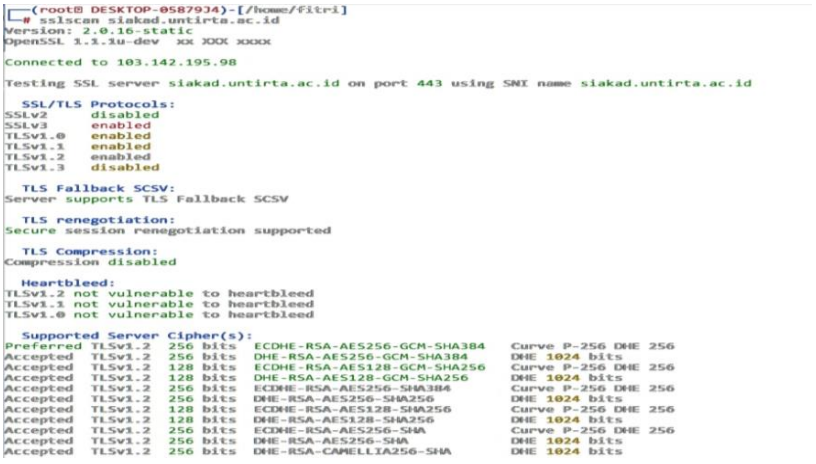
Gambar 4.3 Hasil Pengujian Mengggunakan *Tools* Dnsrecon.

Gambar 4.3 merupakan hasil pengujian menggunakan Dnsrecon, dari hasil pengujian diperoleh bahwa DNSSEC tidak dikonfigurasi. Hal ini dapat menyebabkan DNS *spoofing*, yang memungkinkan penyerang memperoleh domain atau alamat IP dan menggunakannya untuk tujuan tertentu. Sarannya untuk mengkonfigurasi DNS SEC untuk mencegah serangan DNS *spoofing*.

Selanjutnya pengujian menggunakan *tools* Whatweb untuk mendapatkan informasi mengenai teknologi seperti sistem manajemen konten (CMS), platform blog, paket analitik, pustaka JavaScript, server web, dan perangkat lain yang digunakan, berikut hasilnya dapat dilihat pada Gambar 4.4.

Gambar 4.4 Hasil Pengujian Dengan *Tools* Whatweb.

Gambar 4.4 merupakan hasil pengujian menggunakan *tools* Whatweb, didapatkan informasi bahwa Siakad menggunakan web server Nginx 1.10.3, memiliki alamat IP `103.142.195.98`, *text script* yang digunakan javascript dan memiliki halaman untuk pengalihan sisi pengguna yang membuka *website* tersebut ke https://sia.untirta.ac.id/portal/. Berikut Gambar 4.5 hasil pengujian menggunakan *tools* Sslscan.



Gambar 4.5 Hasil pengujian menggunakan *tools* SSLScan.

Berdasarkan Gambar 4.5 hasil pengujian yang diperoleh dengan *tools Sslscan*, penulis memperoleh informasi bahwa website menggunakan SSLv3, TSLv1.0, TSLv1.1, dan TSLv1.2. SSL (*Secure Sockets Layer*) dan TSL (*Transport Security Layer*) adalah protokol kriptografi yang digunakan untuk mengamankan lalu lintas antara pengguna dengan web server di internet. Selain pengujian tersebut, didapatkan informasi bahwa situs tersebut mempunyai sertifikat SSL yang berlaku hingga 11 Juni 2023.

4.1.2 Analisis Pemetaan Jaringan

Tahap selanjutnya adalah melakukan *network maping*, pada tahap ini dilakukan *port scan* untuk mengetahui *port* yang terbuka dan jenis layanan apa saja yang digunakan. Pengujian menggunakan *tools* Nmap, berikut merupakan hasil pengujiannya dapat dilihat pada Gambar 4.6.

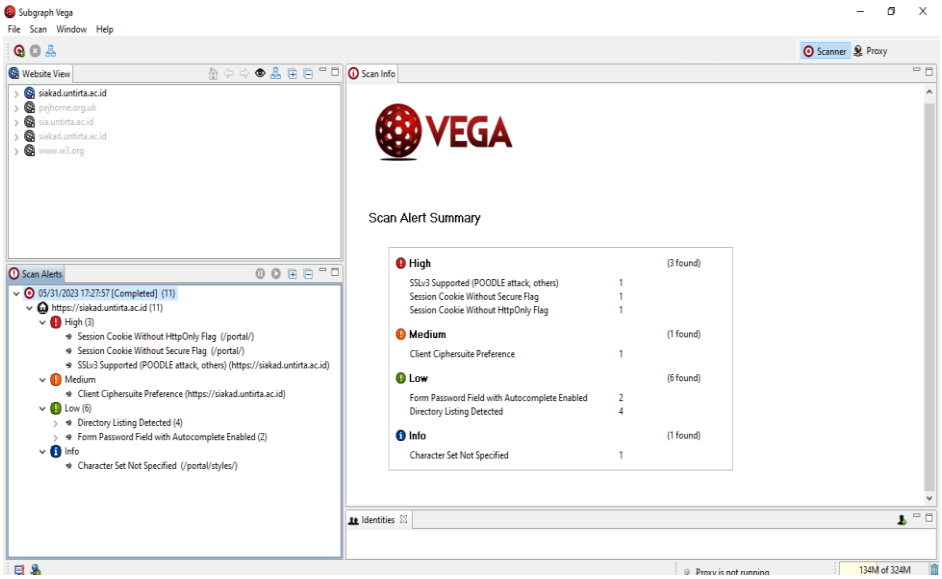
Gambar 4.6 Hasil Pengujian Menggunakan *Tools* Nmap.

Berdasarkan Gambar 4.6 hasil pengujian dengan *tools* Nmap, penulis mendapatkan informasi bahwa ada 4 *port* yang terbuka dan 2 *port* yang tersaring. *Port* 80/tcp adalah *port* yang digunakan untuk layanan HTTP (*hypertext transfer protocol*), *port* 111/tcp adalah protokol yang digunakan untuk layanan utilitas yang mengkonversi nomor program RPC (*remote procedure call*) ke alamat global. *Port* 443/tcp adalah protokol yang digunakan untuk layanan HTTPS saat mentransfer data antara klien dan *server* yang dienkripsi dan dilindungi oleh

sertifikat keamanan. *Port* 3306/tcp adalah *port* bawaan untuk protokol MySQL yang digunakan oleh klien MySQL, konektor MySQL, alat seperti *mysqldump* dan *mysqlpump*.

4.1.3 Analisis Identifikasi Kerentanan

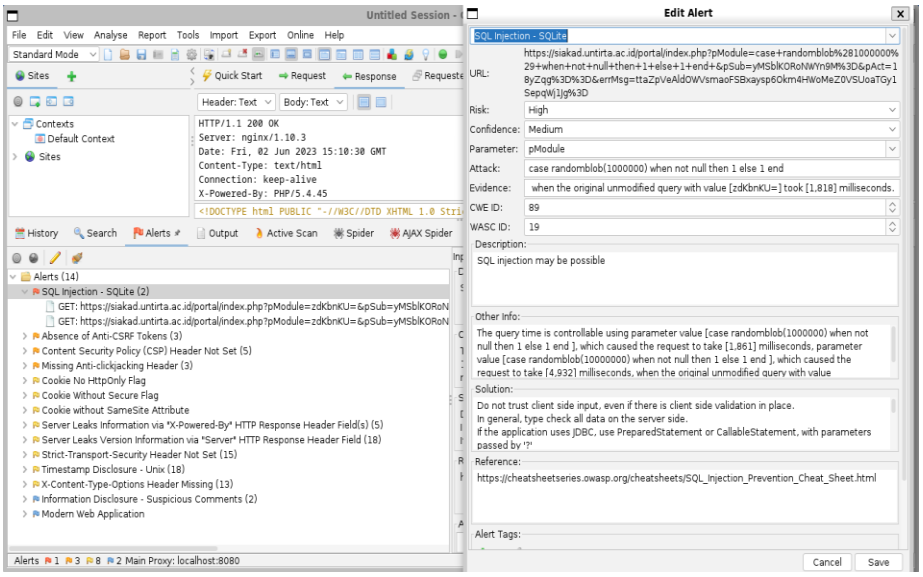
Tahap selanjutnya merupakan mengidentifikasi kerentanan, dimana pada tahap ini akan mencari kelemahan pada *website* https://siakad.untirta.ac.id. Pengujian ini *tools* yang digunakan yaitu Vega *vulnerability* dan Owasp Zap. Berikut Gambar 4.7 merupakan hasil pengujian menggunakan *tools* Vega *vulnerability.*



