IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT AND PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

TUGAS AKHIR

MUHAMMAD ANDI WIBOWO
41517120083

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
MUHAMMAD ANDI WIBOWO
41517120083

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

LEMBAR PERNYATAAN ORISINALITAS

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41517120083
Nama	:	Muhammad Andi Wibowo
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 20 januari 2022

Muhammad Andi Wibowo

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Muhammad Andi Wibowo
NIM	:	41517120083
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 20 Januari 2022

Muhammad Andi Wibowo

iii

SURAT PERNYATAAN LUARAN TUGAS AKHIR

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Muhammad Andi Wibowo
NIM	:	41517120083
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	V
		Jurnal Nasional Terakreditasi	V		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Teknologi Informasi dan Ilmu Komputer		
		ISSN	: 2503-1619		
		Link Jurnal	: https://jurnal.iicet.org/		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Mengetahui
Dosen Pembimbing TA

Muhammad Rifqi, S.Kom, M.Kom

Jakarta, 20 Januari 2022

Muhammad Andi Wibowo

LEMBAR PERSETUJUAN PENGUJI

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120083
Nama	:	Muhammad Andi Wibowo
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 20-01-2022

(Wawan Gunawan, S.Kom, MT)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120083
Nama	:	Muhammad Andi Wibowo
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 20-01-2022

(Emil R. Kaburuan, Ph.D.)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120083
Nama	:	Muhammad Andi Wibowo
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 20-01-2022

(Dr. Nenden Siti Fatonah, S.Si., M.Kom)

LEMBAR PENGESAHAN

NIM	:	41517120083
Nama	:	Muhammad Andi Wibowo
Judul Tugas Akhir	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS PT MESCO MITRA ADITAMA)

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, <diisi tanggal-bulan-tahun sidang>

Menyetujui,

(Muhammad Rifqi, S.Kom, M.Kom)
Dosen Pembimbing

Mengetahui,

(Wawan Gunawan, S.Kom, MT)	(Emil R. Kaburuan, Ph.D.)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Muhammad Andi Wibowo
NIM	:	41517120083
Pembimbing TA	:	Muhammad Rifqi, S.Kom, M.Kom
Judul	:	IMPLEMENTASI AUTOMATION VULNERABILITY ASSESSMENT DAN PATCHING PADA LINUX SERVER (STUDI KASUS DI PT MESCO MITRA ADITAMA)

Di zaman yang semakin berkembang seperti ini, kebutuhan akan security pada sebuah system berkembang pesat terutama pada bisnis skala *enterprise*. Pada saat ini setiap perusaahaan sangat membutuhkan security system yang mampu untuk mencegah adanya celah yang di timbulkan pada *software* yang di gunakan pada *server.*Perkembangan teknologi yang sangat cepat menimbulkan banyak perusahaan yang baru berdiri sehingga banyak juga terciptanya website baru yang dimana menggunakan perangkat server terutama linux sebagai insfrastrukturnya. Oleh karenanya para perusahaan saat ini membutuhkan adanya sebuah system yang mampu memonitor dan mencegah celah – celah yang ditimbulkan oleh sebuah software yang digunakan pada server mereka. Untuk menunjang kebutuhan tersebut perusahaan memerlukan sistem management *vulnerability management* yang baik, andal dan efektif. Pada umumnya proses dari *vulnerability assessment* dan *patching* merupakan kedua hal yang berbeda dan terpisah dalam administrasinya sehingga kurang efektif untuk perusahaan berskala enterprise yang memiliki banyak server untuk kebutuhan baik *staging* maupun *production*. Dalam penelitian ini dibahas mengenai implementasi *Automation vulnerability assessment* dan *patching* pada *linux server* (Studi kasus di PT Mesco Mitra Aditama). Dari hasil penelitian ini menunjukan bahwa dengan integrasi sistem ini diharapkan dapat meningkatkan ke efektifan dan ke andalan untuk memanaged *vulnerability* yang terdapat pada sebuah server dan melakukan *patching* sebagai *remediation* terhadap *software* yang memiliki kerentanan sekaligus memudahkan administrator dalam memanage terhadap keamanan *server* perusahaan.

