e-ISSN: 2549-7952
p-ISSN: 2580-3336

STUDI ANALISA SERANGAN *SQL INJECTION*

Nursapdahi[1], Arif Senja Fitrani[2], Mochamad Alfan Rosid[3], Sukma Aji[4]
[1,2,3,4] Teknik Informatika, Fakultas Sains Dan Teknologi, Universitas Muhammadiyah Sidoarjo
E-mail: [1]nursapdahi98@umsida.ac.id, [2]asfjim@umsida.ac.id, [3]alfanrosid@umsida.ac.id, [4]sukmaaji@umsida.ac.id

Abstract – *At this time the website has become one of the modern information media that is growing very quickly. In making a website, not only the design and information are important, but the security aspect of the website itself has a very important role in a website. The need for website security arises from the need to protect data. First, from data loss and corruption. Second, there are irresponsible parties who want to access and change data. Other problems include self-data protection, excessive delays when accessing or using data. The method used in this test will use tools in the form of software and certain methods used to test the security of a website. To analyze website security, the software used is Snort IDS (Intrusion Detection System) and Wireshark. SQL Injection is actually not a new thing in the world of hacking as a web hacking technique, SQL Injection can damage the database of a website. The technique used in SQL Injection is to input basic SQL commands such as create, insert, update, drop, alter, union and select along with other commands.*

Keywords *— Security, SQL Injection, Snort, IDS, Wireshark.*

Abstrak – *Pada saat ini website menjadi salah satu media informasi modern yang berkembang dengan sangat cepat. Dalam pembuatan website tidak hanya sisi desain dan informasi yang dipentingkan tetapi aspek keamanan dari website itu sendiri mempunyai peranan yang sangat penting dalam sebuah website. Kebutuhan keamanan website timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak bertanggung jawab yang hendak mengakses dan merubah data. Permasalahan lainnya mencakup perlindungan data diri delay yang berlebihan pada saat mengakses atau menggunakan data. Metode yang digunakan pada pengujian ini akan menggunakan tool berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah website. Untuk melakukan analisa keamanan website, software yang digunakan adalah Snort IDS (Intrusion Detection System) dan wireshark. SQL Injection sebenarnya bukan hal yang baru di dunia hacking sebagai salah satu teknik web hacking, SQL Injection sifatnya yang dapat merusak database dari suatu website. Teknik yang digunakan dalam SQL Injection adalah dengan jalan menginputkan perintah-perintah dasar dalam SQL seperti create, insert, update, drop, alter, union dan select beserta perintah-perintah lainnya.*

Kata Kunci *— Keamanan, SQL Injection, Snort, IDS, Wireshark.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat khususnya teknologi nternet, menyebabkan internet dijadikan sebagai salah satu media pertukaran informasi dan data yang utama. Didalam jaringan internet terdapat dua tindakan yang bertentangan dalam hal mengakses informasi. Tindakan yang pertama yaitu proses pengamanan informasi dan data, sedangkan tindakan yang kedua merupakan tindakan pengeksploitasian dari sistem tersebut.[1]

Dalam era teknologi informasi saat ini, hampir seluruh informasi yang penting pada saat ini bagi seluruh institusi dapat di akses secara luas bagi para penggunanya. Keamanan jaringan komputer sebagai bagian dari sebuah sistem merupakan hal yang sangatlah penting dalam menjaga integritas dan validitas sebuah data serta menjamin ketersediaan bagi penggunanya.[2] Sistem harus benar-benar terjaga dan dilindungi dari segala macam bentuk serangan dan usaha-usaha penyusupan dan pemindaian oleh pihak-pihak yang tidak bertanggung jawab. Salah satu seranganyang sering digunakan oleh hacker atau attacker adalah SQL Injection. SQL Injection adalah suatu command injeksi. Kasus ini merupakan kasus yang harus di perhatikan oleh web desainer agar lebih berhati-hati dalam merancang dan membuat suatu website.[3]

