DETEKSI SERANGAN PERETAS MENGGUNAKAN HONEYPOT COWRIE DAN INTRUSION DETECTION SYSTEM SNORT

Roby Rupiat[1*)], Sutan Faisal[1)], Tohirin Al Mudzakir[1)], Santi Arum Puspita Lestari[1)]
[1)] Teknik Informatika, Universitas Buana Perjuangan Karawang, Karawang
*Email Korespondensi : if16.robyrupiat@mhs.ubpkarawang.ac.id

ABSTRAK

Sistem keamanan server menjadi sangat penting dalam menjaga sebuah data. Dinas komunikasi informatika persandian dan statistik kabupaten Bekasi saat ini hanya menggunakan *firewall* sebagai sistem keamanan server, sehingga dapat menyebabkan aktifitas serangan yang dapat mengakibatkan kerugian kehilangan data. Permasalahan tersebut, perlu dibangun sistem keamanan server yang bisa mengamankan data pada sistem server. Penelitian ini menggunakan sistem keamanan server *honeypot cowrie* dan IDS snort. Metode pengembangan sistem yang digunakan yaitu *Network Development Life Cycle* (NDLC). Proses pengujian yang digunakan yaitu teknik serangan *port scanning*, teknik serangan bruteforce attack, dan melakukan blok ip address peretas. Pengujian dengan teknik *port scanning* dapat menghasilkan informasi penting pada suatu jaringan dan mendeteksi *port* yang terbuka, di antaranya *port* 22 yaitu ssh (secure shell). Teknik serangan bruteforce attack dapat menghasilkan kombinasi *username* dan *password* yang ada pada sistem server secara ilegal. *Honeypot cowrie* dapat menjebak peretas dengan server palsu yang telah dibuat. IDS snort dapat mendeteksi serangan yang masuk pada sistem server, kemudian IDS snort dapat memblokir ip address peretas yang melakukan serangan terhadap sistem server. Sehingga data yang ada pada sistem server dapat terjaga dengan aman, karena setiap aktiftas peretasan dapat dipantau oleh administrator untuk ditindak lebih lanjut.

Kata kunci: Cowrie, Honeypot, IDS, NDLC, Snort

ABSTRACT

Server security systems are very im*port*ant in maintaining data. Currently, the Bekasi District Office of Encryption Informatics and Statistics only uses a firewall as a server security system, so it can cause attack activities that can result in data loss. With these problems, it is necessary to build a server security system that can secure data on the server system. This research uses cowrie honeypot server security systems and IDS snort. The system development method used is the Network Development Life Cycle (NDLC). The testing process used is the *port scanning* attack technique, the brute force attack technique, and blocking the hacker's IP address. Testing with *port scanning* techniques can generate im*port*ant information on a network and detect open *port*s, including *port* 22, namely secure shell. The brute force attack technique can illegally generate username and password combinations on the server system. A cowrie honeypot can trap hackers with a fake server that has been created. IDS snort can detect incoming attacks on the server system, then IDS snort can block the IP address of hackers who attack the server system. So that data on the server system can be maintained safely, because every hacking activity can be monitored by the administrator for further action.

Keywords: Cowrie, Honeypot, IDS, NDLC, Snort

PENDAHULUAN

Peranan komputer sangatlah penting bagi suatu pemerintahan, pendidikan, maupun perusahaan swasta dalam membantu kegiatan operasional para karyawan dalam melakukan sistem informasi pengolahan data dan menyajikan suatu informasi yang tepat

ISSN Cetak : 2622-1276
ISSN Online : 2622-1284

dan akurat. Perkembangan teknologi telah menjadikan salah satu media seperti internet menjadi media yang utama dalam pertukaran informasi. Tidak semua informasi dapat diakses untuk umum. Internet merupakan jaringan luas dan bersifat publik, oleh karena itu diperlukan suatu usaha untuk menjamin keamanan informasi terhadap data atau layanan yang menggunakan internet [1]. Sementara itu, masalah keamanan ini masih seringkali kurang mendapat perhatian, seringkali masalah keamanan ini berada diurutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap kurang penting. Apabila menggangu informasi dari sistem, seringkali keamanan dikurangi atau dihilangkan [2]. Banyak sekali data-data penting yang tersimpan didalam database sebuah server, untuk itu diperlukan suatu sistem keamanan yang canggih untuk mengamankan data-data yang tersimpan di database server tersebut. Jika webserver tidak memiliki sistem keamanan yang canggih, maka para peretas atau hacker akan dengan mudah mencuri data-data penting yang tersimpan di database server tersebut.

