Jurnal Teknologi Elektro, Universitas Mercu Buana
ISSN: 2086-9479

Implementasi Metode *Vulnerability* Dan *Hardening* Pada Sistem Keamanan Jaringan

Fadli Sirait
Program Studi Teknik Elektro, Fakultas Teknik
Universitas Mercu Buana
fadli.sirait@mercubuana.ac.id

M. Sofyan K. Putra
Program Studi Teknik Elektro, Fakultas Teknik
Universitas Mercu Buana
mohamad.sofyankp@gmail.com

***Abstrak*— Penggunaan aktivitas komputer meningkat dari hari ke hari, sebagian besar sistem yang terkomputerisasi sekarang telah terhubung ke jaringan internet. Semua aktivitas ini meningkatkan kerentanan dalam sistem terutama dalam bidang jaringan yang menuntut meningkatnya suatu kebutuhan akan kualitas keamanan jaringan. Kerentanan adalah potensi resiko bagi sebuah sistem dan penyerang memanfaatkan sebuah kerentanan ini untuk mengeksploitasi sistem sehingga penyerang mendapatkan akses dan informasi yang tidak sah. Hampir tidak mungkin memiliki sistem bebas kerentanan 100%, namun dengan mengurangi kerentanan dalam sebuah sistem dan jaringan sebanyak mungkin dapat meningkatkan keamanan jaringan. Dalam penelitian ini, melakukan optimalisasi keamanan jaringan dengan pemodelan penilaian kerentanan (vulnerability assessment) dan proses hardening pada sistem dan desain jaringan komputer untuk mengukur tingkat kerentanan dan mengkategorikan aset jaringan yang kritikal, yang selanjutnya dilakukan perbaikan pada sistem dan desain jaringan sesuai standar keamanan jaringan serta dari hasil penilaian tersebut menghasilkan panduan kebijakan prosedur keamanan jaringan pada perusahaan PT XYZ. Dengan metode vulnerability assessment dapat mengidentifikasi OS vulnerability (JunOS, IOS, Debian, Microsoft), Network vulnerability (Mac-Address, IP Address), Open port vulnerability (TCP/UDP), Engine application vulnerability (HTTP, FTP, NTP, Telnet, SSH) dan mengkategorikan tingkat kerentanan yang terbagi 4 kategori, yaitu Critical (10–9), High (8–7), Medium (6–5), Low (4–2), sedangkan hardening dapat meminimalkan tingkat resiko kerentanan dengan melakukan penguatan terhadap sistem, konfigurasi, dan desain topologi pada infrastruktur jaringan computer.**

Kata Kunci*— *Assessment, Keamanan Jaringan, Security, Vulnerability

I. PENDAHULUAN

Penggunaan komputer meningkat dari hari ke hari, kompleksitas sistem juga semakin meningkat. Semua aktivitas ini meningkatkan kerentanan dalam sistem. terutama dalam bidang jaringan menuntut meningkatnya suatu kebutuhan akan kualitas keamanan jaringan. Kerentanan adalah potensi resiko bagi sebuah sistem. Penyerang memanfaatkan sebuah kerentanan ini untuk mengeksploitasi sistem dan mendapatkan akses dan informasi yang tidak sah. Hampir tidak mungkin memiliki sistem bebas kerentanan 100%, namun dengan mengurangi kerentanan dalam sebuah sistem dan jaringan sebanyak mungkin dapat meningkatkan keamanan jaringan.

Dengan menggunakan Penilaian Kerentanan yang teratur dan efisien, dapat mengurangi sejumlah besar resiko untuk diserang dan memiliki sistem yang lebih aman.

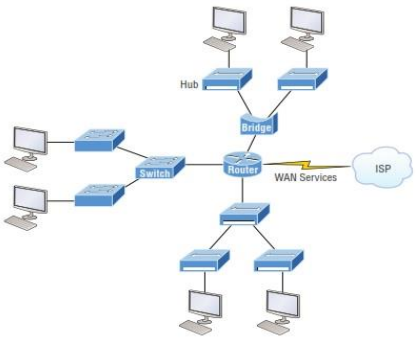
Kelemahan yang dimiliki oleh suatu sistem atau infrastruktur jaringan dapat terjadi dikarenakan kesalahan yang berasal dari faktor internal maupun eksternal.