Sistem deteksi jaringan yang ada pada saat ini umumnya mampu mendeteksi segala bentuk serangan tetapi tidak mampu mengambil tindakan yang lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sitemnya, hal tersebut merupakan hal yang sangat

e-ISSN: 2549-7952
p-ISSN: 2580-3336

tidak efektif terutama apabila sistem berada pada kondisi yang benar-benar darurat. Pada umumnya sistem pertahanan terhadap aktivitas gangguan dilakukan manual oleh administrator, hal tersebut mengakibatkan integritas sistem bergantung pada kecepatan dan ketersediaan administrator dalam menanganinya. Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat.[4]

Salah satu cara untuk meningkatkan keamanan didalam jaringan adalah dengan menerapkan ataupun mengimplementasikan snort sebagai intrusion detection system (IDS). Intrusion Detection System (IDS) merupakan perangkat lunak (software) atau suatu sistem perangkat keras(hardware) yang bekerja secara otomatis untuk menghambat semua serangan yang akan menggangu sebuah jaringan. Kemampuan dari IDS memberikan sebuah peringatan kepada administrator server saat terjadinya sebuah aktivitas yang tentunya tidak diinginkan oleh administrator sebagai penanggung jawab sistem. Selain memberikan peringatan, IDS juga mampu melacak sebuah aktivitas yang dapat merugikan sebuah sistem dengan melakukan pengamatan (monitoring) terhadap paket-paket yang berisi aktivitas mencurigakan sekaligus melakukan tindak lanjut pencegahan.[5]

2. METODE PENELITIAN

1. Penelitian ini dilakukan di laboratorium sistem operasi jurusan Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Sidoarjo, Waktu penelitian dilakukan mulai Desember 2020 sampai dengan Februari 2021.

2. Analisis kebutuhan adalah tahap awal yang menjadi dasar dari proses yang dibutuhkan dalam menganalisa serangan SQL Injection. Berikut ini beberapa kebutuhan perangkat dalam pengujian.

a.Sebuah komputer yang berfungsi sebagai server dan snort IDS.
b. Sebuah Personal komputer/Laptop yang berfungsi sebagai penguji.

3. Alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

a. Laptop HP *inter core i5*
b. Laptop Lenovo *intel core i3*
c. *Oracle VM Virtualbox Manager*
d. *wireshark*
e. *Snort*
f. DVWA

2.1 Sub Bab

a. SQL Injection

SQL Ijection merupakan sebuah teknik pengeksploitasian sebuah aplikasi web memakai data yang diberikan atau yang disisipkan dalam query SQL. Cara kerja dari SQL injection adalah dengan cara memasukkan query SQL atau juga perintah (command) sebagai input yang dimungkinkan melalui halaman web atau command prompt. Halaman web akan mengambil dariuser lalu membuat query SQL untuk masuk kedalam database.[6] Dengan demikian, SQL injection dapat juga disebut sebagai kegiatan yang menipu query dari database, sehingga seseorang yang tidak terotentikasi dapat mengetahui dan mendapatkan informasi yang terdapat pada database sistem (Zam, 2012).[7]

b. IDS (*Intrusion Detection System*)

Intrusion Detection System (IDS) dapat di definisikan sebagai tool, metode ataupun juga sumber daya yang dapat memberikan bantuan untuk melakukan proses identifikasi dan memberikan laporan terhadap aktivitas jaringan komputer. Di sisi lain Intrusion Detection System (IDS) merupakan penghambat dari semua serangan yang akan mengganggu sebuah jaringan. Kemampuan kinerja dari IDS memberikan sebuah peringatan kepada administrator server saat terjadinya sebuah aktivitas tertentu yang tentunya aktivitas tersebut tidak diinginkan oleh administrator sebagai penanggung jawab penuh dari sistem tersebut. Selain memberikan peringatan, IDS juga mampu melacak jenis dari aktivitas yang merugikan sebuah sistem. IDS akan melakukan proses pengamatan (monitoring) terhadap paket yang melewati jaringan dan berusaha menemukan apakah terdapat paket-paket yang berisi aktivitas mencurigakan serta jugamelakukan tindak lanjut pencegahannya.[8]

