Exploring the Depths: An Overview of Penetration Testing

Oleh:
Muhammad Yusuf, Aries Suharso
Universitas Singaperbangsa Karawang, Indonesia
Email: muhammad.yusuf17158@student.unsika.ac.id

Abstract

The security of a web server from data leaks is a critical factor before creating one. Penetration testing is an attempt to exploit a computer system to find data stored within it. This review aims to provide an overview of penetration testing, highlighting its implementation scenarios, models, methodologies, and tools from various existing studies. The results of this review are expected to serve as a reference for understanding the aspects and solutions of penetration testing. The review was conducted by collecting 1,023 articles, which were evaluated based on the PRISMA method, narrowing them down to 12 articles. These 12 articles were then classified based on the tools, models, and methodologies used in penetration testing. This classification aims to provide deeper insights into the best practices for penetration testing and to identify the most effective tools and techniques for securing web servers against threats and data breaches.

Keywords: Web server security, Penetration testing, PRISMA method

A. Pendahuluan

Salah satu bentuk yang dikenal untuk menilai keadaan keamanan dan mengurangi risiko keamanan disebut uji penetrasi (Pentest). Pentest adalah tentatif terkontrol untuk menembus ke dalam sistem atau jaringan untuk mengidentifikasi kerentanan. Pentest menerapkan teknik yang sama yang digunakan dalam serangan biasa oleh seorang hacker. Alternatif ini memungkinkan tindakan yang tepat diambil untuk menghilangkan kerentanan sebelum dapat dieksplorasi oleh orang yang tidak berwenang.[1]

Aspek terpenting sejalan dengan meningkatnya volume data di internet adalah keamanan jaringan. Setiap organsiasi baik sebuah instansi maupun perusahaan wajib hukumnya untuk menjaga kerahasian data dari sebuah web server yang dimiliki. Selain itu, meningkatnya penggunaan masyarakat terhadap sebuah sistem informasi jaringan mengharuskan keamanan dari sebuah sistem harus diperhatikan dan terus ditingkatkan. Seperti kasus yang baru-baru ini terjadi perihal bobolnya sebuah sistem

[1] Whitaker A, Newman D (2005) Pengujian penetrasi dan pertahanan jaringan Cisco. Cisco Press, Indianapolis.

informasi yang dimiliki oleh sebuah intansi pemerintahan yang menyebabkan data pribadi yang tersimpan dalam sistem tersebut berhasil dicuri dan diperjual belikan.

Dalam artikel ini, akan ditinjau secara sistematis dengan mengguanakan metode meta- analisis perihal penetration testing. Metode meta-analisis dan tinjauan sistematis dapat membantu dalam pembuatan evaluasi yang lebih jelas dan lebih ringkas[2]. Selain itu, tinjauan sistematis bisa membantu peneliti dalam membandingkan, berdebat, dan memilih dari literatur yang lebih besar untuk mendapatkan lebih banyak hasil yang dapat dipercaya.[2]

Langkah pertama adalah membuat pertanyaan penelitian (RQ), diantaranya:

- RQ1: Target utama publikasi dalam pengujian penetration testing?
- RQ2: Scenario jenis apa yang menjadi target di penetration testing?
- RQ3: Model jenis apa yang digunakan dalam penetrataion testing?
- RQ4: Batasan ataupun tantangan dalam penetration testing?

Langkah selanjutnya adalah menjawab pertanyaan penelitian diatas menggunakan metode analisis prisma diagram. Kemudian, langkah terakhirnya adalah menyimpulkan jawaban pertanyaan penelitian (RQ) berdasarkan artikel yang telah didapatkan dengan metode analisis prisma diagram.

Proses mencari dan memilih literatur dilakukan menggunakan metode analisis prisma seperti pada gambar 1, sebagai berikut:

1 Identifikasi: pencarian awal dilakukan dengan mengunakan mesin pencari Harzing Publish or Perish edisi 8 dengan menginput judul web penetration dan kata kunci penetration testing. Diperoleh 1000 artikel dari Crossref dan 23 artikel dari Scopus. Kemudian artikel tersebut disorting kembali dengan membatasi minimal 7 sitasi dari setiap artikel untuk mendapatkan artikel populer yang sering dirujuk oleh para peneliti. Hasil dari sorting tersebut didapatkan 44 artikel dari Crossref dan 4 artikel dari Scopus. Jadi, jumlah artikel yang didapatkan adalah 48 artikel.

