Kajian Pustaka: PENETRATION TESTING DENGAN NIST SP 800-115 DAN OSSTMM

Rizky Arisetio Wibowo[1], Setyawan Widyarto[2]
[1]Universitas Budi Luhur, Jakarta Indonesia
rizkywibowo@outlook.com
[2]Centre for Graduate Studies, Universiti Selangor, Shah Alam, Malaysia
swidyarto@gmail.com

ABSTRAK

Perkembangan dalam teknologi saat ini sangat pesat sekali sehingga kita dituntut untuk selalu mengikuti perkembangannya. Dari teknologi yang ada dan percepatan data yang ada, bisa menimbulkan keamanan data yang rentan. Dari kerentanan tersebut bisa di manfaatkan oleh orang-orang yang tidak bertanggung jawab. Perlu adanya antisipasi untuk mengamankan(security). Dalam menanggapi masalah kerentanan dibutuhkan adanya penetrasi tes, penetrasi tes menggunakan pedoman metode NIST SP 800-115 & OSSTMM sehingga mendapatkan sebuah hasil yang digunakan dalam pengetesan security yang ada pada aplikasi yang kita miliki. Dari metode tersebut kita mempunyai perbedaan perbedaan dalam segi pengetesan. hasil dari pengetesan security darimetode OSSTMM yang menghasilkan RAV (Risk Assesment Value) dan hasilnya menggambarkan STAR (Security Test Report Audit). NIST SP 800-115 menghasilan teknik penilaian teknis utama yaitu identifikasi sasaran, teknis analisi dan sasaran teknik kerentanan validasi. Dari review yang dilakukan penulis berpacu pada research question yang di gunakan, dan mendapatkan hasil analisa yang di lakukan.

Keywords – OSSTMM, NIST, NIST SP 800-115, Security, Penetration Test

1. Pendahuluan

Keamanan data merupakan hal penting dalam sebuah aplikasi atau infrastruktur yang kita punya dalam sebuah institut / organisasi. Suatu organisasi yang menjalankan kegiatan operasional yang berbasis teknologi informasi pasti akan menggunakan komputer. Seiring dengan perkembangan teknologi, diperlukan suatu media penyimpanan maupun pusat data yang banyak disebut sebagai server. Namun dengan perkembangan teknologi tersebut, keamanan merupakan aspek yang perlu diwaspadai oleh setiap pihak yang memiliki skema sistem terpusat, karena pembobolan, manipulasi, maupun kehilangan data dapat terjadi jika dilakukan oleh para hacker yang memang berniat mengambil data sensitif dari sebuah organisasi. Untuk dapat mengurangi kerugian yang diakibatkan oleh para hacker, maka langkah awal yang harus dikembangkan adalah melakukan evaluasi terhadap keamanan server yang ada. Hal ini bertujuan untuk mengurangi resiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada organisasi. Sebagian besar orang yang berkecimpung pada dunia sistem informasi disebuah organisasi akan merasa bingung saat diminta untuk melakukan evaluasi keamanan server yang ada. Hal ini dikarenakan memang banyak orang yang merasa awam dengan melakukan

evaluasi sistem server. Istilah penetration testing atau yang lebih dikenal dengan pentesting adalah suatu metode yang dapat digunakan untuk melakukan analisa terhadap suatu objek atau banyak objek yang akan dipenetrasi.

Dari sini kita sebagai mahasiswa ingin membahas metode pengamanan jaringan dari organisasi dan tempat penyimpanan data yang ada. Pembahsan metode OSSTMM dan NIST sebagai metode analisa pengamanan pada sistem informasi suatu oraganisasi yang mempunyai pusat data agar tidak di salah gunakan oleh orang yang tidak bertanggung jawab.

2. Tinjauan Pustaka

2.1 NIST SP 800-115 (*National Instatitute of Standarts and Technolgy*)

Sebuah metode pengujian teknis dan pemeriksaan yang dapat digunakan untuk berbagai penilaian metodologi dan leveraged untuk berbagai tujuan penilitian dengan cakupan tiga teknik penilaian teknis utama : review teknik, identifikasi sasaran dan teknik analisis, dan sasaran teknik kerentanan validasi. tujuan keseluruhannya yaitu fokus pada beberapa elemen kunci penilaian keamanan, publikasi ini juga memberikan rekomendasi praktis dan informasi teknis yang terkait dengan uji penetrasi. Nist sp 800-115 merupakan pembaharuan dari nist sp 800-42 yang sebelumnya menjelaskan mengenai pengujian terhadap keamanan jaringan. Menurut panduan 'Sasaran Teknik Kerentanan Validasi' termasuk "Password cracking, pengujian penetrasi, rekayasa sosial, dan keamanan aplikasi pengujian" [1]. Fokus dari panduan ini digambarkan sebagai "Publikasi ini berfokus pada menjelaskan bagaimana teknik ini teknis yang berbeda dapat dilakukan, dan tidak menentukan teknik yang harus digunakan untuk keadaan yang" [1]. NIST SP800-115 dapat dijadikan sebagai pedoman awal bagi penyedia dan klien, tetapi bukan sebagai pengganti metodologi penetrasi seperti OSSTMM, PTES dan OWASP Testing Guide. Nist SP 800-115 mempuyai 13 teknik penilaian dengan tiga kategori utama.[2]