Kata kunci:
Vulnerability assessment, *Patching*, *Automation,* Ilmu komputer, Universitas mercu buana

ABSTRACT

Name	:	Muhammad Andi Wibowo
Student Number	:	41517120083
Counsellor	:	Muhammad Rifqi, S.Kom, M.Kom
Title	:	*IMPLEMENTATION OF AUTOMATION VULNERABILITY ASSESSMENT AND PATCHING IN LINUX SERVER (CASE STUDY AT PT MESCO MITRA ADITAMA)*

In an era that is increasingly developing like this, the need for security in a system is growing rapidly, especially in enterprise-scale businesses. At this time every company really needs a security system that is able to prevent any gaps caused by the software used on the server. Rapid technological developments have led to many new companies being founded so that many new websites are also created which use server devices, especially Linux. as the infrastructure. Therefore, today's companies need a system that is able to monitor and prevent loopholes caused by software used on their servers. To support these needs, companies need a good, reliable and effective management vulnerability management system. In general, the process of vulnerability assessment and patching are two different and separate things in their administration so that they are less effective for enterprise-scale companies that have many servers for both staging and production needs. This study discusses the implementation of Automation vulnerability assessment and patching on a linux server (a case study at PT Mesco Mitra Aditama). The results of this study indicate that with this system integration, it is expected to increase the effectiveness and reliability for managing vulnerabilities contained in a server and doing patching as a remediation of software that has vulnerabilities while making it easier for administrators to manage security on company servers.

Key words:
Vulnerability assessment, *Patching*, *Automation,* computer science, universitas mercu buana

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT yang telah memberikan nikmat kesehatan kepada penulis untuk dapat melakukan kegiatan penelitian tugas akhir yang bertujuan untuk menyelesaikan program studi pada universitas mercu buana Penulis menyadari bahwa tanpa bantuan dan bimbingan dari banyak pihak, penulisan penelitian tugas akhir yang penulis lakukan untuk menyelesaikan program studi di universitas mercu buana tidaklah mudah. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Kedua Orang Tua penulis karena sudah memberikan semangat dan selalu mendoakan penulis agar dapat menyelesaikan penulisan penelitian tugas akhir pada universitas mercu buana
2. Bapak Muhammad Rifqi, S.Kom, M.Kom selaku dosen pembimbing tugas akhir yang sudah membimbing penulis dalam proses penulisan tugas akhir hingga dapat menyelesaikan dengan baik dan benar
3. Bapak Herry Derajad Wijaya, S.Kom,MM selaku dosen pembimbing metodologi penelitian teknologi informasi yang sudah memberikan bimbingan dan arahan kepada penulis selama proses penentuan judul dan metodologi yang penulis lakukan untuk proses penelitian tugas akhir
4. Bapak Wibawanto selaku Direktur Utama PT Mesco Mitra Aditama yang telah memberikan izin kepada penulis untuk melakukan penelitian di perusahaan yang bapak pimpin.
5. Bapak Mahmud, S,Si selaku Kepala Divisi Teknologi Informasi PT Mesco Mitra Aditama yang telah membantu penulis dalam pengambilan data yang di butuhkan dalam proses penelitan yang penulis lakukan.

Akhir kata, penulis berharap penelitian yang penulis lakukan dapat bermanfaat pada masyarakat luas dan khususnya pada perusahaan yang penulis lakukan penelitian

Jakarta, 31 Desember 2021
Muhammad Andi Wibowo

DAFTAR ISI

NASKAH JURNAL

I.PENDAHULUAN

Perkembangan jaringan komputer dan internet yang begitu pesat telah membawa dampak dan manfaat bagi pengguna, baik dari instansi pemerintahan, perusahaan dan perorangan. Setiap perusahaan mengharapkan dengan adanya kehadiran Teknologi informasi dapat membantu perusahaan meningkatkan kinerja mereka. Tidak hanya meningkatkan kinerja tetapi juga untuk meningkatkan keamanan *server-server* yang berisikan data private dari pihak yang tidak berwenang.

