ANALISIS KEAMANAN SISTEM INFORMASI KEPEGAWAIAN RUMAH SAKIT UMUM PUSAT DR. SARDJITO YOGYAKARTA BERDASARKAN STANDAR ISO 27001

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh:

Sulton Daud Ul Mukarobin

12650035

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-3230/Un.02/DST/PP.00.9/08/2019

Tugas Akhir dengan judul : ANALISIS KEAMANAN SISTEM INFORMASI KEPEGAWAIAN RUMAH SAKIT UMUM PUSAT DR. SARDJITO YOGYAKARTA BERDASARKAN STANDAR ISO 27001

yang dipersiapkan dan disusun oleh:

Nama : SULTON DAUD UL M
Nomor Induk Mahasiswa : 12650035
Telah diujikan pada : Rabu, 31 Juli 2019
Nilai ujian Tugas Akhir : A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhammad Taufiq Nuruzzaman, S.T. M.Eng.
NIP. 19791118 200501 1 003

Penguji I

Aulia Faqih Rifa'i, M.Kom.
NIP. 19860306 201101 1 009

Penguji II

Rahmat Hidayat, S.Kom., M.Cs.
NIP. 19850514 201503 1 002

Yogyakarta, 31 Juli 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Plh. Dekan

Dr. Agung Fatwanto, S.Si., M.Kom.
NIP. 19770103 200501 1 003

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Sulton Daud Ul Mukarobin
NIM	: 12650035
Judul Skripsi	: Analisis Keamanan Sistem Informasi Kepegawaian Rumah Sakit Umum Pusat Dr. Sardjito Yogyakarta Berdasarkan Standar ISO 27001

Sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 26 Juli 2019
Pembimbing

Muhammad Taufiq Nuruzzaman, S.T. M.Eng.
NIP. 19791118 200501 1 003

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Sulton Daud Ul Mukarobin
NIM	: 12650035
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul " **Analisis Keamanan Sistem Informasi Kepegawaian Rumah Sakit Umum Pusat Dr. Sardjito Yogyakarta Berdasarkan Standar Iso 27001**" tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 26 Juli 2019

Yang Menyatakan

Sulton Daud Ul Mukarobin
NIM. 12650035

KATA PENGANTAR

Bismillahirrahmanirrahim, puji syukur atas kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah serta inayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan Sistem Informasi Kepegawaian Rumah Sakit Umum Pusat Dr. Sardjito Yogyakarta Berdasarkan Standar Iso 27001" ini dengan baik sesuai dengan kewajiban dalam memenuhi gelar Strata 1 Komputer (S.Kom) di Jurusan Teknik Informatika Fakultas Sains dan teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Tidak lupa shalawat serta salam tetap tercurah kepada junjungan Nabi Muhammad SAW dan semoga kelak kita mendapat syafaat darinya.

Oleh karena itu, penulis ingin mengucapkan terima kasih sebesarbesarnya kepada:

1. Bapak Prof. Drs. K.H. Yudian Wahyudi, M.A., Ph.D. selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
3. Bapak Sumarsono, S.T., M.Kom., selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
4. Bapak Aulia Faqih Rifa'i, M.Kom., selaku dosen pembimbing akademik kelas reguler Teknik Informatika 2012.
5. Bapak Muhammad Taufiq Nuruzzaman, S.T. M.Eng., selaku Dosen Pembimbing skripsi yang telah memberikan arahan, saran, waktu serta masukan kepada penulis dalam menyusun skripsi.
6. Bapak dan Ibu Dosen Program Studi Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.
7. Pihak Unit Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta yang telah memberikan izin penelitian.
8. Orang tua dan keluarga tercinta yang senantiasa memberikan motivasi serta dukungan baik moril maupun materiil kepada penulis dengan sumua kasih sayangnya.

9. Teman-teman Teknik Informatika yang tidak dapat disebutkan satu persatu yang telah memberikan bantuan, dukungan, serta motivasi kepada penulis.
10. Semua pihak yang telah memberikan bantuan dan dukungan selama menempuh strata satu teknik informatika khususnya dalam penyusunan skripsi ini yang tidak dapat disebut satu persatu. Terima kasih.

Semoga Allah SWT memlalas amal kebaikan dari seluru pihak yang telah membantu penulis menyelesaikan skripsi. Penulis menyadari sepenuhnya masih banyak kesalahan dan kekurangan dalam skripsi ini, maka dari itu berbagai saran dan kritik sangat diharapkan demi perbaikan. Semoga skripsi ini dapat bermanfaat bagi penyusun sendiri pada khususnya dan bagi para pembaca pada umumnya. Terima kasih.

Yogyakarta, 16 Agustus 2019

Penulis

HALAMAN PERSEMBAHAN

Laporan skripsi ini saya persembahkan kepada:

1. Kedua Orang tua, Bapak R. Suroso Sugeng Yuwono dan Alm. Ibu Sri Suprayekti
2. Seluruh anggota keluarga besar Hartowiyono
3. Teman – teman yang selalu memberikan dukungan dalam pembuatan skripsi Ferdian, Anwar, Faizin, Alfian Gautama, Pamuji, Alif Aziz, Fauzi, Wahib, Alfian Nur Jayanto.
4. Teman-teman Teknik Informatika 2012

HALAMAN MOTTO

مَن صَبَرَ ظَفِرَ

Siapa yang bersabar maka ia akan berhasil.

Apa yang kau tanam maka itulah yang akan kau petik.

Syukuri apa yang kita miliki, perjuangkan dan buktikan bahwa kita bisa.

Sesungguhnya dibalik kesulitan terdapat hikmah dan kemudahan.

“Do Or D.O !”

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ANALISIS KEAMANAN SISTEM INFORMASI KEPEGAWAIAN RUMAH SAKIT UMUM PUSAT DR. SARDJITO YOGYAKARTA BERDASARKAN STANDAR ISO 27001

Sulton Daud Ul Mukarobin
12650035

INTISARI

Simetris.net adalah sebuah Sistem Informasi Kepegawaian berbasis web yang dikembangkan oleh Unit Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta guna menunjang proses absensi dan penggajian seluruh karyawan. Data yang tersimpan dalam *website* simetris.net merupakan data penting yang harus dilindungi. Untuk itu perlu dilakukan penelitian yang mencakup pengujian keamanan sistem guna mengetahui tingkat keamanan *website* simetris.net serta audit keamanan sistem informasi untuk memastikan kebijakan keamanan informasi yang diterapkan sesuai prosedur. Pada penelitian ini, pengujian keamanan sistem dilakukan dengan melakukan *penetration testing* terhadap *website* simetris.net menggunakan *tools* berupa perangkat lunak antara lain *Nmap, Zenmap, Maltego, Wapiti, Nikto, SQLmap,* dan *XSSer.* Sedangkan untuk audit keamanan sistem informasi menggunakan ISO/IEC 27001 yang merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI). Hasil *penetration testing* terhadap *website* simetris.net sebagai berikut, dengan Zenmap ditemukan 10 port terbuka. Dengan Nikto ditemukan 2 kerentanan. Pada tahap eksploitasi penulis tidak berhasil melakukan serangan dengan Sqlmap dan XSSer. Sedangkan hasil audit terhadap Unit Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta sebagai penanggung jawab, memperoleh nilai kematangan 3,17 (*Defined Proces*).

Kata kunci: *simetris.net, Penetration testing, Audit Keamanan Sistem Informasi, ISO/IEC 27001.*

SECURITY ANALYSIS OF EMPLOYEE INFORMATION SYSTEM PUBLIC HOSPITAL CENTER Dr. SARDJITO YOGYAKARTA BASED ON ISO 27001 STANDARDS

Sulton Daud Ul Mukarobin
12650035

ABSTRACT

Simetris.net is a web-based Employee Information System developed by the Information Technology Installation Unit of Dr. RSUP Sardjito Yogyakarta to support the attendance and payroll Proceses of all employees. Data stored on the simetris.net *website* is important data that must be protected. For this reason, research needs to be conducted that includes testing system security to determine the level of security of the simetris.net *website* and an information system security audit to ensure that information security policies are implemented according to procedures. In this research, system security testing is done by doing penetration testing on the simetris.net *website* using *tools* such as Nmap, Zenmap, Maltego, Wapiti, Nikto, SQLmap, and XSSer. Whereas the information system security audit uses ISO / IEC 27001 which is a standard document of the Information Security Management System (ISMS). The penetration testing results on the simetris.net *website* are as follows, with Zenmap found 10 open ports. With Nikto found 2 vulnerabilities. At the exploitation stage the author does not succeed in carrying out attacks with Sqlmap and XSSer. While the audit results of the Information Technology Installation Unit Dr. Sardjito Yogyakarta as the person in charge, gets a Maturity value of 3.16 (Defined Proces).

Keywords: simetris.net, Penetration testing, Information Systems Security Audit, ISO / IEC 27001.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang tak terbendung telah menyebabkan banyak bidang terpengaruh. Sehingga banyak organisasi yang mulai menerapkan teknologi informasi dalam proses bisnisnya. Tetapi, perkembangan sistem informasi juga diikuti perkembangan resiko yang ada. Salah satu resiko yang muncul adalah masalah keamanan pada data dalam sistem informasi. Pihak yang tidak bertanggungjawab dapat memanfaatkan kerentanan pada sistem informasi untuk mengambil keuntungan dari data tersebut. Sehingga keamanan data merupakan salah satu keharusan dalam pengembangan sistem informasi.

Rumah Sakit Umum Pusat Dr Sardjito Yogyakarta adalah rumah sakit yang memiliki Sistem Manajemen Terintegrasi Rumah Sakit (SIMETRIS) guna menunjang proses manajemen dalam pengelolaan informasi seluruh aktivitas yang dilakukan rumah sakit secara digital. Guna memudahkan aktifitas seluruh anggota RSUP DR Sardjito khususnya karyawan dan dokter maka dibangun sebuah sistem informasi kepegawaian berbentuk *website* dengan nama domain "simetris.net", fungsinya untuk melihat daftar absensi dan penggajian.

Data pada *website* simetris.net merupakan data penting yang berisi informasi seluruh karyawan RSUP Dr. Sardjito sehingga perlu untuk dilindungi keamanannya. Untuk menanggulangi resiko keamanan pada *website* simetris.net maka diperlukan *penetration testing* dan analisis keamanan sistem informasi. *Penetration testing* dilakukan untuk mencari kerentanan yang ada pada sistem sehingga penanggulangan dapat dilakukan oleh pengembang *website* simetris.net sebelum ada pihak yang ingin memanfaatkan kerentanan sistem informasi tersebut.

