Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 11, No. 5, Oktober 2025, hlm. 1173-1184 e-ISSN: 2528-6579

SISTEM DETEKSI DAN PENCEGAHAN SYSTEM ATTACK PADA INFRASTRUKTUR JARINGAN MENGGUNAKAN REALTIME HONEYPOT DAN AUTOMATIC IPTABLES

Hillman Akhyar Damanik*[1], Merry Anggraeni[2]

[1,2]Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan
Email: [1]hillman.akhyardamanik@budiluhur.ac.id, [2]merryanggraeni@budiluhur.ac.od
*Penulis Korespondensi

(Naskah masuk: 26 September 2024, diterima untuk diterbitkan: 30 Oktober 2025)

Abstrak

Seiring meningkatnya kompleksitas jaringan serta tingginya ketergantungan pada perangkat infrastruktur jaringan, serangan siber terhadap sistem yang terhubung langsung ke internet menjadi tantangan utama dalam pengelolaan keamanan infrastruktur. Eksploitasi pada protokol umum layanan publik seperti SSH, Telnet, SMB, dan FTP sering dimanfaatkan oleh aktor siber untuk menyusup ke sistem menggunakan kredensial lemah atau default. Penelitian ini mengusulkan pendekatan proaktif melalui pemanfaatan honeypot sebagai alat pendeteksi serangan dengan mengimplementasikan sistem yang rentan terhadap eksploitasi. Arsitektur pengujian dirancang dalam dua skenario, yaitu farm server pada virtual (vServer) dan perangkat router, yang masing-masing dilengkapi dengan honeypot jenis Cowrie, Dionaea, Honeytrap, Suricata, dan Mailoney. Serangkaian teknik analisis diterapkan, seperti *Statistical Traffic Analysis*, identifikasi layanan target dan protokol, pemantauan port SSH, deteksi intrusi berbasis jaringan (IDS), serta analisis sampel malware yang berhasil ditangkap. Data log yang dikumpulkan selama dua bulan mencerminkan aktivitas serangan yang cukup tinggi, dengan total catatan sebanyak 2.813.776 entri dari Cowrie, 2.109.900 dari Dionaea, 1.047.814 dari Honeytrap, dan 650.741 dari Suricata. Selain pemantauan serangan, penelitian ini juga mengembangkan mekanisme pertahanan dengan mengintegrasikan pemfilteran otomatis berbasis IPTables. Pendekatan ini terbukti mampu mengurangi beban kerja perangkat jaringan, dengan efisiensi hingga 45% (CPU dan Memory) pada perangkat Router dan sekitar 40% (CPU dan Memory) pada Server Farm. Hasil penelitian ini menunjukkan bahwa penggabungan berbagai jenis honeypot dengan dukungan otomasi mitigasi berbasis filtering firewall iptables mampu meningkatkan deteksi dini dan memperkuat ketahanan jaringan terhadap serangan dari internet.

Kata kunci: *Honeypot, IPtables, Firewall IPSet, Firewall Automation, Malware*

DETECTION AND PREVENTION SYSTEM ATTACK ON NETWORK INFRASTRUCTURE USING REALTIME HONEYPOT AND AUTOMATIC IPTABLES

Abstract

As the complexity of networks increases and the high dependence on network infrastructure devices, cyber attacks on systems directly connected to the internet become a major challenge in managing infrastructure security. Exploits on common public service protocols such as SSH, Telnet, SMB, and FTP are often used by cyber actors to infiltrate systems using weak or default credentials. This study proposes a proactive approach through the use of honeypots as an attack detection tool by implementing a system that is vulnerable to exploitation. The testing architecture is designed in two scenarios, namely a virtual server farm (vServer) and a router device, each equipped with a honeypot type Cowrie, Dionaea, Honeytrap, Suricata, and Mailoney. A series of analysis techniques are applied, such as Statistical Traffic Analysis, identification of target services and protocols, SSH port monitoring, network-based intrusion detection (IDS), and analysis of successfully captured malware samples. The log data collected over two months reflects quite high attack activity, with a total of 2,813,776 entries from Cowrie, 2,109,900 from Dionaea, 1,047,814 from Honeytrap, and 650,741 from Suricata. In addition to monitoring attacks, this study also developed a defense mechanism by integrating IPTables-based automatic filtering. This approach has been proven to be able to reduce the workload of network devices, with an efficiency of up to 45% (CPU and Memory) on Router devices and around 40% (CPU and Memory) on Server Farms. The results of this study indicate that combining various types of honeypots with the support of iptables firewall filtering-based mitigation automation can improve early detection and strengthen network resilience against attacks from the internet.

Keywords: *Honeypot, IPtables, Firewall IPSet, Firewall Automation, Malware*

1. PENDAHULUAN

Infrastruktur jaringan pada organisasi atau perusahaan menjadi salah satu lingkungan internet yang paling populer saat ini, termasuk perangkat router dan server (Damanik, Anggraeni and Nusantari, 2023). Saat ini layanan yang terhubung langsung dengan internet seperti infrastruktur jaringan cloud menyimpan data pelanggannya pada infrastuktur jaringan penyedia (service provider) (Fraunholz et al., 2017) (Damanik, 2022). Kerentanan dan ancaman pada perangkat router dan server yang terdapat di global internet dapat mempengaruhi jutaan kerusakan pada perangkat pengguna atau pelanggan (Damanik and Anggraeni, 2024). Oleh karena itu, service provider memiliki tanggung jawab untuk melindungi infrastruktur pelanggannya dengan cara terbaik, tetapi mereka juga harus mematuhi banyak persyaratan hukum mengenai perlindungan data dan privasi yang diterapakan (Polyakov and Lapin, 2018) (Sokol, Husák and Lipták, 2015).

