p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 10 Nomor 2 Agustus 2018

PEMERINGKATAN RISIKO KEAMANAN SISTEM JARINGAN KOMPUTER POLITEKNIK KOTA MALANG MENGGUNAKAN CVSS DAN FMEA

Betta Wahyu Retna Mulya[1], Avinanta Tarigan[2]
[1]betta.wahyu@gmail.com, [2]avinanta@gmail.com
[12]Program Pascasarjana Teknik Informatika Universitas AMIKOM Yogyakarta

Abstrak

Celah keamanan sistem jaringan komputer merupakan sebuah kelemahan, kekurangan atau lubang pada sistem, yang dapat dimanfaatkan oleh satu atau lebih dari penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem.Proses penambalan memerlukan analisis celah keamanan sesuai dengan tingkat kerusakan untuk menentukan skala prioritas penanganan. Analisis yang digunakan dalam penentuan skala prioritas penanganan merupakan perpaduan metode analisis berbasis CVSS dan FMEA.Hasil analisis dari perpaduan dua metode menunjukkan bahwa nilai *risk priority number* dan jumlah *vulnerability* menjadi tolok ukur dalam memprioritaskan penanganan dan mitigasi risiko kepada pihak Politenik Kota Malang dengan urutan prioritas server singa, server sierra, server dino, dan server leopard. Skala prioritas menunjukkan bahwa tingkat kerentanan yang harus segera ditangani memiliki rentang nilai antara 40% sampai dengan 60%. Penggabungan dua metode CVSS dan FMEA dapat menentukan peringkat penanganan berdasarkan dampak potensial yang ditimbulkan akibat kerentanan di sistem jaringan komputer Politeknik Kota Malang.
Kata kunci: sistem jaringan komputer, celah keamanan, CVSS, FMEA, mitigasi

Abstract

The vulnerability of a computer network system is a weakness, lack or hole in the system, which can be exploited by attackers to carry out an attack that may endanger the confidentiality, integrity or availability of a system. The filling process requires a security vulnerability analysis according to the severity to determine the priority scales of handling. The analysis used in determining priority scales of handling is the combination of CVSS and FMEA-based analysis method. The analysis result from both methods shows that the numbers of risk priority and vulnerability become a benchmark in risk prioritizing and mitigation the risk to Politeknik Kota Malang party, with the priority order: 'Singa', 'Sierra', 'Dino', and 'Leopard'. The priority scales show that the vulnerability levels, that must be handled, have number range between 40% up to 60%. The combination of CVSS and FMEA methods can determine the handling level based on the potential impacts caused by the vulnerability in computer network system of Politeknik Kota Malang.
Keywords: network computer system, vulnerability, CVSS, FMEA, mitigation

1. Pendahuluan

Komunikasi data saat ini memiliki peranan penting diberbagai aspek aktivitas masyarakat. Kebutuhan akan komunikasi data dari tahun ke tahun meningkat. Peningkatan ini mencakup jumlah pengguna, jumlah akses data, dan lama waktu akses. Politeknik Kota Malang (POLTEKOM) membangun jaringan komputer berserta sistem informasinya untuk memenuhi kebutuhan komunikasi. Seiringnya waktu sistem informasi dan jaringan komputer POLTEKOM mengalami beberapa serangan baik dari dalam maupun dari luar. Perlunya analisis pemeringkatan risiko agar mengetahui cara penanganan yang tepat. Analisis yang dilakukan tentunya disesuaikan dengan kebutuhan keamanan dari sistem yang dibangun. Kebutuhan keamanan untuk sebuah sistem komputer berbeda-beda bergantung pada aplikasi-aplikasi yang didalamnya. Dilihat dari kebutuhan keamanan tersebut maka tidak ada jaminan apakah suatu sistem atau jaringan komputer dapat dikatakan *secure* atau *reliable*. Keamanan dapat ditingkatkan dalam skala berkelanjutan dari 0 hingga 1, atau dari kondisi tidak aman menjadi relatif aman [1].

Menghindari konten yang berbahaya bagi sistem dan jaringan komputer dibutuhkan tingkat kesadaran pengguna dalam akses sistem informasi dan jaringan komputer. Tingkat kesadaran pengguna seharusnya didasari oleh pengetahuan tentang celah keamanan dan jenis-jenis ancaman serta serangan dalam jaringan komputer. Guna meningkatkan tingkat kesadaran maka perlunya memahami tentang *network security situation awareness. Network security situation awareness* adalah teknologi keamanan baru yang didasarkan pada analisis data lampau dan deteksi status keamanan jaringan saat ini. Penilaian situasi keamanan jaringan memiliki hubungan erat antara perolehan elemen situasi dan prediksi kecenderungan kesadaran akan keamanan jaringan [2].