Gambar 4.7 Hasil Pengujian Menggunakan Vega *Vulnerability.*

Berdasarkan Gambar 4.7 hasil pengujian yang diperoleh dengan *tools Vega vulnerability* menunjukkan 3 kerentanan pada *website* dengan *level* tinggi, 1 kerentanan pada *level* sedang, 6 kerentanan pada *level* rendah, dan 1 kerentanan informasi. Dilihat dari Gambar 4.7, menunjukkan 3 kerentanan tinggi, yaitu SSLv3 *supported* (POODLE *attack, others*), *session cookie without secure flag,* dan *session cookie without httponly flag*. Dimana kerentanan SSLv3 *supported* (POODLE *attack, others*) memungkinkan penyerang melihat informasi seperti nama pengguna dan *password* melalui serangan m*an in the*

middle (MITM). Kerentanan *session cookie without secure flag* memungkinkan penyerang menangkap *cookie* dari komunikasi yang tidak terenkripsi. Kerentanan *session cookie without httponly flag* memungkinkan penyerang melakukan *sniffing* dan mengambil *cookies* pengguna yang digunakan penyerang untuk mem-*baypass login* aplikasi secara tidak sah dan memanipulasi data. Kerentanan *client ciphersuite pereference* tidak dikonfigurasi pada server dan dapat berbahaya bagi pengguna lama. Kerentanan *directory contents detected* memungkinkan konten direktori memberikan informasi yang berguna bagi penyerang seperti kode sumber atau cadangan, dapat mengakibatkan serangan *brute-force.* Selanjutnya pengujian untuk mengidentifikasi kerentanan dengan Owasp Zap. Hasil pengujian dapat dilihat pada Gambar 4.8.



Gambar 4.8 Hasil Pengujian Menggunakan *Tools* OWASP ZAP

Gambar 4.8 merupakan hasil pengujian yang di peroleh dengan *tools* Owasp Zap, menunjukkan 14 kerentanan pada *website* target. Hasil pengujian didapatkan 1 kerentanan berada pada *level* tinggi, 3 kerentanan berada pada *level* medium, 7 kerentanan berada pada *level low*, dan 2 kerentanan berada pada informasi. Berdasarkan Gambar 4.8 terlihat adanya kerentanan tinggi yaitu SQL Injection, penyerang dapat mengakses *database* sistem, hal ini harus dilakukan penanganan secepatnya. Kerentanan medium yaitu *absence of anti-csrf tokens*

pada *website* Siakad Untirta menunjukkan bahwa token keamanan tidak memberikan perlindungan, penyerang dapat melakukan serangan *cross site request forgery* (CSRF) yang dapat mendorong permintaan agar mengubah informasi seperti profil, email dan yang lainnya. Kerentanan *content security policy* (csp) *header* tidak disetel. Jika *header* CSP tidak disetel, hal ini dapat mengakibtkan XSS¸*clickjacking,* dan kebocoran lalu lintas *website,* sedangkan *header* ini disetel maka dapat mengurangi serangan XSS. Kerentanan *missing anti-clickjacking-header* dapat membuat situs web terkena serangan *clickjacking,* dimana penyerang dapat mengelabui pengguna agar mengklik sesuatu yang tidak diinginkan.

Kerentanan level rendah *cookie without samesite attribute* menjelaskan bahwa ada *cookie* yang tidak disetel pada atribut, sehingga mengirimkan sebagai permintaan lintas situs yang mengakibatkan *cookie* yang disimpan dibaca oleh orang yang tidak bertanggung jawab. Kerentanan *timestamp-disclosure*-unix menjelaskan stempel waktu server yang ditampilkan, dapat dicek terlebih dahulu kesensitifannya, karena jika sensitif penyerang dapat memanfaatkannya untuk mengumpulkan informasi serangan. Kerentanan x-*content-type-options header* menunjukkan bahwa konfigurasi x-*content-type-header* tidak dipasang ke *nosniff,* keadaan ini dapat mengakibatkan *browser* dapat memperlihatkan isi sesungguhnya yang tidak untuk ditampilkan. Kerentanan *strict-transport-security* menunjukkan bahwa *header* tidak disetel, hal ini dapat membuat *website* rentan terhadap serangan MITM, dimana halaman *login* palsu bisa menjadi pilihan.

Kerentanan *server leaks information via x-powered-by HTTP response header field(s)* bahwa server dapat mengembalikan lebih dari satu *header* HTTP *x-powered-by* dengan bidang *header* respons HTTP x-*powered*-by, yang dapat mengakibatkan penyerang mengeksploitasi di situs *website.* Kerentanan *server leaks information via server HTTP response header field* tidak dikonfigurasi, jika situs *website* membocorkan versi lengkap *server web header respons* HTTP "*server"* penyerang dapat mengeksploitasi server *web* tersebut.

4.1.4 Analisis *Penetration Test*

Langkah selanjutnya adalah penetrasi terhadap *website* siakad yang diuji untuk melihat apakah kerentanan yang ditemukan pada tahap *vulnerability identification* dapat dieksploitasi. Alat yang digunakan untuk pengujian penetrasi adalah Sqlmap, berikut Gambar 4.9 hasil penetrasi yang dilakukan.

Gambar 4.9 Hasil Uji Penetrasi Menggunakan Sqlmap

Berdasarkan Gambar 4.9 pengujian penetrasi menggunakan *tools* sqlmap mengecek apa *web* tersebut *vulnerable* terhadap SQL *injection* atau tidak. Berikut merupakan perintah dan *Uniform Resource Locator* (URL) untuk mensimulasikan serangan SQL *injection* `sqlmap --u https://siakad.untirta.ac.id/portal/index.php?id=1 --dbs`. Perintah `sqlmap --u https://siakad.untirta.ac.id/portal/index.php?id=1` untuk mengecek URL target apakah bisa diinjeksi, sedangkan perintah `--dbs` untuk mendapatkan nama *database* yang tersedia. Hasil pengujian pada *website* https://siakad.untirta.ac.id/portal/ tidak berhasil ditambahkan oleh perintah SQL karena sistem telah aman dan sudah tidak memiliki *bug* dibagian SQL-nya.

4.2 Evaluasi Manajemen Layanan Keamanan Siakad

Evaluasi manajemen layanan keamanan Siakad dilakukan untuk mengetahui sejauh mana manajemen layanan keamanan Siakad di Untirta.

Evaluasi terhadap manajemen keamanan Siakad dilakukan dengan menyebarkan kuesioner kepada beberapa staff UPT. PusdaInfo Untirta yang menangani layanan Untirta.

Key Management Practices (KMP) digunakan untuk kuesioner setiap proses yang diberikan pada responden, yaitu *align, plan, and organaise* (APO) dengan fokus pada pengelolaan keamanan (APO13) dan *delivery, service, and support* (DSS) fokus pada pengelolaan layanan keamanan (DSS05). Responden diperoleh dengan mengidentifikasi RACI *chart* yang disajikan pada struktur fungsional COBIT 5 dan stuktur fungsional UPT. PusdaInfo Untirta. Diagram RACI untuk responden kuesioner domain proses APO13 dan DSS05 tersedia pada Lampiran B.1 dan B.2.

Capability level serta *gap analysis* digunakan untung perhitungan kuesioner. Dari hasil perhitungan tersebut, didapatkan analisis *capability* serta *gap analysis* pada masing-masing sub-domain proses APO13 dan DSS05 pada UPT PusdaInfo Untirta.

4.2.1 Analisis Pengelolaan Keamanan APO13

Proses subdomain pengelolaan keamanan APO13 dilakukan evaluasi manajemen layanan Siakad pada setiap aktifitas yang ada dalam domain APO13. Pengelolaan keamanan APO13 memiliki 3 subdomain proses, yaitu mengerjakan dan merawat sistem manajemen keamanan, memastikan dan menyusun rencana pengelolaan risiko keamanan informasi, memantau serta meninjau SMKI.

1. Mengerjakan dan merawat SMKI

Proses APO13-01 merupakan memberikan pendekatan yang terstandarisasi, formal, dan berkelanjutan dan menyediakan SMKI serta proses bisnis yang selaras dengan kebutuhan keamanan dan Universitas. Proses ini membatasi dampak insiden keamanan. Hasil kuesioner subdomain APO13-01 dapat dilihat pada Tabel 4.1.

