Jurnal Infosecure Vol.2 No.1, April 2021
p-ISSN: 2087-1023
MTI-UNLA

Vulnerability Assessment Keamanan Jaringan Menggunakkan Standar NIST SP 800-115 dan ISO/IEC 27001

(Studi Kasus: Universitas Langlangbuana)

Ridwan

Magister Teknik Informatika, Universitas Langlangbuana

ridwan9a@gmail.com

Abstrak- Seiring dengan pesatnya perkembangan teknologi di era digital ini, ancaman kejahatan siber (cybercrime) semakin meningkat dan menjadi isu yang sangat krusial, terutama di institusi pendidikan yang mengelola informasi vital dan sensitif. Universitas Langlangbuana (UNLA) merupakan salah satu contoh perguruan tinggi yang telah menghadapi berbagai insiden peretasan yang merugikan, termasuk peristiwa serius di mana website resminya diubah menjadi situs judi online. Insiden tersebut tidak hanya mencederai reputasi universitas, tetapi juga menunjukkan adanya kerentanan signifikan dalam sistem keamanan jaringan yang ada, sehingga mendesak untuk dilakukan penilaian kerentanan dan langkah mitigasi yang efektif guna menjaga keamanan data serta integritas reputasi institusi. Penelitian ini bertujuan untuk melakukan penilaian kerentanan secara menyeluruh pada jaringan UNLA dengan menggunakan pendekatan yang berdasarkan standar *National Institute of Standards and Technology* (NIST SP 800-115) dan standar ISO/IEC 27001. Pendekatan ini dirancang untuk membantu mengidentifikasi, memperbaiki, dan memitigasi potensi celah keamanan yang ada. Dalam proses penelitian ini, beberapa alat analisis keamanan seperti Kali Linux, Nmap, dan Nessus digunakan untuk melakukan analisis mendalam terhadap jaringan, melakukan pemindaian port, serta mendeteksi berbagai kerentanan yang mungkin ada dalam sistem.
Implementasi kontrol keamanan yang diperlukan meliputi langkah-langkah untuk memperbarui perangkat lunak dan keras yang digunakan, serta memperkuat konfigurasi jaringan agar lebih aman. Dalam pengembangan topologi jaringan yang lebih aman, salah satu peningkatan utama yang direkomendasikan adalah penggunaan VLAN yang lebih terstruktur. Ini akan membantu dalam memisahkan jaringan tiap departemen atau unit, seperti Fakultas Teknik dan Fakultas Hukum, sehingga lalu lintas antar segmen jaringan lebih terkontrol. Selain itu, dua router firewall akan digunakan untuk memberikan perlindungan berlapis, memisahkan server publik dari server internal guna meminimalisir risiko ancaman. Router failover juga ditambahkan untuk memastikan ketersediaan jaringan tetap terjaga meskipun ada gangguan, menjamin operasional universitas berjalan tanpa hambatan.

Kata kunci- Keamanan jaringan, *cybercrime*, Universitas Langlangbuana, NIST SP 800-115, ISO/IEC 27001, penilaian kerentanan.

I. PENDAHULUAN

Di era teknologi yang semakin maju dan berkembang pesat, intensitas penggunaan teknologi komputer telah menjadi bagian integral dari kehidupan manusia (Astriani dkk., 2021). Dengan peningkatan kemampuan dan rasa ingin tahu manusia terhadap teknologi digital, muncul pula berbagai tantangan baru, termasuk ancaman kejahatan dunia maya (*cybercrime*) yang berkaitan erat dengan keamanan jaringan dan perlindungan informasi sebagai aset vital.

Informasi merupakan komponen penting dalam sistem informasi suatu instansi atau organisasi. Keandalan sistem keamanan jaringan sangat penting untuk menjaga validitas, integritas data, serta menjamin ketersediaan layanan bagi pengguna (Sanjaya dkk., 2020). Keamanan informasi mencakup beberapa aspek utama, yaitu confidentiality, integrity, dan availability (Rochmadi & Pasa, 2021). Oleh karena itu, menjaga keamanan sistem informasi menjadi fokus utama bagi setiap organisasi untuk mencegah berbagai serangan dan pencurian data, seperti peretasan pada server jaringan.

Universitas Langlangbuana (UNLA) menghadapi tantangan serius terkait keamanan jaringan, di mana website resminya sering menjadi target peretasan. Insiden peretasan ini telah menimbulkan kerugian material dan non-material yang signifikan, termasuk salah satu insiden mencolok di mana website UNLA diubah menjadi situs judi online. Kejadian-kejadian tersebut tidak hanya merusak reputasi universitas, tetapi juga mengancam privasi dan keamanan data civitas akademika. Hal ini menunjukkan adanya kelemahan dalam sistem keamanan jaringan UNLA yang memerlukan penanganan segera.

