Proceedings

Konferensi Nasional Sistem Informasi 2014

KNSI 2014
Konferensi Nasional Sistem Informasi 2014

STMIK DIPANEGARA
MAKASSAR

27 Pebruari - 01 Maret 2014

Abstract Proceeding Edition

ISSN : 2355-1941

Pusat Penelitian dan Pengabdian Pada Masyarakat (P4M) STMIK Dipanegara Makassar
Jl. Perintis Kemerdekaan Km.9 Makassar, Telp. : 0411-587194 | Fax. : 0411-588283
Email : p4m@dipanegara.ac.id

Dipublikasikan Tahun 2014 oleh:

Pusat Pengembangan, Penelitian, dan Pengabdian Masyarakat (LP4M)

STMIK DIPANEGARA MAKASSAR

SULAWESI SELATAN - INDONESIA

ISSN: 2355-1941

Panitia tidak bertanggung jawab terhadap isi paper dari peserta

PROCEEDINGS

KONFERENSI NASIONAL SISTEM INFORMASI 2014

Ketua Editor

Drs. I Wayan Simpen, M.MSI.

Sekretaris Editor

Yesaya Tommy Paulus, S.Kom., MT.

Anggota Editor

M. Syukri Mustafa, S.Si., M.MSI.

Indra Samsie, M.Kom.

Jufri, S.Kom., MT.

Asran, ST.,MT.

Ahmad Sukarna S.,S.Kom.,MT.

KNSI2014-106

VULNERABILITY ASSESSMENT TERHADAP JARINGAN UNTUK KEAMANAN INFORMASI

Doddy Ferdiansyah.,ST[1]

[1]Jurusan Informatika, Fakultas Teknik, Universitas Pasundan
[1] doddy2112@hotmail.com

Abstrak

Vulnerability dapat diartikan secara langsung sebagai sebuah kelemahan atau ketidakmampuan sebuah sistem untuk menahan efek dari berbagai macam/jenis serangan. Setiap sistem yang canggih atau setiap jaringan yang bagus bahkan setiap peralatan-peralatan modern pasti akan mempunyai *vulnerability* (kerentanan) yang dapat mengakibatkan bencana terhadap sistem, asset bagi organisasi. Beberapa kerentanan dapat dinilai seberapa besar *vulnerability* yang terjadi pada sistem. Untuk melakukan penilaian kerentanan (*vulnerability assessment*) terdapat beberapa proses yang harus dilakukan dan dapat menggunakan beberapa cara. Dalam penelitian ini dilakukan kajian teori tentang analisis penilaian kerentanan dengan menggunakan metode dari IATAC (Information Assurance Technology Analysis Center).Hasil akhir dari penelitian ini merupakan sebuah requirement kebutuhan *vulnerability assessment* sehingga kerentanan dan resiko yang akan terjadi dapat diminimalisir.

Kata kunci : *Vulnerability, Assessment, Risk*

1. Pendahuluan

1.1 Latar Belakang

Keamanan informasi sangat penting di era teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini tidak lagi menggunakan media kertas, tetapi sudah banyak menggunakan teknologi komputer dan internet. Untuk menjaga keamanan informasi tersebut harus mengutamakan 3 faktor yaitu *Confidentiality, Integrity, dan Availability*.

Berbicara mengenai keamanan informasi, harus mendapat perhatian yang lebih terutama pada media akses (jaringan) dan media penyimpanan (server). Banyak sekali perangkat-perangkat dan aplikasi yang digunakan untuk menyimpan dan mengambil data secara public (internet) sehingga banyak pula resiko-resiko yang akan dihadapi. Resiko ini muncul dari kerentanan yang terdapat pada sistem yang dibuat.

Salah satu cara untuk meminimalisir resiko-resiko yang terjadi yaitu dengan menilai kerentanan yang terdapat pada sistem. Salah satu metode yang dapat digunakan untuk *vulnerability assessment* ini yaitu dengan menggunakan metode dari IATAC (Information Assurance Technology Analysis Center).

1.2 Identifikasi Masalah

Kemudian dapat di identifikasi bahwa permasalahan yang timbul adalah bagaimana melakukan penilaian kerentanan sehingga resiko yang muncul dapat diminimalisir.

1.3 Tujuan

Penilaian ini mempunyai tujuan untuk mengenal dan mengetahui kerentanan-kerentanan apa saja yang terdapat pada sebuah sistem.