Penelitian terkait tentang sistem keamanan telah dilakukan oleh Marta, Hartawan dan Santika [3], sistem yang dibangun melakukan pendeteksian intrusi pada server secara realtime menggunakan snort. Ketika terjadi akses yang tidak wajar pada server, maka snort akan mendeteksi dan mengirimkan informasi terjadinya aktivitas yang tidak wajar ke administrator jaringan. Penelitian berikutnya oleh Prabowo , Darusalam dan Ningsih [4], dibutuhkan penanganan keamanan khusus pada server yang tidak terkait dengan aplikasi pihak ketiga. Perancangan keamanan tersebut dapat diterapkan melalui konfigurasi kernel serta tweak yang dapat dilakukan dengan mengandalkan aplikasi bawaan sebuah sistem operasi. Selanjutnya yaitu penelitian yang dilakuka oleh Santoso [5], keamanan server saat ini sangat penting karena menyangkut privasi seseorang maupun privasi sebuah lembaga. Meningkatnya kasus pencurian data di dunia internet juga menjadi salah satu latar belakang pentingnya sebuah keamanan server. Mengukur tingkat keamanan sebuah server dapat dilakukan dengan berbagai cara di antaranya dengan melakukan penilaian kerentanan dan pengujian penetrasi. Penelitian terkait selanjutnya dilakukan oleh Prasetyo [6], honeypot dapat berjalan dan menjebak peretas dengan memberi respon terhadap *scanning* dan memberi informasi palsu seperti url serta *port* yang terbuka yang biasanya dicari penyerang. Selanjutnya penelitian dilakukan oleh Husain, Aksara dan Ransi [7], sistem pendeteksi dan pencegahan serangan dengan cara pemblokiran terhadap Internet Protocol (IP) penyerang, hasil yang diperoleh yaitu penggunaan snort dan IPTables sebagai sistem keamanan server pada jaringan wireless berhasil mengatasi jenis serangan pada *port* ICMP, FTP, SSH, TELNET, dan HTTP menggunakan berbagai macam tools penyerang seperti Angry IP Scanner, Filezilla, Putty, Mozila Firefox dan Zenmap.

Berdasarkan perkembangan teknologi saat ini banyak hal yang dikembangkan salah satunya sistem keamanan server honeypot cowrie dan intrusion detection system snort (IDS), yang digunakan untuk mengamankan suatu sistem server dari kemungkinan serangan yang dilakukan oleh peretas atau hacker. Maka penelitian berjudul "Deteksi Serangan Peretas Menggunakan *Honeypot Cowrie* dan *Instrusion Detection System Snort*".

METODE PENELITIAN

Peralatan Penelitian

Tahapan penelitian ini membutuhkan perangkat keras dan perangkat lunak. Adapun perangkat keras dan perangkat lunak yang digunakan untuk penelitian ini adalah sebagai berikut:

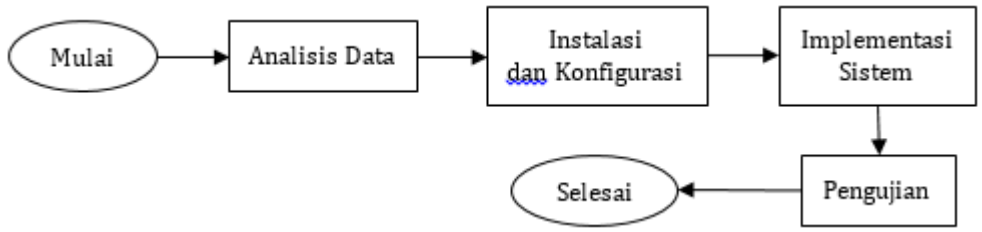
a. Perangkat Keras
   - Raspberry Pi 3 model B+ dengan memori 16GB, *RAM* 1GB dan Sistem Operasi Raspbian Buster untuk Raspberry Pi 3.
   - Power Adapator 5V 2A.

- *Keyboard*
- *Mouse*
- HDMI
- Layar
- Laptop dengan spesifikasi processor (Intel (R) Core(TM) i3 CPU M370 @2.40GHz RAM 4.00GB).
- *Handphone* dengan spesifikasi memori 32GB, *RAM* 3GB, Sistem Operasi Android 9 Pie.

b. Perangkat Lunak
- Nmap
- Hydra dan Medusa
- Putty
- Raspbian OS dan Kali Linux 2020.1

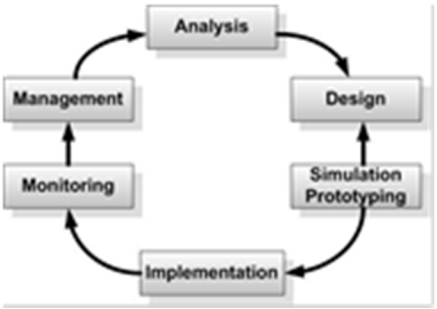
Prosedur Penelitian

Serangkaian kegiatan pada penelitian yang dilakukan secara teratur dan sistematis untuk mencapai tujuan penelitian ditunjukkan pada Gambar 1.