Adapun proses *Vulnerability Assesment* dapat menggunakan alat/tools yang banyak pilihan yang bisa diambil alternatifnya, dari yang gratis, murah ataupun berbayar. Pada tugas akhir ini menggunakan tools *Nessus* (open source) dalam implementasinya.

II. LANDASAN TEORI

A. Konsep Jaringan Komputer

Jaringan komputer adalah sekumpulan peralatan komputer yang dihubungkan agar dapat saling berkomunikasi dengan tujuan membagi sumber daya. Dalam sebuah jaringan komputer dibutuhkan aturan-aturan (*protocols*) yang mengatur komunikasi dan layanan-layanan secara umum untuk seluruh sistem jaringan [7].



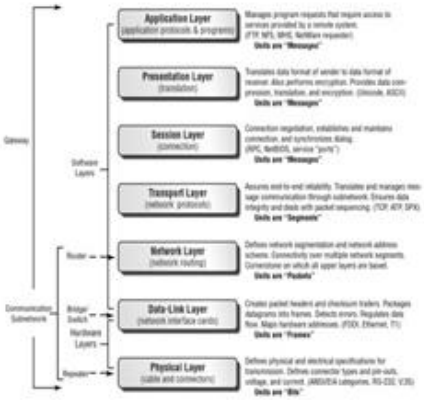
Gambar 1. *Internetworking*

Berdasarkan skala jaringan komputer dibagi atas 4 jenis, antara lain : LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), WAN (Wide Area Network). Dalam

perancangan desain, jaringan komputer dibagi berdasarkan topologi antara lain : Topologi Bus, Topologi Start, Topologi Tree, Topologi Ring, Topologi Mesh, Topologi Extended Star.

B. Model Referensi OSI

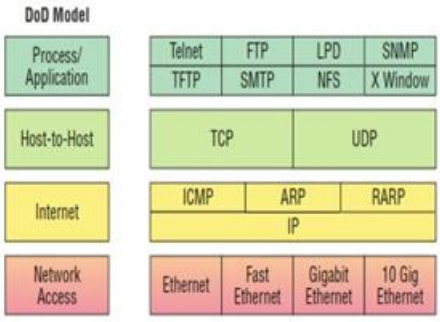
Layer OSI adalah membantu terjadinya transfer data antar host yang berbeda. Layer OSI (*Open System Interconnection*) tercipta pada akhir tahun 1970 oleh *International Organization for Standarization*. Layer OSI terdiri atas tujuh lapisan yaitu *Layer Application, Layer Presentation, Layer Session, Layer Transport, Layer Network, Layer Data Link, Layer Physical.*



Gambar 2. OSI Layer

C. TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) dibuat oleh DoD (*Department of Defense*) untuk memastikan dan menjaga integritas data sama seperti halnya menjaga komunikasi dalam situasi kekacauan perang [7].



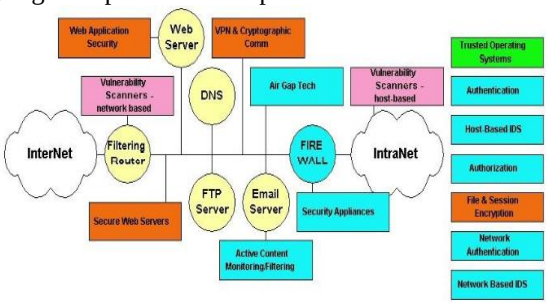
Gambar 3. TCP/IP Layer dan Protokol

D. Konsep Keamanan Jaringan

Komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada host yang tidak terhubung kemana-mana. Pada saat data terkirim dari suatu komputer asal menuju ke komputer tujuan dalam jaringan, data tersebut akan melewati sejumlah komputer-komputer yang lain yang berarti akan memberi kesempatan pada *hacker* untuk menyadap atau mengubah data tersebut. Berikut ini hal-hal yang harus dimengerti dalam perencanaan kebijakan (*policy*) dalam keamanan jaringan komputer meliputi resiko (*risk*), ancaman (*threat*), kelemahan (*weakness*), dan policy keamanan jaringan (*security policy*).

E. Topologi dan Perangkat Jaringan

Topologi jaringan komputer terdiri dari jaringan Internet publik yang menyebar ke seluruh dunia dan jaringan Intranet yang terdapat internal di perusahaan/institusi.



