**JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu**
*E-Mail*: jiifkom@sttrcepu.ac.id

# Analisis Serangan Penetration Testing: Sebuah Review Sistematik

Arya Kukuh Y [1], Geraldo Alfarenb [2], Indra Gunawan[3*]

Jurusan Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe [12]
Jurusan Informatika Sekolah Tinggi Teknologi Ronggolawe [3]

[*]Email: igunsttr@gmail.com

Tentang naskah:
-diterima, 14 Jun 2022
-direview, 27 Jun 2022
-diterbitkan, 1 Jul 2022

Kata kunci: Penetration Testing; Analisis; Review Sistematik

*Keyword*: *Penetration Testing; Analysis; Systematic Review*

**Intisari**

Secara umum, proses penetration testing system banyak disamakan oleh para junior system administrator dengan proses vulnerability system assessment. Kesalahan mindset tersebut menjadi suatu kesalahan fatal dalam pengelolaan keamanan sistem komputer. Vulnerability system assessment merupakan sebuah prosedur scanning terhadap vulnerabilities yang terdapat pada sistem dan melalukan filtering terhadap kelemahan tersebut untuk menghindari aksi eksploitasi oleh hacker. Hal ini jelas hampir mirip dengan pengertian harfiah dari penetration testing yang mana proses pencarian terhadap vulnerabilities (kelemahan) dan melakukan eksploitasi terhadap sistem tersebut hingga tester mengetahui titik lemah sebenarnya dari sistem tersebut.memberikan gambaran bahwa manajemen terhadap system keamanan komputer merupakan sebuah hal keharusan yang harus dilakukan

***Abstract***

*In general, the penetration testing system process is often compared by junior system administrators to the system vulnerability assessment process. This mindset error has become a fatal error in managing computer system security. Vulnerability system assessment is a procedure for scanning for vulnerabilities in the system and filtering these weaknesses to avoid exploitation by hackers. This is clearly almost similar to the literal meaning of penetration testing which is the process of searching for vulnerabilities (weaknesses) and exploiting the system until the tester knows the real weak points of the system*

## 1. Pendahuluan

Ancaman keamanan terhadap sistem Anda dan risiko serangan dapat berasal dari tiga aspek: integritas, kerahasiaan, dan ketersediaan. Oleh karena itu, penting untuk melindungi sistem berbasis digital Anda dari ketiga hal tersebut. (Gunawan, 2021).

Salah satu risiko tersebut adalah ancaman yang biasa disingkat dengan penetration testing, atau pengujian penetrasi. Ini adalah pengujian yang dilakukan untuk mengetahui tingkat keamanan aplikasi atau web Anda. Seperti yang Anda ketahui, teknologi berkembang pesat saat ini. Akibatnya, banyak perusahaan akhirnya memutuskan untuk beralih dan bertransformasi ke digital. Tentunya sistem atau aplikasi keamanan web yang dibuat berisi data penting dalam jumlah besar dan membutuhkan tingkat keamanan yang memadai.

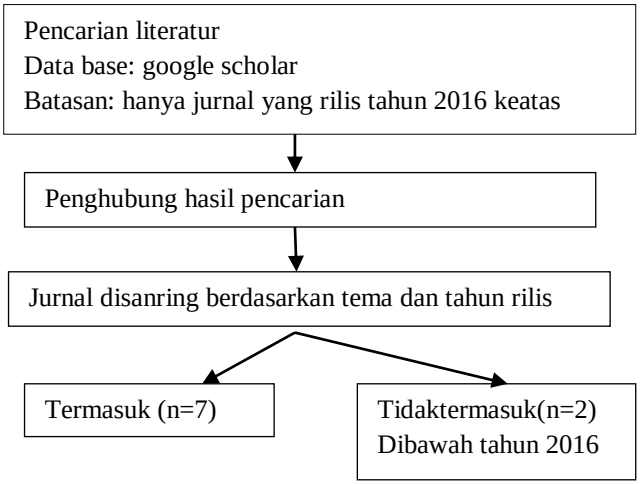
Namun, masih banyak perusahaan yang tidak menyadari bahwa sistem yang mereka buat memiliki kerentanan yang dapat diretas oleh pihak yang tidak bertanggung jawab. Untuk menghindari ini, Anda perlu menjalankan tes penetrasi. Inilah mengapa perusahaan membutuhkan pengujian penetrasi: Mereka yang melakukan tes dapat membantu menemukan kerentanan dalam sistem. Oleh karena itu, sistem keamanan dapat ditingkatkan dan ditingkatkan untuk menghindari serangan dari peretas. Perusahaan tentu memiliki data penting dalam jumlah besar. Namun pada kenyataannya masih banyak perusahaan yang tidak memproteksi datanya. Banyak data penting dapat diretas atau hilang tanpa diketahui. Uji penetrasi ini memperbaiki sistem keamanan yang rentan sehingga data penting dapat disimpan dengan aman di sistem.

