E-ISSN : 3031-9692 Vol. 1 No. 1 2024
Institut Tekno*logi* dan Bisnis STIKOM Bali, 22-04-2024

Perancangan Keamanan Jaringan Menggunakan *Honeypot* Pada UPTD Pengendalian Bencana BPBD Provinsi Bali

Gede Manik Megaputra[1)], Ricky Aurelius Nurtanto Diaz[2)], Ni Wayan Ari Ulandari[3)]
Program Studi Sistem Komputer
Institut Tekno*log*i dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: manikmegaputra47@gmail.com[1], ricky@stikom-bali.ac.id[2], ulandari@stikom-bali.ac.id[3]

Abstrak

Server merupakan sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server menjalankan perangkat lunak yang dapat mengontrol akses terhadap jaringan dan sumber daya yang berada dalam jaringan tersebut seperti server website. Web server biasanya menjadi target serangan seorang hacker untuk mendapatkan akses dan data yang ada pada web server tersebut. Keamanan jaringan komputer sangat penting dalam mengontrol akses jaringan serta mencegah penyalah gunaan sumber daya jaringan yang tidak sah. Salah satu upaya yang bisa diterapkan dalam meningkatkan keamanan jaringan komputer adalah dengan mengaplikasikan IDS. Selain dengan menggunakan IDS untuk mengamankan server dapat juga dengan menambahkan perlindungan berlapis seperti honeypot. Honeypot merupakan suatu sistem proteksi yang menciptakan layanan palsu dari server yang dilindungi, dibuat dengan kode sumber terbuka dan dapat diakses secara gratis oleh calon penggunaPada penelitian ini menggunakan metode pengembangan jaringan PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize). Metode perancangan jaringan yang disebut PPDIOO merupakan siklus hidup layanan jaringan yang dikembangkan oleh Cisco. Hal ini bertujuan untuk mendukung pertumbuhan jaringan yang terus berkembangBerdasarkan penelitian yang dilakukan terhadap perancangan sistem keamanan honeypot, dapat ditarik beberapa kesimpulan. Perancangan keamanan jaringan dan server yang telah dilakukan sebelumnya dapat bekerja dengan cukup baik ketika terjadi ancaman terhadap server.

Kata kunci: *Honeypot, Intrusion Detection System, Keamanan Jaringan, Web Server.*

1. Pendahuluan

Server merupakan sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* menjalankan perangkat lunak yang dapat mengontrol akses terhadap jaringan dan sumber daya yang berada dalam jaringan tersebut seperti *server* website[1]. *Web server* adalah perangkat lunak yang menyediakan layanan data dan bertanggung jawab untuk menerima permintaan HTTP (*HyperText Transfer Protocol*) atau HTTPS yang dikirim oleh client melalui browser dan mengembalikan hasilnya dalam bentuk halaman web, biasanya dalam format HTML. (*HyperText Markup Language*). *Web server* berguna sebagai lokasi aplikasi *web* dan sebagai tujuan permintaan client.[2]. *Web server* biasanya menjadi target serangan seorang *hacker* untuk mendapatkan akses dan data yang ada pada *web server* tersebut.

Keamanan jaringan komputer sangat penting dalam mengontrol akses jaringan serta mencegah penyalah gunaan sumber daya jaringan yang tidak sah[3]. Salah satu upaya yang bisa diterapkan dalam meningkatkan keamanan jaringan komputer adalah dengan mengaplikasikan *IDS*. *Intrusion Detection System* merupakan suatu mekanisme keamanan yang diprogram untuk melakukan pengawasan terhadap titik akses, aktivitas host, dan upaya penyusupan[4]. Suricata merupakan IDS yang dapat mendeteksi indikasi terjadinya penyerangan terhadap jaringan dan server dengan menggunakan aturan yang ada. Suricata bekerja dengan cara memeriksa paket atau serangan yang ada menggunakan aturan yang dibuat oleh Suricata jika terjadi serangan. Jika serangan terdeteksi, Suricata akan membuat log serangan yang dilakukan.[5].