Gambar 4. Topologi Keamanan Jaringan

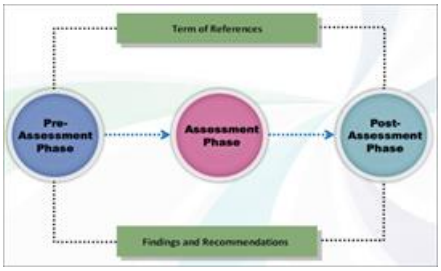
Perangkat keamanan jaringan yang digunakan dalam sebuah jaringan untuk dapat menghubungkan antar host ke host maupun antar host ke server, antara lain : Firewall, Router, Switch.

F. Insiden Keamanan Jaringan

Berikut ini jenis-jenis serangan mendasar yang sering terjadi pada jaringan, antara lain : IP Spoofing/Session Hijacking, Packet Snifer, DDoS, Man-in-the Middle, Back Door.

G. Vulnerabilty Assessment

Vulnerability Assessment adalah suatu langkah untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem atau infrastruktur jaringan komputer.



Gambar 5 Fase Vulnerability Assessment

H. Vulnerability Scanning

Aplikasi yang menjalankan security scan dan penilaian kerentanan sebenarnya menjalankan scanning dan kalkulasi, bukan pada bagaimana kerentanan dideteksi melainkan pada apa yang rentan. Berikut ini Fitur dan Faedah Vulnerability Scanner :

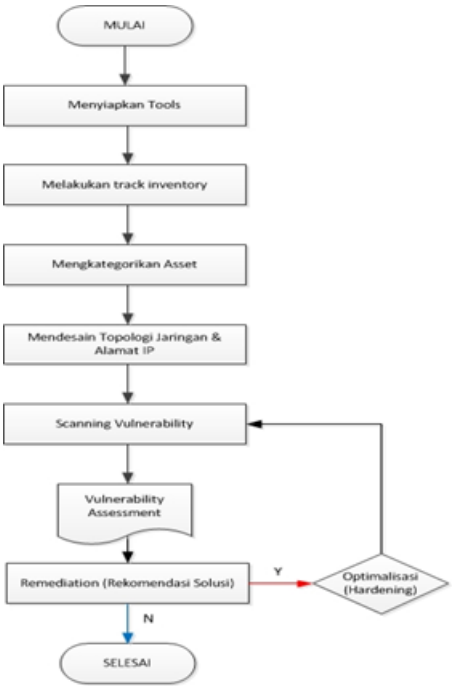
- Akurasi scan dan deteksi
- Dokumentasi dan dukungan
- Pelaporan
- Vulnerability Update

Gambar 6 Nessus

III. PEMODELAN DAN SIMULASI

A. Tahapan-Tahapan Penelitian

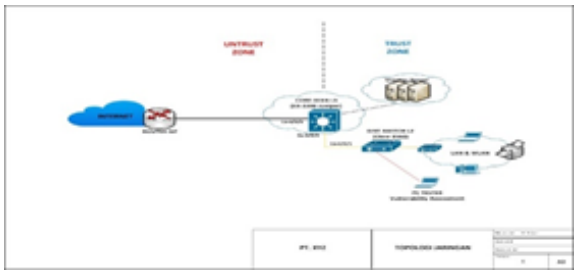
Sistem yang telah dibangun, secara garis besar terdiri dari blok rangkaian seperti terlihat pada gambar dibawah ini :



Gambar 7 Diagram Alir Implementasi

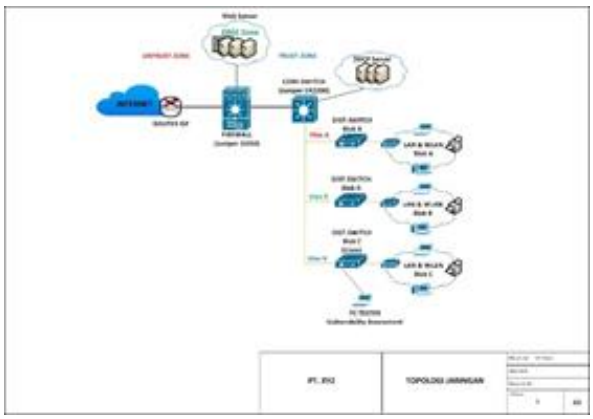
B. Desain Perancangan Implementasi

Dalam perancangan implementasi, terdapat 2 desain topologi jaringan yaitu desain topologi sebelum dioptimalkan dan desain topologi sesudah dioptimalkan.