2 Screening: dari 48 artikel yang telah didapatkan dari tahap identifikasi tersebut, disorting kembali dengan menghapus artikel dengan judul yang

[2] J. L. Peters, A. J. Sutton, D. R. Jones, K. R. Abrams, and L. Rushton, "The contribution of systematic review and meta-analysis methods to human health risk assessment: Neurobehavioral effects of manganese, "Hum. Ecol. Risk Assess.,vol. 14, no. 6, pp. 1250–1272, 2008, doi: 10.1080/10807030802494592

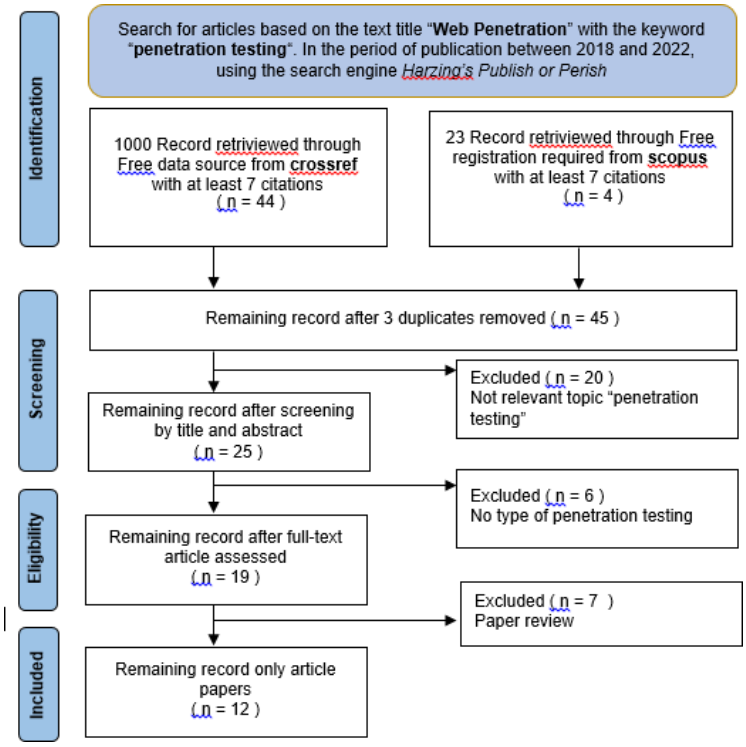
sama. Terdapat 3 artikel dengan judul yang sama. Sehingga didapatkan 45 artikel berbeda.

Kemudian, dari 48 artikel tersebut, disortir kembali dengan menghapus artikel yang tidak mengandung unsur penetration testing. Terdapat 20 artikel yang tidak mengandung topik penetration testing. Sehingga jumlah artikel yang didapatkan adalah 25 artikel.

3 Eligibility: Selanjutnya, dari 25 artikel tersebut disortir kembali dengan membaca abstract artikel tersebut apakah terdapat metode penetration testing. Terdapat 6 artikel yang tidak memuat metode penetration testing dan 19 artikel meneliti metode dari penetrataion testing. Kemudian dari 19 artikel tersebut disortir kembali dengan hanya memasukan artikel penelitian bukan artikel ulasan. Didapatkan 12 artikel yang merupakan artikel penelitian dan 7 artikel ulasan.

4 Included: hasil akhirnya didapatkan 12 artikel yang mengandung konteks web penetration dan penetration testing dengan jenis artikel penelitian yang nantinyan akan digunakan sebagai referensi penelitian meta-analisis.

Gambar 1.1 Prisma Diagram



B. Pembahasan

Menjawab pertanyaan RQ1 ditunjukan pada tabel 1, yang mana dari total 48 artikel yang ada, penerbit menerbitkan artikel penelitiannya dengan topik penetration testing diataranya jurnal Elsevier (8 artikel), IEEE (1 artikel), MDPI (1 artikel), Springer Science and Business Media LLC (1 artikel), dan yang terakhir Taylor & Francis (1 artikel). Jika diperhatikan, bahwa semua jurnal tersebut di atas sebagian besar terindeks dalam Journal Citation Report di kuartil Q1 dan Q2.