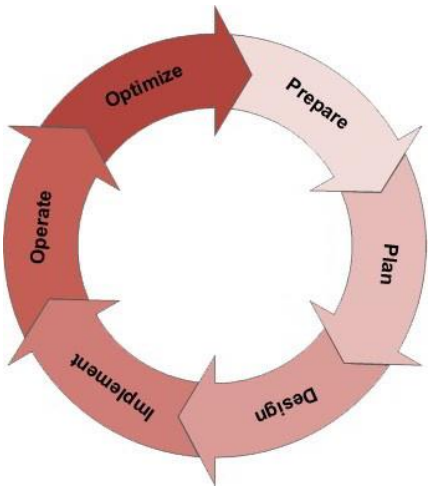
Selain dengan menggunakan *IDS* untuk mengamankan *server* dapat juga dengan menambahkan perlindungan berlapis seperti honeypot. *Honeypot* merupakan suatu sistem proteksi yang menciptakan layanan palsu dari *server* yang dilindungi, dibuat dengan kode sumber terbuka dan dapat diakses secara gratis oleh calon pengguna. *Honeypot* mengambil alih peran *firewall* sebagai pertahanan luar saat biaya menjadi faktor utama dalam upaya untuk melindungi server web.[6].

Honeypot dapat membuat sistem layanan palsu yang sengaja dirancang untuk diserang oleh *hacker* yang menerobos ke *server* tersebut, memberikan kesan bahwa mereka telah berhasil menembus sistem, namun sebenarnya para *hacker* tersebut telah menyusupi sistem palsu yang diterapkan di dalamnya. *Honeypot* dapat menjebak penyerang dengan mengubah *port* yang bertindak sebagai jebakan atau tempat di jaringan untuk menipu penyerang, mengumpulkan *log*, dan aktivitas serangan[4]. *High Interaction Honeypot* adalah layanan ketiga dalam sistem *honeypot* di mana *administrator* jaringan tidak perlu lagi memantau aktivitas peretasan karena *server* asli telah direplikasi sepenuhnya. Hal ini memungkinkan penyerang untuk menyerang server replikasi yang berisi informasi palsu, sehingga mereka merasa telah berhasil dalam upaya peretasan, padahal server asli tetap aman dan tidak terganggu.[7].

Dalam penelitian ini penulis mengambil studi kasus pada UPTD Pengendalian Bencana BPBD Provinsi Bali. Dikarenakan UPTD Pengendalian Bencana BPBD Provinsi Bali memiliki tugas sebagai Pusat Data dan Informasi Kebencanaan, dan menyampaikan informasi terkait kebencanaan kepada seluruh masyarakat, maka diperlukan sebuah sistem untuk mengamankan *server*. Yang dimana cakupannya terlalu luas dan banyak, maka di dalam penelitian ini penulis hanya melakukan penelitian pada *server* yang letaknya di gedung kantor UPTD Pengendalian Bencana BPBD Provinsi Bali.

2. Metode Penelitian

Pada penelitian ini menggunakan metode pengembangan jaringan PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*). Metode perancangan jaringan yang disebut PPDIO merupakan siklus hidup layanan jaringan yang dikembangkan oleh cisco. Hal ini bertujuan untuk mendukung pertumbuhan jaringan yang terus berkembang[8]. Strategi ini digunakan sebagai tahapan dalam pelaksanaan konfigurasi keamanan honeypot dimana teknik ini terdiri dari enam tahapan yang saling berhubungan satu sama lain.