Keamanan informasi di perguruan tinggi diperkuat oleh Permendikbudristek No. 53 Tahun 2023 yang menekankan pentingnya menjaga keamanan, akurasi, dan integritas data akademik. Selain itu, Peraturan BSSN No. 8 Tahun 2020 mewajibkan Universitas Langlangbuana memiliki Sistem Manajemen Pengamanan Informasi untuk melindungi informasi penting. Ancaman siber yang semakin canggih memerlukan langkah proaktif, termasuk penilaian kerentanan pada jaringan lokal dan publik di UNLA. Jaringan lokal rentan terhadap kelemahan internal, sementara jaringan publik terkait kelemahan eksternal yang terhubung ke internet.

Kerentanan jaringan lokal UNLA mencakup kelemahan konfigurasi perangkat internal, sementara jaringan publik terancam oleh kelemahan server eksternal. *Cybercrime* dapat

terjadi kapan saja, terutama pada institusi yang mengabaikan sistem keamanan. Langkah awal untuk mengatasi peretasan adalah penilaian keamanan server. Keamanan jaringan meliputi *confidentiality*, *integrity*, *availability*, dan standar seperti NIST SP 800-115 serta ISO/IEC 27001, yang memandu penilaian kerentanan, penguatan kontrol, dan evaluasi berkelanjutan. UNLA perlu menerapkan langkah strategis untuk meningkatkan keamanan, seperti audit berkala dan pelatihan kesadaran keamanan.

Vulnerability Assessment terdiri dari beberapa tipe: *Network-based scans* (analisis potensi serangan jaringan), *Host-based scans* (identifikasi kerentanan pada server atau host), Wireless network scans (serangan infrastruktur *wireless*), *Application scans* (uji kerentanan pada website), dan *Database* scans (identifikasi kerentanan pada database, seperti SQL injection).

Gambar 1 *Vulnerability Assessment* (Comodo, 2019)

Tahapan dalam *Vulnerability Assessment* mencakup penyesuaian lingkup (menentukan batasan pengujian), enumerasi target (identifikasi topologi dan port terbuka), evaluasi server jaringan (menilai komponen jaringan dan risiko), serta evaluasi aplikasi (analisis aplikasi untuk kerentanan). Kerentanan dinilai dalam tiga level: High (tinggi, potensi ancaman besar), Medium (sedang, lokal dan dapat diatasi), dan Low (rendah, mudah ditangani dengan langkah pencegahan yang memadai).

Gambar 2. *NIST Cybersecurity Framework (University* South Carolina*)*

Kerangka ini terdiri dari lima fungsi utama yang saling terkait: Identifikasi (Identify), Lindungi (Protect), Deteksi (Detect), Respons (Respond), dan Pulihkan (Recover). Fungsi Identifikasi membantu organisasi mengenali dan menilai risiko terkait keamanan siber. Lindungi berfokus pada langkah pertahanan untuk melindungi aset dan data. Deteksi mempercepat identifikasi ancaman melalui pemantauan dan analisis anomali. Respons memastikan tindakan cepat dalam merespon serangan untuk meminimalisir dampak. Pulihkan mendukung pemulihan operasi normal setelah serangan, dengan fokus pada perbaikan berkelanjutan dan komunikasi efektif.

National Institute of Standards and Technology (NIST), yaitu suatu lembaga yang mempunyai misi untuk mempromosikan inovasi dan daya saing industri dengan memajukan standar teknologi (NIST, 2009). NIST telah banyak membuat standar penilaian salah satunya yang telah dibuat yaitu NIST SP 800-115. NIST SP 800-115 adalah standar mengenai technical guide to information security testing and assessment, yaitu sebagai pedoman untuk melakukan penilaian terhadap keamanan informasi.

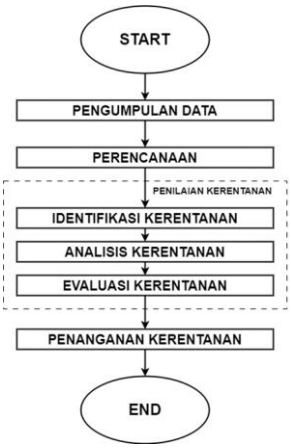
ISO/IEC 27001 adalah standar yang menetapkan persyaratan untuk pengembangan, implementasi, pemeliharaan, dan peningkatan berkelanjutan sistem manajemen keamanan informasi (SMKI) di dalam organisasi. Standar ini mencakup evaluasi dan manajemen risiko keamanan informasi yang disesuaikan dengan kebutuhan spesifik organisasi.

Tiga metrik dampak mengukur bagaimana kerentanan, jika dieksploitasi, secara langsung mempengaruhi aset TI. Dampak ini masing-masing didefinisikan sebagai banyaknya data yang hilang dalam hal kerahasiaan (*Confidentiality*, C), integritas (*Integrity*, I), dan ketersediaan (*Availability*, A).

