ISSN : 1411-1624
e-ISSN: 2621-8089

ANALISIS MANAJEMEN RISIKO KEAMANAN JARINGAN MENGGUNAKAN *FRAMEWORK* NIST

Febriyanti Panjaitan[1], Aldrison Aprilo[2*]
Universitas Bina Darma [1, 2]
Jalan Jenderal Ahmad Yani No.3 Palembang
Sur-el: febriyanti_panjaitan@binadarma.ac.id[1], aldrisonaprilo@gmail.com[2]

Abstract : *The security of a computer network is very important for a computer network, because if something happens it can be used for attacks or intrusions into the computer network. Therefore, it is necessary to guarantee network security, a network (system) in order to create services that provide comfort and trust to users of these services, especially when LANs connected to the Internet will become increasingly important. The importance of this research is to reduce threats that impact negative impact on information security systems, thereby reducing the impact of information system failures and minimizing risks that may arise. In addition, network security system analysis is performed using the NIST (National Institute of Standards Technology) Framework, a framework designed for qualitative calculations based on security system analysis. A network security risk analysis of a banking company was successfully carried out using the NIST SP800-30 framework and it was found that the existing network security systems such as backdoors that have a low risk level, packet sniffing, spoofing and rookies are moderate, and Ddos has a high risk..*

Keywords: *Analysis, Security, Network, NIST Framework*

Abstrak : *Keamanan suatu jaringan komputer sangat penting bagi suatu jaringan komputer, karena jika terjadi sesuatu maka dapat dimanfaatkan serangan atau penyusupan ke dalam jaringan komputer tersebut. Oleh karena itu, perlu adanya jaminan keamanan jaringan, suatu jaringan (sistem) agar tercipta layanan yang memberikan kenyamanan dan kepercayaan kepada pengguna layanan tersebut, terutama pada saat LAN terhubung ke Internet akan menjadi semakin penting.. Pentingnya penelitian ini adalah untuk mengurangi ancaman yang berdampak negatif pada sistem keamanan informasi, sehingga mengurangi dampak kegagalan sistem informasi dan meminimalkan risiko yang mungkin timbul. Selain itu, analisis sistem keamanan jaringan dilakukan dengan menggunakan Framework NIST (National Institute of Standards Technology), kerangka kerja yang dirancang untuk perhitungan kualitatif berdasarkan analisis sistem keamanan. Analsis risiko keamanan jaringan salah satu perusahaan perbankan berhasil dilakukan dengan menggunakan framework NIST SP800-30 dan ditemukan bahwa sistem keamanan jaringan yang telah berjalan selama ini terdapat seperti backdoor yang memiliki tingkat risiko rendah, packet snifing, spoofing dan rookit sedang, dan Ddos memiliki tingkat risiko yang tinggi.*

Kata kunci*: Analisis, Keamanan, Jaringan, Framework NIST*

1. PENDAHULUAN

Penggunaan Teknologi pada perusahaan yang mulai berkembang pesat harus mulai berpikir untuk melindungi semua aset sistem informasi pada era industri 4.0. Melindungi kegiatan-kegiatan operasional dari serangan cyber pada keamanan jaringan komputer menjadi tanggung jawab yang besar, yang harus dilakukan perusahaan. Banyak risiko yang akan dihadapi mulai dari segi ekonomi, operasional dan teknologi yang harus diperhitungkan.

Keamanan jaringan memiliki kelemahan-kelemahan yang jika tidak dilindungi dan dijaga dengan baik maka akan menyebabkan kerugian berupa risiko data loss, kerusakan sistem server,

ISSN : 1411-1624
e-ISSN: 2621-8089

tidak maksimal service nya dan kehilangan objek vital instansi baik perusahaan, organisasi maupun akademisi [1][2]**.**

Salah satu perusahaan dibidang perbankan yang memiliki tujuan untuk selalu mengutamakan kepuasan nasabah dan selalu menjadi agar sistem keamanan jaringan tetap terjaga dan tidak terganggu bahkan sampai rusak oleh serangan penyusup, maka perlu dilakukan analisa manajemen risiko keamanan jaringan sehingga perusahaan dapat memiliki kemampuan untuk memahami posisi keamanan teknologi informasi yang sedang berjalan saat ini.