Gambar 8 Desain Topologi Jaringan sebelum dioptimalisasi

Pada gambar 9 akan terdapat tambahan 1 buah Firewall sebagai penghubung dan pengatur lalu lintas trafik dari zona dmz dan zona trust ke zona untrust (internet), 1 buah Switch L3 (Core-Switch), 3 buah Switch L2 (Dist-Switch), Server (virtual) yang akan digunakan sebagai web server, 1 PC sebagai tester.



Gambar 9 Desain Topologi Jaringan setelah dioptimalisasi

C. Pendukung Implementasi

Pada implementasi ini perangkat dan sarana penunjang yang digunakan sesuai pada topologi jaringan, yaitu :

- 1 unit Firewall Juniper J2350
- 1 unit Switch Juniper EX2200
- 1 unit Cisco Switch C3560G
- 1 Unit Server (Web Server)
- 1 Unit Server (DHCP Server)
- Server yang digunakan yaitu Web Server yang menggunakan OS Debian 5 dan Debian 7.
- 1 Unit Laptop (Client)

Pada unit Laptop dibutuhkan software :

- SecureCRT
- Advanced Port Scanner
- Advanced IP Scanner

D. Konfigurasi Jaringan

Detail desain konfigurasi jaringan sebelum dioptimalisasi dapat dilihat pada tabel 1 berikut ini :

Tabel 1. Desain Konfigurasi Jaringan Pra dioptimalisasi

Perangkat	Port	IP Address	Netmask	Gateway	Sistem Operasi
CORE-WAN L3	ge-0/0/0	Uplink To Router ISP			Juniper (JunOS)
		27.50.23.139	255.255.255.248	27.50.23.137	
	Vlan 10 (PC-Client)	192.168.10.1	255.255.255.0		
	Vlan 50 (Server)	192.168.50.1	255.255.255.0		
	Vlan 305 (MGMT)	192.100.5.10	255.255.255.0		
	ge-0/0/1	Access To Web Server			
	ge-0/0/2	Trunk To SW-DIST			
DIST-SWITCH L2	Gi0/1	Trunk To Core-WAN (Vlan 10; 305)			Cisco (IOS)
	Gi0/2	Access Bridge To LAN (Vlan 10)			
Web-Server	Eth0	192.168.50.10	255.255.255.0	192.168.50.1	Debian 5
PC-Client (LAN)		192.168.10.5	255.255.255.0	192.168.10.1	Windows 7

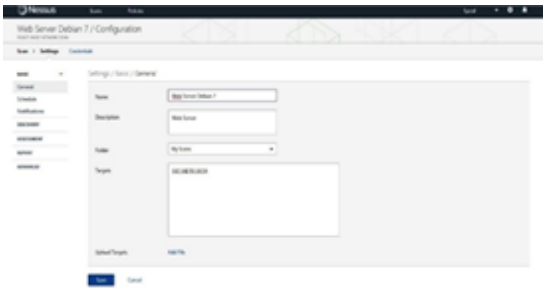
Detail desain konfigurasi alamat jaringan sesudah dioptimalisasi dapat dilihat pada tabel 2 berikut ini :

Tabel 2. Desain Konfigurasi Jaringan Pasca Optimalisasi

Perangkat	Port	IP Address	Netmask	Gateway	Sistem Operasi
Firewall	ge-0/0/0 (To ISP)	27.50.23.139	255.255.255.248	27.50.23.137	Juniper (JunOS)
	ge-0/0/1 (To Zona DMZ)	192.168.50.1	255.255.255.0	27.50.23.140 (NAT DMZ)	
	ge-0/0/2 (To Core-Switch)	192.168.100.1	255.255.255.252	27.50.23.141 (NAT Trust)	
Core-Switch L3	ge-0/0/2 (To Firewall)	192.168.100.2	255.255.255.252		Juniper (JunOS)
	Vlan 10 (PC-Client)	192.168.10.1	255.255.255.0		
	Vlan 20 (Server Farm)	192.168.20.1	255.255.255.0		
	Vlan 305 (MGMT)	192.100.5.10	255.255.255.0		
	ge-0/0/1	Access To Web Server			
	ge-0/0/2	Trunk To SW-DIST			
Dist-Switch L2	Gi0/1	Trunk (Vlan A; Vlan B; Vlan C)			Cisco (IOS)
	Gi0/2	Access (Vlan 10)			
Web-Server	Eth0	192.168.50.10	255.255.255.0	192.168.50.1	Debian 7
DHCP Server (Server Farm)	Eth0	192.168.20.x	255.255.255.0	192.168.20.1	CentOS 6
PC-Client		192.168.10.5	255.255.255.0	192.168.10.1	Windows 7