Gambar 1. Prosedur Penelitian

Gambar 1 merupakan prosedur penelitian yang dilakukan pada penelitian ini. Berdasarkan Gambar 1 prosedur penelitian dimulai dengan melakukan analisis data, yaitu proses pengumpulan data mulai dari proses wawancara dan *survey,* bahan penelitian sampai peralatan penelitian yang digunakan. Kemudian proses instalasi dan konfigurasi yang merupakan tahap instalasi dan konfigurasi alat dan bahan yang digunakan pada raspberry pi. Kemudian melakukan implementasi sistem pada *server* setelah instalasi dan konfigurasi dilakukan pada tahap sebelumnya. Selanjutnya melakukan pengujian pada sistem yang telah dibangun pada *server* raspberry pi. Pada penelitian ini menggunakan metode *Network Development Life Cycle (NDLC).* Metode *NDLC* dipilih karena pengembangan sistem bergantung pada penelitian sebelumnya dan merupakan teknik analisis terstruktur yang digunakan untuk merancang dan mengelola proses pembangunan sistem. *NDLC* memiliki beberapa tahapan, di antaranya: *analysis, design, simulation prototyping, implementation, monitoring* dan *management.*



Gambar 2. Metode *NDLC*

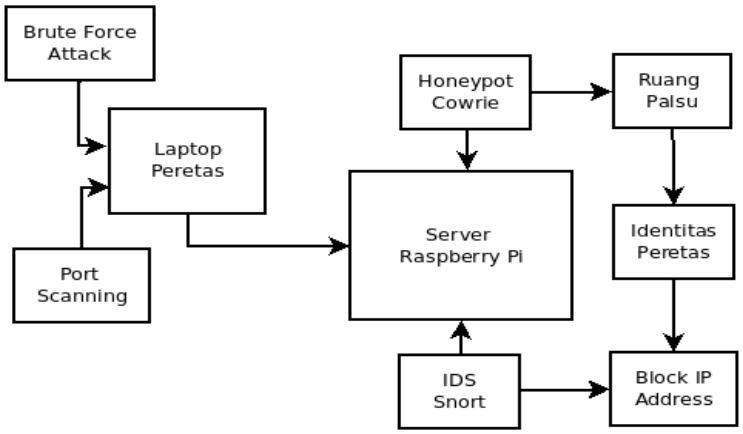
Gambar 2 merupakan metode *NDLC* yang digunakan pada penelitian ini. Berdasarkan Gambar 2 tahapan dari metode *NDLC* dimulai dengan *analysis,* tahap ini peneliti melakukan analisis kebutuhan dan permasalahan yang ada pada sistem *server* dengan cara melakukan

ISSN Cetak : 2622-1276
ISSN Online : 2622-1284

wawancara dan *survey* ke tempat permasalahan sistem *server* secara langsung. Tahap kedua yang dilakukan adalah *design,* tahap *design* peneliti membuat topologi jaringan *server* yang sudah ada sebelumnya, kemudian dibangun sistem keamanan *server* yang baru. Tahap ketiga dari metode *NDLC* adalah *simulation prototyping,* tahap ini peneliti membangun topologi jaringan *server* pada sistem keamanan yang baru menggunakan *software cisco packet tracer* untuk simulasi jaringan yang telah dibangun. Tahap keempat yang dilakukan adalah *implementation*, tahap ini peneliti menerapkan sistem keamanan *server* baru yang telah dibangun yang dapat memberikan pengaruh dan hasil yang berbeda dari sistem sebelumnya. Tahap kelima yang dilakukan adalah *monitoring,* tahap ini peneliti melakukan *monitoring* terhadap sistem keamanan *server* baru yang bertujuan untuk memastikan sistem yang telah dibangun berjalan dengan baik. Tahap keenam dari metode ini adalah *management*, tahap ini peneliti membuat aturan pemeliharaan dan perawatan sistem keamanan baru supaya sistem keamanan dapat berlangsung lama dan berjalan dengan baik.

Proses Pengujian

Proses pengujian pada penelitian ini melakukan uji serangan menggunakan dua teknik serangan dan satu tahap memblokir *ip address* peretas.



Gambar 3. Proses Pengujian

Gambar 3 merupakan proses pengujian yang dilakukan pada penelitian ini. Berdasarkan Gambar 3 proses pengujian dimulai dengan melakukan teknik serangan *port scanning* menggunakan *tools nmap* yang bertujuan untuk mendapatkan kumpulan informasi penting yang ada pada suatu jaringan, di antaranya yaitu *port* 22 *ssh (secure shell).* Tahap selanjutnya yaitu melakukan serangan dengan teknik *bruteforce attack* menggunakan *tools hydra* dan *medusa* yang bertujuan untuk mendapatkan kombinasi *username* dan *password* sistem *server* sercara ilegal. Selanjutnya setelah peretas melakukan serangan menggunakan dua teknik tersebut, *server* raspberry pi yang sudah dibangun sistem keamanan *honeypot cowrie* dan *IDS snort* dapat mendeteksi adanya serangan yang masuk kedalam sistem *server, honeypot cowrie* menjebak peretas menggunakan ruang atau *server* palsu yang telah dibuat, kemudian setelah identitas dan aktifitas peretas terekam dan terdeteksi oleh *honeypot cowrie, IDS snort* dapat memblokir identitas peretas dan dapat menahan paket serangan yang masuk kedalam sistem *server* yang dilakukan oleh peretas.