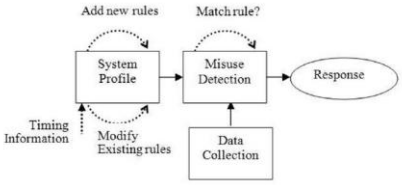
Penyusup (intrusion) didefinisikan sebagai sebuah kegiatan yang bersifat anomaly, incorrectatau inappropriate yang terjadi di jaringan atau host. Pada intrusion detection system, pengenalan terhadap penyusup dibagi menjadi empat bagian, yaitu:

1. *Knowledge based (Misuse Detection)*

Pada bagian ini cara mengenali adanya penyusup yaitu dengan cara menyadap paket data dankemudian membandingkannya dengan database rule (berisikan tentang signature-signatureserangan). Jika paket data yang ditangkap memiliki pola yang sama atau

e-ISSN: 2549-7952
p-ISSN: 2580-3336

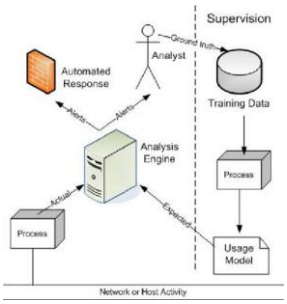
setidaknya ada salah satu polanya yang terdapat di database rule, maka akan dianggap sebagai adanya serangan yang terjadi.[5]



Gambar 1. *Knowledge Based*

2. *Behavior Based (Animali Based)*

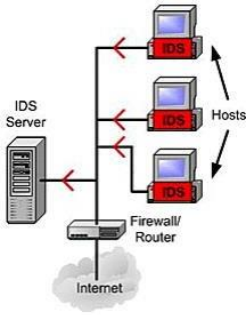
Pada bagian ini cara mengenali adanya penyusup yaitu dengan mengamati adanya kejanggalan-kejanggalan yang terjadi pada sistem, atau adanya penyimpangan-penyimpangan yang terjadi pada kondisi normal. Sebagai contoh adanya penggunaan memori yang melonjak secara terus menerus atau koneksi parallel dari satu port IP dalam jumlah yang banyak dan dalam waktu yang bersamaan.[5]



Gambar 2. *Behavior Based*

3. *Host-Based Intrusion Detection System*

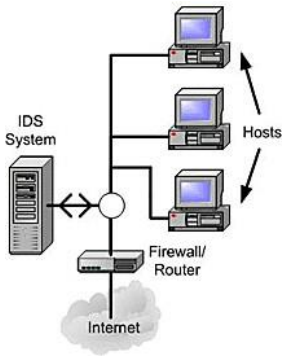
Host based Intrusion detection system juga biasa di sebut dengan HIDS bekerja pada host yang akan dilindungi. Intrusion detection system jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi berbagai macam serangan yang dilakukan pada host tersebut. HIDS dapat melihat kedalam file log ataupun sistem untuk mendeteksi aktifitas intrusi.[9] HIDS ini bersifat reaktif, yang berarti sistem akan memberikan alert pada saat intrusi telah terjadi. Adapaun HIDS yang bersifat proaktif yaitu sistem dapat mengidentifikasi lalu lintas data yang langsung berhubungan dengan host dan langsung memberikan alert kepada pengguna. Penempatan HIDS pada topologi dapat dilihat pada Gambar. 3 Host-based intrusion detection system.[7]



Gambar 3. *Host Based IDS*

4. *Network-based Intrusion Detection System*

Network-based intrusion detection system atau yang biasa disebut juga dengan NIDS biasanyaberupa suatu mesin yang khusus dipergunakan untuk memonitoring seluruh segmen dari jaringan. NIDS akan mengumpulkan paket-paket data yang terdapat pada jaringan dan kemudian menganalisanya serta menentukan apakah paket-paket itu berupa suatu paket yang normal atau suatu serangan atau juga berupa aktivitas yang mencurigakan.[5]