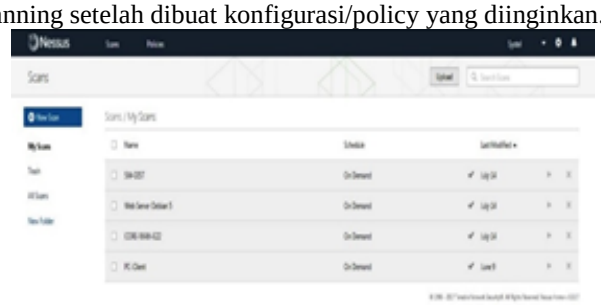
E. Konfigurasi Nessus

Pada gambar 10, diminta untuk menentukan nama scanning, keterangan, policy yang digunakan, dan daftar alamat jaringan (ip address) komputer yang dijadikan target.



Gambar 10 Konfigurasi scanning host

Pada gambar 11, menampilkan daftar host target yang siap discanning setelah dibuat konfigurasi/policy yang diinginkan.



Gambar 11. Daftar host target scan

F. Vulnerability Assessment dan Remediation

Semua informasi yang diperoleh dari aplikasi tools vulnerability scanning, akan disimpan ke dalam komputer untuk dijadikan proses security assessment dalam bentuk report.

Data yang ditemukan dari aplikasi tools Vulnerability scanning, seperti :

a. OS vulnerability
b. Service vulnerability
c. Open port vulnerability
d. Engine website vulnerability

Selanjutnya merekomendasikan rencana perbaikan dari hasil vulnerability assessment yang dikategorikan menjadi 4 tingkatan, yaitu:

1. Sangat Tinggi (Critical) : pada level ini terdapat kelemahan yang berpotensial tinggi menjadi ancaman, sedangkan fitur ataupun langkah untuk tingkat pencegahan maupun penanganannya tidak memadai.
2. Tinggi (High) : pada level ini cakupan kelemahan lebih kecil dibandingkan level sebelumnya. Namun, upaya pencegahan dan penanganan masih tidak memadai.
3. Sedang (Medium) : pada level ini tingkatan kelemahan bersifat lokal dan upaya penanganan dan pencegahan pun bersifat lokal.
4. Rendah (Low) : tingkat kelemahan rendah dan upaya pencegahan dan penanganan yang diharapkan pun sangat memadai.

G. Hardening

Prosedur yang meminimalkan ancaman yang datang dengan mengatur konfigurasi dan menonaktifkan aplikasi dan layanan yang tidak diperlukan. Instalasi firewall, instalasi antivirus, menghapus cookie, membuat password, menghapus program yang tidak diperlukan [14]. Tujuan dari Hardening adalah untuk menghilangkan resiko ancaman yang bisa terjadi pada komputer, hal ini biasanya dilakukan dengan menghapus semua program/file maupun port-port (tcp/udp) yang tidak diperlukan.

IV. PENGUJIAN DAN ANALISA

A. Pengujian Vulnerability Assessment Tahap 1 (Pra-Optimalisasi)

Berikut Tabel 3, perangkat/aset jaringan yang akan dilakukan pengujian dengan vulnerability scanning.

Tabel 3. Perangkat yang diuji Tahap I

No	Network Node	Operating System	IP Address	Fungsi
1	CORE-WAN	JunOS	27.50.23.139	Core-Switch
2	DIST-SWITCH	IOS	192.100.5.7	Switch Akses
3	Server	Debian 5	192.168.50.10	Web-Server
4	PC-Client	Windows 7	192.168.10.5	Client (End User)

Setelah mengetahui hasil-hasil kerentanan pada aset dan kondisi infrastruktur jaringan komputer yang didapat dari pemetaan desain topologi jaringan sebelum dilakukan optimalisasi, maka langkah selanjutnya membuat Vulnerability Assessment yang digunakan untuk menganalisa dan menilai tingkat resiko kerentanan pada sistem dan infrastruktur jaringan terhadap keamanan jaringan yang nantinya akan direkomendasikan untuk dilakukan perbaikan pada sistem jaringan komputer.

