ARTIKEL

SISTEM KEAMANAN JARINGAN MENDETEKSI *BACKDOOR* UNTUK MENEMUKAN CELAH DAN *EXPLOITS* PADA *WEB SERVER* MENGGUNAKAN TEKNIK IDS *(INTRUSION DETECTION SYSTEM)*

NETWORK SECURITY SYSTEM DETECT BACKDOOR TO FIND SECURITY HOLE AND EXPLOITS ON WEB SERVER USING IDS TECHNIQUE (INTRUSION DETECTION SYSTEM)

Oleh:

ALI MAHMUDI

13.1.03.02.0003

Dibimbing oleh :

1. **Fatkur Rhohman, M.Pd**
2. **Danar Putra Pamungkas, M.Kom**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2017

Skripsi Oleh :

ALI MAHMUDI

NPM : 13.1.03.02.0003

Judul :

SISTEM KEAMANAN JARINGAN MENDETEKSI *BACKDOOR* UNTUK MENEMUKAN CELAH DAN *EXPLOITS* PADA *WEB SERVER* MENGGUNAKAN TEKNIK IDS *(INTRUSION DETECTION SYSTEM)*

Telah disetujui untuk diajukan kepada
Panitia Ujian/Sidang Program Studi Teknik Informatika
FT UN PGRI Kediri

Tanggal : 12 Juni 2017

Pembimbing I	Pembimbing II
Fatkur Rhohman, M.Pd	**Danar Putra Pamungkas, M.Kom**
NIDN. 0728088503	NIDN. 0708028704

Skripsi Oleh :

ALI MAHMUDI

NPM : 13.1.03.02.0003

Judul :

SISTEM KEAMANAN JARINGAN MENDETEKSI *BACKDOOR* UNTUK MENEMUKAN CELAH DAN *EXPLOITS* PADA *WEB SERVER* MENGGUNAKAN TEKNIK IDS *(INTRUSION DETECTION SYSTEM)*

Telah dipertahankan di depan Panitia Ujian/ Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik
Universitas Nusantara PGRI Kediri
Pada Tanggal : 03 Agustus 2017

Dan Dinyatakan Telah Memenuhi Syarat

Panitia Penguji :

1. Ketua Penguji : Fatkur Rhohman, M.Pd.
2. Penguji I : Hermin Istiasih, M.T., M.M.
3. Penguji II : Danar Putra Pamungkas, M.Kom.

Mengetahui,
Dekan Fakultas Teknik

DR. SURYO WIDODO, M.Pd
NIP. 19640202 199103 1 002

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2017

Yang bertanda tangan di bawah ini:

Nama Lengkap	: Ali Mahmudi
NPM	: 13.1.03.02.0003
Telepun/HP	: 082332631121
Alamat Surel (Email)	: amc-dev@hotmail.com
Judul Artikel	: Sistem Keamanan Jaringan Mendeteksi *Backdoor* Untuk Menemukan Celah Dan *Exploits* Pada *Web Server* Menggunakan Teknik Ids *(Intrusion Detection System)*
Fakultas – Program Studi	: Teknik/Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jl. KH. Ahmad Dahlan No. 76 Mojoroto - Kediri

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 8 Agustus 2017
Pembimbing I	Pembimbing II	Penulis,
Fatkur Rhohman, M.Pd NIDN. 0728088503	**Danar Putra Pamungkas, M.Kom** NIDN. 0708028704	**Ali Mahmudi** NPM. 13.1.03.02.0003

SISTEM KEAMANAN JARINGAN MENDETEKSI *BACKDOOR* UNTUK MENEMUKAN CELAH DAN *EXPLOITS* PADA *WEB SERVER* MENGGUNAKAN TEKNIK IDS *(INTRUSION DETECTION SYSTEM)*

Ali Mahmudi
13.1.03.02.0003
Teknik – Teknik Informatika
amc-dev@hotmail.com
Fatkur Rhohman, M.Pd dan Danar Putra Pamungkas, M.Kom
UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Kurangnya pengetahuan mengenai *security* atau kurangnya tenaga pengelola dalam manajemen, sehingga menguntungkan bagi seorang *attacker* untuk mudah masuk kedalam *web server*. Berbagai macam teknik yang digunakan seorang *attacker* untuk bisa masuk ke dalam sebuah *web server* salah satunya dengan melakukan sebuah exploitasi dan kemudian memasang *backdoor* berupa *shell* (Terminal yang berisi perintah *bash*) melalui *bug* sebuah *website*.