Gambar 4. *Network Based IDS*

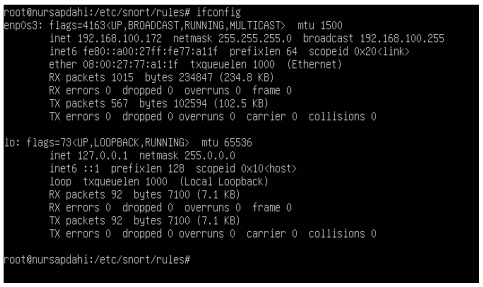
c. SNORT

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisispaket yang melintas pada jaringan secara real time traffic dan logging kedalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort dapat digunakanpada flatform sistem operasi Linux, BSD, Solaris, Windows dan sistem operasi lainnya.[8]

e-ISSN: 2549-7952
p-ISSN: 2580-3336

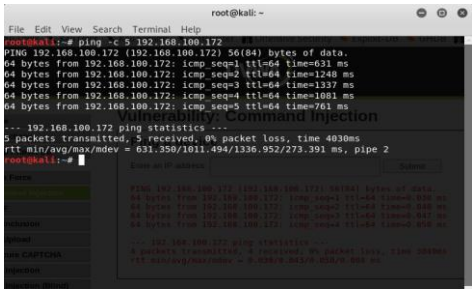
3. HASIL DAN PEMBAHASAN

Sebelum melakukan pengujian, sebaiknya memeriksa *network Interface* dan *IP Address* pada server ID seperti pada gambar dibawah ini:



Gambar 5. *Interface dan IP Address Server*

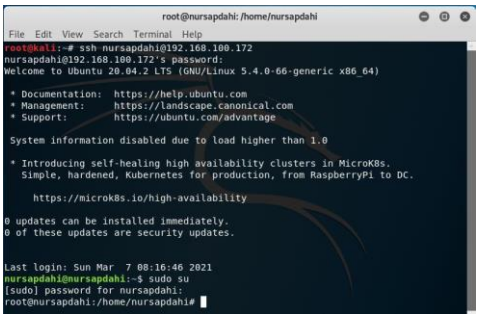
Selanjutnya melakukan tes koneksi jaringan pada kedua computer yang akan di lakukan pengujian. Untuk melakukan pengujian jaringan disetiap computer dapat dilakukan dengan cara *PING* melalui terminal *console* ataupun langsung melalui *web DVWA* ke server yang telah terpasang IDS.



Gambar 6. PING koneksi Terminal *Console*

Gambar 7. PING Koneksi Aplikasi *DVWA*

Setelah server yang telah terpasang IDS terhubung dengan komputer penyerang maka selanjutnya mengecek apakah Snort IDS sudah berjalan dengan baik apakah tidak pada server yang terpasang IDS. Untuk memastikan nya kita harus masuk ke server yang telah terpasang IDS melalui terminal console yang ada di komputer penyerang dengan menggunakan perintah yang ada pada Gambar 8. berikut.



Gambar 8. Login Server Melalui *Device* Penyusup

Setelah berhasil masuk ke server, maka selanjutnya adalah menjalankan snort mode IDS dan juga wireshark untuk mulai melakukan proses monitoring pada jaringan yang masuk menuju server. Setelah memastikan snort IDS telah berjalan dengan baik maka tahap selanjutnya adalah melakukan gangguan dan pengambilan data dari hasil gangguan tersebut, berikut ini adalah hasil dari pengujian yang di lakukan.[10]

Pada pengujian ini dilakukan nya sebuah injeksi query di dalam aplikasi DVWA, tujuan nya adalah untuk melihat isi dari database web DVWA tersebut. Sebelum melakukan injeksi pastikan keamanan dari aplikasi DVWA tersebut berada dalam level low, agar dapat melakukan simulasi serangan dengan mudah seperti pada Gambar 9. di bawah ini.

