Security Assessment Menggunakan Tool Nessus Untuk Mencari Celah Keamanan Web Aplikasi Repositori di Institusi Pendidikan

Security Assessment by using Tool Nessus for Finding Security Gaps of Repository Web Application in Educational Institution.

KAUKA NOOR FATHUR RIZKO, CHAYADI OKTOMY NOTO SUSANTO, DWIJOKO PURBOHADI

ABSTRACT

Paper ini berisi informasi tentang penelitian yang dilakukan untuk mengetahui celah keamanan dan risiko yang \kemungkinan ditimbulkan pada web aplikasi repositori milik institusi pendidikan tersebut. Web aplikasi repositori adalah web yang berisi data penelitian, jurnal, artikel dan paper dari staf pengajar dan mahasiswa di institusi tersebut. Web aplikasi ini belum memiliki dokumentasi tentang celah keamanan dan risiko yang mungkin saja terjadi pada web aplikasi tersebut. Hal ini menyebabkan muncul rasa kekhawatiran pada pihak institusi pendidikan. Oleh karena itu diperlukan adanya kegiatan *security assessment* untuk melakukan penilaian yang berorientasi kepada risiko yang mungkin bisa terjadi jika terjadi karena percobaan serangan. *Security Assessment* menggunakan metode VAPT (*Vulnerbility Assessment and Penetration Testing*). Metode tersebut digunakan untuk melakukan penilaian keamanan dan pengujian terhadap web aplikasi repositori milik institusi pendidikan. Beberapa kerentanan yang ditemukan dengan tool Nessus masih bisa dimanfaatkan dan menghasilkan temuan berupa hak akses yang legal ketika peneliti melakukan simulasi pengujian pada web aplikasi repositori. Penelitian ini digunakan sebagai laporan kepada pihak institusi pendidikan sebagai bahan untuk dilakukan proses evaluasi dan peningkatan keamanan terhadap web aplikasi yang dimilikinya. Penelitian ini hanya dilakukan didalam lingkungan Institusi Pendidikan, sehingga kegiatan ini belum sepenuhnya menggambarkan tentang kemungkinan serangan sebenarnya yang berasal dari luar lingkungan Institusi Pendidikan.

Kata Kunci **:** *Security Assessment*, *Vulnerability Assessment and Penetration Testing*, dan *Nessus*

PENDAHULUAN

Sebuah teknologi informasi dibangun untuk memudahkan manusia dalam mengelola dan menyebarkan informasi yang bersifat publik maupun rahasia [1]. Informasi yang dikelola dan disebarkan harus memiliki integritas atau dapat dipercaya, oleh sebab itu keamanan terhadap informasi menjadi hal yang penting, karena dapat mempengaruhi citra institusi pendidikan tersebut. Ancaman pada informasi dapat bersumber dari mana saja. Untuk mengetahui dan meminimalisir ancaman keamanan yang dapat menyebabkan risiko, perlu dilakukan kegiatan untuk mengukur risiko tersebut. Security Assessment adalah serangkaian kegiatan yang ditempuh untuk menilai sebuah keamanan pada web aplikasi. Penilaian yang dilakukan pada security assessment berorientasi kepada risiko [2]. Tujuan dari kegiatan ini adalah mengetahui celah keamanan dan risiko yang ditimbulkan atas percobaan serangan pada sebuah web aplikasi. Risiko yang dihasilkan dapat berupa pengambilan informasi penting atau upaya untuk menggagalkan proses teknologi informasi yang berjalan. Kegiatan tersebut dinilai perlu untuk meningkatkan mekanisme pelindung keamanan informasi yang bersifat rahasia. Langkah yang dilakukan berupa tindakan pencegahan, deteksi, dan respons [3].

Observasi yang dilakukan pada web aplikasi repositori , diketahui bahwa, web aplikasi tersebut belum pernah dilakukan upaya untuk pengukuran celah keamanan yang dapat menimbulkan risiko atau bisa disebut sebagai security assessment. Hal ini menjadi kekhawatiran tersendiri bagi peneliti jika sewaktu waktu terjadi penyerangan, karena web tersebut berisi informasi tentang peneltian yang dilakukan oleh dosen dan mahasiswa di . Oleh sebab itu perlu adanya penilaian keamanan atau

security assessment pada web aplikasi repositori . Kegiatan tesebut dilakukan dengan metode VAPT (Vulnerability Assessment and Penetration Testing). Metode tersebut digunakan untuk melakukan kegiatan security assessment. Metode VAPT terdiri atas dua kegiatan utama, yaitu Vulnerability Assessment dan Penetration Testing yang ujuannya adalah untuk mendapatkan informasi penting pada sebuah web aplikasi [4].

