

**PENERAPAN SISTEM KEAMANAN JARINGAN SERVER
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
MENGUNAKAN HONEYPOT**

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar
Sarjana Komputer

**DISUSUN OLEH :
DINAMITA ROMADONI
1911102441097**



**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
SAMARINDA
2023**

**Penerapan Sistem Keamanan Jaringan Server Universitas
Muhammadiyah Kalimantan Timur menggunakan
Honeypot**

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar
Sarjana Komputer

Disusun Oleh :

Dinamita Romadoni

1911102441097



**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
SAMARINDA
2023**

HALAMAN PENGESAHAN

PENERAPAN SISTEM KEAMANAN JARINGAN SERVER UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR MENGGUNAKAN HONEYPOT

DISUSUN OLEH :

DINAMITA ROMADONI

1911102441097

Telah melaksanakan ujian skripsi dan dinyatakan lulus,

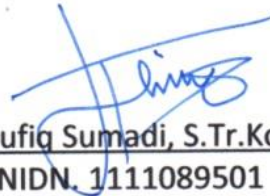
Pada tanggal 4 Juli 2023

Dosen Pembimbing



Faldi, S.Kom., M.Ti
NIDN. 1121079101

Penguji



Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom
NIDN. 1111089501

Dekan



Prof. Ir. Sarjito, MT., Ph.D
NIDN. 0610116204

Ketua Program Studi



Asslia Johar Latipah, M.Cs
NIDN. 1124098902

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Dinamita Romadoni
NIM : 1911102441097
Program Studi : S1 Teknik Informatika
Judul Penelitian : PENERAPAN SISTEM KEAMANAN JARINGAN SERVER
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
MENGUNAKAN HONEYPOT

Menyatakan bahwa penelitian yang saya tulis ini benar-benar hasil karya saya sendiri, bukan merupakan pengambil alihan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri.

Apabila dikemudian hari dapat dibuktikan bahwa terdapat plagiat dalam penelitian ini, maka saya bersedia menerima sanksi sesuai ketentuan perundang-undangan (Permendiknas No.17, tahun 2010).

Samarinda, 4 Juli 2023

Yang Menyatakan,



Dinamita Romadoni

NIM. 1911102441097

PRAKATA



Assalamualaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbil'alam, Puji syukur kita panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul "Penerapan Sistem Keamanan Jaringan Server Universitas Muhammadiyah Kalimantan Timur Menggunakan Honeypot". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana di Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Muhammadiyah Kalimantan Timur.

Pada proses penyusunan skripsi ini, penulis menyampaikan terima kasih kepada beberapa pihak yang ikut mendukung serta membimbing dalam proses penelitian dan penulisan Skripsi hingga selesai tepat waktu. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, kemungkinan akan sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, dalam kesempatan ini saya ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Ibu yang saya cintai Suyati serta kakak-kakak saya Erlinda Yanti dan Erdina Yulianti yang telah memberikan dukungan baik dalam moral maupun materil, cinta dan kasih sayangnya kepada saya, serta doa yang tidak pernah putus dipanjatkan kepada Allah SWT demi kesuksesan saya.
2. Bapak Faldi, S.Kom., M.TI, selaku Dosen Pembimbing yang telah meluangkan waktunya, membimbing, memberi pengarahan dengan kesabarannya, penulis dapat menyelesaikan skripsi ini.
3. Bapak Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom yang telah menjadi penguji dalam seminar proposal penelitian dan seminar hasil penulis.
4. Ibu Asslia Johar Latipah, M.Cs., selaku Ketua Program Studi S1 Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.

5. Bapak Prof.Ir.Sarjito, M.T., Ph.D., selaku Dekan Fakultas Sains & Teknologi Universitas Muhammadiyah Kalimantan Timur.
6. Bapak Prof. Dr. H. Bambang Setiaji, selaku Rektor Universitas Muhammadiyah Kalimantan Timur.
7. Teman-teman seperjuangan KDM skripsi saya Khaerunnisa Marda Tillah, Suci Mawaddah, Ali Jainal Abidin, Trisha NurHalisha dan Putri Dewi Santika yang selalu memberikan semangat dan dukungan kepada saya untuk dapat menyelesaikan skripsi ini.
8. Kekasih saya Muhammad Rizky Prasetyo Hadi yang selalu memberikan dukungan untuk berjuang menyelesaikan skripsi ini hingga tuntas.
9. Serta semua pihak yang tidak dapat disebutkan satu persatu tapi tidak mengurangi sedikit pun rasa terima kasih penulis yang telah memberikan bantuan dan dukungan dalam proses penyusunan skripsi ini.

Semoga Allah SWT memberikan kita semua kebaikan dan Rahmat yang berlimpah. Penulis mengharapkan bahwa skripsi ini dapat memberikan manfaat bagi siapa pun yang membacanya. Penulis menyadari bahwa penulisan ini masih jauh dari sempurna, oleh karena itu, penulis terbuka untuk menerima saran dan kritik yang membangun untuk perbaikan di masa yang akan datang.