Penelitian yang akan dilakukan berjudul "Vulnerability Assessment Keamanan Jaringan Menggunakan Framework NIST SP 800-115 dan ISO/IEC 27001" memiliki tujuan serupa dengan penelitian oleh Afif Saktiansyah dan Muhammad Muharrom, yaitu mengidentifikasi kerentanan jaringan dan memberikan rekomendasi mitigasi. Namun, perbedaannya terletak pada alat yang digunakan, di mana penelitian ini mengandalkan framework NIST SP 800-115 dan ISO/IEC 27001, serta alat tambahan seperti Wireshark, Nmap, dan Nessus, sementara penelitian sebelumnya menggunakan OpenVAS. Penelitian ini juga berfokus pada penerapan kontrol keamanan dan pengujian fungsionalitasnya di Universitas Langlangbuana, dengan lingkup yang terbatas pada jaringan lokal dan publik. Selain itu, *output* penelitian ini mencakup rekomendasi kontrol, implementasi, pengujian, dan peningkatan kesadaran praktik keamanan, berbeda dengan penelitian sebelumnya yang lebih fokus pada identifikasi dan analisis kerentanan.

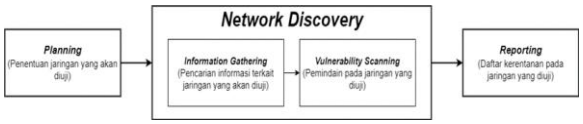
II. METODE

Metode dalam penelitian ini menggunakan standar NIST SP 800-115 dan ISO/IEC 27001. Tahapan penelitian disusun secara sistematis, di mana hasil dari setiap tahap menjadi dasar bagi langkah berikutnya, memastikan analisis dan solusi dilakukan secara komprehensif. Data dikumpulkan melalui metode wawancara dan observasi. Wawancara dilakukan dengan pihak yang memiliki pengetahuan terkait masalah yang diteliti untuk memperoleh informasi mendalam. Observasi dilakukan dengan mengamati langsung perangkat jaringan dan topologi yang digunakan di perusahaan untuk memahami kondisi aktual infrastruktur jaringan dan mengidentifikasi potensi masalah. Metode yang digunakan dalam penelitian ini adalah action research, yang bertujuan untuk menemukan solusi efektif dalam menghasilkan perubahan pada lingkungan yang dikendalikan.



Gambar *3*. Tahapan Penelitian

Proses identifikasi pada sistem jaringan digunakan beberapa *tools* untuk melakukan vulnerability scanning dengan mengikuti metode NIST SP 800-115.



Gambar 4. Vulnerability Scanning

Selain itu, dilakukan juga identifikasi aset, proses bisnis, ancaman, kontrol yang sudah ada, serta dampak yang mungkin terjadi terhadap komponen jaringan.

Tabel 1. Identifikasi Kerentanan Keamanan Sistem Jaringan

Input	Proses	Output
a. Kriteria kemungkinan kerentanan sistem keamanan jaringan b. Kriteria dampak kerentanan *c. Tools*	a) Wawancara b) Observasi c) *Vulnerability Scanning*	Daftar kerentanan keamanan sistem jaringan : a. Daftar aset b. Daftar Ancaman c. Daftar kontrol d. Daftar kerentanan

Proses identifikasi kerentanan keamanan jaringan dimulai dengan menetapkan kriteria kemungkinan dan dampak kerentanan. Data dikumpulkan melalui wawancara, observasi, dan pemindaian kerentanan. Outputnya adalah daftar aset, ancaman, kontrol, dan kerentanan. Identifikasi dilakukan pada sistem jaringan untuk mendeteksi celah keamanan, pada aset untuk menentukan perangkat penting, pada ancaman untuk mengevaluasi risiko yang mengancam jaringan, pada kontrol yang diterapkan, serta pada kerentanan sistem yang dapat dieksploitasi. Tujuan akhirnya adalah memahami dan memperbaiki kelemahan dalam infrastruktur jaringan.

Tahap berikutnya adalah analisis kerentanan. Dalam tahap ini, setiap kerentanan yang ditemukan dianalisis untuk menilai tingkat keparahan dan potensi dampak yang dapat ditimbulkan jika kerentanan tersebut dieksploitasi.

menggambarkan proses analisis kerentanan keamanan sistem jaringan. Tahapan pertama dimulai dengan input, yang mencakup beberapa elemen penting, seperti daftar aset yang berisi perangkat, aplikasi, data, dan sumber daya manusia yang terkait dengan jaringan.

Tabel 2. Analisis Kerentanan Keamanan Sistem Jaringan

Input	Proses	Output
Daftar kerentanan keamanan sistem jaringan: a. Daftar aset b. Daftar ancaman c. Daftar kontrol d. Daftar kerentanan	Analisis kerentanan keamanan sistem jaringan	Daftar penilaian kerentanan keamanan sistem jaringan

Evaluasi kerentanan menjadi langkah selanjutnya. Pada tahap ini, peneliti mengevaluasi hasil analisis kerentanan untuk menentukan risiko yang dapat diterima dan aksi kendali yang diperlukan.