1.4 Metode Penelitian

Metode yang dilakukan dalam studi dan eksplorasi ini adalah sebagai berikut :

1. Studi Literatur

   Mencari dan mempelajari referensi mengenai :

   a. Konsep *Vulnerability*, *Vulnerability assessment*, dan *Management Resiko*

   b. Konsep keamanan informasi pada jaringan

2. Analisis

   Melakukan penyelidikan atau pembelajaran lebih lanjut terhadap

Vulnerability yang mungkin terjadi, metode yang dilakukan oleh IATAC dan tools yang dapat digunakan untuk menilai tingkat kerentanan.

3. Perancangan

Membuat contoh proses penilaian kerentanan berdasarkan IATAC sebagai referensi.

2. Pemahaman *Vulnerability assessment*

2.1 Pemahaman Umum

Kata *vulnerability* atau diterjemahkan ke dalam bahasa Indonesia adalah kerentanan mempunyai arti ketidakmampuan untuk menahan efek dari lingkungan yang tidak bersahabat. Menurut Greg Bankoff [2], konsep dari *vulnerability* adalah mengekspresikan berbagai macam bencana dengan berfokus pada keseluruhan relasi dalam situasi sosial tertentu yang merupakan suatu kondisi yang menghasilkan bencana. Hal ini juga dapat dilihat sejauh mana perubahan bisa membahayakan sistem, atau masyarakat yang dapat dipengaruhi oleh dampak dari bencana tersebut.

Menurut Dymco Inc.,[3] dalam keamanan komputer, arti dari *vulnerability* ini adalah usaha yang diterapkan kepada kelemahan sebuah sistem, yang mengijinkan seorang attacker mengganggu/merusak integritas dari sistem tersebut. Vulnerabilities mungkin dapat dihasilkan dari kombinasi password yang lemah, software bugs, kesalahan konfigurasi, virus komputer dan malware lainnya, script code injection, atau SQL injection.

2.2 *Vulnerability assessment*

Menurut NIST SP 800-37 [1], *vulnerability* analysis and assessment adalah elemen yang sangat penting dari setiap kebutuhan aktifitas didalam NIST Risk Management Framework (RMF). RMF ini mempunyai 6 langkah yang mengintegrasikan *vulnerability* analysis dan *vulnerability assessment* :

1. Categorize Information Systems.
2. Select Security Controls.
3. Implement Security Controls.
4. Assess Security Controls.
5. Authorize Information Systems.
6. Monitor Security Controls.

Vulnerability assessment membantu mengintegrasikan dengan detection, identification, measurement, dan memahami dari *vulnerability* yang ditemukan pada Teknologi Komunikasi dan Informasi (TKI) dan infrastruktur. *Vulnerability assessment* akan sangat bermanfaat/berguna jika diterapkan selama 2 fase dalam lifecycle target :

1. Sebelum membangun sebuah sistem
2. Ketika setelah pembangunan sistem.

Untuk melakukan *vulnerability assessment* ini dibutuhkan tools yang cocok dan sesusai dengan fungsinya. Perangkat-perangkat *vulnerability assessment* secara umun bekerja dengan mengotomatisasikan langkah-langkah yang hampir sama dengan/digunakan untuk mengeksploitasi kerentanan. Langkah ini dimulai dari footprint dimana langkah ini menganalisis untuk menentukan layanan jaringan atau aplikasi (software) yang dijalankan pada target. Perangkat (tools) kemudian mencoba untuk menemukan indicator atau pola untuk mengeksploitasi kerentanan yang telah diketahui dan terdeteksi pada software dan melaporkan hasil temuan tersebut. Butuh perhatian khusus pada saat menjalankan kode eksploit (exploit code) terhadap target langsung "live target" karena hasil yang didapat dapat merusak beberapa sistem. Seperti contoh, menargetkan aplikasi live web dengan perintah "drop tables" di SQL Injection dapat menyebabkan hilangnya data actual.

Untuk menghindari hal diatas terjadi,. Beberapa perangkat *vulnerability assessment* sepenuhnya pasif. Scan pasif, dimana tidak ada data yang di inject dengan tools ke target, membaca dan mengumpulkan data. Dalam beberapa kasus, tools tersebut menggunakan *vulnerability* signatures, yaitu, pola atau atribut yang terkait dengan kemungkinan adanya *vulnerability* atau kerentanan. Tools pasif terbatas dalam hal kegunaanya karena tools tersebut hanya dapat menduga adanya kerentanan berdasarkan bukti, bukan pengujian langsung terhadap kerentanan.