Manajemen risiko yang digunakan beberapa peneliti [3][4][5][6][7][8][9] untuk meningkatkan sistem teknologi informasi untuk menganalisis jaringan adalah framework NIST. Pada penelitian [3] menggunakan NIST sebagai metode yang digunakan untuk menyelesaikan permasalahan sistem informasi yang berkaitan dengan celah kerawanan keamanan informasi pada universitas XYZ terutama pada sistem informasi yang berhubungan dengan civitas akademika. Kemudian pada penelitian [4] menggunakan framework NIST sebagai salah satu panduan dalam Manajemen Risiko untuk meningkatkan sistem teknologi informasi kritis sehingga perusahaam memiliki kemampuan dalam memahami posisi keamanan teknologi informasi dan sistem informasi yang ada, sedangkan pada [9] melakukan analisis manajemen risiko pada sistem informasi, penilaian tingkat risiko meliputi sumber daya manusia memiliki tingkat risiko tinggi, kata sandi memiliki tingkat risiko sedang, serta listik dan jaringan internet memiliki tingkat risiko rendah. Masalah kemanan informasi dapat mempengaruhi operasional di suatu organisasi. Resiko yang timbul dapat berakibat proses bisnis tidak optimal, kerugian finansial, berkurangnya kepercayaan pelanggan, menurunnya reputasi dan yang paling buruk adalah hancurnya bisnis perusahaan, ada 3 jenis gangguan hasil analisis akses keamanan jaringan Lapan yaitu *no matching connection, flooding* dan *port scanning* [11]. NIST CSF dan ISO 27001 memiliki fungsi yang sama yaitu fokus terhadap keamanan informasi dan berbasis manajemen risiko [12], Standar NIST digunakan sebagai acuan melakukan manajemen risiko, mengantisipasi risiko agar kerugian tidak terjadi terhadap organisasi sehingga risiko dapat dikelola ke level yang dapat diterima organisasi [13], Metode *National Institute of Standards and Technology* (NIST) mempermudah dalam menemukan barang bukti kejahatan digital.

*Framework N*IST *(National Institute Standard Technology)* adalah *framework* yang dirancang untuk menjadi sesuatu perhitungan kualitatif dan didasarkan pada analisis sistem keamanan yang cukup sesuai dengan keinginan pengguna dan ahli teknik untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem teknologi informasi. NIST memiliki 9 tahapan, yaitu *System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations dan Results Documentation.* [14] Kerangka kerja NIST dapat meningkatkan kemampuan sebuah institusi dalam mengatasi pemasalahan keamanan komputer, baik saat ini maupun masa yang akan datang

ISSN : 1411-1624
e-ISSN: 2621-8089

2. METODOLOGI PENELITIAN

Penelitian tentang sistem keamanan jaringan ini menggunakan teknik analisis kualitatif, dan pada dasarnya merupakan penelitian eksploratif artinya penelitian dilakukan dengan cara menggali informasi tentang pengelolaan keamanan informasi di PT BRI (Persero) Tbk, KCP Sudirman Palembang, dan hasil penelitian disampaikan dalam bentuk deskripsi yang bersifat kualitatif.

Teknik analisis kualitatif menggunakan observasi dan wawancara langsung untuk mengetahui *software, hardware*, infrastruktur jaringan dan ancaman ancamann pada sistem keamanan jaringan di PT. BRI (Persero) Tbk, KCP Sudirman Palembang. untuk menjawab dan menjelaskan perumusan masalah mengetahui kelola sistem keamanan jaringan internet di PT. BRI (Persero) Tbk, KCP Sudirman Palembang menggunakan *framework* NIST.

2.1 *Framework* NIST

Framework NIST adalah *framework* yang dirancang untuk menjadi sesuatu perhitungan kualitatif dan didasarkan pada analisis sistem keamanan yang cukup sesuai dengan keinginan pengguna dan ahli teknik untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem teknologi informasi. *Framework* NIST SP 800-30 merupakan panduan untuk memproses data yang sangat sensitif. Proses penilaian risiko (*risk assessment*) dilakukan dengan beberapa tahapan, sesuai dengan Proses penilaian risiko (*risk assessmen*t) dilakukan dengan beberapa tahapan, sesuai dengan kerangka kerja NIST SP 800-30. Tahapan-tahapan sebagai berikut [15]

1) *System Characterization*.

Tahapan ini melihat dari aspek aspek seperti hardware, software, interface, data serta karakteristik jaringan , dan lain-lain.

2) *Threat Identification.*

Tahapan ini mengenali berbagai sumber yang akan memungkinkan menjadi gangguan pada sistem, seperti apa saja ancaman ancaman yang akan terjadi.