Gambar 9. *Security Level* Aplikasi *DVWA*

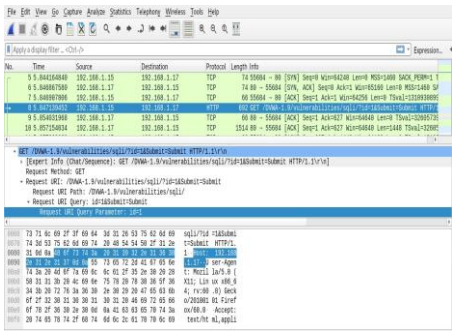
Setelah mengubah security level DVWA menjadi low, maka tahap selanjutnya adalah melakukan injeksi terhadap database dari web DVWA tersebut. Masukan perintah SELECT first_name, last_name FROM users WHERE user_ID = '$id'; dimana '$id' adalah input parameter yang diberikan oleh user, atau mengganti '$id' menjadi '1' atau '2' dan seterusnya. Maka akan muncul pada tampilan DVWA seperti pada Gambar 10. dan Gambar 11. dibawah ini.

e-ISSN: 2549-7952
p-ISSN: 2580-3336

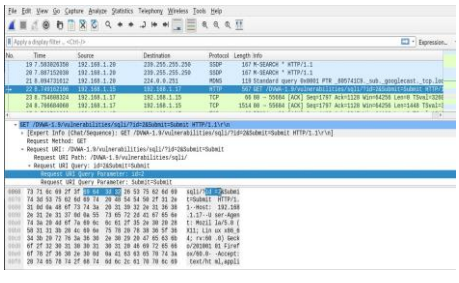
Gambar 10. Input *Query* '1'

Gambar 11. Input *Query* '2'

Setelah memasukkan perintah '1' dan '2' ke aplikasi dvwa maka wireshark menangkap semua lalulintas data yang masuk ketika kita melakukan injeksi tersebut, adapun hasil tangkapan lalulintas yang di tangkap oleh wireshark adalah seperti pada Gambar 12. dan Gambar 13.

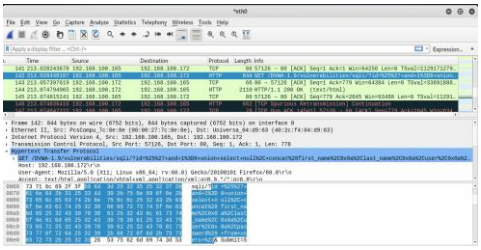


Gambar 12. Lalulintas Data dari *Submit* '1'

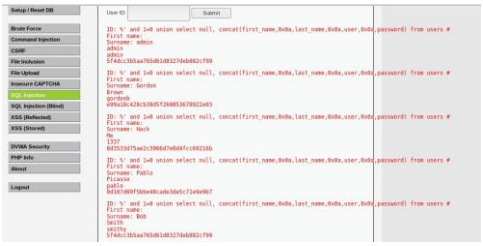


Gambar 13. Lalulintas Data dari *Submit* '2'

Pada tahap selanjutnya adalah melihat password yang digunakan pada setiap user yang ada didatabase website DVWA adalah dengan memasukkan perintah SELECt first_name, last_name FROM users WHERE users_id = '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #,; maka setelah berhasil menginjeksi kan query tersebut akan muncul setiap password dari user yang ada di database DVWA dalam bentuk MD5 yang dapat di crack melalui situs website online atau sebagainya seperti pada gambar 14. hasil dari injeksi query untuk melihat password dan juga hasil lalulintas jaringan pada aplikasi wireshark seperti pada gambar 15.