HASIL DAN PEMBAHASAN

Persiapan Data

Data yang digunakan adalah data dari latop peretas sebagai *attacker* dan mini *server* raspberry pi yang akan diuji sistem keamanannya. Adapun data tersebut ditunjukkan pada Tabel 1.

Tabel 1. Data Laptop Peretas

No	Nama	Keterangan
1	IP Address	192.168.43.120
2	Subnet Mask	255.255.255.0
3	Default Gateway	192.168.43.1
4	Network Band	2.4 GHz

Penelitian ini menggunakan data laptop peretas dengan empat variabel. Data dirangkum pada Tabel 1 dengan data pertama adalah *ip address* peretas, data kedua adalah *subnet mask*, data ketiga adalah *default gateway* dan data keempat adalah *network band*.

Tabel 2. Data Mini *Server* Raspberry Pi

No	Nama	Keterangan
1	IP Address	192.168.43.59
2	Subnet Mask	255.255.255.0
3	Default Gateway	192.168.43.1
4	Broadcast Address	192.168.43.255
5	*Port*	22

Penelitian ini menggunakan data mini *server* raspberry pi dengan lima variabel. Data dirangkum pada Tabel 2 dengan data pertama adalah *ip address,* data kedua adalah *subnet mask,* data ketiga adalah *default gateway,* data keempat adalah *broadcast address* dan data kelima adalah *port*.

Instalasi dan Konfigurasi

Setelah persiapan data selesai, selanjutnya adalah instalasi dan konfigurasi tools yang digunakan pada mini server raspberry pi.

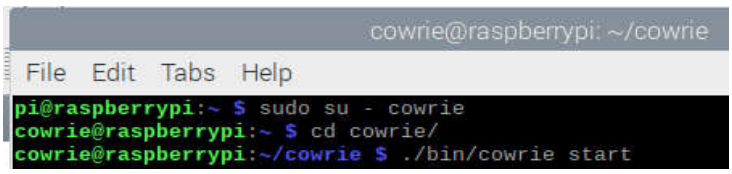
1. Instalasi
   a. Instal sistem operasi raspbian buster 10 pada raspberry pi 3
   b. Instal sistem operasi kali linux 2020.1 pada laptop
   c. Instal *cowrie* pada pada mini *server* raspberry pi 3
   d. Instal *snort* pada mini *server* raspberry pi 3
   e. Instal *kippo graph* pada mini *server* raspberry pi 3
2. Konfigurasi
   a. Konfigurasi *cowrie* sebagai *honeypot* pada mini *server* raspberry pi 3
   b. Konfigurasi *snort* sebagai *IDS* pada mini *server* raspberry pi 3
   c. Konfigurasi *kippo graph* sebagai *web dashboard monitoring* pada mini *server* raspberry pi 3

Implementasi

Setelah tahap instalasi dan konfigurasi dilakukan, selanjutnya adalah mengimplementasikan sistem yang telah di instal dan dikonfigurasi untuk dilakukan pengujian.

1. *Honeypot Cowrie*

   Tahap ini yaitu menjalankan *cowrie* sebagai *honeypot* sebelum peretas melakukan penyerangan terhadap *server*, supaya peretas atau *attacker* dapat terjebak oleh *server* palsu yang dibuat oleh *honeypot cowrie*. Menjalankan *honeypot cowrie* dapat menggunakan perintah yang ditunjukkan pada Gambar 4.



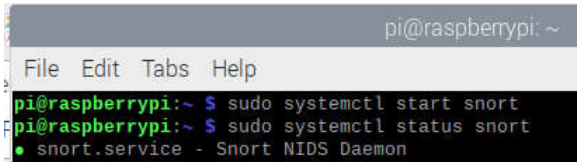
Gambar 4. Perintah *Cowrie Start*

ISSN Cetak : 2622-1276
ISSN Online : 2622-1284

Gambar 4 merupakan perintah untuk menjalakan *honeypot cowrie*. Berdasarkan Gambar 3 tahap pertama untuk menjalankan *honeypot cowrie* adalah dengan cara masuk kedalam *user root cowrie* dengan perintah *sudo su – cowrie,* kemudian masuk kedalam *folder cowrie* dengan perintah *cd cowrie/,* selanjutnya untuk menjalakan *honeypot cowrie* dengan menggunakan perintah *./bin/cowrie start*. Maka *honeypot cowrie* dapat berjalan dengan baik menggunakan perintah tersebut.