1. **Review Teknik**
   a. Documentation Review
   b. Log Review
   c. Ruleset Review
   d. System Configuration Review
   e. Network Sniffing
   f. File Integrity Checking

2. **Target Identification & Analysis Techniques**
   a. Network Discovery
   b. Network port & service identification
   c. Vulnerability Scanning
   d. Wireless Scanning

3. **Target Vulnerability Validation Techniques**
   a. Password Cracking
   b. Penetration Testing
   c. Social Attacking

Selain itu terdapat 4 metode besaran pada nist sp 800-115 :

- External security testing : jenis pengujian yang dilakukan dari luar batas keamanan fasilitas yang diuji. tujuan tes keamanan adalah untuk mereproduksi

pandangan penyerang eksternal dan untuk menarik perhatian pada kerentanan yang sudah terlihat dari luar perusahaan (misalnya dari internet). pengujian eksternal selalu dimulai dengan teknik penemuan yang bertujuan memeriksa pengorganisasian kehadiran public.

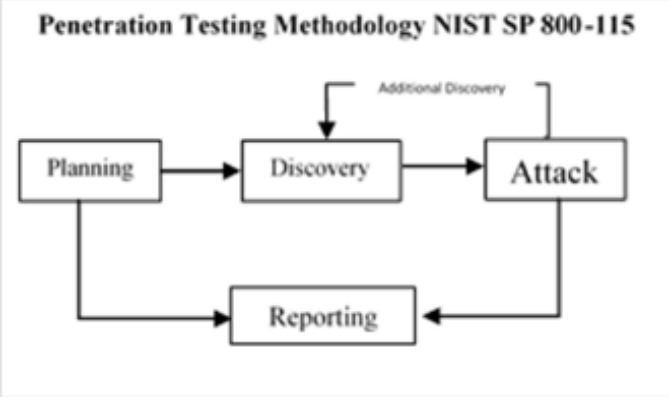
- Internal security testing : jenis pengujian yang dilakukan di dalam primeter organisasi (misalnya jaringan internal). Tujuan dari pengujian keamanan internal adalah untuk menyamar sebagai orang dalam yang dipercaya atau juga seorang penyerang yang telah menembus pertahanan eksternal. tes ini memungkinkan untuk memiliki tingkat akses tertentu ke jaringan dan ke informasi internal, untuk menilai mekanisme keamanan internal.

- Overt Security System : juga dikenal sebagai pengujian topi putih, mendefinisikan dan pengujian internal atau eksternal di mana ahli memiliki pengetahuan penuh tentang sistem dan prosses organisasi. Staf perusahaan juga mengetahui pengujian ini dan biasanya mencoba membatasi dampak pengujian. tes semacam ini sering digunakan sebagai pelatihan perusahaan.

- Covert Security System : Dikenal juga sebagai black hat testing, menggunakan pendekatan dengan tidak memberikan pengetahuan tentang organisasi nya. IT Perusahaan biasanya juga tidak mengetahui akan adanya pengujian dan responnya digunakan untuk menguji teknis dan organisasi.

2.1.1. Fase Penetration Testing

Termasuk meluncurkan serangan nyata pada data dan sistem, yang menggunakan teknik dan alat yang biasa digunakan oleh peretas untuk menentukan metode untuk menghindari aspek keamanan aplikasi, jaringan, atau sistem. [2]



gambar 2.2
Modul pada Channel [3]

Penetration testing mempunya 3 fase y aitu:

- **Fase *Planning***
  Aturan ditentukan, persetujuan manajemen dikonfirmasi & didokumentasikan, dan tujuan pengujian ditetapkan. Tidak ada pengujian aktual yang terjadi pada fase ini.
- **Fase *Discovery***
  - Memulai pengujian yang sebenarnya dan terdiri dari pengumpulan & pemindaian informasi.
  - Termasuk analisis kerentanan yang terdiri dari membandingkan aplikasi, layanan, dan host pindaian OS yang bertentangan dengan basis data kerentanan dan pengetahuan penguji tentang kerentanan.
- **Fase *Attack***
  Proses memvalidasi kerentanan yang ditentukan sebelumnya dengan menangani untuk mengeksploitasinya.
- **Fase *Reporting***
  Terjadi bersamaan dengan tiga fase teknik ini. Laporan ini menggambarkan kerentanan yang ditentukan, memberikan peringkat risiko dan menawarkan panduan untuk mengurangi kelemahan yang ditentukan.

2.1.2. Penetration testing logistics

Skenario pengujian penetrasi harus fokus terutama pada mencari & menargetkan kelemahan yang dapat dieksploitasi dalam desain & implementasi sistem, aplikasi, atau jaringan. Tes harus meniru pola serangan yang paling merusak dan paling mungkin.

Berikut tabel untuk penetrasi testing, password cracking, dan social engineering.