Tabel 4. Vulnerability Assessment Hasil Uji Tahap I

No	Device	Finding Title	Vulnerability Assessment				Remediation Recommendations
			Critical	High	Medium	Low	
1	CORE-WAN	System Security	1				Update Junos Version
		Account Security		3			Disable Telnet, Use with SSH-2.
		Configuration Security		3	15	1	Use with SNMPv2 & SNMP Community String, Do not use Proxy ARP, Port Security, DHCP Snooping, etc.
2	DIST-SWITCH	System Security	1				Update Junos Version
		Account Security		9			Disable Telnet, Use with SSH-2.
		Configuration Security		10	7	1	Use with SNMPv2 & SNMP Community String, Do not use Proxy ARP, Port Security, Root Guard, BPDU Guard, etc.
3	Server	System Security	1				Update OS Patch & Repository, Install Packet Firewall, Proteksi boot loader
		Account Security			2		Use with SSH-2, Management Password
		Configuration Security			1	2	Use with SNMPv2, SNMP Community String, Disable Ctrl-Alt-Delete, Prevent IP Spoofing, Disable ports unused, Disable information Web Server & PHP on Web Browser, Runtime Back-Up
4	PC-Client	System Security	2				Update OS Patch
		Account Security			5		Protect password
		Configuration Security			5	2	Disable ports unused, Disable RDP, Update Antivirus, Disable Sharing

B. Proses Hardening

Proses hardening yang dilakukan, antara lain sebagai berikut :

Tabel 5. Sampling Hardening perangkat Core-WAN-L3

Item	Hardening	Command / Description
1	Require Current Software	The router should run current software
2	Forbid Root Password Authentication	[edit] root#**show system authentication-order | match "password" | count**
3	Forbid Default Login Classes for all Users Accounts	[edit] user@CORE-WAN-L3#**show system login | match "class" | match "superuser|super-user|read-only|operator|unauthorized" | count**
4	Require login message	[edit] user@ CORE-WAN-L3#**show system login message**
5	Require SSH	[edit] user@ CORE-WAN-L3#**show system services ssh**
6	Require external SYSLOG server	[edit] user@ CORE-WAN-L3#**show services | match „syslog host * any "" | count**
7	Require External Time Sources	[edit] user@ CORE-WAN-L3#**show system ntp | match server | except boot-server | count**
8	Forbid Router Model in Hostname	[edit] user@ CORE-WAN-L3#**set system host-name Core-Switch**
9	Require UTC Timezone	[edit] user@ CORE-WAN-L3#**set system time-zone Asia/Jakarta**
10	Restrict and Secure SNMP Access	[edit snmp] user@ CORE-WAN-L3#**set community pu5d4t1n!! Ro**

C. Pengujian Vulnerability Assessment Tahap II (Pasca-Optimalisasi)

Berikut Tabel 6, perangkat/aset jaringan yang akan dilakukan pengujian dengan vulnerability scanning yang telah dilakukan proses Hardening

Tabel 6. Perangkat yang diuji Tahap II

Item	Hardening	Command / Description
1	Require Current Software	The router should run current software
2	Forbid Root Password Authentication	[edit] root#**show system authentication-order | match "password" | count**
3	Forbid Default Login Classes for all Users Accounts	[edit] user@CORE-WAN-L3#**show system login | match "class" | match "superuser|super-user|read-only|operator|unauthorized" | count**
4	Require login message	[edit] user@ CORE-WAN-L3#**show system login message**
5	Require SSH	[edit] user@ CORE-WAN-L3#**show system services ssh**
6	Require external SYSLOG server	[edit] user@ CORE-WAN-L3#**show services | match „syslog host * any "" | count**
7	Require External Time Sources	[edit] user@ CORE-WAN-L3#**show system ntp | match server | except boot-server | count**
8	Forbid Router Model in Hostname	[edit] user@ CORE-WAN-L3#**set system host-name Core-Switch**
9	Require UTC Timezone	[edit] user@ CORE-WAN-L3#**set system time-zone Asia/Jakarta**
10	Restrict and Secure SNMP Access	[edit snmp] user@ CORE-WAN-L3#**set community pu5d4t1n!! Ro**