Gambar 1. Metode PPDIOO

1) *Prepare*: Tahapan ini adalah tahapan yang diperlukan dalam proses penelitian agar penelitian berjalan dengan baik. Pada tahap ini akan dilakukan mulai dari mengumpulkan data dan informasi untuk membangun sebuah sistem keamanan, supaya bisa dilakukan konfigurasi awal hingga siap untuk dioperasikan serta identifikasi permasalahan yang ada.
2) *Plan*: Tahapan kedua akan dilakukannya perencanaan untuk menentukan *hardware* dan *software* apa saja yang digunakan dalam penelitian ini.
3) *Design*: Tahapan pembuatan rancangan dari sistem topologi keamanan jaringan yang akan dipakai pada saat tahap implementasi nantinya.
4) *Implement*: Tahapan *implement* akan dilakukan konfigurasi terhadap sistem yang telah dirancang sebelumnya pada tahap *design* untuk sistem keamanan honeypot.
5) *Operate*: Tahapan dimana dilakukan pengujian terhadap konfigurasi dari sistem yang telah dibangun untuk mengetahui apakah sistem sudah berjalan dengan sesuai serta untuk mengetahui kelebihan dan kekurangan dari sistem yang dirancang.
6) *Optimize*: Merupakan tahapan akhir yang akan dilakukan proses analisis untuk mengevaluasi kinerja sistem honeypot yang telah dirancang dan dibangun untuk mengoptimalkan keamanan jaringan.

3. Hasil dan Pembahasan

3.1 *Prepare* (Persiapan)

Pada tahap *prepare* akan dilakukan peninjauan langsung ke UPTD Pengendalian Bencana BPBD Provinsi Bali, khususnya pada jaringan komputer yang terdapat pada instansi dengan mengamati secara langsung infrastruktur jaringan yang terdapat disana, serta mempersiapkan perangkat dan konfigurasi yang akan dilakukan pada tahap implementasi jaringan nantinya, yang dijelaskan pada tahap selanjutnya yaitu tahapan *plan*.

3.2 *Plan* (Perencanaan)

Pada tahapan ini dilakukan perencanaan perangkat serta aplikasi apa saja yang digunakan nantinya dalam membangun sistem keamanan *honeypot* yang dapat dilihat pada Tabel 1.

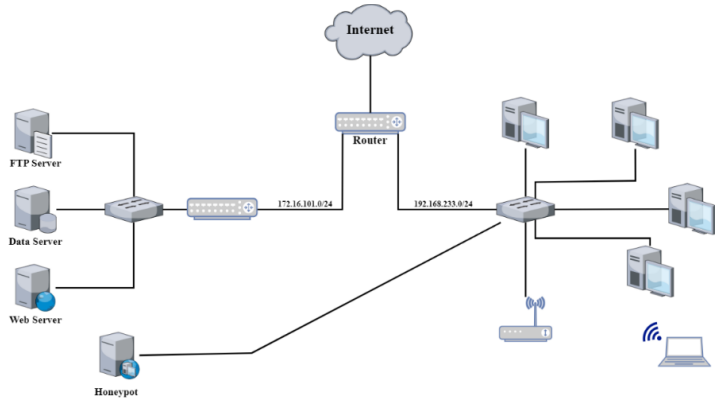
Tabel 1 Perencanaan *Software* dan *Hardware*

No	Jenis	Keterangan
1	Ubuntu *Server*	Sebagai sistem operasi *server*
2	Suricata	Sebagai pencatat dan pengecek *alert* yang masuk
3	*Honeypot* T-pot	*Software* yang diimplementasikan sebagai pengecoh dan tiruan dari *server* sebagai sistem keamanan
4	Nmap	*Software* yang digunakan untuk *tool scanning* jaringan komputer
5	Komputer *Server*	Digunakan sebagai *server* snort dan *honeypot*
6	PC/Laptop	Digunakan sebagai *attacker* untuk melakukan pengujian pada *server honeypot*

Setelah persiapan *hardware* dan *software* telah selesai dilakukan, selanjutnya akan dilanjutkan pada tahapan *design*

3.3 *Design* (Desain)

Pada tahapan desain merupakan tahapan perancangan topologi jaringan yang digunakan dalam proses pembangunan sistem ini yang dimana dalam membangun sebuah jaringan diperlukan sebuah rancangan topologi untuk mempermudah dalam mengatur dan mengetahui lalu lintas yang dibangun.