2.3 Penetration Testing

Menurut SANS Analyst Program, Penetration Testing atau disingkat dengan istilah pentest adalah sebuah proses untuk mencoba mengambil akses kesebuah sumberdaya tanpa pengetahuan tentang username, password, dan keterangan akses yang normal lainnya. Jika fokus dari pentes ini adalah sumberdaya yang terdapat pada komputer, maka contoh hasil dari penetrasi yang berhasil mendapatkan atau menumbangkan (menghancurkan) dokumen-dokumen rahasia, database, dan informasi yang dilindungi lainnya. Hal paling utama yang membedakan antara penetration tester dengan attacker adalah perijinan. Penetration tester akan mendapat

ijin dari yang mempunyai sumberdaya komputer yang akan di tes dan akan bertanggungjawab memberikan laporan. Tujuan utama dari pentest ini adalah untuk meningkatkan keamanan sumberdaya komputer yang sudah di tes.

Ada beberapa alasan kenapa harus melakukan penetration testing :

1. Menemukan lubang/celah kerentanan dari sistem
2. Melaporkan masalah terhadap bagian manejemen
3. Memeriksa keamanan konfigurasi
4. Pelatihan keamanan untuk staff jaringan
5. Menemukan Gaps of Compliance
6. Mengetes teknologi yang terbaru

2.4 Countermeasure

Countermeasure atau dapat diartikan sebagai penanggulangan adalah sebuah tindakan, proses, perangkat, atau sistem yang dapat mencegah atau mengurangi efek dari ancaman kepada komputer, server atau jaringan. Dalam konteks ini, sebuah threat atau ancaman mempunyai potensi atau benar-benar merugikan yang bisa berbentuk malicious atau isidentil dan dapat mengganggu aset dari sebuah perusahaan atau organisasi atau merusak integritas dari komputer dan jaringan. Countermeasure dapat berbentuk berupa perangkat lunak, perangkat keras dan mode perilaku.

Perangkat lunak countermeasure terdiri dari :

1. Personal Firewall
2. Application Firewall
3. Anti-virus Software
4. Pop-up Blocker
5. Spyware Detection / Removel Program

Yang paling umum digunakan untuk countermeasure dengan perangkat keras adalah menggunakan router yang dapat mencegah IP address dari komputer individu yang mengakses secara langsung ke internet. Perangkat keras lainnya yaitu :

1. Biometric Authentication System
2. Physical Restriction (Pencegahan akses terhadap komputer dan alat-alat lainnya)
3. Intrusion Detector
4. Alarms

Behavior atau prilaku countermeasure terdiri dari :

1. Menghapus cookies dan temporary file dari web browser secara berkala
2. Scanning virus dan malware lainnya secara teratur
3. Selalu meng-update dan mem-patch sistem operasi
4. Menolak untuk membuka link yang tidak dikenal yang muncul di e-mail
5. Menjaga jarak dengan semua website yang melakukan/melakukan pertanyaan
6. Mem-backup dan memindahkan data ke media simpan lain secara berkala

3. Penilaian Kerentanan (*Vulnerability assessment*)

Dalam penelitian ini menggunakan metode penilaian dari IATAC [4]. Langkah atau proses penilaian ini terdiri dari 6 tahapan, yaitu :

1. Network Scanners
2. Host Scanners
3. Database Scanners
4. Web Application Scanners
5. Multilevel Scanners
6. Automated Penetration Test

3.1 Network Scanners

Network Scanning merupakan sebuah prosedur untuk mengidentifikasi host yang aktif dan perangkat-perangkat jaringan apa saja yang sedang berjalan. Banyak informasi yang dapat dihasilkan seperti IP address, komputer yang aktif, port yang terbuka, dll.

Dalam melakukan network scanning, IATAC menggunakan tools berikut ini :

Tabel 1. Daftar Tools Networ Scanning

DragonSoft *Vulnerability* Management
Beyond Security® Automated *Vulnerability* Detection System
Black Falcon/Net Security Suite Falcon *Vulnerability* Analysis
FuJian RongJi RJ-iTOP
GFI Sunbelt Network Security Inspector Suite 2.0
eEye® Retina® Network
Global DataGuard® Unified Enterprise Security: *Vulnerability* Scanner Module
Fortinet® FortiScan
Greenbone Security Feed and Security Manager 1.4
GFI LANguard®
Hangzhou DPtech Scanner1000
IBM® Proventia® Network Enterprise Scanner 2.3
Infiltration Systems Infiltrator 2009
Inverse Path TPOL
Lumension® Scan
nCircle® IP360
McAfee® *Vulnerability* Manager
netVigilance SecureScout® SecureScout Easybox 2.0 Scanner
netVigilance SecureScout® (Enterprise Edition)

netVigilance SecureScout® (Windows Edition)
NGSSecure NGS Typhon III
NileSOFT Secuguard NSE
NSasoft Nsauditor
Safety-Lab Shadow Security Scanner
Security System Analyzer 2.0 Beta
StillSecure® VAM 5.5
Xacta® IA Manager
ZOHO® ManageEngine® Security Manager Plus Network Security Scanner component

