Penerapan Keamanan Jaringan Menggunakan *Honeypot Snare & Tanner* Berbasis *Web* Secara *Low Interaction* Pada Layanan *Web Server*

1st Fakhrul Efendi
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
fakhrulefendi@student.telkomuniversity.ac.id

2nd Devie Ryana Suchendra
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
deviersuchendra@telkomuniversity.ac.id

3rd Setia Juli Irzal Ismail
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
julismail@telkomuniversity.ac.id

Abstrak*—Beberapa waktu lalu sering terjadi peretasan terhadap web oleh hacker, seperti yang terjadi pada Lembaga BPJS pada bulan Mei 2021 yang menyebabkan bocornya data pengguna sebanyak 279 Juta dan diperjual belikan dengan harga 0,15 Bitcoin atau 87,6 Juta Rupiah oleh pihak yang tidak bertanggung jawab pada forum online, oleh karena itu dibuatlah sistem yang dapat menjebak hacker ketika melakukan penyerangan terhadap web. Sistem yang dibuat disini menjebak hacker yang akan melakukan penyerangan terhadap web. Sistem akan mendeteksi penyerangan dan akan mengirimkan pemberitahuan bahwa telah terjadi sebuah serangan kepada web, sistem ini dinamakan dengan Honeypot. Honeypot yang digunakan adalah Snare dan Tanner. Snare melakukan penyalinan web yang diserang oleh hacker, ketika serangan terjadi snare akan mengirimkan informasi kepada tanner untuk disimpan, kemudian tanner akan memberikan informasi kepada administrator web bahwa telah terjadi penyerangan. Sistem dibangun pada sistem operasi ubuntu yang berjalan secara virtual menggunakan VMWare dengan menggunakan metode NDLC dan melakukan pengujian dengan menggunakan teknik penyerangan XSS, Brute Force, dan SQL Injection, dari pengujian tersebut Honeypot dapat melakukan deteksi penyerangan dalam bentuk catatan atau Log yang kemudian disimpan dan dapat ditampilkan pada antarmuka web, serangan XSS dideteksi dengan menggunakan emulator XSS yang disediakan oleh Honeypot begitu juga dengan Brute Force, dan SQL Injection pendeteksian dilakukan dengan menggunakan Emulator Brute Force dan SQLi oleh Honeypot.

Kata Kunci: hacker, honeypot, snare dan tanner, ndlc, teknik penyerangan

I. PENDAHULUAN

Kemajuan teknologi internet membuat pengguna semakin mudah untuk mencari informasi yang diperlukan, seperti adanya web yang mempermudah pengguna dalam melihat informasi yang disediakan. Web atau situs adalah kumpulan halaman yang menampilkan informasi data teks, data gambar diam atau gerak, data animasi, suara, video dan atau gabungan dari semuanya.Baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman[1].

Web dikelola oleh seorang administrator dengan memanfaatkan layanan web server, karena web berisi informasi maka tidak jarang adanya pencurian atau perusakan terhadap konten yang ada dengan memanfaatkan celah pada web tersebut. Sehingga membuat pengguna menjadi terganggu karena adanya tindakan tersebut, Contoh kasus yang pernah terjadi adalah peretasan pada Lembaga BPJS pada bulan Mei 2022 yang menyebabkan kebocoran data pengguna dan dijual belikan oleh pihak yang tidak bertanggung jawab[2]. Untuk itu diperlukan keamanan yang dapat membantu menjaga informasi yang ada didalam web tersebut.

Sistem yang akan digunakan adalah dengan memanfaatkan teknologi Honeypot, Honeypot adalah umpan atau perangkap yang dipasang secara khusus untuk memikat peretas dengan tujuan menangkap atau melacak peretas saat serangan terjadi. Sangat mudah untuk menerapkan Honeypot.

Honeypot dapat mengidentifikasi peretas dengan efisien[3]. Untuk itu dibuat sebuah sistem yang memanfaatkan Honeypot dalam menjaga informasi yang disediakan oleh Web, gambaran dari sistem adalah Honeypot diletakkan antara peretas dan web server asli dimana Honeypot berfungsi sebagai perangkap bagi peretas yang ingin memasuki web server, ketika peretas mencoba memasuki web server maka honeypot akan mengirimkan pemberitahuan kepada administrator bahwa telah terjadi penerobosan sistem.

Honeypot dibangun pada sistem virtual dengan memanfaatkan perangkat lunak VMWare dan menggunakan Snare & Tanner sebagai Honeypot, penggunaan Honeypot secara virtual dinamakan dengan Low Interaction Honeypot. Pengujian dilakukan dengan menggunakan teknik penyerangan XSS, Brute Force, dan Injection, dari pengujian tersebut Honeypot berhasil melakukan deteksi penyerangan.

Berdasarkan latar belakang yang dijelaskan dapat diambil rumusan masalah yaitu Layanan Web rentan terhadap serangan seperti XSS, Brute Force, dan SQLi yang berdampak pada keamanan data yang dapat dicuri dengan memanfaatkan teknik SQLi dan pengrusakan Web dengan XSS.

