

Implementasi Honeypot Sebagai Pemantau Parameter Pada HTTP Request Untuk Mengetahui Tujuan Serangan

Isnoor Laksana¹, Nur Rohman Rosyid²

Teknologi jaringan – Sekolah Vokasi – Universitas Gadjah Mada
Gedung SV UGM, Sekip Unit 1 Catur Tunggal Depok Sleman Yogyakarta 55281
Email : isnoor.laksana@mail.ugm.ac.id, nrohmanr@ugm.ac.id

Abstract— Services and internet application are increasingly being used. Internet application communication using http protocol that agreed run on port 80 and 443. Various attacks to web server can be run using port 80. One of the attacks model is client-side attacks that manipulate the parameter which sent through http request.

This study have meaning for develop parameter monitoring which is sent by attacker to web server. Monitoring was done using two honeypot glastopf, that mounted on UGM campus network. Both honeypots are managed using the Modern Honeypot Network (MHN). The result of this study are addition analyzing page in MHN which be able to show the parameter sent by attacker, type of attacked and the method used.

Keywords; *HTTP Parameter; Honeypot; Glastopf; MHN;*

Intisari— Layanan dan aplikasi internet semakin banyak dimanfaatkan. Komunikasi aplikasi internet menggunakan protokol HTTP disepakati berjalan pada port 80 dan 443. Berbagai serangan terhadap web server dapat dijalankan melalui port 80. Salah satu model ancaman yang berasal dari *client* adalah manipulasi parameter yang dikirim melalui HTTP *request*.

Penelitian ini dilakukan untuk mengembangkan pemantauan parameter yang dikirim penyerang menuju web server. Pemantauan dilakukan menggunakan dua honeypot glastopf yang dipasang pada jaringan kampus UGM. Kedua honeypot dimanajemen menggunakan *Modern Honeypot Network* (MHN). Hasil dari penelitian berupa penambahan halaman analisis pada MHN yang mampu menampilkan parameter yang dikirimkan penyerang beserta jenis serangan dan *method* yang digunakan.

Kata kunci; *HTTP Parameter; Honeypot; Glastopf; MHN;*

I. LATAR BELAKANG

Layanan dan aplikasi internet semakin banyak dimanfaatkan. Umumnya perangkat lunak yang menggunakan fasilitas internet berjalan dengan layanan HTTP atau HTTPS. Layanan HTTP disepakati berjalan pada port 80 dan 443. Port 80 yang selalu terbuka menjadi ancaman bagi web server. Symantec dalam laporan yang dirilis tahun 2016 menyebutkan bahwa serangan yang mengancam web server meningkat sebanyak 117% pada tahun 2015 dibandingkan tahun 2014 [1].

Berbagai serangan terhadap web server dapat dijalankan melalui port 80. Model ancaman yang berasal dari *client* dilakukan dengan memanipulasi parameter

yang dikirim melalui HTTP *request*. Manipulasi nilai parameter dapat dilakukan melalui *form* HTML maupun alamat URL. *Form* menjadi sarana menangkap masukan oleh sistem. Sedangkan URL merupakan alamat *file* yang dapat diakses diinternet. Hal-hal tersebut membuat manipulasi nilai parameter selalu bisa dilakukan oleh penyerang. Manipulasi nilai parameter dapat menjadi serangan bagi web server berupa SQL *injection*, *code injection*, *remote code inclusion* dan *cross-side scripting*(XSS). Persentase jenis serangan RFI, SQL *injection* dan XSS dapat dikatakan cukup besar dibandingkan seluruh serangan yang terjadi [2].

Salah satu sistem untuk mengetahui adanya serangan di server adalah dengan pemasangan honeypot. Glastopf merupakan salah satu honeypot yang dibangun untuk mendeteksi serangan SQL *injection* dan RFI [3]. Glastopf menampilkan hasil deteksinya dalam bentuk *command line interface* (CLI). *Modern Honey Network* (MHN) dapat mengelola honeypot glastopf. Selain menampilkan data serangan glastopf, MHN dapat mengelola data honeypot lain. Oleh karena itu MHN hanya menampilkan data serangan secara umum. Aplikasi tersebut belum memfasilitasi tampilan data honeypot glastopf yang lebih spesifik dan terkelompokan.

