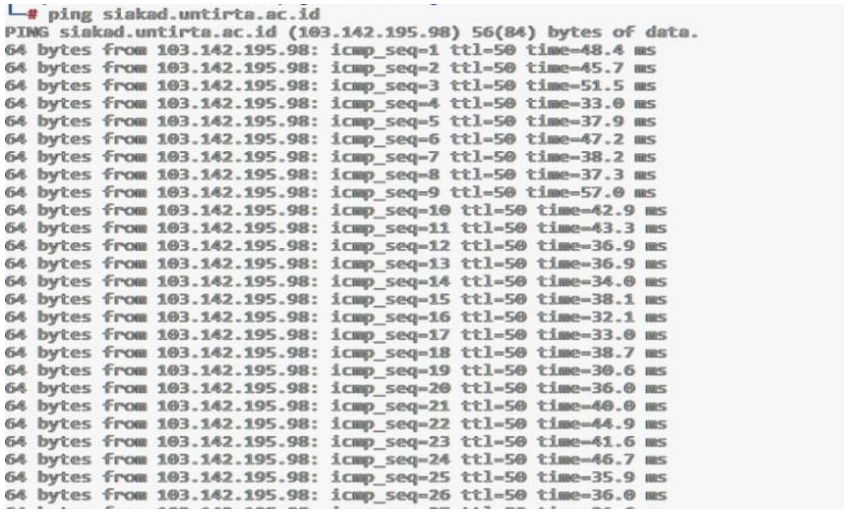
BAB IV
HASIL DAN PEMBAHASAN

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.

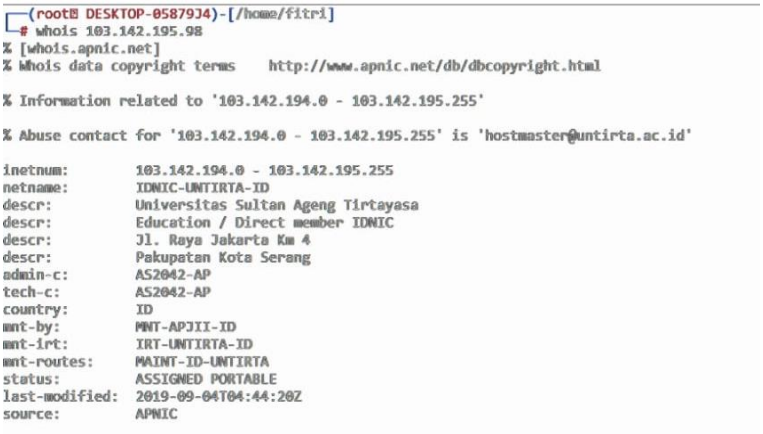
4.1.1 Analisis Pengumpulan Informasi

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.



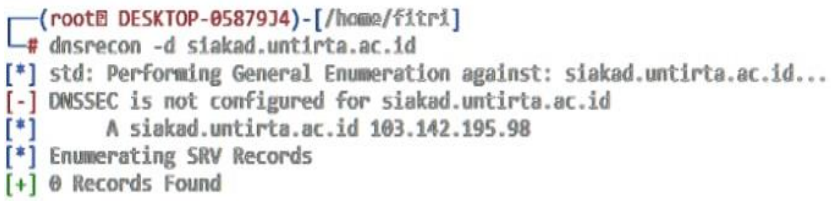
Gambar 4.1 Hasil Pengujian *IP Address* Menggunakan Kali Linux

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.



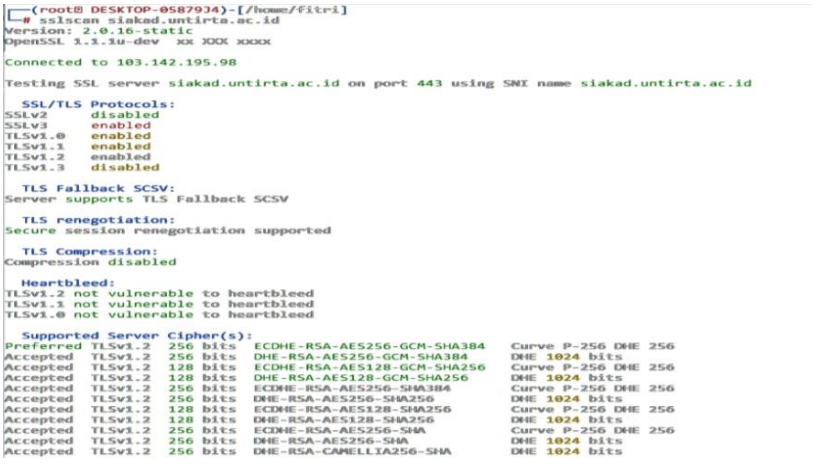
Gambar 4.3 Hasil Pengujian Mengggunakan *Tools* Dnsrecon.