3.2 Host Scanners

Host scanning merupakan sebuah prosedur untuk mengidentifikasi detail dari setiap host yang terhubung dalam sebuah jaringan. Informasi-informasi yang dapat dihasilkan dari host scanning ini seperti OS yang digunakan, aplikasi-aplikasi yang terinstal, nama host, dll. Tools yang digunakan IATAC untuk melakukan host scanning adalah :

Tabel 2. Daftar Tools Host Scanning

Proland Protector Plus
ThreatGuard® Secutor
Assuria Auditor and Auditor RA
Infiltration Systems Infiltrator for Home Users
Microsoft® Attack Surface Analyzer
NileSOFT Secuguard SSE
Numara® *Vulnerability* Manager
SoftRun Inciter *Vulnerability* Manager
Key Resources VAT

3.3 Database Scanners

Database scanning merupakan sebuah prosedur untuk mengidentifikasi database yang terdapat pada sebuah server. Informasi yang dapat diperoleh dari hasil scanning ini seperti jenis databse, user (account) database, versi database, dll. IATAC menggunakan beberapa tools seperti dibawah ini :

Tabel 3. Daftar Tools Database Scanning

Imperva® Scuba
Application Security AppDetectivePro
DBAPPSecurity MatriXay 3.6
Safety-Lab Shadow
Fortinet FortiDB
McAfee Repscan and McAfee *Vulnerability* Manager for Databases
NGSSecure NGS SQuirreL for DB2, SQL Server, Oracle, Informix, Sybase ASE

3.4 Web Application Scanners

Web application scanning merupakan sebuah prosedur untuk mengidentifikasi potensi-potensi kerentanan yang terjadi pada aplikasi web. Scanner ini biasanya tidak melakukan sampai dengan source code dari web, akan tetapi melakukan percobaan secara langsung dengan teknik-teknik tertentu sehingga mendapat kelemahan pada web tersebut. IATAC menggunakan beberapa tools untuk melakukan web application scanning seperti :

Tabel 4. Daftar Tools Web Scanning

Acunetix® Web *Vulnerability* Scanner
Casaba Watcher 1.5.1
Cenzic® Hailstorm® Enterprise Application Risk Controller
Grabber
eEye Retina Web
Hacktics® Seeker®
HP WebInspect®
IBM/Rational® AppScan® Standard, Enterprise, and Express Editions
Mavutina Netsparker®
MAYFLOWER Chorizo! Intranet Edition
MileSCAN ParosPro Desktop Edition 1.9.12
MileSCAN ParosPro Server Edition 1.5.0
nCircle WebApp360
NGSSecure Domino Scan II
NGSSecure OraScan
Nikto2 2.1.4
NOSEC JSky 3.5.1
N-Stalker Web Application Security Scanner 2009
NT OBJECTives NTOSpider
PortSwigger Burp Suite Professional Edition Burp Scanner Component
Subgraph Vega
Syhunt Sandcat and Sandcat Pro
WATOBO

3.5 Multilevel Scanners

Multilevel scanning merupakan prosedur untuk mengidentifikasi kerentanan yang terdapat pada jaringan/server/host dari tingkat paling dasar (fisik) sampai dengan tingkat teratas (aplikasi). Beberapa tools yang digunakan oleh IATAC antara lain :

Tabel 5. Daftar Tools Multilevel Scanning

Belarc® BelManage
Critical Watch FusionVM® Enterprise and FusionVM MSSP
Imperva® SecureSphere®

Integrigy AppSentry
Jump Network Jabil® Network *Vulnerability assessment* System
NSFOCUS Remote Security Assessment System
Open *Vulnerability assessment* System 4
SAINT® Professional and SAINT® Enterprise
SecPoint The Penetrator
SecPoint The Portable Penetrator
Symantec® Control Compliance Suite: *Vulnerability* Manager
Symantec Risk Automation Suite
Tenable® Nessus®
Tenable Passive *Vulnerability* Scanner
Venusense *Vulnerability* Scanning and Management System

3.6 Automated Penetration Test

Sebuah metode dalam mengevaluasi keamanan jaringan dan komputer dengan melakukan simulasi serangan terhadap sistem komputer atau jaringan baik dari dalam maupun dari luar. Beberapa tools yang digunakan oleh IATAC antara lain :

