ISBN: 978–623–91277–6–3

ANALISA KEAMANANAN SERVER IOT

Ahmad Turmudi Zy*, Adi Rusdi Widya, dan Taryana
Fakultas Teknik, Universitas Pelita Bangsa, Kabupaten Bekasi
*E-mail: turmudi@pelitabangsa.ac.id

Abstract

IoT or the Internet of Things is the most dominant thing in the industry 4.0 and is a research that is currently being researcher, its development is very fast so that the security issues of IoT also becomes very interesting. IoT involves servers and sensors as well as local and internet networks. As we know that every system and network must have security holes that must be considered, server security has a big effect on the accuracy of data received from sensors. The server has a big contribution in providing and managing the data received, here it will be checked periodically for its system vulnerabilities then made a cron jobs on the server to determine the order of IoT server security.

Keywords: Internet of Things, Server, Sensor, Cron Jobs.

Abstrak

IOT atau Internet of Things adalah hal yang paling dominan di industri 4.0 dan merupakan penelitian yang sedang ramai diteliti, perkembangannya sangat cepat sehingga masalah keamanan dari Iot ini pun menjadi sangat menarik. IoT melibatkan server dan sensor serta jaringan baik lokal maupun internet. Seperti kita ketahui bahwa setiap system dan jaringan pasti ada celah keamanan yang harus diperhatikan, keamanan server berpengaruh besar terhadap akurasi data yang diterima dari sensor. Server punya andil besar dalam menyediakan dan mengelola data yang diterimanya, di sini akan dicek berkala untuk kerentanan sistemnya kemudian dibuatkan *cron jobs* pada server untuk menentukan urutan pekerjaan pengamanan server IoT tersebut.

Kata kunci: *Internet of Things, Servers, Sensors, Cron Jobs.*

1. PENDAHULUAN

Industri 4.0 sedang berjalan sekarang dimana penggunanan teknologi sensor sangat besar digunakan perannya dalam membantu kegiatan manusia baik personal ataupun organisasi. Beberapa perusahaan di Indonesia sudah banyak yang menggunakan teknologi ini untuk membantu operasional perusahaannya, salah satunya adalah penggunaan Monitoring Mesin, dimana setiap mesin industrinya ditanam wemos mini D1 sebagai sensor untuk mengetahui keadaan mesin (*on, off, error*).

Sensor tersebut mengirim data ke server melalui jaringan Nirkabel, kemudian di server data tersebut dikelola dan disimpan, sedangkan untuk monitoringnya bisa diakses melalui laptop, PC, HP ataupun Gadget lainnya. Hanya saja masalah yang timbul adalah bagaimana keamanan pada server

ISBN: 978–623–91277–6–3

yang merupakan tempat transaksi data tersebut.

Berdasarkan Isu keamanan *Internet of Things* (IoT) maka, Kebutuhan keamanan IoT sangat di butuhkan. Dan IoT tidak akan pernah bisa digunakan lebih jauh jika keamanannya masih belum meyakinkan (M. A. dan S. T., 2015). IoT telah banyak diteliti oleh beberapa peneliti, salah satu hasilnya dapat dilihat di Tabel 1.

Tabel 1. Daftar *IoT Layers* dan Spesifikasinya

HOT Layer	Components	Working of Layer	Security Issues	Security Parameter	Countermeasures
Perception layer	Smart Card, RFID tag, Sensors	Collection of information	Terminal Security issue Sensor network security issue	Authentication Confidentially	Certification and access control Authentication Mechanism
Network layer	Wireless or wired nework computer, components	Transmission of information	Information transmission security	Integrity Availability Confidentially	Hop by Hop Data Encryption
Application layer	Intelligent devices	Analysis of information, Control decision making	Information processing safety of IoT	Privacy	End to end encryption

Pada Tabel 1 disebutkan salah satunya adalah *Network Layer* yang *issue* keamanannya adalah pada sisi transmisi data, yang dimana terlibat langsung adalah jaringan dan server, maka sangat penting untuk memperhatikan lebih mendalam mengenai keamanan IoT. Secara kontruksi masa depannya adalah bahwa perangkat–perangkat IoT akan saling terhubung dari berbagai tempat dengan menggunakan jaringan umum, sehingga banyak informasi yang lalu lalang di jaringan umum, sehingga besar kemungkinan juga bagi orang umum untuk menguping atau mengintip informasi apa yang sedang lalu lalang (Gou et al, 2013).

1.1 Server

Server yang digunakan pada sistem monitoring mesin ini adalah server berbasis *open source* yaitu Ubuntu 18.04 (Gambar 1). Ubuntu 18.04 merupakan versi terbaru untuk versi Lts. Disamping ringan, server ini mudah *update* dan dikenal luas oleh para pengguna *open source*.