Honeypot telah digunakan secara luas untuk meneliti lalu lintas jaringan, dari serangan global internet. Saat ini banyak penelitian dan penerapan yang dilakukan dengan perangkat lunak honeypot, yang beroperasi pada perangkat keras fisik dan pada konektivitas gateway internet. Router mikrotik adalah contoh khusus dari router, yang digunakan untuk menyediakan akses last mile dan core router ke pelanggan seperti, *Small Office Home Office* (SOHO), perusahaan dan service provider, yang biasanya digunakan dalam infrastruktur jaringan inti, penelitian ini dilakukan dengan perangkat router mikrotik dengan menajemen terpusat dan pemantauan dengan honeypot (Ceron and Scholten, 2020). Sistem manajemen teknologi terpusat, pada infrastruktur jaringan server, yang disebut Puppet, digunakan untuk mengimplementasikan solusi honeypot otomatis, dan diterapkan dalam penelitian ini (Samu, 2016). Penelitian ini merancang dan mengimplementasikan sistem Honeynet untuk mendeteksi dan mencegah serangan system layanan Apache Webserver, MySQL, FTP dan SMTP. Hasil penelitian ini digunakan untuk mengumpulkan informasi yang menghasilkan tentang alamat IP sumber, negara, dan timestamp waktu penyerang. Saikawa (Saikawa and Klyuev, 2019) menerapkan Dionaea honeypot yang diinstal pada infrastruktur server cloud, yang disebut Sakura untuk menganalisis informasi serangan, memahami trend serangan saat ini dalam mekanisme serangan di segmen jaringan Jepang, dan menguji mekanisme yang mencegah deteksi Honeypot. Hasil yang diperoleh beberapa Honeypots yang diterapkan membantu untuk meningkatkan teknologi keamanan. Modern Honey Network (MHN) yang dikembangkan menggunakan honeypot Kippo, Glastopf, Dionaea, dengan pengujian sistem honeypot, untuk pemantauan serangan intrusive, dengan kesimpulan dari penelitian ini, sistem honeypot berhasil mengecoh penyerang dengan membuka port pada server dan mengubah port menjadi dummy. Selain itu, aktivitas mencurigakan dicatat untuk setiap serangan (Wafi et al., 2017). Dari beberapa penelitian sebelumnya pada honeypot yang diterapkan hanya menganalisis serangan yang terjadi pada perangkat router (Ceron and Scholten, 2020), server dan pada protocol TCP/UDP (Samu, 2016; Wafi et al., 2017; Saikawa and Klyuev, 2019) tanpa melakukan pencegahan berupa firewall. Ceron (Ceron and Scholten, 2020) pada penelitiannya secara otomatis hanya mengklasifikasikan dan menilai serangan yang disesuaikan pada perangkat MikroTik. Samu (Samu, 2016) dalam penelitiannya menggunakan honeynet untuk mendeteksi dan mencegah serangan dengan menganalisi bukti peretasan hanya pada perangkat virtual Server. Saikawa (Saikawa and Klyuev, 2019) menggunakan dionaea honeypot yang dipasang di Sakura cloud untuk men-*cache* akses berbahaya, menganalisis informasi serangan, memahami gejala dalam mekanisme serangan di segmen jaringan Jepang. Pada penelitian Modern Honey Network (MHN) hanya menggunakan honeypots Kippo, Glastopf, Dionaea pada perangkat server untuk mencatat hasil dari serangan (Wafi et al., 2017).

Sebagian besar penelitian yang telah dilakukan hanya berfokus pada analisis, klasifikasi serangan tanpa pendekatan mitigasi atau automasi penanggulangan berbasis firewall. Oleh karena itu, diperlukan pendekatan otomatisasi dalam pengelolaan kebijakan firewall, untuk mengurangi beban sumber daya perangkat dan meningkatkan respons terhadap serangan yang terdeteksi. Automasi IPTables memungkinkan sistem untuk secara langsung menghasilkan dan menerapkan aturan mitigasi berbasis data log serangan.

Makalah ini bertujuan untuk mengkaji teknologi honeypot sebagai bagian dari sistem deteksi intrusi, dengan menerapkan pemantauan berbasis visualisasi data menggunakan T-Pot Honeypot. Fokus kajian ini mencakup pemahaman lanskap ancaman terhadap perangkat infrastruktur jaringan, router dan server, yang terhubung langsung ke jaringan internet, serta upaya mitigasi yang dilakukan. Pengembangan sistem dalam penelitian ini dirancang untuk menghasilkan pemantauan berupa analisis statistik lalu lintas jaringan, identifikasi target layanan pada protokol SSH, sistem deteksi intrusi berbasis jaringan IDS dan analisis sampel malware yang berhasil ditangkap. Data yang diperoleh dari log masing-masing honeypot T-Pot akan diklasifikasikan pada iptables dan digunakan untuk membentuk aturan mitigasi secara otomatis melalui pemrograman shell script.

2. METODE PENELITIAN

Penelitian ini menggabungkan pendekatan eksperimen dengan memanfaatkan Honeypot T-Pot sebagai sistem deteksi dini terhadap serangan siber dari publik internet, dan IPTables filtering sebagai sistem mitigasi otomatis terhadap IP penyerang. Dataset dikumpulkan dari log *cowrie*, *dionaea*, *honeytrap*, *suricata*, dan *mailoney* dan kemudian dianalisis melalui proses ekstraksi dan agregasi menggunakan *logstash* dan *elasticsearch*. Informasi serangan berupa IP *address* sumber, jenis protokol, kredensial, dan negara asal penyerang digunakan sebagai dasar untuk membuat kebijakan firewall dinamis berbasis IPSet. Teknik mitigasi dengan filtering iptables dilakukan dalam dua pendekatan: pemblokiran IP public hasil log honeypot dan pemblokiran rentang IP berdasarkan negara dengan referensi zona.

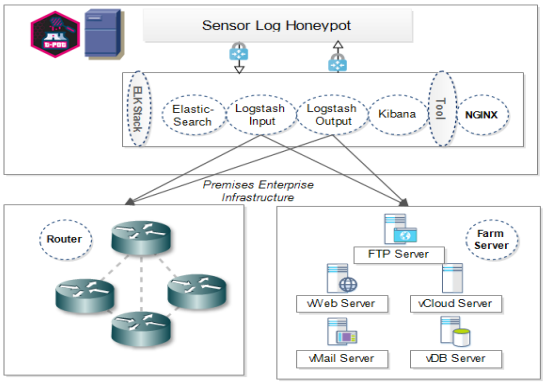
2.1. Pengumpulan Data Serangan melalui Honeypot

Tahap awal dilakukan dengan mengaktifkan honeypot sebagai sumber data utama. Data serangan direkam dan dikirimkan oleh sensor honeypot melalui logstash ke database elasticsearch. Teknik pengumpulan data dilakukan dengan menyaring entri berdasarkan serangan berupa IP *address* sumber, jenis protokol, kredensial, dan negara asal penyerang. Logstash berperan penting dalam membaca log, memfilter, dan menambahkan informasi tambahan GeoIP, serta mengubah format timestamp. Output log akan dikirimkan ke Elasticsearch agar dapat dianalisis lebih lanjut menggunakan Kibana.

2.2. Arsitektur Arsitektur Sistem dan Rangkaian Analisis Honeypot

Tahap ini dilakukan untuk mengekstrak informasi dari dataset honeypot *cowrie*, *dionaea*, *honeytrap*, *suricata*, dan *mailoney*. Bagian ini berisi hasil dari statistik kemudian membandingkan honeypot sensor yang berbeda pada dan dibagi menjadi empat kategori, pertama, teknik analisa statistic trafik, yaitu dengan menganalisis koneksi dan permintaan (*request*) pada network layer (L3). Kedua, target layanan dan protokol, dengan kriteria ini dapat menunjukkan layanan dan *protokol* mana yang ditargetkan. ketiga, layanan SSH port, teknik ini berfokus pada sesi terminal dan command line. Keempat, *Network Based Intrusion Detection System* (IDS), dan Kelima, Teknik *Infection Malware Sample Analysis* yang mendominasi pada serangan yang dilakukan, khususnya bagaimana perangkat dapat terinfeksi.