Penelitian ini akan melaporkan data yang direkam oleh honeypot glastopf selama sekitar 3 minggu mulai dari 11 mei hingga 2 Juni 2017. Glastopf juga berperan sebagai penganalisis data serangan. Data akses yang belum teranalisis sebagai serangan, dianalisis ulang oleh *High Interaction Honeypot Analysis Toolkit* (HIHAT). MHN yang telah dimodifikasi akan menampilkan detail serangan yang terjadi.

II. KAJIAN PUSTAKA

A. Web Server

Web server merupakan program komputer yang melayani HTTP. Web server merupakan komputer yang memiliki tanggung jawab untuk menerima HTTP *request* dari *client* dan mengirimkan HTTP *response* menuju *client*. HTTP *request* umumnya dikirimkan *client* menggunakan web *browser* [4].

HTTP *request* adalah pesan dari *client* ke server, termasuk baris pertama dari pesan tersebut, metode yang digunakan, penanda dari sumber dan versi protokol yang digunakan. HTTP *request* dikirimkan berisi parameter-parameter yang diinginkan. Beberapa penanda parameter pada HTTP *request* antara lain : *accept*, *accept-charset*, *accept-encoding*, *accept-language*, *accept-datetime*, *authorization*, *connections*, *cookie*, *date*, *from*, *host*,

forwarded, origin, content-length, content-MD5, content-type, expect, pragma, user-agent, dan referrer.

HTPP *referrer* merupakan penanda alamat halaman web sebelumnya. HTTP *referrer* dapat digunakan untuk mengetahui website yang berbahaya. Penelitian menggunakan Honeypot YALIH berhasil mengungkap web-web yang hanya bersifat spam dengan cara menganalisis HTTP *referrer* [5].

B. Honeypot dan MHN

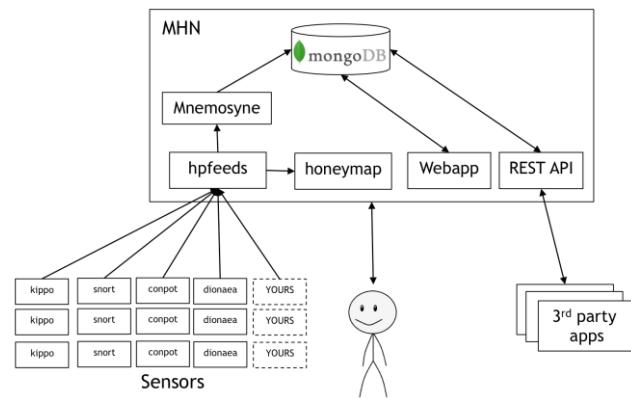
MHN (*Modern Honey Network*) adalah *framework* yang dapat digunakan untuk mempermudah pemasangan dan pengelolaan honeypot. MHN merupakan perangkat lunak berlisensi *open source*. Pada Gambar 1 terlihat MHN menggunakan format data standar hpfeed untuk penerimaan data[6].

Honeypot adalah sistem komputer yang sangat fleksibel pada jaringan internet yang dikustomasi menjadi alat keamanan dan diatur untuk menyerang dan menjebak orang yang berusaha melakukan penetrasi sistem komputer orang lain melalui penelusuran, *scan*, dan penyusupan [7].

Honeypot dikelompokkan dalam beberapa taksonomi, antara lain: berdasarkan *resource* yang diserang, tingkat interaksi dan bidang spesialisasi. Honeypot dibedakan menjadi tiga kelompok berdasarkan interaksinya, yaitu : *low interaction*, *high interaction* dan *hybrid*. Berdasarkan keberadaan *resource* yang diserang, honeypot dibedakan menjadi dua kelompok utama, yaitu : *server-side* dan *client-side*. Sedangkan berdasarkan *resource* yang diteliti, honeypot dibedakan menjadi beberapa kelompok diantaranya : Web *application* honeypot, SSH Honeypot, SCADA Honeypot, VoIP Honeypot, Bluetooth Honeypot, USB Honeypot, *sinkholes* dan honeypot kepentingan umum. Ada beberapa honeypot yang digunakan untuk spesialisasi serangan pada web server, antara lain: *High Interaction Honeypot Analysis Toolkit* (HIHAT), *DShield Web Honeypot*, Google *Hack Honeypot* dan Glastopf [8].

