LOW INTERACTION HONEYPOT UNTUK MEMINIMALISIR SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS): *SLOWLORIS* TERHADAP *WEB SERVER*

TUGAS AKHIR

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik Elektro
Program Studi S-1 Teknik Elektro

Disusun oleh :

Nadya Richna Fitri

E.5051.1506032

PROGRAM STUDI TEKNIK ELEKTRO S1
DEPARTEMEN PENDIDIKAN TEKNIK ELEKTRO
FAKULTAS PENDIDIKAN TEKNOLOGI DAN KEJURUAN
UNIVERSITAS PENDIDIKAN INDONESIA
BANDUNG

2019

LOW INTERACTION HONEYPOT UNTUK MEMINIMALISIR SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS): *SLOWLORIS* TERHADAP *WEB SERVER*

Oleh
Nadya Richna Fitri

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Teknik pada Fakultas Pendidikan Teknologi dan Kejuruan

© Nadya Richna Fitri 2019
Universitas Pendidikan Indonesia
Agustus 2019

Hak Cipta dilindungi undang-undang.
Skripsi ini tidak boleh diperbanyak seluruhya atau sebagian,
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

NADYA RICHNA FITRI

E.5051.1506032

LOW INTERACTION HONEYPOT UNTUK MEMINIMALISIR SERANGAN _DISTRIBUTED DENIAL OF SERVICE_ (DDOS): _SLOWLORIS_ TERHADAP _WEB SERVER_

Disetujui dan disahkan oleh pembimbing:

Pembimbing I	Pembimbing II
Agus Heri Setyabudi M.T.	Iwan Kustiawan, M.T., Ph. D.
NIP. 19720826 200501 1 001	NIP. 19770908 200312 1 002

Mengetahui,
Ketua Departemen Pendidikan Teknik Elektro

Dr. H. Yadi Mulyadi, M.T.
NIP. 19630727 199302 1 001

PERNYATAAN

Dengan ini saya menyatakan bahwa tugas akhir dengan ***judul "LOW INTERACTION HONEYPOT UNTUK MEMINIMALISIR SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS): SLOWLORIS TERHADAP WEB SERVER"*** *ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.*

Bandung, Agustus 2019

Yang membuat pernyataan,

Nadya Richna Fitri

NIM. 1506032

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan Tugas Akhir yang berjudul "***Low Interaction Honeypot* untuk Meminimalisir Serangan *Distributed Denial of Service* (DDoS): *Slowloris* terhadap *Web Server***". Tugas Akhir ini disusun sebagai bagian dari persyaratan untuk mendapatkan gelar Sarjana Teknik di Universitas Pendidikan Indonesia Fakultas Pendidikan Teknologi dan Kejuruan Departemen Pendidikan Teknik Elektro Program Studi S1 Teknik Elektro.

Penulis menyadari banyak pihak yang telah ikut berperan serta membantu dalam menyelesaikan Tugas Akhir ini. Maka dari itu penulis ingin mengucapkan terimakasih kepada:

1. Ibu Hj. Milda Yanuvianti S.Psi., M.A. selaku orang tua dari penulis yang tiada hentinya mendo'akan, memberikan afeksi, dukungan. Serta keluarga drg. H. Maskon Angkaraspati dan keluarga Johansyah Ibrahim yang selalu memberikan motivasi dan nasihat.
2. Bapak Dr. H. Yadi Mulyadi, M.T. selaku Ketua Departemen Pendidikan Teknik Elektro, Universitas Pendidikan Indonesia.
3. Bapak Didin Wahyudin, Ph.D selaku Sekretaris Departemen Pendidikan Teknik Elektro, Universitas Pendidikan Indonesia.
4. Bapak Iwan Kustiawan, M.T., Ph. D. selaku Ketua Program Studi S1 - Teknik Elektro, Universitas Pendidikan Indonesia.
5. Bapak Agus Heri Setyabudi M.T. selaku dosen pembimbing I yang telah membimbing dan memberikan banyak dukungan, motivasi dan masukan kepada penulis.
6. Bapak Iwan Kustiawan, M.T., Ph. D. selaku dosen pembimbing II yang juga telah membimbing dan memberikan banyak dukungan, motivasi dan masukan kepada penulis.
7. Bapak Dandhi Kuswardhana, S.Pd., M.T. selaku dosen Departemen Pendidikan Teknik Elektro yang juga telah membimbing dan memberikan dukungan serta kontribusi dalam penyusunan Tugas Akhir ini.