Berikut tabel 7, hasil penilaian kerentanan (vulnerability assessment) yang yang telah dilakukan proses Hardening

Tabel 7. Vulnerability Assessment Hasil Uji Tahap II

No	Device	Finding Title	Vulnerabilities				Remediation Recommendations
			Critical	High	Medium	Low	
1	Firewall-WAN	System Security					
		Account Security					
		Configuration Security					
2	Core-Switch	System Security					
		Account Security				2	
		Configuration Security			1		
3	Dist-Switch	System Security					
		Account Security					
		Configuration Security			1		
4	Server	System Security					
		Account Security					
		Configuration Security			1		

D. Analisis Data

Setelah dilakukan uji perbandingan penilaian kerentanan (vulnerability assessment) tahap 1 dan tahap 2, maka dilakukan analisis apakah keamanan jaringan komputer yang diberlakukan sudah memenuhi standar referensi keamanan yang mengacu pada SANS dan ID-SIRTII.

1. Analisis Berdasarkan Desain Topologi Jaringan

Arsitektur desain jaringan yang ideal harus mencakup seperti Layer Security, Layer Core, Layer Distribusi, Layer Access. Hal ini dilakukan dengan tujuan untuk melindungi aset-aset kritikal yang terhubung dalam jaringan komputer, baik dengan melakukan filterasi, membatasi ataupun menolak suatu permintaan koneksi dari layanan luar jaringan (internet) maupun dari dalam jaringan (intranet) berdasarkan sumber atau tujuan, berdasarkan isi, dan menggunakan DMZ sebagai perantara area jaringan internal dan area jaringan internet dengan memberi isolasi fisik antara kedua jaringan yang didukung oleh serangkaian konektivitas pada firewall.

2. Analisis Berdasarkan Sistem dan Konfigurasi

Berdasarkan kategori kerentanan yang terbagi pada pengujian yang telah dilakukan, antara lain:

a. Sangat Tinggi (Critical) = 10 - 9
b. Tinggi (High) = 8 - 7
c. Sedang (Medium) = 6 - 5
d. Rendah (Low) = 4 – 2

3. Analisis Berdasarkan Kebijakan Peraturan (SOP)

Kelemahan yang dimiliki dari suatu sistem atau infrastruktur jaringan komputer dapat terjadi dikarenakan kesalahan yang berasal dari faktor internal maupun faktor eksternal. Faktor internal, dikarenakan kurangnya kesadaran administrator atau orang yang berperan sebagai admin dalam menjalankan sistem aplikasi tersebut, sedangkan faktor eksternal bisa terjadi dikarenakan lemahnya sistem yang dibuat (configuration) dan besarnya tingkat kejahatan cyber. Hal ini mendasari perlunya langkah awal yang paling penting untuk melindungi dan mengamankan jaringan dengan membuat kebijakan-kebijakan yang terstandarisasi guna sebagai panduan operasional (Standart Operating Procedur) keamanan jaringan. Penilaian kerentanan (vulnerability) pada pengujian tahap II berkurangnya celah kerentanan pada perangkat jaringan hingga host.

V. KESIMPULAN

Berdasarkan analisa dari hasil simulasi yang telah dilakukan pada tugas akhir ini, dapat diambil beberapa kesimpulan, diantaranya adalah :

1. Dengan metode vulnerability assessment dapat membantu mengidentifikasi, mengkategorikan serta meminimalkan tingkat resiko kerentanan pada infrastruktur jaringan komputer melalui proses pemindaian (scanning) berupa:

- Operating System vulnerability (JunOS, IOS, Debian, Microsoft)
- Network vulnerability (Mac-Address, IP Address)
- Open port vulnerability (TCP/UDP)
- Engine application vulnerability (HTTP, FTP, NTP, Telnet, SSH)

Dan berdasarkan kategori kerentanan dan penilaian (score) tingkat kerentanan yang segera untuk dilakukan perbaikan terbagi 4 kategori, antara lain:

a. Sangat Tinggi (Critical)
Score Kerentanan : 10 – 9
b. Tinggi (High)
Score Kerentanan : 8 – 7
penanganan perbaikannya.
c. Sedang (Medium)
Score Kerentanan : 6 – 5
d. Rendah (Low)
Score Kerentanan : 4 – 2