Vulnerability Assessment adalah pencarian celah keamanan sistem yang dapat menyebabkan kegagalan proses teknologi informasi. Setelah penyerang menemukan celah, penyerang menentukan cara untuk mengaksesnya. Dengan demikian ancaman terhadap kerahasiaan yang dimiliki oleh aplikasi meningkat. Penyerang menggunakan tool untuk mengidentifikasi kerentanan aplikasi [5]. Tool untuk mengidentifikasi kerentanan aplikasi adalah Nessus. Nessus adalah sebuah *tool* untuk mencari celah keamanan pada perangkat lunak atau halaman web. *Tool* ini memungkinkan penyerang untuk menemukan cara untuk menembus keamanan pada sebuah software atau halaman web [6]. Setelah menemukan celah keamanan, selanjutnya dilakukan penetration testing. Penetration testing adalah sebuah cara untuk mengidentifikasi celah keamanan pada penerapan mekanisme keamanan sebuah sistem. Kegiatan ini dilakukan dengan cara menyerang terhadap sistem komputer dengan tujuan menemukan kelemahan keamanan, berpotensi mendapatkan akses ke sana, fungsi dan datanya [7]. Hasil simulasi serangan ini kemudian didokumentasikan dan disajikan sebagai laporan kepada stackholder terkait. Institusi Pendidikan dapat menjadikan paper ini sebagai bahan evaluasi untuk meningkatkan keamanan pada web aplikasi repositori miliknya.

METODE

Kegiatan security assessment ini menggunakan metode VAPT (Vulnerability Assessment and Penetration Testing) yang dilakukan pada web aplikasi repositori institusi pendidikan . Vulnerability Assessment adalah pemindaian pada web aplikasi untuk mencari celah keamanan yang kemungkinan dapat digunakan oleh penyerang untuk mengakses informasi penting pada web aplikasi. Penetration testing adalah kegiatan simulasi penetrasi atau masuk kedalam sebuah sistem dengan memanfaatkan celah keamanan [4]. Langkah langkah yang dilakukan dalam metode ini adalah sebagai berikut [8]:

1. Scope

Scope adalah tahap untuk menentukan cakupan pada penelitian. Peneliti menentukan cakupan terbatas pada web aplikasi repositori institusi pendidikan . Hasil yang akan dicapai adalah hak akses untuk masuk kedalam web aplikasi repositori.

2. Reconnaisance

Reconnaisance adalah mencari informasi dasar seperti sistem operasi, alamat IP, port dan web server yang digunakan pada web aplikasi repositori. Reconnaisance dilakukan dengan menggunakan tool Nmap Version 7.70 pada sistem operasi kali linux.

3. Vulnerability Detection

Mencari celah keamanan pada web aplikasi repositori menggunakan tool Nessus Version 7.1.2 pada aplikasi peramban google chrome sistem operasi windows.

4. Information Analysis & Planning

Menganalisis informasi tentang temuan celah keamanan yang didapatkan pada tahap vulnerability detection dan menentukan metode atau teknik serangan dengan memanfaatkan celah tersebut. Temuan celah keamanan yang digunakan untuk simulasi penyerangan, antara lain:

a. Web Server Transmit Cleartext Credential

Temuan celah keamanan ini mendeskripsikan bahwa data sesi yang berjalan pada web aplikasi repositori tidak terenkripsi, sehingga data sesi dari dan menuju web server bisa diketahui secara plaintext, termasuk diantaranya adalah username dan password. Tool yang digunakan untuk melakukan simulasi serangan ini adalah arpspoof version 2.4 dan SSLStrip version 0.9 pada sistem operasi kali linux.

b. SYN Scanner

Temuan celah keamanan ini mendeskripsikan port-port yang terbuka pada web aplikasi

repositori. Peneliti memanfaatkan salah satu port yang terbuka, yaitu port 5432 yang digunakan untuk port postgreSQL untuk masuk kedalam database tersebut. Tool yang digunakan untuk melakukan simulasi serangan ini adalah metasploit version 4.17.2-dev.

5. Penetration Testing

Simulasi serangan dilakukan pada web aplikasi repositori dengan menggunakan tools yang sudah ditentukan untuk mendapatkan informasi berupa akun yang digunakan pada web aplikasi tersebut.