Sebagai bagian dari proses analisis data serangan, sistem akan menggunakan *logstash* untuk menangani log mentah yang dikumpulkan dari honeypot. Logstash disesuaikan agar dapat membaca sumber log tertentu, melakukan konversi format waktu (*timestamp*), serta memetakan sumber IP *address* penyerang dengan dataset GeoIP guna mengetahui lokasi geografis asal serangan. Setelah proses tersebut, data yang telah diproses selanjutnya disimpan ke dalam elasticsearch, sebagai repositori untuk memudahkan pencarian dan penyusunan informasi. Analisis yang dilakukan untuk memahami karakteristik serangan berbasis malware, dilakukan dengan VirusTotal. Seluruh rangkaian ini dilustrasikan seperti gambar 1. Selama eksperimen berlangsung, semua proses tersebut dijalankan secara bersamaan, memungkinkan sistem honeypot memberikan pemantauan serta analisis serangan secara langsung (*real-time*).



Gambar 1. Architecture with Elasticsearch, Logstash and Kibana interaction

2.3. Sistem Mitigasi Otomatis Berbasis IPSet

Eksperimen ini bertujuan untuk implementasi sistem mitigasi otomatis *ipset* dengan memanfaatkan log hasil pengamatan serangan dari T-Pot Honeypot. Permasalahan utama yang ingin diatasi pada keterbatasan sistem honeypot yang hanya melakukan perekaman dan klasifikasi serangan tanpa adanya upaya mitigasi aktif terhadap sumber serangan yang teridentifikasi dengan *filtering* yang iterasi *ipset file* dan *ipset block countries*.

1. *IPSet File*

Sebagai bagian dari strategi otomatisasi, digunakan fitur ipset untuk mendukung efisiensi dalam pengelolaan daftar alamat IP penyerang. ipset memungkinkan manipulasi *set* IP secara dinamis, tanpa perlu menambah aturan IPTables satu per satu. Firewall ipset merupakan parameter ipset yang diterapkan, untuk ekstensi target yang menyediakan mekanisme, dengan menambahkan dan menghapus entri yang ditetapkan secara dinamis berdasarkan aturan *iptables*. Skrip ipset akan melakukan entri, secara otomatis memblokir semua *ip address* yang dilist pada file data yang dihasilkan dari log honeypot, dengan baris skrip berikut.

```
#!/bin/bash
 echo "### BLOCKING ALL IPs AND NETWORKS
 FROM FILE."
 # File that contains the IPs and Nets to
 block
 FILE="honey_source_attacker.txt"
 ipset -N bad_hosts iphash -exist
 # Flushing the set if it exists
```

```
ipset -F bad_hosts
echo "Adding IPs from $FILE to bad_hosts
set:"
for ip in cat $FILE
do
ipset -A bad_hosts $ip
echo -n "$ip "
Done
echo -e -n "\nDropping with iptables... "
iptables -I INPUT -m set --match-set
bad_hosts src -j DROP
      echo "Done"
```

2. IPSet Block Countries

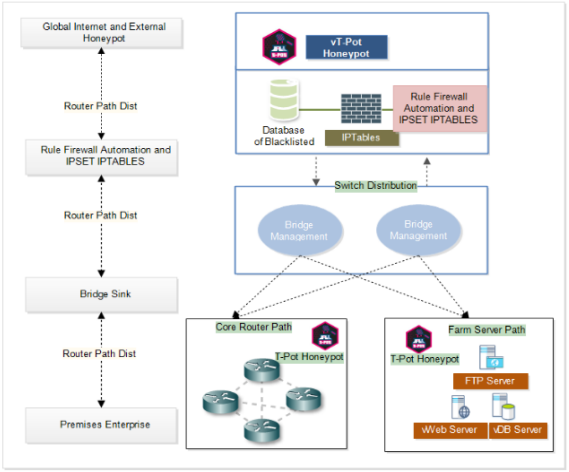
Skrip *block countries* ini digunakan untuk memperluas mekanisme mitigasi serangan dengan menambahkan pemblokiran terhadap rentang IP address berdasarkan negara asal serangan. Skrip ini adalah file zona IP address, dengan format CIDR untuk penerapannya. Pada list zona alamat ini, akan meminimalkan seperti f*loods* dan serangan *brute force*. Skrip ipset *block countries* akan melakukan entri secara otomatis, digunakan untuk memblokir semua *ip address* yang dilist pada file data yang dihasilkan, dari log honeypot.

```
echo "### BLOCKING Countries ###"
if [ -f "cn-aggregated.zone" ]
then
      rm cn-aggregated.zone
fi
wget
http://www.ipdeny.com/ipblocks/data/aggreg
ated/cn-aggregated.zone
if [ $? -eq 0]
then
echo ""
else
echo "
exit 1
fi
ipset -N countries hash:net -exist
ipset -F countries
echo "Adding Networks to set..."
for i in `cat cn-aggregated.zone`
do
ipset -A countries $i
done
echo -n "Blocking"
iptables -I INPUT -m set --match-set
countries src -j DROP
echo "Done"
```

3. HASIL DAN PEMBAHASAN

Arsitektur yang dimodelkan untuk sistem pengujian ditampilkan pada Gambar 2. Dimana pada topologi ini menunjukkan alur komunikasi dan distribusi data dalam lingkungan pengujian honeypot *cowrie, dionaea, honeytrap, suricata,* dan *mailoney*. Sistem yang dirancang ini bertujuan untuk menangkap, memfilter, dan menganalisis serangan yang berasal dari jaringan publik internet, melalui beberapa jalur distribusi router dan virtual server.

Dalam sistem ini, terdapat dua jalur utama untuk target serangan, yaitu *core router path* dan *farm server path* yang terhubung langsung dengan router inti jaringan untuk menangkap lalu lintas mencurigakan. Seluruh lalu lintas dari kedua jalur tersebut didistribusikan melalui manajemen switch dan dikendalikan dengan modul bridge management. Data yang terkumpul kemudian dianalisis dan digunakan untuk mengidentifikasi pola serangan, sumber IP penyerang, protocol dan potensi infeksi malware yang terjadi. Data dataset yang dihasilkan selanjutnya proses pemfilteran berbasis aturan firewall otomatis dan daftar hitam (*blacklist*) IP yang dikelola menggunakan IPSet.



