IMPLEMENTASI SISTEM MONITORING SERANGAN SIBER BERBASIS HONEYPOT PADA JARINGAN SMK MUHAMMADIYAH 7 MALANG

Laporan Tugas Akhir

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Khotibul Ummam
201910370311062

Bidang Minat
Sistem Keamanan dan Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2023

LEMBAR PERSETUJUAN

IMPLEMENTASI SISTEM MONITORING SERANGAN SIBER BERBASIS HONEYPOT PADA JARINGAN SMK MUHAMMADIYAH 7 MALANG

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *27 September 2023*

Dosen Pembimbing 1	Dosen Pembimbing 2
Fauzi Dwi Setiawan Sumadi ST., M.CompSc.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 180307061992PNS.	**NIP. 10816120591PNS.**

LEMBAR PENGESAHAN

IMPLEMENTASI SISTEM MONITORING SERANGAN SIBER BERBASIS HONEYPOT PADA JARINGAN SMK MUHAMMADIYAH 7 MALANG

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

khotibul ummam

201910370311062

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji

pada tanggal 27 September 2023

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Wildan Suharso S.Kom., M.Kom	**Briansyah Setio Wiyono S.Kom., M.Kom**
NIP. 10817030596PNS.	**NIP. 190913071987PNS.**

Mengetahui,

Ketua Jurusan Informatika

Ir. Galih Wasis Wicaksono S.kom. M.Cs.

NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : **khotibul ummam**

NIM : **201910370311062**

FAK./JUR. : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"IMPLEMENTASI SISTEM MONITORING SERANGAN SIBER BERBASIS HONEYPOT PADA JARINGAN SMK MUHAMMADIYAH 7 MALANG"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Fauzi Dwi Setiawan Sumadi ST., M.CompSc.

Malang, 27 September 2023
Yang Membuat Pernyataan

khotibul ummam

ABSTRAK

Keamanan pada jaringan komputer adalah hal yang sangat penting. Dengan lemahnya keamanan pada sebuah jaringan komputer dapat membuat informasi yang ada dapat dicuri ataupun di salah gunakan oleh pihak yang tidak bertanggung jawab. Sistem Modern Honey Network ini dapat meminimalisir serangan *cyber* yang terjadi. Pada penelitian ini, jaringan komputer LAB SMK Muhammadiyah 7 Malang dijadikan sebuah studi kasus. Pada skenario yang dilakukan, Sensor Honeypot *Dionaea* dan sensor Honeypot *Suricata dijadikan* sebagai umpan dengan membuka semua port sebagai celah untuk *attacker* melakukan serangan pada Sensor. Hasil serangan yang dilakukan oleh attacker ditampilkan pada web Modern Honey Network yang selanjutnya dilakukan analisis jenis serangan yang terjadi. Data yang diperoleh dari sensor Honeypot Dionaea dan Honeypot Suricata berupa ip penyerang, protocol, port, sensor yang diserang dan juga data md5. Data md5 ini yang akan digunakan untuk dianalisis lebih lanjut menggunakan www.virustotal.com dan www.hybird-analysis.com. Salah satu hasil yang didapat dari beberapat parameter di atas adalah jenis Malware seperti Malware Trojan.Generic dan CVE-2017-06.

Kata Kunci: MHN. Honeypot, Dionaea, Suricata

ABSTRACT

Security on a computer network is very important. With weak security on a computer network, existing information can be stolen or misused by irresponsible parties. This Modern Honey Network system can minimize cyber attacks that occur. In this study, the computer network LAB SMK Muhammadiyah 7 Malang was used as a case study. In the scenario carried out, the Dionaea Honeypot Sensor and the Suricata Honeypot sensor are used as bait by opening all ports as gaps for attackers to carry out attacks on the Sensor. The results of attacks carried out by attackers are displayed on the Modern Honey Network web, which is then analyzed for the types of attacks that occur. The data obtained from the Dionaea Honeypot and Suricata Honeypot sensors are attacker IP, protocol, port, sensor being attacked and also md5 data. This md5 data will be used for further analysis using www.virustotal.com and www.hybird-analysis.com. One of the results obtained from some of the parameters above is the type of Malware such as Trojan.Generic Malware and CVE-2017-06.