Tabel 3. Evaluasi Kerentanan Keamanan Sistem Jaringan

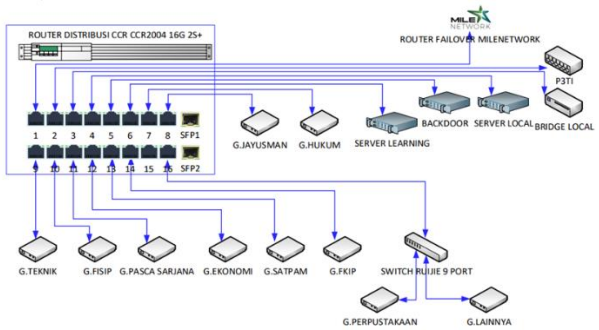
Input	Proses	Output
Daftar penilaian kerentanan keamanan sistem jaringan	Evaluasi kerentanan keamanan sistem jaringan	Daftar prioritas kerentanan

Hasil akhir atau output dari proses ini adalah daftar prioritas kerentanan, yang mengurutkan kerentanan-kerentanan tersebut berdasarkan tingkat atau nilai risiko kerentanan. Selanjutnya dilakukan perancangan dan pemilihan kontrol keamanan yang dipilih didasarkan pada annex A ISO/IEC 27001, yang menyediakan kontrol keamanan, serta mengacu pada ISO/IEC 27002 yang memberikan panduan terperinci untuk implementasi kontrol.

III. HASIL DAN PEMBAHASAN

A. Pengumpulan Data

Topologi adalah skema yang mengatur jaringan komputer dengan elemen-elemen seperti kabel dan komponen (PC, *hub*, *switch*, *router*, *bridge*) disusun secara sistematis sesuai jenis topologi yang digunakan, berikut ini merupakan topologi di Universitas Langlangbuana.



Gambar 5. Topologi Jaringan Utama di Universitas Langlangbuana

Topologi jaringan di Universitas Langlangbuana menggunakan sistem terdistribusi dengan router distribusi CCR2004 16G 2S+ sebagai pusat koneksi, yang terhubung ke berbagai switch dan server di seluruh kampus. Setiap perangkat dan server, seperti Server Lokal, Server Backdoor, dan Server Publik, memiliki alokasi bandwidth 1 Gbps untuk mendukung

operasional yang optimal. Jaringan ini mencakup koneksi ke gedung-gedung fakultas dan ruangan penting dengan switch khusus, serta Pos Satpam dan P3TI. Selain itu, router failover dan bridge lokal digunakan untuk memperkuat jaringan internal kampus.

Pusat Pengembangan dan Pelayanan Teknologi Informasi (P3TI) di Universitas Langlangbuana mengelola tata kelola sistem informasi dan jaringan, yang mencakup perangkat keras, perangkat lunak, dan jaringan serta mendukung berbagai pengguna termasuk pimpinan universitas, fakultas, dan mahasiswa. Meskipun menghadapi tantangan seperti keterbatasan anggaran dan ancaman siber, P3TI belum memiliki SOP formal untuk keamanan, melakukan penanganan masalah secara spontan, dan kekurangan dalam pengelolaan kerentanan yang sering kali dilakukan secara ad-hoc dan tidak tercatat secara formal. Kondisi ini menunjukkan kebutuhan mendesak untuk pembaruan dalam prosedur pencatatan, monitoring, dan penerapan standar keamanan.

B. Perencanaan

Universitas Langlangbuana berkomitmen untuk mengelola, menjaga, dan melindungi ruang lingkup penelitian ini meliputi : aset keamanan jaringan, termasuk perangkat keras, perangkat lunak, dan sumber daya manusia, dari berbagai kerentanan dan ancaman yang mungkin terjadi. Selanjutnya, menetapkan persiapan untuk melakukan identifikasi kerentanan pada sistem jaringan yang dijalankan sesuai dengan panduan yang ada pada NIST SP 800-115.

Tabel 4. Perangkat Keras untuk Proses Identifikasi Kerentanan

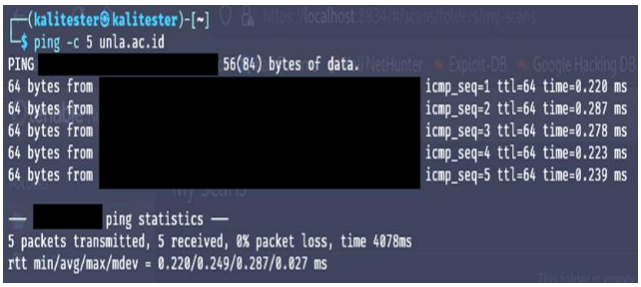
Komponen	Spesifikasi	
Komputer Desktop	*Processor*	Intel(R) Core(TM) i5-10400F CPU 2,90Ghz
	RAM	16 GB
	Storage	1 TB
	VGA	NVIDIA GeForce GTX 1650
	Operating System (OS)	Windows 11 Pro

Tabel 5. Perangkat Lunak Proses Identifikasi Kerentanan

Komponen	Perangkat Keras
Dual OS	Kali Linux
Information Gathering	Ping
	Whois
	SSLScan
Vulnerability Scanning	Nmap
	Nessus
Reporting	Microsoft Word