Target Vulnerable Validation Techniques			
No	Asessment Technique	Capabilities	Skill Required
1	Password Cracking	Identifies weak password and password policy	Knowledge of secure password
2	Penetration Testing	Test security using the same methodologies	Extensive TCP/IP, networking
3	Social engineering	allows testing of both procedures & the human element	Ability to influence and persuade people

2.2 OSSTMM (Open Source Security Testing Methodology

Manual)

Salah satu metodologi pengujian penetrasi tersedia untuk umum yang digunakan dalam benua eropa (Belanda & Inggris) adalah OSSTMM [4]. OSSTMM diciptakan oleh Pete Herzog dan Marta Barcelo yang dikembangkan oleh Spanyol dan Amerika Serikat Institute untuk Keamanan dengan Open Metodologi (ISECOM) [5]. Versi pertama dari OSSTMM diciptakan pada tahun 2000 dan versi saat ini adalah versi 3, yang diterbitkan pada tahun 2010 [5]. Pada April 2019, versi 4 sedang dikembangkan namun belum secara resmi dirilis [6]

Selain tujuan utama ini mereka menentukan tujuan sekunder, yaitu untuk Memberikan pedoman yang, jika diikuti dengan benar, akan memungkinkan analis untuk melakukan audit OSSTMM bersertifikat. Pedoman ini ada untuk menjamin berikut:

1. Pengujian dilakukan secara menyeluruh
2. tes termasuk semua saluran yang diperlukan
3. Postur untuk ujian mematuhi hukum
4. Hasilnya diukur dengan cara diukur
5. Hasil ini konsisten dan berulang
6. Hasil hanya berisi fakta-fakta sebagai berasal dari tes sendiri

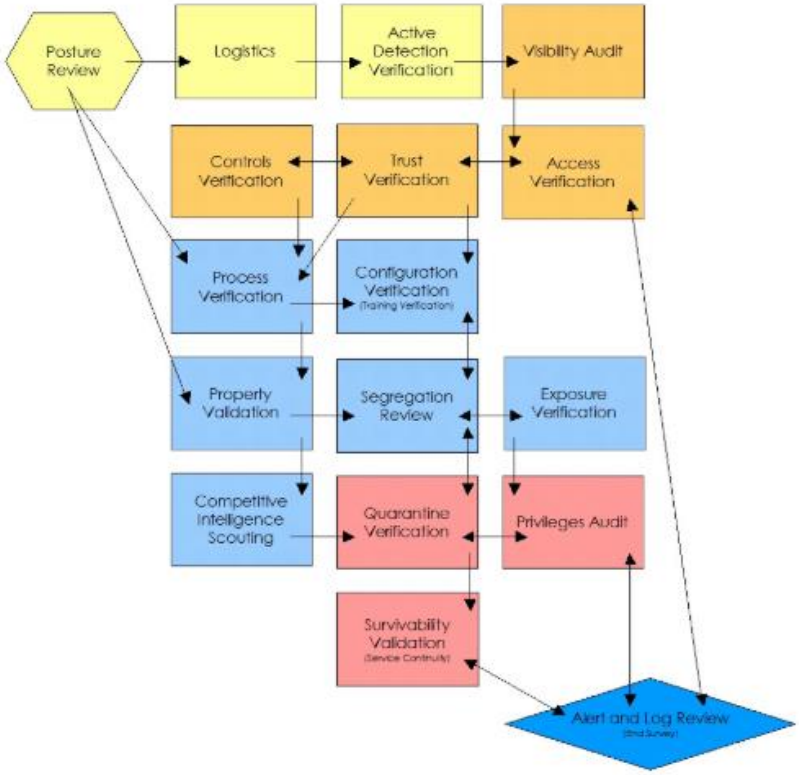
Manfaat tidak langsung dari manual ini adalah bahwa hal itu dapat bertindak sebagai acuan utama dalam semua tes keamanan terlepas dari ukuran organisasi, teknologi, atau perlindungan[5].

Menurut [4] ada beberapa penting yang harus diketahui sebelum melakukan security testing (pengetesan keamanan) menggunakan OSSTMM yaitu :

1. Mendefinisikan apa yang akan diproteksi yang disebut dengan Aset.
2. Mengetahui lingkungan sekitar Aset yang dapat berupa mekanisme proteksi, proses atau service yang berada disekitar Aset. Disini akan terjadi interaksi dengan Aset. Ini disebut dengan Zona Engagement.
3. Mengetahui segala sesuatu yang berada diluar Zona Engagement yang diperlukan untuk menjaga Asset. Semua ini disebut dengan Skop.
4. Bagaimana skop berinteraksi dengan dirinya sendiri dan dunia luar. Aset yang berada dalam skop dikelompokkan melalui arah interaksi .Bisa dipahami sebagai arah darimana dilakukan security testing (pengetesan keamanan) pada penelitian. Hal ini disebut dengan Vektor. Masing-masing vektor harus dites secara terpisah.
5. Identifikasi perlengkapan yang diperlukan untuk melakukan tes. Pada Vektor, interaksi bisa terjadi pada berbagai level. Level-level ini bisa dibagi dalam banyak jalan, semuanya dibagi berdasarkan fungsi dan disebut dengan Channel yakni Human, Physical, Wireless, Telecommunication dan Data Network. Masing-masing

channel harus dites terpisah untuk masing-masing vektor. Setiap channel memiliki 17 modul yang sama. Setiap modul memiliki task yang berbeda-beda tergantung channel masing-masing.

6. Menentukan Tipe Tes. Tentukan informasi apa yang ingin dihasilkan dari sebuah tes. Apakah hanya sekedar melakukan tes pada interaksi dengan Aset atau jangkauan yang lebih seperti mendapatkan respon dari penanganan keamanan. Ini disebut dengan Tipe Tes. Tipe Tes ditentukan setiap kali ingin melakukan tes.