Keywords: MHN. Honeypot, Dionaea, Suricata

LEMBAR PERSEMBAHAN

Alhamdulillahi Robbil alamin puji syukur kehadirat Allah SWT atas rahmat dan karunia-Nya, serta shalawat serta salam kepada Nabi kita Nabi Muhammad SAW, sehingga dengan ridho-Nya peneliti dapat menyelesaikan tugas akhir ini. Peneliti menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah Subhanallah Ta'ala yang telah melancarkan, dan memudahkan penyusunan tugas akhir ini.
2. Bapak Ir. Galih Wasis Wicaksono, S.Kom. M.Cs selaku Ketua Jurusan Program Studi Informatika Universitas Muhammadiyah Malang.
3. Bapak Fauzi Dwi Setiawan Sumadi, ST., M.CompSc dan bapak Denar Regata Akbi, S.Kom., M.Kom sekalu pembimbing tugas akhir yang telah mendampingi penulisan ini.
4. Kedua orang tua peneliti, Wahib Hamam dan Yaumi yang selalu memberikan doa dan dukungan selama melakukan penelitian dan penulisan.
5. Rekan terdekat yaitu Baihaqy, Zidane, Wulan, Abizar, Abi yang telah membatu dan mendukung selama penelian ini.
6. Kepada teman kontrakan saya Budiman, Fandy, Mimi, Momo yang telah berjuang bersama-sama selama ini.
7. Kepada teman kelas B yang sudah bersama selama perkuliahan ini.
8. Rekan Club motor Crim yang telah menemani healing dan mendengarkan keluh kesah peneliti selama penelitian dan penulisan ini.

Malang, 6 Juli 2023

Khotibul Ummam

KATA PENGANTAR

Alhamdulillahi Robbil'alamin dengan memanjatkan puji syukur atas kehadirat Allah SWT, serta shalawat serta salam kepada junjungan kita Nabi Muhammad SAW, sehingga dengan ridho dan rahmat-Nya peneliti dapat menyelesaikan tugas akhir yang berjudul: "**IMPLEMENTASI SISTEM MONITORING SERANGAN SIBER BERBASIS HONEYPOT PADA JARINGAN SMK MUHAMMADIYAH 7 MALANG**".

Di dalam tulisan ini telah dijasikan pokok pahasan yang meliputi bahasan tentang konsep Modern Honey Network, Honeypot Dionaea, dan Honeypot Suricata. Selain itu, telah dijelaskan mengenai implementasi Honeypot Dionaea dan Honeypot Suricata pada sistem Ubuntu Server yang di install pada Raspyberry Pi yang mana digunakan sebagai sensor Honeypot. Kemudian pengujian sistem dilakukan menggunakan pengujian manual dengan menyerang sensor Honeypot dengan Hping3 dan juga penyerangan Metasploit.

Peneliti juga menyadari masih banyaknya kekurangan di penulisan Tugas Akhir ini. Maka dari itu penelitis sangat menerima saran dan juga masukan dari pembaca. Semoga Tugas Akhir ini bermanfaat, dan juga tidak hanya bagi penulis tetapi bagi pembaja juga.

Malang, 6 Juli 2023

KHOTIBUL UMMAM

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[1] F. Mulyani and N. Haliza, "Analisis Perkembangan Ilmu Pengetahuan dan Teknologi (Iptek) Dalam Pendidikan," *J. Pendidik. dan Konseling*, vol. 3, no. 1, pp. 101–109, 2021, doi: 10.31004/jpdk.v3i1.1432.

[2] S. Yoga, "Perubahan Sosial Budaya Masyarakat Indonesia Dan Perkembangan Teknologi Komunikasi," *J. Al-Bayan*, vol. 24, no. 1, 2019, doi: 10.22373/albayan.v24i1.3175.