6. Privilege Escalation

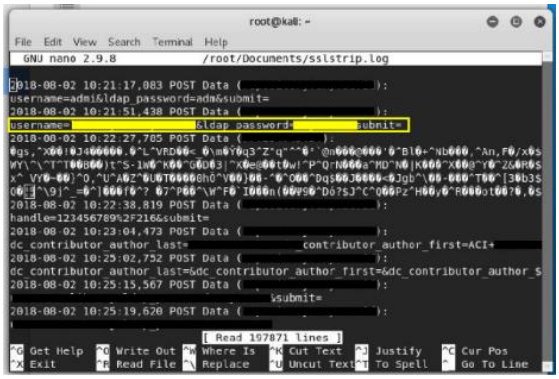
Memanfaatkan hak akses akun yang didapatkan dari langkah simulasi serangan yang dilakukan. Hak akses digunakan untuk mengeksplorasi fitur yang dapat digunakan pada web aplikasi tersebut

7. Report

Kegiatan security assessment yang dilakukan *ini* akan ditulis dalam bentuk laporan dan dilaporkan kepada pihak institusi pendidikan .

DISKUSI DAN HASIL

Security Assessment yang dilakukan pada web aplikasi repositori milik institusi pendidikan menggunakan metode VAPT. Penentuan web aplikasi repositori ini berdasarkan pada penelitian sebelumnya yang membahas tentang pembuatan daftar aset kritis milik institusi pendidikan . Repositori menempati urutan kedua dengan tingkat kerentanan High, dikarenakan web aplikasi tersebut menyimpan informasi sangat penting dan web aplikasi tersebut dilaporkan sering terjadi percobaan serangan [9]. Setelah menentukan cakupan penelitian, selanjutnya adalah mencari celah keamanan pada web aplikasi tersebut. Temuan celah berjudul Web Server Transmit Cleartext Credential didapatkan pada tahap vulnerability assessment menggunakan tool nessus. Celah keamanan ini ada karena web aplikasi tidak dikonfigurasi menggunakan protokol HTTPS. Protokol HTTPS mengenkripsi data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan dari serangan man in the middle attacks [10]. Protokol yang digunakan pada web aplikasi ini adalah protokol HTTP, protokol tersebut tidak mengenkripsi perjalanan data sesi sehingga web aplikasi ini masih bisa diserang dengan menggunakan teknik penyerangan man in the middle. Kegiatan ini berhasil mencatat akun sebagai admin pada web aplikasi tersebut. Hasil dari kegiatan tersebut dijelaskan pada **Gambar 1**.



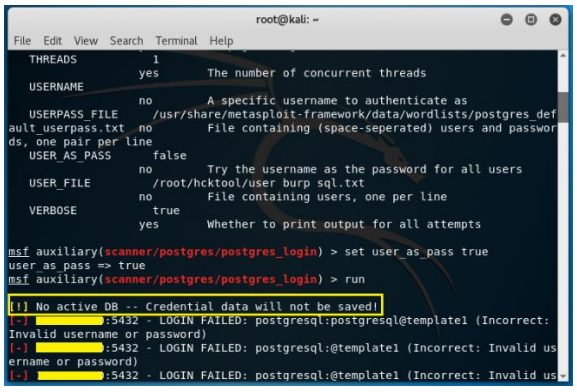
Gambar 1 Percobaan Penetrasi yang Berhasil

Kegiatan simulasi serangan ini menggunakan dua tool, yaitu arpspoof dan sslstrip. Arpspoof digunakan untuk membaca data sesi pada dua host pada saat yang bersamaan [11], kemudian peneliti dapat membaca lalu lintas antara dua host tersebut yang terhubung pada satu jaringan area lokal menggunakan tool SSLStrip.

Pada log SSLStrip diketahui terdapat username dan password yang bersumber dari salah satu end device menuju gateway pada jaringan area lokal di lokasi penelitian. Simulasi serangan ini berhasil mendapatkan akun yang digunakan pada web aplikasi repositori institusi pendidikan . Peneliti melakukan verifikasi dengan cara masuk kedalam web aplikasi repositori menggunakan username dan password yang telah didapatkan.

Simulasi serangan selanjutnya dilakukan dengan memanfaatkan celah keamanan berjudul SYN Scanner. Informasi yang didapatkan dari celah tersebut adalah ada port yang digunakan untuk postgreSQL, yaitu port 5432. Simulasi serangan ini menggunakan tool metasploit dengan teknik penyerangan brute force. Brute Force adalah teknik penyerangan untuk menemukan username dan password yang berjalan secara otomatis untuk

menemukan kombinasi username dan password yang tepat [12]. Kegiatan tersebut dijelaskan pada **Gambar 2**.