PT Mesco Mitra Aditama merupakan sebuah perusahaan yang bergerak di bidang konstruksi stainless steel yang berada di Jakarta. Pada perusahaan ini, teknologi merupakan salah satu aset yang sangat berharga karena tanpa teknologi di dalamnya maka operasional perusahaan akan terganggu. Salah satu teknologi yang harus ada dalam operasional perusahaan yaitu *database server* yang menggunakan *operating system linux* server dimana perusahaan menyimpan data-data penting perusahaan di *database server* internal perusahaan. Data yang di simpan seperti data keuangan, pajak, marketing dan aset penting perusahaan. Dengan adanya *database server* yang merupakan sisi sentral perusahaan, tidak hanya infrastruktur akan tetapi aspek keamanan harus sangat diperhatikan. Untuk Keamanan jaringan pada PT Mesco Mitra Aditama menggunakan Firewall Fortigate sebagai garda terdepan untuk menangkal serangan yang ditujukan untuk PT Mesco Mitra Aditama. Untuk keamanan pada sisi server , Divisi IT PT Mesco Mitra Aditama melakukan pengamanan dengan melakukan *vulnerability assessment* untuk mengidentifikasi kerentatanan pada *server-server* yang dimiliki PT Mesco Mitra Aditama. Setelah mendapatkan hasil dari proses *vulnerability assessment* yang dilakukan secara manual dan dilakukan satu persatu, Divisi IT akan melakukan *planning* untuk melakukan *remediation* pada kerentanan yang di dapatkan dari hasil *vulnerability assessment.* Aksi *remediation* yang di lakukan adalah melakukan *patching* pada *software* yang memiliki kerentanan. *Patching* pada PT Mesco Mitra Aditama masih dilakukan secara manual dan dilakukan satu persatu. Proses *vulnerability assessment* dan *patching* yang dilakukan manual dan satu persatu menimbulkan ketidak efesiensinya waktu dan tidak termonitoring nya *server* yang memiliki kerentanan dikarenakan jumlah *server* yang dimiliki PT Mesco Mitra Aditama bisa di bilang cukup banyak. Dengan metode manual ini dan tidak adanya sistem yang dapat memonitoring secara sentral, Divisi IT PT Mesco Mitra Aditama merasa kewalahan. Oleh karena itu dibutuhkan sebuah sistem yang dapat memonitoring kerentanan *server-server* yang dimiliki PT Mesco Mitra Aditama secara sentral dan dapat melakukan otomatisasi demi menciptakan efisiensi waktu dan melakukan penanganan remediasi dengan cepat untuk menghindari berbagai kerentanan yang muncul seperti *Zero Day* dan kerentanan lainnya. Dibutuhkan juga sebuah metode untuk menghindari *rebooting server* apabila terdapat *kernel patching* terkait dengan *security patch.*

Dari permasalahan yang terjadi diatas terdapat beberapa kerugian yang dialami oleh PT Mesco Mitra Aditama yaitu waktu yang di butuhkan untuk melakukan proses *vulnerability assessment* dan *patching* secara manual , tidak terpusatnya monitoring pada *server* yang dimiliki menimbulkan adanya *server* yang tidak termonitor, proses *patch* yang dilakukan menimbulkan adanya *human error* yang mengakibatkan kesalahan *patch* pada *software* yang memiliki kerentanan dan bisa menimbulkan adanya kerentanan baru, terganggunya kegiatan operasional karyawan dikarenakan proses tersebut dan mendapatkan resiko adanya *down time* pada *server production* apabila memiliki kerentanan pada *linux kernel.*

Untuk mengatasi permasalahan tersebut penulis menggunakan Teknologi *Automation Vulnerability Assessment* dan *patching* dengan di integrasikan dengan metode *Live Patching* . Integrasi ini sangat membantu dalam mengatasi masalah kerugian perusahaan karena sistem monitoring *server* menjadi terpusat, proses *vulnerability assessment* dan *patching* dilakukan secara otomatis sehingga

meminimalisir ketidak efisiensinya waktu , *rebooting server* dan *human error* .

II.LANDASAN TEORI

Penelitian ini merujuk pada penelitian-penelitian terdahulu yang ada kaitannya dengan *Vulnerability assessment*, *Patch Management, Centralized Management,* Adapun *system* atau *software* yang diperlukan dalam penelitian ini diantaranya adalah :

2.1.Linux

Gambar 1. Linux

Linux adalah *operating system* (OS) atau sistem operasi yang berbasis GNU/Linux yang bersifat *Open Source* dan memiliki banyak varian seperti Debian, Slackware, Open Suse, Archlinux, Redhat dan sebagainya.