Gambar 1. Ubuntu Server 18.04

1.2 *Vulnerability*

Vulnerabilty adalah kerentanan pada suatu sistem, dimana keberadaannya adalah hal yang paling diburu oleh para pencari celah keamanan yang tujuannya adalah bisa positif ataupun negatif. Dalam penelitian ini akan digunakan 2 (dua) *tools* yang sudah dikenal umum di dunia IT, yaitu Nessus dan Acunetix.

1.3 NESSUS

Nessus (Gambar 2) adalah organisasi yang telah di percaya oleh 27.000 lebih organisasi sedunia yang menggunakan

ISBN: 978–623–91277–6–3

teknologi keamanan, serta merupakan standard untuk penilaian kerentanan.

Gambar 2. Logo Nessus

Nessus dapat digunakan untuk melakukan audit sebagai berikut:

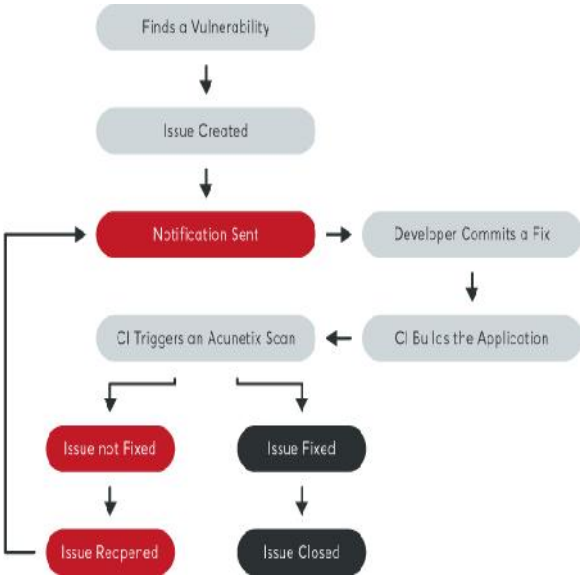
1. Pemindaian *port* yang kredensial dan tidak kredensial.
2. Pemindaian kerentanan berbasis jaringan.
3. Audit *patch* berbasis kredensial untuk Windows dan sebagian besar *platform* UNIX.
4. Audit konfigurasi *redential* dari sebagian besar *platform* Windows dan UNIX.
5. Pengujian keamanan yang kredensial dan komprehensif atas aplikasi pihak ke-3.
6. Pengujian kerentanan aplikasi web khusus dan tertanam.
7. Audit konfigurasi *database* SQL.
8. Pencacahan perangkat lunak pada Unix dan Windows.
9. Menguji penginstalan anti-virus untuk tanda tangan kedaluwarsa dan kesalahan konfigurasi.

1.4 ACUNETIX

Acunetix (Gambar 3) adalah *tools* untuk *scan* keamanan *website*, yang fokus utamanya adalah mencari dan mendeteksi celah kerentanan kemanan pada *website*.

Gambar 3. Logo Acunetix

Bagan alur kerja Acunetix (Gambar 4) adalah sebagai berikut:



Gambar 4. Alur Kerja Scan Website dengan Acunetix

Keuntungan menggunakan Teknologi AcuSensor dari Acunetix:

1. Memungkinkan *user* menemukan dan memperbaiki kerentanan lebih cepat karena kemampuan untuk memberikan lebih banyak informasi tentang kerentanan, seperti nomor baris kode sumber, jejak tumpukan, kueri SQL yang terpengaruh, dll.
2. Secara signifikan mengurangi kesalahan positif ketika memindai situs web karena mampu memahami perilaku aplikasi web dengan lebih baik.
3. Memberitahu *user* tentang masalah konfigurasi aplikasi web yang dapat mengakibatkan kesalahan konfigurasi keamanan, atau mengekspos informasi sensitif. Misalnya. Jika ‘kesalahan khusus’ diaktifkan di .NET, ini dapat memaparkan detail aplikasi sensitif ke pengguna jahat.
4. Memberi tahu *user* cara mengamankan pengaturan server web *user* dengan lebih

ISBN: 978–623–91277–6–3

baik, misal jika akses tulis diaktifkan di server web.