3) *Vulnerability Identification.*

Pada tahapan ini diidentifikasi berbagai kelemahan atau kekurangan dari sistem yang kemungkinan menjadi ancaman terhadap sistem.

4) *Control Analysis.*

Tujuan utama dari tahap ini untuk menganalisis kontrol yang telah diterapkan dan yang akan diterapkan, untuk mengurangi kemungkinan terjadinya ancaman.

5) *Likelihood Determination.*

Digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi atas kelemahan dari sistem.

Tabel 1. Tingkat Kemungkinan

Tingkat Kemungkian	***Definisi Kemungkinan***
Tinggi	Tingkat/Motivasi Ancaman sangat tinggi dimana pengendalian terhadap kemungkinan kelemahan sistem tidak dapat diatasi/tidak efektif
Sedang	Tingkat/Motivasi Ancaman cukup tinggi, pengendalian terhadap beberapa kelemahan sistem masih belum dapat diatasi
Rendah	Tingkat ancaman sangat rendah, dimana pengendalian kelemahan sistem secara umum dapat diatasi.

ISSN : 1411-1624
e-ISSN: 2621-8089

6) *Impact Analysis.*

Pada tahapan ini adalah untuk Menilai dampak yang terjadi terhadap serangan Berdasarkan penentuan kemungkinan risiko yang mengancam sistem informasi.

Tabel 2. Tingkat Dampak

Tingkat Dampak	*Definisi Dampak*
Tinggi	1. Dapat mengakibatkan kerugian yang sangat mahal dari banyak aset berwujud. 2. Dapat menganggu misi dan reputasi organisasi. 3. Dapat mengakibatkan kerusakan sistem yang besar
Sedang	1. Dapat mengakibatkan kerugian dari banyak aset berwujud. 2. Dapat menganggu misi dan reputasi organisasi. 3. Dapat mengakibatkan kerusakan sistem yang ringan
Rendah	Dapat mengakibatkan kerugian dari beberapa aset berwujud

7) *Risk Determination*.

Tujuan pada tahapan ini yaitu Penentuan risiko ini untuk menilai tingkat risiko terhadap sistem, penilaian ini mengacu pada kemungkinan risiko dan dampak risiko yang telah ditentukan. Pada NIST SP800-30 untuk penentuan risiko yang diharapkan dapat mengetahui tingkat prioritas risiko dalam sistem TI, menggunakan matriks 3 x 3 seperti pada Gambar 1 dengan kemungkinan ancaman (tinggi, sedang, dan rendah) dan dampak ancaman (tinggi, sedang, rendah).

Tabel 3. Matriks Tingkat Risiko

Threat Likelihood	*Impact*		
	High (1.0)	*Medium (0.5)*	*Low (0.1)*
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 =1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Keterangan Skala resiko : High (>50 – 100), Medium (>10 – 50, Low (1-10) Dalam memberikan penilaian skor dampak (Impact) dari resiko didasarkan pada kriteria (tabel 4).

Tabel 4. Tingkat Risiko

Tingkat Risiko	*Definisi Risiko*
Tinggi	Sistem yang berjalan tetap beroperasi, namun tindakan perbaikan harus segera dilakukan.
Sedang	Tindakan perbaikan dilakukan sesuai periode waktu yang direncanakan.
Rendah	Tindakan perbaikan masih perlu dilakukan atau resiko tersebut masih bisa ditoleransi/diterima

8) *Control Recommendations.*

Tujuan dari rekomendasi kontrol merupakan hasil dari proses penilaian risiko dan memberikan masukan untuk proses mitigasi risiko, yang dimana kontrol keamanan teknis dan prosedural yang telah direkomendasikan dievaluasi, diprioritaskan, dan diimplementasi.

9) *Results Documentation*.

Tahapan ini merupakan dokumentasi atau laporan dari seluruh kegiatan yang ada, dimulai dari tahap karakteristik hingga rekomendasi control

2.2 Metode Pengumpulan Data

Metode pengumpulan data adalah langkah yang strategis dalam penelitian, karena tujuan utama penelitian yaitu untuk mendapatkan data. Adapun Metode Pengumpulan Data yang digunakan dalam penelitian ini yaitu:

1) Asesmen adalah upaya untuk mendapatkan data/informasi dari proses dan hasil pembelajaran untuk mengetahui seberapa baik kinerja. Adapun subject yang akan

ISSN : 1411-1624
e-ISSN: 2621-8089

menjadi di Asesmen adalah pengelola IT dan s*upervisor*.