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.

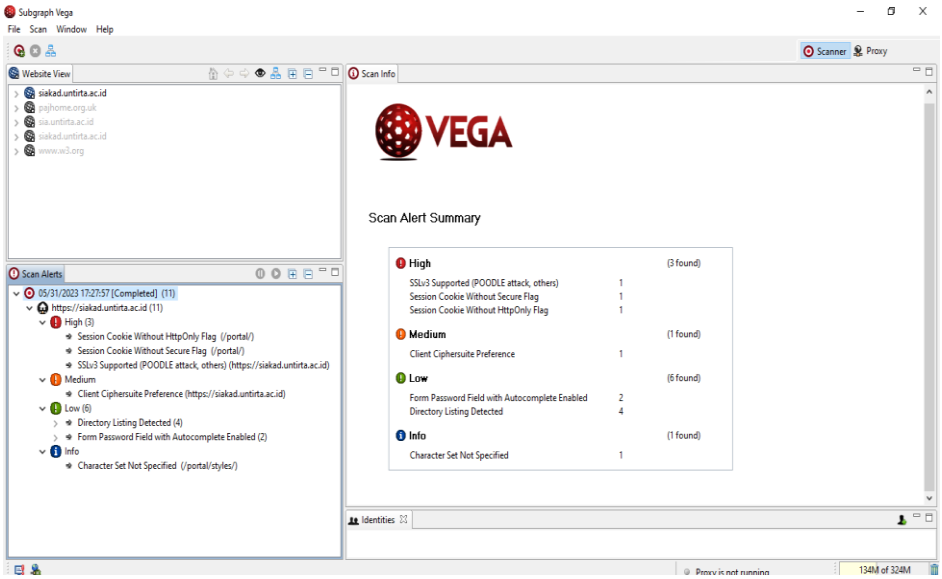
Gambar 4.6 Hasil Pengujian Menggunakan *Tools* Nmap.

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

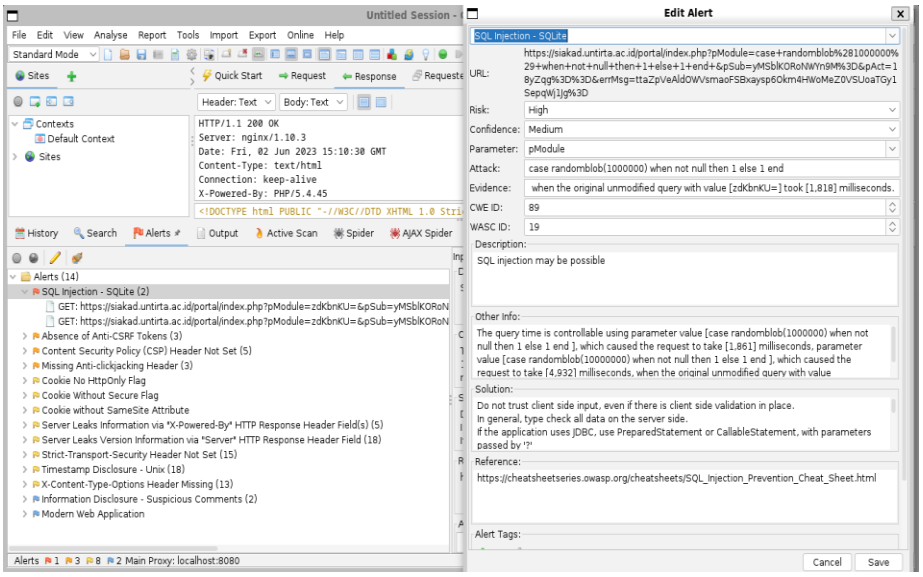
Tahap selanjutnya merupakan mengidentifikasi kerentanan, dimana pada tahap ini akan mencari kelemahan pada *website* https://siakad.untirta.ac.id. Pengujian ini *tools* yang digunakan yaitu Vega *vulnerability* dan Owasp Zap. Berikut Gambar 4.7 merupakan hasil pengujian menggunakan *tools* Vega *vulnerability.*



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.