Tabel 4.1 Hasil Kuesioner APO13-01

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
1	Saat ini				25	50	25
	Diharapkan						100
2	Saat ini		25	25	50		
	Diharapkan					25	75
3	Saat ini				75	25	
	Diharapkan						100
4	Saat ini				50	25	25
	Diharapkan						100
5	Saat ini				25	25	50
	Diharapkan						100
6	Saat ini			25	50		25
	Diharapkan						100
7	Saat ini				50	25	25
	Diharapkan						100
8	Saat ini			25	50		25
	Diharapkan						100
Kondisi saat ini			3,12	9,37	46,87	18,75	21,87
Kondisi yang diharapkan						3,12	96,87

Tabel 4.1 merupakan hasil kuesioner proses APO13 pada subdomain pengelolaan keamanan APO13-01. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau *established process* yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 46,87%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau o*ptimising process* yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 96,87%. Saran untuk UPT PusdaInfo Untirta dalam proses APO13-01 adalah untuk meningkatkan SMKI terutama penyediaan dan perawatan dokumen yang menjelaskan jangkauan dari SMKI.

2. Memastikan dan menyusun rencana pengelolaan risiko keamanan

Proses APO13-02 merupakan untuk pengelolaan rencana SMKI yang mengartikan terkelola dengan strategi serta infrastruktur Universitas. Proses ini mencakup perlengkapan, rancangan, implementasi dan pengamatan metode keamanan. Berikut merupakan hasil kuesioner sub-domain APO13-02 dapat ditunjukan pada Tabel 4.2.

Tabel 4.2 Hasil Kuesioner APO13-02

Aktivitas	**Status**	**Rekapitulasi Kuesioner (%)**					
		A	**B**	**C**	**D**	**E**	**F**
1	Saat ini			50	50		
	Diharapkan						100
2	Saat ini			25	75		
	Diharapkan					25	75
3	Saat ini			50	50		
	Diharapkan						100
4	Saat ini				75	25	
	Diharapkan						100
5	Saat ini			25	75		
	Diharapkan						100
6	Saat ini			25	75		
	Diharapkan						100
7	Saat ini			25	75		
	Diharapkan						100
8	Saat ini				50	25	25
	Diharapkan					25	75
Kondisi saat ini				37.5	75	6,25	0,16
Kondisi yang diharapkan						6,25	93,75

Tabel 4.2 merupakan hasil kuesioner proses APO13-02 pada domain APO13 pengelolaan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 75%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah

93,75%. Saran untuk UPT PusdaInfo Untirta dalam proses APO13-02 adalah untuk meningkatkan pengawasan keamanan informasi terhadap insiden keamanan dapat dicegah secara cepat.

3. Memeriksa dan memantau SMKI

Proses APO13-03 merupakan untuk pengelolaan berulang, hubungan dan maanfaat kebutuhan menggabungkan pemeriksaan data kinerja dari SMKI. Prosedur ini mencakup pengumpulan data serta peningkatan efektivitas sistem manajemen keamanan informasi. Berikut merupakan hasil kuesioner sub-domain APO13-03 ditunjukkan pada Tabel 4.3.

Tabel 4.3 Hasil Kuesioner APO13-03

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
1	Saat ini			25	50	25	
	Diharapkan						100
2	Saat ini				50	25	25
	Diharapkan						100
3	Saat ini			25	50	25	
	Diharapkan						100
4	Saat ini			25	50	25	
	Diharapkan						100
5	Saat ini				50	25	25
	Diharapkan						100
6	Saat ini			25	75		
	Diharapkan					25	75
Kondisi saat ini				16,67	54,17	20,83	8,33
Kondisi yang diharapkan						4,16	95,83

Tabel 4.3 merupakan hasil kuesioner proses APO13-03 pada domain APO13 pengelolaan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 54,17%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan

untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 95,83%. Saran untuk UPT PusdaInfo Untirta dalam proses APO13-03 adalah meningkatkan efektifitas dari SMKI.

4.2.2 Analisis Pengelolaan Layanan Keamanan DSS05

Proses domain DSS05 pengelolaan layanan keamanan dilakukan evaluasi manajemen layanan Siakad di setiap aktifitas yang ada dalam domain DSS05. DSS05 pengelolaan layanan keamanan memiliki 7 sub-domain proses, yaitu melindungi dari serangan, pengelolaan konektivitas jaringan, pengelolaan perangkat, pengelolaan identitas dan fasilitas jangka panjang, pengelolaan fasilitas pada perangkat TI, pengelolaan dokumen sensitif dan instrumen keluaran, serta mengawasi prasarana untuk peristiwa terkait keamanan. Berikut merupakan hasil dari subdomain proses yang ada di DSS05.

1. Melindungi dari serangan

Proses DSS05 merupakan pengelolaan dan penerapkan melindungi sistem TI dari serangan. Proses ini mencakup untuk menyelidiki, mencegah, dan memperbaiki TI dari insiden keamanan seperti, bug, worm, spyware dan lain-lain. Berikut merupakan hasil kuesioner dari subdomain DSS05-01 yang dapat ditunjukkan pada Tabel 4.4.

Tabel 4.4 Hasil Kuesioner DSS05-01

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
1	Saat ini			25	50		25
	Diharapkan						100
2	Saat ini				50		50
	Diharapkan						100
3	Saat ini			25	50	25	
	Diharapkan						100
4	Saat ini			50	25		25
	Diharapkan						100
5	Saat ini				100		
	Diharapkan					25	75
6	Saat ini				25	50	25

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
	Diharapkan						100
7	Saat ini			25	25	25	25
	Diharapkan						100
8	Saat ini			25	50		25
	Diharapkan						100
Kondisi saat ini				18,75	46,87	12,5	21,87
Kondisi yang diharapkan						3,12	96,88

Tabel 4.4 merupakan hasil kuesioner proses DSS05-01 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 46,87%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 96,88%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-01 adalah untuk menjaga layanan TI khususnya Siakad dari insiden keamanan.

2. Pengelolaan konektivitas jaringan keamanan

Subdomain DSS05-02 merupakan proses pengelolaan keamanan konektivitas jaringan. Proses ini mencakup tindakan serta proses administratif mengenai penjagaan informasi seluruh hubungan. Hasil kuesioner dari sub-domain DSS05-02 dapat dilihat pada Tabel 4.5.

Tabel 4.5 Hasil Kuesioner DSS05-02

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
1	Saat ini				25	25	50
	Diharapkan						100
2	Saat ini			25	25	25	25
	Diharapkan						100
3	Saat ini				25		75
	Diharapkan						100
4	Saat ini				25	25	50

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
	Diharapkan						100
5	Saat ini			25	50		25
	Diharapkan						100
6	Saat ini				25	25	50
	Diharapkan						100
7	Saat ini				25	25	50
	Diharapkan						100
8	Saat ini				25	50	25
	Diharapkan						100
9	Saat ini				25	50	25
	Diharapkan						100
Kondisi saat ini				5,55	27,8	25	41,68
Kondisi yang diharapkan							100

Tabel 4.5 merupakan hasil kuesioner proses DSS05-02 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu f, dengan ditentukan pada level kapabilitas berada pada tingkat 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 41,68%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 100%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-02 adalah meningkatkan pencegahan masalah terhadap konektivitas jaringan Untirta.

3. Pengelolaan perangkat

Subdomain pengelolaan perangkat merupakan proses mengelola perangkat, seperti laptop, server dan perangkat lainnya. Proses ini proses menentukan teknologi seperti komputer, desktop, dan lain-lain, dilindungi oleh kualifikasi keamanan untuk memproses, menyimpan, serta mengirimkan data. Hasil kuesioner dari sub-domain DSS05-03 dapat ditunjukan pada Tabel 4.6.

Tabel 4.6 Hasil Kuesioner DSS05-03

Proses	Kondisi	Rekapitulasi Kuesioner (%)					
		A	B	C	D	E	F
1	Saat ini				25	25	50
	Diharapkan						100
2	Saat ini				25	25	50
	Diharapkan						100
3	Saat ini			25	50		25
	Diharapkan						100
4	Saat ini			25	50		50
	Diharapkan						100
5	Saat ini			25	75		
	Diharapkan						100
6	Saat ini			50	25		25
	Diharapkan						100
7	Saat ini				50	25	25
	Diharapkan						100
8	Saat ini				50		50
	Diharapkan						100
9	Saat ini				50	25	25
	Diharapkan						100
Kondisi saat ini				8,33	44,44	13,9	33,33
Kondisi yang diharapkan							100

Tabel 4.6 merupakan hasil kuesioner proses DSS05-02 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 44,44%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 100%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-03 adalah meningkatkan standar keamanan perlindungan akses perangakat layanan teknologi informasi.

4. Pengelolaan identitas dan fasilitas jangka panjang

Subdomain DSS05-04 merupakan proses mengelola akses informasi pengguna dari insiden yang tidak terduga. Proses ini mencakup aplikasi, infrastruktur, sistem operasi, dan *maintenance.* Hasil kuesioner dari subdomain DSS05-04 dapat ditunjukkan pada Tabel 4.7.