2) *Studi Literature*. Studi literature merupakan penelitian yang dilakukan untuk mendapatkan bahan rujukan berupa referensi yang bersifat teoristis dari buku-buku,jurnal-jurnal dan sumber bacaan lain yang dapat mendukung topik.
3) Persiapan *Software*. Pada tahapan ini dilakukan persiapan software yang mendukung untuk menganalisa sistem jaringan.
4) Keamanan Jaringan. Mengidentifikasi sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman Palembang yang berupa spesifikasi perangkat keras *(hardware)* dan perangkat lunak *(software),* dan mengenali ancaman *(threat)* dan kerentanan *(vulnerability*) sistem keamanan jaringan pada PT BRI (Persero) Tbk, KCP Sudirman Palembang.
5) Analisa Risiko. Tahapan ini merupakan tahapan analisa risiko sistem keamanan jaringan dengan *Framework* NIST.

3. HASIL DAN PEMBAHASAN

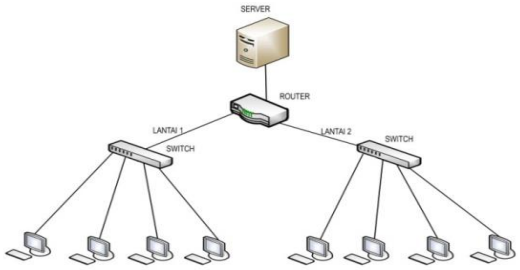
3.1 Hasil

Proses penilaian risiko berdasarkan NIST SP 800-30 terdapat beberapa tahap. Terdapat sembilan tahap dalam proses penilaian risiko berdasarkan NIST SP800-30, namun pada bab ini hanya dilakukan enam tahap yaitu *system characterization, threat identification, vulnerability identification, control analysis, likelihood determination,* dan impack analisi. 3 tahapam sisa nya masuk di bagian pembahasan adapun tahapan nya *risk determination, control recomendations,* dan *result documentation.*

3.1.1 *System Characterization*

Pada tahapan ini, peneliti mencoba mengenali karakteristik sistem jaringan Pada PT BRI (Persero) Tbk, KCP Sudirman Palembang.karakteristik jaringan adalah sebuah sistem yang terdiri atas komputer-komputer yang di desain untuk dapat berbagi sumber daya,berkomunikasi dan dapat mengakses informasi.Maka yang pertama kali dilakukan yaitu mengetahui bagaimana jaringan bekerja melalui topologinya. Jaringan PT BRI (Persero) Tbk, KCP Sudirman menggunakan tipe LAN *(Local Area Network)* dan topologi *hybrid* dengaan server yang mencakup dalam satu gedung. Semuanya terhubung ke satu router server. Kemudian, di router terdapat switch yang mencakup beberapa komputer dan laptop dengan jaringan berkabel dan jaringan nirkabel yang menggunakan *tipe interface serial port*. Sebagai peladen utama pada jaringan, peladen (Server) jaringan PT BRI (Persero) Tbk, KCP Sudirman memiliki beberapa fasilitas yaitu sebagai Web Server dengan perangkat lunak Apache, kemudian FTP Server dengan perangkat lunak Filezilla, IDS *(Intrusion Detection System)* dengan perangkat lunak Snort, dan. Dengan begitu, dapat disimpulkan bahwa setiap perangkat host dalam jaringan PT BRI (Persero) Tbk, KCP Sudirman sudah terlindung dalam sistem keamanan jaringan**.**

ISSN : 1411-1624
e-ISSN: 2621-8089



Gambar 1. Topologi Sistem

Selain dari sisi *software d*an topologi, peneliti juga akan mengenali karakterisasi sistem melalui penggunaan perangkat keras *(hardware)* yang ada. Hasil karakterisasi sistem melalui perangkat keras pada jaringan PT BRI (Persero) Tbk, KCP Sudirman Palembang adalah sebagai berikut:

1) HUB SWITCH,TP LINK 24 Port . *Router* yang dapat digunakan untuk menjadikan komputer biasa menjadi router yang handal, mempunyai banyak fitur yang mencakup untuk IP *Network* dan Jaringan *wireless.* TP LINK 24 Port ini dipilih karena memiliki sistem konfigurasi jaringan yang baik.
2) Switch D-Link CATALYS 800. Switch dengan fitur auto switch membuat instalasi cepat dan bebas kerumitan. Juga terdapat auto-negosiasi pada setiap port yang mendeteksi kecepatan link dari perangkat jaringan serta dengan cerdas menyesuaikan kompatibilitas dan kinerja yang optimal.
3) Kabel UTP CAT5. Digunakan sebagai penghubung suatu jaringan dan juga power untuk koneksi AP ke POE dan Router. Dengan merk AMP original agar bisa digunakan dalam jangka waktu yang lama dan untuk mengurangi masalah yang terdapat pada koneksi kabel.
4) Port Jaringan RJ45. Konektor atau penghubung kabel ethernet yang biasanya dipakai untuk jaringan. Konektor ini juga bisa dipakai pada topologi jaringan komputer LAN (Local Area Network).