Permasalahan yang dihadapi *webmaster* atau pemilik/pengelola *website* adalah (1) Sulitnya mengidentifikasi file *backdoor*. (2) *Webmaster* melakukan *scanning* terhadap direktori website menggunakan tools Virus Scanner built in dari *Web Hosting*, hasil yang ditemukan adalah hanya mendeteksi adanya sebuah *backdoor*. Selanjutnya, *Webmaster* melakukan *patching* dengan cara melakukan *penetrations testing* pada *website* untuk mengetahui lubang keamanan *(security hole)*, setelah itu menutup lubang tersebut berdasar hasil *penetrations test*..

Teknik yang digunakan dalam penelitian ini adalah teknik IDS (Intrusion Detection System) berbasis *signature* dimana data yang digunakan sebagai *signature* adalah laporan data file *backdoor* hasil deteksi pada *web server*. Sistem akan melakukan pencocokan file yang diindikasi sebagai *backdoor* dengan data *signature*.

Hasil pada sistem yang telah dibuat antara lain: (1) Sistem yang dibuat mengacu pada permasalahan yang ada, dimana sistem mampu melakukan proses deteksi *backdoor* serta menemukan celah dan *exploits* yang semula masih menggunakan cara manual. (2) Teknik IDS dapat diterapkan sebagai deteksi intrusi secara otomatis dengan menggunakan *cronjob*.

KATA KUNCI : Keamanan Jaringan, Teknik IDS, Deteksi *Backdoor*, Celah dan *Exploits*.

I. LATAR BELAKANG

Website (disingkat *web*) atau *World Wide Web* (WWW) adalah sebuah *database* (pangkalan data) dari serangkaian komputer di seluruh dunia. *Website* menjembatani para penggunanya untuk mendapatkan berbagai macam informasi dari mana saja. Dengan adanya *website*, berbagai informasi dalam bentuk tulisan, gambar, suara dan video dapat diakses oleh siapa saja yang memiliki komputer dan akses internet, tanpa terikat oleh tempat dan waktu (Nichols, 1996). Akibatnya kebutuhan akan informasi semakin meningkat, sehingga membuat para *developer website* berlomba-lomba menyajikan berbagai inovasi baik dalam *interface*, fitur maupun integrasi plugin terhadap CMS *(Content Management System)* yang mereka gunakan agar pengguna mudah, nyaman dan sering berkunjung untuk mendapatkan informasi baik layanan maupun dukungan. Hal itu memicu timbulnya suatu kebutuhan *security* untuk sistem komputer.

Telah banyak terdengar kejadian, yang marak dengan julukan *Cyber Crime* (Kejahatan melalui jaringan internet) yaitu menghadapi berbagai serangan Virus, *Worm*, Trojan, DoS, *Web Deface*, Pembajakan Software sampai dengan masalah pencurian kartu kredit. Oleh karena keamanan sistem komputer sangat krusial, suatu usaha pencegahan dan pendeteksian diperlukan. Berbagai macam teknik yang digunakan seorang *attacker* untuk bisa masuk ke dalam sebuah *web server* salah satunya dengan melakukan sebuah exploitasi dan kemudian memasang *backdoor* berupa *shell* (Terminal yang berisi perintah *bash*) melalui *bug* sebuah website. *Shell* tersebut akan di simpan kedalam direktori *website* yang kiranya sulit untuk di jangkau atau di deteksi oleh pemilik *website*, dilain itu juga *attacker* akan membuat sanitasi berupa nama yang sama terhadap file yang familiar dengan sistem, sehingga ketika pemilik *website* melihat disangkanya merupakan sebuah sistem. *Backdoor* (Pintu belakang) merupakan akses khusus yang dibuat oleh *programmer* untuk dapat masuk kedalam sistem tanpa diketahui oleh operator sistem. Kebanyakan dari pemilik *website* mengabaikan *security system website* tersebut karena kurangnya pengetahuan mengenai *security* atau kurangnya tenaga pengelola dalam manajemen, sehingga menguntungkan bagi seorang *attacker* untuk mudah masuk kedalam *web server*. Perlu adanya sistem yang mampu mendeteksi *backdoor* secara rinci, diantaranya mampu mengetahui celah *website*, dan *exploits* yang digunakan *attacker*.