2. *IDS Snort*

Tahap ini yaitu menjalan *snort* sebagai *IDS,* supaya aktifitas dan identitas peretas dapat terekam dan tersimpan tanpa sepengetahuan peretas tersebut. Menjalakan *IDS snort* dapat menggunakan perintah seperti yang ditunjukkan pada Gambar 5.



Gambar 5. Perintah *Snort Start*

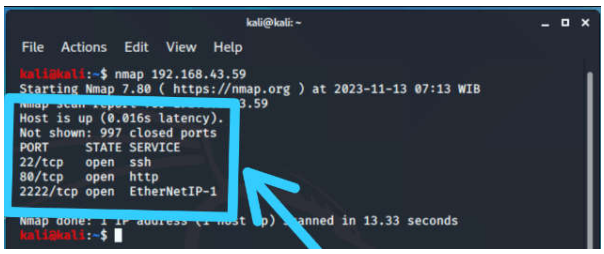
Gambar 5 merupakan perintah untuk menjalankan *IDS snort.* Berdasarkan Gambar 3 tahap pertama untuk menjalakan *IDS snort* adalah dengan cara *sudo systemctl start snort.* Kemudian untuk memastikan *IDS snort* berjalan atau tidak dapat menggunakan perintah *sudo systemctl* status snort. Maka status *IDS snort* dapat terlihat sedang berjalan atau tidak.

Pengujian

Tahap pengujian dilakukan dengan melakukan dua teknik serangan terhadap mini *server* raspberry pi yang sudah dilakukan tahap instalasi dan konfigurasi pada sistem keamanannya. Dua teknik serangan tersebut yaitu teknik serangan *port scanning* dan *bruteforce attack*, kemudian dilakukan blokir *ip address* peretas.

1. Teknik serangan *Port Scanning*

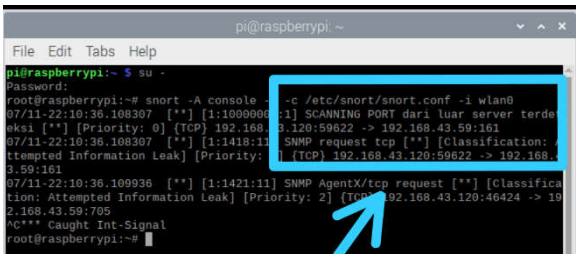
Teknik serangan dengan *port scanning* ini bertujuan untuk mendapatkan kumpulan informasi penting yang ada pada suatu jaringan dan untuk mendeteksi *port* berapa saja yang terbuka pada server utama target. Proses serangan dengan teknik *port scanning* menggunakan tools nmap ditunjukkan pada Gambar 6



Gambar 6. Hasil *Port Scanning*

Gambar 6 merupakan hasil serangan dengan teknik *port scanning*. Berdasarkan Gambar 6 serangan dengan menggunakan teknik *port scanning* dapat menghasilkan informasi penting yang ada pada suatu jaringan yaitu *port* 22/tcp, *port* 80/tcp dan *port* 2222/tcp dengan status terbuka. Hasil pengujian dari teknik serangan *port scanning* dapat mendeteksi *port* berapa saja yang terbuka, di antaranya *port* 22 yaitu *ssh* yang terbuka, *port* yang terbuka tersebut dapat membuka kesempatan bagi peretas untuk menyerang lebih lanjut terhadapt *server* melalui *port* 22 *ssh*. *Server* yang diserang oleh peretas tersebut sebelumnya sudah dilakukan instalasi dan konfigurasi *honeypot cowrie*

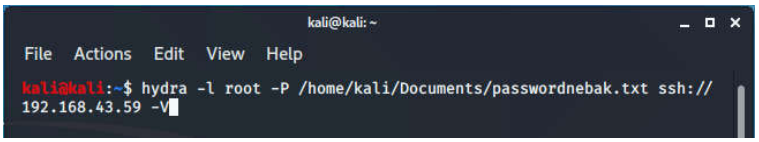
dan *IDS snort*, sehingga *server* utama akan meneruskan permintaan *port* 22 ke *server* palsu *honeypot cowrie* dan *IDS snort* mendeteksi adanya serangan yang berasal dari *server* utama yang di akses oleh peretas.



Gambar 7. *Snort* Mendeteksi Adanya Serangan

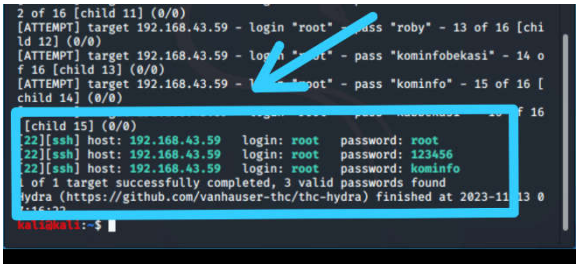
Gambar 7 merupakan serangan yang masuk kedalam sistem *server* yang terdeteksi oleh *IDS snort.* Berdasarkan Gambar 7 *IDS snort* dapat mendeteksi adanya serangan yang masuk kedalam sistem *server* dengan menggunakan perintah *snort -A console -q -c /etc/snort/snort.conf -I wlan0.*

2. Teknik serangan *Bruteforce Attack*
Pengujian dengan tenik serangan *bruteforce attack* bertujuan untuk mendapatkan kombinasi *username* dan *password* sistem *server* menggunakan *wordlist* yang telah dibuat sebelumnya oleh peretas dan untuk masuk kedalam sistem *server* secara tidak sah atau secara ilegal. *Tools* yang digunakan untuk melakukan *bruteforce attack* yaitu *hydra* dan *medusa.* Serangan dengan *tools hydra* dapat menggunakan perintah seperti pada Gambar 8.