3.1.2 *Threat Identification*

Identifikasi ancaman bertujuan untuk mengidentifikasi sumber-sumber ancaman yang potensial dan menghasilkan pernyataan ancaman yang mencantumkan sumber-sumber ancaman potensial yang berlaku untuk sistem TI yang sedang dianalisis. Berdasarkan hasil dari wawancara dan pengamatan langsung. Identifikasi ancaman yang dapat menyebabkan gangguan pada sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman meliputi ancaman packet *snifing, ddos* dan *spoofing.*

1) Paket *Snifing.* Teknik yang digunakan yaitu dengan melakukan pencurian data, cara kerjanya yaitu dengan memonitoring dan menganalisis setiap paket data yang ditransmisikan dari klien ke server.
2) *Ddos.* Jenis serangan DOS yang menggunakan banyak host dan untuk menyerang satu server sehingga mengakibatkan server tidak dapat berfungsi *bagi klien.*
3) *Spoofing.* Teknik yang digunakan yaitu dengan cara memalsukan data sehingga penyerang (attacker) dapat mengakses sistem seperti host yang bisa dipercaya.

Tabel 5. Identifikasi Ancaman

Sumber Ancaman	*Keterangan Ancaman*
Packet Snifing	• seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan komputer
Ddos	• menyebabkan bandwidth yang digunakan oleh korban akan habis yang mengakibatkan terputusnya koneksi antar server

ISSN : 1411-1624
e-ISSN: 2621-8089

	• menyebabkan kerusakan secara permanen terhadap hardware dan software
Spoofing	• merusak sistem keamanan perangkat / server

3.1.3 *Vulnerability Identification*

Berdasarkan hasil dari wawancara dan pengamatan langsung. Identifikasi kerentanan yang dapat menyebabkan gangguan pada sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman meliputi kerentanan miskonfigurasi, backdoor, dan rootkit.

Tabel 6. Identifikasi Kerentanan

Sumber kerentanan	Keterangan kerentanan
Miskonfigurasi	• Terganggunya jaringan • menyebabkan web server mudah diretas
Backdoor	• Merusak sistem keamanan perangkat/server • Merusak situs web
Rootkit	• menyebabkan kerusakan secara permanen terhadap hardware dan software

1) Miskonfigurasi. Kesalahan konfigurasi pada server dan perangkat keras (hardware) sangat sering membuat para penyusup dapat masuk ke dalam suatu sistem dengan mudah.
2) Backdoor. Yaitu langkah memasuki sistem selain akses login utama admin. Biasanya backdoor tersembunyi dan menggunakan jalur autentikasi berbeda dari jalur utama.
3) Rootkit. Merupakan alat yang digunakan untuk menyembunyikan jejak apabila telah melakukan penyusupan.

3.1.4 *Control Analysis*

Tujuan utama dari tahap ini untuk menganalisis kontrol yang telah diterapkan dan yang akan diterapkan, menjabarkan analisa kendali (control analysis) untuk meminimalisir atau menghilangkan bahaya yang dapat menyerang sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman Palembang. Tahapan ini diperlukan agar tahu apa yang harus dilakukan saat adanya ancanan (threat) atau kerentanan (*vulnerability*).