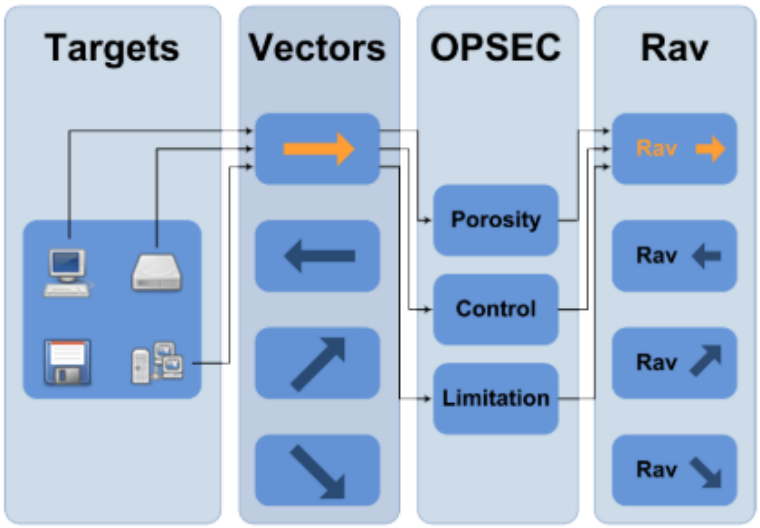
Gambar 2.2
Modul pada Channel [5]

Salah satu tujuan utama dari audit OSSTMM adalah untuk menggambarkan 'Realisasi Keamanan' dari satu (atau lebih) aset, dengan menghitung nya Nilai Risk Assessment (RAV) [5]. Sebuah RAV 100 merupakan keseimbangan sempurna antara kemungkinan interaksi dengan, misalnya, seorang penyerang dan jumlah kontrol dilaksanakan [5]. Para penulis menyebutnya "Keamanan Sempurna[5]. Ketika RAV berada di bawah 100, kontrol diimplementasikan tidak mencukupi. Ketika RAV di atas 100 berarti terlalu banyak dan kontrol yang tidak perlu dilaksanakan. RAV aset dihitung dengan menggunakan beberapa variabel [5], semua independen agen ancaman spesifik. Variabel

utama meliputi porositas (sebagai akibat dari Keamanan Operasional), menerapkan kontrol dan keterbatasan yang ada. Porositas dihitung dengan menambahkan semua kemungkinan akses ke aset. Variabel kontrol dihitung berdasarkan kontrol diimplementasikan yang melindungi aset. Dan variabel keterbatasan dihitung berdasarkan kerentanan atau kelemahan yang ada di kontrol ini. Untuk memahami setidaknya dasar-dasar pendekatan ini, ini bisa, hanya untuk tujuan pemahaman, diringkas sebagai berikut:

$$RAV = Porosity - (Controls_{123415} - Limitations)$$

RAV = 0, means Perfect Security
RAV > 0, means insufficient Controls
RAV < 0, means too many Controls



Gambar 2.3
activity rav dari tes keamanandengan OSSTMM[5]

2.3 Penetration Testing

Standar Eksekusi Pengujian Penetrasi (PTES) adalah standar pengujian penetrasi yang awalnya dibuat pada tahun 2009 oleh Nickerson et al. (n.d). PTES mencakup interaksi pra-keterlibatan, pengumpulan intelijen, ancaman 66 pemodelan, analisis kerentanan, eksploitasi, eksploitasi pasca, dan laporan.[7]

PTES terdiri dari tujuh bagian dan panduan ekstra, yang terdiri dari pedoman teknis. Tujuh bagian antara lain: 'Interaksi Pre-keterlibatan, Intelijen Gathering, Modeling Ancaman, Kerentanan Analisis, Eksploitasi, Pos Eksploitasi, Pelaporan' [8]. PTES menyediakan tingkat tinggi pemahaman untuk melaporkan temuan. Ini menyarankan untuk menggunakan dua bagian terpisah dalam laporan, yaitu ringkasan eksekutif dan bagian menyajikan temuan teknis. utama PTES adalah yang tidak ditulis terlalu konkret

sehingga kreativitas tester tidak akan terbatas, namun penyedia ini tidak menyebutkan bahwa penggunaan metodologi tergantung pada pertanyaan yang tepat dari klien. Tujuan utama PTES adalah “menyediakan penyedia layanan bisnis dan keamanan bahasa umum dan ruang lingkup "dan untuk memungkinkan klien" menuntut garis dasar tertentu pekerjaan ".[1] Penggunaan saat ini dan implementasi metodologi ini menunjukkan bahwa ini tujuan tidak terpenuhi. Beberapa penyedia tidak tahu tentang PTES dan karena itu tidak menerapkannya dan bagi kebanyakan orang lain itu hanya digunakan sebagai inspirasi untuk internal mereka metodologi, tidak ada bagian-bagian tertentu dari metodologi yang digunakan secara konsisten mengakibatkan kurangnya dasar kerja yang jelas dan ruang lingkup serta bahasa yang sama[1]. Itu satu penyedia yang mengatakan mereka sebagian mendasarkan metodologi internal mereka pada PTES, juga mengatakan mereka tidak mengikuti standar yang lengkap, yang lagi-lagi dapat mengakibatkan kurangnya dasar pekerjaan dan bahasa umum yang jelas.