Gambar 2 Percobaan Penetrasi yang Gagal

Pada saat melakukan simulasi serangan, terdapat pesan error yang ditampilkan **[!] No active DB–Credential data will not be saved!**. Kegagalan ini terjadi karena seluruh request yang ditujukan kepada web server, terlebih dahulu melewati firewall. Firewall memiliki fungsi untuk melindungi data dan resource dari kerusakan akibat dari penyusup yang masuk kedalam jaringan komputer [13]. Simulasi serangan ini tidak berhasil masuk kedalam database pada web aplikasi repositori institusi pendidikan .

Peneliti melakukan satu kegiatan lain terkait simulasi serangan, yaitu melakukan social engineering. Social Engineering bisa diartikan sebagai penggunaan trik psikologis dari peretas, untuk memperoleh informasi yang dibutuhkannya untuk mendapatkan akses ke sistem atau bisa dikatakan juga sebagai cara untuk mendapatkan informasi yang dibutuhkan (misalnya, kata sandi) dari seseorang, bukan dengan cara membobol sistem [14]. Social engineering dilakukan dengan wawancara yang difokuskan untuk mengulik informasi tentang siapa saja yang mempunyai hak akses pada web aplikasi tersebut. Social engineering dilakukan kepada staf yang ada di lokasi penelitian. Hasil dari social Engineering ini peneliti mengetahui bahwa akun yang didapatkan adalah satu-satunya akun admin yang digunakan untuk manajemen file pada web aplikasi tersebut. Akun tersebut digunakan oleh lebih daru satu orang staf pada lokasi penelitian. Hal tersebut bisa menjadi masalah ketika terdapat kesalahan manajemen file, karena sulit untuk mengetahui staf yang melakukan kesalahan, karena semua staf menggunakan akun yang sama untuk melakukan manajemen file.

KESIMPULAN

Penggunaan web aplikasi untuk mengelola dan mempublikasikan jurnal dan penelitian dari dosen dan mahasiswa adalah menjadi sebuah kebutuhan. Pengelolaan informasi dilakukan oleh beberapa staf yang ada pada satu ruangan. Seluruh staf tersebut menggunakan akun yang sama untuk menginput data ke web aplikasi. Hal ini akan menyulitkan jika terjadi kesalahan input data, karena akan sulit untuk menelusuri staf mana yang melakukan kesalahan. Penulisan laporan hasil penelitian berdasarkan kegiatan security assessment menggunakan metode VAPT (Vulnerability Assessment and Penetration Testing).

REFERENSI

[1] E. Indrayani, “Pengelolaan Sistem Informasi Berbasis Teknologi Informasi dan Komunikasi(TIK),” vol. 12, no. 1, pp. 45–60, 2011.

[2] A. Abdel-Aziz, “Scoping Security Assessments - A Project Management Approach,” *Security*, 2011.

[3] D. Dalalana Bertoglio and A. F. Zorzo, “Overview and open issues on penetration test,” *J. Brazilian Comput. Soc.*, vol. 23, no. 1, pp. 1–16, 2017.

[4] J. N. Goel and B. M. Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,” *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015.

[5] P. S. Shinde and S. B. Ardhapurkar, “Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing,” *IEEE Spons. World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave)*, pp. 1–5, 2016.

[6] H. Kumar, *Learning Nessus for*

Penetration Testing. 2014.

[7] I. Mukhopadhyay, S. Goswami, and E. Mandal, "Web Penetration Testing using Nessus and Metasploit Tool," *IOSR J. Comput. Eng.*, vol. 16, no. 3, pp. 126–129, 2014.

[8] B. C. Hidayanto, "Evaluasi Keamanan Aplikasi Sistem Informasi Menggunakan Framework VAPT (Studi Kasus : SISTER Universitas Jember)," 2017.

[9] A. M. A. Yuhaz, "Risk Management Aset Teknologi Informasi Menggunakan Framework OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) dan FMEA (Failure Mode and Effect Analysis) di Institusi Pendidikan ," Universitas Muhammadiyah Yogyakarta, 2018.

[10] M. Oni, "Analisis Penggunaan Kriptografi dalam Online Banking," *Anal. Pengguna. Kriptografi dalam Online Bank.*, no. 13508031, pp. 1–8, 2011.

[11] S. Puangpronpitag and N. Masusai, "An efficient and feasible solution to ARP Spoof problem," *2009 6th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, vol. 02, pp. 910–913, 2009.

[12] A. Karawash, S. Ontario, S. Computing, I. Platform, I. C. View, and A. Karawash, "Brute Force Attack," no. November 2015, 2016.

[13] S. Land and M. Breininger, "United States Patent," vol. 1, no. 16, 2002.

[14] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics | Symantec Connect," *Soc. Eng. Fundam.*, vol. 1527, 2001.