Gambar 2. Topologi penerapan sistem honeypot dan firewall

Adapun jenis serangan yang akan dimonitoring, dan dievaluasi dalam 2 bulan dari internet, dengan pemantauan dan analisis serangan berupa sistem *logging*, *timestampt* yang digunakan untuk mengumpulkan informasi tentang alamat IP sumber, negara dan jenis malware yang mendominasi, serta layanan Telnet dan layanan SSH. Dari hasil dataset yang serangan akan diterapkan firewall iptables ipset dan *block countries* untuk menentukan aturan *permit* atau *deny* di infrastruktur jaringan yang dimodelkan. Penempatan honeypot, ditempatkan di depan gateway uplink internet, agar koneksi yang ditangkap oleh honeypot merupakan koneksi trafik murni tanpa adanya filter dari firewall. Pada infrastruktur Farm Server dan Router akan ditempatkan juga honeypot. Terdapat tiga virtual server dan 4 router MikroTik. Pemodelan eksperimen terdiri dari dua honeypots dan sistem tambahan untuk mengumpulkan *log* yang dihasilkan. Sistem berjalan dalam *instance* virtual yang *dihosting* menggunakan proxmox hypervisor dalam subnet yang sama. Ada lima virtual server dan network yang sama untuk dapat membandingkan

dengan benar hasil analisis di antara mereka pada layanan TCP dan UDP yang akan dihasilkan. Selain itu, honeypots mengirim mencatat data ke server internal honeypot.

3.1. Hasil Dataset Honeypot Berdasarkan Distribusi Serangan dan Sumber IP

Sebagai bagian dari pengujian sistem honeypot yang dilakukan dalam penelitian ini, tujuan utama adalah untuk memonitor dan mendeteksi berbagai aktivitas serangan siber terhadap layanan dan perangkat jaringan router dan vServer secara langsung. Pengumpulan data dilakukan secara menyeluruh untuk mengamati karakteristik, sumber, dan frekuensi serangan yang terjadi, dengan harapan dapat menjadi dasar dalam pengembangan strategi pencegahan dan respon terhadap insiden keamanan. Sistem honeypot yang digunakan mencakup beberapa jenis layanan *cowrie, dionaea, honeytrap, suricata,* dan *mailoney*, masing-masing dikonfigurasi untuk menangkap lalu lintas yang mencurigakan dan mencatat setiap interaksi dari serangan.

Hasil dataset pada honeypot menghasilkan 6.622.231 entri serangan. Hasil yang diperoleh sekitar 268.614 unik IP sumber, yang dinyatakan pada, statistik dari hasil layanan honeypot yang berbeda yang dihasilkan dan dikelompokkan.

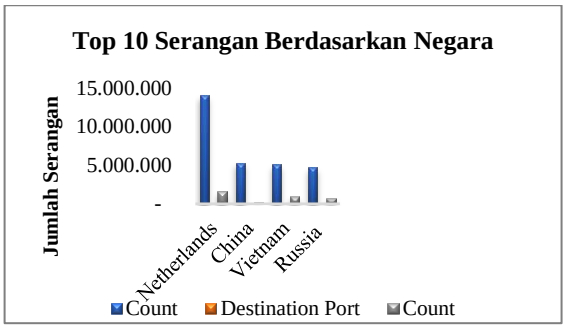
Tabel 1. Honeypot Attack Top 10

Honeypot Attack Top 10 Attacks Count			
Cowrie	**Dionaea**	**Honeytrap**	**Mailoney**
2.813.776	2.109.900	1.047.814	650.741

Dari seluruh dataset hasil serangan pada masing-masing honeypot yang dikumpulkan selama periode pengamatan, tercatat total 6.622.231 aktivitas serangan yang tergolong sebagai upaya serangan. Data ini berasal dari 268.614 IP *address* unik yang secara aktif melakukan koneksi terhadap sistem honeypot. Setiap jenis honeypot memberikan gambaran berbeda terkait jenis serangan yang ditangkap. Honeypot cowrie menjadi layanan yang paling banyak menerima serangan, dengan total 2.813.776 kejadian. Sementara itu, honeypot Dionaea berhasil mencatat 2.109.900 serangan, disusul oleh Honeytrap dengan 1.047.814 interaksi serangan, serta Mailoney yang mencatat 650.741 kejadian serangan.

3.2. Hasil Dataset Honeypot Berdasarkan Negara Penyerang

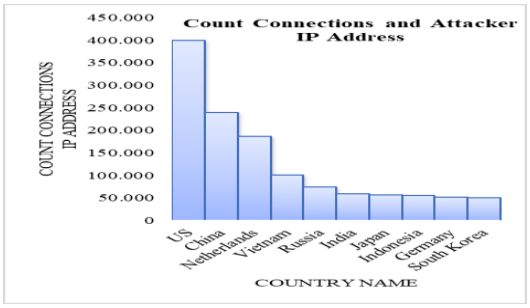
Tujuan selanjutnya dari hasil analisis adalah, mengetahui dari mana asal serangan tersebut berdasarkan negara. Hasil visualisasi dari data IP publik menunjukkan bahwa aktivitas penyerangan paling banyak berasal dari wilayah geografis tertentu. Empat negara yang paling sering terlibat dalam aktivitas serangan adalah Netherlands (Belanda), China (Tiongkok), Vietnam, dan Russia (Rusia) seperti pada gambar 4. Informasi ini diperoleh dari pemetaan IP Address yang dikaitkan dengan lokasi geografis menggunakan basis data GeoIP. Gambar 4 merupakan visualisasi lalu lintas berbahaya cenderung terpusat dari negara-negara dengan volume perangkat kompromi yang tinggi.



Gambar 4. Top 5 Serangan Berdasarkan Negara

Selain pengamatan dari distribusi berdasarkan negara, penting juga untuk melakukan pengamatan berdasarkan alamat IP tertentu yang secara konsisten melakukan koneksi dalam jumlah besar. Informasi ini digunakan untuk mengidentifikasi entitas atau bot yang aktif menyerang honeypot pada perangkat router dan vServer. Berdasarkan hasil pengamatan, alamat IP asal Amerika Serikat (US) mendominasi dengan total 399.422 koneksi, menempati peringkat teratas sebagai pelaku serangan pada honeypot. Negara-negara lain yang juga tercatat secara signifikan dalam data mencakup China, Belanda, Vietnam, dan Rusia, serta negara asia lainnya seperti India, Jepang, Indonesia, dan Korea Selatan.

Secara keseluruhan, lalu lintas berasal dari beberapa negara yang berbeda, namun hasil yang diperoleh dari sumber IP Address, ada sejumlah IP berdasarkan negara yang muncul lebih sering daripada yang lain seperti pada gambar 5.