C. Identifikasi

Penilaian kerentanan (*vulnerability assessment*) proses sistematis yang bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi dalam suatu sistem keamanan jaringan. Langkah awal yag dilakukan yaitu *Discovery network*

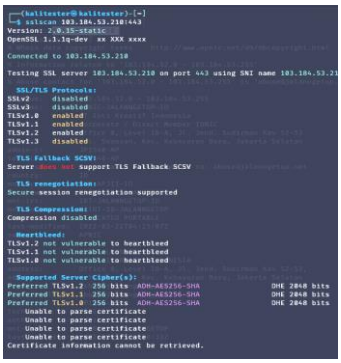


Gambar 6 Hasil Ping

Ping berhasil dilakukan dengan respons dari web server, menggunakan parameter -c 5 untuk membatasi jumlah ping, menunjukkan icmp_seq=5. TTL menunjukkan durasi paket data, sementara time menunjukkan waktu respons dalam milidetik, dengan ping yang baik di bawah 100 ms. Selain itu, bytes menunjukkan jumlah data yang dikirim. Whois digunakan untuk mencari informasi DNS dari IP Address target, dan hasilnya ditampilkan setelah menjalankan perintah whois "IP Address".

Gambar 7. Hasil *Whois*

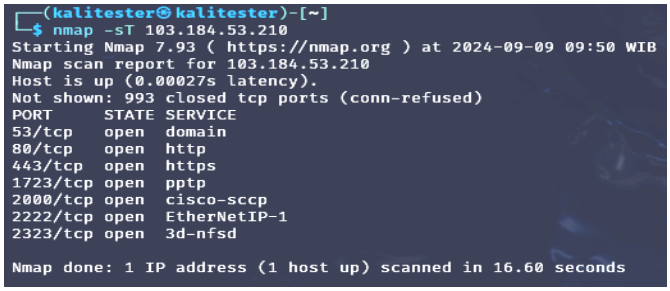
Proses berikutnya adalah melakukan pemindaian terhadap protokol keamanan SSL/TLS.



Gambar 8. Hasil SSLScan

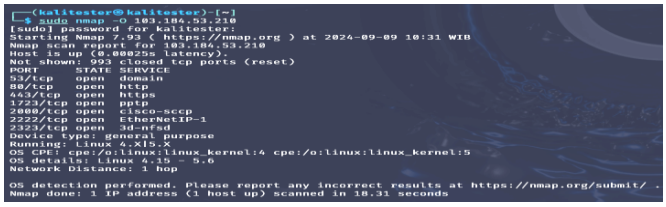
Hasil pemindaian menunjukkan bahwa meskipun server menggunakan protokol dan cipher modern seperti TLSv1.2 dan AES-256, kelemahan masih ditemukan, seperti dukungan untuk TLSv1.0, TLSv1.1, cipher suites ADH yang tidak aman, dan kurangnya sertifikat yang valid. Selain itu, server belum menggunakan HTTPS dan perlu memperbarui protokol ke TLSv1.3 untuk meningkatkan keamanan.

Pada tahap *vulnerability scanning* di mana dilakukan pemindaian terhadap target uji untuk mendeteksi apakah terdapat kerentanan pada sistem informasi yang diuji serta menilai tingkat keparahan dari kerentanan tersebut.



Gambar 9. Hasil Scan TCP Nmap

Hasil pemindaian menggunakan parameter nmap -sU menunjukkan daftar port UDP yang terbuka, salah satunya adalah port isakmp dan L2TP. Port 67, 68, 161 dan 4500 terlihat tertutup atau terfilter.

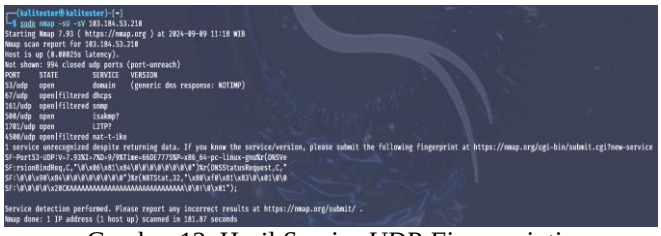


Gambar 10. Hasil Fingerprinting Sistem Operasi

Gambar 11. Hasil Service TCP Fingerprinting

Hasil pemindaian nmap menunjukkan beberapa port penting terbuka, termasuk port 53 (DNS), port 80 (HTTP)

dengan server web nginx versi 1.26.2, port 443 (HTTPS), port 1723 (PPTP), port 2000 (MikroTik bandwidth-test server), dan port 22 (SSH dengan MikroTik RouterOS). Port 23 (telnet) juga terbuka dan terkait dengan sistem operasi Linux, sementara pemindaian UDP akan dilakukan selanjutnya.



Gambar 12. Hasil *Service UDP Fingerprinting*

Hasil scan Nmap menunjukkan host aktif dengan beberapa layanan penting seperti DNS di port 53/UDP yang mengalami kesalahan respon, ISAKMP di port 500/UDP dan L2TP di port 1701/UDP yang mendukung VPN dan IPsec, serta port 4500/UDP yang mendukung NAT Traversal untuk IPsec. Port 67/UDP terfilter, dengan indikasi masalah pada konfigurasi DNS.