Dengan membuat sistem pendeteksi file *backdoor* pada *web server*, maka pengelola atau pemilik *website* dapat mengetahui terkait adanya sebuah celah pada *website* berupa notifikasi yang berisi

informasi terkait *backdoor* yang terdeteksi. Pemilik atau pengelola *website* dapat melakukan beberapa opsi pilihan seperti menghapus *backdoor* guna mencegah *attacker* (penyerang) atau orang yang tidak berhak tidak dapat mengeksekusi *backdoor* untuk tujuan tertentu, atau *tracing exploits* untuk menemukan celah pada website sehingga pemilik atau pengelola dapat melakukan *patching* untuk menutup celah website.

II. METODE

1. IDS *(Intrusion Detection System)*

a. Pengertian IDS

Intrusion Detection adalah proses *monitoring event* yang terjadi dalam suatu jaringan atau suatu sistem komputer dan menganalisanya untuk mengetahui adanya tanda-tanda insiden yang mungkin terjadi (Jannah, 2013). Tanda ini bisa saja mengindikasikan adanya ancaman atau pelanggaran terhadap kebijakan keaman komputer yang diterapkan. Insiden bisa terjadi oleh beberapa sebab, seperti *malware* (misalnya *worm*, *spyware*), akses yang tidak diijinkan, pengguna legal yang menyalahgunakan hak-hak mereka atau mencoba untuk mendapatkan hak tambahan yang bukan wewenangnya. Sedangkan *Intrusion Detection System* adalah perangkat lunak yang mengotomatisasi proses deteksi intrusi (penyusup). IDS akan memonitor file pada *web server*, ketika terdapat file yang diindikasi file *backdoor* sistem akan memberi peringatan kepada pemilik *website* (Putra, 2016).

b. Tipe dasar IDS

1) *Rule based systems*

Berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalu lintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.

2) *Adaptive systems*

Mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada, tetapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk-bentuk penyusupan yang baru.

Bentuk yang sering digunakan untuk komputer secara umum adalah *rule-based systems*. Pendekatan yang digunakan dalam *rule-based systems* ada 2, yaitu pendekatan pencegahan (*preemtory*) dan pendekatan reaksi (*reactionary*). Perbedaannya hanya masalah waktu saja. Pada pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan maka program akan melakukan tindakan yang perlu. Pada pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket

yang mencurigakan program juga akan melakukan tindakan yang perlu.

c. Jenis-jenis IDS

1) *Network-based Intrusion Detection System* (NIDS)

Network-based Intrusion Detection System adalah jenis IDS yang bertanggung jawab untuk mendeteksi serangan yang berkaitan dengan jaringan. NIDS umumnya terletak didalam segmen jaringan penting dimana *server* berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang mengunakan *switch Ethernet*, meskipun beberapa vendor *switch Ethernet* sekarang telah menerapkan fungsi IDS didalam *switch* buatannya untuk memonitor port atau koneksi.

2) *Host-based Intrusion Detection System* (HIDS)

Aktivitas sebuah *host* jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti firewall, *web server*, atau *server* yang terkoneksi ke *internet.*

d. Implementasi IDS

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling popular adalah dengan mengunakan pendeteksian berbasis *signature* (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaharuan terhadap basis data *signature* IDS yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai *Anomaly-based* IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan statistik untuk membandingkan lalu lintas normal yang biasa terjadi (Putra, 2016). Metode ini menawarkan kelebihan dibandingkan *signature-based* IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat didalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan *false positive*. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang melupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul.