Tabel 1.1 Publikasi artikel pilihan

Jurnal	Tahun	Jumlah
Elsevier BV	2021	1
Elsevier BV	2019	2
Elsevier BV	2018	5
IEEE	2018	1
MDPI AG	2019	1
Springer Science and Business Media LLC	2019	1
Taylor & Francis	2019	1

Untuk jawaban dari pertanyan penelitian RQ2, berdasarkan artikel yang telah dipilih melalui proses prisma diagram, diperoleh skenario yang menjadi target utama dari serangkaian kegiatan penetration testing. Tabel 2 mencantumkan skenario penetration testing dan tahun publikasi. Berdasarkan tabel 2, dapat disumpulkan bahwa skenario penetration testing yang seringkali digunakan oleh peneliti adalah Web-based Application.

Tabel 1.2 Skenario penetration testing

Penetration testing	Referensi
Web based application	[5][4][9][10][12]
Web service	[6][3]
Networks protocol and service	[7][11]
Software and application	[1][2][8]

Kemudian, jawaban dari pertanyan penelititan RQ3 dapat dilihat pada tabel 3. Berdasarkan tabel tersebut, diperoleh model yang sering digunakan peneliti adalah OWASP Testing Guide.

Tabel 1.3 Model penetration testing

Model penetration testing	Last Update	Referensi
OSSTMM	2010	[3][6]
ISSAF	2006	[10]
PTES	2012	[1][7][9]
NIST Guidelines	2008	[12]
OWASP Testing Guide	2014	[2][4][5][8][11]

Pertanyaan penelitian RQ4 perihal tantangan dalam penetration testing berdasarkan dari artikel-artikel tersebut, salah satu permasalahan utamanya adalah mengenai keefektifan proses penetration testing, model dan alat untuk memastikan seberapa besar tingkat keamanan suatu sistem informasi dengan berbagai macam skenario yang ada berdasarkan target tertentu. Selain itu, tantangan yang lainnya perihal kompleksitas beberapa serangan, penemuan celah baru, dan kemajuan teknologi dapat mengubah pengaplikasian penetration testing

C. Kesimpulan

Dari tahun 2018, sudah terdapat lebih dari 1023 artikel, baik artikel penelitian maupun artikel review, dan artikel tersebut dari waktu ke waktu diperkirakan akan terus bertambah seiring dengan kompleksnya data yang tersimpan dalam sebuah sistem informasi. Dari hasil sortir yang dilakukan, mendapatkan 12 artikel yang paling banyak disitasi oleh peneliti dan gambaran mengenai penetration testing. Penetration testing dilakukan untuk memperkuat suatu sistem informasi dan sudah menjadi hal wajib bagi setiap sistem informasi untuk memiliki keamanan dari berbagai macam kemungkinan pembobolan data. Berdasarkan penelitian yang telah dilkukan, dapat diketahui bahwa begitu pentingnya untuk meningkatkan dan melengkapi penetration testing.

Referensi

Anton, A., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy, 8(1), 21-27. https://doi.org/10.1109/MSP.2010.56*

Bacudio, A. G., Yuan, X., Chu, B. T., & Jones, L. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications (IJNSA), 3(6), 19-38. https://doi.org/10.5121/ijnsa.2011.3602*

Bejtlich, R. (2004). The Tao of Network Security Monitoring: Beyond Intrusion Detection. *Addison-Wesley Professional.*

Bisong, A., & Rahman, S. M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA), 3(1), 30-45. https://doi.org/10.5121/ijnsa.2011.3103*

Chuvakin, A., Schmidt, C., & Phillips, S. (2004). *Security Warrior. O'Reilly Media, Inc.*

Cox, S., & Gergis, A. (2005). *Ethical Hacking: Network Security Assessment. Syngress.

Farina, B., Scanlon, M., & Le-Khac, N. A. (2015). Overview of the PRISMA method and its applicability in digital forensics. Digital Investigation, 14(Supplement 1), S1-S9. https://doi.org/10.1016/j.diin.2015.05.007

Joshi, R. C., & Joshi, A. (2013). Penetration testing framework for cloud computing systems. Journal of Computer Networks and Communications, 2013, Article ID 726474. https://doi.org/10.1155/2013/726474

McClure, S., Scambray, J., & Kurtz, G. (2012). Hacking Exposed 7: Network Security Secrets and Solutions. McGraw-Hill Osborne Media.

Miller, B., & Gregory, J. (2014). Network Security Evaluation Using Penetration Testing. Springer.

NIST. (2008). Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. NIST Special Publication 800-84. National Institute of Standards and Technology.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. National Institute of Standards and Technology.