Samarinda, 4 Juli 2023



Penulis

ABSTRAK

Keamanan jaringan server merupakan aspek penting dalam memastikan integritas dan ketersediaan sistem informasi. Penelitian ini bertujuan untuk menerapkan keamanan jaringan server Universitas Muhammadiyah Kalimantan Timur menggunakan teknologi *honeypot*. *Honeypot* digunakan untuk menarik perhatian serangan dan memonitor aktifitas yang mencurigakan di jaringan. Metode penelitian yang digunakan adalah NDLC (*Network Development Life Cycle*) meliputi perancangan dan implementasi *honeypot*, serta pengumpulan dan analisis data serangan yang terdeteksi. Hasil penelitian menunjukkan bahwa dengan menggunakan tiga teknik serangan yaitu serangan Slowloris dengan waktu proses *honeypot* 2 detik dan snort 180 detik, serangan GoldenEye dengan waktu proses *honeypot* 2 detik dan snort 180 detik, dan tools LOIC dengan waktu proses snort 180 detik. *Honeypot* tidak dapat mengidentifikasi serangan DDoS karena *honeypot* lebih fokus pada serangan seperti percobaan penetrasi atau aktifitas mencurigakan lainnya.

Kata kunci: Keamanan Jaringan, Honeypot, Slowloris, GoldenEye, Server UMKT.

ABSTRACT

Network server security is an important aspect of ensuring the integrity and availability of information systems. This research aims to implement network server security at Muhammadiyah University of East Kalimantan using honeypot technology. Honeypots are used to attract the attention of attacks and monitor suspicious activities on the network. The research method used is NDLC (Network Development Life Cycle), which includes the design and implementation of honeypots, as well as the collection and analysis of detected attack data. The research results show that by using three attack techniques, namely Slowloris attack with a honeypot processing time of 2 seconds and Snort processing time of 180 seconds, GoldenEye attack with a honeypot processing time of 2 seconds and Snort processing time of 180 seconds, and LOIC tools with a Snort processing time of 180 seconds. Honeypots cannot identify DDoS attacks because they focus more on attacks such as penetration attempts or other suspicious activities.

Keywords: Network security, honeypot, Slowloris, GoldenEye, UMKT server.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
PERNYATAAN KEASLIAN SKRIPSI	iii
PRAKATA	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiv
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan Penelitian.....	2
1.4. Batasan Masalah	2
1.5. Manfaat Penelitian	3
BAB 2 LANDASAN TEORI	4
2.1. Penelitian Terkait.....	4
2.2. Keamanan Jaringan	6
2.3. Klasifikasi Jaringan.....	7
2.3.1. Personal Area Network (PAN).....	8
2.3.2. Local Area Network (LAN).....	8
2.3.3. Metropolitan Area Network (MAN).....	9
2.3.4. Wide Area Network (WAN).....	9
2.3.5. Jaringan Tanpa Kabel	10
2.4. Perangkat Jaringan	11
2.4.1. Ethernet Card	11
2.4.2. Switch	12
2.4.3. Router.....	12

2.4.4.	Modem	12
2.5.	NDLC (Network Development Life Cycle).....	12
2.6.	Firewall	13
2.6.1.	Fungsi Dasar Firewall	13
2.6.2.	Klasifikasi Firewall	14
2.7.	PfSense	14
2.8.	Honeypot	15
2.9.	Alamat IP	16
2.10.	Protokol Jaringan	16
2.10.1.	<i>Transmission Control Protocol/Internet Protocol (TCP/IP)</i>	16
2.10.2.	<i>User Datagram Protocol (UDP)</i>	17
2.10.3.	<i>Internet Control Message Protocol (ICMP)</i>	17
2.11.	Metode Serangan	17
2.11.1.	Slowloris	17
2.11.2.	GoldenEye.....	17
2.11.3.	LOIC (Low Orbit Ion Cannon).....	17
BAB 3	METODOLOGI PENELITIAN	18
3.1.	Subjek Dan Objek Penelitian	18
3.1.1	Subjek Penelitian	18
3.1.2	Objek Penelitian.....	18
3.2.	Metode Penelitian	18
3.2.1	Analisa Kebutuhan	19
3.2.2	Design.....	20
3.2.3	Simulation Prototype	21
3.2.4	Implementasi	22
BAB 4	HASIL DAN PEMBAHASAN.....	23
4.1.	Hasil	23
4.1.1.	Web Server.....	23
4.1.2.	Honeypot.....	23
4.1.2.1.	Konfigurasi Honeypot Pada Pentbox	24