## 2. Kerangka Teori

*Systematic review ini disusun berdasarkan pedoman pelaporan PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) (Liberati et al., 2009).Terdapat beberapa langkahdalam penelitian ini sesuai dengan pedoman tersebut, yaitu:*

- *Mendefinisikan*
- *kriteria kelayakan*
- *Mendefinisikan sumber informasi*
- *Pemilihan studi*
- *Pengumpulan data*
- *dan Pemilihan item data.*

Kepentingan penulis hanya berlaku untuk sistem keamanan jaringan. Gambar 1 merupakan flowchart PRISMA yang menggambarkan langkah-langkah kerja penulis dalam melakukan tinjauan sistematis.




**Gambar 1**. Diagram Aliran PRISMA

### Sumber Informasi

Jurnal-jurnal yang dibutuhkan untuk studi sistematis ini berasal dari database penelitian ilmiah, Google Scholar. Penulis hanya mengakses jurnal yang tidak memiliki persyaratan untuk mengambilnya. Selain itu, penulis mencari referensi yang terdapat dalam makalah untuk menemukan penelitian yang relevan. Seleksi Studi

Seleksi studi dilakukan pada tahap berikutnya.

Pencarian kata kunci dipilih untuk kepentingan penelitian penulis dalam pengujian keamanan jaringan. Kata kunci untuk mencari jurnal dalam database yang disebutkan adalah "Keamanan Jaringan" dan "Sistem Keamanan Jaringan".

Pencarian dan pemilihan judul dan kata kunci dari jurnal yang teridentifikasi berdasarkan kriteria kelayakan.

**Pengumpulan Data**

Pengumpulan data dilakukan secara manual dengan menggunakan perangkat tabel ekstraksi data yang terdiri dari judul, penulis, tahun, nama jurnal/rapat, jenis jurnal, pokok bahasan, metode penelitian, hasil pembahasan, dan kesimpulan. Pekerjaan yang terkait atau mungkin terkait dievaluasi bersama. Peringkat terdiri dari membaca teks lengkap dan data yang diekstraksi. Perbedaan itu diselesaikan melalui diskusi antara penulis. Item data penagihan

Informasi untuk setiap makalah adalah sebagai berikut.

1. Deskripsi Keamanan Jaringan
2. Sistem Keamanan Jaringan
3. Teknologi keamanan yang ada sebagai proteksi.

## 3. Metodologi

### 3.1 Pemilihan jurnal

Memberikan Hasil Pencarian di Basis Data Terpilih Hasil penelusuran di basis data yang dipilih menyediakan total 50 karya bahasa Inggris dari 2009 hingga 2019 yang cocok dengan kata kunci yang ingin Anda analisis. Selain itu, posting ini difilter berdasarkan judul, ringkasan, dan kata kunci. Sisanya 30 makalah kemudian dievaluasi menggunakan full text, dan 14 makalah ditolak karena tidak memenuhi kriteria IC2. Akhirnya, lima artikel dipilih yang memenuhi kriteria kelayakan dan menjadi sumber untuk tinjauan sistematis ini.

### 3.2 Fitur Jurnal

Tabel 1 memberikan informasi rinci tentang lima artikel yang dipilih untuk ekstraksi data akhir. Ekstraksi data akhir ini merupakan tabel ekstraksi data yang hanya berisi artikel yang dipilih berdasarkan kriteria proses seleksi jurnal.

### 3.2 Fitur Jurnal

Informasi rinci tentang lima makalah yang dipilih ditunjukkan pada Tabel 1 untuk ekstraksi data akhir. Ekstraksi data akhir ini merupakan tabel ekstraksi data yang hanya berisi artikel yang dipilih berdasarkan kriteria proses seleksi jurnal.

## 4. Hasil dan Pembahasan

### 4.1 Seleksi Jurnal

Hasil pencarian dalam database google shoolar yang dipilih memberikan total 10 penelitian yang ditulis dalam bahasa Indonesia dari tahun 2019 hingga 2021, cocok dengan kata kunci yang perlu dianalisis. Akhirnya terpilih 5 penelitian yang memenuhi kriteria kelayakan dan menjadi bahan dalam systematic review ini.

### 4.2 Karakteristik Jurnal

Informasi detil dari 6 penelitian/jurnal yang terpilih dapat dilihat pada Tabel 1 tentang ekstrasi data final. Ekstrasi data final ini adalah tabel ekstrasi data yang hanya berisi penelitian-penelitian terpilih berdasarkan kriteria-kriteria yang ada pada proses seleksi penelitian.