8. Seluruh staff dosen dan administrasi Departemen Pendidikan Teknik Elektro FPTK UPI.
9. Bapak Ir. Sri Endang Suwono selaku pembimbing dari Telkom *Corporate University* yang telah membimbing dan memberikan motivasi, dukungan dan kontribusi dalam penyusunan Tugas Akhir ini.
10. Ibu Dr. Rismijati E. Koesma, Psikolog yang telah memberikan nasihat dan motivasi kepada penulis dalam hal non akademik.
11. Annisa Muzdalifa, S.T., Ridho Muhammad Fikri, Wildan Juliardi, S.Pd., Adnan Khairi dan Egawa Mugni Shirath, S.Pd. yang telah membimbing, membantu dan memberikan kontribusi dalam penyusunan Tugas Akhir ini.
12. Gita Ayu Lestari, S.Si., Shofi Azkarifa, S.T., Muthia Nur Faizah, Muhammad Dhafin Fauzan, A.Md., Annisha Livyana, S.Psi., Harashtina Aunurrahim dan Sarah Irish selaku teman dekat yang selalu memberikan afeksi, motivasi dan dukungan kepada penulis.
13. Julian Serly Ayu, S.T., Regita Nurmalita Yuniar, S.T., Putri Ayu Kencana, Farid Miftah Fauzi, Yudha Hardiansyah, S.T. dan Ahmad Raihan Abdurrahman, S.T. yang selalu memberikan afeksi, dukungan dan motivasi kepada penulis selama perkuliahan.
14. Teman-teman kelas Elektronika Telekomunikasi 2015 yang telah memberikan semangat dan motivasi bagi penulis selama perkuliahan.
15. Teman-teman Angkatan 2015 Prodi S1 Teknik Elektro yang telah memberikan semangat dan motivasi bagi penulis selama perkuliahan.
16. Teman-teman Angkatan 2015 Departemen Pendidikan Teknik Elektro yang telah memberikan semangat dan motivasi bagi penulis selama perkuliahan.
17. Semua pihak yang telah membantu yang tidak dapat disebutkan satu persatu.

Semoga Allah SWT membalas kebaikan semua pihak yang telah membantu penulis dalam pelaksanaan dan penyusunan Tugas Akhir ini.

Bandung, Agustus 2019

Penulis

ABSTRAK

Slowloris merupakan salah satu *open-source tool* serangan DDoS yang pada umumnya menyerang *web server* berbasis *software Apache*. Selama ini, untuk mengurangi serangan *Slowloris* digunakanlah *firewall*, *load balancer* dan penambahan jumlah *web server*. Penelitian ini bertujuan untuk merancang mekanisme pertahanan yang terdiri dari *Low Interaction Honeypot* (HoneyPy) dan *stateless firewall* sehingga tak perlu menambahkan jumlah *web server*. Keandalan mekanisme pertahanan tersebut diuji dengan melakukan eksperimen dalam tiga kondisi, yaitu kondisi normal tanpa penyerangan sama sekali, kondisi penyerangan tanpa mekanisme pertahanan dan dengan mekanisme pertahanan. Dampak yang ditimbulkan oleh serangan *Slowloris* dilihat dari jumlah paket *client error*. Penyerangan dilakukan selama 5 menit dengan membuat 1000 koneksi ke *web server.* Ketika kondisi normal, jumlah paket *client error* tidak ada sama sekali karena tidak ada penyerangan. Ketika penyerangan tanpa mekanisme pertahanan, paket *client error* berjumlah 2142 paket. Sedangkan ketika dengan mekanisme pertahanan, jumlah paket *client error* turun menjadi 33 paket. Sehingga, dapat disimpulkan bahwa adanya *Low Interaction Honeypot* dalam mekanisme pertahanan dapat menurunkan dampak serangan *Slowloris* serta memperlambat penyerangan.

Keyword: DDoS, *Slowloris*, *Firewall*, *Low Interaction Honeypot*, HoneyPy, *Security*, *Raspberry Pi*.

ABSTRACT

Slowloris is an open-source DDoS attack tool that generally attacks Apache-based web servers. During this time, Firewalls, load balancers and additional numbers of web servers are used to mitigate the Slowloris attack. This research aims to design the defense mechanism consisting of Low Interaction Honeypot (HoneyPy) and the stateless firewall so we don't need to use more web servers. The reliability of the defense mechanism was tested by conducting an experiment in three conditions, the normal condition when there are no attacks at all, the attacking condition with and without the defense mechanism. The impact caused by the Slowloris attack can be seen from the number of client error packets. The attack was carried out for 5 minutes by making 1000 connections to the webserver. There is no client error packets in the normal condition because there are no attacks. In the attacking condition without the defense mechanism, the client error packets are 2142 packets. Whereas, in the attacking condition with the defense mechanism, the number of client error packets drops to 33 packets. Thus, it can be concluded that the existence of Low Interaction Honeypot in defense mechanisms can reduce the impact of Slowloris attacks and slow down the attacks.

Keyword: DDoS, Slowloris, Firewall, Low Interaction Honeypot, HoneyPy, Security, Raspberry Pi.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Arafat, M. Y., & Alam, M. M. (2015). A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server. *International Journal of Computer Applications (0975 – 8887)*, *131*(1), 13–20.

Avinash, V. (2015). International Journal of Advance Engineering and Research HTTP Reverse Proxy Authentication, 162–167.

Bhosale, K. S., Nenova, M., & Iliev, G. (2017). The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer, 136–139.

Chen, Y., Joseph, J., & Pi, A. R. (2015). Pi-IDS : Evaluation of Open-Source Intrusion Detection Systems on Raspberry Pi 2, 165–170.