3. Metodologi

Systematic review ini disusun berdasarkan pedoman pelaporan PRISMA. Terdapat beberapa langkah dalam penelitian ini sesuai dengan pedoman tersebut, yaitu:

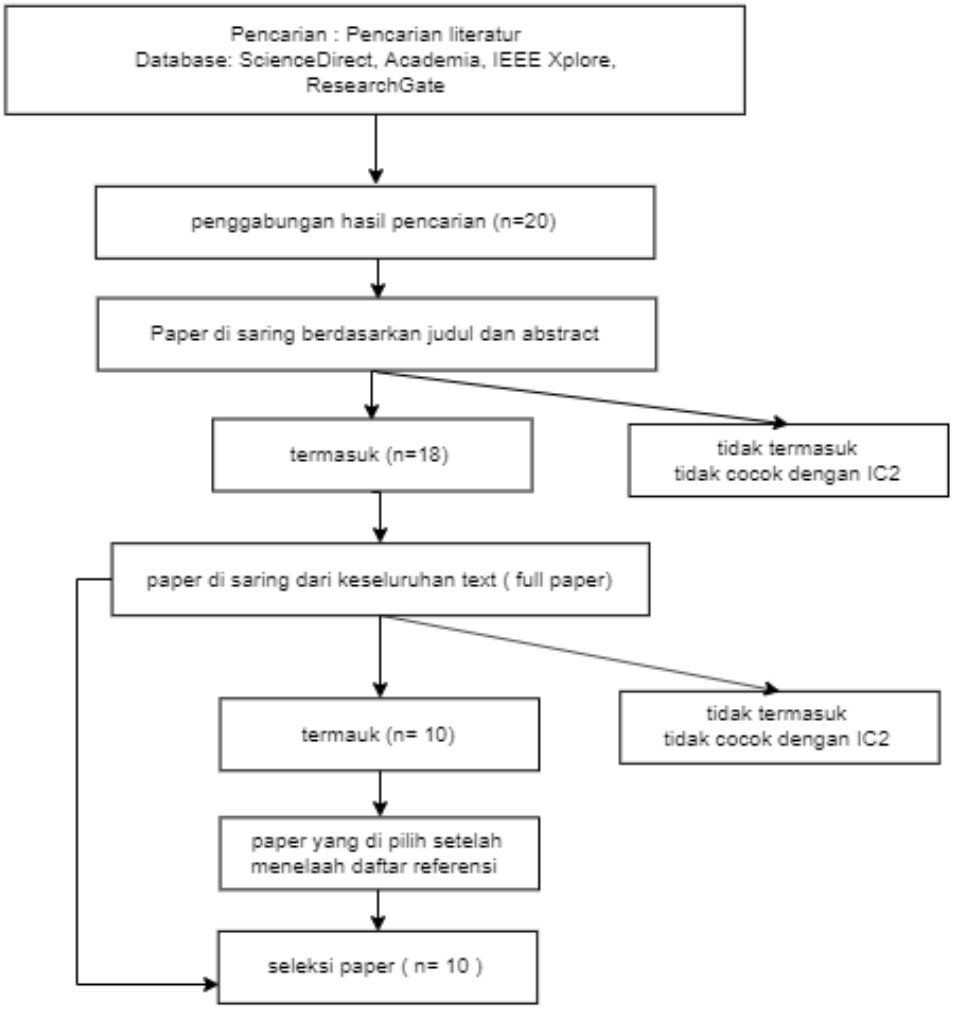
1) mendefinisikan kriteria kelayakan
2) mendefinisikan sumber informasi
3) pemilihan studi
4) pengumpulan data
5) pemilihan item data [13].

A. Kriteria kelayakan

Inclusion criteria (IC) berikut ini ditetapkan sebagai pedoman *review*:

IC1: Penelitian asli dan *peer-reviewed* yang ditulis dalam Bahasa Inggris;
IC2: Penelitian ini bertujuan untuk membahas metode assessment OSSTMM atau NIST 800-115 dalam pengamanan sistem.

Hanya *paper* yang ditulis dalam bahasa Inggris (IC1) yang dipilih karena Bahasa Inggris adalah bahasa yang umum digunakan oleh para peneliti di komunitas ilmiah. IC2 dimasukkan guna menjawab pertanyaan penelitian.
Gambar 1 menjelaskan langkah-langkah pekerjaan penulis dalam melakukan
Systematic review.



Gambar 3.1
Systematic review yang di buat oleh penulis

Ketertarikan penulis bukan hanya terbatas hanya pada metodologi dan teknologi keamanan sebagai perlindungan pada sistem informasi. Selain itu, penulis juga membahas tentang pentesting.

B. Sumber informasi

Paper-paper yang kami butuhkan dalam melakukan systematic research ini berasal dari database studi akademis, yaitu ScienceDirect, Academia, IEEE Xplore, dan ResearchGate.

Penulis hanya mengakses *paper* yang dalam upaya mendapatkannya tidak ada
persyaratan. Selain itu, penulis menelaah daftar referensi yang terdapat dalam *paper* untuk menemukan studi yang relevan.