Glastopf termasuk dalam taksonomi interaksi rendah, *server-side* dan web *application* honeypot. Glastopf merekam dan menganalisis akses keserver honeypot. Kemudian datanya disimpan dalam beberapa format, diantaranya : basis data sqlite, MySql, *file log* dan dikirimkan melalui hpfeed [3]. Sedangkan HiHAT merupakan salah satu honeypot dengan tingkat interaksi tinggi spesialis web server.

Honeypot glastopf maupun HIHAT dapat dipasang pada sebuah komputer berukuran mini. Hal tersebut telah diuji pada penelitian [9] dengan melakukan *stress testing* pada glastopf yang terpasang pada *cubieboard*. Hasilnya perangkat tersebut mampu mendeteksi serangan *brute force*, LFI dan RFI. Glastopf juga sukses menipu *hacking tools* penyerang [10]. Honeypot lain juga dapat dipasang pada komputer mini raspberry pi. Hasilnya honeypot menangkap *query sql injection* yang diberikan penyerang [11]. Selain itu, honeypot juga mampu mengenali serangan XSS dan memicu penyerang mengirimkan identitasnya [12].



Gambar 1 Arsitektur MHN

Penelitian-penelitian sebelumnya fokus mempelajari kehandalan honeypot yang terpasang pada komputer mini. Sedangkan makalah ini menganalisis serangan yang terjadi pada glastopf yang terintegrasi dengan honeypot lain. Integrasi dilakukan dengan MHN. Saat di MHN dilakukan analisis ulang jenis serangan berdasarkan data HTTP request yang tercatat. Analisis dilakukan menggunakan HIHAT.

III. METODOLOGI DAN PERCOBAAN

A. Implementasi honeynet

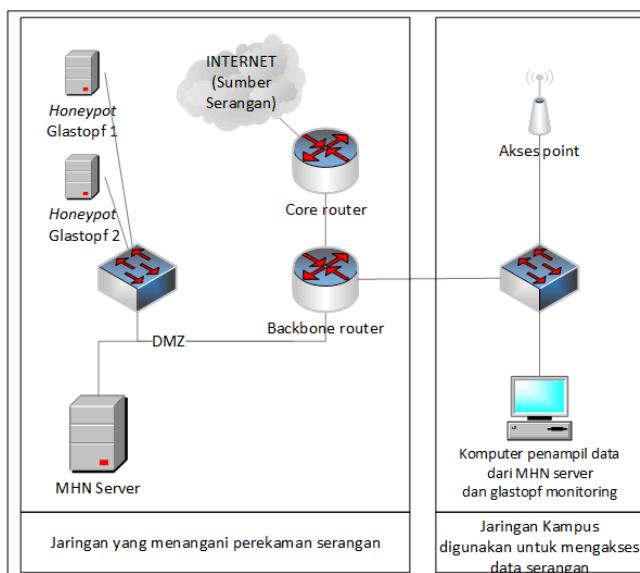
Honeynet terdiri dari dua buah honeypot dan sebuah honeynet server yang terpasang di *Demilitarized Zone* (DMZ) jaringan kampus Universitas Gadjah Mada seperti pada Gambar 2. Honeypot yang digunakan adalah glastopf. Honeypot merekam setiap serangan yang masuk melalui port 80. Masing-masing honeypot glastopf dijalankan pada komputer mini dengan kapasitas penyimpanan data 32 GB. Komputer mini yang digunakan adalah raspberry pi 2 dengan sistem operasi raspbian wheezy. Pada kedua raspberry terpasang dua honeypot lain. Masing-masing raspberry terpasang honeypot glastopf, dionaea dan kippo. Honeypot dionaea dan kippo dipasang untuk menangani serangan selain pada port 80.

Honeynet yang digunakan untuk mengelola semua honeypot adalah *Modern Honey Network* (MHN). MHN dikembangkan oleh Threatstream dapat mengelola honeypot glastopf, dionaea dan kippo. MHN dipasang pada *Virtual Private Server*(VPS) dengan sistem operasi ubuntu 14.04 LTS.