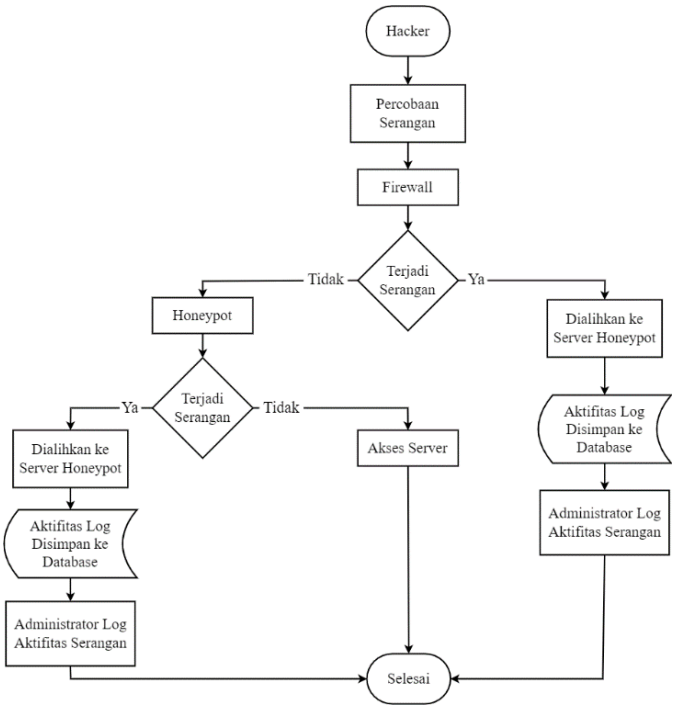
Gambar 2. Rancangan Topologi *Honeypot*

Pada Gambar 2 menjelaskan rancangan dari topologi jaringan yang akan dibangun. Jaringan komputer akan difilter dahulu sebelum bisa mengakses *server* jika ada indikasi dilakukan serangan maka akan dialihkan ke *server honeypot*.

3.4 *Implement* (Implementasi)

Pada tahap implementasi dilakukan proses instalasi dan konfigurasi sistem keamanan *honeypot*. *Firewall* bertugas sebagai penyaring lalu lintas jaringan. Dalam kasusnya *Firewall* akan memfilter jaringan yang mencoba mengakses server, jika tidak terdeteksi ancaman terhadap server maka firewall akan

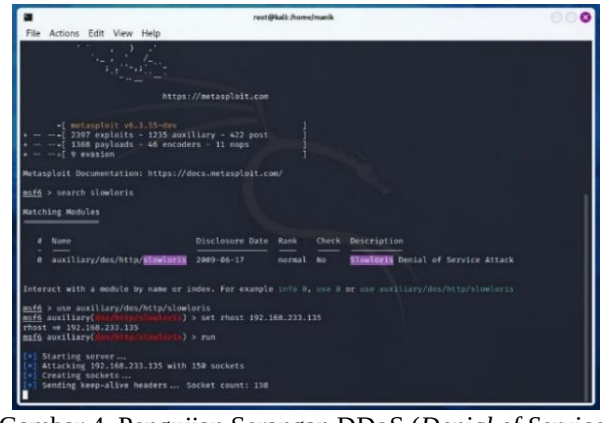
memperbolehkan untuk mengakses server yang asli. Tetapi apabila ada tanda terjadinya serangan, penyerang akan diarahkan ke server tiruan, sehingga aktivitas apa pun di server tiruan tersebut akan dicatat dan disimpan dalam log. Kemudian, dari log tersebut, administrator dapat mengetahui aktivitas apa saja yang dilakukan oleh penyerang. Seperti pada gambar 3. Alur cara kerja *honeypot* dibawah.