Selanjutnya analisis keamanan sistem informasi dapat membantu pengembang membuat mekanisme pengelolaan aset, pengelolaan keamanan fisik

dan lingkungan, serta pengendalian akses untuk *website* simetris.net. Salah satu standar yang sering digunakan untuk melakukan analisis sistem informasi adalah ISO 27001. ISO 27001 merupakan dokumen standar untuk Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan Gambaran umum mengenai apa saja yang harus dilakukan untuk implementasi konsep - konsep keamanan informasi dalam sebuah perusahaan. ISO 27001 sangat fleksibel dikembangkan karena tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai, dan ukuran struktur organisasi.

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang di dapat adalah sebagai berikut :

1. Bagaimana mengetahui kerentanan pada keamanan sistem informasi kepegawaian (*simetris.net*) menggunakan metode *penetration testing*?
2. Bagaimana melaporkan hasil kerentanan pada keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan hasil *penetration testing*?
3. Bagaimana melaksanakan analisis keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan standar ISO 27001?
4. Bagaimana menyusun hasil analisis keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan standar ISO 27001?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. *Penetration testing* dilakukan menggunakan tool.
2. Analisis dilakukan menggunakan standar ISO 27001.
3. Data yang digunakan dalam analisis dan pembahasan masalah adalah data yang diperoleh dari *penetration testing*, observasi dan wawancara.
4. Sistem Informasi yang diperiksa adalah Sistem Informasi Kepegawaian berbentuk *website* bernama simetris.net yang dikelola oleh RSUP Dr. Sardjito Yogyakarta.

5. Analisis yang digunakan adalah metode penilaian (scoring) dengan pendekatan sesuai standar ISO 27001 yaitu model *Maturity level*.

6. Klausul yang digunakan yaitu:

a. Kebijakan Keamanan

b. Pengelolaan Aset

c. Keamanan Fisik dan Lingkungan

d. Manajemen Komunikasi dan Operasi

e. Pengendalian Akses

7. Output yang dihasilkan dalam penelitian ini adalah penilaian dan rekomendasi tentang sistem informasi manajemen terintegrasi rumah sakit.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Mengetahui kerentanan pada keamanan sistem informasi kepegawaian (*simetris.net*) menggunakan metode *penetration testing*.
2. Melaporkan hasil kerentanan pada keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan hasil *penetration testing*.
3. Mendapatkan hasil pengukuran keamanan sistem informasi kepegawaian (*simetris.net*) sesuai standar ISO 27001.
4. Menyusun hasil analisis keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan standar ISO 27001.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, yaitu sebagai berikut:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat menjadi acuan bagi penelitian sejenis dan bagi peneliti diharapkan dapat bermanfaat dalam menambah pengetahuan dan wawasan terutama dalam hal yang sesuai dengan penelitian yang dikaji peneliti

yaitu analisis keamanan sistem informasi kepegawaian (*simetris.net*) berdasarkan standar ISO 27001 pada RSUD Dr. SARDJITO Yogyakarta.

2. Manfaat Praktis

a. Dengan melakukan penelitian ini diharapkan dapat menjadikan suatu bahan kajian yang nantinya dapat meningkatkan mutu program studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta tempat penulis memperoleh ilmu.

b. Pihak-pihak lain yang berhubungan dengan bidang komputer terutama yang berhubungan dengan audit keamanan sistem informasi berdasarkan ISO 27001 yang memerlukan hasil dari penelitian ini.

1.6 Kontribusi Penelitian

Penelitian ini dapat dijadikan sebagai bahan kajian yang nantinya dapat dikembangkan untuk meningkatkan mutu pendidikan..

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini dibuat untuk memberikan Gambaran secara garisbesar tentang penelitian yang dilakukan penulis. Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada bagian bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, keaslian penelitian

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Pada bagian bab ini berisi tentang tinjauan pustaka dan landasan teori yang berhubungan dengan topik yang dibahas dalam penelitian ini.

BAB III METODE PENELITIAN

Pada bagian bab ini berisi tentang uraian rinci tentang metode penelitian yang memberikan penjelasan mengenai detail langkah-langkah yang dilakukan untuk mencapai tujuan dan kesimpulan akhir penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian bab ini memuat hasil dari penelitian dan pembahasan penelitian yang telah dilakukan.

BAB V PENUTUP

Pada bagian bab ini berisi tentang kesimpulan dan saran-saran penelitian selanjutnya.

BAB V
PENUTUP

5.1 Kesimpulan

Setalah proses penelitian Analisis Keamanan Sistem Informasi Kepegawaian Rumah Sakit Umum Pusat Dr. Sardjito Yogyakarta Berdasarkan Standar ISO 27001, yang dimulai dengan *penetration testing* dan dilanjutkan dengan audit menggunakan ISO 27001. Dari hasil penelitian ini didapatkan kesimpulan sebagai berikut:

a) Metode *penetration testing* terdiri dari tahap *information gathering, vulnerability analysis*, dan *exploitation*. Pada tahap *information gathering* menggunakan *tools* Nmap, Zenmap, dan Maltego. Pada tahap *vulnerability analysis* menggunakan Wapiti tidak ditemukan adanya kerentanan, tetapi menggunakan Nikto didapatkan 2 kerentanan. Pada tahap *eksploitation* dilakukan menggunakan Sqlmap dan XSSer.
b) Hasil *penetration testing* terhadap *website* Sistem Informasi Kepegawaian (simetris.net) yaitu pada tahap *information gathering port* yang terbuka adalah port 22, 53, 80, 111, 179, 443, 646, 8080,8443, dan 44443. Sedangkan pada tahap *vulnerability analysis* ditemukan kerentanan yaitu *X-XSS-Protection Header* yang belum terdefinisi dan *X-Content-Type-Option-Header* yang belum di set. Pada tahap *exploitation* tidak berhasil dieksploitasi, karena pada tahap *vulnerability analysis* ditemukan bahwa sistem tidak rentan terhadap serangan Sqlinjection dan *Cross Site Scripting*. Dapat disimpulkan bahwa *website* simetris.net cukup aman.
c) Hasil analisis yang telah dilakukan terhadap Unit Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta selaku penanggung jawab *website* Sistem Informasi Kepegawaian (simetris.net) berdasarkan standar ISO 27001 didapatkan hasil pengukuran *Maturity level* di setiap klausul, untuk klausul kebijakan keamanan sebesar 3.5 (*Managed and Measurable*), klausul pengelolaan aset sebesar 2,42 (*Repeatable but Intuitive*), klausul keamanan

fisik dan lingkungan sebesar 3,62 (*Managed and Measurable*), klausul manajemen komunikasi dan operasi sebesar 3,88 (*Managed and Measurable*), dan klausul pengendalian akses sebesar 2,375 (*Repeatable but Intuitive*).

d) Setelah melakukan proses analisis lebih dalam terhadap hasil audit yang didapatkan dari klausul kebijakan keamanan, klausul pengelolaan aset, klausul keamanan fisik dan lingkungan, klausul manajemen komunikasi dan operasi serta klausul pengendalian akses, diperoleh nilai *Maturity* sebesar 3,16 dengan level *Defined Proces*, maka masih ada beberapa hal yang perlu diperhatikan oleh pengelola sistem informasi, sejauh ini bentuk pengamanan informasi sudah cukup baik, sebagian besar telah didokumentasikan dan dikomunikasikan kepada pihak – pihak yang terkait. Dilihat dari kesiapan RSUP Dr. Sardjito Yogyakarta sebagai pengelola sistem informasi masih dalam tahap penyempurnaan untuk memberikan pelayanan yang lebih baik lagi dalam hal pengamanan dan pengelolaan.

5.2 Saran

Setelah semua proses penelitian yang telah penulis laksanakan, penulis masih merasa ada kekurangan yang harus diperbaiki. Sehingga penulis berharap untuk penelitian lebih lanjut, penulis memberikan saran sebagai berikut:

a) Kami merekomendasikan Bagian Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta untuk menerapkan standar ISO 27001 secara menyeluruh.
b) Diharapkan penelitian lebih lanjut mengenai *website* Sistem Informasi Kepegawaian (simetris.net) dapat menggunakan semua klausul yang ada pada ISO 27001. Sehingga nilai kematangan dapat menyeluruh pada semua proses manajemen keamanan informasi.
c) Kami berharap rekomendasi penulis untuk Unit Instalasi Teknologi Informasi RSUP Dr. Sardjito Yogyakarta baik rekomendasi hasil *penetration testing* maupun hasil audit ISO 27001 dapat dilaksanakan untuk meningkatkan keamanan *website* Sistem Informasi Kepegawaian (simetris.net)

DAFTAR PUSTAKA

Anggraini, Lusi. 2016. *Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001*. Yogyakarta: Skripsi UIN Sunan Kalijaga.

Heri, Setiawan. 2015. *Audit Sistem Informasi Rumah Sakit Menggunakan Standart ISO 27001 (Studi Kasus DI RSU PKU Muhammadiyah Bantul*). Yogyakarta: Skripsi UIN Sunan Kalijaga.

Juhdan. 2016. *Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001*. Yogyakarta: Skripsi UIN Sunan Kalijaga.

Kristanto, Titus; Arief, Rachman; Rozi, Nanang Fakhrur. 2014. *Perancangan Audit Keamanan Informasi Berdasarkan Standar Iso 27001: 2005 (Studi Kasus: Pt Adira Dinamika Multi Finance)*. Surabaya : SESINDO 2014.

Mulyana, Y. B. 2002. *Linux Semudah Windows*. Jakarta : PT. Elex Media Komputindo.

Muniz, J., & Lakhani, A. 2013. *Web Penetration Testing with Kali Linux*. Packt Publishing.

Nasional, Direktorat Badan Standarisasi. 2009. *SNI ISO/IEC 27001: 2009 Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan*. Jakarta: Badan Standardisasi Nasional–BSN.

Permatasari, D. I. 2016. *Audit Keamanan Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta: Skripsi UIN Sunan Kalijaga.

Sarno, Riyanarto. 2009. *Audit Sistem Informasi dan Teknologi Informasi*. Surabaya: ITS Press.

Sarno, Riyanarto dan Iffano, Irsyat. 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya : ITS Press.

Tata Sutabri, 2005. *Sistem Informasi Manajemen.* Yogyakarta : Andi.

Wecan, P. P. 2017. *Pengujian Keamanan Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta.* YOGYAKARTA: Skripsi UIN Sunan Kalijaga.