4.1.2.2.	Rules HoneyPot.....	25
4.1.3.	Implementasi Snort Pada PfSense	30
4.1.3.1.	Konfigurasi Snort Pada PfSense	31
4.1.4.	Serangan.....	32
4.1.4.1.	Slowloris.....	32
4.1.4.2.	GoldenEye	34
4.1.4.3.	LOIC (Low Orbit Ion Cannon)	35
4.2.	Pembahasan	36
4.2.1.	Slowloris	36
4.2.2.	GoldenEye	37
4.2.3.	Firewall Snort pada Pfsense	38
4.2.3.1.	Sensitivity Portscan Detection.....	38
4.2.3.2.	Bogon Network	40
4.2.4.	Hasil Data Serangan	42
BAB 5 PENUTUP		44
5.1.	KESIMPULAN.....	44
5.2.	SARAN	44
DAFTAR PUSTAKA		45

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait.....	4
Tabel 3. 1 Perangkat Keras.....	19
Tabel 3. 2 Perangkat Lunak	19
Tabel 4. 1 Rules Ancaman Honeypot	26
Tabel 4. 2 Rules Ancaman Honeypot	27
Tabel 4.3 Analisa Uji Coba Serangan Slowloris	36
Tabel 4. 4 Analisa Uji Coba Serangan GoldenEye	37
Tabel 4. 5 Analisa Alert pada Snort Pfsense.....	41
Tabel 4. 6 Hasil Data Uji Coba Serangan	42

DAFTAR GAMBAR

Gambar 2. 1 Keamanan Jaringan Komputer	6
Gambar 2. 2 Personal Area Network (PAN)	8
Gambar 2. 3 Local Area Network (LAN)	9
Gambar 2. 4 Metropolitan Area Network (WAN)	9
Gambar 2. 5 Wide Area Network (WAN)	10
Gambar 2. 6 Jaringan Tanpa Kabel.....	11
Gambar 2. 7 Perangkat Jaringan	11
Gambar 2. 8 Firewall	13
Gambar 2. 9 Contoh Penempatan Honeypot Pada Server	15
Gambar 2. 10 Contoh Alamat IP	16
Gambar 3. 1 NDLC (Network Development Life Cycle).....	18
Gambar 3. 2 Perancangan Skema Honeypot	20
Gambar 3. 3 Topologi Jaringan	21
Gambar 3. 4 Simulation Prototype	21
Gambar 4. 1 Web Server	23
Gambar 4. 2 Konfigurasi <i>Honeypot</i> Didalam Pentbox	24
Gambar 4. 3 Konfigurasi Pemilihan Port Pada <i>Honeypot</i>	25
Gambar 4. 4 Mengakses IP Honeypot.....	25
Gambar 4. 5 Rules Ancaman Honeypot	26
Gambar 4. 6 Instalasi Snort Pada PfSense	31
Gambar 4. 7 Interface Snort Pada PfSense	31
Gambar 4. 8 Konfigurasi Snort Subscriber Rules	32
Gambar 4. 9 Snort Block Settings.....	32
Gambar 4. 10 Uji Coba Serangan Slowloris.....	33
Gambar 4. 11 Log Serangan Slowloris Pada Honeypot.....	33
Gambar 4. 12 Alert Slowloris pada Snort Pfsense	33
Gambar 4. 13 Uji Coba Serangan GoldenEye.....	34
Gambar 4. 14 Log Serangan GoldenEye Pada Honeypot.....	34
Gambar 4. 15 Alert GoldenEye pada Snort Pfsense	35

Gambar 4. 16 Uji Coba Serangan LOIC.....	35
Gambar 4. 17 Alert LOIC Pada Snort	36
Gambar 4. 18 Sensitivity Low	38
Gambar 4. 19 Sensitivity Medium.....	38
Gambar 4. 20 Alert Sensitivity Medium.....	39
Gambar 4. 21 Sensitivity High	39
Gambar 4. 22 Alert Sensitivity High	39
Gambar 4. 23 Block Bogon Network.....	40
Gambar 4. 24 Alert Bogon Network.....	40
Gambar 4. 25 Blokir Bogon Network	40

DAFTAR LAMPIRAN

- Lampiran 1. Riwayat Hidup
- Lampiran 2. Serangan Menggunakan Slowloris
- Lampiran 3. Serangan menggunakan GoldenEye
- Lampiran 4. Serangan menggunakan LOIC
- Lampiran 5. Hasil Serangan Slowloris
- Lampiran 6. Hasil Serangan GoldenEye
- Lampiran 7. Hasil Serangan LOIC
- Lampiran 8. Hasil Data Pada Tiga Serangan
- Lampiran 9. Surat Izin Pengambilan Data
- Lampiran 10. Surat Izin Penelitian
- Lampiran 11. Surat Balasan Penelitian
- Lampiran 12. Lembar Konsultasi
- Lampiran 13. Uji Plagiasi
- Lampiran 14. Hasil Uji Plagiasi