Berdasarkan rumusan masalah yang dibuat, maka didapat tujuan sebagai

berikut:

A. Membangun sistem keamanan Honeypot Snare & Tanner pada layanan web server,
B. Menguji sistem keamanan Honeypot Snare & Tanner dalam melindungi layanan web server.

II. TINJAUAN PUSTAKA

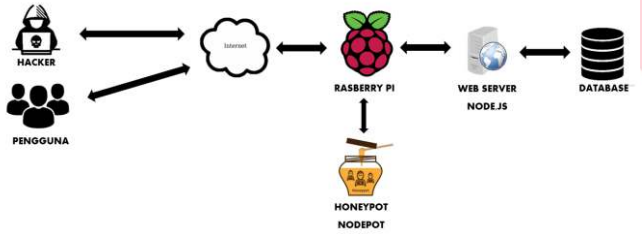
Pada penelitian sebelumnya sistem menggunakan 2 jenis Honeypot yaitu Low Interaction dan High Interaction yang dilakukan oleh LUKITO PRIMA AIDIN. Sistem pada penelitian sebelumnya menggunakan High Interaction yang

di letakkan pada perangkat baru[4]. Penelitian yang dilakukan oleh DANDY KALMA RAHMATULLAH Honeypot dibangun pada Embedded System secara Low Interaction[5].

Penelitian yang dilakukan DENI HERRYANTO Honeypot dibangun pada perangkat IoT menggunakan Elk Stack dan Regular Expression untuk menganalisis Log[6]. Selanjutnya penelitian yang dilakukan oleh DEDY PERMANA Honeypot dibangun sebagai sistem keamanan pada layanan Voip[7].

Penelitian yang dilakukan oleh MUHAMMAD ARIEF Honeypot menggunakan Dionaea pada jaringan Hotspot Fizz[8]. Pada penelitian yang dikerjakan Honeypot tidak dijalankan secara High Interaction dan tidak memasang perangkat Rasberry Pi karena untuk menghemat penggunaan perangkat dan mempermudah dalam pembangunan sistem, dan Honeypot yang digunakan adalah Snare & Tanner pada penelitian sebelumnya Honeypot menggunakan Nodepot.

III. METODEOLOGI



GAMBAR 1
GAMBAR SISTEM SAAT INI

Dari gambar diatas dapat digambarkan sistem saat ini yaitu hacker melakukan penyerangan melalui internet dengan target berada pada perangkat rasberry pi yang sudah terpasang layanan web server dengan database, dan Honeypot Nodepot sebagai pengecoh. Rasberry Pi berfungsi sebagai perangkat server yang sudah terpasang Honeypot Nodepot, dan Webserver dengan database yang terhubung. Honeypot Nodepot berfungsi untuk menangkap serangan pada Web yang berbasis nodejs.

Berdasarkan gambaran sistem saat ini dihasilkan suatu identifikasi untuk membuat sistem Honeypot berbasis web yang memiliki fungsi sebagai detector ketika terjadi sebuah serangan pada web, dan terpasang secara vitual tanpa memanfaatkan perangkat Rasberry Pi tapi menggunakan perangkat lunak VMWare Workstation.

Untuk membangun sistem maka dibutuhkan alat dan bahan yaitu :

A. Perangkat Keras

Perangkat keras yang dibutuhkan pada penelitian ini adalah sebagai berikut:

TABEL 1
PERANGKAT KERAS

Nama	Spesifikasi	Jumlah
Laptop	Intel i7 2,60Ghz Ram 8gb Windows 10 pro-64bit 1,5TB storage 500gb SSD 1TB HDD	1

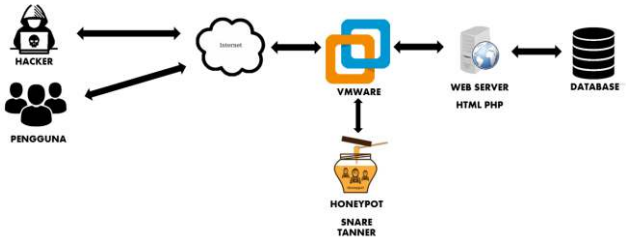
B. Perangkat Lunak

Perangkat lunak yang dibutuhkan pada penelitian ini adalah sebagai berikut:

TABEL 2
PERANGKAT LUNAK

Nama	Spesifikasi
VMWare Work Station Pro	X64-bit 3GHz atau lebih kecepatan core 2GB RAM
Windows 10	1GHz core 1GB Ram 16 GB Storage
Ubuntu 20.04	1GB Storage 512MB Ram PHP ver 7.3 atau lebih 1GHz core
Nama	Spesifikasi
Snare & Tanner	Python3.6
Postgresql	1Ghz kecepatan prosessor 2GB RAM 512MB HDD
Docker	4GB RAM
Nama	Spesifikasi
PHP	512MB RAM 200MB HDD X64/X32-bit processor

Berdasarkan identifikasi pembuatan sistem *H*oneypot dihasilkan suatu rancangan sistem usulan yang dapat dilihat pada gambar 3.2.