Dalam implementasinya, penulis menerapkan deteksi berbasis *signature* dimana data yang digunakan sebagai *signature* adalah laporan data file *backdoor* hasil deteksi pada *web server*. Sistem akan melakukan pencocokan file yang diindikasi

sebagai *backdoor* dengan data *signature*. Jika kemudian hasil deteksi bernilai positif, maka sistem akan menampilkan laporan serta peringatan kepada pengelola website berupa informasi *backdoor* dan celah yang dimanfaatkan untuk menyisipkan file *backdoor*. Jika hasil deteksi bernilai negatif, maka sistem akan menampilkan pesan bahwa sistem aman.

2. Simulasi Teknik *Intrusion Detection System* (IDS*)*

Dalam teknik IDS *(Intrusion Detection System)* dengan deteksi berbasis *signature* sistem akan melakukan *monitoring* terhadap file dan direktori pada *web hosting* dimana data yang digunakan sebagai *signature* adalah laporan data file *backdoor* hasil deteksi pada *web hosting*. Adapun langkah-langkah dalam penelitian ini adalah sebagai berikut (Abdullah, 2016) :

1. Menentukan data *signature*

Dalam penelitian ini, peneliti menggunakan base64_decode, eval, mysql_query, dan method GET/POST sebagai data *signature*.

2. Menentukan data *exploits*

Peneliti memanfaatkan code injek SQli melalui *Unvalidated input, Buffer of Flow,* dan *Injection Flows* dengan PoC *(Proof of Concept).*

3. Menentukan lubang keamanan *(security hole)*

Terkait lubang keamanan, peneliti menggunakan lubang keamanan berupa SQLi dan file uploads.

4. *Monitoring* sistem

Sistem akan melakukan *monitoring* dan pencocokan terhadap file yang diindikasi sebagai *backdoor* dengan data *signature*.

5. Hasil deteksi

Jika kemudian hasil deteksi bernilai positif, maka sistem akan menampilkan laporan serta peringatan kepada pengelola website berupa informasi *backdoor* dan celah yang dimanfaatkan untuk menyisipkan file *backdoor*. Jika hasil deteksi bernilai negatif, maka sistem akan menampilkan pesan bahwa sistem aman.

III. HASIL DAN KESIMPULAN

Dari hasil analisa pada bab sebelumnya, maka dapat disimpulkan bahwa:

1. Sistem mampu mendeteksi file *backdoor* pada *web server* yaitu dengan menggunakan data *signature* base64_decode dan eval.
2. Sistem mampu menemukan celah dan *exploits* pada *web server* yang berkemungkinan digunakan oleh *attacker* untuk bisa masuk kedalam *website* tanpa sepengetahuan pemilik *website* melalui celah SQL Injection dan File Uploads.
3. Teknik IDS *(Intrusion Detection System)* dapat digunakan untuk membantu proses deteksi file *backdoor* pada *web server*

untuk menemukan celah dan *exploits*. Dengan teknik IDS berbasis *signature*, setiap file yang dideteksi akan dicocokan dengan data *signature*.

IV. DAFTAR PUSTAKA

Abdullah, R. Kurnianto. 2016. *Simulasi Celah Keamanan Aplikasi Web dengan Kerangka Kerja OWASP*. Skripsi Institut Teknologi Sepuluh Nopember.

Jannah, M. 2013. *Implementasi Intrusion System (IDS) Snort Pada Laboratorium Jaringan Komputer.* Skripsi Universitas Gunadarma.

Nichols, S.V. 1996. *Yang Perlu Anda Ketahui tentang World Wide Web*. Andi, Yogyakarta.

Putra, A. Restu Kusuma. 2016. *Deteksi Dan Pencegahan Serangan Shellshock.* Skripsi Universitas Muhammadiyah Surakarta.

Putra, D. Nugeraha. 2016. *Rancang Bangun Sistem Keamanan Jaringan Komputer Berbasis Snort – Intrusion Detection System (IDS) Dan Web Monitoring Pada PT. Bangka Bintang Lestari Pangkalpinang.* Skripsi STMIK ATM LUHUR Pangkalpinang.

Retza, L.F. Giri. 2016. *Security Hardening Dengan Cloud Web Service Untuk Pengamanan Website Berbasis Wordpress.* Skripsi Universitas Dian Nuswantoro.

.