C. Pemilihan studi

Pemilihan studi dilakukan dalam fase-fase berikut:

1. Pencarian kata kunci, dipilih sesuai dengan minat penelitian penulis dalam meninjau ancaman atau serangan

keamanan jaringan atau sistem informasi dan teknologi keamanan yang sesuai sebagai tindakan perlindungannya. Kata kunci yang digunakan dalam pencarian paper pada database yang disebutkan di bagian III.B adalah "*network security*", "*security attack and protective countermeasure*","*information security*", dan "*threat, attack and security technology*"

2. Eksplorasi dan pemilihan judul, abstrak, dan kata kunci dari *paper* yang diidentifikasi dilakukan berdasarkan kriteria kelayakan
3. Pembacaan lengkap atau sebagian *paper* yang memenuhi kriteria kelayakan dilakukan untuk menentukan apakah *paper* tersebut layak masuk dalam tinjauan
4. Daftar referensi paper ditelaah untuk menemukan studi yang relevan.

Fase-fase tersebut di atas dilakukan secara kolaborasi oleh seluruh penulis yang melakukan systematic review ini. Sekiranya terdapat perbedaan, maka dilakukan pembahasan sampai dicapai kesepakatan bersama.

D. Pengumpulan data

Pengumpulan data dilakukan secara manual menggunakan instrumen tabel ekstrasi data yang terdiri dari: judul, penulis, tahun, nama jurnal/konferensi, tipe *paper*, topik, metode penelitian, hasil pembahasan dan kesimpulan. Paper yang relevan atau berpotensi relevan dinilai secara bersama-sama. Penilaia terdiri dari membaca teks lengkap dan data yang diekstrasi. Setiap perbedaan diselesaikan melalui diskusi antara Artikel yang berpotensi relevan dinilai oleh masing-masing penulis. Penilaian terdiri dari membaca teks lengkap dan data yang diekstraksi. Setiap perbedaan diselesaikan melalui diskusi antara seluruh penulis.

E. Pemilihan item data

Informasi yang diambil dari setiap paper terdiri dari:

1. penjelasan tentang keamanan jaringan atau sistem informasi
2. ancaman atau serangan keamanan
3. teknologi keamanan yang ada sebagai perlindungan

4. HASIL

a. Seleksi paper

Hasil pencarian dalam database yang dipilih memberikan total 20 paper yang ditulis dalam bahasa Inggris dari tahun 2009 hingga 2019, cocok dengan kata kunci yang perlu dianalisis. Selanjutnya, paper-paper tersebut disaring berdasarkan judul, abstrak, dan kata kunci. Tersisa 18 paper yang kemudian ditinjau berdasarkan teks engkapnya, sebanyak 8 paper dibuang karena tidak memenuhi criteria IC2. Akhirnya terpilih 10 paper yang memenuhi kriteria kelayakan dan menjadi bahan dalam systematic review ini.

b. Karakteristik paper

Demografi Item data dari 10 paper yang dipilih menunjukkan bahwa paper-paper tersebut dapat diklasifikasi menjadi beberapa buah berdasarkan isi penelitian yang terdapat pada paper tersebut. Secara garis besar klasifikasinya berdasarkan pada topik tinjauan yang dilakukan yaitu mengenai OSSTMM, NIST 800-115.

Klasifikasi detil dari 10 paper yang dipilih ditunjukkan pada Tabel 2.

No.	Penulis	Topik	
		OSSTMM	NIST 800-115
1.	Yendri Ikhlas Fernando1, Rahmad Abdillah	√	
2.	Firkhan Ali Hamid Ali1 & M. Tarmizi Abd. Wahab2	√	
3.	Andrea Fiaschetti, Andrea Lanna, Martina Panfili, Silvano Mignanti,Antonio Pietrabissa, Francesco Delli Priscoli	√	
4.	Ayman Al-ahwal1	√	
5.	Yong-Suk Kang1, Hee-Hoon Cho2, Yongtae Shin3 and Jong-Bae Kim4*		√
6.	E.B Setiawan, A. Setiyadi	√	
7.	Cosmos Eko Suharyanto		√
8.	Rubenson Christian Silaban , Erick Wijaya	√	
9.	Aleatha Shanley1, Michael N. Johnstone1,2	√	
10.	Carlos J. Martínez-Santander, Yolanda de la N. Cruz-Gavilanes	√	

Dari 20 jurnal yang penulis review ada beberapa jurnal yang merupakan acuan review dari penulis untuk menulis paper review yang akan di buat jurnal jurnal tersebut di review oleh penulis dan di bandingkan dari penggunaan metode yang kita review. Dari jurnal tersebut pun ada beberapa jurnal yang tidak menyampaikan atau menjelaskan bagaimana proses hasil pengujiannya. Sedangkan review nya dan hasil nya bisa di jadikan sebagai beberpa review untuk pembuatan jurnal baru dari masalah masalah yang pernah di bahas oleh penulis sebulumnya dari masing-masing jurnal yang digunakan dapat dilihat pada tabel berikut:

PENULIS	JUDUL	METODE	HASIL
Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual [9]	Yendri Ikhlas Fernando1, Rahmad Abdillah	OSSTMM	OSSTMM mempunyai kekurangan dari nilai yang di berikan karena bisa berbeda tergantung dari apa yang akan di testing tergantung dari vektor2 yang akan di tes