GAMBAR 2
PERANCANGAN SISTEM

Dari gambar 2 sistem yang dibuat mengganti perangkat Rasberry pi dengan VMWare, Web Server berbasis html dan php, dan Honeypot snare tanner sebagai detector ketika terjadi penyerangan terhadap web, Rasberry pi diganti dengan VMWare untuk mempermudah pembangunan sistem karena dibangun secara virtual dan mengurangi biaya pembuatan sistem. Ketika hacker melakukan penyerangan ke web server, Honeypot akan mendeteksi kegiatan tersebut kemudian menyimpan dalam bentuk log, dan dapat dibaca oleh admin atau pengelola server. Berdasarkan rancangan sistem usulan didapatkan metode pengerjaan yaitu : metode penelitian NDLC (Network Development Life Cycle), dengan tahapan pengerjaan sebagai berikut.

1. Analisis Kebutuhan

   Menganalisis permasalahan yang terjadi dan menganalisa kebutuhan alat dan bahan yang dibutuhkan.

2. Perancangan

   Merancang sistem web server sebagai uji coba sistem.

3. Pengembangan

Mengembangkan sistem dengan memasang sistem Honeypot sehingga bisa dilakukan pengujian.

4. Pengujian

Menguji sistem dengan melakukan penyerangan berupa SQL Injection, XSS, dan Brute Force terhadap webserver dan Honeypot.

5. Maintenance

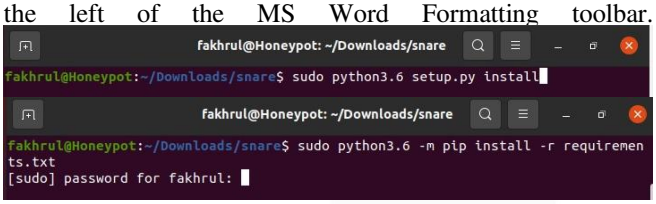
Melakukan pemeliharaan sistem dengan memastikan tidak ada celah yang memungkinkan terjadinya peretasan atau serangan lainnya.

IV. IMPLEMENTASI DAN ANALISIS

Pada bagian ini dilaporkan Langkah pemasangan Honeypot Snare dan Tanner.

A. Proses Pemasangan Honeypot

Bagian ini dijelaskan proses pemasangan Honeypot Snare dan Tanner, Postgresql, PHP dan Docker.After the text edit has been completed, the paper is ready for the template. Duplicate 1the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.



GAMBAR 3
INSTALL PAKET YANG DIBUTUHKAN UNTUK MENJALANKAN SNARE PADA FILE "REQUIREMENT.TXT"

Gambar 3 menunjukkan perintah pemasangan paket yang dibutuhkan oleh snare untuk dapat berjalan pada file "Requirement.txt". file "Requirement.txt" berisi module yang dibutuhkan snare untuk dapat berjalan dengan baik, pada gambar 3 terlihat kode "sudo python3.6" kode ini menunjukkan pemakaian python3.6 sebagai paket utama untuk menjalankan snare dan module pip sebagai sarana pemasangan module lain, perintah berikutnya dengan menggunakan kode "sudo python3.6 setup.py install" yang berfungsi untuk melakukan pemasangan snare dengan menggunakan file "setup.py".

B. Tanner

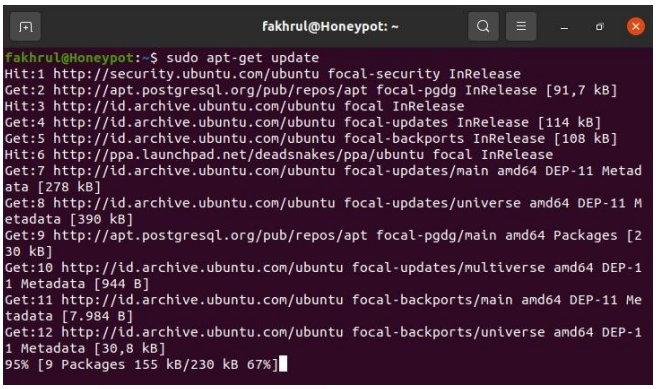
GAMBAR 4
INSTALL PAKET YANG DIBUTUHKAN UNTUK MENJALANKAN TANNER PADA FILE "REQUIREMENT.TXT"

Gambar 4 menunjukkan perintah pemasangan paket yang diperlukan tanner untuk dapat berjalan pada sistem operasi ubuntu. File "Requirement.txt" berisi module yang dibutuhkan tanner untuk dapat berjalan dengan baik, pada gambar 4 terlihat kode "sudo python3.7 -m pip" kode ini menunjukkan pemakaian python3.7 sebagai paket utama untuk menjalankan tanner dan module pip sebagai sarana pemasangan module lain, selanjutnya dilakukan pemasangan tanner dengan menggunakan kode "sudo python3.7 setup.py install".