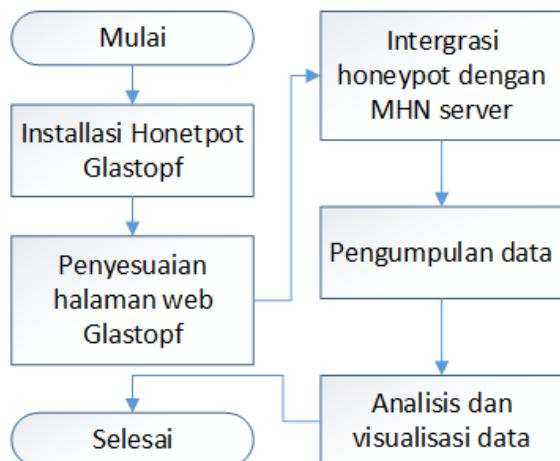
B. Prosedur Penelitian

Langkah-langkah penelitian dilakukan dalam lima tahap seperti pada Gambar 3. Langkah yang pertama dilakukan adalah memasang glastopf pada raspbian wheezy. Pemasangan honeypot dilakukan menggunakan *script* yang tersimpan pada MHN. *Script* tersebut mengalami sedikit perubahan sebelum digunakan.

Halaman web umpan pada glastopf diubah mirip dengan web kampus. Hal tersebut dilakukan untuk mengelabuhi penyerang. Setelah honeypot glastopf terpasang dengan template yang baru, honeypot diatur agar terhubung dengan MHN. Pengaturan dilakukan dengan mengubah IP Address target hpfeed menuju ke MHN. Tahap pengambilan data dilakukan setelah honeypot terintegrasi dengan MHN.



Gambar 2 Topologi jaringan kampus dengan dua honeypot dan sebuah honeynet server



Gambar 3 Flowchart metodologi penelitian

Analisis dilakukan dengan menggunakan data yang disimpan oleh MHN. Data tersebut dipetakan dalam format data yang baru dan divisualkan. Visualisasi data dilakukan pada beberapa menu baru di MHN.

IV. HASIL DAN PEMBAHASAN

Pemantauan serangan dilakukan menggunakan framework MHN yang telah dimodifikasi. Setiap honeypot mengirimkan log serangan ke MHN server. MHN membedakan log yang dikirimkan glastopf dalam 2 tanda yang berbeda. Tanda “*glastopf.events*” digunakan untuk mengetahui bahwa yang disimpan berupa data kejadian serangan. Sedangkan tanda “*glastopf.files*” mengenali penyimpanan data penerimaan file oleh glastopf. Hanya data serangan dengan tanda “*glastopf.events*” saja yang mampu dianalisis. MHN mencatatkan 9577 serangan dengan tanda “*glastopf.event*” yang terjadi dari tanggal 11 mei hingga 2 juni 2017. Pada TABEL 1 terlihat alamat IP honeypot dan jumlah serangan yang terjadi.

TABEL 1 Daftar honeypot glastopf yang terpasang beserta jumlah serangan yang terjadi

No	UUID	IP Address	Count
1	f05447ac-3779-11e7-9e19-0050569163b4	202.xx.xx.xx	661
2	2ae226b4-35e5-11e7-9e19-0050569163b4	202.xx.xx.xx	8916
Total			9577

A. Analisis Method Serangan

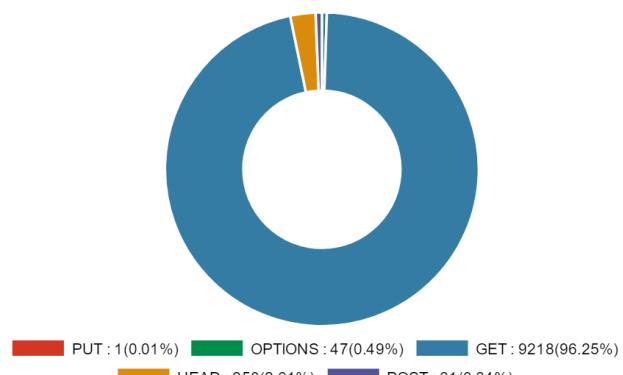
Akses menuju honeypot glastopf dilakukan penyerang dengan berbagai *method* seperti pada Gambar 4. Serangan terbanyak terjadi pada HTTP *request* dengan *method* GET. Jumlahnya mencapai lebih dari 96 % dari total serangan yang terjadi. Hal tersebut menandakan *method* GET terlalu rawan untuk digunakan. Oleh karena itu sebaiknya *form* dan tautan dikirimkan dengan *method* lain.