SK42 Sistem Maklumat Pengujian Keselamatan Teknologi Maklumat Berasaskan OSSTMM[10]	Firkhan Ali Hamid Ali1 & M. Tarmizi Abd. Wahab2	OSSTMM	Dengan metode OSSTMM dapat memudahkan pakar dalam mengendalikan maklumat pengujian, dalam berbentuk grafik
Attack-Surface metrics, OSSTMM and Common Criteria based approach to " Composable Security " in Complex Systems[11]	Andrea Fiaschetti, Andrea Lanna, Martina Panfili, Silvano Mignanti,Antonio Pietrabissa, Francesco Delli Priscoli	OSSTMM & SHIELD METHOD	Dengan mengadopsi dari OSSTMM sebuah metrik perhitungan, maka didapatkan kerangka kerja kontrol untuk skenario sistem keamanan pSHIELD dan nSHIELD
A Developed Tool Matrix for Enhancing the Penetration Testing Methodology[12]	Ayman Al-ahwal1	OSSTMM	dari pengetesan yang di jelaskan dan dari tool yang di gunakan untuk pengetesan di hasilkan bahwa pentesting tidak mempunyai goals atau fokus yang di jalankan tapi pentesting mencari kelemahan yang ada pada suatu sistem yang di analisis kan untuk percobaan pengetesan
Comparative Study of Penetration Test Methods[13]	Yong-Suk Kang1, Hee-Hoon Cho2, Yongtae Shin3 and Jong-Bae Kim4*	OSSTMM,OWASP,ISSFS,RSA	OSSTMM berlaku sebagai inspeksi, OWASP kerangka uji untuk aplikasi web, ISSFS dirancang dalam jenis kerangka kerja terstrukstur untuk dinilai berbagai sistem informasi, RSA menentukan tingkat keamanan berdasarkan point yang dihitung. Bahwasanya pemilihan metodologi pengujian perlu dipertimbangkan dalam berbagai faktor untuk mencapai efisiensi maksimum
Web Vulnerability Analysis and Implementation[14]	E.B Setiawan, A. Setiyadi	OSSTMM	Pengujian keamanan menggunakan sistem situs web dari OSSTM dan mendapatkan hasil bahwa keamanannya mendapatkan nilai 74,5% dari nilai maksimal yaitu 100%. Selain itu, metode lain yang dapat digunakan adalah NIST dan ISSAF, tetapi hasilnya tidak sebagus metode

			OSSTM
Analisis Komparatif Sistem Kemanan Windows 7 & 8[15]	Cosmos Eko Suharyanto	NIST SP 800-115	Dalam penggunaan metode nist sp 800-115 didapatkan windows 8 lebih baik dari windows 7 untuk segi keamanan
Website Vulnerability Analysis Using NIST SP 800-115 and OWASP Method In Diskominfo, Bandung District[16]	Rubenson Christian Silaban1 , Erick Wijaya2	NIST SP 800-115	Dalam penggabungan nist sp 800-115 dengan OWASP dapat mendeteksi adanya kerentanan untuk sql injection untuk web diskominfo bandung terutama terhadap subdomain http://diskop.bandungkab.go.id. Dengan metode tersebut mendapatkan adanya kelemahan patching security OS pada masing – masing server yang berjalan baik itu windows maupun linux.
SELECTION OF PENETRATION TESTING METHODOLOGIES: A COMPARISON AND EVALUATION [7]	Aleatha Shanley1, Michael N. Johnstone1,2	OSSTMM, OWASP,ISSAF	Kerangka kerja baik OSSTMM,OWASP,ISSAF masih kurang dapat digeneralisasi ditarget issue. Karakteristik kualitas dapat dipetakan dengan baik menggunakan kerangka kerha ISSAF & OTG, sehingga dapat mengevaluasi penetrasi kerangka kerja pengujian.
"Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario	Carlos J. Martínez-Santander, Yolanda de la N. Cruz-Gavilanes	OSSTMM	Dengan menggunakan OSSTMM pada windows 64 bit terakhir, terdapat 95% kesalahan keamanan pada sistem tersebut. Dikarenakan para pengguna sistem tersebut minim akan informasi untuk mengoptimalisasikan sistem keamanannya

final"[17]			

Dari hasil review paper mengenai Penetretion testing dan identifikasi metode keamanan menggunakan NIST dan OSSTMM ini penulis menyimpulkan bahwa dari metode metode yang di bahas sama sama memiliki keunggulan dan kelemahan masing masing, untuk akurasi serta implementasi yang di jalankan bahwa metode perlindungan security dari sistem yang di gunakan bisa di cocokan terlebih dahulu dari apa yang ingin kita bangun dari aspek security

5. KESIMPULAN DAN SARAN

Ada beberapa faktor yang menyebabkan perbedaan metodologi penggunaan untuk implementasi security dari sistem yang akan di bangun. Yaitu :

1. Dari peraturan negara dan stadarisasi yang di gunakan dari beberapa negara
2. Adanya perbedaan pada penilaian risk yang ada, di OSSTMM menggunakan Nilai Risk Assessment (RAV) dan di NIST sp 800-115 menggunakan parameter yang di publicasikan oleh NIST.
3. NIST mengeluarkan sebuah publikasi yang di gunakan untuk assesment berdasarkan tujuan dari organisasi yang ingin di testing. Jika OSSTMM bisa di ubah sesuai dengan spesifikasi yang di butuhkan dari segi bisnis.
4. Nist membagi beberapa case dan beberapa seri dari assesment nya dari segi framework, network security, dan information technology,
5. Dari penilaian OSSTMM bisa menggunakan RAV calculator yang di sediakan oleh OSSTMM untuk penghitungan penilaiannya disertai STAR sebagai template dari audit. Sedangkan NIST untuk audit mengaju pada ROE.