LAMPIRAN

LAMPIRAN 1

Sasaran Pengendalian SNI-ISO 27001

Klausul	Kontrol	Pengendalian / Sasaran
A.5	SNI-ISO 27001 A.5.1 Kebijakan Keamanan Informaasi	Memberikan arahan dan dukungan manajemen untuk keamanan informasi menurut persyaratan bisnis dan hukum beserta regulasi yang relevan
A.6	SNI-ISO 27001 A.6.1 Organisasi Keamanan Informasi (internal)	Mengelola keamanan informasi dalam organisasi
	SNI-ISO 27001 A.6.2 Organisasi Keamanan Informasi (eksternal)	Memelihara keamanan informasi organisasi dan fasilitas pengolahan informasi yang diakses, diolah, dikomunikasikan kepada atau dikelola pihak eksternal
A.7	SNI-ISO 27001 A.7.1 Pengelolaan Aset (tanggung jawab terhadap asset)	Mencapai dan memelihara perlindungan yang sesuai terhadap asset organisasi
	SNI-ISO 27001 A.7.2 Pengelolaan Aset (klasifikasi informasi)	Memastikan bahwa informasi menerima tingkat perlindungan yang tepat
A.8	SNI-ISO 27001 A.8.1 Keamanan Sumber Daya Manusia (sebelum dipekerjakan)	Memastikan bahwa pegawai, kontraktor, dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya, dan untuk mengurangi resiko pencurian, kecurangan atau penyalah gunaan fasilitas

Klausul	Kontrol	Pengendalian / Sasaran
	SNI-ISO 27001 A.8.2 Keamanan Sumber Daya Manusia (selama bekerja)	Memastikan bahwa semua pegawai, kontraktor, dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggungan gugatan mereka dan disediakan perlengkapan yang memadai untuk mendukung kebijakan keamanan organisasi selama bekerja dan untuk mengurangi resiko kesalahan manusia
	SNI-ISO 27001 A.8.3 Keamanan Sumber Daya Manusia (pengakhiran atau perubahan pekerjaan)	Memastikan bahwa semua pegawai, kontraktor, dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai
A.9	SNI-ISO 27001 A.9.1 Keamanan Fisik dan Lingkungan (area yang aman)	Mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interfensi terhadap lokasi dan informasi organisasi
	SNI-ISO 27001 A.9.2 Keamanan Fisik dan Lingkungan (keamanan peralatan)	Mencegah kehilangan, kerusakan, pencurian atau gangguan asset dan interupsi terhadap kegiatan organisasi
A.10	SNI-ISO 27001 A.10.1 Manajemen Komunikasi dan Operasi (prosedur operasional dan tanggung jawab)	Memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman

Klausul	Kontrol	Pengendalian / Sasaran
	SNI-ISO 27001 A.10.2 Manajemen Komunikasi dan Operasi (manajemen pelayanan jasa pihak ketiga)	Menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga
	SNI-ISO 27001 A.10.3 Manajemen Komunikasi dan Operasi (perencanaan dan ketertiban sistem)	Mengurangi resiko kegagalan sistem
	SNI-ISO 27001 A.10.4 Manajemen Komunikasi dan Operasi (perlindungan terhadap *malicious* dan *mobile code*)	Melindungi integritas perangkat lunak dan informasi
	SNI-ISO 27001 A.10.5 Manajemen Komunikasi dan Operasi (*backup*)	Memelihara integritas dan ketersediaan informasi dan fasilitas pengolahan informasi
	SNI-ISO 27001 A.10.6 Manajemen Komunikasi dan Operasi (manajemen keamanan jaringan)	Memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung
	SNI-ISO 27001 A.10.7 Manajemen Komunikasi	Mencegah pengungkapan, modifikasi, pemindahan atau pemusnahan asset yang

Klausul	Kontrol	Pengendalian / Sasaran
	dan Operasi (penanganan media)	tidak sah, dan gangguan kegiatan bisnis
	SNI-ISO 27001 A.10.8 Manajemen Komunikasi dan Operasi (pertukaran informasi)	Memelihara keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan setiap entitas eksternal
	SNI-ISO 27001 A.10.9 Manajemen Komunikasi dan Operasi (layanan *electronic commers*)	Memastikan keamanan layanan *electronic commers* dan keamanan penggunanya
	SNI-ISO 27001 A.10.10 Manajemen Komunikasi dan Operasi (pemantauan)	Mendeteksi kegiatan pengolahan informasi yang tidak sah
A.11	SNI-ISO 27001 A.11.1 Pengendalian Akses (persyaratan bisnis untuk pengendalian akses)	Mengendalikan akses kepada informasi
	SNI-ISO 27001 A.11.2 Pengendalian Akses (manajemen akses pengguna)	Memastikan akses oleh pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem informasi
	SNI-ISO 27001 A.11.3 Pengendalian Akses (tanggung jawab	Mencegah akses pengguna yang tidak sah dan gangguan atau pencurian atas informasi dan fasilitas pengolahan

Klausul	Kontrol	Pengendalian / Sasaran
	pengguna)	informasi
	SNI-ISO 27001 A.11.4 Pengendalian Akses (jaringan)	Mencegah akses yang tidak sah kedalam layanan jaringan
	SNI-ISO 27001 A.11.5 Pengendalian Akses (sistem operasi)	Mencegah akses yang tidak sah kedalam layanan sistem operasi
	SNI-ISO 27001 A.11.6 Pengendalian Akses (aplikasi dan informasi)	Mencegah akses yang tidak sah terhadap informasi pada aplikasi sistem
	SNI-ISO 27001 A.11.7 Pengendalian Akses (*mobile computing* dan kerja jarak jauh/*teleworking*)	Memastikan keamanan informasi ketika menggunakan fasilitas *mobile computing* dan kerja jarak jauh (*teleworking*)
A.12	SNI-ISO 27001 A.12.1 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (persyaratan keamanan dari sistem informasi)	Memastikan bahwa keamanan merupakan bagian utuh dari sistem informasi
	SNI-ISO 27001 A.12.2 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (pengolahan yang benar	Mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi

Klausul	Kontrol	Pengendalian / Sasaran
	dalam aplikasi)	
	SNI-ISO 27001 A.12.3 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (pengendalian dengan cara kriptografi)	Melindungi kerahasiaan, keaslian, atau integritas informasi dengan cara kriptografi
	SNI-ISO 27001 A.12.4 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (keamanan *system files*)	Memastikan keamanan *system files*
	SNI-ISO 27001 A.12.5 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (keamanan dalam proses pengembangan dan pendukung)	Memelihara keamanan perangkat lunak sistem aplikasi dan informasi
	SNI-ISO 27001 A.12.6 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (manajemen kerawanan teknis)	Mengurangi resiko terhadap eksploitasi kerawanan teknis yang dipublikasikan
A.13	SNI-ISO 27001 A.13.1	Memastikan kejadian dan kelemahan

Klausul	Kontrol	Pengendalian / Sasaran
	Manajemen Insiden Keamanan Informasi (pelaporan kejadian dan kelemahan keamanan informasi)	keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dapat dilakukan tepat waktu
	SNI-ISO 27001 A.13.2 Manajemen Insiden Keamanan Informasi (perbaikan)	Memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi
A.14	SNI-ISO 27001 A.14.1 Manajemen Keberlanjutan Bisnis (aspek keamanan informasi)	Menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu
A.15	SNI-ISO 27001 A.15.1 Kesesuaian (persyaratan hukum)	Mencegah pelanggaran terhadap undang-undang, peraturan perundang-undangan, atau kewajiban kontrak dan setian persyaratan keamanan
	SNI-ISO 27001 A.15.2 Kesesuaian (pemenuhan terhadap kebijakan keamanan standar, pemenuhan teknis)	Memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi
	SNI-ISO 27001 A.15.3 Kesesuaian (pertimbangan audit	Memaksimalkan keefektifan dari dan untuk meminimalkan interfensi kepada/dari proses audit sistem informasi

Klausul	Kontrol	Pengendalian / Sasaran
	sistem informasi)	

LAMPIRAN 2

TABEL HASIL EVALUASI AUDIT PROSES PERHITUNGAN AKHIR NILAI *MATURITY*

NO	KLAUSUL	KODE	QUESTIONS	FORM QUESTIONS					*SCORE*	*MATURITY*	*SCORE MATURITY*
				FQ1	FQ2	FQ3	FQ4	FQ5			
1	A.5										
	A.5.1										
	A.5.1.1	Q1	Sudah adakah kebijakan keamanan informasi?	3					3	*Defined Proces*	3.5
		Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?	3					3	*Defined Proces*	
		Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?	3					3	*Defined Proces*	
		Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?	3					3	*Defined Proces*	
		Q5	Apakah kebijakan tersebut sudah dikomunikasikan?	4					4	*Managed and Measurable*	
	A.5.1.2	Q6	Apakah sudah dilakukan tinjauan ulang terhadap kebijakan keamanan informasi (untuk antisipasi perubahan yang mempengaruhi analisa resiko)?	4					4	*Managed and Measurable*	
		Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?	4					4	*Managed and Measurable*	

		Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?	3					3	*Defined Proces*	
		Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	4					4	*Managed and Measurable*	
		Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	4					4	*Managed and Measurable*	
2	A.7										
	A.7.1										
	A.7.1.1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?		2				2	Repeateble but Intuitive	2.428571429
		Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?		3				3	*Defined Proces*	
		Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?		4				4	*Managed and Measurable*	
		Q14	Apakah kebijakan pengelolaan inventaris aset tersebuh sudah didokumentasikan?		4				4	*Managed and Measurable*	
	A.7.1.2	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?		2				2	Repeateble but Intuitive	

		Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?		4				4	*Managed and Measurable*	
		Q17	Apakah ada jangka waktu pengecekan inventaris aset secara berkala?		1				1	Initial/Ad - hoc	
		Q18	Apakah sudah diidentifikasi nilai dan tingkat kepentingan aset?		1				1	Initial/Ad - hoc	
	A.7.1.3	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?		2				2	Repeateble but Intuitive	
		Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah di implementasikan?		3				3	*Defined Proces*	
		Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?		2				2	Repeateble but Intuitive	
	A.7.2										
	A.7.2.1	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?		1				1	Initial/Ad - hoc	
		Q23	Apakah ada prosedur yang baik berupa pemberi tanda pelabelan dan penanganan informasi?		3				3	*Defined Proces*	
	A.7.2.2	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?		2				2	Repeateble but Intuitive	
3	A.9										

	A.9.1										
	A.9.1.1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?			2			2	Repeateble but Intuitive	3.625
		Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?			3			3	*Defined Proces*	
		Q27	Apakah ada kontrol akses fisik atau ruang / wilayah sebagai tempat menerima tamu?			4			4	*Managed and Measurable*	
		Q28	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?			2			2	Repeateble but Intuitive	
		Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem informasi manajemen rumah sakit?			4			4	*Managed and Measurable*	
		Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindung dari akses tanpa izin?			4			4	*Managed and Measurable*	
	A.9.1.2	Q31	Apakah pengunjung yang datang diawasi dan menulis tanggal datang dibuku tamu?			1			1	Initial/Ad - hoc	
		Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?			3			3	*Defined Proces*	
	A.9.1.3	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?			5			5	*Optimize*	

		Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?			4			4	*Managed and Measurable*	
	A.9.1.4	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?			4			4	*Managed and Measurable*	
		Q36	Apakah bahan yang berbahaya dan mudah meledak sudah disimpan diwilayah aman?			4			4	*Managed and Measurable*	
	A.9.1.5	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?			4			4	*Managed and Measurable*	
		Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?			5			5	*Optimize*	
		Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?			4			4	*Managed and Measurable*	
	A.9.2										
	A.9.2.1	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?			4			4	*Managed and Measurable*	
		Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?			4			4	*Managed and Measurable*	

	A.9.2.2	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?			4			4	*Managed and Measurable*	
		Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau UPS?			4			4	*Managed and Measurable*	
	A.9.2.3	Q44	Apakah utilitas pendukung seperti sumber daya listrik, genset, UPS selalu dicek keamanannya?			4			4	*Managed and Measurable*	
		Q45	Apakah kabel daya dan telekomunikaasi kebutuha data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman?			4			4	*Managed and Measurable*	
	A.9.2.4	Q46	Apakah peralatan Hardware selalu dijaga dan dipelihara dengan baik?			3			3	*Defined Proces*	
		Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?			3			3	*Defined Proces*	
		Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?			4			4	*Managed and Measurable*	
4	A.10										
	A.10.1										
	A.10.1.1	Q49	Apakah terdapat prosedur pengoperasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?				4		4	*Managed and Measurable*	3.882352941

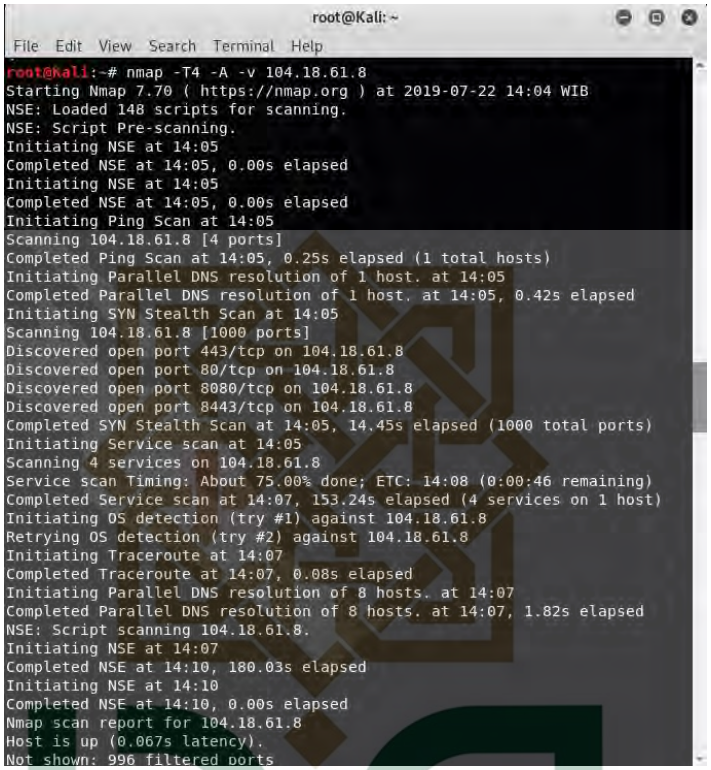
		Q50	Jika ada, apakah prosedur sudah di dokumentasikan dan tersedia bagi pengguna?				4		4	*Managed and Measurable*	
		Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?				4		4	*Managed and Measurable*	
		Q52	Apakah setiap data penting dilakukan back-up?				4		4	*Managed and Measurable*	
	A.10.1.2	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan kepada pihak terkait?				4		4	*Managed and Measurable*	
	A.10.1.3	Q54	Apakah pegawai di ruang sistem informasi sudah dipisahkan menujrut tugas dan tanggung jawabnya masing-masing?				4		4	*Managed and Measurable*	
		Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?				4		4	*Managed and Measurable*	
	A.10.5										
	A.10.5.1	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?				4		4	*Managed and Measurable*	
		Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?				4		4	*Managed and Measurable*	

		Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?				4		4	*Managed and Measurable*	
		Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?				4		4	*Managed and Measurable*	
	A.10.6										
	A.10.6.1	Q60	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?				4		4	*Managed and Measurable*	
		Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?				4		4	*Managed and Measurable*	
		Q62	Sejauh ini, apahak terdapat titik jaringan yang rawan terhadap serangan?				3		3	*Defined Proces*	
		Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?				3		3	*Defined Proces*	
		Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?				4		4	*Managed and Measurable*	
		Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan?				4		4	*Managed and Measurable*	
5	A.11										
	A.11.5										

	A.11.5.1	Q66	Apakah sudah diterapkan prosedur log-in pada sistem informasi?					4	4	*Managed and Measurable*	2.375
		Q67	Apakah sistem sudah membatasi kegagalan percobaan log-in?					1	1	Initial/Ad - hoc	
	A.11.5.2	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda?					3	3	*Defined Proces*	
		Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?					3	3	*Defined Proces*	
	A.11.5.3	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelolaan password untuk memastikan kualitas password?					1	1	Initial/Ad - hoc	
		Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?					2	2	Repeateble but Intuitive	
	A.11.5.4	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?					3	3	*Defined Proces*	
	A.11.5.5	Q73	Apakah sudah menggunakan sesi time-out?					2	2	Repeateble but Intuitive	
TOTAL *MATURITY SCORE*										*Defined Proces*	3.16218487