Choi, D., & Guilley, S. (2004). *Information Security Applications* (Vol. 2908). https://doi.org/10.1007/b95188

Duravkin, I., Loktionova, A., & Carlsson, A. (2014). Method of Slow-Attack Detection, 171–172.

Holz, T. (2003). Department of Computer Science. *Journal of Computational and Applied Mathematics*, *34*(2), N14. https://doi.org/10.1016/s0377-0427(91)90073-s

Ling, A. (2015). [Practical Guide Series Book 3] Adrian Ling - Apache, PHP-FPM & Nginx_ How to Build a Secure, Fast and Powerful Web-Server (2015).

Llaera. (2013). Slowloris. Retrieved July 27, 2019, from https://github.com/llaera/slowloris.pl

Maddux, P. (2016). Introduction to HoneyPy & HoneyDB. Retrieved July 27, 2019, from https://labs.signalsciences.com/honeypots-introduction-honeypy-honeydb

Mahajan, S., Adagale, A. M., & Sahare, C. (2016). Intrusion Detection System Using Raspberry PI Honeypot in Network Security. *International Journal of Scientific and Engineering Research- IJESC*, *6*(3), 2792–2795. https://doi.org/10.4010/2016.651

MazeBolt Security. (2015). Slowloris Attack. Retrieved July 30, 2019, from https://kb.mazebolt.com/knowledgebase/slowloris-attack/

MikroTik. (2011). DDoS Detection and Blocking. Retrieved June 15, 2019, from https://wiki.mikrotik.com/wiki/DDoS_Detection_and_Blocking

MikroTik. (2019a). Manual:IP/Firewall/Filter. Retrieved July 26, 2019, from https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

MikroTik. (2019b). Winbox. Retrieved July 27, 2019, from https://wiki.mikrotik.com/wiki/Manual:Winbox

Mirkovic, J., Dittrich, D., Dietrich, S., & Reihe, P. (2004). Internet Denial of Service Attack and Defense Mechanisms - David Dittrich, Jelena Mirkovic, Peter Reiher, Sven Dietrich - Google Books. Prentice Hall.

Mojidra, N. (2016). Stateful vs. Stateless Firewalls. Retrieved August 19, 2019, from https://www.cybrary.it/0p3n/stateful-vs-stateless-firewalls/

Nallathambi, D. J. (2017). Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks, 8–11.

Odom, W. (2005). *Computer Networking First-Step*. Yogyakarta: Penerbit ANDI Yogyakarta.

Packt. (2014). TCP data communication.

Papadie, R. (2017). Analyzing websites protection mechanisms against DDoS attacks.

Pratama, I. P. A. E. (2015). *Handbook Jaringan Komputer* (Second). Bandung: INFORMATIKA Bandung.

Radware. (2013). *DDoS Survival Handbook*. Radware, Ltd.

Rahmatullah, D. K., Nasution, S. M., Azmi, F., & Server, A. W. (2016). Implementation of Low Interaction Web Server Honeypot Using Cubieboard, 127–131.

Ranjan, S. (2006). DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, *00*(c).

Raspberrypi.org. (2018). Raspberry Pi 3 Model B+. Retrieved from https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

Raspbian. (2012). Raspbian.

Rouse, M. (2014). TCP (Transmission Control Protocol). Retrieved July 17, 2019, from https://searchnetworking.techtarget.com/definition/TCP

Sallowm, H., Assora, M., Alchaita, M., & Aljnidi, M. (2017). A Hybrid Honeypot Scheme for Distributed Denial of Service Attack 4 . Proposed Hybrid Honeypot, *1*(1), 33–39. https://doi.org/10.11648/j.ajece.20170101.15

Shinozaki, T. (2006). Performance Anomalies of Advanced Web Server Architectures in Realistic Environments.

Shorey, T., Subbaiah, D., Goyal, A., & Sakxena, A. (2018). Performance Comparison and Analysis of Slowloris , GoldenEye and Xerxes DDoS Attack Tools. *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 318–322.

Sofana, I. (2017). *Jaringan Komputer Berbasis Mikrotik*. Bandung: INFORMATIKA Bandung.

Stallings, W. (2005). *Wireless Communications and Networks* (Second Edi). New Jersey: Pearson Prentice Hall.

Tambunan, B., Raharjo, W. S., & Purwadi, J. (2017). Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System, (September 2013).

Techopedia. (2016). Tcpdump. Retrieved July 27, 2019, from https://www.techopedia.com/definition/16162/tcpdump

Ubuntu. (2018). Ubuntu. Retrieved July 27, 2019, from https://help.ubuntu.com/lts/installation-guide/s390x/ch01s01.html

Wireshark. (2019a). Tshark. Retrieved July 27, 2019, from https://www.wireshark.org/docs/man-pages/tshark.html

Wireshark. (2019b). Wireshark. Retrieved July 27, 2019, from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

Yu, J., Fang, C., Lu, L., & Li, Z. (2009). A Lightweight Mechanism to Mitigate Application Layer DDoS Attacks, 175–191.