2.2.Windows Server

Gambar 2. Windows Server

Seperti halnya *linux*, Windows server adalaah salah satu *operating system* (OS) yang dikeluarkan oleh Microsoft. Beda halnya dengan *linux* yang merupakan *operating system* yang bersifat *Open Source,* Windows Server memerlukan *license* untuk aktifasinya. Banyak varian Windows server seperti version 2008, 2012, 2016 dan 2019 .

2.3.*IP Address*

Alamat IP (Internet Protokol Address) adalah deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk setiap *computer host* dalam jaringan internet. Panjang dari angka ini adalah 32-bit (untuk IPV4) dan 128-bit (untuk IPv6) yang menunjukan alamat dari computer tersesebut berbasis TCP/IP. Dalam pengertian lain, *Internet Protokol* (IP) address dapat diartikan sebagai alamat numeric yang ditetapkan untuk sebuah komputer yang berpartisipasi dalam jaringan komputer yang memanfaatkan Internet Protokol untuk komunikasi antara node-nya.

2.4.*Manage Engine*

Manage Engine adalah sebuah sistem atau software *vulnerability management* untuk multiplatform *operating system*. Pada sistem *vulnerability management* terdapat *vulnerability database* yang digunakan untuk menyimpan infromasi tentang kerentanan terbaru dan akan selalu update . *Vulnerability management* juga memiliki fitur untuk melakukan *vulnerability scan* dan *deployment patch* .

2.5.Moba XTerm

Moba Xterm adalah salah satu *software* yang berbasis *Open Source* digunakan untuk keperluan SSH Client, Telnet dan SFTP.
Pada penelitian ini lebih digunakan untuk SSH Client untuk terkoneksi dengan *linux server* dan SFTP untuk melakukan transfer file pada *linux server*.

III. METODE PENELITIAN

Penelitian ini bertujuan untuk mengembangkan *Vulnerability assessment* dan *patch* yang biasanya digunakan secara manual dan terpisah, penulis menggunakan *Vulnerability Management* ini dengan tujuan

lain yaitu melakukan otomatisasi *vulnerability assessment* dan *patch* yang di integrasikan dengan metode *live patch*.

Penelitian ini termasuk ke dalam metode penelitian pengembangan *(research and development)*. Penelitian ini merupakan hasil pengembangan dan fungsi baru dari penelitian-penelitian yang telah ada sebelumnya. Dari penelitian tersebut dikembangkan dengan melakukan pengumpulan data dan studi literatur dengan membandingkan *Vulnerability management* dan metode yang tepat dari berbagai sumber sehingga menghasilkan *Vulnerability Management* yang cocok untuk perusahaan berskala enterprise.

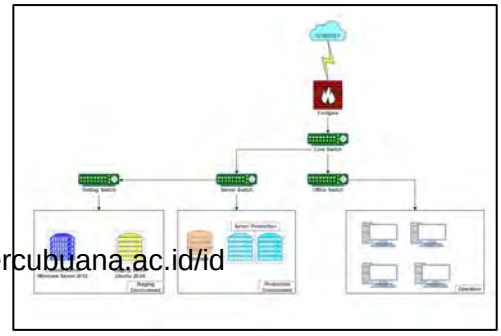
Penelitian ini dibangun menggunakan sistem operasi Linux sebagai target server dan Windows Server sebagai *vulnerability management* dan beberapa *software* pendukung. Penelitiaan ini menekankan bagaimana cara perusahaan dapat mendapatkan *Vulnerability Management* yang cocok untuk perusahaan berskala *Enterprise* dan untuk menunjang ke efektifan perusahaan.