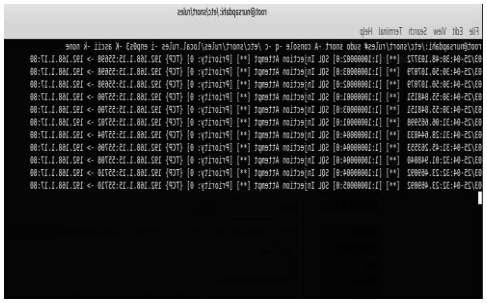


Gambar 14. Hasil Injeksi *Query* Untuk Melihat *Password User*



Gambar 15. Lalulintas Injeksi *Query* Melihat Password User

Pada setiap uji coba injeksi query melalui aplikasi DVWA maka setiap query yang dimasukkan akan dicatat oleh wireshark dan juga diidentifikasi oleh snort sebagai IDS (internet detection system) seperti pada Gambar 16. pada terminal console menunjukkan adanya sebuah upaya serangan melalui SQL Injection.



Gambar 16. Identifikasi Snort Pada Terminal *Console*

4. SIMPULAN

Berdasarkan hasil pembahasan dan juga pengujian yang telah dilakukan terhadap server yang terinstalasi Snort IDS dan juga Wireshark maka dapat diambil kesimpulan sebagai berikut.

a. IDS yang dibangun untuk mendeteksi adanya gangguan dan serangan terhadap jaringan

e-ISSN: 2549-7952
p-ISSN: 2580-3336

dapat dibaca dengan baik oleh snort IDS dan juga Wireshark.

b. Dari hasil pengujian serangan SQL injection terhadap server snort IDS melalui aplikasi DVWA, snort dan juga wireshark dapat mengenali jenis gangguan serangan yang ditimbulkan dan dapat menampilkansecara tepat dan tepat kapan terjadinya serangan dan dari mana serangan itu berasal.

5. SARAN

Saran yang diajukan untuk pengembangan selanjutnya dan melengkapi kekurangan-kekurangan pada penelitian ini adalah sebagai berikut:

a. Adanya penanganan secara langsung terhadap serangan yang dibaca oleh snort IDS dan juga wireshark.
b. Dilalkukannya pengujian serangan dengan jaringan yang berbeda, tidak hanya dengan satu jaringan.

DAFTAR PUSTAKA

[1] Y. W. Pradipta, "IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX," *J. Manaj. Inform.*, vol. Vol. 7 No., 2017.

[2] M. Affandi *et al.*, "Implementasi Snort Sebagai Alat Pendeteksi Intrusi MenggunakanLinux," *J. Teknol. Inf.*, vol. 4, no. 2, 2013, [Online]. Available: www.linux.org.

[3] M. Dahlan, A. Latubessy, M. Nurkamid, and L. Anggraini, "Pengujian Dan Analisa Keamanan Website Terhadap Serangan Sql Injection (Studi Kasus : Website Umk)," *J.Sains dan Teknol.*, vol. 7, no. 1, pp. 13–19, 2014.

[4] C. S. Bayu, "Analisis Penerapan Jaringan Keamanan Menggunakan IDS dan Honeypot,"*Skripsi, Fak. Ilmu Komput.*, pp. 1–23, 2014.

[5] M. Affandi and S. Setyowibowo, "Implementasi Snort Sebagai Alat Pendeteksi Intrusi," *Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux*, vol. 4, no. 2, 2013.

[6] Justin clarke, *SQL Injection Attacks and Defense*. 1967.

[7] A. S. Irawan, E. S. Pramukantoro, and A. Kusyanti, "Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2295–2301, 2018.

[8] D. Ariyus, "Intrusion Detection System: Sistem Pendektesian Penyusup pada Jaringan Komputer," *Language (Baltim).*, vol. 10, no. 294, p. 23Cm, 2007.

[9] Y. W. Pradipta, "IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX Yoga," *J. Manaj.Inform.*, vol. Volume 7 N, pp. 21–28, 2017.

[10] R. Triandini, "Implementasi Intrusion Detection System Menggunakan Snort, Barnyard2 Dan Base Pada Sistem Operasi Linux," *Skripsi*, 2016.