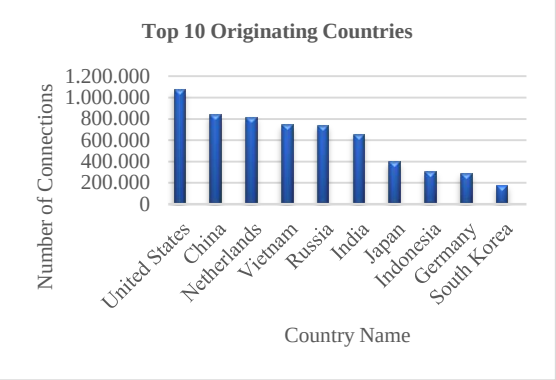


Gambar 5. IP Public penyerang dengan sebagian besar koneksi

Dari hasil temuan ini, dapat disimpulkan peran sistem monitoring jaringan berbasis honeypot sebagai langkah deteksi dini yang efektif. Kemudian

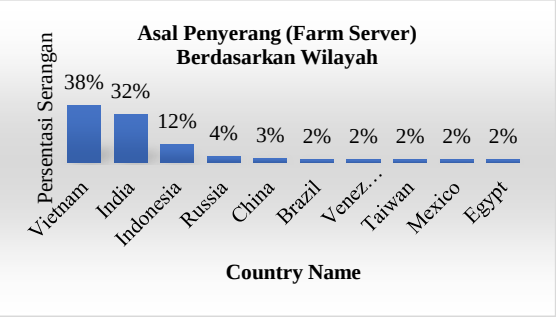
dari data berdasarkan serangan negara penyerang ini, akan dijadikan rujukan dalam pengembangan firewall *ipset* dinamis untuk kebijakan dari sistem keamanan pada perimeter jaringan.

Sebagai kelanjutan dari analisis terhadap sumber serangan berdasarkan IP *address*, diperoleh temuan signifikan mengenai asal negara pelaku. Berdasarkan visualisasi pada Gambar 6, IP *address* dengan jumlah koneksi tertinggi yang menargetkan perangkat router dan vServer tercatat berasal dari wilayah Amerika Serikat, dengan total serangan mencapai 399.422 koneksi. Pola serangan serupa juga teridentifikasi berasal dari beberapa negara lain yang menunjukkan frekuensi koneksi tinggi, antara lain Tiongkok, Belanda, Vietnam, Rusia, serta sejumlah negara di Asia dan Eropa seperti India, Jepang, Indonesia, Jerman, dan Korea Selatan. Dari hasil serangan ini, menunjukkan adanya distribusi serangan yang cukup luas dan tidak terpusat hanya pada satu kawasan geografis, sehingga menegaskan pentingnya pendekatan keamanan jaringan yang bersifat global dan adaptif.



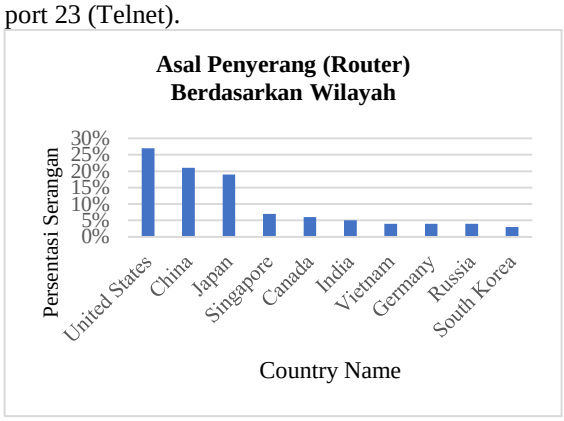
Gambar 6. Top 10 *originating countries*

Gambar 7 secara spesifik, berdasarkan hasil pemantauan terhadap aktivitas serangan yang diarahkan ke perangkat vServer dari implementasi honeypot, ditemukan bahwa sekitar 38% dari total upaya serangan berasal dari IP *address* yang teridentifikasi berlokasi di Vietnam. Persentase ini merupakan yang tertinggi dibandingkan negara lain dalam konteks penargetan terhadap IP publik yang telah dialokasikan pada vServer.



Gambar 7. Perbandingan Asal Penyerang (Farm Server) Berdasarkan Wilayah

Gambar 8 hasil visualisasi dari sebaran infrastruktur router yang memiliki tingkat serangan paling rendah dalam pengamatan. Persentase serangan yang diterima menunjukkan bahwa hanya sebagian kecil dari router yang menjadi sasaran. Berdasarkan konfigurasi port yang terbuka, diketahui bahwa protokol yang tersedia dan dapat diakses oleh pihak luar adalah port 22 (SSH) dan port 23 (Telnet).

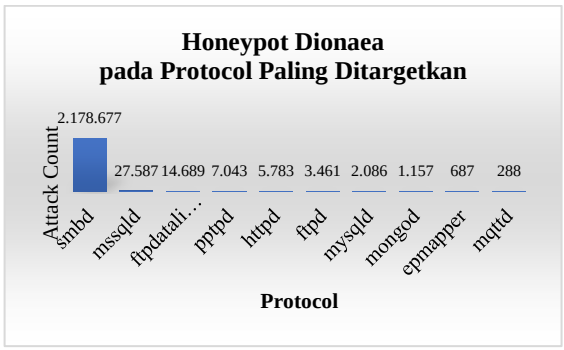


Gambar 8. Perbandingan Asal Penyerang (Router Distribusi) Berdasarkan Wilayah

Dengan melihat masing-masing negara, Vietnam, China, India dan AS menonjol sebagai negara dengan serangan paling banyak dilakukan. Namun, Farm Server lebih sering ditargetkan oleh IP Vietnam (38%), sementara AS (27%) lebih banyak menargetkan perangkat distribusi router. Untuk India, baik China, Jepang maupun indonesia berbagi jumlah serangan yang sama. Dari beberapa hasil analisis yang dilakukan dari rentang waktu yang ada, perubahan serangan terdapat juga perbedaan dan jumlah secara signifikan.

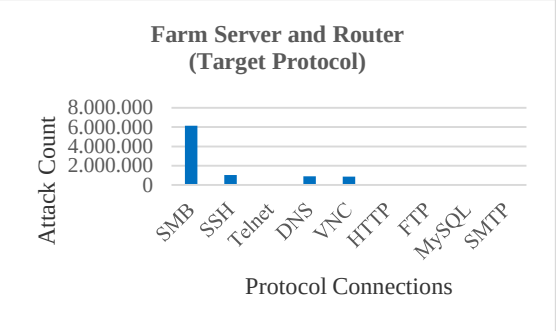
3.3. Analisis Target Layanan and Protokol

Gambar 9 untuk mengetahui jenis layanan atau protokol yang menjadi sasaran utama serangan pada honeypot jenis Dionaea, dilakukan analisis terhadap frekuensi koneksi yang diterima oleh setiap protokol. Berdasarkan visualisasi data yang ditampilkan, terlihat bahwa protokol SMB (*Server Message Block*) mendominasi sebagai target serangan dengan jumlah 2.178.677 serangan.