Tabel 6. Hasil Scan Port Terbuka Menggunakan NMAP

No	Port	Protocol	Service	Keterangan
1	53	TCP dan UDP	Domain	Digunakan untuk DNS (Domain Name System), yang mengubah nama domain menjadi alamat IP dan sebaliknya
2	80	TCP	HTTP	Protokol standar untuk mengakses halaman web (Hypertext Transfer Protocol).
3	443	TCP	HTTPS	Protokol HTTP yang diamankan dengan enkripsi SSL/TLS.
4	1723	TCP	PPTP	Digunakan untuk VPN berbasis PPTP (Point-to-Point Tunneling Protocol)
5	2000	TCP	Cisco-sccp	Digunakan oleh Cisco SCCP (Skinny Client Control Protocol) untuk perangkat telekomunikasi VoIP
6	2222	TCP	EtherhNetIP-1	Digunakan untuk komunikasi jaringan EtherNet/IP
7	2323	TCP	3d-nfsd	Digunakan oleh 3D-NFS daemon (layanan berbagi file network)
8	500	UDP	Isakmp	Digunakan oleh ISAKMP (Internet Security Association and Key Management Protocol) dalam VPN
9	1701	UDP	L2TP	Protokol tunneling untuk VPN (Layer 2 Tunneling Protocol).

Hasil pemindaian NMAP menunjukkan 9 port TCP dan UDP terbuka dengan fungsi beragam. Tahap berikutnya adalah pemindaian kerentanan menggunakan Nessus pada 10 September 2024 dari pukul 18.23 hingga 18.28 melalui metode Black Box testing dari luar jaringan Universitas Langlangbuana, yang mencakup semua kerentanan yang terdeteksi.

Gambar 12. Hasil *Vulnerability Scanning* Menggunakan Nessus

Hasil pemindaian terhadap host IP menunjukkan 1 kerentanan High yang berisiko tinggi, 5 kerentanan Medium yang perlu perhatian, 4 kerentanan Low dengan dampak kecil, dan 42 kerentanan None atau Info yang tidak signifikan terhadap sistem keamanan.

Hasil pemindaian Nessus menunjukkan berbagai kerentanan, termasuk ancaman high seperti DNS Server Spoofed Request Amplification DDoS, serta ancaman medium terkait protokol usang dan risiko serangan MitM, yang dapat mengancam ketersediaan layanan dan keamanan data.

Identifikasi aset di Universitas Langlangbuana mencakup perangkat keras, perangkat lunak, data, dan sumber daya manusia yang mendukung operasional teknologi informasi; ancaman terhadap aset termasuk serangan siber dan fisik, dengan kontrol keamanan diterapkan untuk melindungi aset, meskipun masih ditemukan beberapa kerentanan yang memerlukan perhatian terkait akses, pemeliharaan, dan kebijakan keamanan data.

Analisis ini menilai risiko kerentanan sistem informasi dengan mempertimbangkan dampak dan kemungkinan ancaman. Dampak bervariasi dari rendah hingga sangat tinggi, termasuk serangan DDoS, pencurian data, dan serangan brute force. Probabilitas ancaman juga dievaluasi, menyoroti risiko tinggi pada server, router, dan perangkat jaringan karena autentikasi lemah dan kurangnya pemeliharaan. Hasil analisis risiko menunjukkan bahwa banyak komponen sistem memiliki risiko tinggi hingga sangat tinggi, terutama karena konfigurasi default, akses tidak aman, dan kurangnya pemantauan aktivitas.

D. Evaluasi

Dari evaluasi risiko kerentanan, risiko dikelompokkan dalam empat kategori:

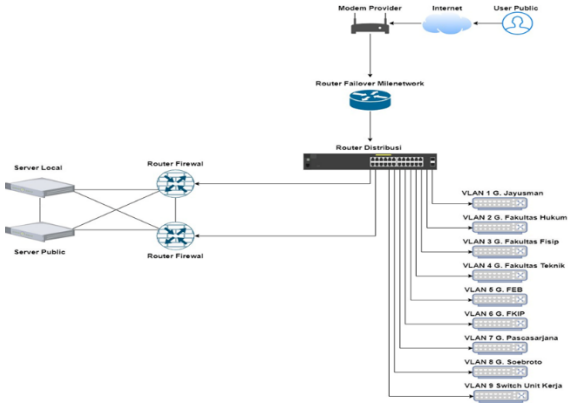
1. Risiko Rendah: Seperti V5, V13, hingga V158. Risiko ini diabaikan, tetapi tetap dipantau secara berkala.
2. Risiko Menengah: Seperti V1, V9, hingga V160. Risiko ini diterima dengan mitigasi menggunakan sumber daya yang tersedia agar tidak berkembang.
3. Risiko Tinggi: Seperti V2, V3, hingga V154. Diterima dengan mitigasi lebih intensif, mungkin memerlukan sumber daya tambahan.
4. Risiko Sangat Tinggi: Seperti V6, V10, hingga V162. Tidak dapat diterima dan harus segera diatasi atau dialihkan untuk mencegah dampak besar.