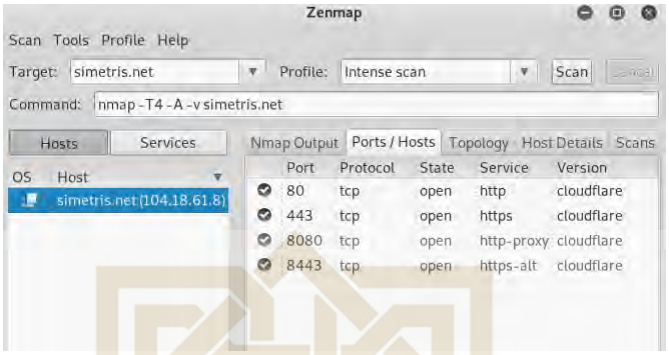
LAMPIRAN 3

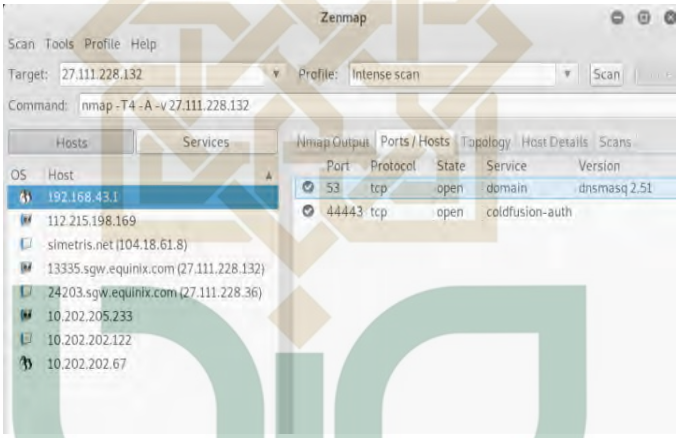
HASIL SCANNING NMAP

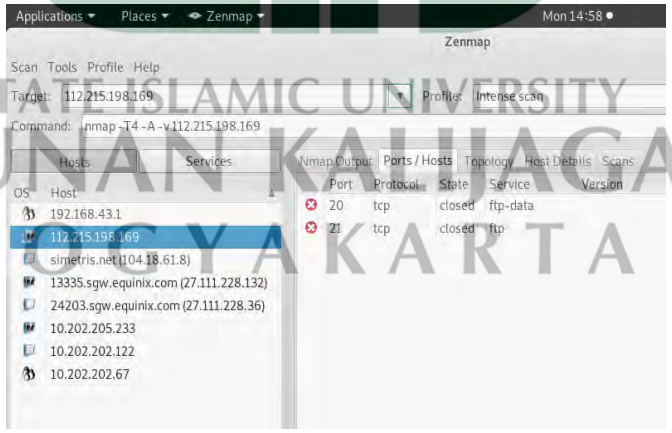


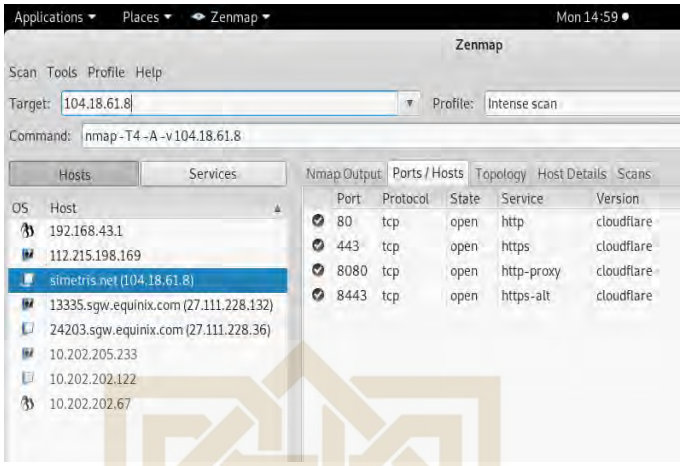
LAMPIRAN 4

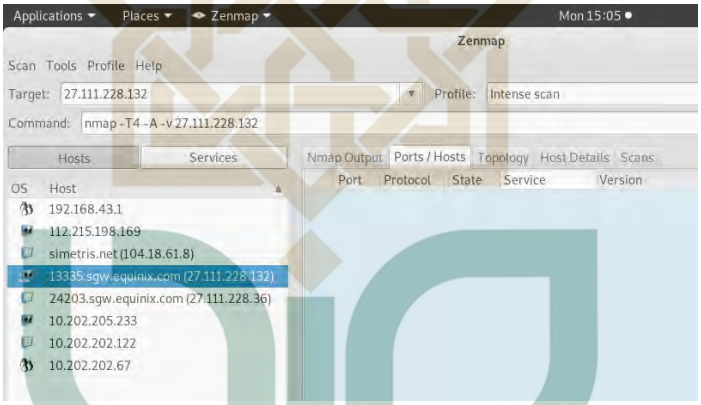
HASIL SCANNING ZENMAP

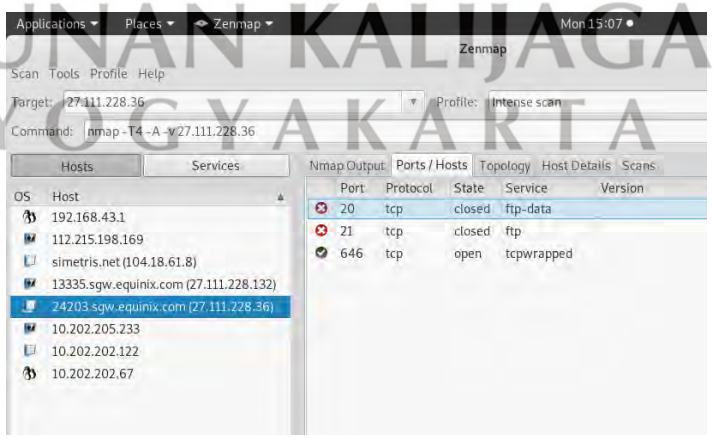


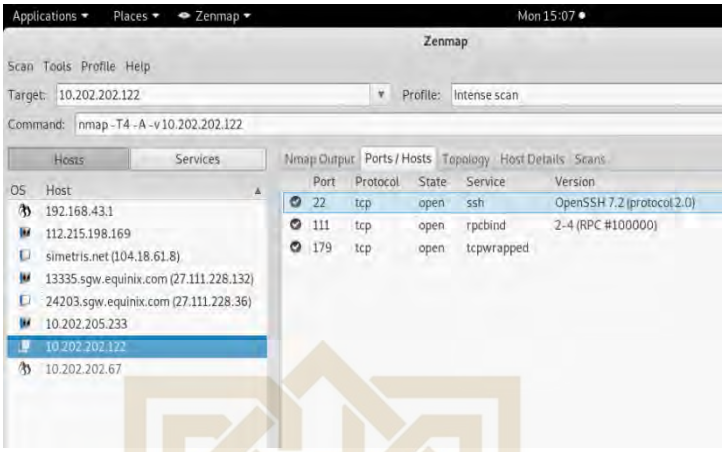


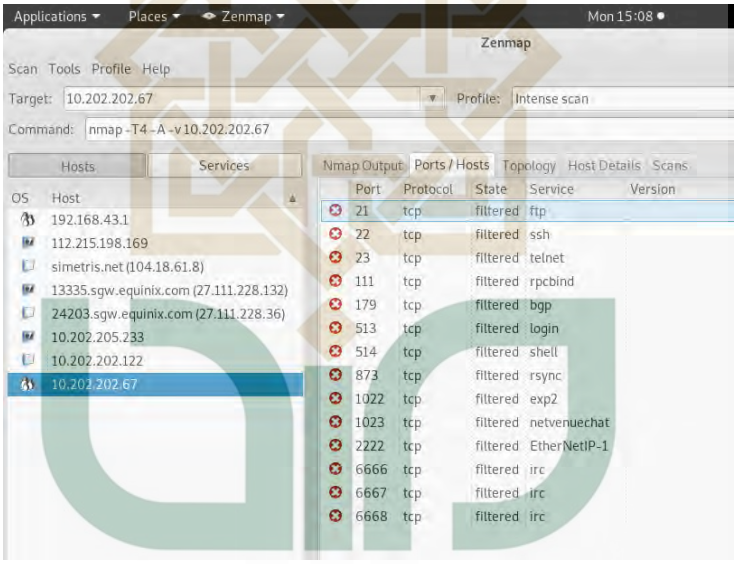




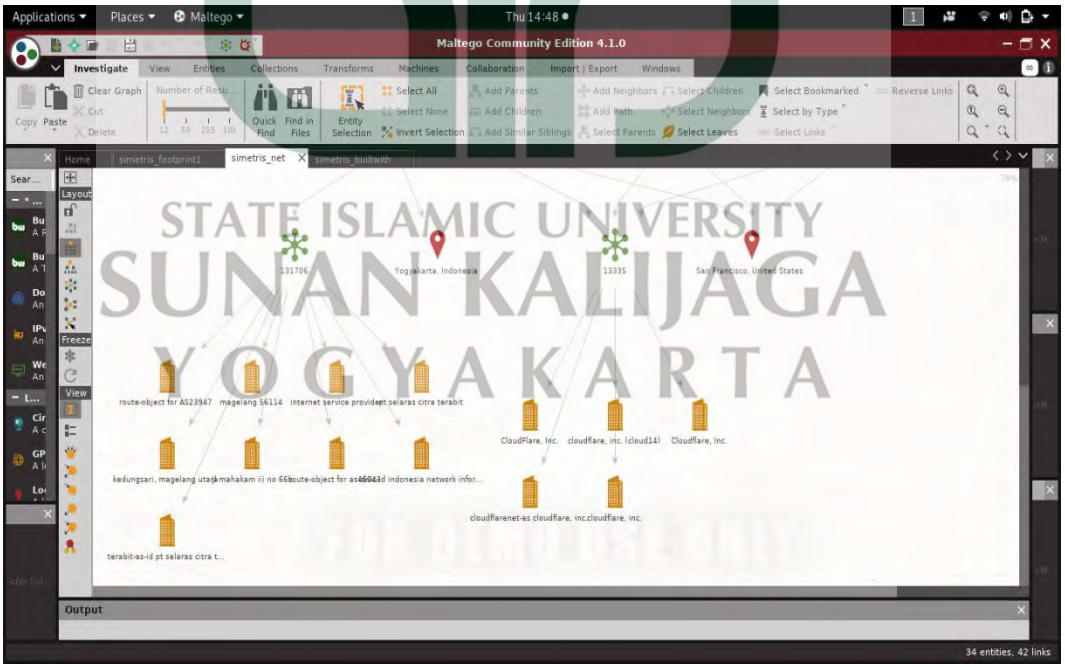


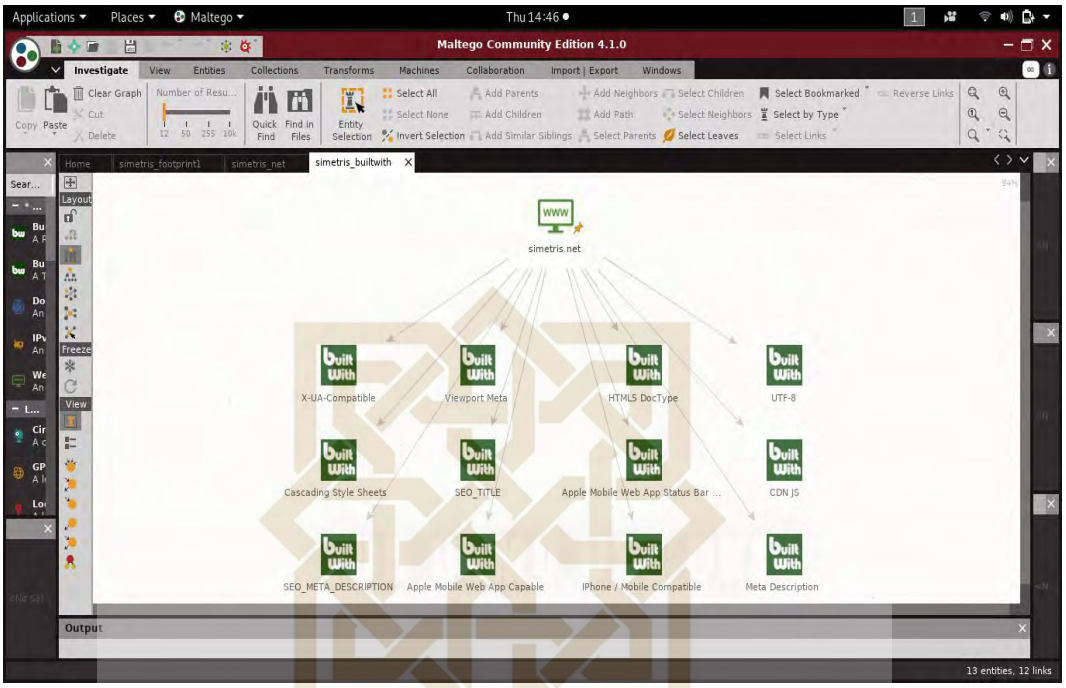