Gambar 9. Layanan *Dionaea* Paling Ditargetkan

Honeypots mengekspos layanan yang sama pada setiap perangkat router dan server. Masing-masing Honeypots diatur dengan konfigurasi yang sama, sehingga dapat diasumsikan bahwa perilaku dan target serupa di semua mesin honeypot. Tinjauan pertama pada gambar 10 menunjukkan bagaimana SMB adalah salah satu protokol yang paling ditargetkan di setiap sistem, mencapai 98% dibandingkan dengna protocol SSH, Telnet, DNS, VNC, HTTP, FTP, MySQL dan SMTP.



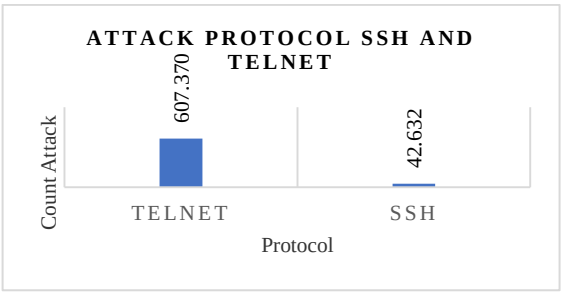
Gambar 10. Perbandingan port yang paling ditargetkan pada Farm Sever dan Router

Dionaea menghitung nilai Hash MD5 dari malware yang sesuai, dan Nilai Hash MD5 ini digunakan untuk tujuan analisis penelitian. Hasil dari nilai hash dikirim ke virus total dan hasil yang dianalisa, penyerang mencoba menyerang sistem honeypot melalui berbagai layanan dan hanya pada protokol SMB, FTP, TFTP, VoIP (Ali and Gireesh Kumar, 2017). Pada penelitian (Sethia and Jeyasekar, 2019) hanya memperkenalkan mekanisme untuk menangkap malware di internet menggunakan cloud pada perangkat *end point* Windows, dengan menyajikan bagaimana contoh EC2, Dionaea terintegrasi bersama untuk menangkap sampel *malware*. Mekanisme yang diusulkan pada penelitian ini pada dionaea tidak hanya berfungsi sebagai detektor layanan yang diserang, tetapi juga mengumpulkan hash file malware yang berhasil ditangkap, termasuk nilai hash MD5, yang kemudian dikirimkan untuk dilakukan analisis lanjutan, misalnya melalui layanan seperti VirusTotal. Hasil pengamatan menunjukkan bahwa sebagian besar serangan diarahkan pada protokol SMB, FTP, TFTP, serta beberapa jenis layanan VoIP.

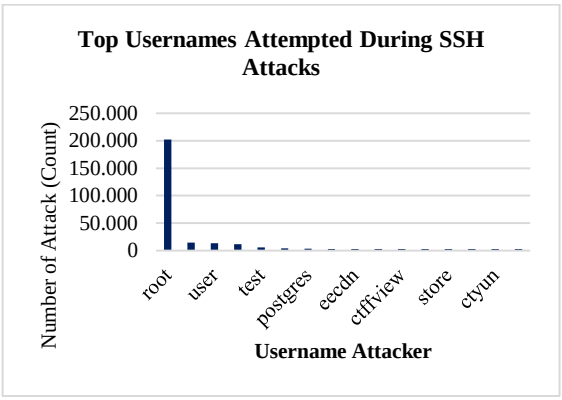
3.4. Analisis Protocol SSH dan Telnet

Gambar 11 merupakah hasil dari honeypot Cowrie yang menerima serangan terbanyak terdapat pada protocol Telnet 607.370 dan protocol SSH 42.632 count.

Gambar 12 menunjukkan 5 nama pengguna teratas dengan jumlah 247.902 yang digunakan selama serangan pada protocol Telnet. Beberapa nama pengguna, seperti root, admin dan user adalah yang paling sering digunakan untuk melakukan serangan.



Gambar 11. *Attempted during SSH and Telnet Layanan attacks*



Gambar 12. Top usernames attempted during SSH attacks

Kredensial yang digunakan untuk menguji atau mengeksploitasi layanan router dan vServer. Sebagai perbandingan, percobaan yang dilakukan dalam makalah ini menghasilkan perbedaan dalam jumlah serangan terhadap dua layanan, di mana Telnet menerima hampir empat belas (14) kali lebih banyak dan akurat daripada layanan SSH. Di satu sisi, ini dapat menyiratkan bahwa layanan Telnet telah menjadi target yang lebih populer bagi penyerang. Di sisi lain, dapat mengidentifikasi bahwa kecenderungan umum adalah bahwa port 23 (plainteks) lebih ditargetkan daripada port 22.

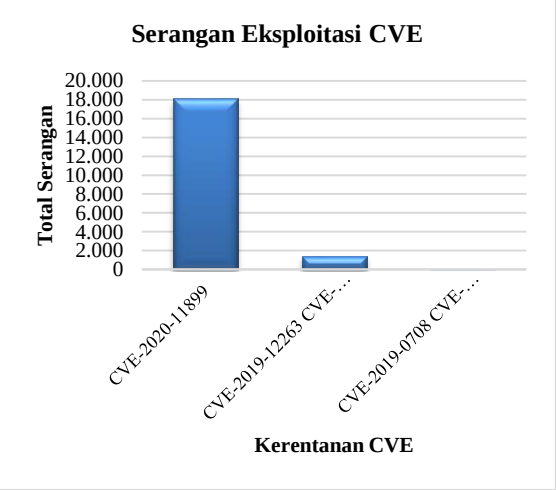
Tabel 2. merupakan perintah teratas yang dimasukkan selama sesi SSH.

Command Line Input	Count
uname -a	12,674
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'	12,280
free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}'	12,279
ls -lh $(which ls)	12,278
which ls	12,278
crontab -l	12,276

Command Line Input	Count
w	12,276
uname -m	12,275
cat /proc/cpuinfo | grep model | grep name | wc -l	12,273
top	12,273

3.5. Analisis *Network Based Intrusion Detection System*

Dalam implementasi sistem honeypot, suricata juga digunakan untuk memantau lalu lintas menuju perangkat router dan vServer, serta mendeteksi aktivitas yang mencurigakan, termasuk upaya eksploitasi kerentanan yang telah diketahui (CVE).



Gambar 13. Kerentanan dalam CVE

Berdasarkan hasil pemantauan selama eksperimen, ditemukan upaya eksploitasi terhadap kerentanan dengan ID CVE tertentu. Pada gambar 13 menunjukkan bahwa eksploitasi terhadap CVE-2020-11899, sebuah kerentanan terkait protokol jaringan di perangkat router dan vServer, merupakan yang paling banyak terjadi, dengan total 18.138 percobaan serangan terdeteksi. Selain itu, 1.470 kali percobaan eksploitasi terhadap kombinasi beberapa kerentanan, yaitu CVE-2019-12263, CVE-2019-12261, CVE-2019-12260, dan CVE-2019-12255, merupakan bagian dari celah keamanan pada protokol komunikasi.