Untuk selanjutnya, penulis berkesimpulan bahwa dalam memilih metode dari kebutuhan yang akan di lakukan dalam assesment. Alangkah baiknya menilai dari segi kebutuhan sumberdaya itu sendiri. Yang menjadi patokan adalah metode yang akan di terapkan, keputusan bisa lebih sulit karena setiap perusahaan memiliki sistem jaringan dan sistem yang berbeda. Akan tetapi pilihan tergantung pada asumsi pengajuan dan tujuannya, diantara banyak metodologi yang tersedia seperti NIST SP 800-115 untuk pengujian dan penilaian keamanan informasi.

Sementara OSSTMM dapat digunakan untuk pengujian yang berfokus pada seluruh telekomunikasi dan infrastruktur jaringan perusahaan, termasuk keamanan lokasi dan pengujian keamanan karyawan. Harus dicatat bahwa analisis teoritis yang terkandung dalam setiap metodologi baik nist sp 800-115 dan OSSTMM hanya membantu dalam melakukan kegiatan berdasarkan prosedur yang ditetapkan masing-masing, tetapi belum tentu menyediakan alat serta solusi siap pakai untuk menjamin tes yang sukses dikarenakan masih mengadopsi alat dan solusi open source.

Dari IC2 kriteria kelayakan,

penulis mereview paper dan menganalisa metode OSSTMM dan NIST 800-115. Banyaknya penggunaan metode OSSTMM dikarenakan adanya penilaian hasil berbentuk matriks atau persentase dalam ruang lingkup infrastruktur yang kecil maupun besar.

DAFTAR PUSTAKA

[1] R. Holloway, "Standardised penetration testing ? Examining the usefulness of current penetration testing methodologies .," no. September, 2019.

[2] Hack2Secure, "A Brief Summary Of Technical Assessment Techniques NIST SP 800 115," *2017-11-10*, 2017. [Online]. Available: https://www.hack2secure.com/blogs/a-brief-summary-of-technical-assessment-techniques-nist-sp-800-115.

[3] K. Scarfone and A. Orebaugh, "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology."

[4] M. Osborne, *Hacking Exposed*, Third Edit. 2007.

[5] P. Herzog, "OSSTMM: The Open Source Security Testing Methodology Manual: v3," *Isecom*, p. 213, 2016.

[6] ISECOM, "Open Source Security Testing Methodology Manual (OSSTMM)," *november 2019*, 2019. [Online]. Available: http://www.isecom.org/research/.

[7] A. Shanley and M. N. Johnstone, "Selection of penetration testing methodologies : A comparison and evaluation," vol. 2015, pp. 65–72, 2015.

[8] PTES, "Penetration Testing Execution Standard." 2014.

[9] Y. I. Fernando and R. Abdillah, "Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM)," vol. 2, no. 1, pp. 33–40, 2016.

[10] F. Ali, H. Ali, and M. T. A. Wahab, "SK42 Sistem Maklumat Pengujian Keselamatan Teknologi Maklumat Berasaskan OSSTMM," no. Skskm, pp. 21–22, 2010.

[11] A. Fiaschetti, A. Lanna, M. Panfili, S. Mignanti, A. Pietrabissa, and F. D. Priscoli, "Attack-Surface metrics , OSSTMM and Common Criteria based approach to " Attack-Surface metrics , OSSTMM and Common Criteria based approach to ' Composable Security ' in Complex Systems," no. September 2016, 2015.

[12] A. Al-ahwal, "A Developed Tool Matrix for Enhancing the Penetration Testing Methodology," vol. 18, no. 3, pp. 74–77, 2016.

[13] Y.-S. Kang, H.-H. Cho, Y. Shin, and J.-B. Kim, "Comparative Study of Penetration Test Methods," vol. 87, pp. 34–37, 2015.

[14] I. O. P. C. Series and M. Science,

"Web vulnerability analysis and implementation," 2018.

[15] C. E. Suharyanto, "Analisis Komparatif Sistem Keamanan Windows 7 Dan Windows 8," *JIF (Jurnal Ilm. Inform.*, vol. 4, no. 1, pp. 1–16, 2016.

[16] R. C. Silaban, E. Wijaya, and J. D. No, "WEBSITE VULNERABILITY ANALYSIS USING NIST SP 800-115 AND OWASP METHOD IN DISKOMINFO , BANDUNG DISTRICT," pp. 2–7.

[17] I. De Sistemas, "Magíster en Seguridad Telemática, Ingeniera en Electrónica y Telecomunicaciones, Dibujante Técnica, Corporación Nacional de Telecomunicaciones.," vol. 3, pp. 505–516, 2017.