Gambar 3. Alur cara kerja *honeypot*

3.5 *Operate* (Operasional)

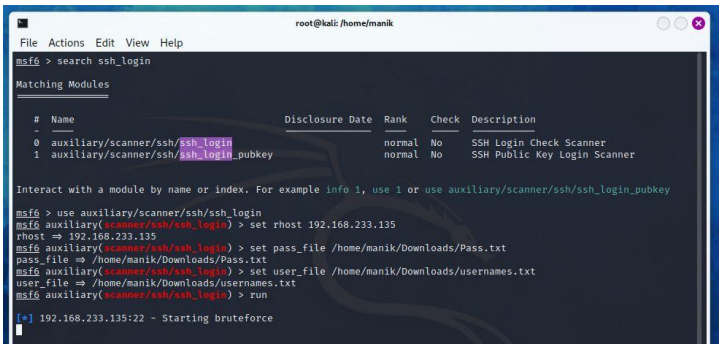
Pada tahap *operate* akan dilakukan proses pengujian menggunakan sebuah komputer yang digunakan sebagai *server honeypot* dan sebuah perangkat laptop yang dipakai sebagai penyerang untuk menguji dan memastikan *sever honeypot* sudah berfungsi dengan baik dengan menjalankan beberapa skema serangan terhadap *server honeypot.*



Gambar 4. Pengujian Serangan DDoS (*Denial of Service*)

Gambar 4 merupakan proses pengujian menggunakan *DDoS (Distributed Denial of Service).* Serangan Jaringan Terdistribusi atau sering disebut serangan *Distributed Denial of Service* (DDoS) merupakan serangan yang dilakukan dengan cara menggangu layanan suatu sistem sehingga tidak dapat diakses oleh pengguna yang sah. Serangan DDoS beroperasi dengan cara menghantam sumber daya server yang diserang dengan sejumlah besar permintaan. Tujuannya adalah untuk melampaui kapasitas server sehingga

server tidak dapat menangani semua permintaan tersebut, akibatnya server tidak dapat berfungsi dengan optimal[9].

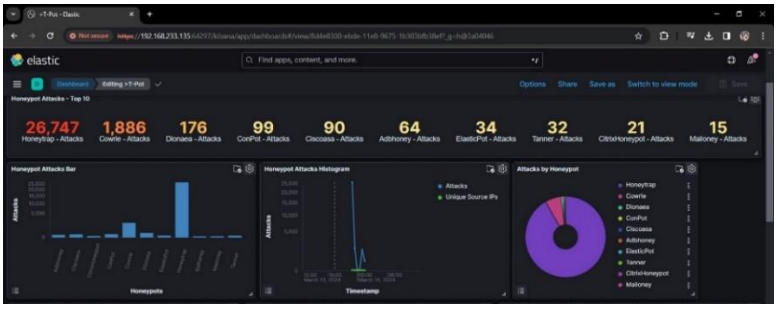


Gambar 5. Pengujian Serangan *bruteforce*

Pada gambar 5 dilakukan proses penyerangan menggunakan *bruteforce* bertujuan untuk mendapatkan *username* dan *password administrator* agar bisa terhubung dengan jaringan ssh. Teknik *hacking Brute Force* adalah salah satu teknik penyerang untuk meretas *password* sebuah *server*, jaringan atau *host*, dengan cara mencoba semua kemungkinan kombinasi *password* yang ada pada *wordlist*[10].

3.6 *Optimize* (Optimasi)

Setelah dilakukan pengujian serangan *DoS (denial of service)* dan *Bruteforce attack* akan dilanjutkan dengan tahapan optimasi. Pada tahapan ini akan dilakukan analisa dan evaluasi dari sistem *honeypot* yang dimana telah dilakukan proses pengujian pada tahapan sebelumnya.