3.6. Analisis Malware Terinfeksi

Pada tahap ini, penulis melakukan proses analisis untuk malware dengan mengambil sampel dari direktori `data/cowrie/downloads` dan `data/dionaea/downloads`. Setiap file yang diperoleh diperiksa menggunakan layanan VirusTotal, yang memanfaatkan 94 mesin antivirus terkemuka untuk analisis statis. Selanjutnya, penulis melakukan pencarian terhadap IP yang direkam Dionaea dan Cowrie, untuk melihat apakah IP Address public tersebut masuk daftar hitam (*blacklisted*) atau tidak. Untuk tujuan ini penulis menggunakan mesin pencari yang memeriksa daftar hitam (*blacklisted*) IP di database anti-spam DNS dan IP Address *Blacklist Checker*. Hasilnya menunjukkan bahwa semua alamat di bawah ini masuk daftar hitam (*blacklisted*), beberapa di antaranya dilaporkan oleh lebih dari 10 basis data anti-spam. Serangan malware lainnya yang berasal dari china berhasil dicatat, salah satunya melalui file bertipe teks dengan nama `1sh`, yang berasal dari alamat IP 61.177.137.133. File ini tercatat melakukan sebanyak 39 kali serangan dalam durasi waktu 60 menit.

Tabel 3. Top IP Address public yang direkam dengan melakukan serangan malware dan malicious.

IP Address	Filename	Countries
2.58.149.116	http://2.58.149.116/w	US
61177137133	http://2.58.149.116/w http://61.177.137.133/x/1sh	China
2.58.149.116	http://2.58.149.116/c	US
	http://2.58.149.116/c	
	http://2.58.149.116/spc	
	http://2.58.149.116/spc	

Jenis dari malware `w,c,c,spc` ini tercatat telah melakukan 200.704 serangan dan berasal dari alamat IP 2.58.149.116, yang terdaftar di wilayah Amerika Serikat, dengan subnet 2.58.148.0/22. Serangan dari file malware ini menjadikannya salah satu yang paling aktif dalam log serangan.

Tabel 4 menyajikan salah satu malware paling aktif yang terdeteksi, yaitu `Eegfim32.exe`. File ini diklasifikasikan sebagai jenis dari Trojan, memiliki ukuran 458.752 byte. Hash yang digunakan dari setiap file (MD5, SHA-1, dan SHA-256) untuk mengidentifikasi jenis dan kategori malware yang menyerang router dan vServer yang menggunakan IP public dan terhubung langsung ke internet.

Tabel 4. Salah satu informasi spesimen malware yang dianalisis.

Spesimen Malware	
Nama	Eegfim32.exe
Tipe File	Win32 EXE
MD5	c21d7343e560afb02ad94f9ddd2bba02
SHA-1	aa38b9548d93abfc16ed7b4bed88e4a1576b92be

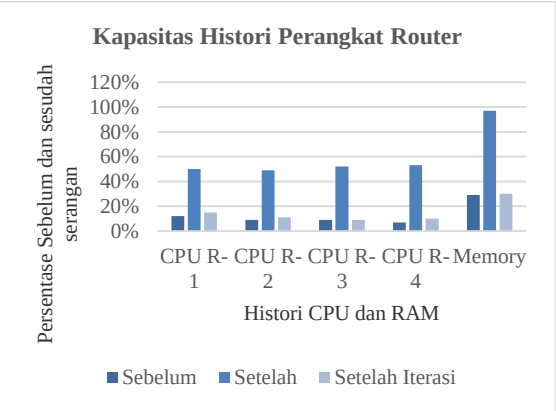
	Spesimen Malware
SHA-256	404c45a45a27f626e3186280425f05db6 0f9fdd3bee63962aec7e82294188088
File size	458752 bytes
Jenis Malware	Trojan

Trojan dengan spesimen ini, digunakan oleh penyerang untuk membuka *backdoor*, mencuri data berupa *username* dan *password*, atau mengontrol perangkat korban dari jarak jauh (*remote*). Fakta dari spesimen malware ini berhasil ditangkap oleh honeypot, menunjukkan bahwa sistem pengumpul data serangan telah berfungsi untuk mendeteksi dan mengarsipkan potensi ancaman terhadap infrastruktur jaringan.

3.7. Evaluasi Kinerja Sistem Firewall

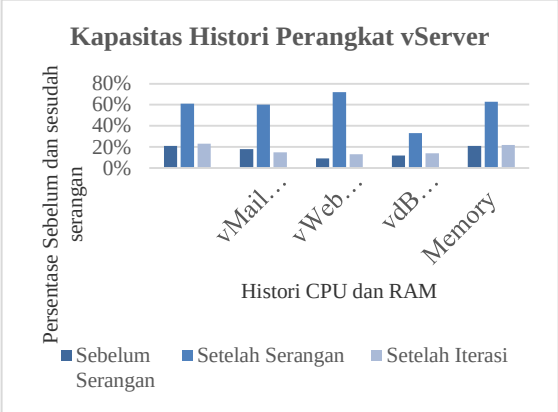
Pengujian untuk evaluasi kinerja dari mitigasi dengan *ipset* firewall yang dimodelkan, dilakukan pada masing-masing perangkat router dan vServer. Sebelum serangan dilancarkan, perangkat jaringan menunjukkan beban kerja rendah dan stabil. Pada gambar 14 berdasarkan hasil pemantauan, sebelum terjadi serangan terlihat *history* CPU menunjukkan beban kerja CPU f^xRouter 1 12%, f^x Router 2 9%, f^x Router 3 9%, f^x Router 4 7%, dan memory 29%. Pada saat terjadi serangan status CPU menjadi high selama menangani proses yang berjalan, pada f^x Router 1 50%, f^x Router 2 49%, f^x Router 3 52%, f^x Router 4 53%, dan memory 97%. Setelah penerapan *rule firewall* diaktifkan secara penuh pada iterasi yang mencakup pemblokiran otomatis berdasarkan deteksi lalu lintas sumber IP address yang mencurigakan kinerja sistem mengalami perbaikan yang signifikan.

Terlihat bahwa *history* dari beban kerja CPU mengalami penurunan. Beban Kerja f^x Router 1 15%, f^x Router 2 11%, f^x Router 3 9%, f^x Router 4 10%, dan memory dengan kapasitas pemakaian menurun menjadi 30%.