Table 1.1 Ekstrasi Data Final

| No | Penulis | Judul | Tipe Jurnal | Topik | Metode | Hasil Pembahasan | Kesimpulan |
|---|---|---|---|---|---|---|---|
| 1 | Harry Dwi Sabdho[1], Maria Ulfa[2] | Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor Pt. Mora Telematika Indonesia Regional Palembang | Research | Keamanan Jaringan | Kualitatif | • Cracking The Ecryption.<br>• Bypassing MAC Authentication.<br>• Attacking The InfrastructureMan In The Middle (MITM) Attack. | Dalam menerapkan penetration testing pada sebuah institusi dibutuhkan jaminan hukum terhadap pelaku dan objek penetration testing |
| 2 | Bambang Pujiarto[1] , Ema Utami[2], Sudarmawan[3] | Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus : Universitas Muhammadiyah Magelang) | Research | Keamanan Jaringan | Kualitatif | Metodologi ISSAF sebagai framework evaluasi sistem keamanan dengan metode penetration testing. | • Planning and preparation, mengahasilkan dokumen kebijakan dan agreement.<br>• Assessment, menghasilkan dokumen assessment.<br>• Reporting, menghasilkan dokumen evaluasi. |
| 3 | I Gede Ary Suta Sanjaya[1], Gusti Made Arya Sasmita[2], Dewa Made Sri Arsa[3] | Evaluasi Keamanan Website Lembaga x melalui Penetration Testing Menggunakan Framework | Research | Keamanan Jaringan | Kualitatif | Pengujian dilakukan pada website utama Lembaga X dan subdomain website yang terkait | Data diperoleh hasil bahwa terdapat celah keamanan yang berbahaya seperti SQL Injection dan XSS |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Issaf | | | | | |
| 4 | Ari Prayoga Hutabarat[1] , Haeruddin[2] | Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration | Research | Keamanan Jaringan | Kualitatif | pada jaringan dapat dilacak pada aplikasi Ettercap | Keamanan jaringan end user tidak dapat dibobol oleh Man In The Middle Attack dengan cara menambah konfigurasi pada router mikrotik |
| 5 | Denis Quroturohma | Penetration Testing Dalam Forensik Digital pada Jaringan Fakultas Teknik Universitas IBN Khaldun Bogor dengan Ping of Death | Research | Keamanan Jaringan | Kualitatif | pemberian serangan, deteksi, identifikasi pada log,dan pemblokiran. | Mengidentifikasikan masalah dalam sistem jaringan untuk menghasilkan kombinasi dalam menemukan kesalahan |

## 5. Simpulan

Dari penelitian tentang systematic review terkait dengan Penetration Testing, maka penulis menyimpulkan bahwaPenetration Testing sebuah metode dimana sistem keamanan suatu perusahaan di uji dan di cari kelemahannya agar sistem suatu perusahaan bisa dikembangkan lenih jauh lagi serta bisa mengantisipasi terjadinya peretasan pada sistem tersebut.

Tingkat keberhasilan proses Penetration Testing terhadap server sendiri ditentukan dari tingkat kreatifitas peretas untuk berpikir mencari jalan terbaik dan terefektif untuk memperoleh hasil seakurat mungkin terhadap kelemahan server.

Penetration testing memliki kekurangan apabila di terapkan sebuah institusi dibutuhkan jaminan hukum terhadap pelaku dan objek penetration testing,serta memeliki banyak kelebihan salah satunya Mengidentifikasikan masalah dalam sistem jaringan untuk menghasilkan kombinasi dalam menemukan kesalahan dan memeliki jangakuan yang lebih dari sitem lainnya.

## Daftar Pustaka


Gunawan, I. (2021). *Keamanan Data: Teori dan Implementasi*. Sukabumi: Jejak Publisher.

Hutabarat, A.P., 2020. Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration. *Journal of Information System and Technology*, *1*(2), pp.31-36.

Quroturohman, D., 2021. PENETRATION TESTING DALAM FORENSIK DIGITAL PADA JARINGAN FAKULTAS TEKNIK UNIVERSITAS IBN KHALDUN BOGOR DENGAN PING OF DEATH. *Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika*, *4*(2), pp.81-84.

Pujiarto, B., Utami, E. and Sudarmawan, S., 2013. Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus: Universitas Muhammadiyah Magelang). *Data Manajemen dan Teknologi Informasi (DASI)*, *14*(2), p.16.

Sanjaya, I.G.A.S., Sasmita, G.M.A. and Arsa, D.M.S., 2020. Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, pp.113-124.

Sabdho, H.D. and Ulfa, M., 2018. Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 1, No. 1, pp. 15-24).