Penelitian ini akan dilihat bagaimana memastikan bahwa penggunakan *Common Vulnerability Scoring System* (CVSS) dan *Failure Mode and Effect Analysis* (FMEA) memungkinkan untuk menilai, membandingkan, memahami, serta memprioritaskan *patching vulnerability* pada sistem jaringan komputer, dengan demikian mampu memprioritaskan penanganannya sesuai dengan tingkat risikonya [3]. Analisis menggunakan CVSS digunakan untuk mengetahui dampak potensial akibat *vulnerability* sedangkan FMEA digunakan untuk mengetahui urutan prioritas penanganan potensi kegagalan yang ditimbulkan oleh celah keamanan.

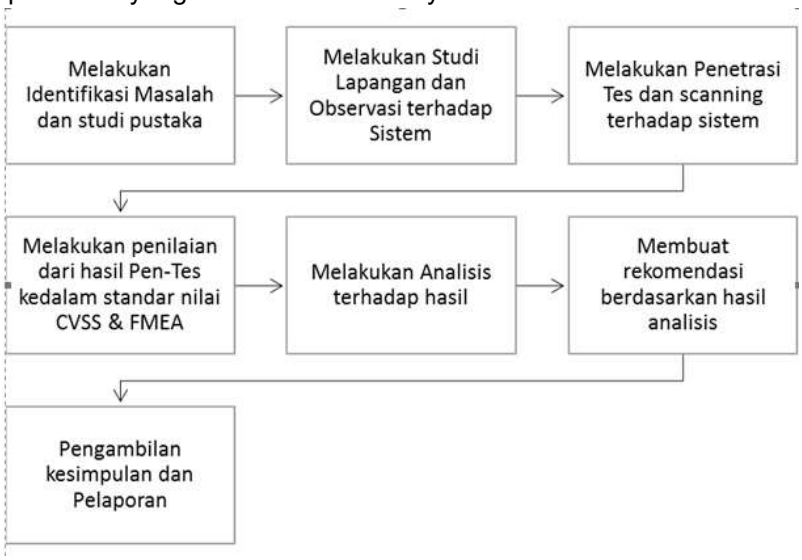
2. Metode

2.1. Sifat dan Pendekatan Penelitian

Sifat jenis data dan analisis dari penelitian ini bersifat kualitatif, dengan melakukan pengkarakteristikan dari penemuan celah keamanan tersebut kemudian memberikan penilaian atau scoring menggunakan *common vulnerability scoring system* dan melakukan penentuan peringkat terhadap sistem yang paling terpengaruh. Menggunakan *failure mode and failure analysis*.. **P**endekatan penelitian ini bersifat *Mix-Method* yaitu memadukan pendekatan kualitatif dan kuantitatif dalam metodologi pengambilan data pada *penetration test*. Pendekatan kualitatif didasari dari base metric group CVSS yaitu penilaian atas dasar kualitas sebuah kelemahan. Pendekatan kuantitatif didasari dari base scoring CVSS dan *Risk Priority Number* pada FMEA sebagai pengukur prioritas risiko terhadap penanganan kelemahan sistem.

2.2. Alur Tahapan Penelitian

Langkah-langkah penelitian yang dilakukan diantaranya :



Gambar 1. Alur tahapan penelitian

Deskripsi alur tahapan penelitian

Tabel 1. Deskripsi alur tahapan penelitian

No	Tahapan	Deskripsi
1	Identifikasi masalah	1. Bagaimana penanganan celah keamanan sistem jaringan komputer Politeknik Kota Malang ? 2. Bagaimana mengukur dampak potensial akibat munculnya *vulnerability* pada sistem jaringan komputer ? 3. Bagaimana menentukan skala prioritas penanganan terhadap sistem jaringan komputer ?
2	Observasi sistem	Melakukan pengamatan dan eksplorasi terhadap perangkat keras dan perangkat lunak pada sistem jaringan komputer Politeknik Kota Malang
3	Tes penetrasi	Melakukan tes penetrasi mulai dari proses

		pemetaan, scanning, dan attacking menggunakan bantuan perangkat lunak zenmap, nessus, owasp, dan vega
4	Assessment hasil	Penilaian hasil tes penetrasi dikomparasi dengan hasil penilaian FMEA hasil observasi bersama pihak UPT PUSKOM Politeknik Kota Malang.
5	Analisis hasil	Menganalisa hasil komparasi dan mengabungkan kedua metode CVSS dan FMEA dan dibuat dalam diagram pareto
6	Rekomendasi hasil	Memberikan rekomendasi kepada UPT PUSKOM untuk menangani kerentanan mulai dari manajemen perangkat keras hingga tingkat kesadaran pengguna
7	Pengambilan kesimpulan	Membuat kesimpulan dari hasil analisis.