Gambar 8. Perintah *Input Tools Hydra*

Gambar 8 merupakan perintah *input* untuk menjalakan *tools hydra*. Berdasarkan Gambar 8 perintah *input* yang digunakan adalah *hydra* untuk menjalankan *tools hydra,* kemudian *-l root* untuk *login* menggunakan *user root, -P /home/kali/Document/passwordnebak.txt* perintah untuk mencari *password* yang dibuat didalam *folder* tersebut, kemudian perintah *ssh://192.168.43.59* digunakan untuk menyerang *host* tersebut dengan *module ssh(secure shell),* selanjutnya *-V* digunakan untuk menampilkan kombinasi *password* hasil serangan menggunakan *tools hydra*. Setelah perintah *input* dilakukan, maka proses *bruteforce attack* dapat berjalan sampai *wordlist* menemukan kombinasi *username* dan *password* yang ada pada sistem *server* target. Hasil dari serangan *bruteforce attack* menggunakan *tools hydra* dapat dilihat pada Gambar 9.

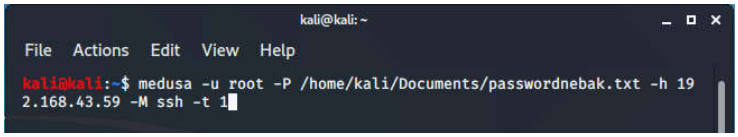


Gambar 9. Hasil Serangan *Bruteforce Attack Hydra*

Gambar 9 merupakan hasil serangan menggunakan teknik serangan *bruteforce attack* dengan *tools hydra*. Hasil pengujian dengan menggunakan teknik serangan *bruteforce attack* dapat menampilkan kombinasi *username* dan *password* yang ada pada

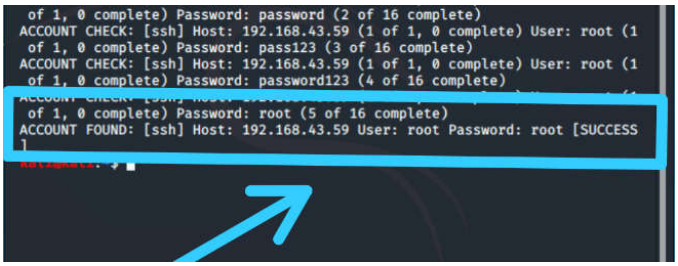
ISSN Cetak : 2622-1276
ISSN Online : 2622-1284

sistem *server*. Setelah *username* dan *password server* didapatkan, maka peretas dapat *login* kedalam *server* target tersebut. Adapun kombinasi *username* dan *password* yang didapatkan oleh peretas tersebut merupakan *username* dan *password* palsu yang dibuat oleh *honeypot cowrie* untuk menjebak peretas, sehingga peretas dapat masuk dan terjebak kedalam *server* palsu tersebut. Serangan dengan *tools medusa* menggunakan perintah yang ditunjukkan pada Gambar 10.



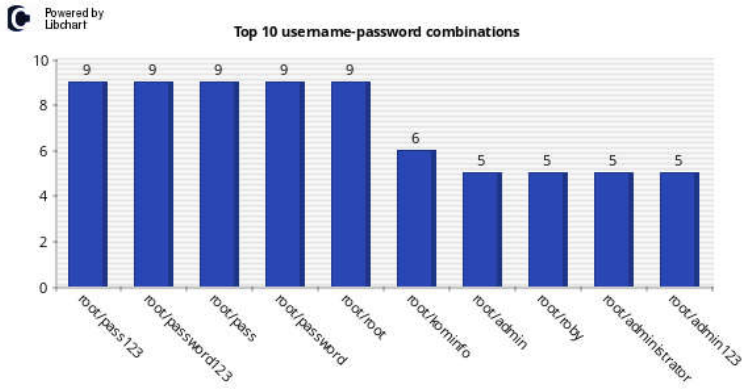
Gambar 10 Perintah *Input Tools Medusa*

Gambar 10 merupakan perintah *input* untuk menjalankan *tools medusa*. Berdasarkan Gambar 10 perintah *input* yang digunakan adalah *medusa* untuk mejalankan *tools medusa*, kemudian *-u root* untuk *login* menggunakan *user root,* selanjutnya *-P /home/kali/Document/passwordnebak.txt* adalah perintah untuk mencari *password* yang dibuat didalam *folder* tersebut. Kemudian perintah -h 192.168.43.59 digunakan untuk menyerang *host* tersebut, perintah -M ssh digunakan untuk menggunakan *module ssh ,* dan perintah *-t 1* digunakan untuk melakukan serangan sebanyak satu kali. Setelah perintah *input* dilakukan, maka proses serangan dapat berjalan sampai *tools medusa* mendapatkan kombinasi *username* dan *password* yang ada pada sistem *server* target. Hasil dari serangan *bruteforce attack* menggunakan *tools medusa* dapat dilihat pada Gambar 11.