2. Dengan Metode Hardening yang dilakukan dapat mengetahui hasil perbandingan pengujian tahap 1 dan tahap 2 pada sistem dan jaringan, dari hasil pengujian tahap 1 terdapat total celah kerentanan (vulnerability) yang terdeteksi sebanyak 71 alerts, sedangkan dari hasil pengujian tahap 2 total celah kerentanan (vulnerability) yang terdeteksi sebanyak 4 alerts. Dari hasil perbandingan tersebut dan berdasarkan analisis yang dilakukan dapat diketahui banyaknya kerentanan yang disebabkan oleh lemahnya konfigurasi, tidak updatenya sistem, port-port komunikasi seperti SNMP (Port UDP 161) yang tidak digunakan terbuka, tidak supportnya enskripsi untuk remote akses yang menggunakan Telnet, dan aplikasi dan layanan yang tidak diperlukan terinstal.

3. Beberapa dampak yang kemungkinan dapat menjadi ancaman terhadap perusahaan yang disebabkan kelemahan sistem infrastruktur jaringan, antara lain:

a. Loss of Integrity : hilangnya integritas sistem dan data.

b. Loss of Availability : hilangnya keberadaan atau kehandalan sistem dan data.
c. Loss of Confidentiality : hilangnya kerahasiaan dari informasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada tim editorial Jurnal Teknologi Elektro atas dipublikasikannya penelitian ini.

DAFTAR PUSTAKA

[1] J. Hallberg, A. Hunstad, and M. Peterson. "A Framework for System Security Assessment," IEEE Workshop on Information Assurance, 2005.

[2] Hussain M.J. Almohri, Layne T.Watson, Danfeng Yao, Xinming Ou. "Security Optimization of Dynamic Network with Probabilitas Graph Modeling and Linier Programming," IEEE Transactions on Dependable and Secure Computing, 2015.

[3] Sudhir Kumar Pandey, Vivek Kumar Yadav, S. Kumar, S. Verma, P. Dansena. "Implementation of A New Framework for Automated Network Security Checking and Alert System," IEEE Eleventh International Conference on Wireless and Optical Communications Networks, 2014

[4] F. Leitold, K. Hadarics, E. Oroszi, K. Gyorffy. "Measuring the information security risk in an infrastructure," IEEE International Conference on Malicious and Unwanted Software (MALWARE), 2015.

[5] Y. Wei, G. Ling. "Design Implemetation of Evolution-Based Vulnerability Assessment System," IEEE International Symposium on Computer, Communication, Control and Automation (3CA), 2010.

[6] "Methodology Vulnerability Assessment", diakses tanggal 30 Juni 2017. https://govcsirt.kominfo.go.id/254/

[7] Lammle, Todd. 2005. Cisco Certified Network Associate Study Guide. Elex Media Komputindo: Jakarta.

[8] Eko Indrajit, Richardus. 2016. Keamanan Informasi dan Internet. Yogyakarta: Preinexus.

[9] Thomas, Tom. 2005. Network Security First-Step. Yogyakarta: ANDI.

[10] Purbo, Onno W. (2011). Buku Keamanan Jaringan. Jakarta

[11] "Tenable Nessus Scanner", diakses tanggal 1 Juli 2017. www.tenable.com/product/nessus

[12] "Type of Vulnerability Assessment", diakses tanggal 1 Juli 2017. http://edysusanto.com/type-of-vulnerability-assessment/

[13] Mansyurin, Pudja. 2009. Konfigurasi Debian Server GNU/Linux TKJ. Jakarta: Al-Mansyurin Informatika Team.

[14] Azis Kurniawan. 2017. Server Hardening. Cetakan ke-1. Jakarta: LEMSANEG.

[15] Doddy Ferdiansyah, "Vulnerability Assessment Terhadap Jaringan Untuk Keamanan Informasi," Jurnal Konferensi Nasional Sistem Informasi, (STMIK Diponegoro Makassar, Maret 2014)

[16] "Vulnerability Assessment Report", diakses tanggal 22 Juli 2017. www.sans.org/reading-room/whitepapers/basics/vulnerability-assessment

[17] SANS Institute. 2014. Router and Switch Security Policy. Australia: SANS.

[18] S'to. 2014. Kali Linux 200% Attack. Jakarta: Jasakom.