5. Mendeteksi lebih banyak kerentanan injeksi SQL. Sebelumnya kerentanan injeksi SQL hanya dapat ditemukan jika kesalahan *database* dilaporkan, sedangkan sekarang kode sumber dapat dianalisis untuk deteksi yang lebih baik.
6. Kemampuan untuk mendeteksi kerentanan injeksi SQL di semua pernyataan SQL, termasuk dalam pernyataan SQL INSERT. Menggunakan pemindai *BlackBox*, kerentanan injeksi SQL seperti itu tidak dapat ditemukan. Ini secara signifikan meningkatkan kemampuan Acunetix untuk menemukan kerentanan.
7. Pemindaian dijalankan menggunakan AcuSensor, menjalankan *crawling Back-end*, menampilkan semua file yang dapat diakses melalui server web ke pemindai; bahkan jika file-file ini tidak ditautkan melalui aplikasi *front-end*. Ini memastikan cakupan aplikasi 100%, dan memberi tahu pengguna file *backdoor* apa pun yang mungkin diunggah dengan jahat oleh penyerang.
8. Teknologi AcuSensor mampu mencegat semua *input* aplikasi web dan membangun daftar komprehensif dengan semua *input* yang mungkin ada di situs web dan mengujinya.
9. Kemampuan untuk menguji kerentanan pembuatan file dan penghapusan yang sewenang-wenang. Misalnya, melalui skrip yang rentan, pengguna yang jahat dapat membuat file di direktori aplikasi web dan menjalankannya untuk memiliki akses istimewa, atau menghapus file aplikasi web yang sensitif.

Penelitian yang dilakukan oleh Li et al, 2011 mengenai keamanan IoT, diperlukan modul pengguna terpercaya, modul-modul persepsi terpercaya, modul terminal terpercaya serta modul jaringan terpercaya. Namun keterbukaan dan pengembangan IoT yang belum matang, cara mengatasi masalah keamanan IoT perlu dipelajari lebih lanjut.

Penelitian yang dilakukan oleh Suo dkk, 2012 tentang keamanan IoT. Perlu diterapkan TLS/SSL atau IPSec untuk mengamankan jaringan. Hanya saja biasanya alat–alat IoT kurang di kekuatan pemrosesan, sehingga perlu dicarikan solusi lain untuk mengamankan jaringan IoT.

Penelitian yang dilakukan oleh (Zhao dan Ge, 2013) mengenai keamanan IoT. Pengembangna keamanan IoT adalah bagian penting dari IoT. Ia adalah sistem besar yang terintegrasi dari berbagai lapisan sehingga ada banyak masalah keamanan di setiap lapisannya, sehingga memerlukan perlindungan keamanan di setiap lapisannya. Arsitektur keamanan IoT masih dalam tahap eksplorasi sehingga menghadapi tantangan keamanan yang lebih parah dari yang diperkirakan.

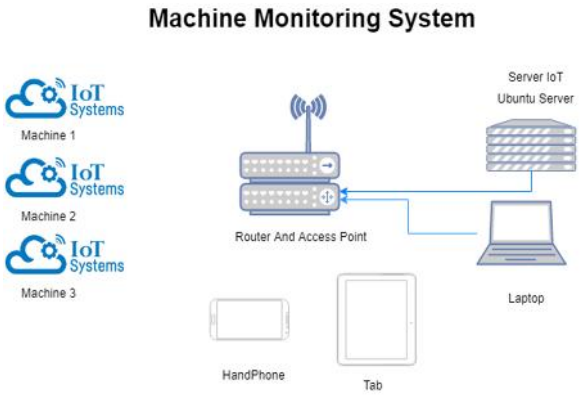
2. METODE PENELITIAN

Pelaksanaan penelitian ini dimulai dengan mengunjungi langsung ke perusahaan yang telah menggunakan sistem monitoring mesin ini (Gambar 5), membuat gambaran topologi sistem IoT yang digunakan di perusahaan tersebut.

Gambar 5. Kunjungan Keperusahaan Pengguna Sistem Monitoring Mesin.

ISBN: 978–623–91277–6–3

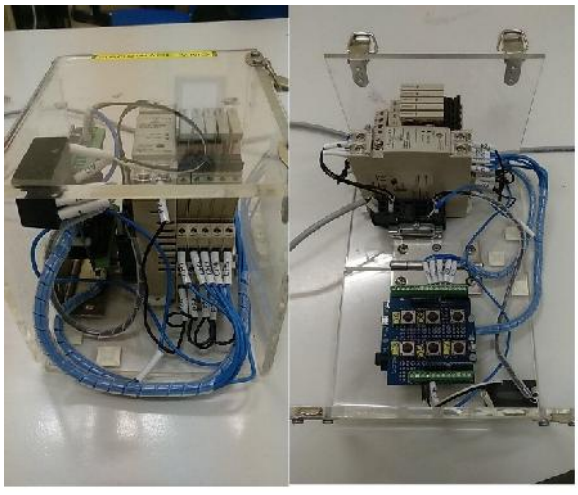
Terdapat beberapa kendala dalam penggunaan IoT diperusahaan tersebut, mulai dari jaringannya sampai server serta hasil yang tidak akurat. Dalam penelitian ini difokus pada kerentanan servernya serta sistem yang dibuat. Gambar 6 adalah gambaran Topologi Sistem Monitoring Mesin yang ada di perusahaan tersebut.



Gambar 6. Topologi Sistem Monitoring Mesin.