Tabel 4.7 Hasil Kuesioner DSS05-04

Proses	**Kondisi**	**Rekapitulasi Kuesioner (%)**					
		A	**B**	**C**	**D**	**E**	**F**
1	Saat ini			50	25		25
	Diharapkan						100
2	Saat ini			25	25		50
	Diharapkan						100
3	Saat ini			25	50	25	
	Diharapkan						100
4	Saat ini			25	50		25
	Diharapkan						100
5	Saat ini			25	25		50
	Diharapkan						100
6	Saat ini			50	25		25
	Diharapkan						100
7	Saat ini			50	25	25	
	Diharapkan						100
Kondisi saat ini				35,71	32,14	7,14	25
Kondisi yang diharapkan							100

Tabel 4.7 merupakan hasil kuesioner proses DSS05-04 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu c, dengan ditentukan pada level kapabilitas berada pada tingkat 2 atau yang artinya proses keamanan terkelola dilaksanakan manajemen prosesnya dengan distribusi presentasenya adalah 35,71%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 100%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-04 adalah meningkatkan pengelolaan hak akses pengguna.

5. Pengelolaan fasilitas pada perangkat TI

Subdomain DSS05-05 merupakan untuk melakukan implementasi proses untuk memberi, membatasi, serta mencabut hak pengguna. Proses ini mencakup dokumentasi, identifikasi, dan pemantauan titik akses dalam fasilitas TI. Hasil kuesioner dari subdomain DSS05-05 dapat ditunjukkan pada Tabel 4.8.

Tabel 4.8 Hasil Kuesioner DSS05-05

Proses	**Kondisi**	**Rekapitulasi Kuesioner (%)**					
		A	**B**	**C**	**D**	**E**	**F**
1	Saat ini			25	50		25
	Diharapkan						100
2	Saat ini				75		25
	Diharapkan						100
3	Saat ini				50	25	25
	Diharapkan						100
4	Saat ini				75		25
	Diharapkan						100
5	Saat ini				75		25
	Diharapkan						100
Kondisi saat ini				5	65	10	20
Kondisi yang diharapkan							100

Tabel 4.8 merupakan hasil kuesioner proses DSS05-05 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 65%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 100%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-05 adalah meningkatkan proses pemberian akses terhadap fasilitas layanan teknologi informasi Untirta.

6. Pengelolaan data kerentanan dan instrumen keluaran.

Subdomain DSS05-6 merupakan proses mengolah data kerentanan dan instrument keluaran dari insiden yang tidak terduga. Proses ini menyediakan keamanan fisik, aktivitas pelaporan, dan pencatatan administrasi peralatan teknologi misalnya, surat, atau kode keamanan. Hasil kuesioner dari subdomain DSS05-06 dapat ditunjukkan pada Tabel 4.9.

Tabel 4.9 Hasil Kuesioner DSS05-06

Status	**Kondisi**	**Rekapitulasi Kuesioner (%)**					
		A	**B**	**C**	**D**	**E**	**F**
1	Saat ini				50		50
	Diharapkan						100
2	Saat ini			25	50		25
	Diharapkan						100
3	Saat ini			25	50	25	
	Diharapkan						100
4	Saat ini				75		25
	Diharapkan						100
5	Saat ini				50	25	25
	Diharapkan						100
Kondisi saat ini				10	55	10	25
Kondisi yang diharapkan							100

Tabel 4.9 merupakan hasil kuesioner proses DSS05-06 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu d, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan dengan distribusi presentasenya adalah 55%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 100%. Saran untuk UPT PusdaInfo Untirta dalam proses DSS05-06 adalah meningkatkan pengelolaan akses dokumen sensitif terutama dalam penyimpanan setiap dokumen yang ada pada layanan teknologi Untirta.

7. Mengawasi prasarana untuk peristiwa terkait keamanan

Subdomain DSS05-07 merupakan proses dalam mendeteksi insiden, memantau prasarana, mencegah hak aspek tidak valid serta menentukan seluruh kejadian terpadu ke dalam pemantauan inti dan proses manajemen. Proses ini mencakup insiden kerentanan. Hasil kuesioner sub-domain DSS05-07 dapat ditunjukkan pada Tabel 4.10.

Tabel 4.10 Hasil Kuesioner DSS05-07

Proses	**Kondisi**	**Rekapitulasi Kuesioner (%)**					
		A	**B**	**C**	**D**	**E**	**F**
1	Saat ini			50	25	25	
	Diharapkan					25	75
2	Saat ini			50	25	25	
	Diharapkan					25	75
3	Saat ini			50	50		
	Diharapkan					25	75
4	Saat ini			25	25		50
	Diharapkan						100
5	Saat ini			50	50		
	Diharapkan						100
6	Saat ini			25	25		50
	Diharapkan						100
Kondisi saat ini				41,66	33,34	8,34	16,66
Kondisi yang diharapkan						12,5	87,5

Tabel 4.10 merupakan hasil kuesioner proses DSS05-07 pada domain DSS05 pengelolaan layanan keamanan. Hasil kuesioner menunjukkan bahwa responden menjawab kondisi saat ini yaitu c, dengan ditentukan pada level kapabilitas berada pada tingkat 2 atau yang artinya proses keamanan terkelola dilaksanakan manajemen prosesnya dengan distribusi presentasenya adalah 41,66%. Sedangkan responden menjawab kondisi yang diharapkan yaitu f, dengan ditentukan di tingkat kapabilitas 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas dengan distribusi presentasenya adalah 87,5%. Saran untuk UPT PusdaInfo Untirta pada proses DSS05-07 adalah meningkatkan penanganan insiden keamanan dalam mengidentifikasi insiden yang terjadi pada layanan Untirta.

4.2.3 Analisis Hasil Perhitungan Keseluruhan *Capability Level*

Berdasarkan perhitungan, nilai kapabilitas setiap proses akan ditentukan dengan membulatkan angka yang diperoleh dari perhitungan terdahulu. Contohnya, jika nilai kemampuan yang dihasilkan sebesar 2,15 akan masuk ke *level 2* pada model *capabilitas* dengan mempunyai nilai kesenjangan 0,15 guna memperoleh level 3. Tabel 4.11 merupakan hasil dariperhitungan nilai dan tingkat kapabilitas APO13.

Tabel 4.11 Hasil Perhitungan Nilai dan Tingkat Kemampuan APO13

Proses	Nilai Kemampuan		Tingkat Kemampuan	
	Saat ini	Diharapkan	Saat ini	Diharapkan
APO13.01	3,47	4,94	3	5
APO13.02	3,26	4,94	3	5
APO13.03	3,21	4,96	3	5
Rata – rata	3,26	4,95	3	5

Berdasarkan Tabel 4.11, nilai kemampuan kondisi saat ini proses pengelolaan keamanan pada UPT PusdaInfo Untirta yaitu 3,26 dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan. Level ini menunjukkan proses sedang berjalan dan perlu dipastikan pelaksanaannya mendukung pencapaian tujuan di UPT PudaInfo Untirta. Sistem yang bermasalah akan diperbaiki untuk memberikan pelayanan yang lebih baik apabila pengguna memakai dalam batas yang diperlukan untuk memperoleh misi yang diharapkan. Sedangkan nilai kemampuan menjawab kondisi yang diharapkan yaitu 4,95 dengan ditentukan di tingkat 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas. Level ini menyatakan bahwa aktifitas tersebut terus dioptimalkan dan dikembangkan secara berkepanjangan untuk mencapai misi Universitas di masa depan. Berikut merupakan hasil perhitungan nilai dan tingkat kemampuan DSS05 dapat ditunjukkan pada Tabel 4.12.

Tabel 4.12 Hasil Perhitungan Nilai dan Tingkat Kemampuan DSS05

Proses	Nilai Kemampuan		Tingkat Kemampuan	
	Saat ini	Diharapkan	Saat ini	Diharapkan
DSS05.01	3,37	4,97	3	5
DSS05.02	4,03	5	4	5
DSS05.03	3,72	5	4	5
DSS05.04	3,21	5	3	5
DSS05.05	3,6	5	4	5
DSS05.06	3,5	5	3	5
DSS05.07	3	4,87	3	5
Rata – rata	3	5	3,43	5

Berdasarkan Tabel 4.12 nilai kapabilitas kondisi saat ini pada proses proses keamanan layanan di UPT PusdaInfo Untirta adalah 3, dengan ditentukan pada level kapabilitas berada pada tingkat 3 atau yang artinya keamanan telah ditetapkan untuk mencapai hasil yang diharapkan. Level ini menunjukkan proses sedang berjalan dan perlu dipastikan pelaksanaannya mendukung pencapaian tujuan di UPT PudaInfo Untirta. Sistem yang bermasalah akan diperbaiki untuk memberikan pelayanan yang lebih baik apabila pengguna memakai dalam batas yang diperlukan untuk memperoleh misi yang diharapkan. Sedangkan nilai kemampuan menjawab kondisi yang diharapkan yaitu 5, dengan ditentukan di tingkat 5 atau yang artinya keamanan terus ditingkatkan untuk melengkapi tujuan Universitas. Level ini menyatakan bahwa aktifitas tersebut terus dioptimalkan dan dikembangkan secara berkepanjangan untuk mencapai misi Universitas di masa depan.