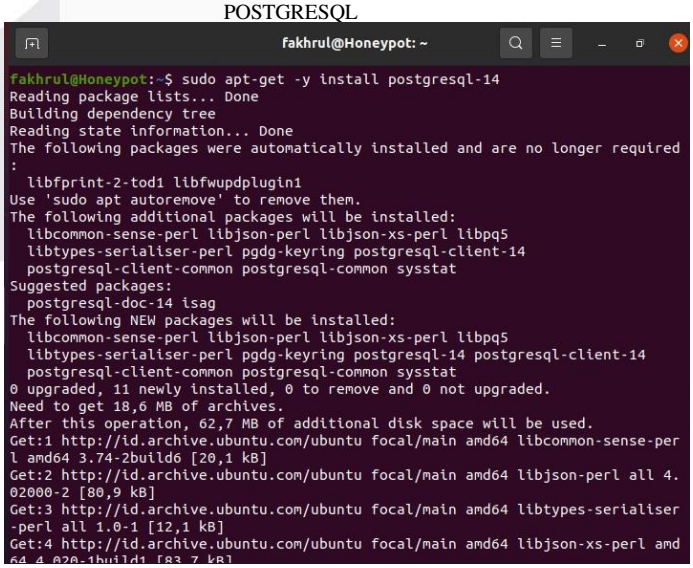
C. Postgresql

GAMBAR 5
BUAT KONFIGURASI REPOSITORI FILE UNTUK POSTGRESQL

Gambar 5 untuk menambahkan repository postgresql ke server digunakan kode "echo" dengan file tujuan berada pada direktori "/etc/apt/sources.list.d/", selanjutnya kode "wget" untuk mengambil kunci dari postgresql untuk digunakan pada server dengan tujuan pada alamat "https://www.postgresql.org/media/keys/ACCC4Cf8.asc" yang kemudian disimpan dengan menggunakan perintah "sudo apt-key add –".

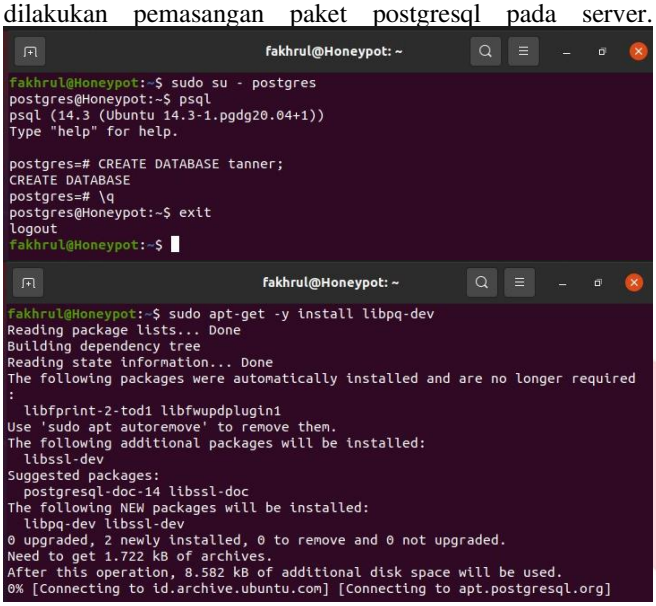


GAMBAR 6
PERBARUI PAKET UBUNTU UNTUK DAPAT MENGAMBIL PAKET POSTGRESQL



GAMBAR 7
PERBARUI PAKET UBUNTU UNTUK DAPAT MENGAMBIL PAKET POSTGRESQL

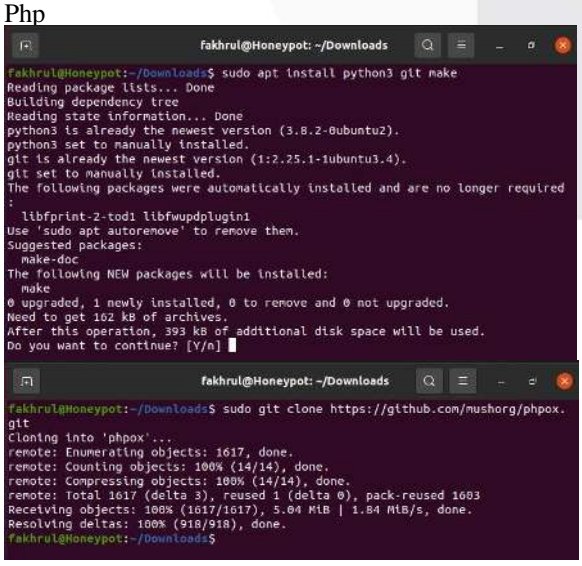
Gambar 6 dan 7 menunjukkan perintah untuk memperbarui paket sistem operasi ubuntu dengan memanfaatkan kode “apt-get update” dapat dilihat server postgresql sudah berhasil ditambahkan selanjutnya dengan menggunakan kode “apt-get -y install postgresql-14” dilakukan pemasangan paket postgresql pada server.



GAMBAR 8
INSTALL LIBRARY YANG DIBUTUHKAN UNTUK MENJALANKAN HONEYPOT

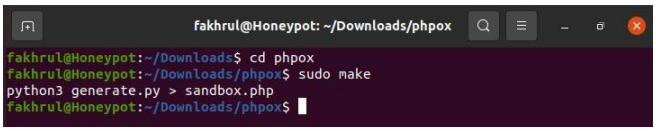
Gambar 8 menunjukkan perintah pemasangan paket yang dibutuhkan oleh honeypot dengan menggunakan kode “apt-get -y install libpq-dev” pemasangan paket membutuhkan 8.582 kB ruang penyimpanan server dan “libssl-dev” sebagai paket tambahan. Kode “sudo su – postgres” digunakan untuk masuk ke database postgres, database tanner dibuat dengan menggunakan kode “CREATE DATABSE tanner;”.