Terbanyak kedua adalah *method* HEAD. Hal tersebut menandakan bahwa ada upaya dari penyerang untuk mengunduh *file* yang ada di web server. Serangan dengan *method* POST, PUT dan OPTIONS terjadi dengan jumlah yang kecil. *Method* OPTIONS menunjukkan bahwa penyerang melakukan pengecekan terlebih dahulu sebelum melakukan penetrasi.

B. Analisis Perangkat Lunak Penyerang

Penyerang menjalankan HTTP *request* melalui sebuah perangkat lunak. Perangkat lunak dapat berupa *web browser* atau perangkat lunak lainnya. Perangkat lunak akan mengirimkan parameter *User Agent* sebagai identitas. *User Agent* dikirimkan didalam HTTP *request*. Tujuh kelompok user agent yang paling banyak digunakan penyerang dapat dilihat pada TABEL 2. Perangkat lunak paling banyak digunakan adalah Nikto. *Web browser* Firefox, chrome, internet explore dan microsoft webDav terlihat cukup sering digunakan. Parameter *User Agent* tidak wajib berada dalam HTTP *request*. Sehingga pada urutan ketiga terlihat kelompok *unknown*.

User agent berupa *web browser* menunjukkan adanya serangan yang dilakukan secara manual. Meskipun kejadiannya lebih sedikit dibandingkan serangan menggunakan *hacking tools*. Tercatat beberapa *hacking tools* yang digunakan diantaranya nikto, zmeu, jexboss, masscan dan kscan.



Gambar 4 Piechart persentase *method* yang digunakan penyerang untuk mengakses honeypot

TABEL 2 Daftar tujuh perangkat lunak yang paling sering digunakan penyerang

No	Taksonomi	Jumlah Serangan
1	Nikto	8218
2	Mozilla	766
3	Unknown	147
4	Firefox	138
5	Chrome	89
6	Internet Explore	47
7	Microsoft WebDAV	43

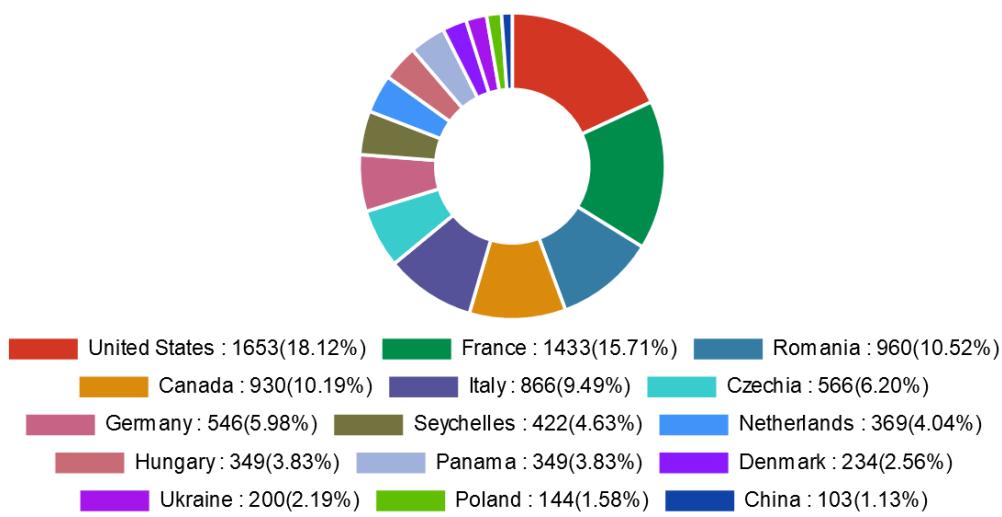
C. Identifikasi Sumber Serangan

Glastopf mencatat alamat IP setiap penyerang. Visualisasi data alamat IP pada Gambar 5 memperlihatkan serangan terbanyak berasal dari *United State*. Jumlah serangan dari negara tersebut mencapai 1653 kali atau 18,12 % dari total akses. Serangan negara *United State* berasal dari 56 alamat IP yang berbeda. Alamat IP dari negara *United state* yang melakukan serangan lebih dari 100 kali, diantaranya : 65.19.167.134, 216.218.222.12, 196.52.39.17, dan 209.222.77.220.