A. Analisis Sistem

Analisis sitem pada penelitian kali ini adalah sebagai berikut :

1. Melakukan wawancara kepada pihak terkait agar dapat dianalisa permasalahan yang ada saat ini. Dalam hal ini permasalahan yang ada adalah meningkatkan keamanan pada *linux server*, ketidak efektifan waktu pada proses *vulenerability assessment* dan *patching*, adanya *case human error* pada proses tersebut.
2. Melakukan Studi literatur terhadap jurnal dengan permasalahan serupa terkait dengan *vulnerability assessment* dan *patching* yang sudah pernah diteliti sebelumnya, hal ini bertujuan agar dapat dilakukan evaluasi–evaluasi terhadap informasi-informasi yang berkaitan

B. Desain Topologi



Gambar 3. Design Topologi jaringan

Pada gambar diatas merupakan topologi yang di gunakan pada infrastruktur PT Mesco Mitra Aditama. Peneliti menggunakan testing switch yang terhubung dengan server switch untuk terkoneksi dengan network PT Mesco Mitra Aditama. Peneliti mendapatkan izin akses untuk melakukan testing pada *staging environment.* Pada testing switch di *assign* menggunakan vlan testing yang sudah ada sebelum penelitian ini. Penelitian ini menggunakan *staging environment* dengan tujuan agar terisolasi dari *production environment* dan meminimalisir terganggunya proses operasional yang sedang berjalan pada PT Mesco Mitra Aditama.

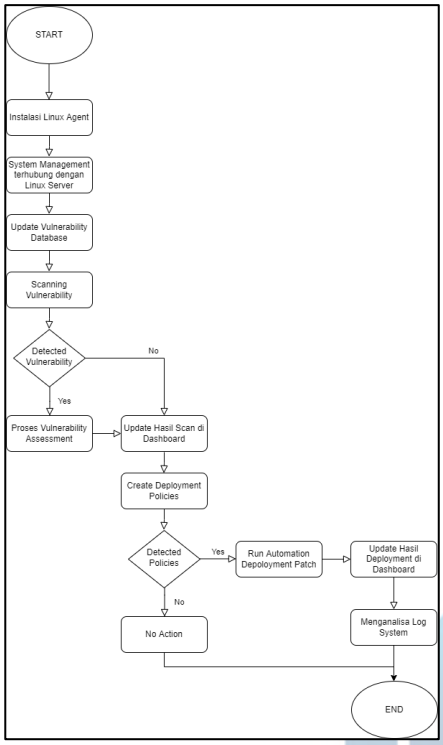
Peneliti menggunakan Server yang sudah berjalan dan disediakan pada s*taging environment*. Adapun detail mengenai perangkat *hardware* dan *software* yang di gunakan pada penelitian ini.

Spesifikasi Hardware dan Software

Untuk merancang infrastruktur ini, kebutuhannya meliputi *hardware* dan *software.* Berikut ini adalah kebutuhan hardware yang digunakan:

Hardware	Spesifikasi	
Server	Operating System	Windows Server 2012
	CPU Cores	4
	RAM	4 GB
	Storage	50 GB
	LAN Port	1
	Software	Manage Engine
Virtual Server	Operating System	Ubuntu Server 20.04
	CPU Cores	2
	RAM	2 GB
	Storage	30 GB
	Software	Canonical
cisco Switch	Memory	256 MB
	Flash Memory	64 MB

C. Alur Kerja Sistem



Gambar 4. Alur kerja sistem

Pada *flowchart* diatas menjelaskan bagaimana tahapan proses *automation vulnerability assessment* dan *patching*. Mulai dari sistem melakukan *Updating vulnerability database, automation vulnerability scanner* berjalan, apabila target *server* terdeteksi memiliki kerentanan sistem akan melakukan assessment terhadap kerentanan yang di temukan dan melakukan *update result* pada *dashboard monitoring*, membuat *deployment patch policies* , sistem akan mendeteksi apakah terdapat *deployment policies* yang harus di jalankan, sistem melakukan *automation remediation / deployment patch* pada software yang memiliki kerentanan, sistem akan melakukan *update result* pada dashboard.

D. Implementation

Pada tahap ini dilakukan instalasi dan konfigurasi, sesuai spesifikasi desain yang telah dibuat. Implementasi pada tahap ini mendiskripsikan tentang implementasi di lapangan, set-up dan konfigurasi yang digunakan dari toologi yang telah dibuat. Dengan menggunakan sistem vulnerability management , peneliti menggabungkan proses vulnerability assessment dan patching yang di automasikan untuk mendapatkan sistem yang andal dan efektif.