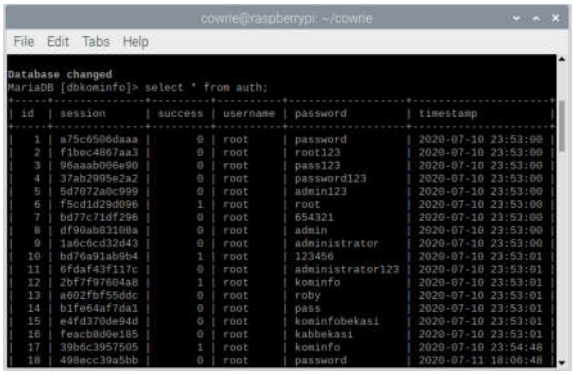
Gambar 11. Hasil Serangan *Bruteforce Attack Medusa*

Gambar 11 merupakan hasil serangan menggunakan teknik *bruteforce attack* dengan *tools medusa*. Hasil pengujian dengan teknik serangan *bruteforce attack* menggunakan *tools medusa* hampir sama dengan *tools hydra*, perbedaan dari *tools medusa* tersebut hanya dapat menampilkan satu kombinasi *username* dan *password* yang ada pada sistem *server* target dan *tools medusa* tidak dapat menyelesaikan semua kombinasi *username* dan *password* yang ada *wordlist*.



Gambar 12 *Log* Serangan *Bruteforce Attack* Pada *Web Dashboard Monitoring Kippo Graph*

Gambar 12 merupakan *log* serangan dengan menggunakan teknik *bruteforce attack* yang dilakukan oleh peretas. *Log* serangan tersebut dapat lihat pada *web dashboard monitoring kippo graph* yang sebelumnya sudah diinstal dan dikonfigurasi pada mini *server* raspberry pi.



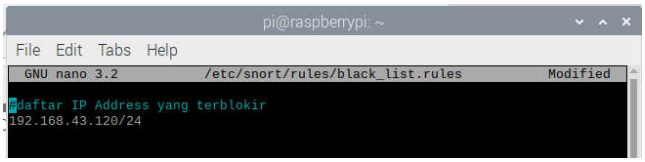
id	session	success	username	password	timestamp
1	a75c6506daaa	0	root	password	2020-07-10 23:53:00
2	f1bec4867aa3	0	root	root123	2020-07-10 23:53:00
3	96aaab066e90	0	root	pass123	2020-07-10 23:53:00
4	37ab2905e2a2	0	root	password123	2020-07-10 23:53:00
5	5d7072a0c999	0	root	admin123	2020-07-10 23:53:00
6	f5cd1d29d096	1	root	root	2020-07-10 23:53:00
7	bd77c71df296	0	root	654321	2020-07-10 23:53:00
8	df90ab83108a	0	root	admin	2020-07-10 23:53:00
9	1a6c6cd32d43	0	root	administrator	2020-07-10 23:53:00
10	bd76a91ab9b4	1	root	123456	2020-07-10 23:53:01
11	6fdaf43f117c	0	root	administrator123	2020-07-10 23:53:01
12	2bf7f97604a8	1	root	kominfo	2020-07-10 23:53:01
13	a602fbf55ddc	0	root	roby	2020-07-10 23:53:01
14	b1fe64af7da1	0	root	pass	2020-07-10 23:53:01
15	e4fd370de94d	0	root	kominfobekasi	2020-07-10 23:53:01
16	feacb8d0e185	0	root	kabbekasi	2020-07-10 23:53:01
17	39b6c3957505	1	root	kominfo	2020-07-10 23:54:48
18	498ecc39a5bb	0	root	password	2020-07-11 18:06:48

Gambar 13 *Log* Serangan *Bruteforce Attack* Pada *Database*

Gambar 13 merupakan *log* serangan yang dilakukan oleh peretas yang tersimpan didalam *database honeypot cowrie* sebelum ditampilkan ke *web dashboard monitroring kippo graph*.