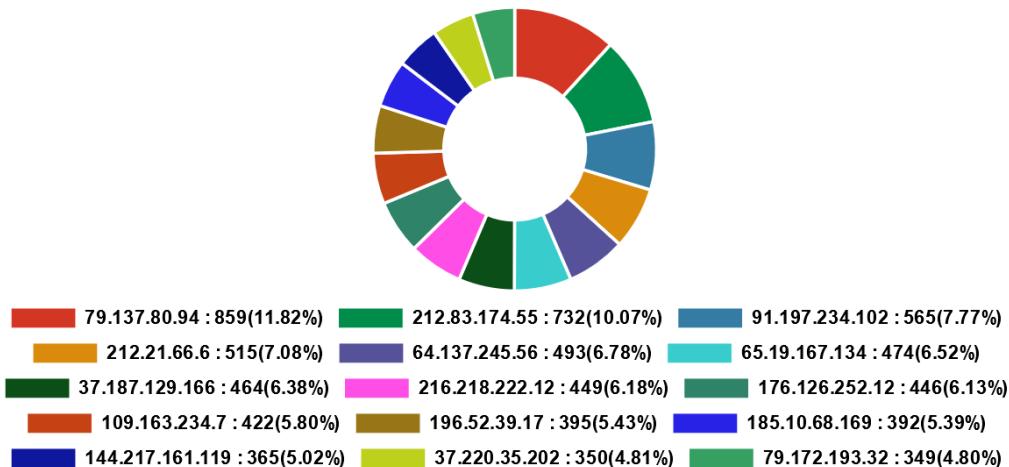
Serangan terbanyak kedua berasal dari negara *France*. Tercatat 12 alamat IP berbeda dari negara *France*. Selain *United State* dan *France*, tercatat ada lima negara lain yang jumlah akses kehoneypot lebih dari 500 kali. Kelima negara tersebut yaitu Romania, Kanada, Italia, *Czechia* dan Jerman. Serangan dari Jerman mencapai 546 kali. Serangan berasal dari 13 alamat IP yang berbeda. Alamat IP dari Jerman yang tercatat paling sering melakukan serangan adalah 212.21.66.6.

Glastopf mencatat terdapat 54 negara yang melakukan akses ke honeypot. Akses berupa serangan ataupun hanya *scanning*. Beberapa negara tercatat ada yang hanya melakukan akses kehoneypot satu kali berupa *scanning*. Negara-negara tersebut antara lain : Kuwait, *Dominican Republic*, Azerbaijan, Filipina, Argentina, Palau, Tanzania, Bahamas, Israel, Peru, Irlandia, Bulgaria, Malaysia, Spanyol dan Turki.

Jumlah IP unik penyerang tercatat sebanyak 259 alamat. Serangan terbanyak dari alamat IP 79.137.80.94. Alamat IP tersebut melakukan serangan sebanyak 859 kali. Alamat IP tersebut terdeteksi berasal dari negara Italia. Detail 15 alamat IP yang melakukan serangan terbanyak dapat dilihat pada Gambar 6.



Gambar 5 Piechart sumber serangan berdasarkan negara



Gambar 6 Piechart alamat IP penyerang

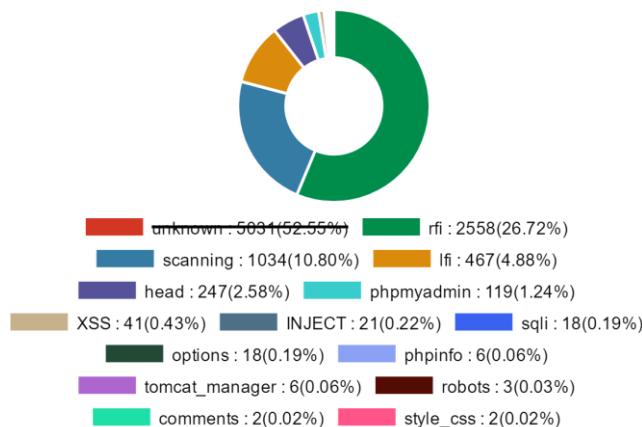
D. Analisis Jenis Serangan dan Parameternya

Analisis jenis serangan yang dilakukan oleh glastopf dan HIHAT belum mampu mengenali semua akses yang masuk. Hal tersebut terlihat dari hasil visualisasi data yang menunjukkan 52,55 % akses termasuk jenis *unknown*. Gambar 7 memperlihatkan 14 jenis serangan yang paling banyak terjadi.