E. Penanganan Kerentanan

Pada tahap Penanganan Kerentanan, dilakukan perancangan dan implementasi langkah-langkah mitigasi risiko berdasarkan evaluasi sebelumnya. Langkah ini melibatkan pemilihan kontrol keamanan yang terdiri dari kontrol administratif (seperti kebijakan, prosedur, dan pemantauan), teknis (seperti firewall, enkripsi, dan otentikasi multifaktor), fisik (akses terbatas melalui kunci elektronik dan CCTV), serta kontrol terkait orang (seperti pemeriksaan latar belakang karyawan dan pelatihan keamanan). Semua kontrol ini merujuk pada standar ISO/IEC 27001:2022 untuk melindungi aset informasi dan sistem dari ancaman seperti serangan DoS dan MITM. Selain itu, rencana implementasi mengikuti pedoman tersebut untuk memastikan kepatuhan terhadap regulasi dan persyaratan hukum yang berlaku.

Kontrol yang dipilih mencakup tindakan sistematis dan berkelanjutan untuk menjaga keamanan informasi, sesuai dengan ISO/IEC 27002:2022. Kontrol organisasi menekankan kebijakan keamanan yang disetujui manajemen dan komunikasi yang efektif kepada seluruh personel, serta perlindungan informasi melalui enkripsi dan pengelolaan akses yang ketat. Kontrol orang mencakup proses disiplin dan NDA untuk menangani pelanggaran kebijakan. Kontrol fisik memastikan pemeliharaan peralatan dan keamanan informasi. Kontrol teknis melibatkan pengelolaan hak akses, pengawasan penggunaan kode sumber, pemantauan kerentanan, dan penerapan autentikasi yang aman. Seluruh kontrol ini bertujuan untuk melindungi informasi dari ancaman dan memastikan kepatuhan terhadap standar internasional.

Rencana topologi jaringan yang diusulkan menawarkan peningkatan dalam segmentasi, keamanan, dan manajemen lalu lintas. Penggunaan VLAN yang terstruktur memungkinkan segmentasi yang lebih baik, memisahkan jaringan tiap departemen untuk efisiensi dan kemudahan pengelolaan. Keamanan ditingkatkan dengan dua router firewall yang memisahkan server publik dan internal, mengurangi risiko penetrasi dan kebocoran data. Fitur router failover memastikan redundansi, menjaga ketersediaan jaringan meskipun terjadi gangguan. Topologi ini dirancang untuk mendukung operasional harian dengan infrastruktur yang efisien, aman, dan mudah dikelola, terutama untuk institusi akademik besar.



Gambar 13. Rencana Pengembangan Topologi Jaringan

IV. SIMPULAN

Dari penelitian ini menjawab perumusan masalah yang telah ditentukan sebelumnya berdasarkan hasil yang diperoleh. Vulnerability assessment yang dilakukan menghasilkan 162 risiko kerentanan, dengan rincian 64 risiko pada level sangat tinggi, 49 risiko pada level tinggi, 21 risiko pada level menengah, dan 28 risiko pada level rendah. Berdasarkan prioritas risiko yang paling kritis, yaitu pada level sangat tinggi, diterapkan 35 kontrol keamanan yang sesuai dengan standar ISO/IEC 27001. Tindakan implementasi selanjutnya dirancang berdasarkan ISO/IEC 27002, serta analisis topologi jaringan yang diusulkan bertujuan untuk meningkatkan efisiensi, keamanan, dan manajemen lalu lintas di Universitas Langlangbuana, dengan mempertimbangkan evaluasi jaringan yang ada dan kebutuhan masing-masing departemen.

REFERENSI

[1] Assetthread. (2024). *Reduce Security Risks with Effective IT Asset Management: A Comprehensive Guide.*
[2] Badan Siber Dan Sandi Negara, 'Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik, 2020.
[3] Baloch, R., 2014, *Ethical Hacking and Penetration Testing Guide*, New York.
[4] Buana, B. S. S., & Rijal, S. (2021). Kekerasan Terhadap Pers Melalui Serangan Siber: Studi Kasus Pada Media Online Tempo.Co. Jurnal Studi Jurnalistik, 3(2). https://repository.uinjkt.ac.id/dspace/handle/123456789/55926
[5] Chouffani, R. (2022). IT asset management (ITAM).
[6] Cisco. (2016). *What Is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity. (Accessed: 16 Agustus 2024)