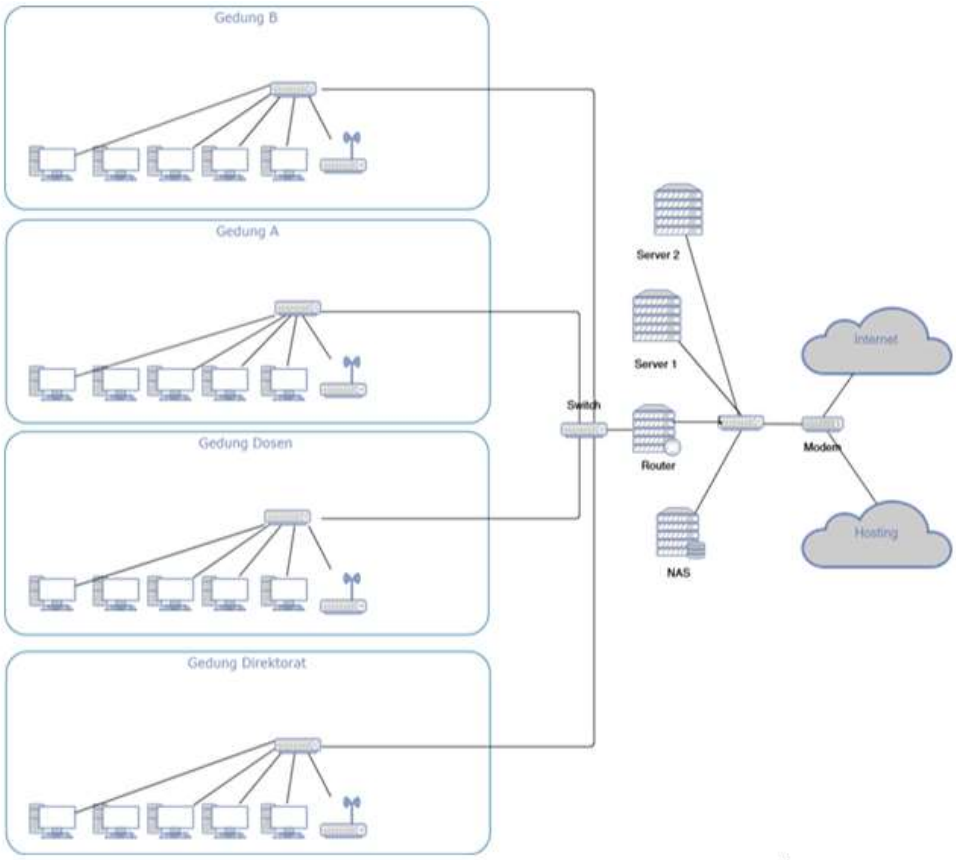
2.3. Topologi Jaringan Komputer

Sistem jaringan komputer di Politeknik Kota Malang digunakan untuk memberikan layanan kepada mahasiswa, pegawai, maupun publik secara daring. Layanan ini meliputi *website*, internet, *elearning*, siakad, pmb, *file sharing*, jurnal, dan perpustakaan. Berikut daftar alamat domain dan subdomain pada Politeknik Kota Malang pada tabel 2 :

Tabel 2. Fungsi 4 Server

No	Hostname	Fungsi dan kegunaan	IP Private
1	dino.poltekom.ac.id	Router dan network manajemen	172.16.0.1
2	singa.poltekom.ac.id	Server cloud dan library	172.16.0.3
3	leopard.poltekom.ac.id	Server lms dan jurnal	172.16.0.4
4	sierra.poltekom.ac.id	Server siakad dan PMB	172.16.0.5

Sistem jaringan komputer Politeknik Kota Malang terdiri dari 4 server, 2 switch *unmanageable*, 1 *network storage*, dan 1 router. Keempat server tersebut memiliki fungsi yang berbeda-beda seperti yang dijelaskan pada gambar 2 :



Gambar 2. Topologi Jaringan Politeknik Kota Malang

2.4. Metode Pengumpulan Data

Pengumpulan data penelitian dilakukan dengan cara, sebagai berikut :

1. Studi dokumentasi, yaitu pengumpulan data penelitian dengan mempelajari buku, file, atau dokumen yang diperlukan seperti *CVSS user guide*, dan *exploit database*.
2. Wawancara, yaitu pengumpulan data penelitian dengan mewawancarai pihak penanggung jawab sistem terkait yaitu UPT PUSKOM tentang ancaman dan serangan pada sistem dan jaringan komputer di Politeknik Kota Malang.
3. Percobaan Laboratorium, yaitu pengumpulan data yang berupa percobaan yang dikendalikan terhadap target penelitian menggunakan penetration test tool. Perencanaan unit penelitian diukur berdasarkan *base metric group* CVSS versi 3 yang kemudian diperingkatkan berdasarkan FMEA sesuai dengan hasil dari RPN-nya
4. Observasi, yaitu pengumpulan data penelitian dengan pengamatan dari hasil penetration test terhadap sistem dan jaringan komputer di Politeknik Kota Malang terkait pengukuran celah keamanannya berdasarkan CVSS Versi 3 dan memberikan rating terhadap sistem mana yang memiliki risiko paling tinggi.