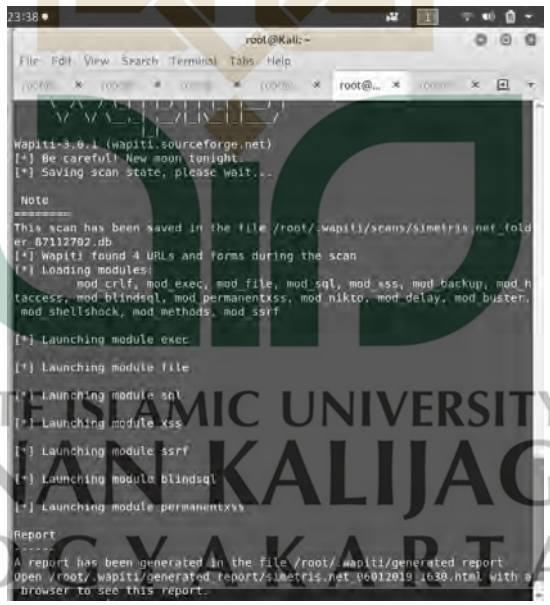
LAMPIRAN 5
HASIL SCANNING MALTEGO

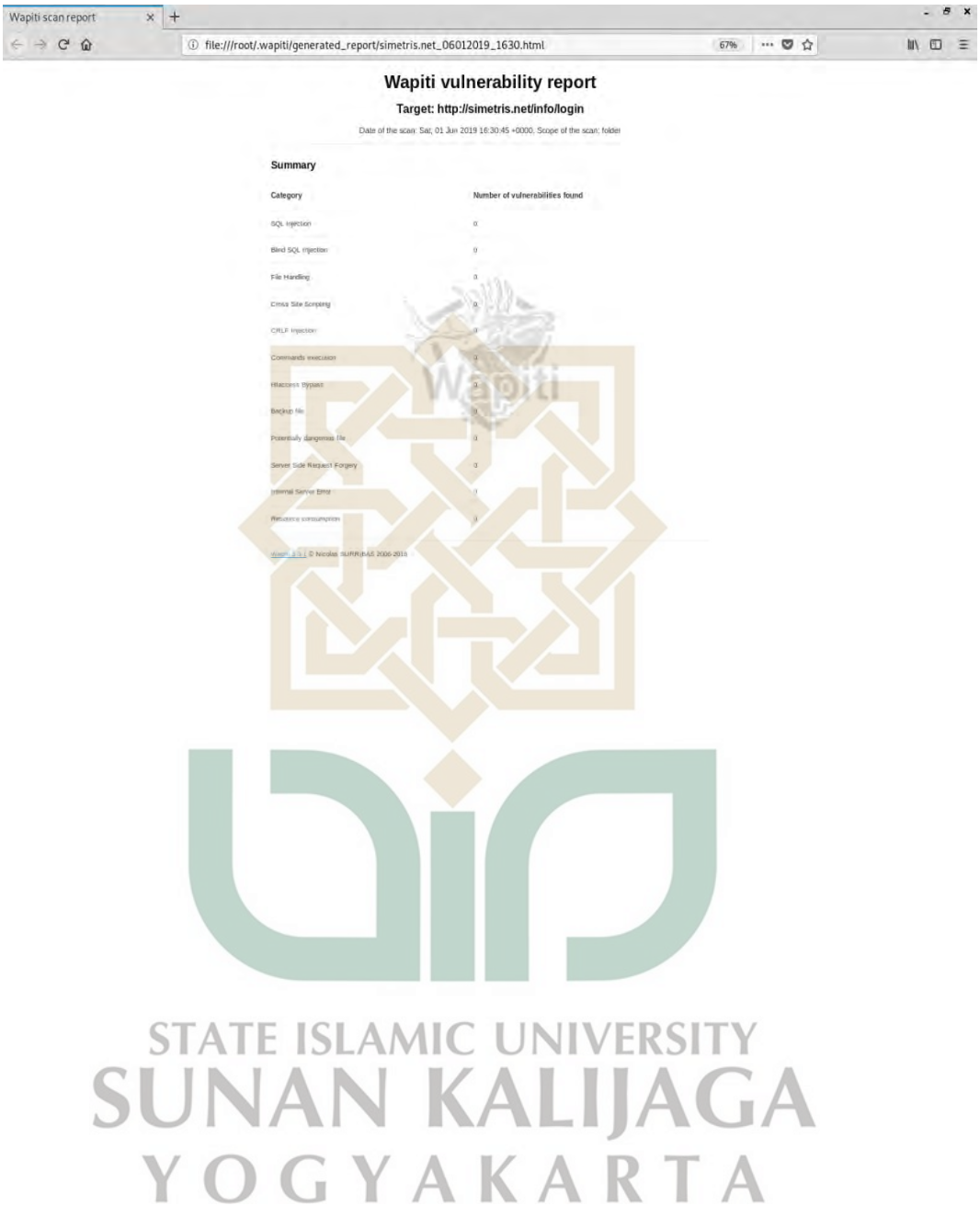




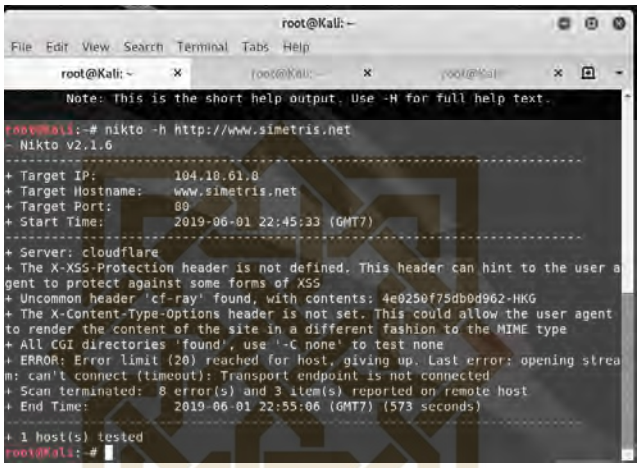
LAMPIRAN 6

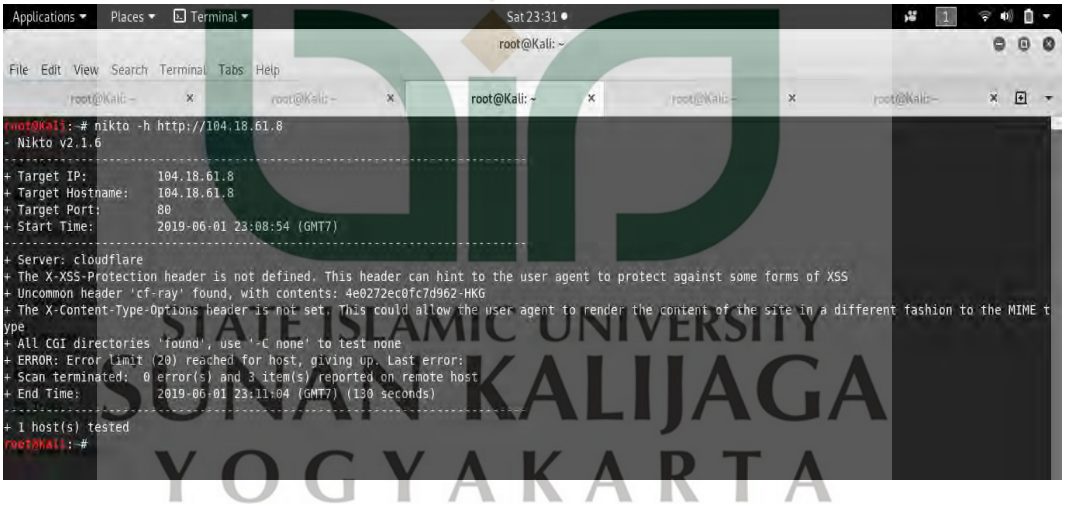
HASIL SCANNING WAPITI



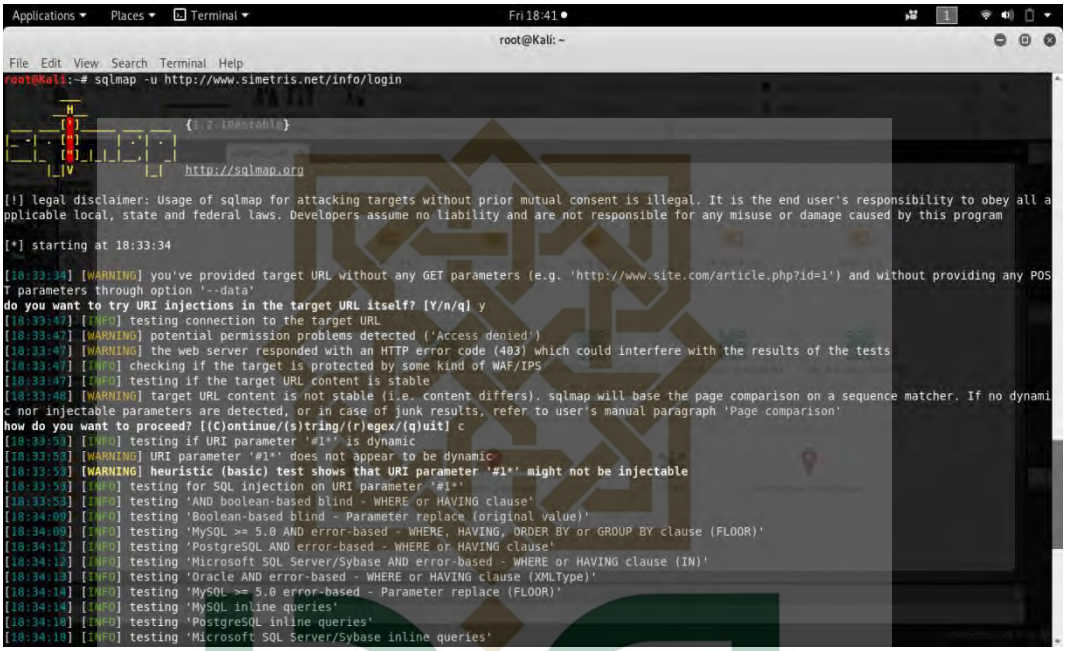


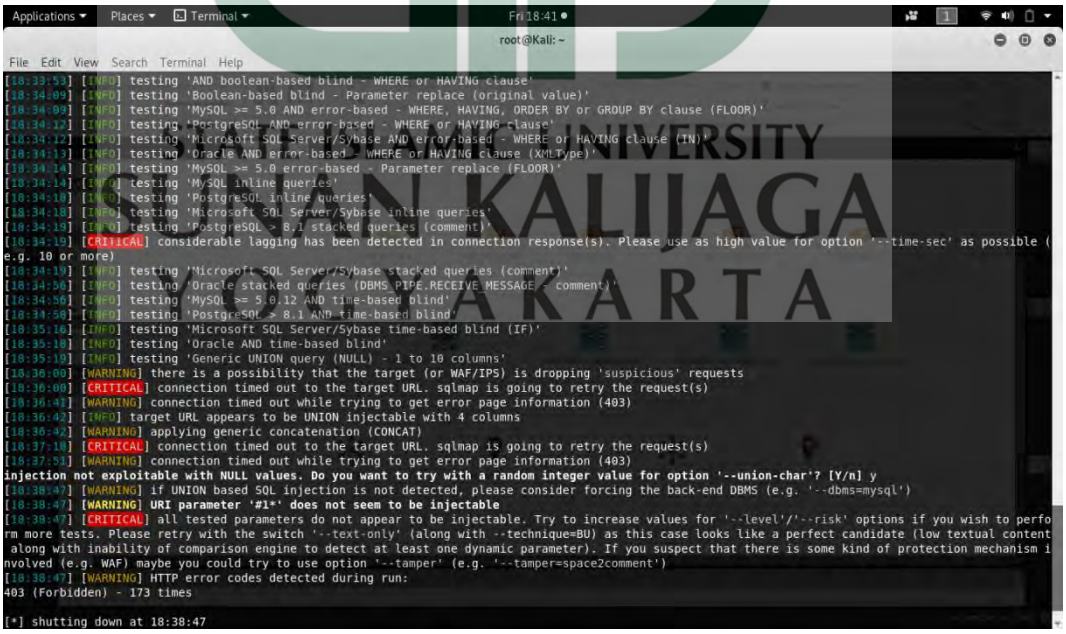
LAMPIRAN 7
HASIL SCANNING NIKTO



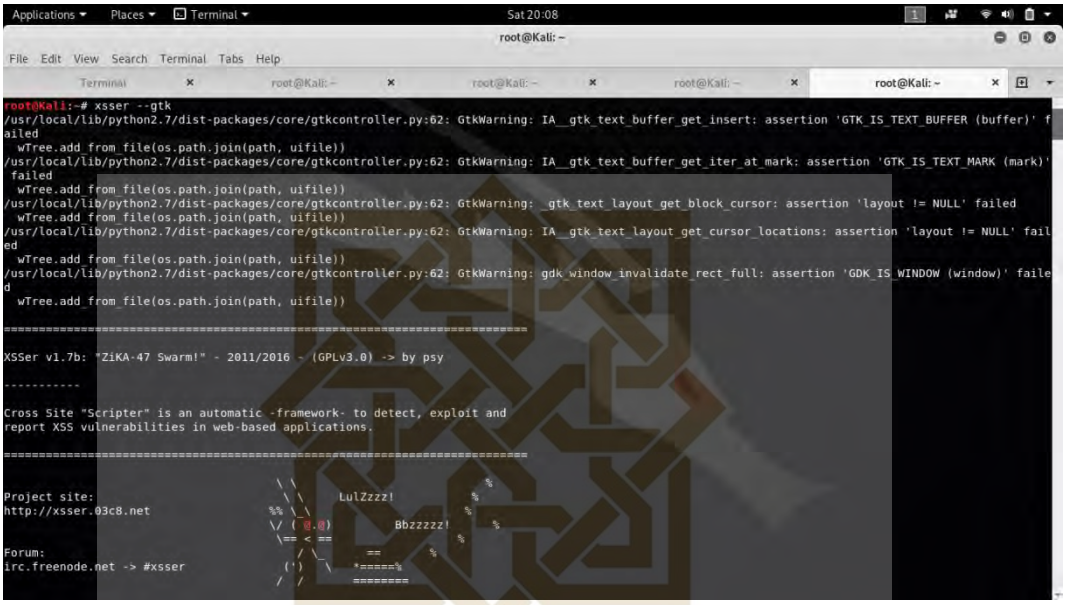


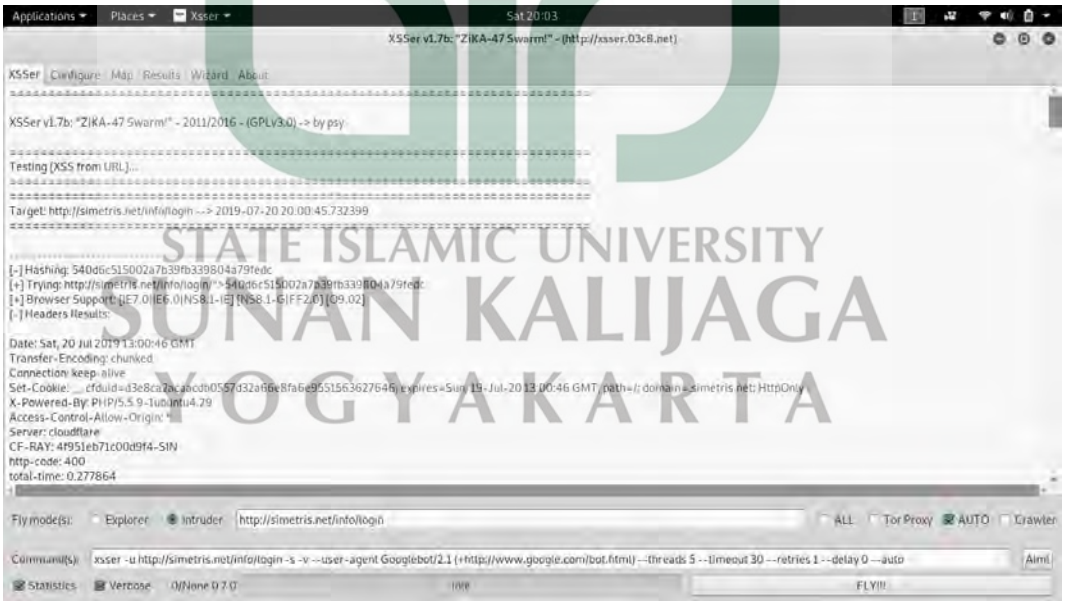
LAMPIRAN 8
HASIL SCANNING SQLMAP

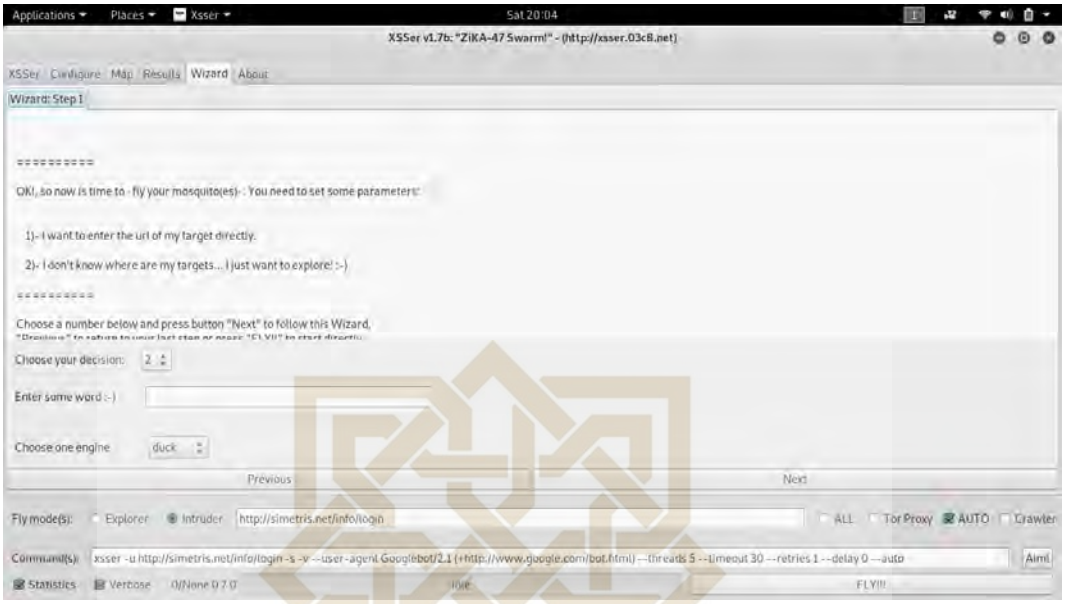