Tabel 7. Analisis Kontrol

Jenis	*Identifikasi*	*Keterangan*	*Kendali*
Packet Snifing	Ancaman	• seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan komputer	• Mulai menggunakan enkripsi yang secure seperti WPA-PSK2 dilengkapi dengan SSH • Mulai menerapkan akses SSL serta Always HTTPS dan enkripsi bertingkat. [7]
Ddos	Ancaman	• menyebabkan bandwidth yang digunakan oleh korban akan habis yang mengakibatkan terputusnya koneksi antar server • menyebabkan kerusakan secara permanen terhadap hardware dan software	• Mengatur sistem pembatasan bandwith upload maupun download pada RouterOS Mikrotik. [7] • Memasang perangkat lunak yang akan segera memotong koneksi jika penggunaan bandwith mulai membanjiri trafik atau bahkan memberi tantangan keamanan seperti Captcha [7]
Spoofing	Ancaman	• merusak sistem keamanan perangkat / server	• Menerapkan sistem whitelist (daftar putih) yang hanya mengizinkan pengguna tertentu untuk mengakses seluruh fitur dan fasilitas

ISSN : 1411-1624
e-ISSN: 2621-8089

Jenis	*Identifikasi*	*Keterangan*	*Kendali*
			jaringan. • Mulai menggunakan sistem identifikasi host yang lengkap yang semestinya menggunakan IP, DNS, MAC Address, hostname, dan autorisasi handshake. [7]
Miskonfigurasi	Kerentanan	• Terganggunya jaringan • menyebabkan web server mudah diretas	• Pastikan konfigurasi port-port akses sistem agar tidak digunakan penyerang, misalnya port 43 telnet, port 20 FTP, dan sebagainya.[7]
Backdoor	Kerentanan	• Merusak sistem keamanan perangkat/server • Merusak situs web	• Mulai menutup setiap backdoor, seperti ditutupnya akses WPS (WiFi Pin Setup) yang hanya memiliki pola 8 digit. • Men-scan sistem dari adanya penanaman shell sebagai remote backdoor. [7]
Rootkit	Kerentanan	• menyebabkan kerusakan secara permanen terhadap hardware dan software	• Menerapkan antivirus guna mendeteksi adanya rootkit dalam sistem operasi jaringan. [7]

3.1.5 *Likelihood Determination*

Pada tahapan Hasil dari menganalisa pada analisa kontrol dijadikan sebagai acuan dalam penentuan kemungkinan risiko. Berdasarkan penjelasan tingkat kemungkinan risiko dan hasil analisis pada setiap jenis risiko. Dapat dikategorikan tingkat kemungkinan risiko hasil dari penentuan kemungkinan risiko.

Tabel 8. Kemungkinan Risiko

Jenis Risiko	*Tingkat Kemungkinan*
Packet snifing	Rendah
Ddos	Tinggi
Spoofing	Sedang
Miskonfigurasi	Sedang
Backdoor	Rendah
Rootkit	Sedang

3.1.6 *Impact Analysis*

Pada tahapan ini adalah untuk menilai dampak yang terjadi terhadap serangan Berdasarkan penentuan kemungkinan risiko yang mengancam sistem informasi.

Tabel 9. Analisis Dampak

Jenis Risiko	*Dampak*	*Tingkat Dampak*
Packet snifing	• seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan computer	Rendah
Ddos	• menyebabkan bandwidth yang digunakan oleh korban akan habis yang mengakibatkan terputusnya koneksi antar server • menyebabkan kerusakan secara permanen terhadap hardware dan software	Tinggi
Spoofing	• merusak sistem keamanan perangkat / server	Sedang
Miskonfigurasi	• Terganggunya jaringan • .menyebabkan web server mudah diretas	Sedang
Backdoor	• Merusak sistem keamanan perangkat/server • Merusak situs web	Rendah
Rootkit	• menyebabkan kerusakan secara permanen terhadap hardware dan software	Sedang

ISSN : 1411-1624
e-ISSN: 2621-8089

3.2 Pembahasan

Proses penilaian risiko berdasarkan NIST SP 800-30 terdapat beberapa tahap. Terdapat sembilan tahap dalam proses penilaian risiko berdasarkan NIST SP800-30, pada pembahasan ini kelanjutan dari tahapan yang ada di hasil adapun tahapan nya *risk determination, control recomendations, dan result documentatio*n.

3.2.1 *Risk Determination*

Tujuan pada tahapan ini yaitu Penentuan risiko ini untuk menilai tingkat risiko terhadap sistem, penilaian ini mengacu pada kemungkinan risiko dan dampak risiko yang telah ditentukan. Pada NIST SP800-30 untuk penentuan risiko yang diharapkan dapat mengetahui tingkat prioritas risiko dalam sistem TI. Pada NIST SP800-30 untuk penentuan risiko yang diharapkan dapat mengetahui tingkat prioritas risiko dalam sistem TI, menggunakan matriks 3 x 3 seperti pada Gambar 1. dengan kemungkinan ancaman (tinggi, sedang, dan rendah) dan dampak ancaman (tinggi, sedang, rendah). Berdasarkan analisis yang dilakukan dengan mengikuti tahap-tahap sebelum penentuan risiko.