Selain itu untuk menjamin Server Availability, peneliti mengintegrasikan Automation vulnerability assessment dan patching dengan metode live patching yang bertujuan untuk menghindari adanya downtime pada proses update linux kernel. Dengan di integrasikan nya Automation vulnerability assessment dan patching dengan metode live patching diharapkan dapat menciptakan sistem vulnerability management yang andal dan efektif.

E. Monitoring

Pada tahap ini melakukan pengujian dan monitoring setelah dilakukan konfigurasi. Pengujian ini dilakukan dengan momonitoring *linux server* melalui *dashboard vulnerability management* dan *log* pada *linux server* bahwa proses *deployment patch* berjalan dengan baik. Serta pengujian setelah melakukan *deployment patch* , *linux server* tidak melakukan proses *rebooting server* yang dapat menimbulkan adanya *downtime* .

Peneliti juga melakukan analisa perbandingan proses *vulnerability assessment* dan patching sebelum dan sesudah penelitian ini dilakukan untuk membuktikan keuntungan yang didapatkan PT Mesco Mitra Aditama dengan terlaksananya implementasi ini.

.

F. Management

Pada tahap manajemen ini akan dilakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yang diharapkan. Diantara langkah-langkah yang perlu dilakukan adalah :

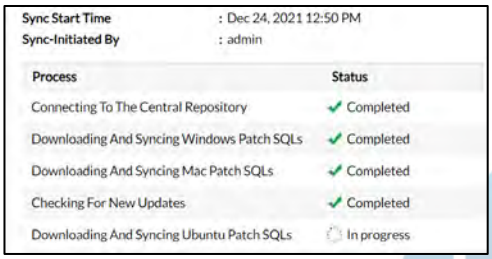
a) Menggunakan *environment* yang terpisah dengan *production* yaitu menggunakan *environment staging* .
b) Membuat *access* pada *windows server* dan *linux server*.
c) Melakukan *Snapshot* pada *server* yang digunakan, dilakukan agar sewaktu-waktu terjadi hal yang

dapat membuat *server error*, kita dapat mengembalikan pada kondisi semula.

IV. HASIL PEMBAHASAN

Proses *automation vulnerability assessment* dan *patching* yang di integrasikan dengan metode *live patch* memiliki beberapa tahap diantaranya adalah sebagai berikut:

4. 1 Update Vulnerability Database

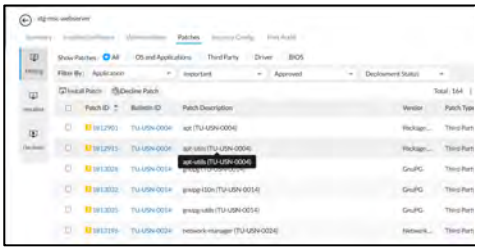


Gambar 5. Update Vulnerability Database

Pada tahap ini dilakukan update pada *Vulnerability Database* yang bertujuan untuk mengupdate informasi terkait kerentanan baru yang sebelumnya tidak ada dalam database.pengujian dengan melakukan perubahan status *IP Address* di *dashboard IP Address management* yang sebelumnya berstatus *active* di data *IPAM*.

4. 2 Vulnerability Scan

Pada tahap ini di lakukan *vulnerability scan* pada targer server. Setelah scanning selesai, Hasil dari *vulnerability scan* pada *linux server* dapat dilihat pada *console dashboard*. Terdapat beberapa *missing patch* yang dapat menimbulkan kerentanan pada *linux server*.



Gambar 6. Hasil *Vulnerability Scan*

4. 3 Remediation / deployment patch

Gambar 7. Hasil dari deployment patch

Pada tahap ini adalah proses *remediation / deployment patch*. Pada sebelum dilakukan *deployement patch* ada sebanyak 164 missing patch yang ditemukan. Setelah proses *remediation / deployment patch* dilakukan sebanyak 160 missing patch berhasil di resolve. Peneliti melakukan pengecekan terhadap 4 missing patch yang tersisa, hasil pengecekan adalah 4 missing patch tersebut tidak tidak dibutuhkan oleh *linux server* karena tidak digunakan.

Selanjutnya kita lakukan verifikasi dengan melakukan pengecekan langsung pada *log linux server* untuk memastikan apakah *proses* dari *automation deployment patch* berjalan dengan baik dan *missing patch* benar benar terinstall.