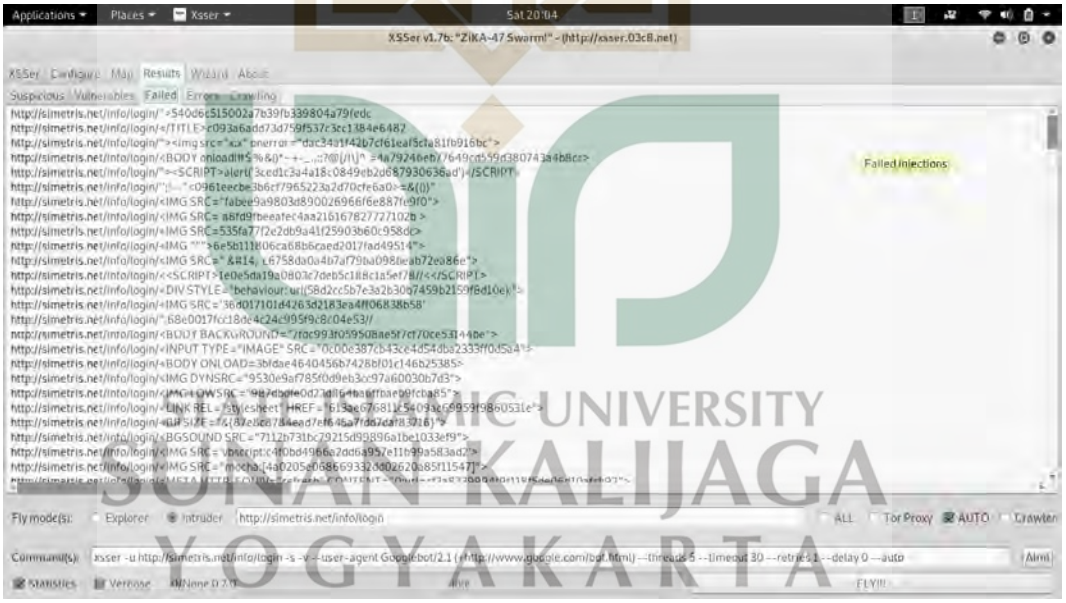


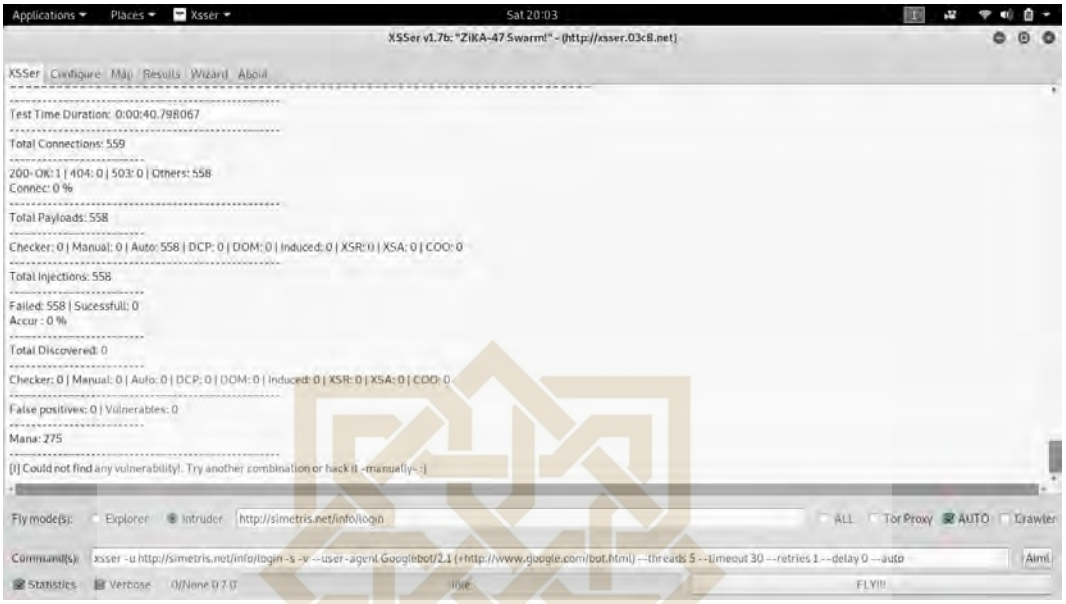
LAMPIRAN 9
HASIL SCANNING XSSER











LAMPIRAN 10
AUDIT CHARTER

Audit Charter

Project ID : ISO 27001 – Audit

Project Name : Audit Keamanan Sistem Informasi

Auditor : Sulton Daud Ul Mukarobin

Projecct Description :

Penelitian yang berkaitan dengan keamanan informasi ini menggunakan parameter ISO 27001. Penelitian ini berfokus pada klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses.