4.2.4 Analisis Kesenjangan

Hasil kuesioner dan perhitungan yang diperoleh melalui tingkat kemampuan saat ini ternyata masih terdapat gap dari tingkat kemampuan yang diharapkan yang berada pada level 5. Gap antara tingkat kemampuan kondisi saat ini dengan tingkat kemampuan yang diharapkan pada domain pengelolaan keamanan APO13 dan pengelolaan layanan keamanan DSS05, dapat dilihat melalui Tabel 4.13 berikut:

Tabel 4.13 Hasil Analisis Kesenjangan

Proses	Saat ini	Diharapkan	Kesenjangan = (saat ini-diharapkan)
APO13	3	5	5-3 = 2
DSS05	3,43	5	5-3,43 = 1,57

Berdasarkan Tabel 4.13, hasil dari analisis kesenjangan nilai kemampuan level kondisi saat ini dan kondisi yang diharapkan, APO13 memiliki kesenjangan 2, sedangkan DSS05 memiliki kesenjangan 1,57. Berdasarkan hasil tersebut dapat dijadikan acuan untuk meningkatkan sistem keamanan teknologi informasi untuk mencapai tingkat keamanan kinerja yang diharapkan.

4.3 Rekomendasi

Menganalisis pengelolaan layanan informasi dan keamanan pada UPT PusdaInfo Untirta, analisis tersebut digunakan untuk memberikan rekomendasi perbaikan layanan TI.

1. Rekomendasi Keamanan dari Celah Kerentanan

Rekomendasi untuk keamanan layanan Siakad adalah memperbaiki layanan dari kerentanan yang ada pada layanan. Rekomendasi untuk keamanan layanan Siakad Untirta dijelaskan pada Lampiran C.1.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran C.1, sebagaian besar yang dilakukan adalah meningkatkan keamanan layanan Siakad dan mengupgrade aplikasi yang digunakan dalam Siakad seperti SSL atau TSL. Selain itu, mengubah kueri dan menambahkan atribut yang diperlukan untuk beberapa aplikasi.

2. Rekomendasi Kuesioner

Rekomendasi untuk layanan manejemen keamanan Siakad adalah meningkatkan pengelolaan manajemen proses serta aktivitas pada pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05). Rekomendasi terkait layanan manejemen keamanan Siakad Untirta dijelaskan pada Lampiran C-2.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran C-2, sebagian besar perlu memaksimalkan peningkatkan pengelolaan setiap proses yang ada di pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05). Sementara itu, perlu adanya evaluasi peningkatan kebijakan keamanan dan pelatihan mengenai keamanan dari serangan pada layanan Siakad agar civitas Untirta dapat memanfaatkannya dengan baik.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan pada bab sebelumnya mengenai Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 pada Universitas Sultan Ageng Tirtayasa, hal ini dapat diberikan kesimpulan sebagai berikut:

1. Hasil identifikasi kerentanan menggunakan *tools* Vega dan Owasp Zap menunjukkan kerentanan yang berbeda. Vega memiliki 11 kerentanan sedangkan pada Owasp ZAP memiliki 14 kerentanan.
2. Hasil dari penelitian ini menujukkan level kemampuan pada proses pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05) di UPT PusdaInfo kondisi saat ini pada level 3 dan tingkat kemampuan yang diharapkan pada level 5 dengan masing–masing nilai kesenjangan APO13 2 dan DSS05 1,57.
3. Hasil rekomendasi dari metode ISSAF adalah mengkonfigurasi DNS SEC agar tidak dapat mengakibatkan serangan DNS *spoofing*, men*disable* SSLv3 untuk mencegah terjadinya serangan POODLE dan Man-in-the-Middle.

5.2 Saran

Penelitian ini masih terdapat kekurangan yang dapat dijadikan sebagai pengembangan penelitian berikutnya:

1. Dapat menggunakan *framework* penetrasi test lain seperti *Penetration Testing Execution Standard* (PTES) dan *framework* audit lainnya seperti ISO dan ITIL untuk memperoleh hasil uji yang lebih baik.
2. Melakukan perbaikan kerentanan sistem yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab sebagai kelemahan mengenai Siakad.
3. Pusat Data dan Informasi dapat memikirkan untuk menerapkan saran dari rekomendasi yang telah diajukan.

DAFTAR PUSTAKA

[1] Novianto, F., dan M. U. Siregar, "Evaluation of E-Government Using COBIT 5 Framework (Case Study of Sistem Database Pemasyarakatan Implementation in Ministry of Law and Human Rights in The Special Region of Yogyakarta)," *IJID: International Journal of Information for Development*, vol. 8, no. 2, pp. 74-83, 2019.

[2] Yunus, M., "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinsasi Security Tools Project Berdasarkan Owasp Versi 4," *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, 2019.

[3] Budi, E., D. Wira, dan A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia* , vol. 3, pp. 223-234, 2021.

[4] Tangka, G. M. W., A. T. Liem, dan J. Y. Mambu, "Information Technology Governance Audit Using The COBIT 5 Framework at XYZ University," *Proceedings on 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020.

[5] Nugroho, H., "A Review on Information System Audit Using COBIT Framework," *International Journal of Applied Information Technology*, vol. 3, no. 2, 2019.

[6] Riantini, F. I., dan D. I. Mulyana, "Implementasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Direktorat Jendral Bea dan Cukai," *Journal Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika*, vol. 12, no. 1, 2019.

[7] Handoyo, E., R. Umar, and I. Riadi, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Intetgration," *Scientific Journal of Informatics*, vol. 6, no. 2, 2019.

[8] Andriyani, S., M. F. Sidiq, dan B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Metode Penetration Testing Dan Framework Issaf Pada

Website SMK Al-Kautsar," *LEDGER: Journal Informatic and Information Technology,* vol. 2, no. 1, 2023.

[9] Wiradarma, A. A. B. A., dan G. M. A. Sasmita, "IT Risk Management Based on ISO 31000 and OWASP Framework Using OSINT at The Information Gathering Stage (Case Study: X Company)," *International Journal Computer Network and Information Security,* vol. 12, pp. 17-29, 2019.

[10] Rusdan, M., D. T. H. .Manurung dan F. K. Genta, "Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)," *Test Engineering & Management,* vol. 83, pp. 15714 - 15719, 2020.

[11] Sanjaya, I. G. A. S., G. M. A. Sasmita, dan D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati,* vol. 8, no. 2, 2020.

[12] Sipayung, A. B., R. Yunis, dan Elly, "Evaluation of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI11 Domain," *International Journal of Research and Applied Technology,* vol. 2, no. 2, pp. 128-143, 2022.

[13] Fahri, F., A. Fadil, dan I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Testing," *Jurnal Informatika,* vol. 8, no. 2, 2021.

[14] Megasyah, Y., dan A. A. Arifnur., "Academic Information System Security Audits Using COBIT 5 Framework Domains APO12, APO13 AND DSS05," *Journal of Applied Engineering and Technological Science (JAETS),* vol. 1, p. 2, 2020.

[15] Alanda, A., D. Satria, M. I. Ardhana, A. A. Dahlan, dan H. A. Mooduto "Web Application Penetration Testing Using SQL Injection Attack,"

JOIV: International Journal on Informatic Visualization, vol. 5, no. 3, pp. 320-326, 2021.

[16] Simmons, G. J., "Contemporary cryptology: The science of information integrity," New York: IEEE press, 1994.

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

[18] Simarmata, J., D. Sasongko, J. I. Sihotang, dan Yuswardi, "Sistem Keamanan Data," Yayasan Kita Menulis, 2022.

[19] Ujung, A. M., dan M. I. P. Nasution, "Pentingnya Sistem Keamanan Database untuk Melindungi Data Pribadi," *JISKA: Jurnal Sistem Informasi Dan Informatika*, vol. 1, no. 2, pp. 44-47, 2023.

[20] Fogie, S., J. Grossman, R. Hansen, A. Rager, dan P. D. Petkov, "XSS Attacks: Cross-site Scripting Exploits and Defense," Syngress, 2007.

[21] Anonim, "What is the Poodle attack?," Acunetix by invicti, 1 June 2020. [Online]. Available: https://www.acunetix.com/blog/web-security-zone/what-is-poodle-attack/. [Accessed 20 December 2022].