3.2.2 *Control Recommendations*

Rekomendasi kontrol merupakan hasil dari proses penilaian risiko dan memberikan masukan untuk proses mitigasi risiko, yang dimana kontrol keamanan teknis dan prosedural yang telah direkomendasikan dievaluasi, diprioritaskan, dan diimplementasi.

Tabel 10. Penentuan Risiko

Jenis Risiko	*Nilai Kemungkinan Ancaman*	*Nilai Dampak*	*Nilai Risiko*	*Tingkat Risiko*
Packet snifing	0.1 (Rendah)	10 (Rendah)	10	Rendah
Ddos	1.0 (Tinggi)	100 (Tinggi)	100	Tinggi
Spoofing	0.5 (Sedang)	50 (Sedang)	25	Sedang
Miskonfigurasi	0.5 (Sedang)	50 (Sedang)	25	Sedang
Backdoor	0.1 (Rendah)	10 (Rendah)	10	Rendah
Rootkit	0.5 (Sedang)	5 (Sedang)	25	Sedang

Tabel 11. Rekomendasi Kontrol

Jenis Risiko	*Tingkat Risiko*	*Rekomendasi*
Packet snifing	Rendah	• Menggunakan keamanan enkripsi WPA2-PSK pada hotspot wifi. • Memperbaharui browser ke versi yang terkini. Keamanan pada browser versi lama berisiko karena kemungkinan celah keamanan browser versi lama telah diketahui dan dapat digunakan untuk mencuri informasi sensitif. • Menggunakan sertifikat SSL pada website Simak Unismuh. Hal ini dilakukan untuk menjaga informasi sensitif akan selama dalam proses pengiriman melalui internet dengan cara dienkripsi.
Ddos	Tinggi	• Memantau lalu lintas secara berkala,dengan melakukan pengecekan maka anda bisa lalu lintas mana yang tergolong normal atau tinggi. • membatasi akses yang akan masuk atau keluar dari sistem. Sehingga traffic yang masuk serta keluar dari perangkat dan server bisa tersaring. • Meningkatkan kapasitas server,dengan Anda memiliki kapasitas bandwidth yang cukup. Agar ketika terjadi lonjakan lalu lintas bandwidth masih tersedia.
Spoofing	Sedang	• Menggunakan SSL Pastikan selalu URL mengecek website benar dan tidaknya dengan melihat apakah menggunaan layanan SSL atau tidak. Website yang menggunakan SSL pada bagian URL nya terdapat logo gembok, berarti website tersebut sudah terproteksi aman dari hacker dan sejenisnya. • Memasang filter di router, Filter IP yang dipasang pada router memungkinkan Anda untuk menyaring dari IP masuk yang mencurigakan, sehingga tindakan IP spoofing

ISSN : 1411-1624
e-ISSN: 2621-8089

Jenis Risiko	*Tingkat Risiko*	*Rekomendasi*
		bisa dihindarkan. • Hindari untuk melakuskan klik link/tautan yang tidak jelas, dari klik tersebut pelaku kejahatan *cyber* sudah bisa melakukan record data Anda.
Miskonfigurasi	Sedang	• Atur dan konfigurasikan perangakat jaringan dengan benar. • memonitoring jaringan selama 24 jam sehingga Anda tidak perlu khawatir lagi akan masalah keamanan seperti ancaman peretas dan sejenisnya.
Backdoor	Rendah	• mengaktifkan *firewall* pada device atau website yang kita gunakan maka akan secara otomatis memblock user yang tidak dikenali atau user tanpa ijin dan mereka tidak akan bisa mengambil dan membuka data dari *device* atau website kita. • Menggunakan software anti virus, *Software* anti virus ini setidaknya bisa menghalangi bahaya dari backdoor untuk memasuki jaringan Anda.
Rootkit	Sedang	• Perbarui komputer secara teratur. Ini berarti seluruh komputer, bukan hanya Windows, antivirus, atau driver graphics card kalian. Itu berarti memperbarui segalanya. • Mengaktifkan *Windows Defender* pada setiap pc . Setiap versi terbaru *Windows* sudah menyertakan *Windows Defender*.

3.2.3 *Results Documentation*

Tahapan ini merupakan akhir dari risk assesment yang dokumentasi atau laporan dari seluruh kegiatan yang ada. Pada langkah ini merupakan langkah terakhir setelah penilaian risiko selesai. Penilaian risiko yang dimaksudnya seperti sumber-sumber ancaman dan kerentanan diidentifikasi, risiko dinilai, dan kontrol yang telah direkomendasikan.