Tabel 6. Daftar Tools Automated Penetration Test

Arachni
CORE IMPACT® Pro
CORE INSIGHT Enterprise
Google® Skipfish
Immunity® CANVAS® Professional
Immunity SILICA®
Parasoft® SOAtest with Parasoft Load Test
Rapid7® Metasploit® Express
Rapid7 Metasploit Pro
Rapid7 NeXpose
Spirent® Avalanche *Vulnerability assessment*
w3af
Wapiti 2.2.1
Websecurify

4. Proses Penilaian

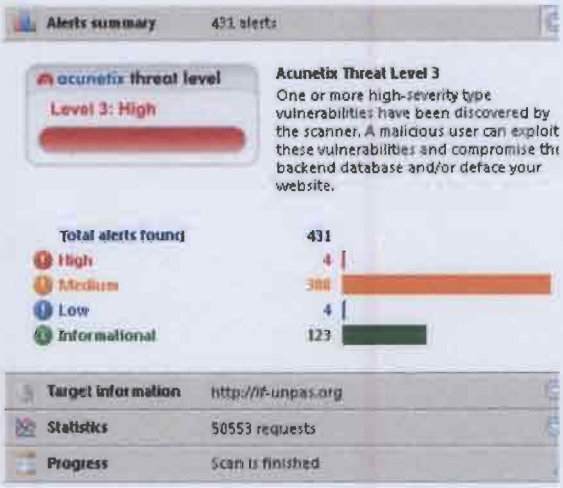
Dalam melakukan *vulnerability assessment* terhadap jaringan, penulis hanya menggunakan beberapa tools dari daftar tools diatas. Fungsi dari masing-masing tools hampir sama, yang membedakannya hanya apakah tools tersebut gratis (free) atau tidak, berbahasa inggris atau tidak, link tersebut masih valid atau tidak, dan tools tersebut berbasiskan windows atau tidak.

Dari secara keseluruhan daftar tools diatas, penulis mempunyai alasan mengapa hanya mengambil sebagian tools sebagai uji coba. Alasan yang dijadikan pertimbangan pemilihan tools dapat dilihat pada lampiran. Berikut tools yang dipilih untuk melakukan *vulnerability assessment* :

Tabel 7. Tools Yang dipilih

Tahapan	Tools yang digunakan
Network Scanners	Security System Analyzer
Host Scanners	Proland Protector Plus
	Microsoft Attack Surface Analyzer.
Database Scanners	Imperva® Scuba
Web Application Scanners	Casaba Watcher
	Grabber
	Acunetix® (opsi)
Multilevel Scanners	Tenable® Nessus®
Automated Penetration Test Tools	Rapid7 Metasploit Express

Berikut ini merupakan contoh dari hasil web scanning yang telah dilakukan dengan menggunakan Acunetix.



Gambar 1. Hasil Web Scanning Dengan Acunetix

Pada tools ini ditemukan 431 alerts yang terdapat pada sebuah web yang telah di scanning dengan tools ini. Disini web yang menjadi contoh kasus adalah if-unpas.org. dari 431 alerts tersebut, yang mempunyai tingkat ancaman yang tertinggi (high) terdapat 4 alerts, tingkat ancaman sedang (medium) terdapat 300 alerts, dan tingkat ancaman redah (low) terdapat 4 alerts. Sedangkan beberapa informasi yang sangat kecil terjadinya vulnerability tetapi mempunyai kemungkinan terjadinya serangan (informational) terhadap web tersebut terdapat 123 alerts.

5. Kesimpulan dan Saran

Setelah melakukan penelitian tentang *vulnerability assessment* yang dimulai analisis sampai dengan tools yang digunakan, maka dapat diambil beberapa kesimpulan yaitu tidak semua daftar tools yang diberikan oleh IATAC harus digunakan. Karena hampir semua fungsi dari tools tersebut sama. Yang terpenting adalah proses melakukan 6 proses *vulnerability assessment* yang di berikan oleh IATAC.

Saran yang dapat diberikan yaitu penelitian ini masih dalam tahap analisis, dan masih belum selesai. Oleh karena itu, setelah melakukan scanning dengan tools yang telah diberikan, maka akan lebih baik jika dibuat sebuah report dari hasil scanning tersebut. Karena dari hasil scanning akan didapatkan kerentanan-kerentanan apa saja yang terdapat pada sistem jaringan.

Daftar Pustaka:

[1] NIST SP800-37., 2010, *Information Security*, Gaithersburg.
[2] Bankoff, Greg., 2004. *Mapping Vulnerability*, London.
[3] Demyo Inc., 2011, *What is Vulnerability assessment*, Miami.
[4] IATAC., 2011, *Vulnerability assessment (Tools Report)*, Virginia.