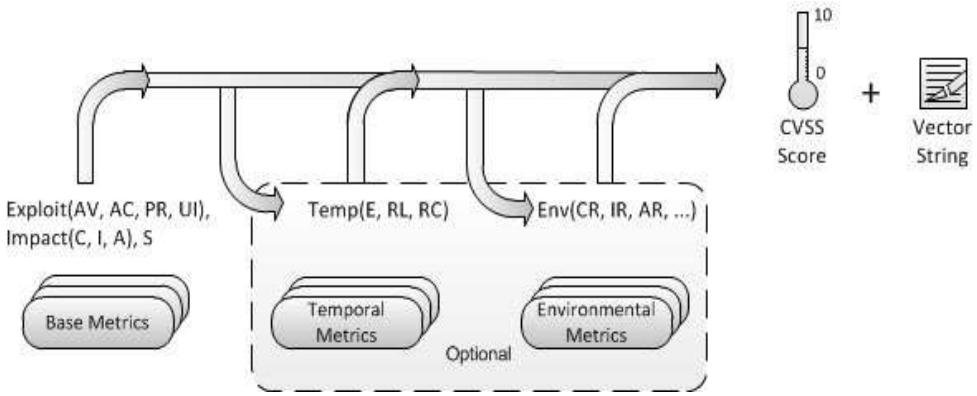
Pengumpulan data menurut perolehannya dan sifatnya sebagai berikut :

1. Data primer yaitu data yang dikumpulkan oleh peneliti melalui hasil dari tes penetrasi terhadap sistem jaringan komputer dengan mendapatkan hasil data kualitatif yaitu *critical, high, medium*, dan *low*.
2. Data Sekunder yaitu data yang dikumpulkan oleh peneliti secara tidak langsung dengan melibatkan tim UPT PUSKOM dalam melakukan penilaian pada FMEA Assessment yang menghasilkan data kuantitatif dengan rentang nilai mulai 0 sampai dengan 1000.

2.5. Metode Analisis Data

Analisis data yang dilakukan dalam penelitian ini melalui pendekatan mix-method. Pendekatan ini digunakan untuk mengetahui kualitas sistem dan jaringan komputer Politeknik Kota Malang berikut metode analisis data :

1. Analisis terhadap pendekatan kualitatif base metric group melalui tes penetrasi terhadap sistem dengan menggunakan perangkat lunak *vulnerability scanner* NESSUS untuk mengetahui jumlah dan kualitas risiko di tiap sistemnya.
2. Analisis terhadap pendekatan kuantitatif base scoring melalui perhitungan dari hasil base metric group untuk mengetahui skala level ancaman beserta *CVE Numbering*. Proses penilaian *score* alurnya dapat dilihat pada gambar 3.



Gambar 3. *CVSS Metrics and Equations*

Rumus perhitungan *base score*

Definisi base score : (1)

```
If(Impact sub score <= 0 ) else, 0)
Scope Unchanged Round up (Minimum[(Impact+Exploitability),10])
Scope Changed Round up (Minimum[1.08 x (Impact + Exploitability),10])
```

Definisi impact sub score : (2)

```
Scope Unchanged 6.42 x ISCBase
Scope Changed 7.52 x [ISCBase-0.029]-3.25 x [ISCBase-0.02]
```


Perhitungannya Impact sub score : (3)

```
ISCBase = 1 – [(1-ImpactConf) x (1-ImpactInteg) x (1-ImpactAvail)]
```

Perhitungan Exploitability sub score : (4)

```
8.22 x AttackVector x AttackComplexity x PriviligeRequired x
UserInteraction
```

3. Analisis terhadap risiko menggunakan dengan menggunakan *network vulnerability assessment* checklist untuk mengetahui jumlah severity, occurence, dan detection.
4. Analisis terhadap risiko menggunakan form FMEA checklist yang dibuat berdasarkan diskusi peneliti dengan UPT PUSKOM untuk melakukan pemeringkatan risiko melalui perhitungan RPN.

3. Hasil dan Pembahasan

3.1 Identifikasi Aset

Penelitian ini dilakukan menggunakan aset sistem jaringan Politeknik Kota Malang. Hasil dari pengamatan aset secara langsung pada Politeknik Kota Malang didapatkan bahwa terdapat 4 buah server yang memiliki fungsi masing-masing.