D. Php



GAMBAR 9
INSTALL PAKET YANG DIPERLUKAN UNTUK PHP

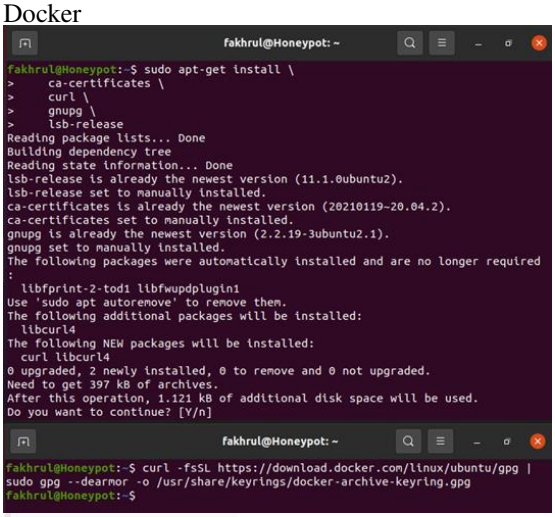
Gambar 9 menunjukkan perintah pemasangan paket git make dengan menggunakan kode “apt install git make”, paket git make dibutuhkan agar proses pembuatan data yang dibutuhkan php bisa dibuat, selanjutnya kode “git clone https://github.com/mushorg/phpbox.git” digunakan untuk mengambil data php yang dibutuhkan pada alamat https://github.com/mushorg/phpbox.git dan disimpan dengan nama direktori “phpbox”.



GAMBAR 10
JALANKAN PERINTAH MAKE UNTUK MENGCOMPILE FILE PHP

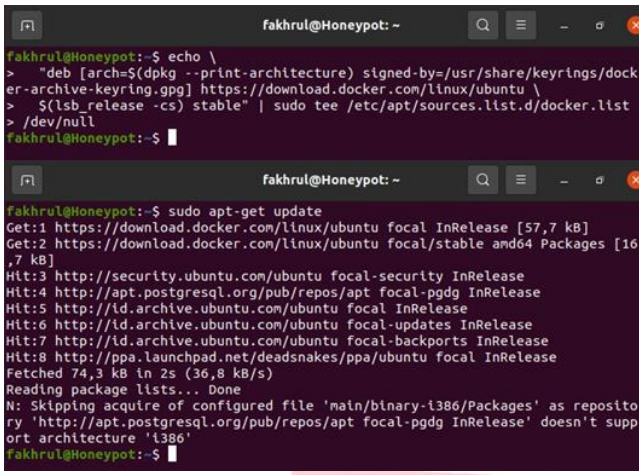
Gambar 10 menunjukkan perintah pembuatan file php yang digunakan oleh honeypot dengan menggunkan kode “make”, server akan melakukan compile file yang menghasilkan file baru bernama “sandbox.php” yang digunakan oleh tanner untuk menyimpan session ketika sedang berjalan.

E. Docker



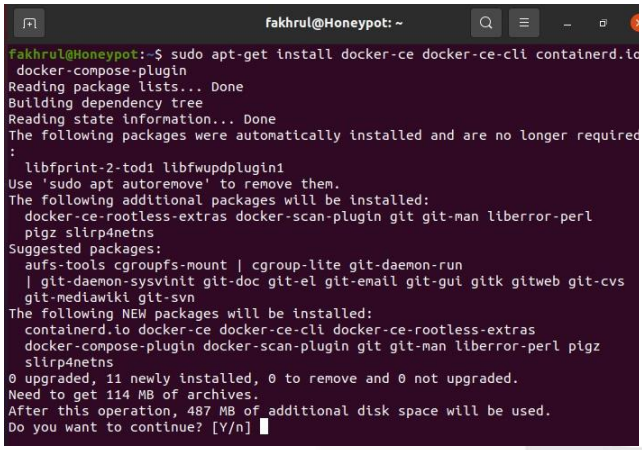
GAMBAR 11
PEMASANGAN PAKET YANG DIBUTUHKAN DAN PENGAMBILAN KUNCI DOCKER

Gambar 11 menunjukkan proses pemasangan paket yang dibutuhkan seperti “ca-certificates, curl, gnupg, dan lsb-release” dengan menggunakan kode “apt-get install” selanjutnya kode “curl” dijalankan untuk mengambil kunci docker yang digunakan oleh server pada alamat “https://download.docker.com/linux/ubuntu/gpg” yang kemudian disimpan pada direktori “/usr/share/keyrings/” dengan nama “docker-archive-keyrings.gpg”.