[7] Comodo. (n.d.). *Types of vulnerability assessments*. *Retrieved from* https://www.comodo.com
[8] First (2021) *Common Vulnerability Scoring System v3.0: User Guide, first.org. Available* at: https://www.first.org/cvss/v3.0/user-guide (Accessed: Maret 2024).
[9] Goel, J. N., & Mehtre, B. M. (2015*). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science*, 57, 710 715. https://doi.org/10.1016/j.procs.2015.07.458
[10] Gov-CSIRT(n.d), *Standard Operational Procedure Incident Handling Network*, Gov-CSIRT diambil dari Kementerian Komunikasi dan Informatika, site : govcsirt.kominfo.go.id/download/SOP/SOP%20IH_Network.pdf
[11] GovCSIRT. (2012). *Methodology Vulnerability Assesment. [online]. Available at*: https://govcsirt.kominfo.go.id/254/ (Diakses: 20 Mei 2019)
[12] Guritno, S., & Rahardja, U. (2011). Theory and Application of IT Research: Metodologi Penelitian Teknologi Informasi. Penerbit Andi.
[13] H. Nugroho, "Analisis Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1," Konf. Nas. ICT-M Politek. Telkom, 2012.
[14] Habib Ahmad Purba. (2010). Jenis-Jenis Server dan Fungsinya. https://habibahmadpurba.wordpress.com/2013/07/10/jenis-jenis-server-danfungsinya/
[15] IBM. (2022). *What Is IT Asset Management* (ITAM)?
[16] Iffano, S. dan Riyanarto (2009) Sistem Manajemen Keamanan Informasi berbasis ISO 27001. Surabaya: ITS Press.
[17] Imperva. (2022). *Vulnerability Assessment. Retrieved January 9*, 2023, from Imperva website: https://www.imperva.com/learn/application-security/vulnerability-assessment/. (Accessed: 16 Agustus 2024)
[18] ISO - ISO/IEC 27000 – key International Standard for information security revised." https://www.iso.org/news/ref2266.html (accessed Juni, 2024)
[19] ISO - ISO/IEC 27001 — Information security management." https://www.iso.org/isoiec-27001-information-security.html (accessed Juni, 2024).
[20] ISO - ISO/IEC 27001: 2022 - *Information technology — Security techniques — Information security management systems — Requirements*." https://www.iso.org/standard/54534.html (accessed Juni, 2024).
[21] ISO/IEC 27002:2005 (2007) Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005 - Final Draft. ISO/IEC JTC 1.
[22] ISO/IEC27002 (2013) ISO/IEC 27002:2013 - *Information Technology - Security Techniques - Code of Practice for Information Security Controls.*
[23] Manuaba, I. B. V. H., Hidayat, R., & Kusumawardani, S. S. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas. Jnteti, 1(1), 5. https://doi.org/10.22146/JNTET I.V1I1.3
[24] Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia, 'Salinan Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 53 Tahun 2023 Tentang Penjaminan Mutu Pendidikan Tinggi', 2023
[25] Mohamad, A., & Musa, P. (2020*). Designing Software Define Network Prototypes with Open vSwitch as Monitoring Traffic Police on The Raspberry* Pi. Avitec, 2(2), 103–109. https://doi.org/10.28989/avitec.v2i2.712.
[26] *National Institute of Standards and Technology* (NIST). (2020). *NIST Special Publication* 800-115, *Technical Guide to Information Security Testing and Assessment.*
[27] NIST SP 800-115. (2021) *Technical Guide to Information Security Testing and Assessment.* https://www.nist.gov/privacy-framework/nist-sp-800-115. guide (Accessed: 10 Maret 2024).
[28] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. The National Institute of Standards and Technology*. United States. https://doi.org/10.6028/NIST.CSWP.04162018
[29] Octariza, N. F. (2019). Analisis sistem manajemen keamanan informasi menggunakan standar iso/Iec 27001 dan iso/lec 27002 pada kantor pusat pt jasa mar (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).
[30] Panuntun, A. A. B. (2016). Analisis Penggunaan Openvas Untuk *Vulnerability Assessment* (Doctoral dissertation, UII).
[31] Paryati (2008) 'Keamanan sistem informasi', 2008(Jurusan Teknik Informatika UPN 'Veteran' Yogyakarta), pp. 379–386.
[32] Permatasari, R. (2016). Analisa Hasil Penetration Testing Sistem Keamanan Web Dengan Menggunakan Metode Issaf (Study Kasus: UIN Jakarta).
[33] Rao dan Nayak. (2014). *The InfoSec Handbook An Introduction to Information Security.* Apress Open.
[34] Rochmadi, T., & Pasa, I. Y. (2021) Menggunakan Indeks Keamanan Informasi di Bkd Xyz *Measurement of Risk and Evaluation of Information Security Using the Information Security Indeks in Bkd Based on ISO 27001 / Sni*. 4(1), 38-43).
[35] Sanjaya, I. G. A. S., Sasmita, G. M. A. & Arsya, D. M. S. (2020) Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Peneitian Akademika Teknologi Informasi)*, 8(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05
[36] Sergio Marphy Junan Lawalata. 2020. "Perancangan Wireless Intrusion DetectionSystem Pada Jaringan WI-FI Berbasis Threats Dan Vulnerabilities Assessment", Tesis. Teknik. Teknik Elektro. Institut Teknologi Bandung.
[37] Waliullah, M., & Gan, D. (2014). *Wireless LAN Security Threats &. Vulnerabilities. International Journal of Advanced Computer Science and. Applications*, 5(1), 176.