Tabel 3. Daftar Aset Server Politeknik Kota Malang

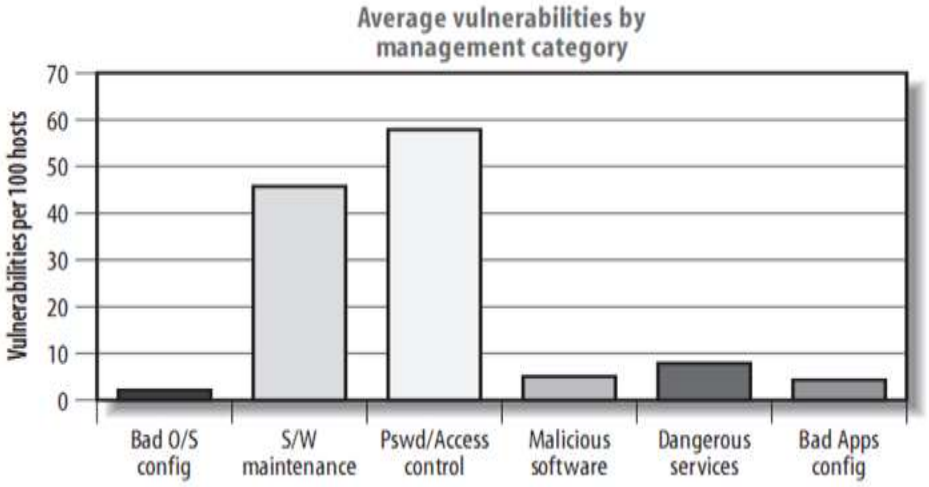
Aset	IP Private	IP Public	Fungsi	Sistem Operasi
Dino	172.16.0.1	36.66.212.105	Firewall, Router, dan DNS Forwarder	Pfsense (freeBSD)
Singa	172.16.0.3	36.66.212.106	Perpustakaan, OJS, dan Weblog	Ubuntu Server 12.04 LTS
Leopard	172.16.0.4	36.66.212.108	LMS dan Cloud	CentOS 7.5
Sierra	172.16.0.5	36.66.212.109	PMB dan Siakad	Ubuntu Server 16.04 LTS

3.2 Analisis Vulnerability

Vulnerabilities dan eksposur pada lingkungan sistem dan jaringan komputer dikarenakan terkait rendahnya pengelolaan sistem, patch yang tidak diinstal secara rutin, penggunaan kata sandi yang lemah, lemahnya pengaturan hak akses, dan sebagainya. Alasan utama dan tujuan di balik pengujian penetrasi harus mampu mengidentifikasi dan memperbaiki apa yang mendasari kegagalan dalam proses pengelolaan sistem sehingga mampu mendeteksi kerentanan pada saat pengujian. Kegagalan proses manajemen sistem yang paling umum ada di bidang berikut:

1. Konfigurasi sistem perangkat lunak
2. Konfigurasi aplikasi perangkat lunak
3. Perawatan perangkat lunak
4. Manajemen dan administrasi pengguna

Keempat bidang tersebut dikategorikan lagi berdasarkan rata- rata kerentanan yang sering mengakibatkan kegagalan sistem. Gambar 3 menunjukkan jumlah kerentanan berdasar kategori [4].



Gambar 4. Kerentanan berdasarkan kategori

3.2.1 Analisis dengan CVSS

Sistem jaringan komputer yang dimiliki oleh Politeknik Kota Malang semuanya terhubung kedalam internet. Untuk mengetahui celah keamanan pada sistem jaringan komputer dalam penelitian ini menggunakan tool analisis berupa *vulnerability scanner* yaitu NESSUS. Hasil dari proses ini didapatkan kategori *vulnerability*nya yaitu *critical, high, medium, dan low* yang dihasilkan berdasarkan *base score* selain itu terdapat juga solusi (*remediation*) untuk mengatasi *vulnerability* tersebut. Analisis menggunakan CVSS dalam prioritas penanganan kelemahan berdasarkan dari dampak bisnis menggunakan skala Franklin Covey.

Tabel 4. Skala Franklin Covey

Skala	Tindakan	Keterangan
1	*Do Right Way*	Segera dan Penting
2	*Plan to Do*	Tidak segera dan penting
3	*Delegate*	Segera dan tidak penting
4	*Postpone/Dump*	Tidak segera dan tidak penting

Penanganan keamanan pada 4 server tersebut berdasarkan tingkat kerusakan (severity) yang paling terdapat. Prioritas penanganan berdasarkan tingkat kerusakan hasil analisis *vulnerability* dengan CVSS ditunjukkan pada tabel 5.