GAMBAR 12
MEMASUKKAN KODE REPOSITORY DAN MEMPERBARUI PAKET SISTEM OPERASI

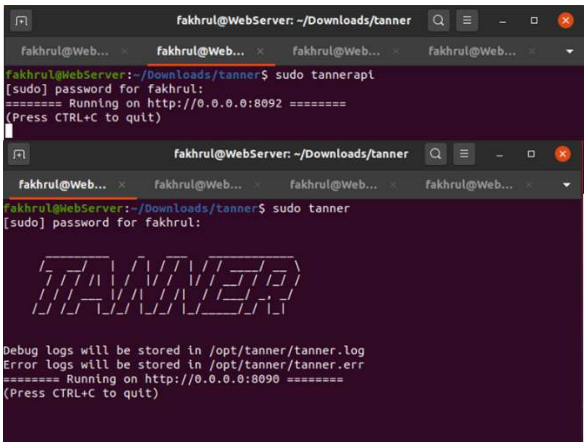
Gambar 12 menunjukkan perintah memperbarui dan memasukkan kode repository paket pada sistem opersi ubuntu dengan kode "apt-get update" dan kode "echo \ "deb [arch=5(dpkg –print-architecture) signed-by=/usr/share/keytings/docker-archive-keyrings.gpg) https://download.docker.com/linux/ubuntu \ $(lsb_release -cs) stable'" dengan tujuan file berada pada direktori "/etc/apt/sources.list.d/" dengan nama file "docker.list".



GAMBAR 13
PEMASANGAN PAKET DOCKER

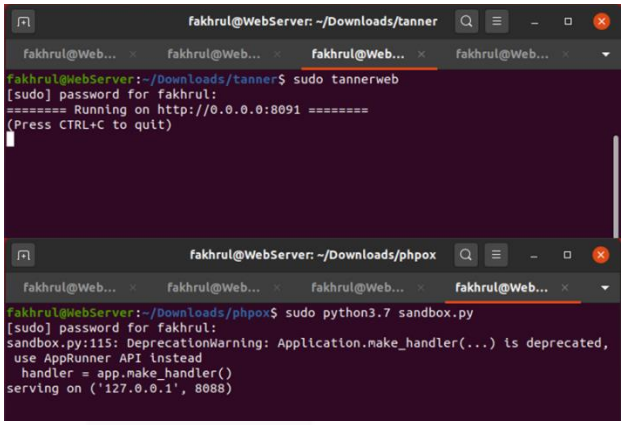
Gambar 13 menunjukkan perintah pemasangan paket docker pada sistem operasi ubuntu dengan menggunakan kode "apt-get install", paket docker dipasang dengan membutuhkan 487 MB ruang penyimpanan, 11 paket baru, dan beberapa paket tambahan lainnya yang dibutuhkan.

F. Memulai sistem Honeypot



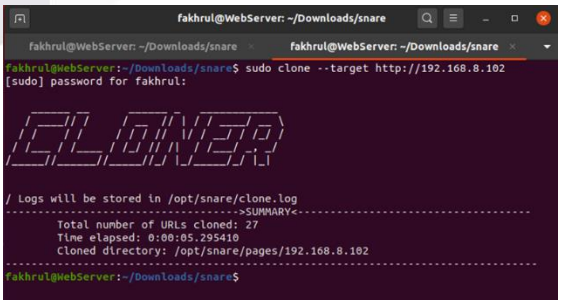
GAMBAR 14
MEMULAI TANNER DAN TANNERAPI

Pada gambar 14 tanner dan tannerapi dijalankan dengan perintah "sudo tanner" dan "sudo tannerapi", tanner dan tannerapi berjalan pada IP 0.0.0.0:8090 dan IP 0.0.0.0:8092, tanner berfungsi menerima data yang dikirimkan snare dan tannerapi berfungsi sebagai penerjemah data yang berada pada tanner



GAMBAR 15
MEMULAI TANNERWEB DAN SANDBOX PHP

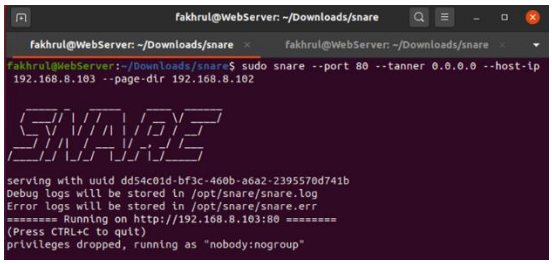
Pada gambar 15 tannerweb dijalankan dengan menggunakan perintah "sudo tannerweb" tannerweb berfungsi untuk menampilkan hasil data penyerang pada halaman web browser, tannerweb berjalan pada IP 0.0.0.0:8091 dan sandbox dijalankan dengan menggunkan perintah "sudo python3.7 sandbox.py" sandbox berfungsi untuk menyimpan session yang berjalan.



GAMBAR 16
MELAKUKAN CLONING WEB

Gambar 16 menunjukkan proses cloning web oleh snare yang digunakan sebagai web pengecoh, perintah yang digunakan adalah "sudo clone –target http://192.168.8.102" hasil cloning web disimpan di dalam direktori

/opt/snare/pages/192.168.8.102 dengan total url 27 dan waktu 0:00:05.295410.