Gambar 14. Pengujian Rule Firewall IP Tables Perangkat Router

Pada gambar 15 menunjukkan hasil beban kapasitas CPU dari proses pengujian selama berlangsung eksperimen yang dilakukan dan hasil dari Rule Firewall IPTABLES dari empat iterasi untuk perangkat Farm Server. Sebelum terjadi serangan terlihat historical CPU menunjukkan beban kerja CPU f^x vFTP Server 21%, f^x vMail Server 18%, f^x vWeb Server 9%, dan f^x vdB Server 12%, dan memory f^x 21%. Pada saat terjadi serangan status CPU menjadi high selama menangani proses yang berjalan, pada CPU f^x vFTP Server 61%, f^x vMail Server 60%, f^x vWeb Server 72%, dan f^x vdB Server 33% dan memory f^x 63%. Setelah iterasi rule firewall dalam status running yaitu pada saat proses blocking diaktifkan, terlihat bahwa history dari beban kerja CPU mengalami penurunan. Beban Kerja f^x CPU vFTP Server 23%, f^x vMail Server 15%, f^x vWeb Server 13%, dan f^x vdB Server 14% dan memory f^x 22%.



Gambar 15. Pengujian *Rule Firewall IP Tables Farm Server*

Dari hasil penerapan mitigasi rule *ipset* firewall, menunjukkan konfigurasi firewall yang didesain secara adaptif dan berbasis analisis trafik mampu memberikan dampak nyata dalam menanggulangi serangan dari jaringan publik. Tidak hanya mampu membatasi berdasarkan sumber IP address yang bersifat serangan, penerapan firewall ini juga mampu menurunkan konsumsi sumber daya perangkat router dan vServer secara signifikan.

4. KESIMPULAN

Berdasarkan penerapan model infrastruktur jaringan pada perangkat router dan vServer, dalam penelitian ini, dapat disimpulkan bahwa jaringan yang terhubung langsung ke internet publik sangat rentan terhadap serangan siber yang bersifat otomatis dan masif, terutama yang berasal dari malware global. Penggunaan honeypot pada berbagai perangkat dalam jaringan berhasil merekam aktivitas mencurigakan seperti pemindaian, koneksi, interaksi berbahaya, serta mengumpulkan sejumlah file malware. Selanjutnya, hasil pengamatan mengindikasikan bahwa pelaku serangan siber secara umum menargetkan layanan yang

menyediakan akses jarak jauh, pada protokol telnet dan SSH, dengan memanfaatkan kredensial default atau kata sandi yang lemah guna memperoleh akses ilegal ke dalam sistem. Hasil serangan juga menunjukkan bahwa negara-negara seperti Amerika Serikat, Vietnam, Tiongkok, dan Belanda menjadi sumber dominan dari lalu lintas berbahaya, dengan satu alamat IP asal Amerika Serikat mencatat lebih dari 399 ribu koneksi serangan. Sementara itu, protokol yang paling sering menjadi target serangan adalah SMB (Server Message Block), yang mencapai lebih dari dua juta upaya eksploitasi, jauh melebihi protokol lain seperti FTP, HTTP, dan MySQL. Dalam upaya mitigasi, penerapan aturan pemfilteran otomatis menggunakan ipset IPTables terbukti mampu menekan intensitas serangan secara signifikan. Dari hasil evaluasi, terdapat penurunan beban serangan sebesar 45% pada perangkat router dan sekitar 40% pada perangkat farm server setelah aturan filtering diterapkan. Hasil ini menunjukkan bahwa penggunaan mekanisme pertahanan berbasis pemfilteran dinamis dapat membantu memperkuat ketahanan jaringan terhadap serangan yang berasal dari luar.

DAFTAR PUSTAKA

ALI, P.D. AND GIREESH KUMAR, T., 2017. Malware capturing and detection in dionaea honeypot. *2017 Innovations in Power and Advanced Computing Technologies, i-PACT 2017*, 2017-Janua, pp.1–5. https://doi.org/10.1109/IPACT.2017.8245158.

CERON, M. AND SCHOLTEN, C., 2020. MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. https://doi.org/10.1109/NOMS47738.2020.9110336.

DAMANIK, H.A., 2022. Securing Data Network for Growing Business VPN Architectures Cellular Network Connectivity. *Acta Informatica Malaysia*, 6(1), pp.01–06. https://doi.org/10.26480/aim.01.2022.01.06.

DAMANIK, H.A. AND ANGGRAENI, M., 2024. Pola Pengelompokan dan Pencegahan Public Honeypot menggunakan Teknik K-Means dan Automation Shell-Script. 12(1), pp.65–79.

DAMANIK, H.A., ANGGRAENI, M. AND NUSANTARI, F.A.A., 2023. *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. Jawa Barat: CV. Mega Press Nusantara.

FAVALE, T., GIORDANO, D., DRAGO, I. AND MELLIA, M., 2022. What Scanners do at L7? Exploring Horizontal Honeypots for Security Monitoring. *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, (September 2024), pp.307–313. https://doi.org/10.1109/EuroSPW55150.2022.00037.

FRAUNHOLZ, D., ZIMMERMANN, M., ANTÓN, S.D., Schneider, J. and Dieter Schotten, H., 2017. Distributed and highly-scalable WAN network attack sensing and sophisticated analysing framework based on Honeypot technology. *Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering*, (11), pp.416–421. https://doi.org/10.1109/CONFLUENCE.2017.7943186.

NWACHUKWU, V., MACGREGOR JOHN-OTUMU, A., C, N. V, O, I.C. AND M, J.-O.A., 2021. An Enhanced Model for Mitigating DDoS Attacks on Linux Servers using IPTables and Bash scripts. *International Journal of Advanced Trends in Computer Applications (IJATCA)*, [online] 8(2), pp.68–74.

POLYAKOV, V. V. AND LAPIN, S.A., 2018. Architecture of the Honeypot System for Studying Targeted Attacks. *2018 14th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering, APEIE 2018 - Proceedings*, pp.202–205. https://doi.org/10.1109/APEIE.2018.8545323.

SAIKAWA, K. AND KLYUEV, V., 2019. Detection and Classification of Malicious Access using a Dionaea Honeypot. *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*, 2, pp.844–848. https://doi.org/10.1109/IDAACS.2019.8924340.

SAMU, F., 2016. Design and Implementation of a Real-Time Honeypot System for the Detection and Prevention of Systems Attacks. pp.1–129.

SETHIA, V. AND JEYASEKAR, A., 2019. Malware capturing and analysis using dionaea honeypot. *Proceedings - International Carnahan Conference on Security Technology*, 2019-Octob, pp.0–3. https://doi.org/10.1109/CCST.2019.8888409.

SOKOL, P., HUSÁK, M. AND LIPTÁK, F., 2015. Deploying honeypots and honeynets: Issue of privacy. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, pp.397–403. https://doi.org/10.1109/ARES.2015.91.

WAFI, H., FIADE, A., HAKIEM, N. AND BAHAWERES, R.B., 2017. Implementation of a modern security systems honeypot Honey Network on wireless networks. *Proceedings - 2017 International Young Engineers Forum, YEF-ECE 2017*, pp.91–96. https://doi.org/10.1109/YEF-ECE.2017.7935647.

Halaman ini sengaja dikosongkan