[3] N. Marufah, H. K. Rahmat, and I. D. K. K. Widana, "DEGRADASI MORAL SEBAGAI DAMPAK KEJAHATAN SIBER PADA GENERASI MILLENIAL DI INDONESIA," *Nusant. J. Ilmu Pengetah. Sos.*, vol. 7, no. 1, pp. 191–201, Apr. 2020, doi: 10.31604/JIPS.V7I1.2020.191-201.

[4] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media SosialDigital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," *Techno.Com*, vol. 20, no. 4, pp. 527–539, 2021, doi: 10.33633/tc.v20i4.5170.

[5] S. D. S. K. Virgiawan A. Manoppo, Arie S. M. Lumenta, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[6] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI," *J. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 64–80, 2019, doi: 10.47080/simika.v2i2.606.

[7] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[8] V. N. June, S. Vokasi, U. G. Mada, S. Vokasi, and U. G. Mada, "Journal of Internet and Software Engineering (JISE), Departemen Teknik Elektro dan Informatika , Departemen Teknik Elektro dan Informatika ," vol. 2, no. 1, 2021.

[9] V. Sethia and A. Jeyasekar, "Malware capturing and analysis using dionaea

honeypot," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019–Octob, pp. 0–3, 2019, doi: 10.1109/CCST.2019.8888409.

[10] A. D. Alexander, R. Salkiawat, and J. Warta, "Perancangan Intrusion Detection System Menggunakan Honeypot Pada Universitas Bhayangkara Jakarta Raya," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 33–37, 2021, doi: 10.14421/csecurity.2021.4.1.2379.

[11] R. Dermawati and M. H. Siregar, "Implementasi Honeypot Pada Jaringan Internet Labor," *J. Ilm. Edutic*, vol. 7, no. 1, pp. 20–30, 2020.

[12] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[13] E. Noor and J. C. Chandra, "Implementasi Firewall Pada Smp Yadika 5 Jakarta," *IDEALIS Indones. J. Inf. Syst.*, vol. 3, no. 1, pp. 449–456, 2020, doi: 10.36080/idealis.v3i1.2088.

[14] M. A. R. Dewi, I. A. Putra, and S. Sulistyo, "Design Integrated Honeypot Untuk Deteksi Dan Identifikasi Serangan Siber," *J. It*, vol. 10, no. 3, pp. 239–244, 2020, doi: 10.37639/jti.v10i3.141.

[15] M. F. Razali, G. Muruti, M. N. Razali, N. Jamil, and F. Z. Mansor, "IoT honeypot: A review from researcher's perspective," *2018 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2018*, pp. 93–98, 2019, doi: 10.1109/IISA.2018.8631494.

[16] S. Touch and J. N. Colin, "A Comparison of an Adaptive Self-Guarded Honeypot with Conventional Honeypots," *Appl. Sci.*, vol. 12, no. 10, 2022, doi: 10.3390/app12105224.

[17] Rakhmadhani, Syaifuddin, and Z. Sari, "Integrasi Visualisasi Modern Honey Network (MHN) dengan Splunk," *Sentra 2019*, pp. 167–172, 2019, [Online]. Available: http://research-report.umm.ac.id/index.php/sentra/article/download/3302/3080

[18] D. K. NURILAHI, R. MUNADI, S. SYAHRIAL, and A. BAHRI, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," *ELKOMIKA J. Tek. Energi Elektr. Tek.*

Telekomun. Tek. Elektron., vol. 10, no. 2, p. 309, 2022, doi: 10.26760/elkomika.v10i2.309.

[19] M. Syani, "Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps)," *J. Inkofar*, vol. 1, no. 1, pp. 13–20, 2020, doi: 10.46846/jurnalinkofar.v1i1.155.

[20] N. Azis, R. Darmawan, and J. Hery, "Jurnal information system vol. i no. i april 2021," *J. Inf.*, vol. I, no. I, pp. 6–11, 2021.