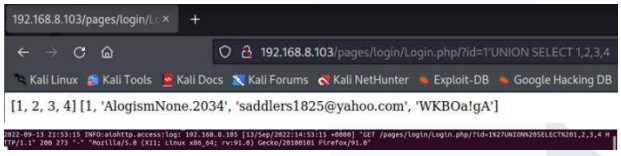
GAMBAR 17
MEMULAI SNARE

Pada gambar 17 menunjukkan snare sedang berjalan dengan menggunakan perintah "sudo snare –port 80 –tanner 0.0.0.0 –host-ip 192.168.8.103 –page-dir 192.168.8.102", dengan ketentuan snare berjalan pada IP 192.168.8.103 port 80 dan tanner dengan IP 0.0.0.0 dan hasil clone pada direktori 192.168.8.102, snare menyimpan log serangan pada direktori /opt/snare/snare.log.

Selanjutnya dilaporkan pengujian dengan melakukan beberapa teknik penyerangan yang ditujukan ke honeypot.

A. SQL Injection

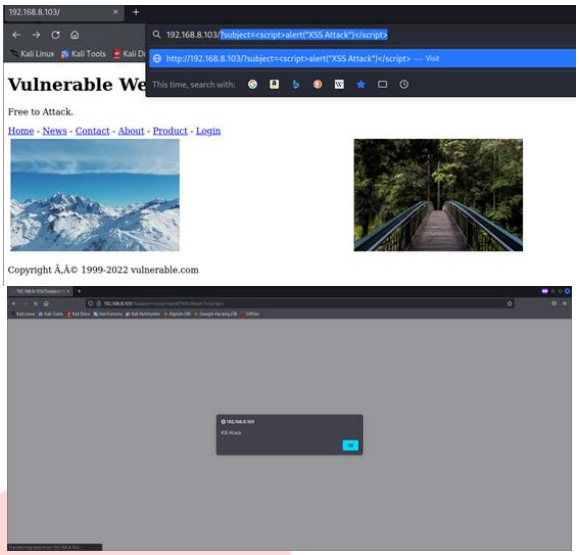
Pengujian dilakukan dengan teknik sql poisoning secara manual dengan menambahkan kode "?id=1'UNION SELECT 1,2,3,4" pada bagian akhir url dapat dilihat pada gambar 4-15, pengujian ini bertujuan untuk mengetahui apakah ada celah pada sistem database web server. Setelah melakukan serangan dapat dilihat web memberikan data yang ada pada server kemudian ditampilkan pada layar penyerang, dapat disimpulkan serangan SQL Injection bisa dilakukan tanpa adanya pencegahan dari Honeypot. Honeypot berhasil mendeteksi serangan dan disimpan pada file log yang dapat dilihat pada gambar 18.



GAMBAR 18
PENYERANGAN MENGGUNAKAN SQL INJECTION

B. XSS Attack

Pengujian XSS Attack dilakukan secara manual dengan menambahkan kode ?subject=<script>alert("XSS Attack")</script> pada akhir url, serangan bertujuan untuk mengetahui apakah web rentan terhadap serangan XSS dan apakah web bisa melakukan tindakan saat serangan terjadi, setelah serangan dilakukan, web tidak dapat mencegah XSS dan web berhasil diserang dapat dilihat pada gambar 4-16, serangan dapat terjadi karena web tidak menggunakan keamanan script html dan php dengan baik sehingga terjadi serangan.



GAMBAR 19
SERANGAN XSS

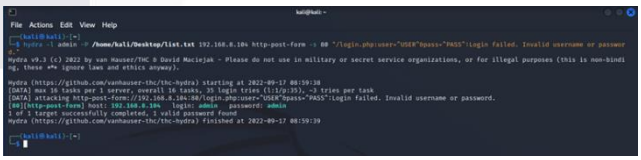
GAMBAR 20
PENYERANGAN DICATAT OLEH HONEYPOT

Pada gambar 20 Honeypot berhasil mencatat bahwa telah terjadi serangan XSS pada tanggal 13-09-2022 jam 21:55:39 dilakukan oleh IP 192.168.8.105 dengan menggunakan metod GET.

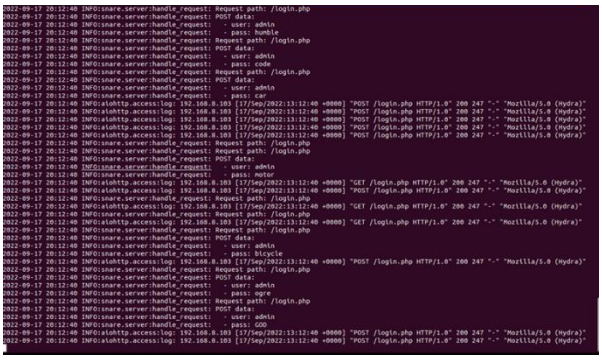
C. Brute Force Attack

Serangan Brute Force Attack dilakukan dengan memanfaatkan perangkat lunak hydra, hydra berfungsi untuk mencari kombinasi nama user dan password yang terdapat pada server, langkah penggunaan hydra adalah dengan menggunakan kode "hydra -l admin -P /home/kali/Desktop/list.txt 192.168.8.104 http-post-form -s 80 "/login.php:user=^USER^&pass=^PASS^:Login failed. Invalid username or password."", dapat dilihat pada gambar 4-17.

