Uji Kerentanan Keamanan Server Menggunakan Scada Shodan

Joko Dwi Santoso
Universitas AMIKOM Yogyakarta, Yogyakarta, Indonesia
e-mail :joko@amikom.ac.id

Abstrak—Keamanan telah menjadi aspek penting bagi dunia internet. Layanan dalam sebuah server harus memiliki tingkat keamanan yang terjamin, agar layanan hanya dapat diakses oleh orang yang berhak untuk mengakses layanan tersebut. Keamanan server saat ini sangat penting karena menyangkut privasi seseorang maupun privasi sebuah lembaga atau perusahaan. Meningkatnya kasus pencurian data di dunia internet juga menjadi salah satu latar belakang pentingnya sebuah keamanan server. Mengukur tingkat keamanan sebuah server dapat dilakukan dengan berbagai cara diantaranya dengan melakukan penilaian kerentanan dan pengujian penetrasi. Penilaian kerentanan dan pengujian penetrasi adalah dua pengujian kerentanan yang berbeda. Dua metode ini memiliki kekuatan yang berbeda dan tentunya menghasilkan sebuah nilai pengukuran yang berbeda. Setelah mendapatkan sebuah nilai kerentanan dalam sebuah server diharapkan kedepanya dapat menentukan solusi yang tepat untuk mengatasi kerentanan tersebut.

Kata Kunci : Server, PengujianKerentanan, Penetrasi Test.

Abstract — Security has become an important aspect of the internet world. Services on a server must have a guaranteed level of security, so that services can only be accessed by people who are entitled to access the service. Server security is very important now because it involves a person's privacy or the privacy of an institution or company. The increasing cases of data theft in the internet world has also become one of the background to the importance of server security. Measuring the level of security of a server can be done in various ways including by conducting vulnerability assessments and penetration testing. Vulnerability assessment and penetration testing are two different vulnerability tests. These two methods have different strengths and of course produce a different measurement value. After getting a vulnerability value in a server, it is expected that in the future it can determine the right solution to overcome the vulnerability.

Keywords: Server, Vulnerability Testing, Penetration Test.

I. PENDAHULUAN

Tercatat lebih dari xx kasus peretasan terjadi dalam dunia internet [1]. Tidak hanya peretasan kini para pengguna internet juga mendapat beberapa macam insiden yang dapat merugikan personal, lembaga, maupun perusahaan. Insiden tersebut dapat digolongkan menjadi tiga bagian utama yaitu vulnerability, attack, dan virus. Pada penelitian ini akan dibahas insiden dalam internet yaitu vulnerability atau yang sering disebut kerentanan. Kerentanan merupakan sebuah celah atau lubang yang berpotensi untuk dimanfaatkan oleh orang yang tidak bertanggung jawab untuk memanipulasi data dalam sebuah database. Database pada umumnya disimpan dalam sebuah komputer yang disebut dengan server.

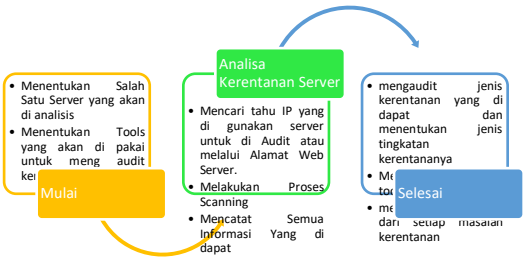
Server menyimpan semua layanan dan data yang dibutuhkan oleh pengguna. Layanan dan data tidak boleh terganggu oleh hal yang dapat menghambat layanan dan menghalangi akses data oleh pengguna. Layanan dan data harus tersedia dalam kondisi yang benar ketika diakses oleh pengguna yang membutuhkan. Dari uraian tersebut maka dapat disimpulkan bahwa server harus memiliki sistem keamanan yang dapat mengamankan server dari gangguan yang ada dalam jaringan. Administrator dari sebuah server harus memastikan bahwa server harus memiliki tingkat kerentanan yang bernilai 0, atau dapat diartikan bahwa server tidak memiliki celah keamanan.