[22] Clarke, J., "SQL Injection Attacks and Defense Second Edition," United State of America: Elsevier, 2009.

[23] Prasetyo, S. E., dan N. Hasannah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *Jurnal Ilmiah Informatika (JIF)*, vol. 09, no. 02, 2021.

[24] Weber, R., "Information Systems Control And Audit," London: Upper Saddle River Prentice-Hall, 1999.

[25] Anonim, "Enterprise Value: Governance of IT Investments : Getting Started with Value Management," Rolling Meadows, IL 60008 USA: ISACA, 2008.

[26] Anonim, "COBIT 5 Enabling Process," Rolling Meadows, IL 60008 USA: ISACA, 2012.

[27] Anonim "COBIT 5 Process Assesment Model (PAM) : Using COBIT 5," Rolling Meadows, IL 60008 USA: ISACA, 2012.

[28] 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.

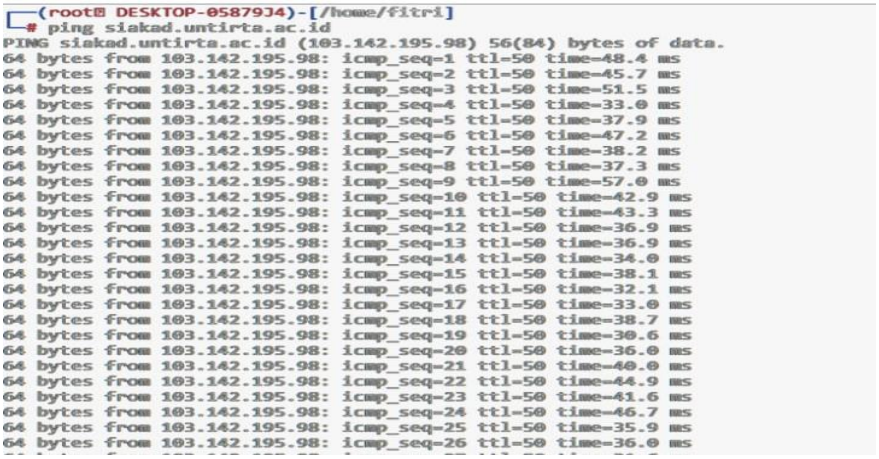
[29] Anonim, "Self-Assessment Guide : Using COBIT 5," Rolling Meadows, IL 60008 USA: ISACA, 2013.

[30] Wibowo, E. Y. A., "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 dan ISO 27002 (Studi Kasus: Pusat Jaringan Komunikasi Badan Meteorologi Klimatologi dan Geofisika)," Jakarta: Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta , 2019.

LAMPIRAN A

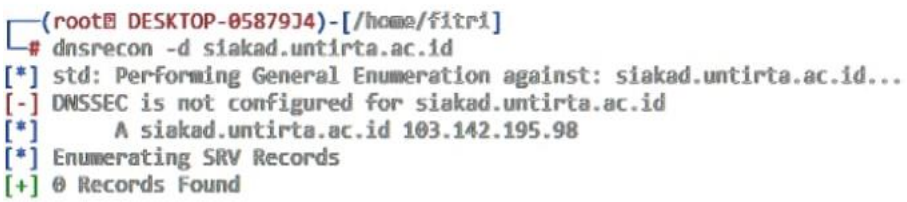
PENETRATION TESTING

Lampiran A-1 Hasil Pengujian untuk mengetahui Alamat IP di Kali Linux



Lampiran A-2 Hasil Pengujian Menggunakan *Tools* whois

Lampiran A-3 Hasil Pengujian Menggunakan *Tools DNSrecon*



Lampiran A-4 Hasil Pengujian Menggunakan *Tools* whatweb

```
┌──(root㉿ DESKTOP-0587QJ4)-[/home/fitri]
└─# whatweb siakad.untirta.ac.id
http://siakad.untirta.ac.id [200 OK] HTML5, HTTPServer[nginx/1.10.3], IP[103.142.195.98], Meta-Refresh-
Redirect[http://sia.untirta.ac.id/portal/], Script[text/javascript], Title[Page Redirection], nginx[1.1
0.3]
ERROR Opening: http://sia.untirta.ac.id/portal/ - no address for sia.untirta.ac.id
```

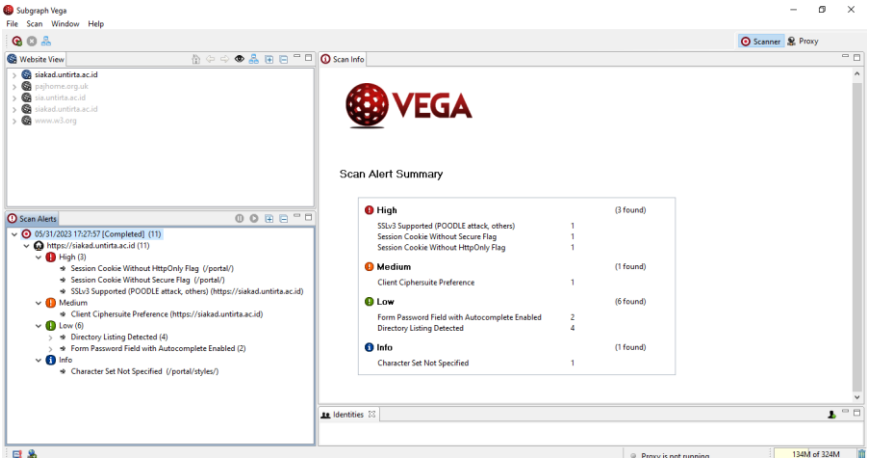
Lampiran A-5 Hasil Pengujian Menggunakan *Tools* sslscan

```
root@DESKTOP-0587QJ4: /home/fitri
┌──(root㉿ DESKTOP-0587QJ4)-[/home/fitri]
└─# sslscan siakad.untirta.ac.id
Version: 2.0.16-static
OpenSSL 1.1.1u-dev  xx XXX xxxx

Connected to 103.142.195.98

Testing SSL server siakad.untirta.ac.id on port 443 using SNI name siakad.untirta.ac.id

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     enabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384    Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256    Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256        DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256        DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA           DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA      DHE 1024 bits
```

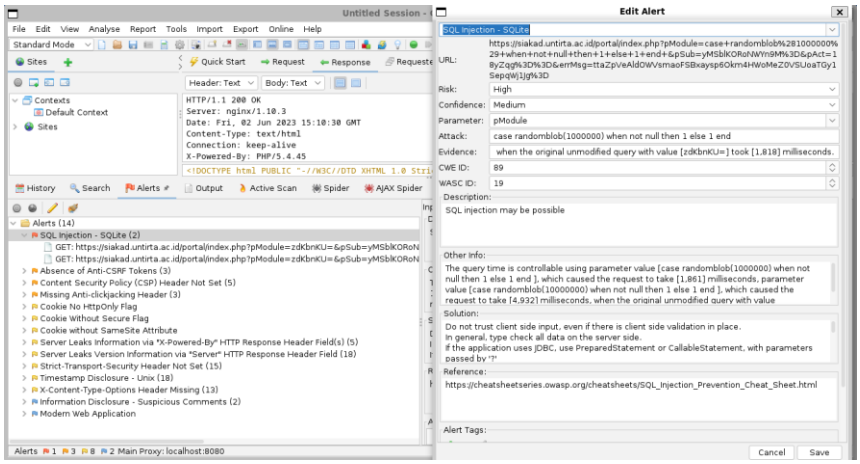
Lampiran A-6 Hasil Pengujian Menggunakan *Tools* Nmap

```
┌──(root㉿ DESKTOP-0587QJ4)-[/home/fitri]
└─# nmap siakad.untirta.ac.id
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 16:22 WIB
Nmap scan report for siakad.untirta.ac.id (103.142.195.98)
Host is up (0.047s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
111/tcp  open     rpcbind
443/tcp  open     https
3306/tcp open     mysql
5678/tcp filtered rrac

Nmap done: 1 IP address (1 host up) scanned in 37.82 seconds
```

Lampiran A-7 Hasil Pengujian Menggunakan *Tools* Vega



Lampiran A-8 Hasil Pengujian Menggunakan *Tools* Owasp Zap



Lampiran A-9 Hasil Pengujian Simulasi Serangan Sql *injection* Menggunakan *Tools* sqlmap

LAMPIRAN B

RACI CHART

Lampiran B-1 Raci Chart APO13

APO13 RACI CHART																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Bussiness Executives	Bussiness Process Owners	Strategy Executives Committee	Steering (Programmes/Project)	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Bussiness Continuity Manager	Privacy Officer
APO13-1		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C C	
APO13-2		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13-3					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Lampiran B-2 Raci chart DSS05