Kode berfungsi dengan memasukkan alamat target file yang berisi kombinasi nama user dan password, port yang digunakan, dan module yang digunakan oleh Hydra. Berdasarkan hasil serangan dapat disimpulkan serangan berhasil dilakukan karena berhasil mendapatkan nama user dan password yang valid digunakan dapat dilihat pada gambar 4-17.



GAMBAR 21
PENYERANGAN MENGGUNAKAN HYDRA



GAMBAR 22
HONEYPOT MENANGKAP SERANGAN BRUTE FORCE ATTACK

Pada gambar 22 Honeypot berhasil menangkap serangan Brute Force Attack yang dilakukan oleh IP 192.168.8.103 dengan metode POST pada tanggal 17-09-2022 jam 20:12:40.

TABEL 3
PENGUJIAN

No	Serangan	Hasil
1	XSS menggunakan *script* "<script>alert("XSS Attack")</script>"	Serangan berhasil dilakukan dan terdeteksi oleh *Honeypot.*
No	Serangan	Hasil
2	SQLi menggunakan *script* "?id=1'UNION SELECT 1,2,3,4"	Serangan berhasil dilakukan dan berhasil dideteksi oleh *Honeypot*
3	Brute Force menggunakan perangkat lunak *Hydra*	Serangan berhasil dilakukan dan mendapatkan kombinasi nama *user* dan *password* yang terdeteksi oleh *Honeypot.*

Setelah melakukan pengujian didapatkan hasil bahwa serangan berhasil dilakukan dan Honeypot dapat mendeteksi serangan bisa dilihat pada tabel 4-3, serangan menggunakan XSS dengan menggunakan script berhasil dilakukan disebabkan web tidak menggunakan keamanan yang baik pada sisi pembuatan html/php sehingga Honeypot dapat mendeteksi serangan.

Serangan menggunakan SQLi berhasil dilakukan karena tidak ada atau kurang amannya sistem Database server dan Honeypot berhasil mendeteksi serangan bisa dilihat pada gambar 4-15, selanjutnya dilakukan serangan menggunakan teknik Brute Force Attack, serangan berhasil dilakukan dan dapat dideteksi oleh Honeypot serangan berhasil dilakukan karena sistem menggunakan sistem keamanan yang sudah kadaluarsa/usang sehingga mudah dilakukan serangan.

V. KESIMPULAN

Berdasarkan hasil dari pengujian dapat diambil kesimpulan berupa :

1. Pengujian berjalan dengan baik dengan beberapa teknik yang dilakukan, dan Honeypot dapat mendeteksi serangan yang dilakukan yang ditampilkan pada web.
2. Honeypot hanya bekerja jika serangan ditujukan langsung kepada Honeypot, jika serangan ditujukan kepada webserver Honeypot tidak dapat mendeteksi serangan dan untuk pencarian hasil serangan memakan waktu yang lama karena Honeypot merekam segala jenis transmisi yang masuk.

REFENRENSI

[1] "What is a Hyperlink? - Definition from Techopedia." https://www.techopedia.com/definition/5175/hyperlink (accessed Jul. 21, 2022).

[2] "8 Kasus Peretasan yang Terjadi di Indonesia Sepanjang 2021 Halaman all - Kompas.com." https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all (accessed Jul. 21, 2022).

[3] "What is a honeypot? How honeypots help security." https://www.kaspersky.co.za/resource-center/threats/what-is-a-honeypot (accessed Jul. 21, 2022).

[4] L. P. AIDIN, "IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER." Universitas Telkom, S1 Sistem Komputer, 2016. Accessed: Jan. 27, 2022. [Online]. Available: https://openlibrary.telkomuniversity.ac.id/home/catalog/id/116784/slug/implementasi-high-interaction-honeypot-pada-server.html

[5] D. K. RAHMATULLAH, "IMPLEMENTASI LOW INTERACTION HONEYPOT PADA EMBEDDED SYSTEM." Universitas Telkom, 2016. Accessed: Jan. 27, 2022. [Online]. Available: https://openlibrary.telkomuniversity.ac.id/home/catalog/id/120994/slug/implementasi-low-interaction-honeypot-pada-embedded-system.html

[6] D. HERRYANTO, "PERANCANGAN DAN IMPLEMENTASI ANALISIS LOG HONEYPOT PADA PERANGKAT INTERNET OF THINGS (IoT) MENGGUNAKAN ELK STACK DAN REGULAR EXPRESSION." Universitas Telkom, S1 Teknik Komputer, 2021. Accessed: Jan. 27, 2022. [Online]. Available: https://openlibrary.telkomuniversity.ac.id/home/catalog/id/170891/slug/perancangan-dan-implementasi-analisis-log-honeypot-pada-perangkat-internet-of-things-iot-menggunakan-elk-stack-dan-regular-expression.html

[7] D. Permana, "Perancangan dan Implementasi Sistem Keamanan Honeypot pada Layanan VoIP," Telkom University, 2012.

[8] M. Arief, "Implementasi Honeypot Dengan Menggunkan Dionaea Dijaringan Hotspot FIZZ," Politeknik Telkom: Bandung, 2012.