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini adalah:

a. Bagaimana melakukan Uji kerentanan pada server Menggunakan Scada Shodan ?
b. Bagaimana menganalisis data hasil penilaian kerentanan dan pengujian pada Server?

II. METODE PENELITIAN

A. Skema Shodan



Gambar 1. AnalisiiSkema Shodan

B. Scada Shodan

Hasil yang di perolehmenggunakanscada Shodan adalahsebagaiberikut :

Tabel 1. Scanning Scada Shodan

203.91.9.42	HTTP/1.1 200 OK Date: Thu, 29 Aug 2019 23:07:39 GMT Server: Apache X-Powered-By: PHP/5.4.41 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=cdd4486b48b2c473c2f244aba9bd991d; path=/ ...

III. HASIL DAN PEMBAHASAN

A. TahapAnalisis CVE

Tahapaninibertujuanuntukmengembangkanhasiltemuankerentanan yang di dapatmenggunakan web tool scanning scadashodan. Nilai batasKerentanandapat di lihat pada lama CVE Deatails.

Tabel 1. CVSS Score 28 – 08 – 2019

CVSS Score	Number Of Vulnerabilities	Percentage	Level
0-1	1147	0.90	LOW
1-2	895	0.70	
2-3	4747	3.90	
3-4	4359	3.60	
4-5	26584	22.00	
5-6	23190	19.20	MEDIUM
6-7	16495	13.70	
7-8	26772	22.20	
8-9	540	0.40	CRITICAL
9-10	16016	13.30	
Total	120745		

B. Hasil Nilai AkhirKerentanan Antara CVE Details dan OOWASP ZAP

1. Analisa IP 203.91.9.43

Dari data Scanning Shodan pada alamat IP inipenelitimendapatkan 2 JenisKodeKerentanan, Antara Lain Sebagaiberikut :

Tabel2.. Hasil Audit IP 203.91.9.42 Menggunakan Web Tools CVE Details

No	Kode CVE	JenisKerentanan	Score
1	CVE-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'	5.0
2	CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.	5.0

2. Hasil AnalisisMenggunakan Teknik Scada Shodan.

Tabel 3. Hasi; Analisis Menggunakan Scada Shodan.

Risk Level	Number of Alerts	Alert Details	Vulnerabilities
High	0		
Medium	1	**Low (Medium)**	**Cookie No HttpOnly Flag**
Low	5	**Low (Medium)**	1. Cross-Domain JavaScript Source File Inclusion 2. X-Content-Type-Options Header Missing 3. Web Browser XSS Protection Not Enabled 4. Absence of Anti-CSRF Tokens 5. Cookie No HttpOnly Flag
Informational	0		

IV. KESIMPULAN

1. Proses identifikasi kerentanan server menggunakan scadasho dan berjalan dengan baik.
2. Analisis data informasi dari pengembangan atau uraian Scada Shodan menghasilkan tingkat kerentanan server rata rata pada level LOW (MEDIUM), sehingga bias dikatakan server dalam kondisi performance kurang baik untuk melindungi asset asetnya. hasil penelitian dan aplikasi lebih lanjut pada penelitian berikutnya.

DAFTAR PUSTAKA

[1] M. Bishop, “About Penetration Testing,” *IEEE Secur. Priv.*, vol. 5, no. 6, pp. 84–87, Nov. 2007.

[2] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, “Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques,” in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 25–30.

[3] D. F. Mosley, "Client-server user-interface testing," *IEEE Softw.*, vol. 12, no. 1, pp. 124–127, Jan. 1995.

[4] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, 2017, pp. 1–6.

[5] Mohmmad Muhsin, Adi Fajaryanto (2015), PenerapanPengujiankeamanan Web Server MenggunakanMetode OWASP Versi 4 (StudiKasus Web Server ujian Online)

[6] Karandeep Singh, Sandeep Sharma (2015), Combating Broken Authentication And Session management