DSS05 RACI CHART																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Bussiness Executives	Bussiness Process Owners	Strategy Executives Committee	Steering (Programmes/Project)	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Bussiness Continuity Manager	Privacy Officer
DSS5-1						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS5-2						I					C	A				C	C	C	I	R	R		I	R		
DSS5-3						I					C	A				C	C	C	I	R	R		I	R		
DSS5-4						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS5-5						I					C	A				C	C	C	I	C	R		I	R	I	
DSS5-6											I					C	C	A			R					
DSS5-7				I		C					I	A				C	C	C	I	C	R		I	R	I	I

LAMPIRAN C

HASIL REKOMENDASI

Lampiran C-1 Hasil Rekomendasi *Vulnerability Assessment*

No	Kerentanan	Rekomendasi
1	*Session cookie without Httponly flag*	Mengkonfigurasi dengan mengatur *session cookie HttpOnly Flag set*
2	*Session cookie without secure flag*	Konfigurasi dengan mengatur *session cookie secure flag set*.
3	*SSLv3 supported (POODLE attack, others)*	Menonaktifkan SSLv3, kemungkinan server https harus di restart agar perubahan konfigurasi dapat diterapkan
4	*Client ciphersuite preference*	Server https harus menkonfigurasi untuk menerapkan preferensi *ciphersuite server*.
5	*Directory listing detected*	Untuk Apache, tambah "indexIgnore *" pada direktori file .htaccess. Mengubah "`dir-listing.activate = "aktif"` ke "`dir-listing.activate = "non-aktif"` dalam konfigurasi `lighttpd`.
6	*Missing anti-clickjacking-header*	Gunakan X-frame-options untuk menghindari website dari penyerang.
7	*Sql injection*	Memeriksa semua data di server, apabila ada validasi sisi klien.
8	*Absence of anti-CSRF tokens*	Gunakan anti-CSRF.
9	*Content-security-policy (CSP) header not set*	Konfigurasi server web untuk mengembalikan header HTTP *content-security -pol*icy (CSP)

No	Kerentanan	Rekomendasi
10	*Cookie without samesite attribute*	Memilih atribut *website* yang sama lalu atur ke lax idealnya *strict* untuk *cookie*.
11	*Server leak information via x-powered-By HTTP response header field(s)*	Memilih *web, application, load balancer* lalu dikonfigurasi untuk mengklik *x-powered-by* header.
12	*Server leaks version information via server HTTP response header field*	Memilih *web, application, load balancer* dikonfigurasi untuk menekan server header.
13	*strict-transport-security header not set*	Konfigurasi keamanan transportasi yang ketat agar memastikan hanya permintaan HTTPS yang dianggap valid dan sangat mengurangi resiko mengakses halaman yang mencurigakan.
14	*Timestamp Disclosure – Unix*	Mengkonfirmasi secara manual bahwa data stempel waktu tidak sensitif, dan data tidak dapat digabungkan untuk diungungkapkan yang dapat dieksploitasi.
15	*X-content-type-options header missing*	Memastikan web mengaktifkan header tipe konten yang tepat, dan menngaktifkan header x-content-type-options ke nosniff untuk semua halaman web.

Lampiran C-2 Hasil Rekomendasi COBIT 5

No	Proses	Rekomendasi
1	APO13	Pusat Data dan Informasi harus memaksimalkan implementasi sistem keamanan manajemen informasi untuk membenarkan keamanan sistem dijaga dengan baik. Pusat Data dan Informasi memastikan bahwa segala sesuatu yang terkait dengan keamanan informasi didokumentasikan serta dipantau untuk dievaluasi lalu digunakan sebagai tolak ukur perbaikan untuk mengurangi risiko TI.
2	DSS05	Pusat Data dan Informasi harus memiliki program audit internal keamanan yang bertujuan untuk memeriksa dan mengevaluasi apakah peningkatan tindakan dan kebijakan keamanan informasi sudah tepat atau belum. Pusat Data dan Informasi harus meninjau ulang mengenai pelatihan tentang serangan keamanan informasi serta melakukan tes penetrasi untuk memastikan perlindungan dari serangan keamanan.

LAMPIRAN D

KUESIONER

Keterangan Level Kuisioner

PROCESS *CAPABILITY LEVEL*

Level 0 : Proses tidak lengkap.

Level 1 : Proses dilakukan.

Level 2 : Proses terkelola.

Level 3 : Proses ditetapkan.

Level 4 : Proses yang dapat diprediksi.

Level 5 : Optimasi proses.

A : Proses tidak dilakukan atau tidak mencapai tujuan.

B : Proses berjalanUniversitas telah melakukan tujuannya, namun misi tersebut belum berhasil.

C : Proses dilaksanakan menggunakan manajemen proses (rencana, memantauan, dan penilaian) untuk memastikan bahwa produk kerja dari proses dijalankan, dikendalikan, dan dikelola dengan benar.

D : Proses telah ditetapkan untuk mencapai tujuan.

E : Proses telah beroperasi melalui batasan untuk memastikan bahwa tujuan telah terpenuhi.

F : Proses terus meningkatkan pemenuhan tujuan Universitas di masa depan.

Kuesioner tingkat kapabilitas ini dirancang untuk menentukan kemampuan manajemen keamanan, dalam keadaan saat ini dan keadaan yang diharapkan, serta mengidentifikasi prioritas untuk perbaikan. Survei disusun dengan format pilihan ganda dan pertanyaan. Pertanyaan tersebut dikelompokkan berdasarkan subdomain proses, dan setiap pertanyaan memiliki dua jawaban, satu untuk kondisi saat ini dan satu lagi untuk kondisi yang diharapkan. Setiap pertanyaan memiliki enam kemungkinan jawaban yang menyatakan kemampuan proses dalam manajemen keamanan. Setiap opsi terdiri dari pilihan a sampai f, dengan mewakili tingkat kemampuan a=0, b=1, c=2, d=3, e=4, f=5.

Jawaban responden dapat menentukan nilai dan tingkat kemampuan. Rekapitulasi jawaban diambil sebagai ekspresi dari keadaan yang diberikan, yang menunjukkan keadaan saat ini atau keadaan yang diharapkan. Tanda menandai (√) ruang yang tersedia, ini terkait dengan proses kemampuan spesifik dari proses manajemen data. Pengisisan kuesioner untuk mendapati kondisi saat ini dan kondisi yang diharapkan, kemudian dianalisis lebih lanjut untuk dilakukan dan dapat menjadi dasar untuk menentukan solusi desain untuk peningkatan proses manajemen konfigurasi.

Pengelolaan Keamanan – APO13

APO13 adalah proses pendefinisian, pengoperasian SMKI.

Tujuan Proses:

Membatasi dampak insiden keamanan pada tingkat risiko yang dapat diterima Universitas.

Mengerjakan dan merawat SMKI

APO13.01 memberikan pendekatan yang terstandarisasi, formal, dan berkelanjutan serta menyediakan (SMKI) serta proses bisnis yang selaras dengan kebutuhan keamanan dan Universitas.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Apakah penetapan capaian dan batasan dari SMKI sesuai dengan prosedur dari Universitas?												
2	Bagaiman pelibatan secara rinci dari tingkat pengesahan untuk setiap pembedaan pada capaian SMKI?												
3	Bagaimana pembentukan SMKI yang terkoordinasi prosedur Universitas?												
4	Bagaimana tingkat penyesuaian SMKI dengan prosedur tata kelola keamanan Universitas?												
5	Bagaimana tingkat kekuasaan pihak yang mengatur dan mengimplementasikan SMKI?												
6	Bagaimana persedian dan penjagaan dokumen yang menjelaskan mengenai capaian SMKI?												
7	Bagaimana penetapan dan penjelasan fungsi dari SMKI?												

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
8	Bagaimana hubungan prosedur SMKI dalam Universitas?												

Memastikan dan menyusun rencana pengelolaan risiko SMKI

APO13.02 digunakan untuk pengelolaan rencana SMKI yang mengartikan terkelola dengan strategi serta infrastruktur Universitas.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Bagaimana mendeskripsikan dan penjagaan mengenai rencana menanggulangi risiko keamanan yang sesuai dengan misi Universitas?												
2	Bagaimana memilih rencana mengenai penyelesaian risiko keamanan yang cocok dan maksimal sesuai kemampuan yang sudah ditetapkan?												
3	Bagaiman penjagaan dan penyimpanan dari pengelolaan mengenai risiko keamanan?												
4	Bagaimana saran untuk mengimplementasikan rencana penyelesaian risiko keamanan yang didukung dengan pengamatan dari peran dan kewajiban?												
5	Bagaimana perancangan prosedur untuk memberi saran untuk penyusunan dan peningkatan implementasi solusi penyelesaian risiko keamanan?												
6	Bagaimana penetapan kinerja dari hasil perhitungan?												
7	Bagaimana referensi mengenai pelatihan keamanan?												
8	Bagaimana menggabungkan implementasi dan pengamatan dari aturan keamanan yang mampu untuk mencegah dan menangani insiden yang tidak diingikan?												