Analisis yang dilakukan dengan glastopf dan HIHAT menunjukkan serangan *Remote File Inclusion* (RFI) paling banyak terjadi. RFI terjadi sebanyak 2558 kali atau 26,72 % dari total akses yang masuk. Serangan RFI dilakukan dengan mengirimkan parameter berupa referensi alamat menuju file yang berisi script server. Pada penelitian ini terdapat 2485 variasi parameter yang dikirimkan pada jenis serangan RFI. Serangan RFI banyak terjadi karena penyerang tertipu oleh glastopf bahwa serangannya selalu berhasil.

TABEL 3 memperlihatkan dua parameter terbanyak yang dikirimkan pada serangan RFI. Parameter pada TABEL 3 no 1 digunakan penyerang untuk mengetahui keberadaan proxy. Sedangkan parameter pada TABEL 3 no 2 digunakan penyerang untuk mengetahui log pengaksesan publik akses point. Keduanya bertujuan melakukan penetrasi jaringan disekitar server.

Pada penelitian ini akses *scanning* terdeteksi banyak terjadi. Tercatat ada 1034 kali akses *scanning*. Beberapa alamat IP terdeteksi hanya melakukan *scanning* saja. Alamat-alamat tersebut tidak melakukan serangan lebih lanjut ke web server. Akses tersebut dilakukan menggunakan perangkat lunak *scanning tools*, diantaranya : zgrab, masscan, scanbot dan ksscan. Hal tersebut menunjukkan banyaknya serangan *scanning* kemungkinan mengincar port lain juga. Port-port yang disimulasikan honeypot menjadi berstatus *open* menjadi faktor terjadi banyaknya serangan *scanning*.



Gambar 7 Piechart 14 jenis serangan terbanyak

TABEL 3 Daftar Parameter Pada Serangan RFI

No	Pattern	Parameter	Jumlah Serangan
1	RFI	http://testp3.pospr.waw.pl/testprox.php	19
2	RFI	http://www.msftncsi.com/ncsi.txt	3

Serangan *local file inclusion* (LFI) teranalisis sebanyak 467 kali. Variasi parameter yang dikirimkan untuk jenis serangan LFI ada 466. Beberapa parameter mirip dengan parameter lainnya. TABEL 4 memperlihatkan beberapa bentuk parameter yang dikirimkan. Beberapa target *file* yang menjadi sasaran penyerang antara lain : win.ini, daftar folder suatu partisi serta *file* password. TABEL 4 no 1 dan no 2 menunjukkan letak file win.ini yang diincar penyerang. Sedangkan no 6, 7 dan 9 menunjukkan bahwa penyerang mengincar file password yang tersimpan di *directory* etc. Folder etc merupakan bawaan sistem operasi linux. Sehingga dapat diketahui bahwa serangan ini mengincar server berbasis sistem operasi linux.

Aplikasi phpmyadmin merupakan perangkat lunak yang digunakan untuk mengelola basis data MySQL. Modul phpmyadmin tercatat banyak mendapatkan serangan. Sebanyak 119 kali akses mengarah kemodul phpmyadmin. TABEL 5 memperlihatkan daftar parameter yang digunakan penyerang untuk mengakses modul phpmyadmin. Berdasarkan pengamatan parameter tersebut, terlihat beberapa tujuan penyerang diantaranya : mengakses aplikasi phpmyadmin, mengakses file pengaturan, masuk aplikasi dengan akun *default*, dan mengakses file log.

TABEL 4 Daftar parameter pada serangan LFI

Akses aplikasi phpmyadmin dilakukan penyerang dengan variasi parameter seperti pada TABEL 5 no 1 , 3 dan 6. Sedangkan no 2, 4, 5 dan 7 menunjukkan penyerang mengincar file pengaturan dari aplikasi phpmyadmin. Serangan *bruce force* juga mengancam modul phpmyadmin. Pada TABEL 5 no 8, 9 dan 10 terlihat penyerang mengirimkan *username* dan *password default*. Hasil tersebut menunjukkan tidak disarankan menggunakan *username default* “admin” dan “test” untuk *login* suatu aplikasi.