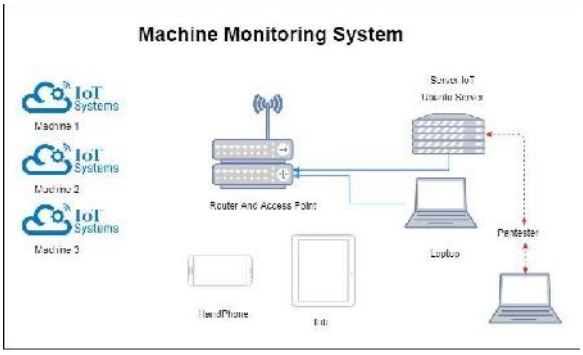
3. HASIL DAN DISKUSI

Pengujian keamanan IoT disini dilakukan pada Server Ubuntu dimana sistem dari Sistem Monitoring Mesin dijalankan. Pembuatan mesin simulasi (Gambar 7) juga telah dilakukan untuk menjalankan Panel Mesinnya, serta server yang telah di install program yang 100% sama dengan yang dijalankan di server produksinya.



Gambar 7. MMCS Simulator

Berikut gambaran topologi *testing server* (Gambar 8) yang dilakukan:



Gambar 8. Topologi Testing Keamanan Server IoT MMCS Simulator.

Berikut beberapa Hasil Scan dengan Nessus dan Acunetix:

ACTIVITY: Vulnerability Assessment
RISK RATING: MEDIUM
ISSUE NAME: Apache Vulnerabilities
ISSUE DESCRIPTION: "An out-of-bounds write flaw exists within the derive_codepage_from_lang() function of the modules/aaa/mod_authnz_ldap.c script due to improper handling of 'Accept-Language' header values that are less than two-bytes. A remote attacker, with a specially crafted request, could potentially crash the process.
(CVE-2017-15710)"
ISSUE MITIGATION: Upgrade to Latest Apache version.

ACTIVITY: Web Pentest
RISK RATING: HIGH
ISSUE NAME: SQL Injection
ISSUE DESCRIPTION: A SQL injection (SQLi) vulnerability exists in phpMyAdmin due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data (CVE-2019-6798).
ISSUE MITIGATION: Upgrade to phpMyAdmin version 4.8.5 or later. Alternatively, apply the patches referenced in the vendor advisories.

ISBN: 978–623–91277–6–3

ACTIVITY: Web Pentest
RISK RATING: HIGH
ISSUE NAME: SQL Injection
ISSUE DESCRIPTION: According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.
ISSUE MITIGATION: Upgrade to phpMyAdmin version 4.8.5 or later. Alternatively, apply the patches referenced in the vendor advisories.

Ditemukan 11 celah keamanan pada server dengan tingkat *Risk rating*: *Medium* (9) dan *High* (2).

4. KESIMPULAN

Setelah dilakukan *scan* dengan *tool*s Nessus dan Acunetix ditemukan banyak sekali CVE sehingga kerentanan pada server IoT sangat banyak celahnya.

Saran

Menindaklanjuti dari kesimpulan di atas penting sekali untuk memperhatikan keamanan server IoT sebelum hal tersebut diimplementasikan, hal pertama yang perlu kita lakukan adalah melakukan *Pentesting* berkala untuk mengetahui celah kemanan pada server yang digunakan, kemudian memperbaiki dari temuan-temuan hasil scan *tools* tersebut. Melakukan penjadwalan untuk *Patch Update* dan *Upgrade* pada server dengan *Cron Job*. Memperbaiki *bug* pada sistem yang dibangun untuk IoT.

Penghargaan/Ucapan Terima Kasih

Terima kasih pada rekan-rekan semua yang telah terlibat dalam penelitian ini sehingga analisa keamanan IoT bisa terwujud dengan baik, dimulai dari pembuatan alat simulatornya oleh Mas Hendra, Pak Yanuar, dan Mas Nunut. Pentest oleh Bang Arjan, dan dari Pihak Perusahaan Pak Didin, yang telah bersedia untuk dianalisa sistem Monitoring Mesinnnya.

DAFTAR PUSTAKA

H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.

K. Zhao and L. Ge, “A survey on the internet of things security,” *Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013*, pp. 663–667, 2013.

M. A. and S. T., “Internet of Things: Architecture, Security Issues and Countermeasures,” *Int. J. Comput. Appl.*, vol. 125, no. 14, pp. 1–4, 2015.

Q. Gou, L. Yan, Y. Liu, and Y. Li, “Construction and strategies in IoT security system,” *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom 2013*, pp. 1129–1132, 2013.

X. Li, Z. Xuan, and L. Wen, “Research on the architecture of trusted security system based on the internet of things,” *Proc. - 4th Int. Conf. Intell. Comput. Technol. Autom. ICICTA 2011*, vol. 2, pp. 1172–1175, 2011.