Memeriksa dan memantau SMKI

APO13.03 digunakan untuk pengelolaan berulang, hubungan dan maanfaat kebutuhan menggabungkan pemeriksaan data kinerja dari SMKI.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Bagaimana melaksanakan evaluasi kinerja dari SMKI yang menyesuaikan dan mengawasi aktifitas prosedur keamanan?												
2	Bagaimana memperhitungkan hasil audit insiden keamanan dari pihak yang bersangkutan?												
3	Bagaimana penyediaan terkait audit internal SMKI yang sudah dijadwalkan?												
4	Bagaimana melaksanakan pemantauan tata kelola SMKI berulang untuk menentukan pencapaiannya tetap sesuai dengan proses SMKI yang teridentifikasi?												
5	Bagaimana perancangan pengarahan rencana keamanan atas penemuan dari proses pengamatan?												
6	Bagaimana melaksanakan pendataan dari proses dan kejadian yang dapat berakibat pada kinerja dari sistem keamanan manajemen informasi?												

Pengelolaan Layanan Keamanan – DSS05

DSS05 adalah Proses pengolahan informasi dan hak akses untuk melaksanakan pemantauan dari ancaman keamanan.

Tujuan Proses:

Untuk mengurangi kelemahan keamanan pada Universitas.

Melindungi dari Serangan

DSS05.01 digunakan untuk menyelidiki, mencegah, dan memperbaiki TI dari insiden keamanan seperti, bug, worm, spyware dan lain-lain.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	B	c	d	e	f
1	Bagaimana informasi pemahaman mengenai serangan keamanan?												
2	Bagaimana pihak yang bertanggung jawab melakukan prosedur pencegahan serangan keamanan?												
3	Bagaimana melaksanakan penjagaan alat-alat mengenai serangan keamanan yang terus diperbaiki?												
4	Bagaimana teknologi keamanan dikirimkan secara terhimpun?												
5	Bagaimana melaksanakan hasil mengenai insiden keamanan modern?												
6	Bagaimana menjaga informasi dari pembersihan data?												
7	Sejauh mana pelatihan yang dilakukan mengenai serangan keamanan?												
8	Sejauh mana melaporkan kepada *user* agar tidak memasang aplikasi yang tidak dikenal oleh Universitas?												

Pengelolaan konektivitas jaringan

Subdomain DSS05.02 digunakan untuk tindakan serta proses administratif mengenai penjagaan informasi seluruh hubungan.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	B	c	d	e	f
1	Sejauh mana peraturan keamanan koneksi mempertimbangkan evaluasi ancaman?												
2	Bagaimana cakupan hak yang mengenai teknologi yang membuka data Universitas?												
3	Bagaimana menentukan teknologi yang dijaga oleh *password* Universitas?												
4	Sejauh mana prosedur pembersihan jaringan untuk menata data masuk keluar Universitas?												
5	Sejauh mana data dienkripsi selama mengirim informasi tersembunyi?												
6	Bagaimana pelaksanaan aturan konektivitas yang diterima Universitas?												
7	Sejauh mana pengarahan konfigurasi mengenai pelaksanaan keamanan?												
8	Sejauh mana penyusunan sistem untuk membantu transfer dan perolehan data?												
9	Sejauh mana melaksanakan tes penetrasi untuk menentukan penjagaan terhadap jaringan Universitas?												
10	Sejauh mana melaksanakan penjagaan tes sistem keamanan Universitas agar berfungsi?												

Pengelolaan perangkat

Subdomain DSS05.03 proses menentukan teknologi (seperti komputer, desktop, dan lain-lain) dilindungi oleh kualifikasi keamanan untuk memproses, menyimpan, serta mengirimkan data.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Sejauh mana menentukan perangkat akan digunakan untuk memenuhi penunjang keamanan?												
2	Bagaimana melaksanakan prosedur penjagaan akses teknologi yang diimplementasikan?												
3	Sejauh mana melaksanakan enkripsi data di area pengolahan tersembunyi?												
4	Sejauhmana mengelola pengaruh fasilitas perangkat Universitas?												
5	Bagaimana manajemen konfigurasi mematuhi penunjang keamanan?												
6	Bagaimana pelaksanaan pemfilteran jaringan ke seluruh teknologi yang dipergunakan?												
7	Sejauh mana menentukan seluruh perangkat (*hardware*, *software*, dan data) yang wajib untuk dijalankan sistem yang sudah dilindungi?												
8	Sejauh mana memberikan penjagaan teknologi yang digunakan? (misalnya, melindungi terhadap kehilangan).												
9	Srjauh mana mencegah informasi dan akses yang sensitif disimpan di perangkat Universitas yang dijual atau sudah tidak digunakan lagi?												

Pengelolaan identitas dan fasilitas jangka panjang

Subdomain DSS05.04 digunakan untuk menentukan seluruh pemakai teknologi mempunyai hak yang diperlukan.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	C	d	e	f
1	Bagaimana mengelola hak pemakai teknologi berlandaskan tujuan dan kualifikasi prosedur?												
2	Sejauh mana menyesuaikan hak pengguna untuk menangkap intruksi kewajiban berlandaskan ketentuan?												
3	Bagaimana pemberian proses data berlandaskan tujuan fungsionalnya?												
4	Sejauh mana melaksanakan sinkronsasi semua peran didentifikasi?												
5	Sejauh mana melakukan pemberian informasi terhadap pihak lain untuk memberikan hak pemakai teknologi?												
6	Bagaimana ruang lingkup seluruh pertukaran hak pengguna?												
7	Bagaimana melakukan pengarahan terhadap seluruh pengguna?												

Pengelolaan fasilitas pada perangkat TI

DSS05.05 digunakan untuk melakukan implementasi proses untuk memberi, membatasi, serta mencabut hak pengguna. Semua persyaratan berlaku untuk semua pihak.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	B	c	d	e	f
1	Bagaimana proses permintaan serta pemberian akses fasilitas TI yang berjalan?												
2	Bagaimana menjaga agar dokumentasi akses tetap mutakhir berdasarkan fungsi kerja serta kewajiban pekerjaannya?												
3	Bagaimana cakupan penyusunan dan pemantauan seluruh kanal dalam sarana teknologi?												
4	Sejauh mana fasilitas teknologi dengan kerentanan tinggi terlindungi?												
5	Bagaimana melaksanakan pembelajaran terhadap pemahaman keamanan teknologi yang dilakukan terstruktur?												

Pengelolaan data kerentanan dan instrument keluaran

Subdomain DSS05.06 digunakan untuk menyediakan keamanan fisik, aktivitas pelaporan, dan pencatatan administrasi peralatan teknologi misalnya, surat, atau kode keamanan.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	D	e	f
1	Sejauh mana prosedur untuk mengontrol penerimaan, pelaksanaan, penghapusan informasi tertentu?												
2	Sejauh mana pelaksanaan untuk mengakses data rentan dan instrument keluaran minimal menyetarakan akibat kualitas Universitas?												
3	Bagaimana manufaktur yang terlibat terutama dalam menyimpan data dan instrument keluaran dalam melaksanakan audit?												
4	Sejauh mana area penyimpanan informasi khusus dan perangkat sensitif dilindungi?												
5	Bagaimana menghilangkan dokumen kerentanan yang tidak digunakan lagi?												

Mengamati prasarana terkait keamanan

DSS05.07 digunakan untuk mendeteksi insiden, memantau prasarana, mencegah hak aspek tidak valid serta menentukan seluruh kejadian terpadu ke dalam pemantauan inti dan proses manajemen.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Sejauh mana aktifitas pemantauan mencatat laporan insiden keamanan dan menentukan sejauh mana data tersimpan berlandaskan akibat peninjauan?												
2	Bagaimana memproses insiden kerentanan yang disimpan untuk mendukung penyelidikan?												
3	Sejauh mana menentukan karakter kejadian kerentanan untuk diidentifikasi dampak dan dikelola dengan tepat?												
4	Sejauh mana tinjauan keamanan yang dilakukan untuk mengidentifikasi insiden yang tidak diinginkan?												
5	Bagaimana pengaturan proses untuk dokumentasi yang dipertahankan agar memastikan bahwa semua staf mengetahui persyaratan atau kebutuhan prosedur keamanan?												
6	Sejauh mana insiden keamanan dicatat ketika proses pemantauan mengidentifikasi insiden keamanan yang mungkin akan berdampak lebih jauh?												