Phpmyadmin menerima banyak serangan karena glastop menyimulasikan beberapa halamannya. Simulasi juga dilakukan pada alamat URL-nya. Sehingga penyerang menganggap sistem web menggunakan aplikasi phpmyadmin. Hal tersebut dapat diatasi dengan tidak memasang aplikasi phpmyadmin di server sebenarnya.

TABEL 5 Daftar parameter serangan pada modul phpmyadmin

No	Pattern	Parameter	Jumlah Serangan
1	phpmyadmin	/phpmyadmin	18
2	phpmyadmin	/phpmyadmin/scripts/setup.php	10
3	phpmyadmin	/phpmyadmin/	5
4	phpmyadmin	//phpmyadmin/scripts/setup.php	4
5	phpmyadmin	//phpMyAdmin/scripts/setup.php	4
6	phpmyadmin	/phpMyAdmin	4
7	phpmyadmin	/phpMyAdmin/scripts/setup.php	3
8	phpmyadmin	pma_username=admin&pma_password=123456	2
9	phpmyadmin	pma_username=admin&pma_password=admin	2
10	phpmyadmin	pma_username=test&pma_password=admin	2

V. KESIMPULAN

Modifikasi *Modern Honey Network* dengan menambahkan HIHAT mampu menganalisis dan memvisualkan data serangan yang tercatat oleh glastopf. *Method*, perangkat lunak, jenis serangan dan sebaran IP yang digunakan penyerang dapat teramat dengan visualisasi dari ekstraksi parameter-parameter data HTTP *request*. Serangan terjadi karena web server nampak lemah dan menunjukkan respon atas serangan yang dilakukan.

REFERENCES.

- [1] Symantec. “Internet Security Threat Report s.l.” online at https://www.symantec.com/content/dam/symantec/docs/reports/ist_r-21-2016-en.pdf, 2016., terakhir diakses 20 April 2017
- [2] Goseva-Popstojanova, Katerina, Goce Anastasovski and Risto Pantev. "Classification of Malicious Web Sessions." 2012 21st International Conference on Computer Communications and Networks (ICCCN). Morgantown: IEEE, 2012, pp. 1 - 9.
- [3] Rist, Lukas, et al. "A dynamic, low-interaction web application honeypot." KYT Paper, 2010.
- [4] McClure, Stuart, Shah Saumil and Shah Shreeraj. “Web Hacking Attacks and Defense: Web Hacking Serangan dan Pertahannanya (Erwin Philipus. Trans)”. Yogyakarta: ANDI, 2003
- [5] Mansoori, Masood, et al. "Empirical Analysis of Impact of HTTP referrer on Malicious Website Behavior and Delivery." 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2016. pp 941-948.
- [6] “MHN Modern Honey Network “ online at <https://threatstream.github.io/mhn/> .., terakhir diakses 20 April 2017
- [7] Thomas, M Tom. “Network Security First-Step”. Boston : Pearson Education Inc publising as Cisco Press, 2004.
- [8] Grudziecki, Tomasz, et al. “Proactive Detection of Security Incidents”. ENISA, 2012
- [9] Rahmatullah, Dandy Kalma, Surya Michrandi Nasution and Fairuz Azmi. “Implementation of Low Interaction Web Server Honeypot Using Cubieboard “. The 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC). IEEE, 2016, pp. 127-131.
- [10] Djanali, S., Arunanto, F., Pratomo, B. A., & Studiawan, H. “Honeypot in Raspberry Pi Cluster for Analyzing Attacker Behaviour”. Engineering International Conference 2013 Proceeding., Semarang, Indonesia., 2013
- [11] Djanali, S., Arunanto, F., Pratomo, B. A., Studiawan, H., & Nugraha, S. G. “SQL Injection Detection and Prevention System with Raspberry Pi Honeypot Cluster for Trapping Attacker”. International Symposium on Technology Management and Emerging Technologies (ISTMET 2014), 2014, pp. 163-166
- [12] Djanali, Supeno, et al. “Aggressive Web Application Honeypot for Exposing Attacker’s Identity.” 2014 1st International Conference on Information Teclmology, Computer and Electrical Engineering (ICITACEE) . IEEE, 2014, pp. 212-216.