Tabel 12. Rekapitulasi Risiko

Kategori Risiko	*Tinggi*	*Sedang*	*Rendah*
Packet sniffing			10
Ddos	100		
Spoofing		25	
Miskonfigurasi		25	
Backdoor			10
Rootkit		25	

4. KESIMPULAN

Berdasarkan hasil analisis sistem keamanan jringan pada PT BRI (Persero) Tbk, KCP Sudirman Palembang menggunakan *framework* NIST, Setelah dilakukan risk assesment dan analisa Tahapan dalam penilaian risiko *Framework* NIST SP 800-30 , ditemukan bahwa sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman Palembang memiliki celah terhadap ancaman Ancaman yang muncul seperti *backdoor* memiliki tingkat risiko rendah, *packet snifing, spoofing,* dan rootkit memiliki tingkat risiko sedang, dan Ddos memiliki tingkat risiko tinggi. Tingkat risiko didapatkan pada proses pengelompokan sumber ancaman. 3. Rekomendasi kontrol yang diberikan pada sistem keamanan jaringan PT BRI (Persero) Tbk, KCP Sudirman Palembang berdasarkan kerangka kerja NIST SP800-30.

DAFTAR PUSTAKA

[1] R. Erlando, D. Diana, and M. Ulfa, "Penerapan Sistem Keamanan Firewall Pada Router Cisco 1841 Dan Monowall Pada Sistem Operasi Bsd (Berkeley Software Distribution)," in *Bina Darma …*, 2020, pp. 236–243.

[2] F. Panjaitan and R. Syafari, "Pemanfaatan Notifikasi Telegram Untuk Monitoring Jaringan," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 10, no. 2, pp. 725–732, 2019.

[3] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol.*

ISSN : 1411-1624
e-ISSN: 2621-8089

Inf., vol. 2, no. 2, pp. 8–13, 2016.

[4] E. Haryadi, D. Yuliandari, A. Abdussomad, D. Wijayanti, M. Amelia, and S. Syafrianto, "Maintaining The Continuity of The Company's Operation using the NIST Framework for SME," *J. Tek. Komput.*, vol. 7, no. 1, pp. 74–78, 2021.

[5] O. Hadikaryana and A. Sasongko, "PENILAIAN RESIKO KEAMANAN INFORMASI PADA INFRASTRUKTUR KRITIS SISTEM SCADA AREA PENGATUR BEBAN XXX BERDASARKAN PANDUAN NIST SP 800-82," *Syntax Lit. J. Ilm. Indones.*, vol. 4, no. 4, pp. 131–145, 2019.

[6] Y. DEWI, "MANAJEMEN RISIKO IT PADA SISTEM IRAISE MENGGUNAKAN METODE NIST SP 800-30." UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU, 2021.

[7] M. Zen Adriyansa and F. Panjaitan, "Analisis Sistem Keamanan Jaringanmenggunakan Framework Nist," in *Bina Darma Conference on Computer Science*, 2020, pp. 265–271.

[8] D. A. Permatasari, W. H. N. Putra, and A. R. Perdanakusuma, "Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 6001–6008, 2019.

[9] V. I. Sugara, H. Syahrial, and M. Syafrullah, "Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute of Standards and Technology (Nist) Cybersecurity Framework," *Komputasi J. Ilm. Ilmu Komput. dan Mat.*, vol. 16, no. 1, pp. 203–212, 2019.

[10] A. J. Subakti, "Analisis akses keamanan jaringan lapan berdasarkan log firewall di lapan pusat," Universitas Negeri Jakarta, 2017.

[11] H. Sama *et al.*, "Studi Komparasi Framework NIST dan ISO 27001 sebagai Standar Audit dengan Metode Deskriptif Studi Pustaka," *RAbit J. Teknol. dan Sist. Inf. Inivrab*, vol. 6, no. 2, pp. 116–121, 2021.

[12] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 02, no. 02, pp. 1–8, 2017.

[13] M. Fitriana, A. Khairan, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020.

[14] R. S. Perdana, "AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 3, no. 1, pp. 9–14, 2018.

[15] A. Elanda and D. Tjahjadi, "Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30 (Studi Kasus Disinfolahtaau Mabes Tni Au)," *Infoman's*, vol. 12, no. 1, pp. 1–13, 2018.