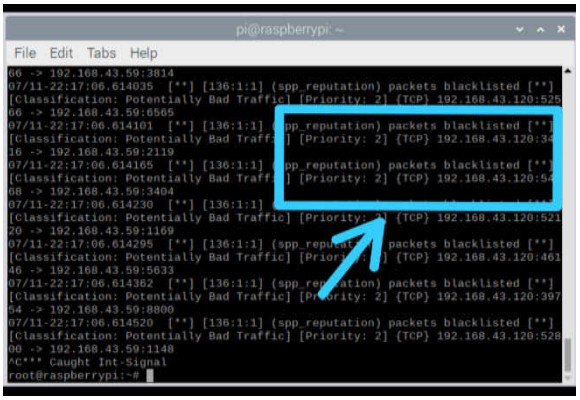
Block IP Address Peretas

Pengujian pada tahap ini yaitu melakukan *block ip address* peretas yang telah melakukan penyerangan terhadap *server* raspberry pi. Tahan memblokir *ip address* peretas yaitu hampir sama dengan melakukan teknik serangan *port scanning*, tapi sebelumnya identitas atau *ip address* peretas dimasukan terlebih dahulu kedalam *file black_list.rules* yang berada pada *IDS snort*.



Gambar 14 Daftar Blokir *IP Address* Peretas

Gambar 14 merupakan daftar *ip address* yang diblokir. Setelah proses memasukan identitas atau *ip address* peretas kedalam daftar blokir, maka ketika terjadi penyerangan kembali oleh peretas dengan *ip address* tersebut, *IDS snort* akan memblokir *ip address* tersebut dan notifikasi dari *local.rule* akan muncul kembali dengan peringatan bahwa *ip address* tersebut melakukan penyerangan kembali, namun *IDS snort* berhasil melakukan blokir *ip address* tersebut dan peretas tidak dapat melakukan penyerangan kembali. Notifikasi *snort* berhasil memblokir *ip address* peretas dapat dilihat pada Gambar 15.



Gambar 15. Snort Berhasil Memblokir *IP Address*

ISSN Cetak : 2622-1276
ISSN Online : 2622-1284

Gambar 15 menunjukan bahwa serangan yang masuk pada *server* raspberry pi yang dilakukan oleh peretas, IDS *snort* berhasil memblokir *ip address* tersebut dan menahan paket yang masuk supaya sistem *server* tidak terjadi *overload* atau *down*.

KESIMPULAN

Berdasarkan hasil pengujian dari semua jenis serangan yang dilakukan oleh peretas atau attacker dengan menggunakan teknik serangan bruteforce attack maupun teknik serangan dengan port scanning terhadap server raspberry pi dapat dengan mudah terdeteksi dan terlacak oleh honeypot cowrie dan IDS snort, kemudian indentitas dan aktifitas peretas tersebut disimpan dalam file log dan database server raspberry pi tanpa sepengetahuan peretas tersebut untuk ditindak lebih lanjut.

Saran untuk penelitian selanjutnya yaitu diharapkan bisa menggunakan metode pengembangan sistem selain network development life cycle dan menggunakan honeypot selain cowrie dan IDS selain snort untuk mengetahui hasil keamanan sistem yang berbeda dari penelitian ini.

UCAPAN TERIMA KASIH

Naskah ilmiah ini adalah sebagian dari penelitian Tugas Akhir milik Roby Rupiat yang dibimbing oleh Sutan Faisal dan Tohirin Al Mudzakir.

REFERENSI

[1] Cahyanto, T. A., (2015). BAUM-WELCH Algorithm Implementation For Knowing Data Characteristics Related Attacks On Web Server Log. Proceeding IC-ITECHS 2014, 1(01).

[2] Awalia, B. (2018). Keamanan Informasi. *Jakarta: Universitas Mercu Buana*.

[3] Marta, I. K. K. A., Hartawan, I. N. B., & Satwika, I. K. S. (2020). ANALISIS SISTEM MONITORING KEAMANAN SERVER DENGAN SMS ALERT BERBASIS SNORT. *INSERT: Information System and Emerging Technology Journal*, *1*(1), 25-40.

[4] Prabowo, M. A., Darusalam, U., & Ningsih, S. (2020). Perancangan Keamanan Server Linux Dengan Metode Hardening Pada Layer 1 dan Layer 7. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(3), 591-603.

[5] Santoso, J. (2019). Uji Kerentanan Keamanan Server Menggunakan Scada Shodan. *TEKNOKOM*, *2*(2), 1-4.

[6] Prasetyo, D. (2019). *PENERAPAN KEAMANAN JARINGAN DENGAN METODE HONEYPOT DALAM MENDETEKSI SERANGAN BRUTE FORCE PADA SERVER EQUAL PAYMENT* (Doctoral dissertation, Universitas Teknokrat Indonesia).

[7] Husain, M. S., Aksara, L. F., & Ransi, N. (2018). IMPLEMENTASI KEAMANAN SERVER PADA JARINGAN WIRELESS MENGGUNAKAN METODE INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)(STUDI KASUS: TECHNO'S STUDIO). *semanTIK*, *4*(2), 11-20.