Project Schedule :

Stakeholder list :

Jabatan	Responden	Klausul Pengendalian
PJ SDM & MGMT	DEDI	Kebijakan keamanan, ISO 27001 A.5 (A.5.1)
PJ SARANA & PRASARANA T.I.	TRISNO	Pengelolaan aset, ISO 27001 A.7 (A.7.1 – A.7.2)
—	TRISNO	Keamanan fisik dan lingkungan, ISO 27001 A.9 (A.9.1 – A.9.2)
PJ ANALIS & INTEGRASI ANTAR SISTEM	AMIR	Manajemen komunikasi dan operasi, ISO 27001 A.10 (A.10.1 – A.10.5 – A.10.6)
PJ PRODUKSI SISTEM INFORMASI	DODY	Pengendalian akses, ISO 27001 A.11 (A.11.5)

Yogyakarta,

Mengetahui	Auditor
RSUP Dr. Sardjito Yogyakarta	Sulton Duad Ul Muarobin
M. DEDI ISKANDAR	
NIP : 19780129 200604 1001	NIM : 12650035

LAMPIRAN 11
KERTAS KERJA AUDIT

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi Terintegrasi
RSUP Dr Sardjito Yogyakarta
Standar ISO 27001

Document ID	:	INTERVIEW - 01
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Sulton Daud Ul Mukarobin
Audite	:	
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Terintegrasi Rumah Sakit RSUP Dr. Sardjito Yogyakarta
Date	:	
Responsible	:	

Approved by

Auditor

Sulton Daud Ul Mukarobin

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi Terintegrasi

Sistem Informasi Manajemen Terintegrasi RSUP Dr. Sardjito Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW - 02
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Sulton Daud Ul Mukarobin
Audite	:	
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengelolaan Aset yang diterapkan oleh pengelola Sistem Informasi Manajemen Terintegrasi Rumah Sakit RSUP Dr. Sardjito Yogyakarta
Date	:	
Responsible	:	

Approved by

Auditor

Sulton Daud Ul Mukarobin

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi Terintegrasi

Sistem Informasi Manajemen Terintegrasi RSUP Dr. Sardjito Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW - 03
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Sulton Daud Ul Mukarobin
Audite	:	
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Keamanan Fisik dan Lingkungan yang diterapkan oleh pengelola Sistem Informasi Manajemen Terintegrasi Rumah Sakit RSUP Dr. Sardjito Yogyakarta
Date	:	
Responsible	:	

Approved by

Auditor

Sulton Daud Ul Mukarobin

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi Terintegrasi

Sistem Informasi Manajemen Terintegrasi RSUP Dr. Sardjito Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW - 04
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Sulton Daud Ul Mukarobin
Audite	:	
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakartá Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Komunikasi dan Operasi yang diterapkan oleh pengelola Sistem Informasi Manajemen Terintegrasi Rumah Sakit RSUP Dr. Sardjito Yogyakarta
Date	:	
Responsible	:	

Approved by

Auditor

Sulton Daud Ul Mukarobin

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi Terintegrasi

Sistem Informasi Manajemen Terintegrasi RSUP Dr. Sardjito Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW - 05
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Sulton Daud Ul Mukarobin
Audite	:	
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengendalian Akses yang diterapkan oleh pengelola Sistem Informasi Manajemen Terintegrasi Rumah Sakit RSUP Dr. Sardjito Yogyakarta
Date	:	
Responsible	:	

Approved by

Auditor

Sulton Daud Ul Mukarobin

LAMPIRAN 12

LEMBAR QUESTIONER AUDIT

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 01
Klausul : Kebijakan Keamanan (A.5)

No	Code	Question	Answer	Score
1	Q1	Sudah adakah kebijakan keamanan informasi?	sudah	
2	Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?	sudah	
3	Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?	sudah	
4	Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?	sudah	
5	Q5	Apakah kebijakan tersebut sudah dikomunikasikan?	sudah.	
6	Q6	Apakah sudah dilakukan tinjauan ulang terhadap kebijakan keamanan informasi (untuk antisipasi perubahan yang mempengaruhi analisa resiko)?	sudah.	
7	Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?	ya	
8	Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?	ya	
9	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	ya	
10	Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	Kepala. Instalasi Teknologi Informasi	

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 02
Klausul : Pengelolaan Aset (A.7)

No	Code	Question	Answer	Score
1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?	Belum Semua.	
2	Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?	YA	
3	Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?	Sudah	
4	Q14	Apakah kebijakan pengelolaan inventaris aset tersebuh sudah didokumentasikan?	Sudah	
5	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?	Ada	
6	Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?	PJ Aset	
7	Q17	Apakah ada jangka waktu pengecekan inventaris aset secara berkala?	Belum	
8	Q18	Apakah sudah diidentifikasi nilai dan tingkat kepentingan aset?	Belum	
9	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?	Ya	
10	Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah di implementasikan?	Ya	
11	Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?	Ada	
12	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?	?	
13	Q23	Apakah ada prosedur yang baik berupa pemberi tanda pelabelan dan penanganan informasi?	Ada	
14	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?	Ya	

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 03
Klausul : Keamanan Fisik dan Lingkungan (A.9)

No	Code	Question	Answer	Score
1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?	Ya	
2	Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?	Ya	
3	Q27	Apakah ada kontrol akses fisik atau ruang / wilayah sebagai tempat menerima tamu?	Ya	
4	Q28	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?	Ya	
5	Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem informasi kearsipan statis?	Ya	
6	Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindung dari akses tanpa izin?	Ya	
7	Q31	Apakah pengunjung yang datang diawasi dan menulis tanggal datang dibuku tamu?	Tidak	
8	Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?	Ya	
9	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?	Iya	
10	Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?	Iya	
11	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?	Sudah	
12	Q36	Apakah bahan yang berbahaya dan mudah meledak sudah disimpan diwilayah aman?	Sudah	
13	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?	Sudah	
14	Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?	Ada	
15	Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?	Sudah	

16	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?	Sudah	
17	Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?	Sudah	
18	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?	Sudah	
19	Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau UPS?	Sudah	
20	Q44	Apakah utilitas pendukung seperti sumber daya listrik, genset, UPS selalu dicek keamanannya?	Sudah	
21	Q45	Apakah kabel daya dan telekomunikaasi kebutuna data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman?	Sudah	
22	Q46	Apakah peralatan Hardware selalu dijaga dan dipelihara dengan baik?	Ya	
23	Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?	Ada	
24	Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?	Ya	

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 04
Klausul : Manajemen Komunikasi dan Operasi (A.10)

No	Code	Question	Answer	Score
1	Q49	Apakah terdapat prosedur pengoperasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?	Ada	
2	Q50	Jika ada, apakah prosedur sudah di dokumentasikan dan tersedia bagi pengguna?	Ada	
3	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?	Ya	
4	Q52	Apakah setiap data penting dilakukan back-up?	Ya dan rutin dilakukan	
5	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan kepada pihak terkait?	Ya	
6	Q54	Apakah pegawai di ruang sistem informasi sudah dipisahkan menujrut tugas dan tanggung jawabnya masing-masing?	Sudah	
7	Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?	Ada	
8	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?	Iya	
9	Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?	Iya, dilakukan back-up real time	
10	Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?	Iya	
11	Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?	Sudah	
12	Q60	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?	Sudah	
13	Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?	Iya	

14	Q62	Sejauh ini, apahak terdapat titik jaringan yang rawan terhadap serangan?	Ada	
15	Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?	Ada	
16	Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?	Ada	
17	Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan?	Ada	

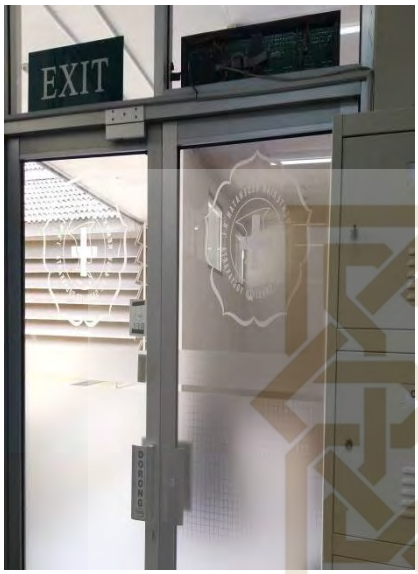
QUESTIONS OF INTERVIEW

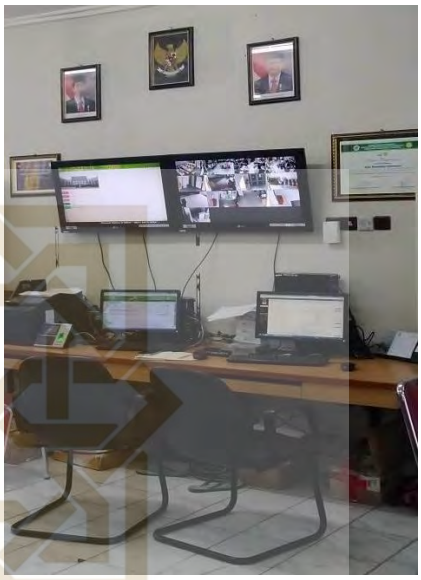
Document ID : INTERVIEW - 05
Klausul : Pengendalian Akses (A.11)

No	Code	Question	Answer	Score
1	Q66	Apakah sudah diterapkan prosedur log-in pada sistem informasi?	Sudah, akses sistem hanya dapat dilakukan oleh yg berhak	
2	Q67	Apakah sistem sudah membatasi kegagalan percobaan log-in?	Tidak dibatasi.	
3	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda?	Ya, semua pengguna memiliki ID masing-masing	
4	Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?	Ya, harus unik.	
5	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelolaan password untuk memastikan kualitas password?	Sudah ada.	
6	Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?	Ya, go han. (dapat disesuaikan waktunya)	
7	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?	ada.	
8	Q73	Apakah sudah menggunakan sesi time-out?	ada, tapi tidak diaktifkan.	

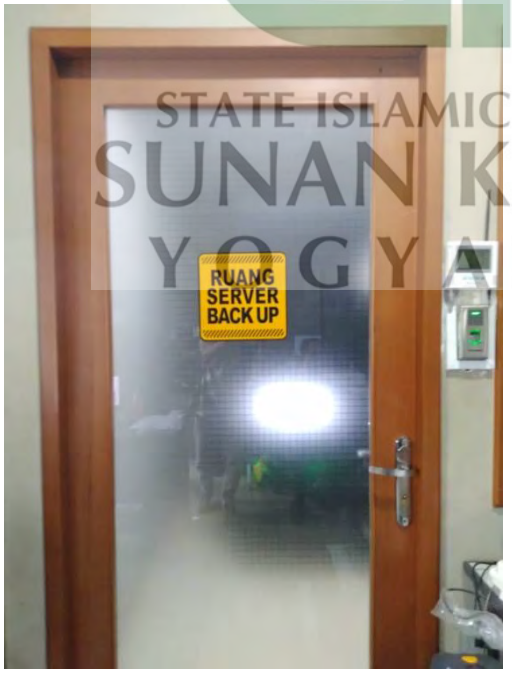
LAMPIRAN 13
RUANG SERVER UTAMA

LAMPIRAN 14
RUANG HELP DESK





LAMPIRAN 15
RUANG SERVER BACK UP



BIODATA

Nama : Sulton Daud Ul Mukarobin

Tempat Lahir : Yogyakarta

Tanggal Lahir : 04 Februari 1994

Golongan Darah : O

Agama : Islam

Kewarganegaraan : Indonesia

Alamat Asal : Jl. Mangkuyudan No. 21 RT 22/RW 06 Mantrijeron Yogyakarta

Email : sulton.mukarobin@gmail.com

No. HP : 085729615042

Riwayat Pendidikan :

2000-2006	SD Kertapawitan Jakarta Barat
2006-2009	SMP 2 Bantul
2009-2012	SMA Negeri 2 Yogyakarta
2012-2019	S1 Teknik Informatika. Universitas Islam Negeri Sunan Kalijaga Yogyakarta