Tabel 5. Prioritas penanganan berdasarkan CVSS

Host name	Kategori Kelemahan				Skala Prioritas Penanganan
	Extreme	High	Medium	Low	
Singa	32	149	141	15	1
Dino	2	31	21	1	2
Sierra	0	19	12	0	3
Leopard	0	0	2	1	4

Hasil proses scanning menggunakan Nessus menunjukkan jumlah *vulnerability* dan rekomendasi

Gambar 5. Salah satu hasil *scanning* menggunakan nessus

3.2.2 Analisis dengan FMEA

Berdasarkan hasil pengamatan pada waktu proses pengambilan data, mode kegagalan dan risiko yang dihasilkan pada sistem jaringan komputer Politeknik Kota Malang teridentifikasi. Selain pengamatan peneliti juga melakukan studi literatur-literatur tentang daftar potensi kegagalan yang dapat terjadi. Tabel 6 merupakan hasil analisis daftar potensi kegagalan yang terjadi pada sistem jaringan komputer Politeknik Kota Malang yang telah diidentifikasi oleh tim PUSKOM dengan peneliti.

Tabel 5. Daftar potensi kegagalan.

Klasifikasi	Kode	Mode Kegagalan	Efek Teknis dari kegagalan	Dampak dari Risiko	Penyebab Kegagalan dan risiko
Hardware / Fisik	A1	Kerusakkan Hardware	Sistem Terhenti, Kehilangan Aset	Pekerjaan terhenti, Proses tidak berjalan normal	Perbaikan dan Perawatan yang tidak teratur
	A2	Server overheat, memori *buffer overflow*	Server lamban, waktu respon lama, server hang	Terganggunya kinerja pegawai, lambatnya proses administrasi	Beban kinerja server yang tinggi
	A3	Sistem tidak bisa diakses	koneksi terputus, sistem offline	Proses pelayanan terganggu, perkuliahan terhambat	Konfigurasi jaringan bermasalah
Software / Non Fisik	B1	Data hilang	Tidak ada data backup, data korup	Proses manajemen organisasi terganggu, Proses akademik mengalami kemunduran	Tidak adanya proses backup

	B2	Perangkat lunak Memiliki kelemahan	Celah masuknya hacker, penguasaan sistem	Modifikasi perangkat lunak, pencurian data, kepercayaan publik yang turun	Perangkat lunak using
	B3	Penyerang menanamkan kode jahat	Modifikasi sistem, terjadinya hacking	Kepercayaan publik turun, proses layanan terganggu	Konfigurasi sistem yang tidak benar
	B4	Serangan Hacker	Sistem dikuasai, Sistem *crash*, pengalihan arus informasi	Pencurian data perusahaan, pemerasan	Tidak adanya filtering dan pembatasan hak akses
	C1	Kehilangan otorisasi	Sistem termodifikasi, perubahan konfigurasi	Aplikasi error, Kecepatan jaringan menurun	Penyalahgunaan hak akses
User Awareness / Pengguna	C2	Infeksi malware	jaringan terbebani, penyadapan informasi	bocornya informasi penting, Kinerja pegawai dalam melayani transaksi terganggu	Pelanggaran Aturan oleh pegawai
	C3	Sistem mengalami kerusakan	Sistem tidak berjalan semestinya, Terhambatnya pekerjaan	Pembengkakan biaya, data sensitif hilang atau korup	Karyawan yang tidak kompeten

Pada tahapan ini dilakukan proses penentuan level severity, occurence, dan detection. Proses pada tahapan ini adalah mendeskripsikan serta mengidentifikasi sistem jaringan komputer berdasarkan potensi kegagalan dan risiko yang akan muncul. Penilaian pada tahapan ini adalah menilai level severity, occurence, dan detection menggunakan skala 1-10 yang nantinya akan menghasilkan nilai akhir berupa risk priority number (RPN) untuk mengetahui prioritas kegagalan yang segera ditangani. Hasil dari penilaian RPN ke 4 buah server sebagai berikut.

Tabel 6. Perhitungan RPN dari hasil analisis FMEA

Nama Server	Potensi Kegagalan	Potensi Kegagalan										Total RPN
		A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	
Server Dino	Severity	4	4	5	5	4	3	3	2	4	2	382
	Occurence	5	2	5	3	3	2	4	2	4	2	
	Detection	4	3	3	5	2	2	4	3	2	2	
	RPN	80	24	75	75	24	12	48	12	32	8	
Server Singa	Severity	4	5	5	6	9	6	7	5	4	2	1079
	Occurence	5	7	4	5	7	4	7	5	4	2	
	Detection	4	2	3	5	3	4	6	4	2	2	
	RPN	80	70	60	150	189	96	294	100	32	8	
Server Sierra	Severity	4	4	5	8	5	4	2	3	3	2	490
	Occurence	5	3	7	5	3	3	4	4	3	3	
	Detection	4	3	2	4	2	3	3	2	2	2	