Gambar 6. Tampilan Elastic Stack *Server Honeypot*

Honeypot mencatat terjadi banyak sekali serangan yang menyerang *server honeypot*. Honeytrap mencatat menerima 26.747 serangan dan Cowrie mencatat menerima 1886 serangan, sebagian besar serangan mengarah pada *port* ssh.

Gambar 7. Tampilan Alamat IP dan *Wordlist* dari *Attacker*

Honeypot mencatat alamat ip dari attacker, yang dimana 192.168.233.131 merupakan alamat ip dari perangkat yang digunakan untuk menguji *server honeypot*. *Honeypot* juga mencatat beberapa kombinasi *username* dan *password* yang merupakan *input* yang digunakan dalam serangan *bruteforce* yang dimana penyerang membuat daftar kemungkinan atau *wordlist* dari kombinasi *username* dan *password* dari *server* yang mereka serang dan mencoba semua kombinasi dari daftar yang telah mereka buat yang mungkin

merupakan *username* dan *password* dari *server* untuk bisa masuk ke *server* ssh atau telnet. Kombinasi dari *username* dan *password* ini terdiri dari huruf, angka, karakter khusus atau gabungan dari ketiganya.

4. Kesimpulan

Berdasarkan penelitian yang dilakukan terhadap perancangan sistem keamanan *honeypot*, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Perancangan keamanan jaringan dan *server* yang telah dilakukan sebelumnya dapat bekerja dengan cukup baik ketika terjadi ancaman terhadap *server*.
2. Jika terjadi serangan *administrator* mendapatkan notifikasi peringatan ketika ada upaya penyerangan sehingga *administrator* dapat melakukan tindakan pencegahan serangan secara efektif, dimana administrator dapat melihat analisis grafis *real-time* yang dapat membantu menganalisis pola serangan dan jenis serangan yang dilakukan penyerang dengan lebih mudah.
3. *Honeypot* dapat menyimpan *log* aktivitas serangan yang dilakukan oleh *attacker*, serta menyimpan informasi dari *attacker* seperti alamat IP serta perangkat yang digunakan.

Daftar Pustaka

[1] R. Firdaus, "Analisis Dan Implementasi High Interaction Honeypot Pada Server," Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau, Pekan Baru, 2020.

[2] D. Lesmideyarti, Q. Hidayati, T. Retno Nugroho, J. Teknik Elektro, J. Perhotelan, and P. Negeri Balikpapan, "Perancangan Infrastruktur dan Implementasi Web Server Untuk Website Sekolah Sebagai Media Informasi dan Komunikasi di SMP PJHI Balikpapan," 2023.

[3] J. D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," 2019.

[4] T. Natanegara, "Implementasi Honeypot Cowrie Dan Snort Sebagai Alat Deteksi," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, 2023.

[5] E. Stephani, F. Nova, E. Asri, and N. # Fitri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," 2020. [Online]. Available: http://jurnal-itsi.org

[6] W. A. Sulaksono, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, 2020, doi: 10.30743/infotekjar.v5i1.2783.

[7] J. Hotspot *et al.*, "Analisis Implementasi Honeypot Dan IDS Pada," Jakarta, 2022. [Online]. Available: https://lib.mercubuana.ac.id/

[8] R. B. Ankhal, "Perancangan Infrastruktur Teknologi Informasi Adaptif pada DISKOMINFO Kabupaten Padang Pariaman dengan Metode PPDIOO Design of Adaptive Information Technology Infrastructure in Communication and Information Department of Padang Pariaman Regency with PPDIOO Method," Bandung, 2023.

[9] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[10] Suliman, A. Achmad, and Adnan, "Implementasi Honeypot Dan Port Knocking Dalam Mendeteksi Serangan DDOS Attack Pada Server Jaringan," *semanTIK*, vol. 7, no. 1, pp. 1–5, 2021, doi: 10.5281/zenodo.5034918.