Gambar 8. Verifikasi pada Log Linux Server

Terlihat pada capture diatas bahwa *linux server* mendapatkan *automation deployment patch* . Verifikasi juga dilakukan untuk mengecek keadaan *linux server* yang tidak melakukan proses *rebooting server*.

KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, terdapat beberapa kesimpulan yang dapat diambil, secara umum bahwa proses *automation vulnerability assessment* dan *patching* dapat meningkatkan kefesienan sistem pada perusahaan berskala *Enterprise*.

. Secara lebih khusus penulis dapat menarik beberapa kesimpulan sebagai berikut:

1. Dengan menerapkan *automation vulnerability assessment dan patching* dapat meminimalisir timbulnya kerentanan pada server yang tidak termonitoring .Karena Sistem akan melakukan scanning secara berkala terhadap server yang menjadi target.
2. Dengan menggunakan *Automation Vulnerability assessment* dan *patching* dapat memudahkan *Security Engineer* ataupun *Management* dalam mengaudit *server* di karenakan banyaknya *server* yang digunakan pada persuhaan berskala *enterprise.*
3. Dengan menggunakan *Automation Vulnerability assessment* dan *patching* dapat memudahkan *Security Engineer* dalam melakukan proses *VA* dan *patching* pada *software* yang memiliki kerentanan dan mendapatkan *security patches* dengan cepat dan mudah dikarenakan efisiensi waktu dibandingkan dengan melakukannya secara manual.
4. Dengan menggunakan *AutomationVulnerability assessment* dan *patching* menggunakan metode *live patching, server production* dapat melakukan patch tanpa melakukan *rebooting server*.
5. Hal lainnya bahwa dengan *Automation Vulnerability* assessment dan patching masih dapat di integrasikan sehingga dapat menciptakan sistem yang lebih andal dan efektif

Selain dari kesimpulan diatas, pada pengimplementasian sistem ini terdapat hal yang perlu dipertimbangkan yaitu dimana implementasi ini dapat integrasikan

dan dikembangkan sesuai kebutuhan perusaan itu sendiri.

REFERENSI

[1] Ari Marta Tania, Didik Setiyadi, Fata Nidaul Khasanah, "Keamanan Website menggunakan vulnerability assessment," *E-ISSN*, 2018.

[2] David Harjowinoto, Agustinus Noertjahyana, Justinus Andjarwirawan , "Vulnerability testing pada sistem administrasi rumah sakit," *Jurnal Infra*, 2016.

[3] M. Fatkhurozzi, "Analisa keamanan website menggunakan metode footprinting dan vulnerability scanning pada website kampus," *Informatics Journal*, 2021.

[4] Fahmi Hardiansyah, IGN. Mantra, "Vulnerability assessment dan kajian aspek application security pada aplikasi skripsi ONLINE (SIPSO)," *SENAMIKA*, 2020.

[5] M. Aziz, "Vulnerability assessment untuk mencari celah keamanan web aplikasi E-learning," *SENAMIKA*, 2021.

[6] Nur Arifin Akbar, Maman Somantri, Rizal Isnanto, "Implementasi penutupan celah keamanan pada aplikasi web berbasis joomla 1.5.5 serta server berbasis ubuntu 8.04 dengan kernel 2.6.24," *TANSIENT*, 2013.

[7] Andri Fauzan, Iskandar Fitri, Novi Dian Nathasia, "Peningkatan keamanan jaringan pada endpoint menggunakan metode host intrusion detection system and prevention system dengan centralized patch vulnerability," *JIMP*, 2018.

[8] Erick Irawadi, Herdianti, Fitriyani Umar, "Analisis keamanan website menggunakan Teknik footprinting dan vulnerability scanning," *SANTIKA*, 2019.

[9] "Manage Engine," Manage Engine, [Online]. Available: https://www.manageengine.com/vulnerability-management/knowledge-base/index.html.

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul Implementasi *Automation vulnerability assessment* dan *patching* pada *linux server* (Studi kasus PT Mesco Mitra Aditama). Kertas kerja berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan:

1. Literature review
2. Analisis dan Perancangan sistem
3. Konfigurasi
4. Tahapan eksperimen
5. Hasil eksperimen secara keseluruhan.