	RPN	80	36	70	160	30	36	24	24	18	12	
Server Leopard	Severity	4	4	5	7	2	3	2	2	3	2	398
	Occurence	5	3	7	5	2	3	4	1	2	2	
	Detection	4	3	2	4	2	2	3	1	2	2	
	RPN	80	36	70	140	8	18	24	2	12	8	

3.3 Pemeringkatan risiko keamanan

Analisis vulnerability dan pemeringkatan risiko menunjukkan data kualitatif dan kuantitatif dari keempat server serta sistem jaringan komputer. Nilai RPN dari FMEA dan nilai vulnerability dari hasil perhitungan CVSS akan dijadikan tolok ukur dalam proses prioritas penanganan dan mitigasi risiko berupa rekomendasi kepada pihak UPT PUSKOM Politeknik Kota Malang. Penentuan skala prioritas penanganan guna menyelesaikan permasalahan yang ada maka penulis melakukan penggabungan skala dari hasil scanning vulnerability dan hasil RPN kemudian ditotal. Dari hasil tersebut akan dilakukan analisis menggunakan diagram pareto dengan prinsip yang menyatakan bahwa untuk banyak kejadian (dalam hal ini kelemahan) , bahwa sekitar 80% dari efek tersebut disebabkan oleh 20% penyebabnya [5]. Tiap metode baik CVSS maupun FMEA masing-masing dapat menghasilkan urutan prioritas akan tetapi dari hasil perbandingannya kedua metode tersebut memiliki perbedaan dalam urutan prioritas. Berikut perbandingan antara kedua metode pada tabel 7 menunjukkan perbedaan dalam pemeringkatan risiko keamanan yang digunakan untuk penanganan atau penambalan celah keamanan.

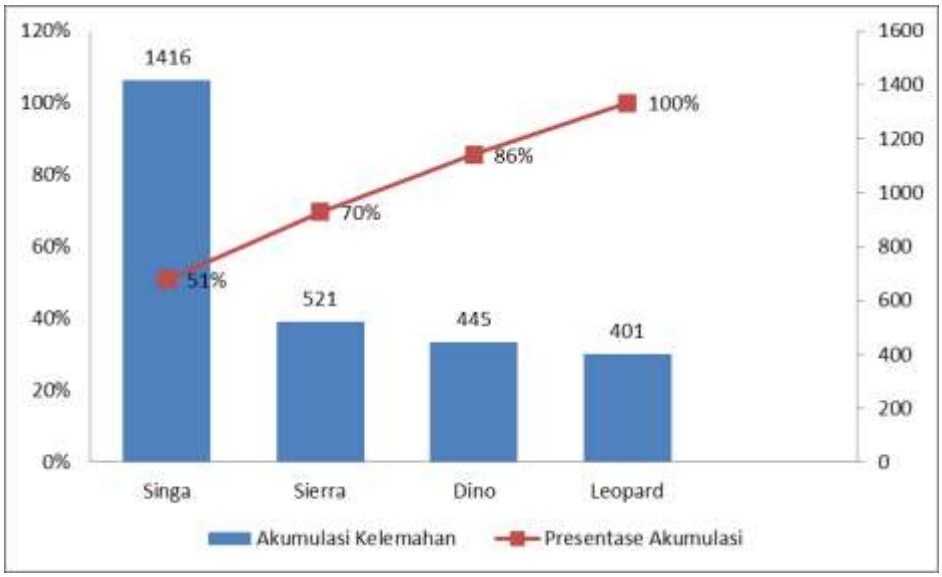
Tabel 7. Perbandingan Urutan Prioritas

Hostname	Skor CVSS	Skor FMEA	Urutan Prioritas CVSS	Urutan Prioritas FMEA
Singa	337	1416	1	1
Dino	55	445	2	3
Sierra	31	521	3	2
Leopard	3	401	4	4

Hasil dari analisis didapatkan bahwa kedua metode tersebut masih memiliki perbedaan dalam hal prioritas penanganan. Perhitungan dari kedua metode tersebut dilakukan proses perhitungan ulang dengan membuat klasifikasi penilaian dan menghitung nilai rata-rata dari keempat klasifikasi.

1. Klasifikasi penilaian kegagalan *hardware*
2. Klasifikasi penilaian kegagalan *software*
3. Klasifikasi penilaian kegagalan *userawareness*
4. Klasifikasi penilaian *vulnerability*

Peneliti mengabungkan dua metode tersebut kemudian dibuat diagram pareto. Gambar 6. menunjukan prioritas penanganan hasil pengabungan dua metode yang dapat dilihat pada tabel 8.