[21] Y. A. Utomo, S. J. I. Ismail, and T. Zani, "Membangun Sistem Analisis Malware Pada Aplikasi Android Dengan Metode Reverse Engineering Menggunakan Remnux," *eProceedings …*, vol. 4, no. 3, pp. 2000–2012, 2018, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/7164%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/download/7164/7052

[22] Y. Ilhamdi and Y. N. Kunang, "Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," *Bina Darma Conf. Comput. Sci.*, vol. 3, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

[23] A. Kartono, A. Sularsa, and S. J. I. Ismail, "Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf," *eProceedings …*, vol. 5, no. 1, pp. 146–151, 2019, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/8563%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/viewFile/8563/8431

[24] J. D. Nugraha, A. Budiono, and A. Almaarif, "Analisis Malware Berdasarkan API Call Memory Dengan Metode Deteksi Signature-Based," *J. Rekayasa Sist. Ind.*, vol. 6, no. 2, p. 77, 2019, doi: 10.25124/jrsi.v6i02.351.

[25] A. Kurniawan, "Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based," *J. Telemat.*, vol. 14, no. 1, pp. 9–18, 2019, [Online]. Available: https://journal.ithb.ac.id/telematika/article/view/267%0Ahttps://journal.ithb

.ac.id/telematika/article/download/267/281

[26] A. Reichenbach *et al.*, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” *Prog. Retin. Eye Res.*, vol. 561, no. 3, pp. S2–S3, 2019.

[27] C. R. Sopaheluwakan and D. W. Chandra, “Anti-WebShell PHP Backdoor Scanner pada Linux Server,” *Ilk. J. Ilm.*, vol. 12, no. 2, pp. 143–153, 2020, doi: 10.33096/ilkom.v12i2.596.143-153.

[28] D. A. Daniswara, A. Budiono, A. Almaarif, and S. Kom, “Analisis Deteksi Malicious Activity Menggunakan Metode Analisis Malware Dinamis Berbasis Anomaly Detection Analysis of Malicious Activity Using Anomaly-Based Dynamic Malware Analysis Method,” *2019, e-Proceeding Eng. Vol.6*, vol. 6, no. 2, pp. 7796–7803, 2019.

[29] F. Adnan and Kusnawi, “Analisis Perbandingan Performa Web Server Apache dan Nginx menggunakan Httperf pada VPS dengan Sistem Operasi CentOs,” *Stmik Amikom Yogyakarta*, p. 6, 2016.

[30] A. D. Rochendi, L. M. Silalahi, I. Uli, V. Simanjuntak, and F. Anggini, “Journal of Informatics and Communications Technology (JICT),” vol. 1089, pp. 1–8, 2020.

[31] A. isador Harsapranata, “Analisa DNS Yang Dimanfaatkan Dalam Filterisasi Domain Di Jaringan WAN Menggunakan Open Source,” *J. IKRA-ITH Inform.*, vol. 3, no. 88, pp. 20–29, 2019, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/287

[32] R. Isum, S. Maryati, and B. Tryatmojo, “Raden Isum Suryani Maryati Akurasi Sistem Face Recognition Akurasi Sistem Face Recognition OpenCV Menggunakan Raspberry Pi Dengan Metode Haar Cascade KATA KUNCI Akurasi Face Recognition Raspberry Pi OpenCV Haar Cascade,” no. Cv, p. 12790, 2019.

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **KHOTIBUL UMMAM**

NIM : **201910370311062**

Judul TA : ***Implementasi Sistem Monitoring Serangan Siber Berbasis Honeypot Pada Jaringan SMK Muhammadiyah 7 Malang***

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	10%
2.	Bab 2 – Daftar Pustaka	25 %	5%
3.	Bab 3 – Analisis dan Perancangan	25 %	14%
4.	Bab 4 – Implementasi dan Pengujian	15 %	14%
5.	Bab 5 – Kesimpulan dan Saran	5 %	0%
6.	Makalah Tugas Akhir	20%	16%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS TEKNIK

(.....)