Gambar 6. Diagram Pareto

Priotitas penanganan dilakukan sesuai dengan prosentase kegagalan yang digambarkan pada gambar 6. Peneliti memberikan keterangan server mana yang harus ditindak lanjuti penanganannya.

Tabel 8. Prioritas penanganan hasil penggabungan 2 metode

Klasifikasi/host	A	B	C	SV	Total	Presentase	Akumulasi Presentase
Singa	210	729	140	337	1416	51%	51%
Sierra	186	250	54	31	521	19%	70%
Dino	179	159	52	55	445	16%	86%
Leopard	186	190	22	3	401	14%	100%

4 Kesimpulan dan Saran

4.1 Kesimpulan

Berdasarkan hasil penelitian, berikut ini merupakan beberapa kesimpulan yang dapat diambil :

1. Hasil analisis dari penelitian ini menjabarkan bahwa sistem jaringan komputer Politeknik Kota Malang terdapat beberapa celah keamanan yang berstatus High Priority yaitu server singa.
2. Penggunaan Metode CVSS versi 3 hanya memperhatikan segi vulnerability saja tanpa memperhatikan celah keamanan dari faktor user awareness dan sistem infrastruktur jaringan komputer.
3. Penentuan variabel FMEA yaitu severity, occurence, dan detection belum memiliki standar baku. Penentuan variable tersebut berdasarkan potensi kegagalan yang dapat diamati oleh UPT PUSKOM.
4. Hasil analisis dari penggabungan dua metode CVSS dan FMEA dapat menentukan peringkat penanganan berdasarkan dampak potensial yang ditimbulkan akibat kerentanan dan celah keamanan disistem jaringan komputer Politeknik Kota Malang.
5. Hasil penelitian ini menunjukkan tingkat kerentanan sistem jaringan komputer memiliki nilai rentang 40% s/d 60%. Dengan demikian tujuan dari penelitian ini tercapai dengan menunjukkan tingkat kerentanan dan pemeringkatan risiko serta menjabarkan rekomendasi penanganan.

4.2 Saran

Pada penelitian ini peneliti memiliki keterbatasan dalam penerapan hasil rekomendasi, serta pembatasan dalam melakukan *penetration test* khususnya untuk situs web pada *domain* maupun *subdomain* poltekom.ac.id yang menyebabkan peneliti tidak dapat melakukan perhitungan ulang RPN dan menambahkan *Common Weak Enumeration* (CWE) dalam perhitungan analisis vulnerability. Berdasarkan kesimpulan yang telah diuraikan, maka untuk penelitian selanjutnya dapat melakukan perhitungan ulang RPN setelah menjalankan rekomendasi. Selain itu menambahkan fitur perhitungan CWE dalam proses penilaian *website* sistem informasi atau *web profile*. Peneliti juga dapat memakai SIX SIGMA sebagai peningkatan perbaikan kelemahan sistem jaringan komputer berdasarkan hasil RPN dari FMEA. Penerapan ISO/IEC 27001atau SIX SIGMA tentang manajemen keamanan informasi belum dilaksanakan di Politeknik Kota Malang, kedepannya peneliti dan Tim PUSKOM melakukan penerapan ISO/IEC 27001 atau SIX SIGMA pada Politeknik Kota Malang.

5 Ucapan Terima Kasih

Peneliti mengucapkan terima kasih atas kesempatan dan izin yang telah diberikan oleh UPT PUSKOM Politeknik Kota Malang dalam menggunakan sistem jaringan komputer.

Daftar Pustaka

[1] F. Masykur, "ANALISIS VULNERABILITY WEB BASED APPLICATION MENGGUNAKAN NESSUS", Prosiding SENATEK, Fakultas Teknik, Universitas Muhammadiyah Purwokerto, p. 320-326, 2015.

[2] F. Li, Q. Huang, J. Zhu, and Z. Peng, “Network Security Risk Assessment Based on Item Response Theory,” Proceedings of the 8th International Conference on Mobile Multimedia Communications, 2015.

[3] G. Spanos and L. Angelis, “Impact Metrics of Security Vulnerabilities: Analysis and Weighing,” Information Security Journal: A Global Perspective, vol. 24, no. 1-3, pp. 57–71, Mar. 2015..

[4] C. McNab, Network security assessment: know your network, 2nd ed. Sebastopol, CA: OReilly, 2017.

[5] K. Ankunda, " The Application Of The Pareto Principle In Software Engineering", pp. 1-12, 2011.
[6] “Penetration Testing for IT Infrastructure,” Core Security, 11-Dec-2017. [Online]. Available: https://www.coresecurity.com/content/penetration-testing. [Accessed: 27-Jan-2018].

